T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

GAZETECİLİK ANABİLİM DALI

BİLİŞİM BİLİM DALI

KAMUSAL WEB GÜVENLİĞİ

(TÜRKİYEDE KAMU KURUMLARINA VE ÖZEL ŞİRKETLERE AİT WEB SİTELERİNİN WEB GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ÜZERİNE BİR ARAŞTIRMA)

Yüksek Lisans Tezi

MESUT GÜLNAZ

İSTANBUL - 2010

T.C.

MARMARA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

GAZETECİLİK ANABİLİM DALI

BİLİŞİM BİLİM DALI

KAMUSAL WEB GÜVENLİĞİ

(TÜRKİYEDE KAMU KURUMLARINA VE ÖZEL ŞİRKETLERE AİT WEB SİTELERİNİN WEB GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ÜZERİNE BİR ARAŞTIRMA)

Yüksek Lisans Tezi

MESUT GÜLNAZ

Danışman: DOÇ.DR. ERHAN AKYAZI

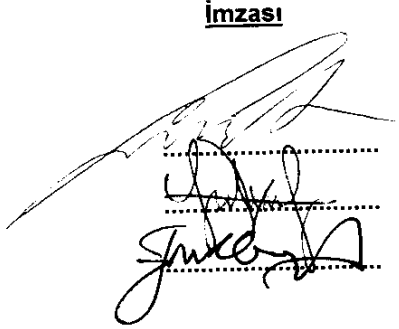
İSTANBUL – 2010

Marmara Üniversitesi
Sosyal Bilimler Enstitüsü Müdürlüğü

Tez Onay Belgesi

İLETİŞİM BİLİMLERİ Anabilim Dalı BİLİŞİM Bilim Dalı Yüksek Lisans öğrencisi MESUT GÜLNAZ nın KAMUSAL WEB GÜVENLİĞİ (TÜRKİYEDE KAMU KURUMLARI VE ÖZEL ŞİRKETLERE AİT WEB SİTELERİNİN WEB GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ ÜZERİNE BİR ARAŞTIRMA) adlı tez çalışması ,Enstitümüz Yönetim Kurulunun 19.07.2010 tarih ve 2010-14/19 sayılı kararıyla oluşturulan jüri tarafından oybirliği/~~oyçokluğu~~ ile Yüksek Lisans Tezi olarak kabul edilmiştir.

	Öğretim Üyesi Adı Soyadı	**İmzası**
Tez Savunma Tarihi	: 02.09.2010	
1) Tez Danışmanı :	**DOÇ. DR. ERHAN AKYAZI**	
2) Jüri Üyesi :	**DOÇ. DR. CEM SEFA SÜTÇÜ**	
3) Jüri Üyesi :	**DOÇ. DR. EMEL KARAYEL BİLBİL**	



TABLO LİSTESİ

Tablo 1 : Saldırı Nedenleri 33

Tablo 2: En Çok Başarılı ve Teyit Edilmiş Tahrifat Yapan Saldırgan Sıralaması 34

Tablo 3 : Aylık Saldırı İstatistikleri 43

Tablo 4 : Bilişim Suçları Tipleri 44

Tablo 5 : Güvenlik Unsurlarına Yapılan Saldırılar, Kullanılan Yaklaşımlar ve Bu Saldırılara Çözümler 52

Tablo 6 : Sosyal Mühendislikte Kullanılan Yöntemler 57

Tablo 7 : PCI DSS Kriter ve Kategorileri 77

Tablo 8 : Web Risk Gruplandırma Seviyeleri, Sebep Ve Etkisine Göre Zayıflık Gruplandırmaları 86

Tablo 9 : Tehdit Sınıflandırması Genel İstatistikleri – Tüm Tarama Sonuçları İçin. 89

Tablo 10 : Risk Gruplandırma Seviyelerine Göre Zayıflık Dağılımı – Tüm Tarama Sonuçları İçin. 92

Tablo 11 : Etki Yerine Göre Zayıflık Dağılımı – Tüm Tarama Sonuçları İçin.92

Tablo 12 : Bulunan Zayıflıkların Bulunma Metotlarına ve Kaynağına Göre Site Başına Oranları 100

Tablo 13 : Erişim Başına Kamu Telekomünikasyon Geliri (USD).....111

Tablo 14 : E-Devlet Modelinin Hukuksal Altyapısı.....114

Tablo 15 : Türkiye'de Mevcut Kamu Internet Uygulamaları 121

Tablo 16 : E-Devlet Projeleri.....122

Tablo 17 : İş ve Hizmetlerde E-Devlet ile Oluşan ve Oluşması Gereken / Beklenen Başkalaşımlar.....128

Tablo 18 : Web Sunucu Türüne ve Yıllara Göre Tahrifata Uğrama İstatistikleri 149

Tablo 19 : İşletim Sistemi Türü ve Yıllara Göre Tahrifata Uğrama İstatistikleri 151

Tablo 20 : Cinsiyet Kriterine Göre Dağılım 159

Tablo 21 : Yaş Kriterine Göre Dağılım 160

Tablo 22 : Öğrenim Durumlarına Göre Dağılım.....161

Tablo 23 : Çalışma Durumlarına Göre Dağılım.....162

Tablo 24 : Kurumların Web Sayfası Olma Durumlarına Göre Dağılım.....163

Tablo 25 : Kurumların Web Sayfalarından Online İşlem Sunma Durumlarına Göre Dağılım 164

Tablo 26 : Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel Sayılarına Göre Dağılım 165

Tablo 27 : Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım..166

Tablo 28 : Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personel Sayılarına Göre Dağılım 167

Tablo 29 : Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım.....168

Tablo 30 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı 171

Tablo 31 : Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı.....172

Tablo 32 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı ...174

Tablo 33 : Web Sitelerinde Bulunan Zfiyetler Dağılımı 176

Tablo 34 : www.turkiye.gov.tr Hakkında Bilgi Sahibi Olma Dağılımı 180

Tablo 35 : www.turkiye.gov.tr Ziyaret Sıklığı Dağılımı.....181

Tablo 36 : Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı.....182

Tablo 37 : Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı 183

Tablo 38 : Kamu Kurumu Sitelerinin İçerik Olarak Beğenilme Dağılımı 184

Tablo 39 : Kamu Kurumu Sitelerinin Tasarım Olarak Beğenilme Dağılımı 184

Tablo 40 : Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Ortalamalı Değerlendirilme Tablosu 187

Tablo 41 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı 189

Tablo 42 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı 190

Tablo 43 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı ..191

Tablo 44 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı 192

Tablo 45 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 194

Tablo 46 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 195

Tablo 47 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 196

Tablo 48 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 197

Tablo 49 : Özel Şirket Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum İle ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 198

Tablo 50 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı.....199

Tablo 51 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 200

Tablo 52 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 201

Tablo 53 : Kamu Kurumlarına Ait Web Sitelerinin
Güvenlik Seviyeleri Dağılımı 202

Tablo 54 : Kamu Kurumlarına Ait Web Sitelerinin Güvenlik
Seviyeleri Genel Olarak Aynı mıdır Dağılımı 204

Tablo 55 : Özel Şirketlere Ait Web Sitelerinin
Güvenlik Durumları Değerlendirme Dağılımı.....205

Tablo 56 : Özel Şirketlere Ait Web Sitelerinin Güvenlik
Seviyeleri Genel Olarak Aynı Mıdır Dağılımı.....206

Tablo 57 : Renk Değerleri Tablosu.....208

Tablo 58 : Kamu Kurumlarına Ait Web Siteleri İle Özel
Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Dağılımı.....248

ŞEKİL LİSTESİ

Şekil 1 : İletişim Temel Kavramları 12

Şekil 2 : İletişim ve İletişim Ortamı 13

Şekil 3 : Veri, Enformasyon, Bilgi ve Bilgelik İlişkisi - 1 21

Şekil 4 : Veri, Enformasyon, Bilgi ve Bilgelik İlişkisi – 2..... 22

Şekil 5 : Bilişim Güvenliği Unsurları 26

Şekil 6 : 1988-2003 Yılları Arasında Bilgisayar Sistemlerine Rapor Edilen Saldırıların Sayısı 31

Şekil 7 : Korsanlık Nedenleri 2002-2004 32

Şekil 8 : Artan Saldırı Sayısı ve Ciddiyet Seviyelerine Karşın Saldırganların Azalan Bilgi Seviyeleri 33

Şekil 9 : Ankete Katılanların Maruz Kaldıkları Atak Türleri 36

Şekil 10 : Ankete Katılanların Maruz Kaldıkları Atak Türleri 37

Şekil 11 : Ankete Katılanların Yaşadığı Maddi Kayıplar..... 38

Şekil 12 : Ankete Katılanların İçerideki Kişiler Nedeniyle Yaşadıkları Kayıplar 39

Şekil 13 : Ankete Katılanların Son Kullanıcı Güvenlik Farkında lığına Ayırdıkları Ödenek Miktarları ve Yeterlilik Durumları 41

Şekil 14 : IT Bütçelerinde Güvenliğe Ayrılan Oranlar 42

Şekil 16 : Korsanlık Hareketi ve Siber Terörizm Genel Analizi..... 45

Şekil 15 : Ankara Emniyet Müdürlüğü Bilişim Suçları İstatistiği 45

Şekil 17 : Kişisel Gizlilik Öğeleri 47

Şekil 18 : Saldırı Tehdit Karakteristikleri 50

Şekil 19 : Saldırıların Sınıflandırılması 53

Şekil 20 : Bilgi ve Bilgisayar Sistemlerine Yapılan Saldırı Türleri 55

Şekil 21 : Bilişim Güvenliği Süreçleri..... 62

Şekil 22 : Sektöre Göre Uygulama Zayıflıkları 74

Şekil 23 : PCI DSS Standartlarına Göre Yapılan İncelemelerde Bu Standartlara Uymayan Sitelerin Tarama Biçimine Göre Dağılımı 79

Şekil 24 : Tarama Şekillerine Göre Web uygulamalarının PCI DSS Standartlarına Uygunluk Oranları 80

Şekil 25 : Web Uygulamalarının PCI DSS Standartlarına Genel Olarak Uygunluk Oranları 81

Şekil 26 : Tarama Çeşidine Göre Zayıflık Bulma İhtimal Oranları 88

Şekil 27 : Zayıflıkların Bulundukları Lokasyonlara Göre Oranları 93

Şekil 28 : En Yaygın Zayıflıklarının Genel Zayıflıklara ve Sitelere Göre Oranları 93

Şekil 29 : Kökenine Göre Zayıflık Bulma Oranları 94

Şekil 30 : Çeşitlerine Göre Zayıflık Yoğunlukları (Genel) 95

Şekil 31 : Derinlemesine ve Özel Taramada Bulunan Zayıflık Oranları 96

Şekil 32 : Derinlemesine ve Özel Taramada Bulunan Zayıflıkların Site ve Toplam Zayıflıklara Oranı 97

Şekil 33 : Bulunan Zayıflıkların Bulunma Metotlarına Göre Dağılım Oranları 98

Şekil 34 : Bulunan Zayıflıkların Bulunma Metotlarına Göre Site Başına Oranları 99

Şekil 35 : OSI Modeli Veri Aktarımı 103

Şekil 36 : Çok Katmanlı Güvenlik Modeli 107

Şekil 37 : Avrupa Topluluğu ve Türkiye'de Telekom Hizmetleri Kesimleri 116

Şekil 38 : E-Devlet'in Unsurları 117

Şekil 39 : Kamu İnternet Sitelerinden Sunulan Bilgi ve Hizmetler (%).....126

Şekil 40 : Ülke Bazında İnternet Kullanım Oranları 131

Şekil 41 : Dünyada e-Devlet Uygulama ve Internet Kullanım Büyüklükleri 132

Şekil 42 : Dünya'da e- Devlet Kullanım Büyüklükleri 132

Şekil 43 : Son Üç Ay İçinde Hane Halkı Bireylerinin
İnternet Kullanma Amaçları (%).....133

Şekil 44 : Kurumsal Web Güvenliği Modeli.....135

Şekil 45 : Örneklemdeki Sitelerin Sayısal Bilgileri 146

Şekil 46 : HTML Doğrulama Hataları - Hata Adedi Ve
Kilobyte Başına Hata Adedinin Dağılımı 147

Şekil 47 : Sayfa Boyutu ve HTML Hataları.....147

Şekil 48 : Sunucu Tercihleri.....148

Şekil 49 : Türkiye Web Sunucusu Tercihleri 149

Şekil 50 : Apache'nin Çalıştırıldığı Platformlar 152

Şekil 51 : Karakter Kodlaması Hataları.....153

Şekil 52 : Uluslar Arası Standartlar Takip Ediliyor mu? (%).....154

Şekil 53 : Kamu İnternet Sitelerinin SSL Sertifikası Sahipliği (%) 154

Şekil 54 : Cinsiyet Kriterine Göre Dağılım Tablosu – Grafiksel Gösterimi..159

Şekil 55 : Yaş Kriterine Göre Dağılım Tablosu – Grafiksel Gösterim.....160

Şekil 56 : Öğrenim Durumuna Göre Dağılım
Tablosu – Grafiksel Gösterim 161

Şekil 57 : Çalışma Durumlarına Göre Dağılım
Tablosu– Grafiksel Gösterim 162

Şekil 58 : Kurumların Web Sayfası Olma Durumlarına
Göre Dağılım Tablosu – Grafiksel Gösterim 163

Şekil 59 : Kurumların Web Sayfalarından Online İşlem
sunma Durumlarına Göre Dağılım Tablosu – Grafiksel Gösterim 164

Şekil 60 : Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel
Sayılarına Göre Dağılım Tablosu – Grafiksel Gösterim 165

Şekil 61 : Web Sayfası Olan Kurumların Web Sayfalarını
Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım
Tablosu – Grafiksel Gösterim 166

Şekil 62 : Web Sayfası Olan Kurumların Web Sayfalarının
Güvenliği İle İlgilenen Personel Sayılarına Göre Dağılım
Tablosu – Grafiksel Gösterim 167

Şekil 63 : Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım Tablosu – Grafiksel Gösterim 169

Şekil 64 : Kurumsal Web Sitesi Olan Kurumların, Sitelerinin Güvenliğini Sağlamak İçin Aldıkları Yöntemler Dağılımı Tablosu – Grafiksel Gösterim 170

Şekil 65 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı 171

Şekil 66 : Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı Tablosu – Grafiksel Gösterim 172

Şekil 67 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı Tablosu – Grafiksel Gösterim 175

Şekil 68 : Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Kamu Kurumlarına Ait Web Siteleri.....177

Şekil 69 : Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Özel Şiretlere Ait Web Siteleri 178

Şekil 70 Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Özelleştiriliş Şiretlere Ait Web Siteleri 178

Şekil 71 : www.turkiye.gov.tr Hakkında Bilgi Sahibi Olma Dağılımı Tablosu – Grafiksel Gösterim 180

Şekil 72 : www.turkiye.gov.tr Ziyaret Sıklığı Dağılımı Tablosu – Grafiksel Gösterim 181

Şekil 73 : Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı Tablosu – Grafiksel Gösterim 182

Şekil 74 : Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı Tablosu – Grafiksel Gösterim 183

Şekil 75 : Kamu Kurumu Sitelerinin İçerik Olarak Beğenilme Dağılımı Tablosu – Grafiksel Gösterim 184

Şekil 76 : Kamu Kurumu Sitelerinin Tasarım Olarak Beğenilme Dağılımı Tablosu – Grafiksel Gösterim 185

Şekil 77 : Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Değerlendirilme Tablosu – Grafiksel Gösterim 186

Şekil 78 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim 189

Şekil 79 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim 190

Şekil 80 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim 191

Şekil 81 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı 192

Şekil 82 : Kamu ve Özel şirket web siteleri kaynaklı maddi ya da manevi zarara uğrama karşılaştırması Dağılımı.....193

Şekil 83 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....194

Şekil 84 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....195

Şekil 85 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....196

Şekil 86 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....197

Şekil 87 : Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum ile ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....198

Şekil 88 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 199

Şekil 89 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterimi 200

Şekil 90 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim.....201

Şekil 91 : Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Dağılımı Tablosu – Grafiksel Gösterim 203

Şekil 92 : Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı Tablosu – Grafiksel Gösterim.....204

Şekil 93 : Özel Şirketlere Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim 205

Şekil 94 : Özel Şirketlere Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı Mıdır Dağılımı Tablosu – Grafiksel Gösterim 206

Şekil 95 : Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim.....248

Şekil 96 : Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri "%" Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim 249

KISALTMALAR

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
ASP	:	Aktif Sunucu Sayfaları (Active Server Pages)
ASV	:	Onaylanmış Tarama Satıcısı (Approved Scanning Vendor)
BDB	:	Berkeley Veri Tabanı (Berkeley DataBase)
BİT	:	Bilgi İletişim Teknolojileri
BTK	:	Bilgi Teknolojileri ve İletişim Kurumu
CD	:	Compact Disk
CDB	:	Daimi Veri Tabanı (Constant Database)
CDMA	:	Kod Bölmeli Çoğul Erişim (Code division multiple access)
CERT/CC	:	Bilgisayar Acil Müdahale Takımı Koordinasyon Merkezi (Computer Emergency Response Team Coordination Center)
CGI	:	Ortak Geçit Arayüsü (Common Gatevay Interface)
CIA	:	Gizlilik (Confidentiality), Bütünlük (Integrity), Erişebilirlik (Availablity)
CLASP	:	Kapsamlı Ve Kolay Uygulama Güvenlik Süreci (Comprehensive, Lightweight Application Security Process)
CMS	:	İçerik Yönetim Sistemi (Content Management Systems)
CPE	:	Müşteri Taraflı Ekipman (Customer Premises Equipmen)
CSI	:	Bilgisayar Suç Enstitüsü (Computer Security Institute)
CSRF	:	Çapraz Site Talep Sahteciliği (Cross Site Request Forgery)
DDOS	:	Distributed Denial of Service

DHTML	:	Değişken Yüksek Metin İşaretleme Dili (Dynamic Hyper Text Markup Language)
DİE	:	Devlet İstatistik Enstitüsü
DNS	:	Alan Adı Sunucusu (Domain Name Server)
DOCTYPE	:	Doküman Türü (Document Type)
DOS	:	Denial Of Service
DPT	:	Devlet Planlama Teşkilatı
DVD	:	Djital Video Disk
DWDM	:	Dense Wavelength Division Multiplexing
EDGE	:	GSM Evrimi ya da Global İletiim Evrimi İçin Geliştirilmiş Data Hızları (Enhanced Data Rates for Global Evolution ya da Global Enhanced Data Rates for GSM Evolution)
EDTR	:	Elektronik Devlet Türkiye
EGM	:	Emniyet Genel Müdürlüğü
FTP	:	Dosya Aktarım Protokolü (File Transfer Protokol)
G.SHDSL	:	Tek Çift Yüksek Hız Sayısal Abone Hattı (Single-Pair High-speed Digital Subscriber Line - (SHDSL))
GPRS	:	Paket Anahtarlamalı Radyo Hizmetler (General Packet Radio Service)
GSM	:	Küresel Mobil İletişim Sistemi (Global System for Mobile Communications)
HIPS	:	Makine Tabanlı Ihlal Engelleme Sistemi (Host-Based Intrusion Prevention System)
HTML	:	Yüksek Metin İşaretleme Dili (Hyper Text Markup Language)
HTTP	:	Yüksek Metin Transfer Protokolü (Hypertext Transfer Protocol)
HTTPS	:	Güvenlik Yüksek Metin Transfer Protokolü (Hypertext Transfer Protocol Secure)
ICQ	:	I Seek You

IIS	:	İnternet Bilgi Sunucusu (Internet Information Server)
IMAP	:	İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol)
INC	:	Limited (İncorporated)
IP	:	İnternet Protokolü (Internet Protocol)
IPS	:	İhlal Engelleme Sistemi (Intrusion Prevention Systems)
ISDN	:	Entegre Servis Sayısal Ağı (Integrated Services Digital Network)
ISO	:	Uluslararası Standardizasyon Organizasyonu (International Organization for Standardization)
IT	:	Bilgi Teknolojileri (Information Technologies)
JCB	:	Japon Kredi Bürosu (Japan Credit Bureau)
KGM	:	Karayolları Genel Müdürlüğü
LDAP	:	Hafif Dizin Erişim Protokolü (Lightweight Directory Access Protocol
LRE	:	Long-Reach Ethernet
M.Ö.	:	Milattan Önce
MEB	:	Milli Eğitim Bakanlığı
MITM	:	Ortadaki Adam (Man In The Middle)
MİT	:	Milli İstihbarat Teşkilatı
MSB	:	Milli Savunma Bakanlığı
MSN	:	Microsoft Ağı (MicroSoft Network)
MSSQL	:	MicroSoft Yapısal Sorgu Dili (MicroSoft Structured Query Language)
MYSQL	:	Benim Yapısal Sorgu Dili (My Structured Query Language)
NMT	:	Kuzeyli Mobil Telefon (Nordic Mobile Telephony)
NVİ	:	Nüfus ve Vatandaşlık İşleri

OECD	:	İktisadi İşbirliği ve Gelişme Teşkilatı (Organisation for Economic Co-operation and Development)
OS	:	İşletim Sistemi (Operating System)
OSI	:	Birbiriyle bağlantılı açık sistemler standardı (Open System Interconnection)
OWASP	:	Açık Web Uygulama Güvenlik Projesi (Open Web Application Security Project)
PCI DSS	:	Ödeme Kart Endüstrisi Veri Güvenlik Standardı (Payment Card Industry Data Security Standard)
PERL	:	Practical Extraction and Report Language
PGSQL	:	Postgre Yapısal Sorgu Dili (Postgre Structured Query Language)
PHP	:	Hypertext PreProcessor
POP	:	Posta Ofisi Protokolü (Post Office Protocol)
POTS	:	Basit Eski Telefon Sistemleri (Plain Old Telephone System)
QSV	:	Kalifiye Tarama Sağlayıcısı (Qualified Scanning Vendor)
RAM	:	Rasgele Erişimli Belleği (Random Access Memory)
RDSL	:	Oran Uyarlanabilir (Rate-adaptive Digital Subscriber Line)
SANS	:	Sistem Yöneticisi, Denetim, Ağ, Güvenlik (SysAdmin, Audit, Network, Security)
SGK	:	Sosyal Güvenlik Kurumu
SMTP	:	Basit E-Posta Gönderme Protokolü (Simple Mail Transfer Protocol)
SNMP	:	Basit Ağ Yönetim Protokolü (Simple Network Management Protokol)
SOAP	:	Basit Nesne Erişim Protokolü (Simple Object Access Protocol)
SPSS	:	Statistical Package for the Social Sciences

SQL	:	Yapısal Sorgu Dili (Structured Query Language)
SSH	:	Güvenli Kabuk (Secure Shell)
SSI	:	Sunucu Taraflı Dahil Etme (Server Side Includes)
SSS	:	Sıkça Sorulan Sorular
TC	:	Türkiye Cumhuriyeti
TCP	:	Transfer Kontrol Protokolü (Transmission Control Protokol)
TELNET	:	Teletype Network
TİB	:	Telekominikasyon İletişim Başkanlığı
TV	:	Televizyon (Television)
UBAK	:	Ulaştırma Bakanlığı
UMTS	:	Evrensel Mobil İletişim Sistemi (Universal Mobile Telecommunications System)
URL	:	Özgün Kaynak Adresi (Uniform Resource Locator)
UTF	:	Unicode Dönüşüm Formatıdır (The Unicode Transformation Format)
VCD	:	Video Compact Disk
VDSL	:	Çok Yüksek Bit Oranlı Sayısal Abone Hattı (Very high bit-rate Digital Subscriber Line)
VOIP	:	Internet Protokolü Üzerinde Ses (Voice Over IP)
W3C	:	Www Konsorsiyumu (World Wide Web Konsorsiyum)
WAF	:	Web Uygulama Güvenlik Duvarı (Web Application Firewall)
WASC	:	Web Uygulama Güvenlik Konsorsiyumu (Web Application Security Consortium)
WDM	:	Wavelength-Division Multiplexing
WİFİ	:	Kablosuz Bağlantı (Wireless fidelity)
WLAN	:	Kablosuz Yerel Alan Ağı (Wireless Local Area Network)
WUGD	:	Web Uygulama Güvenlik Duvarı

XDSL	:	Değişken Sayısal Abone Hattı (Digital Subscriber Line)
XHTML	:	Uzatılabilir Yüksek Metin İşaretleme Dili (EXtensible Hypertext Markup Language)
XML	:	Uzatılabilir İşaretleme Dili (Extensible Markup Language)
XML-RPC	:	Uzatılabilir İşaretleme Dili İle Uzak Yöntem Çağrısı (Extensible Markup Language - Remote Procedure Call)
XSS(CSS)	:	Çapraz Site Betikleme (Cross-site scripting)
YGA	:	Yarı Güvenli Ağ
YGYD	:	Yazılım Geliştirme Yaşam Döngüsü

İÇİNDEKİLER

Sayfa No.

TABLO LİSTESİ I
ŞEKİL LİSTESİ V
KISALTMALAR XI

1. GİRİŞ 1

2. GÜVENLİK VE GÜVENLİK TÜRLERİ 4

2.1. GÜVENLİK KAVRAMI VE UNSURLARI 4
2.1.1. Güvenlik Kavramı 4
2.1.2. Güvenliğin Unsurları 5
2.1.3. Güvenliğin Sınırları 6
2.1.4. Güvenlik ve Tehdit İlişkisi 7
2.2. GÜVENLİK TÜRLERİ VE BİLİŞİM GÜVENLİĞİ 9
2.2.1. Güvenlik Türleri 9
2.2.2. Bilişim ve Bilişim ile İlgili Temel Kavramlar 12
2.2.2.1. Bilişim Güvenliği 22
2.2.2.2. Bilişim Güvenliği Türleri 27
2.2.2.3. Bilişim Güvenliği İhtiyacı 29
2.2.2.4. Bilişim Güvenliğine Yönelik Tehdit ve Saldırılar 48
2.2.2.4.1. Kara Şapkalı Korsan 59
2.2.2.4.2. Beyaz Şapkalı Korsan 60
2.2.2.4.3. Betik Kerataları (Script Kiddy) 60
2.2.2.4.4. "Üzerine Gel ve Tıkla" Korsanlar, Tıklama Korsanları (Click Kiddy) 60
2.2.2.4.5. Sistem Kırıcılar (Cracker) 61
2.2.2.4.6. Web Sitesi Tahrifatçıları 61
2.2.2.4.7. Hacktivizm ve Hacktivistler 62
2.2.2.5. Bilişim Güvenliği Süreçleri 62

3. KAMUSAL WEB GÜVENLİĞİ 65

3.1. KAMU GÜVENLİĞİ VE KAMU KURUMLARINDA GÜVENLİK 65
3.1.1. Kamu ve Kamu Kurumlarında Güvenlik Kavramları 65
3.1.2. Kamu Kurumlarında Bilişim Güvenliği 69
3.2. WEB GÜVENLİĞİ 72
3.2.1. Web Teknolojilerinde Güvenlik İhtiyacı 74
3.2.2. Web Teknolojilerine Yönelik Tehdit ve Saldırılar 82
3.2.3. Web Güvenliği Araçları 101
3.3. ELEKTRONİK DÖNÜŞÜM VE E-DEVLET 108
3.3.1. E-Devlet Ve Web Güvenliği İlişkisi 131
3.3.2. Kamuda Web Güvenliği Standartları (Kurumsal Web Güvenliği Modeli) 135

3.3.3. Kamu Kurumlarında Web Hataları, Güvenlik Açıkları ve Araçları.....146

4. TÜRKİYEDEKİ KAMU KURUMLARINA VE ÖZEL ŞİRKETLERE AİT WEB SİTELERİNİN WEB GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ..... 156

4.1. ARAŞTIRMA AMACI 156
4.2. ARAŞTIRMA METODOLOJİSİ 156
4.3. ARAŞTIRMANIN BULGULARI 159
4.3.1. Tanımsal Bulgular 159
4.3.1.1. Cinsiyet Kriterine Göre Dağılım.....159
4.3.1.2. Yaş Kriterine Göre Dağılım.....160
4.3.1.3. Öğrenim Durumlarına Göre Dağılım.....161
4.3.1.4. Çalışma ve Çalışılan Kurum Türü Durumlarına Göre Dağılım.....162
4.3.1.5. Kurumların Web Sayfası Olma Durumlarına Göre Dağılım.....163
4.3.1.6. Kurumların Web Sayfalarından Online İşlem Sunma Durumlarına Göre Dağılım.....164
4.3.1.7. Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel Sayılarına Göre Dağılım.....165
4.3.1.8. Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım.....166
4.3.1.9. Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği ile İlgilenen Personel Sayılarına Göre Dağılım.....167
4.3.1.10. Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği ile İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım.....168
4.3.1.11. Kurumsal Web Sitesi Olan Kurumların, Sitelerinin Güvenliğini Sağlamak İçin Aldıkları Yöntemler Dağılımı.....170
4.3.1.12. Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı.....171
4.3.1.13. Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı.....172
4.3.1.14. Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı.....174
4.3.1.15. Web Sitelerinde Bulunan Zafiyetler Dağılımı.....176
4.3.1.16. *www.turkiye.gov.tr* Hakkında Bilgi Sahibi Olma Dağılımı.....180
4.3.1.17. *www.turkiye.gov.tr* Ziyaret Sıklığı Dağılımı.....181

4.3.1.18. Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı 182
4.3.1.19. Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı 183
4.3.1.20. Kamu Kurumlarına Ait Web Sitelerinin İçeriksel ve Tasarımsal Beğenilme Dağılımı 184
4.3.1.21. Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Değerlendirilme Dağılımı 186
4.3.1.22. Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı 189
4.3.1.23. Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı 190
4.3.1.24. Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı 191
4.3.1.25. Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı 192
4.3.1.26. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 194
4.3.1.27. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 195
4.3.1.28. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 196
4.3.1.29. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 197
4.3.1.30. Özel Şirket Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 198
4.3.1.31. Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 199

4.3.1.32. Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 200
4.3.1.33. Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum İle İlgili Diğer Özel Şirketlerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı 201
4.3.1.34. Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı 202
4.3.1.35. Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı 204
4.3.1.36. Özel Şirketlere Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı 205
4.3.1.37. Özel Şirketlere Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı 206
4.3.2. Analizler 208
4.3.2.1. Demografik Kriterlere Göre Sorulara Verilen Yanıtlar Analizleri 208
4.3.2.1.1. Cinsiyet Kriterine Göre Sorulara Verilen Yanıtlar Analizi 208
4.3.2.1.2. Öğrenim Durumu Kriterine Göre Sorulara Verilen Yanıtlar Analizi 209
4.3.2.1.3. Kişisel Web Sayfasına Sahip Olma Kriterine Göre Sorulara Verilen Yanıtlar Analizi 210
4.3.2.1.4. Çalışma ve Çalışılan Kurum Kriterine Göre Sorulara Verilen Yanıtlar Analizi 212
4.3.2.2. Kategorik Kriterlere Göre Sorulara Verilen Yanıtlar Analizi 215
4.3.2.2.1. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi 215
4.3.2.2.2. Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi 218
4.3.2.2.3. Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi 219

4.3.2.2.4. Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi 220
4.3.2.2.5. Kurum / Kuruluşun Web Siteleri Üzerinden Online İşlem Sunup Sunmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi.....221
4.3.2.2.6. Kamu Ve Özel Şirket Web Sitelerinin Karşılaştırılmasına Göre Sorulara Verilen Yanıtlar Analizi.....222
4.3.2.2.7. Kurumların, Kurumlarına Ait Web Sitesi İle İlgili Güvenlik Ödenek Kalemi Belirleme Yöntemi Kriterine Göre Sorulara Verilen Yanıtlar Analizi 235
4.3.2.2.8. Herhangi Bir Online Bankacılık Hizmeti Üyeliği Kullanma Ya Da Kullandırma Kriterine Göre Sorulara Verilen Yanıtlar Analizi.....236
4.3.2.3. Ölçekli Soru Türlerine Göre Verilen Yanıtlar Analizi 237
4.3.2.3.1. Yaş Kriterine Göre Sorulara Verilen Yanıtlar Analizi 237
4.3.2.3.2. Web Sayfalarını Hazırlayan ya da Yardımcı Olan Kurum Personel ya da Personellerinin Sayısı Kriterine Göre Sorulara Verilen Yanıtlar Analizi..... 237
4.3.2.3.3. Kurumun Şu Anda Hizmet Veren Web Sayfasının Hazırlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi 238
4.3.2.3.4. Kurumun Şu Anda Hizmet Veren Web Sayfasının Yayınlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi 239
4.3.2.3.5. Kurumun, Kuruma Ait Web Sitesi Güvenliği ile İlgili Ödeneğinin Toplam Ödenek Miktarına Oranına Göre Sorulara Verilen Yanıtlar Analizi..... 241
4.3.2.3.6. Yapılan Araştırma Sonucunda Bulunan Kritik Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi..... 241
4.3.2.3.7. Yapılan Araştırma Sonucunda Bulunan Yüksek Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi..... 242

4.3.2.3.8. Yapılan Araştırma Sonucunda Bulunan Orta Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi.....244
4.3.2.3.9. Yapılan Araştırma Sonucunda Bulunan Düşük Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi.....244
4.3.2.3.10. Yapılan Araştırma Sonucunda Bulunan Bilgisel Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi.....245
4.3.2.3.11. Yapılan Araştırma Sonucunda Bulunan Toplam Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi.....246
4.3.2.3.12. Kamu Kurumları Web Siteleri ve Özel Şirket Web Siteleri Kaynaklı Maddi Zarara Uğrama Oran Karşılaştırması 247
4.3.2.3.13. Kamu Kurumları Web Siteleri ve Özel Şirket Web Siteleri Kaynaklı Manevi Zarara Uğrama Oran Karşılaştırması 247
4.3.2.3.14. Kamu Kurumlarına Ait Web Siteleri ile Özel Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Karşılaştırması.....248
4.3.2.3.15. Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel Sayılarına Göre Sorulara Verilen Yanıtlar Analizi.....250
4.3.2.3.16. Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel ya da Personellerin Bu Konuda Herhangi Bir Sertifikasyona Sahiplik Durumlarına Göre Sorulara Verilen Yanıtlar Analizi 251
4.3.2.4. Anlamsız Etkileşmeler.....252
4.3.2.4.1. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analiz Tablosu – Uygulama Tabanlı IPS.....252
4.3.2.4.2. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Dışarıdan Düzensiz Penetration Hizmeti Alımı.....252
4.3.2.4.3. Kurum / Kuruluşun Web Sitesine Sahip Olup Olmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi.....253

4.3.2.4.4. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Port Tabanlı Güvenlik Duvarı 253
4.3.2.4.5. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Düzenli Olarak Dışarından Alınan Penetration Hizmeti 253
4.3.2.4.6. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Düzensiz Olarak Kurumca Yapılan Güvenlik Taramaları 254
4.3.2.4.7. Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar 254
4.4. ARAŞTIRMA SONUÇLARI 255
5. SONUÇ 263
EKLER 268
EK – 1: Anket Formu 268
EK – 2: Ek Tablolar 276
KAYNAKÇA 324

ÖZET

Bu tez, teknolojik gelişmeler sayesinde oldukça yayılan "internet üzerinden çevrim içi servis verme/alma" hizmeti sunan kamu kurumlarına ve özel şirketlere ait web sitelerinin web güvenlik seviyeleri ve bu seviyelerinin yeterlilik ve etkinlik bakımından araştırılmasını amaçlamaktadır.

Bu kurumların, web sitelerini hazırlatma ve yayınlatma yöntemleri, web sitelerinin güvenliği için ayırdıkları ödenek miktarları, güvenlik personel sayıları, hazırlayan ve güvenliği ile ilgilenen personellerinin sertifikasyon ve yeterlilik seviyeleri gibi kriterlerin, kurumların web sitelerinin güvenliğinin sağlanmasındaki etkinlik seviyelerinin, kamu kurumlarına ait web siteleri ile özel şirketlere ait web siteleri arasında karşılaştırmalı olarak değerlendirilmesi, tezin ana çerçevesini oluşturmaktadır.

Tüm bu kriterlerin sistemlerin ve web sitelerinin güvenliğini baskın olarak etkilemediği, sertifikasyon, güvenlik ödenek miktarları ve diğer etmenlerin sistemlerin güvenliğinde etkin rol oynayamadıkları bu tezde vurgulanan bir argümandır.

Bu tez kapsamında ele alınan web sitelerinin güvenliğini etkileyen tüm etmenler tek taraflı ele alınmamıştır. Kamu kurumları ya da özel şirketlerin, kurum web sistemlerinin güvenliğine verdikleri önem de ele alınmıştır. Bu etmenler birbirini etkileyen ve şekillendiren etkenler olarak değerlendirilmiştir.

Tezde öncelikle kullanılan ana kavramlar hakkında açıklamalar yapılmış, ardından bu kavramların birbirleriyle ilişkilendirmelerine geçilmiştir. Bunu yaparken de, konu ile ilgili çeşitli görüşler ortaya konulmuş, konuya ve bakış açısına en uygun görülenler vurgulanmıştır. Tezin ana yaklaşımını oluştururken, özellikle CSI Computer Crime and Security Survey 2006 ve 2009 raporlarından, "Web Application Security

Statistics 2008", Web Application Security Consortium, 2009 raporundan ve tarafımca yapılan web güvenlik taraması sonuçlarından yararlanılmıştır.

Teorik bölümden sonra, araştırma bölümünde, araştırma anketine cevap veren özel şirket ya da kamu kurum çalışanlarının bağlı oldukları kurumların web siteleri web güvenlik taramasından geçirilmiştir. Bunun için çeşitli güvenlik tarama araçları, yol ve metotları kullanılmıştır. Tüm web sitesi taramalarında aynı metot ve yol ve araçlar aynı ayarlar ile kullanılmıştır. Elde edilen tüm veriler, kurumların güvenlik yeterlilik ve etkinliklerinin belirlenmesi çerçevesinde değerlendirilmiştir.

ABSTRACT

This thesis aims to examine the web security level of web pages and efficiency and sufficiency of this security levels, belonging public institutions and private sector which provides online service input&output trough internet, a tendency becoming widespread thanks to the technological improvements.

Evaluating the level of efficiency to provide security in web pages and criterias such as the method how those institutions prepare and publish their web pages, the way they allocate budget for the security of their web pages and certification and proficiency of the stuff preparing and maintaining the security, in comparison between public institutions and private company web pages makes the main frame of this thesis.

An argument stressed in this thesis is that all those criterias do not predominantly effect the security of web pages and systems, certification, allocation of budget for the security and other elements can not play an active role in the security of the systems.

All the factors effecting the security of the web pages that mentioned in the scope of this thesis are not taken into consideration in a one dimensional aspect. The importance attached by public institutions and private companies to the institution web pages is also taken into consideration. Those factors are evaluated as the factors effecting and shaping each other.

First of all main concepts used in the thesis are explained and then the analogy between concepts are established. When doing this different ideas about the issue are introduced, the most suitable ones to the issue and perspective are stressed. When creating main aproach of the thesis, from result of the web security screening that done by me, and "Web Application Security Statistics 2008", Web Application Security Consortium, 2009 and but especially from the rapport called CSI Computer Crime and Security Survey 2006 and 2009 are benefited.

After the theoretical part, in the research section, web pages of public institutions and private companies whose stuff answered research survey are scanned for security check. To do this various security check tools and methods are used. In all web page security checks same method and tools are used with the same settings. All the data obtained are evaluated in the frame of determining security sufficiency and efficiency of the institutions.

1. GİRİŞ

Son yıllarda, iletişim ve bilişim sistemleri alanındaki hızlı ilerlemeler, teknolojiyi inanılmaz bir cazibe merkezi haline getirmiş ve ülkelerin ve insanların bundan yararlanmak için sabırsızlandıkları bir süreç içerisine girilmiştir. Ancak bu sabırsızlık ve hızlı entegrasyon, sistemlerin teknik alt yapılarının ve bu sistemleri kullanacak, teknik destek verecek ya da kuracak olan kişi ve ya kişilerin yetiştirilmeden bu tam olarak da bilinmeyen bir dünyanın içerisinde tam anlamıyla hazır olunmadan yer almaya neden olmuştur. Gerekli fiziksel, sosyal ve teknik hazırlıklar yapılmadan, hemen acele ile kabul edilerek hayata geçirilen iletişim ve bilişim sistemleri, zaman içerisinde bilinmeyen ve ilk kez karşılaşılan sorun ve problemlerin ortaya çıkmasına, bu sorun ve problemlerin de direkt ya da dolaylı olarak maddi, manevi ve itibar kayıpların yaşanmasına neden oldukları görülmüştür.

Bu durumun birçok örneğini yazılı, görsel ve işitsel medyalarda birçok kez yayınlanan ve yayımlanan örneklerde görmek mümkündür.

18 Haziran 2010 tarihinde, Sansür kararlarını alan ve uygulayan BTK ve TİB ile onların bağlı olduğu Ulaştırma Bakanlığı'nın internet sitelerinin, youtube'a yonelik olarak yürüttükleri 5651 sayılı yasa kapsamındaki hukuksuz çalışmalar sebebi ile hizmet veremez hale getirilmeleri[1],

14 Mayıs 2010'da Trabzon Valiliği'nin resmi internet sitesinin, kendilerini 'El- Kaide Grup' olarak adlandıran kişilerce hacklenerek hizmet veremez hale getirilmesi[2],

12 Şubat 2009 da, Milli Eğitim Bakanlığı'na bağlı 687 bin öğretmenin TC Kimlik numaralarının da yer aldığı tüm bilgilerin Milli Eğitim Bakanlığı'na ait web sitesi üzerinden çalınması ve bir kısmının dosya paylaşım sitesi olan www.rapidshare.com sitesine konması[3],

---

[1] http://www.posta.com.tr/yasam/HaberDetay/Sansur_kararina_hacker_operasyonu.htm?ArticleID=33687 (Haziran 2010)

[2] http://www.hurriyet.com.tr/gundem/14728393.asp (Haziran 2010)

[3] http://www.hurriyet.com.tr/gundem/10988928.asp (Haziran 2010)

2 Mayıs 2008'de Başbakanlığın resmi internet sitesinin "Sen imam atamaya devam et, bu ülke dualarla kurtulur belki" mesajı konularak hacklenmesi ve hizmet veremez hale getirilmesi[4],

14 Haziran 2003'de Cezayir depreminin ardından internet bağlantısında yaşanan sorunlar sebebiyle birçok kullanıcının tepkisini çeken Türk Telekom web sitesinin hacklenmesi ve hizmet veremez hale getirilmesi öne çıkanlar olarak örnek verilebilir.[5]

Yapılan tahrifat işlemleri her ne kadar protesto, kazanç elde etme isteği ve uyarı maksatlı yapılıyor görünseler de, anlaşılmayacak şekilde tahrif edilerek, bilgilerin düzenli olarak tekrar tekrar elde edildiği kamu kurumlarına ait internet sitelerinin de olduğu düşünülmektedir. Bu sorunun sadece kamu kurumlarına ait internet sitelerinde değil özel şirketlere ait internet sitelerinde de olduğu değerlendirilmektedir.

Bu tehlikeler ışığında, yazılı, görsel ve işitsel basın ve yayın organlarında da çıkan haberler, halk arasında yayılan söylentiler ve kişilerin yaşadıkları kişisel tecrübeler nedeniyle insanların bu sitelere olan güvenlerinin farklı derecelerde azaldığı ya da arttığı görülebilmektedir. Bu haberler ya da söylentiler doğru olabileceği gibi farklı amaçlarla da yanlış ya da eksik olabilmektedirler.

Bunların sonucunda, web sitelerinin hazırlanması, yayınlanması, güvenliğinin sağlanması ya da yöneticilik kısımlarından herhangi birinde çalışan kişilerin bu siteler ile ilgili kişisel tecrübeleri sayesinde yaptıkları ya da sorumlu oldukları bu bölümlere farklı ehemmiyet verdikleri ve değişik teknikler kullanarak, hizmet veren sistemlerinin, kendileri üzerinde olumsuz kanaat oluşturan sistemler gibi olmaması, daha iyi ve güvenli olmasını sağladıkları ya da bu alanda çaba gösterdikleri düşünülmektedir.

Bu tezin amacı,öncelikle Türkiye'de ki kamu kurumlarına ve özel şirketlere ait web sitelerinin güvenlik seviyelerinin hazırlanma, yayınlanma, ilgilenen personel sayıları ve yeterlilik seviyeleri, web güvenliklerine ayrılan

[4] http://arsiv.ntvmsnbc.com/news/444885.asp (Haziran 2010)
[5] http://arsiv.ntvmsnbc.com/news/220245.asp (Haziran 2010)

ödenek oranları, web güvenliğinin sağlanması için başvurulan yol ve yöntemlere ve bunların etkinlik ve yeterliliklerine göre karşılaştırmaktır. Ardından yapılan bu karşılaştırma sonucunda elde edilen veriler doğrultusunda, kamu kurumlarının ve özel şirketlerin web sitelerinin güvenliği için yaptıkları çalışmaların ne kadar yeterli ve etkili olduğunun, site güvenliklerinin hangi kriterlere daha çok bağlı hangi kriterlere daha az bağlı ve hangi kriterler ile ilgili olmadığının ortaya çıkarılmasıdır.

Tespit edilen bu kriterlerin kamu kurumları ya da özel şirketlere göre farklılık gösterip göstermediği ve derecesi belirlenmek istenen diğer bir hedeftir.

Tezin ilk kısımlarında, güvenlik, güvenlik ihtiyacı ve türleri anlatılmaya çalışılmış, ardından bir güvenlik türü olan bilişim güvenliği, öncelikle bilişimin temelleri ve gelişim süreci açıklanmaya çalışılarak gereklilikleri belirtilerek teze dahil edilmiştir. Daha sonra bilişim güvenliği türlerine değinilmiş ve bunlardan web güvenliği detaylıca ele alınmıştır. Bu kısımlarda web güvenliğine karşı gerçekleştirilebilecek tehditler ve bunları gerçekleştirebilen kişi ya da kişiler hakkında bilgi verilmeye çalışılmıştır. Bir sonraki kısımda, kamu kurumlarına ait web sitelerinin genel karakteristikleri ve hataları hakkında istatistiki bilgilere değinilmeye çalışılmış ve dünyadaki genel durumlar ile karşılaştırılmıştır. Yine bu kısımda, kamu kurumlarında web hizmetlerinin yaygınlaşması için devlet tarafından yapılan teşvikler ve standartlaştırma çalışmalarından bahsedilmiştir. Bu standartlaştırma çalışmaları içerisinde yer alan kurumların web sitelerinin güvenliklerinin sağlanması amacıyla çıkartılan kanun, yönetmelik ve yönergelerden bahsedilmiştir.

Tezin son kısmı olan araştırma kısmında ise, hazırlanan 34 soruluk anket formu toplam 72 kişiye doldurtularak elde edilen veriler, yapılan web güvenlik taraması sonuçları ile eşleştirilerek ortaya çıkarılan yeni veriler ışığında analiz ve dağılım çalışmaları yapılmıştır. Bu çalışmalar, yukarıda bahsedilen tüm kriterlerin tespiti ve birbirleri ile etkileşim derecelerinin ortaya çıkarılmasına yönelik gerçekleştirilmeye çalışılmıştır.

2. GÜVENLİK ve GÜVENLİK TÜRLERİ

2.1. Güvenlik Kavramı ve Unsurları

2.1.1. Güvenlik Kavramı

Güvenlik, canlı varlıkların varoluşlarından bu yana yaşama, onların içgüdüsünün ilk basamaklarında yer alan ve ihtiyaç duyulan en önemli gereksinimdir. Güvenlik kavramı ise, tüm canlı ve cansız varlıklar için çok önemli bir unsurdur. Cansız varlıkların güvenliği, ona değer veren ya da ona ihtiyacı olan canlı varlıklar için önemlidir. Kendini güvende hissetmeyen yani güvenlik ihtiyacı karşılanmamış canlılar, diğer alt ihtiyaçlar için herhangi bir atılımda bulunmayacak ya da onlara gerek duymayacaklardır.

İnsanoğlu için güvenlik, birey ya da toplumun huzur içinde yaşaması, iç ve dış tehditlere karşı korunabilme yeteneği ve kapasitesidir. Bu ihtiyacı giderilen ve güvenliği sağlanan toplum ise güvenlikli toplum, birey ise güvenli bireydir.[6]

Toplum ve insan için güvenlik ise, korku, çekinme ve ya kuşku duymadan inanma ve bağlanma duygusu, itimat demektir.[7]

Güvenlik farklı bir açıdan ele alındığında, saklanması ya da korunması gereken herhangi bir değerin kendisini ya da önemli niteliklerini korumak için uygulanan bir dizi işlem ve süreçtir denilebilir. Bu işlem ya da süreci gerçekleştirmenin gereklilikleri donanım ya da hareket gibi fiziksel olabilmesinin yanında, yazılım ya da bilgi gibi mantıksal da olabilmektedir. Korunmak istenen değerin güvenliği, belirtilen değerin ulaşılabilirliğini, inanılırlığını, kararlılığını ve en önemlisi gizliliğini doğrudan etkileyen bir faktördür.[8]

---

[6] "**Güvenlik Nedir?**", http://www.mscguvenlik.com/guvenlik_nedir.htm (Eylül 2009)
[7] http://www.tdk.org.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&KELIME=güven (Ocak 2010)
[8] "**Güvenlik Nedir?**", http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.html (Şubat 2009)

2.1.2. Güvenliğin Unsurları

Bu noktada güvenlik unsurlarına değinmek gerekirse bu unsurlar;

Kıymet**,** Korunması gereken her şeydir.

Açıklık**,** Bir kıymeti tehditlere karşı korumasız hale getiren kusurlardır.

Tehdit**,** Bir kıymetteki açıklıkları kullanarak kıymete kısmen ya da tamamen zarar veren etkenlerdir.

Tedbir**,** Bir kıymette bulunan açıklıkları kullanan tehditlerin verdiği zararı sıfırlamak ya da azaltmak amacıyla alınan karşı önlemlerdir.

Risk**,** Zarara yol açan ya da zarar verme kapasitesi olandır."[9]

Güvenlik, güvenliği sağlayan ve sağlananlar tarafından yerine getirilen bir iş ve süreç olduğundan, güvenlikten herkes sorumludur denilebilir. Ancak alınması gereken güvenlik tedbirlerinin belirlenmesi, alt yapının hazırlanması için ödeneğin temini ve uygulanmasından üst düzey görevliler sorumlu olduğundan, ilk başta onlar, ardından da bu önlemleri hayata geçirecek olan teknik güvenlik ekibi, en son olarak da güvenlikleri alınan kişilerin bu durumu korumaları gerektiğinden, güvenlikleri alınan kişiler güvenlikten sorumludurlar.

Tüm uğraşlara rağmen, hiçbir sistemin %100 güvenli olmayacağı unutulmamalıdır. En büyük güvenlik sistemlerinin ise unutulan en ufacık bir zafiyetten dolayı zarar gördükleri unutulmamalıdır. Bilgisayar sistemleri güvenliği ile ilgili olarak her zaman kullanılan "en güvenli bilgisayar, fişi çekik bilgisayardır" sözünün bile yanlış olduğu artık aşikârdır. Zamanların en ünlü üstadı Kevin Mitnick, sosyal mühendislik sayesinde, fişi çekik bilgisayarların fişlerini taktırarak hatta bu bilgisayarları tamire geldiğini belirterek, bu bilgisayarlardan ve bu bilgisayarları ele geçirerek diğer bilgisayarlardan bilgileri çalabilmiştir. O nedenle amaç güvenliği her zaman

[9] Bilge KARABACAK, "**Risk Analizi**", http://www.enderunix.org/docs/disabled/risk_analizi/ (Eylül 2009)

en üst seviyeye getirmek ve orada tutmaya çalışmak olmalıdır. Güvenliği sağlamak için, kullanılan güvenlik politikalarının ve sistemlerinin kolay ve kullanıcı dostu olması gerekmektedir. Bir sistem ya da politika ne kadar karmaşık ve kullanımı zor ise o sistem o derece güvensizdir. Bu nedenle, güvenliğin hiçbir zaman %100 olmayacağı, bir süreç olduğu ve sürekliliğinin sağlanmaya çalışılmasının gerektiği unutulmamalı ve buna göre hareket edilmelidir.[10]

2.1.3. Güvenliğin Sınırları

Kullanıcılar ve sistemler için bilgi güvenliğinin sınırları; tarafların kendilerini ve sistemlerini güven içinde hissetmeleri için gerekli ve düzenleyici politikalar doğrultusunda, güvenin değeri doğrultusunda ve hukuki zorunluluklar çerçevesinde belirlenir.

Güvenliğin sınırları, riskin değerini aşmamalıdır. Bu nedenle de öncelikle risk analizi yapılmalıdır. Risk analizi hesaplamaları için aşağıdaki adımlar izlenmelidir.

- Korunması gereken bilgi ya da varlıkların belirlenmesi;
- Bu varlıkların kuruluşlar açısından ne kadar değerli olduğunun saptanması;
- Bu varlıkların başına gelebilecek bilinen ve muhtemel tehditlerden hangilerinin önlenmeye çalışılacağının ortaya koyulması;
- Muhtemel kayıpların nasıl cereyan edebileceğinin araştırılması;
- Her bir varlığın maruz kalabileceği muhtemel tehditlerin boyutlarının tanımlanması;
- Bu varlıklarda gerçekleşebilecek zararların boyutlarını ve ihtimallerini düşürmek için ilk planda yapılabileceklerin incelenmesi ve ileriye yönelik tehditleri asgari seviyede tutmak için atılması gereken adımların planlanması.[11]

[10] "**Güvenlik Nedir?**"http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.html (Şubat 2009)
[11] Gürol CANBEK, Şeref SAĞIROĞLU, "*A Review on Information, Information Security and Security Processes*", **Politeknik Dergisi,** Cilt:9, Sayı:3, S.170, 2006 http://www.politeknik.gazi.edu.tr/index-s.php?q=9&s=32 (Kasım 2009)

2.1.4. Güvenlik ve Tehdit İlişkisi

- **Güvenlik İhtiyacı**

ABD'li psikolog Abraham Maslow tarafından 1943 yılında yayınlanan ve zamanla geliştirilen insan psikolojisi teorisi olan ve Maslow teorisi ya da Maslow piramidi olarak adlandırılan teoride, insanların belirli kategorilerdeki ihtiyaçları ve bu ihtiyaçların öncelikleri belirtilmiştir. Bu teoride canlıların ihtiyaçlarının karşılanmasıyla, kendi içlerinde bir hiyerarşi oluşturan daha 'üst ihtiyaçlar'ı tatmin etme arayışına girdikleri ve bireyin kişilik gelişiminin, o an için baskın olan ihtiyaç kategorisinin niteliği tarafından belirlendiği anlatılmaktadır. Yine bu teoriye göre, birey, bir kategorideki ihtiyaçları tam olarak gideremeden bir üst düzeydeki ihtiyaçlar kategorisine geçemeyeceği de ifade edilmektedir. Örneğin, günlük olarak anca karnını doyurabilen fakat güvenlik içinde bulunmayan, kendini sürekli olarak olası bir tehdit altında algılayan bir insanın, kültür, saygınlık, sanat gibi gereksinimleri yoktur. Kişi ancak ve ancak güvenlik ihtiyacının karşılanmasından sonra bir üst seviyedeki diğer gereksinimlerini gidermeye yönelecektir.

Maslow, gereksinimleri öncelik sırasına göre şu şekilde kategorize etmektedir.

- Fizyolojik gereksinimler
- Güvenlik gereksinimi
- Ait olma gereksinimi
- Sevgi, sevecenlik gereksinimi
- Saygınlık gereksinimi
- Kendini gerçekleştirme gereksinimi[12]

Abraham Maslow'un belirttiği ihtiyaçlar piramidinde güvenlik ihtiyacı, yaşamak için zorunlu fizyolojik ihtiyaçlardan sonra ikinci sırada yer almaktadır. İnsanlar her ortamda kendini güvende hissetmek isterler. Dolayısıyla insanların huzur ve güvenliğinin sağlanması, sağlanan bu güven ortamının devam ettirilmesi düşüncesi tarih boyunca, vazgeçilmez bir olgu olarak devletlerin karşısına çıkmıştır. Her devlet, varlığını sürdürüp iç güvenliğini sağlayacak kanunlara, onları uygulayacak ve uygulatacak kuvvete ihtiyaç duymuştur.

[12] George BOEREE, "**Maslow**", http://webspace.ship.edu/cgboer/maslow.html (Ekim 2009)

Güvenliğin unsurları ışığında güvenlik ihtiyacı, kıymetlerin zarar görmemiş ve görmeyecek şekilde olması ve kalması ihtiyacından ortaya çıkmakta denilebilir. Kıymete zarar vererek güveni ve güvenliği zedeleyebilecek başlıca tehditler aşağıda belirtilmeye çalışılmıştır.

- Doğal afetler
- İnsan yapımı afetler
- Direkt saldırılar
- Direkt olmayan saldırılar
- Kazalar[13]

Güvenliğin sağlanması hizmetinin, toplu olarak yaşanan bir hayata bakıldığı zaman, kamu düzeninin sağlanması için vazgeçilmez ve birinci derecede bir şart olduğu görülür. Bu nedenle, yeme, içme, nefes alma ve benzeri diğer fiziksel gereksinimlerin karşılanmasının ardından yapılacak ilk iş kişilerin can ve mal güvenliklerinin sağlanmasıdır.

Kişilerin, kendileri ve çevrelerindekilerin güvenlikleri için aldıkları kişisel güvenlik tedbirlerinin yanında, devletlerin de başlıca görevleri, halkının güvenliğini sağlamaktır. Devletler bunu sağlayamadıklarında, devletlerin eğitim, sağlık, sanat, araştırma geliştirme gibi diğer hizmetlerinin bir anlamı olmayacaktır. Bunu devlet adına kolluk kuvvetleri yerine getirir. Ancak kolluk kuvvetlerinin de, bu görevi yerine getirebilmeleri için can ve mal güvenliğine ihtiyaçları vardır. O nedenle öncelikle kamu güvenliğini sağlayacak olan kişilerin can ve mal güvenliklerinin sağlanması önemlidir. Kamu kurumlarının yeterli olmadığı ya da ilgi alanına girmeyen özel kurum, iş ya da bölgelerin de güvenlik ihtiyacı vardır. Bu gibi yerlerin güvenliğini kolluk kuvvetleri değil, özel polis teşkilatı da denilen, özel güvenlik kurum, kuruluş ya da şirketleri sağlamaktadır. Ancak bu gibi oluşumların da öncelikle can ve mal güvenliğine ihtiyaçlarının olduğu göz ardı edilmemelidir.[14]

---

[13] "**Güvenlik Nedir?**"http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.html (Şubat 2009)

[14] Adem KIZILKAYA, Nevzat SÖNMEZ, "**Geçmişten Günümüze Güvenlik İhtiyacı Ve Türk Polis Teşkilatı"**, http://www.caginpolisi.com.tr/18/19-20-21-22-23.htm (Mayıs 2010)

2.2. Güvenlik Türleri ve Bilişim Güvenliği

2.2.1. Güvenlik Türleri

Bir bakış açısına göre güvenlik, tehlikelere karşı koruma derecesine ve riskin niteliğine göre sınıflandırılır.

- Uygulama güvenliği
- Bilgisayar güvenliği
- Veri güvenliği
- Bilgi güvenliği
- Ağ güvenliği

Farklı diğer yaklaşımlara göre güvenlik türleri ise aşağıda belirtilmeye çalışılmıştır.[15]

Fiziksel Güvenlik Türleri

- Havaalanı güvenlik
- Port güvenliği / Tedarik zinciri güvenlik
- Gıda güvenliği
- Ev güvenlik
- Hastane güvenlik
- Fiziksel güvenlik
- Alışveriş merkezi güvenliği
- Altyapı güvenliği

Siyasal Güvenlik Türleri

- Vatan Toprğı Güvenliği
- Insan güvenliği
- Uluslararası güvenlik
- Ulusal güvenlik
- Genel güvenlik

[15] http://www.vik2.com/guvenlik/ (Ocak 2010)

Para ve Gayri Menkul Güvenliği

- Finansal güvenlik

Diğer bir sınıflandırma ise korunan kıymete ve kıymetin bulunduğu ortama göre yapılmıştır.[16]

Fiziki Güvenlik: Yetkililerin haricinde diğer kişi ya da kişilerin, bir tesise, kaynağa veya fiziksel bilgiye ulaşmalarını engellemek veya caydırmak amaçlı alınan önlemlerdir.

Bilgi Güvenliği: Yazılı, sözlü veya elektronik ortamdaki bilgilerin sadece yetkililer tarafından izin verilen erişime açılması, diğer erişimlere kapanması ve doğru bilginin, doğru zamanda, doğru kişiye ulaştırılmasıyla ilgilenir.

Bilişim Güvenliği: Bilişim aygıtlarının kullanımından doğabilecek riskleri ve tehlikeler ile ilgilenmektedir.

Kişi Güvenliği: Ulusal güvenlik, Egemenlik ve İnsan hakları alanında ortaya çıkan kavramsal bir sorunu belirten uluslararası ilişkiler terimidir.

Gıda Güvenliği: İki kavramı belirtmektedir.

- Uluslararası ilişkiler alanında insanların açlık veya kıtlık durumunda bulunmamasını belirtir.
- Yiyeceklerin üretim aşamasından son tüketiciye ulaşmasına kadar geçen sürede gıdanın insan sağlığına uygun şartlarda üretim, depolama, paketleme ve taşımasının yapılmasıdır.

Güvenlik sosyal açıdan değerlendirildiğinde farklı türlere de ayrılabilmektedir.[17]

Personel Güvenliği: Birey güvenliği olarak tanımlanabilinir. Ek olarak, personel güvenliği fiziki olarak alınması gereken tedbirler ile psikolojik olarak rahatlatıcı önleyici tedbirlerden oluşan bir bütündür. Personel güvenliği ayrıca bireyin kendisi tarafından alınması gereken

[16] "Güvenlik", http://tr.wikipedia.org/wiki/G%C3%BCvenlik (Kasım 2009)
[17] "Güvenlik Ve Tehdit Kavramının Evrimi Global Güvenlik İçinde Ulusal Güvenlik Perspektifi", http://www.turksae.com/sql_file/298.pdf (Mayıs 2009)

tedbirlerin yanı sıra kamu otoritesinin sunmakla mükellef olduğu bir kamu hizmeti olarak ta ortaya çıkmaktadır.

Sektör Güvenliği: Grup, örgüt, şirket veya organizasyonların korunma, koruma ve devamlılığı sağlayacak ilgili önleyici tedbirleri alma işlemlerinin gerçekleştirildiği süreçtir. Kendi içerisinde, ünite güvenliği, toplumsal güvenlik, fiziki güvenlik, kurumsal güvenlik ve alan güvenliği gibi kısımlara ayrılmaktadır.

Kamu Güvenliği: Vatandaş ve kamu üst sınırı arasında kalan ve kamusal alan ile özel alanın toplamından oluşan bir çerçeveyi, tanımlanmış kurallar altında koruma ve kamunun kendisine ait korunma faaliyetlerini de içeren süreç kamu güvenliği kavramıdır. Bu konuya Kamu Güvenliği Bölümü altında daha detaylı olarak değinilecektir.

Ulusal Güvenlik: Yukarıda anılan faaliyetlerin yürütülmesi başta olmak üzere, alınması gereken tedbirlerin ve devletin, siyasi, sosyal, dış politik, ekonomik ve askeri çıkarlarının korunması ve geliştirilmesi için stratejik seviyede yapılan çalışmalar bütünüdür.[18]

Konumuz kapsamında bilgi ve bilişim güvenliğinin önemine ve türlerine değinmek gerekirse;

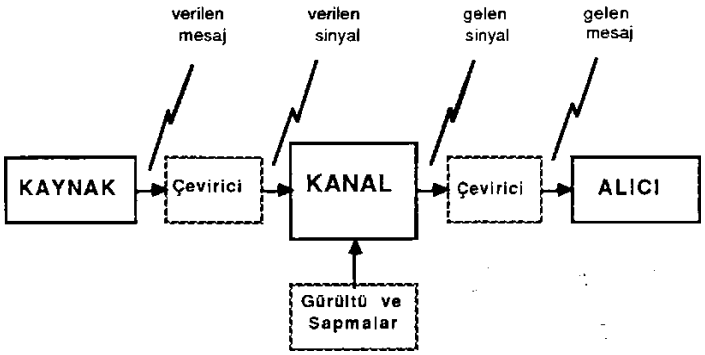
[18] Prof. Dr. Kerem ALKIN, Dr. Can Fuat GÜRLESEL "*Dünya Ekonomisine Yönelik Global Tehditler; Dünyada Güvenlik Ve Tehdit Kavramının Evrimi Global Güvenlik İçinde Ulusal Güvenlik Perspektifi*", **İstanbul Ticaret Üniversitesi Dergisi**, Mayıs 2006, S.14 http://www.iticu.edu.tr/kutuphane/dergi/d6/M00074.pdf (Kasım 2009)

2.2.2. Bilişim ve Bilişim ile İlgili Temel Kavramlar

- **İletişim**

İletişim, verinin, alınması, verilmesi, sevk ve depo edilmesidir.[19]

İletişimin temel kavramları Şekil 1 ve Şekil 2'de gösterilmeye çalışılmıştır.



Şekil 1 : İletişim Temel Kavramları

Kaynak: Orkan, S.4

- **İletişimin Temel Kavramları Ve Unsurları**

Kaynak: iletinin hazırlandığı çıkış noktasıdır.

İleti: kaynak tarafından kodlanmış ve sembollere çevrilmiş mesajdır.

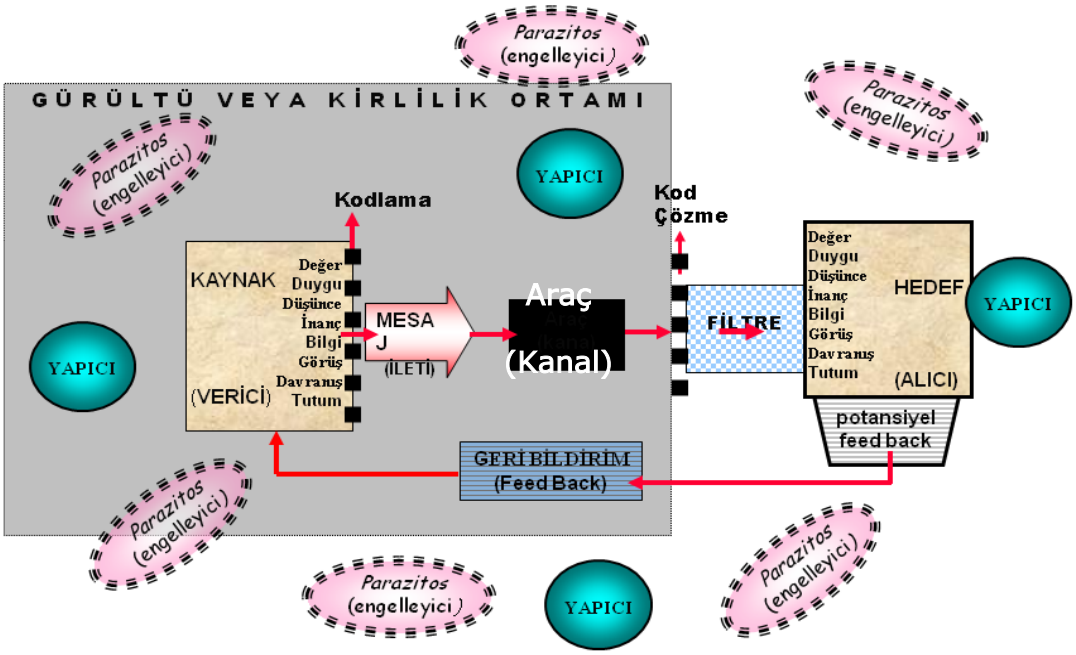
Araç (kanal)**:** iletinin alıcıya ulaşmasını sağlayan ortam, yöntem ve/veya tekniklerdir.

Hedef: kaynaktan gelen iletileri alan veya algılayan, yorumlayan, kişi veya kişilerdir.[20]

---

[19] Orkan A.L., "***Bilişim Teorisi, Temel Kavramlar***", M.Ü.T.E.F.M.B. İstanbul, 1993, S. 3

[20] Ahmet FİDAN, "**Etkili İletişim Sistemleri İletişim Ve Engelleri Sunusu**" http://www.ahmetfidan.com/dersnotlari/digerprogramlar/etkili_iletisim_teknikleri_iletisim_ve_engelleri_dr_ahmet_fidan.ppt S.2 (Kasım 2009)



Şekil 2 : İletişim ve İletişim Ortamı

Kaynak: Fidan, S.2

- **İletişim Sürecinin Temel Kavram Ve Unsurları**

Kodlama: kaynağın iletiyi, anlaşılması veya algılanması için görsel veya işitsel forma sokmasıdır.

Kod çözme: iletinin kaynak tarafından algılanması filtrelenmesidir.

Geri bildirim: filtre edilen iletinin kaynak tarafından cevaplanmasıdır.

Potansiyel geri bildirim: Algılanan iletinin herhangi bir zamanda iletilmek üzere saklanmasıdır.

Engelleyici (parazitoslar): iletinin algılanmasını zorlaştıran ortamdır.

Yapıcı: İletinin algılanmasını kolaylaştıran destekleyen ortamdır.[21]

[21] Fidan, S.4 (Kasım 2009)

- **İletişimin Engelleri**

Psikolojik: verici ve alıcının görüş çerçeveleri, duygu ve heyecanları, saplantılar, ön yargılardır.

Semantik: konuşma ve yazı dilindeki fark ve anlaşmazlıklardır.

Statü: verici ve alıcının akademik ve mesleki gelişme farklılıklarıdır.

Korunma: savunma mekanizmalarıdır.

Alan: iletişim birimleri arasındaki uzaklıktır.

Hiyerarşi: ast-üst çatışmaları, yetkinin az verilmesi, düzensiz haber akışıdır.

Uyutma: karar sürecine katılmayanların emirleri savsaklamasıdır.

Sınırlama: örgütün konumu gereği bazı iletilerin gizli kalmasıdır.[22]

- **Bilişim**

Bilişime giriş yapmadan önce teknoloji teriminin açıklanması uygun olacaktır. Teknoloji "*(technoslogos), techne; yapmak ve logos; bilmek anlamına gelmektedir. İnsanoğlunun gereklerine uygun yardımcı alet ve edevatın yapılması ya da üretilmesi için gerekli bilgi ve yetenektir.*"[23] Diğer bir ifade ile teknoloji, "*insanın bilimi kullanarak doğaya üstünlük kurmak için tasarladığı rasyonel bir disiplin ve somut ve deneysel anlamda temel olarak teknik yönden yeterli küçük bir grubun örgütlü bir hiyerarşi yardımıyla bütünün geri kalanı (insanlar, olaylar, makineler vb.) üzerinde denetimi sağlamasıdır.*"[24]

Bilişim ise, bilgi teknolojileri ve iletişim teknolojileri kavramlarının birleşmesinden ortaya çıkmıştır. Diğer bir deyişle bilişi, "*insanoğlunun teknik, ekonomik ve sosyal alanlardaki iletişiminde kullandığı ve bilimin*

[22] A.G.E., S.5
[23] **"Teknoloji Nedir?",** http://www.msxlabs.org/forum/muhendislik-bilimleri/19503-teknoloji-nedir.html (Mart 2009)
[24] **"Teknoloji Nedir?",** http://www.teknolojide.com/teknoloji-nedir.aspx (Nisan 2009)

dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve ussal biçimde işlenmesi bilimi"[25] dir. Yine farklı bir deyişle bilişim, "*bilgi ve bilginin otomatik olarak işlenmesiyle ilgilenen yapısal bir bilim dalıdır.*"[26]

Bilgilerin saklanmasını, değerlendirilmesini, korunmasını ve iletilmesini sağlayan donanım ve yazılımlar bilgi teknolojilerini, bu bilgilerin ortak ve güvenli şekilde paylaşılmasını sağlayan teknolojiler ise iletişim teknolojilerini oluşturmaktadır.

Bilişim genel itibariyle ele alındığında, bilginin toplanmasını, bu bilginin işlenmesini, saklanmasını ve gerektiğinde herhangi bir yere iletilmesi ya da herhangi bir yerden bu bilgiye erişilmesini elektronik, optik vb. tekniklerle otomatik olarak sağlayan teknolojiler bütünü olarak tanımlanabilmektedir.

Bilişim, internetin kullanımında, bilgisayarların dünya çapında yaygınlaşmasında, firmaların iletişiminde, lojistikte, medyada, ev yaşamında ve daha birçok başka alanda devrim niteliğinde değişimler yaratmıştır.

Özet olarak Bilişim sistemlerinde kullanılan ve değerli olan veri; "*ham olgular, rakamlar ve detayları, bilişim, bu verilerin yararlı, anlamlı ve organize edilmiş halini, bilgi ise bir bilişim sayesinde bu bilişimin en uygun şekilde nasıl kullanılabileceğinin anlaşılabilmesi demektir.*"[27] denilebilir. Çünkü bilişimin bir numaralı ilgi alanı her türlü "bilgi" ve onun her türlü paylaşımı ve korunmasıdır.[28]

---

[25] **"Veri, Bilgi Ve Bilişim",** http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html (Eylül 2009)
[26] A.G.E. Par. 2
[27] A.G.E. Par. 3
[28] Gürol CANBEK, Şeref SAĞIROĞLU, **Bilgi Ve Bilgisayar Güvenliği: Casus Yazılımlar Ve Korunma Yöntemleri**, Grafiker, Ankara, 2006, S.73

- **Veri**

İşlenmemiş ham bilgi de denilen veri İngilizce karşılığı "data" olan ve "datum" sözcüğünün çoğulu olan kavramdır. Almanca dilindeki karşılığı olan "Daten" kelimeleri ise Latince kökenlerinde "verilmiş, verili (şey)" anlamına gelmektedir. Latince data (dedomena) kavramının M.Ö. 300 yıllarında Öklid'in bir çalışmasında geçtiği bilinmektedir. Dilimizde de "verilen şey" anlamında veri olarak kullanılmaktadır.[29]

Türkçe sözlükte ise "bir araştırmanın, bir tartışmanın, bir muhakemenin temeli olan ana öğe, muta, done", "bilgi, data", "bir problemde bilinen, belirtilmiş anlatımlardan bilinmeyeni bulmaya yarayan şey" olarak tanımlanmaktadır. Bilişim literatüründe ise "olgu, kavram veya komutların, iletişim, yorum ve işlem için elverişli biçimli gösterimi", "bir çözüme ulaşmak için işlenebilir duruma getirilmiş gözlemler, ölçümler", "bilgisayar için işlenebilir duruma getirilmiş sayısal ya da sayısal olmayan nicelikler" olarak geçmektedir.

Genel olarak verinin enformasyondan, enformasyonun ise bilgiden daha az bir şey olduğudur. Enformasyon elde etmek için öncelikle veriye sahip olunması gerektiği, bilginin ise ancak enformasyon varsa oluşacağı kabul edilmektedir.[30]

Günümüzde veri, miktarları, eylemleri, olguları vb. temsil eden tesadüfi olmayan rast gele bir araya gelmemiş bulunan sembollerden oluşan bir grup olarak ta tanımlanır. Veri genellikle analiz edilebilecek ya da daha ileri işlemler için kullanılabilecek ham bilgi olarak bilinmektedir. Bilişim teknolojisi açısından veri ise, bir durum hakkında, birbiriyle henüz bağlantısı kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bit dizeleridir.

---

[29] CANBEK ve Diğerleri, S.4

[30] http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)

Veriler, sayısal veya alfa nümerik karakterler ya da semboller olacağı gibi çeşitli biçimlerdeki grafik çizimler ve diğer tüm grafik gösterimler şeklinde de olabilmektedir.[31]

- **Enformasyon**

Enformasyon kelimesi Türkçe dilinde, Danışma, tanıtma, Haber alma, haber verme, haberleşme[32], bilişim literatüründe "bilgi işlemde kullanılan kabul edilmiş kurallardan yola çıkarak veriye yöneltilen anlam", "bilişim kuramında, birçok olası olay arasında belirli bir olayın meydana gelme belirsizliğini, bilinemezliğini azaltan herhangi bir bilgi", "bilgi işlemede, verilerden elde edilen herhangi bir kavram, olgu, anlam" olarak geçmektedir. Latince kökeni olan "informatio" taslak, görüş, düşünce anlamına gelmekle birlikte, kelimenin İngilizce dilindeki kökü "inform" (bilgi vermek, haber vermek) kelimesinin Latince kaynağı olan "informare", "şekillendirmek", "biçim vermek", "eğitmek" ve "göstermek" anlamlarına gelmektedir.

Enformasyon teriminin bugün en çok kullanılan tanımı, 20. yüzyılın ortalarında Shannon ve Weaver'in "matematiksel iletişim kuramı"nda ortaya çıkmıştır. Shannon ve Weaver'in teorisi basitçe şöyle demektedir: Enformasyon, iletilenin semantik ve pragmatik içeriğinden tamamen bağımsız bir şekilde kodlanıp bir kanal aracılığıyla gönderici ve alıcı arasında iletilebilen her şeydir. Enformasyon kavramı "anlam" ile karıştırılmamalıdır. Biri çok "önemli" öteki tamamen "önemsiz" iki ileti enformasyon bakımından tamamen, eşdeğerde olabilir. Shannon bunu, iletişimin anlamsal yanının mühendislik yanı ile ilgisi olmadığını söyleyerek açıklar. Enformasyon kavramı, "anlam" kavramındakinin aksine, tek tek iletilere değil, bütüne uygulanır. Enformasyon olası iletiler arasında seçme özgürlüğüdür.[33]

Farklı bir ifade ile Enformasyon, bir sistemin, kendi durumunu başka bir sisteme bildirmesi olarak tanımlanabilir. Bu bildirme, sistemin alacağı her

---

[31] **"Veri, Bilgi Ve Bilişim",** http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html (Eylül 2009)
[32] http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=enformasyon (Mayıs 2010)
[33] http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)

durum için ayrı bir biçime girebilecek bir işaret [sinyal] gönderilmesiyle gerçekleştirilir.

Enformasyon dendiğinde, yalnızca dil alanında olduğu gibi bir bildirme değil, sibernetikle birlikte kazandığı yeni anlam doğrultusunda, fiziksel bir işaret gönderilmesi de anlaşılabilmektedir. Enformasyon dendiğinde, her şeyden önce, bir süreç(proses)ten; bildirme süreci'nden / bildirme fiili'nden söz edildiği anlaşılmalıdır. Enformasyon kavramı aynı zamanda, bildirme edimi [fiili] sonunda elde edilen veriye, üzerinde uzlaşmaya varılan kurallardan yararlanılarak yöneltilen [atfedilen] anlamı da içermektedir.[34]

Diğer bir ifade ile enformasyon, işlenmiş, düzenlenmiş, ilişkilendirilmiş, anlam katılmış, alıcısında fark yaratan yeni etkilere zemin hazırlayan veridir. Enformasyonda potansiyel bilgi gizlidir ve eğer enformasyondaki veri sonuçlara çıkar yada anlam kazanırsa knowledge yani bilgi adını alır.[35]

- **Bilgi**

Bilgi teriminin birden çok açıklaması olabilmektedir.

Bilginin Türkçe sözlükteki anlamı "insan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, malumat", "öğrenme, araştırma veya gözlem yolu ile elde edilen gerçek, vukuf" ve "insan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü"dür. Bilişim literatüründe ise "kurallardan yararlanarak kişinin veriye yönelttiği anlam", "yapay zekâda bir programın akıllı bir şekilde işlenmesine elveren olaylar, olgular, kurallar ve buluşsal ipuçları" ve "olguların ve bunlardan elde edilen genelleştirmelerin örgütlü bütünü" anlamına gelmektedir. Felsefe alanında ise bilgi, "insanların maddi ve toplumsal anlıksal etkinliğinin ürünü; insansal ve doğasal dünyadaki

---

[34] Aykut GÖKER, "*Bilim ve Teknoloji Politikalarına Giriş İçin 'Enformasyon Toplumu' Üzerine Kavramsal Bir Yaklaşım Denemesi*" **Mülkiye Dergisi**, Eylül 2001 S.2 http://www.mulkiyedergi.org/index.php?option=com_rokdownloads&view=file&Itemid=63&id=825:bilim-ve-teknoloji-politikalarna-giri-icin-enformasyon-toplumu-uezerine-kavramsal-bir-yaklam-denemesi-aykut-goeker (Eylül 2009)

[35] **"Enformasyon",** http://www.uludagsozluk.com/k/enformasyon/ (Mayıs 2010)

nesnel temel özelliklerin ve bağıntıların gösterge biçiminde düşünsel olarak aniden üretilmesi" olarak belirtilmektedir.[36]

Yine bilgi, bir nesne veya olayda veya bunlara ilişkin raporlarda ortaya çıkan mesajla ilgilidir. Bu açıdan ele alındığında, sadece kaynağın bir fonksiyonu olma özeliğini taşır ve bazen veri (data) olarak da ifade edilir. Ancak bu görüş, günümüzde pek benimsenmemektedir. Ve ya bilgi, mesajın iletilmesini açıklayan bir kavramdır. Bu açıdan ele alındığında bilgi, mesajın iletilmesi ile ilgili olasılık hesaplarına dayanan, belirsizliğin azaltılması için gerekli olan bir kavramdır. Bu görüş ise genel kabul gören en yaygın görüştür. Bu görüşe göre bilgi kaynaktan bir alıcıya iletilen mesajın içeriğidir. Başka bir ifadeyle, bu anlamda bilgi iletişim kanalının da bir fonksiyonudur. Diğer bir açıdan ise bilgi, bir alıcı tarafından kazanılan anlam ile ilgilidir. Bu anlamdaki bilgi, hem iletişim kaynağının, hem de alıcının bir fonksiyonudur. Bu görüş, "information" ve "knowledge" kavramlarını eşdeğer kabul etmektedir. Bilginin, iletilen mesajın içeriği olarak kabul eden görüş, bilginin "knowledge" i arttırmak için kullanıldığını ve değişik kişilerin aynı mesajı aldıklarında bunları değişik biçimde algılayabileceklerine dikkat çekilmektedir. [37]

Bilgi yine; verinin belli bir anlam ifade edecek şekilde düzenlenmiş hali diğer bir ifade ile de işlenmiş veri olarak tanımlanabilmektedir. Shannon tarafından "*bir konu hakkında var olan belirsizliği azaltan bir kaynak*" olarak tanımlanmıştır. Özetle, veri üzerinde yapılan uygun bütün işlemlerin (mantığa dayanan dönüşüm, ilişkiler, formüller, varsayımlar, basitleştirmeler, v.s.) çıktısı, bilgi olarak ifade edilebilir.[38]

Farklı bir kaynakta ise bilgi; öğrenmeyi mümkün hale getiren ve sadece bir araya getirmeye dayanmayan aynı zamanda kullanıcının amacına ve yeteneğine bağlı olarak öğrenmeyi mümkün kılan, herkes tarafından paylaşılan, insanların sahip olduğu ve anladığı olgu olarak ifade edilmektedir.

---

[36] http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)
[37] Orkan, S.2
[38] CANBEK ve Diğerleri, S.4

Başka bir ifadeyle bilgi, "*tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Verilerin bir araya getirilip işlenmesiyle bilgi elde edilse de; bilgi, kullanılan bilgilerin toplamından daha üstte bir kavramdır. Bir güç oluşturabilecek, katma değer sağlayabilecek veya bir araç haline dönüşmek üzere, daha fazla ve özenli olarak işlenmiş bilgi, asıl değerli olan bilgidir. Bilgi, ne olduğunu (know-what), niçin olduğunu (know-why), nasıl olduğunu (know-how) ve kim olduğunu (know-who) bilmek şeklinde dört sınıftan oluşur. Ne olduğunu bilmek, gerçeklerin toplamıdır ve bilgiye en yakın olan sınıftır. Niçin olduğunu bilmek, teknolojik gelişmenin altında yatan ilke ve yasaların açıklandığı bilimsel bilgidir. Nasıl olduğunu bilmek, bir şeyi yapabilme becerisidir. Kimin olduğunu bilmek, kimin neyi ve kimin neyi nasıl yapılacağını bildiğini bilmek olarak özetlenebilir."*[39]

Veri ve bilgi kavramları basit bir örnekle birbirinden ayrılabilir. Örneğin doğum tarihi, üzerinde hiç işlem yapılmamış ham veridir. Yaş ise bilgi olup, kişinin yaşının öğrenilebilmesi için kişinin doğum tarihi ve yaşının öğrenilmek istendiği tarihin bilinmesi gerekir. Yaşın öğrenilmek istendiği tarihten doğum tarihi çıkarılarak yaş bilgisi elde edilir. Burada veri işlenmiş ve ortaya bilgi çıkmıştır.[40]

Bilişim teoristleri ise, "information" kavramını, bir mesajı tüm detayları ile bir yerden diğerine iletmek için, bir iletişim kanalından geçirilmesi gereken veri miktarı; "knowledge" ı ise bir mesajı, tüm detayları ile değil, ancak alıcı tarafından anlamı yeterince anlaşılacak şekilde, bir iletişim kanalından geçirilmesi gereken veri olarak tanımlamaktadırlar.

Sosyal olayları sibernetik yöntemlerle açıklamaya çalışanlar ise, karar vermenin en önemli faktörünün bilgi olduğunu savunmaktadırlar. Bu açıdan bilgi, bir sistemin durumunu ve buna bağlı olarak o sistemin diğer bir sisteme ilettiği durumu anlatan nitel bir faktördür.[41]

---

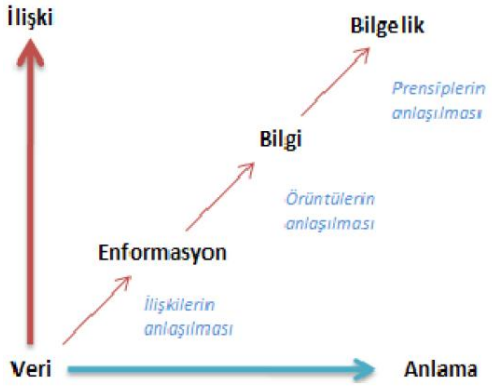
[39] A.G.E, S.5
[40] **"Veri, Bilgi Ve Bilişim",** http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html (Eylül 2009)
[41] Orkan, S.5

Bilginin değerini ve boyutlarını anlayabilmek için aşağıdaki ifadeler yardımcı olabilecektir.

Bilgi;

- Boşlukta ve zamanda yer kaplar.gürültü çıkarmadan hareket edemez.
- Hareketi için enerji gerekir.
- Yaşam ve herhangi bir düzenli etkinlik için gereklidir.
- Hem maddesiz biçim, hem biçimsiz maddedir.
- Ağırlığa sahiptir. Bir giga bayt, bir parmak izinden daha az ağırlıktadır.
- Zaman içinde hareketli veya donmuş olabilir.
- Bir soruya tatmin edici, belki de rahatsızlık verici bir cevaptır.
- Katı hale sahiptir, donarak katılaşır (depolama).
- Sıvı hale sahiptir, akar (iletişim).
- Bir yerlerde bilgi hareket eder, evren gümbürder ve gerçeği gürler.
- Maddeden farklı olarak bilgi aynı anda birden fazla yerde olabilir.
- El sıkışma, baş sallama, bakış veya iç çekiştir.
- Rastsallık denizinde parlar.[42]

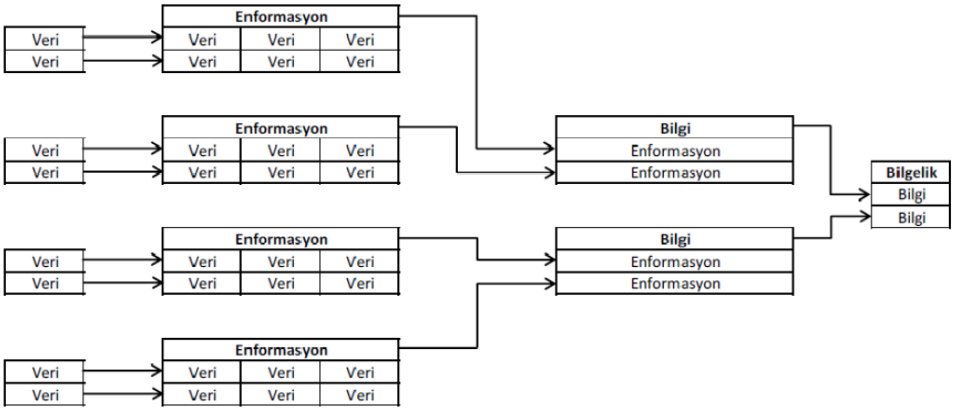
Veri, enformasyon ve bilgi arasındaki ilişki aşağıdaki Şekil 3 ve Şekil 4'de gösterilmeye çalışılmıştır.



Şekil 3 : Veri, Enformasyon, Bilgi ve Bilgelik İlişkisi - 1

Kaynak:
http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)

[42] CANBEK ve Diğerleri, S.2



Şekil 4 : Veri, Enformasyon, Bilgi ve Bilgelik İlişkisi – 2

Kaynak:
http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)

- **Akıl**

"Akıl (wisdom); tasavvur, ileri görüş ve ufkun ötesini görme yetisi ile en ileri seviyede soyutlama ve bir kişinin özel bir iş sahasındaki meslek hayatı boyunca elde edilmiş deneyimin özüdür. akıl, ayrıca, güvenilir yargıda bulunmak ve karar vermek için özbilginin nasıl kullanılacağını kavramak olarak da tanımlanmaktadır. 1954 yılında Einstein hikmet için, "akıl, eğitim ve öğretimin ürünü değil; onu elde etmek için ömür boyu süren bir girişimin sonucudur" demiştir."[43]

2.2.2.1. Bilişim Güvenliği

Bilişim Güvenliği**:** Bilişim aygıtlarının kullanımından doğabilecek riskler ve tehlikeler ile ilgilenen bir alandır.

- **Bilişim Güvenliğinin Unsurları**

"Gizlilik (confidentiality), Bütünlük (integrity), Erişilebilirlik (availability), Kimlik kanıtlama (authentication) ve inkâr edememe (non-repudiation) bilgi güvenliğinin en temel unsurlardır.

[43] A.G.E, S.6

Bu unsurlara değinilecek olursa;

Gizlilik, bilginin sadece erişim hakkı olan yetkili kişilerce erişilebilir olmasıdır.

Bütünlük, bilgi ve bilgi işleme yöntemleri ile veri içeriğinin değişmediğinin doğrulanmasıdır.

Erişilebilirlik, yetkili kullanıcıların ihtiyaç duyduklarında ve istediklerinde, bilgi ve ilişkili varlıklara erişebilir durumda ve erişme hakkının olmasıdır.

Kimlik kanıtlama, geçerli kullanıcı ve işlemlerin tanınması ve doğrulanması ile bir kullanıcının veya işlemin gerçekten "o" kişi ya da işlem olup olmadığının, kullanıcı ya da işlem tarafından kanıtlanması ve hangi sistem kaynaklarına erişme hakkının olduğunun belirlenmesi sürecidir.

İnkâr edememe, bir bilgiyi alan veya gönderen tarafların, o bilgiyi aldığını veya gönderdiğini inkâr edememesini sağlama işlemleridir.

Bunun dışında sorumluluk (accountability), erişim denetimi (access control), güvenirlik (reliability) ve emniyet (safety) etkenleri de bilgi güvenliğini destekleyen unsurlardır.

Erişim denetimi, bir kaynağa erişim için belirli izinlerin verilmesi veya alınması olarak tanımlanabilmektedir.

