T.C.
BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

Yüksek Lisans Tezi

SİBER SUÇLARIN EKONOMİK BOYUTU: ZONGULDAK ÖRNEĞİ

Muhammed Temli

Zonguldak 2017

T.C.
BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İKTİSAT ANABİLİM DALI

Yüksek Lisans Tezi

SİBER SUÇLARIN EKONOMİK BOYUTU: ZONGULDAK ÖRNEĞİ

Hazırlayan
Muhammed Temli

Tez Danışmanı
Yrd. Doç. Dr. Zafer Öztürk

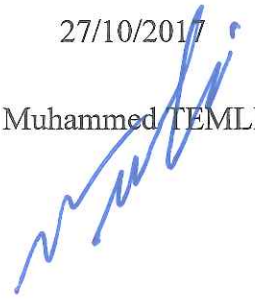
Zonguldak 2017

BİLİMSEL ETİK BİLDİRİMİ

Hazırladığım Yüksek Lisans Tezinin bütün aşamalarında bilimsel etiğe ve akademik kurallara riayet ettiğimi, çalışmada doğrudan veya dolaylı olarak kullandığım her alıntıya kaynak gösterdiğimi ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu, yazımda enstitü yazım kılavuzuna uygun davranıldığını taahhüt ederim.

27/10/2017

Muhammed TEMLI



TEZ ONAY SAYFASI

T.C.
BÜLENT ECEVİT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

TEZ ONAYI

Enstitümüzün İktisat Anabilim Dalında 125282102005 numaralı Muhammed TEMLİ'nin hazırladığı "**Siber Suçların Ekonomik Boyutu: Zonguldak Örneği**" konulu YÜKSEK LİSANS tezi ile ilgili TEZ SAVUNMA SINAVI, Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği uyarınca 27/10/2017 Cuma günü saat 14:00'de yapılmış, sorulan sorulara alınan cevaplar sonunda tezin onayına OYBİRLİĞİYLE/~~OYÇOKLUĞUYLA~~ karar verilmiştir.

Başkan_____
Doç. Dr. Selçuk KOÇ

Üye_____
Doç. Dr. Mehmet PEKKAYA

Üye_____
Yrd. Doç. Dr. Zafer ÖZTÜRK (Danışman)

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

.../.../2017
Doç. Dr. Ertuğrul YILDIRIM
Enstitü Müdürü

ÖZET

Kurum : BEÜ Sosyal Bilimler Enstitüsü, İktisat Anabilim Dalı
Tez Başlığı : Siber Suçların Ekonomik Boyutu: Zonguldak Örneği
Tez Yazarı : Muhammed Temli
Tez Danışmanı : Yrd. Doç. Dr. Zafer Öztürk
Tez Türü, Yılı : Yüksek Lisans Tezi, 2017
Sayfa Adedi : 146

Günümüzde suç ekonomisinin kapsamı ve hacmi önemli boyutlara ulaşmıştır. Gelişen teknolojiyle birlikte birçok suç türü internet ortamına taşınmıştır. Suçlunun mağdura birebir temas etmesini gerektiren suç çeşitlerinin internet ortamına taşınması suç ekonomisini içerik, kapsam ve boyut olarak genişletmektedir. Her gün artan siber saldırılar, ortaya çıkardıkları ekonomik etkiler nedeniyle kayıt dışı ekonominin önemli bir kısmını oluşturmaktadır. Kredi kartı dolandırıcılığı, banka hesaplarının boşaltılması, kullanıcının bilgisayarındaki verileri şifreleyerek tekrar aynı kullanıcıya satılmasını sağlayan cryptolocker virüsleri, DDOS atakları gibi web siteleri ve e-ticaret sitelerinin kullanımının engellenmesi, casusluk, bilgi kaçakçılığı ve yeni türemiş birçok bilişim suçu bu alana örnek olarak gösterilebilir. Çalışma ile Zonguldak ilinde faaliyet gösteren firmaların siber saldırılar nedeniyle uğradıkları maddi zararların ekonomik boyutunun ortaya çıkartılması amaçlanmıştır.

Çalışmada, firma ölçekleri büyüdükçe daha yoğun teknoloji ve bilişim altyapısına ihtiyaç duyulacağı öngörüldüğünden veriler Zonguldak ilinde 20'den fazla personel çalıştıran 336 firmaya TÜİK tarafından anket yöntemi uygulanarak elde edilmiştir. Anket sonuçlarını Ki-Kare Testi, korelasyon tablosu, Çoklu Doğrusal Regresyon ve bağımsız iki grup arası farkların testi (t testi) yöntemleri SPSS programı kullanılarak analiz edilmeye çalışılmıştır. Çalışmanın sonucunda firmaların çoğunun saldırılar konusunda yeterli bilgisi olmadığı görülmüştür. Firmaların yarıdan fazlasının marka ya da firma adını taşıyan kurumsal e-posta kullanmadığı kaydedilirken sistemi durduran en etkin saldırıların e-posta ve virüs saldırıları olduğu ve en yüksek maddi kayba yol açan saldırılar olarak gerçekleştiği sonucuna ulaşılmıştır. Bu sonuçlar çerçevesinde saldırıların tespit ve kaydedilmesini sağlayan yöntemlerin kullanımının artırılması gerektiği görülmüştür.

Anahtar Kelimeler: Kayıt dışı ekonomi, Suç Ekonomisi, Siber Güvenlik, Siber Saldırılar, Bilişim Teknolojisi

ABSTRACT

Institution	: BEÜ Institute of Social Sciences, Department of Economics
Title	: The Economic Dimension of Cyber Crime: The Case of Zonguldak
Author	: Muhammed Temli
Adviser	: Assist. Prof. Zafer Öztürk
Type of Thesis, Year	: MSc. Thesis, 2017
Number of pages	:146

Today, the scope and volume of the crime economy has reached important dimensions. Along with the developing technology, many crime types have been moved to the internet environment. Moving the types of crimes that require criminals to contact each other in an internet environment expands the crime economy in terms of content, scope and dimension. Increasing daily cyber attacks constitute a significant part of the informal economy because of the economic effects they emerge. Examples include fraudulent credit card fraud, the evacuation of bank accounts, cryptolocker viruses that enable users to sell data to the same user again by encrypting the data on their computer, preventing the use of websites and e-commerce sites such as DDOS attacks, espionage, information trafficking and many new computer crimes. The aim of the study is to reveal the economic dimension of the financial losses of companies operating in the province of Zonguldak due to the cyber attacks.

Since the company is expected to require more intensive technology and information infrastructure as the scale of the company grows, 336 firms employing more than 20 personnel in the province of Zonguldak have been obtained by applying the survey method by Turkish Statistical Institute (TSI). The results of the questionnaire were tried to be analyzed using the SPSS program, Chi-Square test, correlation table, Multiple Linear Regression and independent two-group difference test (t test) methods. As a result of the work the majority of the companies did not have enough information about the attacks. While more than half of the companies do not use corporate email with the brand or company name, the most effective attacks that stop the system are email and virus attacks and the result of the attacks that caused the most material loss. It has been seen that the use of methods to detect and record attacks in the framework of these results should be increased.

Keywords: Informal Economy, Crime Economy, Cyber Security, Cyber Attacks, Information Technology

ÖNSÖZ

"Siber Suçların Ekonomik Boyutu: Zonguldak Örneği" konulu tez çalışmamın her aşamasında değerli görüşleri ve eleştirileri ile bana yol gösteren değerli hocam Yrd. Doç. Dr. Zafer ÖZTÜRK'e

Akademik hayatım ve tez çalışmam sırasında bana olan sonsuz güvenleri ve her daim teşviklerinden dolayı sevgili eşim Sibel TEMLİ'ye, destekleri ile her daim motive eden kardeşlerim Mustafa TEMLİ ve Hatice TEMLİ'ye çalışmalarım sırasında vakitlerinden fedakârlık eden çocuklarım Fatih Eymen ve Elif Beril TEMLİ'ye;

Çalışmaya verdiği yapıcı ve olumlu katkılardan ve yönlendirmelerinden dolayı Hasan Özgür OPSAR, Recep Serkan ALKAN, Hakkı Yavuz TOPLU, Doç. Dr. Mehmet PEKKAYA ve TÜİK Bölge Müdür V. Ali GÜNAYDIN'a sonsuz teşekkür ederim.

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

Sayfa

ŞEKİLLER LİSTESİ

Sayfa

GRAFİKLER LİSTESİ

KISALTMALAR LİSTESİ

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
AET	:	Avrupa Ekonomik Topluluğu
AFAD	:	Afet ve Acil Durum Yönetimi Başkanlığı
AKKY	:	Açık Kaynak Kodlu Yazılım Çözümü
AR-GE	:	Araştırma ve Geliştirme
ARPA	:	Gelişmiş Savunma Araştırmaları Projeleri Birimi
ARPANET	:	Gelişmiş Araştırma Projeleri Dairesi Ağı
ATM	:	Automated Teller Machine (Otomatik Vezne Makinası)
BM	:	Birleşmiş Milletler
BTK	:	Bilgi Teknolojileri Kurumu
CD	:	Compact Disc
CERT	:	Certificate of Conformity
CIA	:	Central Intelligence Agency (Merkezi İstihbarat Teşkilatı)
CIH	:	Cernobyl Virüsü
CSIS	:	Uluslararası ve Stratejik Araştırmalar Merkezi
DDOS	:	Distributed Denial of Service (Dağıtılmış Hizmet Reddi)
DVD	:	Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
EGM	:	Emniyet Genel Müdürlüğü
Eurostat	:	Avrupa İstatistik Ofisi
FBI	:	Federal Soruşturma Bürosu
FTP	:	File Transfer Protocol (Dosya Transfer Protokolü)
GSMH	:	Gayri Safi Millî Hasıla
HDD	:	Hard Disk Drive (Sabit Disk Sürücüsü)
http	:	Hyper Text Transfer Protocol (Hiper Metin Transferi Protokolü)
ICA	:	Citrix firmasının çıkarmış olduğu bağlantı protokolü
IMAP	:	Internet Message Access Protocol (İnternet Mesaj Erişim Protokolü)
IoT	:	Internet of Things (Nesnelerin İnterneti)
IP	:	Internet Protocol Address (İnternet Protokol Adresi)
IT	:	Information Technology (Enformasyon Teknolojileri)
İSMMMO	:	İstanbul Serbest Muhasebeci Mali Müşavirler Odası
MIMIC	:	Multiple Indicators and Multiple Causes
MMF	:	Make Money Fast
NCCS	:	National Computer Crime Squad (Ulusal Bilgisayar Suçu Ekibi)
ODTÜ	:	Orta Doğu Teknik Üniversitesi
OECD	:	Ekonomik Kalkınma ve İşbirliği Örgütü
P2P	:	Peer to Peer (Uçtan Uca İletişim)
PIN	:	Personel Identification Number (Kimlik Numarası)
RDP	:	Remote Desktop Protocol (Uzak Masaüstü Protokolü)

SCADA	:	Supervisory Control And Data Acquisition (Merkezi Denetim ve Veri Toplama)
SGK	:	Sosyal Güvenlik Kurumu
SMTP	:	Simple Mail Transfer Protocol (Basit Posta Aktarım Protokolü)
SOME	:	Siber Olaylara Müdahale Ekipleri
SWIFT	:	Society For Worldwide Interbank Financial Telecommunications
T.C.	:	Türkiye Cumhuriyeti
TBMM	:	Türkiye Büyük Millet Meclisi
TCK	:	Türk Ceza Kanunu
TCP/IP	:	Transmission Control Protocol/Internet Protocol (İnternet Protokolü)
TOPSIS	:	Technique for Order-Preference by Similarity to Ideal Solution
TSE	:	Türk Standartları Enstitüsü
TÜBİTAK	:	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
TÜİK	:	Türkiye İstatistik Enstitüsü
TV	:	Televizyon
UBE	:	Unsolicited Bulk E-mail (İstenmeyen Toplu e-posta)
UCE	:	Unsolicited Commercial e-mail (İstenmeyen Ticari e-posta)
UNICEF	:	Birleşmiş Milletler Genel Kurulu tarafından çocuk haklarının savunuculuğunu yapan kuruluş
URL	:	Uniform Resource Locator (Tekdüzen Kaynak Bulucu)
USB	:	Universal Serial Bus (Evrensel Seri Veriyolu)
USOM	:	Ulusal Siber Olaylara Müdahale Merkezi
WEB	:	World Wide Web (www)
WIPO	:	World Intellectual Property Organization (Dünya Fikri Mülkiyet Örgütü)
xDSL	:	Digital Subscriber Line (Sayısal Abone Hattı)

GİRİŞ

Günümüzde gelişmiş ya da gelişmekte olan ülkelerin karşılaştıkları en önemli ekonomik sorunlardan biri de kayıt dışı ekonomidir. Kayıt dışı ekonomik faaliyetler en genel şekliyle Gayri Safi Milli Hâsıla (GSMH) hesaplamalarına dâhil edilmeyen tüm ekonomik faaliyetler olarak tanımlanmaktadır. Kayıt dışı ekonominin enformel yapısının yanında suç teşkil eden yapısı da bulunmaktadır. Enformel ekonomi yasal olarak gerçekleşen faaliyetler sonucu elde edilirken denetim mekanizması ya da mevzuattan kaynaklı bazı yasal boşluklar nedeni ile vergilendirilmeyen gelirlerden oluşmaktadır. Fakat kayıt dışı ekonominin içerisinde yer alan suç ekonomisi kapsamında ise kanunen suç sayılan faaliyetlerin sonucunda elde edilen ekonomik gelirler bulunmaktadır.

Devletin işleyen yapısına zarar verirken aynı zamanda toplumsal huzuru da bozan suç ekonomisinin literatürde birden çok tanımı bulunsa da özet olarak iktisadi menfaatlerinin ihlâl edilmesinden dolayı ortaya çıkan ekonomik faaliyet olarak ifade edilebilir. Suç ekonomisi de kayıt dışı ekonomi gibi kendi içinde farklılık göstermektedir. Üretim ve dağıtım yöntemleri yasal olmayan suç ekonomisi türüne illegal sektör, organize suç şebekeleri tarafından yürütülen kanun dışı faaliyetlerin oluşturduğu tür ise kriminal sektör olarak adlandırılmaktadır. Teknolojinin gelişmesi ve her alanda yoğun kullanımı ile birlikte suç ekonomisinin kapsamı ve hacmi önemli boyutlara ulaşmıştır. Birçok suç türünün internet ortamına taşınması ile birlikte kriminal sektörün boyutu daha da büyümüş ve faaliyetleri on binler ile ifade edilen illegal şebekeler tarafından yürütüldüğü gözlemlenmiştir (Mavral, 2001:176). Suçlunun mağdura birebir temas etmesini gerektiren birçok suç artık internet aracılığı ile uzaktan işlenebilmektedir. Bu nedenle ekonomik etkilere sahip olan bilişim suçları diğer ismi ile siber suçlar içerik, kapsam ve hacim olarak önemli boyutlara ulaşmıştır.

Siber suçlardan kaynaklı ekonomik faaliyetler suç ekonomisinin ve dolayısı ile kayıt dışı ekonominin önemli bir kısmını oluşturmaya başlamıştır. Kredi kartı dolandırıcılığı, banka hesaplarının boşaltılması, kullanıcının bilgisayarındaki verileri şifreleyerek tekrar aynı kullanıcıya satılmasını sağlayan cryptolocker virüsleri, dünya devi şirketlere yapılan siber saldırılar, DDOS atakları ile web

siteleri ve e-ticaret sitelerinin kullanımının engellenmesi, casusluk, bilgi kaçakçılığı ve yeni türemiş birçok siber saldırılar bu alana örnek olarak gösterilebilir. Siber suçların ekonomik boyutları tam olarak kestirilemediği için suç ekonomisinin ne kadarını siber suçların oluşturduğu tam olarak bilinmeyip, bazı verilere göre tahmin edilmektedir.

Örneğin İngiltere'de yapılan bir çalışmada işletmelerin %52'sinin 2016 yılı içerisinde siber saldırıya maruz kaldığı ve yaklaşık 29,1 milyar GBP maddi zarara uğradığı (Kiveko, 2017), Amerika Birleşik Devletlerinin (ABD) ise bir günlük siber saldırı (DDOS) nedeni ile 7 milyar dolar zarara uğradığı kaydedilmiştir (Ensonhaber, 2016). Türkiye'de de durum çok farklı değildir. 2016 yılının ilk altı ayında Türkiye'nin 110 binden fazla siber saldırı yaşadığı raporlanırken, Türkiye'ye yönelik büyük boyutlu siber saldırıların çoğunluğunun ABD, Rusya, Almanya ve yurt içi kaynaklı yapıldığı bilgisine erişilmiştir (STM, 2017). Ülkemizde faaliyette bulunan 250 firmanın katılımıyla gerçekleştirilen bir araştırmaya göre, son beş yıllık dönemde siber saldırıların sayısı ile birlikte ülke ekonomisine yönelik saldırıların arttığı da tespit edilmiştir. STM firmasınan araştırmasına göre, firmaların % 47'si, 2011-2016 yılları arasında karşılaştıkları siber saldırıların sayısında ciddi artış olduğunu bildirmişlerdir. Rapordaki diğer bir sonuca göre ise sadece zararlı yazılımlar ve kötü niyetli saldırganlar tarafından değil, aynı zamanda çalışanlar da istemeden şirketlerinin siber güvenliklerini tehdit etmektedirler (STM, 2017). IBM yetkililerinin açıklamalarına göre dakikada 4.800 cihazın birbirine bağlandığı internet ortamında yaşanan siber saldırıların dünyaya maliyetinin 2,1 trilyon doları bulabileceği belirtilmiştir (Hürriyet, 2017).

Siber saldırılar tüm dünyada ve ülkemizde artış gösterdiği gibi Zonguldak ilinde de artış göstermektedir. Yapılan akademik çalışmalarda 1990 - 2011 yılları arasında Türkiye çapında bilişim sistemleri banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçundan 24.254 dava, başkasına ait banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlama suçundan 14.166 dava açılmıştır. Zonguldak ilinde ise 2002 ve 2004 yıllarında 1'er, 2005 yılında 12, 2006 yılında 44, 2007 yılında 59, 2008 yılında 82, 2009 yılında 95,

2010 yılında 108, 2011 yılının temmuz ayına kadar ise 79 bilişim suçları ile ilgili dava olduğu kaydedilmiştir (İlbaş ve Köksal, 2011).

Bu çalışma, yıllar itibariyle sayısı giderek artan siber saldırıların Zonguldak ilinde sebep olduğu ekonomik zararların boyutunu ortaya çıkarmak amacı ile yapılmıştır. Siber saldırıların ekonomik büyüklüğü hakkında net bilgi verecek kamu ya da özel sektörde herhangi bir kurum bulunmadığından veriler anket yolu ile elde edilmeye çalışılmıştır. Anket uygulaması siber saldırılarla karşılaşma ihtimali yüksek olan özel firmalar ile gerçekleştirilmiştir. Anket yapılacak firma seçiminde firma büyüklüğü dikkate alınmıştır. Özellikle personel sayısının artması ile kullanılan bilişim altyapılarının büyüyeceği öngörülmüştür. Bu öngörü ile bilişim altyapısı büyüyen firmaların siber saldırılardan daha çok etkileneceği tahmin edilmiştir. Araştırma Zonguldak ilinde 20'den fazla personel çalıştıran 336 firmaya, bilişim altyapısına verdiği önemi ve karşılaşılan siber saldırıları tespit etmek amacı ile yerinde anket uygulanarak TÜİK Zonguldak Bölge Müdürlüğü tarafından gerçekleştirilmiştir.

Konulara göre elde edilen anket verileri, ilgili değişken endeks değerini belirlemek için içeriğindeki konular uzman görüşleri doğrultusunda ağırlıklandırılarak ve TOPSIS (Technique for Order-Preference by Similarity to Ideal Solution) yöntemi kullanılarak değişkenin endeks puanı hesaplanmıştır. Çalışmada nominal ölçekli değişkenler arasında sistematik bir ilişkinin olup olmadığını öğrenmek için ki-kare testi, metrik ölçekli olan endeks değişkenlerinin arasındaki ilişkileri incelemek üzere korelasyon analizi, değişkenler arasındaki ilişkinin modellenmesinin incelenmesinde çoklu doğrusal regresyon analizi kullanılmıştır. Ayrıca endekslenen değişkenlerin alt gruplara göre farklılıkları bağımsız iki örnek t testi ile analiz edilmiştir.

Çalışmanın ilk bölümünde kayıt dışı ekonomi ele alınarak kayıt dışı ekonomiyi ortaya çıkaran nedenler açıklanmıştır. Kayıt dışı ekonominin olumlu ve olumsuz etkilerinin yanı sıra, kamu gelirlerine, işgücü piyasasına ve en önemlisi de sosyal hayata etkisi irdelenmiştir. Ayrıca bu bölümde kayıt dışı ekonominin farklılık gösteren unsurları incelenerek konusu suç olan unsurlardan elde edilen suç ekonomisini oluşturan illegal sektör ve kriminal sektör ayrımlarından bahsedilmiştir. Suç - ekonomi ilişkisi ve ekonomik suç teorilerinin

inceleneceği bu bölüm siber saldırıların bölge ekonomisine etkisinin anlaşılmasına katkı sağlamıştır.

İkinci bölümde bilişim ve bilişim suçlarının türleri açıklanmıştır. Özellikle günümüzde en sık görülen ve suç ekonomisi içerisinde yer alabilecek yetkisiz erişimler, hesap ihlalleri, bankacılık faaliyetlerinin gayrı resmi kullanılması, çocuklara ya da kadınlara yönelik siber zorbalık, taciz ve şantaj, siber terör faaliyetleri, bebek, kadın ve organ ticareti, uyuşturucu ve kaçak silah ticareti gibi siber suçlara değinilerek siber saldırıların yaşanmasında en sık kullanılan yöntemler incelenmiştir.

Son bölüm çalışmanın analiz kısmı olup bu bölümde anket hakkında bilgiler verilerek analiz bulguları üzerinde durulmuştur. Bölümde Zonguldak ilindeki firmaların bilişim suçları nedeni ile uğradıkları ekonomik zararlar irdelenirken bilgi işlem alt yapılarına gösterilen önem de incelenmiştir.

Çalışmanın sonuç bölümünde ise, elde edilen bulgular kamuoyuna sunulup bu doğrultuda siber saldırıların gerek Zonguldak gerekse ülkemiz açısından yol açtığı kayıp vurgulanmıştır.

1. KAYIT DIŞI EKONOMİ VE SUÇ EKONOMİSİ

1.1. Kayıt Dışı Ekonomi

Çağımızda ulusal ve uluslararası alanda ismini sıkça duyduğumuz kayıt dışı ekonomi ile ilgili çalışmalar 1970'li yıllarda artsa da bu konudaki ilk araştırma Philliph Cagan'nın, Amerika Birleşik Devletlerinde (ABD) 2. Dünya Savaşı yıllarındaki bildirimi yapılmamış gelirlerin parasal karşılığını tahmin etmeye yönelik çalışmasıdır (Ilgın, 1995:1).

Kayıt dışı ekonomi literatürde kavramsal olarak birçok şekilde tanımlanmaktadır. Yabancı kaynaklarda, gizli ekonomi (clandestine economy), ikili ekonomi (dual economy), gizli ekonomi (submerge economy), kara ekonomi (black economy), nakit para ekonomisi (cash economy), yeraltı ekonomisi (subterranean economy), paralel ekonomi (parallel economy), gölge ekonomi (shadow economy), alt ekonomi (subeconomy), gri ekonomi (gray economy), gizli ekonomi (hidden economy) gibi kavramlarla ifade edilmektedir (Ilgın, 1999:8). Ayrıca İtalya′da ″lavoro nero″ yani ″kayıt dışı″, Almanya′da ″schwarzarbeit″ yani ″ikinci işte çalışma″, eski Sovyet Ülkeleri'nde ″parallel, secondary″ yani ″parelel ve ikincil ekonomi″ tanımlamaları yapılmaktadır (NAS, 2014:66).

Yukarıda sayılan gizli ekonomi, görünmeyen ekonomi, yeraltı ekonomisi, gibi kavramlar daha çok ana başlık olan kayıt dışı ekonomiyi ifade etmekte iken, kural dışı ekonomi, gayri resmi ve hane halkı ekonomisi gibi kavramlar kayıt dışı ekonominin içerisindeki değişik özelliklere vurgu yapmak için kullanılmaktadır (Dinçer, 2007:4).

Özsoylu (1994:14) gayri safi milli hâsıla hesaplamalarına dâhil edilmeyen tüm ekonomik faaliyetleri kayıt dışı olarak ifade etmektedir. Akalın (1996:29) ise kayıt dışı ekonomiyi kamunun piyasaya sert müdahalesi nedeni ile firmaların elde ettiği gelirin, milli gelire dâhil edilmemesi olarak tanımlamaktadır. Maliye Bakanlığı Gelir İdaresi Başkanlığı, 2008 – 2010 yıllarını kapsayan Kayıt Dışı Ekonomi ile Mücadele Stratejisi Eylem Planında kayıt dışı ekonomiyi, resmi makamlardan gizlenen ve bu nedenle kamu tarafından kontrol edilemeyen

faaliyetler olarak tanımlamaktadır. Kısaca kayıt dışı ekonomi devlet mekanizmalarının denetiminin dışında olan tüm ekonomik faaliyetler olarak tanımlanabilir.

Avrupa İstatistik Ofisi (Eurostat), Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) gibi kurumların yaptığı tanımlar da bulunmaktadır. Eurostat tarafından kabul edilen kavramlar Eurostat Ulusal Hesaplar Çalışma Grubu tarafından 1980 yılındaki çalışmaları neticesinde oluşmuştur. Eurostat, kara ekonomiyi ibraz edilmemiş ekonomik faaliyet olarak tanımlamaktadır. Eurostat tanımlamasında yeraltı ekonomisi, bildirilmemiş legal üretim faaliyetleri ile illegal (yasadışı) üretim faaliyetlerini kapsamaktadır (UNECE, 1993:1).

Kayıt dışı ekonomi, vergiden muaf tutulmuş olan enformel ekonomi ile birlikte suç ekonomisini de içermektedir. Suç ekonomisi, silah kaçakçılığı, uyuşturucu kaçakçılığı, tarihi eser kaçakçılığı gibi örgütlü suçlar ile birlikte hırsızlık, gasp, yankesicilik, alıkoyma gibi adi suçlardan oluşan kazançları da ifade etmektedir. Enformel ekonomi ise üretimi ve tüketimi yasal olan ancak işportacılık gibi alım-satımı vergilendirilmemiş gelirlerin toplamı olarak açıklanabilir. Kapsam olarak kayıt dışı ekonomik faaliyetler uyuşturucu ticareti, kahinlik, vergi kaçakçılığı, kişinin vücudunun parçalarını satması gibi yasadışı faaliyetlerin yanı sıra akrabalara yada başkalarına yardım, günlük ev işlerinin yapılması gibi zararsız faaliyetlerden de oluşabilmektedir (Özsoylu, 1996:10).

Kayıt dışı ekonominin, içerdiği faaliyetlerin kapsamından dolayı, kolay anlaşılabilir bir tanımı yapılamamaktadır (Çokgezen, 1993:22). Kayıt dışı ekonomi evrensel bir olgu olarak ve dünya genelinde gözlenmektedir.

1.2. Kayıt Dışı Ekonominin Nedenleri

Kayıt dışı ekonominin nedenleri ülkeden ülkeye farklılık göstermektedir. Gelişmiş ülkeler ve gelişmekte olan ülkelerdeki kayıt dışı ekonomi olgusu birbirinden farklıdır. Gelişmekte olan ülkelerde vergiden kurtulmak asıl neden olmakla birlikte gelişmiş ülkeler üzerine yapılan çalışmaların büyük kısmında vergi kaçırmanın yanı sıra yasal düzenlemelerden kaçmak içinde kayıt dışına yönelmeler mevcuttur (Losby vd., 2002).

Kayıt dışı ekonominin ülkelerde gelişmesinin birden çok sebebi vardır. Ülkelerde bulunan yasal düzenlemeler öncelikli olmakla birlikte ekonomik istikrarsızlık, düşük gelir düzeyi, yasal düzenlemelerin net olmaması, sosyal güvenlik yükleri, vergi dairelerin durumu ve tutumu, erken emeklilik, kayıt dışılığın kabul görmesi, vasıfsız iş gücü, rüşvet ve yolsuzluk gibi nedenler sebep olarak gösterilebilmektedir.

Enformel ekonomik faaliyetin ortaya çıkmasına, fayda-maliyet analizi açısından bakıldığında temel neden şöyle açıklanabilir. Kaynaklar enformel ekonomide kullanılırsa net kazanç "K", kayıtlı ekonomide kullanıldığında "R" olduğu kabul edilirse ve "K>R" olursa firmalar enformel ekonomik faaliyete yönelecektir (Dura, 1997:5).

Kayıt dışı ekonominin daha detaylı incelenmesi için ülkelerin içinde bulunduğu mevcut durumların mali, ekonomik ve sosyal yönden değerlendirilmesi gerekir. Johnson vd. (2000:496) tarafından yapılan çalışmada işletmelerin neden enformel sektörde yer aldığı ile ilgili olarak dört madde belirlenmiştir. Çalışmada vergi oranlarının yüksek olması, kayıtlı firmalardan rüşvet alma çabaları, girişimcilerin mafyaya haraç vermemek için gelirlerinin bir miktarını gizlemesi ve kurumsal çerçevenin yetersizliği sebep olarak ileri sürülmüştür. Kahya ve Irmak (2014:18) ise çalışmalarında kayıt dışı ekonomiye neden olan faktörleri çeşitli kaynaklardan toplamışlardır. Bu faktörler Tablo 1.1'de gösterilmektedir.

Tablo 1.1:Kayıt Dışı Ekonominin Nedenleri

Ekonomik nedenler	- Yüksek enflasyon, - İşsizlik oranlarının yüksek olması, - Ekonomik istikrarsızlıklar, - Gelir düzeyinin düşük oluşu, - Adil olmayan vergiler, - Rekabet koşulları,
Kanuni nedenler	- Mevzuattan kaynaklanan boşluklar, - Vergi kaçırma imkanları, - Vergilerdeki yüksek oranlar, - Sosyal güvenlik masrafları, - Vergide istisna uygulamaları,
Yönetimsel nedenler	- İktidarın ülke yönetimindeki hataları, - Vergi dairelerinin hantallığı, - Teknik kapasite, - Niteliksiz personel, - Kamunun yetersiz hizmet anlayışı
Sosyal nedenler	- Vergi ahlakı, - Göçler, - Vasıfsız iş gücü, - Rüşvet, - Mükellef psikolojisi, - Tarihsel nedenler,
Siyasi nedenler	- Baskı grupları.

Kaynak: Kahya, Yavuz ve Fatih Irmak (2014), "Kayıt Dışı Ekonomi ve Suç Örgütlenmeleri İlişkisinin Sosyolojik Açıdan Değerlendirilmesi," *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi* 2014:353.

Kayıt dışı ekonominin ortaya çıkmasına yol açan en önemli sebeplerin başında ekonomik nedenler gelmektedir. Ekonomik nedenleri kanuni nedenler, yönetimsel nedenler, sosyal nedenler ve siyasi nedenler takip etmektedir.

1.2.1. Ekonomik ve Mali Nedenler

Kayıt dışı ekonominin ortaya çıkmasına yol açan önemli sebeplerin başında ekonomik faktörler gelmektedir. Gelişmekte olan ülkelerde genellikle gelir adaletsizliği bulunmaktadır. Kayıtlı olarak çalıştığı işten aldığı ücretin yetersiz olduğu durumda bireylerin ilave olarak farklı bir işte çalışması kayıt dışına sebep olmaktadır. Gelir dağılımından düşük pay alan bireyler ise geçim standardını yakalamak için enformel sektör içerisinde yer almaktadır. Özellikle tarım sektöründe çocuk ve kadın işçilerin yoğunluklu çalıştığı görülmektedir (Us, 2004:11).

Ekonomik nedenler arasında yer alan diğer bir sebep ise işsizliktir. Köylerden kentlere göç nedeni ile şehirlerde işsizlik oranında artışlar yaşanmaktadır. Kayıt dışı ekonomiye giriş çıkışların maliyetinin düşük olması

işsiz olan bireyleri kayıt dışı çalışmaya sevk etmektedir (Önder, 2012:15). Bu nedenle kayıt dışı ekonomi ile işsizlik arasında pozitif bir ilişki bulunmaktadır (Kahya ve Irmak, 2014:354).

Kayıt dışına iten nedenlerden bir diğeri de enflasyonun yüksek olmasıdır. Yüksek enflasyon ödenecek vergi miktarını da değiştirmektedir. Çünkü verginin hesaplanmasında kullanılan bazı oranlar enflasyonun etkisi ile artmaktadır (Karaman, 1999:431). Diğer taraftan yüksek enflasyon girdi maliyetlerini de artırmaktadır. Girdi maliyetlerini borçlanarak ödeyen firmalar kredi maliyetlerinin de yüksek olması nedeni ile kayıt dışı yollardan kaynak edinme yoluna gidebilmektedir. Çünkü enflasyonun yüksek olması faiz oranlarının da yüksek olmasına neden olmaktadır (Özcan, 2003:46-48).

Çalışma koşulları kayıt dışılığa sebep olan diğer bir faktördür. Kayıtlı sektörde sosyal güvenlik için hem işverenden hem işçinin alacağı ücretten kesintiler olmaktadır. Bu kesintiler sosyal güvenlik sisteminin işlemesi için kullanılmaktadır. Ancak bu kesintiler olumsuz sonuçlar da doğurmaktadır. SGK ödemeleri gelire göre yüksek külfet oluşturduğundan firmaları kayıt dışına itmektedir. Diğer taraftan birtakım faaliyetlerin tespitinin zor olması ve iş hacminin küçük görülmesi de kişileri sosyal güvenlik sisteminin dışına yönlendirmektedir. Ev hanımlarının kendi ailesi için yaptığı işler, komşusuna ücretsiz yardım eden kişilerin kayıt altına alınmasının imkânsız oluşu kayıt dışı ekonominin oluşmasında olmasa da boyutlarının genişlemesinde en önemli etkenlerinden biri olarak görülmektedir (Mavral, 2001:181).

1.2.2. İdari ve Hukuki Nedenler

Gelir elde edenler dünyanın hiçbir yerinde gelirlerinin büyük bir kısmını vergi olarak ödemek istememektedirler (Aydemir, 1995a:46). Eğer toplum vergi kaçırmayı basit ve sıradan olarak görürse gelir elde edenler gelirlerini kayıt dışına çıkarmakta rahat davranacaklar ve bir suçluluk duymayacaklardır. Kimse gelirlerini azaltacağı için vergi ödemek istemez, vergi devletin yükümlülüklerini yerine getirebilmesi için kanuni haktan doğan bir zorunluluktur (Karaman, 1999:430).

Vergi mevzuatının karmaşıklığı, vergi oranlarında yapılan değişiklikler mükellefleri vergi ödemeye karşı soğutmaktadır. Adam Smith'in vergilemede belirlilik ilkesi, vergilendirme sisteminin net ve kesin olmasını öngörmektedir. Yani vergisel olarak yapılacak her unsur yükümlüler için açık ve şeffaf olmalıdır (Önder, 2012:30).

Diğer taraftan sıklıkla çıkarılan vergi afları da mükelleflerin vergi sistemine bakış açısını değiştirmektedir. Mükelleflerin vergisini ödemesinin ardından yeni bir vergi affı veya zamana yayan taksitlendirme olanakları, vergisini ödeyen mükelleflerin vergi sistemine güvenini azaltmaktadır (DPT, 2007:12). Ayrıca vergisini ödemeyen mükellefler için ödül niteliği taşımaktadır.

Diğer taraftan vergi denetimlerinin etkin bir şekilde yapılması da önem taşımaktadır. Mükelleflerin yasalara uygun hareket edip etmediği vergi denetlemeleri ile mümkündür. Etkin bir şekilde yapılan denetim mükellefleri yasalara uymaya zorlayacağından denetlenmeyen mükellefler içinde caydırıcı olacaktır (Karatay, 2009:39).

Vergi ödenmemesinin hukuki nedenlerden bir diğeri ise yüksek vergi oranlarıdır. Vergilerin yüksek olması mükelleflerin vergiye karşı tepki göstermelerine neden olmaktadır (Güngör, 2003:112). Vergi oranlarının ekonomik faaliyetlere olan etkisini inceleyen Arthur Laffer çalışmasında bireylerin vergi sonrası gelir düzeyinde yükselme olursa daha çok çalışacakları ya da girişimcilerin vergi sonrası karları artarsa daha çok yatırım yapacaklarını ileri sürmektedir (Özçelik, 2005:54).

Vergi cezalarının etkisizliği de kayıt dışılığa yol açabilmektedir. Kanunda vergi cezalarını içeren hükümlerin net olmaması uygulamada adaletsizliklere ve objektif olmayan davranışlara neden olabilmektedir. Dolayısıyla net olmayan kanunlar nedeni ile vergi cezalarının uygulanmasında her zaman güçlükler oluşabilmektedir (Biçer, 2006:64).

Kanunlarca düzenlenmiş vergi istisnaları ve vergi muafiyetleri de dolaylı olarak kayıt dışı ekonomiyi genişleteceğinden kayıt dışı ekonominin hukuki nedenlerinden biri olarak sayılmaktadır. Küçük işletmeler, çiftçiler ve serbest

meslek mensuplarına getirilen muafiyetler yasalarca koyulmuş ve suç unsuru oluşturmuyor olsa da iktisatçılar tarafından kayıt dışı olarak kabul edilmektedir.

Kayıt dışı ekonomiyi genişleten faktörlerden bir diğeri ise bürokratik engellerdir. İş yapmak için karşılaşılacak formaliteler kişileri resmiyetten uzaklaştırarak kayıt dışına itmektedir.

1.2.3. Sosyolojik Faktörler

Toplumun yaşam standartları, sosyal ve kültürel yapısı, ahlaki değerler, toplumsal motivasyon, göç olgusu gibi sosyal faktörler diğer ekonomik ve idari faktörler gibi enformel ekonominin sebepleri arasına girmektedir (Ilgın, 1999:31).

Gerek köylerden kasabalara gerekse bir ülkeden başka bir ülkeye iş bulabilmek ve daha rahat hayat standardı yakalayabilmek için göçler gerçekleşirken, bu göçler beraberinde nüfus artışını getirmektedir. Nüfus artışının ekonomik büyümenin üzerinde seyretmesi ise işsizlik oranını artırmaktadır. İşsizliğin artması iş bulamayan bireyleri kayıt dışına yöneltmektedir. Bu durum göç olgusunun kayıt dışılığın önemli sebeplerinden biri olduğunu göstermektedir.

Toplumun ahlaki değerlerinin bozulması bireyleri kayıt dışı ekonomiye yönlendiren nedenlerden bir diğeridir. Ahlaki değerleri çöken toplumlar özellikle uyuşturucu satışı, kumar, tefecilik, fuhuş ve kaçakçılık gibi kanun dışı faaliyetlere yönelmektedir (Tanzi, 1984:72-73). Yasak hizmetler riskli olsa da yüksek gelir getirdiğinden bireyleri kayıt dışına yöneltmektedir (Uyanık, 2001:319).

Eğitim düzeyi de önemli sosyolojik etkenlerden bir tanesidir. Özellikle fabrikalar alanında uzman bireyleri istihdam etmek isterken eğitim seviyesi düşük olan bireyleri ise daha vasıfsız işlere yöneltmektedir. Vasıfsız işlerde çalışan bireylerin ekonomik gelirleri daha düşük olduğu için kayıt dışı ekonomiye yönelmeleri daha kolay olmaktadır. Eğitim düzeyinin yüksek olduğu toplumlarda devlet bilinci daha yüksek olmaktadır. Dolayısı ile eğitim seviyesi yüksek olan bireyler kamu yatırımları ile vergiler arasındaki ilişkiyi daha iyi kurabilmektedirler (Önder, 1992:51).

1.2.4. Siyasi Nedenler

Siyasi yapı kayıt dışı ekonomiyi etkileyen nedenlerden biridir. Demokratik yapısı gelişmiş ülkelerde, devlet vatandaşı denetleyebildiği gibi vatandaş ta devleti denetleyebilmektedir. Gelişmekte olan ülkelerde ve az gelişmiş ülkelerde demokratik yapı tam olarak oturmadığından halk devleti denetleme hakkına da genelde sahip değildir. Devletin şeffaf olmaması ve toplumun devletine olan güveninin azalması ise kişileri kayıt dışılığa itmekte ve vergi ödemesinde direnç göstermeye sebep olmaktadır (Özçelik, 2005:44).

Siyasi iktidarların birden çok vergi affı getirmesi, vatandaşı kayıt dışı ekonomiye yönlendiren bir diğer siyasi nedendir. Bunun en iyi örneklerinden biri Türkiye'dir. Türkiye'de 1924 ile 2013 yılları içerisinde vergi borçlarının da affedildiği otuz iki adet kanun çıkarılmıştır (Edizdoğan ve Gümüş, 2013:114). Vergi affının defalarca çıkması ise mükellefleri yeni af beklentilerine itmektedir.

1.3. Kayıt Dışı Ekonominin Etkileri

Kayıt dışı ekonomik faaliyetlerin ekonomiye etkisi hakkında iktisatçılar arasında görüş ayrılıkları mevcuttur. Kimi iktisatçılar kayıt dışı faaliyetlerin ülke ekonomisine zarar verici etkilerinin olduğunu ileri sürerken, farklı görüşte olan iktisatçılar ise sanılanın aksine kayıt dışı ekonomik faaliyetlerin olumlu etkilerinin olduğunu ileri sürmüşlerdir (Özsoylu, 1994:14).

İktisatçılar tarafından kayıt dışı ekonominin olumlu etkisi olarak insan hayatına ve ekonomik hayata refah artırıcı etkileri gösterilmiştir. Özellikle kayıt dışı sektörde istihdam oluşturarak işsizlik sorunun çözümüne katkı sağladığı bu sayede gelir dağılımını iyileştirmenin yanı sıra bireysel refahı artırdığı ileri sürülmektedir (Önder, 2012:41). İktisatçıların ileri sürdüğü en belirgin olumsuz etki ise kayıt dışı ekonominin büyümesinin zamanla kayıtlı ekonomiyi küçülteceğidir.

1.3.1. Kayıt Dışı Ekonominin Olumsuz Etkileri

Kayıt dışı ekonominin ekonomi üzerindeki olumsuz etkisi değerlendirildiğinde kayıt dışı ekonominin büyümesinin, kayıtlı ekonominin küçülmesi anlamına geldiği görülmektedir. Kayıtlı ekonominin küçülmesi ise

devletin vergi gelirlerini azaltmaktadır. Kayıt dışı ekonomi beraberinde kayıt dışı istihdamı da getirmektedir. Kayıt dışı istihdamın artması ise sosyal güvenlik sisteminin çalışma sistematiğini bozmaktadır. Hem vergi vermeyen, hem de sigortasız işçi çalıştıran kayıt dışına yönelmiş firmalar nedeni ile rekabet şartları bozulmaktadır. Haksız rekabet karşısında devlet yeterli önlem alamadığı takdirde ise dürüst mükellefler olumsuz etkilenmektedir. Dürüst mükelleflerin devlete güvenin azalması sosyal yapıyı bozmakta ve kayıt dışı ekonomik yaklaşımları daha cazip hale getirmektedir. Kayıt dışı ekonomik faaliyetler ekonomik göstergeleri olduğundan farklı göstereceğinden ekonomi politikasının belirlenmesinde yanıltıcı etkisi olacaktır (Tütüncü, 2013:32-39, Önder, 2012:41-48).

1.3.1.1. Kamu Gelirlerine Etkisi

Kayıt dışı ekonomik faaliyetlerin devlete verdiği en büyük zararlardan biri de vergi gelirlerindeki kayıplardır. Vergi, devlet açısından bir gelir kapısıdır. Kayıt dışı faaliyetlerin artmasının vergi adaletini bozması nedeniyle vergi mükelleflerinin yükü de artmaktadır. Çünkü devlet geliri kadar hizmet vermekte ve bu gelirini de büyük oranda vergilerden kazanmaktadır. Vergi yükünün artması ise kayıt dışı ekonomiye yönelmeyi daha fazla artırdığından kısır döngü oluşturmaktadır.

Vergi gelirlerinin azalması ülkede bütçe açıkları meydana getirir. Bütçe açıkları oluştuğunda ise ülkeler borçlanma veya para basma yoluna gidebilirler. Bütçe açıkları eğer borçlanma yoluyla kapatılmaya çalışılıyorsa bu kez de faiz oranlarında yükselme olur. Faiz oranlarının yükselmesi ise firmaların yatırım maliyetlerini artırmakta dolayısı ile yatırımların düşmesine sebep olmaktadır (Nas, 2014:43). Oluşan bütçe açıklarının ülkeler tarafından para basılarak karşılanması enflasyon oranlarını yükseltmektedir (Sarıkaya, 2007:47).