Güvenirlik, bir bilgisayarın, bir bilginin veya iletişim sisteminin şartnamesine, tasarım gereksinimlerine sürekli ve kesin bir şekilde uyarak çalışması ve bunu çok güvenli bir şekilde yapabilmesi ve sistemin bunu başarabildiğine inanmanın sağlanabilmesidir.

Emniyet, bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gömülü olduğunda, kendisi veya gömülü olduğu ortam için istenmeyen

potansiyel veya direkt tehlike oluşturacak etkinlik veya olayları önleme tedbirlerini içermektedir.44

Bütün kullanıcı hareketlerini kontrol altında tutmak, izinli girişlerin ve izinsiz girişlerin kayıtlarını tutmak ve daima kontrol etmek çok önemlidir. Bu nedenle güvenlik süreci CIA denilen 3 temelden oluşan bir zincirdir.

CIA, Confidentiality (Gizlilik) - Integrity (Bütünlük)- Availablity (Erişilebilirlik) kelimelerinin baş harflerinden oluşur. Bu üç unsur birbiri ile iç içedir. Kafalarda bir üçgen canlandırıldığında ki adı "Güvenlik üçgeni" olsun, üçgenin her bir köşesinde isim olarak sırasıyla C, I ve A harflerini verilerek anlatılabilir. Dolayısı ile her bir harf diğer 2 harfle doğrudan bağlantılıdır. Birindeki aksama diğerlerini çok rahat bir şekilde etkilemektedir.

Bütün bu işlemlerin tabanında yatan kavram ise sorumluluktur. Bu kavramın anlamına sözlükten bakıldığında "Sorumluluk" olduğu görülmektedir. Ancak bilişim camiasında bu kelimenin tam Türkçesi "izlenilebilirlik"tir. Ek olarak sorumluluk, belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirleyebilmedir. Tipik olarak iş ve işlemlerin kayıtlarını tutmak için bir kayıt tutma (logging) sistemine ve bu kayıtları araştıracak bir hesap inceleme (auditing) sistemine ihtiyaç duyulmaktadır.

Sistemler izlenilebilir değilse sistemdeki hareketlerin ve işlemlerin kontrol edilebilir olması mümkün olmayacaktır. O yüzden önce sistemlerin Accountability'sini sağlayıp ondan sonra CIA hakkında konuşulmasında fayda vardır.

<u>İzlenilebilirlik Temel Olarak 5 Adımda Sağlanır:</u>

1. Identification (Teşhis) **:** Bu adımda sisteme giren kişi teşhis edilir. Bu en basit olarak "Kullanıcı Adı" ile sağlanır. Sistemdeki her kullanıcının kendisine ait ve kendisini tanımlayan ya da temsil eden bir kullanıcı adı ya da numarası olması gereklidir.

2. Authentication (Doğrulama) **:** Bu adım sisteme giriş yapmaya çalışan kullanıcının, sisteme o kişinin gerçekten kendisi olduğunu

[44] A.G.E. S.86

kanıtladığı adımdır. Bu adımda giriş yapmaya çalışan kullanıcı sisteme "şifre" sini iletir. Şifre ile kullanıcı adı birbiri ile uyuşuyorsa doğrulanmış olur. Diğer bir ifade ile sadece izin verilen kullanıcıların erişimlerinin sağlanmasını içermektedir.

3. Authorization (Yetkilendirme): Kullanıcı sistem tarafından doğrulandıktan sonra bu adımda o kullanıcının sahip olduğu yetkiler kendisine sistem tarafından tahsis edilir ve kullanıcının kullanımına sunulur. Diğer bir ifade ile ilgili servise izin verilen ilgili kullanıcıların sadece kendilerine izin verilen iş ve işlemleri yapmalarının sağlanmasını içermektedir.

4. Auditing (Denetim) **:** Sisteme girebilen ve iş ve işlem yapan kullanıcıların, bütün aktivitelerinin ve hareketlerin izlendiği safhadır. Hangi kullanıcı hangi işlemi yapmış. Nereye girmiş neyi silmiş hani ayarı değiştirmiş gibi iş ve işlemlerin denetlenip kayıt altına alındığı safhadır. Diğer bir ifade ile ilgili servise izin verilen ilgili kullanıcıların, yetkili iş ya da işlemleri dışında iş ya da işlemler yapıp yapmaması ya da yapmaya çalışması konularının izlenmesini içerir.

5. Accountability (izlenilebilirlik) **:** İzlenilebilirlik temasının son elemanı yine izlenilebilirliğin kendisidir. Bu safhada ilk 4 safhada elde edilen bilgiler bir araya getirilmiş, yorumlanmış ve izlenilebilirliğin kendisi ortaya çıkmış olur.

Bu şekilde sağlanmış olan bir güvenlik uygulaması, sadece müsaade edilen kişilerin sisteme giriş yaptığından emin olunmasına ve giren kişilerin sistemde neler yaptığından haberdar olunmasına olanak sağlamaktadır.[45]

Bu unsurların tamamının gerçekleştirilmesiyle, bilgi güvenliği %100 sağlanmış olmayacaktır. Halen geçerliliğini koruyan Şekil 5'den de görülebileceği gibi; bu unsurların bir veya birkaçının eksikliği, güvenlik boyutunda aksamalara sebebiyet verebilecektir. Bu unsurların birbirini tamamlayıcı unsurlar olduğu hiçbir zaman unutulmamalıdır.

[45] "**Güvenlik Nedir?**", http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.html (Şubat 2009)



Şekil 5 : Bilişim Güvenliği Unsurları

Kaynak: CANBEK ve Diğerleri, S.86

2.2.2.2. Bilişim Güvenliği Türleri

- **Fiziksel Güvenlik**

Sistemlerin, fiziksel olarak, güvende olması ifade edilmektedir. Sistemlerin elektronik ortamlarda güvende olması ilk olarak bu sistemlerin fiziksel olarak güvende olmasına bağlıdır. Sunucular, iletişim donanımları ve ekipmanları için düşünüldüğünde, tüm bunların kesinlikle, erişimin yetkili kişiler dışında yasak olduğu kilitli merkezlerde tutulmalıdır. Bu sayede fiziksel erişimin verdiği avantajları sistem sorumluları haricinde hiç kimse kullanamaz ve yetkisiz kişi ya da kişilerin sistemlere fiziki temasları ve fiziki temas ile ortaya çıkabilecek tüm riskler ortadan kaldırılmış ve engellenmiş olur.

- **Sunucu Güvenliği (Donanım - OS)**

Sunuculara üçüncü kişilerin fiziksel olarak müdahale etmemelerini, edememelerini, etseler dahi donanım içerisindeki bilgi ve belgelere erişememelerini, erişseler dahi bir anlam çıkaramamalarını, donanımların herhangi bir sebepten dolayı zarar görmemesini ifade etmektedir.

İşletim Sistemi (OS – Operating System) ise tehdit ve saldırılara en az maruz kalacak ve etkilenecek olan ancak kullanıcının tüm ihtiyaçlarını karşılayabilen işletim sisteminin seçilmesi ve bu işletim sisteminin güncellemelerinin düzenli olarak kontrol edilmesi konularını içermektedir.

- **İletişim Güvenliği**

Yetkili, izinli ve doğru kaynak/kaynaklar ve alıcı/alıcılar arasındaki haberleşmenin, istenmeyen diğer kişi ya da kişilerce kullanılabilir bir şekilde ele geçirilmesinin önlenmesini içermektedir.

- **Servis Güvenliği**

Verilecek olan servisin, ilgili servisi verebilen, tehdit ve saldırılara en az maruz kalacak ve en az etkilenecek olan ancak kullanıcının tüm ihtiyaçlarını karşılayabilen servisin seçilmesi konusunu içermektedir.

- **Veri Güvenliği**

Kısaca, elde edilen tüm verilerin herhangi bir veri kaybı ihtimaline karşın yedeklenmesi, izinsiz kişi ya da kişilerin eline geçmemesi, geçse dahi anlam ifade etmemesi ve ayrı ortamlar üzerinde saklanması konularını içermektedir.

- **Bilgi Güvenliği**

Bilişim sistemlerinde bilgi güvenliği, korunması ya da saklanması gereken değerlerin, elektronik ortamlarda olanlarının, bütünlüğünün, değişmemişliğinin ve kendisinin bozulmadan kullanımının sağlanması ve izinsiz erişimlerden korunması için güvenli bir bilgi işleme platformu oluşturma çabalarının tümü olarak tanımlanmaktadır.

Başka bir deyişle, bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla, doğru zamanda, doğru yerde ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak tanımlanabilmektedir.

Mükemmellik, diğer bir deyişle %100 güvenlik, bilgi güvenliğinde söz konusu olamamaktadır. Zaten "mükemmel bir güvenlik" de hedef olmamalıdır. Bu hedeflense bile bunun mümkün olmadığı ve ya olamayacağı, gereğinden fazla kaynak israfına sebebiyet verilebileceği unutulmamalıdır. Bunun yerine, problemleri tespit edebilme ve karşı koyabilme kabiliyetine sahip olmaya, karşı atakları tasarlayarak yapılan saldırılardan korunmaya kilitlenilmeli ve amaç bu olmalıdır.

İyi bir güvenlik politikası oluşturulmaya çalışılmalı ve bu politikada bilgi sistemlerini kullanan her kullanıcıya en az hak verme yaklaşımı benimsenmelidir. Bu karşılaşılabilecek problemleri azaltacaktır. Bunun yanında, güvenli sistem bileşenlerini tanımlama ve güvenlik gerektiren bileşenlerin sayılarını en aza indirme de karşılaşılabilecek sıkıntıları ciddi ölçüde azaltacaktır.[46]

[46] CANBEK ve Diğerleri, S.69

2.2.2.3. Bilişim Güvenliği İhtiyacı

- **Bilgi ve Bilişim Güvenliği İhtiyacı**

Bilgi teknolojilerinin yaygınlaşması ile beraber bilgi üretimi de ciddi boyutlarda artmıştır. Günümüzde her kayıt, oluşur ya da oluşturulur oluşturulmaz anında veriye ve bilgiye dönüştürülebilmektedir. Bilgi teknolojileri yaygınlaşmadan önce, bilginin büyük bir çoğunluğu basılı dokümanlarda yer almaktaydı ve bu kayıtlar bilişim sistemleri tarafından işlenebilir hale getirmek çok uzun zaman ve para kaybettirmekteydi. Bu nedenle günümüzde bilgiye erişme imkânları geçmiş ile karşılaştırılamayacak seviyede artmıştır.

Bu durum, birçok dezavantajı da beraberinde getirmektedir. Bilgi teknolojileri üzerinde bilinçli veya bilinçsiz yapılan hataların çok ciddi sonuçlar doğurması olasıdır. Bilgi teknolojilerinde ortaya çıkan açıklıklar, dikkatsizce, yanlışlıkla ya da bilinçli olarak yapılan hatalar ve iş ve işlemler bilgiye yetkisiz ve zararlı erişime yol açabilmektedir. Bu durumda bilginin yetkisiz imhası, değiştirilmesi ve ya elde edilmedi söz konusu olabilmektedir. Geçmişte sadece fiziksel güvenliğin tesis edilmesi ile sağlanan bilgi güvenliği, günümüzde kurumların en çok zorlandıkları ihtiyaçların başında gelmektedir.[47]

II. Dünya Savaşı'ndan 35 yıl sonra açıklanan bir raporda, İngiltere ile Almanya arasındaki savaşın seyrinin, savaş taktiklerini içeren mesajların çözülmesiyle (deşifre) değiştiği yer almaktadır. Bu şifre çözme işlemi, savaşın müttefikler tarafından kazanılmasında büyük rol oynamıştır. Boston Globe gazetesi bir haberinde bu olayın, II. Dünya Savaşı hakkında daha önce tarih kitaplarında yazılmış olanların değiştirilmesi gerektiğini önemle vurgulamıştır. Tarihi değiştirecek kadar önemli olan şifre çözme olayı, bu konunun önemini vurgulamada verilebilecek en iyi örneklerden biridir. Günümüzde insanı gerçekten hayrete düşürecek bu ve buna benzer milyonlarca örnek bulunabilir. Bilişim toplumu olma yolunda hızla ilerlediğimiz günümüzde, sayısal ortamın hızla yaygınlaşması kaçınılmazdır.

[47] "**Türkiye'de Bilişim Güvenliği Analizi**", http://www.turkishajan.com/bilisim-suclari-analizi-ve-kriminal-olaylar/turkiye8217de-bilisim-guvenligi-analizi-34075.html (Ocak 2009)

Bunun sonucu olarak, bilginin iletilmesi, alınması ve saklanması ise daha da önem arz etmektedir. Bu nedenle kişisel ve kurumsal bilgi güvenliği için şifreleme metotlarının veya kriptolojik sistemlerin kullanımı bir zorunluluk haline gelmiştir.

Avrupa Komisyonu Bilgi Topluluğu eEurope+ Şubat 2004 tarihli raporunda Türkiye'de her 100 kişi başına düşen kişisel bilgisayar sayısındaki artışı; 2001 yılında 3, 2002 yılında 4, 2003 yılında ise 5 olarak vermektedir. Yine her 100 kişi için Internet kullanıcısı sayısını; 2001 yılında 6 kişi, 2002 yılında 7 kişi, 2003 yılında ise 9 kişi olarak vermektedir.

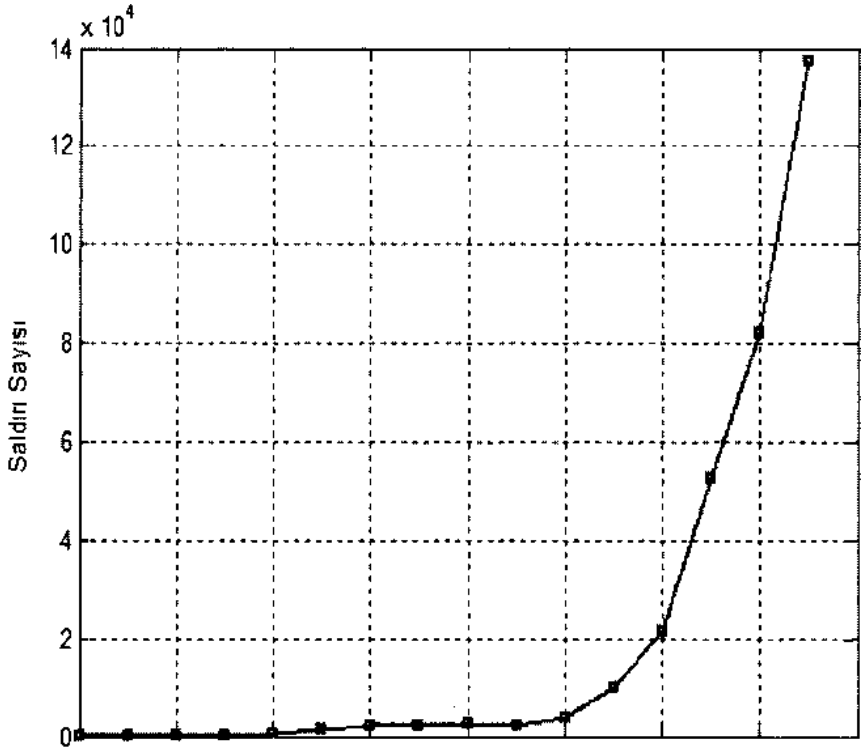
DİE'nin Ekim 2004 raporundan da anlaşıldığı üzere ülkemizde bu oranın hızla artmaya devam ettiği anlaşılmaktadır. Her on evden birinde bilgisayar olduğu, 16-74 yaş grubundaki 47 milyon bireyin 7,9 milyonunun bilgisayar ve 6,2 milyonunun İnternet kullandığı, son üç ay içinde bilgisayar kullananların oranının %16,8, son üç ay içinde İnternet kullananların oranının %13,25 arttığı saptanmıştır.

2004 yılında Koç Sistem'in yayınladığı bir raporda ise, sayısal veriler ve istatistiksel bilgilerin, kurumların karşılaştığı bilgi güvenliği sorunlarını daha net bir şekilde ortaya koymaktadırlar. Türkiye'de 1000 civarında firma üzerinde yapılan testlerde bu kurumların ve şirketlerin;

- %87'sinin farklı düzeylerde güvenlik riski taşımakta oldukları, %56'sının web sunucu bilgilerine kolaylıkla erişilebildiği ve ana sayfalarının değiştirilebildiği veya bir başka adrese yönlendirilebildiği,
- %43'ünün DNS sunucularındaki açıklardan dolayı posta adres ve içeriklerinin ele geçirilebildiği veya çalışanların bankacılık vb. işlemlerde kullandıkları şifrelerin çalınabildiği,
- %28'inin güvenlik duvarı yapılandırması kötü olduğu için by-pass edilerek her türlü bilgiye erişilebildiği ve
- %29'unun sistemlerinde çok yüksek seviyede açıklar bulunduğu belirtilmiştir.

2005 yılında CERT/CC İstatistiklerinde rapor edildiği gibi, 2000 yılından beri var olan korunmasızlık çeşidi 6 kat artarak 2005'de 4.000'e kadar ulaşmış, yaklaşık 150.000 saldırı olayı saptanmıştır. Rapora göre 1998 ve 2003 yılları arasında kendilerine bildirilen saldırı sayıları Şekil 6'da

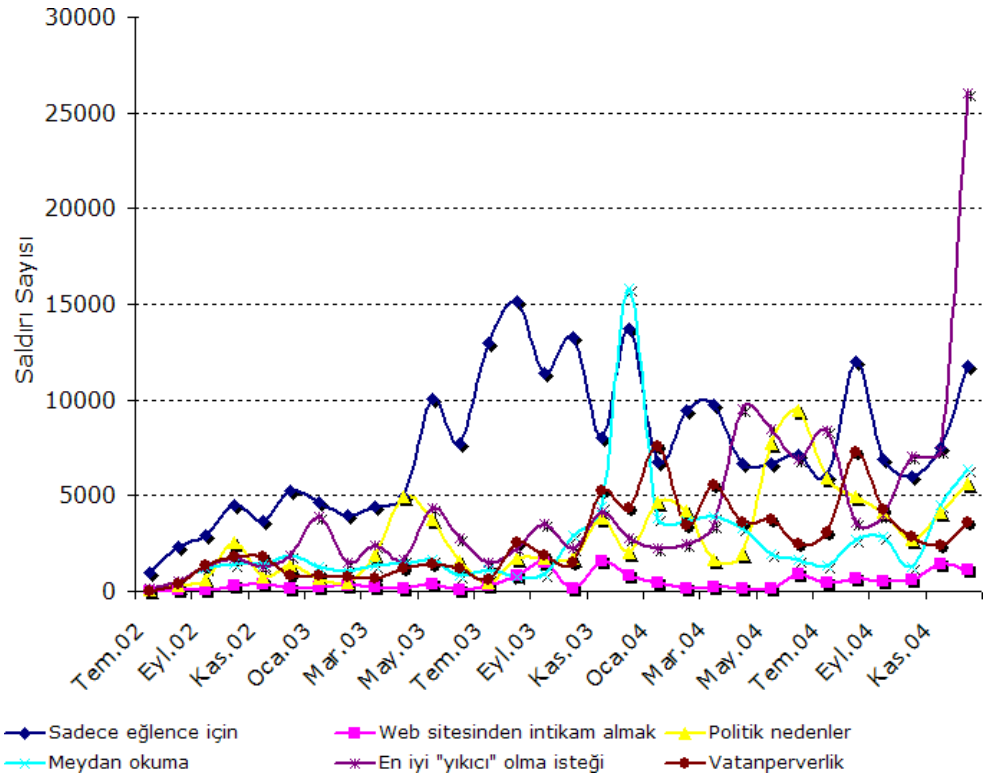
gösterilmektedir. Bu istatistiklerde yer alan zafiyet ve saldırı olaylarının artış yüzdeleri göz önüne alındığında, geçen zaman içerisinde, günümüzde bu rakamların çok daha yüksek oldukları düşünülmektedir.



Şekil 6 : 1988-2003 Yılları Arasında Bilgisayar Sistemlerine Rapor Edilen Saldırıların Sayısı

Kaynak: CANBEK ve Diğerleri, S.159

Saldırganların neden sistemlere saldırdıkları ve ne amaç güttükleri ile ilgi yapılan çalışmalarda, saldırganların "bu işte en iyi olma" istekleri nedeniyle, bu saldırıları yaptıkları saldırı oranlarının inanılmaz bir artış gösterdiği ve ciddi bir sorun teşkil ettiği görülmüştür. Anlaşıldığı üzere, sistemlerde kimseye karşı meydan okuma, rahatsızlık verme gibi bir durum olmasa dahi, bu tür saldırılar ile karşı karşıya kalınabilmektedir. Şekil 7'de belirtilen değerler göz önüne alınarak artış oranları değerlendirildiğinde, "en iyi olma" amacıyla yapılan saldırıları oranlarının açık ara farkla günümüzde de yine en üst seviyelerde olduğu değerlendirilmektedir.



Şekil 7 : Korsanlık Nedenleri 2002-2004

Kaynak: A.G.E., S.160

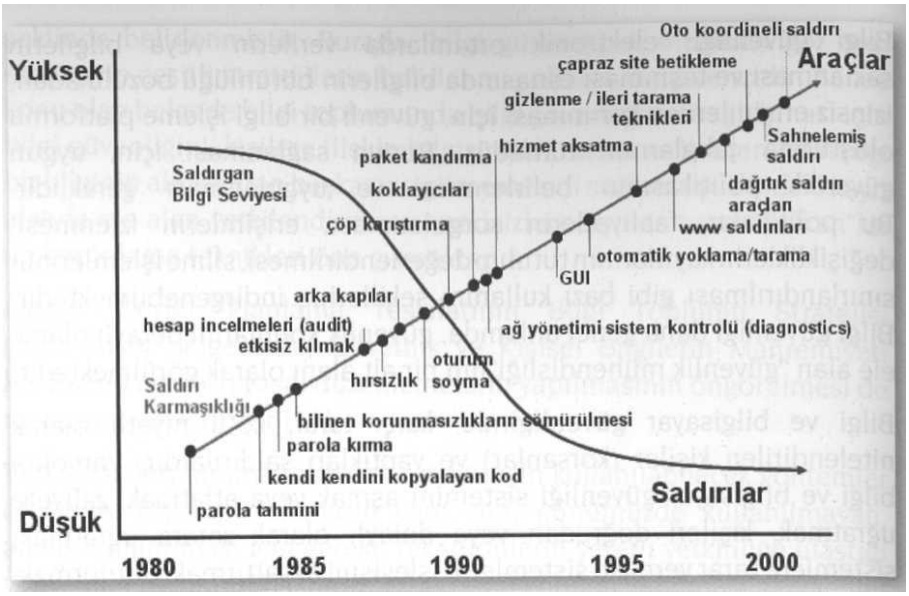
Diğer bir istatistikî veriye göre ise saldırı nedenlerinin son yıllarda farklılık gösterdiği ve "sadece eğlence için" yapılan saldırı sayısının ciddi bir fark ile ön sıra yer aldığı anlaşılmaktadır. Bu kanı Tablo 1'den de görülebilmektedir.

Tablo 1
Saldırı Nedenleri

Saldırı Nedenleri	2008	2009	2010
En iyi "yıkıcı" olma isteği	201.270	122.442	78.761
Sadece eğlence için	96.438	176.725	179.707
Meydan okuma	61.112	26.921	13.422
Politik nedenle	50.578	72.767	19.360
Vatanperverlik	46.619	40.374	17.877
Web sitesinden intikam almak	4.802	23.513	15.147
Diğer	56.640	81.667	28.545

Kaynak: "Tahrifat İstatistikleri", http://www.zone-h.org/news/id/4735 (Haziran 2010)

Bunlara ek olarak, işinin ehli kişilerce hazırlanan saldırı araçlarının fazlalaşması ile saldırı yapacak kişilerin bilgiye ihtiyaç duymadan ciddi saldırılar yapabilecekleri bir ortam hazırlanmış olmaktadır. Teknolojinin ilerlemesi ile saldırıların çeşidini ve etkisini arttıran yeni uygulamaların çoğalması ve kolayca paylaşılması sayesinde, Şekil 8'de belirtilen, daha az bilgi ile daha etkili saldırı yapabilme oranlarının ters orantılı bir şekilde çok daha yüksek seviyelerde seyrettiği değerlendirilmektedir.



Şekil 8 : Artan Saldırı Sayısı ve Ciddiyet Seviyelerine Karşın Saldırganların Azalan Bilgi Seviyeleri

Kaynak: CANBEK ve Diğerleri, S.74

Tüm bunlara rağmen özellikle Türk tahrifatçıların tüm dünyaca bilinen ve takip edilen, tüm dünyadaki özellikle Türk tahrifatçıların, tahrifata uğrattıkları ya da zarar verdikleri web sayfalarını, bu işi başardıklarını belgelemek, kendilerini kanıtlamak ve marifetlerini ya da kabiliyetlerini tüm dünyaya göstererek şöhret ve saygı sahibi olmak için kaydettirdikleri, dolayısı ile de tahrifata uğrayan ya da zarar verilen sayfaların bilgilerinin tutulduğu www.zone-h.org sitesinde, en başarılı tahrifatçılar olarak listelendikleri görülmektedir. İlk 50 de oldukça fazla Türk tahrifatçının olduğu Tablo 2'den de görüldüğü gibi dikkat çeken bir nokta olarak değerlendirilmektedir.

Tablo 2
En Çok Başarılı ve Teyit Edilmiş Tahrifat Yapan Saldırgan Sıralaması

Sıra	Tahrifatçı	Tekil Tahrifat	Toplu Tahrifat	Toplam Tahrifat	Ana Sayfa Tahrifatı	Alt Dizin Tahrifatı
1	iskorpitx	27613	271095	298708	166775	131933
2	1923Turk	18642	52488	71130	30958	40172
3	Fatal Error	17960	34032	51992	45690	6302
4	GHoST61	15590	52193	67783	53620	14163
5	SPYKIDS	8717	21750	30467	29488	979
6	Red Eye	8581	37378	45959	45632	327
7	ZoRRoKiN	8420	6893	15313	4097	11216
8	aLpTurkTegiN	7820	19001	26821	16627	10194
9	caprazates.org	7728	7143	14871	8974	5897
10	BeLa	7280	5270	12550	7727	4823
11	Secrethackers.org	7188	1425	8613	1878	6735
12	Thehacker	7158	40363	47521	42511	5010
13	linuXploit_crew	6949	15884	22833	22833	0
14	Ir4dex	6441	31787	38228	37986	242
15	federal-atack.org	5599	6413	12012	3655	8357
16	AYYILDIZ	5594	7035	12629	4724	7905
17	reDMin	5555	5471	11026	3300	7726
18	hackbsd crew	5490	8409	13899	7612	6287
19	Swan	5125	6931	12056	5065	6991
20	SanalYargic	4935	5011	9946	2770	7176
21	Dengesiz Team	4911	5541	10452	3726	6726
22	JaCKaL	4856	2433	7289	4206	3083
23	uykusuz001	4832	4437	9269	992	8277
24	DARK_MARE	4739	11141	15880	12037	3843
25	THE FREEDOM	4423	7224	11647	780	10867

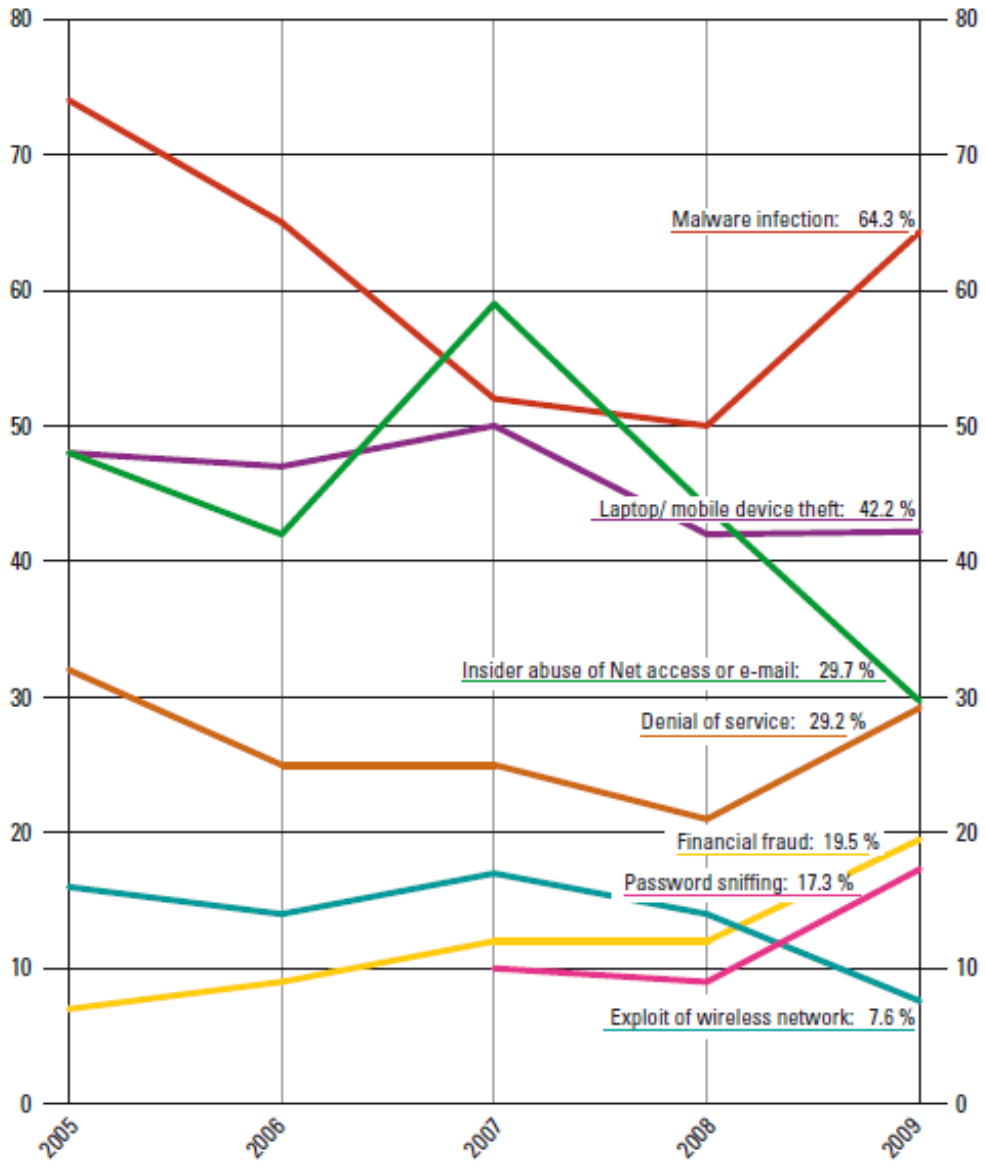
Sıra	Tahrifatçı	Tekil Tahrifat	Toplu Tahrifat	Toplam Tahrifat	Ana Sayfa Tahrifatı	Alt Dizin Tahrifatı
26	simiens	4415	33293	37708	37644	64
27	TechTeam	4397	32049	36446	36421	25
28	core-project	4376	9780	14156	14096	60
29	nEt^DeViL	4228	13976	18204	15767	2437
30	Persian Boys Hacking Team	4064	5143	9207	1493	7714
31	Yusuf	4058	666	4724	684	4040
32	r00t_System	4055	19218	23273	21043	2230
33	vezir.04	4023	1354	5377	2869	2508
34	Infektion Group	3985	30980	34965	33227	1738
35	eno7	3914	9505	13419	5147	8272
36	XTech Inc	3744	8954	12698	12684	14
37	NobodyCoder	3622	21835	25457	21666	3791
38	D.O.M	3562	18921	22483	22088	395
39	HEXB00T3R	3506	15671	19177	8998	10179
40	EL_MuHaMMeD	3503	8872	12375	7303	5072
41	bY_FatiH	3457	1286	4743	1589	3154
42	BoZKuRTSeRDaR	3426	304	3730	998	2732
43	Spyhackerz.com	3411	4477	7888	3600	4288
44	Real_Karizma	3386	6410	9796	6573	3223
45	sinaritx	3284	5154	8438	3791	4647
46	BloodBR	3262	16426	19688	19681	7
47	Mafia Hacking Team	3227	10841	14068	4328	9740
48	ION	3113	3320	6433	5128	1305
49	PcDelisi	3109	3488	6597	681	5916
50	PoW3RFuL	3077	1158	4235	1412	2823

Kaynak: http://www.zone-h.org/stats/notifier (Haziran 2010)

Amerika Birleşik Devletleri'nin FBI (Federal Bureau of Investigation) biriminin içerisinde, bilişim suçlarının artış göstermesi üzerine kurulan CSI (Computer Security Institute) kısmının her yıl yaptığı araştırmanın sonuçları, bu saldırıların neticesinde ortaya çıkan zararları net olarak göstermektedir.

CSI, bu araştırmasını 2009 yılında Amerika'daki 443 farklı organizasyon, devlet kurumu, eğitim, finans ve sağlık sektöründe çalışanlar ile gerçekleştirmiştir.

Şekil 9'da ankete ve çalışmaya katılan katılımcıların maruz kaldıkları saldırı türlerinin yıllara göre artış ve azalış seviyeleri gösterilmektedir. Görülüyor ki alınan teknik ve kanuni önlemlerle mobil cihaz hırsızlıkları azalma göstermekte ancak diğer saldırı türlerinde herhangi ciddi bir değişiklik gözlemlenememektedir.



Şekil 9 : Ankete Katılanların Maruz Kaldıkları Atak Türleri

Kaynak: "**Computer Crime And Security Survey**", 2009, CSI - Computer Security Institute, S.10, http://gocsi.com/survey (Aralık 2009)

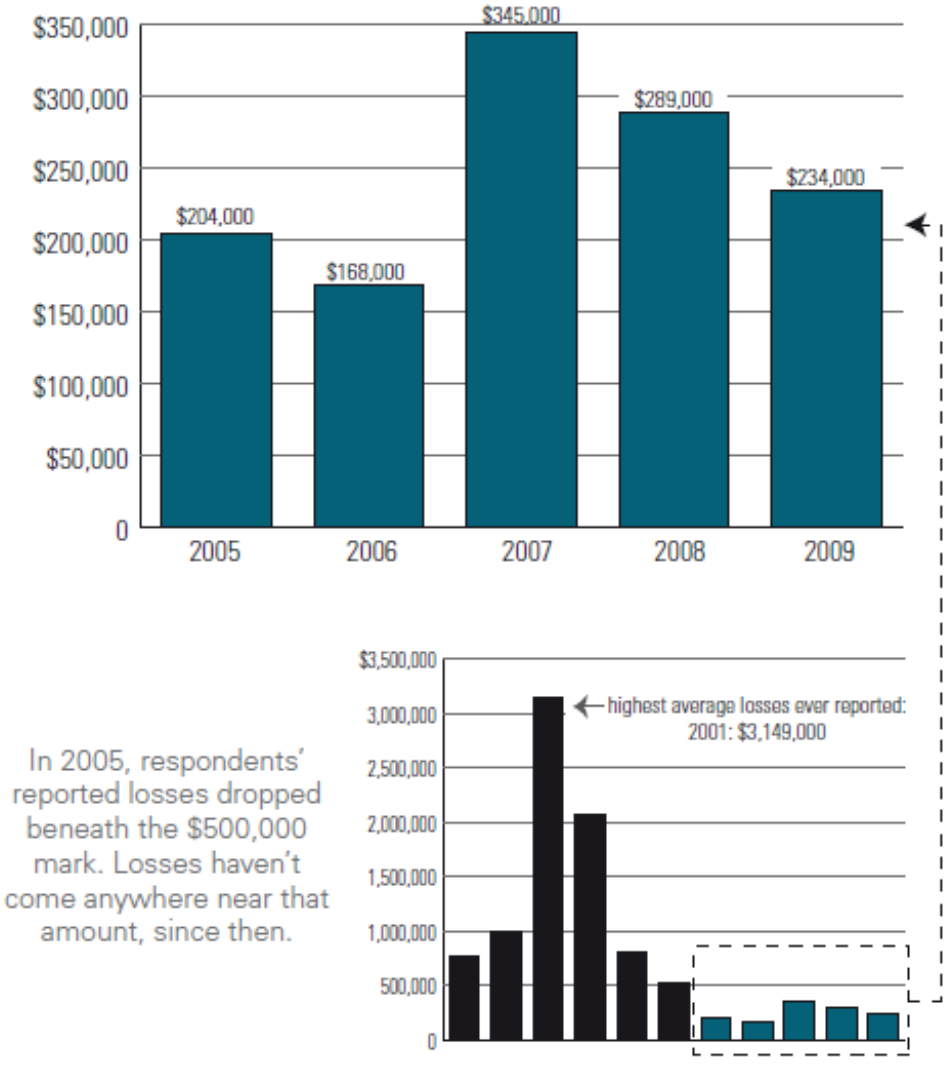
Bu grafiğe farklı bir şekilde bakıldığında, teknolojik gelişmeler neticesinde yıllara göre, ortaya, bot ve zombie organizasyonları, şifre dinleme, DNS sunucularının, facebook, twitter gibi sosyal paylaşım site profillerinin ele geçirilmesi gibi yeni saldırı türlerinin çıktığı görülmektedir. Şekil 10'da bahse konu yeni saldırı türleri ve saldırıların yıllara göre oranları gösterilmeye çalışılmıştır.

Type of Attack	2005	2006	2007	2008	2009
Malware infection	74%	65%	52%	50%	64%
Bots / zombies within the organization	added in 2007		21%	20%	23%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%
Password sniffing	added in 2007		10%	9%	17%
Financial fraud	7%	9%	12%	12%	20%
Denial of service	32%	25%	25%	21%	29%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%
Web site defacement	5%	6%	10%	6%	14%
Other exploit of public-facing Web site	option altered in 2009				6%
Exploit of wireless network	16%	14%	17%	14%	8%
Exploit of DNS server	added in 2007		6%	8%	7%
Exploit of client Web browser	option added in 2009				11%
Exploit of user's social network profile	option added in 2009				7%
Instant messaging abuse	added in 2007		25%	21%	8%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%
System penetration by outsider	option altered in 2009				14%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%

Şekil 10 : Ankete Katılanların Maruz Kaldıkları Atak Türleri

Kaynak: A.G.E., S.11

Yapılan bu saldırılar karşısında kurum ve şirketlerin zarara uğramaları kaçınılmazdır. Şekil 11'de bahse konu kurum ve şirketlerin bu saldırılar karşısında uğradıkları maddi zararlar gösterilmeye çalışılmıştır. Her ne kadar 2001 yılındaki rekor kayıplar her yıl düşüş gösterse de, yeni saldırı türleri ile zaman zaman artışlar yine yaşanabilmektedir. 2001 yılından sonraki hızlı düşüsün, bilişim sistemlerine yapılan saldırılar yüzünden bu kadar çok maddi zarar eden kurum ve kuruluşların, bilişim güvenliğini ciddiye alarak yüksek yatırımlar yapmaları ve bilişim güvenliklerini her yıl arttırmaları olarak görünmektedir.

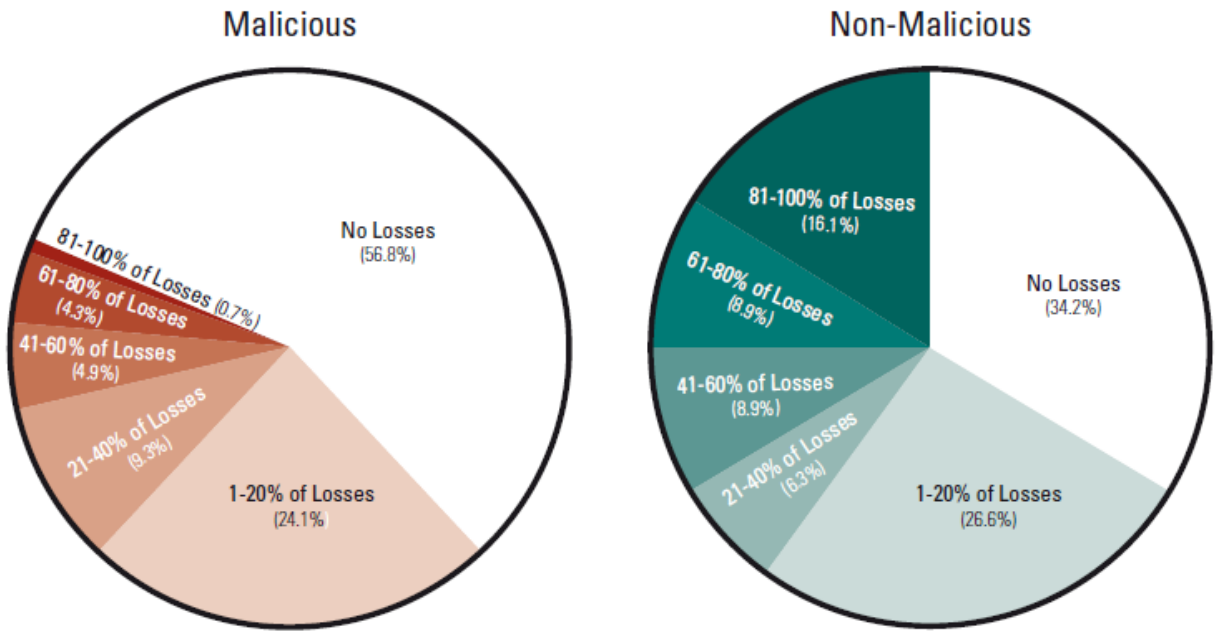


Şekil 11 : Ankete Katılanların Yaşadığı Maddi Kayıplar

Kaynak: A.G.E., S.13

Şekil 12'de yapılan çalışmaya katılanların uğradıkları zararların içerideki kişi ya da kişilerce gerçekleştirilenler ile ilgili yapılan değerlendirme yer almaktadır. Bu değerlendirmeye göre, içeriden bilinçli olarak yapılan saldırılar sonucunda % 1 - %20 arasında kayıp yaşayanların oranının %24,1 olduğu görülmektedir. İçeriden bilinçli yapılan saldırıların genel olarak %43.2 lük bir kısmının ise başarılı olduğu görülebilmektedir.

İçeride kişi ya da kişilerin, bilgisayar ya da sistemlerine virüs, malware, trojan ve ya bot gibi zararlı yazılım ve ya uygulamaların bulaşması nedeniyle, sistemlere bilinçsizce yaptıkları saldırılar neticesinde ise, %1 - %20 arasında kayıp yaşayanların oranının % 26.6 olduğu görülmektedir. İçeriden bilinçsizce yapılan saldırıların genel olarak % 65.8 lik bir kısmının ise başarılı olduğu görülebilmektedir. Bu nedenle saldırıların içeriden ya da dışarından, bilinçli ya da bilinçsiz olduğuna bakılmaksızın her saldırı ihtimali olan erişim noktalarının aynı çatı altında değerlendirilmesi gerektiği anlaşılmaktadır.



Şekil 12 : Ankete Katılanların İçerideki Kişiler Nedeniyle Yaşadıkları Kayıplar

Kaynak: A.G.E., S.15

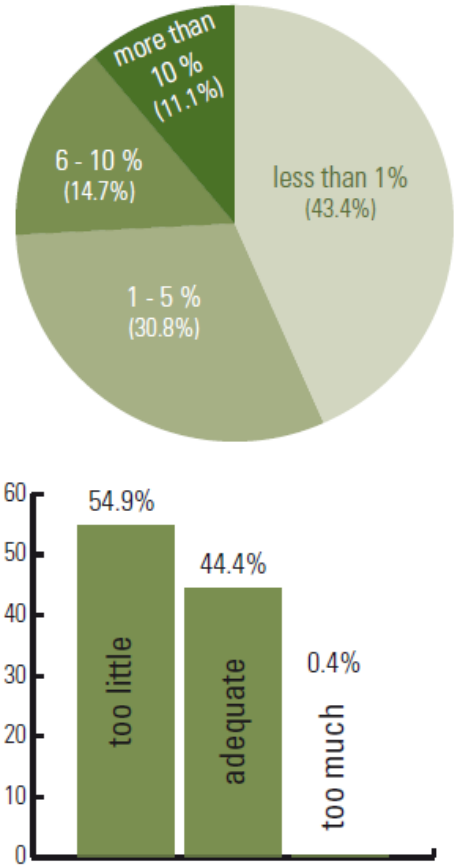
Görüldüğü gibi, kurumun içerisinden gelen bilinçli ve bilinçsiz saldırılardan doğan kayıplar ve zararlar, kurumun genel zararlarına ve

kayıplarına oranı göz ardın edilemeyecek miktardadır. Buradan da anlaşıldığı üzere, son kullanıcının bilinçsizce neden olduğu kayıpların önüne geçmek için çalışmalarda bulunulması gerektiği ortaya çıkmaktadır.

Şekil 13'de, kurum ve şirketlerin bu amaçla yürüttükleri çalışmalar neticesinde, bu amaca yönelik ayrılan ödenek miktarlarının genel ödenek miktarlarına oranları ve bu oranların, ilgili kurumların bilişim güvenliği birimlerince değerlendirilmelerine dayanılarak ayrılan ödenek miktarların yeterlilikleri gösterilmektedir.

Görüldüğü gibi kurumların %43.4 ü, kurumun genel ödenek miktarının %1'den daha azı kadar bir ödeneği, son kullanıcı güvenliği ve bilinçlendirme çalışmaları için ayırmaktadır. Bu konuda %10'dan daha fazla ödenek ayıran kurumların oranının ise %11.1 olduğu görülmektedir. Yine görülmektedir ki, son kullanıcı güvenliği ve bilinçlendirme çalışmaları için, kurumun genel ödenek miktarının %10'una kadar bir ödeneği ayıran kurumların oranı % 88.9'dur.

Ayrılan bu ödenek miktarlarının ise, kurum bazında % 54.9'unun çok az olduğu değerlendirilmiştir. %44.4'ünün ihtiyacı karşıladığı, %0.4'ünün ise gereğinden fazla olduğu düşünüldüğü tespit edilmiştir.

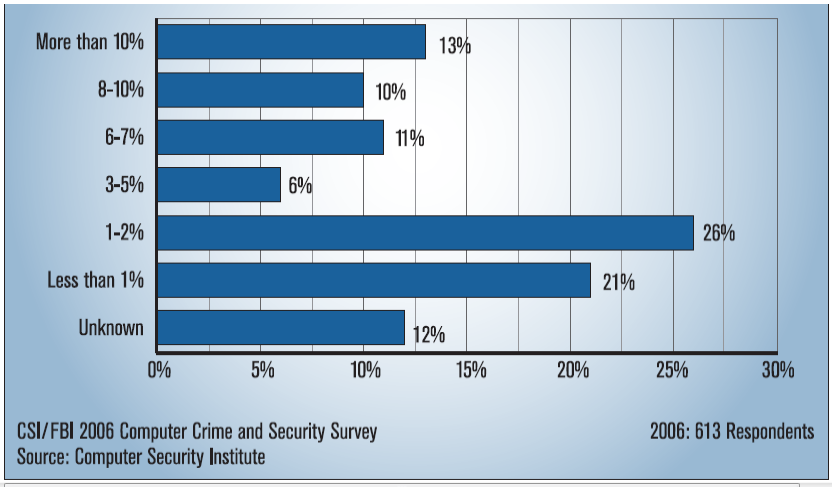


Şekil 13 : Ankete Katılanların Son Kullanıcı Güvenlik Farkında lığına Ayırdıkları Ödenek Miktarları ve Yeterlilik Durumları

Kaynak: A.G.E., S.16

Son kullanıcı güvenliği ve bilinçlendirmenin yanında, genel olarak bilişim güvenliği ile ilgili gereksinimler de vardır. Veri kaybının yaşanmaması için yüksek erişebilirlik, sunucu güvenliği, iletişim güvenliği gibi bilişim güvenliği türlerinin yerine getirilmesi adımları buna örnek verilebilir. Bu kapsamda çalışmaya katılan kurumların bilişim güvenliğine ayırdıkları bütçeler Şekil 14'de gösterilmiştir.

Görüldüğü gibi, çalışmaya katılan şirket ya da kurumlarda, bilişim güvenliğine ayrılan bütçenin genel bütçenin %10'undan daha fazla olma oranı %13'dür. Buradan anlaşıldığı üzere, bilişim güvenliğine ayrılan bütçenin, genel bütçeye oranı %10'un altında olma oranı %87'dir. Bu oranlar göz önüne alındığında, IT bütçelerinde güvenliğe ayrılan oranların günümüzde de aynı oranlarda seyrettiği değerlendirilmektedir.



Şekil 14 : IT Bütçelerinde Güvenliğe Ayrılan Oranlar

Kaynak: "Computer Crime And Security Survey", 2006, CSI - Computer Security Institute, S.13, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf (Mart 2009)

www.zone-h.org sitesinde, 2008 ile 2010 ilk çeyrek yılları arasındaki zarar verilen ya da hacklenen web sitesi ya da sistemlerin istatistiki verileri yayınlanmıştır.

Raporda, www.zone-h.org sitesine 2002 yılından beri ayda ortalama 2500 site tahrifatı kaydının sisteme girildiği ve bu rakamların giderek arttığı belirtilmiştir. Bu bilgi Tablo 3'den de görüldüğü gibi 2009 Nisan ayında kaydedilen 60.000 site tahrifatına karşılık 2010 Nisan ayında kaydedilen 95.000 site tahrifatı ile doğrulanmıştır.

Raporda ayrıca, site tahrifatı yapmak için kullanılan yöntemlerin çoğunun halen web uygulamalarındaki zafiyet sömürüsü (vulnerability exploitation) olduğu belirtilmiştir. Toplam saldırı rakamları ile karşılaştırıldığında son yıllardaki saldırıların büyük oranda arttığı gözlemlenmiştir. Bunun sadece web uygulamalarındaki zafiyetlerden kaynaklanmadığı, bunda oldukça çok sayıda karşılaşılan güvenlik ayarlamaları sağlıklı, tam ve doğru yapılmayan sunucu işletim sistemlerinden yararlanılarak, hackerların sistemlere tam erişim sağlayabilmelerinin de büyük rol oynadığına dikkat çekilmiştir.

Raporda ek olarak, mpack/zeus gibi virüs ya da solucanlar kullanarak sitelerin dosya transfer erişim bilgilerini ele geçiren tahrifatçıların, bu

bilgileri siteleri tahrifata uğratmak ya da zarar vermek için değil, bu sitelere farklı virüs, solucan ya da arka kapı uygulamalarını yükleyerek o siteyi ziyaret eden kişilerin de bilgisayarlarında sakladıkları tüm bilgileri ele geçirmek ya da ziyaretçilerin bilgisayarlarını kendi kontrolü altına almak için kullanabildikleri vurgulanmıştır.[48]

Tablo 3
Aylık Saldırı İstatistikleri

Aylık Saldırılar	2008	2009	2010
Ocak	18.562	37.968	53.921
Şubat	51.925	2.919	57.869
Mart	48.138	7	73.715
Nisan	41.492	60.471	95.090
Mayıs	29.017	48.087	
Haziran	38.445	43.569	
Temmuz	39.549	45.480	
Ağustos	74.121	83.850	
Eylül	42.379	74.384	
Ekim	54.971	54.462	
Kasım	44.486	43.177	
Aralık	34.374	50.035	

Kaynak: "Tahrifat İstatistikleri", Par.1

Tüm dünyada olduğu gibi ülkemizde de, uğranan zararların oranının büyük bir kısmının bilişim iş, hizmet ve işlemlerinden kaynaklandığı düşünülmektedir. Bunun birçok nedeni olabileceği gibi en önemli nedenlerinden birisi de, bilişim suçları da denilen, yasa dışı ve bilinçli olarak dışarında yapılan saldırılardır. Bahse konu bu suçun tipler Tablo 4 'de belirtilmeye çalışılmıştır.

[48] "**Tahrifat İstatistikleri**", Par.1

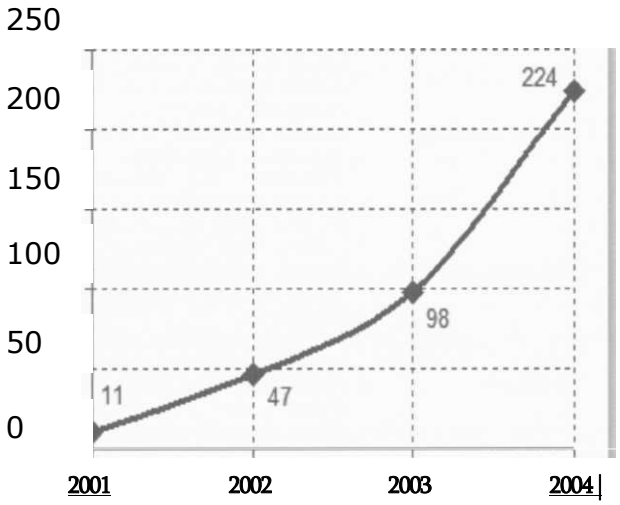
Tablo 4
Bilişim Suçları Tipleri

Ana Suçlar	Alt Suçlar	Tanım ve Kullanılan Kötücül Yazılımlar
Kişisel Gizlilik İhlalleri		Kurum ve kuruluşlarda tutulan kişisel verilerin çeşitli yollarda başkalarının eline geçmesi. Casus yazılım, reklâm yazılım, iz sürme çerezleri, klavye dinleme sistemleri, arka kapılar, şifre kırıcılar, turta (PIE), web böcekleri
Ekonomik Saldırılar	Bilişim korsanlığı	Genelde güvenlik önlemlerini aşmak amacıyla bilgisayar sistemlerine girme, Truva atları, solucanlar, kök kullanıcı takımı (rootkit), korumasızlık sömürücü, arka kapılar, ağ taşkını (flooder), port tarayıcı, açıklık tarayıcı, koklayıcı (sniffer), kandırıcı (spoofer)
	Bilgisayar casusluğu	Sistemlerde tutulan bilgilere izinsiz ve yetkisiz erişim. Casus yazılım, klavye dinleme, arka kapılar, şifre kırıcılar
	Yazılım korsanlığı ve diğer ürünlerin korsanlığı	Yazılım ürünlerin kurulumlarını kırmak veya kaynak kodlarını ele geçirmek veya tersine mühendislik gibi yöntemlerle üretmek. CD, VCD, Ses CD'si ve DVD gibi çoklu ortam ürünlerinin kopyalanması.
	Bilgisayarla sabotaj ve gasp	Bilgisayar sistemlerine yönelik hasar verici veya yıkıcı girişimler. Virüsler, ağ taşkını {flooder), mesaj sağanakları (spam), bot ağı (botnet), DoS (hizmet aksattırma saldırıları).
	Bilgisayar sahtekârlığı	Kişileri bilgisayar ve İnternet ortamında yanıltarak maddi ve manevi zararlara uğratma. Kredi kartı, sahte bahis, ATM ve telefon sahtekârlığı, saadet zincirleri. Aldatmaca (hoax), şehir efsanesi (urban legend), sazan avlama (phishing), web sahtekârlığı (web scam) - dolandırıcılığı (fraud)
Yasadışı ve Zararlı İçerik		Özellikle İnternet üzerinde yanıltıcı, yasa dışı ve ahlak dışı, özellikle çocukların kötüye kullanımına yönelik içerikler.
Diğer Saldırılar	Hayata saldırı	Parasal menfaatlerle bilgisayarın kötüye kullanımı dışında insanların hayatına mal olacak girişimler. Örneğin hastane bilgisayarlarını veya uçuş kontrol sistemlerini bozma.
	Örgütlü suç	Daha karmaşık bir yapıda bir grup tarafından yönetilen suçlar.
	Elektronik savaş	Rakip şirket, düşman ülke gibi hasımlara yönelik yürütülen saldırılar.

Kaynak: CANBEK ve Diğerleri, S.421

Bilişim suçları ülkemizde de hızla artmaktadır. Bu konuda sadece Ankara Emniyet Müdürlüğü'nce 2001-2004 yılları arasında tespit edilen bilişim suçlarının sayısında ciddi bir artış olduğu görülebilmektedir. Bu artış Şekil 15'de de gösterilmektedir.[49] Bu artış oranı ele alındığında, günümüzde bilişim suçlarının ciddi bir artış sergilediği ve artmaya da devam ettiği değerlendirilmektedir.

[49] A.G.E., , S.417



Şekil 15 : Ankara Emniyet Müdürlüğü Bilişim Suçları İstatistiği

Kaynak: A.G.E., S.422

Bahse konu bilişim suçlarının genel özellikleri, etkileştiği alanlar ve kullandığı yöntemler genel hatları ile Şekil 16'da gösterilmektedir.



Şekil 16 : Korsanlık Hareketi ve Siber Terörizm Genel Analizi

Kaynak: A.G.E, S.142

- **Mahremiyet, İhlali ve Muhtemel Sonuçları**

Bunlara ek olarak güvenlik ihtiyacının ortaya çıkmasına ve artmasına neden olan diğer bir etken de mahremiyetin ihlalidir denilebilir. Kurumsal ya da kişisel haberleşme ve verilerin gizliliğinin ihlal edilmesi bu ihtiyacı tetikleyen en önemli nedenlerden birisidir denilebilir.

Birleşmiş Milletler Genel Kurulu'nda 1948 yılında ilan edilen ve ülkemizde 27 Mayıs 1949'da Resmi Gazete'de yayınlanan insan Haklan Evrensel Beyannamesi'nin 12. maddesi, kişisel gizliliği "özel yaşam" olarak şu şekilde ifade etmektedir.

"Madde 12- Kimsenin özel yaşamına, ailesine konutuna ya da haberleşmesine keyfi olarak karışılamaz, şeref ve adına saldırılamaz. Herkesin bu gibi karışma ve saldırılara karşı yasa tarafından korunmaya hakkı vardır."[50]

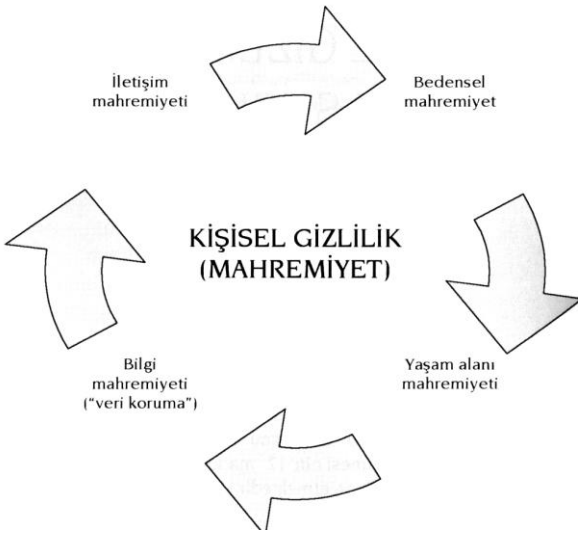
Westin, mahremiyeti, kişinin özgürce gerçekleştirdiği tavır ve davranışlarını, başkalarının bilmesine razı olmasıyla alakalı bir kavram olarak ifade etmiştir. Bloustein'a göre bu kavramı insan kişiliği ile ilişkilendirilmiştir. Gavison'a göre mahremiyet, birbirinden bağımsız olan gizlilik, kamunun bir ferdi olma ve yalnızlık gibi üç unsuru içermektedir. Calcutt Komisyon raporunda ise mahremiyet, *"kişinin şahsı hayatının, evinin, ilişkilerinin, ailesinin ve evraklarının korunması hakkı"* olarak tanımlanmıştır. Beaney'e göre mahremiyet, insanın, fikirlerini ve sevinçlerini başkalarıyla paylaşmada, kendisi ve sorumlu olduğu şahıslar hakkında bilgi elde etme ve açıklamada, fiziksel yaşam ortamına müdahalede özgürce karar verme hakkıdır.Lusky mahremiyeti "*kişinin kendi hakkındaki bir bilgiyi nerede, ne zaman, nasıl ve kimlere vereceği konusunda karar verme hakkı"* olarak yorumlamıştır. Banisar, mahremiyeti dört grupta sınıflandırmıştır: Bilgi, haberleşme, fiziki ve coğrafi alana ait mahremiyet. [51]

Banisar'ın gruplaması Şekil 17'de ifade edilmeye çalışılmıştır.

---

[50] A.G.E, S.417

[51] Hakan YILDIRIM - Volkan KAPLAN - Tuncay ÇAKMAK - Cem Cihangir ÜSTÜN, **Her Şeyi E-leştirdik**, 2. Baskı, Başkent Klişe, Ankara, Mayıs 2003, S.151



Şekil 17 : Kişisel Gizlilik Öğeleri

Kaynak: CANBEK ve Diğerleri, S.418

Gary Marx, haberleşme izlemenin, insanın özel hayatını ihlal ettiğini, insanlar arası güven bunalımına yol açtığını, sosyal düzenin temellerini sarstığını ve insanlarda otoriteye karşı gelme isteği ve paranoya oluşturduğunu belirtmektedir. Zahit İMRE'ye göre, özel hayatına ilişkin konuşmaların başkalarınca öğrenildiğini bilen bireylerden kurulu bir toplumun çehresi değişir. Bunun sonucunda da korkak ve esir psikolojisine sahip insanlardan kurulu bir toplum ortaya çıkar. bunu önlemek için hukuki esas ve kuralları tespit ederek gerekli hukuki tedbirlerin alınması zorunludur. "Özel hayat duvarlarla çevrilmelidir." şeklindeki bir Fransız atasözü de mahremiyetin hukuk tarafından korunması gereken bir temel hak olduğu şeklinde yorumlanabilmektedir. [52]

Sonuçta mahremiyetin ihlali ve haberleşme izleme, bir yönüyle anayasal bir hakka uygun olmayan bir durum, diğer yönüyle de bilgi toplumunda polisinin suçla mücadelede kullanması gereken bir araçtır. Anayasal hak ile polisiye hizmetler arasındaki denge de yapılacak ve alınacak hukuki düzenleme ve önlemler ile sağlanmalıdır.

[52] A.G.E, S.152

2.2.2.4. Bilişim Güvenliğine Yönelik Tehdit ve Saldırılar

- **Tehdit, Saldırı ve Saldırgan**

Tehditler güçlerini, kabiliyetlerini ve özelliklerini sistemlerdeki zafiyetlerden (açıklıklardan) alırlar. Bu güvenlik zafiyetleri birçok sebepten dolayı ortaya çıkabilmektedir. Güvenlik sisteminin tasarımındaki veya kurulumundaki zayıflıklar bu zafiyetlere neden olan en büyük etkenlerdir. Sistemlerdeki zafiyetler olduğu sürece saldırılara maruz kalınma ihtimali vardır. Aslında daha doğru bir tabir ile sistemlerde zafiyetler olmasa bile daima saldırılara maruz kalınabilir. Aradaki fark birisinde zarar görülür diğerinde ise zarar görülmez. Yıkılmayacak ve halka açık bir köprüye, köprüden geçerken sertçe vurulmasının engellenecek bir tarafı ya da anlamı yoktur. Tüm tehditler, güvenliğin tüm çeşitleri ve unsurları için geçerlidir.

Saldırı denilince akla ilk olarak sistemlere saldıran bir kırıcı gelmemelidir. Direkt olmayan saldırılar denilen saldırılar da mevcuttur. En basit örnek olarak bilgisayarlara virüs bulaşması verilebilir. Bunlar hedeflenmiş saldırılar değildir. Ancak saldırı olarak nitelendirilmektedirler. Çünkü virüs bulaşması gerçekleşmiş ise, bu sistemin zafiyetinden kaynaklanan bir sorundur. Sistemin zafiyetini kullanarak sisteme zarar veren her şey saldırı olarak nitelendirilebilir.

Saldırılar Temel Olarak 3 Ana Kategoride Toparlanabilir.

- Intrusion denilen sisteme izinsiz giriş (sisteme tecavüz).
- Destruction denilen sisteme gerek maddi gerek manevi zarar verme.
- Theft denilen hırsızlıktır.[53]

Hırsızlık denildiğinde akla sadece bilgi hırsızlığı gelmemelidir. Önemli bir cihazınız fiziksel olarak çalınıp götürülmesi de hırsızlık kategorisi altına giren saldırı metodudur. O cihaz çalındığında sistem saldırılara karşı korumasız ya da daha az korumalı hale gelebilmektedir. Ya da içerisindeki bilgiler değerli olduğundan saldırı amacına ulaşmış olabilir.

[53] "**Güvenlik Nedir?**", http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.html (Şubat 2009)

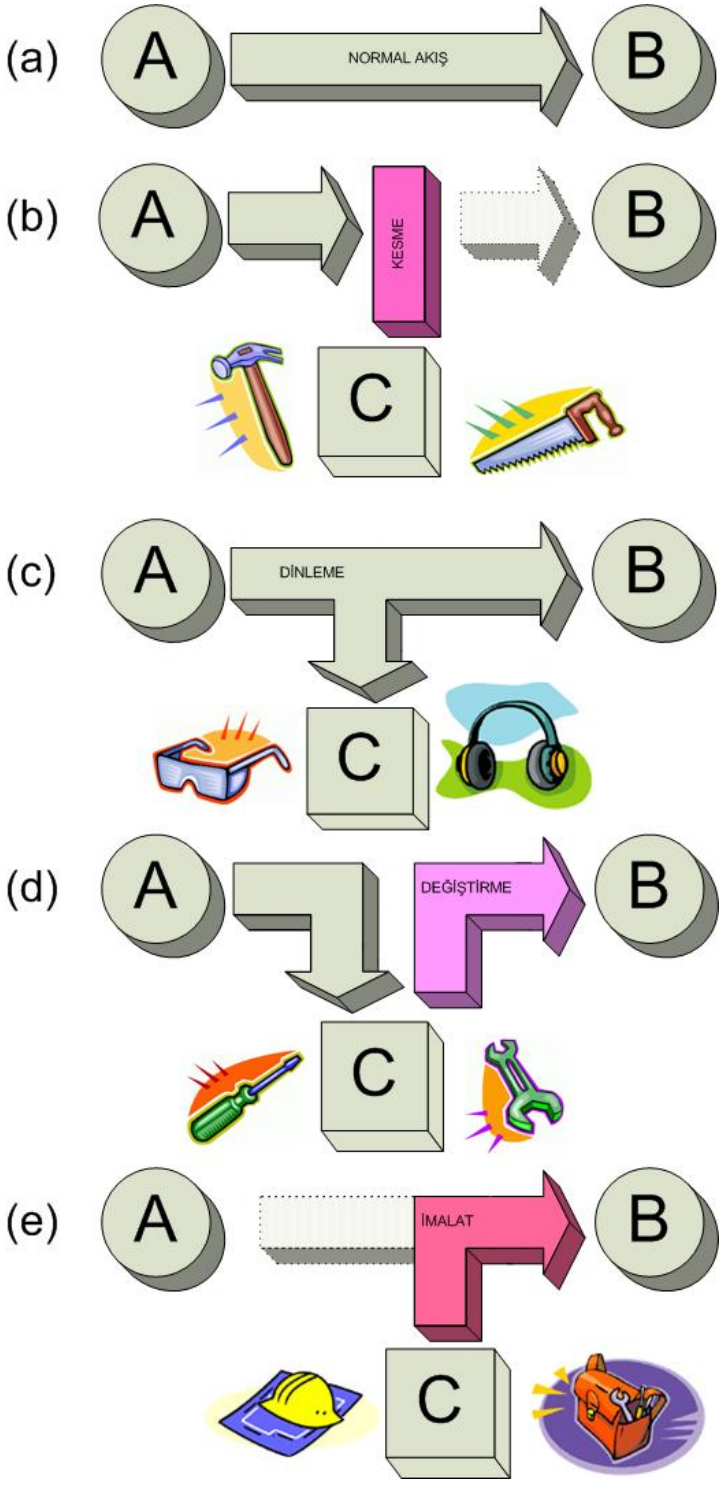
Bu saldırılar dışarıdan yapılabileceği gibi içeriden de yapılabildiğinden ve saldırı denildiğinde sadece dışarıdaki kişilerden gelen tehditler algılanmaması gerektiğinden güvenlik zincirinin en zayıf halkası "İNSAN" dır denilebilir.

Unutulmamalıdır ki, toplam saldırıların %55'i içeriden gerçekleştirilmektedir.[54]

- **Saldırı Karakteristikleri Ve Sınıflandırmaları**

Bilgi akışına yapılan saldırılar dört değişik karakteristik sergileyebilmektedir. Bunlar yarıda kesme (interruption), gizli dinleme (intercept), değiştirme (modification) ve imalat veya üretim (fabrication) olarak adlandırılmaktadır. Şekil 18'de bu karakteristikler temsilen ifade edilmeye çalışılmıştır.

[54] http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/msids.pdf (Ocak 2009)



Şekil 18 : Saldırı Tehdit Karakteristikleri

(a) Normal bilgi akışı. (b) kesme (c) dinleme (d) değiştirme (e) imalat veya üretim.

Kaynak: CANBEK ve Diğerleri, S.161

Bunlar;

- Yarıda kesmede, kaynak ve hedef arasındaki bilgi akışına engel olunarak iletişimin koparılmasıdır. Burada sistemin değerli bir varlığı (yazılım, belge, veri, bilgi, vb.) yok edilir, erişilemez veya elde edilemez hale getirilir.

- Gizli dinlemede, kaynak ve hedef arasındaki enformasyon ya da iletişim içerisindeki bilgi, saldırgan tarafından çeşitli şekillerde elde edilerek okunur. Burada yetkisiz taraf sistemin değerli bir varlığına yani bilgiye erişim kazanmaktadır. Pasif saldırı olarak da tanımlanır. Gizli dinleme dışındaki diğer tüm karakteristikler aktif saldırı olarak sınıflanmaktadır.

- Değiştirmede, kaynak tarafından hedefe gönderilmek istenen bilgi, araya girilerek elde edilir ve bu bilgi üzerinde değişiklik yapılarak, hedefe kaynaktan geliyormuş gibi tekrar gönderilir. Burada, yetkisiz taraf sisteme erişim hakkını kazanmakla kalmaz; ayrıca sistemin değerli bir varlığını değiştirir ve hedefe sanki kaynaktan geliyormuş gibi tekrar gönderilir. Burada kaynak ve hedef arasında, iletilen bilginin yetkisiz kişi ya da kişilerce elde edilmemesini, elde edilse dahi anlaşılır olmamasını ve ya değiştirilip değiştirilmediğini kontrol eden bir mekanizma yoksa, saldırgan amacına ulaşmış ve kaynak ve hedefe yanlış bilgi gönderme yetisine sahip olabilecektir.

- İmalat veya üretimde ise, saldırgan tarafından üretilen suni bir bilgi, sanki kaynaktan geliyormuş gibi hedefe gönderilmektedir. Burada yetkisiz taraf, sisteme sahte nesneler ekler. İlk iletişimi başlatma isteğinin hangi taraftan geldiği önemli değildir. Saldırgan iletişimi kendisi başlatabileceği gibi, isteğin karşı taraftan gelmesini de bekleyerek amacına ulaşabilmektedir. Burada da değiştirmede önemli olan kimlik doğrulama ve iletişim güvenliğindeki gereksinimler ve konular aynen geçerlidir.

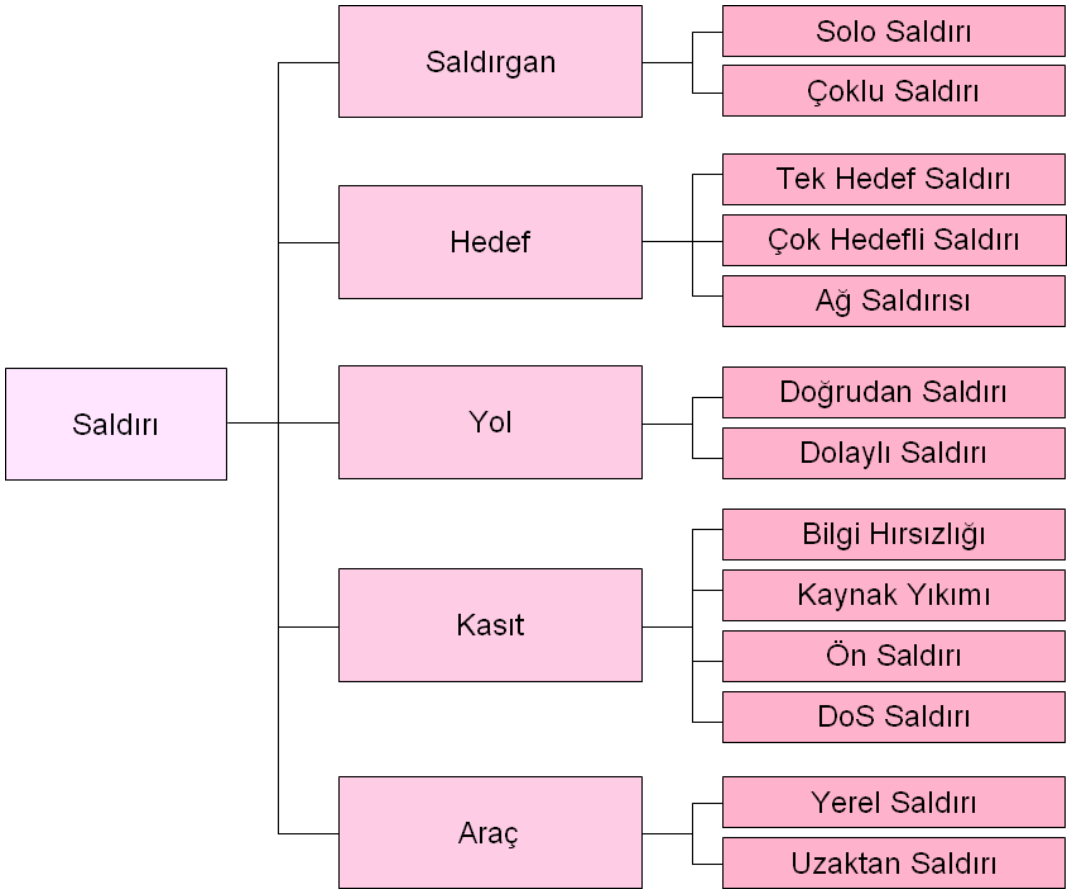
Tablo 5'de her bir saldırı karakteristiğin hangi güvenlik unsuruna karşı yapıldığı, bu saldırıda kullanılan yaklaşımlara örnekler ve her bir saldırı karakteristiğine karşı geliştirilen genel çözüm önerileri gösterilmeye çalışılmıştır.

Tablo 5
Güvenlik Unsurlarına Yapılan Saldırılar, Kullanılan Yaklaşımlar ve Bu Saldırılara Çözümler

Saldırı	Hedef Güvenlik Unsuru	Saldırı Şekli	Çözüm
Yanda kesme (interruption)	Erişilebilirlik (availability)	Donanım yıkımı	Etkin bir çözüm yok.
		İletişim hatlarına fiziksel hasar verme	
		Gürültü yayma	
		Rota (routing) şaşırtma	
		Program ve dosya silimi	
		DoS (hizmet aksattırma) saldırıları	
Gizli dinleme (intercept)	Gizlilik (confidentiality) ve kişisel gizlilik (privacy)	Gizli dinleme (Eavesdropping)	Şifreleme/şifre çözme
		Hat izleme	
		Paket yakalama	
		Sistemle uzlaşma	
Değiştirme (modification)	Bütünlük (integrity)	Veritabanı kayıtlarını değiştirme	Her bir mesaj paketi için sayısal imza kullanımı
		İletişimde gecikmelerden yararlanma	
		Donanımda değişiklik yapma	
İmalat veya üretim (fabrication)	Asillik (authenticity)	Veritabanına yeni kayıt ekleme	Kimlik kanıtlama (authentication)
		IP kandırma ile yeni ağ paketi ekleme	
		Sahte e-posta veya bölge adlan kullanma	

Kaynak: A.G.E., S.162

Yapılan saldırı türlerini sınıflandırmak mümkündür. Tek bir saldırı için çok farklı sınıflandırmalar yapılabilmektedir. Çoklu, tekli, tek ve çoklu kaynak ve hedeflere göre çeşitli sınıflamalar yapılabilmektedir. Saldırıların sınıflandırılma şeması Şekil 19'da gösterilmeye çalışılmıştır.



Şekil 19 : Saldırıların Sınıflandırılması

Kaynak: A.G.E., S.163

Tek bir saldırgan tarafından gerçekleştirilen saldırılar, en genel saldırılardır. Bu saldırıların saptanması diğer saldırı türlerine nazaran daha kolaydır. Sistem korunmasızlık saldırıları ve yetkisiz erişim, bu saldırı türündedir.

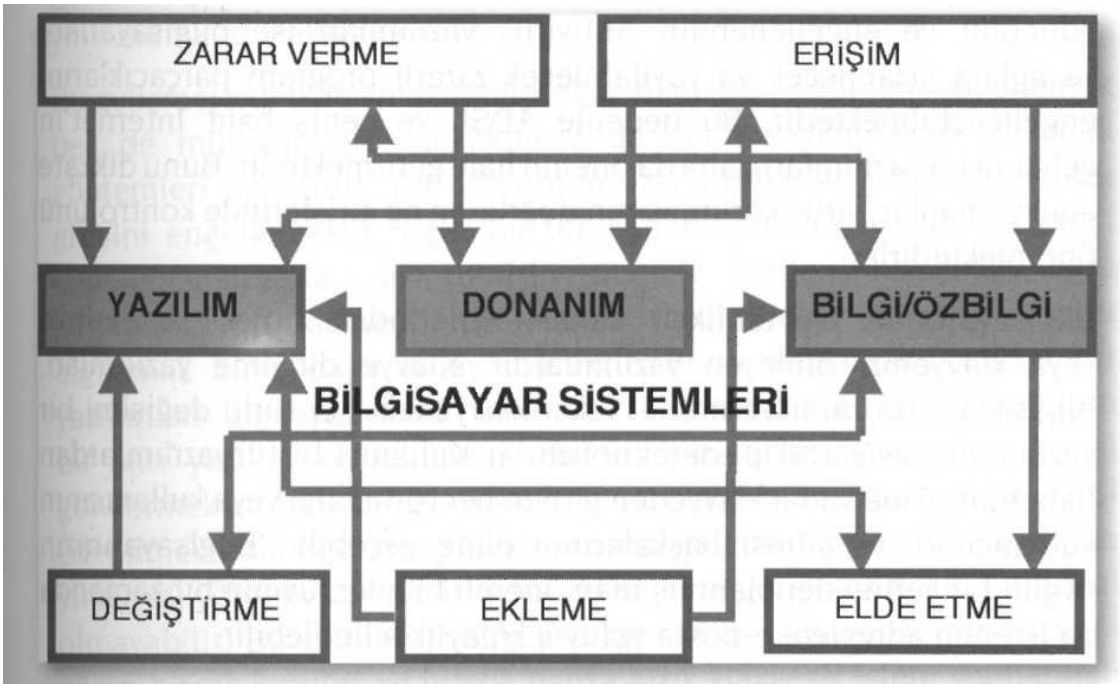
Birden fazla saldırgan tarafından gerçekleştirilen saldırılar, çoklu saldırı olarak adlandırılır. IP kandırma (spoofing), e-posta bombardımanı ve ağ taşkını (flooding) saldırıları bu tür saldırılardandır.

"Back Orifice" ve Winnuke saldırıları gibi saldırılar ise tek hedefe yönelik saldırılardır. Anormal paket yayınlama saldırıları, tarama saldırıları ve anonim FTP saldırıları ise çok hedefli saldırılardandır.

DNS kandırma (DNS Spoofing), yönlendirme (router) saldırıları ile DoS ve DDOS çeşidi (Denial of Service, hizmet aksattırma) saldırılar, ağ saldırı türüdür.

Arabellek taşması, "ölümüne ping" (ping of death) saldırıları doğrudan saldırılar arasındadır. Sisteme giriş (login) yapıldıktan sonra gerçekleştirilen saldırılar ise yerel saldırılara örnek verilebilir.

Yapılan saldırıların, saldırılan unsur ve hedefine göre yapılan başka bir sınıflandırma da aşağıda yer almaktadır. Şekil 20'de unsurlar ile hedef arasındaki ilişki belirtilmeye çalışılmıştır.



Şekil 20 : Bilgi ve Bilgisayar Sistemlerine Yapılan Saldırı Türleri

Kaynak: A.G.E., S.79

- **Başlıca Genel Saldırı Türleri**

Başlıca saldırı türleri arasında, kaynak kod istismarı, gizli dinleme (eavesdropping), sosyal mühendislik ve insan hatası, hizmet aksattırma saldırıları (DoS), dolaylı saldırılar, arka kapılar (backdoor), doğrudan erişim saldırıları ve kriptografik saldırıları saymak mümkündür.

  - **Kaynak Kod İstismarı**

Tüm sistemde kullanılan (işletim sistemi için hazırlanan sistem programları dâhil) ve tüm yazılımlarda var olabilecek arabellek taşması (buffer overflow), CGI betikleme (scripting) hataları, SQL zerki (SQL injection) ve şifreleme hataları gibi yazılım kusurları kaynak kod istismarı saldırıları için kullanılmaktadırlar. Eğer bir uygulamada bu tür bir zafiyet varsa, bu tür bir saldırı ile karşı karşıya kalınması durumunda, bahse konu uygulamanın kontrolü ele geçirilebilir veyahut o uygulamanın beklenmedik bir şekilde çalışmasına neden olunabilir.

- **Gizli Dinleme**

Kablolu veya kablosuz iletişim kanalları üzerinden aktarılan verinin, kötü niyetli üçüncü kişiler tarafından araya girilerek alınmasını ifade etmektedir. Eğer bu gerçekleşirse, kaynaktan hedefe giden verinin değiştirilerek sanki kaynaktan geliyormuş gibi hedefe, gönderilmesi bile mümkün olabilmektedir. İngilizce "eavesdropping" (saçak damlası) olarak adlandırılır. Bu saldırı aktif ve pasif olmak üzere iki yolla gerçekleştirilmektedir.

- **Hizmet Aksattırma Saldırıları (Denial of Service, DoS)**

Bu saldırının tek amacı bir bilgisayar, sunucu veya ağa, kaldırabileceğinden daha fazla yük bindirilmesi demektir. Bu sayede sistemin kullanılmaz hale gelmesi sağlanır. Bu tip saldırılar genelde bant genişliği, boş disk alanı, bağlantı sayısı veya karşılık verme zamanı gibi bilgi işlem kaynaklarının tüketilmesi, yönlendirme (routing) bilgileri gibi yapılandırmaların ve fiziksel ağ bileşenlerinin bozulması ile sistemlerin hizmet veremez hale gelmesini içermektedir.

Bu tip saldırılar genel olarak en kolay ve en etkili saldırı türüdür. Bu tip saldırılar yine genellikle, saldırmak istenen sistemde herhangi bir zafiyet bulunamaması durumunda, kişi ya da kişilerin amaçlarına ulaşmak için başvurdukları bir yoldur. Başka bir kullanım alanı ise, kişilerin kendilerini tatmin için kullanımıdır.

- **Arka Kapılar (Backdoor)**

Bilgisayar sistemleri üzerinde sıradan taramalar ve incelemeler ile bulunamayan ve normal kimlik kanıtlama süreçlerini atlatan veya daha önceden kurulan ve hazırlanan bir sistemden haberdar olan kişiye o bilgisayara ya da sisteme uzaktan erişmeyi sağlayan yöntemlerdir. Bu saldırının gerçekleşebilmesi için, ya kullanılan yazılım ya da sistemin yazılması ya da hazırlanması esnasında bilinçli olarak, hazırlayan kişi ya da kişilerce bu zafiyetin yapılandırılması, ya da hazırlama esnasında göz önüne

alınamayan bir zafiyetin daha sonradan başkaları tarafından ortaya çıkartılması gerekmektedir.

- **Sosyal Mühendislik veya Toplum Mühendisliği**

Bu da bir saldırı türüdür. Bu saldırı türünce saldırgan, ilgilendiği bilgisayar sistemini kullanan veya yöneten meşru kullanıcılar üzerinde psikolojik ve sosyal numaralar ile, sisteme erişmek için gerekli bilgiyi elde etmeye çalışmaktadır.

Sosyal mühendislikte kullanılan ilginç yöntemler, risk alanı, korsanın uyguladığı taktik ve bunlara karşı mücadelede yapılması gerekenler Tablo 6'da listelenmeye çalışılmıştır.

Tablo 6
Sosyal Mühendislikte Kullanılan Yöntemler

Risk Alam	Korsan Taktiği	Mücadele Stratejisi
Telefon (Yardım Masası)	Taklit ve inandırma	Çalışanların ve yardım masasının telefonla hiç bir şekilde şifre veya diğer *gizli* bilgilerin verilmemesi için eğitilmesi
Binaya giriş	Yetkisiz fiziksel erişim	Sıkı kimlik kartı güvenliği, çalışanların eğitilmesi ve güvenlik görevlilerin çalıştırılması
Ofis	Omuz sörfü	Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız.
Telefon (Yardım Masası)	Yardım masası aramalarında taklit etme	Bütün çalışanlara yardım masası desteği alabilmesi için tekil bir PIN numarası atanması.
Ofis	Kimsenin olmadığı açık odalar bulabilmek için koridorlarda dolaşma	Bütün misafirlere işyerinden bir refakatçi sağlanması
Posta odası	Sahte notlann sokulması	Posta odasını kilitle ve izlemeye tabi tut
Makine odası – Santral	Erişmeye teşebbüs, cihazların kaldırılması ve gizli bilgileri elde edebilmek için bir protokol analizcisi eklenmesi	Santral, sunucu odaları v.s. her zaman kilitli tut ve cihazların güncel dökümünü tut
Telefon ve PBX	Telefon görüşme ücreti erişimi çalma	Şehirlerarası, milletlerarası ve cep telefonu aramalarını kontrol et, konuşmaları izle, aktarmaları reddet
İş yeri atık deposu (dumpster)	Çöplük karıştırma	Bütün çöp kutularını güvenli ve izlenen alanlarda tut. Önemli belgeleri kesme makinesiyle yok et, manyetik ortamdaki verileri sil.
intranet - İnternet	Şifre araklamak için intranet veya İnternet üzerinde sahte yazılımların oluşturulması ve konulması	Sistem ve ağ değişikliklerinden sürekli haberdar olma, şifre kullanımı eğitimi
Ofis	Hassas belgelerin çalınması	Belgelere gizlilik derecesi ver ve bu belgeleri kilitli yerlerde sakla
Genel - Psikolojik	Taklit ve ikna	Bütün çalışanları sürekli uyanık tutarak ve eğitim programlarına tabi tutarak bilinçlendirme

Kaynak: A.G.E, S.167

- **Dolaylı Saldırılar**

Bu saldırı türünde, saldırgan direkt olarak kendisi saldırmaz ve saldırısını kendi bilgisayarı üzerinden gerçekleştirmez. Daha önceden bir şekilde ele geçirilen ve saldırganın vereceği komut ve emirleri birebir yerine getirmeye hazır olan bilgisayar, bilgisayarlar ya da sistemler (Hayalet bilgisayar (zombie computer)) üzerinden, onlara bağlanarak, onlara hedef gösterip saldırıya geçmelerini emretme ve başlatma şeklinde gerçekleştirilmektedir.

- **Doğrudan Saldırılar**

Dolaylı saldırıların tam tersine bu saldırı türünde saldırgan, kendi sistemi üzerinden kendisi direkt olarak hedefine saldırmaktadır. Aynı zamanda bu saldırı türü, bir bilgisayar sistemine doğrudan fiziksel erişime sahip olan bir kişinin yaptığı saldırıları da içermektedir.

- **Kriptografik Saldırılar**

Şifrelenmiş veri ve bilgilerin şifresini kırmak veya şifreli veriyi anlaşılır hale getirmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Bunlar arasında kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack - MITM), salt şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ya ilişkili anahtar (related key attack) saldırılarını içermektedir.[55]

- **Kimlik Hırsızlığı**

Kimlik hırsızlığı (identity theft), bir başkasına ait kişisel bilgilerin, yasa dışı yok ya da yöntemlerle ele geçirilerek, yetkisiz olarak kullanılması suretiyle işlenen bir dolandırıcılık yöntemi ve saldırı türüdür. Bu saldırı türünde kredi kartı ve internet bankacılığı bilgileri, şifre ve parolalar,

[55] A.G.E., S.157 - 169

elektronik posta, MSN sohbet programı parolaları ve diğer önemli kişisel bilgilerinin bir başkası tarafından çıkar sağlamak amacıyla kullanılmaktadır.

Bu saldırıların neden olduğu zararların boyutlarına bakacak olursak, hiç de azımsanmayacak büyüklükte zararlara neden olduklarını görülebilmektedir.

- **Saldırgan Türleri**

Bilişim sistemlerine bilinçli ya da bilinçsiz olarak, çeşitli yollarla, suç sayılan eylemleri gerçekleştirmek için girişimlerde bulunarak başaramayan ya da amacına ulaşan kişi ya da kişilere verilen isim ya da takmak adlar çeşitlilik arz etmektedir. Başlıca saldırgan türlerine aşağıda değinilmeye çalışılmıştır.

2.2.2.4.1. Kara Şapkalı Korsan

Hacker olarak da bilinen korsanlar, teknik bilgilerini ve yazılımların zafiyetlerini kullanarak, erişimleri izne bağlı yerlere, izinsiz erişebilen kişiler olarak tanımlanmaktadır. Sanal dünyanın mafyaları ya da bilgisayar korsanları olarak da isimlendirilmektedirler.[56]

Kara şapkalı korsanlar bilgisayar güvenliğinin en önemli düşmanlarıdırlar. Ancak kendilerini kötü birer karakter olarak görmezler. Onarla göre kötü olan, güvensiz yazılım satan ve altında yatan temeli bilmeden, kendileri tarafından yazılan uygulamaları kullanarak sistemlere saldıran betik keratalarıdır. Teknik bilgi seviyeleri beyaz şapkalılarla eş değerdir.[57]

Bu saldırganların, kendilerine özgü ahlaki kuralları ve dünya görüşleri vardır. Örneğin, güvenli yazılım satmayan ya da sattıktan sonra gerekli geliştirme ve iyileştirmelerini yapmayan, program ve sistem satıcıları, uygulamalarını sattıkları kişileri kandırmakta ve haksız kazanç elde etmektedirler. Bu nedenle hem bu kişilerin hem de bu zafiyetleri takip

[56] Onur OKTAY, **"Türkiye'de Hacker Grupları ve Faaliyetleri-1",** http://turk.internet.com/haber/yazigoster.php3?yaziid=16661 (Eylül 2009)
[57] CANBEK ve Diğerleri, S.120

etmeyerek, satıcılardan gerekli iyileştirme ve güncelleştirmeleri talep etmeyen güvenlik ve sistem yöneticilerinin cezalandırılmaları gerekmektedir. Genellikle çalandan çalmak gibi bir mantık denilebilir. Genellikle, uygulamalarda ve sistemlerde kendilerinin bulduğu zafiyetleri kendileri için, kendi faydalarına farklı çıkarlar için kullanmaktadırlar.

2.2.2.4.2. Beyaz Şapkalı Korsan

Bu korsanlar ise, bilgisayar ya da sistemlerindeki zafiyetlerin ve bu yolla elde edilen diğer güçlerin kötüye kullanımına karşı olan ve bu yönde faaliyetler yürüten kişilerdir. Kara şapkalı korsanlardan farkları genel ahlaki kurallara bağlılıklarıdır. Beyaz şapkalı korsanlar da en az kara şapkalı korsanlar kadar derin bir sistem bilgisine ve tecrübesine ve ileri yeteneklere sahiptir. Bu bilgi, tecrübe ve yeteneğini sistemlerin ve kullanıcıların yararına kullanırlar.[58]

Onlara göre çalmak, kimden olursa olsun yanlıştır ve eğer ortada bir yanlış var ise kanuni yollardan halledilmelidir. Ancak bunları ortaya çıkartmak için her türlü araştırma ve yasal yola başvurulmalıdır.

2.2.2.4.3. Betik Kerataları (Script Kiddy)

Betik kerataları, şapkalı korsanlar veya başka kaynaklardan temin ettikleri uygulama ve ya komut dizilerini, belirtilen yol ve şekillerde çalıştırarak sistemlere, amaçlarına yönelik saldırılardan bulunan ya da bulunmaya çalışan kişiler olarak tanımlanmaktadırlar.

2.2.2.4.4. "Üzerine Gel ve Tıkla" Korsanlar, Tıklama Korsanları (Click Kiddy)

Bu kişiler (bilişim korsanı heveslisi tıklama kerataları), hiç bir teknik bilgi ve becerisi olmayan, şapkalı korsanlar tarafından hazırlanan ve son günlerde yaygınlaşan, oldukça etkili ve oldukça iyi bir kullanıcı arabirimi ile hiç bir beceri gerektirmeden kullanılabilen araçlarla istedikleri bir hedefe saldırı düzenleyebilen kişiler olarak tanımlanmaktadırlar.[59]

---

[58] A.G.E, S.118
[59] A.G.E, S.126

Güvenlik dünyasında, uygulamaları direk olarak kullanarak, uygulamaların çalışma temellerini anlamaya ve kendilerini geliştirmeye çalışmadan, kötü maksatlı olarak saldırıda bulunduklarından pek sevilmezler.

2.2.2.4.5. Sistem Kırıcılar (Cracker)

Sistem kırıcılar ya da kısaca kırıcılar, bir bilgisayar ya da sistemine, o sistem ya da bilgisayarda, önceden var olan ve bilinen bir zafiyeti kullanarak izinsiz olarak giren; bir yazılım ya da uygulamadaki güvenlik veya lisans korumasını atlatabilen ya da bir güvenlik sisteminde kasten gedik açan kişilerdir. Kırıcılar çoğunlukla kendilerini bilişim korsanı (hacker) olarak tanımlamaktan hoşlansalar da; kırıcı (cracker), bilişim korsanı (hacker) ile aynı anlam ifade etmemektedir. Çünkü kırma işi genellikle, korsanlık kadar hayranlık uyandıran bir zekâ isteyen bazı gizemli atlatmalar içermez. Bunun yerine, hedef alınan sistem üzerinde bulunan yaygın zayıflık noktalarını sömüren ve genelde bilinen numaraların, şaşılacak bir sebat içinde tekrarından oluşmaktadır.[60]

2.2.2.4.6. Web Sitesi Tahrifatçıları

Web sitesi tahrifatı, herhangi bir Internet sitesinin giriş sayfasının (home page) aslının bir sistem kırıcı tarafından değiştirilmesidir. Elektronik grafiti olarak da adlandırılan web sitesi tahrifatı son zamanlarda siyasi güdüleri olan siber kınayıcılar veya korsanlık eylemcileri (haktivist) tarafından mesajlarını yaymak amacıyla da kullanılmaktadır. Tahrifatçı genel olarak tahrif ettiği web sayfasının giriş sayfasına amacına yönelik mesajını ve takma adını yazar. Bu sayede tahrifatçılar arasında popüler, saygı duyulan ve en iyi olmaya çalışır.[61]

[60] A.G.E, S.126
[61] A.G.E., S.127

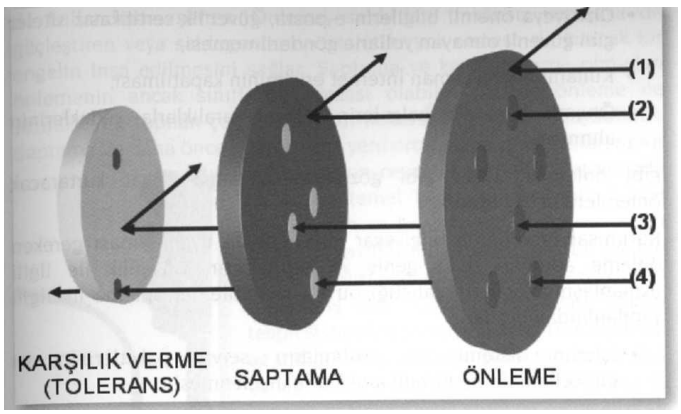
2.2.2.4.7. Hacktivizm ve Hacktivistler

Hactivizm, İngilizce hacking (korsanlık) ve activism (hareket) birleşimi şeklinde türetilen bir terimdir. Bir haktivist (korsanlık hareketçisi), savunduğu siyasi, sosyal veya dini bir mesajı yaymak için bilişim teknolojilerini kullanan kişilerdir. Kendilerine hedef olarak popüler ve herkesçe bilinen ve vermek istediği mesajı yerleştirdiği zaman, geniş kitlelere anında iletilebilecek Web sitelerini hedef olarak almaktadırlar. İleri düzey ve derinlemesine bilgi ve tecrübeye ihtiyaçları yoktur.[62]

Amaçları sistemlere saldırmak ya da zarar vermek değildir. Tabiî ki buradaki zarardan kasıt, sistemlerin çalışamaz hale gelmesi ya da kontrol altına alınması değildir. Aslında maddi ya da manevi zarar ya da kazanç da değildir. Ancak tahrif edilen sitenin, tahrif edildikten sonra, eski haline getirilene kadar, şirket ya da kurumun kaybettiği ya da kazanamadığı maddi miktar ve itibar ortaya çıkmaktadır. Bu da dolaylı da olsa bir nevi zarar olarak kabul edilebilir.

2.2.2.5. Bilişim Güvenliği Süreçleri

Bilişim Sistemlerinde Bilgi güvenliğinin ideal yapılandırılması üç süreç ile gerçekleştirilir. Bu süreçler, önleme (prevention), saptama (detection) ve karşılık vermedir (response ya da reaction). Bu süreçler Şekil 21'de belirtilmiştir.



Şekil 21 : Bilişim Güvenliği Süreçleri

Kaynak: A.G.E., S.89

[62] A.G.E., S.138

Şekil 21'den de anlaşıldığı gibi, 4 farklı saldırı 1 den 4'e kadar gösterilmiştir. Bu saldırılardan, (1) numaralı saldırı, hemen önleme safhasında engellenirken; (2), (3) ve (4) numaralı saldırılar bu safhada önlenememiştir. Önleme sürecini atlatan bu saldırılardan (2) numaralı saldırı, saptama aşamasında tespit edilip, bertaraf edilirken; (3) ve (4) numaralı saldırılar, saptama aşamasından da geçebilmiştir. Belirlenen tolerans ile tasarlanmış son aşama olan karşılık verme safhasında, (3) numaralı saldırı önlenirken; bütün aşamaları atlatıp geçen (4) numaralı saldırı, bütün güvenlik süreçlerini geçip, sisteme zarar vermiştir.

- Önleme

Önleme, güvenlik sistemlerinin ve güvenlik çalışanlarının en çok üzerinde durduğu süreçtir. Genellikle fiziksel önlemleri ve güvenlik alanında ilk öncelikle alınması gereken en basit güvenlik tedbirlerini içerir.[63]

- Saptama

Güvenlik duvarları, saldırı tespit sistemleri (intrusiondetection system), ağ trafiği izleyiciler, kapı (port) tarayıcılar, bal çanağı (honeypot) kullanımları, gerçek zamanlı koruma sağlayan anti virüs ve anti casus yazılım araçları, dosya sağlama toplamı (checksum) kontrol programları ve ağ koklayıcı (sniffer) algılayıcıları, saptama sürecinde kullanılan en başta gelen yöntem ve cihazlardan bazılarıdır.[64]

- Karşılık verme

Karşılık verme, önleme süreci ile baş edilemeyen ve saptama süreçleri ile belirlenmiş saldırı girişimlerine, mümkünse anında veya en kısa zamanda cevap vererek saldırıyı bertaraf etmek olarak tanımlanabilir. Saptama sürecinde belirlenen ve tespit edilen saldırı türleri, bu tespite cevap verecek bir sistemin olması ile anlam kazanabilir. Tespit etmenin bir

[63] A.G.E., S.89
[64] A.G.E., S.91

faydası yoktur. Tespit edilen saldırının engellenmesi gerekmektedir. Bu engelleme de bu aşamada gerçekleştirilmektedir.[65]

[65] A.G.E., S.91

3. KAMUSAL WEB GÜVENLİĞİ

3.1. Kamu Güvenliği ve Kamu Kurumlarında Güvenlik

3.1.1. Kamu ve Kamu Kurumlarında Güvenlik Kavramları

Kamu kelimesinin iki anlamı vardır. Bunlardan birincisi, halk hizmeti gören devlet organlarının tümü, diğeri ise bir ülkedeki halkın bütünü, halk, amme dir.[66]

Görüldüğü gibi kamu kelimesi hem, halka hizmet eden devlet organlarının tümünü, hem de devlet organlarının hizmet ettiği halkı temsil etmektedir.

Kamu düzeni ise, toplumun bütününü ilgilendiren düzen anlamındadır. Kamu kavramı, bu örneklerde olduğu gibi "resmiyeti" ve "genelliği" anlattığı kadar, "özel"in, "gizlilik"in ve "kapalı"lığın zıddı olarak "açık"lığı, "halka ait oluş"u ve "görülebilir"liği de ifade etmektedir. Kamu malları, kamu hayatı ve halk (amme) kütüphanesi gibi.[67]

Kamu güvenliği konusuna, güvenik türleri bölümünde değinilmişti. Hatırlamak için tekrar değinmek gerekirse;

Kamu Güvenliği: Vatandaş ve kamu üst sınırı arasında kalan ve kamusal alan ile özel alanın toplamından oluşan bir çerçeveyi, tanımlanmış kurallar altında koruma ve kamunun kendisine ait korunma faaliyetlerini de içeren süreç kamu güvenliği kavramıdır. Ek olarak, kamu güvenliği, toplum anlamına gelmesi itibariyle vatandaşları; devlet anlamına gelmesi itibariyle de yönetim ünitelerini kapsayan faaliyetler bütünüdür. Bu açıdan vatandaş-devlet ilişkilerinin düzenlenmesinde etkin bir rol oynamaktadır.[68]

---

66 http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=kamu (Eylül 2009)

67 **"Kamu Yönetimi",** http://www.ekodialog.com/kamu_yonetimi/kamu_yonetimi_nedir.html (Mayıs 2009)

68 İstanbul Ticaret Üniversitesi Dergisi, S.14

Başka bir deyişle kamu güvenliği; "*bir devlette kolluk kuvvetleri hizmetleri ile halka sağlanan can ve mal güvenliğidir*."[69]

Aşağıda da görüldüğü gibi, kamu aynı zamanda halkın tamamı manasına da geldiğinden ve halkın tamamı da milleti yani ulusu oluşturduğundan burada ulus güvenliğinden de bahsetmekte fayda olacaktır.

Millet, "*Çoğunlukla aynı topraklar üzerinde yaşayan, aralarında dil, tarih, duygu, ülkü, gelenek ve görenek birliği olan insan topluluğu, ulus. Bir yerde bulunan kimselerin bütünü, herkes*"[70] demektir.

Ulusal Güvenlik**:** Yukarıda anılan faaliyetlerin yürütülmesi başta olmak üzere, alınması gereken tedbirlerin ve devletin, siyasi, sosyal, dış politik, ekonomik ve askeri çıkarlarının korunması ve geliştirilmesi için stratejik seviyede yapılan çalışmalar bütünüdür.[71]

Ulus ve halk bir toplumu meydana getirdiğinden burada toplum teriminden de bahsetmek gerekmektedir.

Toplum; "*Aynı toprak parçası üzerinde bir arada yaşayan ve temel çıkarlarını sağlamak için iş birliği yapan insanların tümü, cemiyet*:"[72]

Görüldüğü gibi toplum, iş birliği yapan bir unsurdur. Günümüz gelişen ve gelişmekte olan devletler, bu iş birliğini hızlı ve güvenli bir şekilde yapmak için iyileştirme ve geliştirmelerde bulunmakta ve bulunmaya da devam etmekte ve sonunda ortaya bilgi toplumu çıkmaktadır.

Bilgi toplumu; "*yeni temel teknolojilerin gelişimiyle bilgi sektörünün, bilgi üretiminin, bilgi sermayesinin ve nitelikli insan faktörünün önem kazandığı, eğitimin sürekliliğinin ön plana çıktığı, iletişim teknolojileri, bilgi*

---

[69] **"Kamu Güvenliği",** http://sozluk.bilgiportal.com/nedir/kamu%20güvenliği (Mayıs 2009)

[70] http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=millet (Mayıs 2009)

[71] İstanbul Ticaret Üniversitesi Dergisi, S.14

[72] http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=toplum (Haziran 2009)

otoyolları, elektronik ticaret gibi yeni gelişmeler ile toplumu ekonomik, sosyal, kültürel ve siyasal açıdan sanayi toplumunun ötesine taşıyan bir gelişme aşaması olarak tanımlanabilir."[73]

- **Bilgi Toplumunun Özellikleri**

Bilgi toplumunun temel özellikleri ve geleceğe olan etkileri aşağıda özet olarak belirtilmeye çalışılmıştır.

- Bilgi toplumunun gelişme dinamiğini, bilgisayar teknolojisi, bilgisayara dayalı enformasyon ve internet şebekeleri ile veri bankaları yönlendirmektedir.
- Bilgi toplumunda, bilgi önemli ve temel kaynaktır. Bireyler ve toplumlar bu temel kaynağa sahip olmak için yarış halindedirler.
- Hızla bilgi artışı, değişme ve gelişmenin temel kaynaklarıdır.
- Sanayi toplumunun aksine bilgi toplumu, çok merkezli ve yaygın olacaktır.
- Bilgi toplumunda toplumsal değerlerin zayıflaması söz konusu değildir.
- Bilgi toplumunun siyasal sistemi katılımcı demokrasi ve büyük ölçüde bilgiye dayanacaktır. Bilim insanlarının düşünürlerin siyasetle doğrudan ve dolaylı etkileri olacaktır.
- Bilgi üretimi ve bilgilerin pazarlanması, bilgi toplumunda yeni iş alanlarının başında gelecektir.
- İş dünyasında bilgi üretenlerin ve çalışanların sayısı çoğalacak, bilgi birikimi; bilgide seçiciliğe yol açacaktır.
- Sanayi toplumunda temel değerler, maddi gereksinimlerin doyumuna dayanırken, bilgi toplumunda temel değerler "amaçlara ulaşmanın verdiği doyumdan kaynaklanacaktır.
- Bilgi toplumunda, sosyo ekonomik sistem alt yapısının üstünlüğü ile kendisini gösteren "gönüllü ve sivil toplum"dan oluşacaktır.
- Eğitim öğretimde süreklilik yerleşecek, okul öğrenimi yanında, yaşamın başlangıcından sonuna kadar aktif öğrenme gereksinimi ön planda olacaktır.
- Belirli konuları öğrenme yerine, "öğrenmeyi öğrenmek" ve "bireysel öğrenme" eğitim sürecinin temeli olacaktır.
- İşlevleri çok gelişmiş bilgisayarlar, çeşitli yayın olanakları, bilgi iletimi ve haberleşmeyi daha kolay hale getirecek ve bu alanda uzaklıklar azalarak dünya gerçekten küçülmüş olacaktır.[74]

Bilgi toplumu, ortaya çıkan faydalardan her bireyin eşit şekilde yararlanmasına önem ve öncelik vermektedir. Bu gerçekleştirildiğinde,

[73] "**Bilgi Toplumu Ve Özellikleri**", http://www.canaktan.org/yeni-trendler/bilgi-toplumu/bilgi_toplumu-ozellik.htm (Temmuz 2009)
[74] http://www.maltepe.edu.tr/05_haber/reh_sempozyum/gulbahar_gul.doc (Temmuz 2009)

toplumda bu durumun korunması, ilerletilmesi ve geliştirilmesi için bir heves, istek ve nu amaca yönelik bir bilinç ortaya çıkmaktadır. Bunun doğru ve eşit bir şekilde sağlanması işi ise hukuk tarafından üstlenilmelidir. Bu noktada, bilgiye erişme ve erişilen bilgiyi özgürce kullanma çok önemli bir rol oynamaktadır. "Kamusal Bilgilere Erişim Özgürlüğü" veya "Bilgi Özgürlüğü" olarak uluslar arası hukukta belirlenen temel çerçeve 4982 sayılı "Bilgi Edinme Hakkı Kanunu" ile ülkemizde de bir ölçüde gerçeklik boyutuna taşınmıştır.[75]

Bilgi toplumunda, bilgiyi paylaşmak için geliştirilen iletişim yolları ve bu yolların ülkeler arasında birleştirilmesi ile dünyada küreselleşme eğilimleri oluşmuştur. Böylelikle bilgi evrensel olmakta ve bilgiye erişim kolaylaşmaktadır. Bu sayede global bir toplum meydana gelmektedir.[76]

Bilgi toplumunda, meydana gelen değişim ve gelişimler nedeniyle, bilgi toplumunun en önemli girdilerinden olan insan faktörü ve bilginin niteliklerinde farklılıklar ortaya çıkmaktadır. Önceleri bilgi hem kişisel hem de kilit bir ekonomik kaynak olarak görülmekte iken, günümüzde bilgi anlamlı tek kaynak olarak görülmekte ve benimsenmektedir. Bilgi toplumunda, geleneksel üretim faktörleri olan doğal kaynaklar, emek ve sermaye ortadan kalkmamakla birlikte ikinci plana düşmektedir. İlk planda bilgi yer almaktadır. Ancak tüm bilgiler değerli ve ön planda değildir. Sosyal ve ekonomik sonuçlar ortaya çıkarabilecek bilgiler önemli olmaktadır. Bu bilgiyi de insan kullanacağından, bilgi toplumunun diğer önemli bir girdisi de insan olmaktadır. Bilgiyi ortaya çıkaracak olan da insan faktörü olduğundan, ortaya bilgi çıkaracak insan faktörlerine yatırım yapmak bilgi toplumunda büyük önem arz etmektedir.[77]

---

[75] **"İletişim Altyapısı",** http://www.bilisimsurasi.org.tr/altyapi/docs/iletisim_altyapisi_taslak_raporu_20040219.doc (Aralık 2009)

[76] **"Bilgi Toplumu",** http://ansiklopedi.turkcebilgi.com/Bilgi_toplumu (Ocak 2010)

[77] "**Bilgi Toplumu Ve Özellikleri**", http://www.canaktan.org/yeni-trendler/bilgi-toplumu/bilgi_toplumu-ozellik.htm (Temmuz 2009)

3.1.2. Kamu Kurumlarında Bilişim Güvenliği

Devlet Planlama Teşkilatı Müsteşarlığı Bilgi Toplumu Dairesi tarafından hazırlanmış olan Bilgi Toplumu Stratejisi Eylem Planı 87 numaralı madde bilgi güvenliği ile ilgili yasal düzenlemeleri içermektedir. Bu maddeye göre ülke güvenliğini ilgilendiren bilgilerin elektronik ortamda korunması ve devletin bilgi güvenliği sistemlerinin geliştirilmesi amacına uygun yasal altyapıyla ilgili düzenlemelerin yapılması ve uygulamaya konulması hedefi ortaya konulmuştur. Bu husus ile ilgili olarak, 2009 hükümet programının e-devlet uygulamalarının yaygınlaştırılması ve etkinleştirilmesi başlığı altında, politika öncelikleri ve tedbirleri kapsamında Ulusal Bilgi Güvenliği'nin sağlanmasına ilişkin yasal düzenleme yapılması hedefi konulmuştur. 2009 hükümet programında ortaya konulan hedefleri gerçekleştirmek için T.C. Başbakanlık'ın önderliğinde ilgili kamu kurumlarının katılımı ile e-devlet mevzuat çalışma grubu oluşturulmuştur. Hâlihazırda, çalışma grubu bilgi güvenliği mevzuatının yanı sıra e-devlet düzenlemeleri ile ilgili öncelikleri belirlemekte ve bu konudaki diğer çalışmaları gerçekleştirmektedir.[78]

5070 sayılı elektronik imza kanunu ile birlikte güvenli elektronik imza, elle atılan ıslak imzaya eşdeğer kabul edilmiş ve aynı hukuki sonuçları doğuracağı belirtilmiştir. Kanunların resmî şekle veya özel bir merasime tabi tuttuğu hukukî işlemler ile teminat sözleşmelerinin güvenli elektronik imza ile gerçekleştirilemeyeceği kanunda ifade edilmiştir. (Örn: emlak alım satımı, veraset ve intikal, evlenme gibi işlemler)

Ek olarak Elektronik sertifika hizmet sağlayıcıları, elektronik imzalarla ilgili hizmetleri sağlamalarına rağmen bu kurum ya da kuruluşların elektronik imza kanununun uygulanmasına ilişkin faaliyet ve işlemlerinin denetimi Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.[79]

5809 sayılı elektronik haberleşme kanunu elektronik haberleşme sektöründe düzenleme ve denetleme getiren bir kanundur. Bu düzenleme

---

[78] "*Bilgi Toplumu Stratejisi Eylem Planı*", **Devlet Planlama Teşkilatı Yayınları**, Temmuz 2006 http://www.dpt.gov.tr/DocObjects/Download/2227/Eylem_Plani.pdf (Ocak 2010)

[79] **5070. Sayılı Elektronik İmza Kanunu** http://www.tbmm.gov.tr/kanunlar/k5070.html (Nisan 2009)

ve denetleme unsurları içerisinde bilgi güvenliği ile ilgili hususlar da yer almaktadır. Örneğin, kanunun Madde:4'de ilgili merciler tarafından elektronik haberleşme hizmetinin sunulmasında ve bu hususta yapılacak düzenlemelerde "bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi" ilkesinin göz önüne alınması gerektiği ifade edilmektedir. Kanunla verilen düzenleme ve denetleme görevleri Bilgi Teknolojileri ve İletişim Kurumu tarafından yerine getirilmektedir.[80]

26942 sayılı Resmi Gazete'de yayınlanan "Elektronik Haberleşme Güvenliği Yönetmeliği" elektronik haberleşme güvenliğine ilişkin işletme ve bu işletmelerin yöneticilerinin uyması gereken usul ve esasları düzenlemektir. Bu usul ve esaslar, işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması ile ilgili hususları içermektedir.[81]

Bankacılık Düzenleme ve Denetleme Kurumu, bankalarda bağımsız denetimlerin gerçekleştirilmesi ile ilgili olarak yönetmelik ve tebliğleri hazırlamıştır. Kurumlar yani bankalar bu yönetmelik ve tebliğlerin yürütülmesinden sorumludur. Bankalarda Bağımsız Denetim Gerçekleştirilecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik ve Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ bu mevzuata örnek olarak verilebilir. Banka denetimleri kapsamında, bankaların bilgi güvenliği ile ilgili gerçekleştirdiği aktiviteler de denetlenmektedir.[82]

25897 sayılı Resmi Gazete'de yayınlanan E-dönüşüm Türkiye Projesi Birlikte Çalışabilirlik Esasları Rehberi'nin amacı ise birbiri ile bütünleşmiş, etkin, şeffaf ve basitleştirilmiş iş süreçlerine sahip bir e-devlet yapılanması için kurumların kullanacakları ortak norm ve standartları belirlemektedir. Bu

---

[80] **5809. Sayılı Elektronik Haberleşme Kanunu, Madde: 4,** http://www.tbmm.gov.tr/kanunlar/k5809.html (Nisan 2009)

[81] **26942. Sayılı Resmi Gazete** http://rega.basbakanlik.gov.tr/main.aspx?home=http://rega.basbakanlik.gov.tr/eskiler/2008/07/20080720.htm&main=http://rega.basbakanlik.gov.tr/eskiler/2008/07/20080720.htm (Aralık 2009)

[82] http://www.bddk.org.tr/WebSitesi/turkce/Raporlar/Calisma_Raporlari/Calisma_Raporlari.aspx (Şubat 2010)

rehberin dört numaralı "güvenlik" başlığı altında, bilgi güvenliği yönetim sistemi, ortak kriterler standardı, elektronik imza ve kriptografi ile ilgili birlikte çalışabilirlik esasları yer almaktadır.

T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü tarafından hazırlanan ve 17 Şubat 2003 tarihinde imzalanan "Bilgi Sistem ve Ağları için Güvenlik Kültürü" konulu Başbakanlık Genelgesi, OECD Bilgi Güvenliği ve Kişisel Mahremiyet Çalışma Grubu tarafından hazırlanmış olan rehberin Türkçe çevirisidir. Söz konusu genelge bilgi güvenliği ile ilgili bilinç, sorumluluk, risk değerlendirmesi, güvenlik tasarımı ve uygulama, güvenlik yönetimi gibi hususlar hakkında iyi pratiklere dayanan önerileri içermektedir.[83]

Ülkemizde doğrudan bilgi güvenliğini konu alan bir mevzuat altyapısı henüz bulunmamaktadır. Bankacılık ve haberleşme sektörlerini düzenleyen mevzuatta bilgi güvenliği bir unsur olarak geçmektedir. Ancak bu durum Ulusal Bilgi Güvenliği ile ilgili hususları düzenlemek için maalesef yeterli düzeyde değildir. Hâlihazırdaki, bilgi güvenliği ile ilgili hususları kapsayan genelgeler yürürlükteki kanun ve yönetmeliklere göre bilgi güvenliğine daha çok vurgu yapmakta ve değinmektedir. Öte yandan, bu genelgelerin dayanak olabileceği yönetmelik, tüzük ve kanun olmadığından, genelgeler etkili olamamaktadır. Ülkemizde, bilgi güvenliği mevzuatı ile ilgili çalışmalar Bilgi Toplumu Stratejisi Eylem Planı içerisinde yer alan 87 numaralı eylem maddesi çerçevesinde ve Başbakanlık tarafından yürütülen e-devlet mevzuat çalışmaları kapsamında gerçekleştirilmektedir.[84]

Bilgi toplumu gelişmesine ancak ve ancak bilginin hızlı ve güvenli paylaşımı ile devam edebilecektir. Bunun yolu da bilişim teknolojilerinin kullanılarak istenilen iletişimin, istenilen şekilde, şartlarda ve standartlarda sağlanabilmesidir.

---

[83] **2003/10 sayılı Bilgi Sistem ve Ağları İçin Güvenlik Kültürü Genelgesi,** http://www.basbakanlik.gov.tr/genelge_pdf/2003/2003-0320-02789.pdf (Mayıs 2009)

[84] "**Türkiye'de Bilişim Güvenliği Analizi**", http://www.turkishajan.com/bilisim-suclari-analizi-ve-kriminal-olaylar/turkiye8217de-bilisim-guvenligi-analizi-34075.html (Ocak 2009)

Bu iletişim türlerinden birisi de; bilgisayar sistemleri üzerinden yapılan internet sitesi yayınları olarak bilinen web siteleridir. Tüm iletişim sistemlerinde olduğu gibi web siteleri ile yapılan iletişimde de güvenlik önemlidir. Web siteleri yayınlarında, ister kişisel ister kurumsal olsun, alınması gereken tedbirler ve uyulması gereken adımlar ve standartlar hemen hemen aynıdır. Ayırt edici özellik, kaybedilecek ya da zarar görecek kıymetin değeri ve bunu zararı engellemek ya da azaltmak için feda edilebileceklerdir.

Unutulmamalıdır ki, "*Kurumsal bilişim güvenliği çok bileşenli, önemli ve yönetimi zor bir süreçtir.*"[85]

3.2. Web Güvenliği

Yüksek lisans çalışmamızın inceleme kapsamı olan web güvenliğinin iki yönü bulunmaktadır.

Bunlardan birincisi, başkaları tarafından hazırlanarak yayınlanan web sayfalarını uzaktan ziyaret etme, diğer bir deyişle web sayfalarında gezinme ile ilgili olan güvenlik konularını içermektedir. Bu kısım, kişilerin ya da kurumların, internette gezinirken ziyaret ettikleri web sayfalarından kaynaklı uğrayabilecekleri zararları ve bunları engellemek ya da azaltmak için yapılması ya da alınması gereken önlem ve tedbirleri kapsamaktadır.

İkincisi ve asıl konumuz olan ise, web sayfaları hazırlama ve sunma ile ilgili güvenlik konularını içermektedir. Bu kısım ise, kişilerin ya da kurumların kendileri ya da kurumları ile ilgili iş ya da işlemleri dış dünyaya da kullandırmak ve paylaşmak amacıyla hazırladıkları ya da hazırlattıkları web sayfalarındaki ya da bu web sayfalarının yayınlandıkları sistemlerdeki zafiyetlerden dolayı uğrayabilecekleri zararları ve bu zararları engellemek ya da azaltmak için yapılması ya da alınması gereken önlem ve tedbirleri kapsamaktadır.

Sektörlerin hepsinde son kullanıcıya ya da müşterilerine yönelik ve ya hizmet içi yayın yapan web uygulamaları bulunmaktadır. Web

[85] "**Bilişim Güvenliği Raporu**", Pro-G Bilişim Güvenliği ve Araştırma Ltd., Sürüm 1.1, 2003, S.59 http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf (Ocak 2010)

uygulamalarının işlevi; bulunduğu sektör ve hizmet ettiği amaca bağlı olarak değişmektedir. Bir e-ticaret uygulamasında ürün pazarlaması ve satışı yapılırken, bir sağlık sektörüne ait web uygulamasında ise hayati önem taşıyan bilgiler bulunabilmektedir.

Web uygulamalarında "internet dilleri" olarak da adlandırılan pek çok uygulama dili kullanılmaktadır. HTML, DHTML, XML, XHTML, PHP, ASP, Java, Perl gibi uygulama dilleri, MSSQL, MySQL, PgSQL, CDB, BDB, Oracle gibi veritabanları; Activex, CGI gibi mekanizmalar ve IIS, , Lightttpd, Apache gibi web sunucuları internette kullanılan teknolojilere örnek olarak verilebilirler.

Şimdiye kadar anlatılan saldırı yöntemlerinin hemen hepsi, web hizmetleri de bilişim sistemleri içerisinde değerlendirildiğinden (keşif yapmak, taramak, şifre kırmak, sniffing, spoofing, DoS, DDoS vs...) web tabanlı sistemlere de uygulanabilir. Ancak özel olarak web teknolojilerine karşı kullanılan saldırı yöntemleri de vardır. Bu saldırıların temelinde, web sitesine izinsiz girmeye çalışmak, sitede kullanılan uygulamalardaki güvenlik açıklarından yararlanarak siteyi hack etmek ya da web sunucusundan şirketin ağına sızmak fikirleri vardır.

3.2.1. Web Teknolojilerinde Güvenlik İhtiyacı

Web sistemleri de birer bilgi teknolojileri sistemi olduğundan, bilgi güvenliğine gereken önemin verilmemesi durumunda özel ya da kamu kurum ya da kuruluşlarının ne gibi zararlara uğradığı "Bilişim Güvenliği İhtiyacı" bölümünde anlatılmıştı. Aynı gereklilik nedenleri web güvenliğinde de geçerli olmakla birlikte, web güvenliğini biraz daha önemli kılan bir diğer sebep, diğerlerine nazaran çok daha yoğun kullanılan web sistemlerinin güvenliğine gereken önemin verilmediğidir. Şekil 22'de sektörlere göre web uygulamalarındaki zayıflıkların oranları görülebilmektedir. Buradan da anlaşılmaktadır ki, web sistemleri bu kadar yaygın kullanılmalarına rağmen, web sistemleri yayıncıları, sistemlerinin güvenliği için gerekli önlemleri almamaktadırlar.[86]



Şekil 22 : Sektöre Göre Uygulama Zayıflıkları

Kaynak: "Yazılımcılar ve Denetimciler için Web Uygulamaları Güvenliği", Par.1

Ayrıca, dünya üzerinde Web Uygulamalarının güvenliği ile ilgili çalışmalarda bulunan ve tüm dünyada bu konuda saygın bir yer sahibi olan "WASC" (Web Application Security Consortium) isimli bir Güvenlik Konsorsiyumu vardır. Bu konsorsiyum Amerika'nın Newyork eyaletinde yer alan Hazine Bakanlığı İdaresi Başkanlığı'na "1023" kod isimli form ile yapılan

[86] Onur YILMAZ, **"Yazılımcılar ve Denetimciler için Web Uygulamaları Güvenliği"**, http://docs.google.com/Doc?id=d4w2g9c_1hpj4w7ft (Eylül 2009)

müracaat sonucunda elde edilen "501c3" kurum statüsünde kuruluştur. Bu statüye sahip olan kurum ya da kuruluşlar, Amerika çapında global dokuda, organizasyona destek veren ya da sponsorluk yapan kişi ya da şirketlere, verdikleri destek ya da servis değeri oranı kadar vergiden muafiyet kazanmaktadırlar. Bu statüdeki bu kurum da, kar amacı gütmeyen, alanlarında uzman, WWW için, açık kaynak ve yaygın olarak bilinen en iyi pratik güvenlik standartlarını sunan uluslar arası endüstri öncüleri ve organizasyonel temsilciliklerden oluşmaktadır.

WASC aktif bir topluluk olarak, fikirlerin değiş tokuşunu kolaylaştırır ve birkaç endüstri projesini birleştirerek organize eder. WASC devamlı olarak teknik bilgi, yararlı makale, güvenlik rehberleri ve diğer kullanışlı doküman yayınlar. Dünyanın dört bir yanındaki, ticari, eğitsel enstitüler, uygulama geliştiricileri, güvenlik uzmanları ve yazılım dağıtıcıları, bu kurumun materyallerinden, web uygulama güvenliği ile ilgili ortaya çıkan sorunları çözmede yardımcı olmak için yararlanırlar.[87]

Bu çalışmalarda kullanılan en önemli terim korunmasızlıktır. Bu nedenle öncelikle bu kavramın tanımının yapılması uygun olacaktır. Korunmasızlık (vulnerability), "*ilgili sistem, ağ, uygulama veya protokolün güvenliğini tehlikeye atan; beklenmeyen ve istenmeyen bir olaya sebep olabilecek bir zayıflığın varlığı, tasarım veya gerçekleme hatası olarak tanımlanmaktadır*."[88]

Otomatik test sonuçları, tarama uygulamalarında hiçbir özel ayar yapılmadan yer sağlayıcı sitelerin taranması ile elde edilen verileri içermektedir. Bu data analiz edilirken, interaktif bileşen kullanan tüm sitelerin taranmadığının dikkate alınması önerilmektedir. Uzman bir kişi tarafından otomatik tarama uygulamalarında yapılan geleneksel özelleştirme ayarları, zayıflık tespit etme etkinliğini arttıracaktır.

Beyaz kutu ve kara kutu güvenlik değerlendirme istatistikleri, elle ve otomatik analiz istatistiklerini içermektedir. Bu analizler, otomatik test

[87] http://www.webappsec.org/ (Şubat 2010)
[88] Guttman, E., Leong, L., Malkin, G., Request for Comments: 2504, **Users' Security Handbook**, ISOC, RFC 2504, 1999, S.31

sonuçları elde etmeden kullanılan araçların varsayılan ve özel ayarlamalar yapılarak elde edilen analizlerle, otomatik aramalarla bulunamayan zayıflıkların elle aranması ve kaynak kod analizlerini içermektedir.[89]

- **Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (Payment Card Industry Data Security Standard - PCI DSS) Nedir?**

Ödeme Kartları Endüstrisi Veri Güvenliği Standardı (PCI DSS) kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla uluslararası kabul görmüş ödeme markaları olan American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. International kurumlarınca oluşturulmuş PCI Komitesi tarafından geliştirilmiştir.

PCI DSS, kartlı ödeme sistemlerinde yer alan kurum ve kuruluşlarda bilgi güvenliğini sağlamak için bilgi sistemlerinde bilgi iletimini, bilgi işleyişini ve bilgi depolamayı esas alan 6 temel kriter baz alınarak oluşturulmuş 12 gereksinim kategorisi ve bu kategoriler altında yer alan 200 üzerindeki kontrolden oluşmaktadır. Bunlar Tablo 7'de belirtilmeye çalışılmıştır.

[89] "Web Applıcatıon Securıty Statistics", **Web Application Security Consortium Reports** (WASC), 2008, S.4 http://projects.webappsec.org/f/WASS-SS-2008.pdf (Ekim 2009)

Tablo 7
PCI DSS Kriter ve Kategorileri

TEMEL KRİTER	PCI GEREKSİNİMİ
Güvenli bir ağ oluştur ve bakımını üstlen.	**1.** Kart verisini korumak için firewall kur ve çalışırlığını sağla. **2.** Üretici tarafından oluşturulmuş varsayılan kullanıcı şifreleri ile sistem parametrelerini kullanma.
Kart sahibi verilerini koru.	**3.** Depolanmış kart verisini koru. **4.** Açık genel ağlar üzerinde kart verisi iletimini şifrele.
Güvenlik açıklarını tespit eden programların çalışırlığını sağla.	**5.** Antivirüs yazılımı ve programı kullan ve düzenli olarak güncelle. **6.** Güvenli sistemler ve programlar geliştir ve bakımını yap.
Güçlü erişim kontrol ölçümleri oluştur.	**7.** Kart bilgisine erişimi yalnızca bilinmesi gereken prensibi ile kısıtla. **8.** Bilgisayar erişimi olan herkese tekil erişim kimliği belirle. 9. Kart bilgisine fiziksel erişimi kısıtla.
Ağları düzenli olarak gözlemle ve test et.	10. Ağ kaynaklarına ve kart verisine erişimi izle ve gözlemle. 11. Güvenlik sistemlerini ve işleyişini düzenli olarak test et.
Bilgi güvenliği politikasının işleyişini sağla.	12. Çalışanlar ve sözleşmeliler için bilgi güvenliğini açıklayan bir politika hazırla.

Kaynak: Sertaç ÖZİNAL, **"PCI DSS Nedir? ",** http://www.btnet.com.tr/wps/portal/teknoloji-ekonomisi/egilimler/detay?wcm.haberId= btnethaber_1231424270390 (Mart 2009)

- **PCI DSS Yararları**

Bilindiği gibi bilgi güvenliği her türlü işletmede, özellikle kartlı ödeme sistemlerinde dikkate alınması gereken hassas ve çok önemli bir konudur. PCI DSS, 12 kategorisi ile kart bilgisini taşıyan, işleyen ve saklayan kurum ya da kuruluşların bilgi güvenliğine uyum süreçlerini yönetmekte ve bu kurum ya da kuruluşlarda bilgi güvenliği disiplininin oluşmasına katkıda bulunmaktadır. Kartlı ödeme sistemi içerisinde yer alan kurum ve kuruluşlarda gerek kart kabul eden, gerek kart çıkaran gerekse kart işlemlerini çalıştıran tarafların her hangi birinde bilgi güvenliğinin sağlanmadığı durumda kart bilgilerini açığa çıkma olasılığı nedeniyle bu sistem içerisinde yer alan diğer kurum ve kuruluşlarda da güvenlik riski oluşmaktadır. PCI DSS uyumu ile kartlı ödeme sistemleri içinde yer alan tüm kurum ve kuruluşların veri güvenliği riskinin en aza inmesi amaçlanmaktadır.[90]

[90] A.G.E. Par. 1

- PCI DSS Uyumu

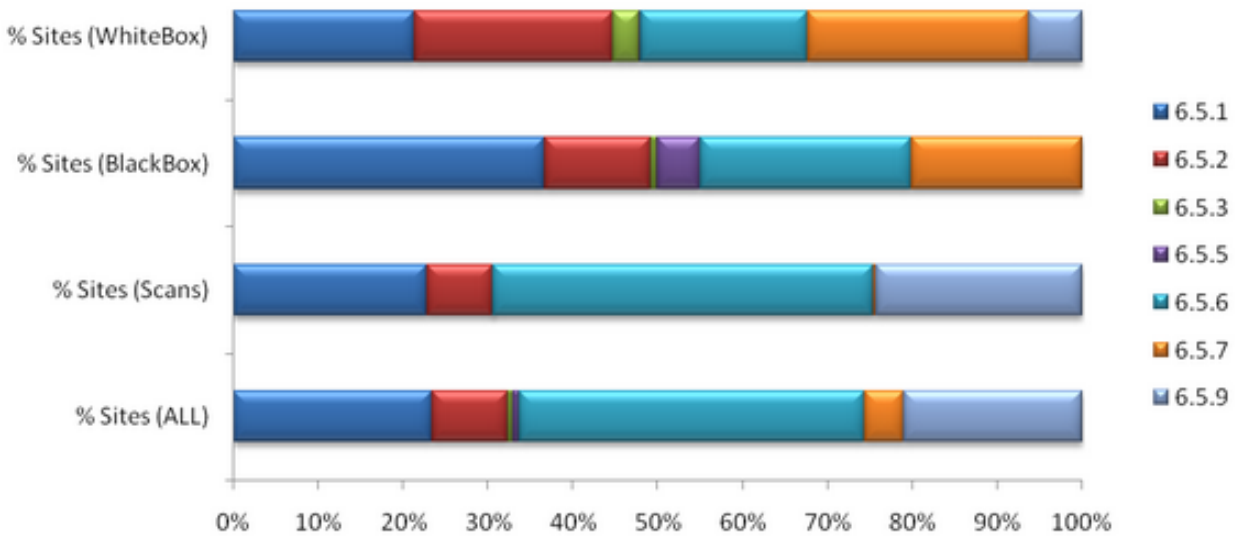
PCI DSS uyumu kontrolleri, VISA ve MasterCard kuruluşlarınca belirlenmiş kriterler doğrultusunda PCI DSS uyumu için gerekli PCI Council tarafından onaylanmış yetkili firmalar (Approved Scanning Vendor - ASV) tarafından; ya uzaktan yapılan güvenlik tarama testleri (Vulnerability Scan) ya da Hem Vulnerbility Scan hem de standarddaki 12 gereksinim kategorisi altında yer alan 200'den fazla kontrol için hazırlanmış olan güvenlik değerlendirme prosedürleri (Security Assessment Procedures) baz alınarak yapılan yerinde denetimler ile gerçekleştirilmektedir.

PCI Council tarafından yetki verilmiş QSV listesine PCI Council, VISA ve MasterCard kuruluşlarının web sitelerinden erişilebilmektedir.

3 tarama çeşidinde de yapılan ve Şekil 23'de belirtilen incelemelerde, PCI DSS in temel güvenlik gereksinimleri olan ve aşağıda belirtilen zafiyetlerin, taranan sitelerde bulunma yani PCI standartlarının bu maddelerine uymama durumlarının tarama çeşidine göre dağılımları belirtilmeye çalışılmıştır.

- 6.5.1 Cross-site scripting (XSS)
- 6.5.2 Injection flaws. particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
- 6.5.3 Malicious file execution
- 6.5.5 Cross-site request forgery (CSRF)
- 6.5.6 Information leakage and improper error handling
- 6.5.7 Broken authentication and session management
- 6.5.9 Insecure communications

PCI DSS standartlarına uyulmama sayılarının geneline bakıldığında, standart taramalarda en fazla olarak information leakage, CSS ve insecure communications bulunmakta, ancak özel taramalarda Injection flaws ve Broken authentication and session management zafiyetlerinin de daha yüksek oranda bulunabildiği görülmektedir.



Şekil 23 : PCI DSS Standartlarına Göre Yapılan İncelemelerde Bu Standartlara Uymayan Sitelerin Tarama Biçimine Göre Dağılımı

Kaynak: "Web Application Security Consortium Reports", S. 16

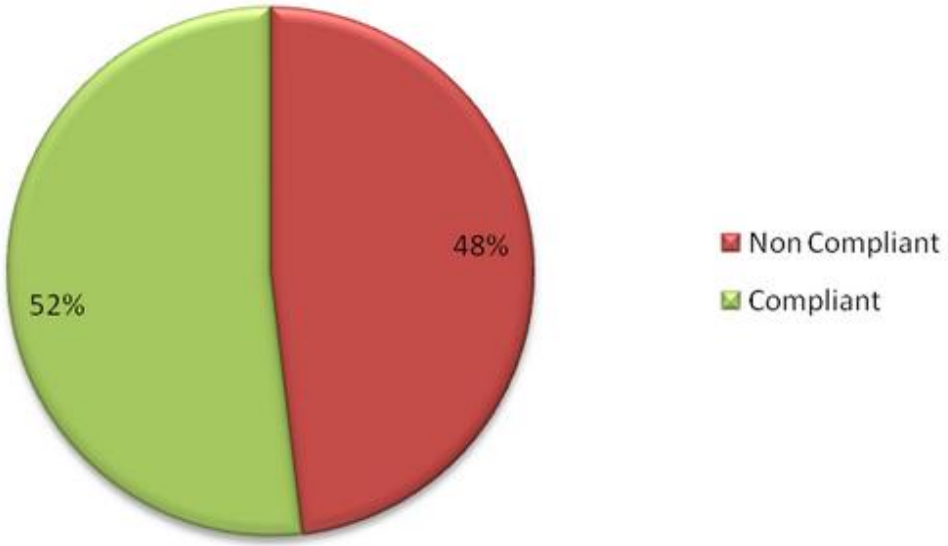
Durum genel olarak Şekil 24'de ifade edilmeye çalışıldığı gibi değerlendirildiğinde, sitelerin PCI DSS standartlarına uyumluluk oranlarının %10.38 olduğu, ancak bu oranın standart taramalarda %8.42, derinlemesine taramalarda %13,67 ve özel taramalarda %1,33 olduğu görülmektedir. Buradan da anlaşılmaktadır ki, aslında siteler güvenlik standartlarına neredeyse hiç uymamakta, uyamamakta ya da uymaya çalışmamaktadırlar.



Şekil 24 : Tarama Şekillerine Göre Web uygulamalarının PCI DSS Standartlarına Uygunluk Oranları

Kaynak: A.G.E., S.16

Sitelerin PCI DSS standartlarından ASV gereksinimleri (genel olarak kabul gören tarama dağıtıcıları - Approved Scanning Vendors - ASV) ne göre yapılan taramalarda sonucu elde edilen Şekil 25'de ise, sitelerin %52 si temel gereksinimleri karşılayarak PCI DSS standartlarına uygunluk göstermekte, ancak %48 i temel PCI standartlarına dahi uygunluk gösterememektedir. Bu veriler, sitelerde iş ya da işlem yaparken kişilerin kendilerini ne derecede güvende hissetmeleri gerektiği konusunda fikirler vermektedir.



Şekil 25 : Web Uygulamalarının PCI DSS Standartlarına Genel Olarak Uygunluk Oranları

Kaynak: A.G.E., S.17

3.2.2. Web Teknolojilerine Yönelik Tehdit ve Saldırılar

- **Kimlik Doğrulama**
  - **Kaba Kuvvet**

Kişilerin kullanıcı isimlerinin, parolalarının, kredi kart numaralarının veya kriptografik anahtarlarının tahmin edilmesi için kullanılan otomatik bir deneme yanılma işlemidir. Birden fazla çeşidi ve yöntemi bulunmaktadır.

  - **Yetersiz Kimlik Doğrulama**

Bir web sitesinin saldırgana, beklenen ve istenen yani yasal ve olması gereken bir kimlik doğrulama gerçekleştirmeden hassas bilgi içeriğine ya da fonksiyonlara erişim izni vermesiyle gerçekleşir.

  - **Zayıf Parola Kurtarma Denetimi**

Bu terimde zayıf olan parola değildir, parola kurtarma denetimidir. Bir web sitesinin saldırganın illegal olarak bir başkasının parolasını ele geçirmesine, değiştirmesine veya kurtarmasına izin verdiği durumdur.[91]

- **Yetkilendirme**
  - **Yetki/Oturum Bilgisi Tahmin Etme**

Bir web sitesi kullanıcısını taklit etme / edebilme (kullanıcının rolüne girme) durumudur.

  - **Yetersiz Yetkilendirme**

Bir web sitesinin erişim kontrol sisteminin, yetkisiz kişi ya da kişilerce erişilmemesi gereken hassas bilgi içeriğine ya da fonksiyonlarına yetkisizlere erişim izni vermesidir.

---

[91] "*Tehdit Sınıflandırması*", **Web Application Security Consortium Reports**, 2004, S. 5 http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.tr.pdf (Haziran 2009)

- Yetersiz Oturum Sonlandırma

Web sitesinin yetkilendirme için kullandığı eski oturum kimlik bilgisi veya numarasının saldırgan tarafından tekrar kullanılmasına imkanı verilmesidir.

- Oturum Belirleme

Web kullanıcısını, bilinen bir değerdeki oturum numarasını kullanmaya zorlayan saldırı tekniğidir.[92]

- İstemci Taraflı Saldırılar
  - İçerik Sahteciliği

Bir kullanıcının bir web sitesindeki belirli içeriğin meşru olduğuna ve bu içeriğin harici bir kaynağa ait olmadığına inandırılmasını sağlayan bir saldırı tekniğidir.

- Siteler Ötesi (Arası) Betik Yazma

Web sitesinin saldırgan tarafından belirlenen ve hazırlanan çalıştırılabilir bir kodu normal bir kullanıcıya göndermesi ve bu kodun kullanıcı web tarayıcısına ziyaret edilen site tarafından yüklenerek çalışmasıyla gerçekleşen bir saldırı çeşididir.[93]

- Komut Çalıştırma
  - Ara Bellek Taşması

Bir uygulamanın akışının, o uygulamanın kullanması için ayrılan sistemin RAM (Random Access Memory) adı verilen hafızasının dışında farklı kısımlarının üzerine yazılarak değiştirmesiyle gerçekleşen saldırılardır.

[92] A.G.E., S. 5
[93] A.G.E., S. 5

- **Dizgi Formatı Saldırısı**

Uygulamaya ayrılmış hafıza alanlarına dizgi formatlama kütüphanelerinin özellikleri yardımıyla erişilerek, söz konusu uygulamanın akışının değiştirilebildiği saldırılardır.

- **LDAP Enjeksiyonu**

Kullanıcıların sağladığı bilgi girdilerinden LDAP ifadeleri (komutları) oluşturan web sitelerini istismar etmek için kullanılan bir saldırı metodudur.

- **İşletim Sistemi Komut Saldırıları**

Uygulama girdilerinin manupilasyonu ile işletim sistemi komutlarının çalıştırılarak web sitelerinin istismar edilmesini sağlayan saldırı metodudur.

- **SQL Enjeksiyonu**

Sistemde yer alan bilgi girdilerinden, sistemdeki zafiyetten dolayı, SQL ifadelerinin (komutları) çalıştırılabilmesi ile web sitelerinin istismar edilebildiği bir saldırı metodudur.

- **SSI Enjeksiyonu (Server-side Include)**

Saldırganın web uygulamasına kod göndermesine ve bu kodun web sunucuda lokal olarak çalışmasına neden olan, sunucu taraflı istismar etme metodudur.

- **XPath Enjeksiyonu**

Kullanıcıların sağladığı bilgi girdilerinden XPath sorguları oluşturan web sitelerini istismar etmek için kullanılan bir saldırı metodudur.[94]

[94] A.G.E., S. 6

- **Bilgi Açığa Çıkarma (Bilgi İfşası)**
    - **Dizin İndeksleme/İndeksleme**

Ana sayfanın mevcut olmadığı ya da görüntülenemediği durumlarda, talep edilen dizindeki tüm dosyaları listeleyen bir web sunucu fonksiyonudur.

    - **Bilgi Sızması**

Saldırgana sistemi istismar etmede yardım edebilecek yazılım geliştirici yorumları, hata mesajları, kullanılan dil, sunucu ya da servislere ait bilgilerin web sitesinde açığa vurulmasıdır.

    - **Yol Takibi**

Web sunucusu ana dizini dışında bulunan dosyalara, dizinlere ve komutlara erişimi sağlayan bir saldırı metodudur.

    - **Tahmin Edilebilir Kaynak Konumu**

Gizlenmiş web sitesi içeriğini ve fonksiyonlarını ortaya çıkarmak için kullanılan bir saldırı metodudur.[95]

- **Mantıksal Saldırılar**
    - **Fonksiyonelliğin Kötüye Kullanımı**

Web sitesinin kendi özelliklerinin ve fonksiyonlarının erişim kontrol mekanizmalarının kaynaklarını tüketme veya bu mekanizmaları atlatmak amacıyla kullanılmasını sağlayan saldırı metodudur.

    - **Servis Dışı Bırakma**

Web sitelerinin normal kullanıcılara verdiği hizmeti engellemek adına gerçekleştirilen saldırı metodudur.

[95] A.G.E., S. 6

- **Yetersiz Anti-Otomasyon**

Web sitesinin sadece elle gerçekleştirilebilmesi gereken bir işlemin saldırgan tarafından otomatik olarak yapılabilmesine izin verilmesi durumudur.

- **Yetersiz İş Denetimi (Tasdiki)**

Web sitesinin hedeflenen uygulama akışı kontrolünün atlatılabilmesi durumudur.[96]

Bahse konu bu tehditlerin, uluslar arası değerlendirmelerdeki isimleri, PCI DSS Risk seviyeleri, zafiyet yeri ve etki ettiği yerlerin sınıflandırması Tablo 8'de belirtilmeye çalışılmıştır.

Tablo 8
Web Risk Gruplandırma Seviyeleri, Sebep Ve Etkisine Göre Zayıflık Gruplandırmaları

Tehdit Sınıflandırması	PCI DSS Risk Seviyesi	Zaafiyet Yeri	Etkilenen Yer
Abuse of Functionality	Orta	Kod	Sunucu
Brute Force Attack	Kritik	Yönetim	Sunucu
Buffer Overflow	Hayati	Kod	Sunucu
Content Spoofing	Yüksek	Kod	Ziyaretçi
Credential/Session Prediction	Kritik	Kod	Sunucu
Cross-Site Scripting	Kritik	Kod	Ziyaretçi
Cross-Site Request Forgery	Yüksek	Kod	Ziyaretçi
Denial of Service	Yüksek	Yönetim	Sunucu
Format String Attack	Hayati	Kod	Sunucu
HTTP Request Splitting	Kritik	Kod	Ziyaretçi
HTTP Response Splitting	Kritik	Kod	Ziyaretçi
HTTP Request Smuggling	Kritik	Yönetim	Ziyaretçi
HTTP Response Smuggling	Kritik	Yönetim	Ziyaretçi
Integer Overflow	Hayati	Kod	Sunucu
LDAP Injection	Hayati	Kod	Sunucu
Mail Command Injection	Yüksek	Kod	Sunucu
OS Commanding	Hayati	Kod	Sunucu
Path Traversal	Kritik	Kod	Sunucu
Predictable Resource Location	Yüksek	Yönetim	Sunucu
Remote File Inclusion	Hayati	Kod	Sunucu
Routing Detour	Yüksek	Kod	Sunucu

[96] A.G.E., S. 7

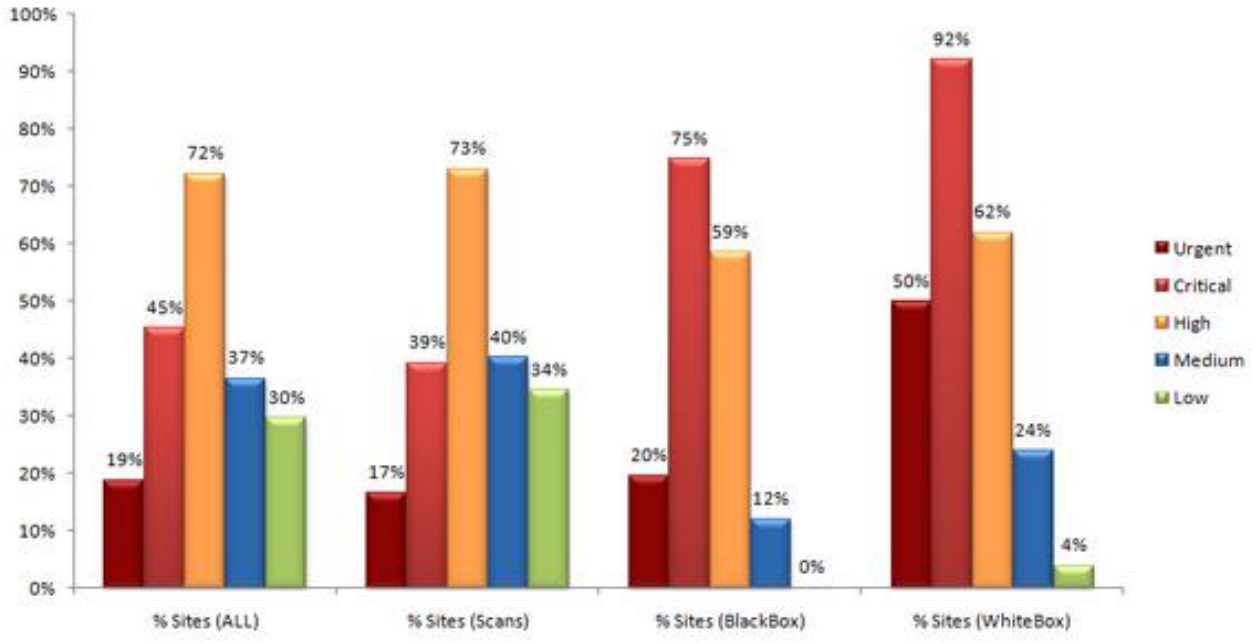
Tehdit Sınıflandırması	PCI DSS Risk Seviyesi	Zaafiyet Yeri	Etkilenen Yer
SOAP Array Abuse	Yüksek	Kod	Sunucu
SSI Injection	Hayati	Kod	Sunucu
Session Fixation	Kritik	Kod	Sunucu
SQL Injection	Hayati	Kod	Sunucu
URL Redirectors	Orta	Kod	Ziyaretçi
XPath Injection	Hayati	Kod	Sunucu
XML Attribute Blowup	Yüksek	Kod	Sunucu
XML External Entity	Yüksek	Kod	Sunucu
XML Entity Expansion	Yüksek	Kod	Sunucu
XML Injection	Kritik	Kod	Sunucu
XQuery Injection	Hayati	Kod	Sunucu
Application Misconfiguration	Orta	Yönetim	Sunucu
Directory Indexing	Yüksek	Yönetim	Sunucu
Fingerprinting	Low	Yönetim	Sunucu
Improper Parsing	Hayati	Kod	Sunucu
Improper Permissions	Hayati	Yönetim	Sunucu
Information leakage	Yüksek	Yönetim	Sunucu
Insecure Indexing	Yüksek	Yönetim	Sunucu
Insufficient Anti-automation	Orta	Kod	Sunucu
Insufficient Authentication	Kritik	Kod	Sunucu
Insufficient Authorization	Kritik	Kod	Sunucu
Insufficient Data Protection	Yüksek	Yönetim	Sunucu
Insufficient Process Validation	Orta	Kod	Sunucu
Insufficient Session Expiration	Kritik	Kod	Sunucu
Insufficient Transport Layer Protection	Orta	Yönetim	Ziyaretçi
Server Misconfiguration	Orta	Yönetim	Sunucu

Kaynak: A.G.E., S.19 - 23

Aşağıdaki istatistikler, WASC tarafından yapılan web güvenlik taramalarında değerlendirilen 12.186 site ve 97.554 adet değişik önem derecesindeki zayıflıkların analizlerini içermektedir. Zayıflık analizleri PCI DSS standartlarına uygun olarak gerçekleştirilmiştir.

Şekil 26'da, 3 farklı zafiyet tarama çeşidine göre yapılan inceleme sonuçları ortak olarak değerlendirilmiş şekilde yer almaktadır. Görüldüğü gibi zafiyet olmayan web sitesi bulunmamaktadır. Ancak tarama çeşidine göre zafiyet türü ve oranının değiştiği görülmektedir. Görüldüğü gibi, standart tarama araçları ile yapılan taramalarda "Yüksek" önem derecesine sahip zafiyetler çoklukla bulunabilmekte iken, blackbox ve whitebox

taramalarında "Hayati" ve "Kritik" zafiyetlerin daha etkin ve çoklukla bulunduğu tespit edilmiştir. Bu da, web siteleri ve sunucularının hazırlanması ve kurulması aşamasında gerekli güvenlik unsurlarına ve adımlarına dikkat edilmediğini ile birlikte hazırlanan web sitelerinin hiç birisinin %100 güvenli olmadığını göstermektedir.



Şekil 26 : Tarama Çeşidine Göre Zayıflık Bulma İhtimal Oranları

Kaynak: A.G.E., S.6

Şekil 26'nın detaylandırılmış tablo halTablo 9'da görüntülenmektedir.

Tablo 9
Tehdit Sınıflandırması Genel İstatistikleri – Tüm Tarama Sonuçları İçin.

Tehdit Sınıflandırması	PCI DSS Risk Seviyesi	Zaafiyet Yeri	Etkilenen Yer	Zaafiyet Sayısı	Web Sitesi Sayısı	% Zaafiyet	% Web Sitesi
Abuse of Functionality	Orta	Kod	Sunucu	153	83	0.16%	0.68%
Brute Force Attack	Kritik	Yönetim	Sunucu	79	51	0.08%	0.42%
Buffer Overflow	Hayati	Kod	Sunucu	537	84	0.55%	0.69%
Content Spoofing	Yüksek	Kod	Ziyaretçi	1564	304	1.60%	2.49%
Credential/Session Prediction	Kritik	Kod	Sunucu	794	147	0.81%	1.21%
Cross-Site Scripting	Kritik	Kod	Ziyaretçi	37624	4686	38.57%	38.45%
Cross-Site Request Forgery	Yüksek	Kod	Ziyaretçi	285	161	0.29%	1.32%
Denial of Service	Yüksek	Yönetim	Sunucu	42	36	0.04%	0.30%
Format String Attack	Hayati	Kod	Sunucu	52	43	0.05%	0.35%
HTTP Request Splitting	Kritik	Kod	Ziyaretçi	311	162	0.32%	1.33%
HTTP Response Splitting	Kritik	Kod	Ziyaretçi	2592	161	2.66%	1.32%
HTTP Request Smuggling	Kritik	Yönetim	Ziyaretçi	0	0	0.00%	0.00%
HTTP Response Smuggling	Kritik	Yönetim	Ziyaretçi	0	0	0.00%	0.00%
Integer Overflow	Hayati	Kod	Sunucu	79	46	0.08%	0.38%
LDAP Injection	Hayati	Kod	Sunucu	41	16	0.04%	0.13%
Mail Command	Yüksek	Kod	Sunucu	1	1	0.00%	0.01%

Tehdit Sınıflandırması	PCI DSS Risk Seviyesi	Zaafiyet Yeri	Etkilenen Yer	Zaafiyet Sayısı	Web Sitesi Sayısı	% Zaafiyet	% Web Sitesi
Injection							
OS Commanding	Hayati	Kod	Sunucu	76	30	0.08%	0.25%
Path Traversal	Kritik	Kod	Sunucu	1563	139	1.60%	1.14%
Predictable Resource Location	Yüksek	Yönetim	Sunucu	1507	295	1.54%	2.42%
Remote File Inclusion	Hayati	Kod	Sunucu	99	44	0.10%	0.36%
Routing Detour	Yüksek	Kod	Sunucu	0	0	0.00%	0.00%
SOAP Array Abuse	Yüksek	Kod	Sunucu	2	1	0.00%	0.01%
SSI Injection	Hayati	Kod	Sunucu	157	33	0.16%	0.27%
Session Fixation	Kritik	Kod	Sunucu	137	123	0.14%	1.01%
SQL Injection	Hayati	Kod	Sunucu	6345	1555	6.50%	12.76%
URL Redirectors	Orta	Kod	Ziyaretçi	5	4	0.01%	0.03%
XPath Injection	Hayati	Kod	Sunucu	64	19	0.07%	0.16%
XML Attribute Blowup	Yüksek	Kod	Sunucu	0	0	0.00%	0.00%
XML External Entity	Yüksek	Kod	Sunucu	0	0	0.00%	0.00%
XML Entity Expansion	Yüksek	Kod	Sunucu	0	0	0.00%	0.00%
XML Injection	Kritik	Kod	Sunucu	0	0	0.00%	0.00%
XQuery Injection	Hayati	Kod	Sunucu	0	0	0.00%	0.00%
Application Misconfiguration	Orta	Yönetim	Sunucu	85	60	0.09%	0.49%
Directory Indexing	Yüksek	Yönetim	Sunucu	370	184	0.38%	1.51%
Fingerprinting	Low	Yönetim	Sunucu	3663	3604	3.75%	29.57%
Improper Parsing	Hayati	Kod	Sunucu	1464	524	1.50%	4.30%
Improper Permissions	Hayati	Yönetim	Sunucu	4	4	0.00%	0.03%
Information leakage	Yüksek	Yönetim	Sunucu	31527	7942	32.32%	65.17%

Tehdit Sınıflandırması	PCI DSS Risk Seviyesi	Zaafiyet Yeri	Etkilenen Yer	**Zaafiyet Sayısı**	**Web Sitesi Sayısı**	**% Zaafiyet**	**% Web Sitesi**
Insecure Indexing	Yüksek	Yönetim	Sunucu	8	7	0.01%	0.06%
Insufficient Anti-automation	Orta	Kod	Sunucu	108	36	0.11%	0.30%
Insufficient Authentication	Kritik	Kod	Sunucu	806	304	0.83%	2.49%
Insufficient Authorization	Kritik	Kod	Sunucu	615	286	0.63%	2.35%
Insufficient Data Protection	Yüksek	Yönetim	Sunucu	64	21	0.07%	0.17%
Insufficient Process Validation	Orta	Kod	Sunucu	52	34	0.05%	0.28%
Insufficient Session Expiration	Kritik	Kod	Sunucu	169	71	0.17%	0.58%
Insufficient Transport Layer Protection	Orta	Yönetim	Ziyaretçi	4317	4195	4.43%	34.42%
Server Misconfiguration	Orta	Yönetim	Sunucu	193	113	0.20%	0.93%
Total				**97554**	**12186**	**99.99 %**	

Kaynak: A.G.E., S.19 - 23

Bu tarama sonuçlarının, önem derecelerine göre sınıflandırılmış hali Tablo 10'da belirtilmeye çalışılmıştır. Görüldüğü gibi genel itibari ile sitelerin %72.27 sinde, yüksek seviyeli güvenlik açığı tespit edilmiştir. Kritik seviye güvenlik açığına sahip web sitelerinin oranının ise %45.22 olduğu görülmüştür.

Tablo 10
Risk Gruplandırma Seviyelerine Göre Zayıflık Dağılımı – Tüm Tarama Sonuçları İçin.

Tehdit Seviyesi	Zaafiyet Sayısı	Web Sitesi Sayısı	% Zaafiyet	% Web Sitesi
Hayati	8918	2287	9.14%	18.77%
Kritik	44669	5511	45.79%	45.22%
Yüksek	35375	8807	36.26%	72.27%
Orta	4908	4455	5.03%	36.56%
Düşük	3663	3618	3.75%	29.69%

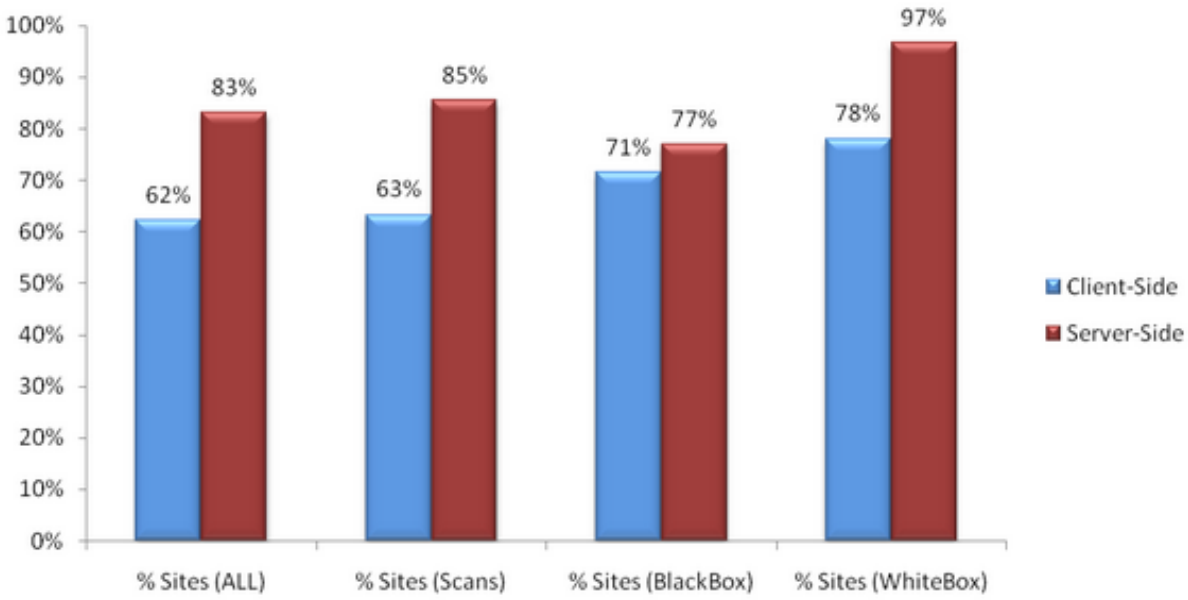
Kaynak: A.G.E., S.26

Bu tarama sonuçları etkilenen yer bakımından sınıflandırılmaya çalışıldığında Tablo 11'deki gibi bir durum ortaya çıkmaktadır. Görüldüğü gibi, bulunan bu zafiyetlerin %52'si sunucu sistemlerine %48'i ise ziyaretçilere zarar vermektedir.

Tablo 11
Etki Yerine Göre Zayıflık Dağılımı – Tüm Tarama Sonuçları İçin.

Etkilenen Yer	Zaafiyet Sayısı	% Zaafiyet
Sunucu	50856	52 %
Ziyaretçi	46698	48 %

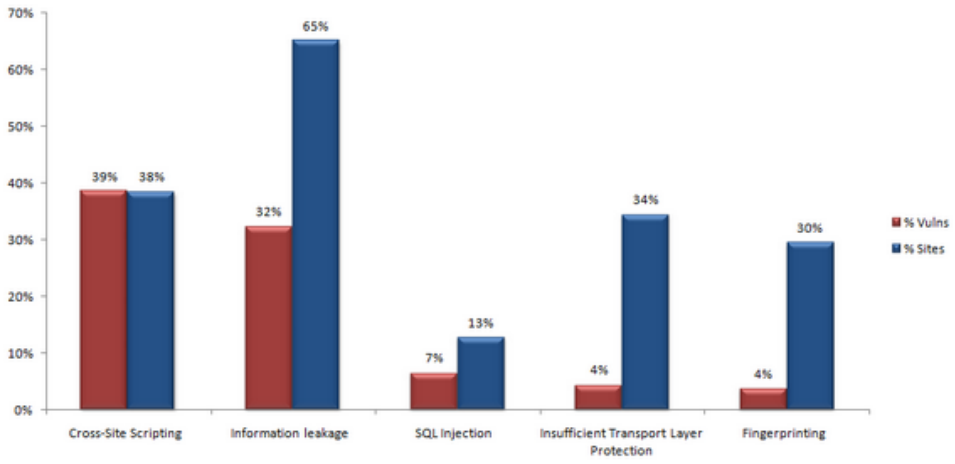
Bu zafiyetlerin 3 farklı tarama çeşidine göre etki ettiği lokasyonlara Şekil 27'de göz atıldığında, zafiyetlerin genel olarak %83'ünün sunucu sistemlerine zarar verdiği, %62'sinin ise ziyaretçilere zarar verdiği görülebilmektedir.



Şekil 27 : Zayıflıkların Bulundukları Lokasyonlara Göre Oranları

Kaynak: A.G.E., S.11

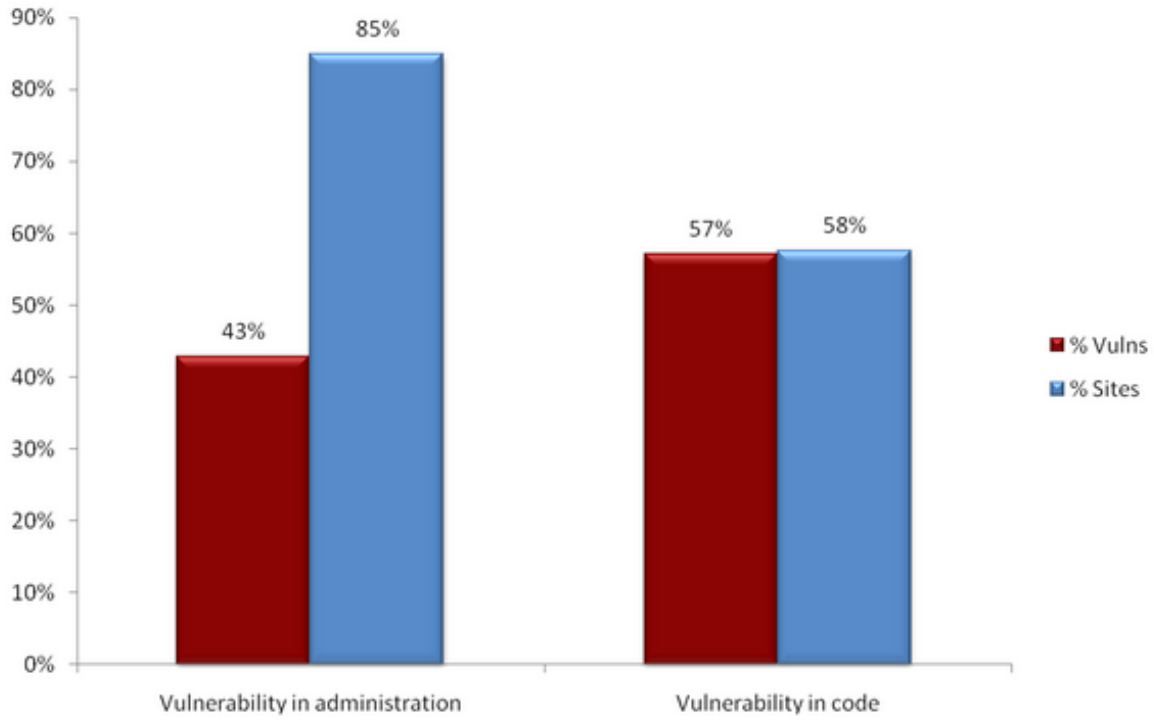
Yapılan incelemelerde elde edilen ve saptanan zafiyetlerden en yaygın ve sık rastlananları ele alındığında, bu zafiyetlerin genel zafiyetlere ve sitelerde bulunma oranları Şekil 28'de gösterilmeye çalışılmıştır. Görüldüğü gibi, information leakage zafiyeti tüm sitelerin %65 inde bulunmakta ve genel zafiyetlerin %32'sini oluşturmaktadır. Cross-site scripting zafiyeti ise tüm sitelerin %38 inde bulunmakta ve genel zafiyetlerin %39'unu oluşturmaktadır.



Şekil 28 : En Yaygın Zayıflıklarının Genel Zayıflıklara ve Sitelere Göre Oranları

Kaynak: A.G.E., S.7

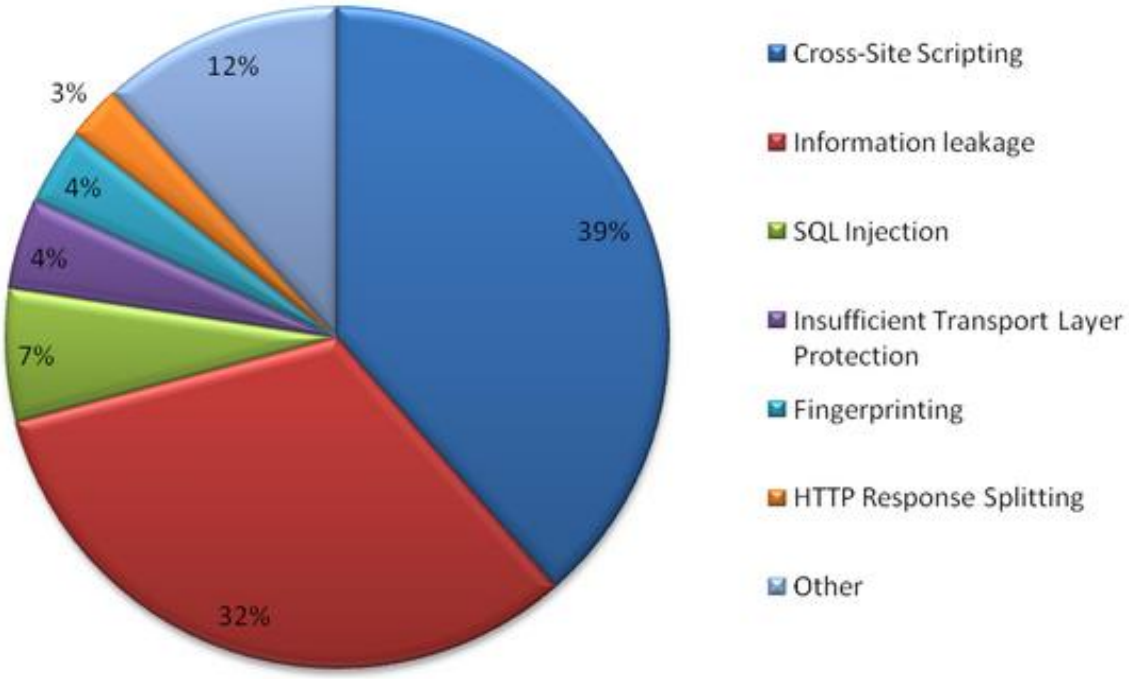
Elde edilen bu zafiyetlerin kökenine Şekil 29 üzerinden bakıldığında, sitelerin yayınlandığı sistemlerin yönetiminden kaynaklanan zafiyetlerin tüm sitelerin %85 inde bulunduğu ve bu tür zafiyetlerin tüm zafiyetlerin %43'ünü oluşturduğu görülmektedir. Web sitelerinin hazırlanması aşamasında kullanılan yazılım yani kodlamadan kaynaklanan zafiyetlerin ise %58 inde bulunduğu ve bu tür zafiyetlerin tüm zafiyetlerin %57'sini oluşturduğu görülmektedir.



Şekil 29 : Kökenine Göre Zayıflık Bulma Oranları

Kaynak: A.G.E., S.9

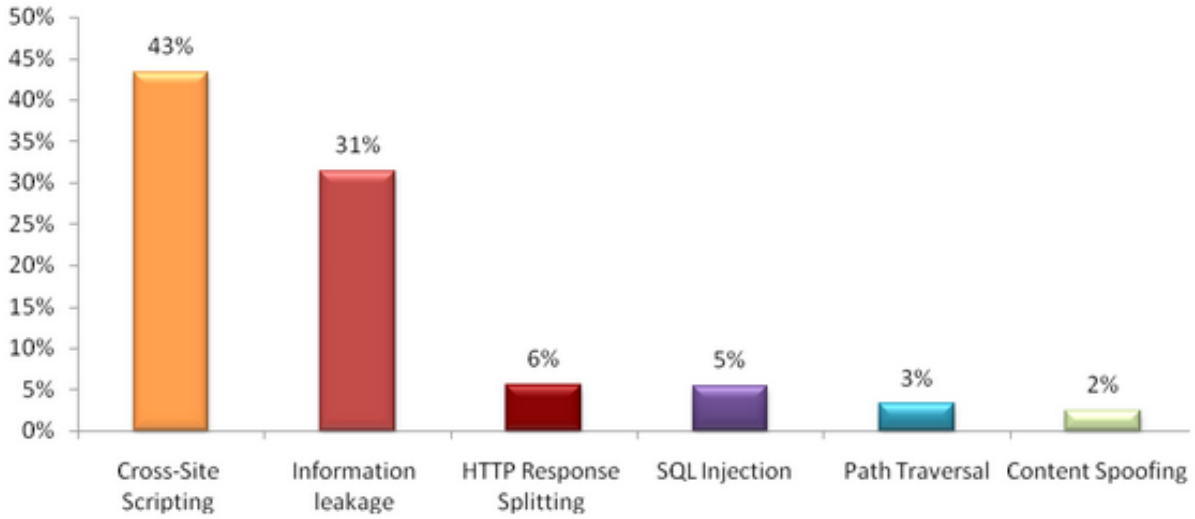
Zafiyetler genel olarak sıklık oranlarına göre sınıflandırıldıklarında, en çok ve sık olarak rastlanan zafiyetlerin Cross-site scripting ve information leakage oldukları tespit edilmiştir. Bu durum Şekil 30'dan da görülebilmektedir.



Şekil 30 : Çeşitlerine Göre Zayıflık Yoğunlukları (Genel)

Kaynak: A.G.E., S.8

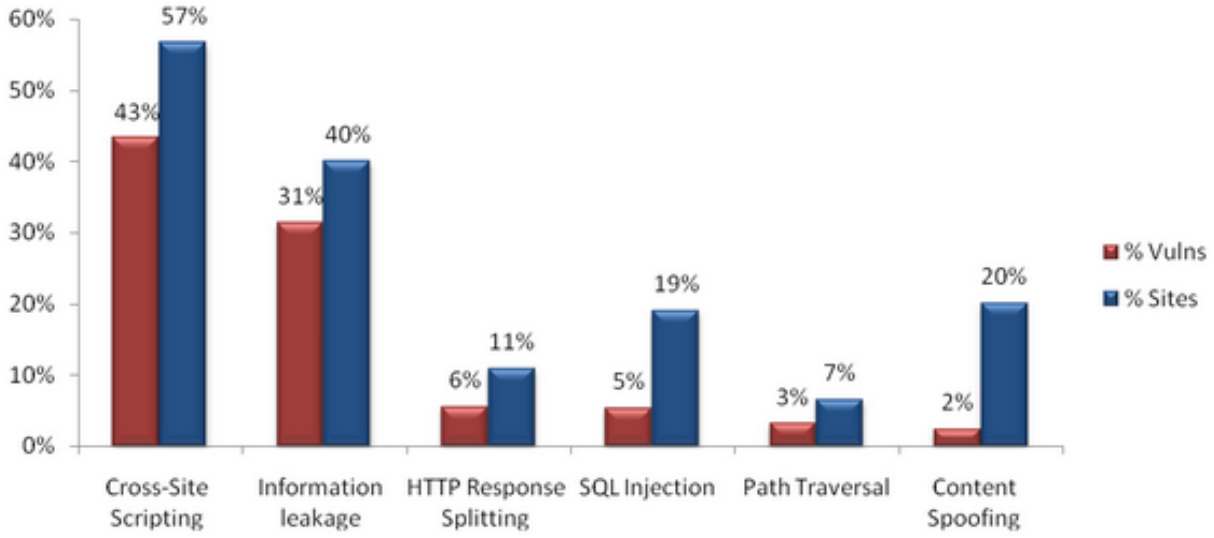
Farklı tarama çeşitleri olmasına karşın, standart tarama araçlarından farklı olarak, standart taramaya göre daha fazla bilgi ve tecrübe gerektiren derinlemesine ve özel taramalarda elde edilen zafiyetlerinde de yine çok farklılık göstermediği ve bulunan zafiyetlerin tam olarak olmasa da genel olarak farklılık göstermediği tespit edilmiştir. Bu tür taramalarda da yine en fazla cross-site scripting ve information leakage zafiyetlerinin bulunduğu Şekil 31'de gösterilmeye çalışılmıştır.



Şekil 31 : Derinlemesine ve Özel Taramada Bulunan Zayıflık Oranları

Kaynak: A.G.E., S.9

Derinlemesine ve özel taramada tespit edilen zafiyetlerin, bu taramalarda elde edilen diğer zafiyetlere ve sitelere göre oranlarına bakıldığında, yine en sık ve çok rastlanan zafiyetlerin Cross-site scripting ve information leakage olduğu Şekil 32'de görülmektedir. Cross-site scripting zafiyetinin sitelerin %57 sinde bulunduğu ve sayısının ise bu taramadaki zafiyetlerin %43'ünü oluşturduğu görülmektedir. İnformation leakage zafiyetinin ise sitelerin %40 ında bulunduğu ve sayısının ise bu taramadaki zafiyetlerin %31'ini oluşturduğu görülmektedir.

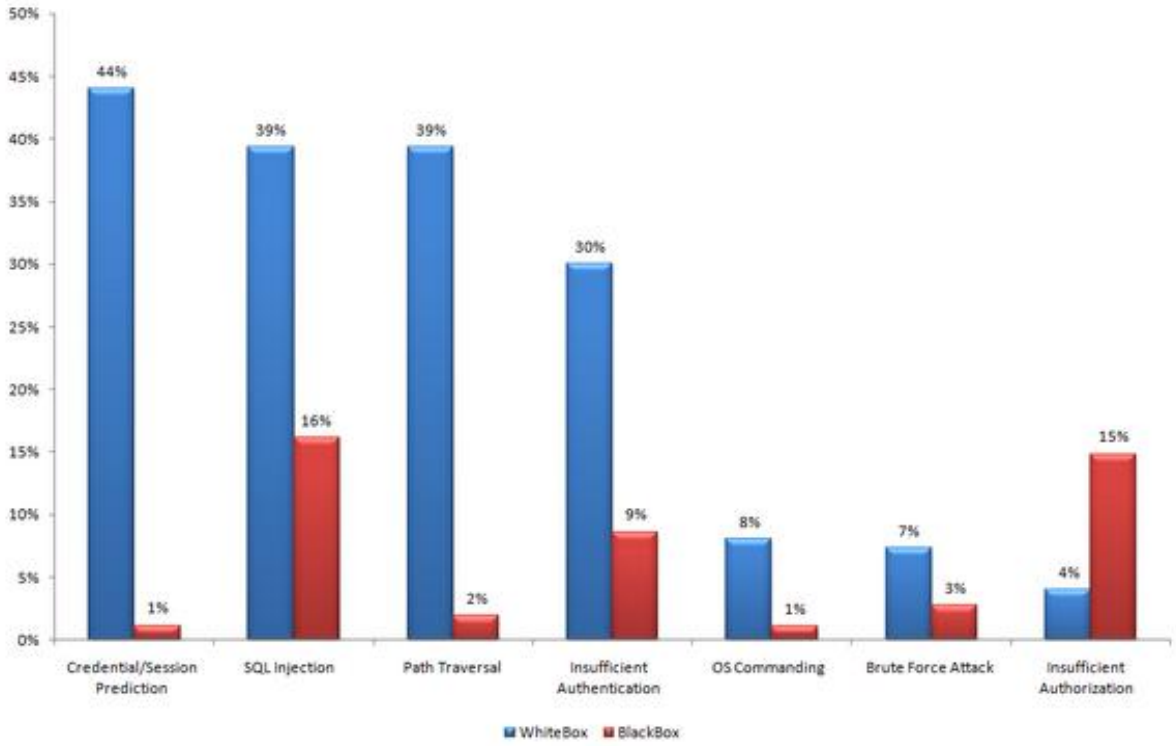


Şekil 32 : Derinlemesine ve Özel Taramada Bulunan Zayıflıkların Site ve Toplam Zayıflıklara Oranı

Kaynak: A.G.E., S.10

Zafiyetleri bulmak için standart, derinlemesine ve özel olmak üzere 3 farklı tarama çeşidi olmasına karşın, bu taramalarda kullanılan yöntemler aynıdır. Diğer bir tabir ile, tarama çeşitlerinde kullanılan zafiyet bulma metotları mantık olarak aynı olmalarına rağmen, bu metotlar tarama çeşidine göre uygulanma şekilleri bakımından farklılık göstermektedir.

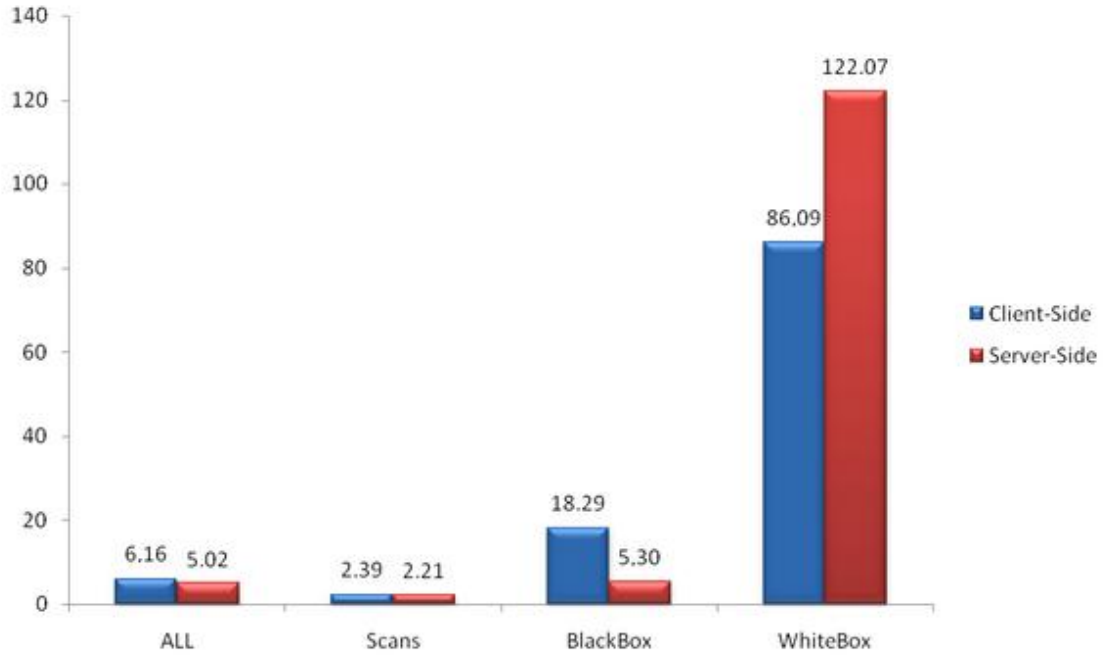
Bu kapsamda, derinlemesine ve özel tarama çeşitlerinde kullanılan metotlara göre bulunabilen zafiyet oranları Şekil 33'de belirtilmeye çalışılmıştır. Görüldüğü gibi, derinlemesine taramada zafiyetler en fazla SQL injection ve insufficient authorization metotları ile bulunabiliyorken, özel taramada en fazla zafieytler credential / session prediction metotları ile bulunabilmektedir. Bu nedenle, bir sistemin güvenliğinin sağlanması amacı ile herhangi bir güvenlik taraması hizmeti alındığında, her tarama çeşidinin tüm metotlar ile gerçekleştirilmesi, sistemdeki tüm zafiyetlerin bulunması ve gerekli önlemlerin alınması için gerekli birer adımdır.



Şekil 33 : Bulunan Zayıflıkların Bulunma Metotlarına Göre Dağılım Oranları

Kaynak: A.G.E., S.11

Tüm bunlar göz önüne alındığında, tarama çeşidine göre sitelerde bulunan zafiyetlerin sunuculara ve ziyaretçilere zarar verenlerin site başına ortalamaları Şekil 34'de belirtilmeye çalışılmıştır. Görüldüğü gibi, standart taramalarda elde edilen ortalama sunucuya zarar veren zafiyet sayısı 2.21 ve ziyaretçilere zarar veren zafiyet sayısı 2.39 iken, bu oran özel taramada sunucular için 122.07 ve ziyaretçiler için 86.09 dur. Bu durum yine, güvenlik testi hizmeti alırken özel tarama çeşidinin seçilmesinin önemini göstermektedir.



Şekil 34 : Bulunan Zayıflıkların Bulunma Metotlarına Göre Site Başına Oranları

Kaynak: A.G.E., S.12

Görüldüğü gibi sürekli olarak standart, derinlemesine ve özel olmak üzere 3 çeşit tarama metodundan bahsedilmektedir. Bu metotların başarı oranları, zafiyet aranan lokasyonlara ve zafiyetin risk seviyesine göre değişmekle birlikte, white-box adı verilen tarama çeşidinin çoğu alanda önde olduğu

Tablo 12'den de anlaşılabilmektedir.

Tablo incelendiğinde, özel tarama metodunun sunucularda zafiyet bulma başarısının %96.67 olduğu ve site başına ortalama zafiyet sayısının ise 122.07 gibi yüksek bir rakam olduğu görülmektedir.