Gelir üzerinden alınan vergiler azaldığında, hükümetler bütçe açıklarını kapatmak için, harcamalar üzerinden alınan vergi oranlarını da artırmayı seçebilirler. Bu durum ise "*daha adaletsiz olan dolaylı vergilerin*" (Dağ, 2005) tüm vergiler içerisindeki oranının artmasına sebep olmaktadır (Kanlı, 2007:41).

1.3.1.2. İşgücü Piyasasına Etkisi

Kayıt dışı faaliyet yürüten firmalar vergi ödememelerinin yanı sıra sigorta ve diğer kesintileri ödemediklerinden dürüst firmalara göre daha düşük maliyetlerle ürün ve hizmet üretebilmekte ve piyasaya daha ekonomik ürünler sunabilmektedir (Sarılı, 2002:32). Dolayısı ile bu tip firmaların satış rakamları ve karlılıkları artmaktadır (Öğünç ve Yılmaz, 2000:5). Zaman içerisinde kayıt dışı ekonomik faaliyet gösteren firmalar ile dürüst mükellefler arasında haksız rekabet doğmaktadır (Sarılı, 2002:12). Haksız rekabet arttıkça kayıtlı firmalar da kayıt dışına yönelmekte ve bu süreç kayıt dışılığı artırmaktadır.

Kayıt dışı ekonomide iş, bölümlere ayrılarak yapılmaktadır. Dolayısı ile firmalar bütünleşmiş yapılar şeklinde değil, daha küçük işletmeler düzeyindedir. Küçük işletmelerde daha az işgücü çalıştığından sendikalaşma olmamaktadır (Altuğ, 1999:481). Bireyler gayri resmi olan bu sistemde daha korunmasız olduklarından işyeri ve iş güvenliği olmadan, istismara açık olarak çalışmaya mecbur kalmaktadır (Önder, 2012:44). Bu durum sosyal güvenlik kurumlarının aktif işleyişinde sorunlar oluşturduğu gibi bireylerin sosyal yaşamını da etkilemekte ve devlete olan güvenine zarar vermektedir. Ayrıca Kanlı (2007:36-37)'ya göre kayıt dışı ekonomik faaliyet gösteren sektörlerde kadın ve çocuk işçiler de yer aldığından, dezavantajlı grupların işgücünün de istismar edilmesi söz konusudur.

1.3.1.3. Sosyal Etkisi

Kayıt dışı ekonominin oluşturduğu olumsuzluklardan bir tanesi de sosyal hayata etkisidir. Kayıt dışı ekonominin büyüklüğü, özellikle yasadışı ve kayıt dışı faaliyetlerin sonucu olarak artması toplumun moral, motivasyon ve genel ahlaki değerlerinin bozulmasına ayrıca sosyal devlet anlayışının zedelenmesine sebebiyet vermektedir. Yasa dışı (fuhuş, uyuşturucu satıcılığı, kumar ve illegal diğer faaliyetler gibi) ve kayıt dışı faaliyetlerin toplumda yaygınlaşması, bu sebeple kayıt dışı ekonominin adeta kanıksanması ve dolayısı ile toplum yapısının derin yaralar almasına neden olmaktadır. Bunun sonucu olarak halkın, tamiri çok zor olacak ve etkisi uzun yıllar sürebilecek sosyal maliyetlere katlanması gerekebilmektedir (Nas, 2014:45).

Kayıt dışı ekonomik faaliyet gösteren işletmelerin devlet otoritesine karşı çıkabileceğini de belirten İkiz (2000:32) 1996 yılında yapılan bir çalışmaya[1] atıfta bulunarak Ukrayna'da ki her 10 firmadan 7'sinin kayıt dışı ekonomik faaliyette bulunduğunu, hükümetin önlem almak amacıyla 1998 yılında enformel işletmelerin mallarına el koyulabilmesi için çalışma başlattığını fakat gayri resmi bu yapıdaki işletmelerin buna engel olmaya çalıştığını ve bunun da enformel yapının devlet otoritesine karşı çıkmaya başladığını göstermek açısından iyi bir örnek olduğunu ileri sürmüştür.

Diğer taraftan pazar ekonomisinin olmazsa olmazlarından birisi de rekabetin tam ve aynı şartlarda tesis edilmesidir. Haksız rekabet yoğun olduğunda, kayıt dışından olumsuz etkilenen firmalar faaliyetlerini devam ettirebilmek için kayıt dışı ekonomiye yönelebilirler. Bu dönüşüm ekonomik olduğu kadar sosyal olarak da ülkenin temel olgularını etkilemektedir.

1.3.2. Kayıt Dışı Ekonominin Olumlu Etkileri

İktisatçıların bir bölümü tarafından sadece olumsuz özellikleri anlatılan enformel ekonominin olumlu yönlerinin olduğunu ileri süren iktisatçılar da bulunmaktadır. Örneğin Hoiser'ın kayıt dışı ekonomiyi ifade etmek için kullanmış olduğu evrimci (evolutionist) görüşe göre enformel ekonomik faaliyetler daha düşük imkanlarla iş olanakları sağlayarak işsizliği azaltırlar (Latham,1998:72-73 aktaran İkiz, 2000:33). Latham Zimbabwe ekonomisi için yapmış olduğu çalışmada, kayıt dışı sektörde yaratılan istihdam olmasaydı ülkenin mevcut durumundan çok daha kötü olacağını belirterek Zimbabwe'nin kayıt dışı ekonomideki istihdam oranının %80 olduğunu ifade etmiş ve "kurtarıcı sektör" olduğunu ileri sürmüştür (Latham, 1998:72 aktaran İkiz, 2000:34).

Klasik iktisatçıların ileri sürdüğü *homo economicus* anlayışına göre bireyler kendi çıkarlarını en yüksek düzeye yükseltmek üzerine hareket ederken toplum refahını da en yüksek düzeye çıkarmaktadır (Öztürk, 2006:20). İkiz (2000)'in aktarmış olduğu enformel ekonominin boyutunu konu alan Güney Afrika için yapılan çalışmada ilginç sonuçlar elde edilmiştir. Çalışma kayıt dışı ekonominin

[1] Kaufmann, Daniel, and Aleksander Kaliberda. "Integrating the Unofficial Economy into the Dynamics of Post-Socialist economies: A Framework of Analysis and Evidence." World Bank Policy Research Working Paper 1691, (1996).

kayıtlı ekonomiden daha etkin çalıştığını ve sektörün daha hızlı büyüdüğünü ileri sürmüştür[2] (İkiz, 2000:34).

Kayıt dışı ekonomiyi olumlu bulan diğer bir görüş ise, kayıt dışı ekonominin ülkelerde oluşabilecek ekonomik kriz süreçlerinde, bireylere istihdam imkânı sağlayarak, ekonominin hareketlenmesine olanak sağlamasıdır (Ilgın, 1999:45). Ekonomi bu sayede bir nebze de olsa canlanacak ve krizin etkileri daha az hissedilecektir.

Rekabet yönünden olumlu etkiler oluşturacağını ileri süren iktisatçılara göre firmalar devlete ödenmesi gereken yasal ödemeleri yapmadıklarından üretim maliyetleri düşmektedir. Uluslararası pazarlarda daha düşük fiyattan mal satabilen kayıt dışı firmalar rekabet üstünlüğü sağladığından ihracatın ve dolayısı ile yurtiçi gelirlerin artmasını sağlamaktadır (Kalça, 1995:52).

Olumlu görüşlerden bir diğeri ise "tüketim etkisidir". Enformel ekonomide gelirden devlete ödeme yapılmadığı için kullanılabilir geliri artırdığı dolayısı ile marjinal tüketim eğiliminin yükselmesine neden olmaktadır (Özsoylu, 1996:49).

Diğer bir görüşe göre enformel ekonomi bürokratik engelleri de azaltmaktadır. Bürokrasinin azalmasının ise ekonomi açısından iki avantajı bulunmaktadır. Birincisi bürokratik engeller ve düzenleyici tedbirler için kaynak ayrılmayarak bu kaynağın doğrudan üretim amacı ile kullanılmasıdır. İkincisi ise bürokratik engellere (rüşvet gibi) herhangi bir sebepten dolayı takılan ve bu yüzden ülkeye giremeyen yabancı yatırımların ülke ekonomisine girerek ekonomik büyümeyi sağlamasıdır. Bu durum ekonomide "etkin yağ"[3], "mekanizmanın yağı" hipotezi olarak adlandırılmaktadır (Bardhan, 1997:1322-1323 aktaran Özçelik, 2005: 48).

1.4. Kayıt Dışı Sektörü Kayıtlı Sektörden Ayıran Farklar

Kayıtlı sektörü kayıt dışı sektörden ayıran bazı niteliksel farklılıklar mevcuttur. Bu farklılıkları iş güvencesi, çalışma saatleri, iş yeri standartları,

[2] Douw Van der Walt, spotting opportunities, Finance week, 1998: 68
[3] Leff Nathaniel (1964) tarafından ortaya atılan görüşe göre daha çok rüşvetin "etkin yağ" yani "hızlandıran paranın" bürokratik engelleri kaldıracağı görüşü vurgulanmıştır.

kanuni yasal haklar gibi başlıklar halinde toplamak mümkündür. Özçelik (2005:10) tarafından derlenen farklılıklar Tablo 1.2'de sunulmuştur;

Tablo 1.2: Kayıt Dışı Sektör ve Kayıtlı Sektör Arasındaki Niteliksel Farklar

Nitelik	Kayıtlı Sektör	Kayıt Dışı Sektör
İş güvencesi	İş kanunları ile koruma altındadırlar	İş güvencesi bulunmamaktadır
Ücret farklılıkları	En az asgari ücret uygulanmaktadır	Asgari ücretin altında çalışanlar mevcuttur
Dinlenme ve izin hakları	Kanunlarda belirtilenlere uymaktadır	Kanuni hakların çok altındadır
Sosyal güvenlik hakları	Sosyal güvenceleri mevcuttur	Sosyal güvenlik kurumlarına kayıtları yoktur
Sendikal haklar	Sendikal haklar bulunmaktadır	Böyle bir hak söz konusu değildir
Çalışma saatleri	Kanunlarda belirtilen çalışma saatlerine riayet edilmektedir.	Daha uzun çalışma saatlerine tabi olabilmektedir
İşyeri standartları	Kanunların belirlediği asgari standartlar bulunmaktadır	Daha sağlıksız koşullar mevcuttur

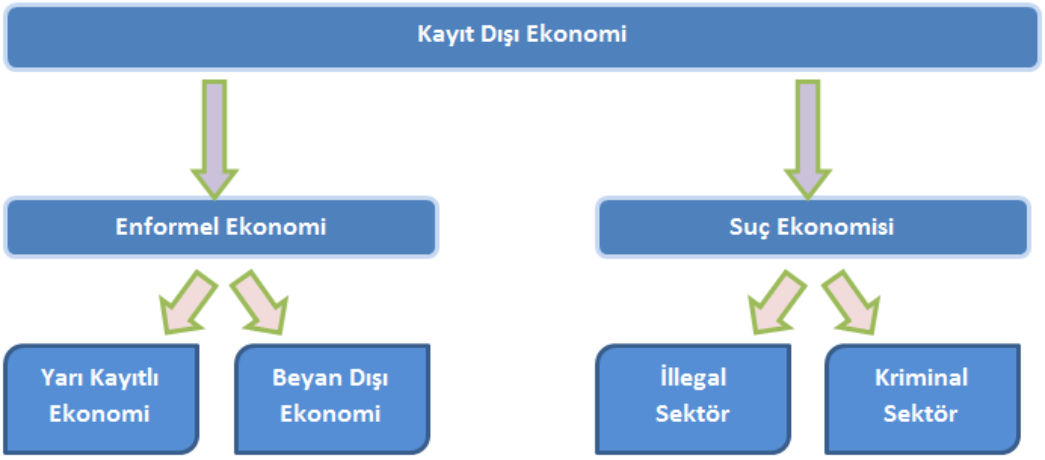
Kaynak: Özçelik, Özer (2005); "*Teorik ve Kavramsal Perspektiften Kayıt Dışı Ekonomi Sorunu, Ölçümü ve Çözüm Önerileri,"* Dumlupınar Üniversitesi, Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı, Yüksek Lisans Tezi.

Enformel işgücünün en temel özelliği daha korumasız çalışma standardı sunmasıdır. Bireyler kayıt dışı istihdam edildiğinde kamunun kayıtlarında yer almadığından daha düşük gelirle, sosyal güvence ve sosyal statüden yoksun olarak çalışma hayatında yer almaktadırlar. Kayıt dışı ekonomik faaliyet yapan firmalarda istihdam edilen bireyler daha düşük ücret alıp daha fazla çalışmak zorunda kalabilirler. Ayrıca firma çalışma ortamı olarak asgari şartları sağlamadığından kayıtlı firmalara göre daha sağlıksız ortamlar mevcuttur.

1.5. Kayıt Dışı Ekonominin Türleri

Kayıt dışı ekonominin enformel yapısının yanında suç teşkil eden yapısı da bulunmaktadır. Enformel ekonomi ise faaliyetlerinin bir bölümünün kaydedildiği yarı kayıtlı ekonomi ve beyan dışı tutulan ekonomi olarak iki bölüme ayrılmaktadır.

Şekil 1.1: Kayıt Dışı Ekonominin Türleri



Kaynak: Ülker Mavral, (2001); "Kara Para, Kayıtdışı Ekonomi İlişkisi ve Türkiye‟ ye Yansımaları," *Vergi Denetmenleri Derneği Yayını, Ankara.*

Literatürde kayıt dışı ekonominin suç teşkil eden bölümünde illegal ekonomik faaliyetler ve kriminal sektör yer almaktadır. Kayıt dışı ekonominin farklılık gösteren unsurları Şekil 1.1'de gösterilmiştir (Mavral, 2001:181).

1.5.1. Enformel Ekonomi (Resmi Kaydı Olmayan Ekonomi)

Enformel kelimesi devlet otoritesinin eksikliğini anlatmak için kullanılan bir tabirdir. Enformel ekonomi yasal olarak gerçekleşen faaliyetler sonucu elde edilen fakat mevzuattaki boşluklar, denetim mekanizmalarının eksikliği, kamu kurumlarının yetersizliği gibi sebepler ile vergilendirilmemiş gelirlerdir (Mavral, 2001:171).

Elde ettikleri kazançları kamunun bilgisi dışında yürütenlerin kayıt dışı ekonomik faaliyetlerini kapsayan enformel ekonomide genel olarak mükelleflerin vergi dairelerinde bir kaydı bulunmadığı görülmektedir. Yılmaz (2006:32) enformel ekonomiyi "yasalarda konulmuş resmi kurallarca ya tanımlanmış ya da belirlenmiş olan kuralların dışında kalan ekonomik faaliyet" olarak tanımlarken, Şişman (1999:29) "hukuken statü tanınmamış olan ya da hukuken statü tanınmış olsa da kurallara uygun işlemeyerek kural dışı konuma düşen ve böylece kurumsallaşamayan bir yapı arz eden üretim ve çalışma ilişkileri alanı" şeklinde tanımlamıştır. Enformel ekonominin genellikle daha çok teknolojinin çok kullanılmadığı alanlarda yoğunlaştığı görülmektedir (Özsoylu, 1996:91).

Resmi olarak kamunun ilgili kurumlarına kayıtlı olmayan enformel girişimciler, faaliyetleri için herhangi bir izne de ihtiyaç duymazlar. Yasal işletmecilerin bağlı olduğu kurumsal düzenlemeler dışında kalırlar. Örneğin burslu öğrencilerin çalışmaları, emekli olan kişilerin ayrıca çalışmaları, ek iş ile çocuk işçiliğini bu kapsamda saymak mümkündür (Yılmaz, 2006:32).

Amacı kişiye gelir yaratmak olan kayıt dışı ekonomiye geçiş kolaydır. Çoğunlukla işletmeler yerli sermayeye ve aile mülkiyetine dayanır. İşletmelerde eğitim seviyesi önemli değildir ve genellikle gelir seviyesi düşüktür (Bulut, 2007:22). Bu sektördeki işleri genellikle kırdan kente işsizlik nedeni ile göç eden vasıfsız işgücü tarafından yapıldığı görülmektedir. Genellikle küçük faaliyetler olarak görülmekle birlikte, bazı iş kollarında ekonomik olarak etkisi daha büyüktür. Semt pazarlarında yapılan sebze ve meyve ticareti ile inşaat sektöründe vergi dairesinin bilgisi dışında çalışan işçiler ve tarım sektöründe çalışan işçilerin meydana getirdiği gelir toplamda yüksek bir boyuta ulaşmaktadır (Demir, 2007:12). Enformel sektör çalışanları kayıtlı sektör çalışanlarına göre daha az gelir elde ederken, enformel sektör yatırımcılarının kazançları formel sektör yatırımcılarından yüksektir.

Ekonominin içerisinde yer almalarına rağmen vergi dairesi kaydı bulunmayan genellikle alt gelir grubundaki kişilerden oluşan, büyük şehirlerde oldukça sık görülen sektörleri Aydemir (1995:80) şu şekilde sıralamıştır:

- Hamallar,
- İş takipçileri,
- İşportacılar,
- İnşaat işçileri,
- Canlı hayvan ticareti yapanlar,
- Belediye hallerine girmeyen sebze ve meyve satıcıları,
- Boş buldukları yerleri otopark olarak işletenler,
- Tarım işçileri.

Kayıtlarda yer almayan faaliyetlerden bir kısmı da yasa dışı niteliktedir. Bu faaliyetler resmileşmesi ve kayıt altına alınması bakımından resmi olmayan

faaliyetler olarak tanımlanır (Ekin, 1995:13). Bu tür faaliyetlere katılanlar, tüm yapılan işlerini devletten gizlemeye çalışırlar.

1.5.1.1. Yarı Kayıtlı Ekonomi

Yarı kayıtlı ekonomi, üretimi, dağıtımı ve tüketiciye ulaşmasında elde edilen gelirin bir kısmının kayıt dışında tutulmasıdır. Tunç (2007:6), yarı kayıtlı ekonomiyi yasalarca yapılması uygun olan işler yapan vergi mükelleflerinin elde ettikleri gelirlerinin bir miktarını ya da tamamını kamudan gizlemesi olarak tanımlamaktadır. Demir (2007:10), kayıt dışılığın en geniş kapsamını oluşturan grubun yarı kayıtlı ekonomide yer aldığını ifade etmektedir. Bu mükellefler defter tutan, beyanname veren ve azda olsa vergi ödeyen kayıtlı mükelleflerdir (Aydemir, 1995:14). Yetim (1999:5) kanunlarca muafiyet tanınan ya da götürü olarak tabir edilen şekilde gelirlerini kayıt dışında tutan kesimin yarı kayıtlı ekonomide yer aldığını ifade etmektedir. Yarı kayıtlı ekonomi iki alt başlıkta incelenmektedir (Demir, 2007:10):

- Yasal olarak gelirin kayıt dışında kalması
- Yasa dışı yöntemlerle gelirin kayıt dışına çıkartılması.

1.5.1.2. Yasal Olarak Gelirin Kayıt Dışında Kalması

Gelirin hesaplanmasının oldukça güç olduğu sektörlerde kazancın tamamı ya da bir kısmı yasal olarak kayıt dışı bırakılmakta, devletin denetlemekte zorlandığı bazı sektörlere muafiyet uygulanmaktadır. Bu sektörlerde faaliyet gösterenlerin gelirlerini gizleme olanakları olduğundan enformel ekonomiyi engellemek zorlaşmaktadır (Karatay, 2009:13). Vergi kanunlarında istisna olanaklarının geniş olması gelirlerin kayıt dışında kalmasını artırmaktadır. Mükelleflerin kayıt dışı ekonomiye etkileri iki şekilde ortaya çıkmaktadır. Birincisi kendilerinin kazandıkları gelirleri kayıt altına almamaları, ikincisi ise belge vermedikleri için ekonomik ilişki içerisinde bulundukları diğer mükelleflerden belge almadıklarından vergi sistemine zarar vermeleridir (Demir, 2007:10).

1.5.1.3. Yasa Dışı Yöntemlerle Gelirin Kayıt Dışına Çıkartılması

Vergi mükellefleri verginin bir kısmını ya da tamamını ödememek amacıyla faaliyetlerin bir kısmını veya tamamını kayıt dışında tutmaktadırlar. Hemen her sektörde görülebilen bu tür faaliyetlerin kayıt dışına yansımaları sektörün büyüklüğüne göre değişiklik göstermektedir (Karatay, 2009:12).

Milli gelirden düşük pay alan vatandaşlar kazançlarını artırmak için enformel ekonomiye yönelmektedir. Yasaların net olmaması, yüksek vergi oranları, sosyal güvenlik kurumlarının oluşturduğu yükler ayrıca adil olmadığı düşünülen vergi muafiyetleri ve istisnalar kayıt dışına yönelimi ve vergi kaçırmalarını artırmaktadır. Vergi mükellefleri kazançlarının bir kısmını sistemden saklayarak kayıt dışı ekonominin artmasına neden olabilmektedir. Hükümetlerin belirli dönemlerde çıkarmış oldukları vergi afları da vergisini zamanında ödeyen mükelleflere kötü örnek oluşturmaktadır.

Vergi yasaları, sosyal güvenlik kurumlarındaki bürokratik işlemlerin karmaşık ve zorlu oluşu, cezaların caydırıcı olmayışı, vergi mükelleflerinin daha basit ve karlı gördükleri kayıt dışı faaliyetlere yönelmelerindeki etkenlerdendir. Bunun yanı sıra birtakım sektörlerin zor denetlenebilen bir yapıya sahip olması, bazı sektörlerde imalatçıdan tüketiciye kadar herkesin bu kayıt dışılığı benimsemesi, faturasız çalışmayı doğal gibi göstermektedir. Kereste ve mobilya alım satımı yapanlar, kuyumcu ve döviz ofisleri, proje ofisleri, tarımsal ürün alım satımı yapanlar, özel inşaat müteahhitleri, emlak ofisleri ve oto galericiler, kum ocakları, tekstil piyasasında çalışanlar, oto tamir ve bakımı ile uğraşanlar, doktorlar, avukatlar, muhasebeciler gibi bazı serbest meslek icra edenler, deri imalatı ve satışı ile uğraşanlar kayıt dışılığın normal karşılandığı sektörler olarak sıralanmaktadır (Aydemir, 1994:17-18).

1.5.1.4. Beyan Dışı Ekonomi

Beyan dışı ekonomi olarak ifade edilen bu ekonomi türü vergi kanunlarına göre devlete ibraz edilmesi gerektiği halde bilinçli ya da bilinçsiz olarak ibraz edilmeyen faaliyetler sonucunda kar elde edilmesi olarak tanımlanmıştır (Yılmaz, 2006:28). Beyan dışı ekonomi, beyan edilmeyen her türlü vergiyi, SGK ödemelerini, kanunla belirlenmiş yasal düzenlemeler olan asgari ücret, iş

güvenliği ve diğer standartları, bilgilendirme amaçlı anketler ve resmi evrakların ibrazı gibi sorumluluklardan kaçınarak yapılan bütün yasal ekonomik faaliyetleri kapsamaktadır (Kanlı, 2007:6).

1.5.2. Suç Ekonomisi

Suç ekonomisi de kayıt dışı ekonomide olduğu gibi birden çok isime ve birden çok tanıma sahiptir. Bireylerin veya toplumun iktisadi menfaatlerinin ihlâl edilmesiyle ortaya çıkan suçlar genel olarak ekonomik suçları ifade ederken (Tiryaki ve Gürsoy, 2004:54), ekonomik suçtan dolayı ortaya çıkan ekonomi ise suç ekonomisini oluşturmaktadır (Yücebaş, 2010:30). Literatürde suç ekonomisi yasa dışı ekonomi, yeraltı ekonomisi, kurşun ekonomisi, mafya ekonomisi olarak da adlandırılmaktadır (Altuğ, 1999:3). Suç ekonomisi için yapılan tanımlardan bir kısmı şu şekildedir:

- Ekonomik suçların sonucunda sağlanan gelirlerin meydana getirdiği ekonomiye suç ekonomisi denir (Özsoylu, 2003:243).
- Kanunen suç sayılan işlemlerden elde edilen tüm ekonomik gelirler suç ekonomisini oluşturur (Demir, 2007:9).
- Konusu suç olan ve bu nedenle cezai yaptırımları olan yasa dışı faaliyetler sonucunda oluşan ekonomik değerler, elde edilmesinde kullanılan yöntemler nedeni ile suç ekonomisini oluşturmaktadır (DPT, 2001:vii). Bu nedenle yasal faaliyetlerden oluşmayan yer altı ekonomisine suç ekonomisi denilmektedir (Aydın, 2006:127).

Bütün bu tanımlardan hareket ederek genel bir şekilde suç ekonomisini, üretilmesi, satılması, tüketilmesi kanunlarca men edilmiş olan faaliyetlerden elde edilen kazançlar olarak tanımlayabiliriz.

Suç ekonomisindeki ana unsur, faaliyetlerin yasalara aykırı olması nedeniyle bu faaliyetlerden kazanılacak gelirin de kayıt dışı olmasıdır (Aktürk, 2005:300). Bunun ile birlikte literatür taramalarında aslında kayıt dışı ekonominin suç ya da kara para sektörünü kapsayan kısmının suç ekonomisi olduğu gözlemlenmektedir.

Uyuşturucu ticareti, silah kaçakçılığı, organ kaçakçılığı, canlı insan kaçakçılığı, dolandırıcılık, tefecilik, hırsızlık, elektronik yöntemlerle yapılan soygunlar gibi faaliyetlerden elde edilen gelirler suç ekonomisi içerisinde yer almaktadır. Yılmaz (2006:34) suç ekonomisi içerisindeki bu tür faaliyetlerin GSMH hesaplarına dâhil edilmesi veya vergilendirilmesi değil, önlenmesi amaçlandığını ifade etmiştir. Diğer yandan yasanın suç saydığı bütün faaliyetlerde kayıt dışı içerisinde yer almayabilir. Örneğin hırsızlık, gasp, yankesicilik veya kumar oynayarak sağlanan kazanç katma değer yaratmadığı için ekonomiyi genişleten bir gelir değil, gelirin el değiştirmesi olarak görüldüğünden kayıt dışı ekonomik faaliyet sayılmazlar (Yılmaz, 2006:34).

Suç ekonomisini oluşturan sektörler oluş şekline göre ikiye ayrılmaktadır. Üretim ve dağıtım yöntemleri yasal olmayan şekilde gerçekleşen sektörlere illegal sektör denir. Mülki hakların ihlali (copyright), vergi kaçakçılığı, patent hakları ihlali, yasalara aykırı çocuk istihdamı, vergi kaçakçılığı gibi faaliyetler illegal sektöre örnek olarak gösterilebilir. Organize suç örgütleri yoluyla yürütülen yasa dışı faaliyetlerin oluşturduğu sektöre ise kriminal sektör denir. Kaçakçılık, kumar, uyuşturucu dağıtımı kriminal sektöre örnek olarak verilebilir (Özsoylu, 1998a:5-7).

1.5.2.1. İllegal Sektör

Üretilmesi ve dağıtılması kanunlar tarafından men edilmiş olan illegal sektörde en çok görülen ihlallerden biri fikri ve sınai hakların (patent, telif, marka vs, gibi) ihlali ile yapılan üretimlerdir (Mavral, 2001:177). İllegal sektör gri (gray) veya düzensiz ekonomi olarak da adlandırılır (Özsoylu, 1998b:12). İllegal sektör yapısı gereği enformel sektöre benzemektedir. Ayırt edici en önemli özellik ise enformel sektörde elde edilen gelir yasalara aykırı olarak kayıt dışına çıkartılırken, illegal sektörde yapılan üretim yasalara aykırı olarak gerçekleşir. Yasadışı üretimin doğal sonucu olarak elde edilen gelirde kayıt dışında kalır (Özsoylu, 1998b:12).

1.5.2.2. Kriminal Sektör (Yeraltı Ekonomisi)

Hukuka ve ahlak değerlerine aykırı faaliyetlerden oluşan yer altı ekonomisi organize olmuş örgütler aracılığı ile yürütülen yasa dışı faaliyetlerden oluşmaktadır. Bu sektörün faaliyetlerinin temel özellikleri, örgütlü olması ve

şiddet içermesidir. Özellikleri bakımından mafya ekonomisi olarak da isimlendirilmektedir (Özsoylu, 1998b:13). Yeraltı ekonomisinin faaliyet alanlarında silah kaçakçılığı, uyuşturucu kaçakçılığı, arsa ve arazi yağmalama, kara para aklama, tefecilik, dolandırıcılık, yolsuzluk, insan ticareti, fahişelik, yasadışı kumar, stratejik madde kaçakçılığı örnek olarak verilebilir.

Kriminal sektör faaliyetlerinde, risk unsurunun yüksekliği nedeni ile kar marjları çok yüksektir. Kriminal sektördeki faaliyetlerin yasalara aykırı olması arzı kısıtlasa da buna karşılık talep inleastiktir. Suç ekonomisinin kar marjının yüksek olması nedeni ile piyasaya giriş talebi de yüksektir (Özsoylu, 1998b:13).

Günümüzde yeraltı ekonomisi faaliyetleri, kapsamı ve hacmi bakımından kayıt dışı ekonomi içinde veya paralelinde ulusal ve uluslararası çok önemli boyutlara ulaşmıştır. Öyle ki kriminal sektör faaliyetleri ve bu faaliyetlere katılan kadro sayıları on binler ile ifade edilen örgütler aracılığı ile gerçekleşmektedir (Mavral, 2001:176).

Kriminal sektör faaliyetleri içinde yer alan bir diğer önemli suç türü de siber suçlardır. Bilişim teknolojisinin gelişmesi ile birlikte teknoloji her sektörde görüldüğü gibi kriminal sektörde de yerini almıştır. Her gün artan siber saldırılar kayıt dışı ekonominin önemli bir kısmını oluşturmaya başlamıştır. Kredi kartı dolandırıcılığı, banka hesaplarının boşaltılması, kullanıcının bilgisayarındaki verileri şifreleyerek tekrar aynı kullanıcıya satılmasını sağlayan cryptolocker virüsleri, dünya devi şirketlere yapılan siber saldırılar, DDOS atakları gibi web siteleri ve e-ticaret sitelerinin kullanımının engellenmesi, casusluk, bilgi kaçakçılığı ve yeni türemiş birçok siber saldırılar bu alana örnek verilebilir (Temli, 2014:80).

Siber saldırılar sadece bilgi hırsızlığı ve casusluk ile sınırlanamaz. Siber teröristler tarafından gerçekleştirilen karalama, propaganda, anketlere hile karıştırma, bilgi kirliliği, yalan haber, kamuoyu oluşturma gibi faaliyetlerde bu kapsamda değerlendirilmektedir. Siber dünya artık kriminal sektörün ayrılmaz bir parçası olmuştur. İleriki bölümlerde siber saldırılar ve zararlarına ayrıntılı olarak değinilecektir.

1.6. Suç Ekonomisinin Kavramsal ve Teorik Yaklaşımı

Temel olarak çalışmamız suç ve suçun ekonomik boyutları hakkında olduğundan dolayı ilk olarak suçun tanımını yapmamız gerekmektedir. Farklı disiplinler tarafından suç ve suç biliminin yorumlanmasına dair birbirinden değişik tanımlamalar yapılmıştır. Suç tarih boyunca süregelen ve bütün insanlar için sorun oluşturan bir olgudur. Suça neden olan faktörler toplumdan topluma değişiklik gösterse de evrensel olarak suç büyük sorunlar oluşturmuştur. Toplum düzenini bozması nedeniyle kanunlarca yasaklanmış fiiller suç teşkil etmektedir. Suç, bir sosyal kümenin mensuplarınca doğru ve faydalı olarak değerlendirilmiş inançların, gelenek ve göreneklerin temelini oluşturduğu kuralların tam aksi yönünde yapılmış davranıştır (Kulaksızoğlu, 1999:229). Yavuzer'e (1996:6) göre suçun işaretleri evrensel olarak tanımlanmıştır. Suç oranlarının toplumlara göre farklılık göstermesi günümüzde üzerinde durulan önemli bir konudur. Akdeniz ve Üzümcü'ye (2013:118) göre suç teorileri bilimsel bakış açısı ile yürütülen suçla mücadele çalışmaları sonrasında ortaya çıkmıştır. Suçun, kişi veya toplum üzerine yoğunlaşması, suçu etkileyen nedenlerin yorumlanmasındaki farklılıklardan ötürü suç teorilerinde farklı sonuçlara ulaşılmıştır.

Sosyolojik yaklaşım, suç oluşturan insan davranışını genel kabul görmüş normlardan sapmış eylem olarak tanımlamaktadır. Suçun belirli dönemlere göre farklı tanımlamaları yapılmıştır (Soyaslan, 1998:14). Auguste Comte tarafından belirtilen insanlık tarihinin üç aşamasına göre suç (Yücebaş, 2010:26):

1. Teolojik çağda, suçu oluşturan davranışlar şeytani bir hareket olarak değerlendirilmiştir.
2. Metafizik çağda, akıl sahibi insanın elde edeceği menfaati ve alacağı cezayı değerlendirerek yaptığı seçim olarak görülmüş ve günümüzdeki ceza hukukunun temelini oluşturmuştur.
3. Pozitif çağda, gözlem veya deney yönteminden faydalanılarak, nedensellik ilişkisiyle koşulların sonucu doğal bir olay olarak açıklanmakta olup bu metot ve yorum biçimi, 19. yy dan günümüze kadar kabul görmüştür.

Suç kavramı aynı zamanda ceza hukukunun temelini de oluşturmaktadır (Dönmezer, 2003:4). Suç bir toplumdaki düzenin sürekliliği bakımından

korunması zorunlu olan kanuni değerlere uyulmama veya bu değerlere önem göstermeyen insan davranışıdır (Özgenç, 2007:164). Bir kimsenin hukuka aykırı, kusurlu hareketine suç denilmekte olup bu suça tatbik edilecek ceza yaptırımına ise ceza hukuku denilmektedir (Öztürk, 2004:3).

Günümüzde suç ülkeden ülkeye farklılık göstermektedir. Bu nedenle kanunlarda ve uygulamalarda farklılıklar bulunmaktadır. Ülkeler bu farklılığı ortadan kaldırmak için müşterek bir ceza hukuku oluşturmaya çalışmaktadır. Müşterek çalışmadaki unsurlar şu şekilde özetlenmektedir (Dönmezer, 2003:26-27):

- Ceza sorumluluğu kusur esasına dayanmalıdır,
- Tehlike durumuna dayanan güvenlik önlemleri vazgeçilmez yaptırımlar arasındadır,
- Suçun bastırılması yerine sosyal savunma ve suçun önlenmesi kavramları önem kazanmıştır,
- Ceza kavramı, iyileştirme kavramının yerini almıştır,
- Suç konusu fiiller sosyal olaylar ve ihtiyaçtan doğmuştur,
- Ceza hukuku ilgisinin suçu yalnızca hukuki bakımdan incelemek olduğu kabullenilmiş ve bilimsel araştırma ve incelemesini kriminolojik bilimler üstlenmiştir,
- Farklı uluslararası kuruluşlar (Avrupa Konseyi ve BM) ceza hukuku esaslarını birleştirme çabalarını artırmışlardır.

Akdeniz ve Üzümcü suç olgusunu, psikoloji, psikiyatri, antropoloji, ekonomi, hukuk ve sosyoloji gibi farklı birçok bilimsel disiplin tarafından ele alınıp analiz edildiğini ileri sürmüşlerdir.

Suç olgusu; ekonomik durum, kültürel ve soy geçmişi, sosyal statü, eğitim durumu ile diğer faktörlerle çok güçlü ilişki içerisindedir (Buonanno, 2003:11). Benzer şekilde Akdeniz ve Üzümcü'ye (2013:118) göre; suç türü sayısının fazlalığı (hırsızlık, tecavüz, cinayet, zimmete para geçirme, gasp, vb.), suçlulukla alakalı farklı değişkenler (yoksulluk, işsizlik, eşitsizlik, problemli aile profili, iç/dış göç, alkolün ile narkotik maddeler, yerleşim alanının nitelikleri, kültür, vb.) ve suçluların taşıdığı değişik şahsi özellikler (cinsiyet, medeni hal, yaş, mesleki durum, sosyal statü, vb.) nedenleriyle suç olgusunun açıklanmasına yönelik

geliştirilen teori sayıları artmış, açıklama perspektiflerinin içeriği ve sayısı çoğalmıştır.

1.6.1. Suç-Ekonomi İlişkisi ve Ekonomik Suç Teorileri

Sebep olan faktörler toplumlara göre değişse de yüz yıllardır suç toplumlar ve kişiler bakımından sıkıntı oluşturmaktadır. Suçlunun rasyonel davranışları, suç ekonomisinin temel varsayımıdır (Aksu ve Akkuş, 2010:193). Suçun iktisadi modeli ya da suç ekonomisi, Fleisher (1963) ve Becker (1968) gibi ekonomistlerin liderliğinde gelişmiştir (Yıldız vd, 2011:17). Suç ekonomisinde modelleme yoluyla yapılan ilk çalışma Gary Becker tarafından gerçekleştirilmiştir. Becker'in değerlendirmeleri, Ehrlich (1973), Heineke (1978) ve Schmidt ve Witte (1984) tarafından geliştirilerek daha ileri boyutlara taşınmıştır (Yıldız vd., 2011:17). Suç ekonomisinin modeli, suçun maddi olarak tanımlanabilen bir kazanç erişimine uygun olduğu değerlendirmesine dayanarak, genel itibarıyla zamanın iş ve suç arasındaki planlı dağılımının değerlendirilmesi ile ilgilidir (Witte ve Tauchen, 1994:1-2). 1980'lerden sonra suçluların tekrar suç işleme eğilimini belirlemek üzere mikro analizler yapılmış ve analizlerde genel caydırmanın suçu engelleme gücüne ek olarak özellikli (spesifik) caydırma konusu da ele alınmıştır (Aksu ve Akkuş, 2010:196).

Fleisher'in 1963 yılında yayınlamış olduğu "İşsizliğin Çocuk Suçlarına Etkisi" adlı amprik çalışması, bireysel suçlu davranışları için ekonomik belirleyicileri keşfetmeyi amaçlayan ilk çalışma olmuştur. Suça ekonomik açıdan bakan Fleisher'in çalışması kamu politikaları açısından, suç işleme ve emek piyasası durumu arasındaki ilişkiyi ortaya koymak için önemlidir. Fleisher çalışmasında, yaş ile suç oranı ve diğer değişkenleri inceleyerek; işsizliğin, çocuk suçlarını olumsuz etkilediğini söylemiştir (Aktaran: Yıldız vd., 2011:17). Fleisher 1966 yılındaki çalışması ise işsizliğin suç işlemeyi doğrudan artırmasına rağmen dolaylı yönden etkisi olmadığını göstermektedir (Fleisher, 1966:128-129).

Becker'in 1968 yılında "Crime and Punishment, An Economic Approach" adlı makalesinde, suçlu davranışları hakkındaki düşünceyi radikal bir şekilde değiştirerek suç tercihinin ilk modelini kurmuştur. Becker "Bazı bireylerin suç sonrası cezalandırılmanın derecesi ve mahkûmiyet, suçtan duyulan korku ve hesap

verme ihtimali ile yasal işlerden elde edilecek gelirin karşılaştırılmalı olarak suçtan gelen finansal ve diğer ödüllendirmeler çerçevesinde suçlu hale geleceğini vurgulamıştır" (Aktaran: Öcal, 2010:12-13). Becker'in 1993 yılındaki çalışmasında ise suçlu davranışın nedeni olarak akıl hastalığı ve sosyal baskının varlığını belirtmiş ve suçlular için yardıma muhtaç kurbanlar ifadesini kullanarak bireylerin yasal işlerden kazanacaklarına göre, suçtan kazanacaklarını karşılaştırarak suça karışıp karışmamaya karar vereceklerini ileri sürmüştür (Becker, 1993:390).

Ehrlich, Becker'in 1968 yılındaki çalışmalarını ilerleterek, farklı gelir seviyesi ve dağılımının suç oranlarına etkisi ile birlikte mala karşı suç olarak potansiyel suç mağdurlarınca oluşturulan imkânları vurgulamıştır. Ehrlich 1973 yılında 1960 yılı Amerika Birleşik Devletleri için yapmış olduğu suç oranları belirleyicileri çalışmasında, gelir seviyesi yüksek olan ailelerin saldırı, cinayet, tecavüz ve hırsızlık gibi suç oranları ile daha çok ilişkili olduğu, ayrıca gelir seviyesi bakımından en düşük olan bireylerde yüksek suç oranları olduğu sonucuna ulaşmıştır (Öcal, 2010:16).

Sjoquist 1973 yılındaki çalışmasında Fleisher ve Becker tarafından kullanılan yaklaşımı izlemiş ve bazı durumlar altında suçluların rasyonel ve ekonomik varlıklar gibi davranabileceğini belirterek, diğer bireylerin risk altında suçluların verdikleri ekonomik kararlar gibi tutum sergileyebileceğini ifade etmiştir (Öcal, 2010:18).

Block ve Heineke tarafından 1975 yılında yapılan analizlerde Becker, Ehrlich ve Sjoquist'in geliştirdiği teorik yapı takip edilmiştir. Bu çalışmalara ek olarak yasal ve yasadışı faaliyetlerde harcanan zamanın ele alınması suretiyle suçlu tercih problemine alternatif bir bakış açısı getirilmiştir (Aktaran: Öcal, 2010:18).

Suça ekonomik yaklaşım, diğer bilimlerden farklı bir şekilde; suçu bir ekonomik faaliyet olarak değerlendirmektedir (Aksu ve Akkuş, 2010:195). Dolayısı ile suç ekonomisinde analizi yapılacak ve yorumlanacak en önemli faktör ekonomik uygulamalardır (Scorzafave ve Soares, 2009:40).

Akdeniz ve Üzümcü (2013:120) suç ekonomisi teorilerinin, mikro ekonomik yaklaşımlarla değerlendirildiğinde, suçlu kişilerin davranışlarını açıkladığını belirtmişlerdir. Suçun "herhangi bir iş gibi belirli bir zamanda yapılan ve maddi kazancı olan" bir eylem olarak değerlendirilmesi, bu saptamaların rasyonel tercih teorisine *"ekonomik akılcılık teorisi"* nin dayandığını göstermektedir.

Öcal (2010:7) suç kuramını, iktisadi karar analizine dayandırarak suçun ekonomik modellerinin, suçlunun ve bireylerin faydasını maksimum yapmaya çalıştığını varsayar. İktisatçılar, suç faaliyetini diğer ekonomik faaliyetler gibi değerlendirmektedir. Bu nedenle iktisatçıların suç ekonomisine yaklaşımı diğer disiplinlerden farklıdır. Birey için suç diğer ekonomik faaliyetler şeklindedir. Bireyin suçu işlemesi için suç ekonomisine konu olan yasadışı davranışlardan sağladığı yararın yasal etkinliklerdekilere oranla daha yüksek olması gerekmektedir. Buonanno (2003) ve diğer ekonomistler suçun yoksulluk, ücret ve gelir eşitsizliği, eğitim seviyesi, sosyal dışlanma ve diğer sosyo-ekonomik faktörlerle çok güçlü ilişkilerinin olduğunu ileri sürmüşlerdir.

Literatürde ekonomik suçlar, insanların ya da toplumun herhangi bir ekonomik faaliyetinin ihlal edilmesi nedeni ile oluşan suçlar olarak tarif edilmektedir (Tiryaki ve Gürsoy, 2004:55). Başka bir ifade ile kanunlar açısından suç olarak tanımlanmış faaliyetler sonucundaki kazançlar da suç ekonomisi ifade edilmiştir. Aydın (2006:127)'a göre suç ekonomisi illegal faaliyetlerden oluşan yeraltı ekonomisidir. Kılıçdaroğlu (2000:18) suç ekonomisini tanımlarken yasadışı üretimler sonucu oluşan kayıt dışı ekonomi ifadesini kullanmıştır. Kılıçdaroğlu'na göre suç ekonomisinin temel özelliğinin tümüyle yasalarca yasaklanmış olmasıdır. Demir (2007) ve Güvel (2004)'e göre ekonomik suç, profesyonel veya teknik kabiliyetlere sahip kişiler tarafından haksız gelir elde etmek üzere yalan beyanda bulunma, aldatma, teknik becerileri kullanarak kandırma gibi profesyonel teknikler kullanma yoluyla işlenen yasa dışı bir eylem olarak tanımlanmaktadır.

Günümüzde ekonomik suçun evrensel bir tanımı bulunmamaktadır. Ekonominin birey ve toplum üzerinde etkilerinin sürekli artması, bu etkilerin başı ve sonunun belli olmaması, aynı zamanda dinamik olması suç ekonomisinin

sınırlarını çizmeyi zorlaştırmaktadır. Ekonomik suçlar diğer (soygun, yaralama, adam öldürme gibi) suçlardan oldukça farklıdır. Özellikle son yıllarda internet ve bilişim sistemlerinin ilerlemesi firmaların iş yapma şekillerini değiştirmiş ve bu kapsamda işlenen suçlara da ayrıca farklı nitelik kazandırmıştır.