Buna karşın, black-box metodunun ise, ziyaretçilerinde zarara neden olan zafiyetleri bulma başarısının %76 olduğu görülebilmektedir.

Tablo 12
Bulunan Zayıflıkların Bulunma Metotlarına ve Kaynağına Göre Site Başına Oranları

İncelenen Yer	Zaafiyet Sayısı	Web Sitesi Sayısı	% Zaafiyet	% Web Sitesi	Web Sitesindeki Ortalama Zaafiyet Sayısı
Genel Durum (Sunucu)	50856	10125	52.13%	83.09%	05.Şub
Genel Durum (Ziyaretçi)	46698	7580	47.87%	62.20%	Haz.16

Genel Tarama (Sunucu)	19746	8922	55.60%	85.40%	Şub.21
Genel Tarama (Ziyaretçi)	15767	6607	44.40%	63.24%	Şub.39
Derinlemesine Tarama (Sunucu)	4260	804	23.77%	76.86%	May.30
Derinlemesine Tarama (Ziyaretçi)	13665	747	76.23%	71.41%	18.29
Özel Tarama (Sunucu)	17700	145	63.73%	96.67%	122.07
Özel Tarama (Ziyaretçi)	10072	117	36.27%	78.00%	86.09

Kaynak: A.G.E., S.12

3.2.3. Web Güvenliği Araçları

Web güvenliğini kişisel ve kurumsal olarak, kurumsalı da kamu kurumlarında ve özel kurumlarda olarak ikiye ayırmaya, tüm alanlarda uygulanması ve alınması gereken web güvenliği tedbirleri aynı olduğundan gerek görülmemektedir. Çünkü hepsinde, korunması gereken bir bilgi, veri ya da verilmesi gereken bir hizmet devamlılığı vardır. Bunlardan herhangi birisi ya da birkaçının tamamen ya da kısmen kaybedilmesi sonucu uğranacak olan zarar ya da kıymet kaybının ölçümlenmesine göre güvenlik tedbirleri ve bu tedbirlerin dereceleri belirlenmektedir. Bu da kişisel, kurumsal ya da özel ve ya kamu kurumu olarak değil, kıymete göre değişmektedir.

Bir kurumun web sitesinde kıymetli hiçbir bilgi ya da veri olmayabilir, ya da kurum kaybedecek bir itibarı önemsemeyebilir, buna karşın evden iş ve hizmetlerini yürüten bir kişinin web sitesinde çok değerli bilgi ve ya verileri olabilir ve sitesinin devre dışı kalması kendisinin itibar kaybına sebep olabilir. Bunun gibi ya da bunun tam tersi durumlar farklı kişi ya da kurumlar için geçerli olabilir.

Web güvenliğini sağlamak için yapılması ve alınması gereken önlemler, iş ve işlemler aşağıda belirtilmeye çalışılmıştır.

- Sunucu Tabanlı Atak Engelleme Sistemi

HTTP ve HTTPS istekleri web sunucuları üzerinde işleme tabi tutulur. Sunucu Tabanlı Atak Engelleme Sistemleri (Hostbased Intrusion Preventation System - HIPS) bilinen ve bilinmeyen açıklara karşı koruma sağlayabilir. Doğru HIPS seçimi için korunacak sistemin analizi yapılması gerekir. Örneğin korumamız gereken platformda bir MySQL sunucusu bulunuyorsa, kullanacağımız HIPS sisteminin de MySQL destekli bir ürün olması gerekir. HIPS üreticilerinin bazılarında değişik platformlar için değişik

çözümler mevcuttur. Doğru seçimi ve konfigürasyonu yaratmak için güvenlik danışmanlarına başvurulmasının uygun olacağı düşünülmektedir.[97]

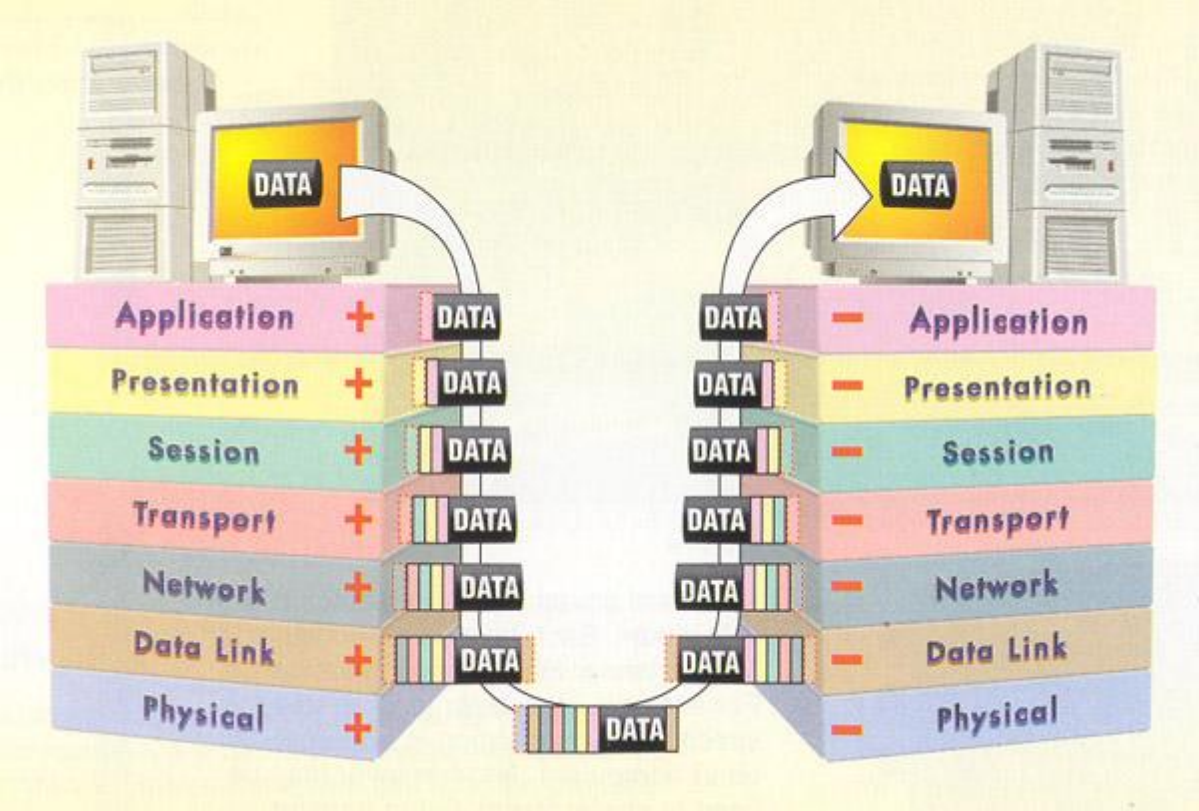
- **Güvenlik Duvarları Seçimi**

Günümüzde hemen hemen tüm kurum ve kuruluşlar hatta ev kullanıcıları dahi güvenlik duvarı (firewall) kullanmaktadırlar. Güvenlik duvarları, bilişim iletişim teknolojilerinin temeli olan TCP/IP (Transmission Control Protokol/Internet Protokol) nin standartları üzerinde aldıkları önlemler ile sistemleri korumaktadırlar. TCP/IP nin 7 temel katman standardı vardır. Bunlar, OSI (Open System Interconnection) adı verilen katmanlardır ve tüm bilişim iletişim teknolojileri bu 7 temel katmana sadık kalarak yapılmaktadır. Bu katmanlar;

7.Uygulama Katmanı(Application Layer)
6.Sunum Katmanı(Presentation Layer)
5.Oturum Katmanı(Session Layer)
4.Nakil Katmanı(Transport Layer)
3.Ağ Katmanı(Neywork Layer)
2.Data Link Katmanı(Data Link Layer)
1.Fiziksel Katman(Physical Layer)

Ters yazılmasının nedeni iletişim yönünü ifade etmektedir. Sistemler arasındaki iletişim giriş – çıkış şeklinde olmaktadır. Bu durum Şekil 35'de gösterilmeye çalışılmıştır.

[97] "**Uygulama Güvenliği**", http://fentanyl.wordpress.com/2009/04/29/uygulama-guvenligi/ (Haziran 2009)



Şekil 35 : OSI Modeli Veri Aktarımı

Kaynak: Osman ÇAKIR, "**OSI Modeli-OSI Katmanları Nelerdir?**", http://www.osmancakir.net/osi-modeli-osi-katmanlari-nelerdir-82.html (Mart 2010)

Günümüzde çoğu güvenlik duvarı 4. Katmana kadar koruma sağlamaktadır. Ancak 7. Katmana kadar da güvenlik sağlayan güvenlik duvarları vardır. Ancak sayıları, bu işin çok zor ve performans gerektiren bir iş olması dolayısı ile yok denecek kadar azdır. Ancak artık port kavramının herhangi bir önemi kalmadığından yakın gelecekte port yerine uygulama bazında kural yazılabilen güvenlik duvarlarının çıkması kaçınılmazdır.

Günümüz güvenlik duvarları, OSI katmanlarından 4. Katmana hatta çoğu 3. Katmana kadar koruma yapabildiklerinden ve klasik saldırıların çoğunun da bu katmanlara gelmesinden dolayı yine tek başlarına belirli bir seviyeye kadar yeterli olabilmekteydiler. 4. Katmana kadar gelen saldırı türleri geliştiğinden, ancak bilişim iletişim teknolojileri standartları aynı kaldığından, 3 ve 4. Katmana kadar koruma sağlayan güvenlik duvarları tek başlarına artık yeterli olamamaktadırlar. Bu katmanlara kadar olan standart güvenlik önlemlerine ek olarak IPS (Intrusion Prevention System) sistemleri

eklenerek günümüz saldırılarının önüne geçilmeye çalışılmaktadır. Bu sayede güvenlik duvarı + IPS ile katman 4 e kadar olan saldırılar bertaraf edilebilir duruma gelinebilmektedir.

Ancak gelişen teknoloji ile birlikte, yapılan saldırılar da gelişerek 4. Katmandan daha yukarıdaki iletişim ve sistem teknolojilerine yönelmiştir. Yapılan saldırıları 4. Katmana kadar koruma sağlayan IPS ve güvenlik duvarları engelleyemeyeceğinden bu katmanlardaki sistem koruması için uygulama güvenlik duvarları ortaya çıkmıştır. Bu uygulamalar hemen hemen tüm iletişim protokollerini (HTTP, SMTP, IMAP, POP, TELNET, SSH vs…) içerdiğinden çok çeşitlilik göstermektedir.[98]

Bahsedilen bu uygulama tabanlı güvenlik duvarları ürünleri, uygulamaları korumak üzere dizayn edilmiş özel ürünlerdir. Bu ürünlerde Cookie/session poisoning, Sql injection veya Cross-site scripting gibi atakların tamamına karşı koruma kalkanı bulunmaktadır. Microsoft tarafından ücretsiz olarak sağlanan yazılımlar olan IISLock ve URLScan bu Application Firewall ürünlerin basit olanlarına örnek verilebilirler.

Ancak bu işi çok ciddi yapabilen ürünlere F5 Networks TrafficShield, SecureComputing G2 Firewall/Security Appliance, Imperva, InterDo, NetContinuum, AirLock ve e-Gap gibi sektörde yer edinmiş ve kaliteleri ile kendilerini ispatlamış olanlar örnek verilebilirler.[99]

Ancak temel uygulamalar ve protokoller hariç, yeni geliştirilen iletişim araçları (Google Talk, MSN, ICQ, web tabanlı iletişim arabirimleri vs…) genel olarak hep aynı iletişim protokolünü, http'yi tercih etmektedirler. Bu nedenle diğer protokollerden ziyade özellikle http trafiğinin ve iletişimin önemi, yüksek erişilebilirliği ve güvenliği ön plana çıkmaktadır. O nedenle ortaya sadece http trafiğinin güvenliğini, erişilebilirliğini ve güvenilirliğini

---

[98] Huzeyfe ÖNAL, "*Web Uygulama Güvenlik Duvarı Tercih Rehberi*", **Beyaz Şapka Bilişim Güvenliği Dergisi**, Kasım 2008, S.12

[99] "**Uygulama Güvenliği**", http://fentanyl.wordpress.com/2009/04/29/uygulama-guvenligi/ (Haziran 2009)

sağlayan web uygulama güvenlik duvarları (WAF - Web Application Firewall) olarak adlandırılan sistemler ortaya çıkmıştır.

Bu sistemler, karmaşıklaşan ve artan yüksek miktardaki web trafiği üzerinde detaylı inceleme yaparak anormal trafiği engelleyebilmektedirler. Daha teknik bir tanımla WAF sistemleri HTTP/HTTPS/SOAP/XML-RPC/Web Servisleri üzerinde detaylı paket incelemesi yaparak zararlı istekleri engellemek için kullanılan araçlardır. Bilgi güvenliğine önem veren standartlar incelendiğinde bazıları WAF sistemlerinin kullanımını tavsiye etmekte, bazıları da duruma göre zorunlu kılmaktadır. Bunların başında duruma göre WAF kullanımını zorunlu tutan ve yukarıda bahsedilen PCI DSS Veri Güvenliği standardı gelmektedir.[100]

- **Penetration Test Hizmeti Alımı**

Sistemlerdeki hata, eksiklik ve ya zafiyetleri, kötü niyetli kişi ya da kişilerden önce, tespit ederek ya da ettirerek bunlardan haberdar olmak ve gerekli güncelleştirme, iyileştirme ve geliştirmelerde bulunmak ya da bulunmak için gerekli çalışmaları başlatmak olarak nitelendirilebilmektedir. Bu işlem aynı zamanda, sistemlerin ve verilerin güvenliği için bu zamana kadar yapılmış olan yatırım ve alınan önlemlerinde ne kadar yeterli, yerinde ya da tam tersi olduklarının anlaşılmasına yardımcı olacaktır.[101]

- **Web Yazılım Geliştiricilerine Düşen Görevler**

Geliştirilmiş olan yazılımların kullanıma geçmesi için tüm kodların güvenlik denetiminden geçmiş olması gerekmektedir. Web yazılımcılarının görevi yazdıkları kodlarında herhangi bir güvenlik açığının olmaması için tüm olasılıkları düşünerek, işlerine hakim bir şekilde kodlama yapmak ve kodlamam tamamlandıktan sonra, kodların tamamını özel sözleşme ya da anlaşmalarla kendi kurum ya da kuruluşlarından farklı olan ve tek işi kod

[100] Beyaz Şapka Bilişim Güvenliği Dergisi, S.12
[101] "**Uygulama Güvenliği**", http://fentanyl.wordpress.com/2009/04/29/uygulama-guvenligi/ (Haziran 2009)

güvenliği testleri yapan kurum, kuruluş ya da firmalardan ilgili standartlara göre kod güvenliği testinden geçirtmektir.

- **Sistem Yöneticilerine Düşen Görevler**

Yazılımlar geliştirildikten sonra hizmet vermesi için sunuculara yüklenirler. Bu güvende olunduğu manasına gelmemektedir. Bir web yazılımının (web siteleri dahil) kodlarının güvenli olması gerektiği kadar sunucunun da güvende olması gerekmektedir. Sistem yöneticilerine düşen görev sunucuların ve sunucularda verilen servislerin de güvenliğinin sağlanmasıdır. Bunun da yukarıda belirtilen şekillerde birden fazla yolu ve adımı bulunmaktadır.

- **Denetçilere Düşen Görevler**

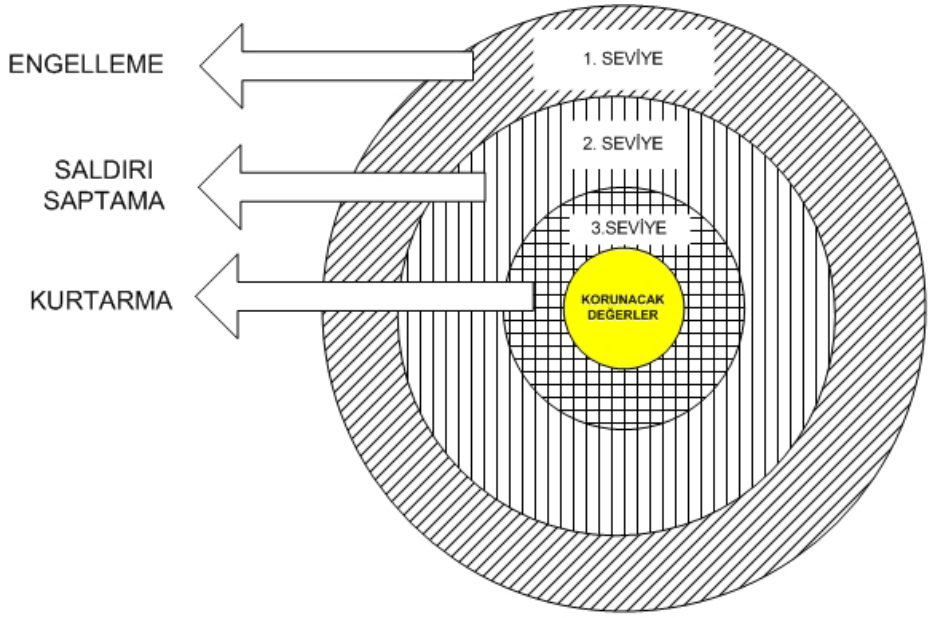
Denetimler, iç denetim ve dış denetim olarak ikiye ayrılır. Bu denetim süreçlerinde kurum çalışanları ya da dış kurum ya da kuruluşlar sistemleri denetlerler. Ağ, sunucu, web servisi, web uygulamaları ve işlevsellik baştan sona denetime tabi tutulur. Bu unsurlar web hizmetinin birer parçasıdır. Denetim süreçlerinde ticari güvenlik tarama yazılımları, ticari web uygulama güvenliği tarama yazılımları ve açık kaynak kodlu yazılımlar kullanılabilir. Sistemlerin güvenliğinin devamı için denetçiler tarafından bahse konu denetlemelerin düzenli olarak yapılması gerekmektedir.[102]

- **Web Güvenliği Katmanları**

Web güvenliğini tanımlarken, farklı ve birbirini tamamlayan işlevlere ait çok katmanlı güvenlik sistemlerinden söz edilmelidir. Katman yapısını, kurulacak güvenlik sistemlerinin özelliğine göre farklılaştırmak ve her katmanda alt katmanlar kullanmak olasıdır. Genel olarak üç katmandan oluşan bir yapıdan söz etmek mümkündür. Bu genel model Şekil 36'da gösterilmiştir.

---

[102] Serkan AKCAN, "*Uygulama Güvenliği*", **Beyaz Şapka Bilişim Güvenliği Dergisi**, Kasım 2008, S.4



Şekil 36 : Çok Katmanlı Güvenlik Modeli

Kaynak: "*Kurumsal Web Güvenliği Yapısı*", **Akademik Bilişim 2008 Sempozyumu Sunumları**, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale, S.2 http://ab.org.tr/ab08/bildiri/49.doc (Nisan 2009)

İlk katman- Engelleme: Saldırı olasılıklarını azaltmakla sorumlu olan ilk katmandır.

İkinci katman - Saptama: Saldırıları saptama ve uygun alarmları oluşturma katmanıdır.

Üçüncü katman – Kurtarma: Saldırının etkilerini temizleme ve sistemi yeniden çalışır hale getirme katmanıdır.

Web güvenliğini tam olarak sağlamak için çok katmanlı güvenlik modeli, alt sistemlerin birbirleriyle etkileşimli çalışması sağlayacak şekilde kullanılmalıdır.[103]

Tüm güvenlik açıklarının hatalı kod yazılmasından ortaya çıktığı unutulmamalıdır. Güvenli bir sistem için, yazılım ekibinin eğitimli ve tecrübeli kişilerden oluşturması önemlidir. Bir web uygulamasında binlerce aktif sayfa çalışır ve insan hatası sebebiyle bazılarında hata bulunması

[103] A.G.E., S.2

kaçınılmazdır. Hatalı kod üretimini engellemek için kodları analiz eden ve hataları tespit edip önerilerde bulunan yazılımlar kullanılmalıdır. Bu sebeple uygun kod denetimi yazılımını bulmak için güvenlik danışmanlarına ve uygulama geliştirme platformu üreticilerine danışılması önerilmektedir.[104]

3.3. Elektronik Dönüşüm ve E-Devlet

Kamu kurumlarında web güvenliği, dünyada ve Türkiye'de internet kullanımının artması sonucunda, kamu kurumlarının da, bu teknolojiye ayak uydurarak, vatandaşlara internet üzerinde hizmet vermek amacıyla web sayfaları hazırlatmaları ile daha da önem kazanmıştır.

Türkiye'de ve dünyada internet'in yaygınlaşmasında etkin olan ve gelişen iletişim teknolojileri aşağıdaki gibi sıralanabilmektedir.

- Telekomünikasyon Alanındaki Gelişmeler

  - Küresel İletişim Altyapısının yaygınlaşması ve ülkelerin birbirleri ile olan bağlantı kapasitelerini arttırmaları,[105]
  - Xdsl, G.Shdsl, Vdsl, Rdsl gibi bakır kablolu iletişim teknolojilerinin,[106]
  - Yüksek İrtifa Platformları, Kablo TV, Uydu-Uzun Mesafe Taşıyıcı Teknolojilerinin,[107]
  - Sabit Kablosuz-Bir Noktadan Birçok Noktaya Geniş Bant Erişimi teknolojilerini oluşturan, Cdma 450, WiFi-Kablosuz Abone Erişimi, 801, Wlan-Kablosuz Yerel Alan Ağları teknolojilerinin,[108]
  - Optik Abone Erişimi teknolojilerini oluşturan, LRE, Ethernet Uzantısı, Optik Ethernet, Wdm, Dwdm ve Isdn teknolojilerinin,[109]
  - Analog teknolojiden, sayısal teknolojiye geçilmesi,
  - Devre anahtarlamadan paket anahtarlamaya geçilmesi,
  - İletimde bakır kablo yerine optik kablo'ya doğru bir geçiş olması,

---

[104] "**Uygulama Güvenliği**", http://fentanyl.wordpress.com/2009/04/29/uygulama-guvenligi/ (Haziran 2009)
[105] "*Broadband Internet Access in OECD Countries: A Comparative Analysis*", **A Staff Report of the Office of Strategic Planning and Policy Analysis and International Bureau**, October 2003, S.11 http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-239660A2.pdf (Mart 2009)
[106] "*TBS-İletişim Alt Yapısı Raporu*", **Telekomünikasyon İşletmecileri Derneği Dergisi**, 2007, S.25 http://www.telkoder.org.tr/files/2-report/iletisim.doc (Ekim 2009)
[107] A.G.E., S.77
[108] A.G.E., S.71
[109] "*Ankara Raporu*", **Türkiye 2. Bilişim Şurası**, 10-11 Mayıs 2004, S.59 - 60

- Telekomünikasyon hizmetlerinin iletimi için gerekli olan araç ve gereçlerde (Costumer Premises Eguipment-CPE) yenilikler ortaya çıkması,
- Çağrı Sistemi (Paging) de telekomünikasyon devriminin bir parçası olması,
- Özel uydu iş şebekelerinin telekomünikasyonda yeni bir çağ yaratması,
- Mainframe lerin icat edilmesi ve bilginin paylaşımının kolaylaşması,
- Datanın telekomünikasyon şebekelerinin üzerinden taşınmaya başlanması,
- Modemin icadı, (zaten evlere kadar gitmiş olan telefon şebekeleri üzerinden data iletişimine imkan verdi)

- Mobilite Alanındaki Gelişmeler

- Hücresel Televizyon ve dijital yayıncılık teknolojilerinin,[110]
- Hücresel Erişim Teknolojilerini oluşturan, Gsm, Gprs, Edge, Umts, NMT Ve Çağrı Cihazları teknolojilerinin,[111]
- Ses İletişimi-VOIP[112], Pots gibi kablo modem teknolojilerinin, ulusal Numaralandırma-Numara Taşınabilirliği ile birlikte Ulusal Dolaşım-Ara Bağlantı teknoloji ve çalışmalarının tamamlanarak gelişmesi ve yaygınlaşması sıralanabilmektedir.[113]
- Hareket halindeki (mobil) araçlarda (gemi, uçak, karayolu taşıtları vs.) haberleşmenin sağlanması hücresel teknoloji sayesinde daha kolay olması,
- Hücresel hizmet, sabit ve hareketli (mobil) aboneler arasında iletişim sağlayarak kamu şebekesinin imkanlarını artırması,

- Hukuksal Alanındaki Gelişmeler

Haberleşme hizmetlerinin devlet tekelinde olmasının aşağıdaki sorunlara neden olmasından dolayı, bu hizmetlerin tekelden çıkartılması söz konusu olmuştur.

- Hizmet Etkinliğinin Düşük Olması,
- Hizmet Kapasitesinin Tam ve Etkin Olarak Kullanılamaması,
- Görüşme Tamamlama Oranlarının Düşük Olması,
- Aşırı İstihdamın Söz Konusu Olması.[114]

---

[110] "TBS-İletişim Alt Yapısı Raporu", S.27
[111] "Ankara Raporu", S.54 - 58
[112] "TBS-İletişim Alt Yapısı Raporu", S.33
[113] "Ankara Raporu", S.61
[114] Coşkun Can AKTAN, İstiklal Y. VURAL, "*Haberleşme Hizmetlerinin Devlet Tarafından Sunulmasının Ortaya Çıkardığı Sorunlar*", **Telekomünikasyon Ve Regülasyon Dergisi**, 2005, Sayı:2, S.84 http://www.tk.gov.tr/yayin/Sureli_Yayinlar/trd/pdf/trd_2005_2.pdf (Ekim 2009)

Bunlara ek olarak;

- Kamu tekelinde olan telekomünikasyon hizmetlerinin halkın taleplerini karşılayamaması ve bütçe açıklarının büyümeye başlaması nedenleri ile özelleştirmelerin gündeme gelmesi,[115]
- Uluslar arası mobil dolaşım, para transferleri ve internetin dünyaya geneline yayılması gibi ihtiyaçlardan dolayı iletişimin de globalleşmesi için hukuksal alt yapıların zorunlu hale gelmesi.[116]

- Siyasi Alanındaki Gelişmeler

- İkna eden ve özelleştirme savunucularını bir araya getiren yönetici yetenekleri olarak nitelendirilen politik faktörler,

- Ekonomik Alandaki Gelişmeler

- "telekomünikasyon sektöründeki reformların birincil amacı tüketicilere daha iyi, yeni ve daha ucuz hizmetler sunabilmektir" olarak nitelendirilen mikroekonomik faktörler,
- Mali açıklarla ve ekonomik krizlerle mücadele etmek amacıyla telekom şirketlerinin özelleştirilmesini kasteden makroekonomik faktörler,

- Bilgisayar Teknolojileri Alanındaki Gelişmeler

- Bilgisayarın icat edilmesi ve yazılı kaynakların sayısal ortama geçmesi,
- PC'nin icadı, (bilgisayarların evlere girmesi PC ile başlar)
- Yazılım ve donanım alanında görülen olağan üstü gelişmeler,
- Çip boyutlarının milyonlarca kat küçülmesi ve fiyatlarının ucuzlaması, buna bağlı olarak bilgisayar ve iletişim teknolojisinin ucuzlaması,
- İşletim sistemlerinin görselleşmesi ve kullanımının olağan üstü kolaylaşması.[117]

Tüm bunlara rağmen ülkemizde kişi başına telekomünikasyon harcaması, AB ülkelerine göre çok düşük seviyelerdedir. OECD'nin 2005 yılı ile 2007 yılları arasında Erişim Başına Kamu Telekomünikasyon Geliri ile ilgili yaptığı çalışmada Sektörde en az geliri sağlayan yada en verimsiz çalışan

[115] "**Özelleşme, Serbestleşme ve Düzenleme Etkileşim Raporu**", Telekomünikasyon Kurumu, Mayıs 2003, S. 6 – 18, http://www.tk.gov.tr/Yayin/Raporlar/pdf/ozellesme.pdf (Haziran 2009)
[116] A.G.E., S. 91
[117] YILDIRIM ve Diğerleri, S.21

ülkenin Türkiye olduğu belirlenmiştir. Bu oranlar Tablo 13'de belirtilmeye çalışılmıştır. Bu durum, toplumun bilgi çağından geri kalması gibi, bir endişeye de yol açmaktadır.

Tablo 13
Erişim Başına Kamu Telekomünikasyon Geliri (USD)

	2005	2007
İzlanda	880	1000
İsviçre	1050	980
Avustralya	820	978
Belçika	700	850
İrlanda	802	810
Amerika	825	800
İspanya	770	790
Danimarka	700	770
Hollanda	720	770
Fransa	770	760
Kanada	700	760
Japonya	760	750
Yeni Zellanda	748	740
İngiltere	610	630
Norveç	612	625
Finlandiya	600	625
OECD	625	620
Lüksemburg	580	610
Kore	550	600
Almanya	628	590
Avusturya	602	580
Portekiz	578	575
Yunanistan	525	520
İsveç	400	405
İtalya	415	390
Macaristan	385	370
Slovak Cum.	315	335
Çek C um.	300	310
Meksika	301	300
Polanya	290	285
Türkiye	198	198

Kaynak: "Erişim Başına Kamu Telekomünikasyon Geliri ",OECD Raporları, Ağustos 2009, S.127, http://www.bitdunyasi.com/tr/?Sayfa=Detay&Id=2705 (Aralık 2009)

- **E-Devlet Nedir?**

E-Devlet tanımından önce, devlet kavramının anlaşılması daha uygun olacaktır. Bu nedenle devlet kavramı incelendiğinden birden fazla tanımı bulunduğu görülmektedir. Bunlar;

"*Ortak bir hayatı ve kültürü paylaşan bir toplumda, bu toplumu düzenleme, bu topluma güvenlik, refah ve huzur sağlama amacını güden ve bu amaca yönelik olarak kanun koyma, bu kanunları uygulama, yargılama, cezalandırma gibi güçlere sahip olan kurumdur.*"[118]

"*Ülke adı verilen belirli bir toprak üzerinde yaşayan insan topluluklarının bir egemenlik anlayışı ve hukuku içinde bir siyasi iktidar altında örgütlenmesidir.*"[119]

"*Üzerinde yaşayacak toprağı olan, üzerinde yaşayan insanları olan, üzerinde yaşayan insanları bir arada tutan kuvveti olan ve öğeleri olan siyasal bir kurumdur.*

- Devleti *Oluşturan Öğeler*

  - *Toprak(Kara parçası)*
  - *Millet(Halk - insan)*
  - *Kuvvet(Askeri kuvvet - Polis...)*"[120]

Devletin elektronik ortamda olan hali olan E-Devlet'in de bir çok tanımı bulunmaktadır. Bunlar;

"*Vatandaşlara devlet tarafından verilen hizmetlerin elektronik ortamda sunulması, devlet hizmetlerinin vatandaşa en kolay ve en etkin yoldan, kaliteli, hızlı, kesintisiz ve güvenli bir şekilde ulaştırılmasıdır.*"[121]

---

[118] **"Devlet Nedir?"**, http://www.atamizindeyiz.com/03/ata03.htm (Ekim 2009)
[119] Mert DUMAN, **"Devlet Nedir?"**, http://www.habercumhuriyeti.com/yazar/MERT-DUMAN/642/Devlet-Nedir-Ne-Is-Yapar.html (Ekim 2009)
[120] **"Devlet Nedir?"**, http://www.etarih.net/tr/vatandaslik/devletnedir.html (Ekim 2009)
[121] https://www.turkiye.gov.tr/static/sss/001.html (Ekim 2009)

"*Temel olarak kamunun hizmet verdiği alanlarda bilgi ve iletişim teknolojilerinin kullanılması yoluyla şeffaf, vatandaşa yakın, daha ucuz ve verimli çalışan bir idari yapı.*"[122]

"*Devletin kendi iç işleyişinde ve sunduğu hizmetlerde bilişim teknolojilerinin kullanılması olarak ya da devletin vatandaşlarına karşı yerine getirmekle yükümlü olduğu görev ve hizmetlerle vatandaşların devlete karşı olan görev ve hizmetlerinin karşılıklı olarak elektronik iletişim ve işlem ortamlarında kesintisiz ve güvenli olarak yürütülmesidir.*"[123]

"*Yurttaşların "müşteri", kamu yönetimi faaliyetlerinin de "hizmet" olarak görüldüğü, "kalite / fiyat performansı" ölçütlerinin uygulandığı, en az maliyet ve emekle en kaliteli hizmetin üretilmesini hedefleyen bir verimlilik yönetimi sistemidir.*"[124]

Nisan 2004'de, 4982 sayılı Bilgi Edinme Hakkı Kanunu yürürlüğe girmesiyle, kurumsal internet sitesi bulunmayan kurum ve kuruluşlara sitelerini oluşturma, kurum ve kuruluşların bilgi edinme birimlerinin elektronik posta yoluyla başvuru kabul etmeleri ve elektronik posta adreslerini oluşturarak internet sitelerinden kamuoyunun bilgisine sunma gibi birçok uygulamayı internet siteleri aracılığı ile yapmalarına yönelik düzenlemeler getirilmiştir. Bu düzenlemeye göre, kamu kurum ve kuruluşlarının internet sitelerinde, elektronik yayıncılık olarak adlandırılan asgari ikinci aşamada hizmet sunmaları gerekmektedir.

Nitekim, söz konusu yasal düzenlemenin de etkisiyle, kamu hizmeti veren kuruluşlara ait internet sitesi sayısında hızlı bir artış olmuş; 2004 yılı

---

[122] **"E-Devlet Nedir?"**, http://www.makaleler.com/oku-edevlet+nedir (Eylül 2009)
[123] Demokaan DEMİREL, "**E-Devlet ve Dünya Öernekleri**", http://www.sayistay.gov.tr/yayin/dergi/icerik/der61m6.pdf (Ağustos 2009)
[124] Özgür UÇAN, "**E-Devlet, E-Demokrasi Ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü**", http://www.stradigma.com/turkce/haziran2003/makale_09.html (Ağustos 2009)

başında 2.785 olan sayı, 2005 yılı sonunda 8.115'e, Haziran 2006 itibarıyla da, yaklaşık 4 kat artarak 10.359'a ulaşmıştır.[125]

E-Devlet sistemlerinin, 4982 sayılı kanunla hız kazanması, bu kavramın hukuki alt yapısının olgunlaşmasına vesile olmuştur. Bu kapsamdaki E-Devlet Modelinin Hukuksal alt yapısı Tablo 14'de belirtilmeye çalışılmıştır.

Tablo 14
E-Devlet Modelinin Hukuksal Altyapısı

Doğrudan	Dolaylı	Özel
Kamu bilgilerine erişim özgürlüğü konusunda düzenlemeler (Bilgi Özgürlüğü Yasası)	Anayasa değişiklikleri (ifade özgürlüğü, kamu bilgilerine erişim özgürlüğü, kişisel bilgilerin korunması gibi temel hak ve özgürlüklere zemin hazırlayacak değişiklikler)	
Elektronik belgelere ve iletişime yasal kimlik kazandıracak düzenlemeler (Elektronik İmza Yasası, onay kurumlarının, elektronik noterlik kurumunun oluşturulması); delil ve ispat hukukunda (usul hukuku) buna uygun düzenlemelerin yapılması	İhale yasalarında şeffaflığı sağlayacak ve elektronik ortamın kullanımına izin verecek düzenlemeler	3046 sayılı bakanlıkların örgütlenmesini düzenleyen ve 3056 sayılı, kamu yönetiminin yapılanmasını düzenleyen yasalarda gerekli değişikliklerin yapılması
Kişisel bilgilerin korunması ile ilgili yasal düzenlemeler (Kişisel Verileri Koruma Yasası)	Özelleştirme kapsamında özel düzenlemeler (Telekom'un özelleştirilmesi ve ulusal bilişim ve iletişim altyapısıyla ilgili özel düzenlemeler)	E-devlet modelinin yerleştirilmesi için gerekli özel kurumsal düzenleme ve kararlar (BTYK, Kamu-Net Üst Kurulu gibi..);

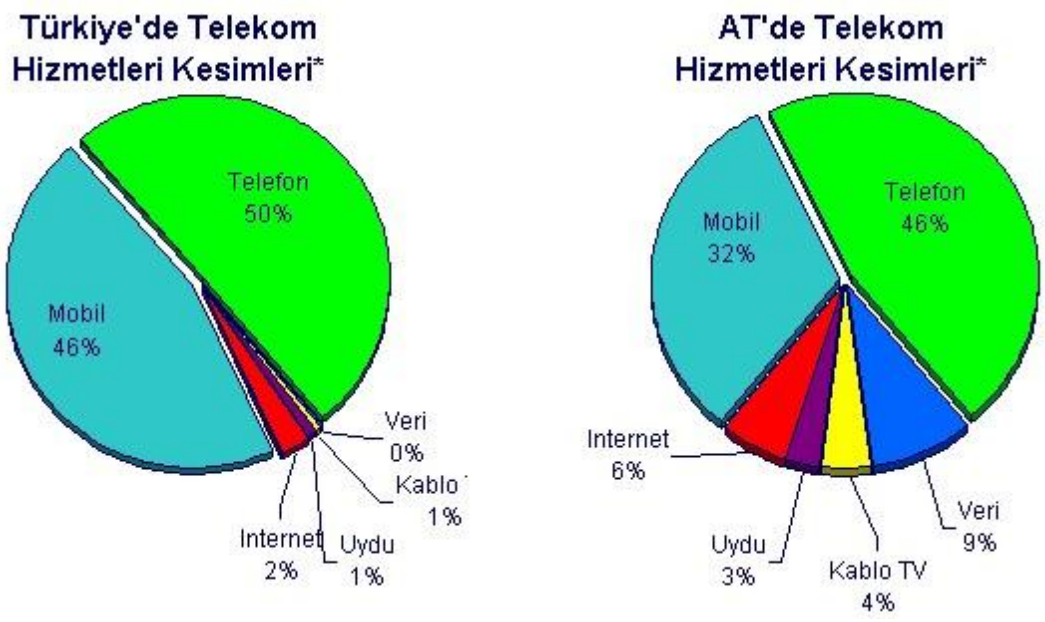
[125] "**E-Devlete Geçişte Kamu Kurumları İnternet Siteleri Performans Denetimi Raporu**", T.C. Sayıştay Başkanlığı, Ankara, 2006, S.85
http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-2Web/2006-Web.pdf (Ocak 2010)

Doğrudan	Dolaylı	Özel
		kamu kurum ve kuruluşlarının arasındaki yatay ilişki ve koordinasyonu düzenleyen kararlar
Fikri mülkiyet haklarını koruyan düzenlemeler	Seçim ve siyasi partiler yasalarında teknoloji kullanımıyla ilgili güncellemeler (e-sayım, e-oylama vb.)	Bilgi Personeli Yasasının çıkartılması
Devlet sırlarının güvenliğini teminat altına alan, hangi bilgilerin paylaşıma açılabileceği, hangilerinin açılamayacağı konusunda sınırlandırmalar ve standartlar getiren bir Ulusal Bilgi Güvenliği Yasası	Bilişim ve iletişim teknolojilerinin yaygınlaşmasını ve dijital bölünmenin önüne geçilmesini sağlamaya yönelik teşvik kararları ve politikalar	Bilgi merkezleri ve hizmetleri alanında özel düzenlemeler
Ceza ve Ceza Usul yasalarında, kişisel hak ve özgürlüklere saygılı ve uluslararası mevzuatlara uygun bir biçimde, bilişim ve iletişim suçlarını düzenleyen maddeler	Yerel yönetimlerle ilgili yasal düzenlemelerde, gayri-merkeziyetçi yapıyı teminat altına alıcı ve yurttaş katılımını artırıcı güncellemeler	
Elektronik ortamda sözleşme usul ve ilkelerini belirleyecek ve elektronik satışlarda hizmet, ürün iade vb. konuları kapsayacak bir biçimde güncellenmiş Tüketiciyi Koruma Yasası	Elektronik fon transferi, e-para vb. yeni finansal araçlarla ilgili düzenlemeler	
Vergi yasalarında e-ticarete uygun güncellemeler ve yeni teknolojilerin vergi tahsilatında kullanımına izin veren düzenlemeler	Basma Yazı ve Resimleri Derleme Kanunu", "Milli Kütüphane Kanunu", Muhasebe-i Umumiye Kanunu" ve "Ayniyat Talimatnamesi"nin yeniden düzenlenmesi	
Gümrük mevzuatında ödeme sistemleri, ürün	Kamu yönetiminde kağıt temelli iletişimden	

Doğrudan	Dolaylı	Özel
teslimatları ve gümrükleme konusunda yeni teknoloji kullanımına izin veren güncellemeler	elektronik iletişime geçişi özendirecek, tasarruf ve teşvik kararları	

Kaynak:
http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Feb/att-0002/01-e-devlet_hukuki_altyapi.doc (Eylül 2009)

Çok hızlı bir şekilde teknolojiye nerde ise bağımlı hale gelmeye başlayan dünyanın hızına Türkiye yetişememekte ve bu yarışta özellikle Internet, Kablo TV, uydu hizmetleri gibi pek çok alanda dünya istatistiklerinde alt sıralarda yer almaya başlamaktadır. Bu hizmetlerden sağlanan gelir, Türkiye telekomünikasyon hizmetleri gelirlerinin %4'ünü oluştururken bu oranının Avrupa ortalamasının ise %22 olduğu gözlenmektedir. Bu durum Şekil 37'de de belirtilmeye çalışılmıştır.[126]



Şekil 37 : Avrupa Topluluğu ve Türkiye'de Telekom Hizmetleri Kesimleri

Kaynak: "İletişim Altyapısı Raporu", Türkiye 1. Bilişim Şurası, 10-12 Mayıs 2002, S.8 – 9 http://bilisimsurasi.org.tr/cg/rapor/iletisim.zip (Mart 2009)

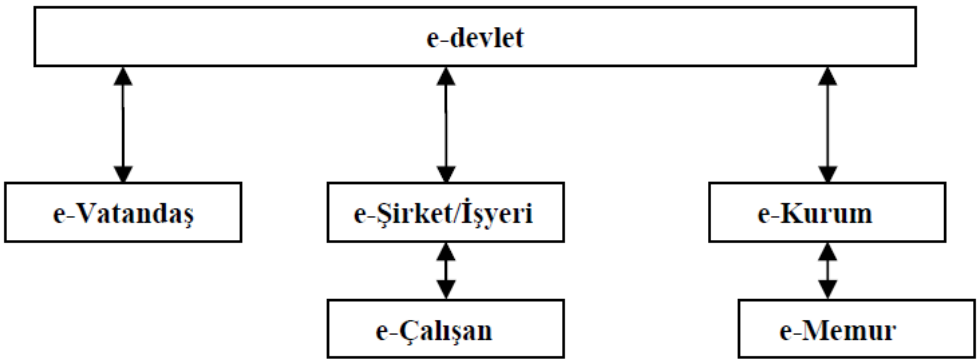
[126] "Telekomünikasyon İşletmecileri Derneği Dergisi", S.27

- **E-Devlet Portalı**

Portallar, "*internet veya intranet bilgi ve uygulama kaynaklarına kolay ve hızlı erişmek üzere tasarlanmış başlangıç noktası olarak kabul edilen, içeriğe bağlı olarak kullanıcılara farklı bilgi ve etkileşim noktaları (e-posta, anlık mesajlaşma, sohbet, tartışma grupları, güncel haberler gibi) içeren giriş kapılarıdır.*"[127]

Portallar ayrıca, "*her yerden erişilebilen, veritabanına dayalı web siteleri ile dinamik bilgi bankalarından bilgi sunulan, tarayıcı tabanlı, söyleşi odaları, forum alanları, kataloglar, canlı haberler, e-posta ve kişiselleşme gibi birçok özelliği etkinliği kapsayan, daha ucuz, hızlı ve güvenli olarak bilgiye ve hizmete erişimi ve entegrasyonu sağlayan web hizmetleridir.*"[128]

e-Devlet Portalı ise, amacı kamu hizmetlerini, vatandaşlara, işletmelere, kamu kurumlarına bilgi ve iletişim teknolojileriyle etkin ve verimli bir şekilde sunmak olan, tüm kamu hizmetlerine tek bir noktadan erişim imkanı sağlayan büyük bir internet sitesidir. E-Devlet portalı, Şekil 38'den de görüldüğü gibi, "Vatandaş", "İş" ve "Devlet" olmak üzere üç ana unsurdan oluşmaktadır.[129]



Şekil 38 : E-Devlet'in Unsurları

Kaynak: "E-Devlet Çalışma Grubu Raporu", S. 11

[127] **"Portal Nedir?",** http://www.pbs.com.tr/DesktopDefault.aspx?tabid=395 (Temmuz 2009)
[128] **"Portal Nedir?",** http://www.odakdizayn.com/portal_tasarimi (Temmuz 2009)
[129] https://www.turkiye.gov.tr/static/sss/002.html (Şubat 2009)

- **E-Devlet Portallarının Sahip Olması Gereken Özellikler**

Bir E-Devlet portalının, portal niteliklerini taşıyabilmesi, başarılı olabilmesi ve amacına uygun olarak hizmet verebilmesi için aşağıdaki özellikleri taşımaları gerekmektedir.

İnternet sitesi adresleri kolay ve akılda kalıcı olmalıdır.

- İnternet sitesi erişimi ve işlem gücü hızlı olmalıdır.
- İnternet sitesi kullanımı kolay (user - friendly) olmalıdır.
- İnternet sitesi tıpkı bir sanat eseri gibi dizayn edilmeli ve göze hitap etmelidir.
- İnternet siteleri ait oldukları kurumlar hakkında tarihı geçmişleri, hizmet çeşitleri, hizmet alanları, çalışan sayısı, erişim adresleri gibi bilgiler içermelidir.
- internet siteleri, ait oldukları kurumların misyon, vizyon ve hedefleri hakkında bilgi vermelidir.
- İnternet sitesi kurumlara erişim yol ve metotlarını içermelidir.[130]

- **Ed-tr Projesinin Amaç Ve Hedefleri**

Başbakanlık tarafından desteklenen, yürütülen ve takip edilen E-Devlet Türkiye Projesinin kısaltması olan Ed-tr projesinin amaç ve hedefleri aşağıda belirtilmeye çalışılmıştır.

- BİT alanındaki gelişmelerden vatandaşların, işletmelerin ve kamu kurumlarının en üst düzeyde faydalanmalarının sağlanması,
- Vatandaşlara daha kaliteli ve hızlı kamu hizmeti sunabilmek amacıyla; katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş bir devlet yapısının oluşturulması,
- BİT politikaları ve mevzuatının öncelikle AB müktesebatı çerçevesinde gözden geçirilerek yeniden düzenlenmesi ve bu konuda e-Avrupa+ kapsamında aday ülkeler için öngörülen eylem planının ülkemize uyarlanması amaçlanmaktadır. eDTr Projesi kapsamında DPT Müsteşarlığının koordinatörlüğünde, AB'nin e-Avrupa eylem planının hedefleri ile uyumlu, 2003-2005 yıllarını kapsayan iki eylem planı hazırlanmıştır.
- E-Avrupa eylem planlarında olduğu gibi eDTr Projesinde de ucuz, hızlı, güvenli internet alt yapısının oluşturulması ve kamu hizmetlerine elektronik erişimin sağlanması"[131]

[130] YILDIRIM ve Diğerleri, S.85
[131] "e-Devlete Geçişte Kamu Kurumları İnternet Siteleri, S.9

- Kurum İnternet Sitelerinden Beklenen en önemli fayda; verimliliği artırması ve bürokrasiyi etkin bir şekilde azaltmasıdır.[132]

- **E-Devlet Portallarının Getireceği Kolaylıklar**

E-Devlet portalının vatandaşa, özel kurum ve kuruluşlara ve kamu kurumlarına getireceği faydalar ve kolaylıklar ise aşağıda belirtilmeye çalışılmıştır.

- Elektronik ortamdan sunulan kamu hizmetlerine tek bir internet sitesi üzerinden erişim imkanı sunmaktadır.
- Kamu hizmetleri ile ilgili doğru ve güncel bilgilere ulaşma imkanı sağlamaktadır.
- Tek bir kimlik doğrulaması sayesinde birçok hizmete ikinci bir kimlik doğrulamasına gerek duyulmadan erişilebilmektedir.
- e-Devlet Portalı üzerinden alınacak elektronik hizmetler için (vergi, harç vb.) ödeme yapılması gerektiğinde ilerleyen dönemde devreye alınacak ödeme birimi hizmeti sayesinde bu işlem Portal üzerinden kolayca yapılabilecektir.
- Elektronik hizmetler yüksek güvenlikle (kapalı zarflarla kullanıcıya ulaştırılacak şifre, elektronik imza veya mobil imza) sunulmaktadır.[133]

- **E-Devlete Geçişte İnternet Sitelerinin Aşamaları**

E-Devlete geçiş sürecince tüm kamu kurumlarının internette aynı ve yüksek kabiliyette ve özellikte kurum siteleri tasarlanması ve bunun talep tüm kurumlardan talep edilmesi, taleplerin başarılı ve eksiksiz şekilde karşılanmasını sağlamayacak, tam tersine çok sorunlu, eksik ya da yanlış portalların ortaya çıkmasına neden olacaktır. Bu nedenle bu geçiş sürecinde kurumların kabiliyet ve özelliklerine göre farklı seviyelerde kurum sitesi profilleri çıkartılmış ve her kurumdan, o kurumun uygun olduğu profile uygun web sayfası hazırlanması talep edilmiştir. Bu kapsamda belirlenen portal çeşitleri ve özellikleri aşağıda belirtilmeye çalışılmıştır.

- Basit Bir İnternet Sitesi. Bu sitelerde kurum hakkında temel bilgiler ve halkın kullanımına sunulan belli başlı basılı dokümanların elektronik versiyonları yer alır.

---

[132] A.G.E., S.13
[133] https://www.turkiye.gov.tr/static/sss/005.html (Şubat 2009)

- Elektronik Yayıncılık. Kurum, iletişim stratejisinin önemli bir parçası olarak, web sitesinin kapsamını, çok sayıda sayfa ekleyerek ve kurum bilgilerinin önemli bir bölümünü koyarak genişletir. Kullanıcı formları indirebilir.
- İnteraktif (Etkileşimli) e-Yayıncılık. Bu düzeyde, kullanıcı hizmetle ilgili başvurularını internetten gönderilebilir, internet üzerinden sorgulama yapabilir.
- İşlem Yapılabilen İnternet Sitesi. Kullanıcı kurum ile çevrimiçi bağlantı kurarak, güvenilir bir şekilde kimliğini belgeleyip onaylatarak, özel işlemlerini tam olarak internet üzerinden gerçekleştirebilir.
- Katılımcı e-Yönetişim. Kullanıcı, kamu kurumlarının internet sitelerinde verilen hizmetlere, çevrimiçi olarak ve bir hizmetin tüm süreçlerinin entegre edildiği bir yapıda tek bir noktadan ulaşabilir.[134]

Türkiye'deki kamu internet sitelerine Tablo 15'den bakıldığında, toplam 109 kamu web sayfası üzerinde yapılan incelemede, sadece bilgi verilmek maksatlı hazırlanan 4 adet site olduğu ve bu nedenle de önemsenmeyerek sürekli erişime açık halde tutulmadığı ya da tutulamadığı görülmektedir. Bu tarz sitelerin erişilebilirlik oranlarının %4 olduğu bunu göstermektedir.

Karşılıklı iletişime imkan sağlayan sitelerin ise erişilebilirliklerinin %74 olduğu görülmektedir. Elektronik belge sunabilen sitelerin ise, bu önemli hizmetlerine rağmen erişilebilirliklerinin, karşılıklı iletişime imkan sağlayan siteler kadar bile olmadığı ve %21,5 seviyesinde olduğu tespit edilmiştir.

[134] "e-Devlete Geçişte Kamu Kurumları İnternet Siteleri", S.11

Tablo 15
Türkiye'de Mevcut Kamu Internet Uygulamaları

No	Sınıflandırma	Kurum Sayısı	Erişilebilenlerin Yüzdesi	Genel Toplamın Yüzdesi
1	Sadece bilgi vermeye yönelik olanlar	4	4.0	2.5
2	Karşılıklı iletişime imkan sağlayanlar	81	74.5	51.0
3	Elektronik belge sağlayabilenler	24	21.5	15.0
	Erişilebilen Kurumların Toplamı	**109**	**%100**	**%68.5**
1	Hazırlık Aşamasında Olanlar	4		2.5
2	Web Sayfaları Sorunlu Olanlar	7		4.5
3	Web Sayfası Bulunmayanlar	38		24.5
	Genel Toplam	**158**		**%31.5**

Kaynak: "Ankara Raporu", Türkiye 2. Bilişim Şurası, S.289,

E-Devlet kapsamında hizmet veren kamu kurumları ve bu kurumların kendi kurumlarının ve ya bağlı bulundukları üst kurumların internet siteleri, portalları ve ya diğer bilişim / iletişim sistemleri üzerinden verdikleri projeler Tablo 16'da listelenmeye çalışılmıştır.

Tablo 16
E-Devlet Projeleri

e-Devlet Projeleri	
Tarım Bakanlığı	**Sağlık Bakanlığı**
MIS (Management Information System) Projesi	TSİM Projesi
TAP (Tarımsal Araştırma Projesi	ÇKYM Projesi
TUYAP (Tarımsal Uygulama, Araştırma ve Yayım Projesi)	HBS Projesi
Milli Eğitim Bakanlığı	**İçişleri Bakanlığı**
MEB-NET (MEB Yönetim Bilgi Sistemi)	İLEMOD Projesi (İl Envanterinin Modernizasyonu)
MEB-SİS (İLSİS, OKULSİS, PERSİS Projeleri)	MERNİS Projesi
BİLDEMER (Bilgisayar Destekli Meslek Rehberliği Projesi)	**Emniyet Gn.Md.**
DÖNERSİS Projesi	POL-NET 2000 Projesi
Etkileşimli Uzaktan Eğitim Kablo Yayıncılığı Uygulamaları Projesi	Mobil Bilgisayar Projesi
Açık Öğretim Lisesi Projesi	**Adli Sicil Gn. Müd**
EMP (Eğitimde Modernizasyon Projesi)	Adli Sicil Projesi
Çalışma Bakanlığı	**Sanayi Bakanlığı**
SSK Projesi	Elektronik Ticaret Projesi
Bağ- Kur Projesi	KOSBİLTOP (Küçük ve Orta Ölçekli Sanayi Bilgi Toplama Projesi)
Orman Bakanlığı	**KOSGEB**
Coğrafi Bilgi Sistemleri Projesi	KOBİ- NET
Maliye Bakanlığı	**Posta İşletmesi Gn. Md.**

e-Devlet Projeleri	
Maliye Bakanlığı Projesi	Havale Çek Tahsil at Gişeciliği Projesi
GELNET Projesi (Gelirler Projesi)	OCR Projesi (Optik karakter Tanıma)
VEDOP (Vergi Dairesi Otomasyon)Projesi	Elektronik Tartı ve Bilgisayar Projesi
Saymanlık Projesi	Internet Projesi
Emekli Sandığı Projesi	**Karayolları Gn.Md.**
Hukuk Bilişim Sistemi Projesi	Yol Bilgi Ağı Projesi
TAKBİS (Tapu Kadastro Bilişim Sistemi) Projesi	Otomatik Geçiş Sistemi Projesi (OGS)
Milli Emlak Projesi	Trafik Yönetim Sistemi Projesi (TYS)
Dış Ticaret Müsteşarlığı	Acil Haberleşme Sistemi Projesi
İHRACAT- NET Projesi (Dış Ticaretin İzlenmesi)	Coğrafi Bilgi Sistemi Projesi
Hazine Müsteşarlığı	**TCDD Gn.Md.**
HAZİNE- NET Projesi	Rezervasyon ve OMIS (Operasyonel Yönetim Bilişim Sistemi) Projesi
TÜBİTAK- BİLTEN	CTC (Merkezi Trafik Kontrol Projesi)
ETSOP (Elektronik Ticaret Stratejik Odak Noktası Projesi)	**THY Gn.Md.**
Gümrük Müsteşarlığı	Elektronik Bilet Projesi
BİLGE- EDİ Projesi	**Turizm Bakanlığı**
GİBOS Projesi	TURİZM-NET Projesi
T.C. Merkez Bankası	TURSAB Projesi
EFT-I Projesi	Yurtdışı Bürolara Otomasyon Projesi
EFT-II Projesi	Devlet Malzeme Ofisi

e-Devlet Projeleri	
EMKT (Elektronik Menkul Kıymet Sistemi Projesi)	Elektronik Satış Merkezi
Ulusal Veri Tabanları Projesi	Özürlüler İdaresi Başkanlığı
TOBB	Özürlülere yönelik Bilgi Erişim sistemi
Borsalararası Bilgi Ağı Projesi	Emekli Sandığı Genel Müdürlüğü
Odalararası Bilgi Ağı Projesi	Sağlık Projesi
İGEME	KOBİ- NET
GTP-NET Projesi (Küresel Ticaret Noktası Projesi)	Posta İşletmesi Gn. Md.
Coğrafi Bilgi Sistemleri Projesi	Havale Çek Tahsil at Gişeciliği Projesi
Maliye Bakanlığı	OCR Projesi (Optik karakter Tanıma)
Maliye Bakanlığı Projesi	Elektronik Tartı ve Bilgisayar Projesi
GELNET Projesi (Gelirler Projesi)	Internet Projesi
VEDOP (Vergi Dairesi Otomasyon)Projesi	Karayolları Gn.Md.
Saymanlık Projesi	Yol Bilgi Ağı Projesi
Emekli Sandığı Projesi	Otomatik Geçiş Sistemi Projesi (OGS)
Hukuk Bilişim Sistemi Projesi	Trafik Yönetim Sistemi Projesi (TYS)
TAKBİS (Tapu Kadastro Bilişim Sistemi) Projesi	Acil Haberleşme Sistemi Projesi
Milli Emlak Projesi	Coğrafi Bilgi Sistemi Projesi
Dış Ticaret Müsteşarlığı	TCDD Gn.Md.
İHRACAT- NET Projesi (Dış Ticaretin İzlenmesi)	Rezervasyon ve OMIS (Operasyonel Yönetim Bilişim Sistemi) Projesi
Hazine Müsteşarlığı	CTC (Merkezi Trafik Kontrol Projesi)
HAZİNE- NET Projesi	THY Gn.Md.

e-Devlet Projeleri	
TÜBİTAK- BİLTEN	Elektronik Bilet Projesi
ETSOP (Elektronik Ticaret Stratejik Odak Noktası Projesi)	**Turizm Bakanlığı**
Gümrük Müsteşarlığı	TURİZM-NET Projesi
BİLGE- EDİ Projesi	TURSAB Projesi
GİBOS Projesi	Yurtdışı Bürolara Otomasyon Projesi
T.C. Merkez Bankası	Devlet Malzeme Ofisi
EFT-I Projesi	Elektronik Satış Merkezi
EFT-II Projesi	Özürlüler İdaresi Başkanlığı
EMKT (Elektronik Menkul Kıymet Sistemi Projesi)	Özürlülere yönelik Bilgi Erişim sistemi
Ulusal Veri Tabanları Projesi	Emekli Sandığı Genel Müdürlüğü
TOBB	Sağlık Projesi
Borsalararası Bilgi Ağı Projesi	
Odalararası Bilgi Ağı Projesi	
İGEME	
GTP-NET Projesi (Küresel Ticaret Noktası Projesi)	

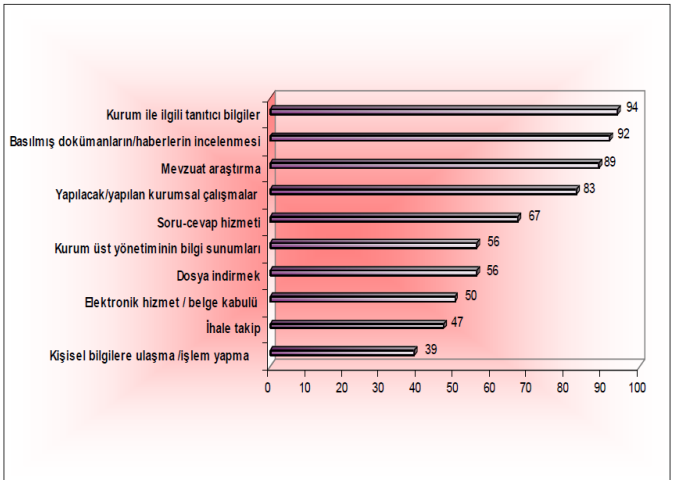
Kaynak: "Ankara Raporu", S.291 – 293

- **E-Devlet Portalından Verilecek Hizmetler**

E-Devlet Portalı üzerinden vatandaşlara verilen hizmetler genel olarak şöyle gruplandırılabilir:

- Bilgilendirme hizmetleri
- e-Hizmetler
- Ödeme işlemleri
- Kurum ve kuruluşlara kısayollar
- Güncel bilgiler ve duyurular
- Kurumlardan vatandaşlara mesajlar

Bunun yanı sıra kamu kurumları arasında bilgi ve belgelerin paylaşımı e-Devlet portalı tarafından sunulan hizmetler ile sağlanmaktadır. Bunlara ek olarak e-Devlet portalı ile sunulan hizmetler Şekil 39'daki gibi listelenebilir.[135]



Şekil 39 : Kamu İnternet Sitelerinden Sunulan Bilgi ve Hizmetler (%)

Kaynak: "E-Devlete Geçişte Kamu Kurumları İnternet Siteleri Performans Denetimi Raporu", T.C. Sayıştay Başkanlığı, Ankara, 2006, S.88
http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-2Web/2006-Web.pdf (Ocak 2010)

[135] https://www.turkiye.gov.tr/static/sss/004.html (Mayıs 2010)

- **Vatandaşlar E-Devlet Portalını Nasıl Kullanabilecekler?**

Yukarıda bahsedilen E-Devlet portalının sunduğu bilgi ve hizmetleri vatandaşlar aşağıda belirtilmeye çalışılan yol ve yöntemlerle kullanabileceklerdir.

- Internet ve web aracılığı ile işlem,
- Etkileşimli telefon (sabit veya mobil) kullanılarak işlem,
- Kiosk kullanımı yoluyla işlem,
- Sayısal Televizyonlar aracılığıyla işlem olarak belirtilebilir.

www.turkiye.gov.tr adresinde ise, tüm kamu kurumları hakkında genel bilgiler sağlayan içeriklere ulaşmak mümkündür. Yine bu adreste, kişisel bilgilere erişerek işlem yapmak veya kimlik doğrulama gerektiren e-hizmetlere erişim için şifre, e- imza veya mobil imzaya ihtiyaç duyulmakta ve herhangi bir kimlik doğrulaması (şifre, e-imza ve mobil imza) ile kullanıma sunulan pek çok e-hizmet bu adresten alınabilmektedir. Şu anda, bahse konu portal üzerinden herhangi bir ödeme işlemi yapılmamaktadır. Ayrıca, e-Devlet portalı üzerinden alınacak elektronik hizmetler için (vergi, harç vs. gibi) ödeme yapılması konusu, önümüzdeki dönemde devreye alınacak olan ödeme birimi hizmeti sayesinde güvenli bir ortamda e-Devlet portalı üzerinden yapılabilecektir.[136]

[136] https://www.turkiye.gov.tr/static/sss/003.html (Ocak 2009)

- **E-Devlet Uygulamaları**

E-Devlet uygulamaları sayesinde, günlük iş ve süreçlerde bir değişim ve başkalaşım oluşması beklenmektedir. Beklenen bu değişimler Tablo 17'de belirtilmeye çalışılmıştır.

Tablo 17
İş ve Hizmetlerde E-Devlet ile Oluşan ve Oluşması Gereken / Beklenen Başkalaşımlar

Geleneksel Devlet	E-Devlet
Pasif Yurttaş	Aktif Müşteri-Yurttaş
Kağıt-temelli İletişim	Elektronik İletişim
Dikey/Hiyerarşik Yapılanma	Yatay/Koordineli Ağ Yapılanması
Yönetimin Veri Yüklemesi	Yurttaşın Veri Yüklemesi
Eleman Yanıtı	Otomatik Sesli Posta, Çağrı Merkezi vb.
Eleman Yardımı	Kendi kendine Yardım / Uzman Yardımı
Eleman-temelli Denetim Mekanizması	Otomatik Veri Güncellemesiyle Denetim
Nakit Akışı / Çek	Elektronik Fon Transferi (EFT)
Tektip Hizmet	Kişiselleştirilmiş/Farklılaştırılmış Hizmet
Bölümlenmiş / Kesintili Hizmet	Bütünsel / Sürekli / Tek-duraklı Hizmet
Yüksek İşlem Maliyetleri	Düşük İşlem Maliyetleri
Verimsiz Büyüme	Verimlilik Yönetimi
Tek Yönlü İletişim	Etkileşim
Uyruk İlişkisi	Katılım İlişkisi
Kapalı Devlet	**Açık Devlet**

Kaynak: "Ekonomik Suç Kavramı ve Sigortacılık Suçlarının Bu Açıdan Değerlendirilmesi", Sayıştay Dergisi, S.88 – 89
http://www.tk.gov.tr/yayin/Sureli_Yayinlar/trd/pdf/trd_2005_2.pdf (Şubat 2010)

E-Devlet uygulamaları sayesinde, devletten vatandaşa, devletten devlete ve devletten iş dünyasına olmak üzere 3 yönlü olarak sunulmaktadır. Bunlara değinilecek olursa,

- Devletten Vatandaşa

1. Bilgi sağlama/verme amacıyla sunulan hizmetler:
    a. Haberler, dokümanlar, raporlar,
    b. Kamu bilgileri,
    c. Hava durumu ve meteoroloji hizmetleri,
    d. Yol durumu ve ulaşım bilgileri,
    e. Döviz kurları, İstatistiksel bilgiler,
    f. Resmi gazete, mevzuat ve kanunlar,
    g. Sanatsal ve kültürel etkinlikler.
2. Sorgulama ve yanıt alma alma şeklinde sunulan hizmetler:
    a. Sosyal yardımlar, sağlık, aile ve çocuk,
    b. Eğitim,
    c. Yerel yönetimler,
    d. Kurumlara dilekçe vermek,
    e. Ehliyet, pasaport vb. talepler,
    f. Telefon başvurusu, nakil ve kapama,
    g. İş/eleman arama,
    h. Güvenlik ve askerlik,
    i. Yargı işlemleri,
    j. Yer sorma işlemleri (semt, bina, hastane vb),
3. Çevrimiçi işlemler olarak sunulan hizmetler:
    a. Vergi beyannamesi ve tahakkuk işlemleri,
    b. Bankacılık işlemleri,
    c. Sigorta işlemleri,
    d. Kamu alımları,
    e. Hastane randevu sistemi,
    f. Dispanser ve sağlık ocakları,
    g. Acil yardım, itfaiye ve ambulans hizmetleri,
    h. Hazine bonoları, devlet tahvili işlemleri,
    i. Standart, Marka, patent başvurusu,
    j. Sertifikasyon,
    k. Bilimsel araştırma formlarına başvuru,
    l. Öğrenci kredisi başvurusu, okullara başvuru ve kayıt,
    m. Demokratik yönetim ve seçim,
    n. Askerlik başvurusu,
    o. Ulaşım, rezervasyon ve bilet alma.

- **Devletten Devlete**

Bu paylaşımda amaç, E-Devlet ortamında, herhangi iki kamu kurum/kuruluşu arasındaki ilişkilerin bütünüyle elektronik ortamda gerçekleştirilmesidir.

- **Devletten İş Dünyasına**

Bu paylaşımda ise amaç, e-beyanname, gümrük vergisi, mernis, e-randevu gibi projelerin özel kurum ya da kuruluşlar ile paylaşılarak verinin en etkin şekilde bilgiye dönüştürülerek kullanılmasının sağlanmasıdır.

3.3.1. E-Devlet Ve Web Güvenliği İlişkisi

Yukarıda belirtilen tüm E-Devlet hizmetlerine rağmen, E-Devlet uygulama kullanımlarının o ülkedeki internet kullanımı ile doğru orantılı olduğu unutulmamalıdır. Dünya geneline bakıldığında Türkiye'de bu oranların 2001 yılında da düşük olduğu Şekil 41'de net bir biçimde ortaya çıkmaktadır. Aradan geçen zamana rağmen, Türkiye'deki internet kullanımı Şekil 40'da da belirtildiği üzere artmış olsa da e-devlet uygulamalarının kullanım oranlarının aynı oranda artmadığı düşünülmektedir.

Total Internet Users by Country*

April 2009

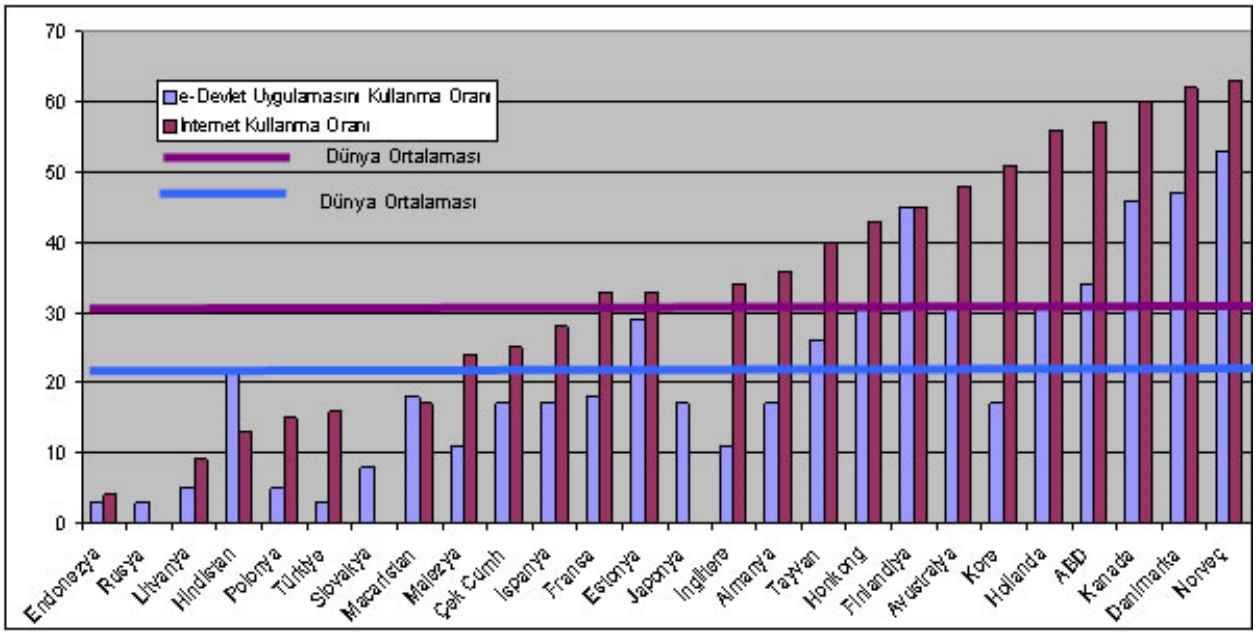
Total Europe, Age 15+ - Home & Work Locations

Source: comScore World Metrix

Country	Total Unique Visitors (000)	Average Hours per Visitor	Average Pages per Visitor
Germany	40,000	22	2,601
United Kingdom	36,820	29	2,482
France	36,348	28	2,971
Russia	31,303	15	2,228
Italy	21,230	19	1,790
Spain	18,636	25	2,398
Turkey	17,762	32	3,044
Netherlands	12,009	25	2,712
Sweden	5,671	25	2,712
Belgium	5,470	19	2,032
Switzerland	4,439	20	2,011
Austria	4,403	14	1,562
Portugal	3,774	19	1,725
Denmark	3,429	18	1,890
Finland	3,174	26	2,777
Norway	3,007	21	1,921
Ireland	1,749	17	1,

Şekil 40 : Ülke Bazında İnternet Kullanım Oranları

Kaynak: "Türkiye Raporu", ComScore Şirketi, Mayıs 2009, S.1 http://www.comscore.com/Press_Events/Press_Releases/2009/5/Turkey_has_Seventh_Largest_Online_Audience_in_Europe/(language)/eng-US (Mayıs 2009)



Şekil 41 : Dünyada e-Devlet Uygulama ve Internet Kullanım Büyüklükleri

Kaynak: "Benchmarking Research Study TNS Consultants" Goverment Online Şirketi, 2001, S.17, http://www.bibliotheque.assnat.qc.ca/01/mono/2010/02/1022345.pdf (Mart 2009)

Yine dünya geneline bakıldığında, ülkelerin ve ülke halkının E-Devlet kullanım oranları içerisinde Türkiye'nin %3 ile en alt sıralarda yer aldığı Şekil 42'de görülmektedir.

Yüksek	Orta	Düşük
Norveç (%53)	Estonya (%25)	İngiltere (%11)
Danimarka (%47)	Hindistan (%22)	Malezya (%11)
Kanada (%46)	Fransa (%18)	Letonya (%8)
Finlandiya (%45)	Macaristan (%18)	Slovakya (%8)
ABD (%34)	İspanya (%17)	Litvanya (%5)
Hong Kong (%31)	Çek Cum. (%17)	Polonya (%5)
Avustralya (%31)	Almanya (%17)	Rusya (%3)
Hollanda (%31)	Kore (%17)	Türkiye (%3)
Tayvan (%26)	Japonya (%16)	Endonezya (%3)

Şekil 42 : Dünya'da e- Devlet Kullanım Büyüklükleri

Kaynak: "Ankara Raporu", S.290

Bu oranlar içerisinde interneti kullanan nüfusun ise, internet kullanım amaçlarına bakıldığında, internete daha çok bilgi ve araştırma yapmak için girildiği bu oranın ise giderek düşmekte olduğu, buna rağmen iletişim kurma amaçlı internet kullanım oranlarının giderek yükseldiği

anlaşılmaktadır. Ek olarak kamu kurum ve kuruluşları ile irtibat kurmak, sağlık, eğitim ve e-ticaret kullanım oranlarının düşmekte oldukları görülmektedir. Son 3 ay içerisinde internet kullananlar üzerinde yapılan bir incelemenin sonuçlarını içeren Şekil 43'e bakıldığında ise bu kanı hemen hemen doğrulanmaktadır.

Amaçlar	2004	2005
Bilgi arama ve çevirimiçi (on-line) hizmetler	93, 18	90, 16
İletişim	76, 10	78, 23
Kamu kurum/kuruluşlarıyla iletişim	45, 39	39, 97
Kamu kuruluşlarına ait internet sitelerinden bilgi edinmek	43, 03	37, 64
Resmi formların/dokümanların indirilmesi	20, 69	10, 65
Doldurulmuş form göndermek	10, 37	6, 02
Eğitim	42, 72	30, 71
Sağlık	?	22, 97
Mal ve hizmet siparişi vermek ve satmak, bankacılık	17, 38	15, 95

Şekil 43 : Son Üç Ay İçinde Hane Halkı Bireylerinin İnternet Kullanma Amaçları (%)

Kaynak: "e-Devlete Geçişte Kamu Kurumları İnternet Siteleri", S.87

Web uygulamalarının yaygınlaşması, bu uygulamaları geliştirmek için yeni teknolojilerin ortaya çıkması ve uygulamalarının son kullanıcıya sağladığı hizmetlerin daha geniş bir perspektife yayılması, web uygulamalarının güvenli kılınması noktasını daha da belirgin hale getirdi.

E-Devlet uygulamaları, internet bankacılığı işlemleri, online alışveriş ve benzeri birçok web uygulamasının hayatımızda önemli rol oynamaya başlaması, hatta sağlık ve finans sektörleri gibi doğrudan kişileri etkileyen sektörlerin web uygulamaları aracılığıyla hizmet vermesi, hem kullanıcı bazlı kişisel güvenliğin önemini artırmış hem de bu hizmetlerin kullandığı web sistemlerinin güvenli hizmet vermesini zorunlu hale getirmiştir.[137]

[137] **"Yazılımcılar ve Denetimciler için Web Uygulamaları Güvenliği"**, (Eylül 2009)

Kurumsal ortamlarda bilgisayar güvenliğinde uygulanması gereken önleme adımları daha geniş ve karmaşıktır. Güvenlik ile ilgili uzmanlaşmış kişilerin çalıştığı bu tür sistemlerde, önleme ile ilgili yapılanlardan bazıları aşağıda belirtilmeye çalışılmıştır.

- İşletim sistemi ve yazılımların servis paketlerinin ve güncellemelerin düzenli aralıklarla incelenmesi,
- Kullanıcı haklarının asgari seviyede tutulması,
- Kullanılmayan protokol, servis, bileşen ve proseslerin çalıştırılmaması,
- Veri iletişimindeşifrelemetekniklerinin, korunmasızlıktarayıcıları, Sanal Özel Ağ (Virtual Private Netvvork) kullanılması,
- Açık anahtar altyapısı (Public Key Infrastructure) ve e-imza kullanımı ile
- Biyometrik tabanlı sistemlerin kullanımı olarak sıralanabilirler.

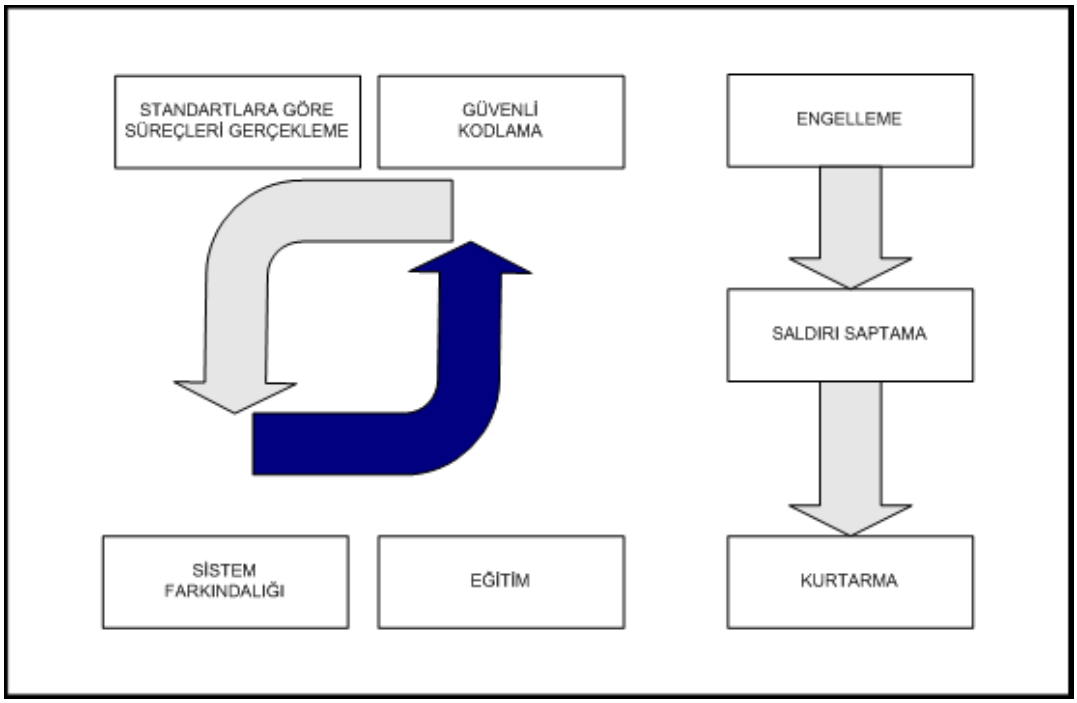
Büyük ağlarda olduğu gibi kurumsal ağlarda da, farklı web sistemleri, bunları yöneten ve üzerindeki yazılımları hazırlayan farklı ekipler bulunmaktadır. Bu nedenle bu sistemlerin güvenliğini sağlamak için daha kapsamlı sistemlere gereksinim duyulmaktadır. "Bir zincir ancak en zayıf halkası kadar güçlüdür." sözünün de belirttiği üzere, güvenliğin sağlanması için zayıf noktalardan doğacak sorunların mümkün olduğu kadar çözülmesi gerekmektedir. Bu da birbirini tamamlayan ve birlikte etkileşimli çalışan güvenlik sistemleri ile mümkün olabilmektedir. Bu tür bir yapılanmaya çok katmanlı güvenlik ve kademeli savunma (defense in depth) denilmektedir. Sel suyunu engelleyen ardışık bentler gibi; her katman, bir sonraki katmana geçilmeden önce sorunun bir kısmını çözmüş olacaktır.[138]

[138] Akademik Bilişim 2008 Sempozyumu Sunumları, S.1

3.3.2. Kamuda Web Güvenliği Standartları (Kurumsal Web Güvenliği Modeli)

Özel ya da kamu olsun, hizmet veren ve alan tüm birimler birer özel ya da tüzel ve ya kamusal "kurum" olduklarından burada her ikisini de kapsayacak olan "Kurumsal Web Güvenliği" modeli ele alınacaktır.

Kurumsal web güvenliği modeli, birbirleriyle etkileşimli çalışan çeşitli ve değişik güvenlik yöntemlerinden oluşan bir güvenlik sistemidir. Bu model Şekil 44'de gösterilmiştir.[139]



Şekil 44 : Kurumsal Web Güvenliği Modeli

Kaynak: "*Kurumsal Web Güvenliği Yapısı***",** S.2

[139] A.G.E., S.2

- Standardizasyon

Daha kararlı ve güvenli bir web bilgi sistemi için; standartların ve kuralların, kullanım ve güvenlik politikaları içerisinde tanımlanması ve uygulanabilirliğinin garanti edilmesi gerekmektedir. Bu konuda SANS Güvenlik Politikaları Projesi sayfasından (http://www.sans.org/resources/policies/) ayrıntılı bilgi edinmek mümkündür. Bu konuda ki örnekler, incelenmeli ve kurumun ihtiyaç ve yapısına göre güvenlik politikaları revize edilerek düzenlenmelidir. Kurumsal olarak tanımlanabilecek web güvenliği standartlarına aşağıdaki maddeler örnek olarak verilebilir.

- Web Sunucu düzlem (işletim sistemi, web sunucu yazılımı, yazılım geliştirme ortamı...vb.) kısıtlamaları, zafiyet çözümleme yöntemleri, yama yönetimi ve yedekleme sistemlerinin tanımlaması yapılmalıdır.
- Mümkün olduğunca az web sunucusu kullanılmalıdır (yönetimi kolaylaştırmak için). Merkezi bir web sunucusu ve ya hizmeti kullanmak ve kuruma ait birimlerin sadece bu sunucu ya da hizmeti kullanmalarını sağlamak iyi bir uygulama örneği olmaktadır.
- Web sitelerinde, güvenlik ve kişisel gizlilik politikaları verilmelidir. Dünya çapında kamu web sitelerinin sadece %29'unda kişisel gizlilik politikasının bulunduğu ve sadece %21'inde güvenlik politikası açıklamalarının bulunduğu saptanmıştır.
- Web uygulamaları geliştirilirken güvenli kodlama esaslarına uyulması gerekmektedir.
- Zaafiyet sınamasının, yazılım geliştirme yaşam döngüsü (YGYD) içinde de (beyaz kutu güvenlik taraması) gerçekleştirilmesinin sağlanmalıdır.
- Web uygulamalarına ait belgelemelerin kesinlikle yapılması ve yapılırken de javadoc, phpdoc gibi uygun araçların kullanılması uygun olacaktır.
- Kurumsal web sayfalarının belirli bir yapıya ve şablona uyması sağlanmalıdır. E-dönüşüm Türkiye Projesi kapsamında hazırlanan kılavuzla, kamu kurumlarının İnternet sitelerinde asgari düzeyde içerik ve tasarım uyumunun sağlaması için gerekenler anlatılmıştır. Bu belge, web sitelerinin yapısal gereksinimleri anlatmakla beraber, güvenliğin sağlanması konusunda yapılması gerekenlere ilişkin bilgiler içermemekte, çok basit, yetersiz ve yüzeysel olarak değinmektedir.
- Kurumlar, Web İçerik Yönetim Sitemlerini (Web Content Management Systems- CMS) ve portal yazılımlarını mümkünse

kendileri geliştirmelidir. Ancak kurumda bu konu ile ilgili yeterli ve yetkin personel ve ödenek olmaması durumunda, kurum bunun yerine, özel bir içerik yönetim sistemini seçip bu sistemin yamalarını düzenli olarak izlemeyi de tercih edebilir. Ancak bu tür bir durumda, seçilen CMS uygulamasının, güvenli bir şekilde kurulumunun sağlanması ve güvenlik yamalarının yine kurumca takip edilerek sisteme entegre edilerek uygulanması gerekmektedir.

- Web sayfası yüklenirken kasti veya teknik nedenlerden dolayı web yazılımlarında oluşan hatalarda, kullanıcıya kurumun şablon hata sayfası gönderilmelidir. Böylece saldırganların sistemle ilgili hassas bilgiler edinmesi engellenmiş olacaktır.
- Ağ yönetim grubu, standartlara uyulmaması durumunda web sitesine ya da servisine erişimini kapatma hakkına sahip olmalıdır.[140]

- Güvenli Kodlama

Web uygulamaları geliştirilirken tasarım sürecinden itibaren güvenli kodlama esaslarına uyulmalıdır. OWASP'ın (http://www.owasp.org) Güvenli Kodlama İlkeleri belgesi ve Güvenli Web Uygulamaları Geliştirme Kılavuzu belgesi kurum içi eğitimlerde kullanılmalı ve yazılım geliştiricilerin bu esaslara uyup uymadıkları kontrol edilmelidir. Yazılım geliştirme yaşam döngüsünün ilk aşamalarından itibaren güvenlik süreçlerini eklemek için yapısal bir yaklaşım sunan OWASP CLASP Projesi (Kapsamlı ve Kolay Uygulama Güvenlik Süreci - Comprehensive, Lightweight Application Security Process) incelenmeli ve uygulanmalıdır. Ek olarak, Microsoft'un yazılım geliştirme süreci için oluşturulan, güvenilir bilişim güvenlik geliştirme yaşam döngüsü de kullanılabilir.

Yazılım geliştirirken uyulması gereken temel ilkeleri aşağıdaki gibi özetlemek mümkündür.

- Görev tanımlama: Kullanıcıların görevleri ve yetkileri tanımlanmalıdır. Her kullanıcıya veya kullanıcı grubuna farklı güvenlik düzeyleri tanımlanmalıdır.
- Farklı güvenlik düzeyleri: Yazılımın ve işlenen verinin önemine göre farklı güvenlik düzeyleri ve önlemleri kullanılmalıdır.
- En az yetki: Kullanıcıya ve alt sistemlere mümkün olan en az yetkinin verilmesi sağlamalıdır.

[140] A.G.E., S.2 - 3

- Güvenli varsayılan ayarlar: Varsayılan olarak güvenlik mümkün olan en yüksek düzeyde tutulmalı, kullanıcının isterse güvenlik düzeyini düşürme ve yükseltme yönünde ayarlama yapmasına izin vermelidir.
- Kademeli savunma: Herhangi bir işlem ile ilgili bir denetimin yeterli olması durumunda bile, kullanıcıya aksettirilmeden birden fazla denetimi uygulayarak daha güvenli ortamlar sağlanmalıdır.
- Önlemleri yalın tutmak: Alınan önlemlerin karmaşık olması, her zaman daha güvenli olacağı anlamına gelmediğinden, yazılımcının nasıl çalıştığını anladığı ve sorun olduğunda çözüm sürecinde kolaylıkla çözebileceği yalınlıkta sistemler tasarlanmalıdır.
- Saldırı alanını azaltmak: Yapılan denetlemeler ve kısıtlamalarla, olabilecek saldırı etkisi, hedefi, zararları ve alanı azaltılmalıdır.
- Güvenli düşmek: Yazılımın hata vermesi durumunda, güvenlik açığına yol açmadan sonlanması sağlanmalıdır.
- Kurumlar ortak projelerde kullanmak üzere, kendilerine ait yazılım kütüphanelerini ve sınıflarını güvenli kodlama esaslarına uyarak geliştirmelidirler. Bu yazılım kodlarının bütün yazılım projelerinde kullanılması sağlanmalıdır.
- Yazılımcıları güvenli kodlama esaslarına göre yazılım geliştirmeye zorlayan Struts yazılım geliştirme çerçeve sistemleri (http://struts.apache.org/) gibi ortamların kullanılması sağlanmalıdır.[141]

- Sistem Farkındalığı

Ağ ve güvenlik yöneticileri, ağ üzerinde nelerin olup bittiğinden haberdar olmalıdırlar. Bu, ağ üzerinde korunması gereken aygıtları, onların şu anki durumunu, tehditleri ve saldırıya açık noktaları bilmeyi içerir. Sistem Farkındalığı olarak adlandırılan bu sistem, aşağıdaki düzeneklerden oluşmalıdır:

Web Bilgi Sistemi Farkındalığı: Web Bilgi Sistemi Farkındalığı, web sunucuları ve üzerlerinde çalışan web uygulamalarına ilişkin ayrıntılı bilgilerin saptanması, belirlenmesi ve bilinmesidir. Etkin (servis ve port tarayıcıları) ve edilgen (pasif ağ dinleyicileri) tekniklerin birbirleriyle etkileşimli kullanıldığı ve web sunucu altyapısına ilişkin güncel bilgilerin edinildiği bir yapı önerilmiştir. Bu sisteme, kurumun gereksinimlerine göre

[141] A.G.E., S.3 - 4

özelleştirilmiş bir arama motorunun eklenmesi ile kurumun bilgi sistemindeki web içeriği endekslenebilecektir.

Saldırıya Açıklık Çözümlemesi: Web sistemleri ve üzerlerinde çalışan web uygulamalarına ait güvenlik açıkları, zafiyet (zayıflık) çözümleme sistemleri kullanılarak saptanabilmektedir. Web uygulamalarının saldırıya açıklık çözümlemeleri için kullanılan iki tür yöntemden söz etmek mümkündür.

Açık Kutu Sınaması: Web yazılımının kaynak kodu üzerinde yapılan sınamadır. Yazılım koduna erişimin mümkün olduğu durumlarda mutlaka kullanılması ve sınamanın mümkünse yazılım geliştirme yaşam döngüsü (YGYD) içerisine eklenmesi önerilmektedir. Bu yöntemle birçok olası saldırıya imkan sağlayan zafiyetlerin bulunması sağlanabilecektir. OWASP'ın "WebScarab", Firefox'un "Web Developer Toolbar", "Greasemonkey" ve "XSS Assistant" bu sınama için kullanılabilecek programlara örnek olarak verilebilir.

Kapalı Kutu Sınaması: Web sistemine dışarıdan yapılan sınamadır. Web yazılımı koduna erişim mümkün olmadığında tercih edilen bir saldırıya açıklık sınamasıdır. Kapalı kutu sınaması, genel ve herkes tarafından bilinen zafiyetleri tarayarak inceleme yaptıklarından sadece saldırıya açıklıkların bir kısmını saptayabilmektedir. Bu sınamanın daha etkin olması için web sistemleri üzerindeki bazı bölüm ya da kısımların üzerine özel olarak eğilerek denemeler yapılmalıdır. Nikto, Wapiti, Paros Proxy ve Burpsuite bu sınama için kullanılabilecek programlara örnek olarak verilebilir.

Web sistemleri dönemsel olarak kapalı kutu ve eğer mümkünse de açık kutu yöntemleri ile ilgili yöntem araçları yardımlarıyla taranmalı ve sınamaya ilişkin rapor teknik sorumlulara ulaştırılmalıdır. Bu raporlar saldırı yaşanmadan önce teknik personelin saldırıya açık noktalarda gerekli önlemleri almalarını sağlayacaktır. Saldırıya açıklık sınama sistemleri, Web Bilgi Sistemi Farkındalığı ve Saldırı Saptama Sistemleri (SSS) ile işbirliği içerisinde çalışmalıdır.