Ekonomik suç kavramı geniş bir alanı içermekte ve ticari, iktisadi ve mali suçların tamamını kapsamaktadır. İktisatçılar suç konusunu dört farklı şekilde ele almaktadır. Bunları şu şekilde sıralayabiliriz (Güvel, 2004; Öcal, 2010:11):

- İşgücünün ve sermayenin yasa dışı faaliyetlerde kullanılmasına yol açan özelliklerinin belirlenmesi,
- Ekonomik büyüklüklerin ve suç oranlarının birbirleri üzerindeki etkilerinin açıklanması, geleneksel iktisat politikalarının suç oranlarındaki artışı engelleyici yönde nasıl kullanılabileceğinin belirlenmesi,
- Yasal ve yasa dışı faaliyetler arasında ekonomik kaynakların en uygun dağılımını gerçekleştirecek ve sosyal refahı en yüksek seviyeye çıkaracak hukuk uygulamalarının belirlenmesi,
- Ekonomik kaynakların yasa dışı faaliyetlere yönelmesinin, ekonomik sonuçlarının incelenmesi.

Ekonomistlerin tek amacı suçun sosyal, siyasal ve iktisadi belirleyicilerini ortaya çıkarmak değil, etkili politikaları da belirleyerek düzenlemektir. Ekonomik araştırmalar, politika yapıcıları suçu azaltma konusunda etkin bir şekilde tamamlamalı ve onları alınan kararların uygulanma sürecinde yalnız bırakmamalıdır.

1.6.2. Ücret, İşsizlik, Gelir ve Suç Arasındaki İlişki

İşsizliğin suç miktarını olumsuz şekilde artırdığına yönelik çok sayıda çalışma vardır. Bu konuda ilk çalışmalar Fleisher (1963-1966) ve Ehrlich (1973) tarafından yapılmıştır. İşgücü piyasasının birçok açıdan yetersizliği, iş bulamama ve düşük gelirlerin sebep olduğu işsizlik suç oranını ve suçun kapsamını artırmaktadır (Güvel, 2004). Becker (1968) ve Ehrlich (1973)'in çalışmalarında suç oranı ile işsizlik oranı arasında anlamlı ve pozitif bir bağın bulunduğunu ileri sürerken maaşlar ile suç sayıları arasında negatif bir bağın olduğu ileri sürülmüştür (Ata, 2009: 126).

Öcal (2010:20) suç istatistiklerini geleneksel olarak incelendiğinde, işsizliğin suç üzerinde etkili olduğunu ve işsizliğin suçun belirleyicilerinden bir tanesi olduğunu ileri sürerken çalışmalarda suç-işsizlik takası kurulduğunu belirtmiştir. Ayrıca 1980'lerde yapılan çalışmalarda, yüksek işsizlik oranının, suç artışına yol açacağını da ileri sürmüştür. Chiricos (1987:188) çalışmasında 1950'lerden 1990'lara kadar işsizliğin artmasına rağmen suç eğiliminde işsizliğin etkisinin az olduğunu belirtirken ayrıca işsizlik ile suç ilişkisi arasında yapılan çalışmaların bu iki veri arasındaki ilişkinin hem tutarsız, hem de önemsiz olduğunu ileri sürmüştür. Box'un 1987 yılındaki işsizlik ve suç oranları arasındaki ilişki düzeyini incelediği çalışmalardan 33 tanesinde pozitif bir ilişki tespit edildiğini ancak 19 tanesinde işsizlik ve suç oranları arasında negatif ilişki bulunduğunu ileri sürmüştür. Gould, Weinberg ve Mustard (2002) gibi iktisatçılar çalışmalarında, bazı iktisatçıların suç ve işsizlik oranı üzerine odaklandıklarını ama belirsiz sonuçlara ulaştıklarını fakat, hem ücretin, hem de işsizliğin suç etkisini araştırmak için suç ve emek piyasası arasındaki ilişkinin ortaya konulması gerektiğini ileri sürmüşlerdir. Montolio (2008) İspanyanın illeri arasında yaptığı suçun sosyo-ekonomik belirleyicilerini tanımlayan makalesinde, işsizlik ile her türlü suç arasındaki ilişkiyi zayıf ve negatif görmüştür. Yine benzer bir çalışma Türkiye'de yapılmıştır (Pazarlıoğlu ve Turgutlu, 2007:65). Güvel (2004)'in, 1995-2002 yılları arasındaki Türkiye'deki cinayet, hırsızlık ve soygun gibi suç verileri ile sosyo-ekonomik değişkenleri kıyasladığı çalışmasında her çeşit suçlar ile işsizlik arasındaki bağın, doğrusal olması ile birlikte zayıf olduğu sonucuna ulaşılmıştır. Bu farklı sonuçlar karşısında Pazarlıoğlu ve Turgutlu (2007:65) suç oranındaki değişmelerin sadece işsizlik gibi tek bir değişkenden olmadığını, diğer birçok farklı değişkeninde çalışmalara eklenmesi gerektiğini ileri sürmüşlerdir.

Sadece işsizler suça yönelmemektedir. Yasadışı suç unsurlarına yönelmeye asıl neden olan unsur gelir olarak görülmektedir. Kişi, kanuni yoldan çalışarak kazanacağı gelir ile kanunsuz faaliyetlerden kazandığı gelir ve yakalanıp cezalandırılma riskini kıyaslayarak bir tercih yapmaktadır. Kişinin kanuni geliri, yasal olmayan gelir ve beraberindeki maliyetlerden daha fazlaysa, suça meyil etmeyecektir (Ata, 2011:116). Fleisher (1966:120) ise, suçu oluşturan en önemli iktisadi unsurun yasal gelir olduğunu ileri sürmüştür. Fleisher, daha az gelir elde eden çalışanın kanunsuz yollardan elde edeceği gelire yönelmesini, alternatif

maliyetin düşük olmasına bağlamıştır. Çünkü yakalandıklarında kaybedecekleri ekonomik maliyet çok azdır.

Bireyin suça yönelmesinin bir diğer nedeni de gelir dengesizliğidir (Fowles ve Merva, 1996:165). Kamu kesimi çalışanları ile özel sektör çalışanlarının gelirleri arasındaki yüksek farklar kamuda çalışanları suç işlemeye yönlendirecek önemli etkenlerden biridir (Ata, 2011:123). Ayrıca yüksek düzeyde parasal işlerle uğraşanların düşük ücret alması kişilerin özel sektörde de olsa suça yönelmesini sağlayabilmektedir. Örneğin bir ildeki ATM cihazlarına para yükleyen para nakil görevlisinin suça meyilli olması bir inşaat işçisine göre daha fazladır. Çünkü para nakil görevlisinin uğraştığı miktar fazla iken bu iş karşılığında aldığı ücret oldukça düşüktür. Aynı durum gişe görevlileri, veznedarlar ve kuyumcu çırakları için de geçerlidir. Bu nedenle sorumluluklar zaman içerisinde birden fazla kişiye bölünerek risk azaltılmaya çalışılmıştır. Cezai yaptırımların yeterli olmaması da kişileri suç işlemeye sevk edebilen bir diğer unsurdur.

Değerlendirmeler sonucunda kişileri suç işlemeye itecek ana unsurun kazançlarını en yükseğe çıkarma güdüsü ve kazanılabilecek olan yasal gelirlerin seviyesi olduğu görülmüştür. Bu da bize, suç ile ücret düzeyi arasında ilişki olduğunu göstermektedir. Kişinin gelir seviyesi yüksek olduğunda daha az suça yönelecektir (Burdett vd., 2003: 9).

1.6.3. Suç ve Diğer Ekonomik Faktörler

Genel kabule göre gelir düzeyi ile suç eylemleri arasında sıkı ilişki vardır. Gelir seviyesinin düşük olması kişiyi suç işlemeye yönlendiren önemli unsurlardan biridir. Gelir seviyesi artan bireyler, eğitim alarak suç ve cezayı öğrendikleri için suç miktarı azalacaktır (Becker, 1968:177). Bununla birlikte zengin bireyler de suç işlemektedir. Gelir seviyesi yüksek olan suçlular suç karşılığında katlanması gereken maliyeti iyi hesaplayarak maddi gücü ile iyi avukat tutma, rüşvet verme ve delil gizleme imkânlarını düşük gelir gurubundakilere göre daha fazla kullanmaktadır. Çünkü yüksek gelir gruplarının hapis cezası aldıklarındaki maliyet, suçu gizlemek için harcadığı maliyetten daha fazla iken düşük gelir gruplarında bu oran daha düşüktür (Akkuş ve Aksu 2010:195).

Benzer bir durum bilişim suçlarında da bulunmaktadır. İnternet teknik alt yapısını iyi bilen hacker kendisini çoğu zaman suçtan gizleyebilmektedir. IP gizleme, zombi[4] üzerinden atakta bulunma, ele geçirilmiş bir sunucuya açılan arka kapı üzerinden suç işleme, kimlik hırsızlığı üzerinden suç işleme gibi farklı tekniklerle suçu başkası üzerinden işleme yöntemleri çoğu zaman suçu işleyeni yasalara karşı korumaktadır. Bunun için kullanılan farklı teknik ve yöntemler hakkında ilerleyen bölümlerde ayrıntılı olarak bahsedilecektir.

Witte ve Tauchen (1993) bir işte uzun süre çalışma ve eğitime uzun süre devam etme durumunun suç işleme olasılığını azalttığını ileri sürmüştür. Engelhardt (2008) ise ilave olarak küçük çaplı ücret yardımlarının da suç oranlarını azalttığını ileri sürmüştür.

Sonuç olarak Bentham (1843)'e göre bireyleri yasa dışı yöntemlerle gelir elde etmeye yönlendiren ana unsur suçun karıdır. Ceza ise suçtan uzak kalmayı sağlayan etkendir. Eğer ilk unsur daha büyük ve güçlü ise kişiler suç işler. Eğer diğer unsur daha büyük ve güçlü ise kişi suç işlemeyecektir (Aktaran: Yıldız, vd., 2011:17).

1.6.4. Ekonomik Suçların Özellikleri

Ekonomik suçların kendine özgü bazı özellikleri bulunmakta olup bu özellikleri aşağıdaki gibi sıralamak mümkündür (Kocasakal, 2005:22-23):

- Ekonomik suçlar doğal suçlar arasında yer almadığından yapay bir durum oluşturur.
- Ekonomik suçlar siyasi ve ekonomik durum ile yakından ilişkilidir. Bu nedenle değişken özellikler taşır.
- Ekonomik suçlar sert yaptırımlara tabidir. Tüzel kişilerin de ceza sorumluluğunu gündeme taşımaktadır.
- Ekonomik suçlar genel olarak teknik bir suç olduğundan değerlendirme için bilirkişiye ihtiyaç duyulur. Bu özellikleri nedeni ile ihtisas mahkemelerinde gerçekleştirilecek özel soruşturma ve yargılama teknikleri kullanılır.

[4] İnternete bağlı ve bir hacker tarafından bilgisayar virüsü veya truva atı ile kontrol altına alınmış bilgisayardır.

- Bu suçlar ceza kanunlarında olmadığı gibi toplu bir başlık altında da bulunmazlar. Çeşitli yasal düzenlemeler ile dağınık bir biçimde yer almaktadır.
- Ekonomik suçlarda idarenin düzenleyici işlemleri büyük ve önemli bir yere sahiptir. Bu sebeple suçların içeriğinin doldurulması suçlardaki kanunilik ilkesinin tartışılmasına neden olmaktadır.
- Ekonomik suçlarda oldukça yaygın bir mağdur kitlesi olmakta ve çoğu kez bu kişiler suçun mağduru olduklarını fark etmemektedir.
- Gelişen teknolojiyle birlikte ekonomik suçlar yeni suç tekniklerini de ortaya çıkarmaktadır.
- Ekonomik suçlarda beyaz yaka suçluluğu yaygın olup, suçun failleri genellikle mesleki saygınlığı olan ekonomik ve kültür seviyesi yüksek eğitimli kişiler olmaktadır.

1.6.5. Suç Ekonomisine Konu Olan Suçlar ve Diğer Suç Tasnifleri

Demirbaş (2001:210-265) genel suç tasnifleri gibi işleniş süreçleri ve şekilleri bakımından ele alınan diğer suç tasniflerini şu şekilde açıklamıştır:

- Şiddet Suçları: Bu grupta adam öldürme, yağmalama, aile içi şiddet, müessir fiil, kurumlarda ve sporda şiddet gibi suçlar yer almaktadır.
- Cinsel Suçlar: Bu suçların arasında birçok cinsel istismar suçları bulunmaktadır.
- Mal Aleyhine İşlenen Suçlar: Bu suçlar malı çalma, kaçırma ve zarar verme olarak nitelendirilmektedir.
- Ekonomik Suçlar: Kendi içinde birkaç alt gruba ayrılan bu suçlar genel olarak her türlü kaçakçılık, tefecilik, sahtecilik, beyaz yaka suçluluğu, kamu alanında yapılan yolsuzluklar olarak tanımlanmaktadır.

Suç ekonomisine konu olan diğer önemli suç grupları ise, bilişim suçları, çevre suçları, trafik suçları ve bağımlılık maddeleri suçlarıdır.

Teknolojinin ilerlemesi ile birlikte birçok suç türü artık internet üzerinden işlenebilir duruma gelmiştir. Eskiden hırsızlık için suçlunun mağdura birebir temas etmesi gerekirken artık uzaktan ve internet aracılığı ile bu işlemler gerçekleştirilebilmektedir. Bu nedenle ekonomik suçun kapsamı zaman içerisinde

genişlemektedir. Bilişim ve ekonomik suçlardan bilişim alt yapısı ile işlenen suçların hukuki boyutları sonraki bölümde ayrıntılı olarak anlatılacaktır.

1.7. Kayıt Dışı Ekonomi ve Suç Ekonomisi İlişkisi

Yeraltı ekonomisi diğer ismi ile suç ekonomisi kayıt altına alınmamış yasa dışı ekonomik faaliyetlerden oluşmaktadır. Suç ekonomisi mal ve hizmet üretiminin yasa dışı yapılması sonucunda oluşan kayıt dışı ekonomik faaliyet olarak da ifade edilebilir. Suç ekonomisinde ana unsur faaliyetlerin kanunlara uygun olarak yapılmaması değil, faaliyetin yasaklanmış olmasıdır. Kayıt dışı ekonominin birçok tanımında gelirin kanunsuz olarak kayıt dışına çıkartılıyor olması asıl konu iken, suç ekonomisinde konu daha geniş ele alınmış ve üretim sürecinden itibaren tüm sürecin kanunsuz olarak gerçekleştiği ileri sürülmüştür. Suç ekonomisinde yapılan faaliyetler yasa dışı olduğundan elde edilen gelirde kayıt dışı ekonomi alanına girmekte ve elde edilen gelir doğal olarak gizlenmektedir (Önder, 2012:8). Araştırmacıların yapmış olduğu tanımlamalarda kayıt dışı ekonomik faaliyetler özellikleri bakımından her zaman suç sayılmayabilir. Örneğin yasal olarak götürü usulü çalışan bireyler, bir işinin görülmesi için arkadaşından yardım alma, bir kişiye karşılıksız burs verme, bireysel ihtiyaçlarını karşılamak için ikinci bir iş olarak kendi tarla bağ bahçesinde çalışması suç teşkil etmeyen kayıt dışı ekonomik faaliyetlerdir. Bu sebeple kayıt dışı ekonomi, yasadışı olabileceği gibi yasal da olabilmektedir.

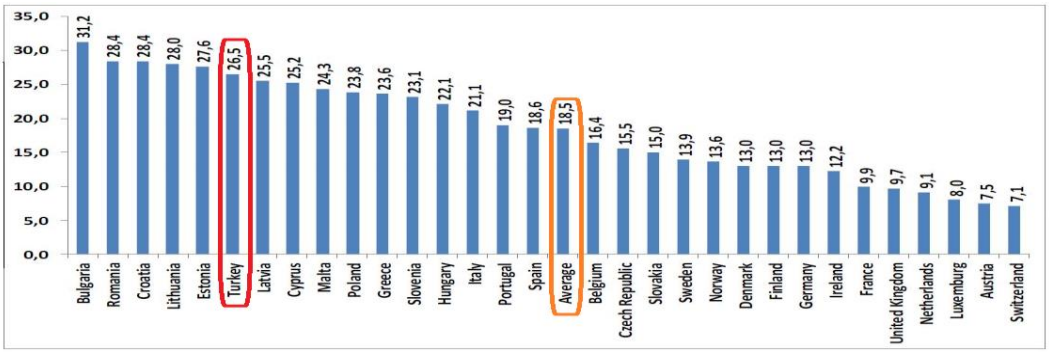
Suç ekonomisinde faaliyetler maddi bir menfaatin temin edilmesi amacı ile gerçekleştirilmektedir. Kişisel ya da örgütsel kazanç ile birlikte haksız kazanç sağlama amacı ile özel, üst düzey donanımlı ve teknik becerileri yüksek kişiler tarafından genellikle aldatma veya yalan beyanatla işlenen yasadışı eylemler ekonomik suçları oluşturur (Güvel, 2004:5). Kayıt dışı ekonomi içerisindeki diğer faaliyetlerin asıl amacı hiç vergi ödememek veya kazancın bir kısmının görünmesini engelleyerek düşük vergi ödemek, sosyal güvenlik kurumlarına eksik beyanda bulunarak yapılan ödemeleri düşürmektir. Fakat suç ekonomisi sonucunda kazanç elde edenlerin amacı bu ödemelerden kaçmak değildir. Hatta bu ödemeleri yaparak kazançlarını meşrulaştırmak istemektedirler. Suç ekonomisi yaklaşımında asıl amaç kazanılan paranın vergilerinin ödenmesi değil bilakis bu tür yasaklanmış faaliyetlerin gerçekleşmesinin önlenmesidir. Çolak (2012:7-8),

kayıt dışı ekonomiyle mücadele ile suç ekonomisiyle mücadele arasında fark olduğunu ileri sürmüş ve kayıt dışı ekonomiyle mücadelede asıl amaç kayıt dışı ekonomik faaliyetleri kayıt altına almak iken suç ekonomisi ile mücadelede temel amaç bu sektörden elde edilen kazancın tamamen ortadan kaldırılması olduğunu ifade etmiştir.

1.8. Türkiye'de Kayıt Dışı Ekonominin Boyutu

Türkiye'de kayıt dışı ekonomi vergi kaçakçılığı bakımından 1990'lı yıllardan itibaren ilgi görmeye başlamıştır. Literatürde mahiyeti, boyutu, sebepleri, sonuçları ve vergi boyutu ile ilgili çok sayıda çalışma bulunmaktadır. Kayıt dışı ekonominin tahmin edilen hacmi ile mali, ekonomik, sosyal, siyasal ve hukuki maliyetlerinin yüksekliği siyasetçilerin de konuya ilgisini çekmiştir. Türkiye'deki kayıt dışı ekonominin boyutu incelendiğinde AB üyesi birçok ülkeden daha geniş olduğu görülmektedir. Ülkemizde kayıt dışı ekonomik faaliyetlerin, ekonomik beklentiler ve gerçekleşmeler değerlendirildiğinde, rakam bazında tüm verilere erişim pek mümkün olmasa da, oldukça yüksek bir seviyede olduğu belirlenmiştir.

Grafik 1.1: Avrupa Ülkelerinin 2013 Kayıt Dışı Ekonomi Verileri



Not: Grafikteki kayıt dışı ekonomi verileri, GSMH'nin % oranı olarak verilmiştir.

Kaynak: http://www.econ.jku.at/members/schneider/files/publications/2013/shadeceurope31_jan 2013.pdf, (Erişim Tarihi: 24.12.2015).

Grafik 1.1 incelendiğinde Türkiye'nin 2013 yılı kayıt dışı ekonomi verilerinin Avrupa ülkeleri ortalamasından yüksek olduğu görülmektedir.

Tablo 1.3: Türkiye'nin Diğer Avrupa Ülkelerinin Ortalamasına Göre 2003 – 2013 Yılları Kayıt Dışı Ekonomi Oranları

Ülke / Yıl	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013
Türkiye	32,2	31,5	30,7	30,4	29,1	28,4	28,9	28,3	27,7	27,2	26,5
27 Avrupa Birliği Üye Ülkenin Ortalaması	22,3	21,9	21,5	20,8	19,9	19,2	19,8	19,6	19,2	18,9	18,4
31 Avrupa Ülkesinin Ortalaması	22,4	22,1	21,6	20,9	20,1	19,4	19,9	19,7	19,3	19,0	18,5

Not: Tablodaki gayri safi milli hasıla %'si olarak kayıt dışı ekonomi oranları

Kaynak: Schineider, Friedrich Size (2015); Development of the Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2013. http://www.econ.jku.at/members/schneider/files/publications/2013/shadeceurope31_jan2013.pdf , (Erişim Tarihi: 24.12.2015).

Tablo 1.3 incelendiğinde Türkiye'deki kayıt dışı rakamlarının Avrupa'ya oranla oldukça yüksek olduğu görülmekle birlikte yıllara göre düşüş gözükmektedir. Buna rağmen rakamlar arasında ciddi farklılıklar vardır. Kayıt dışılığın tamamen bitmesi beklenmese de rakamlara bakıldığında ve Avrupa ülkelerine kıyasla üzerinde çok çalışılması gerekli olan bir konu olarak gözükmektedir.

Tablo 1.4: Gelişmekte Olan Ülkelerde Kayıt Dışı Ekonominin Boyutları

Ülkeler/Yıl	1999	2000	2001	2002	2003	2004	2005	2006	2007
Türkiye	32,7	32,1	32,8	32,4	31,8	31,0	30,0	29,5	29,1
Afrika	39,1	38,9	38,6	38,5	38,0	37,4	37,2	36,2	33,5
Orta ve Güney Amerika	42,2	42,1	42,2	42,6	42,2	41,3	40,4	39,5	37,2
Asya	30,8	30,3	30,3	30,0	29,7	29,3	28,8	28,32	27,9

Kaynak: Demir, Halil İbrahim (2007); "*Kayıt Dışı Ekonomi ve Kara Para İlişkisi*" Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Isparta.

Tablo 1.4'te 1999-2007 dönemleri arasında bazı gelişmekte olan ekonomilerde Schneider (2013) tarafından MIMIC[5] yöntemiyle yapılan çalışmanın sonuçları aktarılmıştır. Çalışmada gelişmekte olan ülkeler Afrika, Orta ve Güney Amerika ve Asya olmak üzere 3 bölgeye ayrılmıştır. Afrika'da 8 ülke, Botsvana, Fas, Güney Afrika, Moritus, Mısır, Nijerya, Tanzanya, Tunus ülkelerini, Orta ve Güney Amerika'da 15 ülke Arjantin, Bolivya, Brezilya, Ekvator, Guatemala, Honduras, Kolombiya, Kostarika, Meksika, Panama, Paraguay, Peru, Şili, Uruguay, Venezüella'yı ve Asya'da 11 ülkede Filipinler,

[5] MIMIC (Multiple Indicators and Multiple Causes - Çoklu Neden ve Çoklu Gösterge) kayıt dışılığın hem nedenlerini hede göstergelerini model bütünlüğü içinde ele alan bir yöntemdir. Literatürde sıkça kullanılmaktadır.

Güney Kore, Hindistan, Hong Kong, İsrail, Kıbrıs, Malezya, Singapur, Tayland, Tayvan, Türkiye ülkelerindeki kayıt dışı ekonominin boyutları gösterilmiştir.

Afrika'daki 8 ülke arasında, Tanzanya ve Nijerya, kayıt dışı ekonomi oranının en yüksek olduğu ülkelerdir. En düşük kayıt dışı ekonomi oranı ise Moritus ve Güney Afrika′da görülmektedir. Orta ve Güney Afrika′da 15 ülke arasında en düşük kayıt dışı ekonomi oranı Şili′de görülmektedir. En yüksek kayıt dışı ekonomi oranı ise Bolivya′da görülmektedir. Asya′da 11 ülke arasında en düşük kayıt dışı ekonomi oranı Singapur ve en yüksek oran Tayland'da görülmektedir. Türkiye′de kayıt dışı ekonominin boyutu 1999 yılında %32,7 ve bu oranın 2007 yılında %29,1′e düştüğü görülmektedir.

Dünya'da ülkelerin ekonomik risklilik ve güvenilirlik düzeyini ölçmek üzere farklı araştırma kuruluşları çalışmalar yapmaktadır. Araştırmalarda ülkedeki ekonomik istikrarı bozabilecek ekonomik yolsuzluklar ve bu yolsuzlukların sonuçları geniş hatları ile araştırılmaktadır.

OECD suç istatistikleri ile Emniyet Genel Müdürlüğü Faaliyet Raporu verileri üzerinden yapılan bir incelemeye göre, suç ekonomisinin temelinde direk olarak suç ile elde edilen "kriminal sektör" ile kaçakçılık menşeili "illegal sektör" den oluşmaktadır. Kanunsuz ve hukuksuz olarak üretim ve dağıtım illegal sektörü, direk olarak suç işleme ile ilgili, yüksek riskli ve karlılığı yüksek girişimler ise kriminal sektörü oluşturmaktadır (İSMMMO, 2011).

Türkiye'de kaçak içkiden yaşanan ölümlerin yanı sıra, kaçak çay, esrar, fuhuş gibi ekonomik faaliyetler çokça tartışılmaktadır. İSSMMMO'nun 2010 yılındaki araştırmasına göre Türkiye'deki yasal olmayan faaliyetlerden elde edilen gelirin en az 8 milyar TL olduğu ileri sürülmektedir (İSMMMO, 2011:1). 2010 yılı suç gelirleri Tablo 1.5'te incelenmektedir**.**

Tablo 1.5: 2010 Yılı Suç Gelirleri

Suçun Niteliği	Yakalanan	Suçun TL olarak birim karşılığı	Yıllık ciro (Milyon TL)
Fuhuş	15 000 Kişi	24 000 TL/Kişi	1 800,00
İnsan kaçakçılığı	33 000 Kişi	4 500 TL/Kişi	742,50
Esrar	70 000 Kg.	3 000 TL/Kg	1 050,00
Eroin	12 000 Kg.	30 000 TL/Kg	1 800,00
Kaçak çay	2 286 000 Kg.	18 TL/Kg	205,74
Kaçak et	75 000 Kg.	17 TL/Kg	6,37
Akaryakit	7 652 838 Lt.	4 TL/Lt	153,06
Organize suç	112 Örgüt	500 000 TL/Örgüt	280,00

Kaynak: İSMMMO (2011); "Suç Ekonomisinin Türkiye Bilançosu," İstanbul Serbest Muhasebeci Mali Müşavirler Odası Raporu, s:2011/15.

İSMMMO'nun raporunda suç sonrasındaki somut kazanç ile yakalanma sonrasındaki kayıplar arasındaki dengenin suç işlemedeki temel güdüyü oluşturduğu belirtilmekte, özellikle kaçakçılık ile elde edilen çok yüksek gelir nedeniyle giderek artan bir faaliyet olarak ortaya çıktığı ifade edilmektedir (İSMMMO, 2011:3).

Bilişim yoluyla işlenen suçlar kayıt dışı ekonominin boyutunu artırmaktadır. Virüsler, kredi kartı dolandırıcılığı, cryptolocker yazılımları ile şifrelenen verilerin tekrar satılması gibi örnekler ülkemizde de bu konunun önemine dikkat çekmektedir. Ülkemizde ilk bilişim suçu kayıtlara 1990 yılında geçmiştir. 1990 ve 2003 yılları arasında toplam bilişim suçu dava dosyası sayısı 389 dur. 2004 yılında ise bu sayının 429 olduğu ve sonraki yıllarda ise hızla artarak ilerlediği gözlemlenmiştir. Bu durumun temel sebebi hanelerde internet kullanımının 2000 yılından itibaren yaygınlaşmasıdır. 1990 - 2010 yılları arasında toplam bilişim suçu dava sayısı 61.520 adet olarak görülmektedir. İnternetin zaman içerisinde yaygınlaşması ve suç örgütlerinin internet ve bilişim sektörünü kullanıyor olması bilişim suçlarını daha da ön plana çıkarmaktadır.

2. BİLİŞİM VE BİLİŞİM SUÇLARI

2.1. Bilgisayar ve Temel Kavramlar

İnsan müdahalesi olmadan çalışan ilk bilgisayarın (Mark1) 1937 tarihinde üretilmesinin ardından 1945 yılında elektron lambaları kullanılarak ENIAC adlı bilgisayar yapılmıştır. Bilgisayarda transistörün kullanılmaya başlaması ile gelişimine devam etmiş ve bütünleşmiş devrelerin kullanılmaya başlaması ile yeni jenerasyon bilgisayarlar üretilmiştir. Teknolojinin hızla ilerlemesi ile 90'lı yıllarda bilgisayar hacimleri küçülmeye başlamış internetin kullanılmaya başlaması ile birlikte bilgisayarlar her alanda kullanılabilecek çeşitli ölçü ve ebatta yapılarak önü alınamaz şekilde ilerleme kaydetmiştir (Wikipedia, 2017). Teknolojik gelişmeler sadece boyut ve ebatlarının küçülmesi ile kalmamış kullanılmakta olan işlemci, rem ve sabit disklerde de benzer şekilde gelişmeler kaydedilerek bilgisayar dünyası günümüz teknolojisine ulaşmıştır. Bilgisayarlar artık hayatın her alanında kullanılmaktadır. Kamu kurumlarından bankalara özel işletmelerden üniversitelere kadar her düzeyde insan aktif olarak bilgisayarları kullanmaya başlamış ve aynı doğrultuda bilgi alışverişi için kullanılan bağlantı türleri de gelişme göstermiştir.

Bilgisayarlar kullanım alanlarına göre çeşitlendirilmektedir. Süper bilgisayarlar günümüzde kısıtlı yerlerde kullanılmakla birlikte çok güçlü donanım özelliklerine sahip ve bir çok komplike işlemi kısa sürede yapabilen yüksek işlem hızına sahip bilgisayarlar şu an bazı üst düzey kurumlarda kullanılmaktadır. Maliyeti yüksek bir ürün olduğu için dünya üzerinde yaygın değildir. Donanımsal olarak daha alt özelliklere sahip olanlar bazı AR-GE merkezlerinde kullanılmaktadır (Wikipedia, 2017).

Ana bilgisayar (server) ya da sunucu olarak adlandırılan bu bilgisayarlar bir bilgiyi birden çok kullanıcıya dağıtmak için tasarlanmıştır. Sunucular kapanmadan 7 gün 24 saat çalışacak şekilde ve aynı anda çoklu kullanıcıya hizmet verecek şekilde bir donanıma sahiptir. Bankalarda olduğu gibi ortak veri tabanı kullanımları, merkezi noktadan kullanıcı kayıtlarının tutulması, ortak kullanılan elektronik belge yönetim sistemleri (EBYS), web sitesi hizmetleri, dosya paylaşım hizmetleri, merkezi yedekleme hizmetleri bu tip sunucuların kullanımı

sonucu rahatlıkla yapılabilmektedir. Mükerrer kayıtları önleyen ve zaman kayıplarını en aza indiren sunucular günümüzde her sektörde ve kurumsallaşabilen tüm kurum ve firmalarda kullanılmaktadır. Bu nedenle artık birçok bilgiye her noktadan ulaşılmaktadır (İHS, 2016).

Kullanıcı bilgisayarları kişisel kullanımlar amaçlanarak yapılmış bilgisayarlar olup masaüstü ve diz üstü olarak yaygın biçimde kullanılmaktadır. Ülkemizde iş istasyonları şeklinde kullanımı yaygın olsa da asıl amacı ev kullanımı ve küçük iş yerlerinde hizmet vermektir. Donanım olarak biraz daha güçlü olan bu bilgisayarlar iş istasyonu şeklinde karşımıza çıkmaktadır. İş istasyonlarında görsellikten çok spesifik ihtiyaçlara cevap vermek amaçlanmıştır.

Aptal terminal (Thin Client) olarak adlandırılan bu cihazlar Remote Desktop Protocol RDP ve Citrix firmasının çıkarmış olduğu bağlantı protokolü olan ICA iletişim kuralları üzerinden sunuculara bağlanarak oradaki çalışma platformunu kendi üzerine taşıyan cihazlardır. Bu cihazlar bilgisayar gibi çalışmakla birlikte kendi üzerinde veri tutmazlar. Linux, Windows ve AS/400 tabanlı sunuculara bağlanarak çalışma platformu oluştururlar. Kullanım amacı, lisans, donanım ve eğitim giderlerini azaltmak içindir. Ülkemizde e-devlet projelerinin bazılarında da aktif olarak kullanılmıştır. Merkezi yönetimi kolaylaştıran bu sistemler yedekleme maliyetlerini ve zamanını önemli ölçüde düşürmektedir.

Teknolojinin ilerlemesi sonucu günümüzde tablet ve mobil bilgisayarlarda kullanılmaya başlamıştır. Boyutları ve ağırlığı itibari ile kolay taşınabilen tabletler genelde 7” ve 10.1” arasında olmaktadır. Teknolojileri veri oluşturabilmelerini, veri depolayabilmelerini ve verileri paylaşabilmelerini sağlamaktadır. Ses, görüntü, fotoğraf ve çizim işleri ile uğraşanların ideal bulduğu bu cihazların Wifi ve mobil internet teknolojileri mobilite özelliğini artırmakta olup dokunmatik özelliği ile kolay kullanılabilmektedir. Cihaz proje yapmaya, tasarım yapmaya ve oyun oynamaya elverişli olduğu için kullanım kitlesinin daha da artacağı görülmektedir.

İleriki bölümlerde bahsedeceğimiz veri güvenliği ve siber suçlar bölümü için bu tanımlamalar yeterli olacaktır. Her ne kadar bilgisayarların güvenliği

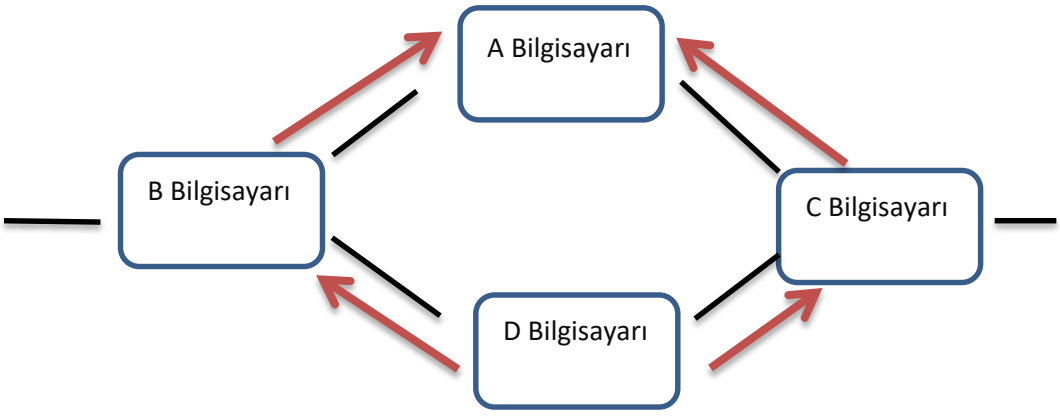
önemli olsa da bilişim suçları, internet bağlantıları sayesinde çok uzaklardan işlenebilmekte ve bilişim suçu işleyenlerin yakalanmalarını zorlaştırmaktadır.

2.2. İnternet ve Temel Kavramlar

İnternet, dünyadaki birçok network ağlarını birbirine bağlayan ve ilişkilendiren iletişim alt yapısına denilmektedir. Türk Dil Kurumu, internet kelimesi yerine "genel ağı" kullanmayı tavsiye etmiştir. İnternet kelimesinin yerine sadece net ifadesinide kullanılmaktadır (wikipedia, 2017). İnternet, sözcük anlamından da anlaşılacağı üzere, "Interconnected set of Networks" (birbirine bağlı ağ) anlamına gelmektedir. Dünya üzerinde bulunan ağların TCP/IP protokolü üzerinden birbirlerine bağlanması ile bu ağ oluşmaktadır.

İnternetin tarihi 1960'lı yıllara kadar uzanmaktadır. İlk kullanılan internet bir sunucu üzerinden çalışmaktadır. Sunucunun zarar görmesi ya da bozulması halinde ise veri aktarımı yapılamadığından dolayı merkezi olmayan dinamik bağlantı yönlendirme (dynamic re-routing) modeli ABD Savunma Bakanlığı tarafından geliştirilmiştir (Alaca, 2008:17). Dinamik Bağlantı Yönlendirme modelinde bağlantı sağlayan bilgisayarlardan herhangi biri zarar görür ise bağlantı aktif olan diğer bilgisayar üzerinden devam etmektedir (Şekil 2.1).

Şekil 2.1: Dinamik Bağlantı Yönlendirme

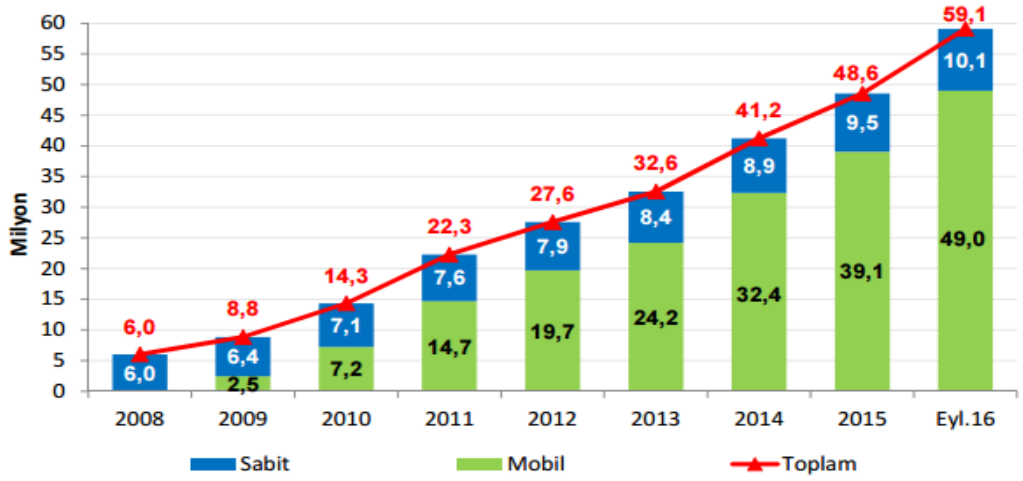


ABD Savunma Bakanlığının bir projesi kapsamında ARPANET projesi çalışmaya başlamış ve ARPANET'in oluşturduğu protokolleri kullanan tüm bilgisayarlar bu ağa bağlanabilmiştir. İlk etapta askeri amaçlı kurulan bu network

daha sonradan ortak protokollerin oluşması ile birlikte geniş kitlelere açılmıştır (Alaca, 2008:17).

Ülkemizde internet bağlantısı ODTÜ ile birlikte TÜBİTAK'ın 1993 yılındaki ortaklaşa yapmış oldukları projesi ile başlamıştır. Dünya üzerinde şu anda 3.576.287.603 internet kullanıcısı bulunmakta olup bu sayı her saniye artmaktadır (Worldometers, 2017).

Grafik 2.1: Bilgi Teknolojileri Kurumu 2016 Yılı Pazar Verileri Raporu



Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, *Türkiye Elelktronik Haberleşme Sektörü, Üç Aylık Pazar Verileri Raporu 2016 yılı 3. çeyrek*

Türkiye'de internet kullanıcı sayıları da sürekli artış göstermektedir. 2016 yılı üçüncü çeyrek sonu itibariyle 59,1 milyon kullanıcıya ulaşmıştır. İnternet kullanıcı sayısının yıllık baremde artış oranı ise %26,5'dır (BTK, 2016). Yıllara göre internet kullanıcı sayıları Grafik 2.1'de görülmektedir.

Tablo 2.1: İnternet Çeşitleri Kullanım Rakamları

	2015-3	**2016-2**	**2016-3**
xDSL	6.946.553	7.444.432	7549.868
Mobil Bilgisayardan İnternet	1.662.797	1.329.239	1.287.931
Mobil Cepten İnternet	35.876.101	43.992.910	47.690.135
Kablo İnternet	596.056	664.095	688.143
Fiber	1,603242	1.775.593	1.822.494
Diğer	92.385	99.479	117.652
TOPLAM	46.777.134	55.305.748	59.156.223

Kaynak: Bilgi Teknolojileri ve İletişim Kurumu, *Türkiye Elektronik Haberleşme Sektörü, Üç Aylık Pazar Verileri Raporu 2016 yılı 3. Çeyrek s: 30*

BTK verilerine göre internet çeşitleri kullanım rakamları Tablo 2.1'de görülmektedir.

2.3. Bilişim ve Bilişim Sistemleri Kavramı

İçinde yaşadığımız çağın her alanında bilişim sistemleri yer almaktadır. Özellikle internetin gelişmesi birçok teknoloji ürününü birbirine bağlamış ve fiziki sınırları ortadan kaldırmıştır. Bu gelişmeler ışığında bilgiye ulaşmak daha da kolaylaşmış ve bu teknolojiyi çağa ayak uyduran tüm kurumlar kullanmaya başlamıştır. Üniversitelerde bulunan online eğitimler, hastane otomasyon sistemleri, muhasebe sistemleri, bankacılık sistemleri, uzaktan eğitim hizmetleri, Resmi gazete ve mevzuat hizmetleri, belediye hizmetleri hayatı kolaylaştıran başlıca örneklerdendir.

Bilişim (informatics) bilgilerin elektronik cihazlar aracılığı ile işlenmesidir. Ceyhun ve Çağlayan (1997:7) bilişimi, teknik, ekonomik ve toplumla ilgili alanlarda elektronik makinalar aracılığı ile bilgilerin düzenli olarak işlenmesi şeklinde ifade etmiştir. Aydın (1992:3) ise bilişimi, bilginin derlenmesi depolanması, tekrar çağrılması ve analiz edilmesi için gerekli yöntemler olarak tanımlamaktadır. Değirmenci ve Yenidünya (2003:27) ise bilişimi birçok alanda elde edilen verinin saklanması, işlenmesi, düzenlenmesi ve istiflenmesi, ihtiyaç duyulduğunda analiz edilebilmesi ve farklı kaynaklara yönlendirilmesi ile ilgili bir bilim dalı olarak tanımlamıştır. Benzer bir tanımı da Dülger (2004:47) yapmış ve bilişim tanımına ek olarak tüm süreçlerin sanal olarak tekrar oluşturulması, stoklanması ve ilgili kişilerin ulaşımına açılması gerekliliğini ileri sürmüştür.

Bilişim sistemi Türk Ceza Kanunu madde 243'te "verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağı veren manyetik sistemler" olarak ifade edilmiştir.

Genel olarak tanımlara bakıldığında bilişim insanların ekonomik, sosyal, kültürel ve toplumsal yaşam gibi birçok alanda sahip oldukları verilerin alınarak depolanması, depolanan bu verilerin işlenerek uygun biçimde derlenmesi, düzenlenmesi ve farklı ortamlara farklı veri aktarma yolları ile aktarılması olarak ifade edilebilmektedir.

2.4. Bilişim Suçları

Dünyada teknolojik gelişmelerin yaşanması ile birlikte birçok bilişim aracı yaşamımızın bir parçası olmuştur. Yeni suç yaklaşımları oluşmakta, suçlular yeni sistemleri kullanarak kanuna aykırı yaşamlarını ve icraatlarını devam ettirmektedirler. Özellikle teknolojik yaklaşımların oyuna katılması ile işlenen suçlarda oldukça fazla artış gözlenmektedir. Bilişim suçları için Türkçe literatürde siber suçlar, internet suçları, dijital suçlar, yüksek teknoloji suçları, sanal suç, internet suçu, bilgisayar suçu, siber suç gibi isimler kullanılırken uluslararası literatürde Computer Crimes, Cyber Crimes, Crime of Networks, IT Crimes, High Tech Crimes isimleriyle adlandırılmaktadır (Dülger, 2004:64-65). Bilişim suçları özellikle internetin kullanımının yaygınlaşmasıyla hızlı bir şekilde ilerlemiş ve 1995 yılından itibaren bu tip suçların yapısı, özellikleri ve tekrarlanma sıklığı hissedilir düzeyde artmıştır (Carter, 2002:183).

Dünyada siber suçlar için genel kabul görmüş tek bir tanım bulunmazken Avrupa Ekonomik Topluluğu 1983'te "bilgileri otomatik olarak işleme tabi tutan yahut verilerin nakline yarayan bir sisteme karşı veya sistem ile gayri kanuni, ahlak dışı ve yetkisiz gerçekleştirilen her türlü davranıştır" ifadeleri ile siber suçlar için tanımlama yapmıştır. Aydın (1992) bilişim suçlarını bilgisayar veri ve yazılımlarına izinsiz girilmesi, izinsiz kullanılması ve tahrip edilmesi olarak tanımlamıştır. Avrupa Konseyi Bakanlar Komitesi tarafından oluşturulan *Avrupa Siber Suçlar Sözleşmesi,* bilişim suçlarını şu şekilde sınıflandırmıştır;

1- Dijital verilerin ve sistemlerin bütünlüğüne, ifşasına ve ulaşılabilirliğine ilişkin suçlar;
   a- Kanunsuz erişim
   b- Yasal olmayan bir şekilde araya girme,
   c- Verilere kanunsuz müdahale,
   d- Bilişim sistemine müdahale,
   e- Bilişim ekipmanlarının kötü amaçla kullanımı,
2- Bilgisayarlara bağlantılı suçlar;
   a- Bilgisayarla bağlantılı sahtecilik,
   b- Bilgisayarla bağlantılı dolandırıcılık,

3- İçerik ile ilgili suç unsurları;
   a- Çocuğun cinsel içerikli kullanıldığı suçlar,
   b- Patent gibi haklar ve ihlali ile ilgili suçlar,

Bilişim sistemlerinin gelişmesi sonucunda her yerden ve her noktadan bankacılık, alışveriş, kredi kartı işlemleri, e-devlet işlemleri, çocukların uzaktan izlenmesi gibi güvenlik işlemleri, okul notu girme ya da öğrenci işlemlerinin yapılması gibi birçok çalışma uzaktan yapılabilir bir duruma gelmiştir. Bu gelişmeler hayatımızı oldukça kolaylaştırmakta fakat yeni güvenlik açıklarının oluşmasına sebep olmaktadır. Örneğin daha önceki dönemlerde nakit paranın çalındığı adi hırsızlık vakaları görülürken günümüzde banka hesapları üzerinden bu paraların çalınabildiği gözlemlenmektedir. Önceki suçlarda kişinin yakınları rehine olarak kullanılırken günümüzde kişinin şirketindeki veri tabanın şifrelenmesi ve para karşılığı tekrar kişilere satıldığı görülmektedir.

Bilişim suçları diğer adi suçlara göre daha farklı şekillerde karşımıza çıkmaktadır. Dolayısı ile bu suçlar diğer adi suçlara göre daha zor tespit edilebilmekte ya da tespit edilebilse dahi adli işlem yapılamamaktadır. Bu durumun nedenlerini şu şekilde sıralayabiliriz;

1. Siber saldırıya uğrayanların şahsi bilgileri çalınsa dahi şahsi verilerinin çalındığını duyurmak istememektedir.
2. Şirketlere yapılan siber saldırıların duyurulması şirketleri ortakları nezdinde zor duruma düşürmekte ve işlem görülen borsada çok ciddi tepki gördükleri için saldırılar gizlenmektedir.
3. Lokasyon farklılıkları yapılan siber saldırıların çözümünü zorlaştırmaktadır. Saldırganın çok uzakta olması farklı yasalara tabi olması ve suçun karşılığında doğrudan şahıs tespit edilememesi saldırıyı ve yapılan saldırının takibini güçleştirmektedir. Bu nedenle siber saldırıya uğrayanlar saldırıya uğradıklarını zorunlu olmadıkça kolluk kuvvetlerine bildirmek istememektedir.
4. Siber saldırılar konusunda yetişmiş kolluk kuvvetleri personeli sayısının azlığı saldırıya uğrayanların nasıl olsa bulunamaz düşüncesi ile davranmalarına sebep olmaktadır.

5. Saldırıya uğrayanların büyük bir kısmı saldırıya uğradığının farkına varamamaktadır. Bu nedenle masum kişiler bilinçsiz olarak suça maruz kalabilmektedir.
6. Doğrudan maddi zarar görmeyen kişiler saldırıyı önemsememekte dolayısı ile genel çözüm üretilememektedir.

2.4.1. Bilişim Suçlarının Tanımı

Bilişim vasıtasıyla işlenen suçlar bilişim suçları olarak değerlendirilmektedir. Bilişim suçları için dilimizde "bilgisayar suçları, teknolojik suçlar, dijital suçlar, siber suçlar, internet suçları" gibi tanımlamalar kullanılmakla birlikte diğer birçok ülkede; computer crimes, crimes of network, IT crimes (information technologies), cyber crimes gibi isimlerle anılmaktadır (Pocor, 2004:27-37).

Bilişim terimi birçok teknolojik alanı kapsamaktadır. Bilişim sistemleri kapsam olarak, sunucu, bilgisayar, network, internet gibi bilgisayar ve iletişim alt yapısının oluşturduğu teknolojileri ihtiva ettiğinden, bu çerçevede işlenen bütün suç çeşitleri de "Siber Suçlar" başlığında toplanmıştır (Yılmaz, 2014).

Siber suçların ne olduğu ve tarifi hakkında birbirinden farklı tanımlamalar yapılmaktadır. Günümüzde gelişen teknoloji göz önüne alındığında siber suçlarında sürekli şekil ve yöntem değiştirmesi, bunun yanında suçun hukuki ve cezai yaptırımının bulunması tarafların üzerinde mutabık kalacağı ortak bir tanım yapılmasını zorlaştırmaktadır. Her ne kadar birbirinden farklı yorumlar yer alsa da AT uzmanlarının 1983 yılında ortaya koyduğu tanıma göre bilgileri işleyen veya taşınmasına yarayan sistemlere kanun dışı, ahlaka uygun olmayan ve yetkisiz olarak gerçekleştirilen her türlü davranış bilişim suçu olarak adlandırılmaktadır. Birçok tanıma göre daha kapsamlı olan bu tanım bazı uzmanlar tarafından eleştirilmesine rağmen bilişim suçlarının toplumsal boyutlarını da kapsadığı için geniş bir kesim tarafından kabul görmüştür (Kurt, 2005:50).

5237 sayılı Türk Ceza Kanununda ise "bilişim alanında suçlar" kapsamında bulunan "bilişim sistemine girme" (m. 243), "sistemi engelleme, bozma, verileri yok etme veya değiştirme" (m. 244) ve "banka veya kredi kartlarının kötüye kullanılması" (m. 245) suç tanımlamaları kullanılmıştır.

Bilişim suçları, BM ve AB verilerine göre altı konu başlığında listelenmiştir. Bu suçlar (Kuplay, 2007);

- Bilişim Sistemleri Sabotajı,
- Bilişim Sistemlerine Kanunsuz Ulaşım,
- Bilgisayar Yoluyla Dolandırıcılık,
- Bilişim Yolu İle Sahtecilik,
- Koruma Altındaki Yazılımın İzin Dışı Kullanımı,
- Pornografik Paylaşımlar.

Amerika Birleşik Devletler hükümeti Federal Soruşturma Bürosunun (FBI) hazırlamış olduğu çalışmada bilişim suçları aşağıdaki şekilde sıralanmıştır (İlbaş, 2009:3);

- Telefon santrallerinin ihlal edilmesi,
- Network yapılarının ihlal edilmesi,
- Ağ bağlantılarındaki yapının ihlal edilmesi,
- Kişilerin yaşamlarını ilgilendiren verilerin ihlal edilmesi,
- Endüstriyel casusluk,
- Korsan yazılımlar
- Bilişim alt yapısı kullanılarak işlenilen her türlü suçlar

2.4.2. Bilişim Suçları ve Hukuk

Bilişim suçları temelde klasik suçlar ile benzerlik gösterse de içeriği birbirinden farklıdır. Bilişim sistemleri ve internet uygulamaları işin içerisine girdiğinde suçun şekilleri ve boyutları değişmekte, etkisi yükselmektedir. Hırsızlık, dolandırıcılık, sahtecilik ve benzeri gibi suçların bilişim yolları ile işlenme süreleri ve hırsız üzerindeki psikolojik etkileri birbirlerinden ayrılarak farklılık göstermektedir. Başta ceza kanunu olmak üzere ilgili mevzuatımıza bilişim terminolojisi ve bilişim sistemlerinin mantığını eklemeden bilişim suçları

ile ilgili karar ve hüküm vermek oldukça zordur. Bu kapsamda bilişim alanındaki gelişmelere paralel olarak uluslararası hukukta bir takım düzenlemeler yapılması zarureti doğmuş ve 2001 yılında Avrupa Konseyi Siber Suç Sözleşmesi imzalanmıştır. 2010 tarihi itibari ile 46 ülke tarafından imzalanan sözleşmeyi birçok ülke henüz kendi ülkesinde tasdik etmemiştir (Convention on Cybercrime,2010). Türkiye ise bu sözleşmeyi henüz imzalamamıştır.

Türkiye'de bilişim suçları 5237 sayılı yeni TCK'da, Bilişim Alanında Suçlar adı ile 243 ile 246. maddeler arasında bilişim sistemine girme, bilişim sistemi engelleme, bozma, verileri yok etme veya değiştirme, banka kartlarının kötüye kullanılması, tüzel kişiler hakkında güvenlik tedbiri uygulanması olarak düzenlenmiştir.

Aynı zamanda siber suçları, bahse konu kanunun bir diğer bölümü olan özel hayatın gizliliğine karsı suçlar başlığı altında 132. ve 138. maddeler arasında haberleşme gizliliğinin ihlâl edilmesi, bireylerin kendi aralarındaki konuşmaların dinlenmesi ve kaydedilmesi, özel hayatın gizliliğinin ihlâl edilmesi, şahsi verilerin kanunsuz yedeklenmesi, verileri kanunsuz olarak alma, başkaları ile paylaşma, verileri imha etmeme olarak tanımlanmıştır. Şerefe Karşı Suçlar başlığı altında 125. Maddede ise hakaret (bilişim sistemi kanalıyla hakaret) yer almıştır.

2.4.3. Zonguldak'ta Bilişim Suçlarının Adli Boyutu

Türkiye'de bilişim suçları başlıklı bölge ve il düzeyinde en sık karşılaşılan bilişim suçlarının tespit edilmesi, Türkiye'deki bilişim suçu profilinin çıkarılması için 2011 yılında bir çalışma yapılmıştır. Çalışmada 1990 yılından 2011 yılının temmuz ayına kadar yıl ve il bazında mahkemelere intikal eden 41 farklı suç maddesine ait 73.185 adet ceza ve hukuk davası dosya ve sanık sayıları açısından incelenmiştir (İlbaş ve Köksal, 2011). Söz konusu çalışmada Türkiye çapında bilişim sistemleri banka veya kredi kurumlarının araç olarak kullanılması suretiyle dolandırıcılık suçundan 24.254 dava, başkasına ait banka veya kredi kartının izinsiz kullanılması suretiyle yarar sağlama suçundan 14.166 dava açılmıştır. Ayrıca bilişim sistemine hukuka aykırı müdahale suretiyle haksız çıkar sağlama suçundan 4258 dava, bilişim sistemlerinin kullanılması suretiyle hırsızlık

suçundan 3517 dava açıldığı görülmüştür. Çalışmaya ilişkin bazı veriler Tablo 2.2'de gösterilmektedir.

Tablo 2.2: Türkiye'de 1990 -2011 Yılları Arası Bilişim Suçları Dosya Sayısı

Sıra	Şehir	Toplam	Nüfus (2000)	Sıra	Şehir	Toplam	Nüfus (2000)
1	İstanbul	20412	10 018 735	16	Yalova	182	168 593
2	Muğla	1444	715 328	17	Çanakkale	481	464 975
3	Antalya	3469	1 719 751	18	Edirne	410	402 606
4	İzmir	5876	3 370 866	19	Gaziantep	1299	1 285 249
5	Aydın	1491	950 757	20	Eskişehir	711	706 009
6	Denizli	1286	850 029	21	Bolu	270	270 654
7	Ankara	5984	4 007 860	22	Kayseri	1046	1 060 432
8	Bursa	3120	2 125 140	23	Kırklareli	301	328 461
9	Kocaeli	1674	1 206 085	24	Balıkesir	950	1 076 347
10	Adana	2468	1 849 478	25	Manisa	1084	1 260 169
11	Batman	561	456 734	26	Konya	1795	2 192 166
12	Uşak	360	322 313	27	Karabük	178	225 102
13	Mersin	1836	1 651 400	28	***Zonguldak***	***481***	***615 599***
14	Tekirdağ	684	623 591	29	Isparta	397	513 681
15	Sakarya	822	756 168	30	Rize	279	365 938

Kaynak: İlbaş, Çığır ve Mehmet Ali Köksal (2011); "Türkiye'de Bilişim Suçları (1990 -2011)", http://www.cigir.com/tr/images/bsraporu.pdf, (Erişim Tarihi: 10.06.2014).

Tablo 2.2 incelendiğinde; 2000 yılındaki nüfus sayımına göre 10.018.735 nüfuslu İstanbul 20.412 toplam dosya sayısı ile başı çekerken 4.007.860 nüfuslu Ankara 5.984 dava dosyası ile 7.sırada, 615.599 nüfuslu Zonguldak ise 481 dava dosya sayısı ile 28. sırada bulunduğu kaydedilmiştir.

Tablo 2.3: Zonguldak'ta 2002 -2011 Yılları Arası Dava Sayıları

Yıllar	2002,2004	2005	2006	2007	2008	2009	2010	2011*	Toplam
Dava Sayıları	2	12	44	59	82	95	108	79	481

*2011 Temmuz ayına kadar

Tablo 2.3'te görüldüğü üzere Zonguldak ilinde 2002 ve 2004 yıllarında 1'er, 2005 yılında 12, 2006 yılında 44, 2007 yılında 59, 2008 yılında 82, 2009 yılında 95, 2010 yılında 108, 2011 yılı temmuz ayına kadar ise 79 bilişim suçları ile ilgili dava sayısı olduğu görülmüştür. Bu tarihler arasında kararı çıkan dosya sayısı 357 olurken sanık sayısı 619 olarak kaydedilmiştir.

2.5. Bilişim Suçlarının Sınıflandırılması

Bilişim suçlarının belirli özelliklerine göre sınıflandırılması, anlaşılması açısından kolaylık sağlayacaktır. Belirli suç türleri arasındaki ilişki ve birbirilerine benzeyen suç türleri arasındaki fark tanımlamalar içerisinde daha net anlaşılacaktır. Bilişim alanındaki suç tipleri incelenirken en fazla karşılaşılan temel suçlar şu şekilde açıklanmaktadır.

2.5.1. Yetkisiz Erişim

Bir ağa bağlı veya çevrim dışı olarak çalışan bilgisayar, sunucu gibi sistemlere giriş izni olmaksızın sistem açığı, personel hatası gibi farklı sebeplerden dolayı izinsiz olarak erişim sağlanmasına "yetkisiz erişim" denilmektedir. Yetkisiz erişim en yaygın ve en çok bilinen bilişim suçu türüdür. Yetkisiz erişim, bilişim alt yapısının az bir parçasına ya da sistemin bütününe olabileceği gibi uzak mekânlardan ya da direk ulaşma şeklinde de olabilir (Akkan, 2013:6). Yetkisiz erişim sadece bilgisayar açıklarından yararlanılarak yapılmamaktadır. Bir kullanıcının ortak internet kullanılan ortamlarda oturumunu açık bırakmasından ya da bilgisayarını açık bırakarak uzaklaşmasından da kaynaklanabilmektedir. Yetkisiz erişim TCK'nın bilişim başlığında 243. maddesinde tanımlanarak suç kapsamında olduğu belirlenmiştir.

2.5.2. Hesap İhlali

Hesap ihlali, bir kullanıcının hesabına yetkisiz bir şekilde erişerek bu durumdan istifade etmesiyle ortaya çıkmaktadır. Bir kişinin ya da kurumun bilişim cihazlarına izinsiz olarak, kişinin rızası olmadan, kanun dışı bir şekilde kullanılması hesap ihlali olarak tanımlanmaktadır (Tulum, 2006:25).

2.5.3. Yetkisiz Dinleme

Bir bilgisayarın, telefonun veya diğer iletişim araçlarının kanunen yetkisiz kişiler tarafından dinlenmesidir. Akkan(2013:6)'a göre suçun hedefi her türlü bilgisayar iletişimidir. Ağ trafiğinde yetkisiz dinleme yapabilmek için bazı veri

yakalama "*Sniffing*"[6] araçları da kullanılabilmektedir. Bu programlar ile Telnet, http, FTP, SMTP, IMAP gibi hemen hemen her türlü protokol takip edilebilmektedir. Örneğin Mailsnarf programı ile dinlenen ağ trafiği üzerinden geçen SMTP bağlantıları toplanıp anlaşılabilir hale getirilebildiği gibi Urlsnarf programı ile dinlenen ağ trafiği üzerinden geçen http trafiğindeki linkler takip edilebilmektedir. İnternetin büyük oranda şifresiz protokollerden oluştuğu düşünülürse yetkisiz dinleme siber güvenlik için büyük bir tehdit oluşturmaktadır. Pasif dinleme programları hedef sistem ile iletişime geçmediği için izlemeye dair bir izde bulunmamaktadır.

2.5.4. Banka Kartı Dolandırıcılığı

Banka kartı dolandırıcılığı özellikle geçtiğimiz son birkaç yılda büyük artış gösteren bir konudur. ATM (Automated Teller Machine) ve pos makinalarında kullanılmak üzere üretilen bu kartların kullanım esnasında PIN – (Personel Identification Number) bilinmesi gerekmektedir. Geçtiğimiz yıllarda post makinalarından şifresiz, sadece imza ile kullanılabilen bu kartlardan dolayı bir çok mağduriyet yaşanmış ve çalınan kredi kartları ve bankamatik kartları alış verişlerde sıkça kullanılmıştır. Bankamatik ve Kredi kartı dolandırıcıları ATM'nin kart okuyucusuna yerleştirilen özel bir düzenek ile bankamatik kartını kart okuyucu içerisinde alıkonulmuş gibi göstermekte dolandırıcı kart sahibinin ATM'nin başından uzaklaşmasının ardından kartı alarak başka bir ATM cihazından hesaptaki parayı çekmektedir. Kullanılan yöntemlerden bir diğeri de kullanıcının bankamatik kartını kopyalamaktır. Bu yöntemde dolandırıcı bankamatik kart okuyucusunun önüne yerleştirmiş olduğu manyetik kart okuyucu ile o ATM de kullanılan tüm kartları okutarak bilgilerini depolayabilmektedir. Daha sonradan aynı kartın benzerleri üretilerek dolandırıcılık gerçekleşmektedir. Kart kopyalama gibi girilen şifreleri kaydeden klavyeler ve ATM'nin önüne yerleştirilebilen gizli kameralarda dolandırıcıların kullandığı diğer yöntemlerdendir. En etkili dolandırıcılık türlerinden bir tanesi de mağazalarda kredi kartlarının kopyalanmasıdır. Bu tür kopyalama işlemlerinde veriler gerçek olduğu için dolandırıcılığın ispatı da zor olmaktadır (Ntvmsnbc, 2014).

[6] Sniffing teknik olarak transfer edilen verinin yolunu keserek kullanıcı ismi ve şifreler ile diğer dosyaları yakalamak için kullanılan bir ağ dinleme tekniğidir. Sniffing Pasif ve Aktif olarak iki yöntem ile yapılabilmektedir.

2.5.5. İnternet Bankası Dolandırıcılığı

İnternet Bankacılığı, her türlü banka işlemlerinin internet ortamında sunulduğu bir hizmettir. Bir bankanın şubeden sağladığı birçok hizmet, zaman sorunu olmadan kolay bir şekilde sağlanmaktadır. Benzer şekilde kredi katları ile birçok web sitesi üzerinden alışveriş yapmak mümkündür. Kredi kartı bilgileri ile sanal pazarlarda yapılan alışverişlerde kullanıcıları bazı tehditler ve risklerde beklemektedir. Bilişim Suçları ile Mücadele Şube Müdürlüğünün verilerine göre mail yolu ile gönderilen virüslü programlar, download sitelerinden indirilen programlar, ya da benzer yollar ile kullanıcın bilgisayarına virüs bulaşması ve kullanıcının daha sonra internet bankacılığına giriş yapması sonucu ikiz sayfa yöntemi ile şifre bilgilileri dolandırıcıların eline geçmektedir (Milliyet, 2012).

2.5.6. Bilgisayar Yazılımının İzinsiz Kullanımı

Gerek ticari amaçlı yapılan gerekse bireysel ihtiyaçları karşılamak üzere hazırlanan yazılımları yazılım firmaları hazırlamak için AR-GE aşamasında yüksek miktarda kaynak ayrılmaktadır. Lisans bedellerinin ödenmemesi, yazılımın lisans şifresinin kırılması yada kopya lisanslar ile firma zarara uğramaktadır. Hukuken yazılımının izin alınmadan kullanılması yasalar ile korunurken yazılımların izinsiz bir şekilde yaygınlaştırılması da yasaklanmıştır (İlbaş, 2009:25-28).

2.5.7. Sahte Kimlik Kullanma ve Kimlik Taklidi

Dolandırıcıların en çok kullandığı yöntemlerden biri olan ve "yetkisiz erişim", "hesap ihlali", "yetkisiz dinleme", "banka kartı dolandırıcılığı", "internet bankası dolandırıcılığı" gibi bilişim suçları işlerken kullanılan yöntemlerden bir tanesi de "sahte kimlik kullanma ve kimlik taklidi" yapmaktır. Dolandırıcının amacı legal kullanıcılar gibi davranarak onların hesaplarına erişmektir. Bu yöntem sosyal medyadaki oturumları ele geçirmek için de kullanılmaktadır (Sofaer vd., 2001:291). Oturumu ele geçirmek için iki farklı yöntem kullanılmaktadır. Bunlardan birincisi kullanıcı güvenlik aşamalarını kendisi geçer ve işlem esnasında dolandırıcı oturumu çalarak işlemine devam eder. İkinci yöntem ise dolandırıcı daha önceden "sosyal mühendislik" gibi çeşitli hileler ile elde ettiği verileri kullanarak legal kullanıcının dolandırmak istediği hesabına erişim sağlamaktadır.

Sahte kimlik kullanımı bilişim yolu ile işlenebileceği gibi gündelik hayatta da işlenebilmektedir. Norton Anti virüs firmasına göre kimlik hırsızlığı iki aşamalı olarak gerçekleşmektedir. Bireysel bilgileriniz çalınması birinci aşamada gerçekleşmektedir. İkinci aşamada ise çalınan bilgileriniz dolandırıcılık yapmak için kullanılmaktadır (Merritt, 2014). Merritt in aynı yazısındaki tespitlerine göre ABD Federal Ticaret Komisyonu'na en çok bildirilen tüketici şikâyeti kimlik hırsızlığıdır. Bu komisyon sadece 2013 yılında 250 binden fazla çalınmış kimlik ihbarı aldıklarını açıklamışlardır (Merritt, 2014).

Kimlik hırsızlığı yıllara göre artış göstermektedir. ABD verilerine göre 2005 yılındaki kimlik hırsızı mağduru sayısı 6.424.900 iken 2010 yılında bu rakam 8.571.900'i ulaşmıştır (Hekim ve Başıbüyük, 2013:139). Kimlik hırsızlığı çoğu zaman iktisadi amaçlarla yapılıyor olsa da kişiyi itibarsızlaştırmak amaçlı (internetten uygunsuz içerikli materyaller satın almak, sanal kumar oynamak, o kişinin hesabından istemediği kurum ve kuruluşlara bağışlarda bulunmak) kullanımları da görülmektedir.

Türkiye'de durum daha ürkütücüdür. 2010 yılında bir çetenin yakalanması sonucu ortaya çıkan duruma göre 70 milyon vatandaşın adres, kimlik ve telefon numarası bilgileri çalınarak satışa sunulmuş olduğu ortaya çıkmıştır. İstanbul Emniyet Müdürlüğü Bilişim Suçları ve Sistemleri Şube Müdürlüğüne göre bu veriler resmi kurumların veri tabanlarından alınarak ve sigorta bilgileri, adres bilgileri veya araç bilgileri ile birleştirilip paket programı haline getirilerek özellikle hukuk bürosu gibi kurumlara satışı yapılmaktadır (Ntvmsnbc, 2010).

2.5.8. Yasadışı Yayınlar

Kanunun yasaklamış olduğu materyalleri; web siteleri, DVD, CD, USB kartı, harici disk ya da mail gibi internet aracılığı ile dağıtılması, yayınlanması ve yaygınlaştırılması olarak ifade edilmektedir. Tulum (2006:33) yasadışı yayınları, kanuna uygun olmayan unsurların yayınlanması ve yaygınlaştırılması amacı ile bilişim sistemlerinin kullanılması olarak tanımlarken yasadışı her türlü materyalin, web siteleri, haber grupları ve dijital veri taşıyıcılar ile yayınlanması olarak ifade etmiştir.

2.5.9. Telif Hakları ve Ticari Sırların Çalınması

Ticari sırlar firmalar için oldukça önemli olup kaybedilmesi ya da çalınması firmalara maddi ve manevi zararlar vermektedir. Şener (2013) ve Alaca (2008:93) ticari olarak sır kabul edilen verilerin çalınmasını, firmayı ekonomik zarara uğratmak amaçlı veri hırsızlığı, kanunsuz olarak alınan bu verilerin ifşa edilmesi veya yok edilmesi olarak tanımlamıştır. 2008 yılında hazırlanan Avrupa Konseyi Siber Suçlar Sözleşmesi Taslağına göre (2008), telif hakları patent ve fikri hakların ticari kısımlarını kapsayan sözleşme ve WIPO[7] kararları uyarınca bilişim alt yapısı ile ticari içerikli saldırılar yapılması durumunda kendi ulusal kanunlarınca da suç olarak tanımlanması için tüm tarafların çalışma yapmasını şart koşmuştur.

2.5.10. TV Kartları ile Şifreli Yayınları Çözme

Bilgisayara takılarak kullanılan TV kartlarının yaygınlaşması ve sektördeki teknolojinin ilerlemesi ile birlikte şifreli programların şifresinin kırılabilmesi olanakları da doğmuştur. Televizyon kartları ile birlikte şifre çözücü yazılımların (Soft Cam) kullanılması şifreli yayınları şifresiz olarak seyredebilme imkânı sağlanmıştır (Boğa, 2011:32). TV kartları ile şifrelerin çözülmesi, yayını hazırlayan ve ücret karşılığında şifreli olarak satan yayıncı firmayı maddi zarara uğratmaktadır. Şener (2013)'e göre 5846 sayılı kanunda bahsedilen Fikir ve Sanat Eserleri Kanunu uyarınca şifreyi kıran, izleten ve izleyene cezai hükümler uygulanacağı ileri sürülmektedir.

TV kartları ile yapılabilecek bir diğer uygulama ise "Kanca/Olta yöntemi" olarak da bilinen offline downloaddır. Bu yöntem ile uydu kullanıcılarına gönderilen programları TV kartı ve uygun programlar ile tutmak ve aynı uygulamaları bilgisayara indirmek için kullanılmaktadır. Offline download yapılırken istediğiniz programlar inmemekte, o uydudan verilen yayınlar alınabilmektedir. Offline downlad, uydudan internet hizmetinin verildiği uydu ve frekanstan yapılabilmektedir. Offline downlad, internet hizmetini kullanmamakta ve tek taraflı indirme yapmaktadır. Bu nedenle tespiti oldukça zordur.

WIPO (World Intellectual Property Organization) 1967 yılında Birleşmiş Milletler tarafından Dünyadaki fikri mülkiyet haklarının korunmasını teşvik etmek amacıyla kurulmuştur.

Offline download yapılırken inen dosyaya göre önemli birtakım bilgilere ulaşılabilmektedir;

1- Uydu internet alıcısından dosya talep eden cihazın MAC adresi,
2- Dosyanın talep edildiği IP adresi,
3- Dosyayı talep edenin IP adresi,
4- Data miktarları ile ilgili birtakım bilgiler.

Bu bilgiler hacking yada istihbarat çalışmaları için kullanılabilmektedir.

2.5.11. Çocuk Pornografisi

"Pornographie" sözcüğü, geç dönem Yunancasındaki "Fahişelik Hakkında Yazan" anlamına gelen "pornographos" tan alınan "pornographe" dan türemiştir. Fransızcadan dilimize "pornografi" olarak girmiş olan müstehcenlik "Açık saçık yayın veya resim; edebe aykırı kitap veya resim" anlamında kullanılmaktadır (Erbaşı, 2007:1615).

T.C. İçişleri Bakanlığı Araştırma ve Etütler Merkezine göre, sosyal hayatı birçok yönden olumsuz etkileyen etkenlerin başında, "müstehcenlik", "erotizm" ve "pornografi" gelmektedir. Birleşmiş Milletler Çocuk Hakları Sözleşmesinin 1. Maddesi her bireyi 18 yaşına kadar çocuk olarak nitelendirmiştir. Bu sözleşmeye ek olarak, Avrupa Konseyinin 1991 yılında çocukların cinsel sömürüsü, pornografisi ve satışıyla ilgili olarak almış olduğu tavsiye karar doğrultusunda cinsel olarak kullanımı amaçlı görsel ve işitsel tüm materyalleri bu kapsamda değerlendirmektedir (EC, 2001).

Her ne kadar farklı tanımlar olsa da çıkan sonuca göre çocuk pornografisi çocuğun cinsellik amacı ile sesli ve görüntülü istismarı olarak nitelendirilebilir. Çocuk pornografisi tanımı ülkeden ülkeye değişiklik göstermektedir. Dünya ülkelerinin birçoğunda çocukluk yaşı kendi mevzuatlarına göre farklılık gösterdiğinden suç unsuru da ülkeden ülkeye değişiklik göstermektedir. Bu yasal açıklıklar çocukların daha fazla istismar edilmesine neden olmakta ve bir ülkede suç olan unsurun başka bir ülkede suç teşkil etmediği gözlenmektedir.

2.5.12. Siber Zorbalık Taciz ve Şantaj

Siber zorbalık gerçek hayattaki zorbalığın sanal dünyaya taşınmasıdır. Yaygınlaşan internet kullanımıyla birlikte siber saldırı olayları da artmaktadır. Siber taciz sanal dünyadaki her türlü ekipmanın kullanılarak kişilerin rahatsız edilmesidir. Sanal olarak başlayan, bazen taciz olarak kalan bazen de tehdit ve şantaj olarak ileri seviyelere taşınan, tecavüz ve öldürme gibi sanal dünyadan gerçek dünyaya taşan adi suçların kuluçka dönemi olması nedeni ile önem arz etmektedir (Hekim ve Başıbüyük, 2013:141).

Siber Şantaj suçunda, saldırganlar sunucuların veri tabanındaki ya da kişisel bilgisayardaki bilgileri ele geçirmektedir. Ardından bu bilgilerin internette yayınlamakla şantaj yapıp para talep edilmektedir. Günümüzde bu ve benzeri yöntemlerle birçok dolandırıcılık yapılmakta firmalar ve kişiler maddi ve manevi zarara uğratılmaktadır. Prestij kaybına sebep olan ve kişisel mahremiyeti ihlal eden siber şantaj suçu sadece Türkiye'de işlenmemekte yurt dışı menşeili çetelerle de işbirlikleri yapılmaktadır.

Siber şantaj sadece firmalara ya da önemli kişilere yapılmamaktadır. Çocuk istismarı içinde siber şantaj yöntemi kullanılmaktadır. Ele geçirilen kişisel veriler ile çocuğu komuta eden sanal zorbalar intihara kadar ulaşan pek çok duruma neden olmaktadırlar.

2.5.13. İnternet ve Kumar

5237 sayılı TCK'nin 228. maddesindeki topluma karşı suçlar başlığında "kumar oynanması için yer ve imkân sağlanması suçu" düzenlenmiştir. Her ne kadar kanunda sanala atıfta bulunulmasa da sanal kumarhane sahipleri sunucularını kumarın suç teşkil etmediği ülkelere kurmaktadırlar. Kanun koyucu bu ülkelerdeki sanal kumarhanelerin IP'lerine erişimi kapatmaktadır. Ancak erişime kapalı IP'lere ulaşmak için farklı yöntemler kullanılmakta ve takibi zorlaşmaktadır.

İnternetin dünyaya açık doğal yapısı, ülkelerin hukuk sistemleri arasında farklılıklarının bulunması, küçük ada devletlerinin diğer devletlere göre yasalarında eksikliklerinin bulunması internetin suça bakışta yapısal sorununu

teşkil etmektedir. Bilişim suçlarının kaynağı incelendiğinde çoğunlukla küçük ada devletleri çıkmaktadır (İlbaş, 2009:93).

2.5.14. Terörist Faaliyetler/ Siber Terör

Siber terörizm, terör faaliyetlerinin sanal ortama taşınmasıdır. Teröristler için siber terörizm birçok açıdan önemlidir. Özellikle sanal âlemde saklanabilmeleri, ekonomik olması, daha az insana ihtiyaç duyulması, etkisinin yüksek olması ve terör eylemlerinin yanı sıra önemli bilgilere de ulaşılabilmesi terör eylemleri için bilişim altyapısını çekici hale getirmektedir. Hedef olarak seçilebilecek noktaların sayısının çokluğu ve bomba niteliği taşıyabilecek virüslerin uzaktan kontrol edilebilmesi terör eylemlerini de nitelik açısından ileri seviyelere götürmektedir.

Türk Asya Stratejik Araştırmalar Merkezinin "Siber Terörizm" konulu raporunda Amerikan askerlerinin Afganistan'daki operasyonlarda ele geçirilen El Kaide'ye ait bilgisayarları incelediğinde örgütün beklenenden çok daha yüksek düzeyde teknolojik donanıma sahip olduğu görülmüştür (Tasam, 2004:9). Yine aynı rapora göre Irak tarafından 1990 ların başından itibaren "Irak Ağı" kurulmuş ve DoS (Denial of Service) saldırıları ile özellikle Amerikan şirketlerine saldırılar yaparak sistemi erişilemez duruma getirmişlerdir (Tasam, 2004:3). Literatürde siber terör yapanlara göre kategorize edilmiş ve şu şeklide sıralanmıştır:

- Devletler, düşmanlarından istihbarat toplamak, zayıflatmak ve kargaşa oluşturmak için,
- Politik örgütler, ekonomik ve sosyal yapıyı bozmak için,
- Kurum içi ve dışı düşmanlar, sanayi casusluğu ve kara propaganda yapmak için,
- Kriminaller, neler yapabildiğini görmek ve herkese göstermek için.

Her ne kadar ülkemizde büyük kapsamda bir siber terör eylemi ile karşılaşılmasa da dünya geneline bakıldığında ciddi siber saldırılar ile karşılaşmak mümkündür. Siber saldırılar oldukça yaygın olmakla birlikte bu saldırılardan büyük çoğunluğu siber terörizm olarak tanımlanmamıştır. Dikkate değer bir takım siber saldırılar şu şekildedir;

- Körfez Savaşı sırasında Hackerlar tarafından Pentagon'un bilişim sistemlerine sızılmış ve ABD'nin savaş ile ilgili bir takım dosyaları değiştirilmiş ve kopyalanmıştır (Kayaokay, 2014).
- ABD yetkililerinin açıklamalarına göre 1996 yılında CIA'in web sitelerine saldırı yapılmış ve internet siteleri üzerinde bulunan veriler değiştirilmiştir.
- 2009 yılında Fransız Savunma Bakanlığına yapılan bir saldırı sonucunda Villacoublay Hava Üssü bir müddet kullanılamaz duruma gelmiştir (Keçeci,2012:8).
- 2010 yılının haziran aylarında İran'ın nükleer programını hedef alan stuxnet virüsü geliştirilmiştir. Solucanı inceleyen araştırmacılar stuxnetin yapısı nedeni ile farklı uzmanlık düzeyindeki kişilerin üzerinde uzun bir dönem çalışarak yapabileceği konusunda ortak kanı bulunmaktadır (Avcı, 2014).

Tanımlardan anlaşılacağı gibi siber terör kavramı üzerine bir birleşme mevut değildir. Bu nedenle birçok saldırı siber saldırı olarak nitelendirilmekte olup siber terör olarak ifade edilmemektedir. Ayrıca Nato dergisine göre "Siber alandaki en tehlikeli oyuncular hala büyük devletlerdir. Organize suç örgütlerinin saldırı yetenekleri giderek artmaktadır ve bunlar gelecekte teröristler tarafından kullanılabilirler" (Nato Dergisi, 2014).

2.5.15. Bebek, Kadın ve Organ Ticareti

Klasik suç türlerinin bilgisayar ortamına taşınması ile ortaya çıkan suç türlerindendir. İlk etapta legal internet ortamları olan sosyal paylaşım siteleri, forum ve web sitesi üzerinden yapılan satışların büyük bölümü zaman içerisinde çokta bilinmeyen ve kolay takip edilemeyen derin internet (deep internet) olarak adlandırılan alana taşınarak faaliyetlerine devam etmektedirler. Alıcıların satıcılarını bulduğu gibi satıcıların alıcılarını da buldukları ortamlar mevcuttur. Örneğin bebek sahibi olamayan bir kadının bunu forum sitelerinde belirtmesi ve satıcının farklı bir kimlik ile bebek sahibi olamayan kişiyi bu yönde telkin ederek yönlendirmesi ve satıcı ile buluşturulması bu konuda verilebilecek örneklerdendir. Tulum (2006:45) bebek ticaretini gelişmemiş ülkelerde yaşayan aileler tarafından bebeklerin para karşılığında ya da suç örgütleri tarafından kaçırılan bebeklerin zengin ailelere satılması ile açığa çıkan suç olarak nitelendirmektedir.

UNICEF[8]'in açıklamasına göre her yıl 4 milyon kadın ve çocuk suç örgütlerinin hedefi olmaktadır (Yenisafak, 2003).

2.5.16. Uyuşturucu ve Kaçak Silah Ticareti

Uyuşturucu ticareti ve kaçak silah ticareti özellikle derin internette yaygın biçimde görülmektedir. Sadece ticareti değil, uyuşturucu yapımı, uyuşturucu hammadde yapımı ve tedarik edilmesi, uyuşturucu çeşitleri ve özellikleri internet üzerinden anlatılmakla birlikte tedarik etmek isteyenlere kargo ile satışı da yapılmaktadır. Silah satışı içinde durum aynıdır. İnternet üzerinden satışı, tamiri, silah yapımını anlatan web siteleri görülmekte özellikle terör guruplarının yararlanması üzerine yasaklanmalardan etkilenmemek için derin internette faaliyetlerini devam ettirmektedir.

Sağlık Bakanlığının verilerine göre ülkemizde sentetik uyuşturucu olan bonzai kullanımının 2010 yılında başlamasının ardından 22 web sitesinden satışının yapıldığı tespit edilmiştir (Haber Türk, 2014).

2.6. Bilişim Suçlarının Verdiği Ekonomik Zararlar

Bilişim sistemleri kullanılarak kişilere ait özel bilgiler çalınmakta ve derin (deep) internette alınıp satılmaktadır. Çalınan ve bu kapsamda satışa sunulan bilgilerin başında ise kredi kartı bilgileri, mail hesapları ve TC kimlik numaraları gelmektedir. Ünver ve Canbay (2010:5) 'a göre bilişim suçları ekonomisinde pay sahibi ülkeler arasında Türkiye'nin % 1'lik oranda olduğu ve dünya sıralamasında ise 7. olduğu izlenmektedir.

Stratejik ve Uluslararası Çalışmalar Merkezi'nin (CSIS) raporuna göre siber suçlarının iktisadi yansımasının 445 milyar ABD doları olduğu tahmin edilmektedir. Aynı rapora göre, ABD'nin 2013 yılında 3000 şirkete saldırıya uğradıklarına dair bildirim gönderildiğini, İngiltere'de ise perakendecilerin 850 milyon dolardan fazla para kaptırdığını ileri sürmüşlerdir. Avustralyalı yetkililer, havayolu şirketleri, otel zincirleri ve mali hizmet firmalarına yönelik büyük çaplı saldırıların 100 milyon dolar zarara yol açtığını açıklamışlardır (İHA, 2014).

[8] UNICEF, Birleşmiş Milletler Genel Kurulu tarafından çocuk haklarının korunması adına tanıtım ve farkındalık çalışmaları yapan bir kuruluştur.

STM Savunma Teknolojileri 2016 yılı ekim - aralık dönemi siber tehdit durum raporunda en ciddi saldırıların DDoS[9] saldırıları olduğu belirtilmektedir. Dünya genelinde ciddi DDoS saldırıları olmasına rağmen 2016 yılı ekim ayında ABD'de konuşlu Dyn DNS firmasına yapılan saldırı Türkiye'nin de içinde bulunduğu birçok ülkede farklı boyutlarda ulaşım sorunlarına sebep olması ve kullanılan yöntem nedeni ile en dikkat çekici saldırı olarak gösterilmektedir. Bu saldırının en dikkat çeken ve farklı yönü ise "Mirai" adlı IoT[10] olarak adlandırılan ve internet ortamındaki birçok cihazın siber saldırı içerisinde kullanılmasıdır. Ayrıca aynı raporda Avrupa genelinde fidye amaçlı siber saldırının en çok yaşandığı ülkenin Türkiye olduğu ve dünya geneline bakıldığında ABD ve Brezilya'dan hemen sonra üçüncü sırada yer aldığı belirtilmektedir. Çalışma Türkiye için tehlikenin üst düzeyde olduğunu göstermektedir.

2016 yılında özellikle bankacılık sektörüne de önemli saldırılar olmuştur. Şubat ayında Bangledeş bankalarına sızan saldırganlar, tüm dünyada uluslararası para transfer işlemleri için geliştirilmiş olan SWIFT (Society for Worldwide Interbank Financial Telecommunication) sistemini kullanılarak 951 milyon dolarlık hırsızlık gerçekleşmiştir. Ayrıca aralık ayında Rusya Merkez Bankasına yapılan aynı tür saldırı sonucunda ise 31 milyon dolarlık hırsızlık gerçekleşmiştir. Aralık ayında Türk bankalarına karşıda SWIFT saldırısı yapılmıştır. Sadece Akbank tarafından kendi sistemlerine yöneltilen saldırıların bertaraf edildiği, sistemlerin düzeltildiği, maddi kayıpların bankayı koruyan 4 milyon dolarlık sigorta fonundan karşılanarak müşterilerine herhangi olumsuz bir durum yansımayacağı açıklanmıştır. Diğer bankalardan ise herhangi bir bildiri yapılmamıştır.

Maalesef ülkemizde olan bilişim suçlarının ekonomik zararlarını gösteren istatistiki bilgiler oldukça sınırlıdır. Bunun başlıca nedenleri arasında firmaların prestij kaybı, psikolojik ve ekonomik nedenlerden dolayı kendilerine yapılan siber saldırıları açıklamamasından kaynaklanmaktadır. Dünya örneklerinde izlendiği gibi her türlü siber saldırının ekonomik bir karşılığı olduğu görülmektedir. Ayrıca siber saldırıya uğrayan firmalar bu saldırıya neden olan virüsleri sistemlerinden

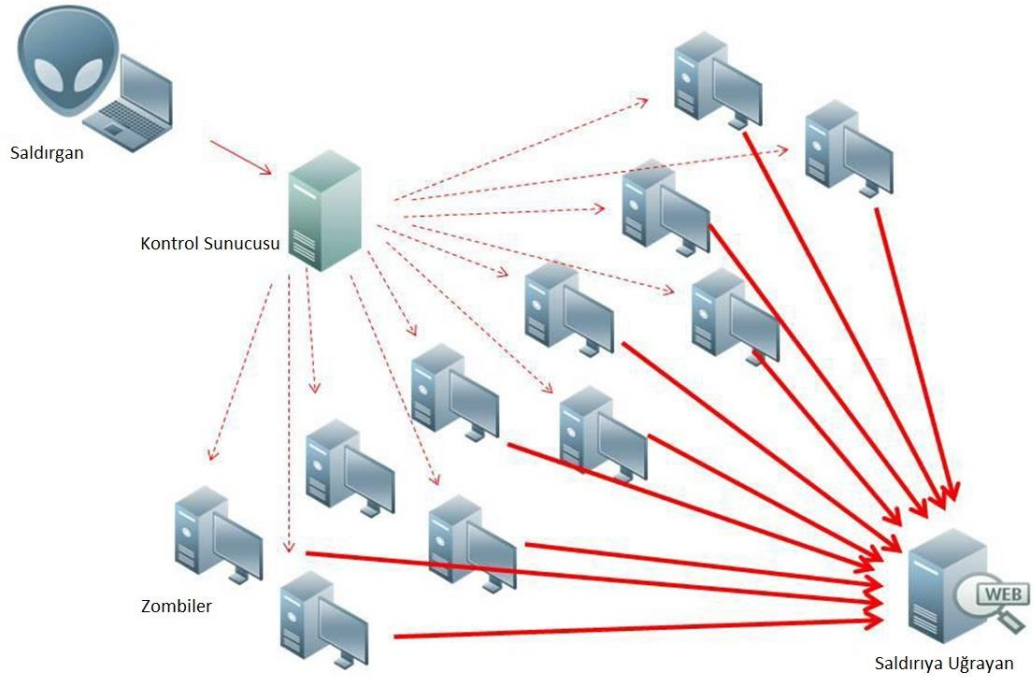
[9] Distributed Denial of Service olarak adlandırılmakta ve bu kelimelerin baş harfleri ile anılmaktadır. Türkçeye Dağıtık hizmet dışı bırakma saldırısı olarak çevrilmiştir.
[10] Internet of Things olarak isimlendirilmiş olup Türkçeye Nesnelerin İnterneti olarak çevrilmiştir.

temizlemek, sistem açıklarını kapatmak ve sistemleri tekrar eski haline getirmek için ek bir maliyete katlanmaktadır.