Web Sunucu İzleme: Web sunucuları, olağan dışı durumlara karşı sürekli olarak izlenmelidir. Bunun için kullanılan en etkin yöntem, basit ağ yönetim protokolü (SNMP) araçlarının kullanılmasıdır. Web sunucularına ait ağ trafiği, işlemci gücü, bellek kullanımı ve süreç istatistikleri gibi bilgiler SNMP araçları tarafından toplanmalı; çözümleme süreçleri ile daha ayrıntılı incelemeler yapılmalıdır.[142]

- Eğitim / Sınama

Web uygulama geliştiricileri ve web sunucu yöneticilerinin var olan güvenlik tehditleri ve bu tehditlere karşı alınması gereken önlemler hakkında bilgilendirilmeleri gerekmektedir. Bunun için de ilgili personellere gerekli eğitim ve öğretim verilmelidir. Bu amaçla kullanılmak üzere eğitim ve sınama için aşağıdaki düzenekler kullanılabilir:

Çalıştay ve Çalışma Grupları: Kurumdaki uygulama geliştiricileri ve web sunucu yöneticilerini bilgilendirmek amacıyla toplantılar, çalıştaylar yapılmalıdır. Uygulama geliştiricilerle yapılan toplantılarda güvenli kodlamanın ve web uygulamalarına girdi denetimi ve çıktı süzmesinin önemi örneklerle onları ikna ederek vurgulanmalı ve gösterilmelidir. Bu toplantılar sonucunda çalışma gruplarının oluşturulmalı ve bu çalışma gruplarına, kuruma özgü yazılımlar için girdi/çıktı denetimi yapan yazılım kütüphanelerini geliştirmek gibi görevler verilmelidir. Aynı zamanda içeri sızma sınamaları kullanılarak, saldırganların web uygulaması açıklarını kullanarak neler yapabileceğinin örneklerle gösterilmesi gerekmektedir.

Eğitim Portalı: Eğitim portalı, teknik sorumluların kurum iç ağından ulaşarak web güvenliği konusunda bilgilere ulaşabileceği bir bilgi ortamıdır. Bu bilgi ortamında sunulabilecek içeriğe örnek olarak aşağıdakiler verilebilir:

- Kurumda uyulması gereken web güvenliği standartları,
- İyi güvenli kodlama uygulama örnekleri,
- Yapılması ve yapılmaması gerekenlerin örneklerle açıklaması,
- Web sunucu yapılanma ayarları ve kontrol listeleri.

[142]A.G.E., S.4 - 5

Sınama Sunucuları: Kuruma özgü ya da kurumca hazırlanan web uygulamaları, sunucu güvenliği sağlanmış bir web sunucu üzerine konulmalı ve güvenlik uzmanlarının bu uygulamalardaki güvenlik açıklıklarını beyaz ya da kara kutu yöntemleri ile bulmaları istenmelidir.[143]

- Saldırı Saptama

Bilgisayar ağındaki olağan dışı etkinliklerin saptanması için çeşitli düzenekler kullanılmalıdır. Aşağıdaki düzenekler örnek olarak verilebilir.

Saptama Sistemleri: Saldırı Saptama Sistemleri (SSS), saldırıların ve olağan dışı etkinliklerin saptanması için kurulan sistemlerdir. Bir veya daha fazla ağ tabanlı SSS, kritik ağ kesimlerinde konuşlandırılabilir. SSS'in etkin çalışması, güncel ağ ve sistem bilgisine sahip olması ile gerekmektedir. Bu sistemler SSS'in ağ farkındalığı sistemi ile etkileşimli çalışmasını gerektirmektedir. SSS'in yapılanış ve kuralları web güvenliği için özerkleştirilmelidir. Bunun yanı sıra, sunucuların yerel güvenliği için sunucu tabanlı SSS'ler konuşlandırılabilir. Saldırganların sistemde yapabilecekleri değişikliklerin takibi açısından, Tripwire (http://sourceforge.net/projects/tripwire/) ve benzeri programlarla kritik sistem dosyalarında yaşanan değişimler izlenmelidir. Ancak bu sistemlerin adından da belli olduğu gibi saldırıları sadece saptadıkları unutulmamalıdır.

Günlük Denetimi: Sunucu günlük kayıtları (log), sunucu makineleri üzerindeki web sunucu yazılımları (örneğin apache) ve web uygulama güvenlik duvarı (örneğin Mod Security) gibi çeşitli sistemlerin günlük erişim ve iletişim bilgilerini içermektedir. Bu günlüklerin yorumlanarak çözümlenmek ve amaca yönelik bilgi elde etmek üzere eşgüdüm merkezi olarak adlandırılan ortak bir merkezde toplanması önerilmektedir. Web sunucu yazılımına ait erişim ve hata günlüklerinin ayrıntılı olarak çözümlenmesi, olağan erişimler dışındaki davranışların saptanmasını sağlayacağından, saldırı girişimlerine ilişkin bilgi sağlayacaktır.

[143] A.G.E., S.5

Saldırgan Tuzağı: Saldırgan tuzağı (honeypot), sisteme saldırı yapacak kişiler için kurulan tuzak sistemlerdir. Bu sistemler, saldırı saptama sistemleri tarafından yakalanamayan yeni zayıflıkların öğrenilmesi, saldırganlara daha korumasız sanal sistemler varmış gibi göstererek onların yanlış hedefler ile uğraşmalarının sağlanarak asıl sistemlerin korunması ve saldırganların saldırı anındaki davranışlarına ilişkin bilgi toplamak için kurulmaktadır. Kuruma özgü web uygulamaları sahte verilerle bu saldırgan tuzakları üzerinde konuşlandırılabilir. Saldırgan tuzakları, saldırgan etkinliklerine karşı sürekli olarak izlenmelidir.

Birden fazla saldırgan tuzağının oluşturduğu ağa, saldırgan tuzağı ağı (honeynet) denir. Genellikle saldırgan tuzaklarını izleyerek ayrıntılı istatistik ve günlük toplamak amacıyla da bu tür ağlar kurulmaktadır. Bu konuda Honeynet (http://project.honeynet.org) projesinin ayrıntılı çalışmaları bulunmaktadır.[144]

- Saldırı Engelleme

Engelleme ve diğer risk azaltıcı ve koruyucu sistemler, mümkün olduğunca kullanılmalıdır. Sistem aşağıdaki düzeneklerden oluşmaktadır:

Erişim Denetimi: Kurum, bazı web sunucuların ve üzerlerinde çalışan servislerin sadece kurum ağından erişilebilmesini ve dış dünyaya kapalı olmasını hedefleyebilir. Bu kuruma özel sunuculara erişim, kurumun kendi iç ağı (intranet) veya kurumun birlikte çalıştığı ortak kurumları da içeren bir harici ağ (extranet) ile kısıtlanabilir. Bunun yanı sıra, aygıtları yönetmek amaçlı olarak web sunuculara yapılan uzaktan erişimler de denetlenmeli ve kısıtlanmalıdır. Bütün bu denetimler ağ üzerinde, ağ tabanlı güvenlik duvarındaki yapılandırmayla ve/veya yönlendirici aygıtlarında devreye alınacak erişim listeleri ile gerçekleştirilebilir. Dışarıdan erişime açık sunucular için yapılması önerilen önlemler aşağıdaki gibidir:

  - Dış ağlara açık sunucuların sayısı mümkün olduğunca az tutulmalıdır.

[144] A.G.E., S.5 - 6

- Dış ağlara açık sunucular tercihen ayrı bir sanal yerel ağda (VLAN) veya ağ güvenlik duvarına bağlı ayrı bir ağ kesimi olan "yarı güvenli ağ" adı da verilen (Demilitarized Zone) olarak da adlandırılan YGA'da bulundurulmalıdır.
- Veritabanı servisi, tercihen web hizmeti veren sunucudan ayrı bir sunucu üzerinde hizmet vermelidir. Web hizmeti veren sunucu üzerinde veritabanı hizmeti de verildiğinde, veritabanı servislerinin çalıştığı ağ kapısına erişim engellenmeli ya da sadece gerekli noktalardan erişilebilecek şekilde kısıtlanmalıdır.

Kuruma özel, dış ağlara kapalı sunucular için yapılması önerilen ek önlemler ise aşağıdaki gibidir:

- Bu sunuculara erişim için gelişmiş kimlik doğrulama düzenekleri kullanılmalıdır.
- Bu sunuculara erişim izni sadece belirli ağ kesimlerine verilmelidir. Bu önlemin güvenliği arttırdığı aşikardır, yalnız saldırganların bu izin verilen ağ kesimlerinden bir kullanıcı makinesini ele geçirebileceği ve ele geçirilen makine üzerinden bu özel sunuculara erişmeye çalışabilecekleri de mümkün olduğundan diğer güvenlik önlemlerini almaya devam edilmelidir.

Sunucu Yerel Güvenliği**:** Web sunucularının bulunduğu makinenin işletim sisteminin ve üzerinde çalışan servis/sistemlerin güvenliği sağlanmalıdır. Web sunucusu üzerinde alınabilecek önlemler aşağıda özetlenmeye çalışılmıştır:

- İşletim sistemi ve üzerinde çalışan servis/yazılımların güvenlik güncellemelerinin düzenli olarak kontrol edilmesi ve gerekli yamalarının uygulanması,
- Sunucu üzerinde mümkün olduğunca az servisin/yazılımın çalıştırılması,
- Kurumda ağ tabanlı sistemler üzerinde erişim kısıtlamaları uygulanmakta olsa da, uzaktan erişim kısıtlamalarının sunucuda ayrı olarak tanımlanması,
- Web sunucu yazılımı ve veritabanları için gerekli güvenlik ayarlarının ve yapılanmalarının yapılması,
- İmkânsızlıklardan dolayı yapılabilecek hiç bir şey yoksa bile en azından sunucu tabanlı web uygulama güvenlik duvarı (örneğin, mod security) yazılımlarının sunucu üzerinde yerel olarak kurulması,
- Web sunucu üzerindeki günlüklerin düzenli olarak incelenmesidir.

Web Uygulama Güvenlik Duvarı / Ters Vekil: Bazı sistemlerde çeşitli nedenlerden dolayı web güvenliğinin istenen kriterlerde sağlanması mümkün olmayabilir. Bunun başlıca nedenleri:

- Sistem yöneticilerinin sunuculara ulaşmada yaşanan problemler,
- Sistem üzerinde çalışan yazılımların yeterli belgelemelerinin bulunmaması ve o yazılımı hazırlayan programcılara ulaşılamaması yüzünden gerekli yazılım düzeltmelerinin, geliştirme ve güncelleştirmelerin gerçekleştirilememesi,
- Donanımsal kısıtlama nedenlerinden dolayı gerekli güncelleme veya sürüm terfilerinin gerçekleştirilememesidir.

Web sunucularının güvenliğini sağlamak için, sunuculara gelen ağ trafiğini süzen ve saldırı girişimlerini mümkün olduğunca engelleyen sistemler entegre edilmelidir. Bu tür çözümlere Web Uygulama Güvenlik Duvarı (WUGD) denmektedir. Bu çözümler, daha çok ters vekil sunucu olarak uygulanmaktadır.

WUGD çözümlerinde, web sunucularına gidecek bütün ağ trafiği zorunlu olarak ters vekil sunucu üzerinden geçecek şekilde ayarlanmalıdır. WUGD; sadece web trafiği için değil, bütün iletişim kuralları için de güvenlik duvarı görevini yerine getirecek şekilde kullanılmalıdır. WUGD'un, süzme işlemini gerçekleştirmek için süzme yeteneği olacak şekilde yapılandırılması gerekecektir.

- Kurtarma

Muhtemel bir saldırı sonrasında uğranacak zararlar ve her bir zarar durumu için nelerin yapılması gerektiği tanımlanmalı ve mümkünse aralıklı olarak gerekli tatbikatlar gerçekleştirilmelidir. Saldırı sonrasında gerçekleştirilecek aşamaları aşağıdaki şekilde sınıflandırmak mümkündür:

- Sunucuya erişimin engellenmesi: Saldırganın, saldırısı sonucunda sunucuyu ele geçirmesi halinde, sunucu üzerinden yayın yapması veya başka saldırılara kalkışmasını engellemek için öncelikle sunucuya erişim engellenmelidir.
- Ayrıntılı inceleme: Saldırının boyutu ve bilgi sisteminde yarattığı zarar en kısa sürede saptanabilir olmalıdır. Sistemdeki hangi zayıflığın bu saldırıyı başarılı kıldığı belirlenebilmelidir.

Saldırının kuruma ait başka sistemlerde de etkili ve mümkün olup olmadığı incelenmelidir. Saldırganın saldırıdan sonra sistemde bir noktada herhangi bir arka kapı bırakmış olma ihtimali değerlendirilerek, sunucu, saldırıya ilişkin yeterli bilgi toplanması ve çekirdek düzeyinde sistemde bir değişiklik yapılıp yapılmadığının denetlenmesi için ayrıntılı incelemeye alınmalıdır.

- Saldırıların etkilerini temizleme: Sistemin tekrar etkinleştirilmeden öncelikle eski haline geri getirilmesi gerekebileceğinden, bu tür bir durum söz konusu olduğunda, yeni sistemin aynı saldırıya maruz kalmaması için, bu saldırıya neden olan zayıflık giderilmelidir. Mümkünse yeni bir sunucuda sistem ayağa kaldırılmalıdır.
- Sistemi yeniden çalıştırma: Verilerin yedeklerden alınarak yeni kurulan sisteme taşınması gerekebilecektir. Bunun için kurumun öncelikle düzenli bir sistem yedekleme politikasına sahip olması gerekmektedir.
- Kullanıcıların durumdan haberdar edilmesi: Kullanıcıların kişisel bilgilerinin saldırganların eline geçmesi durumunda, kullanıcıların gerekli önlemleri alması için kendilerine bir an önce gerekli bilgilendirme yapılmalıdır. Böylece kullanıcı, başka sistemlerde de aynı parolayı kullanıyorsa değiştirebilecek veya kredi kartı gibi mali değerleri için gerekli önlemleri alabilecektir.
- Saldırganın saptanması: Saldırganın saptanması için sunucu makinesi ve sistemdeki diğer aygıtlardaki kayıtlar ayrıntılı olarak incelenmelidir. Olayın teknik ve hukuki süreçleri bulunmaktadır. Türkiye'deki hukuki süreçler yeterince gelişmiş ve hızlı olmadığından verilerin delil niteliği taşıyacak ve bu özelliği bozulmayacak şekilde uzun süreli olarak saklanması sağlanmalıdır.[145]

- **Eşgüdüm Merkezi**

Web güvenliği konusunda sağlam bir altyapı ancak çok katmanlı güvenlik modelinin uygulanması ile mümkündür. Kurumsal web güvenliğinde tanımlanan modeller içerisindeki düzenekler, ancak birlikte etkileşimli çalıştırıldığında en iyi sonuca ulaşabilmektedir. Bu düzeneklerin eşgüdümü, merkezi bir sistem tarafından sağlanmalıdır.

Eşgüdüm merkezi ile hedeflenenler aşağıdaki gibidir:

- Modeller ve düzenekler arasındaki etkileşimi sağlamak,
- Sistemin başarımını ölçekleme ve en iyisi için çalışma,

[145] A.G.E., S.7

- Yanlış uyarıların azaltılması ve böylece gerçek uyarılar üzerinde yoğunlaşmanın sağlanması,
- Sistemdeki saldırıya açık noktaların saptanması ve aciliyet/tehdit durumuna göre hareket planının belirlenmesi,
- Saldırı saptama sistemi gibi etkin sistemlerin yapılanma ve ayarlarının dinamik olarak değiştirmek.[146]

3.3.3. Kamu Kurumlarında Web Hataları, Güvenlik Açıkları ve Araçları

- **Sayfa Boyutları ve Html Hataları**

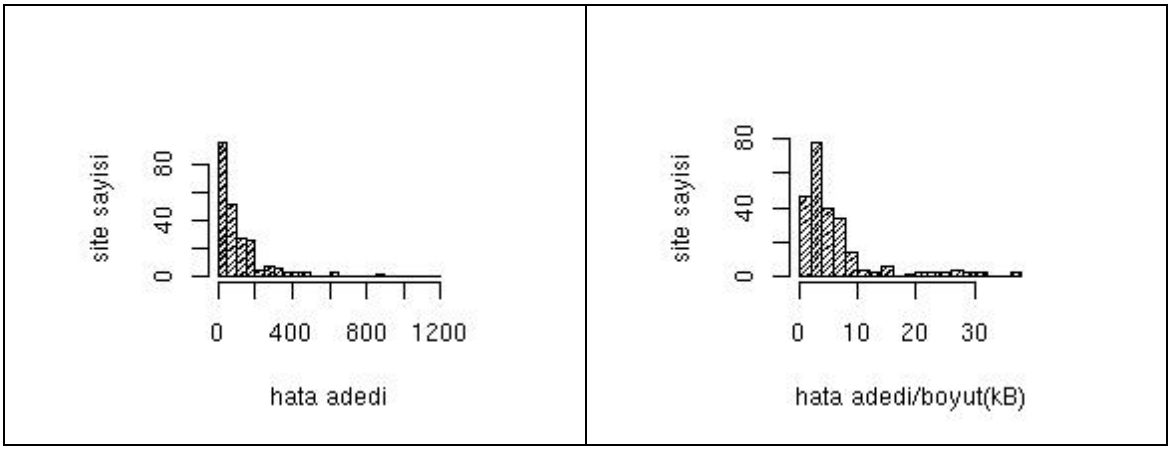
World Wide Web Konsorsiyum (W3C), sayfalardaki uyumluluk hatalarının tespitini sağlayan araçlar temin etmektedir. Bu araçlar kullanılarak Şekil 45'de sayıları belirtilen örneklemdeki sitelerin ana sayfalarındaki hata miktarı ölçülmüştür ve Şekil 46'da gösterilmiştir. Örneklemdeki sitelerde minimum 2, maksimum 1186 hata bulunmuştur; ortalaması ise 127 olarak tespit edilmiştir. Ayrıca hiçbir sitede en son W3C standartlarında öngörülen DOCTYPE etiketi bulunmamaktadır.[147]

```
Kamu kurumları (.gov.tr)           : 99
Üniversiteler (.edu.tr)            : 74
Askeri Birimler (.mil.tr)          :  4
Sivil Toplum Kuruluşları (.org.tr) : 37
Özel ticari kurumlar (.com.tr)     : 27
```

Şekil 45 : Örneklemdeki Sitelerin Sayısal Bilgileri

Kaynak: A.G.E., Par.1

[146] A.G.E., S.8
[147] Mehmet GENÇER, "**Türkiye İnternet Sitelerinde Standartlara Uyumluluk: Karşılaştırmalı Ölçümler ve Stratejik Açılımlar**", http://www.cs.bilgi.edu.tr/~mgencer/pub/inet06trpaper.pdf (Mart 2009)

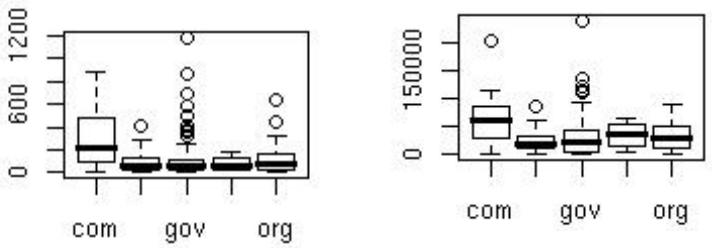


Şekil 46 : HTML Doğrulama Hataları - Hata Adedi Ve Kilobyte Başına Hata Adedinin Dağılımı

Kaynak: A.G.E., Par.1

Farklı gruplardaki site ana sayfalarının byte cinsinden boyutları ve sayfalardaki HTML hata adedi Şekil 47'de gösterilmektedir. Ana sayfa boyutu sayfanın görüntülenme hızını etkilediğinden dolayı aşırı büyük sayfalar erişilebilirlik açısından bir engel olarak görülmektedir.

Burada ticari siteler hem daha büyük ana sayfa boyutuna sahip hem de HTML hata yoğunluğu diğer gruplardan kayda değer şekilde yüksek olarak göze çarpmaktadır. Bununla birlikte her iki ölçümde de aşırı yüksek uçtaki değerlerin kamu siteleri arasında bulunması, e-Devlet sitelerinin oluşturulmasında genel bir yaklaşımın ve standardın bulunmadığına işaret ettiği değerlendirilebilmektedir.[148]



Sayfa Boyutu HTML Hataları

Şekil 47 : Sayfa Boyutu ve HTML Hataları

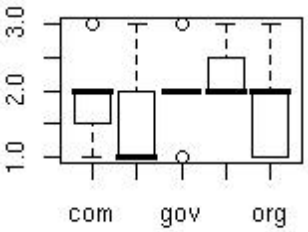
Kaynak: A.G.E., Par.2

[148] A.G.E., Par.2

- **Sunucu Tercihleri**

Grupların sunucu tercihleri Şekil 48'de belirtilmeye çalışılmıştır. Burada dikey eksende 0 Apache sunucusuna, 1 ise Microsoft-IIS sunucuya karşılık gelmektedir. Burada yalnızca üniversite sitelerinde ağırlıklı olarak açık kaynaklı olan Apache sunucusunun tercih edildiği görülmektedir. Daha da ilginç olan ise ticari ve sivil toplum sitelerinin bir kısmında Apache kullanılırken kamu kurumlarında hemen hemen hiç kullanılmıyor olmasıdır. Bu da Türkiye 'Internet sitelerinde açık kaynak sunucu tercih edilme oranının Dünya ortalamasının neredeyse yarısı düzeyinde olduğunu göstermektedir.[149]

	Adet	Oran
Microsoft-IIS :	138	58%
Apache :	90	37%
Diğer :	13	5%



0:Apache, 1:MS-IIS, 2:Diğer

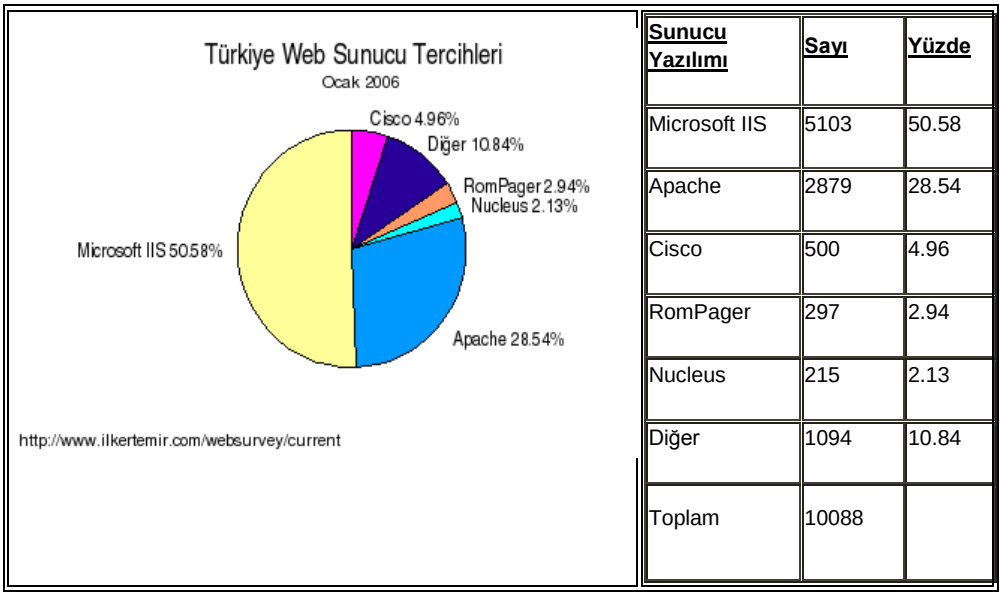
Şekil 48 : Sunucu Tercihleri

Kaynak: A.G.E., Par.2

"*Bu tercih dağılımı Dünya genelinden oldukça farklı görünmektedir. Dünya istatistikleri açık kaynak Apache sunucu kullanım oranını %62 olarak göstermektedir.*"[150]

Bu konuda Türkiye'de yer alan toplam 10,088 IP adresi üzerinden yapılan diğer bir araştırmaya göre ise, Apache kullanım oranının ise diğer test sonuçlarına göre daha düşük olduğu Şekil 49'da da görülebilmektedir.

[149] A.G.E., Par.2
[150] A.G.E., Par.2



Sunucu Yazılımı	Sayı	Yüzde
Microsoft IIS	5103	50.58
Apache	2879	28.54
Cisco	500	4.96
RomPager	297	2.94
Nucleus	215	2.13
Diğer	1094	10.84
Toplam	10088	

Şekil 49 : Türkiye Web Sunucusu Tercihleri

Kaynak: İlker TEMİR, "Türkiye Internetinde Tercih Edilen Web Sunucuları", http://www.ilkertemir.com/websurvey/current/ (Mart 2010)

Zone-h verilerine bakıldığında en çok tahrifata uğratılan web sunucusunun ise Tablo 18'de de görüldüğü gibi "Apache" isimli web sunucusu olduğu görülmektedir.

Tablo 18
Web Sunucu Türüne ve Yıllara Göre Tahrifata Uğrama İstatistikleri

Web Sunucu Türü	2008	2009	2010
Apache	390.141	486.294	319.439
IIS/6.0	126.403	180.926	113.935
IIS/5.0	12.551	66.304	23.664
Unknown	4.974	8.805	16.741
Zeus	1.059	506	1.972
NOYB	0	1.308	1.920
IIS/4.0	5.846	3.952	1.149
nginx	3.465	870	729
IIS/5.1	540	412	308
Rapidsite	158	110	244
SonataServer	4	557	178
A-NETEK RobustWeb	4	4	92
Zope	106	67	80
LiteSpeed	3	150	65
IdeaWebServer	50	191	60

Web Sunucu Türü	2008	2009	2010
E-Neverland DataPalm	15	16	41
lighttpd	25	33	37
DinaHTTPd Server	52	89	36
Boa	6	59	26
Sil ver Stream Server	36	40	20
SAMBAR	0	18	17
thttpd	8	29	15
SunONE Web Server	165	670	12
ConcentricHost-Ashurbanipal	18	12	11
Lasso	18	26	11
Cougar	1	21	10
NetWare-Enterprise-Web-Server	5	3	8
Sun Java Sys tem Web Server 6.1	0	6	8
GWS	2	4	8
DataPalm	0	7	7
Abyss	0	0	5
OBEC-Web-Serv	0	13	5
InfomexWebServer	2	14	4
tigershark	54	9	4
4D_WebSTAR_S	34	169	4
IBM HTTP SERVER	7	17	4
Jetty	0	0	4
Netscape-Enterprise	37	21	4
OmniHTTPd	7	3	4
AOL server	28	15	3
IIS/30	3	4	3
exteNd Appli ca tion Server	3	2	2
RaidenHTTPD	5	5	2
Resin	9	25	2
Replica	1	0	2
RRRPHP/942	1	0	2
CoffeeMaker	0	0	1
Hix Web server	0	0	1
KFWebserver	5	5	1
NetCache	5	8	1
Ora cle AS	0	3	1

Kaynak: "Tahrifat İstatistikleri", Par.1

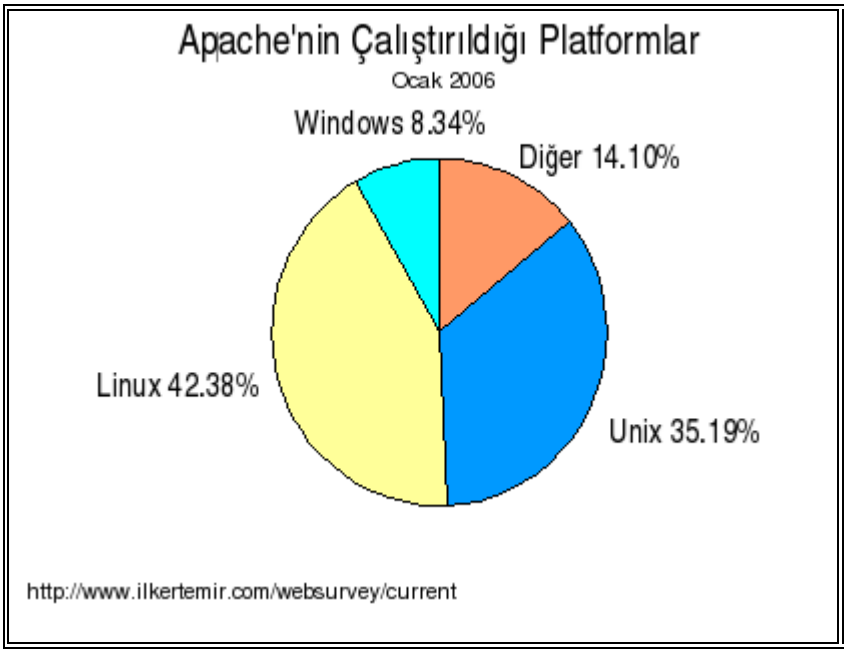
Bahse konu Web sunucularının çalıştırıldığı işletim sistemlerinin türleri ile ilgili olarak yapılan diğer bir değerlendirmede ise en çok tahrifata uğrayan işletim sisteminin Tablo 19'dan da görüldüğü gibi "Linux" işletim sistemi olduğu tespit edilmiştir.

Tablo 19
İşletim Sistemi Türü ve Yıllara Göre Tahrifata Uğrama İstatistikleri

İşletim Sistemi	2008	2009	2010
Linux	352.468	378.744	256.648
Win dows 2003	117.978	127.128	81.785
Win dows 2000	21.929	12.529	2.805
FreeBSD	13.418	10.050	5.503
Unknown	4.642	3.933	1.815
Solaris 9/10	3.002	7.699	364
SolarisSunOS	1.629	16	10
MacOSX	893	510	384
Win NT9x	440	225	132
Win 2008	364	2.977	3.165
Win XP	329	270	72
HP-UX	216	85	32
NetBSDOpenBSD	69	99	39
Solaris 8	35	41	5
BSDOS	10	14	2
AS/400	6	1	1
Com paq Tru64	6	16	2
NovellNetware	5	5	0
Unix	3	29	43
IRIX	3	12	5
OpenVMS	3	1	0
AIX	3	1	0
MacOS	3	0	2
OpenBSD	1	0	0
Win Vista	1	1	0
OpenServer	1	0	0
Win .NET	1	1	0
OS2	1	0	5
Dig i tal Unix	0	3	0

Kaynak: A.G.E., Par.1

Açık kaynak kodlu ve ücretsiz olan "Apache" web sunucusunun çoğunlukla lisansız ve ücretsiz olan işletim sistemleri üzerinde çalıştırılabilmesine rağmen, ücretli ve lisanslı işletim sistemleri üzerinde de çalıştırıldığı tespit edilmiştir. İnceleme sonuçları Şekil 50'de paylaşılmıştır.



Platform	Sayı	Yüzde
Linux	1220	42.38
Unix [1]	1013	35.19
Windows	240	8.34
Diğer [2]	406	14.10
Toplam	2879	

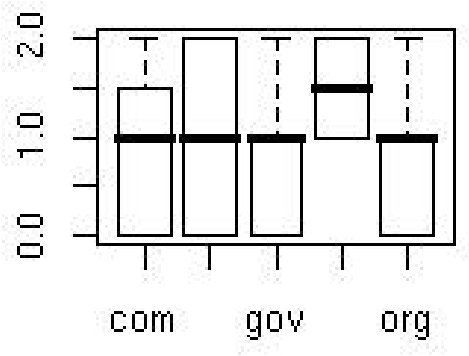
Şekil 50 : Apache'nin Çalıştırıldığı Platformlar

Kaynak: "Türkiye Internetinde Tercih Edilen Web Sunucuları", Par.1

- **Karakter Kodlaması**

Örneklemdeki sitelerde en yaygın olarak görülen hatanın uluslararası standartlarda yeri olmayan ve ticari bir şirkete Özgü windows-1254 tipi karakter kodlamasının kullanılması karşılaşılan diğer bir hatadır. Oysa Türkçe içerik için tercih edilen kodlamalar ISO-8859-9 ya da UTF-8 olarak belirlenmiştir. Buna ilaveten pek çok site karakter kodlamasını belirten HTML etiketlerinden birden fazla içermekte ve her birinde başka karakter kodlaması belirtilmektedir, ki bu da karakter kodlaması meselesinin web tasarımcıları tarafından anlaşılamadığını göstermektedir. Şekil 51'de de görüldüğü gibi bu sitelerin %54'ünde standartlarda olmayan karakter kodlaması kullanılmış, %32'si ise birden fazla karakter kodlaması etiketi içermektedir. Ayrıca 26 sitede karakter kodlaması hiç belirtilmemiştir. Sadece 6 sitede UTF-8 kodlaması tercih edilmiştir. Ne yazık ki ölçümler bu

konuda oldukça yüksek sayıda hata göstermektedir. Kamu siteleri ve sivil kurumların siteleri göreceli olarak daha az probleme sahip görünmektedirler. Öte yandan az sayıdaki askeri sitelerin en problemli grubu oluşturduğu tespit edilmiştir. Bu gruptaki veriler karakter kodlamasının, ele alınan ölçütler içinde, standartlara uyumluluk konusunda en az bilinen konu olduğuna işaret etmektedir. Oysa UTF-8 kodlaması Internet uygulamalarının yerel dillere uygunluğunun sağlanması konusunda en çok gelecek vadeden standart olarak kabul edilerek, bu konuda sürmekte olan standardizasyon çalışmaları içerisinde kritik ve üzerine çok çalışılan bir konudur.[151]

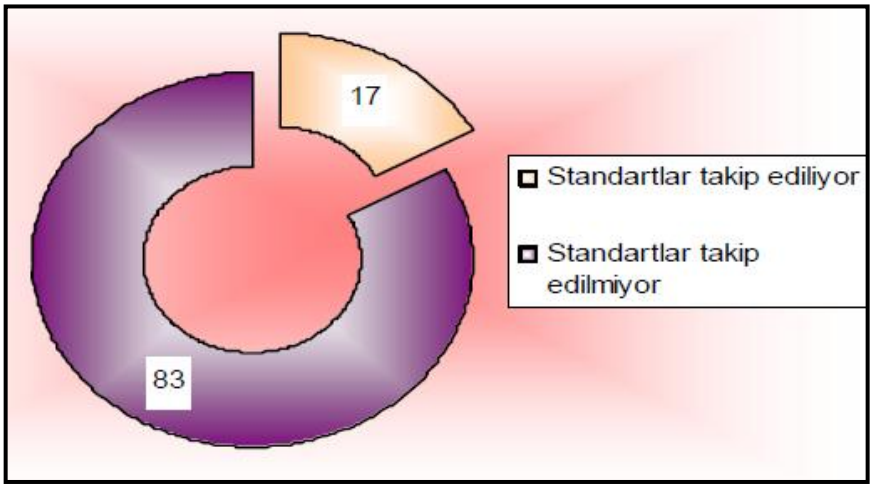


Şekil 51 : Karakter Kodlaması Hataları

Kaynak: A.G.E., Par.2

[151] "**Türkiye İnternet Sitelerinde Standartlara Uyumluluk: Karşılaştırmalı Ölçümler ve Stratejik Açılımlar**", Par. 2

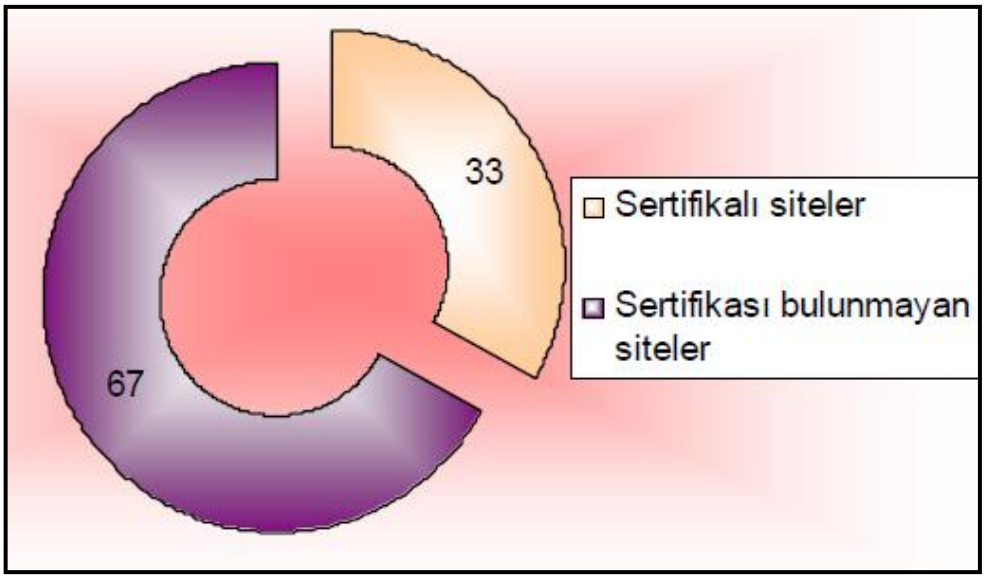
Bu konuda yapılan diğer bir araştırma sonucunda elde edilen ve Şekil 52'de sunulan sonuçlara göre, kamu internet sitelerinde diğer uluslar arası standartlara da uyulmadığı tespit edilmiştir.



Şekil 52 : Uluslar Arası Standartlar Takip Ediliyor mu? (%)

Kaynak: "E-Devlete Geçişte Kamu Kurumları İnternet Siteleri Performans Denetimi Raporu", S.86

Kamu internet sitelerinin kişisel veri transferi yapan kısımlarında güvenliği arttırmak ve güvenilirliliği sağlamak için güvenlik sertifikası kullananların sayısının ise yüksek olmadığı Şekil 53'de görülmektedir.



Şekil 53 : Kamu İnternet Sitelerinin SSL Sertifikası Sahipliği (%)

Kaynak: A.G.E., S.92

Kısıtlı bir örneklem üzerinde de olsa bu çalışmadaki sonuçlar, kamu sitelerinin hem uluslararası standartlara uygunluk yönünden ciddi eksiklikleri olduğunu, hem de kamuda ortak stratejilerin gelişmediğini göstermiştir. Bu sonuçlar ayrıca, ticari İnternet sitelerinin göreceli olarak daha yüksek miktarlarda HTML içeriği hataları içerdiği ortaya çıkartmıştır. Ayrıca Türkçe içeriğin doğru görüntülenmesi açısından önem taşıyan karakter kodlamasının web tasarımı süreçlerinde kurum ve kurum web sitesi hazırlayıcıları tarafından hemen hemen hiç anlaşılmadığı ve bu konudaki geçerli uygulamaların bilinmediğini ortaya çıkartmıştır.

Sunucu tercihleri konusundaki veriler, ister kamu, ister özel olsun örneklemdeki tüm gruplarda üretim şekli itibariyle açık kaynak yazılımların ticari yazılımlara göre daha yüksek standart uyumluluğu gösterdiğinin bilinmesine ve tedarikçiye bağımlılık riski taşımadığından süreklilik gerektiren kamu hizmetlerinde kullanılmaya çok daha uygun olmalarına rağmen, ticari yazılımların hem web içeriğinin tasarımı hem de görüntülenmesi konusunda hegamonik bir ağırlığı olduğunu göstermektedir.

Bu sebeplerden dolayı, e-Devlet sürecinde kamuda gözlemlenen stratejik eksikliklerinin çok daha kapsamlı bir vizyon eksikliğinden kaynaklandığı düşünülebilir. Standartlara uygunluk ve yazılım tercihleri konusunda kamunun aldığı tavır kurumsal ortamdaki diğer aktörlerin tavrını doğrudan etkileyebilecektir. Örneğin e-Devlet ihalelerinde yaygın olarak kullanılan web tarayıcılarıyla uyumluluk, W3C standartları, karakter kodlaması kriterleri konusunda şartlar getirildiğinde özel sektör web sitelerindeki ihalelerin de bu kriterleri taklit etmesi beklenen bir hareket tarzıdır. Ek olarak açık kaynak kodlu yazılımların kullanılması tedarikçiye bağımlılık riski taşımadığından süreklilik gerektiren kamu hizmetlerinde kullanılmaya çok daha uygundurlar.[152]

[152] "Türkiye İnternet Sitelerinde Standartlara Uyumluluk: Karşılaştırmalı Ölçümler ve Stratejik Açılımlar", Par. 2

4. TÜRKİYEDEKİ KAMU KURUMLARINA ve ÖZEL ŞİRKETLERE AİT WEB SİTELERİNİN WEB GÜVENLİĞİ AÇISINDAN DEĞERLENDİRİLMESİ

4.1. Araştırma Amacı

Bu araştırmanın amaçları aşağıda belirtilmeye çalışılmıştır.

- Çalışmayan kişilerin, internete olan ilgileri ve internette yer alan kamu internet siteleri hakkındaki bilgi ve güvenlerinin incelenmesi,
- Çalışan kişilerin, yine aynı konulardaki düşünceleri ve eğer varsa çalıştıkları kurumların web sitelerinin yayınlanması, hazırlanması ve güvenliklerinin sağlanması ile ilgili alınan tedbir, iş ve hizmetlerin değerlendirilmesi,
- Yayınlanan siteler için alınan güvenlik önlemlerinin yeterli olup olmadıklarının yapılacak "kara kutu" güvenlik taramasından geçirilerek değerlendirilmesidir.

Sonuç olarak, kamu kurumları ve özel şirket web sayfalarının web güvenliklerinin sağlanması için alınan önlem ve tedbirlerin arasındaki fark ve bu farkların nelere neden olduğunun tespit edilmesidir.

4.2. Araştırma Metodolojisi

Araştırma niceliksel araştırma metodoloji kullanılarak hazırlanmıştır.

Bu araştırma için öncelikle veri toplanmasına çalışılmıştır. Bu amaçla 34 sorudan meydana gelen bir anket hazırlanmış ve bu anket http://anket.marmara.edu.tr adresinde yer alan online anket sistemine girilerek herkese yetki verilmiş ve çeşitli yollar ile internette anket linkleri dağıtılarak internet kullanıcılarının anketi cevaplamaları sağlanmıştır. Anket toplam 72 kişi tarafından cevaplandırılmıştır.

Bu kapsamda öncelikle katılımcıların yaş aralığı, cinsiyet, eğitim seviyesi, iş durumları gibi demografik veriler toplanmış ve birimlerinde bilişim hizmetlerinin sunulması ile ilgilenme durumları hakkında bilgiler istenmiştir.

Ek olarak eğer kurumlarındaki bilişim hizmetlerinin verilmesi ile ilgileniyorlarsa ve kurumsal web siteleri varsa, bahse konu bu web

sitelerinin güvenliğinin sağlanması için hangi önlemleri aldıkları ya da almaya çalıştıkları, bunun için ayırmaya çalıştıkları ödenek miktarları öğrenilmeye çalışılmıştır.

Anketteki diğer sorular ile katılımcıların kamu kurumlarına ait web siteleri ile özel şirket web sitelerini hakkındaki tasarımsal ve içeriksel düşünceleri anlaşılmaya çalışılmıştır. Bunlara ek olarak katılımcıların bahse konu sitelerin güncellenme ve düzenleme hakkında fikirleri de sorulmuştur.

Ardından anket soruları ile katılımcıların, bazı kamu kurumlarına ait web siteleri ve birkaç web sitesi türlerinin güvenlik seviyeleri hakkında görüşleri istenmiş, kamu ve özel web sitelerinden kaynaklı uğradıkları maddi ya da manevi zararlar hakkında bilgiler talep edilmiş, kamu kurumu ve özel şirket web sitelerine güvenleri hakkındaki düşünceleri öğrenilmeye çalışılmıştır.

Verilen cevaplar incelenmiş ve kurum sitesi adresi verilen cevaplardan, kurum sitelerinin listesi çıkartılarak bu web siteler kara kutu tarama yöntemi kullanılarak güvenlik taramasından geçirilmiştir. Toplamda 17 adet özel şirketlere ait web sitesi, 15 adet de kamu kurumlarına ait web sitesi ve 3 adet özelleştirilmiş şirketlere ait web sitesi güvenlik taramasından geçirilmiştir. Güvenlik taraması sonucunda bulunan zafiyetler kritik, yüksek, orta, düşük ve bilgi olmak üzere 5 farklı kategoride gruplandırılmıştır.

Elde edilen verilerden yeni veriler elde edilerek toplam zafiyet değerleri ve ortalamalar elde edilmiştir.

Verilen tüm cevaplar ve güvenlik taraması sonucunda elde edilen veriler SPSS uygulamasına teker teker işlenmiştir. SPSS den elde edilen veriler birkaç grafiksel gösterim için Microsoft Excel uygulamasına da işlenmiştir.

Bu veriler ışığında katılımcıların kamu ve özel şirket web sitelerine olan ilgi ve güvenleri, bu kurumların web sitelerinin yayınlanması,

hazırlanması, güvenlikleri için alınan önlemler arasındaki farklar ve bu farkların yeterli olup olmadıkları ortaya çıkarılmaya çalışılmıştır.

4.3. Araştırmanın Bulguları

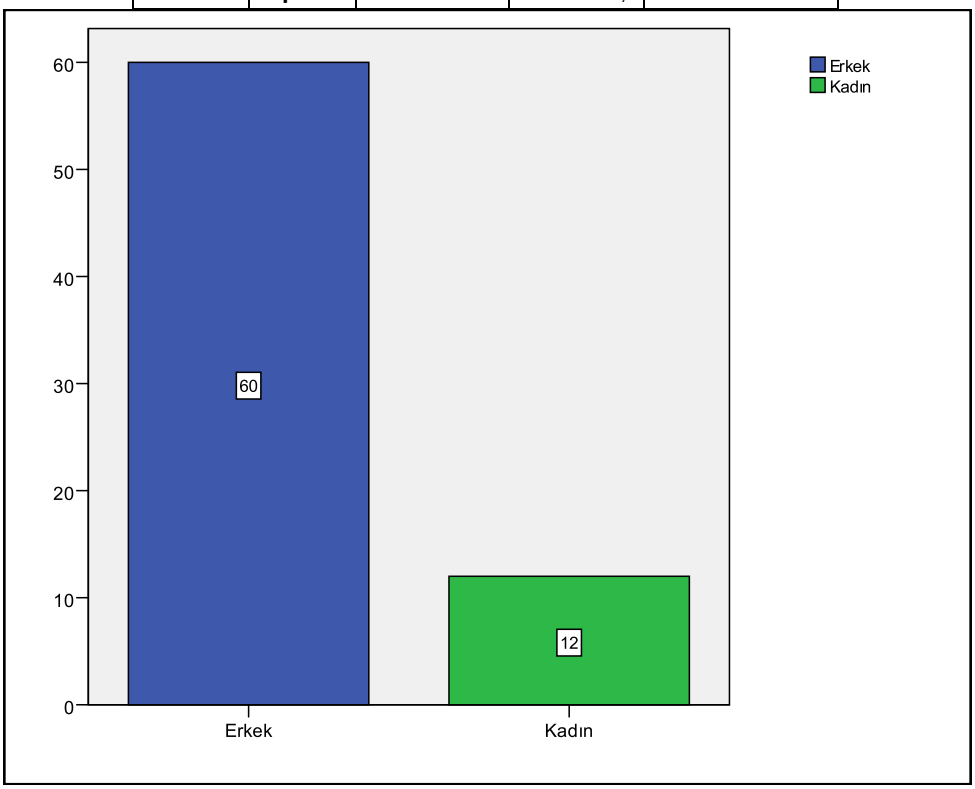
4.3.1. Tanımsal Bulgular

Ankete katılan katılımcılar ile ilgili tanımsal bulgular aşağıda belirtilmeye çalışılmıştır.

4.3.1.1. Cinsiyet Kriterine Göre Dağılım

Tablo 20
Cinsiyet Kriterine Göre Dağılım

		Frekans	Yüzde	Kümülatif Yüzde
Cinsiyet	Erkek	60	83,3	83,3
	Kadın	12	16,7	100,0
	Toplam	72	100,0	



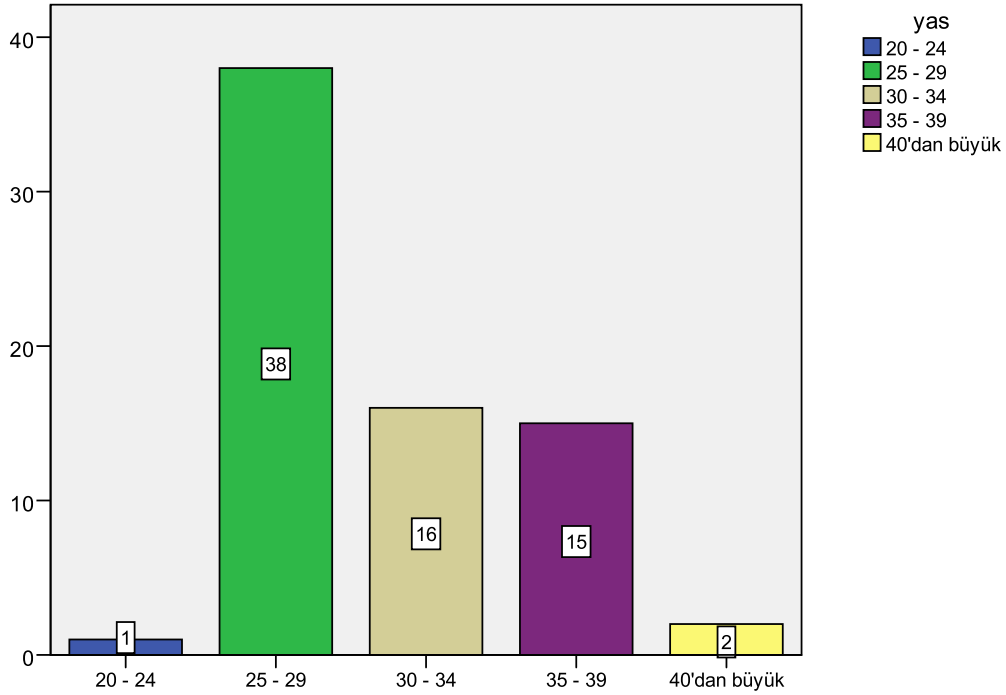
Şekil 54 : Cinsiyet Kriterine Göre Dağılım Tablosu – Grafiksel Gösterimi

Ankete katılanların cinsiyetlerine göre dağılımlarına bakıldığında 72 kişiden, 60'ının (%83,3) erkek, 12'sinin (%16,7) ise kadın olduğu görülmektedir.sonuçlara göre erkeklerin kadınlara oranla bilişim sektörü ile daha ilgili olduğu anlaşılmaktadır.

4.3.1.2. Yaş Kriterine Göre Dağılım

Tablo 21
Yaş Kriterine Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	20 - 24	1	1,4	1,4
	25 - 29	38	52,8	54,2
	30 - 34	16	22,2	76,4
	35 - 39	15	20,8	97,2
	40'dan büyük	2	2,8	100,0
	Toplam	72	100,0	



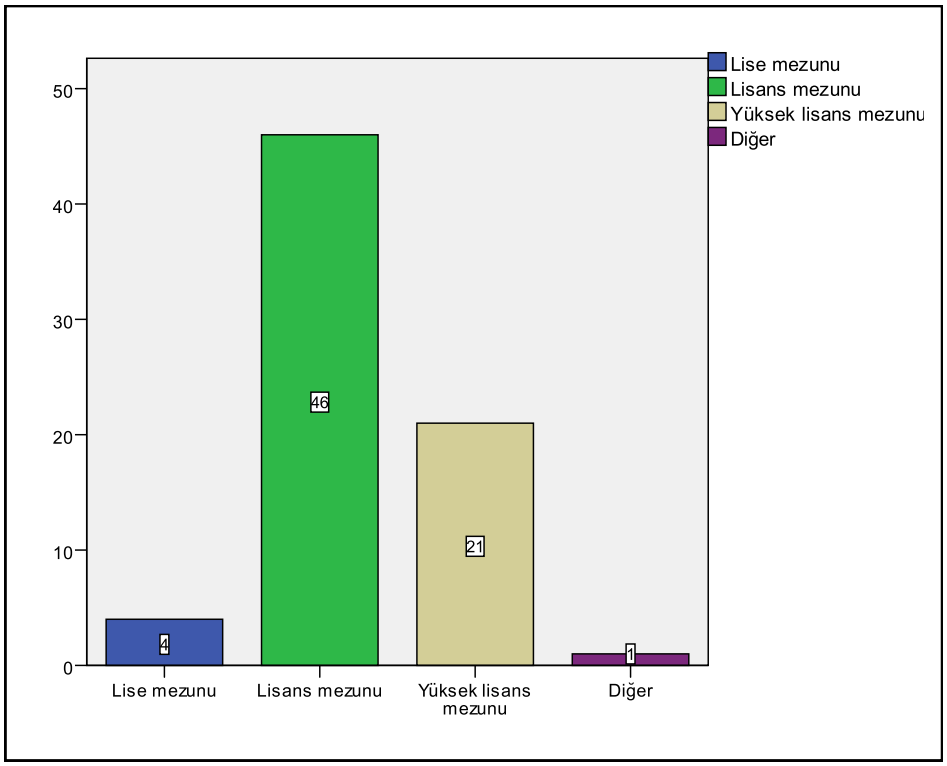
Şekil 55 : Yaş Kriterine Göre Dağılım Tablosu – Grafiksel Gösterim

Bilişim ile ilgilenen anket katılımcılarının verdikleri cevaplara göre, ankete katılanların 1'inin (%1,4) 20 – 24 yaş arasında olduğu, 38'inin (%52,8) 25 – 29 yaş arasında olduğu, 16'sının (%22,2) 30 – 34 yaş arasında olduğu, 15'inin (%20,8) 35 – 39 yaş arasında olduğu 2'sinin ise (%2,8) 40 yaşından daha büyük olduğu belirlenmiştir. Bu verilere göre bilişim ile ilgilenen kişilerin büyük oranda 25 – 29 yaş arasında olduğu görülmüştür.

4.3.1.3. Öğrenim Durumlarına Göre Dağılım

Tablo 22
Öğrenim Durumlarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Lise mezunu	4	5,6	5,6
	Lisans mezunu	46	63,9	69,4
	Yüksek lisans mezunu	21	29,2	98,6
	Diğer	1	1,4	100,0
	Toplam	72	100,0	



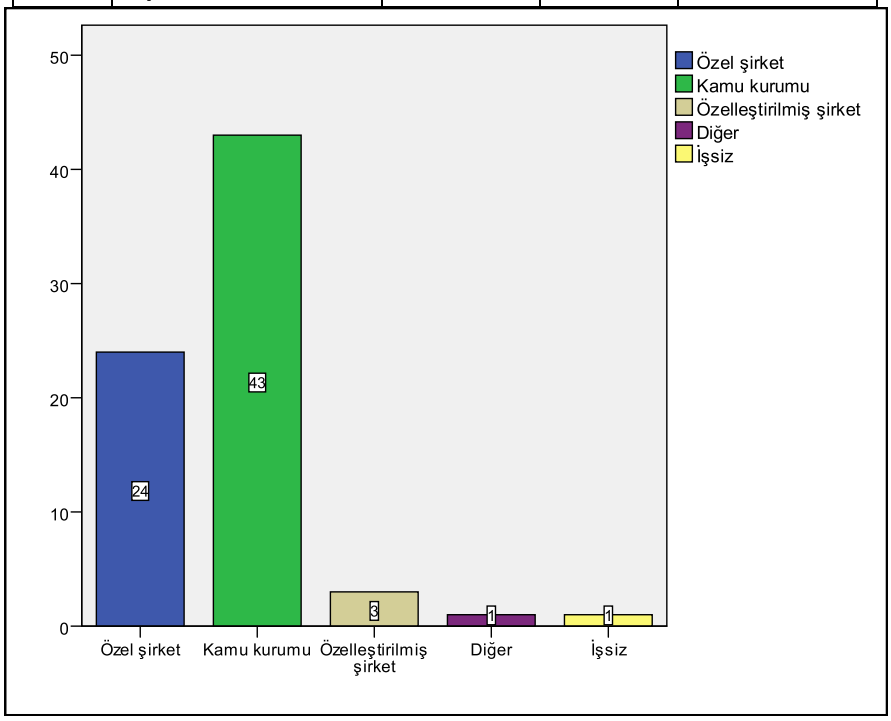
Şekil 56 : Öğrenim Durumuna Göre Dağılım Tablosu – Grafiksel Gösterim

Bilişim ile ilgilenen anket katılımcılarının verdikleri cevaplara göre, ankete katılanların 4'ünün (% 5,6) lise mezunu olduğu, 46'sının (%63,9) lisans mezunu olduğu, 21'inin (%29,2) yüksek lisans mezunu olduğu tespit edilmiştir. Görülmektedir ki, bilişim ile ilgilenen kişilerin çoğunlukla en az lisans mezunu olduğu görülmektedir.

4.3.1.4. Çalışma ve Çalışılan Kurum Türü Durumlarına Göre Dağılım

Tablo 23
Çalışma Durumlarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Özel şirket	24	33,3	33,3
	Kamu kurumu	43	59,7	93,1
	Özelleştirilmiş şirket	3	4,2	97,2
	Diğer	1	1,4	98,6
	İşsiz	1	1,4	100,0
	Toplam	72	100,0	



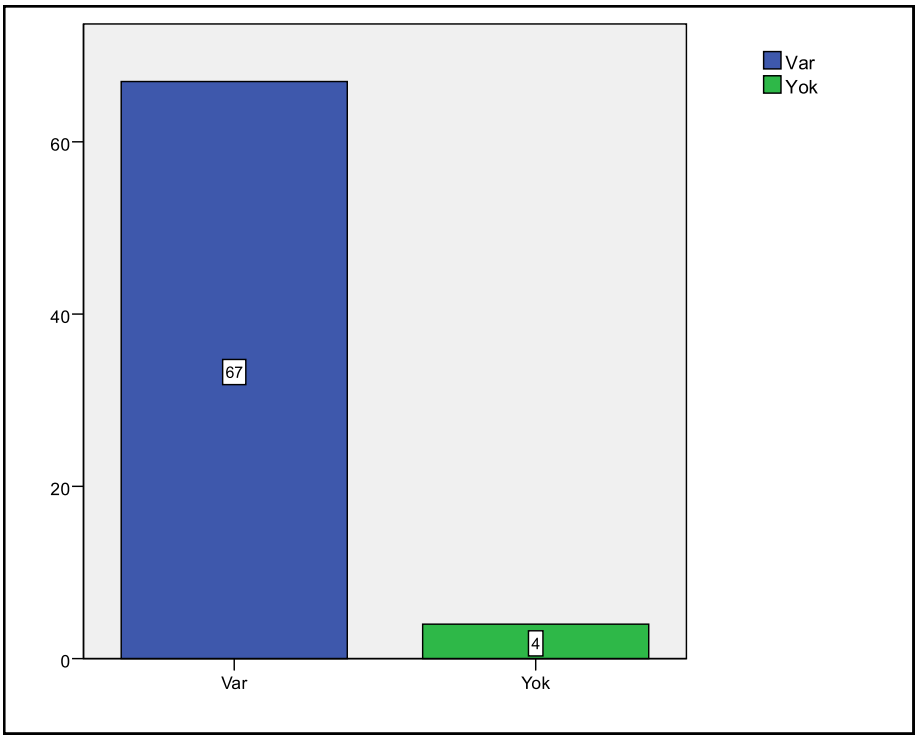
Şekil 57 : Çalışma Durumlarına Göre Dağılım Tablosu– Grafiksel Gösterim

Bilişim ile ilgilenen anket katılımcılarının verdikleri cevaplara göre, ankete katılanların 24'ünün (%33,3) özel şirketlerde çalıştığı, 43'ünün (%59,7) kamu kurumlarında çalıştığı, 3'ünün (%4,2) özelleştirilmiş kamu şirketlerinde çalıştığı, 1'inin (%1,4) diğer iş sektöründe çalıştığı, 1'inin (%1,4) ise işsiz olduğu tespit edilmiştir. Görülmektedir ki, bilişim ile ilgilenen kişi ya da kişiler büyük ölçüde çalışmaktadırlar ve işsizlik gibi bir sorunları bulunmamaktadır.

4.3.1.5. Kurumların Web Sayfası Olma Durumlarına Göre Dağılım

Tablo 24
Kurumların Web Sayfası Olma Durumlarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Var	67	94,4	94,4
	Yok	4	5,6	100,0
	Toplam	71	100,0	



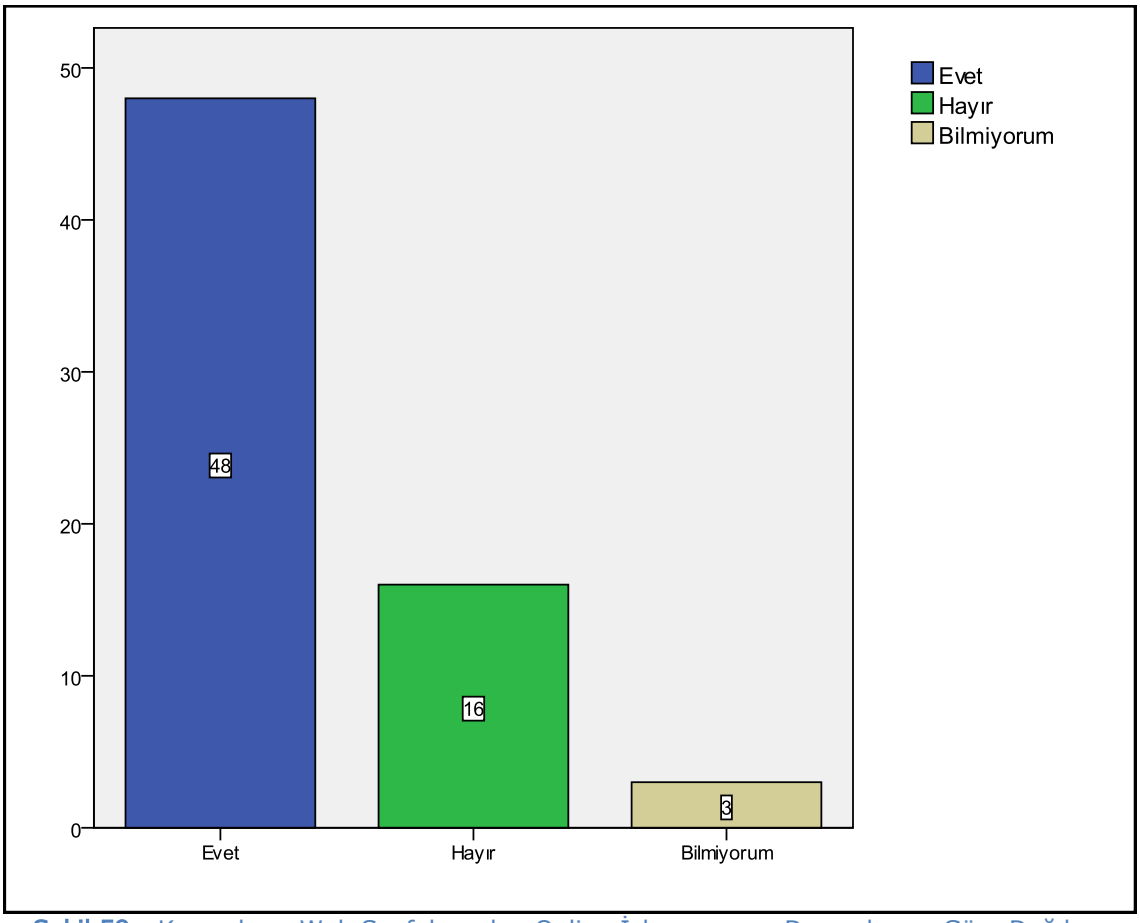
Şekil 58 : Kurumların Web Sayfası Olma Durumlarına Göre Dağılım Tablosu – Grafiksel Gösterim

Bilişim ile ilgilenen anket katılımcılarının verdikleri cevaplara göre, ankete katılanların çalıştıkları kurumların 67'sinin (%94,4) web sitesine sahip olduğu, 4'ünün (%5,6) ise web sitesi olmadığı tespit edilmiştir. Görülmektedir ki, kurumların çoğunun web sitesi mevcuttur.

4.3.1.6. Kurumların Web Sayfalarından Online İşlem Sunma Durumlarına Göre Dağılım

Tablo 25
Kurumların Web Sayfalarından Online İşlem sunma Durumlarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Evet	48	71,6	71,6
	Hayır	16	23,9	95,5
	Bilmiyorum	3	4,5	100,0
	Toplam	67	100,0	



Şekil 59 : Kurumların Web Sayfalarından Online İşlem sunma Durumlarına Göre Dağılım Tablosu – Grafiksel Gösterim

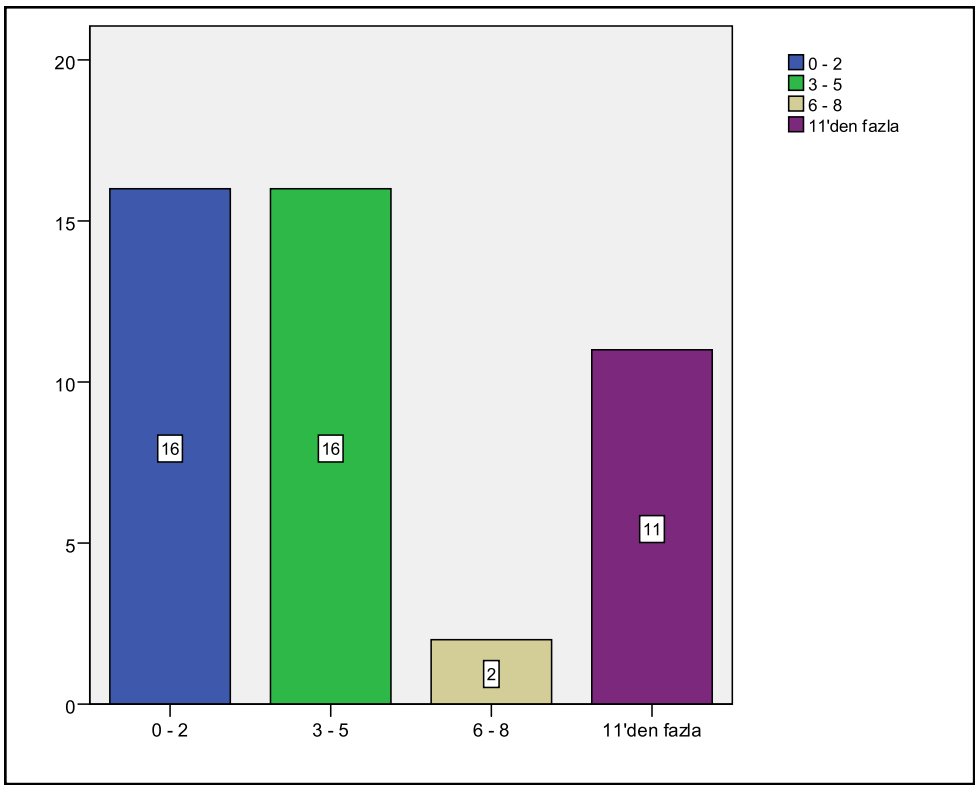
Bilişim ile ilgilenen anket katılımcılarının verdikleri cevaplara göre, ankete katılanların çalıştıkları kurumlardan web sitesi olanların, bu web siteleri üzerinden online işlem verme oranlarına bakıldığında, bu kurum sitelerinden 48'inin (%71,6) online işlem sunduğu, 16'sının (%23,9) sunmadığı, 3'ünün (%) ise o sitede çalışan kişi tarafından bilinmediği tespit

edilmiştir. Bu da göstermektedir ki, sitelerin hemen hemen dörtte üçü üzerinden online işlem sunulmaktadır.

4.3.1.7. Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel Sayılarına Göre Dağılım

Tablo 26
Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel Sayılarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	0 - 2	16	35,6	35,6
	3 - 5	16	35,6	71,1
	6 - 8	2	4,4	75,6
	11'den fazla	11	24,4	100,0
	Toplam	45	100,0	



Şekil 60 : Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personel Sayılarına Göre Dağılım Tablosu – Grafiksel Gösterim

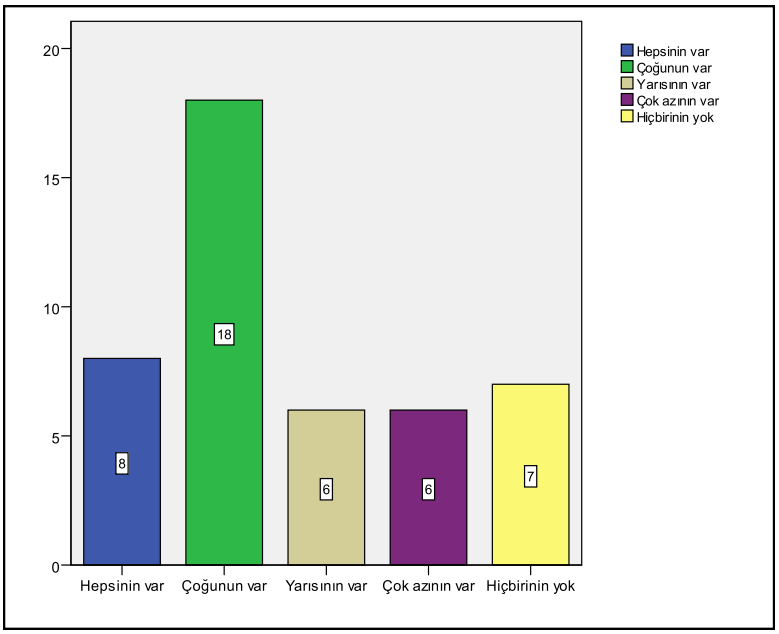
Web Sayfası olan kurumların web sitesini hazırlayan personel sayılarına bakıldığında, web sayfası olan kurumların 16'sının (%35,6) web

sitesini 0-2 kişi, diğer 16'sının (%35,6) 3-5 kişi, 2'sinin (%4,4) kişi, 11'inin ise (%24,4) 11'den fazla kişi tarafından hazırlandığı tespit edilmiştir. Görülmektedir ki, kurum web siteleri % 71,2 oranında 0 ile 5 kişi arasında gruplar tarafından hazırlanmaktadırlar.

4.3.1.8. Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım

Tablo 27
Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Hepsinin var	8	17,8	17,8
	Çoğunun var	18	40,0	57,8
	Yarısının var	6	13,3	71,1
	Çok azının var	6	13,3	84,4
	Hiçbirinin yok	7	15,6	100,0
	Toplam	45	100,0	



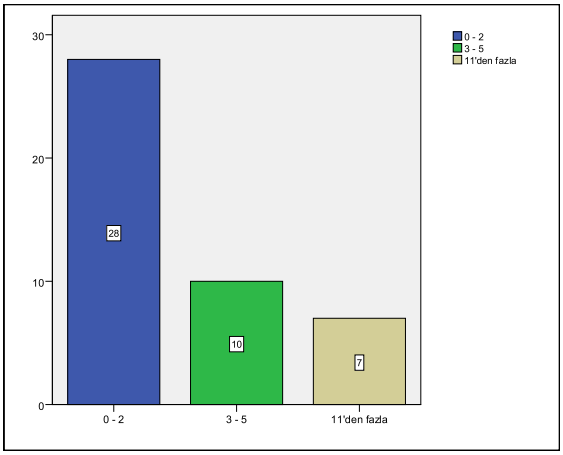
Şekil 61 : Web Sayfası Olan Kurumların Web Sayfalarını Hazırlayan Personelin Sertifikasyon Durumuna Göre Dağılım Tablosu – Grafiksel Gösterim

Kurumsal web sitelerini hazırlayanların yeterlilik yani sertifikasyon durumlarına bakıldığında, web sitelerinin hazırlayanların tamamının hiçbir sertifikasyona sahip olmayan kurum web sitelerinin sayısının 7 (%15,6), web sayfasını hazırlayanların çok azının sertifika sahibi olan kurum web sitelerinin sayısının 6 (%13,3), web sitesini hazırlayanların yarısının sertifika sahibi olduğu kurum web sitelerinin sayısının da 6 (%13,3), web sitesini hazırlayanların çoğunun sertifika sahibi olduğu kurum web sitesi sayısının ise 18 (%40), tamamen sertifika sahibi personellerce hazırlanan kurum web sitesi sayısının ise 8 (%17,8) olduğu tespit edilmiştir. Görülmektedir ki, kurum web siteleri genellikle sertifikasyon sahibi kişi ya da kişilerce hazırlanmaktadırlar.

4.3.1.9. Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği ile İlgilenen Personel Sayılarına Göre Dağılım

Tablo 28
Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personel Sayılarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	0 - 2	28	62,2	62,2
	3 - 5	10	22,2	84,4
	11'den fazla	7	15,6	100,0
	Toplam	45	100,0	



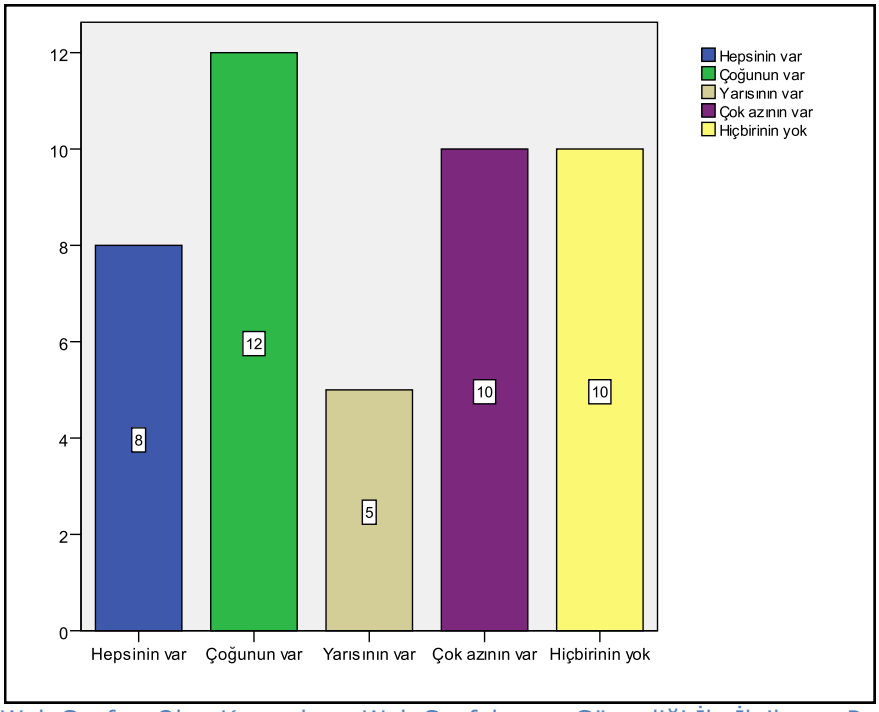
Şekil 62 : Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personel Sayılarına Göre Dağılım Tablosu – Grafiksel Gösterim

Kurumsal web siteleri olan kurumların web sitelerinin güvenliği ile ilgilenen personel sayıları incelendiğinde, web sitesinin güvenliği ile ilgilenen personel sayısı 0-2 arasında olan kurum web sitesi sayısının 28 (% 62,22), web güvenliği ile ilgilenen personel sayısı 3 - 5 arasında olan web sitesi sayısının 10 (%22,2), web sitesi olmadığı, 11 den fazla güvenlik personeli olan web sitesi sayısının 7 (%15,6) olduğu, web güvenliği ile ilgilenen personel sayısı 6 ile 11 arasında olan web sitesinin ise olmadığı tespit edilmiştir. Görülmektedir ki, web sitelerinin güvenliği genellikle 0-2 kişi arasındaki gruplar tarafından sağlanmakta ya da sağlanmaya çalışılmaktadır.

4.3.1.10. Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği ile İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım

Tablo 29
Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım

		Frekans	Yüzde	Toplam Yüzde
	Hepsinin var	8	17,8	17,8
	Çoğunun var	12	26,7	44,4
	Yarısının var	5	11,1	55,6
	Çok azının var	10	22,2	77,8
	Hiçbirinin yok	10	22,2	100,0
	Total	45	100,0	

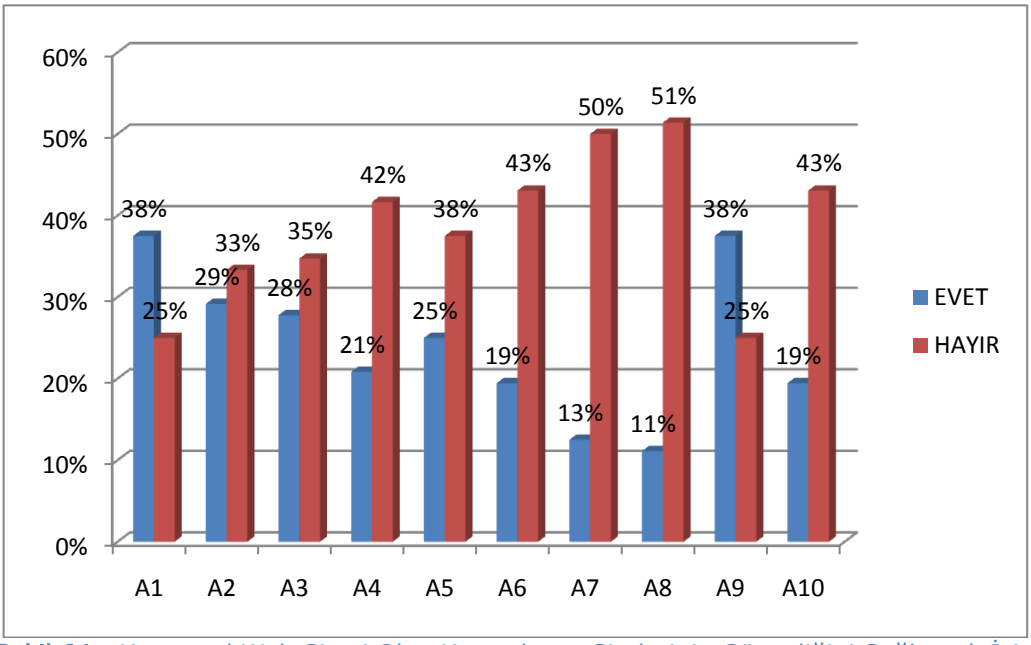


Şekil 63 : Web Sayfası Olan Kurumların Web Sayfalarının Güvenliği İle İlgilenen Personellerin Sertifikasyon Sahiplik Sayılarına Göre Dağılım Tablosu – Grafiksel Gösterim

Kurumsal web sitelerinin güvenliği ile ilgilenen personellerin yeterlilik yani sertifikasyon durumlarına bakıldığında, web sayfalarının güvenliği ile ilgilenen personellerinin hiçbirinin güvenlik sertifikasyonuna sahip olmadığı kurum web sitelerinin sayısının 10 (%22,2), personellerin çok azının sertifika sahibi olduğu kurum web sitelerinin sayısının 10 (%22,2), yarısının sertifika sahibi olduğu kurum web sitelerinin sayısının 5 (%11,1), çoğunun sertifika sahibi olduğu kurum web sitesi sayısının 12 (%26,7), tamamının sertifika sahibi olduğu kurum web sitesi sayısının ise 8 (%17,8) olduğu görülmüştür. Görülmektedir ki, web sitelerinin güvenliği genellikle sertifikasyon sahibi kişi ya da sertifikasyon sahibi en az bir kişiden meydana gelen gruplarca yerine getirilmekte ya da getirilmeye çalışılmaktadır.

4.3.1.11. Kurumsal Web Sitesi Olan Kurumların, Sitelerinin Güvenliğini Sağlamak İçin Aldıkları Yöntemler Dağılımı

Kurumsal web sitesi olan kurumların, sitelerinin güvenliğini sağlamak için aldıkları yöntemler incelendiğinde, en çok kullanılan ve tercih edilen iki yöntemin, port tabanlı FW kullanımı ve düzenli yedekleme olduğu tespit edilmiştir. En az tercih edilen iki yöntemin ise düzensiz olarak dışarıdan alınan penetration hizmeti alımı ve kurumca yapılan düzensiz güvenlik taramalar olduğu görülmüştür.



Şekil 64 : Kurumsal Web Sitesi Olan Kurumların, Sitelerinin Güvenliğini Sağlamak İçin Aldıkları Yöntemler Dağılımı Tablosu – Grafiksel Gösterim

A1: Port tabanlı FW kullanımı

A2: Uygulama tabanlı FW kullanımı

A3: Servis tabanlı IPS kullanımı

A4: Uygulama tabanlı IPS kullanımı

A5: Kurumca yapılan düzenli güvenlik taraması

A6: Dışarından düzenli penetration hizmeti Alımı

A7: Kurumca yapılan düzensiz güvenlik taraması

A8: Dışarından düzensiz penetration hizmeti Alımı

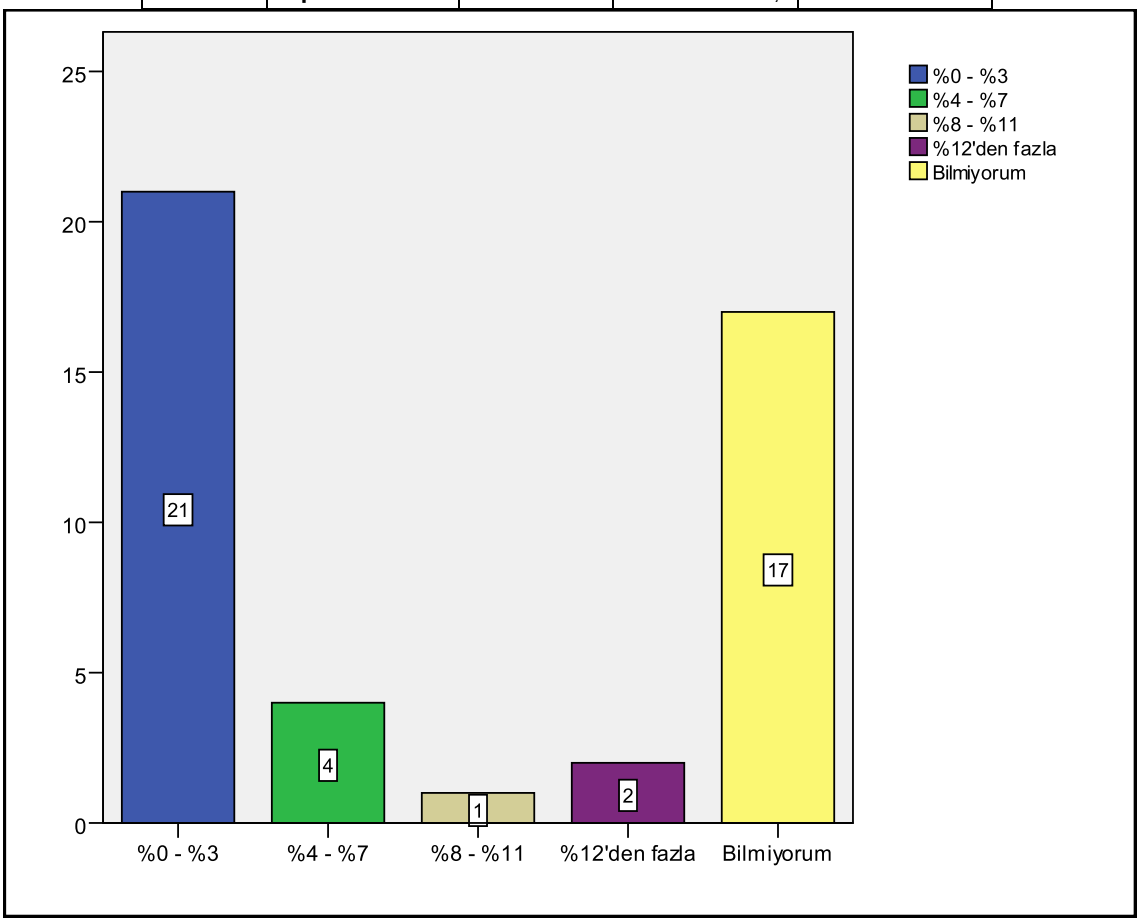
A9: Düzenli yedekleme

A10: Diğer

4.3.1.12. Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı

Tablo 30
Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	%0 - %3	21	46,7	46,7
	%4 - %7	4	8,9	55,6
	%8 - %11	1	2,2	57,8
	%12'den fazla	2	4,4	62,2
	Bilmiyorum	17	37,8	100,0
	Toplam	45	100,0	



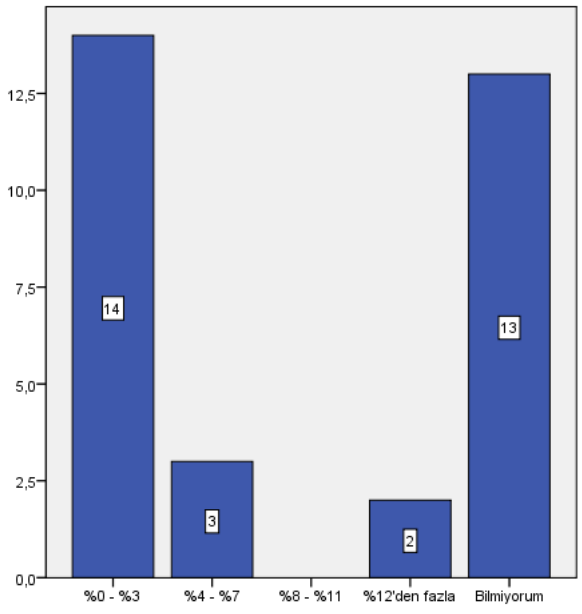
Şekil 65 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı

Web sitesi olan kurumların, web sitelerinin güvenliğine ayırdıkları ödeneğin, kurumun genel harcama ödenek miktarlarına oranlarına bakıldığında, 21 sitenin (46,7) %0-%3 arasında olduğu, 4 sitenin (%8,9) %4-%7 arasında olduğu, 1 sitenin (%2,2) %8-%11 arasında olduğu, 2 sitenin (%4,4) %12'den fazla olduğu, 17 sitenin (%37,8) ise site güvenliği ödenek miktarının çeşitli sebeplerden dolayı bilinmediği tespit edilmiştir. Görülmektedir ki, kurumların sitelerinin güvenlikleri için ayırdıkları ödenek miktarları toplam ödenek miktarlarının genellikle %0-%3 arasındadır.

4.3.1.13. Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı

Tablo 31
Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı

Kurumsal Web Sayfasından Online İşlem Sunma Durumu		Site Güvenliği Ödenek Miktarı					Toplam
		%0 - %3	%4 - %7	%8 - %11	%12'den fazla	Bilmiyorum	
Evet	Adet	14	3	0	2	13	32
	%	43,8%	9,4%	,0%	6,3%	40,6%	100,0%
Hayır	Adet	6	1	1	0	4	12
	%	50,0%	8,3%	8,3%	,0%	33,3%	100,0%



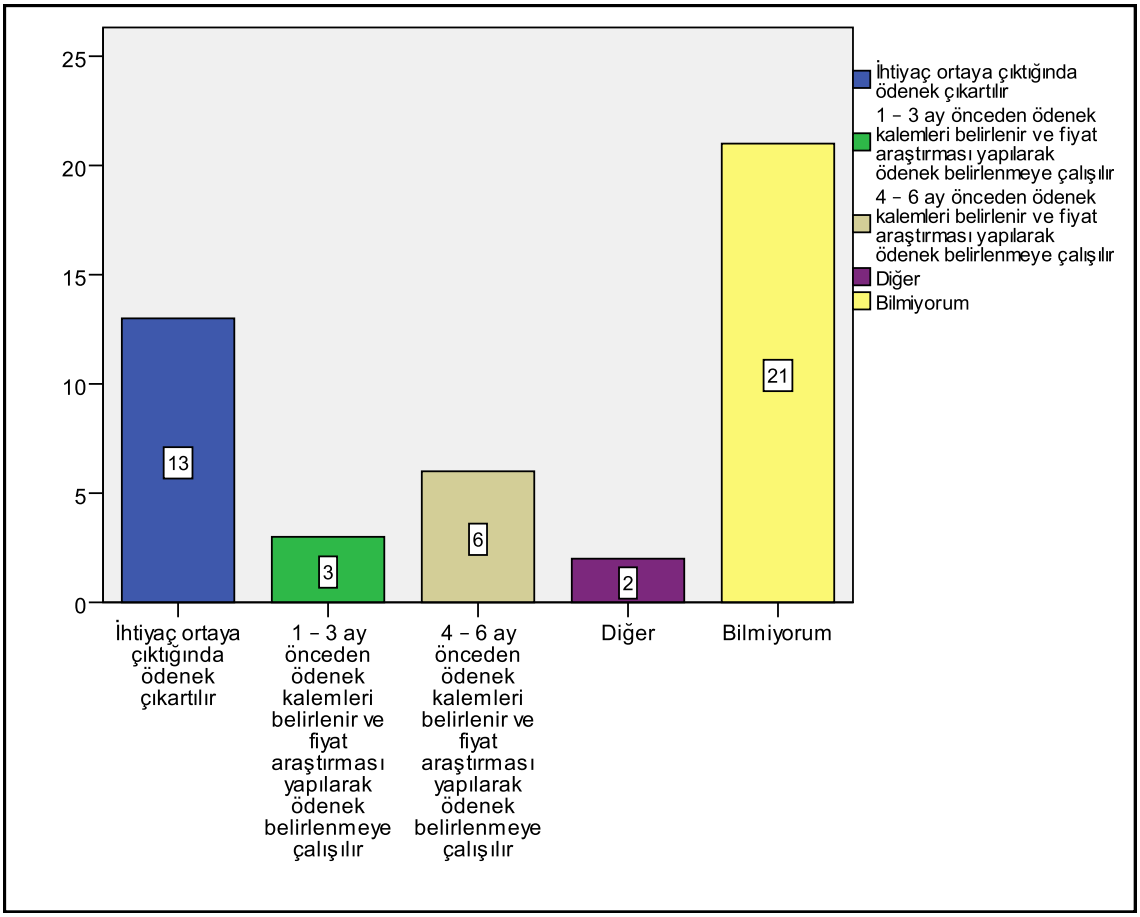
Şekil 66 : Web Sitesi Olup Bu Sitelerinden Online İşlem Sunan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Dağılımı Tablosu – Grafiksel Gösterim

Sitelerinden online işlem veren kurumların, sitelerinin güvenliği için ayırdıkları ödenek miktarlarına bakıldığında ise, 14 (%43,8) kurumun site güvenliği için %0-3 oranında ödenek ayırdığı, 3 (%9,4) kurumun %4-7, 2 (%6,3) kurumun %12'den fazla ödenek ayırdığı, 13 (%40,6) kurumun ise ödenek miktarlarının belli olmadığı ya da diğer çeşitli sebeplerden dolayı bilinmediği görülmüştür. Görülmektedir ki, sitelerinden online işlem veren kurumlar, bu sitelerinin güvenliği için genel ödenek miktarlarının %0-3 aralığında bir kısmı ayırmakta ve bu miktar ile sitelerinin güvenliğini sağlamakta ya da sağlamaya çalışmaktadırlar.

4.3.1.14. Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı

Tablo 32
Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	İhtiyaç ortaya çıktığında ödenek çıkartılır	13	28,9	28,9
	1 – 3 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	3	6,7	35,6
	4 – 6 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	6	13,3	48,9
	Diğer	2	4,4	53,3
	Bilmiyorum	21	46,7	100,0
	Toplam	45	100,0	



Şekil 67 : Web Sitesi Olan Kurumların, Web Sitelerinin Güvenliğine Ayırdıkları Ödenek Miktarını Belirleme Yöntemleri Dağılımı Tablosu – Grafiksel Gösterim

Web sitesi olan kurumların, web sitelerinin güvenliğine ayırdıkları ödeneğin belirlenme yöntemleri incelendiğinde, 13 (%28,9) kurumun ihtiyaç olduğunda belirledikleri, 3 (%6,7) kurumun 1-3 ay önceden ödenek kalemlerini belirleyerek, fiyat araştırması yaparak belirledikleri, 6 (%13,3) kurumun 4-6 ay önceden ödenek kalemlerini belirleyerek, fiyat araştırması yaparak belirledikleri, 2 (%4,4) kurumun farklı bir yöntem kullandığı, 21 (%46,7) kurumun ise bahse konu ödenek miktarlarını belirlemek için ne şekilde bir yöntem izlediğinin bilinmediği tespit edilmiştir. Görülmektedir ki, kurumlar sitelerinin güvenliği ile ilgili güvenlik ödeneklerini, genel olarak herhangi bir sorun ile karşılaştıklarında ya da ihtiyaç duydukları anda ya da belirlemeye çalışmaktadırlar.