2.7. Bilişim Suçlarının İşlenmesinde Kullanılan En Yaygın Yöntemler

Bir hacker bilişim sistemleri üzerinden, başka bir bilgisayara, sunucuya, akıllı cihazlara veya mobil cihazlara saldırmak, onlardan bir veri almak, kullanıcı ismi ve şifresini ele geçirmek, başka açık kapılar bırakmak veya o cihazlar üzerinden başka sistemlere saldırmak için bazı yöntem ve teknikler kullanmaktadır. Öncelikle bir sistemin açığı bulunmakta ya da açık oluşturabilecek virüsler hazırlanılarak hedef bilgisayara mail, web siteleri, sosyal mühendislik gibi tekniklerle bulaşması sağlanmaktadır. Ardından açık üzerinden bu sistemler kontrol altına alınarak hedefler gerçekleştirilmektedir. Çoğu zaman sıradan bir bilgisayarı ele geçirmek çok fazla önem teşkil etmemektedir; çünkü içerisindeki bilgilerin genelde büyük bir önemi yoktur. Hackerlerin bir bilgisayara saldırı yapmaktaki amacı çoğu zaman veri kaçırmak değil o bilgisayar ile daha sonradan yapmayı planladıkları illegal faaliyetlerde aracı olarak kullanmaktır. Hackerlerin bu işler için hazırladıkları bilgisayarlar ve kullanıcılar "zombi bilgisayarlar" olarak adlandırılmaktadır. Kelime anlamı olarak zombi için yaşayan ölü diyebiliriz. Zombiler medyada bir ölünün doğa üstü bir güç sonucu uyanması ve kontrolsüz olarak etrafa zarar vermesi olarak tasvir edilmektedir. Bilgisayar içinde durum aynıdır. Bir bilgisayar bir hacker tarafından ele geçirildikten sonra kullanıcısının taleplerini yerine getirmekle beraber arka planda hackerın kontrolünde çalışmaktadır. Yani bilgisayar kullanıcısının kontrolünden çıkarak hackerin kontrolünde hareket etmektedir. Örnek bir saldırı ile Zombilerin kullanımı Şekil 2.2'de gösterilmiştir.

Şekil 2.2: DOS Atağı



Kaynak: Wikimedia, "Ddos Attack," https://commons.wikimedia.org/wiki/File:Ddos-attack-ex.png, (Erişim Tarihi: 07.11.2017).

Şekil 2.2'den de anlaşılacağı üzere hedefin saldırgan olarak gördükleri sadece zombilerdir. Saldırgan bu şekilde kimliğini korumakta ve aynı zamanda saldırısını daha güçlü kılmaktadır.

Saldırganlar zombi oluşturmak için hiç kuşkusuz tek tek uğraşmazlar. Bunun için virüsler, turuva atları ve spam mailler gibi farklı yöntemler kullanarak zombi grupları oluşturulmaktadır.

Gerek zombiler aracılığı ile gerekse direk hedef odaklı bilişim suçları için en çok kullanılan bazı teknik ve yöntemler şu şekildedir:

2.7.1. Bilgisayar Virüsleri (Computer Viruses)

Virüs, bilgisayara gizlice giren, bilgisayardaki verileri bozabilen, değiştirebilen, kaçırabilen terim olarak biyolojik muadilinden türetilen ve onunla aynı mantıkta kullanılabilen yazılım ve kod parçacıklarıdır. Microsoft bilgisayar virüslerini, bilgisayardan başka sistemlere amacı dışında çalışmak üzere bulaşan yazılımlar olarak tanımlamaktadır" (Microsoft, 2014).

Bilgisayar virüsleri farklı yöntem ve tekniklerle yazılmakta ve birçok çeşitten oluşmaktadır. Bilgisayar virüsleri genelde malware[11] olarak isimlendirilen bir çok kötü amaçlı yazılımı anlatmak için kullanılmaktadır. Virüsler kendi kendini çalıştırma ve kendini kopyalama gibi görevleri yapmak durumundadır (Wikipedia, 2016b). Bulaştığı zaman itibari ile bilinen en zararlı virüsler şu şekildedir;

- CIH (1998) : Çernobil virüsü olarak nam salmıştır. Ekonomik olarak 80 milyon dolar zarara uğrattığı tahmin edilmektedir. Odabaşı ve Uysal (2006:3)'na göre CIH (Chernobyl) virüsü Türkiye'de hava limanlarının yanı sıra radyo-televizyon istasyonları ve kritik kurumlardan olan banka sunucularındaki bilgilerin silinmesine neden olmuştur. Ayrıca Güney Kore'de yaklaşık 300,000, Hindistan'da 30,000, Çin'de 360,000, Norveç'te ise 2000'den fazla bilgisayar virüsten etkilenmiştir.
- Melissa (1999) : Microsoft Word dokümanlarını veya e-posta eklentilerini kullanarak yayılan virüs dünya üzerinde birçok ülkede kendini göstermiştir. Dönemin en tehlikeli virüslerindendir. Atalıç Taş (2010:3)'a göre 80 milyon dolar hasara yol açıldığı sanılmakta olup virüsün yazarı iki yıl hapse mahkûm edilmiştir.
- I Love You (2000): En tehlikeli virüslerden biri olarak anılmaktadır. Bir bilgisayara bulaştığında o kişinin mail adresinde bulunan tüm kişilere mail göndererek yayılmaktadır. Virüs bulaştığı bilgisayarlardaki önemli bilgileri silmesi ve bilgisayar şifrelerini göndermesi nedeni ile 8.7 milyar dolarlık maddi zarar yaşanmıştır (Süer, 2011).
- Code Red (2001): Sunuculara saldırmayı hedefleyen virüs bulaştığı bilgisayarlara arka kapılar açmaktadır. Etkili olduğu süre boyunca verdiği zararın günlük 200 milyon $ olduğu tahmin edilmektedir (Sabah, 2011).
- Slammer (2003): 2003 yılına kadar bilinen zararlı virüsler içerisinde en hızlı yayılan virüs olarak bilinmektedir. Kendisini rastgele IP'ler üzerinden bilgisayarlara yollayarak bulaşmaktadır. Virüs dünya çapında 75 bin bilgisayara yayılarak 750 milyon dolarlık zarara neden olduğu tahmin edilmektedir (CHIP, 2008).

[11] Kötü amaçlı olarak hazırlanmış yazılımlardır.

- MyDoom (2004): Microsoft tarafından piyasaya sürülen yazılımların açıklarını hedef alan virüs Outlook listesinde yer alan adreslere kendini göndererek çoğalmaktadır (BBC, 2004). MyDoom'un yarattığı maddi zarar 38 milyar dolar olarak tahmin edilmektedir (Star Teknoloji, 2013).
- SOBİG.F (2003): Bilgisayarları kullanılmayacak derecede yavaşlatan virüs, aynı zamanda dünya çapındaki e-posta sunucularına aşırı derecede yükleyerek tüm dünyadaki mail trafiğini durduracak dereceye getirmiştir. Dünya çapında 500 milyondan fazla bilgisayara bulaşan virüsün 35 milyar dolarlık zarara neden olduğu tahmin edilmektedir (Star Teknoloji, 2013).
- Samy XSS (2005): Active X yapısını kullanan solucan myspace üzerinde çalışmakta olup ilk 20 saat içinde 1 milyon profilden daha fazlasına bulaşmıştır.
- Nyxem (2006) Mail yoluyla yayılan "Mac OS X" isimli malware yazılımı, "OSX/Leap-A" veya "OSX/Oompa" adıyla bilinen trojan olarak çıkmıştır (Atalıç Taş, 2010). Virüsün özellikle ev kullanıcılarını hedef aldığı ve Office yazılımları ve sıkıştırılmış yazılımlar gibi dosyaları sildiği görülmektedir.
- Torpig (2008): Diğer ismi Sinowal'dir. Windows programlarını etkileyen, anti-virüs programlarını kapatan ve kullanıcıların özel verilerini çalan bir Truva atı olarak ortaya çıkmıştır. Carnegie Mellon University göre Turuva atı kişisel, kurumsal ve finansal bilgiler gibi bilgileri çalarak kimlik hırsızlığı yapmaktadır.
- Conficker (2009): 200 ülkeye yayılmış ve on milyonlarca bilgisayar ve sunucuya bulaşmış tüm zamanların en tehlikeli virüsüdür. Microsoft virüsün internet, USB sürücüler ve diğer çıkartılabilir aygıtlar ile bulaştığını ve ayrıca çalışma şeklini de değiştirdiğini belirtmektedir.

2.7.2. Truva Atı (Trojan Horses)

"Truva Atı" trojeni ismini tarihteki truva atından almıştır. Trojan zararsız görünmesine rağmen içinde zararlı programları barındıran bir yazılımdır (Atalıç Taş, 2010:11). Truva atları, kullanıcıların doğru bir kaynaktan geldiğini düşündükleri bir programı açmalarıyla yayılmaktadır.

Yüklenen bir yazılıma gizlenmiş olan trojen bilgisayarlar ve ortamda çalışan sunucular hakkında veri toplar ve bu verileri trojeni hazırlayanın bildirdiği IP

adresine transfer eder. Saldırgan turuva atı sayesinde almış olduğu veriler ile sisteme giriş yaparak hedefindeki eylemleri gerçekleştirir.

2.7.3. Solucanlar

Bilgisayar solucanı, bilgisayara gizlice bulaşan ve çoğunlukla kullanıcıların fark edemediği ağ bağlantıları nedeni ile kendi kendine çoğalabilen kötü amaçlı yazılımlardır. Solucan yazılımlar kendi kendine çoğalabildiği için hızla yayılabilir (Kaspersky, 2014). Solucanlar bağımsız bir programdır (Haeni, 1997:10). Solucanların en büyük tehlikesi, kendilerini çok sayıda çoğaltmasıdır. Örneğin bir solucan, e-posta adres listenizdeki herkese kendisinin bir kopyasını iletebilir ve sonra onların mail listesindende atakta bulunabilir. Solucanlar çoğalırken kullanıcıların network altyapısını kullandıklarından dolayı ağların kilitlenmesine sebep olabilmektedirler (İTÜ BİDB, 2013).

Bilinen çoğu solucan, sistem açıkları ile, e-posta eki olarak gönderilen dosyalarla, P2P dosya paylaşımı ve diğer web veya FTP bağlantısı ile yayılırlar. Solucanlar genellikle bilgisayar belleğinde çalışırlar.

Solucanlar Truva Atı gibi bir programın çalışmasını beklemezler. Otomatik olarak bulaştığı sistemlerde çalışırlar. Solucanları Truva Atından ayıran diğer bir özellikse zarar vermemesidir. Solucanların yapılış amacı bir bilgisayarın kullanıcısının kullanıcı ismini, kullanıcının şifresini, kullanıcının çalıştırdığı yazılımları, aktif çalışmalarını, anlık mesajlaşma programları ile neler yazıştığını almak ve bu bilgileri solucanı yazan yazılımcıya iletmektir. İnternet üzerinden e-posta ile gelen solucan örnekleri şu şekildedir:

- Tebrikler 5000 sms veya kontör kazandınız yüklemek isterseniz ilgili linki takip ediniz.
- Tebrikler Amerika'ya gitme şansı yakaladınız. Ayrıntılar için lütfen linki takip ediniz.
- Kredi kartınızla kullanmak için bonus kazandınız. Hemen kartınıza yüklemek için lütfen tıklayınız.
- Sitemize giren 1.000.000. kişisiniz. 1000$ tutarında hediye puanınızı almak için linki takip ediniz.
- Tebrikler şanslı gününüzdesiniz. Ödülünüzü görmek için lütfen tıklayınız.

- Bir adet kol saati kazandınız (Muğla Emniyet Müdürlüğü, 2013).

2.7.4. İstem Dışı E-Posta (Spam)

İstenmeyen ve çoğunlukla engellenmek istenen e-posta olarak tanımlanmasının yanında genellikle tanıtım, pazarlama, reklam ve satış yapmak isteyen firmalar tarafından çok sayıda kişiye gönderilmektedir (Uydacı, 2004:80). Türkçe 'de "yığın ileti" olarak da ifade edilmektedir. Atabek (2006:3)'e göre spam mail, ticari bir faaliyet olmasına rağmen yanlış kabul edilen bir davranıştır. Ticari faaliyet olarak kullanılan spam mailler kullanıcının onayı olmadan, kullanıcı tarafından talep edilmeden izni dışında e-posta göndermeyi kapsamaktadır.

Spam mailin en çok kullanılan şekli UCE'dir[12] Önemsiz mail olarak tabir edilen ve istek dışında genellikle ticari amaçlı gelen maillerdir (İkizler ve Başar, 2006:92).

Yaygın kullanılan bir diğer spam türü ise UBE'dir.[13] Kitlesel mesajlar için kullanılır. Çoğunlukla belirli bir konudaki bir fikrin duyurulmasını amaçlayan mesajlar olarak karşılaşılmaktadır.

Bir diğer yaygın yöntem ise MMF'dir.[14] Kolay yoldan ekonomik kazanç elde edilmesine yönelik ve piramitsel yaklaşımlar ile karşılaştığımız e-posta türleridir (Chip, 2009). MMF e-postalar zincir oluşturmak için aktif kullanılan ve bir zamanların en etkili e-posta türleridir.

Tüm kurumlar spam maillere karşı önlem almaya çalışsa da bu önlemler çoğu zaman %100 başarı sağlamamaktadır.

2.7.5. Sistem Güvenliğinin Kırılması ve Siber Güvenlik

Sistem güvenliğinin kırılması, Hacker olarak adlandırılan bilgisayar korsanlarının gerçekleştirdiği saldırılar sonucu sisteme erişim sağlanması olarak ifade edilmektedir. Sistem güvenliği herkes için önemli olup tüm kullanıcıların

[12] UCE Unsolicited Commercial E-mail isimlendirmesinin baş harflerinden oluşmaktadır. önemsiz maillerdir
[13] Unsolicited Bulk E-mail isimlendirmesinin baş harflerinden oluşmaktadır.
[14] Make Money Fast isimlendirmesinin baş harflerinden oluşmaktadır.

önem göstermesi gereken bir çalışmadır. Bir kurumda sistem güvenliğini sağlamak için bilgi işlem personellerinin yanı sıra aynı kurumda çalışan güvenlik personelinden, hizmetlisine, yönetim kadrosundaki personelden, siber güvenlik personeline kadar tüm çalışanlara farklı görevler düşmektedir. Siber saldırı altındaki bir sistemin güvenliği en zayıf olduğu yerden kırılır. Bu nedenledir ki siber güvenlik, tüm disiplinleri bir araya getiren geniş ve komplike bir olgudur.

2.7.6. Kullanıcı Tabanlı Siber Güvenlik Zafiyetleri

Siber Güvenlik zafiyetinin kullanıcı kaynaklı olması durumudur. Kullanıcı kaynaklı hatalar siber zafiyetin oluşturulmasında en büyük etkendir. Bir saldırgan kurum sistemine her zaman sistem açıklarını aşarak girmez. Çoğu zaman en zayıf nokta kullanıcı olduğundan dolayı saldırgan, kullanıcı hataları sonucu oluşan zafiyet noktalarından sistemlere girmektedir. Kullanıcı, dalgınlık, ihmal, hata ya da bilinç eksikliği gibi nedenler ile kullandığı bilgisayarda zafiyete sebep olabilmektedir. Aynı zafiyetler kritik altyapılar ile ilgilenen sistem uzmanları içinde geçerlidir. Kullanılan sistemlerde güvenlik protokolü oluşturulmaması ve zayıf şifre kullanılması, kritik açıklara yönelik güncelleştirilmelerin yapılmaması, ilgisiz portların gereksiz yere açık bırakılması ve uzak erişim için yetersiz güvenlik önlemleri sistemler için açıklar oluşturmaktadır.

2.7.7. Omuz Sörfü

Omuz sörfü, bir kullanıcının bilgisayarına ya da yetkili olduğu programlara girerken kullanmış olduğu şifrenin başkası tarafından görülmesidir. Lashkarı vd., (2009:145)'a göre meraklı kişilerin anlattıklarınızı dinlemesi şifrelerin yanı sıra kişisel diğer bilgileri alarak şifreleri tahmin etmesi de omuz sörfü olarak nitelendirilmektedir.

2.7.8. Yazılım Açıkları

Siber güvenliğin sağlanmasında hiç şüphesiz yazılım açıkları önemli yer tutmaktadır. Bilgisayar üzerinde kullanılan herhangi bir program açığı tüm sistemi tehlikeye düşürmek için yeterlidir. Bir saldırgan bir bilgisayara girmek istediğinde o bilgisayar için veri toplar. Kullanılan işletim sistemi, üzerinde çalışan office yazılımları, sıkıştırma programları, kullanılan diğer program sürümleri hackerlar

için önemli veri kaynaklarıdır. Kullanılan programın bir açığı var ise ve bu 0. Gün (Zero Day) olarak tabir edilen hiç kimsenin bilmediği bir açık değil ise bir çok kişi ve hacker tarafından bilinmekte ve istismar edilmektedir.

Bir açık bilgisayarda olabileceği gibi, bir dosya sunucusunda, web sunucusunda, domain sunucusunda, mail sunucusunda, güvenlik duvarında ya da VPN sunucularında da olabilir. Örneğin hedef olarak bir web sunucusunu ele alalım. Sunucuya bağlantı gerçekleştirdiğimizde versiyon bilgisi olarak bize 2.1.8 bilgisini dönsün. Sunucun son versiyonun 4.1.5 olduğunu bilen güvenlik tarama araçları aradaki güncelleştirmelerin yapılmadığını anlar ve bu açıkların neler olduğunu raporlar. Dolayısı ile hacker hangi açık üzerinden sisteme giriş yapacağını öğrenmiş olur. Bu nedenle tüm cihazların güncelleştirme kontrolleri yapılmasının ardından bu cihazlar üzerinde çalışan programlarında güncelleştirilmesinin yapılması ve bilinen açıkların araştırılarak güvenlik önlemleri alınması yazılım açıklarının kapatılmasında önem teşkil etmektedir.

Yazılım zafiyetleri sadece açıklar ile ilgili olmayabilir. İhlaller sonucu da oluşmaktadır. Yazılımın legal giriş ekranı olan kullanıcı ismi ve şifrenin yazıldığı ekranda brute force attack (kaba kuvvet atakları) yapılması, ya da kullanıcının özelliklerine göre saldırgan tarafından şifre testlerinin yapılması da güvenlik ihlali olarak nitelendirilebilir.

2.7.9. Donanımsal ve Yazılımsal Key Logger Kullanımı

Key loggerlar klavyeden yapılan tüm işlemlerin kayıtlarını tutan casus yazılımlardır. Key logger girilen kullanıcı isimlerini, şifreleri, adresleri ve diğer bilgilerinizi bir metin dosyasına kaydedip e-posta, ftp ya da uzak bağlantı ile saldırgana ulaştırırlar. Bir klavyenin ya da USB belleklerin içine gizlenebileceği gibi yazılımsal da olabilir. Donanımsal key logger bir klavyeye saklanmış ise genellikle anti virüs programlarına yakalanmazlar. Kullanılmaya başlandığı anda saldırgana bağlantı kurarak yazılan komutların takibini yapmaktadırlar.

Key logger her ne kadar saldırganlara bilgi kaçırmak için kullanılsa da geçmiş yıllarda şirket yöneticileri personelini izlemek için de kullanmaktaydılar. Günümüzde kullanılmaya devam etse de şu an birçok şirket bunun için farklı servisler kullanmaktadır.

2.7.10. Kaba Kuvvet Kullanımı – Sözlük Atakları (Brute Force ve Dictionary Attacks)

Sözlük saldırıları bir sistemi veya belgeyi korumak için kullanılan şifrenin, bütün harf, rakam ve özel karakter kombinasyonlarını kullanarak kırmaya çalışan saldırı yöntemidir (İlbaş, 2009:29). Deneme yanılma yöntemi olarak da ifade edilmektedir. Çok kullanılan şifreler, doğum tarihleri, standart şifreler, kişi, hayvan isimleri bu sözlüklerde bulunur ve sözlükteki sözcük ile eşleşen bir şifre kullanıldığında şifre kırılmış olur ve sisteme veya belgeye girilmiş olur. Brute force ataklarında sözlük kullanımına "Dictionary Attack" (Sözlük atağı) denir. Brute force kullanarak atak yapan birçok yazılım artık sözlük ataklarını da kullanmaktadır. Sözlükler underground (yeraltı) sitelerde cihaza göre, ülkeye göre, web sitelerine göre ve boyutlarına göre ayrıştırılarak satışları yapılmaktadır.

2.7.11. Ekran Kaydedici Yazılımlar (Screenlogger)

Kullanıcın her mouse (fare) hareketinin resmini çekip küçük boyutlar halinde saldırgana ulaştıran yazılımlardır. Kullanım şekli Keyloggerlar ile aynıdır. Genel itibari ile bankacılık sektöründe kullanılan şifreler ile ekran şifresi isteyen web sitelerindeki programlarda girilen şifreleri çalmayı hedeflemiştir. Saldırganın amacı tüm ekran görüntüsü olmayıp şifre girişi için yapılan Mouse hareketleridir.

2.7.12. Çöpe Dalma (Scavenging)

Scavenging, bir çalışmanın sonucunda elde kalan artıkların toplanması, depolanması ve verilerin çeşitli şekillerde analiz edilerek kullanılmasını ifade etmektedir. Örneğin çöpe atılan kâğıtlar, post-it, yazıcı şeritleri, yedekleme kartuşları, CD, disket, depolama üniteleri ve geçici kullanılan hard disklerin analiz edilmek için toplanıp depolanmasını ifade eder (Uzunay, 2005:14).

Bu verilere ilaveten bozulduğu düşünülen, veya kullanımdan çıkartılmış diskler üzerindeki silinmiş verilerde çeşitli programlar yardımı ile toplanarak analiz edilir ve çalışmalara ait verilere dahil edilerek sisteme erişim için kullanılır.

2.7.13. Oltalama (Phishing)

Password Harvesting Fishing kelimelerinin kısaltmasından oluşan phishing yöntemi oltacılık ve yemleme olarak da adlandırılmaktadır. Özellikle e-posta ya

da sahte web siteleri olarak karşımıza çıkar. Kullanıcılara gelen e-postalar bilinir bir kaynaktan geliyormuş gibi görülmekle birlikte acil bir mesaj, avantajlı veya cazip bir fırsat, dikkatinizi çekecek düzeyde yüksek fatura borcu, uygun kredi bilgileri içerir. Gelen e-postanın linkini takip ettiğinizde kullanıcı adı/parolanızı ele geçirmeye çalışan kötü niyetli bir web sitesine yönlendirilmektedir (Sans, 2013). Saldırganın hedefi çok sayıda kullanıcı bilgilerini kısa sürede ele geçirmek olduğu için en güzel yöntem e-posta ile birlikte kullanmaktır. Bu yöntem kullanılarak kullanıcılar her yıl milyarlarca dolar maddi zarara uğratılmaktadır.

Saldırganların kullanmış olduğu bir diğer yöntem ise hedefe yönelik oltalama saldırısıdır. Bu saldırı türünü klasik yemleme saldırısından ayıran en bariz özellik bir hedefe yönelik olmasıdır. Bu hedef kimi zaman bir organizasyon, kimi zaman bir şirketin çalışanları, kimi zaman bir kamu kurumunun personelleri olabilir. Saldırgan hedef odaklı yemleme yapmadan önce hedef kullanıcının sosyal medya hesaplarını takip eder, kullanıcılar hakkında bilgi edinir ve kullanıcıları daha net etkileyebilecek e-posta iletileri göndererek başarı şansını artırmaktadır. Sans (2013)'e göre bu tip saldırılar kullanıcıların banka bilgilerini çalmaktan öte şirketler için ticari sır niteliği taşıyan, verileri çalmak için kullanılmaktadır. Hedef odaklı saldırılar için özel tasarım yapıldığı ve saldırı sürdürülebilir olduğu için tehlike düzeyi daha yüksektir.

2.7.14. Yerine Geçme (Masquerading)

Bir ağda kullanıcıların yetkileri farklı farklı olmaktadır. Bir birimin ilgili klasöre erişebildiği bir ağda diğer birim aynı klasöre genelde erişemez ya da izinli erişim sağlayabilmektedir.

Bir sunucuya, bilgisayara ya da dosyaya erişimi olan kullanıcının hesap bilgilerinin bir başkası tarafından giriş yapılması sonucu oluşacak açığa denilmektedir. Yerine geçerken kullanıcı fiziki olarak orada olmak zorunda değildir. Hak ve yetkilerinin kullanılması sonucu oluşmaktadır.

Yerine geçme sosyal medyada da yapılabilmektedir. Bir kişinin kullanıcı ismi ve şifresinin başka bir kişi tarafından kullanılması veya bir kullanıcı kendi oturumunu açtıktan sonra oturumunun (çerezlerin alınması ile (cookie)) kopyalanarak farklı bir bilgisayarda çalıştırılması da bu kapsamda

değerlendirilebilir. Benzer olay ATM kullanıcılarını da kapsamaktadır. Kullanıcı ATM'den para çekmesinin ardından dikkatsizlik sonucu ATM'deki oturumunu kapatmadan ve bankamatik kartını almadan uzaklaşması ve başka bir kişi tarafından aynı oturumun kullanılması o kişinin yerine geçerek işlem yapılması olarak adlandırılır. Bu tip durumlarda kullanılan cihazlar kullanıcının değiştiğini anlamaz ve işlem yapmaya devam ederler.

2.7.15. Port Tarama Teknikleri

Günümüzde işletim sistemleri farklı programın eş zamanda işlem yapmasına olanak sağlamaktadır. Sunucular veya bilgisayarlar kullanıcıdan gelen istekleri almakta ve uygun olarak gördüklerini cevaplamaktadır. Aktif bir sisteme IP üzerinden ulaşılmasının ardından çalışan programlara ulaşım port'lar sayesinde sağlanır (Atakan, 2001).

Port tarama hedef sistemin, belirtilen portlarına bağlantı kurmaya çalışarak gelen cevaplara göre açık, kapalı ya da engellenmiş olup olmadıklarını öğrenme yöntemidir. Port tarama tek başına kullanıldığında bir keşif çalışmasıdır. Taratılan sisteme göre Port tarama sonucunda zafiyet görülen portlar farklı saldırı tipleri ile birleştirildiğinde sisteme erişim için tehlikeli olmaktadır (Cyber-Warrior, 2015).

2.7.16. Arka Kapılar (Backdoors)

Sistem üzerindeki sıradan incelemelerle görülmeyen, uzaktan bağlanacak saldırgana kimlik kontrollerini atlatarak bağlantı yapmasını sağlayan yöntemlerdir. Bir sisteme sızmak için birçok farklı yöntem kullanıp akabinde sisteme erişen saldırganlar, daha sonraki erişimlerinin zahmetsiz olması için kendilerinin bilecekleri farklı açık kapılar oluştururlar. Bu yöntem ile sonraki bağlantılar daha kısa sürede ya da her bilgisayar açıldığında otomatik olarak sağlanır (Haeni, 1997:11).

Arka kapı oluşturmak için her zaman bir bilgisayara saldırmak gerekmez. Saldırganların hazırlamış olduğu genelde ücretsiz olan programların kullanıcılar tarafından bilgisayara yüklenmesi sonucu da bu zafiyet oluşabilir. Bazı sistem yöneticilerinin sisteme test yapmak, güncelleştirme yapmak, hata kontrolü yapmak gibi nedenler ile oluşturdukları arka kapıları unutması sonucu da benzer zafiyetler açığa çıkabilmektedir.

Arka kapılar için bilişim forumlarında oldukça güçlü iddialar da bulunmaktadır. Özellikle yazılım ve donanım üreticileri kendi ülkelerinin istihbarat servislerinin erişimine açık olması için bu tip arka kapılar bıraktığı söylemi oldukça yaygındır (BGA, 2014). Özellikle milli yazılımın öneminin arttığı günümüz dünyasında arka kapılar üzerinden bilgisayarlara izinsiz veri yüklenmesi ve veri kaçırılması engellenmeli ve bu konuda ulusal tedbirlerin alınması için çalışmalar yapılması milli menfaatlerimizin korunması için büyük önem arz etmektedir.

2.7.17. Dos/Ddos Atakları (Servis Engelleme)

Servis yıkımı (Denial of Service, DoS) saldırılarının temel prensibi, sisteme zarar vermekten ziyade, sunucuya ulaşımı sınırlayarak sistemin sağlıklı çalışmasını engellemektir. Sistemleri çalışmaz hale getiren saldırı tiplerine DOS saldırısı, DOS saldırısının çoklu kaynaklardan yapılmasına da DDOS (Distrubuted Denial of Service) saldırısı denilmektedir (Önal, 2012:7). DOS saldırısını hizmeti gerçekten kullanmak isteyen kullanıcıların kullanılmasını engellemek için yapılan atak olarak ifade etmektedir. Bu saldırılar genellikle, ağın bant genişliği, güvenlik cihazları ve sunucuların tampon bellekleri, CPU gücü, hafıza, TCP/IP protokolü gibi hassas kısımlarını hedef alarak, sistemin normal servis sağlamaya elverişsiz duruma gelmesine sebep olmaktadır.

DOS saldırıları internetin en belirgin sorunlarındandır. 1996 yılından beri, internet ortamındaki birçok site, bu saldırı tipleri ile saldırılara uğramış ve akabinde saldırıların engellenmesi yönünde çeşitli yöntemler denenmiştir. DDOS saldırıları ise DOS saldırılarından daha tehlikeli olmaktadır. Kaydı tutulmuş en büyük DDOS saldırısı 1999 yılında olmuştur (Tandoğan, 2007:3). Her ne kadar farklı çözüm önerileri geliştirilse de yaygın kullanıma uygun kesin ve net bir çözüm henüz üretilememiştir. Bilinçli bir sistem yöneticisi ile iyi tasarlanmış bir sistem oluşturulması ve bu konuda kaynak ayrılması bu saldırıların etkisini azaltabilmektedir.

2.7.18. Web Uygulamalarındaki Güvenlik Zafiyetleri

Web uygulaması, kullanıcı ile etkileşime giren veya veri tabanına dayalı web tabanlı yazılımlardır (Yılmaz, 2009:1). Bir çalışmanın web sitesi veya uygulaması olabilmesi için;

- Domain: Uygulamaya erişilebilmek için gerekli olan alan adı,
- Sunucu: web çalışmasının yayın yapabileceği bir sunucu,
- Web sitesi/web uygulaması: çalışması planlanan web sitesi veya uygulamasının yazılımı,
- Kullanıcılar olması gerekir.

Hackerler, web uygulamalarındaki ve yazılımlarındaki güvenlik zafiyetlerinden faydalanıp yetkisiz olarak bilişim sistemlerine erişme (sızma), kullanıcılarının yetkilerini içeren giriş bilgilerini çalma, web sunucularını ve akabinde sistemleri ele geçirme gibi faaliyetlerde bulunmaktadırlar. Ülkemizde de sık sık görülen web sitelerini ele geçirme saldırıları kurumlar açısından prestij kaybına neden olmaktadır. Yılmaz (2009:2)'ında ifade ettiği gibi yapılan saldırılar, domain adı üzerinden, server üzerinden, uygulama veya yazılım üzerinden, kullanıcılar üzerinden olabilmektedir.

2.8. Bilişim/Siber Suçları ile Mücadele

Siber/Bilişim suçları ile mücadele, çok yönlü ve kapsamlı bir çalışmadır. Birçok ülke siber saldırılara karşı bilinçlendirme çalışmaları yaparken beraberinde kritik altyapıların belirlenmesi ve savunma stratejilerinin üretilmesine odaklanmaktadır.

Siber suçlardan korunmak için birtakım çalışmalar yapmak standartlar oluşturmak ya da bu konuda oluşturulan standartları uygulamak oldukça önemlidir. Siber saldırılardan sadece, kurumlar değil bireylerde etkilenmektedir. Bireylerin güvenliği aynı zamanda kurumların güvenliğine de destek sağlayacaktır. Bu konuda çalışmalara başlamadan önce mevcut durumun belirlenmesi ve siber saldırıların fark edilmesi önem arz etmektedir.

2.8.1. Siber Saldırıların Fark Edilmesi

Bir sisteme izinsiz olarak giriş yapmaya saldırı (sızma), saldırıyı yapan kişiye ise saldırgan denilir. Saldırıların fark edilmesi için öncelikle nelerin saldırı

olduğunun tanımlanması gerekmektedir (Sancak, 2008:4). McEachen ve Zachary (2007:84-85) ye göre saldırganlar 3'e ayrılır.

Gerçeği Gizleyen (The Masquerader): Sisteme giriş için yetkisi olmasa da yetkili bir kullanıcı bilgileri ile sisteme sızan saldırgana denir,

Gizli Kullanıcı (The Clandestine User): Bir sisteme sızmış ve yönetici haklarını ele geçirmiş saldırgana denir. Gizli kullanıcı tespit edilmesi en zor olan saldırgan tipidir. Saldırgan yönetici şifrelerini ele geçirmiş olduğundan tüm sistem içerisinde rahatça dolaşabilir.

Yasal Kullanıcı (The Legitimate User) : Sisteme giriş imkânlarına sahip gerçek bir kullanıcının saldırı yapmak için yetkisini kötüye kullanmasıdır.

Siber saldırıların çözümü çoğu zaman zor bir süreçtir. Ayrıca tüm siber saldırılarda gerçek saldırganların bulunabilmesi kolay olmayabilir. Saldırıları tespit etmek için farklı yaklaşımlar bulunmakta olup bu yaklaşımlar çerçevesinde farklı saldırı tespit sistemleri ve çözüm önerileri geliştirilmiştir.

Siber saldırılar olmadan önce önleme çalışmaları yapmak, siber saldırı esnasında fark ederek tedbir almak saldırının zararını azaltmada etkin rol oynamaktadır. Saldırıyı fark etmek saldırganın vereceği zararı asgari seviyeye indirecektir.

2.8.2. Önleyici Tedbirler

Önleyici tedbirler bireyden bireye, kurumdan kuruma, sistemden sisteme değişiklik göstermektedir. Önleyici tedbirler saldırı aşamalarına göre farklılık göstermekte birlikte sistemin mevcut durumuna göre de maliyeti değişmektedir. Saldırı aşamaları tipik olarak şu şekildedir;

Bilgi Toplama: Saldırganın saldırı yapmak istediği kurum ve kuruluş hakkında bilgi toplamasıdır. Amaç saldırganın saldırı yapmak istediği sistemi tanıması ve zafiyet olan kısımların belirlenmesidir. Bu aşamada öğrenilen her tür bilgi değerlidir.

Hazırlık Aşaması: Başarılı bir saldırı için gerekli olan yazılımsal ve donanımsal araçların hazırlanması sürecidir. Saldırgan nerden sızması gerektiğini nerelerde arka kapı oluşturması gerektiğini bilir ve ona göre araçlarını hazırlar.

Hedefe Varış: Saldırganın hazırlamış olduğu saldırı sistemlerini hedefe ulaştırılması aşamasıdır.

İstismar: Saldırı başlamıştır. Bu süreçte hazırlanan yazılımlar ve donanımlar hedefte çalıştırılmış ve ihtiyaç olabilecek arka kapılar açılarak uzaktan erişim sağlayacak sistemler aktif hale getirilmiştir.

Test Aşaması: Uzaktan erişim sağlanarak eylemler için tüm sistemlerin çalıştığının kontrolü sağlanır. Bağlantı sorunlarının olmaması ve kopmalardan sonra tekrar bağlantının aktif olması için arka kapılar kontrol edilir. Ek bir çalışma gerekiyorsa uzaktan yapılabilecek tüm uygulamalar aktif hale getirilir.

Saldırı: Asıl amacı gerçekleştirme sürecidir. Bu süreçte bilgi sızdırma, sisteme zarar verme, başka kurumlara istismar edilen bu sistemler üzerinden ulaşma, sistem içerisine sahte veri konumlandırma gibi saldırılar yapılmaktadır.

Yukarıdaki saldırı aşamalarının bir noktasından kırarak saldırının başarıya ulaşmasının engellenmesi için sistemin durumu hakkında bilgi sahibi olunması ve sistemin izlenmesi gerekir. Saldırı adımlarının her aşamasında çözüm yöntemleri ve maliyetler değişiklik göstermekte olup etkileri de aynı oranda değişmektedir. İlk aşamalardaki çözümler hem savunmayı kolaylaştırmakta hem de daha fazla kaynak ayrılmasını engellediği için maliyetleri azaltmaktadır.

Önleyici tedbirler saldırı aşamalarının birden fazla noktada etkisiz hale getirilmesi ile oluşur. Bu aşamalar bir zincir olarak kabul edilirse zinciri farklı noktalardan kıracak önleyici tedbirleri almak savunma mekanizmasını artıracağı gibi saldırının zararını da minimuma indirir.

2.8.3. Kritik Altyapıların Belirlenmesi

Literatürde kritik altyapılar konusunda ortak bir tanım bulunmazken, devre dışı kalmaları halinde can ve mal kaybına, halkın huzurunun bozulmasına veya ulusal güvenliğin sekteye uğramasına neden olan sistemler kritik alt yapı olarak

kabul edilmektedir. Ünver ve Canbay (2010:2) ABD ve Avustralya için yapılan kritik alt yapı tanımlamasında ulusal güvenliğin sağlanmasına vurgu yapması nedeni ile AB ve Japonya için yapılan insan merkezli tanımına göre bir takım farklılıklar olduğunu ileri sürmektedir.

Kritik alt yapıların belirlenmesi önleyici tedbirlerin alınması ve olası bir saldırı esnasında oluşabilecek etkilerinin azaltılması konusunda tedbirli davranılmasını sağlayacaktır. Bu neden ile ABD kritik altyapıların korunması "Ulusal Altyapı Koruma Planı" ile belirlemiş ve çalışmalarını Ulusal Güvenlik kapsamında değerlendirmiştir (Ünver ve Canbay, 2010:3). ABD'nin Ulusal Altyapı Koruma Planında 16 adet kritik altyapıya vurgu yapılmıştır (DHS, 2014).

Bu sektörler; Kimya sektörü, ticari işletmeler, iletişim ve kritik üretim yapan sektörler, barajlar ile her türlü savunma içerikli sanayiler, acil sağlık hizmetleri, enerji konulu sektörler, bankacılık ve finans sektörü, tarım ve gıda sektörü, devlet işletmeleri, sağlık ve kamu sağlığını ilgilendiren sektörler, bilişim teknolojileri, nükleer reaktör ve atıkları, ulaşım sistemleri ve su olarak belirlenmiştir.

Kritik altyapıların korunması Türkiye'de de ulusal düzeyde değerlendirilmiş olup bilgi güvenliği kapsamına alınmıştır. 2012 yılındaki Resmi Gazetede Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi ve Koordinasyonuna ilişkin Bakanlar Kurulu Kararı yayınlanmıştır. Bu karar ile siber güvenliğinin ülke çapında sağlanması konusunda idari, teknik ve hukuki çalışmalar hız kazanmış, siber güvenliğe ilişkin usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak üzere "Siber Güvenlik Kurulu" oluşturulmuştur. 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı olarak *"Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"* yayımlanmıştır. Bu eylem planına göre ülkemizin kritik altyapıları ilk etapta aşağıdaki gibi sıralanmaktadır (AFAD, 2014:34);

- Ulaşım,
- Enerji,
- Elektronik haberleşme,
- Finans,

- Su yönetimi,
- Kritik kamu hizmetleri,

Kritik alt yapılar, ülke vatandaşlarının olumsuz etkilenmesini önlemek için tüm tehditlere karşı korunması gerekir. Ayrıca siber saldırılardan önce kurum ve kuruluşların teknik olarak önlemlerini alması ve kendi bünyesinde kurmuş oldukları kurumsal SOME birimlerini güçlendirmeleri, siber saldırı olduğunda ise savunmanın yanı sıra Ulusal Siber Olaylara Müdahale Merkezi (USOM)'a bilgi vermeleri saldırının bertaraf edilmesi ve etkilerinin azaltılması açısından önem taşımaktadır.

2.8.4. Güvenlik Önlemlerinin Alınması

Siber saldırıları önlemeye yönelik gerekli güvenlik tedbirleri alınması gerekir. Aksi takdirde siber güvenlik suçlarının işlenmesine imkân sağlanmış olur (Tulum, 2006:76). Hiçbir güvenlik tedbiri almayan bir kurumun bilgisayarlarından iç ya da dış suç işlenmiyor olma ihtimali nerede ise yok denecek kadar azdır. Bu neden ile kurum içinde ya da bireysel bilgisayar tabanlı ürünlerde bir takım güvenlik tedbirleri alınmalıdır. Güvenlik tedbirlerinin başında anti virüs kullanımı, işletim sistemi ya da firewall güvenlik duvarı kullanımı, açık kaynak kodlu yazılımların kullanımı ve bu yazılımların eğitimleri verilerek yetkin kullanıcı yetiştirilmesi, log kayıtlarının izlenmesi, internet kullanım politikalarının belirlenmesi, fiziksel güvenlik duvarının belirlenmesi, kablosuz ağların güvenliği, sosyal mühendislik saldırılarına karşı farkındalık oluşması ve politikalar izlenmesi, şifreleme politikaları, e-posta politikaları, bal küpü sistemlerinin kurulması ve işletilmesi, tüm bilişim güvenliği hakkında personel eğitimleri ve tüm toplumun bilgilenmesi için farkındalık çalışmalarının yapılması gelmektedir. Bazı önemli güvenlik tedbirleri aşağıda açıklanmıştır.

2.8.4.1. Anti Virüs Yazılımları

Anti virüs, bilgisayar tabanlı cihazları (bilgisayar, cep telefonu, mobil sistemler vb.) zararlı programlardan korumak için hazırlanan ve artık günümüzde sezgisel analizler yaparak istenmeyen hareketler karşısında kullanıcıları uyaran yazılımlardır (Garland, 1996:443). Anti virüsler bilgisayara her yüklenen programı, indirilen tüm dosyaları, web sitelerinden bulaşan trojan, spy, malware,

worm'ları kullanıcıya gelen her maili tarayarak zararlı kodlar karşısında kullanıcıyı uyarır ve programın bilgisayara bulaşmasını ve virüsün arka planda çalışmasını engellemeye çalışır. Ayrıca anti virüsler belirli periyodlar ile sistemleri tarayarak gözden kaçan ya da belirli bir süre sonraya çalışmaya programlanan virüsleri de engellemeye çalışırlar. İmza tabanlı koruma, sezgisel analiz ve bulut yardımlı kötü amaçlı yazılımdan koruma teknolojileri son zamanlarda anti virüslere eklenen yeni özelliklerdendir. Bu sayede sistemler sürekli izlenir ve arka planda gizlice değişiklik yapmaya çalışan programların tespit edilmesi sağlanmaktadır. Yapılan tespitlerde değişiklik yapmaya çalışan yazılım zararlı ise sistemden silinir ve değişiklik yapılan kayıtlar eski durumuna geri çevrilmektedir. Bir diğer yeni özellik ise bulut teknolojisidir. Bu sayede yeni tespit edilen virüsler diğer kullanıcıların bilgisayarında tespit edildiğinde sizin bilgisayarınızda bu virüse karşı duyarlı olacak güncellemeyi alır ve virüsü tanır duruma gelir.

Anti virüsler her ne kadar birçok işletim sistemi için önemli olsa da her zaman tüm virüsleri tanımayabilir. Virüsler ilk çıktığında anti virüsler tarafından tanınmayabilir. Bu zararlı yazılımlar anti virüs firmaları tarafından tespit edilinceye kadar yaygınlaşmaya devam ederler ve çalıştıklarında çok büyük zararlar verirler. Virüslerin tanınmasını engellemek için kullanılan karmaşık kod yapısı karşısında klasik anti virüs yaklaşımları yeterli olmamaktadır. Bu neden ile anti virüs yazılımlarında ar-ge çalışmaları çok önemlidir.