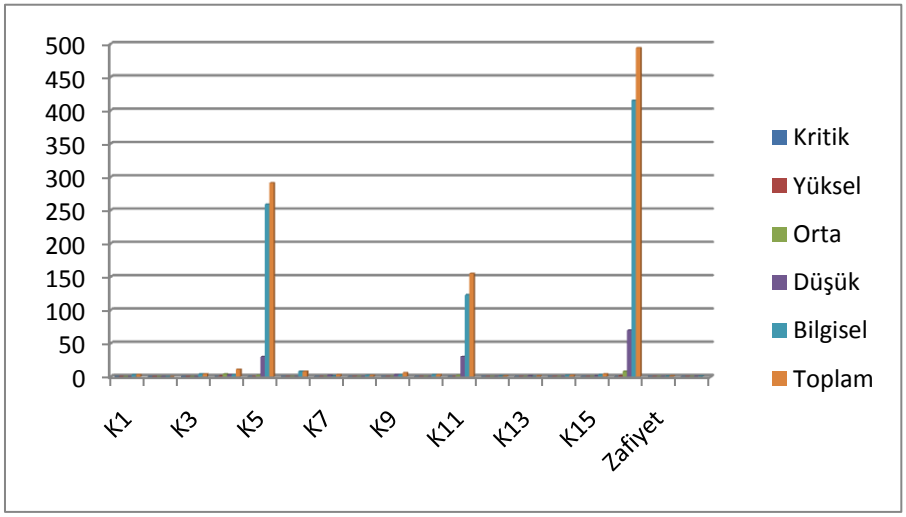
4.3.1.15. Web Sitelerinde Bulunan Zafiyetler Dağılımı

Tablo 33
Web Sitelerinde Bulunan Zfiyetler Dağılımı

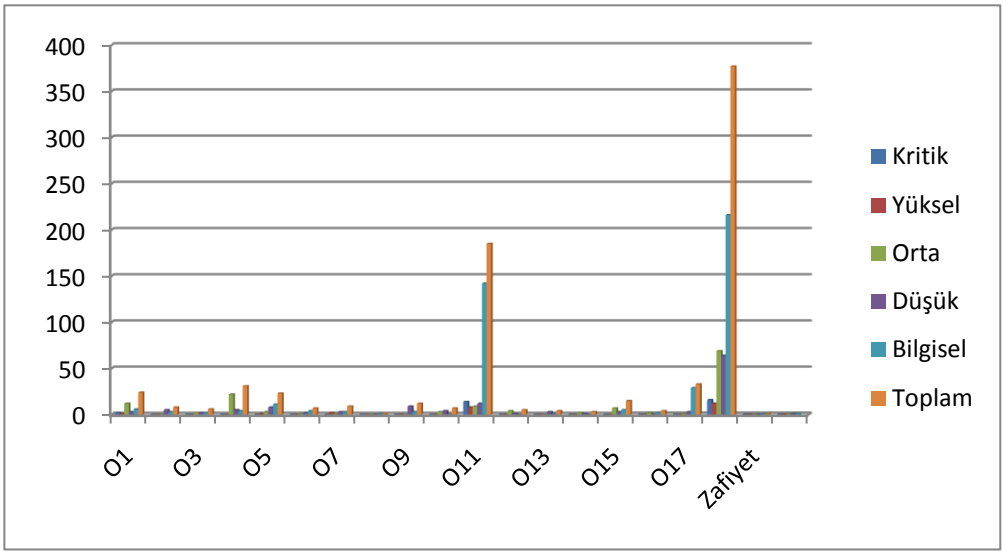
	Site	Kritik	Yüksel	Orta	Düşük	Bilgisel	Toplam
Özel Şirketlera Ait Web Siteleri	**O1**	2	1	12	3	6	24
	O2	0	0	0	5	3	8
	O3	0	0	2	2	2	6
	O4	0	0	22	5	4	31
	O5	0	1	3	8	11	23
	O6	0	0	1	2	4	7
	O7	0	2	1	3	3	9
	O8	0	0	0	0	1	1
	O9	0	0	0	9	3	12
	O10	0	0	3	4	0	7
	O11	14	8	9	12	142	185
	O12	0	0	4	1	0	5
	O13	0	0	0	3	1	4
	O14	0	0	2	1	0	3
	O15	0	0	7	3	5	15
	O16	0	0	2	0	2	4
	O17	0	0	1	3	29	33
	Toplam	**16**	**12**	**69**	**64**	**216**	**377**
	Zafiyet	**4%**	**3%**	**18%**	**17%**	**57%**	**100%**
	Firma	**12%**	**24%**	**76%**	**88%**	**82%**	

	Site	Kritik	Yüksel	Orta	Düşük	Bilgisel	Toplam
Özelleştirilmiş Şirketlere Ait Web Siteleri	**OZ1**	0	0	3	1	2	5
	OZ2	0	0	1	0	1	5
	OZ3	0	0	2	2	3	5
	Toplam	**0**	**0**	**6**	**3**	**6**	**15**
	Zafiyet	**0%**	**0%**	**40%**	**20%**	**40%**	**100%**
	Firma	**0%**	**0%**	**100%**	**67%**	**100%**	

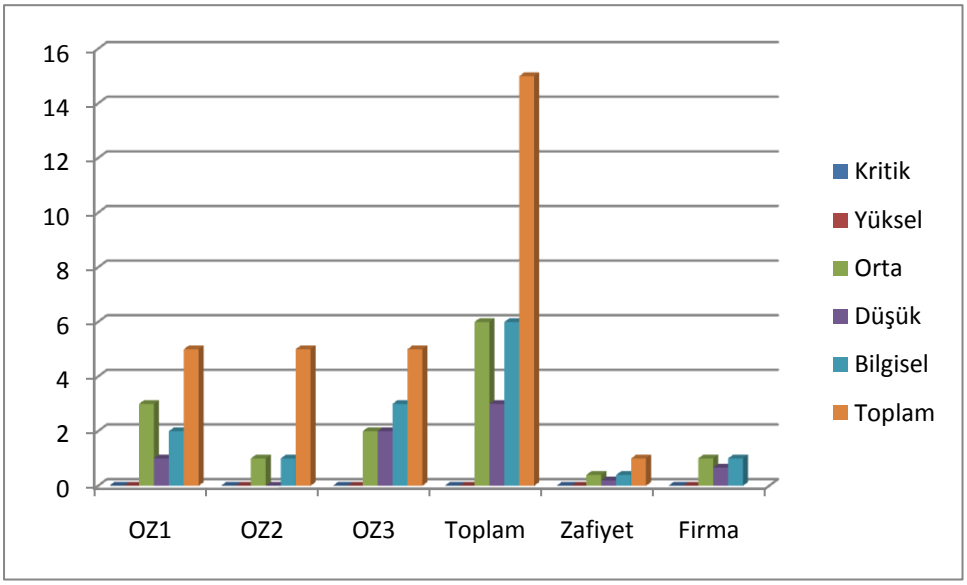
Kamu Kurumlarına Ait Web Siteleri	Site	Kritik	Yüksel	Orta	Düşük	Bilgisel	Toplam
	K1	0	0	0	0	3	3
	K2	0	0	0	0	0	0
	K3	0	0	0	0	4	4
	K4	0	1	4	3	3	11
	K5	0	0	2	30	259	291
	K6	0	0	0	0	8	8
	K7	0	0	0	2	1	3
	K8	0	0	0	0	2	2
	K9	0	0	0	3	3	6
	K10	0	0	0	0	3	3
	K11	0	0	2	30	123	155
	K12	0	0	0	0	1	1
	K13	0	0	0	1	0	1
	K14	0	0	0	0	2	2
	K15	0	0	0	1	3	4
	Toplam	**0**	**1**	**8**	**70**	**415**	**494**
	Zafiyet	**0%**	**0,2%**	**2%**	**14%**	**84%**	**100%**
	Firma	**0%**	**7%**	**20%**	**47%**	**87%**	



Şekil 68
Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Kamu Kurumlarına Ait Web Siteleri



Şekil 69
Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Özel Şiretlere Ait Web Siteleri



Şekil 70
Web Sitelerinde Bulunan Zfiyetler Dağılımı – Grafiksel Gösterim (Özelleştiriliş Şiretlere Ait Web Siteleri

Ankete cevap veren 72 kişinin çalıştıkları özl şirketlerin internet siteleri web güvenlik taramasından geçirildiğinde, kritik risk seviyesine sahip güvenlik zafiyetine sahip özel şirketlere ait 2 (%12) web sitesi olduğu, bunların da toplam 16 (%4) adet olduğu, yüksek risk seviyesine sahip özel şirketlere ait web sitesinin 4 (%24) adet olduğu ve bunların da 12 (%13) adet olduğu, orta risk seviyesine sahip zafiyeti olan özle şirketlere ait web sitesinin 13 (% 76) adet olduğu, bunların da toplam 69 (%18) adet olduğu, düşük risk seviyesine sahip zafiyeti olan özel şirketlere ait web sitesinin 15 (%88) adet olduğu ve bu zafiyetlerin de toplam 64 (%17) adet olduğu, bilgisel risk seviyesine sahip zafiyeti olan özel şirketlere ait web sitesinin 14 (%82) adet olduğu, bunların da toplam 216 (%57) adet olduğu, toplam zafiyet sahipliğine bakıldığında incelenen özel şirketlere ait web sitelerinin

toplam 377 (%100) adet zafiyete sahip oldukları ve herhangi bir zafiyete sahip olmayan özel şirket web sitesi olmadığı tespit edilmiştir.

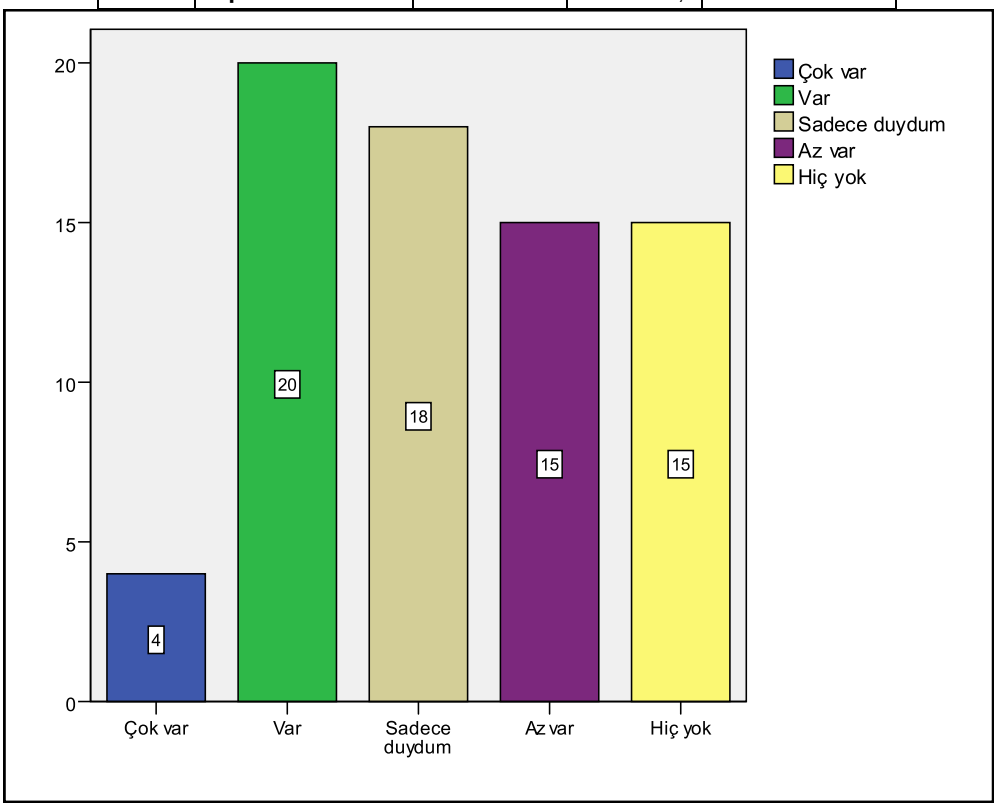
Kamu kurmlarına ait web siteleri incelendiğinde, Kritik risk seviyesine sahip güvenlik zafiyetine sahip kamu kurumlarına ait web sitesi olmadığı, yüksek risk seviyesine sahip kamu kurumu web sitesinin 1 (%7) adet olduğu onun da 1 (%0,2) adet olduğu, orta risk seviyesine sahip zafiyeti olan kamu kurumu web sitesinin 3 (%20) adet olduğu, bunların da toplam 8 (%2) adet olduğu, düşük risk seviyesine sahip zafiyeti olan kamu kurumu web sitesinin 7 (%47) adet olduğu ve bu zafiyetlerin de toplam 70 (%14) adet olduğu, bilgisel risk seviyesine sahip zafiyeti olan kamu kurumu web sitesinin 13 (%87) adet olduğu, bunların da toplam 415 (%84) adet bilgisel risk seviyesine sahip zafiyeti olduğu, toplam zafiyet sahipliğine bakıldığında incelenen kamu kurumu web sitelerinin toplam 494 (%100) adet zafiyete sahip oldukları herhangi bir zafiyete sahip olmayan 1 (%7) adet kamu kurumlarına ait internet web sitesi olduğu tespit edilmiştir.

Özelleştirilmiş şirketlere ait web siteleri incelendiğinde, Kritik ve yüksek risk seviyesine sahip güvenlik zafiyetine sahip özelleştirilmiş şirktlere ait web sitesi olmadığı, orta risk seviyesine sahip zafiyeti olan özelleştirilmiş şirktlere ait web sitesinin 3 (%100) adet olduğu, bunların da toplam 6 (%40) adet olduğu, düşük risk seviyesine sahip zafiyeti olan özelleştirilmiş şirktlere ait web sitesinin 2 (%67) adet olduğu ve bu zafiyetlerin de toplam 3 (%20) adet olduğu, bilgisel risk seviyesine sahip zafiyeti olan özelleştirilmiş şirktlere ait web sitesinin 3 (%100) adet olduğu, bunların da toplam 6 (%40) adet bilgisel risk seviyesine sahip zafiyeti olduğu, toplam zafiyet sahipliğine bakıldığında incelenen özelleştirilmiş şirktlere ait web sitelerinin toplam 15 (%100) adet zafiyete sahip oldukları ve herhangi bir zafiyete sahip olmayan özelleştirilmiş şirketlere ait internet web sitesi olmadğı tespit edilmiştir.

4.3.1.16. www.turkiye.gov.tr Hakkında Bilgi Sahibi Olma Dağılımı

Tablo 34
www.turkiye.gov.tr Hakkında Bilgi Sahibi Olma Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Çok var	4	5,6	5,6
	Var	20	27,8	33,3
	Sadece duydum	18	25,0	58,3
	Az var	15	20,8	79,2
	Hiç yok	15	20,8	100,0
	Toplam	72	100,0	



Şekil 71 : www.turkiye.gov.tr Hakkında Bilgi Sahibi Olma Dağılımı Tablosu – Grafiksel Gösterim

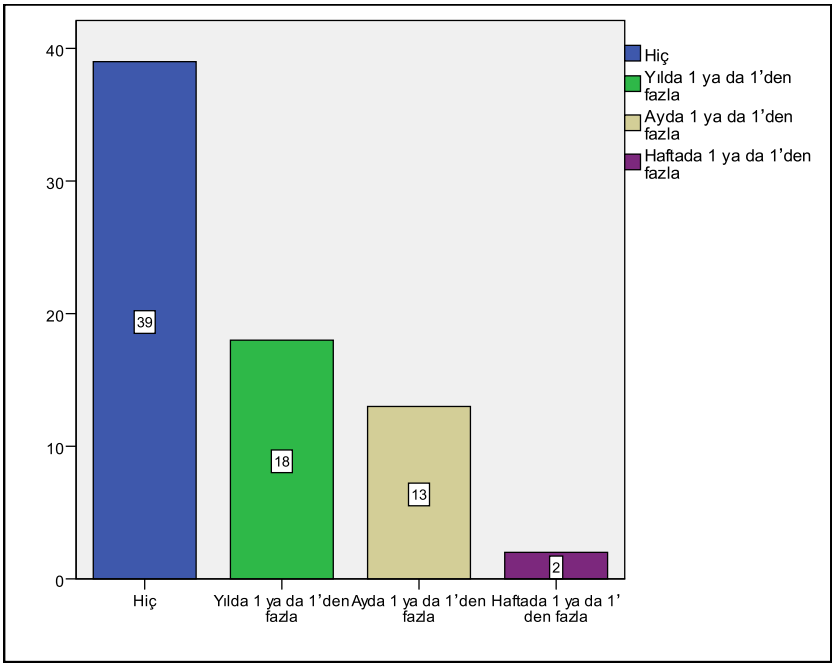
Ankete katılanların Başbakanlık tarafından 2009 yılında hayata geçirilen www.turkiye.gov.tr web sitesi hakkında bilgi sahipliklerine bakıldığında, 4'ünün (%5,6) çok bilgisi olduğu, 20'sinin (%27,8) siteyi sadece bildikleri, 18'inin (%25,0) siteyi sadece duydukları, 15'inin (%20,8) site hakkında çok az bilgisi olduğu, diğer 15'inin ise (%20,8) site hakkında hiç bilgilerinin olmadığı tespit edilmiştir. Görülmektedir ki,

www.turkiye.gov.tr sitesi hakkında genel olarak bilgi sahipliği bulunmaktadır.

4.3.1.17. www.turkiye.gov.tr Ziyaret Sıklığı Dağılımı

Tablo 35
www.turkiye.gov.tr Ziyaret Sıklığı Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Hiç	39	54,2	54,2
	Yılda 1 ya da 1'den fazla	18	25,0	79,2
	Ayda 1 ya da 1'den fazla	13	18,1	97,2
	Haftada 1 ya da 1'den fazla	2	2,8	100,0
	Toplam	72	100,0	



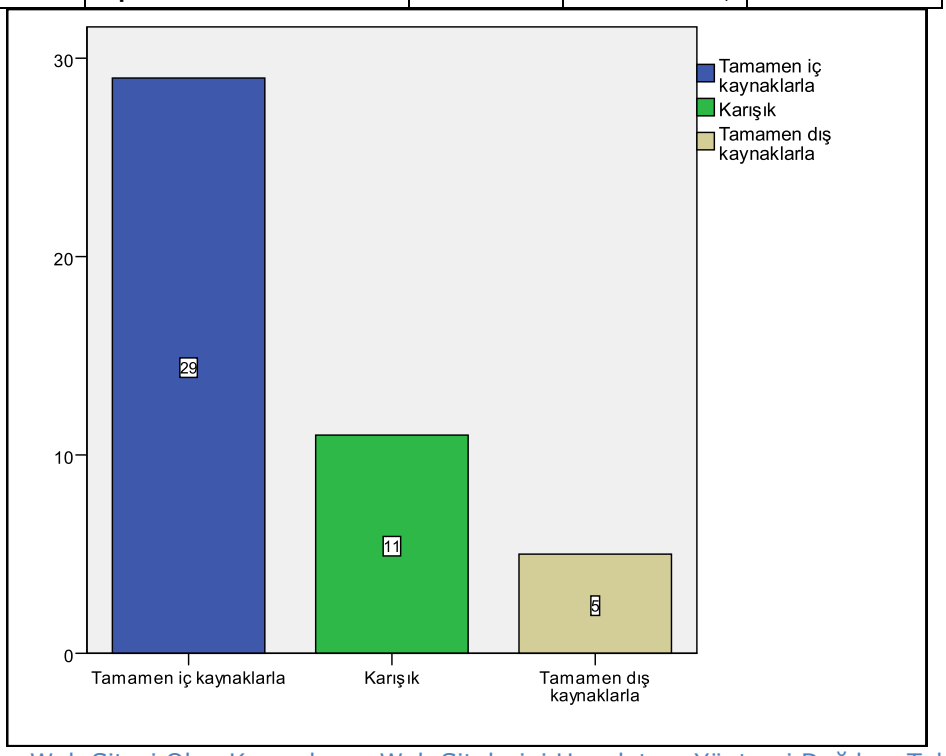
Şekil 72 : www.turkiye.gov.tr Ziyaret Sıklığı Dağılımı Tablosu – Grafiksel Gösterim

Ankete katılanların Başbakanlık tarafından 2009 yılında hayata geçirilen www.turkiye.gov.tr web sitesini ziyaret sıklıkları incelendiğinde, 39'unun (%54,2) bu siteyi hiç ziyaret etmedikleri, 18'inin (%25,0) siteyi yılda 1 ya da 1'den fazla ziyaret ettikleri, 13'ünün (%18,1) siteyi ayda 1 ya da 1'den fazla ziyaret ettikleri, 2'sinin ise (%2,8) siteyi haftada 1 ya da birden fazla ziyaret ettikleri tespit edilmiştir. Görülmektedir ki, www.turkiye.gov.tr sitesi çok fazla ziyaret edilmemektedir.

4.3.1.18. Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı

Tablo 36
Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Tamamen iç kaynaklarla	29	64,4	64,4
	Karışık	11	24,4	88,9
	Tamamen dış kaynaklarla	5	11,1	100,0
	Toplam	45	100,0	



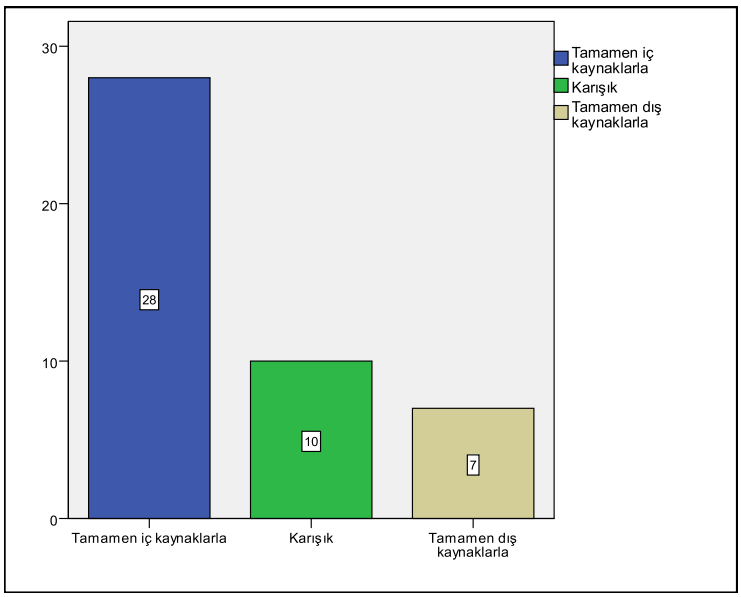
Şekil 73 : Web Sitesi Olan Kurumların, Web Sitelerini Hazırlatma Yöntemi Dağılımı Tablosu – Grafiksel Gösterim

Web sitesi olan kurumların, web sitelerini hazırlatma yöntemleri incelendiğinde, 29 (%64,4) kurumun, sitelerini tamamen iç kaynaklar ile hazırladıkları, 11 (%24,4) kurumun, sitelerini iç ve dış kaynaklar ile ortaklaşa hazırlattıkları, 5 (%11,1) kurumun ise sitesini tamamen dış kaynaklar ile hazırlattıkları tespit edilmiştir. Görülmektedir ki, kurumlar web sitelerinin hazırlanması esnasında genellikle iç kaynaklarını kullanmaktadırlar, tamamen iç kaynaklar ile gerçekleştiremedikleri durumlarda ise, kendi iç kaynaklarını sitenin hazırlanması esnasında sürece bir şekilde dahil etmekte ya da ettirmektedirler.

4.3.1.19. Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı

Tablo 37
Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Tamamen iç kaynaklarla	28	62,2	62,2
	Karışık	10	22,2	84,4
	Tamamen dış kaynaklarla	7	15,6	100,0
	Toplam	45	100,0	



Şekil 74 : Web Sitesi Olan Kurumların, Web Sitelerini Yayınlama Yöntemi Dağılımı Tablosu – Grafiksel Gösterim

Web sitesi olan kurumların, web sitelerini yayınlama yöntemleri incelendiğinde, 28 (%62,2) kurumun, sitelerini tamamen iç kaynaklar ile yayınladıkları, 10 (%22,2) kurumun, sitelerini iç ve dış kaynaklar ile ortaklaşa yayınladıkları, 7 (%15,6) kurumun ise sitesini tamamen dış kaynaklar ile yayınladıkları tespit edilmiştir. Görülmektedir ki, kurumlar web sitelerinin yayınlanması esnasında genellikle iç kaynaklarını kullanmaktadırlar, tamamen iç kaynaklar ile gerçekleştiremedikleri durumlarda ise, kendi iç kaynaklarını sitenin yayınlanması esnasında sürece bir şekilde dahil etmekte ya da ettirmektedirler.

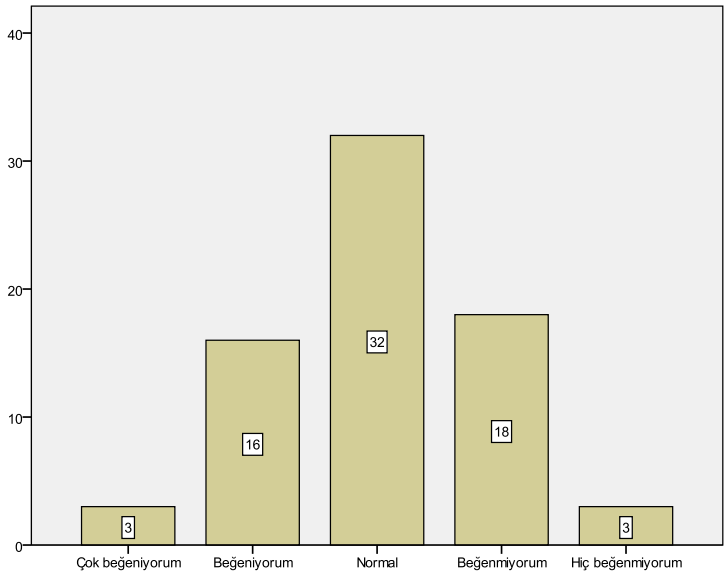
4.3.1.20. Kamu Kurumlarına Ait Web Sitelerinin İçeriksel ve Tasarımsal Beğenilme Dağılımı

Tablo 38
Kamu Kurumu Sitelerinin İçerik Olarak Beğenilme Dağılımı

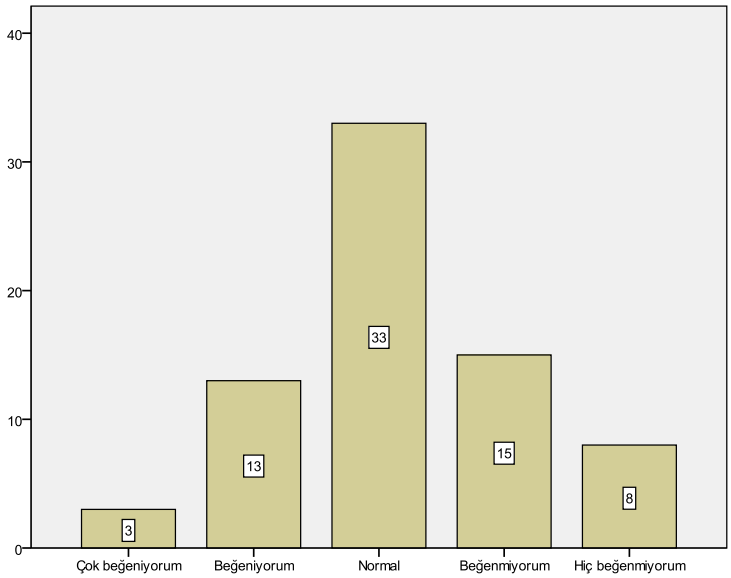
		Frekans	Yüzde	Toplam Yüzde
	Çok beğeniyorum	3	4,2	4,2
	Beğeniyorum	16	22,2	26,4
	Normal	32	44,4	70,8
	Beğenmiyorum	18	25,0	95,8
	Hiç beğenmiyorum	3	4,2	100,0
	Toplam	72	100,0	

Tablo 39
Kamu Kurumu Sitelerinin Tasarım Olarak Beğenilme Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Çok beğeniyorum	3	4,2	4,2
	Beğeniyorum	13	18,1	22,2
	Normal	33	45,8	68,1
	Beğenmiyorum	15	20,8	88,9
	Hiç beğenmiyorum	8	11,1	100,0
	Toplam	72	100,0	



Şekil 75 : Kamu Kurumu Sitelerinin İçerik Olarak Beğenilme Dağılımı Tablosu – Grafiksel Gösterim



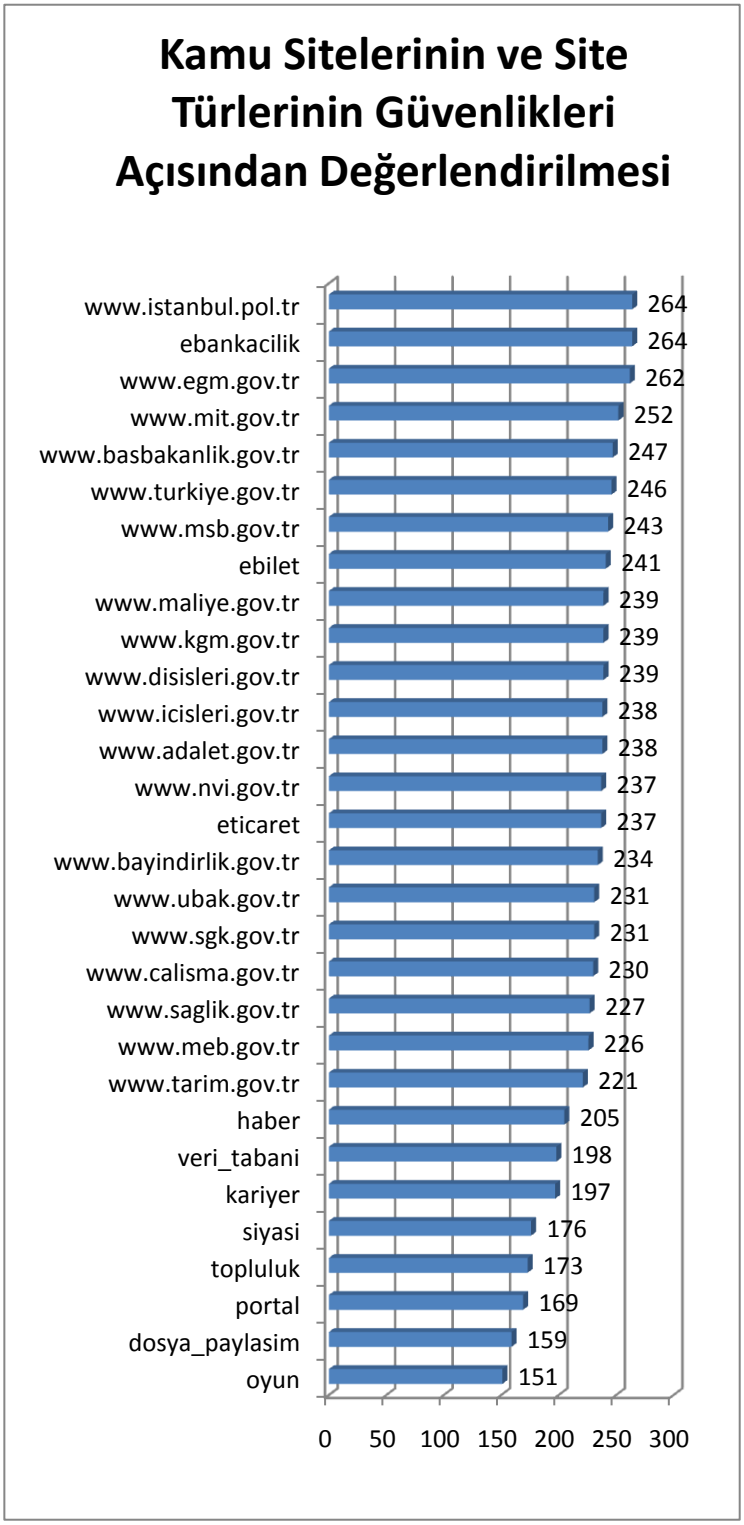
Şekil 76 : Kamu Kurumu Sitelerinin Tasarım Olarak Beğenilme Dağılımı Tablosu – Grafiksel Gösterim

Kamu kurumlarına ait olan web sitelerinin içeriksel olarak beğenilme oranları incelendiğinde, kamu kurumlarına ait sitelerin içeriksel olarak 3 (%4,2) kişi tarafından çok beğenildiği, 16 (%22,2) kişi tarafından beğenildiği, 32 kişi tarafından (%44,4) normal bulunduğu, 18 (%25) kişi tarafından beğenilmediği, 3 (%4,3) kişi tarafından ise hiç beğenilmediği tespit edilmiştir.

Kamu kurumlarına ait olan web sitelerinin tasarımsal olarak beğenilme oranları incelendiğinde, kamu kurumlarına ait sitelerin tasarımsal olarak 3 (%4,2) kişi tarafından çok beğenildiği, 13 (%18,1) kişi tarafından beğenildiği, 33 kişi tarafından (%45,8) normal bulunduğu, 15 (%20,8) kişi tarafından beğenilmediği, 8 (%11,1) kişi tarafından ise hiç beğenilmediği tespit edilmiştir.

Genel olarak bakıldığında, kamu kurumlarına ait web sitelerinin içeriksel ve tasarımsal olarak genellikle "normal" ve daha üstü şekilde beğenilir bulundukları tespit edilmiştir.

4.3.1.21. Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Değerlendirilme Dağılımı



Şekil 77 : Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Değerlendirilme Tablosu – Grafiksel Gösterim

Tablo 40
Kamu Sitelerinin ve Site Türlerinin Güvenlikleri Açısından Ortalamalı Değerlendirilme Tablosu

Sıra No	Web Sitesi Adresi / Türü	Cevap Veren Sayısı	Ortalama (5 üzerinden)
1	www.turkiye.gov.tr	72	3,42
2	www.basbakanlik.gov.tr	72	3,43
3	www.adalet.gov.tr	72	3,31
4	www.msb.gov.tr	72	3,38
5	www.icisleri.gov.tr	72	3,31
6	www.disisleri.gov.tr	72	3,32
7	www.maliye.gov.tr	72	3,32
8	www.meb.gov.tr	72	3,14
9	www.bayindirlik.gov.tr	72	3,25
10	www.saglik.gov.tr	72	3,15
11	www.ubak.gov.tr	72	3,21
12	www.tarim.gov.tr	72	3,07
13	www.calisma.gov.tr	72	3,19
14	www.mit.gov.tr	72	3,50
15	www.egm.gov.tr	72	3,64
16	www.istanbul.pol.tr	72	3,67
17	www.kgm.gov.tr	72	3,32
18	www.sgk.gov.tr	72	3,21
19	www.nvi.gov.tr	72	3,29
20	Dosya Paylaşım	72	2,21
21	E-bankacılık	72	3,67
22	E-ticaret	72	3,29
23	E-bilet	72	3,35

Sıra No	Web Sitesi Adresi / Türü	Cevap Veren Sayısı	Ortalama (5 üzerinden)
24	Haber	72	2,85
25	Kariyer	72	2,74
26	Oyun	72	2,10
27	Portal	72	2,35
28	Siyasi	72	2,44
29	Topluluk	72	2,40
30	Veri Tabanı	72	2,75

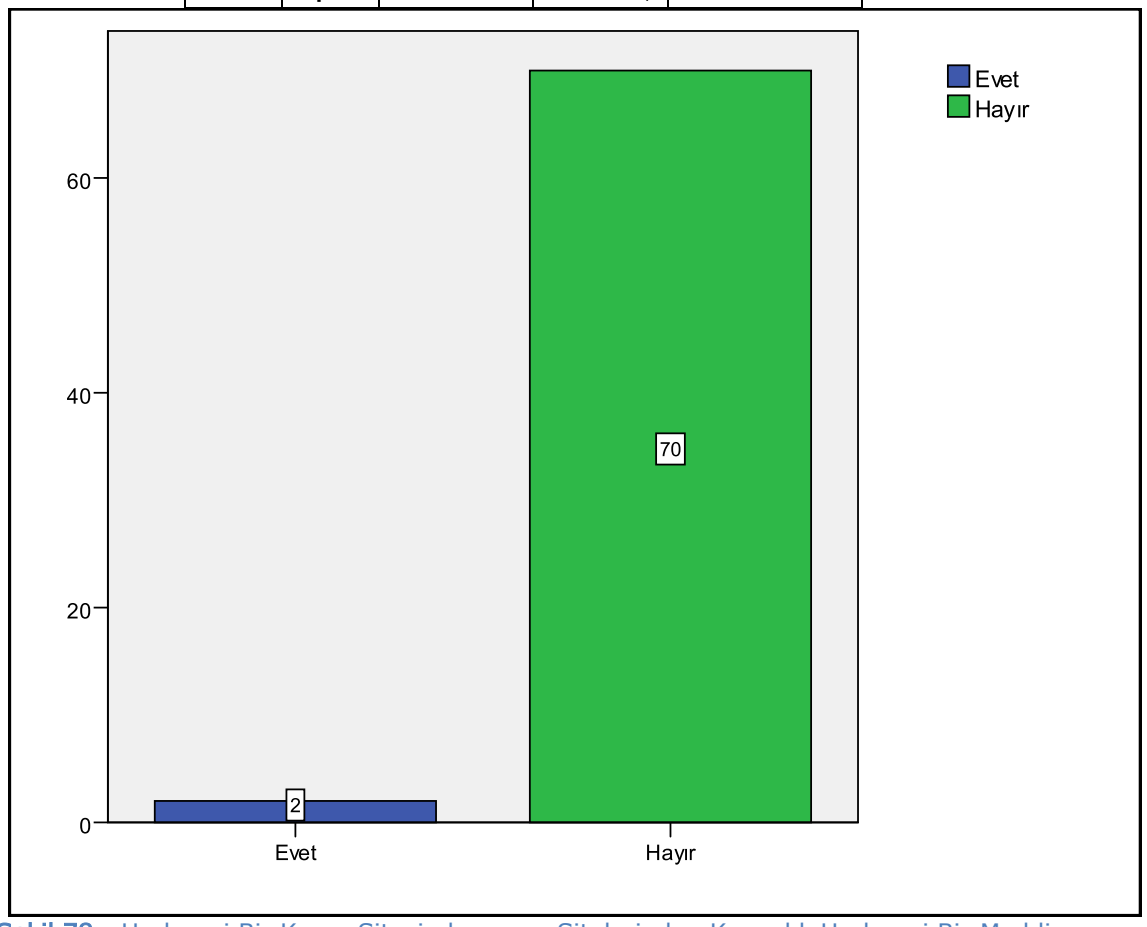
Ankete katılanlar tarafından kamu kurumlarına ait olan belli başlı siteleri ve web sitesi türlerinin güvenlik seviye puanlama cevapları değerlendirilerek incelendiğinde, en güvensiz bulunan web sitelerinin 151 puan ile "oyun" web siteleri türü olduğu düşünüldüğü, en güvenli web sitesi türünün ise 264 puan ile"e-bankacılık" web siteleri türünün olduğu düşünüldüğü ortaya çıkmıştır.

En güvensiz kamu web sitesinin ise, 221 puan ile www.tarim.gov.tr olduğu düşünüldüğü, en güvenli kamu web sitesinin ise 264 puan ile www.istanbul.pol.tr olduğu düşünüldüğü görülmüştür.

4.3.1.22. Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı

Tablo 41
Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	2	2,8	2,8
	Hayır	70	97,2	100,0
	Toplam	72	100,0	



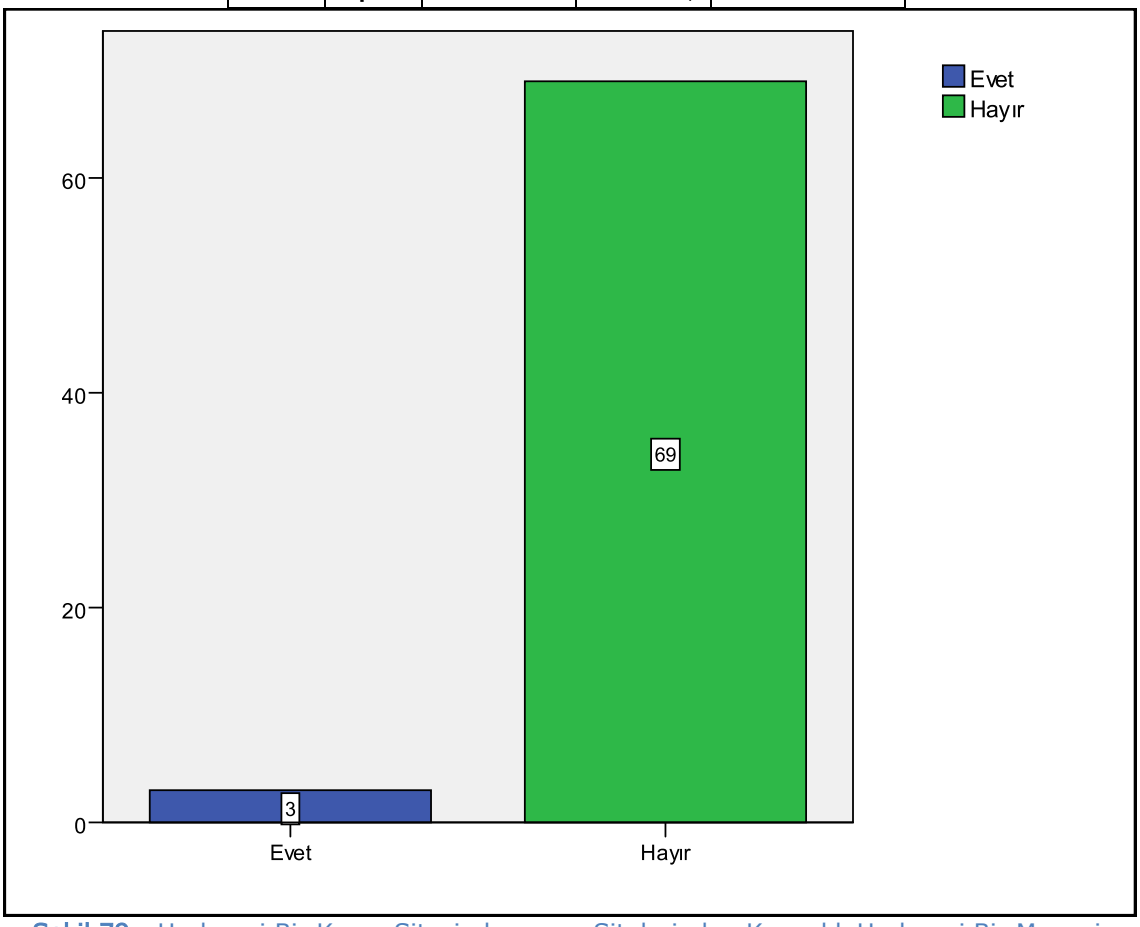
Şekil 78 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim

Ankete katılanların herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı herhangi bir maddi zarara uğrama dağılımı incelendiğinde, 2'sinin (%2,8) maddi zarara uğradığı, 70'inin (%97,2) maddi zarara uğramadığı görülmüştür.

4.3.1.23. Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı

Tablo 42
Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	3	4,2	4,2
	Hayır	69	95,8	100,0
	Toplam	72	100,0	



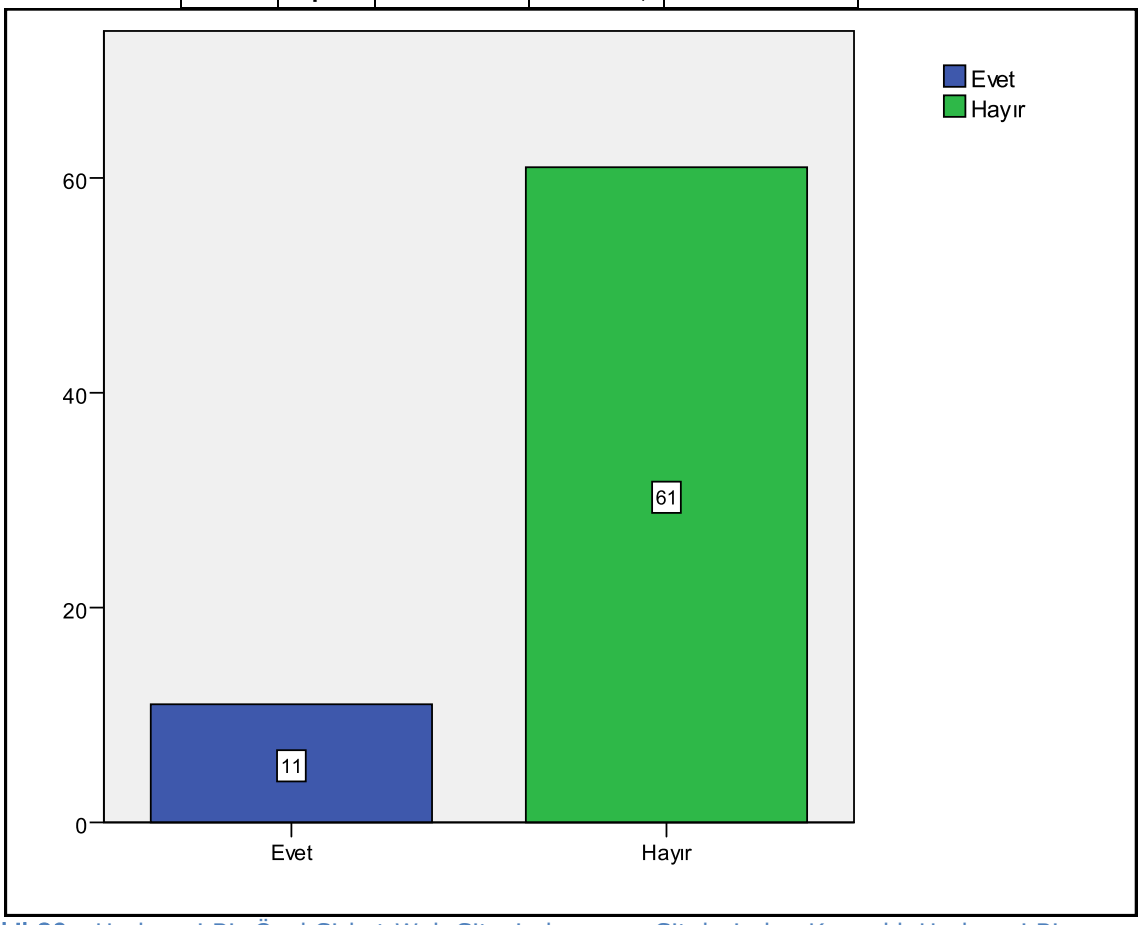
Şekil 79 : Herhangi Bir Kamu Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim

Ankete katılanların herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı herhangi bir manevi zarara uğrama dağılımı incelendiğinde, 3'ünün (%4,2) manevi zarara uğradığı, 69'unun (%95,8) manevi zarara uğramadığı görülmüştür.

4.3.1.24. Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı

Tablo 43
Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	11	15,3	15,3
	Hayır	61	84,7	100,0
	Toplam	72	100,0	



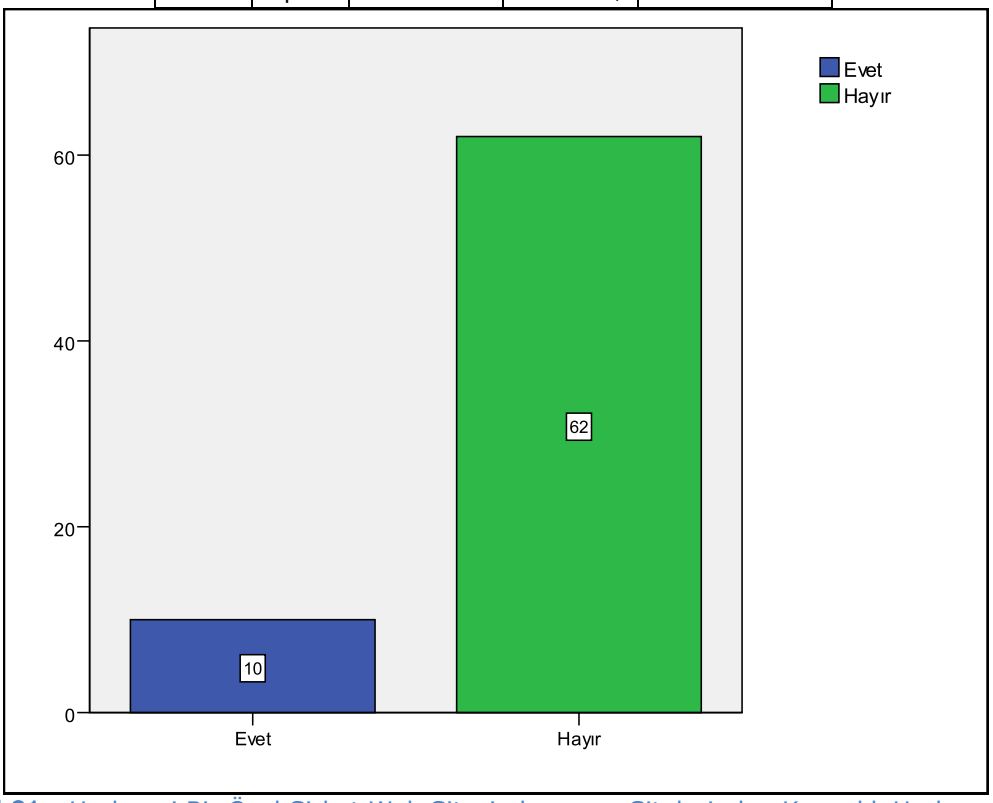
Şekil 80 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Maddi Zarara Uğrama Dağılımı Tablosu – Grafiksel Gösterim

Ankete katılanların herhangi bir özel şirket web sitesinden veya bu sitelerden kaynaklı herhangi bir maddi zarara uğrama dağılımı incelendiğinde, 11'inin (%15,3) maddi zarara uğradığı, 61'inin (%84,7) maddi zarara uğramadığı görülmüştür.

4.3.1.25. Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı

Tablo 44
Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı

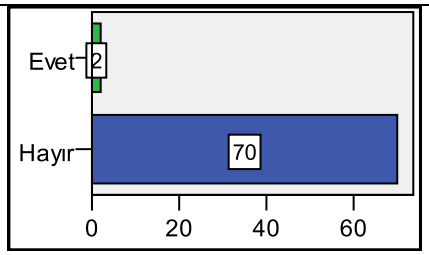
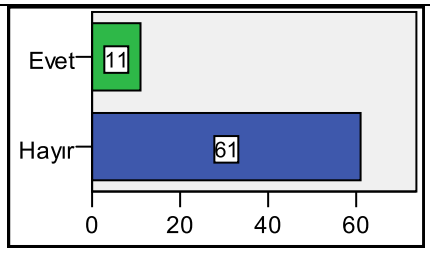
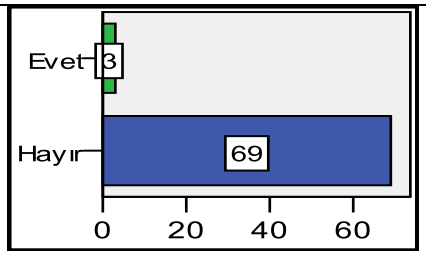
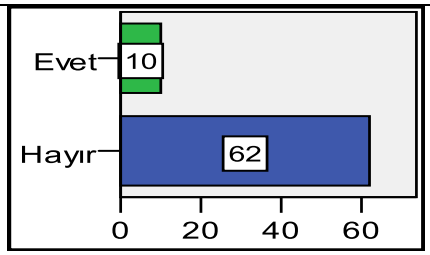
		Frekans	Yüzde	Toplam Yüzde
	Evet	10	13,9	13,9
	Hayır	62	86,1	100,0
	Toplam	72	100,0	



Şekil 81 : Herhangi Bir Özel Şirket Web Sitesinden veya Sitelerinden Kaynaklı Herhangi Bir Manevi Zarara Uğrama Dağılımı

Ankete katılanların herhangi bir özel şirket web sitesinden veya bu sitelerden kaynaklı herhangi bir manevi zarara uğrama dağılımı incelendiğinde, 10'unun (%13,9) manevi zarara uğradığı, 62'sinin (%86,1) manevi zarara uğramadığı görülmüştür.

Kamu kurumları ve özel şirket web sitelerini uğranan zarar miktarlarına göre karşılaştırdığımızda, insanların özel şirket web sitelerinden, kamu web sitelerine göre daha fazla maddi (5,5 kat) ve manevi (3,3 kat) zarara uğradıkları görülmektedir.

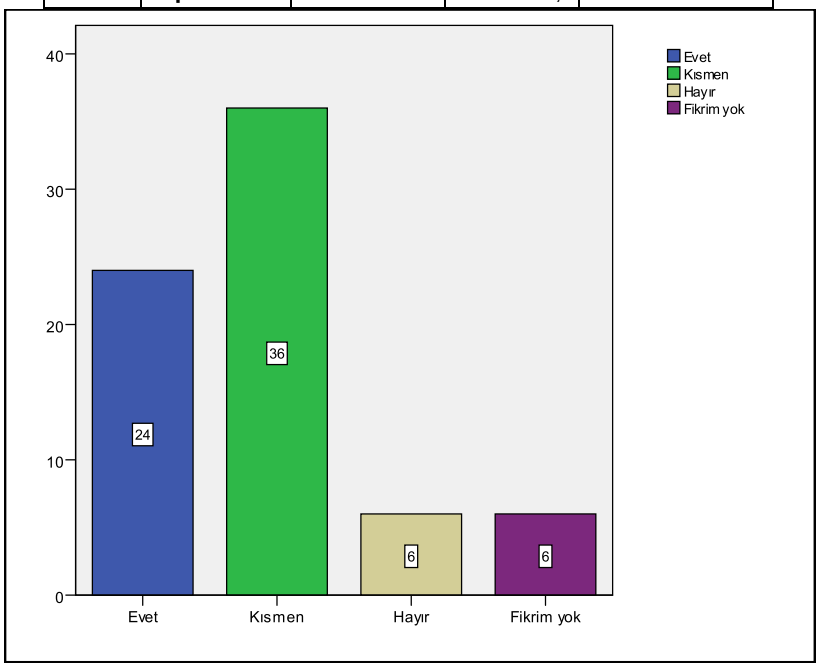
Soru		Kamu Kurumları Web Sitelerinden ya da bu Sitelerden Kaynaklı	Özel Şirket Web Sitelerinden ya da bu Sitelerden Kaynaklı
Daha önce hiç herhangi bir zarara uğradınız mı?	Maddi		
	Manevi		

Şekil 82 : Kamu ve Özel şirket web siteleri kaynaklı maddi ya da manevi zarara uğrama karşılaştırması Dağılımı

4.3.1.26. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 45
Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	24	33,3	33,3
	Kısmen	36	50,0	83,3
	Hayır	6	8,3	91,7
	Fikrim yok	6	8,3	100,0
	Toplam	72	100,0	



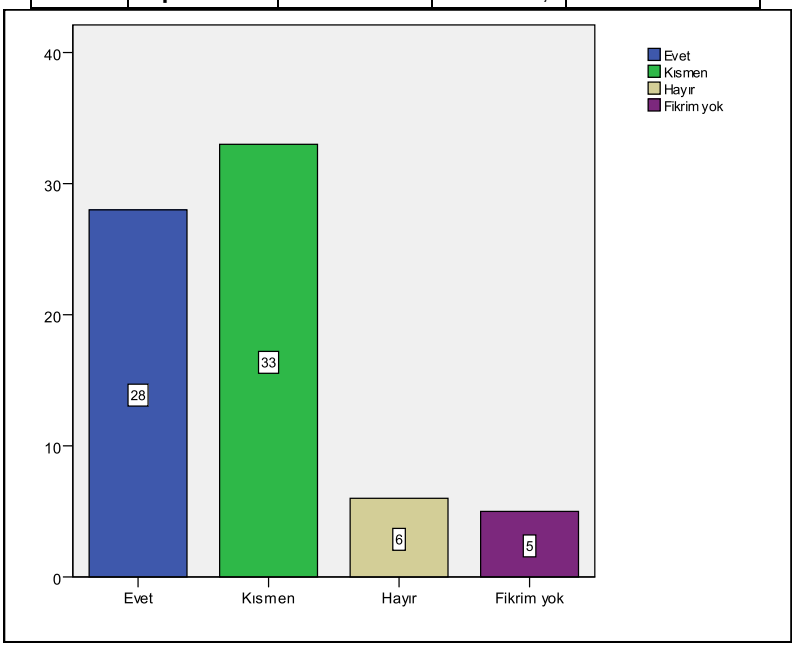
Şekil 83 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

Herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 24 (%33,3) kişinin bu bilgilerin ele geçirilebileceğini, 36 (%50) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 6 (%8,3) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 6 (%8,3) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.27. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 46
Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	28	38,9	38,9
	Kısmen	33	45,8	84,7
	Hayır	6	8,3	93,1
	Fikrim yok	5	6,9	100,0
	Toplam	72	100,0	



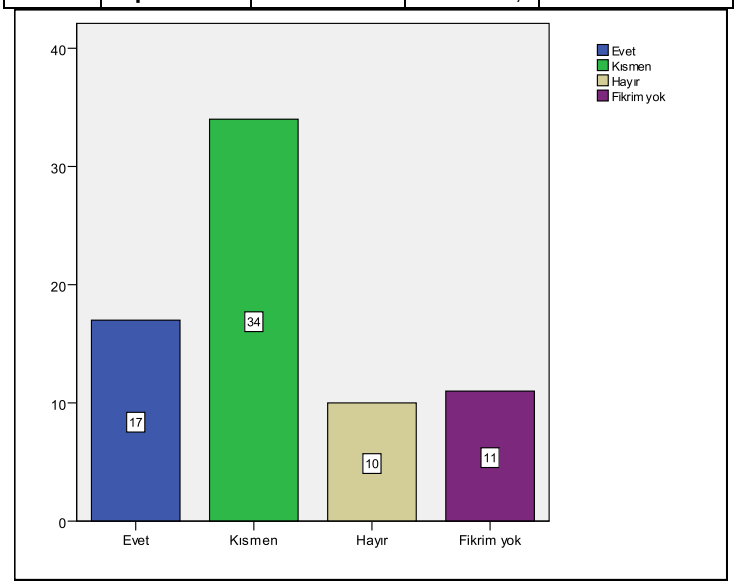
Şekil 84 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

Herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı o kurumda çalışanların özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 28 (%38,9) kişinin bu bilgilerin ele geçirilebileceğini, 33 (%45,8) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 6 (%8,3) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 5 (%6,9) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.28. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 47
Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	17	23,6	23,6
	Kısmen	34	47,2	70,8
	Hayır	10	13,9	84,7
	Fikrim yok	11	15,3	100,0
	Toplam	72	100,0	



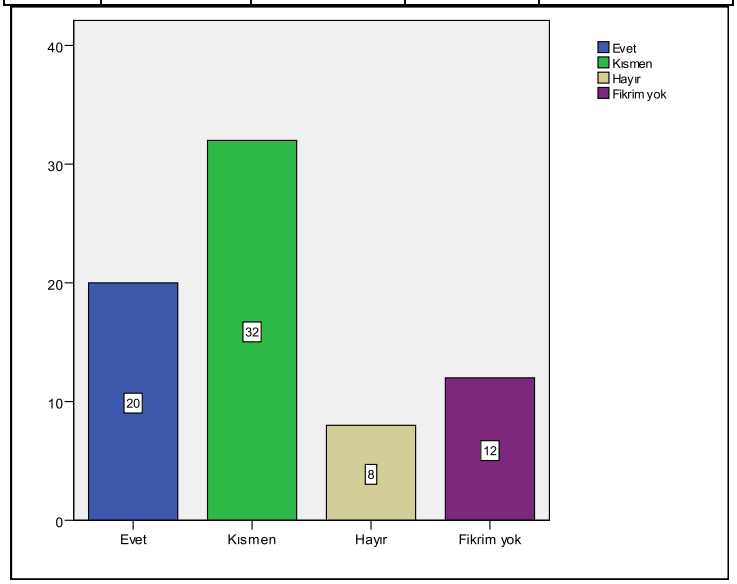
Şekil 85 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

Herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 17 (%23,6) kişinin bu bilgilerin ele geçirilebileceğini, 34 (%47,2) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 10 (%13,9) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 11 (%15,3) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.29. Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 48
Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	20	27,8	27,8
	Kısmen	32	44,4	72,2
	Hayır	8	11,1	83,3
	Fikrim yok	12	16,7	100,0
	Toplam	72	100,0	



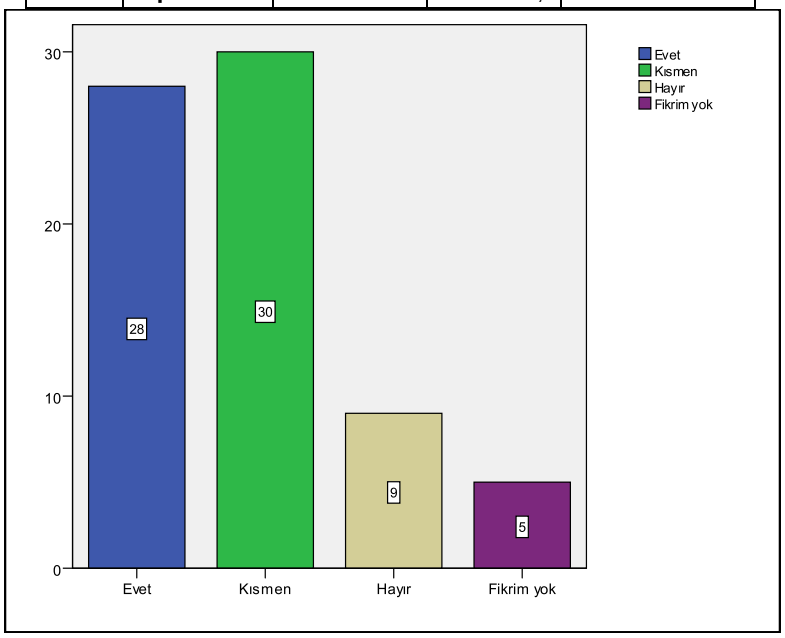
Şekil 86 : Herhangi Bir Kamu Sitesinden veya Kamu Sitelerinden Kaynaklı O Kurum ile İlgili Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

Herhangi bir kamu sitesinden veya kamu sitelerinden kaynaklı o kurum ile ilgili özel şirketlerin özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 20 (%27,8) kişinin bu bilgilerin ele geçirilebileceğini, 32 (%44,4) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 8 (%11,1) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 12 (%16,7) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.30. Özel Şirket Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 49
Özel Şirket Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum İle ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	28	38,9	38,9
	Kısmen	30	41,7	80,6
	Hayır	9	12,5	93,1
	Fikrim yok	5	6,9	100,0
	Toplam	72	100,0	



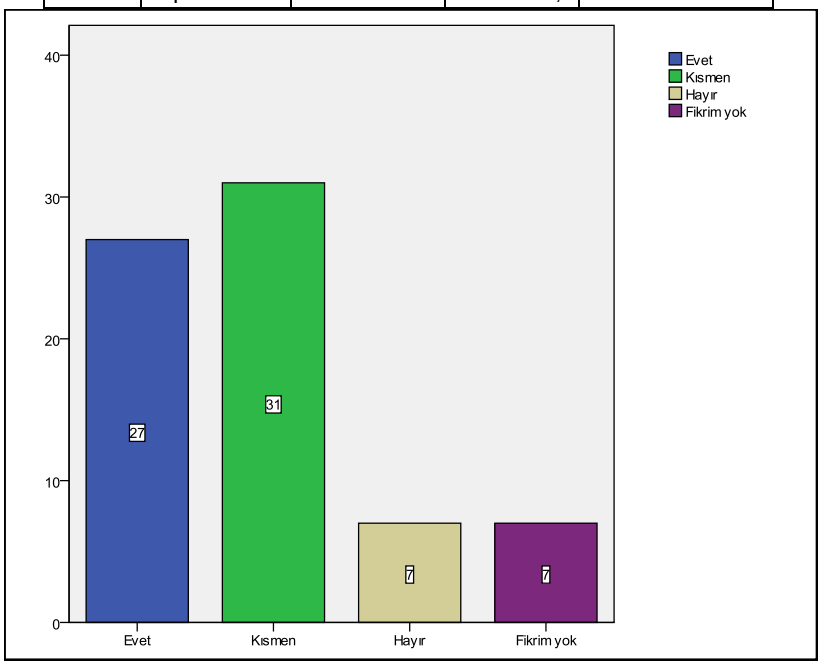
Şekil 87 : Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum ile ilgili Vatandaşların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

Özel şirket web sitelerinde ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 28 (%38,9) kişinin bu bilgilerin ele geçirilebileceğini, 30 (%41,7) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 9 (%12,5) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 5 (%6,9) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.31. Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 50
Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	27	37,5	37,5
	Kısmen	31	43,1	80,6
	Hayır	7	9,7	90,3
	Fikrim yok	7	9,7	100,0
	Toplam	72	100,0	



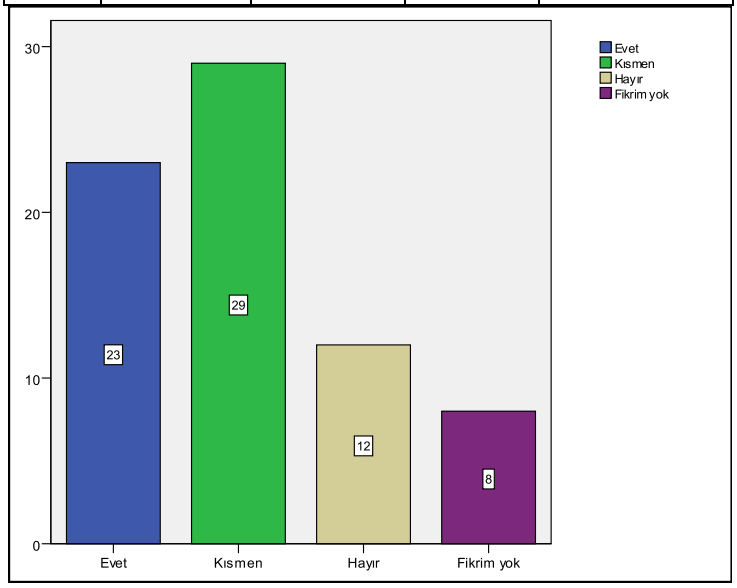
Şekil 88 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurumda Çalışanların Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Özel şirket web sitelerinde ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 27 (%37,5) kişinin bu bilgilerin ele geçirilebileceğini, 31 (%43,1) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 7 (%9,7) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 7 (%9,7) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.32. Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 51
Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	23	31,9	31,9
	Kısmen	29	40,3	72,2
	Hayır	12	16,7	88,9
	Fikrim yok	8	11,1	100,0
	Toplam	72	100,0	



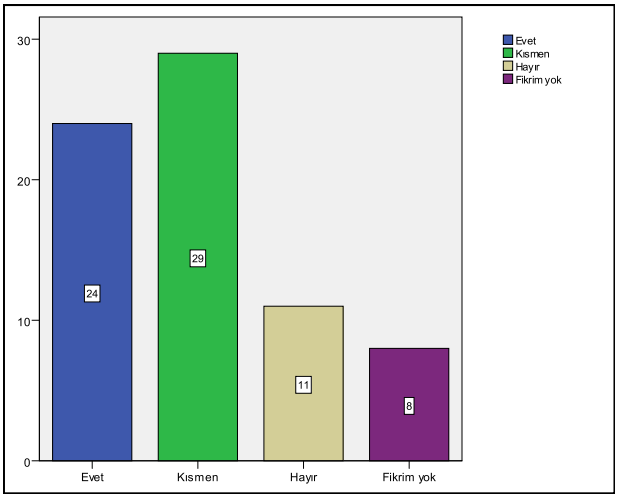
Şekil 89 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Kamu Kurumlarının Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterimi

Özel şirket web sitelerinde ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 23 (%31,9) kişinin bu bilgilerin ele geçirilebileceğini, 29 (%40,3) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 12 (%16,7) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 8 (%11,1) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

4.3.1.33. Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı O Kurum İle İlgili Diğer Özel Şirketlerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

Tablo 52
Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	24	33,3	33,3
	Kısmen	29	40,3	73,6
	Hayır	11	15,3	88,9
	Fikrim yok	8	11,1	100,0
	Toplam	72	100,0	



Şekil 90 : Özel Şirket Web Sitelerinde ya da Bu Sitelerden Kaynaklı O Kurum ile İlgili Diğer Özel Şirketlerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Dağılımı Tablosu – Grafiksel Gösterim

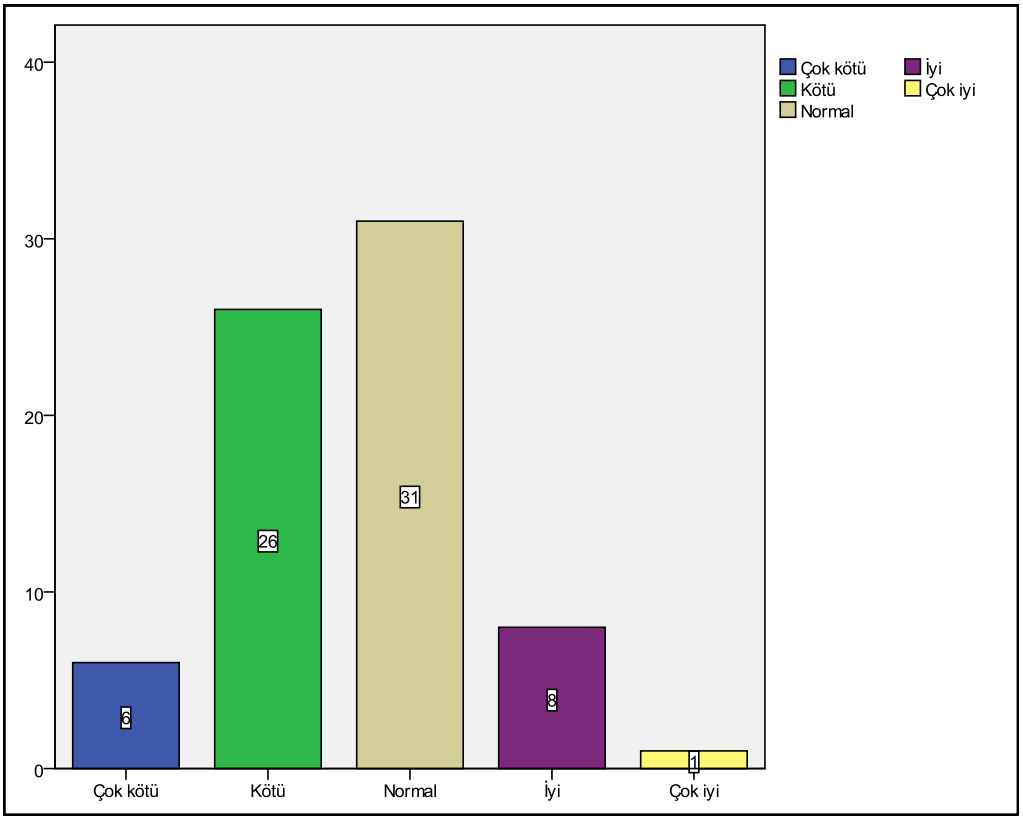
Özel şirket web sitelerinde ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel şirketlerin özel ve önemli bilgileri ele geçirilebilir mi dağılımı incelendiğinde, 24 (%33,3) kişinin bu bilgilerin ele geçirilebileceğini, 29 (%40,3) kişinin bu bilgilerin kısmen ele geçirilebileceğini, 11 (%15,3) kişinin bu bilgilerin ele geçilemeyeceğini düşünmekte oldukları, 8 (%11,1) kişinin ise bu konuda fikri olmadığı tespit edilmiştir. Görülmektedir ki, katılımcıların büyük bir kısmı, bu bilgilerin kısmen ya da tamamen ele geçirilebileceğini düşünmektedir.

Bahse konu siteleri, o kurum ile ilgili özel ya da tüzel kişiliklere ait özel bilgilerin ifşasına göre karşılaştırdığımızda ise, özel şirket web sitelerinden o kurum ile ilgililerin bilgilerinin ifşa edilebileceğini düşünenlerin oranı, kamu kurumları web sitelerinden bu bilgilerin ifşa edilebileceğini düşünenlerin 1,15 (89/102) katıdır. Bu bilgilerin kısmen ele geçirilebileceğini düşünenlerin oranı ise, kamu kurumları web sitelerinde daha yüksek çıkmaktadır. Bu bilgilerin kamu kurumlarına ait web sitelerinden kısmen elde edilebileceğini düşünenlerin oranı, bu bilgilerin özel şirket web sitelerinden kısmen elde edilebileceğini düşünenlerin (1,13) (135/119) katıdır.

4.3.1.34. Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı

Tablo 53
Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Çok kötü	6	8,3	8,3
	Kötü	26	36,1	44,4
	Normal	31	43,1	87,5
	İyi	8	11,1	98,6
	Çok iyi	1	1,4	100,0
	Toplam	72	100,0	



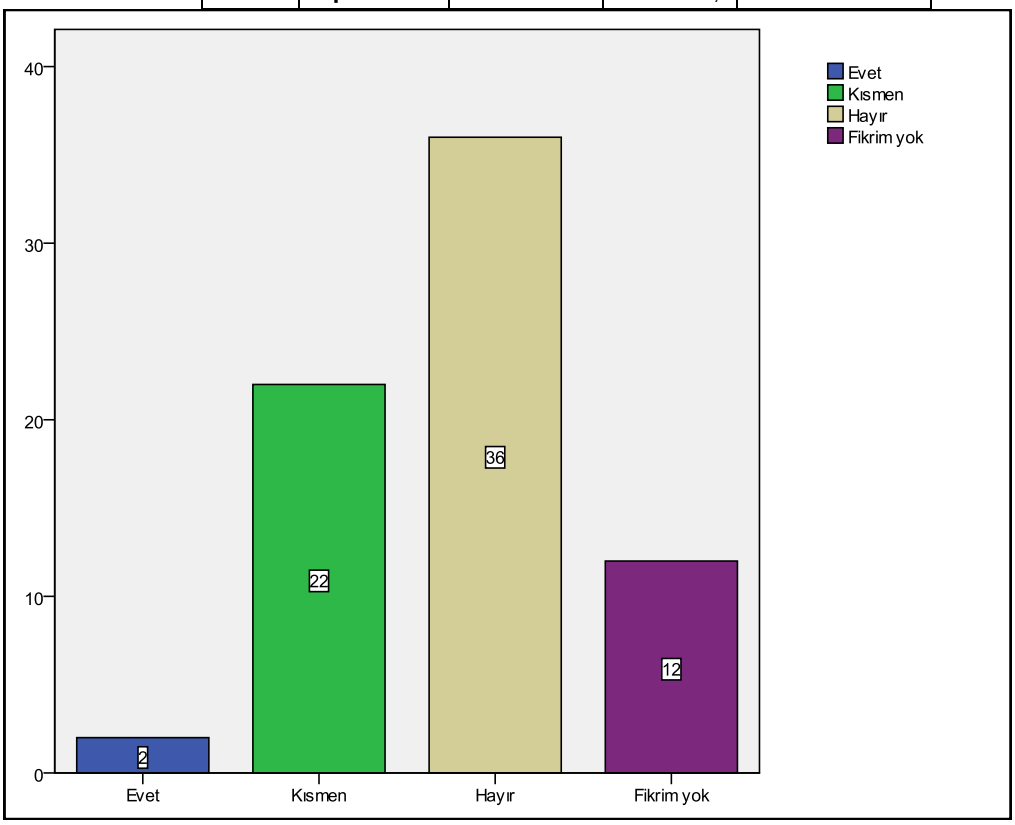
Şekil 91 : Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Dağılımı Tablosu – Grafiksel Gösterim

Kamu kurumlarına ait web sitelerinin güvenlik seviyeleri değerlendirildiğinde, katılımcıların 6'sının (%8,3) kamu kurumlarına ait web sitelerinin güvenliklerinin çok kötü olduğunu, 26'sı (%36,1) kötü olduğunu, 31'i (%43,1) normal olduğunu, 8'i (%11,1) iyi olduğunu, 1'i (%1,4) ise çok iyi olduğunu düşünmekte olduğu tespit edilmiştir. Görülmektedir ki, kamu kurumlarına ait web sitelerinin güvenlik seviyeleri genel olarak normal ve daha kötü olarak düşünülmektedir.

4.3.1.35. Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı

Tablo 54
Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	2	2,8	2,8
	Kısmen	22	30,6	33,3
	Hayır	36	50,0	83,3
	Fikrim yok	12	16,7	100,0
	Toplam	72	100,0	



Şekil 92 : Kamu Kurumlarına Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı Tablosu – Grafiksel Gösterim

Kamu kurumlarına ait web sitelerinin güvenlik seviyeleri genel olarak aynı mıdır dağılımı incelendiğinde, katılımcıların 2'si (%2,8) aynı olduğunu, 22'si (%30,6) kısmen aynı olduğunu, 36'sı (%50) aynı olmadığını düşündükleri, 12'sinin (%16,7) ise konu hakkında fikri olmadığı anlaşılmıştır. Görülmektedir ki, kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin genel olarak aynı olmadığı, değişkenlik gösterdiği

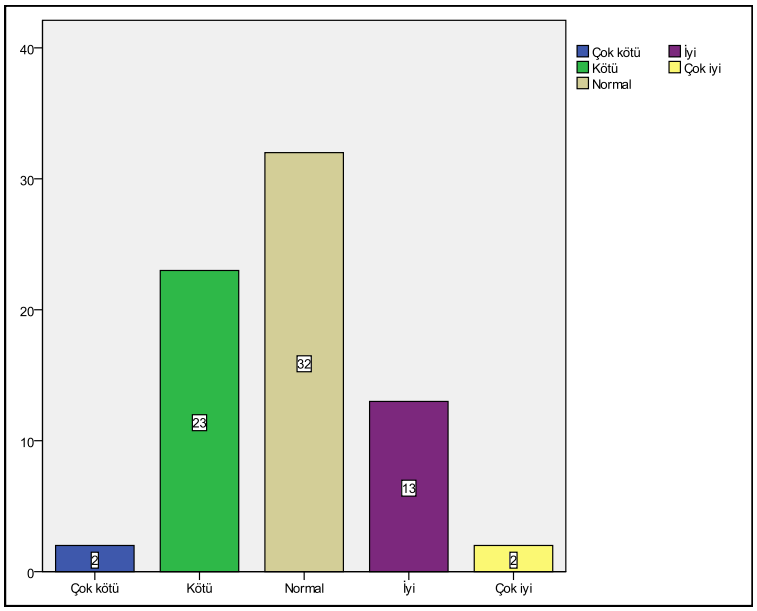
düşünülmekle birlikte, kısmen aynı olduğunu düşünenlerin oranının da azımsanmayacak seviyede olduğu düşünülmektedir.

Kamu kurumlarına ait web sitelerini uğranan zarar miktarlarına ve güvenlik seviyelerine göre karşılaştırdığımızda, kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin genel olarak normal ve daha kötü olarak düşünüldüğü ve bu seviyenin de tüm kamu sitelerinde aynı oranda olmadığı, kurumdan kuruma farklılık gösterdiği görülmektedir.

4.3.1.36. Özel Şirketlere Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı

Tablo 55
Özel Şirketlere Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Çok kötü	2	2,8	2,8
	Kötü	23	31,9	34,7
	Normal	32	44,4	79,2
	İyi	13	18,1	97,2
	Çok iyi	2	2,8	100,0
	Toplam	72	100,0	



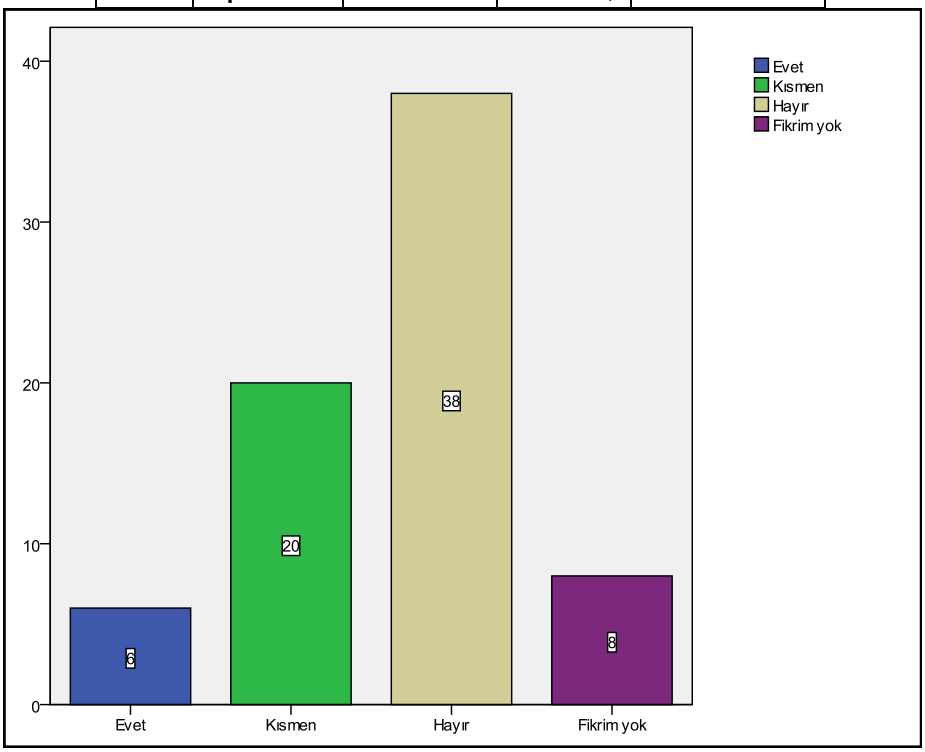
Şekil 93 : Özel Şirketlere Ait Web Sitelerinin Güvenlik Durumları Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim

Özel şirketlere ait web sitelerinin güvenlik seviyeleri değerlendirildiğinde, katılımcıların 2'sinin (%2,8) özel şirketlere ait web sitelerinin güvenliklerinin çok kötü olduğunu, 23'ünün (%31,9) kötü olduğunu, 32'sinin (%44,4) normal olduğunu, 13'ünün (%18,1) iyi olduğunu, 2'sinin (%2,8) ise çok iyi olduğunu düşünmekte olduğu tespit edilmiştir. Görülmektedir ki, özel şirketlere ait web sitelerinin güvenlik seviyeleri genel olarak normal, kötü ve iyi olarak düşünülmektedir.

4.3.1.37. Özel Şirketlere Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı mıdır Dağılımı

Tablo 56
Özel Şirketlere Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı Mıdır Dağılımı

		Frekans	Yüzde	Toplam Yüzde
	Evet	6	8,3	8,3
	Kısmen	20	27,8	36,1
	Hayır	38	52,8	88,9
	Fikrim yok	8	11,1	100,0
	Toplam	72	100,0	



Şekil 94 : Özel Şirketlere Ait Web Sitelerinin Güvenlik Seviyeleri Genel Olarak Aynı Mıdır Dağılımı Tablosu – Grafiksel Gösterim

Özel şirketlere ait web sitelerinin güvenlik seviyeleri genel olarak aynı mıdır dağılımı incelendiğinde, katılımcıların 6'sı (%8,3) aynı olduğunu, 20'si (%27,8) kısmen aynı olduğunu, 38'i (%52,8) aynı olmadığını düşündükleri, 8'inin (%11,1) ise konu hakkında fikri olmadığı anlaşılmıştır. Görülmektedir ki, özel şirketlere ait web sitelerinin güvenlik seviyelerinin genel olarak aynı olmadığı, değişkenlik gösterdiği düşünülmekle birlikte, kısmen aynı olduğunu düşünenlerin oranının da azımsanmayacak seviyededir.

4.3.2. Analizler

4.3.2.1. Demografik Kriterlere Göre Sorulara Verilen Yanıtlar Analizleri

Demografik kriterlerin ve kategprik değerlerin kategorileri arasında anket sorularına verilen cevaplar bakımından anlamlı fark olup olmadığını tespit edebilmek için 2 ve K independent Samples testleri yapılmıştır. Anket içerisinde yer alan sıralı ölçekli sorular arasında anlamlı bir ilişki olup olmadığını anlamak için korelasyon testleri yapılmıştır. Adet içeren sorular ile ilişkisel değerlendirmeler yapmak için ise Anova ve T testleri yapılmıştır.

Uygulanan testlerde yer alan p (Sig.) değerleri aşağıdaki kriterlere göre değerlendirilerek kategori ortalamalarının arasındaki Anlamsız Fark'dan Çok Anlamlı Fark'a doğru dört farklı derecelendirme yoluna gidilmiştir.

Tablo 57
Renk Değerleri Tablosu

1	>	p	>	0,1	Anlamsız
0,1	>	p	>	0,05	Az Anlamlı
0,05	>	p	>	0,01	Anlamlı
0,01	>	p	>	0	Çok Anlamlı

Bu derecelendirme sonucunda aşağıda yer alan testler içerisinde p değeri "Anlamsız" çıkanlar dışındakilerin detayına girilmiştir.

4.3.2.1.1. Cinsiyet Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 2'ye bakınız.)

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - E-ticaret Siteleri

Bu soruya verilen cevaplar neticesinde, erkek katılımcıların bu siteleri kadın katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 2'ye bakınız):

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - E-bankacılık Siteleri

Bu soruya verilen cevaplar neticesinde, erkek katılımcıların bu siteleri kadın katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

  - E-bilet Siteleri

Bu soruya verilen cevaplar neticesinde, erkek katılımcıların bu siteleri kadın katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin cinsiyete göre farklılık göstermediği tespit edilmiştir.

- www.turkiye.gov.tr sitesi hakkında bilgi sahibi olma,
- www.turkiye.gov.tr sitesini ziyaret sıklığı,
- Kamu kurumlarına ait web sitelerinin içerik ve tasarım açısından beğenilmesi,
- Web sitelerinin güvenlik durumları değerlendirmesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanım sıklığı.

4.3.2.1.2. Öğrenim Durumu Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 3'e bakınız)

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - www.egm.gov.tr

Bu soruya verilen cevaplar neticesinde, lisans mezunu katılımcıların bu siteleri lise ya da yüksek lisans mezunu katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 3'e bakınız)

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - www.tarim.gov.tr
  - www.mit.gov.tr
  - www.istanbul.pol.tr
  - www.nvi.gov.tr

Bu soruya verilen cevaplar neticesinde, lisans mezunu katılımcıların bu siteleri lise ya da yüksek lisans mezunu katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin öğrenim durumuna göre farklılık göstermediği tespit edilmiştir.

- www.turkiye.gov.tr sitesini ziyaret sıklığı,
- Kamu kurumlarına ait web sitelerinin içerik ve tasarım açısından beğenilmesi,
- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı
- Sitelerde bulunan zafiyet sayıları

4.3.2.1.3. Kişisel Web Sayfasına Sahip Olma Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 4'e bakınız)

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - www.disisleri.gov.tr
  - www.mit.gov.tr

Bu soruya verilen cevaplar neticesinde, kişisel web sitesine sahip olmayan katılımcıların bu siteleri kişisel web sitesine sahip olan katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 4'e bakınız):

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5
    - www.icisleri.gov.tr

Bu soruya verilen cevaplar neticesinde, kişisel web sitesine sahip olmayan katılımcıların bu siteleri kişisel web sitesine sahip olan katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- 24. Soru: Genel olarak kamu kurumlarına ait web sitelerini içerik açısından beğeniyor musunuz?

Bu soruya verilen cevaplar neticesinde, kişisel web sitesine sahip olan katılımcıların kamu kurumlarına ait web sitelerini kişisel web sitesine sahip olmayan katılımcılara nazaran içeriksel olarak daha çok beğendikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kişisel web sayfasına sahip olmaya göre farklılık göstermediği tespit edilmiştir.

- www.turkiye.gov.tr sitesi hakkında bilgi sahibi olma,
- www.turkiye.gov.tr sitesini ziyaret sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Sitede bulunan zafiyet sayıları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı.

4.3.2.1.4. Çalışma ve Çalışılan Kurum Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 5'e bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, özelleştirilmiş şirket çalışanı olan katılımcıların kamu kurumlarına ait web sitelerinin güvenlik durumlarını kamu kurumu ya da özel şirket çalışanı olan katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

- **Güvenlik Taraması: Orta Risk Seviyesine Sahip Zafiyet Tespiti**

Yapılan inceleme neticesinde, en fazla orta seviye güvenlik zafiyeti bulunma oranının özelleştirilmiş şirket web sitelerinde mevcut olduğu, en az orta seviye güvenlik zafiyeti bulunma oranının ise kamu kurumlarına ait web sitelerinde mevcut olduğu tespit edilmiştir.

- **Güvenlik Taraması: Düşük Risk Seviyesine Sahip Zafiyet Tespiti**

Yapılan inceleme neticesinde, en fazla düşük seviye güvenlik zafiyeti bulunma oranının özel şirket web sitelerinde mevcut olduğu, en az orta seviye güvenlik zafiyeti bulunma oranının ise kamu kurumlarına ait web sitelerinde mevcut olduğu tespit edilmiştir.

- **Güvenlik Taraması: Toplam Risk Seviyesine Sahip Zafiyet Tespiti**

Yapılan inceleme neticesinde, en fazla toplam güvenlik zafiyetinin özel şirket web sitelerinde mevcut olduğu, en az toplam seviye güvenlik zafiyetinin ise kamu kurumlarına ait web sitelerinde mevcut olduğu tespit edilmiştir.

2) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 5'e bakınız):

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5

    - www.adalet.gov.tr
    - www.msb.gov.tr
    - www.disisleri.gov.tr
    - www.bayindirlik.gov.tr
    - www.saglik.gov.tr
    - www.tarim.gov.tr
    - www.calisma.gov.tr
    - www.istanbul.pol.tr
    - www.nvi.gov.tr

Bu soruya verilen cevaplar neticesinde, özelleştirilmiş şirket çalışanı olan katılımcıların bu siteleri kamu ve özel şirket çalışanı olan katılımcılara nazaran daha güvenlik buldukları tespit edilmiştir.

3) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 5'e bakınız)

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5

    - www.basbakanlik.gov.tr
    - www.icisleri.gov.tr
    - www.maliye.gov.tr
    - www.meb.gov.tr
    - www.ubak.gov.tr
    - www.mit.gov.tr
    - www.egm.gov.tr
    - www.kgm.gov.tr
    - www.sgk.gov.tr

Bu soruya verilen cevaplar neticesinde, özelleştirilmiş şirket çalışanı olan katılımcıların bu siteleri kamu ve özel şirket çalışanlarına nazaran daha güvenlik buldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kamu kurumu çalışanı olan katılımcıların kamu kurumlarına ait web sitelerini özel şirket ve özelleştirilmiş şirket çalışanı olan katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş ve işlemlerin özel şirket ya da kamu kurumuna göre farklılık göstermediği tespit edilmiştir.

- www.turkiye.gov.tr sitesi hakkında bilgi sahibi olma,
- www.turkiye.gov.tr sitesini ziyaret sıklığı,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini hazırlayan personel sayısı ve bu personellerin sertifikasyon durumları
- Web sitelerinin güvenliği ile ilgilenen personel sayısı ve bu personellerin sertifikasyon durumları
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı

4.3.2.2. Kategorik Kriterlere Göre Sorulara Verilen Yanıtlar Analizi

4.3.2.2.1. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi

a) Uygulama tabanlı güvenlik duvarı (Ek Tablo 6'ya bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- **Güvenlik Taraması: Kritik Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar neticesinde, uygulama tabanlı güvenlik duvarı **kullanmayan** katılımcıların sitelerinde, kullanan katılımcıların sitelerine nazaran daha fazla kritik risk seviyesine sahip zafiyet bulunduğu tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- **Güvenlik Taraması: Yüksek Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar neticesinde, uygulama tabanlı güvenlik duvarı **kullanmayan** katılımcıların sitelerinde kullanan katılımcıların sitelerine nazaran daha fazla yüksek risk seviyesine sahip zafiyet bulunduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin uygulama tabanlı güvenlik duvarı kullanmaya göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı.

b) Servis tabanlı IPS (Ek Tablo 7'ye bakınız.)

1) Az Anlamlı fark bulunan karşılaştırmalar

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, servis tabanlı IPS kullanan katılımcıların, kamu kurumlarına ait web sitelerinin güvenliği kullanmayan katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin servis tabanlı IPS kullanmaya göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Sitede bulunan zafiyet sayıları.

c) Düzenli kurumca yapılan güvenlik taraması sonuçları değerlendirmeleri (Ek Tablo 8'e bakınız.)

1) Az Anlamlı fark bulunan karşılaştırmalar:

- 14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?

Bu soruya verilen cevaplar neticesinde, düzenli kurumca yapılan güvenlik taraması metodu kullanmayan katılımcıların sitelerinin güvenliği için ayırdıkları ödenek miktarının kullanan katılımcıların ayırdığı ödenek miktarına nazaran daha yüksek oranda olduğunu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumca yapılan düzenli güvenlik taramasına göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Sitede bulunan zafiyet sayıları.

d) Düzenli yedekleme (Ek Tablo 9'a bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- 14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?

Bu soruya verilen cevaplar neticesinde, düzenli yedekleme kullanmayan katılımcıların, sitelerinin güvenliği için ayırdıkları ödenek miktarının kullanan katılımcıların ayırdığı ödenek miktarına nazaran daha yüksek oranda olduğunu tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- Güvenlik Taraması: Yüksek Risk Seviyesine Sahip Zafiyet Tespiti

Bu soruya verilen cevaplar neticesinde, düzenli yedekleme **kullanan** katılımcıların sitelerinde, kullanmayan katılımcıların sitelerine nazaran daha fazla yüksek risk seviyesine sahip zafiyet bulunduğu tespit edilmiştir.

- Güvenlik Taraması: Orta Risk Seviyesine Sahip Zafiyet Tespiti

Bu soruya verilen cevaplar neticesinde, düzenli yedekleme **kullanan** katılımcıların sitelerinde kullanmayan katılımcıların sitelerine nazaran daha fazla orta risk seviyesine sahip zafiyet bulunduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin düzenli yedeklemeye göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı.

e) Diğer (Ek Tablo 10'a bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- 14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?

Bu soruya verilen cevaplar neticesinde, diğer güvenlik önlemlerini kullanan katılımcıların, sitelerinin güvenliği için ayırdıkları ödenek miktarının, kullanmayan katılımcıların ayırdığı ödenek miktarına nazaran daha yüksek oranda olduğunu tespit edilmiştir.

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, diğer güvenlik önlemlerini kullanan katılımcıların kamu kurumlarına ait web sitelerini kullanmayan katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin diğer yöntemlere göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin güvenlik durumları düşüncesi,
- Sitede bulunan zafiyet sayıları,

4.3.2.2.2. Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 11'e bakınız)

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5
  - www.basbakanlik.gov.tr

Bu soruya verilen cevaplar neticesinde, Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden Ve Ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara uğramayanların, bu siteyi, uğrayanlara nazaran daha güvenli buldukları tespit edilmiştir.

- **Güvenlik Taraması: Orta Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar neticesinde, Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden Ve Ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara uğrayanların, kurumsal web sitelerinde, uğramayanların kurumsal web sitelerine nazaran daha fazla orta risk seviyesine sahip güvenlik zafiyeti bulunduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin daha önce hiç herhangi bir kamu kurumuna ait web sitesinden ve ya bu sitelerden kaynaklı herhangi bir maddi zarara uğramaya göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi.

4.3.2.2.3. Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 12'ye bakınız)

- **Güvenlik Taraması: Orta Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar neticesinde, daha önce hiç herhangi bir kamu kurumuna ait web sitesinden ve ya bu sitelerden kaynaklı herhangi bir manevi zarara uğrayanların kurumsal web sitelerinde, uğramayanların kurumsal web sitelerine nazaran daha fazla orta risk seviyesine sahip güvenlik zafiyeti bulunduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin daha önce hiç herhangi bir kamu kurumuna ait web sitesinden ve ya bu sitelerden kaynaklı herhangi bir manevi zarara uğramaya göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı

4.3.2.2.4. Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 13'e bakınız)

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
  - Haber Siteleri

Bu soruya verilen cevaplar neticesinde, herhangi bir özel şirkete ait web sitesinden ve ya bu sitelerden kaynaklı herhangi bir maddi zarara uğramayanların, bu siteyi, uğrayanlara nazaran daha güvenli buldukları tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin daha önce hiç herhangi bir özel şirket web sitesinden ve ya bu sitelerden kaynaklı herhangi bir maddi zarara uğramaya göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

4.3.2.2.5. Kurum / Kuruluşun Web Siteleri Üzerinden Online İşlem Sunup Sunmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 14'e bakınız):

- **9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?**

Bu soruya verilen cevaplar neticesinde, Kurum / Kuruluşun Web Siteleri Üzerinden Online hizmet sunan kurumların, kurumsal web sitelerini hazırlayan personel sayılarının, sunmayan kurumlara nazaran daha fazla olduğu tespit edilmiştir.

- **11. Soru: Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin sayısı nedir?**

Bu soruya verilen cevaplar neticesinde, Kurum / Kuruluşun Web Siteleri Üzerinden Online hizmet sunan kurumların, kurumsal web sitelerinin güvenliği ile ilgilenen personel sayılarının, sunmayan kurumlara nazaran daha fazla olduğu tespit edilmiştir.

- **23. Soru: Kurumunuzun şu anda hizmet veren web sayfasının hazırlanması ve yayınlanması aşağıdaki durumların hangisinde ifade edilmektedir işaretleyiniz?**

Bu soruya verilen cevaplar neticesinde, Kurum / Kuruluşun Web Siteleri Üzerinden Online hizmet sunmayan kurumların, kurumsal web sitelerini, sunmayan kurumlara nazaran daha fazla dış kaynaklarda yayınladıkları, online işlem sunan kurumların ise iç kaynaklarla yayınlamayı tercih ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurum / kuruluşun web siteleri üzerinden online sunup sunmama kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Sitede bulunan zafiyet sayıları.

4.3.2.2.6. Kamu Ve Özel Şirket Web Sitelerinin Karşılaştırılmasına Göre Sorulara Verilen Yanıtlar Analizi

a) **Kamu Kurumları Web Sitelerinden Ya Da Bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Vatandaşların, Ek Tablo 15'e bakınız.)**

1) Anlamlı fark bulunan karşılaştırmalar:

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**

  - www.basbakanlik.gov.tr
  - www.msb.gov.tr
  - www.meb.gov.tr
  - www.bayindirlik.gov.tr
  - www.saglik.gov.tr
  - www.ubak.gov.tr

- www.calisma.gov.tr
- www.kgm.gov.tr
- www.sgk.gov.tr
- www.nvi.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünenlerin, bu siteleri, bu bilgilerin tamamen ya da kısmen ele geçirilebileceğini düşünenlere nazaran daha güvenli buldukları tespit edilmiştir.

- Oyun Siteleri

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği konusunda fikri olmayan katılımcıların, bu siteyi, bu bilgilerin tamamen ya da kısmen ele geçirilebileceğini ya da geçirilemeyeceğini düşünen katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerinin güvenlik durumlarının, diğer katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, özel şirketlere ait web sitelerinin güvenlik durumlarının, diğer katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili

vatandaşların özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- 21. Soru: 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesi hakkında bilginiz var mı?

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların, www.turkiye.gov.tr sitesi hakkına diğer katılımcılara nazaran daha az bilgi sahibi oldukları tespit edilmiştir.

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5
  - www.adalet.gov.tr
  - www.disisleri.gov.tr
  - www.mit.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteleri, bu bilgilerin tamamen ya da kısmen ele geçirilebileceğini ya da geçirilemeyeceğini düşünen katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5
  - www.tarim.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların, bu siteyi, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerini diğer kullanıcılara rağmen daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgililerin vatandaşların özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Kamu kurumlarına ait web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

b) Kamu Kurumları Web Sitelerinden Ya Da Bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Kurum Çalışanlarının, Ek Tablo 15'e bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**
    - E-Bankacılık Siteleri

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum çalışanlarının özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- 21. Soru: 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesi hakkında bilginiz var mı?

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum çalışanlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların, www.turkiye.gov.tr sitesi hakkına diğer katılımcılara nazaran daha az bilgi sahibi oldukları tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum çalışanlarının özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Kamu kurumlarına ait web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Kamu kurumlarına ait web sitelerinin güvenlik durumları düşüncesi.
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

c) Kamu Kurumları Web Sitelerinde Ya Da Bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Diğer Kamu Kurumlarının, Ek Tablo 15'e bakınız.)

1) Çok Anlamlı fark bulunan karşılaştırmalar:

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5
    - www.basbakanlik.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteyi, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- www.bayindirlik.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceğini hakkında fikri olmayan katılımcıların, bu siteyi, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Anlamlı fark bulunan karşılaştırmalar:

- **14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan kurumların, kurumlarına ait web sitelerinin güvenliği ile ilgili ödenek miktarların diğer kurumlara nazaran daha fazla olduğu tespit edilmiştir.

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**

  - www.msb.gov.tr
  - www.ubak.gov.tr
  - www.calisma.gov.tr
  - www.sgk.gov.tr
  - www.nvi.gov.tr
  - E-bilet
  - E-Topluluk

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

  - www.disisleri.gov.tr
  - www.egm.gov.tr
  - www.istanbul.pol.tr
  - www.kgm.gov.tr

- E-Bankacılık
- E-Ticaret

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

3) Az Anlamlı fark bulunan karşılaştırmalar:

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**

  - www.adalet.gov.tr
  - www.icisleri.gov.tr
  - Portal Siteleri

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceğini hakkında fikri olmayan katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

  - www.mit.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, özel şirketlere ait web sitelerinin güvenlik durumlarının, diğer katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerini diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı diğer kamu kurumlarının özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

d) Kamu Kurumları Web Sitelerinde Ya Da Bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Diğer Özel Kurumların, Ek Tablo 15'e bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- **25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5**

  - www.basbakanlik.gov.tr
  - www.msb.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel kurumların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceğini

hakkında fikri olmayan katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- 10. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin bu konuda herhangi bir sertifikasyonu var mı? (eğitim değil sertifikasyon sorulmaktadır.)

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel kurumların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceğini hakkında fikri olmayan katılımcıların kurumlarının, kurumlarına ait web sitelerini hazırlayan sertifikalı personel sayılarının, diğer katılımcılara nazaran daha az olduğu tespit edilmiştir.

- 25. Soru: Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız. Çok Güvensiz: 1, Çok Güvenli: 5

  - www.ubak.gov.tr
  - www.calisma.gov.tr
  - www.mit.gov.tr
  - www.kgm.gov.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel kurumların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

  - www.istanbul.pol.tr

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel kurumların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların, bu siteleri, diğer katılımcılara nazaran daha güvenli buldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel kurumların özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerini diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kamu kurumları web sitelerinden ya da bu sitelerden kaynaklı diğer özel kurumların özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumları düşüncesi.
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

e) Özel Şirket Web Sitelerinden ya da bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Vatandaşların, Ek Tablo 16'ya bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- **14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların kurumlarının, web siteleri için ayırdıkları ödenek miktarlarının, diğer katılımcılara nazaran daha yüksek olduğu tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgilerinin ele geçirilemeyeceğini düşünen katılımcıların özel şirketlere ait web sitelerinin güvenlik durumlarının, diğer katılımcılara nazaran daha iyi olduğunu düşündükleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin özel şirket web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili vatandaşların özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin yayınlanma durumları,
- Web sitelerinin güvenlik durumları düşüncesi.
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

f) Özel Şirket Web Sitelerinden ya da bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Diğer Kamu Kurumlarının, Ek Tablo 16'ya bakınız.)

1) Anlamlı fark bulunan karşılaştırmalar:

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerini, diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen diğer cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, özel kurumlara ait web sitelerini, diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- 14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer kamu kurumlarının özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların kurumlarının, kurumlarına ait web sitelerinin güvenliği için ayırdıkları ödeneğin, toplam ödenek miktarına oranının, diğer katılımcılara nazaran daha yüksek olduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin özel şirket web sitelerinden ya da bu sitelerden kaynaklı kamu kurumlarının özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumları düşüncesi,
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

g) Özel Şirket Web Sitelerinden ya da bu Sitelerden Kaynaklı O Kurum İle İlgililerin Özel Ve Önemli Bilgileri Ele Geçirilebilir Mi? (Diğer Özel Şirketlerin, Ek Tablo 16'ya bakınız)

1) Anlamlı fark bulunan karşılaştırmalar:

- 21. Soru: 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesi hakkında bilginiz var mı?

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel şirketlerin özel ve önemli bilgilerinin kısmen ele geçirilebileceğini düşünen katılımcıların, www.turkiye.gov.tr sitesi hakkında, diğer katılımcılara nazaran daha az bilgiye sahip oldukları tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel şirketlerin özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, kamu kurumlarına ait web sitelerini, diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel şirketlerin özel ve önemli bilgilerinin ele geçirilebileceğini düşünen katılımcıların, özel şirketlere ait web sitelerini, diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar:

- **14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?**

Bu soruya verilen cevaplar incelendiğinde, özel şirketlere ait web sitelerinden ya da bu sitelerden kaynaklı o kurum ile ilgili diğer özel şirketlerin özel ve önemli bilgilerinin ele geçirilip geçirilemeyeceği hakkında fikri olmayan katılımcıların kurumlarının, kurumlarına ait web sitelerinin güvenliği için ayırdıkları ödeneğin, toplam ödenek miktarına oranının, diğer katılımcılara nazaran daha yüksek olduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin özel şirket web sitelerinden ya da bu sitelerden kaynaklı diğer özel şirketlerin özel ve önemli bilgileri ele geçirilebilir mi kriterine göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumları düşüncesi,
- Kurumların kurumsal web sitelerindeki zafiyet sayısı

4.3.2.2.7. Kurumların, Kurumlarına Ait Web Sitesi İle İlgili Güvenlik Ödenek Kalemi Belirleme Yöntemi Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 19'a bakınız)

- **14. Soru: Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?**

Bu soruya verilen cevaplar neticesinde, 4 – 6 ay önceden ödenek kalemlerini belirleyen ve fiyat araştırması yaparak ödenek belirlenmeye çalışan kurumların, kurumsal web sitelerinin güvenlikleri için ayırdıkları ödenek miktarlarının, diğer yöntemleri kullanan kurumların ödenek miktarlarına nazaran daha yüksek olduğu tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 19'a bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumlarının web sitelerinin güvenliği için ayrılacak ödenek kalemlerinin nasıl belirlendiği bilmeyen katılımcıların, kamu kurumlarına ait web sitelerini geri kalan yöntemleri kullanan kurumlara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumlarının web sitelerinin güvenliği için ayrılacak ödenek kalemlerinin belirlenmesi için diğer yöntemleri kullanan kurumların, özel şirketlere ait web sitelerini geri kalan yöntemleri kullanan kurumlara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumların, kurumlarına ait web sitesi ile ilgili güvenlik ödenek kalemi belirleme yöntemine göre farklılık göstermediği tespit edilmiştir.

- Sitede bulunan zafiyet sayıları,
- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,

- Web sitelerinin güvenlik durumları düşüncesi,

4.3.2.2.8. Herhangi Bir Online Bankacılık Hizmeti Üyeliği Kullanma Ya Da Kullandırma Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 20'ye bakınız)

- **22. Soru: 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesini ziyaret sıklığınız nedir?**

Bu soruya verilen cevaplar incelendiğinde, herhangi bir online bankacılık hizmeti üyeliği kullanan ya da kullandırtan kişilerin, www.turkiye.gov.tr sitesini, diğer katılımcılara nazaran daha sık ziyaret ettikleri tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 20'ye bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar incelendiğinde, herhangi bir online bankacılık hizmeti üyeliği kullanan ya da kullandırtan kişilerin, özel şirketlere ait web sitelerini, diğer katılımcılara rağmen daha sık ziyaret ettikleri tespit edilmiştir.

- **9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?**

Bu soruya verilen cevaplar incelendiğinde, herhangi bir online bankacılık hizmeti üyeliği kullanan ya da kullandırtan kişilerin kurumlarına ait web sitelerini hazırlayan personel sayısının, diğer katılımcılara nazaran daha fazla olduğu tespit edilmiştir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kişilerin herhangi bir online bankacılık hizmeti üyeliği kullanma ya da kullandırmasına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurumların web sitelerinin güvenliğini sağlamak için ayırdıkların ödenek miktarının, toplam harcama ödenek miktarlarına oranı

- www.turkiye.gov.tr web sitesi hakkında bilgi sahibi olma
- Kamu kurumlarına ait web sitelerini içeriksek ya da tasarımsal olarak beğenme
- Web sitelerinin güvenlik durumları düşüncesi,

4.3.2.3. Ölçekli Soru Türlerine Göre Verilen Yanıtlar Analizi

4.3.2.3.1. Yaş Kriterine Göre Sorulara Verilen Yanıtlar Analizi

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yaşa göre farklılık göstermediği tespit edilmiştir.**(Ek Tablo 21'e bakınız)**

- www.turkiye.gov.tr sitesi hakkında bilgi sahibi olma,
- www.turkiye.gov.tr sitesini ziyaret sıklığı,
- Kamu kurumlarına ait web sitelerini içerik ve tasarım açısından beğenme,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.2. Web Sayfalarını Hazırlayan ya da Yardımcı Olan Kurum Personel ya da Personellerinin Sayısı Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 22'ye bakınız)

- **11. Soru: Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin sayısı nedir?**

Bu soruya verilen cevaplar neticesinde, web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı ile web sitelerinin güvenliği ile ilgilenen personel sayıları arasında doğru orantı olduğu, hazırlayan personel sayısı arttıkça güvenlik personel sayısının da arttığı tespit edilmiştir.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 22'ye bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı ile özel şirketlerin web sitelerini ziyaret sıklığı arasında ters orantı olduğu, hazırlayan personel sayısı arttıkça, özel şirket web sitelerini ziyaret sıklığının

azaldığı tespit edilmiştir. Hazırlayan personel sayısı arttığında özel şirket web sitelerinin daha az ziyaret edildiği görülmektedir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personellerin sertifikasyon durumları,
- Web sitelerinin güvenlik durumları düşüncesi

4.3.2.3.3. Kurumun Şu Anda Hizmet Veren Web Sayfasının Hazırlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 23'e bakınız)

- **23. Soru: Kurumunuzun şu anda hizmet veren web sayfasının hazırlanması ve yayınlanması aşağıdaki durumların hangisinde ifade edilmektedir işaretleyiniz?**

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin hazırlanma yöntemleri ile bu web sitelerinin yayınlanma yöntemleri arasında doğru orantı olduğu tespit edilmiştir. Sitelerin hazırlatılmasında dış kaynaklara yönelen kurumların siteleri yayınlamak için de yine dış kaynaklara yöneldiği anlaşılmıştır.

2) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 23'e bakınız):

- **Güvenlik Taraması: Kritik Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin hazırlanma yöntemleri ile kurumun bu yöntem tarafından hazırlanan web sitelerinde kritik risk seviyesine sahip zafiyet mevcut olma arasında doğru orantı olduğu tespit edilmiştir. Sitelerin hazırlatılmasında dış kaynaklara yönelme olduğunda kurumların bu yöntem tarafından hazırlanan web sitelerinde kritik risk seviyesine sahip zafiyet bulunma oranının da arttığı görülmektedir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun şu anda hizmet veren web sayfasının hazırlanmasına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.4. Kurumun Şu Anda Hizmet Veren Web Sayfasının Yayınlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 24'e bakınız)

- **23. Soru: Kurumunuzun şu anda hizmet veren web sayfasının hazırlanması ve yayınlanması aşağıdaki durumların hangisinde ifade edilmektedir işaretleyiniz?**

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin yayınlanma yöntemleri ile bu web sitelerinin hazırlanma yöntemleri arasında doğru orantı olduğu tespit edilmiştir. Sitelerin yayınlatılmasında dış kaynaklara yönelen kurumların siteleri hazırlatmak için de dış kaynaklara yöneldiği anlaşılmıştır.

2) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 24'e bakınız):

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin yayınlanma yöntemleri ile kamu kurumlarına ait web sitelerinin güvenlik durumları düşünceleri hakkında ters orantı olduğu tespit edilmiştir. Kurumların şu anda hizmet veren web sitelerinin yayınlanma yöntemleri dış kaynaklara doğru yöneldikçe, kamu kurumlarına ait web sitelerinin güvenliğinin düşük olduğu düşüncesinin daha hâkim olduğu görülmüştür.

3) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 24'e bakınız)

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin yayınlanma yöntemleri ile kamu kurumlarına ait web sitelerinin kullanım sıklığı arasında ters orantı olduğu tespit edilmiştir. Kurumların şu anda hizmet veren web sitelerinin yayınlanma yöntemi dış kaynaklara doğru yöneldikçe, kamu kurumlarına ait web sitelerinin kullanım sıklığının da düştüğü görülmüştür.

- Güvenlik Taraması: Orta Risk Seviyesine Sahip Zafiyet Tespiti

Bu soruya verilen cevaplar neticesinde, kurumların şu anda hizmet veren web sitelerinin yayınlama yöntemleri ile kurumun bu yöntem tarafından hazırlanan web sitelerinde orta risk seviyesine sahip zafiyet mevcut olma arasında doğru orantı olduğu tespit edilmiştir. Sitelerin yayınlanma yöntemleri dış kaynaklara yöneldikçe kurumların bu yöntem ile yayınlanan web sitelerinde orta risk seviyesine sahip zafiyet bulunma oranının da arttığı görülmektedir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun şu anda hizmet veren web sayfasının yayınlanmasına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları

4.3.2.3.5. Kurumun, Kuruma Ait Web Sitesi Güvenliği ile İlgili Ödeneğinin Toplam Ödenek Miktarına Oranına Göre Sorulara Verilen Yanıtlar Analizi

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranına göre farklılık göstermediği tespit edilmiştir. **(Ek Tablo 25'e bakınız)**

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.6. Yapılan Araştırma Sonucunda Bulunan Kritik Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan kritik seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarına ait web sitelerinin kullanım sıklıkları arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarına ait web siteleri ziyaret sıklığı azaldıkça kurumların web sitelerinde tespit edilen kritik seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan kritik seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarının güvenlik durumları değerlendirmesi arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildiğinde, kurumların web sitelerinde tespit edilen kritik seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan kritik seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları

4.3.2.3.7. Yapılan Araştırma Sonucunda Bulunan Yüksek Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarına ait web sitelerinin kullanım sıklıkları arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarına ait web siteleri ziyaret sıklığı azaldıkça kurumların web sitelerinde tespit edilen yüksek seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

2) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- 26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarının güvenlik durumları değerlendirmesi arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildikçe, kurumların web sitelerinde tespit edilen yüksek seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

3) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız):

- 12. Soru: Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin bu konuda herhangi bir sertifikasyonu var mı? (eğitim değil sertifikasyon sorulmaktadır.)

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayıları ile kurumların web sitelerinin güvenliği ile ilgilenen sertifikalı personel sayısı arasında ters orantı olduğu tespit edilmiştir. Kurumların web sitelerinin güvenliği ile ilgilenen sertifikalı personel sayısı arttıkça, kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayısının azaldığı görülmüştür. Diğer bir deyişle kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayısının, sertifikalı güvenlik personeli sayısının artması halinde azaldığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan yüksek seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları

4.3.2.3.8. Yapılan Araştırma Sonucunda Bulunan Orta Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan orta seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarının güvenlik durumları değerlendirmesi arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildikçe, kurumların web sitelerinde tespit edilen orta seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan orta seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.9. Yapılan Araştırma Sonucunda Bulunan Düşük Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan düşük seviyeye sahip güvenlik zafiyeti sayıları ile kamu kurumlarının güvenlik durumları değerlendirmesi arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildiğinde, kurumların web sitelerinde tespit edilen düşük seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- 9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan düşük seviyeye sahip güvenlik zafiyeti sayıları ile kurumların web sitelerini hazırlayan personel sayıları arasında ters orantı olduğu tespit edilmiştir. Kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan düşük seviyeye sahip güvenlik zafiyeti sayılarının azaldığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan düşük seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumlarının karşılaştırması değerlendirmesi.
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.10. Yapılan Araştırma Sonucunda Bulunan Bilgisel Seviye Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız)

- 9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan bilgisel seviyeye sahip güvenlik zafiyeti sayıları ile kurumların web sitelerini hazırlayan personel sayıları arasında ters orantı olduğu tespit edilmiştir. Kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan bilgisel seviyeye sahip güvenlik zafiyeti sayılarının azaldığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan bilgisel seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerinin güvenlik durumlarının karşılaştırması değerlendirmesi.
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.11. Yapılan Araştırma Sonucunda Bulunan Toplam Zafiyet Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 26'ya bakınız):

- **9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?**

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan toplam güvenlik zafiyeti sayıları ile kurumların web sitelerini hazırlayan personel sayıları arasında ters orantı olduğu tespit edilmiştir. Kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan toplam güvenlik zafiyeti sayılarının azaldığı görülmüştür.

- **26. Soru: Kamu ve özel şirket web sitelerinin karşılaştırılması.**

Bu soruya verilen cevaplar neticesinde, kurumların web sitelerinde bulunan toplam güvenlik zafiyeti sayıları ile kamu kurumlarının güvenlik durumları değerlendirmesi arasında ters orantı olduğu tespit edilmiştir. Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildiğinde, kurumların web sitelerinde tespit edilen toplam güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan toplam zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.3.12. Kamu Kurumları Web Siteleri ve Özel Şirket Web Siteleri Kaynaklı Maddi Zarara Uğrama Oran Karşılaştırması

Uğranan maddi zararlar, Kamu kurumları web siteleri kaynaklı olanlar ve özel şirket web siteleri kaynaklı olanlar olarak karşılaştırıldığında, özel sitelerden kaynaklı maddi zarara uğrayanların, kamu kurumlarına ait web sitelerinden kaynaklı maddi zarara uğrayanların ortalama 5,5 kat daha fazla olduğu tespit edilmiştir.(Ek Tablo 27'ye bakınız)

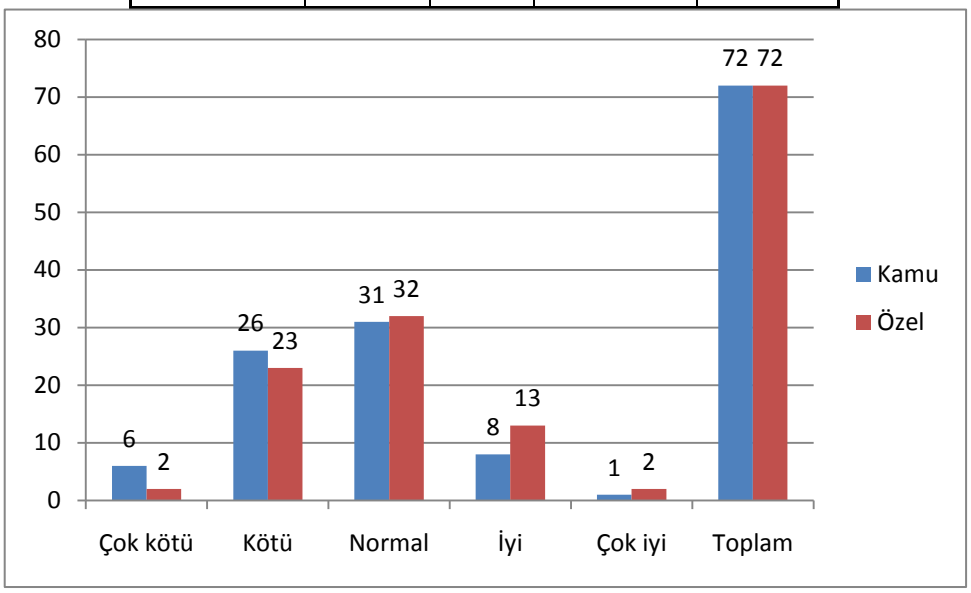
4.3.2.3.13. Kamu Kurumları Web Siteleri ve Özel Şirket Web Siteleri Kaynaklı Manevi Zarara Uğrama Oran Karşılaştırması

Uğranan manevi zararlar, Kamu kurumları web siteleri kaynaklı olanlar ve özel şirket web siteleri kaynaklı olanlar olarak karşılaştırıldığında, özel sitelerden kaynaklı manevi zarara uğrayanların, kamu kurumlarına ait web sitelerinden kaynaklı manevi zarara uğrayanların ortalama 3,3 kat daha fazla olduğu tespit edilmiştir.(Ek Tablo 28'e bakınız)

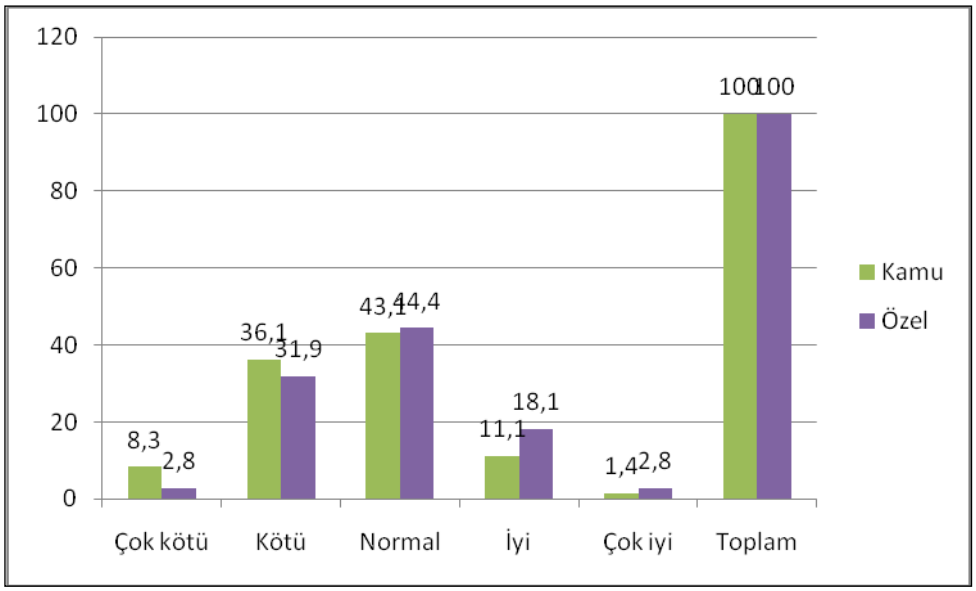
4.3.2.3.14. Kamu Kurumlarına Ait Web Siteleri ile Özel Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Karşılaştırması

Tablo 58
Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Dağılımı

	Kamu	Özel	Kamu %	Özel %
Çok kötü	6	2	8,3	2,8
Kötü	26	23	36,1	32
Normal	31	32	43,1	44
İyi	8	13	11,1	18
Çok iyi	1	2	1,4	2,8
Toplam	72	72	100	100



Şekil 95 : Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim



Şekil 96 : Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri "%" Değerlendirme Dağılımı Tablosu – Grafiksel Gösterim

Kamu Kurumlarına Ait Web Siteleri İle Özel Şirket Web Sitelerinin Güvenlik Seviyeleri değerlendirildiğinde, katılımcıların %8,3'ünün kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin çok kötü olduğunu düşünmekte oldukları, özel şirket web sitelerinin güvenlik seviyelerinin çok kötü olduğunu düşünen katılımcı sayısının ise %2,8 olduğu tespit edilmiştir. Görüldüğü gibi kamu sitelerine ait web sayfalarının güvenlik seviyesinin çok kötü olduğunu düşünenler, özel şirket web sitelerinin güvenlik seviyesinin çok kötü olduğunu düşünenlerin ortalama 3 katıdır.

Katılımcıların %36,1'inin kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin kötü olduğunu düşünmekte oldukları, özel şirket web sitelerinin güvenlik seviyelerinin kötü olduğunu düşünen katılımcı sayısının ise %31,9 olduğu tespit edilmiştir. Burada birbirine yakın oranlarda aynı düşünceye sahip olunduğu görülmektedir.

Katılımcıların %43,1'inin kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin normal olduğunu düşünmekte oldukları, özel şirket web sitelerinin güvenlik seviyelerinin normal olduğunu düşünen katılımcı sayısının ise %44,4 olduğu tespit edilmiştir. Burada da birbirine yakın oranlarda aynı düşünceye sahip olunduğu görülmektedir.

Katılımcıların %11,1'inin kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin iyi olduğunu düşünmekte oldukları, özel şirket web sitelerinin güvenlik seviyelerinin iyi olduğunu düşünen katılımcı sayısının ise %18,1 olduğu tespit edilmiştir. Burada da yine birbirine yakın oranlarda aynı düşünceye sahip olunduğu görülmektedir.

Katılımcıların %14,8'inin kamu kurumlarına ait web sitelerinin güvenlik seviyelerinin çok iyi olduğunu düşünmekte oldukları, özel şirket web sitelerinin güvenlik seviyelerinin çok iyi olduğunu düşünen katılımcı sayısının ise %2,8 olduğu tespit edilmiştir. Görüldüğü gibi burada, özel şirket web sitelerinin güvenlik seviyesinin çok iyi olduğunu düşünenlerin oranının, kamu sitelerine ait web sayfalarının güvenlik seviyesinin çok iyi olduğunu düşünenlerin oranının 2 katıdır.

4.3.2.3.15. Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel Sayılarına Göre Sorulara Verilen Yanıtlar Analizi

1) Çok Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 29'a bakınız)

- **9. Soru: Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?**

Bu soruya verilen yanıtlar incelendiğinde, Kurumun Web Sitesinin Güvenliği İle İlgilenen Personel Sayıları ile Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personel sayıları arasında doğru orantı olduğu tespit edilmiştir. Web sitesi güvenlik personel sayısı arttıkça web sitelerini hazırlayan personel sayılarının da arttığı görülmüştür.

2) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 29'a bakınız)

- **12. Soru: Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin bu konuda herhangi bir sertifikasyonu var mı? (eğitim değil sertifikasyon sorulmaktadır.)**

Bu soruya verilen yanıtlar incelendiğinde, Kurumun Web Sitesinin Güvenliği İle İlgilenen Personel Sayıları ile bu personellerin sertifikasyon durumları arasında ters orantı olduğu tespit edilmiştir. web sitesi güvenlik

personel sayısı arttıkça bu personellerin sertifikasyon durumlarının azaldığı tespit edilmiştir.

- **23. Soru: Kurumunuzun şu anda hizmet veren web sayfasının hazırlanması ve yayınlanması aşağıdaki durumların hangisinde ifade edilmektedir işaretleyiniz?**

Bu soruya verilen yanıtlar incelendiğinde, Kurumun Web Sitesinin Güvenliği İle İlgilenen Personel Sayıları ile web sitelerinin hazırlanmak yöntemleri arasında doğru orantı olduğu tespit edilmiştir. Güvenlik personel sayısı arttıkça, kurumların web sitelerinin hazırlanma yöntemlerinde dış kaynaklara yönelme olduğu görülmüştür.

4.3.2.3.16. Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel ya da Personellerin Bu Konuda Herhangi Bir Sertifikasyona Sahiplik Durumlarına Göre Sorulara Verilen Yanıtlar Analizi

1) Az Anlamlı fark bulunan karşılaştırmalar (Ek Tablo 30'a bakınız)

- **11. Soru: Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin sayısı nedir?**

Bu soruya verilen cevaplar incelendiğinde, Kurumun Web Sitesinin Güvenliği İle İlgilenen sertifikalı Personel Ya Da Personellerin Durumu ile kurumun web sitesinin güvenliği ile ilgilenen personel ya da personellerin sayısı arasında ters orantı olduğu tespit edilmiştir. Kurumun web sitesinin güvenliği ile ilgilenen personel sayısı arttıkça bu personellerin sertifikasyon oranlarının azaldığı görülmüştür.

- **Güvenlik Taraması: Yüksek Risk Seviyesine Sahip Zafiyet Tespiti**

Bu soruya verilen cevaplar incelendiğinde, kurumun web sitesinin güvenliği ile ilgilenen sertifikalı personel ya da personellerin durumu ile kurumların web sitelerinde tespit edilen yüksek risk seviyesine sahip zafiyet bulunma oranı arasında ters orantı olduğu tespit edilmiştir. Sertifikalı personel sayısı arttıkça orta seviye risk seviyesine sahip güvenlik zafiyet bulunma oranının azaldığı görülmüştür.

4.3.2.4. Anlamsız Etkileşmeler

Sorulara verilen cevaplar incelendiğinde aşağıdaki değerlerin birbirini etkilemediği ya da birbiri ile arasında herhangi anlamlı bir ilişki olmadığı tespit edilmiştir.

4.3.2.4.1. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analiz Tablosu – Uygulama Tabanlı IPS

Ek Tablo 31'e bakıldığında, bu güvenlik önleminin aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı
- Kamu ve özel şirketlere ait web sitelerinin güvenlik durumlarının değerlendirilmesi
- Kamu ve özel şirketlere ait web sitelerinin günlük iş ve işlemlerde kullanma sıklığı
- Sitelerde bulunan zafiyet sayı ve seviyeleri

4.3.2.4.2. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Dışarıdan Düzensiz Penetration Hizmeti Alımı

Ek Tablo 32'ye bakıldığında, bu güvenlik önleminin aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı
- Kamu ve özel şirketlere ait web sitelerinin güvenlik durumlarının değerlendirilmesi
- Kamu ve özel şirketlere ait web sitelerinin günlük iş ve işlemlerde kullanma sıklığı
- Sitelerde bulunan zafiyet sayı ve seviyeleri

4.3.2.4.3. Kurum / Kuruluşun Web Sitesine Sahip Olup Olmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin web sayfasına sahip olmaya göre farklılık göstermediği tespit edilmiştir. **(Ek Tablo 33'e bakınız)**

- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- www.turkiye.gov.tr bilgisi
- www.turkiye.gov.tr ziyaret sıklığı
- Kamu kurumlarına ait web sitelerinin içerik ya da tasarım bakımından beğenme

4.3.2.4.4. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Port Tabanlı Güvenlik Duvarı

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin port tabanlı güvenlik duvarı kullanmaya göre farklılık göstermediği tespit edilmiştir. **(Ek Tablo 34'e bakınız)**

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı

4.3.2.4.5. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Düzenli Olarak Dışarından Alınan Penetration Hizmeti

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin düzenli olarak dışarından alınan penetration hizmeti almaya göre farklılık göstermediği tespit edilmiştir.**(Ek Tablo 35'e bakınız)**

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin güvenlik durumları düşüncesi,

- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Sitede bulunan zafiyet sayıları

4.3.2.4.6. Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi – Düzensiz Olarak Kurumca Yapılan Güvenlik Taramaları

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin düzensiz olarak kurumca yapılan güvenlik taramalarına göre farklılık göstermediği tespit edilmiştir. **(Ek Tablo 36'ya bakınız)**

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Sitede bulunan zafiyet sayıları.

4.3.2.4.7. Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin daha önce hiç herhangi bir özel şirket web sitesinden ve ya bu sitelerden kaynaklı herhangi bir manevi zarara uğramaya göre farklılık göstermediği tespit edilmiştir. **(Ek Tablo 37'ye bakınız)**

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Web sitelerini günlük ve olağan iş ve işlemlerde kullanma sıklığı,
- Web sitelerinin güvenlik durumları düşüncesi,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

4.4. Araştırma Sonuçları

Anket sonuçları ve yapılan web güvenlik taraması sonuçlarına dayanılarak yapılan araştırma sonucunda aşağıdaki durumlar tespit edilmiştir.

Kurumların %94,4 gibi çok büyük bir oranda internet sitesine sahip oldukları ve %74 gibi bir oranda da bu siteleri üzerinden çevrim için hizmet sundukları görülmüştür. Bu oran bilgi toplumuna doğru ilerleyişte oldukça yüksek bir oran olarak değerlendirilebilmektedir.

Kurumların web sitelerini hazırlayan personel sayılarının toplamda %71,2 gibi bir oranda 0 – 5 arasında olduğu, %24,4 lük bir kısmın ise sitelerini 11'den fazla kişinin hazırladığı, bu personellerin ise çoğunun sertifikasyona sahip olma oranlarının %40 olduğu tespit edilmiştir. Bunun da sitelerin bir kişiye bağımlı olmaması, bir ekip çalışması ile ortaya çıkarılması gibi olumlu yansımalarının yanında, birden fazla kişinin müdahale etmesi dolayısı ile güvenlik risklerinin artması gibi olumsuz yansımalarının olduğu görülmüştür.

Kurumların web sitelerinin güvenliği ile ilgilenen personel sayılarına bakıldığında, kurumların %62,2 lik gibi bir kısmının web sitelerinin güvenliğinin 0 – 2 kişi tarafından sağlandığı, bu personellerin ise çok azının ya da hiç birisinin sertifikasyona sahip olmama durumlarının %44,4 lük gibi bir oran olduğu tespit edilmiştir. Bunun da sitelerin güvenliklerinin kişilere bağlı olmasına ve bu kişilerin de sertifikasyona sahip olmadıklarından yeterlilik derecelerinin belgelenemediği görülmüştür. Ancak bu durumun sitelerdeki zafiyet seviye ve sayılarına etki etmediği gözlemlenmiştir. Bu durum, verilen sertifikaların ve alınan sertifikasyon eğitimlerinin yeterli olmadığını, bu eğitimlerde gerekli bilgi ve tecrübenin kazanılmadığını gösterebileceği gibi kişilerin bu bilgi ve deneyimleri bu eğitimlere katılmadan gerçek hayatta kend çabaları ile öğrenebildiklerine de işaret edebilmektedir.

Kurumsal web sitesi olan kurumların, sitelerinin güvenliğini sağlamak için aldıkları yöntemler incelendiğinde, en çok kullanılan ve tercih edilen iki yöntemin, port tabanlı FW kullanımı ve düzenli yedekleme olduğu

tespit edilmiştir. Bu yöntemlerin ise en ucuz ve ek maliyet getirmeyen basit önlemler olduğu görülmektedir. En az tercih edilen iki yöntemin ise ek maliyet çıkartan düzenli ya da düzensiz olan dışarıdan alınan penetration hizmeti alımı ve ileri düzey bilgi ve deneyim, diğer bir ifade ile sertifikasyon gerektiren kurumca yapılan düzensiz güvenlik taramaları olduğu görülmüştür.

Bu ödenek miktarlarının ve kalemlerinin belirlenme yöntemlerine bakıldığında %48,9 luk bir kısmın bu kriterleri 4 – 6 ay öncesinden belirledikleri görülmüştür. Bu durum sitelerin güvenliğinin kurumlar tarafından artık rutin olarak ele alınması gereken bir konu olarak kabul edildiğini göstermektedir.

Sitelerde bulunan zafiyetlere bakıldığında, özel şirketlere ait web sitelerinin %12 sinde kritik risk seviyesine sahip zafiyet olduğu tespit edilmişken, bu oranın kamu kurumlarına ait web sitelerinde %0 olduğu görülmektedir. Yüksek risk seviyesine sahip zafiyet oranlarına bakıldığında ise bu oranın özel şirket web sitelerinde %24, kamu kurum web sitelerinde ise %7 olduğu, orta risk seviyesine sahip güvenlik zafiyetlerinde ise özel şirketlerde %76 kamu kurumlarında ise %20 olduğu görülmüştür. Buradan da görülmektedir ki, bilgi toplumuna geçiş ve E-Devletleşme kapsamında, devletin ilgili birimlerinin tüm kamu kurumlarındaki web sitelerinin standartlaştırılması ve güvenliklerinin sağlanmasına yönelik yaptığı araştırma, yayınladığı yönetmelik, yönerge, kılavuz, kanun ve kanun tasarıları ile bunu büyük ölçüde başarıya ulaşmıştır. Daha önceden kamu kurumu olmalarına rağmen özelleştirilmeleri sonucunda yarı özel olan şirket web sitelerinin ise kamu kurumu yapılarını kaybetmeyerek kamu kurumlarına ait özellikleri taşıdıkları tespit edilmiştir.

Kişilerin ise %54,2 oranının www.turkiye.gov.tr sitesini hiç ziyaret etmedikleri görülmektedir. Bunda da en önemli rolun, uzun yıllardır tasarlanan ve üzerinde çalışılan bu sistemin ilgili birimlerce halka tanıtılmasında yetersiz kalındığında gösterilebilmektedir. Bu nedenle bu sistemin kabiliyetleri ve yararları insanlar tarafından bilinmemekte ve dolayısı ile de ihtiyaç duyulmamaktadır.

Sitelerin hazırlanma ve yayınlanma oranlarına bakıldığında tüm kurumların hazırlanma bakımında %64,4 yayınlanma bakımından %62,2 iç kaynaklardan yararlandıkları tespit edilmiştir. Bu da Türkiye'deki bilişim ile ilgilenen kişi ya da kişilerin daha fazla iş sahibi olmalarını sağlamaktadır. Birden fazla şirkete hizmet veren daha az şirket yerine, her şirket kendi içerisinde kendi bilgi işlem merkezlerine kuran bir yapı söz konusudur.

Kamu kurumlarına ait web siteleri arasında güvenlik derecelendirmesi yapıldığında, katılımcıların en güvenli bulduğu web sitesinin www.istanbul.pol.tr olduğu görülmektedir. Katılımcıların diğerlerine nazaran bu kurumdan daha fazla katılım sağlanmaları nedeniyle bu site göz ardı edildiğinde en güvenli olduğu düşünülen internet sitesinin E-Bankacılık siteleri olduğunun düşünüldüğü tespit edilmiştir. En güvensiz internet sitesinin ise oyun internet siteleri olduğunun düşünüldüğü görülmüştür.

İnsanların kamu kurumlarına ait web sitelerinden, özel şirketlere ait web sitelerine nazaran daha az maddi ve manevi zarara uğradıkları ve kişilerin özel şirketlere ait web sitelerinden diğer kişi ya da kurumlara ait verilerin elde edilme olasığının kamu kurumlarına ait web sitelerine nazaran daha yüksek olduğunun düşünüldüğü tespit edilmiştir. Bunlarda kamu kurumlarına ait web sitelerinin özel şirketlere ait web sitelerine nazaran daha güvenli olmalarının rolü olduğu değerlendirilmektedir.

Bu düşüncelere rağmen, kamu kurumlarına ait web sitelerinin güvenlikleri katılımcıların %43,1 i tarafından normal, %36,1 i tarafından kötü olarak değerlendirilmektedir. Özel şirket web sitelerinde ise bu oran %44,4 normal, % 31,9 kötü dür. Görülmektedir ki, katılımcılar web sitelerinde verilen bilgi sızıntısı olabilecek çevrimiçi hizmetler ile web sitesinin kendisini ayrı ayrı değerlendirmişlerdir. Kamu kurumlarının güvenliğinin özel şirketlere nazaran daha az olduğu düşünülmesine rağmen, bilgi sızıntısı kamu kurumu web sitelerinde daha az olabileceği değerlendirilmiştir.

Uygulama tabanlı güvenlik duvarı kullanmayan kurumların web sitelerinde, kritik ve yüksek risk seviyesine sahip zafiyet bulunma oranının

kullanan katılımcılara oranla daha fazla olduğu tespit edilmiştir. Bu da normal ve beklenen bir durumdur. Uygulama tabanlı güvenlik duvarı kullanımı web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranına göre faklılık göstermemektedir.

Servis tabanlı IPS kullanımı web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranına ve sitelerde bulunan zafiyet sayılarına göre faklılık göstermemektedir.

Düzenli kurumca yapılan güvenlik taraması metodunu kullanan kurumların sitelerinin güvenliği için ayırdıkları ödenek miktarının kullanmayan kurumlara nazaran daha az olduğu görülmektedir.

Düzenli yedekleme metodunu kullanan kurumların sitelerinin güvenliği için ayırdıkları ödenek miktarının kullanmayan kurumlara nazaran daha az olduğu görülmektedir. Ek olarak bu metodu kullanan kurumların web sitelerinde yüksek ve orta risk seviyesine sahip güvenlik zafiyeti bulunma oranının bu metodu kullanmayan kurumlara nazaran daha yüksek olduğu görülmektedir. Çünkü bu metod veriyi yetkisiz kişilerden korumak içim kullanılan bir zafiyet kapatma yöntemi değil, veriyi fiziksel arızalara karşın korumak amaçlıdır.

Web sitelerinin güvenliği için daha farklı yol ve yöntemler kullanan kurumların, sitelerinin güvenliği için ayırdıkları ödenek miktarının ankette belirtilen yöntemleri kullanan kurumlara nazaran daha fazla olduğu görülmektedir. Anlaşılmaktadır ki, ankette yer almayan diğer yol ve yöntemler daha pahalı ve iç kaynaklar ile yerine getirilemeyen yöntemlerdir.

Daha önce kamu kurumlarına ait web sitelerinden maddi ya da manevi zarara uğrayan kurum çalışanlarının (kurumların) web sitelerinde orta risk seviyesine sahip güvenlik zafiyeti bulunma oranının uğramayanlara nazaran daha fazla olduğu görülmektedir. Kurumların kamu kurumlarından zarar görmelerine rağmen gerekli önlemleri almadıkları ya da alamadıkları görülmektedir.

Web siteleri üzerinden çevrimiçi hizmet sunan kurumların, web sitelerini hazırlayan ve bu sitelerin güvenliği ile ilgilenen personel sayılarının sunmayan kurumlara nazaran daha fazla olduğu görülmüştür. Bu kurumların yine web sitelerini iç kaynaklarla yayınlama taraftarı oldukları ve bu yolu daha fazla tercih ettikleri tespit edilmiştir.

Kamu kurumlarına ve özel şirketlere ait web sayfalarından ya da bu sayfalardan kaynaklı o kurum ile ilgililerin özel ve önemli bilgileri ele geçirilebilir mi kriterinin kamu kurumlarına ait web sitelerinde bulunan zafiyet sayılarına etki etmediği tespit edilmiştir.

Web sitelerini hazırlayan ya da yardımcı olan personel sayıları arttıkça, bu sitelerin güvenliği ile ilgilenen personel sayılarının da arttığı tespit edişmiştir. Bunda, web sitelerini hazırlayan kişi ya da kişilerin aynı zamanda bu sitelerin güvenliği ile de ilgilendikleri kanısı çıkabilmektedir. Ek olarak bu sayının aşağıdaki iş, işlem ve düşüncelerin farklılık göstermediği görülmüştür.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personellerin sertifikasyon durumları,

Kurumların şu anda hizmet veren web sitelerinin hazırlanma yöntemleri ile bu web sitelerinin yayınlanma yöntemleri arasında doğru orantı olduğu tespit edilmiştir. Sitelerin hazırlatılmasında dış kaynaklara yönelen kurumların siteleri yayınlamak için de yine dış kaynaklara yöneldiği anlaşılmıştır. Ayrıca sitelerin hazırlatılmasında dış kaynaklara yönelme olduğunda kurumların bu yöntem tarafından hazırlanan web sitelerinde kritik risk seviyesine sahip zafiyet bulunma oranının da arttığı görülmektedir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun şu anda hizmet veren web sayfasının hazırlanmasına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları.

Sitelerin yayınlanma yöntemleri dış kaynaklara yöneldikçe ise kurumların bu yöntem ile yayınlanan web sitelerinde orta risk seviyesine sahip zafiyet bulunma oranının da arttığı görülmektedir.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun şu anda hizmet veren web sayfasının yayınlanmasına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları

Kamu kurumlarına ait web siteleri ziyaret sıklığı azaldıkça kurumların web sitelerinde tespit edilen kritik ve yüksek risk seviyesine sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür. Görülmektedir ki, özel şirketlerin kamu kurumlarını ziyaret ederek bu sitelerde alınan güvenlik önlemleri ve tekniklerden bilmediklerinden dolayı yararlanmadıkları ve kendi sistemlerinde uygulayamadıkları görülmektedir.

Ayrıca kurumların web sitelerinin güvenliği ile ilgilenen sertifikalı personel sayısı arttıkça, kurumların web sitelerinde bulunan yüksek seviyeye sahip güvenlik zafiyeti sayısının azaldığı görülmüştür.

Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildikçe, kurumların web sitelerinde tespit edilen orta seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

Kamu kurumlarının güvenlik durumları kötü olarak değerlendirildiğinde, kurumların web sitelerinde tespit edilen düşük seviyeye sahip güvenlik zafiyeti bulunma oranının arttığı görülmüştür. Ayrıca kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan düşük seviyeye sahip güvenlik zafiyeti sayılarının azaldığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan düşük seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları.

Kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan bilgisel seviyeye sahip güvenlik zafiyeti sayılarının azaldığı görülmüştür.

Kurumların web sitelerini hazırlayan personel sayıları arttıkça, kurumların web sitelerinde bulunan toplam güvenlik zafiyeti sayılarının azaldığı görülmüştür. Ayrıca kamu kurumlarının güvenlik durumları kötü olarak değerlendirildiğinde, kurumların web sitelerinde tespit edilen toplam güvenlik zafiyeti bulunma oranının arttığı görülmüştür.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan toplam zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları.

Web sitesi güvenlik personel sayısı arttıkça bu personellerin sertifikasyon durumlarının azaldığı tespit edilmiştir. Ek olarak güvenlik personel sayısı arttıkça, kurumların web sitelerinin hazırlanma yöntemlerinde dış kaynaklara yönelme olduğu görülmüştür. Ek olark sertifikalı personel sayısı arttıkça orta seviye risk seviyesine sahip güvenlik zafiyet bulunma oranının azaldığı görülmüştür.

Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlerden olan uygulama tabanlı IPS kullanımının aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı
- Sitelerde bulunan zafiyet sayı ve seviyeleri.

Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlerden olan Dışarıdan Düzensiz Penetration Hizmeti Alımının aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı
- Sitelerde bulunan zafiyet sayı ve seviyeleri.

Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlerden olan port tabanlı güvenlik duvarı kullanımının aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlerden olan düzenli olarak dışarıdan alınan penetration hizmeti alımının aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlerden olan düzensiz olarak kurumca yapılan güvenlik taramaları kullanımının aşağıdaki iş ve işlemler ile herhangi bir ilişkisinin olmadığı tespit edilmiştir.

- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

5. SONUÇ

Yapılan çalışma sonucunda görülmüştür ki, güvenlik artık günümüzde sadece fiziksel olarak değil, sanal olarak da büyük önem arz etmektedir. Bütünleşen dünyada, veri ve bilgi inanılmaz bir hız ve miktarda paylaşılmaya başlamıştır. Bu paylaşım fiziksel olmayan ortamlarda gerçekleştirildiğinden, bunun getirdiği tehlikeleri de beraberinde getirmektedir. Bunların en başında verinin sadece doğru yetkili kişiler ile, sadece yetkileri olan miktar kadar, sadece yetkileri olan amaç doğrultusunda kullanılmak üzere ve yine sadece yetkileri olan sürede geçerli olmak üzere paylaşımı gelmektedir. Bu amaçla bir çok önlem alınsa da, bu önlemleri aşmanın bir yolu anında olmasa da zamanla mutlaka bulunabilmektedir. Bu nedenle önlemler alınırken, daha önceden aşılma yöntemi keşfedilmiş bir önlem almamaya ya da aşılma yöntemi yeni keşfedilmiş bir yöntemin değiştirilmesi ya da yenilenmesine dikkat edilmesi gerekmektedir.

Türkiyenin, E-Devletleşme kapsamında hız verdiği kamu kurumlarına ait web siteleri üzerinden çevrimiçi hizmet verme konusunda oldukça ilerlemiş ve halka yönelik ya da kurum içi otomatize bilişim sistemlerine geçiş yapmış olduğu görülmektedir. Bu geçiş esnasında devletin ilgili birimlerce güvenlik, tasarım, içerik ve prosedüler hakkında çalışmalar yapılmış, bu konularda kanun, yönetmelik, kanun tasarısı, kılavuz ve benzeri çalışmalar hazırlatılarak, bunların tüm kamu kurumlarına ulaştırılması sağlanmış ve bu hususlara dikkat edilmesi istenmiştir. Devlet birimlerinde hazırlanan bu çalışmalara ek olarak kurumsal web güvenliği alanında söz sahibi olan ve çalışmaları bulunan kişi ve kişilerce hazırlanan çalışmaların da göz önünde bulundurulduğu görülebilmektedir. Gönderilen bu dökümanların bir kısmı tavsiye niteliği taşısa da emir niteliğinde olan yazılarda mevcuttur ki verinin ve bilginin güvenliğini asıl ilgilendiren kısımları bunlar oluşturmaktadır. Devletin bu çalışmaları sayesinde, kamu kurumlarına ait web sitelerinin özel şirket web sitelerine nazaran daha fazla web güvenliğine sahip olduğu görülmektedir.

Bu durumda etkili olan diğer bir faktörün ise kamu kurumlarının web sitelerinde sadece kod güvenliğine değil bilişim güvenliğin tüm unsurlarına mümkün olduğunda riayet etmeye çalıştıkları belirtilebilmektedir.

Tüm bunlara rağmen halka yeterli tanıtım, bilgilendirme ve eğitimde yeterli seviyere gelinmediğinden aktif olarak kullanılamamıştır. Bu nedenle Türkiye giderek artmasına rağmen halen yeterli olmayan internet kullanımı ile aynı oranda E-Devlet kullanımını gerçekleştirememektedir. Diğer gelişmiş ülkelere nazaran Türkiye halen E-Devlet kullanımında alt sıralarda yer almaktadır. Bunda diğer bir etkenin ise kamu kurumları üzerinden verilen çevrimiçi hizmetlerin halkı tatmin etmemesi gösterilebilmektedir. Bu sistemlerin birbirleri ile entegre olamayışı ise ayrı bir etmendir. Entegre olunamamada en etkili unsurun kurumlar arasında hatta aynı kurum içerisinde birimler arasındaki bilgi paylaşımın gerçekleştirilememesi olduğu düşünülmektedir.

Sitelerde tespit edilen orta risk seviyesine sahip güvenlik zafiyeti oranlarına bakıldığında, özelleştirilmiş şirketlere ait web sitelerinde bu zafiyetin bulunma oranının daha fazla olduğu, bu oranın en az kamu kurumlarına ait web sitelerinde gerçekleştiği görülmüştür. Düşük risk seviyesine sahip güvenlik zafiyeti oranlarına bakıldığında, bu zafiyetin bulunma oranının özel şirket web sitelerinde daha fazla olduğu, bu oranın en az kamu kurumlarına ait web sitelerinde gerçekleştiği görülmüştür.

Yapılan incelemeler neticesinde, aşağıdaki iş, işlem ve düşüncelerin özel, özelleştirilmiş ya da kamu kurumlarına göre farklılık göstermediği tespit edilmiştir.

- Web sitelerinin hazırlanma ve yayınlanma durumları
- Web sitelerini hazırlayan personel sayısı ve bu personellerin sertifikasyon durumları
- Web sitelerinin güvenliği ile ilgilenen personel sayısı ve bu personellerin sertifikasyon durumları
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı.

Kurumların web sitelerinin güvenlikleri için ayırdıkları ödenek miktarlarına bakıldığında, kurumların %46,7 gibi bir kısmının bu güvenlik

için ayırdığı ödenek miktarının %0 - %3 arasında olduğu görülmektedir. Buradan da görülmektedir ki, kurumlar web sitelerinin güvenliğe çok fazla ödenek ayırmamakta ve maliyetsiz ancak etkili önlemler almaya çalışmaktadıralr. Web siteleri üzerinden çevrim için hizmet sunan siteler ele alındığında ise, bu oranın %43,8 oranında %0 - %3 olduğu görülmektedir. Ancak çevrim içi hizmet sunmayan web sitesine sahip kurumlara bakıldığında %0 - %3 oranında ödenek sağlayan kurumların oranının %50 olduğu tespit edilmiştir. Görülmektedir ki, web siteleri üzerinden online işlem sunan kurumların, sunmayan kurumlara nazaran bu web sitelerinin güvenliğine daha az ödenek ayırdıkları görülmektedir. Bunda etkili olan faktörün, çevrim içi hizmet sunan sitelerin hazırlık aşamasında, diğer sitelere nazaran çok daha fazla standar ve güvenlik önlemi uygulandığından, yüksek miktarda güvenlik yatırımına ihtiyaç duyulmaması gösterilebilmektedir.

Düzenli kurumca yapılan güvenlik taraması metodunun kullanımı sitelerde bulunan zafiyet sayılarına göre faklılık göstermemektedir.

Daha önce kamu kurumlarına ait web sitelerinden maddi ya da manevi zarara uğrama oranının aşağıdaki iş, işlem ve düşüncelere göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları.

Özel şirketlere ait web sitelerinden kaynaklı herhangi bir maddi zarara uğrayıp uğramamanın ise aşağıdaki iş, işlem ve düşüncelere göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

Çevrimiçi hizmet sunup sunmamaya göre, aşağıdaki iş, işlem ve düşüncelerin farklılık göstermediği görülmüştür.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Sitede bulunan zafiyet sayıları.

Yapılan analizler sonucunda, aşağıdaki iş, işlem ve düşüncelerin kurumun, kuruma ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin hazırlanma ve yayınlanma durumları,
- Sitelerde bulunan zafiyet sayılarına.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan kritik seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları ve bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin yayınlanma durumları

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan yüksek seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan orta seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personel sayıları ve bu personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları.

Yapılan analiz sonucunda, aşağıdaki iş, işlem ve düşüncelerin yapılan araştırma sonucunda bulunan bilgisel seviye zafiyet sayılarına göre farklılık göstermediği tespit edilmiştir.

- Kurum web sitelerini hazırlayan personellerin sertifikasyon durumları,
- Kurum web sitelerinin güvenliği ile ilgilenen personel sayıları bu personellerin sertifikasyon durumları,
- Web sitelerinin güvenliği ile ilgili ödeneğin toplam ödenek miktarına oranı,
- Web sitelerinin hazırlanma ve yayınlanma durumları.

EKLER

EK – 1: Anket Formu

ANKET SORULARI

AÇIKLAMA: Bu anket, Marmara Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim Bilim Dalı'nda, Doç. Dr. Erhan AKYAZI tarafından yönetilen, Mesut GÜLNAZ'ın yapmış olduğu "Kamusal Web Güvenliği" konulu yüksek lisans çalışmasında bilimsel veri olarak yararlanılmak ve hiçbir şekilde başka bir amaçla kullanılmamak üzere, kişilerin kamu ve özel şirket web sitelerine olan ilgi ve güvenlerini ölçme amaçlı hazırlanmıştır.

1) Cinsiyetiniz?
   1. Bay
   2. Bayan

2) Yaşınız?
   1. 20 – 24
   2. 25 – 29
   3. 30 – 34
   4. 35 – 39
   5. 40'dan büyük

3) Öğrenim durumunuz?
   1. İlköğretim mezunu
   2. Lise mezunu
   3. Lisans mezunu
   4. Yüksek lisans
   5. Diğer

4) Kişisel bir web sayfanız var mı?
   1. Evet
   2. Hayır

5) Çalıştığınız kurum/kuruluş?
   1. Özel şirket
   2. Kamu kurumu
   3. Özelleştirilmiş kurum
   4. Diğer
   5. İşsiz (bu şıkkı seçtiyseniz 17. Soruya geçiniz)

6) Kurum/kuruluşunuzun web sayfası var mı?
   1. Var (yazmanızda sakınca yoksa yazabilir misiniz?
      ……)
   2. Yok (bu şıkkı seçtiyseniz 17. Soruya geçiniz)
   3. Bilmiyorum (bu şıkkı seçtiyseniz 17. Soruya geçiniz)

7) Kurumunuz web sayfası üzerinden online işlem sunuyor mu?
   1. Evet
   2. Hayır
   3. Bilmiyorum

8) Çalıştığınız kurum/kuruluşta, kurum/kuruluşunuzun bilişim hizmetlerinin verilmesi ile ilgileniyor musunuz?
   1. Evet
   2. Hayır (bu şıkkı seçtiyseniz 17. Soruya geçiniz.)

9) Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin sayısı nedir?
   1. 0-2
   2. 3-5
   3. 6-8
   4. 9-11
   5. 11'den fazla

10) Web sayfalarını hazırlayan ya da yardımcı olan kurum personel ya da personellerinin bu konuda herhangi bir sertifikasyonu var mı? (eğitim değil sertifikasyon sorulmaktadır.)
   1. Hepsinin var
   2. Çoğunun var
   3. Yarısının var
   4. Çok azının var
   5. Hiç birinin yok

11) Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin sayısı nedir?
   1. 0-2
   2. 3-5
   3. 6-8
   4. 9-11
   5. 11'den fazla

12) Kurumunuzda web sitenizin güvenliği ile ilgilenen personel ya da personellerin bu konuda herhangi bir sertifikasyonu var mı? (eğitim değil sertifikasyon sorulmaktadır.)
1. Hepsinin var
2. Çoğunun var
3. Yarısının var
4. Çok azının var
5. Hiç birinin yok

13) Web sitenizin saldırılara karşı güvenliği nasıl sağlanmaktadır? (birden fazla seçilebilir)
1. Port tabanlı güvelik duvarı ile
2. Uygulama tabanlı güvenlik duvarı ile
3. Servis tabanlı IPS ile
4. Uygulama tabanlı IPS ile
5. Düzenli kurumca yapılan güvenlik taraması sonuçları değerlendirmeleri ile
6. Düzenli dışarıdan alınan penetration test sonuçları değerlendirmeleri ile
7. Düzensiz kurumca yapılan güvenlik taraması sonuçları değerlendirmeleri ile
8. Düzensiz dışarıdan alınan penetration test sonuçları değerlendirmeleri ile
9. Düzenli yedekleme ile
10. Diğer

14) Kurumunuzun, kurumunuza ait web sitesi güvenliği ile ilgili ödeneğinin toplam ödenek miktarına oranı nedir?
1. %0 - %3
2. %4 - %7
3. %8 - %11
4. %12'den fazla
5. Fikrim Yok

15) Kurumunuzun, kurumunuza ait web sitesi ile ilgili güvenlik ödenek kalemi nasıl belirlenir?
1. İhtiyaç ortaya çıktığında ödenek çıkartılır
2. 1 – 3 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır
3. 4 – 6 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır
4. Diğer
   ……
5. Bilmiyorum

16) Herhangi bir özel e-posta adresi / hizmeti kullanıyor musunuz?
1. Evet
2. Hayır (bu şıkkı seçtiyseniz 19. Soruya geçiniz)

17) Bu özel e-posta adresine iş yerinizden erişebiliyor musunuz?
1. Evet
2. Hayır

18) Herhangi bir kurumsal e-posta adresi / hizmeti kullanıyor musunuz?
1. Evet
2. Hayır

19) Herhangi bir e-posta adresinizde herhangi bir e-posta **listesi** hizmeti kullanıyor musunuz?
1. Evet
2. Hayır

20) Herhangi bir online bankacılık hizmeti üyeliği kullanıyor ya da kullandırtıyor musunuz?
1. Evet
2. Hayır

21) 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesi hakkında bilginiz var mı?
1. Çok var
2. Var
3. Sadece duydum
4. Az var
5. Hiç yok

22) 2009 yılında hayata geçirilen http://www.turkiye.gov.tr sitesini ziyaret sıklığınız nedir?
1. Hiç
2. Yılda 1 ya da 1'den fazla
3. Ayda 1 ya da 1'den fazla
4. Haftada 1 ya da 1'den fazla
5. Her gün

23) Kurumunuzun şu anda hizmet veren web sayfasının hazırlanması ve yayınlanması aşağıdaki durumların hangisinde ifade edilmektedir işaretleyiniz?

		Web Sitesinin Hazırlanması	
		Kurum İçi Kaynaklar	Dış Kaynak
Web Sitesinin Yayınlanması	Kurum İçi Kaynaklar	a) Tamamen İç Kaynaklarla	b) Yarı Yarıya
	Dış Kaynak	c) Yarı Yarıya	d) Tamamen Dış Kaynaklarla

24) Genel olarak kamu kurumlarına ait web sitelerini içerik ve tasarım açısından beğeniyor musunuz?

	İçerik	Tasarım
Çok beğeniyorum		
Beğeniyorum Normal		
Beğenmiyorum		
Hiç beğenmiyorum		

25) Kendi fikrinize göre, kamu kurumları ve özel kurum ya da kuruluş web sitelerinden aşağıda listede yer alanları, güvenlikleri yönünden numaralandırınız ve sizce en güvenli olması gerektiğini düşündüğünüzden güvensize doğru sıralayınız.(Liste kamu kurumları ve özel web sayfaları olarak iki gruba ayrılmıştır. Bu nedenle sıralamayı her iki grup için ayrı ayrı yapınız) Çok Güvensiz: 1, Çok Güvenli: 5

	Varolan Durum				
KAMU WEB SAYFALARI	1	2	3	4	5
www.turkiye.gov.tr					
www.basbakanlik.gov.tr					
www.adalet.gov.tr					
www.msb.gov.tr					
www.icisleri.gov.tr					
www.disisleri.gov.tr					
www.maliye.gov.tr					
www.meb.gov.tr					
www.bayindirlik.gov.tr					
www.saglik.gov.tr					
www.ubak.gov.tr					
www.tarim.gov.tr					
www.calisma.gov.tr					
www.mit.gov.tr					
www.egm.gov.tr					
www.istanbul.pol.tr					
www.kgm.gov.tr					
www.sgk.gov.tr					
www.nvi.gov.tr					
Dosya Paylaşım Siteleri					
E-Bankacılık Siteleri					
E-Ticaret siteleri					
E-bilet Siteleri					
Haber Siteleri					
Kariyer Siteleri					
Oyun Siteleri					
Portal Siteleri					
Siyasi Siteleri					
Topluluk Siteleri					
Veritabanı Siteleri					

26) Kamu ve özel şirket web sitelerinin karşılaştırılması ile ilgili sorular aşağıda tablo halinde verilmiştir. Size uygun olan şıkları işaretleyiniz.

Soru		Kamu Kurumları Web Sitelerinde ya da bu Sitelerden Kaynaklı	Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı
Daha önce hiç herhangi bir zarara uğradınız mı?	**Maddi**	**a)** Evet **b)** Hayır	**a)** Evet **b)** Hayır
	Manevi	**a)** Evet **b)** Hayır	**a)** Evet **b)** Hayır
O kurum ile ilgililerin özel ve önemli bilgileri ele geçirilebilir mi?	**Vatandaşların**	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok
	O Kurumda Çalışanların	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok
	Diğer Kamu Kurumlarının	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok
	Diğer Özel Şirketlerin	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok	**1.** Evet **2.** Kısmen **3.** Hayır **4.** Fikrim yok
Sizce **Genel Olarak** web sitelerinin güncelleme düzenleri ve sıklıkları nasıldır?	**Düzenleri**	**1.** Çok düzenli **2.** Düzenli **3.** Normal **4.** Düzensiz **5.** Çok düzensiz	**1.** Çok düzenli **2.** Düzenli **3.** Normal **4.** Düzensiz **5.** Çok düzensiz
	Sıklıkları	**1.** Çok sık **2.** Sık **3.** Normal **4.** Nadiren **5.** Çok nadir	**1.** Çok sık **2.** Sık **3.** Normal **4.** Nadiren **5.** Çok nadir
Sizce web sitelerinin güvenlik seviyeleri **genel olarak** aynı mıdır?		**1.** Evet **2.** Hayır **3.** Fikrim YOK	**1.** Evet **2.** Hayır **3.** Fikrim YOK
Sizce **genel olarak** web sitelerinin güvenliği ne durumdadır?		**1.** Çok kötü **2.** Kötü **3.** Normal **4.** İyi **5.** Çok iyi	**1.** Çok kötü **2.** Kötü **3.** Normal **4.** İyi **5.** Çok iyi

Soru	Kamu Kurumları Web Sitelerinde ya da bu Sitelerden Kaynaklı	Özel Şirket Web Sitelerinde ya da bu Sitelerden Kaynaklı
Web sitelerini günlük ve olağan iş ve işlemlerde ne sıklıkta kullanırsınız?	1. Hiç 2. Yılda 1 ya da 1'den fazla 3. Ayda 1 ya da 1'den fazla 4. Haftada 1 ya da 1'den fazla 5. Her gün	1. Hiç 2. Yılda 1 ya da 1'den fazla 3. Ayda 1 ya da 1'den fazla 4. Haftada 1 ya da 1'den fazla 5. Her gün

ANKETE KATILDIĞINIZ İÇİN TEŞEKÜR EDERİZ...

EK – 2: Ek Tablolar

Ek Tablo 1 : Renk Değerleri Tablosu 279

Ek Tablo 2 : Cinsiyet Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....279

Ek Tablo 3 : Öğrenim Durumu Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 280

Ek Tablo 4 : Kişisel Web Sayfasına Sahip Olma Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....281

Ek Tablo 5 : Çalışma ve Çalışılan Kurum Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 282

Ek Tablo 6 : Uygulama Tabanlı Güvenlik Duvarı Kullanma Etki Analizi Tablosu.....285

Ek Tablo 7 : Servis Tabanlı IPS Kullanma Etki Analizi Tablosu 285

Ek Tablo 8 : Düzenli Kurumca Yapılan Güvenlik Taraması Sonuçları Kullanma Etki Analizi Tablosu 286

Ek Tablo 9 : Düzenli Yedekleme Kullanma Etki Analizi Tablosu 286

Ek Tablo 10 : Diğer Yöntemler Kullanma Etki Analizi Tablosu 287

Ek Tablo 11 : Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....288

Ek Tablo 12 : Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....289

Ek Tablo 13 : Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....290

Ek Tablo 14 : Kurum / Kuruluşun Web Siteleri Üzerinden Online İşlem Sunup Sunmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....291

Ek Tablo 15 : Kamu Kurumları Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analizi Tablosu 292

Ek Tablo 16 : Özel Şirketlere Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analizi Tablosu 294

Ek Tablo 17 : Kamu Kurumlarına Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analiz Değerleri Tablosu 296

Ek Tablo 18 : Özel Şirketlere Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analiz Değerleri Tablosu 304

Ek Tablo 19 : Kurumların, Kurumlarına Ait Web Sitesi İle İlgili Güvenlik Ödenek Kalemi Belirleme Yöntemi Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 312

Ek Tablo 20 : Herhangi Bir Online Bankacılık Hizmeti Üyeliği Kullanma ya da Kullandırtma 313

Ek Tablo 21 : Yaş Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....314

Ek Tablo 22 : Web Sayfalarını Hazırlayan ya da Yardımcı Olan Kurum Personel ya da Personellerinin Sayısı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 315

Ek Tablo 23 : Kurumun Şu Anda Hizmet Veren Web Sayfasının Hazırlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 316

Ek Tablo 24 : Kurumun Şu Anda Hizmet Veren Web Sayfasının Yayınlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....316

Ek Tablo 25 : Kurumun, Kuruma Ait Web Sitesi Güvenliği ile İlgili Ödeneğinin Toplam Ödenek Miktarına Oranına Göre Sorulara Verilen Yanıtlar Analizi Tablosu 317

Ek Tablo 26 : Yapılan Araştırma Sonucunda Bulunan Zafiyet Çeşit Ve Sayılarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu 318

Ek Tablo 27 : Kamu Kurumları Web Siteleri Ve Özel Şirket Web Siteleri Kaynaklı Maddi Zarara Uğrama Oran Karşılaştırması 319

Ek Tablo 28 : Kamu Kurumları Web Siteleri Ve Özel Şirket Web Siteleri Kaynaklı Manevi Zarara Uğrama Karşılaştırması 319

Ek Tablo 29 : Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel Sayılarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu 319

Ek Tablo 30 : Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel ya da Personellerin Bu Konuda Herhangi Bir Sertifikasyona Sahiplik Durumlarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu.....320

Ek Tablo 31 : Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi Tablosu – Uygulama Tabanlı IPS 320

Ek Tablo 32 : Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi Tablosu – Dışarıdan Düzensiz Penetration Hizmeti Alımı 321

Ek Tablo 33 : Kurum / Kuruluşun Web Sitesine Sahip Olup Olmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 321

Ek Tablo 34 : Port Tabanlı Güvelik Duvarı Kullanma Etki Analizi Tablosu.....322

Ek Tablo 35 : Düzenli Dışarıdan Alınan Penetration Test Sonuçları Kullanma Etki Analizi Tablosu 322

Ek Tablo 36 : Düzensiz Kurumca Yapılan Güvenlik Taraması Sonuçları Kullanma Etki Analizi Tablosu.....322

Ek Tablo 37 : Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu 323

Ek Tablo 1
Renk Değerleri Tablosu

1	>	p	>	0,1	Anlamsız
0,1	>	p	>	0,05	Az Anlamlı
0,05	>	p	>	0,01	Anlamlı
0,01	>	p	>	0	Çok Anlamlı

Ek Tablo 2
Cinsiyet Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_1	,745	Anlamsız
S25_2	,830	Anlamsız
S25_3	,968	Anlamsız
S25_4	,455	Anlamsız
S25_5	,751	Anlamsız
S25_6	,593	Anlamsız
S25_7	,575	Anlamsız
S25_8	,892	Anlamsız
S25_9	,871	Anlamsız
S25_10	,832	Anlamsız
S25_11	,961	Anlamsız
S25_12	,923	Anlamsız
S25_13	,802	Anlamsız
S25_14	,402	Anlamsız
S25_15	,266	Anlamsız
S25_16	,793	Anlamsız
S25_17	,602	Anlamsız
S25_18	,885	Anlamsız
S25_19	,587	Anlamsız
S25_20	,473	Anlamsız
S25_21	,039	**Anlamlı**
S25_22	,003	**Çok Anlamlı**
S25_23	,012	**Anlamlı**
S25_24	,505	Anlamsız
S25_25	,774	Anlamsız
S25_26	,918	Anlamsız
S25_27	,949	Anlamsız
S25_28	,437	Anlamsız
S25_29	,872	Anlamsız
S25_30	,762	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S21	,406	Anlamsız
S22	,105	Anlamsız
S24_1	,607	Anlamsız
S24_2	,854	Anlamsız
S26_20	,746	Anlamsız
S26_21	,378	Anlamsız
S26_22	,181	Anlamsız

	S1	Adet	Ortalama
S25_21	Erkek	60	38,67
	Kadın	12	25,67
	Total	72	
S25_22	Erkek	60	39,62
	Kadın	12	20,92
	Total	72	
S25_23	Erkek	60	39,13
	Kadın	12	23,33
	Total	72	

Ek Tablo 3
Öğrenim Durumu Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_1	,826	Anlamsız
S25_2	,139	Anlamsız
S25_3	,171	Anlamsız
S25_4	,141	Anlamsız
S25_5	,192	Anlamsız
S25_6	,146	Anlamsız
S25_7	,148	Anlamsız
S25_8	,304	Anlamsız
S25_9	,122	Anlamsız
S25_10	,140	Anlamsız
S25_11	,179	Anlamsız
S25_12	,065	Az Anlamlı
S25_13	,176	Anlamsız
S25_14	,064	Az Anlamlı
S25_15	,035	Anlamlı
S25_16	,055	Az Anlamlı
S25_17	,115	Anlamsız
S25_18	,192	Anlamsız
S25_19	,072	Az Anlamlı
S25_20	,236	Anlamsız
S25_21	,106	Anlamsız
S25_22	,498	Anlamsız
S25_23	,512	Anlamsız
S25_24	,547	Anlamsız
S25_25	,854	Anlamsız
S25_26	,532	Anlamsız
S25_27	,819	Anlamsız
S25_28	,894	Anlamsız
S25_29	,622	Anlamsız
S25_30	,910	Anlamsız
S21	,731	Anlamsız
S22	,371	Anlamsız
S24_1	,188	Anlamsız
S24_2	,856	Anlamsız
S26_21	,854	Anlamsız
S26_22	,194	Anlamsız
S26_20	,151	Anlamsız
S9	,995	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S10	,593	Anlamsız
S11	,728	Anlamsız
S12	,576	Anlamsız
S14	,246	Anlamsız
A_1	,732	Anlamsız
A_2	,508	Anlamsız
A_3	,140	Anlamsız
A_4	,183	Anlamsız
A_5	,423	Anlamsız
A_6	,210	Anlamsız

	S3	Adet	Ortalama
S25_12	Lise mezunu	4	20,50
	Lisans mezunu	46	39,78
	Yüksek lisans mezunu	21	30,67
	Total	71	
S25_14	Lise mezunu	4	14,13
	Lisans mezunu	46	37,45
	Yüksek lisans mezunu	21	37,00
	Total	71	
S25_15	Lise mezunu	4	15,25
	Lisans mezunu	46	39,49
	Yüksek lisans mezunu	21	32,31
	Total	71	
S25_16	Lise mezunu	4	14,88
	Lisans mezunu	46	38,71
	Yüksek lisans mezunu	21	34,10
	Total	71	
S25_19	Lise mezunu	4	17,00
	Lisans mezunu	46	38,29
	Yüksek lisans mezunu	21	34,60
	Total	71	

Ek Tablo 4

Kişisel Web Sayfasına Sahip Olma Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_1	,723	Anlamsız
S25_2	,114	Anlamsız
S25_3	,147	Anlamsız
S25_4	,116	Anlamsız
S25_5	,084	**Az Anlamlı**
S25_6	,048	**Anlamlı**
S25_7	,109	Anlamsız
S25_8	,795	Anlamsız
S25_9	,277	Anlamsız
S25_10	,234	Anlamsız
S25_11	,263	Anlamsız
S25_12	,540	Anlamsız
S25_13	,282	Anlamsız
S25_14	,047	Anlamlı
S25_15	,521	Anlamsız
S25_16	,109	Anlamsız
S25_17	,228	Anlamsız
S25_18	,519	Anlamsız
S25_19	,949	Anlamsız
S25_20	,176	Anlamsız
S25_21	,599	Anlamsız
S25_22	,683	Anlamsız
S25_23	,634	Anlamsız
S25_24	,979	Anlamsız
S25_25	,963	Anlamsız
S25_26	,559	Anlamsız
S25_27	,640	Anlamsız
S25_28	,359	Anlamsız
S25_29	,779	Anlamsız
S25_30	,709	Anlamsız
S21	,950	Anlamsız
S22	,557	Anlamsız
S24_1	,084	**Az Anlamlı**
S24_2	,467	Anlamsız
S26_21	,830	Anlamsız
S26_22	,715	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S26_19	,216	Anlamsız
S26_20	,870	Anlamsız
A_1	,638	Anlamsız
A_2	,477	Anlamsız
A_3	,539	Anlamsız
A_4	,307	Anlamsız
A_5	,491	Anlamsız
A_6	,573	Anlamsız
S9	,833	Anlamsız
S10	1,000	Anlamsız
S11	,162	Anlamsız
S12	,801	Anlamsız

	S4	Adet	Ortalama
S25_5	Evet	22	30,39
	Hayır	50	39,19
	Total	72	
S25_6	Evet	22	29,55
	Hayır	50	39,56
	Total	72	
S25_14	Evet	22	29,45
	Hayır	50	39,60
	Total	72	
S24_1	Evet	22	42,55
	Hayır	50	33,84
	Total	72	

Ek Tablo 5

Çalışma ve Çalışılan Kurum Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_1	0,358	Anlamsız
S25_2	0,073	Az Anlamlı
S25_3	0,024	Anlamlı
S25_4	0,043	Anlamlı
S25_5	0,06	Az Anlamlı
S25_6	0,027	Anlamlı
S25_7	0,089	Az Anlamlı
S25_8	0,073	Az Anlamlı
S25_9	0,045	Anlamlı
S25_10	0,033	Anlamlı
S25_11	0,077	Az Anlamlı
S25_12	0,045	Anlamlı
S25_13	0,016	Anlamlı
S25_14	0,077	Az Anlamlı
S25_15	0,082	Az Anlamlı
S25_16	0,05	Anlamlı
S25_17	0,056	Az Anlamlı
S25_18	0,061	Az Anlamlı
S25_19	0,034	Anlamlı
S25_20	0,777	Anlamsız
S25_21	0,612	Anlamsız
S25_22	0,952	Anlamsız
S25_23	0,527	Anlamsız
S25_24	0,434	Anlamsız
S25_25	0,378	Anlamsız
S25_26	0,464	Anlamsız
S25_27	0,888	Anlamsız
S25_28	0,397	Anlamsız
S25_29	0,889	Anlamsız
S25_30	0,84	Anlamsız
S21	0,389	Anlamsız
S22	0,205	Anlamsız
S24_1	0,241	Anlamsız
S24_2	0,619	Anlamsız
S26_21	0,054	Az Anlamlı

	S5	Adet	Ortalama
S25_2	Özel şirket	24	29,63
	Kamu kurumu	43	38,14
	Özelleştirilmiş şirket	3	60,33
	Diğer	1	24,00
	Total	71	
S25_3	Özel şirket	24	27,79
	Kamu kurumu	43	38,98
	Özelleştirilmiş şirket	3	62,33
	Diğer	1	26,00
	Total	71	
S25_4	Özel şirket	24	29,08
	Kamu kurumu	43	38,69
	Özelleştirilmiş şirket	3	56,50
	Diğer	1	25,00
	Total	71	
S25_5	Özel şirket	24	29,81
	Kamu kurumu	43	37,85
	Özelleştirilmiş şirket	3	62,17
	Diğer	1	26,50
	Total	71	
S25_6	Özel şirket	24	30,10
	Kamu kurumu	43	37,67
	Özelleştirilmiş şirket	3	62,67
	Diğer	1	25,50
	Total	71	
S25_7	Özel şirket	24	28,98
	Kamu kurumu	43	38,72
	Özelleştirilmiş şirket	3	56,83
	Diğer	1	25,00
	Total	71	
S25_8	Özel şirket	24	32,00
	Kamu kurumu	43	36,43
	Özelleştirilmiş şirket	3	63,50
	Diğer	1	31,00
	Total	71	
S25_9	Özel şirket	24	29,88

S26_22	0,229	Anlamsız
S26_19	0,001	**Çok Anlamlı**
S26_20	0,116	Anlamsız
A_1	0,222	Anlamsız
A_2	0,15	Anlamsız
A_3	0,00	**Çok Anlamlı**
A_4	0,00	**Çok Anlamlı**
A_5	0,252	Anlamsız
A_6	0,002	**Çok Anlamlı**
S9	0,384	Anlamsız
S10	0,652	Anlamsız
S11	0,232	Anlamsız
S12	0,708	Anlamsız
S14	0,343	Anlamsız
S23_1	0,365	Anlamsız
S23_2	0,15	Anlamsız

	S5	Adet	Ortalama
S26_21	Özel şirket	24	29,58
	Kamu kurumu	43	41,02
	Özelleştirilmiş şirket	3	26,67
	Diğer	1	2,00
	Total	71	
A_4	Özel şirket	17	29,65
	Kamu kurumu	22	15,48
	Özelleştirilmiş şirket	3	19,50
	Total	42	
A_6	Özel şirket	17	29,03
	Kamu kurumu	22	15,41
	Özelleştirilmiş şirket	3	23,50
	Total	42	
A_3	Özel şirket	17	28,65
	Kamu kurumu	22	14,82
	Özelleştirilmiş şirket	3	30,00
	Total	42	
	Kamu kurumu	43	37,99
	Özelleştirilmiş şirket	3	59,67
	Diğer	1	26,50
	Total	71	
S25_10	Özel şirket	24	29,35
	Kamu kurumu	43	38,12
	Özelleştirilmiş şirket	3	61,00
	Diğer	1	29,50
	Total	71	
S25_11	Özel şirket	24	29,27
	Kamu kurumu	43	38,26
	Özelleştirilmiş şirket	3	59,83
	Diğer	1	29,00
	Total	71	
S25_12	Özel şirket	24	29,69
	Kamu kurumu	43	37,81
	Özelleştirilmiş şirket	3	61,67
	Diğer	1	32,50
	Total	71	
S25_13	Özel şirket	24	27,85
	Kamu kurumu	43	39,02
	Özelleştirilmiş şirket	3	60,33
	Diğer	1	28,50
	Total	71	
S25_14	Özel şirket	24	30,96
	Kamu kurumu	43	37,52
	Özelleştirilmiş şirket	3	59,00
	Diğer	1	22,50
	Total	71	
S25_15	Özel şirket	24	28,00
	Kamu kurumu	43	39,84
	Özelleştirilmiş şirket	3	50,50
	Diğer	1	19,50
	Total	71	
S25_16	Özel şirket	24	28,27
	Kamu kurumu	43	39,70
	Özelleştirilmiş şirket	3	50,50
	Diğer	1	19,00
	Total	71	

S25_17	Özel şirket	24	28,58
	Kamu kurumu	43	38,86
	Özelleştirilmiş şirket	3	58,00
	Diğer	1	25,00
	Total	71	
S25_18	Özel şirket	24	30,13
	Kamu kurumu	43	37,52
	Özelleştirilmiş şirket	3	63,83
	Diğer	1	28,00
	Total	71	
S25_19	Özel şirket	24	28,23
	Kamu kurumu	43	39,06
	Özelleştirilmiş şirket	3	57,33
	Diğer	1	27,00
	Total	71	
S26_19	Özel şirket	24	22,79
	Kamu kurumu	43	42,51
	Özelleştirilmiş şirket	3	53,83
	Diğer	1	19,50
	Total	71	

Ek Tablo 6
Uygulama Tabanlı Güvenlik Duvarı Kullanma Etki Analizi Tablosu

S14	,970	Anlamsız
S26_19	,247	Anlamsız
S26_20	,855	Anlamsız
S26_21	,201	Anlamsız
S26_22	,521	Anlamsız
A_1	,012	Anlamlı
A_2	,093	Az Anlamlı
A_3	,376	Anlamsız
A_4	,885	Anlamsız
A_5	,701	Anlamsız
A_6	,617	Anlamsız

	S13_2	**Adet**	**Ortalama**
A_1	Evet	16	,00
	Hayır	12	1,33
A_2	Evet	16	,25
	Hayır	12	,75

Ek Tablo 7
Servis Tabanlı IPS Kullanma Etki Analizi Tablosu

S14	,358	Anlamsız
S26_19	,058	**Az Anlamlı**
S26_20	,271	Anlamsız
S26_21	,377	Anlamsız
S26_22	,695	Anlamsız
A_1	,959	Anlamsız
A_2	,630	Anlamsız
A_3	,745	Anlamsız
A_4	,849	Anlamsız
A_5	,552	Anlamsız
A_6	,981	Anlamsız

	S13_3	**Adet**	**Ortalama**
S26_19	Evet	20	26,88
	Hayır	25	19,90
	Total	45	

Ek Tablo 8

Düzenli Kurumca Yapılan Güvenlik Taraması Sonuçları Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,094	Az Anlamlı
S26_19	,664	Anlamsız
S26_20	,487	Anlamsız
S26_21	,738	Anlamsız
S26_22	,581	Anlamsız
A_1	,959	Anlamsız
A_2	,654	Anlamsız
A_3	,960	Anlamsız
A_4	,445	Anlamsız
A_5	,215	Anlamsız
A_6	,287	Anlamsız