Siber Güvenlik kapsamında anti virüs yazılımları önemli bir yer kaplasa da tek başına yeterli olmamaktadır. Bu yaklaşımın en yakın örneklerinden biride Stuxnet solucanıdır. Stuxnet diğer virüsler gibi DDOS atakları, kişisel hesap bilgilerini çalmak için hazırlanmamıştır. Özellikle hedefinde su kaynakları, petrol santralleri, enerji santralleri ve diğer sanayi tesislerinin kontrolü için kullanılan SCADA[15] sistemlerini ele geçirerek çalışma şekillerini değiştirmek için hazırlanmış komplike bir yazılımdır. Uzun süre hiçbir anti virüs yazılımları tarafından tanınmaması 0. gün açıklarını kullanması ve karmaşık yapısı nedeni ile siber güvenlik uzmanlarının dikkatle eğildiği ve incelediği bir konu olmuştur. Bu

[15] SCADA terimi "Supervisory Control And Data Acquisition kelimelerinin baş harflerinden oluşturulmuştur. Dilimize "Uzaktan Kontrol ve Gözleme Sistemi "olarak çevrilmektedir.

gibi nedenler ile bir sistemin kurulumunda anti virüs yazılımlarının yanında farklı çözüm önerileri de kullanılmalıdır.

2.8.4.2. Ağ Güvenlik Duvarı (Firewall)

Ağ güvenlik duvarı (network firewall), kurumun kendi networkü (ağı) ile internet dünyasındaki diğer ağlar arasında köprü olarak çalışan ve kurumun karşılaşabileceği birçok siber saldırı sorunlarını çözmek üzere tasarlanan ürün bazlı ya da açık kaynak kodlu çözümlerdir (Karaarslan vd., 2003:2). Güvenlik duvarları çift taraflı erişim denetimi yapabilirler, karşılaştıkları ve çözemedikleri sorunlar için sistem yöneticilerini bilgilendirirler. Firewall'lar networkü dinlemek ve log üretmek içinde başarılı ürünlerdir. Üretilen bağlantı logları analiz edildiğinde kuruma yapılan siber saldırı türleri hakkında fikir sahibi olunabilmektedir. Bu neden ile kurumsal siber güvenlik çözümleri için kullanıcıya önemli yararlar sağlayacaktır.

2.8.4.3. LOG Kayıtlarının Tutulması ve Kontrolü

Bilgisayar üzerinde ve network düzeyinde yapılan çalışmaların kayıtlarının tutulması sonucu oluşan yazılı çıktılara Log kayıtları denilmektedir. Log kayıtları kimi zaman sorun çözümlerinde kullanılırken kimi zaman bazı ihtilaflı durumları çözmek için kullanılmaktadır. Log kayıtlarının bir diğer kullanıldığı alan ise siber güvenlik kapsamındadır.

5651 sayılı kanun gereği internet bağlantısı erişim hizmeti sağlayan tüm kuruluşların log kayıtları tutması ve günlük olarak zaman ve tarih mührü ile imzalaması gerekir. Ayrıca imzalanan veriler 6 ay boyunca kanunen saklanması gerekmektedir.

2.8.4.4. Açık Kaynak Kodlu Yazılımların Kullanılması

Kaynak kodunun herkes tarafından görülebildiği ve özgürce herkesin kullanılabildiği yazılımlara Açık Kaynak Kodlu Yazılımlar denilmektedir. Kullanıcı yazılımın kullanım hakkı ile birlikte geliştirme ve geliştirilmiş şeklini bir başkasına devretme/satma yetkisine de sahiptir (Schmidt ve Schnitzer, 2003: 475). 1960'lı yıllardan itibaren hacker kültürünün bir özelliği olarak açık kaynak

kodlu yazılımlar kullanılmış, yazılımlarda ek bir geliştirme yapılmasında ise yeni kodların geliştirici topluluklarına gönderilmesi kararı alınmıştır (Arslan, 2011:5).

Ülkemizde açık kaynak kodlu yazılımların geliştirilmesi ve kurumlarımızda kullanılmasının siber güvenliğe çok büyük katkısı olacaktır. Ulusal güvenlik açısından milli yazılımların geliştirilerek kullanılması, siber savunma için alınabilecek tedbirlerden en önemlisidir. İçeriğini kendi geliştirdiği bir işletim sistemi veya yazılım için standart virüsler işlemeyeceğinden, zararlı yazılımların birçoğundan kurumların korunması sağlanacaktır. Ayrıca her kurumda standart olarak kullanılan bilgisayar işletim sistemleri, sunucu işletim sistemleri, firewall gibi lisanslama ücretleri olan birçok yazılım için ücret ödenmeyerek bu kaynak ile AR-GE yatırımları geliştirilebilecektir. Yeni bir yazılım üretilmesinin yatırım ve AR-GE maliyetleri yüksek olsa da ilave bir yazılım geliştirildiğinde maliyet oldukça düşmektedir. Kamunun milli yazılım kullanım projesi gerçekleştiğinde milli yazılımların kalitesi artacak ve sayıları çoğalacaktır. Avusturalyalı bir yazılım firması olan Cybersource'un 2003 senesinde yapmış olduğu bir çalışmada çalışan sayılarındaki farklılığa göre 3 firmanın kullandıkları işletim sistemlerine göre katlanması gereken maliyetler Tablo 2.4'te gösterilmiştir.

Tablo 2.4: Yazılım Maliyetlerinin Karşılaştırılması

	Microsoft Yazılımları	**AKKY***	**Tasarruf**
50 kullanıcılı A Firması	87.988$	80$	87.908$
100 kullanıcılı B Firması	136.734$	80$	136.654$
250 K C Firması	282.974$	80$	282.894$

Kaynak: Wong ve Sayo (2004:10) ***AKKY:** Açık Kaynak Kodlu Yazılım

Tablo 2.4'e göre A firmasının 50, B firmasının 100, C Firmasının 250 kullanıcı olduğu varsayılmaktadır. Wong ve Sayo (2004:10) firmanın kullanıcı sayısına göre Açık kaynak kodlu yazılımlara ve Microsoft'a ödemesi gereken ücretleri kıyaslamaktadır. Ödenmesi gereken ücretler arasında oldukça yüksek farklılıklar bulunmaktadır.

2.8.4.5. Kurumsal Ağ ve Sistem Güvenliği Politikaları

Bilişim sistemlerine içeriden ve dışarıdan yapılan saldırılar, ya da personelin yaptığı kritik hatalar nedeni ile kritik olan bilgi ve belgelerin yetkisiz kişiler tarafından okunması ya da değiştirilmesine neden olmaktadır. Bu nedenle kurumunun bilgi güvenliğini içeriden ve dışarıdan gelecek tehditlere karşı korunmak üzere önlem alınmalıdır. Güvenlik politikaları gelecek tehditleri en aza indirmek ve bir tehdit algılandığında neler yapılacağını, hangi yöntemler izleneceğini gösteren kurallar bütünüdür. Güvenlik politikalarının oluşturulmasında planlama yapılmalı kurumun güvenlik gereksinimleri göz önüne alınmalı ve sisteme erişim prosedürleri de incelenerek dikkatli ve titizlikle oluşturulmalıdır. Aksi halde güvenlik sağlanacakken açıklar verilebilmekte, ya da güvenlik sağlandığında ilgili kişilerin erişimleri engellenebilmektedir. Sistem üzerindeki herhangi bir servisin hangi koşullar altında nasıl kullanılabileceği politikalar ile belirlenmelidir (Kagal vd., 2004:50-56).

2.8.4.6. Bal Küpü (Honey Pot)

Daha çok büyük şirketler ve ortak güvenlik önlemlerinin alındığı merkezi sistemler tarafından uygulanabilecek bir güvenlik yöntemi olarak ülkemizde kullanılmaktadır. Balküpü bir bilgisayar, sunucu ya da sistem olarak tasarlanabilir. Bilgisayarlar arasında en fazla açık barındıran bilgisayar, sitemler arasında en fazla açık barındıran sistem ya da sunucular arasında en fazla açık barındıran sunucu olarak tasarlanmaktadır (Ulak-CSIRT, 2009).

İsminden de anlaşılacağı üzere asıl amaç saldırıyı özel hazırlanmış bu sisteme çekmektir. Saldırgan bir sisteme girdiğinde genel olarak bir network taraması yapar ve en rahat kırabileceği sistem üzerine ilerlemeye başlar. Açığını bulduğu sisteme sızdıktan sonra buradan edindiği bilgiler ile network üzerinde ilerlemesine devam eder.

İşte tam bu noktada bal küpü sistemi devreye girmektedir. Amaç saldırganın networke sızdıktan sonra balküpü sistemine sızması ve buradan ilerlemesini sağlamaktır. Bu nedenle oluşturulacak tuzak sistem gerçeğine çok yakın bir şekilde uyarlanır. Günümüzde bazı ülkelerde bal küpü sistemleri karadelik

sistemleri ile birleştirilerek kullanılmakta ve saldırganların vereceği zararları en aza indirgemektedir.

2.8.4.7. Personel Eğitimleri ve Farkındalık Eğitimleri

Güvenlik konuları çerçevesinde personel eğitimleri bir saldırı olmadan önlem almak açısından önem arz etmektedir. Çoğu siber saldırının en önemli unsurlarından biri de sosyal mühendisliktir. Sosyal mühendislik çalışmaları kurumlardan telefon, mail ya da evrak ile birtakım bilgilerin alınarak saldırıya zemin hazırlamaktadır. Günümüzde sosyal mühendislik oltalama sistemi ile birlikte kullanılmaktadır. Bu kapsamda belirgin bir hedef olmamakla birlikte veri alınan kişi ya da kurumlar üzerine saldırı çalışmaları başlatılmakta ve ilerletilmektedir.

Mesleki eğitim, belirli çerçeveler doğrultusunda insanların davranışlarında belli gelişmeler sağlamaya yarayan planlı çalışmalar olarak tanımlanır. Personel eğitimleri bu neden ile farklı başlıklar altında olabilmektedir. Tüm personel meslek hayatları boyunca benzer saldırılara maruz kaldığından dolayı eğitimler asgari bu düzeyde uygulamalı olarak verilmeli akabinde personelin stratejik durumuna göre ileri seviye eğitimler ile devam etmelidir. Bu eğitimler diğer teknik eğitimlerden farklı olarak sadece işin güvenlik boyutunu içermeli ve farklı senaryolar ile desteklenmelidir (Kaspersky, 2016).

2.8.4.8. Sosyal Ağların Kullanım Güvenliği

Sosyal medya, hassas bilgilerin kritik bilgilerin toplanması için yaygın kullanılan bir kaynaktır. Sosyal medyadan alınabilecek kritik veriler saldırganlar için yol gösterme açısından önem arz etmektedir. Sosyal siteler genellikle kullanıcıların kişisel bilgilerini, hobilerini, yerleşim yerini, iş ve mesleki bilgilerini, evlilik, eş, çocuk, anne, baba ve kardeş gibi ailevi bilgilerini, alışkanlıklarını, merak duyduğu alanlarını, dergi, kitap, site gibi üyelik bilgilerini barındırırlar. Bu kapsamdaki bilgi birikimleri saldırganların özellikle beklediği sosyal mühendislik bilgileridir. Bu bilgiler ışığında saldırgan, saldırı yapmak istediği kişinin ön bilgilerine ulaşmış olur ve birçok sosyal mühendislik saldırıları için yeterlidir. Özellikle bu bilgilerine ulaşılan kişilere farklı kimliklerle yapılan hile, rüşvet, şantaj ve korkutma gibi çalışmalar ile maddi ve manevi zararlar

verilebilmektedir. Bu saldırıların günümüzde birçok örneği bulunmaktadır. Kullanıcılar açısından yararlı gibi gözüken bazı yazı, makale ve programlar ile bilgisayar, tabletler ve akıllı telefonlara virüsler, trojenler, wormlar dağıtılmakta ve ele geçirilen cihazlar ile farklı saldırılar düzenlenmektedir.

2.8.4.9. Bilgi işlem Sorumlularının Yetkinliği

Bilgi işlem birimlerinin temel hedefi bilişim sistemlerinin yönetimini yapmak ve mükellefi olduğu sistemlerin çalışmalarının sürekliliğini sağlamaktır. Ayrıca yönettiği sistemlerin güvenlik açıklarını fark edip bu kapsamda çalışmalar yapmak, yeni açıkların oluşmasını önlemek ve var olan açıkların kapatılmasını sağlamak görevleri arasında gözükmektedir. Kurumlarda siber olaylarla öncelikli ilgilenmesi gereken birim Kurumsal Siber Olaylara Müdahale Ekipleridir. Bu ekipler siber güvenliğe ilişkin olarak hazırlanmış politikalara uygun hareket etmek, gereksinimleri raporlayarak ilgili makamlara iletmek ve çözüm önerileri geliştirmek gibi görevleri üstlenirler (UDHB, 2014:18-24). Ancak henüz tüm kurumlarda bilgi işlem birimleri ile siber olaylara müdahale ekipleri arasında görev ayrılığı ilkesi oluşturulmadığından siber güvenliğinde bilgi işlem personelleri tarafından sağlanması beklenir.

Kurumların en önemli departmanlarından biri olan bilgi işlem birimi personelleri sürekli gelişen yeni teknolojiler, sistemler ve yazılımlar üzerinde kendilerini geliştirmeleri gerekmektedir. Yeni teknoloji yeni siber güvenlik açıklarını da beraberinde getirir. Bir sistemin açığını görmek bazen uzun zaman ve uğraşlar almaktadır. Bu nedenle bilgi işlem personelleri bilişim açıkları ile sürekli ilgili olmalı ve yıl içerisinde araştırmalar, eğitimler, seminer ve konferanslara katılımlar ile bilgilerini güncel tutası gerekmektedir.

2.8.4.10. Penetrasyon Testleri

Penetrasyon testi; firmaların bilişim sistemlerini oluşturan donanım, yazılım ve network yapılarındaki uygulamalara bir saldırgan gözüyle (hacker) yapılan saldırılar ve kurumların güvenlik açıklarının tespit edilmesidir. Tespit edilen açıklıklara bir saldırgan yöntemi ile sızılmaya çalışılır ve elde edilen sonuçlar raporlanmaktadır (Şahinaslan, 2013).

3. SİBER SUÇLARIN ZONGULDAK İLİNDEKİ EKONOMİK BOYUTU

Önceki bölümlerde kayıt dışı ekonomi, suç ekonomisi ve bilişim suçları ayrıntılı bir şekilde ele alınmıştır. Çalışmanın bu bölümünde ise önceki bölümlerde anlatılan konular çerçevesinde, yıllar itibariyle sayısı giderek artan siber saldırıların, Zonguldak ilinde sebep olduğu ekonomik zararların boyutu analiz edilmektedir.

3.1. Çalışmanın Kapsam ve Metodolojisi

- **Çalışmanın Önemi**

Siber güvenlik olgusu her geçen gün önemi daha da çok anlaşılan bir konudur. Siber güvenlik çalışmalarına sebep olan siber saldırılar sadece öylesine yapılan, ya da gençlerin eğlenmek için yapmış oldukları bir eğlence aracı değildir. "Bir ara anti virüs ile sistemi taratır gerekirse bilgisayarı yeniden kurarız. Çok önemli değil" algısı ile konuya yaklaşan şirketler artık gerçeğin öyle olmadığını yüksek miktarda maddi ve manevi kayıplar ile anlamaya başlamıştır. Siber saldırılar sadece bilgisayarları ve teknolojik aletleri değil insan hayatını da tehdit eder duruma gelmiştir. Amerika Birleşik Devletlerinde 12 yaşındaki bir genç kızın uzun süre maruz kaldığı siber zorbalık nedeniyle intihar etmesi (Milliyet, 2013), Avustralya'da, internet hesaplarına dadanan kişilerin baskısı yüzünden bir lise öğrencisinin kendisini trenin altına atarak intihar etmesi (Hürriyet, 2012) gibi bireylere yapılan siber saldırılar, bu saldırıların sonucunun nereye varacağını çok net göstermektedir.

Açtığı arka kapılar nedeni ile kullanıcılarını zombilere dönüştüren bilgisayar virüslerinin yanı sıra, bulaşmasının ardından bilgisayardaki tüm verileri şifreleyip açılması için para talep eden birçok fidye yazılımlarının verdiği maddi zararlar, dünyada 2016 yılında bir milyar doları geçmiştir (Xtrlarge, 2017). Özellikle 2017 yılında WannaCry adlı fidye yazılımının aralarında Rusya bankaları, İngiltere hastaneleri ve Avrupa otomobil fabrikaları da olmak üzere 150 ülkeden 200 bin kişi ve firmayı etkilemesi siber saldırılar nedeni ile maddi kayıpların çok daha büyük olacağını göstermektedir (İnternethaber, 2017).

Siber saldırıların farklı disiplinlerle farklı yönleri olmasına rağmen bu çalışmada siber saldırıların maddi boyutları incelenmiştir. Hayatın her alanıyla içli dışlı olan iktisat biliminin siber dünya ile bağı sürekli kuvvetlendiğinden Zonguldak ilinde yaşanan siber saldırılarında boyutunun büyüdüğü tahmin edilmektedir. Bu çalışmada Zonguldak ilinde yaşanan siber saldırıların verdiği zararların ekonomik boyutu ortaya çıkartılmaya çalışılmıştır. Çalışma ile Zonguldak ilindeki siber saldırılar karşısında durumun net bir şekilde anlaşılması ve ayrıca daha sonraki bölgesel ya da ulusal çalışmalara katkı sağlaması hedeflenmektedir.

- **Çalışmanın Amacı**

Çalışmada Zonguldak ilinde yaşanan siber saldırıların ekonomik boyutları incelenmektedir. Bu genel amaç doğrultusunda Zonguldak ilinde bulunan firmaların siber güvenlik kültürü, siber saldırılara ne düzeyde maruz kaldığı, saldırıları engelleyici tedbirlere karşı bakış açıları, bilgi işlem birimlerine ne kadar kaynak ayırdığı, bilişim altyapıları, maddi zararlı saldırıların boyutlarının tespit edilip edilemediği, saldırıların ne kadar işgücü kaybına sebep olduğu ve firmaların bunu ne düzeyde tespit edebildiği, firmanın işi gereği kullandığı bilişim alt yapısını ne düzeye taşıdığını anlamaya yönelik sorular yöneltilmiştir.

Ankete dayalı analizde aşağıdaki soruların cevapları aranacaktır;

- Oltalama (phishing) saldırıları veya sosyal mühendislik olarak tabir edilen yöntemler ile Zonguldak ilindeki firmaların siber saldırıya uğrama oranları ve ekonomik zararı,
- Bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımların ekonomik zarar verecek etkileri,
- Bilgi işlem altyapısına göre firmaların siber saldırılardan etkilenme oranları,
- Zonguldak ilinde karşılaşılan en yoğun siber saldırı yöntemleri,
- Firmaların büyüklüklerine göre siber güvenlik yaklaşımları,
- Bilişim altyapısına ayrılan maddi kaynak ile saldırılardan etkilenme oranlarının karşılaştırılması,

Genel olarak “kayıt dışı ekonomi”, “suç”, “ekonomi” ve “suç ekonomisi” literatürde farklı disiplinlerce detaylıca incelenmesine rağmen bilişim suçlarının çeşitlerine göre ekonomik yansımalarına henüz tam olarak dikkat çekilmediği

gözlemlenmiştir. Bu çalışma siber suçların sadece mühendislik bölümlerince değil diğer tüm dallarda kendi alanlarınca araştırılmasına da dikkat çekecektir.

- **Çalışmanın Metodolojisi**

Bu çalışmada alan araştırması uygulaması yapılmıştır. Araştırmada anket yöntemi kullanılmıştır. Tarama modeli olarak bilinen anket yönteminde devam etmekte olan ya da belirlenen süre içinde gerçekleşmiş durumu öğrenmeye çalışan bir araştırma modeli kullanılmaktadır. Araştırma nedenini oluşturan her türlü veri olduğu gibi tanımlanmaya çalışılmaktadır (Karasar, 1991:77).

Araştırma soruları için en sık karşılaşılan siber saldırı türleri seçilmiştir. Bu saldırı türleri ikinci bölümde, ayrıntılı olarak ve literatürdeki önemi ile birlikte anlatılmıştır. Uygulama aşamasında ikinci bölümde anlatılan fakat daha çok makro ölçekte araştırılması gereken konular çıkartılmıştır. Çıkartılan diğer kısımlara çalışmanın sınırlılıkları olarak ayrıca değinilecektir. İlk etapta anket uygulaması bireysel olarak geliştirilmiştir. Fakat uygulama aşamasında firmalardan veri alımında sorunların yaşanması, firmaların ankete katılmama istekleri, soruların yapısı nedeni ile firmada yetkililerin tek başına cevap verememesi gibi sorunlar yaşanmıştır. Bu nedenle proje TÜİK ile paylaşılmış ve ilgili şartların sağlanmasının ardından TÜİK tarafından alan uygulaması yapılması kararı verilmiştir. TÜİK yetkilileri projenin amaç ve hedeflerine uygun olarak sorular ve soruların sorulma amaçlarını oluşturan tabilasyon planlarını tekrar kontrol ve revizesini yapmasının ardından ankete son şekli verilmiştir. Nihai aşamaya getirilen anket TÜİK tarafından kendi ilgili makamlarına sunulmuş onaylarının alınmasının ardından saha uygulamasına geçilmiştir.

2016 yılını kapsayan anket 2017 yılı Nisan – Mayıs ayları içerisinde yapılmıştır. Elde edilen anket verileri çalışmadaki araştırmacılar tarafından analiz edilmiştir. İzleyen alt bölümler bu analizlerden elde edilen bulguları içermektedir. Anket sorularından elde edilen veriler, konu temelli faktörlerin oluşturulmasını sağlanmıştır. Faktör skorlarının oluşturulmasında, faktör içeriğindeki konular, uzman görüşleri doğrultusunda derecelendirilmiş ve TOPSIS (Technique for Order-Preference by Similarity to Ideal Solution) yöntemi kullanılmıştır. Çalışmada metrik olmayan değişkenler arasında sistematik bir ilişkinin olup olmadığını öğrenmek için ki-kare testi, oluşturulan faktör/boyut değişkenleri

arasındaki ilişkileri incelemek üzere korelasyon analizi, değişkenler arasındaki ilişkinin modellenmesi için çoklu doğrusal regresyon analizi kullanılmıştır. Ayrıca faktör /endeks skorlarının alt kategorilere göre farklılığı, bağımsız iki örnek t testi kullanılarak analiz edilmiştir. Çalışmada örneklem rassal seçildiğinden analizlerden yapılan tüm çıkarsamaların Zonguldak'ı temsil ettiğine karar verilmiştir.

- **Çalışmanın Sınırlılıkları**

Çalışmada bilişim suçları kısmında işlenen, ancak anket sorularında yer almayan daha çok makro ölçekte araştırılması gereken konular bulunmaktadır. Bu bilgiler genel anlamda suç ekonomisi içerisine yer alsa da ölçümleri ve tespitleri yerelde zor olduğundan kapsam dışı bırakılmıştır. Bu konularda daha otoriter kurumlar tarafından daha büyük veri setleri ile ölçüm ve analiz yapılması gerekmektedir. Örneğin, TV kartları ile şifreli yayınları çözme, çocuk pornografisi, terörist faaliyetler/siber terör, bebek, kadın ve organ ticareti bu kapsamda değerlendirilebilir.

Yapılan kurum araştırmalarında görülen bazı kısımlar çalışmaya dâhil edilmemiştir. Özellikle yoğun olarak karşılaşılan sosyal medya hesaplarının çalınması, bireysel bankacılık ve bireysel kredi kartı şifrelerinin çalınması, siber saldırılara bireysel olarak maruz kalınması gibi adli vakalara yansımış fakat direk firma düzeyinde bir maddi zarara yol açmamış saldırılar bu çalışmanın kapsamında değerlendirilmemiştir.

Araştırmada 20'den daha az personel çalıştıran firmalar kapsam dışı bırakılmıştır. Özellikle emek yoğun işlerde örneğin, nakliye, bakkal, tamir işleri, halı yıkama gibi işletmelerde ya hiç bilişim altyapısı kullanılmaması ya da iş dışı kullanılması nedeni ile örneklemi bozmaması için personel sayı sınırlaması düşünülmüştür.

- **Çalışmanın Kapsamı**

Araştırma Zonguldak ilinde 20 den fazla personel çalıştıran firmalara uygulanmıştır. TÜİK verilerine göre 20+ firma sayısı 386 dır. Bu firmalardan 42 tanesi kapalı olup 4 firmaya ise kayyum atanmıştır. 3 firma gayri faal ve 1 firma

mükerrer olduğu için anket kapsamına alınmamıştır. Bu nedenle anket 336 firmaya uygulanmıştır.

Araştırma ham verilerinin üzerinde yapılan çalışmada ankete 33, 63, 99, 139, 175, 204, 216, 218, 221, 316. sırada cevap veren girişimler hem bilgisayar hem internet kullanmadıklarını söyledikleri için,

119,120,129,187. sırada cevap veren girişimler sadece 1 bilgisayar kullanıp internet dahil diğer bilişim altyapılarını kullanmadığı için,

330. sırada cevap veren girişim ise 2 bilgisayar kullandığını ancak internet dahil diğer bilişim altyapılarını kullanmadığı için verilerin frekans ve yüzde dağılımlarında kullanılmış, diğer analizlerde ise kapsam dışı bırakılmıştır.

- **Ön Çalışma**

Bu çalışmada kullanılmak için bireysel olarak anket hazırlanmıştır. Anket 3 firmaya uygulanarak sorun oluşturabilecek ve yanlış anlaşılacak kısımları düzeltilmiştir. Nihai hali verilen anket Zonguldak Ticaret ve Sanayi Odası (ZTSO) ve Batı Karadeniz Kalkınma Ajansının (BAKKA) firma toplantılarında uygulanmıştır. Bu uygulama aşamasında ortaya çıkabilecek sorunlar Tablo 3.1'de gösterilmiştir.

Tablo 3.1: Karşılaşılan Örnek Sorunlar

N.	DERECESİ	ÖRNEK SORUN
1	Kritik	Firmalar siber saldırılar sonucunda oluşan hasarı farklı sebepler ile kimseyle paylaşmak istememektedir.
2	Kritik	Firmalar siber saldırılar nedeni ile uğranılan maddi zararı itibar kaybı yaşamamak için paylaşmak istememektedir.
3	Kritik	Firma herhangi bir siber saldırıya uğrayıp uğramadığını tespit edememektedir
4	Orta	Firma sahipleri bilişim alt yapısı ile ilgili bazı sorular hakkında bilgi sahibi değildir.
5	Orta	Firma yetkilileri birtakım siber saldırıya uğramış olsa da bu saldırının hangi saldırı tipi olduğunu anket üzerinde anlayamamaktadır
6	Orta	Firmalar daha önce siber saldırı sonucu oluşacak maddi zarar harici diğer zararları hesaplamadığı için bu tip sorulara cevap vermekte zorlanmaktadır
7	Az	Bazı firmalar her türlü bilgisayar arızasını siber güvenlik kapsamında değerlendirmektedir
8	Az	Firma yetkilisi yerine toplantıya gelenler bu bilgilere vakıf olmayabilmektedir

Tablo 3.1'de gösterilen sorunlar gruplandırılarak çözüm yoluna gidilmiştir. Ancak daha efektif bir yöntem bulunmadığı takdirde bazı sorunların devam edeceği ve anketin geçerliliğinin azalacağı sonucuna varılarak farklı arayışlara girilmiştir. Bu kapsamda görüşülen TÜİK ile hem sorun hem de anketin önemi üzerine istişareler yapılmıştır. TÜİK tarafından projenin kabul edilmesinin ardından anket soruları tekrar ele alınmış ve Tablo 3.1'de görülen sorunlar için adımlar atılmıştır.

Kritik seviye: Özellikle TÜİK'in bu konudaki uzmanlığı ve güvenilirliği neticesinde firmaların yaklaşımları değiştiği için sorunlar büyük ölçüde azalmıştır. Ancak firmanın siber saldırıya uğrayıp uğramadığını anlamamasına karşı sorularda bir miktar değişikliğe gidilip daha çok hasar veren siber saldırılar sorulmaya çalışılmıştır. Fakat tüm saldırıların öğrenilmesi mümkün olmamıştır.

Orta seviye: Sorular için firma adresine gidildiğinden firma sahipleri, bilgi işlem sorumluları ve muhasebe yetkililerinden veri alınması neticesinde ilk aşamaya göre çok daha sağlıklı veri elde edilmiştir.

Az seviye: Sorunun sorulma yöntemleri değiştirilerek ve disk arızası soruları eklenerek sorunlar çözülmeye çalışılmıştır.

Her ne kadar doğru bilgiye ulaşılmaya çalışılsa da siber saldırıya uğramış olan firmaların bu saldırılardan bir kısmını anlamadığı gözlenmektedir. Özellikle firewall kullanmayan ve saldırı tespit sistemleri ile firmalarını takip etmeyen, ayrıca bu takipleri yapabilecek alt yapıya sahip teknik personel çalıştırmayan firmaların bazı siber güvenlik sorularına doğru cevap verememesi muhtemeldir. O nedenle bu çalışmada firmaların karşılaştıkları tüm saldırılar ele alınmayıp, daha çok maddi zarar veren saldırılar üzerinde durulmuştur.

3.2. Frekans Analizi

Örneklemde firmaların anket sorularına verdiği cevaplara göre frekans analizi yapılmıştır. Soru gruplarına göre verilen cevaplar da gruplandırılarak analiz edilmiştir.

3.2.1. Firmaların Bilgi İşlem Altyapısı

Tablo 3.2'de Zonguldak ilindeki firmaların %80,10'u 10 bilgisayar ya da daha azına sahipken 10 – 20 arası bilgisayarlara sahip firmalar %13,10 olduğu görülmektedir. Örneklemde 20 -100 arasında bilgisayara sahip %5,40 oranında firma bulunmaktadır.

Tablo 3.2: Firmaların Bilgisayar Sayıları

Bilgisayar sayısı	< 10	10 - 20	20 - 100	100 <
Firma Oranı %	80,10	13,10	5,40	1,50

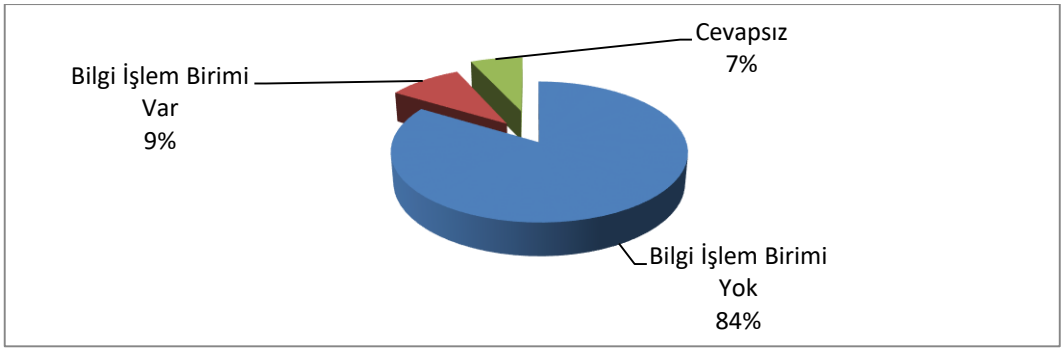
Örneklemden çıkan bir diğer sonuçta firmaların 149'unda sunucu bulunurken bu oran ankete katılanların %45,8'ini oluşturmaktadır. Tablo 3.3'de görüldüğü gibi networkünde sunucu bulunduran firmaların %37,8'inde 1 sunucu bulunmakta iken %4,8'inde 2 sunucu bulunduğu görülmektedir. 2 den fazla sunucu barındıran firmalar ise %2,4'tür. Firmaların sunucu barındırmaları sunuculara yapılan siber saldırılara direk maruz kalmaları ile ilişkili olduğundan önemlidir.

Tablo 3.3: Firmalardaki Sunucu Sayısı

Sunucu Sayısı	1	2	2+	**Toplam**
Firma Sayısı	127	16	8	151
Yüzde	37,8	4,8	2,4	44,9

Bünyesinde bilgi işlem birimi bulunduran firmaların oranı Şekil 3.1'de gösterilmektedir. Grafik 3.1 incelendiğinde firmaların %84'ünde bilgi işlem birimi bulunmadığı, toplamda bilgi işlem birimi olan firmaların oranı ise %9 olduğu görülmektedir.

Grafik 3.1: Bilgi İşlem Birimi Oluşturma Durumu



Bilgi işlem birimi olan firmaların %5,3'ünde 1 personel, %2,7'sinde 2 personel, %1,2'sinde ise 2 den fazla personel istihdam edilmektedir. Bu durum Tablo 3.4'te gösterilmiştir. Siber güvenlik yaklaşımındaki en büyük öneme sahip olgu insandır (Akurgal, 2016:2). Bilgi işlem personelinin girişimin içerisinde bulunmasının diğer personellerin gerek soru sormasına, gerekse organizasyondaki hizmet içi eğitimlere destek vermesine katkı sağlayacağı için önem arz edeceği gözlenebilir.

Tablo 3.4: Bilgi İşlem Personel Sayısı

Bilgi İşlem Personel Sayısı	0	1	2	2+
Firma Sayısı	305	18	9	4
Yüzde	90,8	5,3	2,7	1,2

Anket sonuçlarına göre Zonguldak'ta 2016 yılında bilgi işlem birimine yapılan toplam yatırım miktarının 4.323.208 TL olduğu görülmektedir. Firmaların %60'ı 20.000 TL ve üzerinde yıllık yatırım yapmaktadırlar.

Tablo 3.5: Bilgi İşlem Hizmeti İçin Dış Destek Kullanma Durumu

	Firma	**Yüzde (%)**
Hayır	99	29,5
Evet	221	65,8
Toplam	320	95,2
Cevapsız	16	4,8
Genel Toplam	336	100,0

Tablo 3.5'te bilgi işlem için dışarıdan hizmet alım durumu görülmektedir. Tabloya göre firmaların %65,8'i dışarıdan destek aldığını ifade etmektedir. Bu durumdan da anlaşıldığı üzere firmaların büyük oranı bilgi işlem işlerini firma dışı kaynaklardan temin etmekte olup bilgi işlemle ilgili birçok iş için personel istihdam etmemeyi tercih ettiği görülmektedir.

3.2.2. Firmalarda Network Güvenliği

Çalışmada birçok kurum için olmazsa olmaz olarak kabul edilen firewall kullanım bilgileri sorulmuştur.

Tablo 3.6: Firewall Kullanım Çeşitleri

	Açık Kaynak Kodlu Güvenlik Duvarı	Kutu Çözüm Güvenlik Duvarı	Telekom firmalarının sunmuş olduğu hizmet
Firewall Kullanımı	%7,7	%11,6	%13,4
Firma Sayısı	26	39	45

Firmalardan %61,6'sı firewall kullanmadığını ifade ederken Tablo 3.6'da görüldüğü gibi firmaların %7,7'si açık kaynak kodlu, %11,6'sı kutu çözüm güvenlik duvarı ve %13,4'ü Telekom firmalarının sunmuş olduğu firewall hizmetlerini kullanmaktadır.

Zonguldak'ta büyük oranda lisanslı anti virüs yazılımı kullanılmaktadır. Tablo 3.7 incelendiğinde firmaların %66,78'i bilgisayarlarında lisanslı anti virüs yazılımı kullandığını beyan ederken, %6,31'i lisanslı ve lisanssız anti virüs yazılımı kullanmadığını belirtmiştir.

Tablo 3.7: Bilgisayarlarda Anti Virüs Kullanımı

		Bilgisayarlarda Lisanssız Anti Virüs Kullanımı		
		Hayır	**Evet**	**Toplam**
Bilgisayarlarda Lisanslı Anti Virüs Kullanımı	**Hayır**	19; *%6,31*	69; *%22,92*	88; *%29,24*
	Evet	201; *%66,78*	12; *%3,99*	213*; %70,76*
	Toplam	220; *%73,09*	81; *%26,91*	301; *%100*

Not: Lisanslı anti virüs kullanımı sorusuna firmaların %5,1'i, lisanssız anti virüs kullanımı sorusuna ise firmaların %9,8'i cevap vermemiştir.

Ayrıca Tablo 3.7'de, firmaların bilgisayarlarında lisanssız anti virüs kullanım oranı %22,92 olarak izlenirken, firmaların %9,8'i bu soruya cevap vermemiştir. Firmaların lisanslı ürün kullanarak güncelleştirmeleri yakından takip etme oranları yüksek bir oranda olsa da gerek ekonomik, gerekse ihtiyaç olmadığı düşüncesi ile lisanslı ürün kullanmayan profesyonel girişimlerin bulunduğu da gözlenmiştir. Her dört firmanın birinde lisanssız anti virüs kullanılıyor olması ya da herhangi bir anti virüs kullanmıyor olması o networkteki diğer bilgisayarları da riskli duruma düşürmektedir. Firmalarla yapılan ikili görüşmelerde muhasebe ve satış gibi önemli görülen bilgisayarlarda lisanslı anti virüs yazılımı kullanılırken, CD, USB ve internet kullanımlarına da özen gösterilmektedir. Fakat firmalarda gişe, barkot yazımı gibi daha önemsiz gördükleri işler için kullanılan bilgisayarlarda, anti virüs kullanımına özen gösterilmediği gibi "virüs bulaşsa da

önemli değil" yaklaşımı izlenmiştir. Bu durum firmaların yüksek oranda önem vermesi gereken siber güvenlik yaklaşımını tehdit etmektedir.

Tablo 3.8: Sunucularda Anti Virüs Kullanımı

		Sunucularda Lisanssız Anti Virüs Kullanımı		
		Hayır	**Evet**	**Toplam**
Sunucularda Lisanslı Anti Virüs Kullanımı	**Hayır**	12; *%12,62*	12; *%3,99*	24; *%16,61*
	Evet	115; *%39,20*	4; *%1,33*	119; *%40,53*
	Toplam	127; *%51,83*	16; *%5,32*	143; *%57,14*

Not: Lisanslı anti virüs kullanımı sorusuna firmaların %43,2'si, lisanssız anti virüs kullanımı sorusuna ise firmaların %48,5'i cevap vermemiştir.

Firmaların ana bilgisayarlarına verdikleri önem de birbirinden farklıdır. Birçok networkte en kritik bilgileri sunucular barındırmaktadır. Dolayısı ile firmaların en mahrem bilgileri de bu sistemlerde bulunmaktadır. Tablo 3.8'de görüldüğü gibi firmaların sadece %39,20'si sunucularında lisanslı anti virüs bulundururken hem lisanslı hem lisanssız anti virüs kullanmayan firmaların oranı ise %12,62'dir. Ana bilgisayarların kritik öneme sahip olduğunu bilen birçok saldırgan tarafından yapılan siber saldırılar çoğunlukla sunuculara erişim için daha zayıf olan bilgisayarları kullandığı bilinmektedir. Ana bilgisayara erişimin daha kısıtlı tutulması, firewall, anti virüs ve kurum içi saldırı tespit algılayıcıların bulunması kadar bu ürünlerin doğru yapılandırılmaları ve takip edilmeleri de önemlidir. Bu nedenle her ne kadar anket düzeyindeki çalışmalarda kullanım bilgileri sorulsa da girişimlerin networklerinde bulunan güvenlik ürünlerinin doğru konumlandırılıp konumlandırılmadığı da önem arz etmektedir.

Kötü niyetli ağ hareket ve bağlantılarının tespiti için Intrusion Detection Systems (IDS) kullanılmaktadır. Kötü niyetli ağ hareket ve bağlantılarının önlenmesi için ise Intrusion Prevention Systems (IPS) kullanılmaktadır (Işık, 2013:2).

Tablo 3.9: IPS/IDS Kullanım Durumu

	IPS/IDS Kullanmıyorum	**IPS/IDS Kullanıyorum**	**Bu Konuda Fikrim Yok**	**Toplam**	**Cevapsız**	**Genel Toplam**
Firma	263	42	4	309	27	336
Yüzde	78,3	12,5	1,2	92	7,8	100

IPS ve IDS kullanımının Zonguldak ilinde çok yaygın olmadığı Tablo 3.9'da görülmektedir. Firmaların %78,3'ünde bu ürünler kullanılmazken girişimlerin sadece %12,5'inde bu amaçla çalışan ürünler bulunmaktadır. Bu konuda hiçbir fikrinin olmadığını söyleyen girişimlerin sayısı %1,2'dir. Soruya cevap vermeyen girişimin oranı ise %7,8 dir.

3.2.3. Firmalarda Yazılımsal Uygulamalar

Firmaların web sitesi ve mobil uygulama kullanım durumları Tablo 3.10'da gösterilmektedir.

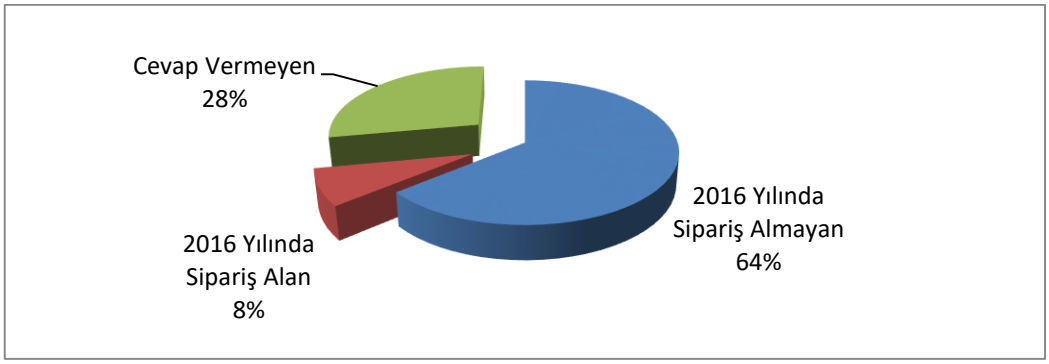
Tablo 3.10: Firmaların Web Sitesi ve Mobil Uygulama Kullanım Durumları

	Hayır	Evet	Toplam	Cevapsız	G.Toplam
Web Sitesi Kullanımı (%)	42	53,5	95,5	4,5	100
Mobil Uygulama Kullanımı (%)	87,2	4,8	92	8	100

Tablo 3.10'da görüldüğü gibi firmaların %42'sinin web sitesinin olmaması günümüzde firmaların dijital hayata bakış açıları ile ilgili farklı çalışmalar yapılması gerektiğini göstermektedir. Firmalar üretim de yapsalar satış da yapsalar global dünyadan kendilerini soyutlayamazlar. Özellikle en büyük reklam kapasitesine sahip olan internetin hayatın her aşamasında kullanıldığı gibi firmaların tanıtımında da kullanması girişimlere çok büyük artılar katacaktır. Zonguldak'taki 20'den fazla personel çalıştıran firmaların sadece %53,5'inin web sitesinin olduğu görülmektedir.

Firmalar reklamlarını en iyi şekilde yapmak ve bunun yanında tüm dünyaya ürünlerini pazarlamak için web sitelerini kullanmaktadır. Ancak gelişen dünyada bilgisayarların mobil cihazlara dönmesi firmaların mobil uygulamalara da yatırım yapmasına neden olmuştur. Özellikle ürüne ihtiyaç duyan kişiler mobil cihazlar üzerinden ürünleri en iyi şekilde tanımak ve fiyatlarını incelemek için mobil cihazlara uyumlu yazılımlar kullanmaktadır. Mobil yazılımın üretilmesi ve takip edilerek versiyonlarının güncellenmesi zaman ve kaynak isteyen bir işlem olduğu için asıl işi son kullanıcı olmayan birçok firma tarafından yeterince önemsenmediği tahmin edilmektedir. Tablo 3.10'da Zonguldak'taki firmaların %87,2'sinin mobil uygulaması bulunmadığı gözlenirken %4,8'inin ise mobil uygulama kullanmadığı görülmektedir.

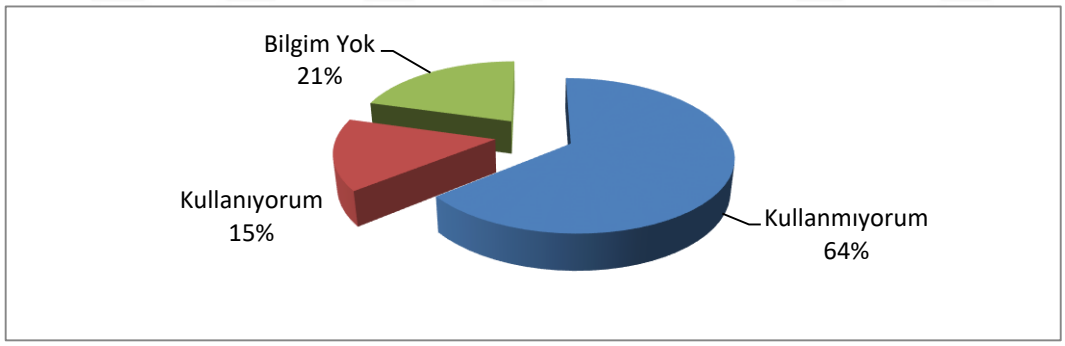
Grafik 3.2: Web Sitesi ya da Mobil Uygulamalardan Ürün/ Hizmet Siparişi Alma Durumu



Grafik 3.2'de web sitesi veya mobil uygulama üzerinden 2016 yılında ürün ya da hizmet siparişi alan firmaların oranının %8 olduğu, fakat firmaların %64'lük bir kısmının henüz e-ticaret yapmadığı görülmektedir. Araştırmada bu soruya cevap vermeyenlerin oranı ise %28'dir.

Bilginin taşınması sürecinde güvenlik ve gizliliği sağlamak için SSL protokolü geliştirilmiştir. SSL, sunucu ile istemci arasındaki iletişimin şifreli olarak güvenli bir şekilde yapılmasını sağlamaktadır (İsimtescil, 2016).

Grafik 3.3: SSL Kullanım Oranı



Grafik 3.3'te web sitesi ya da mobil uygulamalarında gizlilik mührü veya sertifikası bulunduran firmaların oranının %15 olduğu görülmektedir. Firmaların %64'ü ise SSL kullanmamaktadır. E-ticaretin az olması, girişimlerin web sitesi ya da mobil uygulamalar üzerinden hizmet yada ürün satışındaki oranın düşük olması SSL kullanımına da yansıdığı görülmektedir.

Çağımız dünyasında e-posta kullanımı en önemli iletişim aracından biridir. Kurumsal e-posta kullanımı firmaların iletişimindeki kurumsallığı göstermektedir. Önceleri kişisel iletişimde kullanılan e-postalar, günümüzde kurumsal bilgi birikimin en önemli parçalarını oluşturmaktadır (Özdemirci ve Aydın, 2007:174).

Tablo 3.11: E-posta Kullanım Durumu

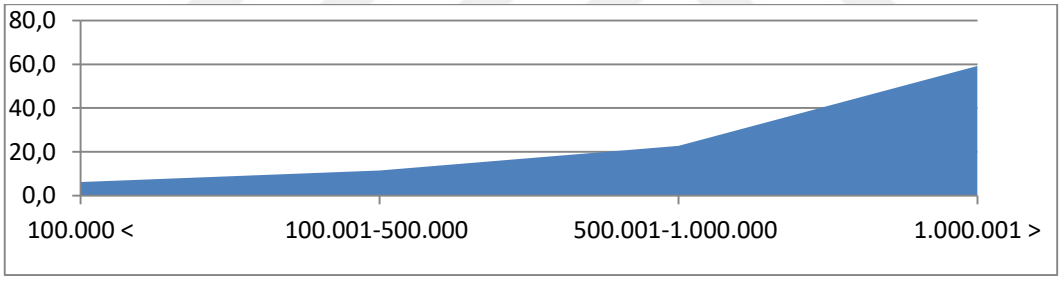
	Hayır	Evet	Toplam	Cevapsız	Genel Toplam
Firma	211	110	321	15	336
Yüzde	62,8	32,7	95,5	4,5	100

Kurumsal e-postalar çoğunlukla kurumlarının ismini ya da kısaltmasını taşıyan domainlerden oluşmaktadır. Girişimlerin e-posta kullanım durumları incelendiğinde kurumsal domain ismi ile e-posta hizmeti kullanan firmalar %32,7 iken henüz kendi domaini ile yani kurumsal olarak e-posta hizmeti kullanmayan girişimlerin oranının %62,8 olduğu Tablo 3.11'de gösterilmektedir.

3.2.4. Firmaların Ekonomik Yapısı

Ankete katılan firmaların %58'inin bir milyon liranın üzerinde, %22,9'unun 500 – 1 milyon arası, %11,9'unun 100 -500 bin TL arası, %6,5'inin ise 100.000 liranın altında ciroya sahip olduğu Grafik 3.4'te görülmektedir.

Grafik 3.4: Firmaların Ciro Bilgileri (TL)



Firmaların %2,7'inde 250 ve üzerinde personel çalışırken 100 -250 arası personel çalıştıran firmaların oranı %8,9, 50 -99 arası personel çalıştıran firmaların oranı ise %15,8'tir. 20-49 arası personel istihdamı ise %46,1 dir.

3.2.5. Firmaların Karşılaştıkları Siber Saldırılar

Birçok insanın internet uygulamaları arasında en çok kullandığı servis e-postadır. E-posta saldırıları firmalara çoğunlukla vakit kaybı olarak dönmektedir. Ancak saldırganların günümüzde farklı saldırıları birleştirerek yöneltmesi maddi zararlara da neden olabilmektedir. Örneğin oltalama saldırısı için saldırganlar telefon yöntemini kullanabildiği halde daha çok kitlelere ulaşması ve aynı süre içerisinde birden çok kişiyi kandırabilmesi açısından e-posta yöntemini tercih etmektedir.

Tablo 3.12: Firmaların Saldırıya Uğrama Oranları

	Mobil/Web Sitesi Saldırıları	E-posta ile Saldırı	Sunucu Saldırısı	Virüs Saldırısı	Oltalama
Hayır	73,5	56,0	66,7	89,6	87,5
Evet	3,9	11,6	4,2	6,0	7,7
Toplam	77,4	67,6	70,8	95,5	95,2
Cevapsız	22,6	32,4	29,2	4,5	4,8
Genel Toplam	100,0	100,0	100,0	100,0	100,0

Tablo 3.12'de Zonguldak ilinde yapılan siber saldırı çeşitleri gösterilmektedir. Bu veriler incelendiğinde ilk sırada firmaların e-posta saldırılarıyla karşılaştığı görülmektedir.

Tablo 3.13: Firmaların e-posta Saldırısına Uğrama Durumu

Saldırı Sayısı	**1**	**2**	**2+**
Firma Yüzdesi (%)	5,1	3,0	2,9
Firma Sayısı	17	10	10

Tablo 3.13'de spam mail dışında 2016 yılı içerisinde firmaların %5,1'inin en az 1 defa, %3'ünün 2 defa saldırıya uğradığı görülürken, 2 den fazla saldırıya uğrayan firmaların oranı ise %2,9 olarak görülmektedir. Ayrıca bazı firmalarda ciddi zarara uğratan saldırıların olduğu gözlemlenirken e-posta saldırıları nedeni ile 2 firmanın 1 er gün, 6 firmanın 2'şer gün, 2 firmanın 3'er gün, 1 firmanın 4 gün, 2 firmanın 7'şer gün, 2 firmanın ise 10'ar gün sistemlerinin devre dışı kaldığı kaydedilmiştir.

E-posta saldırılarından 1 firma 600 TL, 1 firma 1.500 TL tutarında zarar görürken 7.500 TL, 10.000 TL ve 15.000 TL tutarında mağduriyet yaşayan 4 firmanın bulunduğu kaydedilmiştir. Zonguldak'taki firmaların büyük bölümünün kurumsal e-posta kullanmadığı (%62,8 oranında) belirlenmiştir. Firmaların kurumsal e-posta kullanma sayesinde, kurumsal kimlik ve prestij kazanımı ile birlikte daha rahat iş takibi nedeniyle maddi getirisinin yüksek olacağı öngörülebilir. Ancak kurumsal e-posta kullanmamanın firmalara sağladığı en büyük avantajın firmaları e-posta saldırılarına daha az hedef yaptığı tahmin edilmektedir.

Oltalama saldırıları virüs saldırıları gibi sistemin genelini bozarak zaman kaybına neden olmasından daha çok doğrudan maddi kayba neden olabilmektedir. Yapılan analizler ve firma görüşmelerinde oltalama saldırısını yapan saldırganın amacının çok net para kazanmak olduğu gözlenmektedir.

Tablo 3.14: Oltalama Saldırısı ile Karşılaşma Oranı

Saldırı Sayısı	Firma Sayısı	Yüzde
1	12	3,6
2	2	0,6
3	4	1,2
3+	8	2,4

Oltalama saldırısına maruz kalan firmalar ve oranları Tablo 3.14'te verilmiştir. Zonguldak'ta 2'den fazla saldırıya uğrayan firma sayısı 14 iken 12 firmaya ise 1 defa oltalama saldırısı olduğu kaydedilmiştir.

Bu saldırılar neticesinde özellikle verilerin şifrelenmesi ve kullanıcıya tekrar satılması gibi teknikler de uygulanabilmektedir. Örneklem içerisinde 2 firmanın sisteminin birer gün, 1 firmanın iki gün, 1 firmanın ise beş gün aksadığı ayrıca örneklem içerisinden bir firmanın 1.000 TL maddi zarara uğradığı görülmüştür.

Virüsler internetin gelişimiyle birlikte birçok çalışanı etkileyen maddi ve manevi zararlar veren yazılımlardır. Zonguldak örnekleminde virüsler nedeni ile zarara uğrama oranı %6 olarak gözükmektedir. 8 firmanın 2016 yılında bir defa, 4 firmanın 2 defa, 6 firmanın 3 defa, 1 firmanın 25 defa, saldırıya uğradığı kaydedilmiştir. Ayrıca Tablo 3.15'te de görüldüğü gibi, firmaların %2,7'sinin 1 gün %0,6'sının 2 gün sistemleri devre dışı kalırken 3 günden fazla sistemi devre dışı kalan firma oranı %0,3'tür.

Tablo 3.15: Virüslerinin Sistemi Devre Dışı Bırakma Süresi

Devre Dışı Kalma (Gün)	Firma Sayısı	Yüzde
1	9	2,7
2	2	0,6
3	1	0,3
3+	2	0,6

Virüslerin etkisi incelendiğinde sadece sistemleri devre dışı bırakmadığı maddi zarara da neden olduğu görülmüştür. Örneklemdeki firmaların 2016 yılındaki maddi kayıpları incelendiğinde 1 firmanın 200 TL, 2 firmanın 500 TL,

1 firmanın 1.000 TL maddi zarara uğradığı görülürken 1 firmanın 100.000 TL maddi zarara uğradığı tespit edilmiştir.

Sunucular genel itibari ile sistemlerin beyni olarak tabir edilmektedirler. Birçok kurumda en stratejik bilgiler sunucularda barındırılırken, süreçlerin yürümesi ve mükerrer kayıtların engellenmesi gibi önemli görevleri de üstlenmektedirler. Firmalarda ana bilgisayarlara yapılan siber saldırılar incelendiğinde 14 firmanın siber saldırıya maruz kaldığı kaydedilmektedir. Firmalardan %2,1'i birer kez, %1,2'si 2 kez, %0,3'ü ise 10 kez ana sunucularına siber saldırı aldıkları Tablo 3.16'da görülmektedir. Bir firmanın 7 gün, 1 firmanın 5 gün, 5 firmanın ise 1 gün siber saldırılar nedeni ile hizmetinin aksadığı kaydedilmiştir.

Tablo 3.16: Ana Sunucuya Yapılan Saldırı Sayıları

Saldırı Sayısı	Firma Yüzdesi	Firma Sayısı
1	2,1	7
2	1,2	4
3	0,3	1
10	0,3	1

Ana sunuculara yapılan saldırıların maddi boyutları incelendiğinde 2016 yılında 2 firma 15.000 TL, 3 firma 4.000 TL, 1 firmanın ise 500 TL tutarında maddi zarara uğradığı tespit edilmiştir.

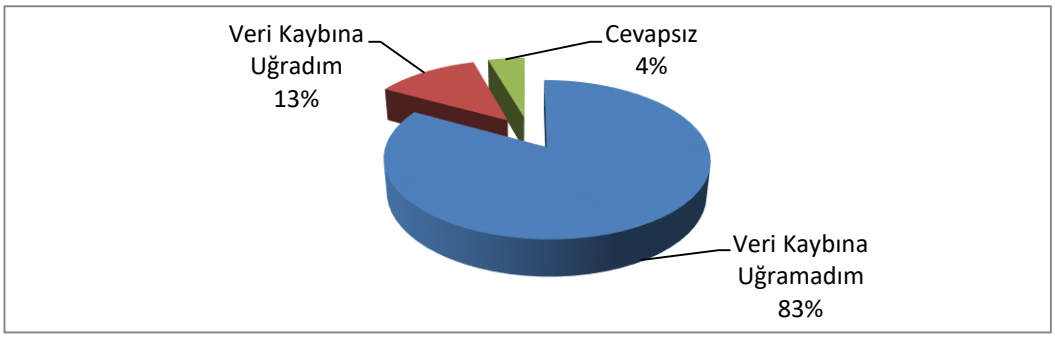
13 firmanın mobil uygulamalarına ya da web sitelerine siber saldırı olduğu kaydedilen örneklemde Tablo 3.17'de görüldüğü gibi firmaların %1,8'ine 1 kez, %1,2'sine 2 kez ve %0,3'ün 10 kez saldırıyla karşılaştığı tespit edilmiştir. Firmaların 5 tanesinin toplamda 10 gün sistemleri durduğundan hizmet verememiştir. Ayrıca firmaların biri 1.600 TL ve bir diğeri ise 4.000 TL olmak üzere doğrudan maddi zarara uğradığı da tespit edilmiştir.

Tablo 3.17: Mobil Uygulamalar ve Web Sitesi Saldırı Sayıları

					Toplam
Saldırı Sayısı	1	2	3	10	16
Firma	6	4	1	1	12
Yüzde	1,8	1,2	,3	,3	3,6

Yapılan çalışmada siber saldırılar kadar harddisk arızalarının da firmalara zarar verdiği görülmektedir. Grafik 3.5'de görüldüğü gibi firmaların %13'ü harddisk bozulması nedeni ile veri kaybına uğramıştır.

Grafik 3.5: HDD Arızası Nedeni ile Veri Kaybı Yaşanması



Firmaların 21 tanesi HDD nedeni ile direk olarak maddi zarara uğradığını belirtirken, rakamsal olarak zararlar en az 250 TL en fazla 6.000 TL olarak ölçülmüştür. Toplamda firmaların uğramış oldukları zarar ise tahmin edilenin çok altında olup 25.670 TL civarındadır. Firmalarla yapılan ikili görüşmelerde firmaların yaşamış olduğu veri kaybının maddi karşılığı tam olarak tespit edilemediği gözlemlenmiştir. Bazı verilerde ise disk bozulmasının ardından çok eski yedeğine ulaşıldığı için veri kaybı olarak görülmeyip iş kaybı olarak görüldüğü izlenmiştir.

Firmalarda henüz tam olarak siber olaylara müdahale ekipleri (SOME) olgusu gelişmemiştir. Zonguldak'taki 4 firmanın SOME birimi varken 6 firma önümüzdeki dönemde kuracaklarını ifade etmişlerdir.

Bir firmanın bilgi teknolojisi (BİT) varlıklarını korumak için resmi olarak tanımladığı ve düzenli olarak gözden geçirdiği bilgi ve iletişim teknolojisinin güvenliği sağlamak için oluşturduğu politikalara güvenlik politikaları yada diğer bir ismi ile siber güvenlik politikaları denilmektedir (Çınar, 2013). Zonguldak ilinde firmaların 13 tanesi bu standardı sağlarken, ayrıca firmaların %86,7'si beklenmeyen bir olay veya saldırı nedeniyle verilerin bozulması ya da kaybolması ile ilgili tedbirlere güvenlik politikasında yer vermiştir. Bununla birlikte firmaların %46,7' si başka siteye yönlendirilerek şifre çalınması ile ilgili, %53,3'ü istenmeden güvenli verilerin açıklanması ile ilgili, %60,0'ı dışarıdan saldırı nedeniyle BİT hizmetlerinin verilememesi ile ilgili tedbirlere güvenlik politikalarında yer vermişlerdir.

Tablo 3.18: Uygulanan Güvenlik Yöntemleri

	Güçlü parola		Akıllı kartlar		Biometrik		FMVY		G.O.Analizi	
	Firma	Yüzde	Firma	Yüzde	Firma	Yüzde	Firma	Yüzde	Firma	Yüzde
Hayır	119	35,4	280	83,3	310	92,3	184	54,8	299	89,0
Evet	200	59,5	39	11,6	8	2,4	136	40,5	20	6,0
Toplam	319	94,9	319	94,9	318	94,6	320	95,2	319	94,9
Cevapsız	17	5,1	17	5,1	18	5,4	16	4,8	17	5,1
Genel Toplam	336	100,0	336	100,0	336	100,0	336	100,0	336	100,0

FMVY: Farklı Mekânlarda Veri Yedekleme
G.O.Analizi: Siber Güvenlik Olaylarının Analizi

Girişimlere güçlü parola ve kimlik doğrulama (Örneğin: minimum 8 karma karakter, maksimum 6 ay süre, şifrelenmiş iletim ve depolama) uygulanıp uygulanmadığı sorulduğunda 200 firma ile büyük oranda uygulandığı görülse de 119 firmanın uygulamadığı Tablo 3.18'de görülmektedir. Ayrıca firmaların %11,6'sının akıllı kartlar gibi donanımlar yardımıyla kullanıcı tanımlama ve kimlik doğrulama kullandığı, %2,4'ünün biometrik yöntemlerle kullanıcı tanımlama ve doğrulama kullandığı izlenmiştir. Firmaların %40'ı farklı mekânlarda veri yedekleme yapmakta ve firmaların %6'sı güvenlik olaylarının analizini gerçekleştirmektedir.

3.3. Kontenjans Tabloları ve Ki-Kare Testleri

Ki- kare testi bağımsız guruplar için iki kategorik değişken arasında bir ilişkinin olup olmadığını test etmek için kullanılmaktadır. Ki-kare testinin varsayım olarak gerekli kıldığı şekilde verilerimiz kategorik değişkenlerden oluşmaktadır. Test ile beklenen frekanslar arasındaki ilişki incelenecektir. İlişkileri incelenecek araştırma hipotezleri aşağıdadır.

H_1: Firmalarda kullanılan firewall cihazlarının varlığı ile ana sunuculara yapılan saldırılar arasında ilişki vardır.

H_1 hipotezi ki-kare testi ile incelendiğinde bir hücrenin beklenen değeri (frekansı) 5 ten küçük olduğunda ki-kare istatistiği yerine Fisher's test istatistiğine ait anlamlılık dikkate alınmıştır. Ki-kare testinde p değeri: 0,021 olarak kaydedilmiştir. Bu nedenle %5 anlamlılıkta istatistiksel olarak Firewall kullanımı ile e-posta saldırısına uğrama arasında ilişki olduğuna karar verilmiştir. Bu nedenle H_0 hipotezi reddedilmiştir. Ki-kare istatistiğine en büyük katkı iki soruya da evet cevabı veren gurupta beklenen değer 4,98 iken gözlemlenen değer 9

olarak kaydedilmiştir. Post hoc verisi ile ilgili 4. hücrenin 3,24 oranında katkı yaptığı[16] hesaplanmıştır. Bu durumda firewall cihazının kullanılmasında, ana bilgisayara yapılan saldırılar beklenenden anlamlı derecede fazla olduğu gözlenmiştir. Firewall'un olması, ana bilgisayara yapılan saldırıları görünür yaptığı unutulmamalıdır.

Tablo 3.19: Firewall Bulunması ve Ana Bilgisayarlara Saldırısı Arasındaki İlişki

			Ana Bilgisayar Saldırı		
			Hayır	**Evet**	**Toplam**
Firewall Kullanımı	**Hayır**	**Gözlem**	147	5	152
		Beklenen Sayı	143,0	9,0	152,0
		% Firewall	96,7	3,3	100
	Evet	**Gözlem**	75	9	84
		Beklenen Sayı	79,0	5,0	84,0
		% Firewall	89,3	10,7	100
Toplam			222	14	236

Tablo 3.19 incelendiğinde firewall kullanan 75 kullanıcının ana bilgisayarına siber saldırı olmazken 9 kullanıcının firewall kullanmasına rağmen siber saldırı ile karşılaştığı gözlenmiştir. Anket verilerinden, ana bilgisayarına saldırı alan firmaların mı firewall kullandığı, firewall kullanan bilgisayarların mı ana bilgisayarına saldırı yapıldığı tespit edilememiştir.

H2: Firmalarda firewall cihazlarının kullanılması ile e-posta saldırıları arasında ilişki vardır.

Tablo 3.20'de ki-kare testinde p değerinin 0,019 olması nedeni ile firmada firewall cihazının bulunması ile e-posta saldırıları arasında istatistiki olarak 0,05'te anlamlı bir ilişki (p=0,019<0,05) olduğu kaydedilmiştir.

[16] Ki-kare istatistiğine katkı: ki-kare istatistiğine $Toplam\ (Gi - Bi)^2 / Bi$ formülü (tahmincisi) ile hesaplanmaktadır. Çapraz kontenjans tabloda her hücre için (beklenen ve gözlenen değerleri ($Gi - Bi)^2/Bi$) skoru hesaplanıp toplanması ile ki-kare istatistiği hesaplandığından her hücre için hesaplanan bu skor ki-kare istatistiğine katkı olarak değerlendirilebilmektedir. Bu da bir çeşit ki-kare için post hoc olarak değerlendirilebilir (Çavuşoğlu ve Pekkaya, 2015:99-100).

Tablo 3.20: Firewall Bulunması ve e-Posta Saldırısı Arasındaki İlişki

			E-posta Saldırısı		
			Hayır	Evet	Toplam
Firewall Kullanımı	Hayır	Gözlem	128	19	147
		Beklenen Sayı	121,6	25,4	147
		% Firewall	87,1	12,9	100
	Evet	Gözlem	59	20	79
		Beklenen Sayı	65,4	13,6	79
		% Firewall	74,7	25,3	100
Toplam			187	39	226

Tablo 3.20'de görüldüğü üzere firewall kullananların %74,7'si e-posta saldırısına uğramazken %25,3'nün saldırıya uğradığı tespit edilmiştir. Ayrıca kurumsal e-posta kullanmayan firma sayısı frekans değerinde 211 olarak kaydedilmiş olduğundan ki-kare testinde kurumsal e-posta kullananlar temel alınarak tekrar hipotez kurulmuştur.

H3: Firmalarda firewall ve kurumsal e-posta kullanan firmaların e-posta saldırılarına uğraması arasında ilişki vardır.

H3'te firewall kullanımı ve kurumsal e-posta kullanan firmaların siber saldırıya uğraması arasındaki ilişki incelenmiştir. Ki-kare testinde p değerinin 0,034 olması nedeni ile kurumsal e-posta ve firewall cihazı kullanımıyla ve e-posta saldırıları arasında istatistiki olarak 0,05 anlamlılıkta bir ilişki ($p=0,034<0,05$) olduğuna karar verilmiştir.

Tablo 3.21: Firewall ve Kurumsal e-Postaya Sahip Firmaların e-Posta Saldırısına Uğraması Arasındaki İlişki

			E-posta Saldırısı		
			Hayır	Evet	Toplam
Firewall Kullanımı	Hayır	Gözlem	50	12	62
		Beklenen Sayı	45,2	16,8	62,0
		% Firewall	80,6	19,4	100
	Evet	Gözlem	28	17	45
		Beklenen Sayı	32,8	12,2	45
		% Firewall	62,2	37,8	100
Toplam			78	29	107

Tablo 3.21'de kurumsal e-posta kullanıp saldırıya uğramayan firma oranı %80,6 iken e-posta saldırısına uğrama sayısı 12 olarak görülmektedir. Ayrıca kurumsal e-posta saldırısına uğramayan ve firewall kullanan firmaların sayısı 28

iken e-posta saldırısına uğrayanlarının sayısı 17 dir. Çalışmadan görüldüğü üzere firewall kullanımı ile saldırılar arasında ilişki kaydedilebilmektedir. Bunun nedeni firewall kullananların saldırıları gözlemleyebilme imkânından da olabilmektedir.

H4: Bilgisayarlarda lisanslı anti virüs kullanımı ile virüs saldırıları arasında ilişki vardır.

Bilgisayarlarda lisanslı anti virüs kullanımı ile bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımların kullanımı arasındaki ilişki incelendiğinde p değeri 0,457 çıktığından (p=0,457>0,05) H0 hipotezi reddedilememiştir. Dolayısı ile analizde bu değişkenler arasında ilişki çıkmamıştır.

H5: Bilgisayarlarda lisanssız anti virüs kullanımı ile virüs saldırıları arasında ilişki vardır.

Bilgisayarlarda lisanssız anti virüs kullanımı ile bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımların kullanımı arasındaki ilişki incelendiğinde p değeri 0,736 çıktığından (p=0,736>0,05) H0 hipotezi kabul edilmektedir. Dolayısı ile analizde bu değişkenler arasında ilişki çıkmamıştır.

H6: Sunucularda lisanslı anti virüs kullanımı ile virüs saldırıları arasında ilişki vardır.

Sunucularda lisanslı anti virüs kullanımı ile bilgisayar virüsleri, Truva atı, solucan gibi zararlı yazılımların kullanımı arasındaki ilişki incelendiğinde p değeri 0,798 çıktığından (p=0,798>0,05) H0 hipotezi reddedilememiştir. Dolayısı ile analizde bu değişkenler arasında ilişki çıkmamıştır.

H7: Sunucularda lisanssız anti virüs kullanımı ile virüs saldırıları arasında ilişki vardır.

Sunucularda lisanssız anti virüs kullanımı ile bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımların kullanımı arasındaki ilişki incelendiğinde p değeri 0,484 çıktığından (p=0,484>0,05) H0 hipotezi reddedilememiştir. Dolayısı ile analizde bu değişkenler arasında ilişki çıkmamıştır.

3.4. Bilişim Yatırımları ve Siber Saldırı Endeksleri

Çalışmada alt başlıklar ile birlikte toplam 78 soru sorulmuştur. Bazı sorular geçiş soruları olarak kullanılmış, analize soru başlıkları dâhil edilmemiş, analiz sürecinde sadece alt başlıklar değerlendirilmiştir. Örneğin C16 sorusuna evet cevabı verenler C16.1, C16.2, C16.3 sorularını cevaplandırdığından C16 analize dâhil edilmemiş, C16.1,2,3 dâhil edilmiştir. Analiz için ankete verilen cevaplar iki grupta değerlendirilirken toplam 54 ana ve alt soru kullanılmıştır. İlgili sorulardan 32 tanesi X bilişim altyapısı için 8 değişken oluşturulmasında ve 18 tanesi Y siber saldırıları için 6 değişken oluşturulmasında, 2 grupta toplam 14 değişken (faktör) endeks skorları üretebilmek için kullanılmıştır. Anket yapılan işletmenin, ilgili konu hakkında ortalama 3-4 soruya verdiği cevaplardan birer endeks oluşturulmuştur. Endekslerin oluşturulmasında uzman görüşleri doğrultusunda her soru derecelendirilerek ve TOPSIS yöntemi kullanılarak firmanın endeksteki skoru hesaplanmıştır.

TOPSIS, çok kriterli karar verme yöntemlerinden olup, sıralama, seçim yapma ve karar verme birimlerinin endekslenmesinde de kullanılan yaygın ve pratik bir yöntemdir. Hesaplama aşamaları aşağıdaki gibi özetlenebilir (Pekkaya ve Başaran, 2011; Pekkaya ve Aktogan 2014:165).

Aşama 1: Hücre elemanları aij olmak üzere karar matrisi (A) hazırlanır. Burada firmalar j=1, 2, 3, …J olup kriterler i=1, 2, 3, …n'dir.

Aşama 2: Ağırlıklı standardize karar matrisi hücre değerleri $v_{ij} = w_i \cdot r_{ij}$ formüllüyle hesaplanarak oluşturulur. Buradaki wi, her bir kriter için ağırlıkları temsil etmekte ve toplamı 1'i vermektedir.

$$r_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{n} a_{ij}^2}} \tag{3.1}$$

Aşama 3: Kriter temelli, firmalar için en çok istenen ideal (A*) ve en istenmeyen negatif ideal (A-) çözümler belirlenir. Buradaki *J* faydayı, *J'* ise maliyeti temsil etmektedir.

$$A^{*} = \{(\max_{i} v_{ij} \mid j \in J), (\min_{i} v_{ij} \mid j \in J')\} \quad (3.2)$$

$$A^{-} = \{(\min_{i} v_{ij} \mid j \in J), (\max_{i} v_{ij} \mid j \in J')\} \quad (3.3)$$

Aşama 4: Her alternatifin, ideal ve ideal olmayan çözüm kümelerinden sapmalar hesaplanır.

$$D_j^{*} = \sqrt{\sum_{i=1}^{n} (v_{ij} - v_i^{*})^2} \quad D_j^{-} = \sqrt{\sum_{i=1}^{n} (v_{ij} - v_i^{-})^2} \quad (3.4)$$

Aşama 5: Her firmanın ideal çözüme bağıl uzaklıkları hesaplanır.

$$C_j^{*} = D_j^{-} / (D_j^{*} + D_j^{-}) \quad (3.5)$$

Aşama 6: İdeal çözüme bağıl uzaklıklara göre endeks skorları hesaplanır. Bu skorlarda X değişkenleri yüksek için en güçlü bileşim yatırımı yapan, Y skorları ise en çok siber saldırıdan etkilenme şiddetini temsil eden skorlardır.

TOPSIS ile oluşturulan skorlar ile X ve Y değişkenleri oluşturulmuştur. Y grubu değişkenler/faktörler; karşılaşılan siber saldırıları, bu saldırılar nedeni ile sistemin devre dışı kalması neticesinde oluşan maddi zararları göstermektedir. X grubu değişkenler/faktörler ise bilişim alt yapısına yapılan yatırımları ve yatırım kapsamındaki tercihleri göstermektedir.

3.4.1. Bilişim Yatırımlarını Gösteren Endeksler

Firmaların öncelikle bilişim alt yapılarının hesaplanacağı değişkenler, özellikle gurup bazında kıyaslamalar ve karşılaştırmalar yapabilmek için X ana grubu değişkenler olarak ifade edilmiştir.

Tablo 3.22: Endeks Hesaplamasında Kullanılan Sorular ve Ağırlıkları (X)

Endeks	Hesaplamada Kullanılan Sorular	Endeksteki Ağırlığı
X1	C1, C2, C3	Eşit Ağırlıkta
X2	C4.1, C4.2, C5	Eşit Ağırlıkta
X3	C7.1, C7.2, C7.3, C10, C14	Eşit Ağırlıkta
X4	C8.1, C8.2, C9.1, C9.2	0,333- 0,167 - 0,333 - 0,167
X5	C11.1, C11.2, C12, C13, C15, C30.1	Eşit Ağırlıkta
X6	C24, C25	0,667 - 0,333
X7	C27.1, C27.2, C27.3, C27.4	Eşit Ağırlıkta
X8	C29.1, C29.2, C29.3, C29.4, C29.5	Eşit Ağırlıkta

Tablo 3.22'de Endeksler ve endekslerin oluşturulmasında kullanılan sorular ile soruların endeksteki ağırlığı görülmektedir. TOPSİS ile endekslerin oluşturulmasında kullanılan ağırlıklar uzman görüşü üzerinden ters reciprocal yöntemi ile hesaplanmıştır (Pekkaya, 2016:976). Ters reciprocal'in formülü Wi = (1/ri) / (∑ (1/ri)) dir. Firmanın yatırımlarını, kaynaklarını ve bilişim alt yapılarını gösteren bağımsız X değişkenlerinin içeriği aşağıdaki gibidir.

X1, Bilgi işlem teknik alt yapısı: Masaüstü bilgisayar, dizüstü, tablet dahil olmak üzere firmadaki bilgisayar sayıları, firmanın internet erişiminin olup olmaması, fiziki ve sanal sunucuların olup olmaması bu bağımsız gurupta değerlendirilmiştir.

X2, Doğrudan bilgi işlem yatırımları: Firmanın bilgi işlem personeli çalıştırması, çalıştırıyor ise çalıştırılan personel sayısı ve 2016 yılı içerisinde firmanın yaptığı harcama bu bağımsız değişken altında toplanmıştır. Ayrıca bilgi işlem personeli dışında alınan dış destek de bu değişken altında değerlendirilmiştir.

X3 Güvenlik duvarı ve IPS-IDS kullanımı: Firmalarının güvenlik bazında veri trafiğinin hareketlerini kontrol etmek için kullandığı ilk yatırımlardan birisi de firewall cihazlarıdır. Piyasa şartlarında ve dilinde kullanılan cihaz özelliklerine göre firewall cihazının açık kaynak kodlu olup olmaması, donanım tabanlı kutu çözüm cihazları ile son zamanlarda özellikle servis sağlayıcıların sağlamış olduğu bulut destekli firewall ürünlerine verilen cevaplar bu kategori altında toplanmıştır.

X4, Anti virüs kullanımı: Yaygın kullanılan bir diğer güvenlik çözümü ise anti virüs yazılımlarıdır. Firmalara bilgisayarlarında ve sunucularında lisanslı ve lisanssız anti virüs yazılımları kullanıp kullanmadığı sorulmuş ve kategori olarak bu başlık altında toplanmıştır.

X5, Web sitesi ve mobil uygulamalar: Firmaların yazılımsal olarak hangi kaynaklara sahip olduklarını öğrenmek için bir takım sorular bu faktörün içeriğindedir. Firmanın web sitesinin ve mobil uygulamasının olup olmaması, web sitesi ve mobil uygulama üzerinden ürün/hizmet siparişi alınıp alınmaması, eğer sipariş alınıyorsa bunun toplam ciro içerisindeki payı bu değişken altında toplanmıştır. Firmanın kurumsal mail sunucu kullanım durumlarına verilen cevaplar da kategoriye dâhil edilmiştir.

X6, SOME birimi: Firma kaynakları içerisinde yeni yeni yerini alan ve bazı firmalar için artık zorunlu hale gelen siber olaylara müdahale ekiplerinin olması ya da kurmayı planlaması bu değişkenimizi oluşturmaktadır.

X7, BİT güvenlik politikası: Güvenlik politikaları neyi, nasıl ve ne şekilde yapacağını gösteren yazılı materyallerdir. Bu nedenle güvenlik politikaları gerek son kullanıcı gerekse ilgili kişilerin siber olay karşısında alacakları aksiyonları belirlemektedir. Firmalara; beklenmeyen bir olay veya saldırı nedeniyle verilerin bozulması ya da kaybolması, başka siteye yönlendirilerek şifre çalınması, istenmeyen güvenli verilerin açıklanması, dışarıdan saldırı nedeniyle BİT hizmetlerinin verilememesi gibi başlıkların güvenlik politikalarında olup olmadığına ait cevaplar bu değişken içeriğindedir.

X8, Politikaların uygulanması: Veri ihlalleri yoluyla 2016 yılında sızan 10 milyon şifrenin analiz edilmesi sonucu birçoğunun 6 karakter ve altında olduğu için çok hızlı olarak kırılabildiği görülmektedir (Tapan, 2017). Zonguldak'ta hangi şifreleme sisteminin yoğun kullanıldığını tespit etmek için firmalara güçlü parola ve kimlik doğrulama (Örneğin: minimum 8 karma karakter, maksimum 6 ay süre, şifrelenmiş iletim ve depolama) kullanılma durumu, donanımsal ya da biometrik şifre kullanılma durumları sorularak gelen cevaplar bu değişken içeriğini oluşturmaktadır.

3.4.2. Firmaların Uğradıkları Siber Saldırılardan Etkilenme Şiddetlerini Gösteren Endeksler

Dünya çapındaki internet trafiğinin ve siber tehditlerin izlenmesine olanak veren bazı platformlar, günümüzde dünyada haftada ortalama 124 bin, Türkiye'de ise haftada 18 bin saldırı gerçekleştiğini rapor etmektedir (Kara, 2016). Güvenlik şirketlerinden Trendmicro' verilerine göre Türkiye'de en çok karşılaşılan beş siber saldırı çeşidinin mobil saldırılar, DDoS saldırıları, kredi kartı dolandırıcılığı, oltalama saldırıları ve fidye yazılımları yoğun olduğu görülmektedir (Terzioğlu, 2016). Bu kapsamda firma düzeyinde yapılan ankette karşılaşılan siber saldırılar ile ilgili bir takım sorular sorulmuştur.

Özellikle ilde karşılaşılan saldırılardan genel bir endeks oluşturmak amacı ile YY değişkeni oluşturulmuştur.

Tablo 3.23: Endeks Hesaplamasında Kullanılan Sorular ve Ağırlıkları (Y)

Endeks	Hesaplamada Kullanılan Sorular	Endeksteki Ağırlığı
Y1	C16.1, C16.2, C16.3	0,200 - 0,400 - 0,400
Y2	C17.1, C17.2, C17.3	0,200 - 0,400 - 0,400
Y3	C18.1, C18.2, C18.3	0,200 - 0,400 - 0,400
Y4	C19.1, C19.2, C19.3	0,200 - 0,400 - 0,400
Y5	C20.1 C20.2 C20.3	0,200 - 0,400 - 0,400
Y6	C28.1, C28.4, C28.5	0,333 – 0,333 – 0,333
YY	Y1,Y2,Y3,Y4,Y5,Y6	Eşit Ağırlıkta

Tablo 3.23'de endeksler ve endeks hesaplamasında kullanılan sorular ve ağırlıkları görülmektedir. Buradaki ağırlıklarda TOPSİS yöntemi ile hesaplanan endekslerde kullanılmış ve uzman görüşleri üzerinden ters reciprocal yöntemi ile elde edilmiştir. Y grubu değişkenler, siber saldırı tipi olarak farklılık gösterse de firmaların ilgili saldırıya ne kadar maruz kaldığı, sistemlerin olası devre dışı kalma süresi ve bu saldırılar neticesinde karşılaşılan maddi zararlar ile ilgili sorular faktörün/değişkenin içeriğini oluşturmaktadır.

Y1, Mobil uygulamalara yapılan siber saldırılar: Mobil uygulamalara ya da web sitesine yapılan siber saldırılar ve bu saldırılar ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

Y2, E-posta ile yapılan siber saldırılar: Günümüzde birçok saldırının aracı olarak görülen e-posta yoluyla saldırıya uğrama ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

Y3, Ana bilgisayara yapılan siber saldırılar: Kritik bilgileri taşıyan ana bilgisayarlara yapılan saldırılar ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

Y4, Virüs solucan vb siber saldırılar: Bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımlar ile çalışanlardan kaynaklı (şifresini başkasına verme, başkasının şifresini kullanma, dikkatli davranmama gibi) nedenlerden dolayı karşılaşılan siber saldırılar ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

Y5, Oltalama siber saldırıları: Firmaların, oltalama (phishing) saldırıları veya sosyal mühendislik olarak tabir edilen telefon ya da e-posta ikna yöntemleriyle saldırıya uğrama durumları ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

Y6, BİT güvenliği: Direk olarak siber saldırı olmasa da gerek siber saldırı sonucu olarak gerekse donanımsal nedenler ile veri kaybı yaşanması, veri kaybının neden olduğu maddi zarar bu grubu oluştururken ayrıca donanım veya yazılım hataları nedeniyle verinin bozulması ya da kaybolması sonucunda BİT hizmetlerinin verilememesi, istenmeden güvenli verilerin elektronik ortamda açıklanması, kötü amaçlı yazılım veya yetkisiz erişim nedeniyle verinin bozulması veya kaybolması gibi nedenler ile ilgili firmanın cevapları bu değişken içeriğini oluşturmaktadır.

3.5. Korelasyon Analizi

Buradaki korelasyon matrisi, araştırmada endekslenerek dikkate alınan tüm değişkenleri içeren matristir. Tüm endekslenerek oluşturulan bağımsız değişkenler arasındaki doğrusal ilişkinin yönünü ve kuvvetini belirtmektedir. Korelasyon tablosu Tablo 3.24'de görülmektedir.

Korelasyon katsayısı için 0 - 0,4 arası zayıf ilişkiyi, 0,4 - 0,6 arası orta düzeyde bir ilişkiyi, 0,6 – 0,8 arası yüksek düzeyde bir ilişkiyi, 0,8 - 1 ise çok yüksek düzeyde bir ilişkiyi gösterdiği söylenebilir (Pekkaya ve Akıllı, 2013).

Tablo 3.24: Değişkenler Arasındaki Korelasyon Matrisi

	Y1	Y2	Y3	Y4	Y5	Y6	X1	X2	X3	X4	X5	X6	X7
Y2	,028												
Y3	,086	-,011											
Y4	-,007	,527**	,000										
Y5	-,009	-,014	-,013	-,007									
Y6	-,007	-,001	,199**	,018	-,007								
X1	,001	,000	,001	-,006	,005	-,004							
X2	-,005	-,003	-,006	-,002	,000	-,004	,995**						
X3	,039	,033	,174**	-,029	,180**	-,017	,092	,075					
X4	,069	-,036	,092	-,055	,055	,059	,088	,043	,367**				
X5	-,020	,020	,016	-,011	-,018	,035	,398**	,394**	,419**	,162**			
X6	,047	-,018	,374**	-,010	,057	-,011	,494**	,486**	,258**	,093	,200**		
X7	,033	-,024	,311**	-,010	,204**	,082	,006	,011	,379**	,200**	,117*	,173**	
X8	,047	,015	,327**	-,003	,078	,085	,012	,003	,343**	,144**	,233**	,178**	,355**

Not: ** 0,01 anlamlılık düzeyi

Bağımsız değişkenler arasındaki korelasyonlar incelendiğinde, en yüksek ilişki seviyesinin 0,995 pearson korelasyon skoruna sahip bilgi işlem teknik alt yapısı (X1) ile doğrudan bilgi işlem yatırımları (X2) arasında olduğu istatistiksel olarak %1 anlamlılık düzeyinde gözlemlenmektedir. Diğer korelasyon değerleri incelendiğinde tüm değişkenlerin bu rakamın altında kaldığı görülmektedir. Ancak bu durumunun beklenen bir durumdur.

E-posta yoluyla siber saldırıya uğranılması (Y2) ve bilgisayar virüsleri, truva atı, solucan gibi zararlı yazılımlar ve çalışanlardan kaynaklı (şifresini başkasına verme, başkasının şifresini kullanma, dikkatli davranmama gibi) nedenlerden dolayı (Y4) siber saldırıya uğranılması arasında 0,527 düzeyinde pozitif yönlü anlamlı bir ilişki vardır. Buradan da anlaşıldığı üzere firmaların e-posta saldırılarına uğraması ile virüsler ve türevlerinin orta kuvvette bir ilişkisi gözlenmektedir.

Ana bilgisayara yapılan siber saldırılar (Y3) ile bilgi işlem teknolojisinin güvenliği (Y6) arasında istatistiki olarak 0,01 anlamlılıkta 0,199 skor ile zayıf

sayılabilecek bir ilişki olduğu görülmektedir. Çoğunlukla donanımsal veri kayıplarının harddisk arızalarından kaynaklandığı bilinmektedir. Özellikle sunucu yapılarında kullanılan güvenliğe dayalı raid[17] yapıları nedeni ile firmaların her türlü disk arızasından veri kaybı olarak etkilenmemesi sistemin kullanıcıyı uyararak disk değişimine zaman tanımasının veri kaybını önlemede etkili olduğu tahmin edilmektedir.

Firmaların firewall ve IPS - IDS kullanmalarındaki tutum (Y3) ile ana bilgisayarlara yapılan saldırılar (X3) düzeyinde 0,174 oranında zayıf bir ilişki olduğu görülürken özellikle direk saldırıyı engelleme nedeni ile firmada bulunan SOME birimlerinin (X4) arasındaki ilişki 0,374 skorla daha kuvvetli gözlenmiştir. Ana bilgisayarlar açıkları ve hatalı yapılandırılmaları nedeni ile siber saldırıya uğrayabilirler (CNNTÜRK, 2017). Fakat bilgisayarların birinde bulunan bir açık ya da yapılandırma hatası nedeni ile de saldırılar ana bilgisayara ulaşabilmektedir. Firmalar çoğunlukla bu duruma dikkat çekmek için güvenlik politikaları oluştururlar (X7) ve bu politikaların uygulanmasını isterler (X8) (SANS, 2013). Ana bilgisayarlara yapılan siber saldırılar ile X7 arasında 0,311 düzeyinde, politikaların uygulanmasını konu alan X8 ile de 0,327 düzeyinde bir ilişki olduğu gözlenmektedir.

Firmaların firewall kullanımının (X3) oltalama (phishing) saldırıları (Y5) ile ilişki durumu incelendiğinde 0,180 skorla zayıf düzeyde ilişkili olduğu kaydedilmiştir. Oltalama saldırıları yapılabilmesi için öncelikle personelin kandırılması ayrıca kişinin bilgilerinin ele geçirilmesi gerekmektedir (SANS, 2013). Bu nedenle iki aşamalı olan bu saldırının firewall sadece bir kısmında etkili olmaktadır. Bilgi işlem güvenlik politikaları oluşturmanın (X7) oltalama saldırıları (Y5) ile zayıf ama ilişkili olduğu 0,204 skorundan anlaşılmaktadır. Özellikle iyi hazırlanmış ve personel tarafından özümsenmiş bir güvenlik politikasının etkisinin oltalama saldırılarında oldukça etkili olduğu tahmin edilmektedir (SANS, 2013).