	S13_5	Adet	Ortalama
S14	Evet	18	19,31
	Hayır	27	25,46
	Total	45	

Ek Tablo 9

Düzenli Yedekleme Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,040	Anlamlı
S26_7	,186	Anlamsız
S26_8	,194	Anlamsız
S26_9	,309	Anlamsız
S26_10	,448	Anlamsız
S26_11	,912	Anlamsız
S26_12	,696	Anlamsız
S26_17	,215	Anlamsız
S26_18	,656	Anlamsız
S26_19	,239	Anlamsız
S26_20	,224	Anlamsız
S26_21	,830	Anlamsız
S26_22	,682	Anlamsız
A_1	,322	Anlamsız
A_2	,063	Az Anlamlı
A_3	,066	Az Anlamlı
A_4	,702	Anlamsız
A_5	,541	Anlamsız
A_6	,434	Anlamsız

	S13_9	Adet	Ortalama
S14	Evet	27	19,98
	Hayır	18	27,53
	Total	45	

	S13_9	Adet	Ortalama
A_2	Evet	19	,68
	Hayır	9	,00
A_3	Evet	19	3,16
	Hayır	9	,67

Ek Tablo 10
Diğer Yöntemler Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,028	**Anlamlı**
S26_19	,555	Anlamsız
S26_20	,665	Anlamsız
S26_21	,017	**Anlamlı**
S26_22	,150	Anlamsız
A_1	,406	Anlamsız
A_2	,164	Anlamsız
A_3	,885	Anlamsız
A_4	,762	Anlamsız
A_5	,742	Anlamsız
A_6	,683	Anlamsız

	S13_10	Adet	Ortalama
S14	Evet	14	28,89
	Hayır	31	20,34
	Total	45	
S26_21	Evet	14	28,89
	Hayır	31	20,34
	Total	45	

Ek Tablo 11

Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S11	,278	Anlamsız
S12	,612	Anlamsız
S9	,884	Anlamsız
S10	,439	Anlamsız
S23_1	,298	Anlamsız
S23_2	,278	Anlamsız
S26_21	,972	Anlamsız
S26_22	,562	Anlamsız
S26_19	,430	Anlamsız
S26_20	,714	Anlamsız
S14	,905	Anlamsız
A_1	,823	Anlamsız
A_2	,714	Anlamsız
A_3	,063	**Az Anlamlı**
A_4	,216	Anlamsız
A_5	,307	Anlamsız
A_6	,161	Anlamsız
S25_1	,472	Anlamsız
S25_2	,140	Anlamsız
S25_3	,174	Anlamsız
S25_4	,154	Anlamsız
S25_5	,189	Anlamsız
S25_6	,169	Anlamsız
S25_7	,162	Anlamsız
S25_8	,284	Anlamsız
S25_9	,166	Anlamsız
S25_10	,221	Anlamsız
S25_11	,205	Anlamsız
S25_12	,306	Anlamsız
S25_13	,205	Anlamsız
S25_14	,092	**Az Anlamlı**
S25_15	,692	Anlamsız
S25_16	,718	Anlamsız
S25_17	,104	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_18	,139	Anlamsız
S25_19	,192	Anlamsız
S25_20	,629	Anlamsız
S25_21	,109	Anlamsız
S25_22	,217	Anlamsız
S25_23	,176	Anlamsız
S25_24	,560	Anlamsız
S25_25	,642	Anlamsız
S25_26	,483	Anlamsız
S25_27	,801	Anlamsız
S25_28	1,000	Anlamsız
S25_29	,927	Anlamsız
S25_30	,626	Anlamsız

	S26_1	Adet	Ortalama
S25_14	Evet	2	13,00
	Hayır	70	37,17
	Total	72	
A_3	Evet	1	22,00
	Hayır	41	1,49

Ek Tablo 12

Daha Önce Hiç Herhangi Bir Kamu Kurumuna Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S11	,916	Anlamsız
S12	,762	Anlamsız
S9	,564	Anlamsız
S10	,538	Anlamsız
S23_1	,830	Anlamsız
S23_2	,916	Anlamsız
S26_21	,684	Anlamsız
S26_22	,340	Anlamsız
S26_19	,856	Anlamsız
S26_20	,175	Anlamsız
S14	,620	Anlamsız
A_1	,823	Anlamsız
A_2	,714	Anlamsız
A_3	,063	Az Anlamlı
A_4	,216	Anlamsız
A_5	,307	Anlamsız
A_6	,161	Anlamsız
S25_1	,275	Anlamsız
S25_2	,267	Anlamsız
S25_3	,157	Anlamsız
S25_4	,130	Anlamsız
S25_5	,169	Anlamsız
S25_6	,326	Anlamsız
S25_7	,858	Anlamsız
S25_8	,687	Anlamsız
S25_9	,412	Anlamsız
S25_10	,583	Anlamsız
S25_11	,856	Anlamsız
S25_12	,787	Anlamsız
S25_13	,525	Anlamsız
S25_14	,606	Anlamsız
S25_15	,131	Anlamsız
S25_16	,119	Anlamsız
S25_17	,316	Anlamsız
S25_18	,471	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_19	,185	Anlamsız
S25_20	,362	Anlamsız
S25_21	,894	Anlamsız
S25_22	,930	Anlamsız
S25_23	,847	Anlamsız
S25_24	,719	Anlamsız
S25_25	,603	Anlamsız
S25_26	,615	Anlamsız
S25_27	,918	Anlamsız
S25_28	,928	Anlamsız
S25_29	,798	Anlamsız
S25_30	,350	Anlamsız

	S26_2	Adet	Ortalama
A_3	Evet	1	42,00
	Hayır	41	21,00
	Total	42	

Ek Tablo 13

Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Maddi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S11	,931	Anlamsız
S12	,330	Anlamsız
S9	,742	Anlamsız
S10	,300	Anlamsız
S23_1	,888	Anlamsız
S23_2	,390	Anlamsız
S26_21	,808	Anlamsız
S26_22	,554	Anlamsız
S26_19	,907	Anlamsız
S26_20	,121	Anlamsız
S14	,859	Anlamsız
A_1	,559	Anlamsız
A_2	,338	Anlamsız
A_3	,581	Anlamsız
A_4	,882	Anlamsız
A_5	,853	Anlamsız
A_6	,839	Anlamsız
S25_1	,940	Anlamsız
S25_2	,669	Anlamsız
S25_3	,497	Anlamsız
S25_4	,824	Anlamsız
S25_5	,501	Anlamsız
S25_6	,716	Anlamsız
S25_7	,752	Anlamsız
S25_8	,901	Anlamsız
S25_9	,940	Anlamsız
S25_10	,939	Anlamsız
S25_11	,776	Anlamsız
S25_12	,399	Anlamsız
S25_13	,893	Anlamsız
S25_14	,781	Anlamsız
S25_15	,961	Anlamsız
S25_16	,967	Anlamsız
S25_17	,637	Anlamsız
S25_18	,947	Anlamsız
S25_19	,947	Anlamsız
S25_20	,618	Anlamsız
S25_21	,954	Anlamsız
S25_22	,794	Anlamsız
S25_23	,307	Anlamsız
S25_24	,058	**Az Anlamlı**
S25_25	,454	Anlamsız
S25_26	,730	Anlamsız
S25_27	,480	Anlamsız
S25_28	,675	Anlamsız
S25_29	,537	Anlamsız
S25_30	,213	Anlamsız

	S26_3	Adet	Ortalama
S25_24	Evet	11	26,14
	Hayır	61	38,37
	Total	72	

Ek Tablo 14
Kurum / Kuruluşun Web Siteleri Üzerinden Online İşlem Sunup Sunmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S9	,011	**Anlamlı**
S10	,884	Anlamsız
S11	,023	**Anlamlı**
S12	,715	Anlamsız
S14	,547	Anlamsız
S23_1	,156	Anlamsız
S23_2	,033	**Anlamlı**
S26_19	,605	Anlamsız
S26_20	,750	Anlamsız
S26_21	,930	Anlamsız
S26_22	,735	Anlamsız
A_1	,572	Anlamsız
A_2	,871	Anlamsız
A_3	,820	Anlamsız
A_4	,671	Anlamsız
A_5	,596	Anlamsız
A_6	,289	Anlamsız

	S7	Adet	Ortalama
S9	Evet	32	25,34
	Hayır	12	14,92
	Total	44	
S11	Evet	32	24,84
	Hayır	12	16,25
	Total	44	
S23_2	Evet	32	20,34
	Hayır	12	28,25
	Total	44	

Ek Tablo 15
Kamu Kurumları Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analizi Tablosu

Soru	S26_5		S26_6		S26_7		S26_8	
S2	,150	Anlamsız	,797	Anlamsız	,663	Anlamsız	,333	Anlamsız
S9	,665	Anlamsız	,575	Anlamsız	,634	Anlamsız	,908	Anlamsız
S10	,106	Anlamsız	,154	Anlamsız	,330	Anlamsız	,069	**Az Anlamlı**
S11	,303	Anlamsız	,648	Anlamsız	,946	Anlamsız	,994	Anlamsız
S12	,262	Anlamsız	,525	Anlamsız	,957	Anlamsız	,921	Anlamsız
S14	,304	Anlamsız	,649	Anlamsız	,050	**Anlamlı**	,519	Anlamsız
S21	,052	**Az Anlamlı**	,095	**Az Anlamlı**	,301	Anlamsız	,139	Anlamsız
S22	,773	Anlamsız	,452	Anlamsız	,469	Anlamsız	,598	Anlamsız
S23_1	,503	Anlamsız	,765	Anlamsız	,729	Anlamsız	,623	Anlamsız
S23_2	,430	Anlamsız	,694	Anlamsız	,603	Anlamsız	,255	Anlamsız
S24_1	,123	Anlamsız	,307	Anlamsız	,731	Anlamsız	,906	Anlamsız
S24_2	,884	Anlamsız	,801	Anlamsız	,952	Anlamsız	,612	Anlamsız
S25_1	,222	Anlamsız	,861	Anlamsız	,412	Anlamsız	,719	Anlamsız
S25_2	,012	**Anlamlı**	,436	Anlamsız	,004	**Çok Anlamlı**	,045	**Anlamlı**
S25_3	,065	**Az Anlamlı**	,436	Anlamsız	,054	**Az Anlamlı**	,208	Anlamsız
S25_4	,047	**Anlamlı**	,446	Anlamsız	,023	**Anlamlı**	,028	**Anlamlı**
S25_5_	,230	Anlamsız	,764	Anlamsız	,071	**Az Anlamlı**	,152	Anlamsız
S25_6	,093	**Az Anlamlı**	,429	Anlamsız	,026	**Anlamlı**	,108	Anlamsız
S25_7	,158	Anlamsız	,600	Anlamsız	,191	Anlamsız	,480	Anlamsız
S25_8	,020	**Anlamlı**	,559	Anlamsız	,401	Anlamsız	,742	Anlamsız
S25_9	,013	**Anlamlı**	,591	Anlamsız	,009	**Çok Anlamlı**	,124	Anlamsız
S25_10	,049	**Anlamlı**	,531	Anlamsız	,214	Anlamsız	,379	Anlamsız
S25_11	,026	**Anlamlı**	,490	Anlamsız	,031	**Anlamlı**	,073	**Az Anlamlı**
S25_12	,073	**Az Anlamlı**	,248	Anlamsız	,258	Anlamsız	,278	Anlamsız
S25_13	,014	**Anlamlı**	,368	Anlamsız	,012	**Anlamlı**	,065	**Az Anlamlı**
S25_14	,097	**Az Anlamlı**	,150	Anlamsız	,087	**Az Anlamlı**	,093	**Az Anlamlı**
S25_15	,194	Anlamsız	,221	Anlamsız	,018	**Anlamlı**	,187	Anlamsız
S25_16	,135	Anlamsız	,353	Anlamsız	,011	**Anlamlı**	,091	**Az Anlamlı**
S25_17	,050	**Anlamlı**	,761	Anlamsız	,025	**Anlamlı**	,091	**Az Anlamlı**
S25_18	,027	**Anlamlı**	,423	Anlamsız	,015	**Anlamlı**	,160	Anlamsız
S25_19	,025	**Anlamlı**	,607	Anlamsız	,046	**Anlamlı**	,339	Anlamsız
S25_20	,213	Anlamsız	,833	Anlamsız	,780	Anlamsız	,919	Anlamsız
S25_21	,128	Anlamsız	,043	**Anlamlı**	,011	**Anlamlı**	,157	Anlamsız
S25_22	,183	Anlamsız	,215	Anlamsız	,042	**Anlamlı**	,161	Anlamsız
S25_23	,304	Anlamsız	,261	Anlamsız	,038	**Anlamlı**	,279	Anlamsız
S25_24	,587	Anlamsız	,670	Anlamsız	,966	Anlamsız	,891	Anlamsız
S25_25	,222	Anlamsız	,867	Anlamsız	,722	Anlamsız	,928	Anlamsız
S25_26	,036	**Anlamlı**	,438	Anlamsız	,328	Anlamsız	,495	Anlamsız

Soru	S26_5		S26_6		S26_7		S26_8	
S25_27	,488	Anlamsız	,845	Anlamsız	,081	**Az Anlamlı**	,907	Anlamsız
S25_28	,120	Anlamsız	,779	Anlamsız	,165	Anlamsız	,390	Anlamsız
S25_29	,177	Anlamsız	,185	Anlamsız	,035	**Anlamlı**	,617	Anlamsız
S25_30	,500	Anlamsız	,100	Anlamsız	,411	Anlamsız	,886	Anlamsız
S26_13	,350	Anlamsız	,844	Anlamsız	,917	Anlamsız	,913	Anlamsız
S26_14	,951	Anlamsız	,917	Anlamsız	,919	Anlamsız	,114	Anlamsız
S26_15	,114	Anlamsız	,630	Anlamsız	,832	Anlamsız	,479	Anlamsız
S26_16	,462	Anlamsız	,876	Anlamsız	,896	Anlamsız	,581	Anlamsız
S26_19	,039	**Anlamlı**	,687	Anlamsız	,597	Anlamsız	,434	Anlamsız
S26_20	,027	**Anlamlı**	,423	Anlamsız	,077	**Az Anlamlı**	,184	Anlamsız
S26_21	,060	**Az Anlamlı**	,183	Anlamsız	,066	**Az Anlamlı**	,096	**Az Anlamlı**
S26_22	,731	Anlamsız	,107	Anlamsız	,536	Anlamsız	,146	Anlamsız
A_1	,562	Anlamsız	,562	Anlamsız	,702	Anlamsız	,559	Anlamsız
A_2	,540	Anlamsız	,745	Anlamsız	,633	Anlamsız	,503	Anlamsız
A_3	,385	Anlamsız	,329	Anlamsız	,388	Anlamsız	,766	Anlamsız
A_4	,502	Anlamsız	,205	Anlamsız	,108	Anlamsız	,387	Anlamsız
A_5	,283	Anlamsız	,989	Anlamsız	,250	Anlamsız	,861	Anlamsız
A_6	,720	Anlamsız	,516	Anlamsız	,156	Anlamsız	,765	Anlamsız

Ek Tablo 16
Özel Şirketlere Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analizi Tablosu

Soru	S26_9		S26_10		S26_11		S26_12	
S2	,834	Anlamsız	,695	Anlamsız	,598	Anlamsız	,655	Anlamsız
S9	,333	Anlamsız	,659	Anlamsız	,829	Anlamsız	,433	Anlamsız
S10	,241	Anlamsız	,331	Anlamsız	,166	Anlamsız	,102	Anlamsız
S11	,912	Anlamsız	,921	Anlamsız	,766	Anlamsız	,904	Anlamsız
S12	,636	Anlamsız	,819	Anlamsız	,589	Anlamsız	,507	Anlamsız
S14	,031	**Anlamlı**	,262	Anlamsız	,097	**Az Anlamlı**	,080	**Az Anlamlı**
S21	,321	Anlamsız	,153	Anlamsız	,207	Anlamsız	,022	**Anlamlı**
S22	,408	Anlamsız	,652	Anlamsız	,485	Anlamsız	,776	Anlamsız
S23_1	,132	Anlamsız	,484	Anlamsız	,865	Anlamsız	,881	Anlamsız
S23_2	,188	Anlamsız	,481	Anlamsız	,901	Anlamsız	,866	Anlamsız
S24_1	,955	Anlamsız	,950	Anlamsız	,939	Anlamsız	,566	Anlamsız
S24_2	,607	Anlamsız	,509	Anlamsız	,761	Anlamsız	,931	Anlamsız
S25_1	,957	Anlamsız	,635	Anlamsız	,987	Anlamsız	,987	Anlamsız
S25_2	,403	Anlamsız	,990	Anlamsız	,444	Anlamsız	,531	Anlamsız
S25_3	,848	Anlamsız	,883	Anlamsız	,661	Anlamsız	,794	Anlamsız
S25_4	,666	Anlamsız	,893	Anlamsız	,671	Anlamsız	,647	Anlamsız
S25_5_	,885	Anlamsız	,982	Anlamsız	,863	Anlamsız	,995	Anlamsız
S25_6	,806	Anlamsız	,994	Anlamsız	,394	Anlamsız	,905	Anlamsız
S25_7	,950	Anlamsız	,795	Anlamsız	,996	Anlamsız	,711	Anlamsız
S25_8	,321	Anlamsız	,373	Anlamsız	,839	Anlamsız	,719	Anlamsız
S25_9	,611	Anlamsız	,509	Anlamsız	,680	Anlamsız	,662	Anlamsız
S25_10	,505	Anlamsız	,386	Anlamsız	,456	Anlamsız	,738	Anlamsız
S25_11	,647	Anlamsız	,500	Anlamsız	,690	Anlamsız	,654	Anlamsız
S25_12	,587	Anlamsız	,366	Anlamsız	,322	Anlamsız	,754	Anlamsız
S25_13	,540	Anlamsız	,507	Anlamsız	,467	Anlamsız	,509	Anlamsız
S25_14	,725	Anlamsız	,792	Anlamsız	,857	Anlamsız	,656	Anlamsız
S25_15	,871	Anlamsız	,735	Anlamsız	,783	Anlamsız	,936	Anlamsız
S25_16	,457	Anlamsız	,511	Anlamsız	,405	Anlamsız	,551	Anlamsız
S25_17	,749	Anlamsız	,782	Anlamsız	,995	Anlamsız	,879	Anlamsız
S25_18	,407	Anlamsız	,837	Anlamsız	,811	Anlamsız	,893	Anlamsız
S25_19	,236	Anlamsız	,518	Anlamsız	,735	Anlamsız	,795	Anlamsız
S25_20	,442	Anlamsız	,710	Anlamsız	,270	Anlamsız	,185	Anlamsız
S25_21	,398	Anlamsız	,457	Anlamsız	,284	Anlamsız	,798	Anlamsız
S25_22	,273	Anlamsız	,462	Anlamsız	,174	Anlamsız	,725	Anlamsız
S25_23	,252	Anlamsız	,800	Anlamsız	,912	Anlamsız	,941	Anlamsız
S25_24	,842	Anlamsız	,532	Anlamsız	,632	Anlamsız	,485	Anlamsız
S25_25	,915	Anlamsız	,903	Anlamsız	,971	Anlamsız	,954	Anlamsız
S25_26	,194	Anlamsız	,922	Anlamsız	,915	Anlamsız	,709	Anlamsız

Soru	S26_9		S26_10		S26_11		S26_12	
S25_27	,199	Anlamsız	,547	Anlamsız	,283	Anlamsız	,521	Anlamsız
S25_28	,272	Anlamsız	,762	Anlamsız	,853	Anlamsız	,710	Anlamsız
S25_29	,271	Anlamsız	,692	Anlamsız	,395	Anlamsız	,345	Anlamsız
S25_30	,747	Anlamsız	,714	Anlamsız	,299	Anlamsız	,751	Anlamsız
S26_13	,514	Anlamsız	,638	Anlamsız	,264	Anlamsız	,446	Anlamsız
S26_14	,513	Anlamsız	,875	Anlamsız	,764	Anlamsız	,575	Anlamsız
S26_15	,577	Anlamsız	,619	Anlamsız	,988	Anlamsız	,915	Anlamsız
S26_16	,118	Anlamsız	,504	Anlamsız	,631	Anlamsız	,589	Anlamsız
S26_19	,529	Anlamsız	,684	Anlamsız	,630	Anlamsız	,770	Anlamsız
S26_20	,013	**Anlamlı**	,532	Anlamsız	,404	Anlamsız	,150	Anlamsız
S26_21	,106	Anlamsız	,154	Anlamsız	,047	**Anlamlı**	,022	**Anlamlı**
S26_22	,137	Anlamsız	,142	Anlamsız	,014	**Anlamlı**	,042	**Anlamlı**
A_1	,589	Anlamsız	,531	Anlamsız	,700	Anlamsız	,651	Anlamsız
A_2	,709	Anlamsız	,522	Anlamsız	,777	Anlamsız	,711	Anlamsız
A_3	,709	Anlamsız	,885	Anlamsız	,575	Anlamsız	,603	Anlamsız
A_4	,432	Anlamsız	,472	Anlamsız	,522	Anlamsız	,398	Anlamsız
A_5	,157	Anlamsız	,863	Anlamsız	,952	Anlamsız	,478	Anlamsız
A_6	,406	Anlamsız	,518	Anlamsız	,684	Anlamsız	,464	Anlamsız

Ek Tablo 17

Kamu Kurumlarına Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analiz Değerleri Tablosu

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
S2	Evet	24	33,23	28	35,00	17	32,12	20	33,85
	Kısmen	36	41,42	33	36,53	34	38,44	32	38,72
	Hayır	6	27,58	6	43,67	10	34,40	8	27,25
	Fikrim yok	6	29,00	5	36,10	11	39,18	12	41,17
	Total	72		72		72		72	
S9	Evet	17	23,06	19	22,84	14	25,04	16	22,97
	Kısmen	22	22,89	19	23,47	20	20,83	19	21,84
	Hayır	4	18,75	4	16,50	6	27,00	5	26,20
	Fikrim yok	2	32,25	3	29,67	5	21,20	5	24,30
	Total	45		45		45		45	
S10	Evet	17	18,32	19	19,50	14	18,14	16	17,25
	Kısmen	22	27,61	19	27,95	20	24,33	19	24,74
	Hayır	4	17,25	4	17,25	6	25,42	5	24,50
	Fikrim yok	2	23,50	3	21,50	5	28,40	5	33,30
	Total	45		45		45		45	
S11	Evet	17	22,21	19	22,39	14	22,50	16	22,69
	Kısmen	22	22,09	19	23,29	20	23,80	19	23,29
	Hayır	4	24,00	4	19,25	6	20,83	5	22,10
	Fikrim yok	2	37,75	3	30,00	5	23,80	5	23,80
	Total	45		45		45		45	
S12	Evet	17	23,62	19	24,03	14	21,43	16	22,56
	Kısmen	22	25,02	19	24,42	20	23,55	19	23,18
	Hayır	4	16,00	4	16,25	6	23,92	5	20,60
	Fikrim yok	2	9,50	3	16,50	5	24,10	5	26,10
	Total	45		45		45		45	
S14	Evet	17	20,29	19	24,08	14	22,29	16	22,50
	Kısmen	22	23,64	19	22,24	20	26,20	19	24,26
	Hayır	4	24,00	4	17,50	6	11,00	5	16,20
	Fikrim yok	2	37,00	3	28,33	5	26,60	5	26,60
	Total	45		45		45		45	
S21	Evet	24	32,65	28	30,52	17	28,88	20	27,68
	Kısmen	36	40,83	33	40,71	34	39,76	32	40,88
	Hayır	6	18,83	6	30,50	10	34,60	8	36,69
	Fikrim yok	6	43,58	5	49,40	11	39,91	12	39,42

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Total	72		72		72		72	
S22	Evet	24	35,96	28	36,27	17	42,53	20	41,35
	Kısmen	36	35,96	33	36,94	34	34,31	32	34,31
	Hayır	6	44,17	6	44,17	10	37,35	8	36,19
	Fikrim yok	6	34,25	5	25,70	11	33,18	12	34,46
	Total	72		72		72		72	
S23_1	Evet	17	24,18	19	22,16	14	23,29	16	23,50
	Kısmen	22	23,36	19	23,63	20	24,20	19	24,68
	Hayır	4	15,00	4	20,00	6	18,33	5	19,00
	Fikrim yok	2	25,00	3	28,33	5	23,00	5	19,00
	Total	45		45		45		45	
S23_2	Evet	17	22,71	19	21,84	14	22,50	16	21,50
	Kısmen	22	24,68	19	23,39	20	24,75	19	26,74
	Hayır	4	14,50	4	21,38	6	17,67	5	18,30
	Fikrim yok	2	24,00	3	30,00	5	23,80	5	18,30
	Total	45		45		45		45	
S24_1	Evet	24	40,27	28	37,54	17	40,71	20	38,73
	Kısmen	36	35,43	33	37,64	34	34,38	32	36,59
	Hayır	6	20,50	6	22,08	10	34,95	8	34,69
	Fikrim yok	6	43,83	5	40,50	11	37,95	12	33,75
	Total	72		72		72		72	
S24_2	Evet	24	37,60	28	37,11	17	36,68	20	37,90
	Kısmen	36	36,97	33	34,45	34	37,65	32	36,83
	Hayır	6	30,67	6	41,92	10	34,90	8	27,94
	Fikrim yok	6	35,08	5	40,10	11	34,14	12	39,00
	Total	72		72		72		72	
S25_1	Evet	24	32,60	28	36,88	17	30,09	20	35,78
	Kısmen	36	36,01	33	36,89	34	37,54	32	36,03
	Hayır	6	50,42	6	38,50	10	37,80	8	32,19
	Fikrim yok	6	41,08	5	29,40	11	42,00	12	41,83
	Total	72		72		72		72	
S25_2	Evet	24	27,75	28	33,98	17	22,26	20	28,98
	Kısmen	36	37,96	33	37,11	34	38,13	32	34,98
	Hayır	6	55,33	6	48,17	10	45,80	8	45,88
	Fikrim yok	6	43,92	5	32,60	11	45,00	12	46,83
	Total	72		72		72		72	
S25_3	Evet	24	30,13	28	32,11	17	26,94	20	32,40

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Kısmen	36	37,85	33	38,27	34	36,85	32	34,88
	Hayır	6	53,75	6	44,17	10	39,35	8	37,31
	Fikrim yok	6	36,67	5	40,20	11	47,59	12	47,13
	Total	72		72		72		72	
S25_4	Evet	24	27,65	28	32,66	17	24,12	20	26,88
	Kısmen	36	39,51	33	38,62	34	38,50	32	37,17
	Hayır	6	46,67	6	45,17	10	41,80	8	40,63
	Fikrim yok	6	43,67	5	33,60	11	44,64	12	48,00
	Total	72		72		72		72	
S25_5	Evet	24	30,65	28	34,38	17	26,35	20	31,03
	Kısmen	36	38,07	33	38,27	34	38,19	32	36,02
	Hayır	6	47,75	6	40,75	10	37,85	8	35,44
	Fikrim yok	6	39,25	5	31,60	11	45,73	12	47,63
	Total	72		72		72		72	
S25_6	Evet	24	29,46	28	32,68	17	23,88	20	28,93
	Kısmen	36	38,65	33	38,39	34	39,57	32	36,94
	Hayır	6	50,33	6	45,92	10	40,40	8	38,75
	Fikrim yok	6	37,92	5	34,10	11	42,95	12	46,46
	Total	72		72		72		72	
S25_7	Evet	24	30,88	28	32,98	17	28,32	20	33,55
	Kısmen	36	37,63	33	38,91	34	37,71	32	34,94
	Hayır	6	50,67	6	41,67	10	37,90	8	39,00
	Fikrim yok	6	38,08	5	34,10	11	44,14	12	43,92
	Total	72		72		72		72	
S25_8	Evet	24	30,33	28	33,20	17	29,41	20	33,45
	Kısmen	36	37,15	33	37,98	34	38,16	32	36,14
	Hayır	6	58,42	6	44,83	10	39,75	8	41,69
	Fikrim yok	6	35,33	5	35,20	11	39,36	12	39,08
	Total	72		72		72		72	
S25_9	Evet	24	26,96	28	32,77	17	24,53	20	29,95
	Kısmen	36	39,14	33	38,09	34	37,62	32	35,75
	Hayır	6	51,25	6	40,83	10	38,75	8	41,56
	Fikrim yok	6	44,08	5	41,70	11	49,50	12	46,04
	Total	72		72		72		72	
S25_10	Evet	24	27,58	28	32,38	17	28,85	20	31,40
	Kısmen	36	40,29	33	38,77	34	37,65	32	36,45
	Hayır	6	44,25	6	41,67	10	37,25	8	38,94

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Fikrim yok	6	41,67	5	38,40	11	44,09	12	43,50
	Total	72		72		72		72	
S25_11	Evet	24	27,25	28	32,14	17	25,94	20	28,80
	Kısmen	36	39,39	33	39,91	34	37,60	32	36,66
	Hayır	6	47,50	6	37,25	10	38,20	8	38,75
	Fikrim yok	6	45,17	5	37,50	11	47,86	12	47,42
	Total	72		72		72		72	
S25_12	Evet	24	28,69	28	30,77	17	29,29	20	29,55
	Kısmen	36	38,76	33	40,71	34	37,49	32	37,86
	Hayır	6	42,58	6	40,17	10	37,05	8	41,13
	Fikrim yok	6	48,08	5	36,40	11	44,09	12	41,38
	Total	72		72		72		72	
S25_13	Evet	24	26,46	28	31,57	17	26,00	20	28,90
	Kısmen	36	39,82	33	38,89	34	36,38	32	35,97
	Hayır	6	47,83	6	40,83	10	39,15	8	41,56
	Fikrim yok	6	45,42	5	43,10	11	50,68	12	47,21
	Total	72		72		72		72	
S25_14	Evet	24	28,60	28	30,55	17	25,74	20	27,68
	Kısmen	36	39,85	33	41,82	34	39,43	32	38,39
	Hayır	6	46,67	6	39,50	10	41,85	8	38,25
	Fikrim yok	6	37,83	5	31,10	11	39,23	12	45,00
	Total	72		72		72		72	
S25_15	Evet	24	31,83	28	36,14	17	27,21	20	30,80
	Kısmen	36	36,67	33	35,92	34	36,09	32	35,41
	Hayır	6	51,17	6	50,33	10	52,30	8	46,75
	Fikrim yok	6	39,50	5	25,70	11	37,77	12	42,08
	Total	72		72		72		72	
S25_16	Evet	24	29,54	28	34,11	17	25,94	20	28,40
	Kısmen	36	38,36	33	36,64	34	37,93	32	36,77
	Hayır	6	47,33	6	49,83	10	51,85	8	46,31
	Fikrim yok	6	42,33	5	33,00	11	34,45	12	42,75
	Total	72		72		72		72	
S25_17	Evet	24	28,38	28	34,13	17	24,53	20	28,28
	Kısmen	36	38,83	33	37,82	34	38,54	32	37,11
	Hayır	6	49,25	6	42,25	10	40,55	8	42,44
	Fikrim yok	6	42,25	5	34,20	11	45,00	12	44,63
	Total	72		72		72		72	

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
S25_18	Evet	24	28,75	28	32,50	17	24,09	20	29,50
	Kısmen	36	37,56	33	39,00	34	38,15	32	36,63
	Hayır	6	53,33	6	44,33	10	40,95	8	40,69
	Fikrim yok	6	44,33	5	33,00	11	46,55	12	45,04
	Total	72		72		72		72	
S25_19	Evet	24	29,13	28	33,27	17	26,21	20	30,48
	Kısmen	36	37,78	33	37,91	34	36,74	32	36,97
	Hayır	6	55,92	6	44,25	10	44,35	8	40,25
	Fikrim yok	6	38,92	5	36,00	11	44,55	12	42,79
	Total	72		72		72		72	
S25_20	Evet	24	36,31	28	34,82	17	38,21	20	34,20
	Kısmen	36	35,28	33	37,92	34	36,07	32	36,94
	Hayır	6	29,17	6	32,58	10	31,40	8	36,44
	Fikrim yok	6	51,92	5	41,20	11	39,82	12	39,21
	Total	72		72		72		72	
S25_21	Evet	24	32,98	28	30,23	17	28,21	20	31,18
	Kısmen	36	36,10	33	38,32	34	33,43	32	34,78
	Hayır	6	54,50	6	54,83	10	49,50	8	41,75
	Fikrim yok	6	35,00	5	37,60	11	47,00	12	46,46
	Total	72		72		72		72	
S25_22	Evet	24	35,27	28	31,77	17	29,18	20	31,33
	Kısmen	36	34,46	33	38,70	34	33,94	32	34,86
	Hayır	6	53,67	6	49,17	10	48,10	8	40,13
	Fikrim yok	6	36,50	5	33,30	11	45,18	12	47,08
	Total	72		72		72		72	
S25_23	Evet	24	37,33	28	34,00	17	33,41	20	35,78
	Kısmen	36	33,25	33	35,71	34	31,54	32	32,58
	Hayır	6	49,17	6	51,67	10	47,00	8	41,88
	Fikrim yok	6	40,00	5	37,50	11	47,05	12	44,58
	Total	72		72		72		72	
S25_24	Evet	24	37,96	28	35,34	17	35,35	20	37,58
	Kısmen	36	33,85	33	36,27	34	36,10	32	37,02
	Hayır	6	44,92	6	45,75	10	36,95	8	37,81
	Fikrim yok	6	38,17	5	33,40	11	39,09	12	32,46
	Total	72		72		72		72	
S25_25	Evet	24	39,33	28	36,79	17	36,47	20	37,58
	Kısmen	36	32,28	33	37,47	34	35,56	32	37,28

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Hayır	6	39,33	6	30,25	10	33,40	8	33,00
	Fikrim yok	6	47,67	5	36,00	11	42,27	12	34,96
	Total	72		72		72		72	
S25_26	Evet	24	41,50	28	36,04	17	42,32	20	40,93
	Kısmen	36	32,57	33	38,67	34	35,41	32	36,70
	Hayır	6	24,75	6	24,42	10	28,10	8	28,94
	Fikrim yok	6	51,83	5	39,30	11	38,50	12	33,63
	Total	72		72		72		72	
S25_27	Evet	24	37,25	28	36,02	17	35,79	20	35,88
	Kısmen	36	33,78	33	36,53	34	34,07	32	36,28
	Hayır	6	39,58	6	32,83	10	30,65	8	33,69
	Fikrim yok	6	46,75	5	43,40	11	50,41	12	40,00
	Total	72		72		72		72	
S25_28	Evet	24	36,83	28	36,36	17	38,68	20	35,60
	Kısmen	36	35,17	33	37,20	34	32,09	32	34,44
	Hayır	6	26,83	6	29,50	10	36,30	8	33,75
	Fikrim yok	6	52,83	5	41,10	11	46,95	12	45,33
	Total	72		72		72		72	
S25_29	Evet	24	35,90	28	35,27	17	35,71	20	33,75
	Kısmen	36	34,90	33	39,50	34	34,18	32	36,86
	Hayır	6	31,83	6	21,33	10	29,00	8	32,94
	Fikrim yok	6	53,17	5	41,80	11	51,73	12	42,50
	Total	72		72		72		72	
S25_30	Evet	24	38,42	28	32,18	17	34,24	20	33,90
	Kısmen	36	33,22	33	42,53	34	34,03	32	36,94
	Hayır	6	44,00	6	25,58	10	39,75	8	36,63
	Fikrim yok	6	41,00	5	34,00	11	44,68	12	39,58
	Total	72		72		72		72	
S26_13	Evet	24	35,83	28	35,43	17	35,53	20	35,20
	Kısmen	36	39,51	33	38,59	34	35,84	32	38,25
	Hayır	6	24,67	6	32,92	10	40,55	8	36,38
	Fikrim yok	6	32,92	5	33,00	11	36,36	12	34,08
	Total	72		72		72		72	
S26_14	Evet	24	37,27	28	38,30	17	37,41	20	35,50
	Kısmen	36	36,46	33	35,80	34	37,62	32	41,97
	Hayır	6	32,25	6	35,25	10	34,10	8	31,81
	Fikrim yok	6	37,92	5	32,50	11	33,82	12	26,71

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Total	72		72		72		72	
S26_15	Evet	24	31,54	28	33,09	17	32,79	20	32,15
	Kısmen	36	41,54	33	37,95	34	37,31	32	37,64
	Hayır	6	26,00	6	39,33	10	37,90	8	33,88
	Fikrim yok	6	36,58	5	42,60	11	38,45	12	42,46
	Total	72		72		72		72	
S26_16	Evet	24	36,15	28	38,02	17	36,79	20	36,25
	Kısmen	36	38,97	33	35,73	34	37,87	32	39,39
	Hayır	6	26,42	6	38,08	10	33,05	8	30,56
	Fikrim yok	6	33,17	5	31,20	11	34,95	12	33,17
	Total	72		72		72		72	
S26_19	Evet	24	30,15	28	33,14	17	31,18	20	32,28
	Kısmen	36	36,32	33	39,24	34	37,15	32	35,58
	Hayır	6	53,00	6	37,00	10	39,80	8	41,31
	Fikrim yok	6	46,50	5	36,60	11	39,73	12	42,79
	Total	72		72		72		72	
S26_20	Evet	24	29,94	28	32,04	17	28,41	20	31,50
	Kısmen	36	36,99	33	40,44	34	38,34	32	35,88
	Hayır	6	56,50	6	36,08	10	47,75	8	49,31
	Fikrim yok	6	39,83	5	36,00	11	33,09	12	37,96
	Total	72		72		72		72	
S26_21	Evet	24	43,54	28	41,57	17	47,18	20	45,85
	Kısmen	36	31,33	33	32,48	34	31,06	32	31,98
	Hayır	6	46,42	6	43,08	10	35,75	8	31,44
	Fikrim yok	6	29,42	5	26,70	11	37,50	12	36,33
	Total	72		72		72		72	
S26_22	Evet	24	37,90	28	40,66	17	40,71	20	42,33
	Kısmen	36	35,76	33	32,73	34	33,28	32	32,14
	Hayır	6	41,50	6	46,50	10	39,50	8	44,00
	Fikrim yok	6	30,33	5	26,10	11	37,23	12	33,42
	Total	72		72		72		72	
A_1	Evet	13	20,50	15	20,50	7	20,50	10	20,50
	Kısmen	21	22,50	21	22,50	19	21,63	19	21,63
	Hayır	6	20,50	4	20,50	9	22,78	7	23,43
	Fikrim yok	2	20,50	2	20,50	7	20,50	6	20,50
	Total	42		42		42		42	
A_2	Evet	13	20,69	15	20,47	7	22,14	10	21,20

Soru No		S26_5		S26_6		S26_7		S26_8	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Kısmen	21	22,95	21	22,00	19	21,26	19	21,26
	Hayır	6	19,00	4	24,00	9	23,44	7	24,71
	Fikrim yok	2	19,00	2	19,00	7	19,00	6	19,00
	Total	42		42		42		42	
A_3	Evet	13	18,42	15	18,90	7	17,21	10	19,25
	Kısmen	21	24,45	21	22,86	19	24,11	19	23,45
	Hayır	6	18,00	4	18,50	9	18,11	7	19,86
	Fikrim yok	2	21,00	2	32,75	7	23,07	6	21,00
	Total	42		42		42		42	
A_4	Evet	13	20,19	15	19,20	7	14,43	10	19,95
	Kısmen	21	23,60	21	23,31	19	25,95	19	23,95
	Hayır	6	15,83	4	14,50	9	17,72	7	15,36
	Fikrim yok	2	25,00	2	33,75	7	21,36	6	23,50
	Total	42		42		42		42	
A_5	Evet	13	16,27	15	20,77	7	13,50	10	18,90
	Kısmen	21	23,71	21	21,71	19	24,08	19	22,03
	Hayır	6	23,25	4	22,88	9	21,61	7	21,79
	Fikrim yok	2	27,00	2	22,00	7	22,36	6	23,83
	Total	42		42		42		42	
A_6	Evet	13	18,92	15	19,47	7	13,50	10	19,20
	Kısmen	21	23,26	21	22,19	19	25,03	19	23,21
	Hayır	6	19,83	4	20,00	9	19,28	7	19,00
	Fikrim yok	2	24,75	2	32,50	7	22,79	6	22,83
	Total	42		42		42		42	

Ek Tablo 18

Özel Şirketlere Ait Web Sitelerinden ya da Bu Sitelerden Kaynaklı O Kurum ile İlgililerin Özel ve Önemli Bilgileri Ele Geçirilebilir Mi Analiz Değerleri Tablosu

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
S2	Evet	28	37,48	27	39,26	23	40,67	24	39,19
	Kısmen	30	36,72	31	35,19	29	35,28	29	37,28
	Hayır	9	31,22	7	30,43	12	32,08	11	31,73
	Fikrim yok	5	39,20	7	37,71	8	35,56	8	32,19
	Total	72		72		72		72	
S9	Evet	15	20,77	17	20,79	13	21,42	14	20,50
	Kısmen	20	26,70	19	24,32	19	23,16	18	22,61
	Hayır	6	18,00	4	28,38	8	26,31	9	28,83
	Fikrim yok	4	20,38	5	21,20	5	21,20	4	20,38
	Total	45		45		45		45	
S10	Evet	15	18,07	17	19,41	13	17,27	14	16,36
	Kısmen	20	26,85	19	26,97	19	27,34	18	26,22
	Hayır	6	23,33	4	22,00	8	23,31	9	27,44
	Fikrim yok	4	21,75	5	20,90	5	20,90	4	21,75
	Total	45		45		45		45	
S11	Evet	15	23,23	17	23,32	13	23,12	14	23,86
	Kısmen	20	22,85	19	23,29	19	24,29	18	22,25
	Hayır	6	20,83	4	19,25	8	19,25	9	21,78
	Fikrim yok	4	26,13	5	23,80	5	23,80	4	26,13
	Total	45		45		45		45	
S12	Evet	15	22,43	17	23,03	13	20,42	14	21,14
	Kısmen	20	24,98	19	24,55	19	24,24	18	25,75
	Hayır	6	22,50	4	20,63	8	26,81	9	23,50
	Fikrim yok	4	16,00	5	18,90	5	18,90	4	16,00
	Total	45		45		45		45	
S14	Evet	15	18,07	17	21,03	13	21,15	14	20,43
	Kısmen	20	24,90	19	23,61	19	24,97	18	23,56
	Hayır	6	19,67	4	17,50	8	15,81	9	19,67
	Fikrim yok	4	37,00	5	31,80	5	31,80	4	37,00
	Total	45		45		45		45	
S21	Evet	28	33,75	27	29,96	23	29,63	24	28,38
	Kısmen	30	39,78	31	38,58	29	40,41	29	43,90
	Hayır	9	29,06	7	44,50	12	35,79	11	29,91
	Fikrim yok	5	45,60	7	44,50	8	43,13	8	43,13

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Total	72		72		72		72	
S22	Evet	28	33,21	27	35,33	23	36,76	24	37,25
	Kısmen	30	40,02	31	39,37	29	39,72	29	35,26
	Hayır	9	39,28	7	34,43	12	33,17	11	40,95
	Fikrim yok	5	28,80	7	30,36	8	29,06	8	32,63
	Total	72		72		72		72	
S23_1	Evet	15	27,27	17	24,65	13	23,92	14	24,71
	Kısmen	20	22,80	19	23,21	19	23,63	18	22,56
	Hayır	6	15,00	4	15,00	8	20,00	9	22,56
	Fikrim yok	4	20,00	5	23,00	5	23,00	4	20,00
	Total	45		45		45		45	
S23_2	Evet	15	25,07	17	23,82	13	23,12	14	22,50
	Kısmen	20	24,75	19	23,84	19	23,84	18	24,36
	Hayır	6	14,50	4	14,50	8	20,31	9	22,72
	Fikrim yok	4	19,25	5	23,80	5	23,80	4	19,25
	Total	45		45		45		45	
S24_1	Evet	28	37,91	27	34,91	23	37,30	24	36,19
	Kısmen	30	36,12	31	37,74	29	37,24	29	39,55
	Hayır	9	33,83	7	38,00	12	35,75	11	29,68
	Fikrim yok	5	35,70	7	35,64	8	32,63	8	35,75
	Total	72		72		72		72	
S24_2	Evet	28	34,93	27	35,56	23	36,30	24	35,21
	Kısmen	30	38,05	31	38,29	29	34,07	29	36,21
	Hayır	9	31,56	7	27,21	12	40,13	11	37,23
	Fikrim yok	5	44,90	7	41,50	8	40,44	8	40,44
	Total	72		72		72		72	
S25_1	Evet	28	36,00	27	38,61	23	36,07	24	37,40
	Kısmen	30	35,75	31	37,31	29	37,22	29	36,26
	Hayır	9	39,28	7	29,29	12	36,88	11	36,59
	Fikrim yok	5	38,80	7	32,00	8	34,56	8	34,56
	Total	72		72		72		72	
S25_2	Evet	28	33,02	27	35,59	23	32,76	24	34,19
	Kısmen	30	36,30	31	36,98	29	35,52	29	34,64
	Hayır	9	45,39	7	38,07	12	43,63	11	41,50
	Fikrim yok	5	41,20	7	36,29	8	40,13	8	43,31
	Total	72		72		72		72	
S25_3	Evet	28	34,18	27	35,37	23	34,70	24	37,21

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Kısmen	30	37,13	31	35,76	29	34,95	29	33,91
	Hayır	9	39,56	7	40,57	12	38,96	11	38,68
	Fikrim yok	5	40,20	7	40,07	8	43,63	8	40,75
	Total	72		72		72		72	
S25_4	Evet	28	32,93	27	34,52	23	32,76	24	32,46
	Kısmen	30	39,30	31	38,00	29	37,41	29	39,47
	Hayır	9	37,00	7	39,14	12	41,21	11	37,23
	Fikrim yok	5	38,80	7	34,86	8	36,88	8	36,88
	Total	72		72		72		72	
S25_5	Evet	28	35,55	27	37,44	23	35,30	24	36,00
	Kısmen	30	36,32	31	35,47	29	35,21	29	36,34
	Hayır	9	36,28	7	37,79	12	39,46	11	36,82
	Fikrim yok	5	43,30	7	36,14	8	40,19	8	38,13
	Total	72		72		72		72	
S25_6	Evet	28	33,66	27	35,93	23	32,41	24	34,33
	Kısmen	30	38,43	31	37,00	29	35,74	29	37,05
	Hayır	9	37,28	7	37,57	12	44,13	11	39,50
	Fikrim yok	5	39,40	7	35,43	8	39,56	8	36,88
	Total	72		72		72		72	
S25_7	Evet	28	34,93	27	36,26	23	36,50	24	37,17
	Kısmen	30	37,17	31	38,37	29	35,91	29	34,22
	Hayır	9	37,50	7	30,14	12	37,17	11	42,18
	Fikrim yok	5	39,50	7	35,50	8	37,63	8	34,94
	Total	72		72		72		72	
S25_8	Evet	28	32,18	27	35,20	23	35,59	24	34,58
	Kısmen	30	36,93	31	39,79	29	36,97	29	35,28
	Hayır	9	44,22	7	25,64	12	33,71	11	42,05
	Fikrim yok	5	44,20	7	37,79	8	41,63	8	39,06
	Total	72		72		72		72	
S25_9	Evet	28	32,95	27	34,20	23	33,74	24	34,67
	Kısmen	30	37,72	31	38,94	29	36,78	29	35,12
	Hayır	9	40,61	7	29,36	12	36,46	11	39,05
	Fikrim yok	5	41,70	7	41,71	8	43,50	8	43,50
	Total	72		72		72		72	
S25_10	Evet	28	32,57	27	34,69	23	36,04	24	33,79
	Kısmen	30	38,88	31	39,50	29	38,22	29	36,55
	Hayır	9	36,67	7	26,64	12	29,33	11	38,05

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Fikrim yok	5	43,90	7	40,07	8	42,31	8	42,31
	Total	72		72		72		72	
S25_11	Evet	28	33,11	27	33,48	23	34,78	24	33,71
	Kısmen	30	37,98	31	39,90	29	38,31	29	35,74
	Hayır	9	38,56	7	30,50	12	32,25	11	41,14
	Fikrim yok	5	42,90	7	39,07	8	41,25	8	41,25
	Total	72		72		72		72	
S25_12	Evet	28	33,52	27	31,89	23	33,37	24	33,52
	Kısmen	30	37,80	31	40,61	29	40,22	29	36,95
	Hayır	9	36,22	7	33,36	12	30,04	11	38,05
	Fikrim yok	5	45,90	7	39,21	8	41,69	8	41,69
	Total	72		72		72		72	
S25_13	Evet	28	32,52	27	32,89	23	34,96	24	33,88
	Kısmen	30	38,43	31	38,81	29	37,55	29	35,19
	Hayır	9	38,78	7	33,57	12	31,33	11	39,59
	Fikrim yok	5	43,10	7	43,14	8	44,88	8	44,88
	Total	72		72		72		72	
S25_14	Evet	28	33,43	27	34,74	23	33,70	24	32,44
	Kısmen	30	39,45	31	39,03	29	38,55	29	39,19
	Hayır	9	36,50	7	36,43	12	37,04	11	38,41
	Fikrim yok	5	36,00	7	32,14	8	36,31	8	36,31
	Total	72		72		72		72	
S25_15	Evet	28	35,25	27	35,09	23	34,54	24	34,96
	Kısmen	30	36,00	31	38,34	29	37,91	29	37,05
	Hayır	9	41,50	7	39,93	12	39,75	11	39,32
	Fikrim yok	5	37,50	7	30,36	8	32,13	8	35,25
	Total	72		72		72		72	
S25_16	Evet	28	32,32	27	33,00	23	31,30	24	31,83
	Kısmen	30	39,62	31	40,40	29	40,16	29	39,29
	Hayır	9	41,06	7	36,64	12	39,29	11	37,05
	Fikrim yok	5	33,00	7	32,57	8	34,00	8	39,63
	Total	72		72		72		72	
S25_17	Evet	28	34,43	27	35,81	23	36,37	24	35,92
	Kısmen	30	36,20	31	38,61	29	36,05	29	35,07
	Hayır	9	42,06	7	30,50	12	36,79	11	40,41
	Fikrim yok	5	39,90	7	35,79	8	38,06	8	38,06
	Total	72		72		72		72	

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
S25_18	Evet	28	33,57	27	34,07	23	33,50	24	34,42
	Kısmen	30	35,65	31	38,81	29	38,10	29	36,53
	Hayır	9	45,33	7	36,57	12	36,17	11	38,55
	Fikrim yok	5	42,10	7	35,57	8	39,81	8	39,81
	Total	72		72		72		72	
S25_19	Evet	28	32,52	27	34,17	23	34,96	24	33,60
	Kısmen	30	35,92	31	39,56	29	38,10	29	37,22
	Hayır	9	46,67	7	29,00	12	32,46	11	37,50
	Fikrim yok	5	44,00	7	39,43	8	41,19	8	41,19
	Total	72		72		72		72	
S25_20	Evet	28	36,57	27	35,94	23	38,35	24	36,35
	Kısmen	30	35,58	31	37,34	29	37,14	29	32,95
	Hayır	9	32,00	7	29,64	12	26,88	11	36,00
	Fikrim yok	5	49,70	7	41,79	8	43,31	8	50,50
	Total	72		72		72		72	
S25_21	Evet	28	36,98	27	33,89	23	35,15	24	36,23
	Kısmen	30	34,33	31	35,85	29	32,71	29	34,69
	Hayır	9	45,94	7	47,21	12	44,92	11	41,77
	Fikrim yok	5	29,80	7	38,71	8	41,50	8	36,63
	Total	72		72		72		72	
S25_22	Evet	28	34,20	27	33,83	23	31,20	24	32,73
	Kısmen	30	36,37	31	37,39	29	36,16	29	38,45
	Hayır	9	47,94	7	46,64	12	47,08	11	39,14
	Fikrim yok	5	29,60	7	32,71	8	37,13	8	37,13
	Total	72		72		72		72	
S25_23	Evet	28	37,16	27	34,39	23	34,70	24	36,06
	Kısmen	30	33,90	31	37,23	29	36,17	29	37,03
	Hayır	9	47,50	7	42,50	12	38,79	11	33,91
	Fikrim yok	5	28,60	7	35,43	8	39,44	8	39,44
	Total	72		72		72		72	
S25_24	Evet	28	36,05	27	35,24	23	35,37	24	34,10
	Kısmen	30	34,97	31	39,71	29	38,88	29	39,88
	Hayır	9	40,78	7	28,21	12	30,79	11	30,50
	Fikrim yok	5	40,50	7	35,43	8	39,69	8	39,69
	Total	72		72		72		72	
S25_25	Evet	28	37,77	27	36,72	23	35,48	24	35,83
	Kısmen	30	34,58	31	37,76	29	37,02	29	37,19

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Hayır	9	37,83	7	32,21	12	35,58	11	34,36
	Fikrim yok	5	38,50	7	34,36	8	38,94	8	38,94
	Total	72		72		72		72	
S25_26	Evet	28	37,11	27	35,56	23	34,89	24	37,38
	Kısmen	30	35,68	31	36,48	29	36,91	29	34,66
	Hayır	9	28,50	7	35,43	12	35,83	11	34,41
	Fikrim yok	5	52,40	7	41,29	8	40,63	8	43,44
	Total	72		72		72		72	
S25_27	Evet	28	38,50	27	37,30	23	36,78	24	36,56
	Kısmen	30	32,28	31	33,90	29	33,17	29	33,74
	Hayır	9	35,72	7	35,57	12	35,88	11	36,95
	Fikrim yok	5	52,00	7	45,86	8	48,69	8	45,69
	Total	72		72		72		72	
S25_28	Evet	28	37,86	27	35,87	23	34,63	24	33,33
	Kısmen	30	35,43	31	35,05	29	35,91	29	36,60
	Hayır	9	28,61	7	38,36	12	38,50	11	39,86
	Fikrim yok	5	49,50	7	43,50	8	41,00	8	41,00
	Total	72		72		72		72	
S25_29	Evet	28	38,79	27	37,15	23	34,91	24	35,54
	Kısmen	30	33,33	31	34,85	29	34,66	29	36,07
	Hayır	9	32,44	7	33,64	12	36,58	11	31,64
	Fikrim yok	5	50,00	7	44,14	8	47,63	8	47,63
	Total	72		72		72		72	
S25_30	Evet	28	35,48	27	33,15	23	30,46	24	33,10
	Kısmen	30	35,50	31	38,92	29	37,72	29	37,38
	Hayır	9	38,00	7	36,00	12	40,63	11	38,73
	Fikrim yok	5	45,50	7	39,21	8	43,25	8	40,44
	Total	72		72		72		72	
S26_13	Evet	28	35,45	27	34,15	23	32,70	24	32,21
	Kısmen	30	39,97	31	37,76	29	38,03	29	40,53
	Hayır	9	33,06	7	43,64	12	44,50	11	37,68
	Fikrim yok	5	27,80	7	32,86	8	29,88	8	33,13
	Total	72		72		72		72	
S26_14	Evet	28	40,73	27	38,15	23	37,54	24	38,69
	Kısmen	30	34,65	31	35,11	29	37,62	29	38,17
	Hayır	9	31,72	7	39,50	12	36,42	11	32,36
	Fikrim yok	5	32,50	7	33,29	8	29,56	8	29,56

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Total	72		72		72		72	
S26_15	Evet	28	35,16	27	34,33	23	37,26	24	34,25
	Kısmen	30	39,63	31	39,27	29	36,26	29	37,36
	Hayır	9	30,06	7	30,50	12	36,92	11	37,91
	Fikrim yok	5	36,80	7	38,57	8	34,56	8	38,19
	Total	72		72		72		72	
S26_16	Evet	28	41,96	27	40,83	23	40,46	24	40,56
	Kısmen	30	34,63	31	33,95	29	35,36	29	35,36
	Hayır	9	25,39	7	33,00	12	34,71	11	33,95
	Fikrim yok	5	37,10	7	34,57	8	31,94	8	31,94
	Total	72		72		72		72	
S26_17	Evet	28	33,50	27	33,35	23	36,07	24	34,13
	Kısmen	30	36,20	31	36,40	29	34,57	29	38,22
	Hayır	9	32,83	7	25,93	12	30,42	11	26,68
	Fikrim yok	5	61,70	7	59,64	8	53,88	8	50,88
	Total	72		72		72		72	
S26_18	Evet	28	33,79	27	34,43	23	36,85	24	37,21
	Kısmen	30	36,93	31	37,31	29	39,19	29	37,19
	Hayır	9	28,28	7	22,93	12	21,58	11	24,68
	Fikrim yok	5	63,90	7	54,50	8	48,13	8	48,13
	Total	72		72		72		72	
S26_19	Evet	28	33,39	27	33,91	23	33,09	24	35,19
	Kısmen	30	36,42	31	36,50	29	37,36	29	36,14
	Hayır	9	43,22	7	43,14	12	36,42	11	35,36
	Fikrim yok	5	42,30	7	39,86	8	43,31	8	43,31
	Total	72		72		72		72	
S26_20	Evet	28	30,25	27	32,70	23	31,17	24	31,60
	Kısmen	30	38,08	31	39,65	29	38,14	29	35,38
	Hayır	9	54,00	7	40,07	12	42,13	11	47,41
	Fikrim yok	5	30,50	7	33,64	8	37,44	8	40,25
	Total	72		72		72		72	
S26_21	Evet	28	43,46	27	43,50	23	46,13	24	46,81
	Kısmen	30	30,77	31	32,90	29	30,83	29	32,00
	Hayır	9	37,17	7	30,50	12	32,50	11	28,45
	Fikrim yok	5	30,70	7	31,43	8	35,38	8	32,94
	Total	72		72		72		72	
S26_22	Evet	28	42,27	27	41,93	23	44,17	24	44,48

Soru No		S26_9		S26_10		S26_11		S26_12	
	Cevap	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama	Adet	Ortalama
	Kısmen	30	32,73	31	32,37	29	28,98	29	31,57
	Hayır	9	36,89	7	41,29	12	43,04	11	38,18
	Fikrim yok	5	26,10	7	29,07	8	31,88	8	28,13
	Total	72		72		72		72	
A_1	Evet	16	20,50	15	20,50	13	20,50	14	20,50
	Kısmen	16	21,84	17	21,76	14	22,04	16	21,84
	Hayır	8	23,06	7	23,43	11	22,36	9	22,78
	Fikrim yok	2	20,50	3	20,50	4	20,50	3	20,50
	Total	42		42		42		42	
A_2	Evet	16	20,38	15	20,47	13	20,69	14	20,57
	Kısmen	16	22,94	17	21,53	14	22,07	16	21,69
	Hayır	8	21,50	7	24,71	11	22,64	9	23,44
	Fikrim yok	2	19,00	3	19,00	4	19,00	3	19,00
	Total	42		42		42		42	
A_3	Evet	16	19,69	15	21,90	13	22,42	14	20,39
	Kısmen	16	24,06	17	21,06	14	21,71	16	23,91
	Hayır	8	20,13	7	19,86	11	18,18	9	18,11
	Fikrim yok	2	21,00	3	25,83	4	26,88	3	24,00
	Total	42		42		42		42	
A_4	Evet	16	19,47	15	20,37	13	18,62	14	19,18
	Kısmen	16	22,44	17	21,91	14	22,75	16	23,84
	Hayır	8	20,63	7	18,79	11	20,86	9	18,44
	Fikrim yok	2	33,75	3	31,17	4	28,25	3	29,00
	Total	42		42		42		42	
A_5	Evet	16	17,91	15	21,87	13	20,38	14	20,25
	Kısmen	16	21,28	17	21,97	14	21,46	16	21,72
	Hayır	8	25,63	7	18,29	11	21,86	9	19,72
	Fikrim yok	2	35,50	3	24,50	4	24,25	3	31,50
	Total	42		42		42		42	
A_6	Evet	16	18,63	15	21,27	13	19,81	14	19,61
	Kısmen	16	21,97	17	22,03	14	21,71	16	23,25
	Hayır	8	23,56	7	17,29	11	20,86	9	18,67
	Fikrim yok	2	32,50	3	29,50	4	28,00	3	29,50
	Total	42		42		42		42	

Ek Tablo 19

Kurumların, Kurumlarına Ait Web Sitesi İle İlgili Güvenlik Ödenek Kalemi Belirleme Yöntemi Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
A_1	,550	Anlamsız
A_2	,139	Anlamsız
A_3	,287	Anlamsız
A_4	,481	Anlamsız
A_5	,590	Anlamsız
A_6	,454	Anlamsız
S14	,002	Çok Anlamlı
S9	,205	Anlamsız
S10	,417	Anlamsız
S11	,229	Anlamsız
S12	,296	Anlamsız
S23_1	,622	Anlamsız
S23_2	,516	Anlamsız
S26_19	,142	Anlamsız
S26_20	,112	Anlamsız
S26_21	,054	Az Anlamlı
S26_22	,090	Az Anlamlı

	S15	Adet	Ortalama
S14	İhtiyaç ortaya çıktığında ödenek çıkartılır	13	11,96
	1 – 3 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	3	19,33
	4 – 6 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	6	29,25
	Diğer	2	24,00
	Bilmiyorum	21	28,48
	Total	45	
S26_21	İhtiyaç ortaya çıktığında ödenek çıkartılır	13	24,19
	1 – 3 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	3	11,33
	4 – 6 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	6	12,00
	Diğer	2	22,50
	Bilmiyorum	21	27,12
	Total	45	
S26_22	İhtiyaç ortaya çıktığında ödenek çıkartılır	13	24,38
	1 – 3 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	3	7,83
	4 – 6 ay önceden ödenek kalemleri belirlenir ve fiyat araştırması yapılarak ödenek belirlenmeye çalışılır	6	18,00
	Diğer	2	33,00
	Bilmiyorum	21	24,79
	Total	45	

Ek Tablo 20
Herhangi Bir Online Bankacılık Hizmeti Üyeliği Kullanma ya da Kullandırtma

Soru	Anlamlılık Düzeyi	Anlamlılık
S26_19	0,955	Anlamsız
S26_20	0,872	Anlamsız
S26_21	0,492	Anlamsız
S26_22i	0,098	**Az Anlamlı**
S24_1	0,352	Anlamsız
S24_2	0,532	Anlamsız
S21	0,774	Anlamsız
S22	0,01	**Anlamlı**
S14	0,506	Anlamsız
S9	0,074	**Az Anlamlı**
S10	0,198	Anlamsız
S11	0,828	Anlamsız
S12	0,211	Anlamsız

	S20	Adet	Ortalama
S26_22	Evet	60	38,12
	Hayır	12	28,42
	Total	72	
S22	Evet	60	39,07
	Hayır	12	23,67
	Total	72	
S9	Evet	38	24,42
	Hayır	7	15,29
	Total	45	

Ek Tablo 21
Yaş Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S25_1	,221	Anlamsız
S25_2	,477	Anlamsız
S25_3	,761	Anlamsız
S25_4	,479	Anlamsız
S25_5	,142	Anlamsız
S25_6	,363	Anlamsız
S25_7	,441	Anlamsız
S25_8	,375	Anlamsız
S25_9	,359	Anlamsız
S25_10	,337	Anlamsız
S25_11	,433	Anlamsız
S25_12	,527	Anlamsız
S25_13	,652	Anlamsız
S25_14	,144	Anlamsız
S25_15	,769	Anlamsız
S25_16	,740	Anlamsız
S25_17	,670	Anlamsız
S25_18	,285	Anlamsız
S25_19	,280	Anlamsız
S25_20	,440	Anlamsız
S25_21	,486	Anlamsız
S25_22	,860	Anlamsız
S25_23	,455	Anlamsız
S25_24	,719	Anlamsız
S25_25	,769	Anlamsız
S25_26	,893	Anlamsız
S25_27	,162	Anlamsız
S25_28	,124	Anlamsız
S25_29	,326	Anlamsız
S25_30	,475	Anlamsız
S21	,819	Anlamsız
S22	,557	Anlamsız
S24_1	,467	Anlamsız
S24_2	,773	Anlamsız
S26_5	,996	Anlamsız

Soru	Anlamlılık Düzeyi	Anlamlılık
S26_6	,508	Anlamsız
S26_7	,451	Anlamsız
S26_8	,622	Anlamsız
S26_9	,666	Anlamsız
S26_21	,107	Anlamsız
S26_22	,795	Anlamsız
S26_19	,410	Anlamsız
S26_20	,362	Anlamsız

Ek Tablo 22
Web Sayfalarını Hazırlayan ya da Yardımcı Olan Kurum Personel ya da Personellerinin Sayısı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S10	,798	Anlamsız
S23_1	,606	Anlamsız
S23_2	,378	Anlamsız
S11	,000	Çok Anlamlı
S12	,179	Anlamsız
S26_19	,499	Anlamsız
S26_20	,439	Anlamsız
S26_21	,105	Anlamsız
S26_22	,051	Az Anlamlı
S25_1	,920	Anlamsız
S25_2	,299	Anlamsız
S25_3	,513	Anlamsız
S25_4	,942	Anlamsız
S25_5	,598	Anlamsız
S25_6	,681	Anlamsız
S25_7	,591	Anlamsız
S25_8	,434	Anlamsız
S25_9	,371	Anlamsız
S25_10	,770	Anlamsız
S25_11	,859	Anlamsız
S25_12	,860	Anlamsız
S25_13	,832	Anlamsız
S25_14	,415	Anlamsız
S25_15	,934	Anlamsız
S25_16	,672	Anlamsız
S25_17	,475	Anlamsız
S25_18	,327	Anlamsız
S25_19	,313	Anlamsız
S25_20	,463	Anlamsız
S25_21	,409	Anlamsız
S25_22	,110	Anlamsız
S25_23	,259	Anlamsız
S25_24	,725	Anlamsız
S25_25	,233	Anlamsız
S25_26	,653	Anlamsız
S25_27	,481	Anlamsız
S25_28	,285	Anlamsız
S25_29	,930	Anlamsız
S25_30	,852	Anlamsız

		S9
S26_22	Korelasyon	-,292
	Anlamlılık Düzeyi	,051
	Adet	45
S11	Korelasyon	,627**
	Anlamlılık Düzeyi	,000
	Adet	45

Ek Tablo 23

Kurumun Şu Anda Hizmet Veren Web Sayfasının Hazırlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S9	,691	Anlamsız
S10	,850	Anlamsız
S11	,210	Anlamsız
S12	,578	Anlamsız
S23_2	,000	Çok Anlamlı
S26_19	,109	Anlamsız
S26_20	,429	Anlamsız
S26_21	,193	Anlamsız
S26_22	,552	Anlamsız
A_1	,039	Anlamlı
A_2	,148	Anlamsız
A_3	,137	Anlamsız
A_4	,438	Anlamsız
A_5	,466	Anlamsız
A_6	,446	Anlamsız

	S23_1
S23_2	,846**
A_1	,176

Ek Tablo 24

Kurumun Şu Anda Hizmet Veren Web Sayfasının Yayınlanması Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S9	,645	Anlamsız
S11	,669	Anlamsız
S12	,592	Anlamsız
S26_19	,048	Anlamlı
S26_20	,103	Anlamsız
S26_21	,095	Az Anlamlı
S26_22	,511	Anlamsız
A_1	,271	Anlamsız
A_2	,819	Anlamsız
A_3	,092	Az Anlamlı
A_4	,502	Anlamsız
A_5	,848	Anlamsız
A_6	,559	Anlamsız
S23_1	,000	Çok Anlamlı
S10	,762	Anlamsız

	S23_2
S23_1	,846**
S26_19	-,310*
S26_21	-,291
A_3	,304

Ek Tablo 25
Kurumun, Kuruma Ait Web Sitesi Güvenliği ile İlgili Ödeneğinin Toplam Ödenek Miktarına Oranına Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S9	,944	Anlamsız
S10	,811	Anlamsız
S11	,342	Anlamsız
S12	,206	Anlamsız
S23_1	,842	Anlamsız
S23_2	,790	Anlamsız
S26_19	,255	Anlamsız
S26_20	,310	Anlamsız
S26_21	,665	Anlamsız
S26_22	,909	Anlamsız

Ek Tablo 26

Yapılan Araştırma Sonucunda Bulunan Zafiyet Çeşit Ve Sayılarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu

	S9	S10	S11	S12	S14	S23_1	S23_2	S26_19	S26_20	S26_21	S26_22	
A_1	,339	,572	,476	,899	,768	,371	,476	,076	,643	,036	,302	**Anlamlılık Düzeyi**
A_2	,995	,413	,617	,093	,433	,760	,808	,033	,254	,007	,627	
A_3	,949	,981	,614	,860	,846	,523	,116	,076	,253	,275	,210	
A_4	,080	,945	,383	,357	,771	,808	,669	,022	,418	,151	,622	
A_5	,063	,754	,731	,732	,250	,273	,595	,106	,698	,274	,204	
A_6	,040	,755	,348	,744	,808	,904	,877	,012	,769	,189	,199	

	S9	**S10**	**S11**	**S12**	**S14**	**S23_1**	**S23_2**	**S26_19**	**S26_20**	**S26_21**	**S26_22**
A_1	,188	,112	,140	-,025	-,058	,176	,140	-,277	-,074	-,325*	,163
A_2	-,001	-,161	-,099	-,323	-,154	-,060	,048	-,330*	-,180	-,408**	,077
A_3	-,013	,005	-,100	-,035	,038	,126	,304	-,277	-,181	-,172	,198
A_4	-,336	,014	-,171	,181	,058	,048	,085	-,353*	-,128	-,225	,078
A_5	-,355	-,062	-,068	-,068	,225	-,215	-,105	-,253	,062	-,173	,200
A_6	-,391*	-,062	-,184	,065	,048	-,024	,031	-,383*	-,047	-,207	,202

Ek Tablo 27
Kamu Kurumları Web Siteleri Ve Özel Şirket Web Siteleri Kaynaklı Maddi Zarara Uğrama Oran Karşılaştırması

Maddi Zarar	Frekans	Yüzde
Kamu Kurumları Web Siteleri kaynaklı	2	2,8
Özel Şirket Web Siteleri kaynaklı	11	15,3

Ek Tablo 28
Kamu Kurumları Web Siteleri Ve Özel Şirket Web Siteleri Kaynaklı Manevi Zarara Uğrama Karşılaştırması

Manevi Zarar	Frekans	Yüzde
Kamu Kurumları Web Siteleri kaynaklı	3	4,2
Özel Şirket Web Siteleri kaynaklı	10	13,9

Ek Tablo 29
Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel Sayılarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S9	0,001	Çok Anlamlı
S12	0,055	Az Anlamlı
S14	0,342	Anlamsız
S21	0,443	Anlamsız
S22	0,497	Anlamsız
S23_1	0,08	Az Anlamlı
S23_2	0,385	Anlamsız
S26_19	0,909	Anlamsız
S26_20	0,395	Anlamsız
S26_21	0,169	Anlamsız
S26_22	0,147	Anlamsız
A_1	0,476	Anlamsız
A_2	0,617	Anlamsız
A_3	0,614	Anlamsız
A_4	0,383	Anlamsız
A_5	0,731	Anlamsız
A_6	0,348	Anlamsız

	S11
S9	,627
S12	-,288
S23_1	,080

Ek Tablo 30
Kurumun Web Sitesinin Güvenliği ile İlgilenen Personel ya da Personellerin Bu Konuda Herhangi Bir Sertifikasyona Sahiplik Durumlarına Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S11	,055	**Az Anlamlı**
S9	,179	Anlamsız
S14	,206	Anlamsız
S21	,783	Anlamsız
S22	,312	Anlamsız
S23_1	,325	Anlamsız
S23_2	,402	Anlamsız
S26_19	,904	Anlamsız
S26_20	,595	Anlamsız
S26_21	,180	Anlamsız
S26_22	,750	Anlamsız
A_1	,899	Anlamsız
A_2	,093	**Az Anlamlı**
A_3	,860	Anlamsız
A_4	,357	Anlamsız
A_5	,732	Anlamsız
A_6	,744	Anlamsız

	S12
S11	-,288
A_2	-,323

Ek Tablo 31
Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi Tablosu – Uygulama Tabanlı IPS

S14	,447	Anlamsız
S26_19	,847	Anlamsız
S26_20	,680	Anlamsız
S26_21	,243	Anlamsız
S26_22	,472	Anlamsız
A_1	,629	Anlamsız
A_2	,172	Anlamsız
A_3	,531	Anlamsız
A_4	,442	Anlamsız
A_5	,901	Anlamsız
A_6	,555	Anlamsız

Ek Tablo 32
Web Sitelerinin Saldırılara Karşı Güvenliği Sağlanmak İçin Alınan Önlemlere Göre Sorulara Verilen Yanıtlar Analizi Tablosu – Dışarıdan Düzensiz Penetration Hizmeti Alımı

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,961	Anlamsız
S26_19	,525	Anlamsız
S26_20	,567	Anlamsız
S26_21	,748	Anlamsız
S26_22	,805	Anlamsız
A_1	,502	Anlamsız
A_2	,964	Anlamsız
A_3	,870	Anlamsız
A_4	,641	Anlamsız
A_5	,385	Anlamsız
A_6	,782	Anlamsız

Ek Tablo 33
Kurum / Kuruluşun Web Sitesine Sahip Olup Olmama Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S26_21	,680	Anlamsız
S26_22	,591	Anlamsız
S26_19	,790	Anlamsız
S26_20	,790	Anlamsız
S21	,356	Anlamsız
S22	,880	Anlamsız
S24_1	,873	Anlamsız
S24_2	,802	Anlamsız

Ek Tablo 34
Port Tabanlı Güvelik Duvarı Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,910	Anlamsız
S26_10	,384	Anlamsız
S26_19	,710	Anlamsız
S26_20	,315	Anlamsız
S26_21	,166	Anlamsız
S26_22	,710	Anlamsız
A_1	,322	Anlamsız
A_2	,484	Anlamsız
A_3	,851	Anlamsız
A_4	,721	Anlamsız
A_5	,333	Anlamsız
A_6	,596	Anlamsız

Ek Tablo 35
Düzenli Dışarıdan Alınan Penetration Test Sonuçları Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,139	Anlamsız
S26_19	,948	Anlamsız
S26_20	,674	Anlamsız
S26_21	,172	Anlamsız
S26_22	,315	Anlamsız
A_1	,545	Anlamsız
A_2	,632	Anlamsız
A_3	,893	Anlamsız
A_4	,721	Anlamsız
A_5	,430	Anlamsız
A_6	,940	Anlamsız

Ek Tablo 36
Düzensiz Kurumca Yapılan Güvenlik Taraması Sonuçları Kullanma Etki Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S14	,746	Anlamsız
S26_19	,761	Anlamsız
S26_20	,903	Anlamsız
S26_21	,682	Anlamsız
S26_22	,583	Anlamsız
A_1	,502	Anlamsız
A_2	,225	Anlamsız
A_3	,974	Anlamsız
A_4	,555	Anlamsız
A_5	,514	Anlamsız
A_6	,926	Anlamsız

Ek Tablo 37
Daha Önce Hiç Herhangi Bir Özel Şirkete Ait Web Sitesinden ve ya Bu Sitelerden Kaynaklı Herhangi Bir Manevi Zarara Uğradınız Mı Kriterine Göre Sorulara Verilen Yanıtlar Analizi Tablosu

Soru	Anlamlılık Düzeyi	Anlamlılık
S11	,142	Anlamsız
S12	,105	Anlamsız
S9	,830	Anlamsız
S10	,138	Anlamsız
S23_1	,183	Anlamsız
S23_2	,637	Anlamsız
S26_21	,656	Anlamsız
S26_22	,949	Anlamsız
S26_19	,675	Anlamsız
S26_20	,139	Anlamsız
S14	,825	Anlamsız
A_1	,599	Anlamsız
A_2	,388	Anlamsız
A_3	,848	Anlamsız
A_4	,718	Anlamsız
A_5	,575	Anlamsız
A_6	,749	Anlamsız
S25_1	,306	Anlamsız
S25_2	,505	Anlamsız
S25_3	,660	Anlamsız
S25_4	,637	Anlamsız
S25_5	,126	Anlamsız
S25_6	,476	Anlamsız
S25_7	,149	Anlamsız
S25_8	,569	Anlamsız
S25_9	,937	Anlamsız
S25_10	,647	Anlamsız
S25_11	,601	Anlamsız
S25_12	,735	Anlamsız
S25_13	,986	Anlamsız
S25_14	,469	Anlamsız
S25_15	,745	Anlamsız
S25_16	,493	Anlamsız
S25_17	,752	Anlamsız
S25_18	,561	Anlamsız
S25_19	,973	Anlamsız
S25_20	,832	Anlamsız
S25_21	,720	Anlamsız
S25_22	,440	Anlamsız
S25_23	,945	Anlamsız
S25_24	,477	Anlamsız
S25_25	,972	Anlamsız
S25_26	,726	Anlamsız
S25_27	,186	Anlamsız
S25_28	,944	Anlamsız
S25_29	,795	Anlamsız
S25_30	,548	Anlamsız

KAYNAKÇA

Süreli Yayınlar

"A Review on Information, Information Security and Security Processes", **Politeknik Dergisi**, Cilt:9, Sayı:3, 2006 http://www.politeknik.gazi.edu.tr/index-s.php?q=9&s=32 (Kasım 2009)

"Dünya Ekonomisine Yönelik Global Tehditler; Dünyada Güvenlik Ve Tehdit Kavramının Evrimi Global Güvenlik İçinde Ulusal Güvenlik Perspektifi", **İstanbul Ticaret Üniversitesi Dergisi**, Mayıs 2006 http://www.iticu.edu.tr/kutuphane/dergi/d6/M00074.pdf (Kasım 2009)

"Bilim ve Teknoloji Politikalarına Giriş İçin 'Enformasyon Toplumu' Üzerine Kavramsal Bir Yaklaşım Denemesi" **Mülkiye Dergisi**, Eylül 2001 http://www.mulkiyedergi.org/index.php?option=com_rokdownloads&view=file&Itemid=63&id=825:bilim-ve-teknoloji-politikalarna-giri-icin-enformasyon-toplumu-uezerine-kavramsal-bir-yaklam-denemesi-aykut-goeker (Eylül 2009)

"Bilgi Toplumu Stratejisi Eylem Planı", **Devlet Planlama Teşkilatı Yayınları**, Temmuz 2006 http://www.dpt.gov.tr/DocObjects/Download/2227/Eylem_Plani.pdf (Ocak 2010)

26942. Sayılı Resmi Gazete http://rega.basbakanlik.gov.tr/main.aspx?home=http://rega.basbakanlik.gov.tr/eskiler/2008/07/20080720.htm&main=http://rega.basbakanlik.gov.tr/eskiler/2008/07/20080720.htm (Aralık 2009)

"Web Applıcatıon Securıty Statistics", **Web Application Security Consortium Reports** (WASC), 2008 http://projects.webappsec.org/f/WASS-SS-2008.pdf (Ekim 2009)

"Tehdit Sınıflandırması", **Web Application Security Consortium Reports**, 2004 http://www.webappsec.org/projects/threat/v1/WASC-TC-v1_0.tr.pdf (Haziran 2009)

"Web Uygulama Güvenlik Duvarı Tercih Rehberi", **Beyazşapka Bilişim Güvenliği Dergisi**, Kasım 2008

"Uygulama Güvenliği", **Beyazşapka Bilişim Güvenliği Dergisi**, Kasım 2008

"TBS-İletişim Alt Yapısı Raporu", **Telekomünikasyon İşletmecileri Derneği Dergisi**, 2007 http://www.telkoder.org.tr/files/2-report/iletisim.doc (Ekim 2009)

"Haberleşme Hizmetlerinin Devlet Tarafından Sunulmasının Ortaya Çıkardığı Sorunlar, "**Telekomünikasyon ve Regülasyon Dergisi**, Sayı:2, 2005 http://www.tk.gov.tr/yayin/Sureli_Yayinlar/trd/pdf/trd_2005_2.pdf (Ekim 2009)

"Ekonomik Suç Kavramı ve Sigortacılık Suçlarının Bu Açıdan Değerlendirilmesi", **Sayıştay Dergisi**, Sayı:55 http://www.tk.gov.tr/yayin/Sureli_Yayinlar/trd/pdf/trd_2005_2.pdf (Şubat 2010)

"Bilişim Güvenliği", **Pro-G Bilişim Güvenliği ve Araştırma Ltd. Raporu**, Sürüm 1.1, 2003 http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf (Ocak 2010)

Kitaplar

Orkan A.L., **Bilişim Teorisi, Temel Kavramlar**, M.Ü.T.E.F.M.B. İstanbul, 1993

Gürol CANBEK, Şeref SAĞIROĞLU, **Bilgi Ve Bilgisayar Güvenliği: Casus Yazılımlar Ve Korunma Yöntemleri**, Grafiker, Ankara, 2006

Hakan YILDIRIM - Volkan KAPLAN - Tuncay ÇAKMAK - Cem Cihangir ÜSTÜN, **Her Şeyi E-leştirdik**, 2. Baskı, Başkent Klişe, Ankara, Mayıs 2003

Guttman, E., Leong, L., Malkin, G., Request for Comments: 2504, **Users' Security Handbook,** ISOC, RFC 2504, 1999

İnternet Kaynakları

"**Güvenlik Nedir?**", http://www.mscguvenlik.com/guvenlik_nedir.htm (Eylül 2009)

http://www.tdk.org.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&KELIME=güven (Ocak 2010)

"**Güvenlik Nedir?**", http://www.pcnet.com.tr/forum/internet-ag-ve-guvenlik/177569-guvenlik-nedir-guvenlige-giris.htm (Şubat 2009)

Bilge KARABACAK, "**Risk Analizi**", http://www.enderunix.org/docs/disabled/risk_analizi/ (Eylül 2009)

George BOEREE, "**Maslow**", http://webspace.ship.edu/cgboer/maslow.html (Ekim 2009)

Adem KIZILKAYA, Nevzat SÖNMEZ, **Geçmişten Günümüze Güvenlik İhtiyacı Ve Türk Polis Teşkilatı**, http://www.caginpolisi.com.tr/18/19-20-21-22-23.htm (Mayıs 2010)

http://www.vik2.com/guvenlik/ (Ocak 2010)

"Güvenlik", http://tr.wikipedia.org/wiki/G%C3%BCvenlik (Kasım 2009)

"**Güvenlik Ve Tehdit Kavramının Evrimi Global Güvenlik İçinde Ulusal Güvenlik Perspektifi**", http://www.turksae.com/sql_file/298.pdf (Mayıs 2009)

Ahmet FİDAN, "**Etkili İletişim Sistemleri İletişim Ve Engelleri Sunusu**", http://www.ahmetfidan.com/dersnotlari/digerprogramlar/etkili_iletisim_teknikleri_iletisim_ve_engelleri_dr_ahmet_fidan.ppt (Kasım 2009)

"Teknoloji Nedir?", http://www.msxlabs.org/forum/muhendislik-bilimleri/19503-teknoloji-nedir.html (Mart 2009)

"Teknoloji Nedir?", http://www.teknolojide.com/teknoloji-nedir.aspx (Nisan 2009)

"Veri, Bilgi Ve Bilişim", http://www.chip.com.tr/blog/thecrowsalvation/veri-bilgi-ve-bilisim_3332.html (Eylül 2009)

http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=enformasyon (Mayıs 2010)

"Enformasyon", http://www.uludagsozluk.com/k/enformasyon/ (Mayıs 2010)

"**Türkiye'de Bilişim Güvenliği Analizi**", http://www.turkishajan.com/bilisim-suclari-analizi-ve-kriminal-olaylar/turkiye8217de-bilisim-guvenligi-analizi-34075.html (Ocak 2009)

http://behlulcaliskan.com/fileadmin/user_upload/dersler/basic_concepts_of_informatics/03.pdf (Mart 2010)

http://www.bilmuh.gyte.edu.tr/~ispinar/BIL673/msids.pdf (Ocak 2009)

Onur OKTAY, "**Türkiye'de Hacker Grupları ve Faaliyetleri-1**", http://turk.internet.com/haber/yazigoster.php3?yaziid=16661 (Eylül 2009)

http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=kamu (Eylül 2009)

"Kamu Yönetimi", http://www.ekodialog.com/kamu_yonetimi/kamu_yonetimi_nedir.html (Mayıs 2009)

"Kamu Güvenliği", http://sozluk.bilgiportal.com/nedir/kamu%20güvenliği (Mayıs 2009)

http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=millet (Mayıs 2009)

http://tdk.gov.tr/TR/Genel/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=toplum (Haziran 2009)

"**Bilgi Toplumu Ve Özellikleri**", http://www.canaktan.org/yeni-trendler/bilgi-toplumu/bilgi_toplumu-ozellik.htm (Temmuz 2009)

http://www.maltepe.edu.tr/05_haber/reh_sempozyum/gulbahar_gul.doc (Temmuz 2009)

"İletişim Altyapısı", http://www.bilisimsurasi.org.tr/altyapi/docs/iletisim_altyapisi_taslak_raporu_20040219.doc (Aralık 2009)

"Bilgi Toplumu", http://ansiklopedi.turkcebilgi.com/Bilgi_toplumu (Ocak 2010)

http://www.bddk.org.tr/WebSitesi/turkce/Raporlar/Calisma_Raporlari/Calisma_Raporlari.aspx (Şubat 2010)

Onur YILMAZ, **"Yazılımcılar ve Denetimciler için Web Uygulamaları Güvenliği",** http://docs.google.com/Doc?id=d4w2g9c_1hpj4w7ft (Eylül 2009)

http://www.webappsec.org/ (Şubat 2010)

Sertaç ÖZİNAL, **"PCI DSS Nedir? ",** http://www.btnet.com.tr/wps/portal/teknoloji-ekonomisi/egilimler/detay?wcm.haberId=btnethaber_1231424270390 (Mart 2009)

"**Uygulama Güvenliği**", http://fentanyl.wordpress.com/2009/04/29/uygulama-guvenligi/ (Haziran 2009)

"Devlet Nedir?", http://www.atamizindeyiz.com/03/ata03.htm (Ekim 2009)

Mert DUMAN, **"Devlet Nedir?",** http://www.habercumhuriyeti.com/yazar/MERT-DUMAN/642/Devlet-Nedir-Ne-Is-Yapar.html (Ekim 2009)

"Devlet Nedir?", http://www.etarih.net/tr/vatandaslik/devletnedir.html (Ekim 2009)

https://www.turkiye.gov.tr/static/sss/001.html (Ekim 2009)

https://www.turkiye.gov.tr/static/sss/004.html (Mayıs 2010)

"E-Devlet Nedir?", http://www.makaleler.com/oku-edevlet+nedir (Eylül 2009)

Demokaan DEMİREL, "**E-Devlet ve Dünya Öernekleri**", http://www.sayistay.gov.tr/yayin/dergi/icerik/der61m6.pdf (Ağustos 2009)

Özgür UÇAN, "**E-Devlet, E-Demokrasi Ve E-Yönetişim Modeli: Bir İlkesel Öncelik Olarak Bilgiye Erişim Özgürlüğü**", http://www.stradigma.com/turkce/haziran2003/makale_09.html (Ağustos 2009)

"İletişim Altyapısı Raporu", http://www.telkoder.org.tr/2-report/iletisim.doc (Temmuz 2009)

"Portal Nedir?", http://www.pbs.com.tr/DesktopDefault.aspx?tabid=395 (Temmuz 2009)

"Portal Nedir?", http://www.odakdizayn.com/portal_tasarimi (Temmuz 2009)

https://www.turkiye.gov.tr/static/sss/002.html (Şubat 2009)

https://www.turkiye.gov.tr/static/sss/005.html (Şubat 2009)

https://www.turkiye.gov.tr/static/sss/003.html (Ocak 2009)

Mehmet Gençer, "**Türkiye İnternet Sitelerinde Standartlara Uyumluluk: Karşılaştırmalı Ölçümler ve Stratejik Açılımlar**", http://www.cs.bilgi.edu.tr/~mgencer/pub/inet06trpaper.pdf (Mart 2009)

Osman ÇAKIR, "**OSI Modeli-OSI Katmanları Nelerdir?**", http://www.osmancakir.net/osi-modeli-osi-katmanlari-nelerdir-82.html (Mart 2010)

http://bilisimsurasi.org.tr/listeler/tbs-hukuk/Feb/att-0002/01-e-devlet_hukuki_altyapi.doc (Eylül 2009)

İlker TEMİR, "**Türkiye Internetinde Tercih Edilen Web Sunucuları**", http://www.ilkertemir.com/websurvey/current/ (Mart 2010)

"**Tahrifat İstatistikleri**", http://www.zone-h.org/news/id/4735 (Haziran 2010)

http://www.zone-h.org/stats/notifier (Haziran 2010)

Diğer

Broadband Internet Access in OECD Countries: A Comparative Analysis, A Staff Report of the Office of Strategic Planning and Policy Analysis and International Bureau, October 2003 http://hraunfoss.fcc.gov/edocs_public/attachmatch/DOC-239660A2.pdf (Mart 2009)

5070. Sayılı Elektronik İmza Kanunu
http://www.tbmm.gov.tr/kanunlar/k5070.html (Nisan 2009)

5809. Sayılı Elektronik Haberleşme Kanunu,
http://www.tbmm.gov.tr/kanunlar/k5809.html (Nisan 2009)

2003/10 sayılı Bilgi Sistem ve Ağları İçin Güvenlik Kültürü Genelgesi
http://www.basbakanlik.gov.tr/genelge_pdf/2003/2003-0320-02789.pdf (Mayıs 2009)

Akademik Bilişim 2008 Sempozyumu Sunumları, Çanakkale Onsekiz Mart Üniversitesi, Çanakkale http://ab.org.tr/ab08/bildiri/49.doc (Nisan 2009)

"**E-Devlete Geçişte Kamu Kurumları İnternet Siteleri Performans Denetimi Raporu**", T.C. Sayıştay Başkanlığı, Ankara, 2006 http://www.sayistay.gov.tr/rapor/perdenrap/2006/2006-2Web/2006-Web.pdf (Ocak 2010)

"**Türkiye Raporu**", ComScore Şirketi, Mayıs 2009 http://www.comscore.com/Press_Events/Press_Releases/2009/5/Turkey_has_Seventh_Largest_Online_Audience_in_Europe/(language)/eng-US (Mayıs 2009)

"**Benchmarking Research Study TNS Consultants**" Goverment Online Şirketi, 2001, http://www.bibliotheque.assnat.qc.ca/01/mono/2010/02/1022345.pdf (Mart 2009)

"**Ankara Raporu**", Türkiye 2. Bilişim Şurası, 10-11 Mayıs 2004, http://www.scribd.com/doc/17017490/2-Bilisim-Surasi-Taslak-Raporu (Mayıs 2009)

"**İletişim Altyapısı Raporu**", Türkiye 1. Bilişim Şurası, 10-12 Mayıs 2002, http://bilisimsurasi.org.tr/cg/rapor/iletisim.zip (Mart 2009)

"**E-Devlet Çalışma Grubu Raporu**", Türkiye 1. Bilişim Şurası, 10-12 Mayıs 2002, http://bilisimsurasi.org.tr/cg/rapor/iletisim.zip (Mart 2009)

"**Özelleşme, Serbestleşme ve Düzenleme Etkileşim Raporu**", Telekomünikasyon Kurumu, Mayıs 2003, http://www.tk.gov.tr/Yayin/Raporlar/pdf/ozellesme.pdf (Haziran 2009)

"**Computer Crime And Security Survey**", Computer Security Institute, 2009, http://gocsi.com/survey (Aralık 2009)

"**Computer Crime And Security Survey**", Computer Security Institute, 2006, http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf (Mart 2009)

"**Erişim Başına Kamu Telekomünikasyon Geliri**", OECD Raporları, Ağustos 2009, http://www.bitdunyasi.com/tr/?Sayfa=Detay&Id=2705 (Aralık 2009)