Firmanın web sitesinin ve mobil uygulamasının olup olmaması, web sitesi ve mobil uygulama üzerinden ürün/hizmet siparişi alınıp alınmamasının (X5) bilgi

[17] Raid, çeşitli nedenlerle bozulabilen harddisklerdeki kritik veri kayıplarını önlemek yada azaltmak için geliştirilmiş, farklı ihtiyaçlara göre konfigüre edebilen yapısal özelliktir (CHIP, 2009).

işlem teknik alt yapısına yapılan yatırımlar ile ilişkili olduğu 0,398 skoru ile bulunmuştur. Bilgi işlem alt yapısına önem veren firmaların aynı zamanda mobil uygulamalara ve web sitelerine yöneldiği ancak bu ilişkinin şiddetinin zayıf olduğu gözlenmektedir. Bilgi işlem biriminde yapılan yatırımlar ile SOME birimine yapılan yatırımlar arasındaki ilişki incelendiğinde ise orta düzeyde 0,494 skorla pozitif yönlü ilişkili olduğu görülmektedir.

Bilgi işlem teknik alt yapısı (X1) ile doğrudan bilgi işlem yatırımları arasındaki ilişkinin (X2) çok yüksek oranda olması nedeni ile X'in ilişkili olduğu diğer değişkenler ile X2 arasındaki ilişkinin yaklaşık olarak aynı olduğu görülmektedir. X2 ile X5 arasında 0,394 düzeyinde ve X2 ile X6 arasında 0,486 düzeyinde pozitif yönlü anlamlı ilişkili olduğu değerlendirilmektedir.

Güvenlik duvarı ve IPS-IDS kullanımı ile diğer yatırımların ilişkili olduğu izlenmektedir. Bilişime yatırım yapan firmaların çoğunlukla firewall satın aldığı yada firmaların bilişim yatırımlarına belirli oranlarda yatırım yaptığı tahmin edilmektedir. Korelasyon matrisinden de görüldüğü üzere X3 ün X4 ile 0,367 skorla X5 ile 0,419 skorla, X6 ile 0,258 skorla, X7 ile 0,379 skorla istatistiksel olarak 0,01'de pozitif yönlü anlamlı bir ilişkinin olduğu bulunmuştur.

Anti virüs yatırımı ile diğer yatırım değişkenleri arasındaki ilişkiler incelendiğinde X4 ile X5 arasında 0,162 skorla, X7 ile 0,200 skorla, X8 ile 0,233 skorla pozitif yönlü anlamlı ancak zayıf bir ilişkiye sahip olduğu ancak SOME birimi yatırımı olan X6 ile istatistiki olarak 0,01'de anlamlı bir ilişkinin olmadığı belirlenmiştir.

Web sitesi ve mobil uygulama yazılımlarına yatırım (X5) yapan firmaların, SOME yatırımları (X8), bilgi teknolojileri güvenlik politikaları (X7) ve bu politikaların uygulanmasının gruplandığı değişkenler ile ilişkili olduğu gözlenmiştir. X5 ile X6 arasında 0,200 skor ile X7 ile 0,117 skorla X8 ile 0,233 skor ile istatistiki olarak 0,01'de pozitif yönlü anlamlı bir ilişki olduğu görülmektedir.

SOME birimi olan firmaların (X6) genellikle ilk olarak hazırlayıp kaydettikleri bilgi işlem güvenlik politikaları (X7) ile 0,173 skorla ve bu

politikaların uygulanması (X8) ile ise 0,178 skorla istatistiki olarak pozitif yönlü anlamlı bir ilişki olduğu gözlemlenmiştir.

Bilgi işlem teknolojileri güvenlik politikasının oluşturulması (X7) ve bu politikanın uygulanması (X8) arasındaki ilişki incelendiğinde 0,355 skorla istatistiksel olarak 0,01'de pozitif yönlü anlamı bir ilişki bulunmuştur.

3.6. Yapılan Yatırımların Siber Saldırılar Üzerindeki Etkisi

En küçük kareler yöntemi (EKK), basit doğrusal, çoklu regresyon modellerinin çözümlenmesinde kullanıldığı gibi, çok denklemli ekonometrik modellerde de kullanılan tekniklerden biridir. Yapılan regresyon analizinde EKK'nin varsayımlarından özellikle değişen varyans ve normal dağılım sağlamadığı, değişen varyans problemi çözümlendiğinde ise model anlamlılığı ve yapısı bozulduğundan analiz bulguları burada raporlanmamıştır. İstatistiksel çözümlemelerde EKK yöntemi, matematiksel işlemlere en uygun tahmin yöntemi olarak kullanılmasına rağmen varsayımların karşılanmasına karşı direncinin zayıf olmasından dolayı eleştirilmektedir ve bununla birlikte alternatif daha güçlü yöntemler önerilmektedir (Neter vd., 1996 alıntı Gürünlü ve Vupa, 2008:220). Değişen varyans sorunu çözülerek (White yöntemi) yapılan regresyon analizinde BİT güvenlik politikası (X7) anlamlı (p değeri 0,044) çıktığı gözlenmiştir. Bu durumda BİT güvenliğine yapılan yatırımların siber saldırıları pozitif yönde etkilediği sonucuna varılabilir. Ancak (X7) değişkeni için gözlem sayısı ve ilişki içeriği kontrol edildiğinde, bu bulguların yorumlamaya açıklığı açısından araştırmacılar için sonucun anlamlı çıkmamasından dolayı regresyon modeli bulgularına yer verilmemiştir.

3.7. Bilişim Yatırımları ve Siber Saldırıların Firma Özelliklerine Göre Farklılaşması

Bu bölümde endekslenerek oluşturulan değişken skorlarının firmaların bazı özelliklerine göre ne ölçüde farklılaştığı incelenmiştir.

H_8: E-posta saldırısına uğrayan firmaların teknik alt yapısı farklıdır.

Tablo 3.25: Teknik Alt Yapıdaki Farklılık

E-posta Saldırısı	N	X	SS	Sd	t	p
Yok	187	,6609	,35561	38,008	-1,032	,309*
Var	39	3,2871	15,89838			

*p>0,05

Firmalara yapılan e-posta saldırılarının firmaların yapmış olduğu teknik alt yapıya etkisinin incelendiği Tablo 3.25'te p değerinin 0,309 olduğu ve 0,05'ten büyük olduğundan dolayı firmaların teknik alt yapısının oluşturulmasında firmaların e-posta saldırıları ile karşılaşıp karşılaşmaması arasında istatistiksel olarak 0,05'te anlamlı bir fark olmadığına karar verilmiştir.

H9: Güvenlik politikalarının olması firmaların bilişim yatırımları ya da siber saldırılardan etkilenme endekslerini farklılaştırmaktadır.

Firma cevaplarının frekans değerleri incelendiğinde, firmalarda resmi olarak tanımlanmış ve düzenli olarak gözden geçirilen planlı bir bilgi ve iletişim teknolojisi güvenliği politikası kullanmayanların sayısının 306 birimden oluştuğu ve bu açıdan merkezi limit teoremine göre verilerin normal dağıldığı kabul edilmiştir. BİT Güvenlik politikasının 13 birimde olmasından dolayı verilerin normal dağılımları Kolmogorov-Smirnov (Lilliefors düzeltmeli) ve Shapiro-Wilk testi ile incelenmiştir. Firmada resmi olarak tanımlanmış ve düzenli olarak gözden geçirilen planlı bir bilgi ve iletişim teknolojisi var diyenlerin hiç birinin normal dağılımı sağlamadığı %5 anlamlılık düzeyinde gözlemlenmiştir. Bu durumda gruplar arasındaki fark nonparametrik test olan Mann-Whitney U testi ile incelenmesine karar verilmiştir.

Tablo 3.26 incelendiğinde (Y6) hariç tüm seçenekler için istatistiksel olarak 0,05 anlamlılıkta H0 hipotezinin doğru olduğuna karar verilmiştir. Firmaların yaptıkları yatırımlar ve karşılaşılan siber saldırılar açıcından güvenlik politikaların olup olmaması arasında fark yoktur.

Tablo 3.26: BİT Güvenlik Politikasının Olup Olmamasının Siber Saldırılar ve Yatırımlar Açısından Fark Oluşturma Durumu

	BİT Güvenlik Politikası		K-S	S-W	t testi	Mann-Whitney U
	Yok (n=306)	Var (n=13)				
YY	,5218	,5104	,000	,000	,988	,643
Y1	,5214	,0000			,735	,468
Y2	1,1486	,1002	,000	,000	,595	,222
Y3	,6879	,4509	,000	,000	,901	,484
Y4	,4943	,2162	,000	,000	,844	,756
Y5	,4061	,0098	,000	,000	,736	,946
Y6	,3268	1,5385	,000	,000	,368	,010
X1	,9726	,6841	,000	,000	,855	,471
X2	,5499	,2161	,000	,000	,834	,340
X3	11,8299	14,7669	,015	,011	,572	,367
X4	26,1085	35,6492	,005	,009	,059	,167
X5	2,3435	3,5940	,000	,000	,491	,630
X6	1,4006	,0000			,612	,509
X7	2,8122	1,2979	,000	,000	,729	,527
X8	7,2963	8,1567	,000	,000	,832	,905

K-S : Kolmogorov-Smirnov (Lilliefors düzeltmeli)
S-W: Shapiro-Wilk

Tablo 3.26'ya göre (Y6) için H_0 hipotezi reddedilerek firmanın siber saldırıları ile karşılaşması açısından bir firmada resmi olarak tanımlanmış ve düzenli olarak gözden geçirilen planlı bir bilgi ve iletişim teknolojisinin olması ile olmaması arasında fark olduğu görülmüştür. Güvenlik politikaları olan firmaların değerinin ortalaması 1,5385, güvenlik politikaları olmayan firmaların değerinin ortalaması ise 0,3268 olduğundan güvenlik politikaları olan firmalar için (Y6) daha yüksek skorlandığı söylenebilir.

H_{10}: Firmanın bilgi işlem personeli çalıştırması firmaların bilişim yatırımları endekslerini farklılaştırmaktadır.

Sorunun frekans değerleri incelendiğinde bünyelerinde bilgi işlem birimi bulundurmayan firmalar 280 birim ve bilgi işlem birimi bulunduran 32 birimden oluştuğundan dolayı merkezi limit teoremine göre 30'dan büyük hacimde olmaları nedeniyle verilerin normal dağıldığı kabul edilir.

Tablo 3.27: Bilgi İşlem Personeli Varlığının Firmanın Bilişim Endekslerindeki Oluşturduğu Fark

B.İ.Y.	Yok (n=280)	Var (n=32)	t-testi
X3	9,6488	32,0029	,000
X4	24,6292	43,8338	,000
X5	1,4861	8,6907	,001
X6	1,1735	3,1250	,484
X7	1,4372	10,4296	,98
X8	6,3502	15,6453	,009

B.İ.Y: Bilgi İşlem Yatırımları

Tablo 3.27'de firmaların bünyesinde bilgi işlem personelinin varlığının firmanın bilişim yatırımları endekslerindeki farklılaşması araştırılmıştır. Tablo 3.27'ye göre bünyesinde bilgi işlem personeli çalıştıran firmalar ile çalıştırmayan firmaların yapmış oldukları bilgi işlem yatırımları arasında fark incelendiğinde X3, X4, X5, X8 için %5 anlamlılık düzeyinde istatistiki olarak fark olduğu görüldüğü için H_0 hipotezi reddedilmiştir. X6, X7 için ise %5 anlamlılık düzeyinde istatistiki olarak fark olmadığına karar verilmiştir. Sonuç olarak anket verilerine göre bilgi işlem personeli istihdam eden firmaların güvenlik duvarı, lisanslı anti virüs yatırımları, web sitesi ve mobil uygulamalar için oluşturulan güvenlik tedbirleri ve firmaların bilgi güvenliği politikalarının uygulanması, bilgi işlem personeli istihdam etmeyen firmalara göre daha fazla yatırım yaptıkları (endekslerin daha yüksek olduğundan) gözlenebilmektedir.

Sonuçtan anlaşıldığı üzere firmalar bilgi işlem personeli istihdam ettiklerinde diğer bilgi işlem yatırımlarını da yapmaktadırlar. Dolayısı ile bilgi işlem personeli çalıştıran firmalar saldırıların anlaşılmasına katkı sağlayan donanım ve yazılımları aldığından siber saldırıya uğradığını da anlayabilmektedir. Ayrıca siber saldırının önlenmesine yardımcı olacak diğer araçlara da yatırım yapmaktadır. Ancak son birkaç yıl içerisinde yaygınlaşan SOME biriminin oluşturulmasında bilgi işlem personelinin istihdam edilip edilmemesi arasında fark olmadığı da görülmüştür.

H_{11}: Bilgi işlem hizmetleri için dış destek alan firmaların yapmış olduğu bilgi işlem yatırımları ile dış destek almayan firmaların yapmış olduğu yatırımlar arasında fark vardır.

Sorunun frekans değerleri incelendiğinde bünyelerinde bilgi işlem birimi bulundurmayan firmalar 98 birim ve bilgi işlem birimi bulunduran 221 birimden oluştuğundan dolayı merkezi limit teoremine göre normal dağıldığı kabul edilmiştir. Bulgular Tablo 3.28'de incelenmiştir.

Tablo 3.28: Dış Destek Alınması ile Alınmamasının Yatırımların Yapılmasında Oluşturduğu Fark

B.İ. Y.	Yok (n=98)	Var (n= 221)	t-testi
X1	,5265	1,1448	,362
X2	0,286	,7600	,284
X3	7,7049	13,5245	**,004**
X4	21,4941	28,3310	**,001**
X5	1,7561	2,3841	,364
X6	,4373	1,7453	,110
X7	,8728	2,9440	,116
X8	4,6585	8,2752	**,006**

B.İ.Y.: Bilgi işlem Yatırımları

Tablo 3.28 incelendiğinde dış destek alan firmaların güvenlik duvarı, IPS/IDS yatırımları, anti virüs yatırımları, güvenlik politikaların uygulanması ile dış destek almayan firmalar (yok) arasında %5 anlamlılık düzeyinde istatistiki olarak fark olduğu görüldüğünden X3, X4 ve X8 için H_0 hipotezi reddedilmektedir. Çalışmada firmalar dış destek almaları firmaların yapmış oldukları teknik alt yapı, doğrudan bilgi işlem yatırımları, web sitesi ve mobil uygulama güvenlikleri, siber olaylara müdahale ekipleri, BİT güvenlik politikaların hazırlanmasında fark oluşturmadığına karar verilmiştir. Bu nedenle X1, X2, X5, X6, X7 yatırımları için H_0 hipotezi istatistiki olarak 0,05'te reddedilememiştir. Bu durumda dış destek alan firmaların bileşim yatırımlarının daha fazla olduğu söylenebilir.

H_{12}: Firmaların bilgisayarlarında lisanssız anti virüs çalıştırması, firmaların karşılaştıkları siber saldırı endekslerini farklılaştırmaktadır.

Soru ile ilgili frekans değerleri incelendiğinde bilgisayarlarında lisanssız anti virüs bulundurmayan firmalar 220 birim ve bilgi işlem birimi bulunduran 82 birimden oluştuğundan dolayı merkezi limit teoremine göre normal dağıldığı kabul edilmektedir. Bulgular Tablo 3.29'da raporlanmıştır.

Tablo 3.29: Bilgisayarlarında Lisanssız Antivirüs Kullanan Firmaların e-posta Saldırıları Almasındaki Fark

Siber Saldırılar	Kullanmıyorum*	Kullanıyorum**	t-testi
Y1	,6274	,2342	,702
Y2	,9713	,0006	,026
Y3	,1864	,0000	,031
Y4	,0487	,0438	,941
Y5	,7921	,0033	,583
Y6	,1282	,0000	,742

*Lisanssız anti virüs kullanmıyorum 228 birim
**Lisanssız anti virüs kullanıyorum 82 birim

Tablo 3.29'da bilgisayarlarında lisanssız antivirüs kullanan firmaların e-posta saldırıları alması ve lisanssız anti virüs kullanmayan firmaların aldığı e-posta saldırıları arasında istatistiki olarak %5 anlamlılıkta fark olduğu görülmektedir. Ayrıca bilgisayarlarında lisanssız anti virüs kullanan firmaların ana bilgisayarlarına yapılan siber saldırılar ile lisanssız anti virüs kullanmayan firmaların ana bilgisayarlarına yapılan siber saldırılar arasında istatistiki olarak %5 anlamlılıkta fark olduğu görülmektedir. Bu nedenle (Y2) e-posta saldırıları ve (Y3) ana bilgisayarlara yapılan siber saldırılar için H_0 hipotezi reddedilir. Bu durumda lisanssız anti virüs kullanmayan firmaların Y2 ve Y3 tipi siber saldırılara daha az maruz kaldıkları söylenebilir.

Diğer siber saldırılar olan ve Tablo 3.29'da verilen Mobil Uygulamalara yapılan siber saldırılar (Y1), Virüs solucan ve turuva atı şeklinde yapılan siber saldırlar (Y4), Oltalama saldırıları (Y5), BİT güvenil saldırıları (Y6) için lisanssız anti virüs kullanıp kullanmamaları arasında istatistiki olarak anlamlı bir fark bulunmadığından ($p>0,05$) H_0 hipotezi reddedilememiştir.

Yapılan t-testi sonucunda hipotezi reddedilen Y2 ve Y3 değişkenlerinin ortalama değerleri incelendiğinde Y2 için kullanmıyorum 0,9713 iken kullanıyorum 0,0006 ortalamasına sahiptir. Ayrıca Y3 için ortalama değerler incelendiğinde kullanmıyorum 0,1864 birim iken kullanıyorum ,0000 birim ortalamaya sahiptir. Buna göre lisanssız anti virüs kullanmayan firmaların ana bilgisayar saldırısına uğrama düzeyi lisanssız anti virüs kullanan firmaların ana bilgisayar saldırısına uğrama seviyesinden daha yüksektir. Aynı şekilde diğer sonuçta incelendiğinde lisanssız anti virüs kullanmayan firmaların e-posta saldırılarına uğrama düzeyi lisanssız anti virüs kullanan firmaların e-posta

saldırılarına uğrama düzeyinden daha yüksek olup istatistiki olarak anlamlı değillerdir.

H_{13} Firmaların farklı mekânlarda veri yedeklemesi ana bilgisayar saldırıları endekslerini farklılaştırmaktadır.

Hipotezde geçen sorularda ilişkin frekans analiz verileri incelendiğinde, firma verilerini farklı mekanlara yedekleyenler 135 birimden oluşurken yedeklemeyenler ise 183 birimden oluşmaktadır. Veriler incelendiğinde normal dağıldığı görülmektedir. Bulgular Tablo 3.30'da raporlanmıştır.

Tablo 3.30: Uzak Yedeklemenin Ana Bilgisayar Saldırı Farklılığı

Uzak Yedekleme	N	X	SS	Sd	t	p*
Yok	183	,0449	,42016	147,238	-1,998	,082
Var	135	,2958	1,62755			

*p<0,05

Tablo 3.30'da p değerinin 0,082 bulunmasından dolayı farklı mekânlara veri yedeklendiği zaman ana bilgisayarlara yapılan siber saldırıların görülmesi ile uzak mekânlara yedeklenmediğinde ana bilgisayara yapılan saldırıların görülmemesi arasında %5 anlamlılık düzeyinde istatistiki olarak anlamlı bir fark olmadığına karar verilmiştir. Yani H_0 hipotezi reddedilemez. Ancak bu durum 0,10 anlamlılıkta incelenirse farklılığın varlığı istatistiki olarak zayıf olarak kabul edilmektedir.

SONUÇ

Her geçen gün artan siber saldırıların birden çok etkisi görülmektedir. Yapılan teorik ve pratik çalışmalar siber saldırıların sadece mühendislik olarak değil diğer bilimler tarafından da incelenmesi gerektiğini göstermiştir. Kişilere, kurumlara ve devletlere itibar ve veri kaybı yaşatan siber saldırıların en büyük zararlarından biri de hiç şüphesiz ekonomik kayıplardır. ABD'de bulunan Ulusal Siber Güvenlik Birliği verilerine göre siber saldırı nedeni ile mağdur olan orta ve küçük ölçekli şirketlerin %60'ının mağduriyet yaşamasından sonraki 6 ay içerisinde iflas ettiği tespit edilmiştir (İHS, 2016a). Gelişen teknolojinin de bir sonucu olarak suç ekonomisinin oluşmasında bilişim teknolojisinin yoğun olarak kullanılması, tüm dünyada yaygın bir mağdur kitlesi oluşturmaktadır. Bilişim yolu ile gerçekleşen saldırıların anlaşılması güç olduğundan çoğu kez kişiler suçun mağduru olduklarını fark etmemektedir.

Siber saldırıların etkilerinin suç ekonomisi çerçevesinden irdelendiği bu çalışma Zonguldak ilinde siber saldırılardan kaynaklı ekonomik zararların ölçülmesi amacı ile yapılmıştır. Siber saldırıların ekonomik büyüklüğünün kaydedildiği bir kurum olmadığı için veriler anket uygulaması yolu ile elde edilmiştir. Anket, alt yapı ve teknik yeterlilik düşünüldüğünde siber saldırılar ile daha çok karşılaşma ihtimalinden dolayı firmalara uygulanmıştır. Araştırma için anket çalışması 2016 yılı ile sınırlı olmak üzere Zonguldak ilinde bulunması ve 20'den fazla personel çalıştırması kısıdında 336 firmaya, TÜİK Zonguldak Bölge Müdürlüğü tarafından uygulanmıştır.

Bu kısıtlar çerçevesinde anket verileri genel olarak incelendiğinde ekonomik zararların beklenilenden düşük geldiği görülmüştür. Bu çalışmaya başlanmasında etkili olan gerek birebir görüşmeler gerekse ön anket raporları daha büyük bir mağdur kesime işaret etmekteydi. Ancak firmaların uğradıkları siber saldırıları kaydetmesine yarayan ağ cihazlarının yetersiz olması ve firmaların kaydedilmeyen verileri vermek istememeleri, anket verilerindeki mağduriyet oranını düşürmüştür. Ayrıca firmalar itibar kaybı yaşayacağını düşündükleri için uğradıkları siber saldırıları aksettirmek istememektedir. Diğer bir etken ise firmaların karşılaştıkları siber saldırılardan doğan mağduriyeti anlayamamış olmalarıdır. Firmalar yeterli düzeyde bilgi işlem konularında yetkin insan kaynağı çalıştırmadıklarından

karşılaştıkları siber saldırılar maddi zarar verse bile çok fazla anlaşılamamaktadır. Firmalar ile yapılan ikili görüşmelerde, mağduriyetin sanki doğal bir olaymış gibi algılandığı tespit edilmiştir. Bir diğer etken ise çalışmanın 2016 yılı ile kısıtlı olmasıdır. Firmalar 2016 yılı içerisinde mağduriyet yaşamamasına rağmen, 2014 – 2015 yıllarında mağduriyet yaşamış olabilmektedir. Bu gibi nedenler ile siber saldırı sayıları ve yaşanan maddi zararlar olduğundan daha az kaydedilmesine ilişkilendirme modellerinin daha zayıf olmasına neden olmuştur.

Anketten elde edilen verilere göre firmaların bilişim ağında 10 bilgisayar ya da daha düşük donanım bulunduğu kaydedilirken firmaların yarıya yakınının bilişim ağında en az bir adet sunucu bulunmaktadır. Zonguldak ilindeki firmaların network yapısına bakıldığında ise çok büyük olmadığı görülmektedir. Firma görüşmelerinden ve örneklemdeki verilerden elde edilen bilgiler ışığında sunucu sayısının az olması daha çok muhasebe kayıtlarının yerelde tutulduğunu, diğer bilişim ihtiyaçların ise daha çok firma dışından karşılandığını göstermektedir.

Çalışmada firmaların kendi bünyesi içerisinde ya da dış dünya ile iletişiminde kurumsal e-posta kullanımının oldukça az olduğu görülmektedir. Bu durumun e-posta üzerinden saldırıya uğrama oranlarına da yansıdığı düşünülmektedir. Ayrıca ilimiz genelinde büyük sayılabilecek firmaların %42'sinin web sitesinin olmaması şaşırtıcı bir durum olarak karşımıza çıkmıştır.

Çalışmada firmaların sadece %4,8'inin mobil uygulama kullanması teknolojik yatırımların değerlendirilmesi açısından kayda değer bir durumdur. Mobil yatırımlar web sitesine oranla daha maliyetli gözükebilir. Ancak yatırım yapıldıktan sonra içerik yönetim yazılımları sayesinde uzun vadede bu maliyet azalmaktadır. E-ticaretin her geçen gün büyüdüğü yeni ve çok büyük cirolu şirketlerin doğduğu, ticaretin sınırlarının tekrar çizildiği yeni dünyada Zonguldak ilindeki firmaların %67'sinin henüz e-ticaret yapmadığı kaydedilmiştir. Bu durum irdelenmesi gereken diğer bir konu olarak gözükmektedir.

Firmaların anti virüs kullanımları incelendiğinde büyük oranda bilgisayarlarında anti virüs kullandığı % 67,9 oranla kaydedilmiştir. Ayrıca birçok şirkette mahrem kabul edilen bilgilerin bulunduğu sunucularında anti virüs kullanım oranı %41,1 olarak tespit edilmiştir.

Firmalardan %27,4'ü firewall kullanırken, bu firmaların %30,2'si açık kaynak kodlu, %43,8'i kutu çözüm güvenlik duvarı kullandığı örneklemden görülmektedir. Firmaların gelen ve giden trafiğini organize ve kontrol eden bu cihazların ayrıca kullanıcı hareketlerini loglama özellikleri de bulunmaktadır. Ülkemizde 5651 sayılı yasaya göre log tutulması ve elektronik olarak imzalanması zorunludur. Bu nedenle firewall kullanmayan firmaların başka çözümleri yok ise farkındalığının artırılması gerekmektedir.

Anketteki ilgili bölüme cevap veren firmaların %9,5'inin bilgi işlem birimi bulunmaktadır. Örneklemde bilgi işlem hizmetini dışarıdan aldığını belirten firmaların oranı ise % 65,8 olarak kaydedilmiştir. Firmaların maliyetleri indirmek için dış destek aldıkları görülmektedir. Ancak firma içerisinde alanında uzman bir kişi bulunmaz ise ya da alınan dış destek hizmeti kapsamında personel firma içerisinde istihdam edilmez ise siber güvenlik açıklarının görülebilmesinin çok kolay olmayacağı düşünülmektedir.

Firmaların %59,5'inin güçlü parola kullandığı, %11,6'sının akıllı kart kullandığı, %2,4'ünün ise biometrik yöntemler kullandığı görülmektedir. Bu veriler ışığında firmaların aslında siber güvenliğe önem vermek istediği düşünülebilir. Ayrıca firmaların %40,5'inin farklı mekânlarda veri yedeklemesi yaptığı kaydedilirken işletmelerin %6'sının ise karşılaştıkları siber saldırıları analiz etmek gibi zor ve yetenekli personel istihdam etmeyi gerektiren işleri yapıyor olması siber güvenliğe önem veren oldukça bilinçli firmaların bulunduğunu da göstermektedir.

Firmalarda kullanılan ve yukarıda bahsedilen teknik özelliklerin siber güvenliğe ne tür katkılar yaptığı da incelenmiştir. Bu sebeple ilk olarak oluşturulan ki-kare testi ile firmalarda kullanılan firewall cihazlarının varlığı ile ana sunuculara yapılan saldırılar arasında ilişki incelenmiştir. İncelemede firewall kullanımı ile sunucu saldırıları arasında bir ilişki tespit edilmiştir. Ayrıca oluşturulan tablolardan görüldüğü üzere firewall kullanan 75 kullanıcının ana bilgisayarına siber saldırı olmazken, 9 kullanıcının firewall kullanmasına rağmen siber saldırı ile karşılaştığı kaydedilmiştir.

Ki-kare testinde firewall cihazının bulunması ile e-posta saldırıları arasında istatistiki olarak anlamlı bir ilişki ($p=0,019<0,05$) olduğu ve firewall kullanımının e-

posta saldırılarını direk olarak azaltmadığı söylenebilir. Bu test sadece kurumsal e-posta kullanan kişilere yenilenerek uygulandığında sonucun değiştiği gözlenmiştir. Analizde firewall kullanımının e-posta saldırıları üzerindeki etkisi sadece kurumsal mail kullanıldığı takdirde izlenmektedir.

Bağımsız değişkenlerin kendi arasındaki korelasyon skorları incelendiğinde en yüksek ilişki seviyesinin 0,995 pearson korelasyon skoruna sahip bilgi işlem teknik alt yapısı ile doğrudan bilgi işlem yatırımları arasında olduğu gözlemlenmektedir. X2 ile X5 arasında 0,394 oranında ve X2 ile X6 arasında 0,486 oranında pozitif yönlü anlamlı ilişkili olduğu kaydedilmiştir. Korelasyon matrisinde ayrıca X3 ün X4 ile 0,367 skorla X5 ile 0,419 skorla, X6 ile 0,258 skorla, X7 ile 0,379 skorla istatistiksel olarak pozitif yönlü anlamlı bir ilişkinin olduğu kaydedilmiştir.

Çalışmada saldırıların sistemlere zarar verdiği analiz edilmiştir. Özellikle 2016 yılında uygulamalar veya web sitelerine yapılan siber saldırılar neticesinde firmaların toplamda 11 gün sistemi devre dışı kalmış ve ayrıca 2 firma 5600 TL doğrudan maddi zarara uğramıştır. Bununla birlikte firmalar 166 kez zarar verici e-posta saldırılarına maruz kalırken 32 gün süreli hizmet kesintisi olmuş ve 44.600 TL doğrudan maddi kayıp yaşanmıştır.

En ciddi saldırılardan biri de ana sunuculara yapılan saldırıdır. Saldırı alan firmaların 15 gün boyunca sistemleri dururken, 6 firmanın 42.500 TL tutarında doğrudan maddi zarara uğradığı kaydedilmiştir. Örneklemde firmaların virüsler nedeni ile 28 gün boyunca hizmetlerinin durduğu ayrıca 116.200 TL doğrudan maddi zarara uğradığı kaydedilmiştir. Araştırmada direk maddi zarar olarak en yüksek saldırının bu saldırı olduğu görülmüştür.

Zonguldak'ta 91 kez kaydedilmiş oltalama (phishing) saldırı olduğu görülürken 9 gün hizmet aksaması ve saldırının maddi zararlar verdiği analiz edilmiştir. Yedeklemenin öneminin açıkça görüldüğü araştırmada firmaların %12,5'inin harddisk bozulması nedeni ile veri kaybına uğradığı, %6,3'ünün ise maddi zarara uğradığı, yaşanan doğrudan maddi kaybın ise 40.970 TL olduğu kaydedilmiştir.

Sonuç olarak Zonguldak'ta özellikle bilişim personeli istihdamının az olduğu görülmektedir. Bilgi işlem tarafından yapılacak çalışmalar ise daha çok dış kaynaklara paslanmaktadır. Bu konunun avantaj ve dezavantajlarının ayrıca araştırılması önerilmektedir.

Ayrıca firmalarda henüz web sitesi kullanımı yeterince yaygınlaşmamıştır. Bu çalışmaya başlamadan önce gerek yasal zorunluluklardan gerekse reklam boyutundan dolayı ölçek olarak seçilen firmaların tamamının web sitesini kullandığı tahmin edilmekteydi. Ancak bu çalışma ile Zonguldak'taki firmaların %42 oranında web sitesi kullanmadığı ve bununla birlikte gerek iletişimin sağlanması, gerekse kurumsal kimliği tamamlayıcı etkisi olduğundan dolayı firmaların kurumsal e-posta kullanımının önemli olmasına rağmen beklenen düzeyde kullanmadığını görülmektedir. Bunun nedeninin seçilen bağımsız değişkenlerden mi kaynaklandığı yoksa firmaların gmail, yandex, hotmail vb.. gibi daha büyük sistemleri tercih etmesinden dolayı mı kaynaklandığının araştırılması önerilmektedir.

İncelemede firewall kullanımı ile sunucu saldırıları arasında bir ilişki tespit edilmiştir. Ancak bilindiği üzere ana sunucu saldırılarında saldırgan en zayıf halkayı seçerek firma ağı içerisine girmektedir. Bu nedenle en zayıf halka olarak görülen insan faktörünün etkisi araştırmada da yüksek çıkmıştır. Firmaların oluşturduğu politikaların ve bu politikaların uygulanmasının daha uzun kapsamlı çalışmalar ile araştırılması önerilmektedir.

Firmaların karşılaştıkları saldırıların zararları genel olarak ele alındığında, siber saldırılar tüm dünyada olduğu gibi Zonguldak'ta da etkisini göstermektedir. Özellikle virüs saldırılarının ve virüsleri bir kapı olarak kullanan diğer saldırı türlerinin etkilerinin azaltılması yönünde çalışmalar yapılması gerekmektedir. Ayrıca il düzeyinde gerek firewall kullanımının yaygın olmaması gerekse diğer saldırı tespit sistemlerinin kullanımın az olması siber saldırıların tam olarak kaydedilemediğini göstermektedir. Bu nedenle gerçek maddi zararların verilerden çok daha yüksek olduğu tahmin edilmektedir. Bu çalışma il bazındaki siber saldırıları genel anlamda gösterse de saldırıların etkilerini daha ayrıntılı görmek için uzun süreli çalışmaların yapılması uygun olacaktır.

KAYNAKÇA

AFAD, (2014); 2014 -2023 *Kritik Altyapıların Korunması Yol Haritası Belgesi*, Eylül 2014.

Akalın, Güneri (1996); "Kayıt Dışı Ekonomi Sorunu ve Yasa Tasarısı (I)," *Vergi dünyası* 178 s.27-38.

Akdeniz, Sıdıka ve Adem Üzümcü (2013); "Suç ve Sosyoekonomik Değişkenler Arasındaki Bağımlılık İlişkisi: Kars Cezaevi Üzerine Bir İnceleme," *Kafkas Üniversitesi İktisadi ve İdari Birimler Fakültesi Dergisi,* Cilt:4, Sayı:6, s.115-138.

Akkan, Gülşah (2013); *"Parmak İzi ve Ses Tanıma Sayısal Kanıt İşlemlerinin Analizi,"* Yayınlanmamış Yüksek Lisans Tezi, T.C. Fırat Üniversitesi Fen Bilimleri Enstitüsü.

Aksu, Hayati ve Yakup Akkuş (2010); "Türkiye'de Mala Karşı Suçların Sosyoekonomik Belirleyicileri Üzerine Bir Deneme: Sınır Testi Yaklaşımı (1970-2007)," *Sosyoekonomi*, Cilt 11, Sayı 11.

Aktürk, Engin (2005); " Türkiye′de Kayıt Dışı Ekonomi: Sebepleri ve Çözüm Önerileri," *Ekev Akademi Dergisi*, Sayı 23, s. 285 – 300.

Akurgal, Ali (2016); "Herkese Bilim" *Teknoloji Dergisi,* S:8.

Alaca, Bahaddin (2008); *"Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik Ve Hukuki Boyutları İle)*," Yayınlanmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Antropoloji (Sosyal Antropoloji) Anabilim Dalı.

Altuğ, Osman (1999); *Kayıtdışı Ekonomi,* Türkmen Kitabevi, İstanbul.

Arslan, Oğuz, M. (2011); *Yeni Kamusal Mal, Özgür ve Açık Kaynak Kodlu Yazılım*, Nisan Kitabevi, Ankara.

Ata, Ahmet Yılmaz (2009); "Kurumsal İktisat Çerçevesinde Yolsuzluğun Fırsat ve Motivasyonları: AB Ülkeleri Üzerine Bir İnceleme," *İktisadi Araştırmalar Vakfı Yayınları,* İstanbul.

Ata, Ahmet Yılmaz (2011); "Ücretler, İşsizlik ve Suç Arasındaki İlişki: Yatay-Kesit Analizi," *Çalışma ve Toplum Dergisi* 4, 113-134.

Atabek, Ümit (2006); "İnternette Etik Sorunların Ekonomi Politik Bağlamı," *Küresel İletişim Dergisi*, Sayı 2. 1-9.

Atakan, Mustafa (2001); "Internet Teknolojileri Güvenliği," http://www.bilisimterimleri.com/bilgisayar_bilgisi/bilgi/32.html, (Erişim Tarihi:10.10.2016).

Atalıç Taş, K. (2010); "*Bilişim Suçları ve Adana İlinde 2006-2009 Yılları Arasında Meydana Gelen Bilişim Suçlarının Değerlendirilmesi,"* Yayınlanmamış Yüksek Lisans Tezi, Çukurova Üniversitesi Sağlık Bilimleri Enstitüsü. Adana.

Avcı, Burak (2014); "Stuxnet Virüsü Nedir, Nasıl Çalışıyor? ve Kaynak Kodları," http://www.burakavci.com.tr/2014/06/stuxnet.html,(Erişim tarihi: 2.1.2015).

Aydemir, Şinasi (1994); "KOBİ'ler ve Kayıt Dışı Ekonomi," *TOSYÖV,* Ankara.

Aydemir, Şinasi (1995); "Türkiye'de Kayıtdışı Ekonomi," *Maliye Hesap Uzmanları Derneği,* İstanbul.

Aydemir, Şinasi (1995a); "Kayıt Dışı Ekonomi Üzerine (I)," *Vergi Dünyası*, Sayı: 161, Ocak, 72-86.

Aydemir, Şinasi (1995b); "Kayıt Dışı Ekonomi Üzerine (II)," *Vergi Dünyası,* Sayı: 162, Şubat, 35-47.

Aydın, Emin D. (1992); *Bilişim Suçları ve Hukukuna Giriş*, Doruk Yayınevi, Ankara.

Aydın, Süleyman (2006); *Türkiye'de suç ekonomisi ve Organize suçlar*, Turhan Kitapevi, Ankara.

Bardhan, Pranab (1997); "Corruption and Development: A Review of Issues," *Journal of Economic Literature,* 35(3), s.1320-1346.

Becker, Gary S. (1968); "Crime and Punishment: An Economic Approach," *Journal of Political Economy*, s.169-217.

BGA (2014); "Siber Savunma Sistemlerinde Profesyonel Arka Kapılar," http://www.slideshare.net/bgasecurity/siber-savunma-rnlerinde-profesyonel-arka-kaplar, (Erişim Tarihi: 31.12.2016).

Biçer, Yalın (2006); *"Türkiye'de Kayıt Dışı Ekonomiyi Önlemeye Yönelik Vergi Politikaları ve Değerlendirilmesi,"* Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Maliye Anabilim Dalı. Isparta.

Boğa, Uğur (2011); *"Bilişim Suçlarıyla Mücadele Yöntemleri,*" Yayınlanmamış Uzmanlık Tezi, *TC Radyo Televizyon Üst Kurulu,* Ankara.

Box, Steven (1987); "*Recession, Crime and Punishment*," Hong Kong/London: Macmillan Education.

BTK (2016); "Türkiye Elektronik Haberleşme Sektörü," *Üç Aylık Pazar Verileri Raporu 2016 yılı 3. Çeyrek Raporu,* Ankara.

Bulut, M.H. (2007); "*Kayıt Dışı Ekonominin Boyutları, Etkileri ve Kayıt Dışı ile Mücadele Yöntemleri: Türkiye Örneği,"* Yayınlanmamış Yüksek Lisans Tezi, T.C. Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi İktisat Anabilim dalı.

Buonanno, Paolo (2003); *"The Socioeconomics Determinant of Crime. a Review of the Literature,"* Working Paper Series- Dipartimento di Economia Politica-Universita delgi Studi Milano Bicocca, Sayı:63, s.1-35.

Burdett, K., R. Lagos ve R., Wright (2003); "Crime, Inequality and Unemployment," *American Economic Review,* 93(5), s.1764-1777.

Carter, D., Bannıster,A.,J., (2002); "Computer-Related Crime, Readings in White Collor Crime," *Waveland Press, Inc*., Illinois 2002.

Çavuşoğlu, Hüseyin ve Mehmet Pekkaya (2015); "Siyasal Propaganda Araçlarının Seçmen Tercihine Etkisi: Zonguldak Örneği," *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* cilt:10 sayı: 3., Eskişehir.

Ceyhun, Yurdakul ve M. Ufuk Çağlayan (1997); "*Bilgi Teknolojileri Türkiye için Nasıl Bir Gelecek Hazırlamakta*," Türkiye İş Bankası Kültür Yayınları.

CHIP (2008); "Dünyanın En Tehlikeli 10 Virüsü," http://www.chip.com.tr/haber/en-unlu-virusler-sl-slammer-2003_8489_6.html, (Erişim Tarihi: 14.08.2016).

CHIP (2009); "Spam Nedir?," https://www.chip.com.tr/blog/clever74/spam-nedir_4442.html, (Erişim Tarihi: 12.09.2016).

CHIP (2009); "Raid Nedir? Nasıl Yapılır?," https://www.chip.com.tr/forum/raid-nedir-nasil-yapilir_t100852.html, (Erişim Tarihi: 12.09.2016).

Chırıcos, Theodore G. (1987); *"*Rates of Crime and Unemployment; An Analysis of Aggregate Research Evidence*," Social Problems,* 34.2, s.187-212.

CNNTÜRK (2017); "Wannacry siber saldırı hakkında bilinmesi gerekenler," https://www.cnnturk.com/dunya/wannacry-siber-saldiri-hakkinda-bilinmesi-gerekenler?page=1, (Erişim Tarihi: 25.10.2017).

Convention on Cybercrime (2010); "Convention on Cybercrime," http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=28/10/2010&CL=ENG , (Erişim Tarihi:18.02.2015).

Cyber-Warrior (2015); "Port Tarama Metotları ve Korunma Yolları," https://www.cyber-warrior.org/Dokuman/Default.Asp?Data_id=4642 (Erişim Tarihi: 18.08.2015).

Çınar, Seda Nur (2013); "Neden ve Nasıl Bir Güvenlik Politikası?," http://www.bthaber.com/guvenlik/neden-ve-nasil-bir-guvenlik-politikasi/1/11160, (Erişim Tarihi:11.04.2015).

Çokgezen, Murat (1993); "Türkiye'de Kayıt Dışı Ekonomi ve Boyutları," *İktisat ve İş Dünyası,* Yıl 2, Sayı 16, s. 23-25.

Çolak, Mustafa (2012); *"Kayıtdışı Ekonomi ile Mücadelede Hukuki Düzenleme Politikası,"* Yayınlanmamış Doktora Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Mali Hukuk Anabilim Dalı.

Dağ, Gökhan (2005); "Dolaylı-Dolaysız Vergiler," http://gokhandag.blogcu.com/dolayli-dolaysiz-vergiler-ve-vergi-adaleti-acisindan-karsilastir/758253, (Erişim Tarihi:11.01.2017).

Demir, Halil İbrahim (2007); "*Kayıt Dışı Ekonomi ve Kara Para İlişkisi*," Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü, Isparta.

Demirbaş, Timur (2001); *Kriminoloji*, Seçkin Yayıncılık A.Ş., Ankara.

DHS (2014); "Critical Infrastructure Sectors," http://www.dhs.gov/critical-infrastructure-sectors, (Erişim tarihi: 11.11.2014).

Dinçer, Burcu (2007); *"Kayıt Dışı Ekonomi ve Rekabetçi Piyasalar Üzerine Etkisi,"* Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Dönmezer, Sulhi (2003); *Genel Ceza Hukuku Dersleri*, Bahçeşehir Üniversitesi Yayınları, İstanbul.

DPT (2001): *Kayıt dışı Ekonomi,* Özel İhtisas Komisyonu Raporu, Yayın No: 2603, Ankara.

DPT (2007); *IX. Beş Yıllık Kalkınma Planı(2007–2013),* Vergi Özel İhtisas Komisyonu Raporu, Ankara.

Dura, Cihan (1997); "Kayıt Dışı Ekonomi Kavramı, Sebep ve Etkileri, Ölçülmesi, Mücadele Yolları ve Türk Ekonomisindeki Yeri," *Maliye Dergisi* 1.124, s. 3-12.

Dülger, Murat Volkan, (2004); *Bilişim Suçları*, Seçkin Yayınları, Ankara.

EC (European Council) (2001); *Bilişim Suçları Sözleşmesi,* Avrupa Konseyi, Budapeşte, Macaristan, Kabul tarihi: 23.11.2001.

Ehrlich, Isaac (1973); "Participation in Illegitimate Activities; a Theoretical and Emprical Investigation," *Journal of Political Economy,* 81, s.521-565.

Ekin, Nusret (1995); *Kayıt dışı Ekonomi Enformel İstihdam*, İTO Yayını, İstanbul.

Engelhardt, Bryan, Guillaume Rocheteau, and Peter Rupert, (2008); "Crime and the labor market: a search model with optimal contracts," *Journal of Public Economics,* Sayı 92, Cilt 10, s.1876-1891.

Ensonhaber, (2016); "Siber Saldırının ABD'ye Maliyeti: 7 Milyar Dolar," http://www.ensonhaber.com/siber-saldirinin-abdye-maliyeti-7-milyar-dolar-2016-10-22.html, (Erişim Tarihi: 08.08.2017).

Erbaşı, Ayşe Aslıhan (2007); *Çocuk Pornografisi,* İstanbul Barosu Dergisi, Cilt 8, Sayı: 4.

Fleisher, Belton M. (1963); "The effect of unemployment on juvenile delinquency," *Journal of Political Economy*, 71.6, s.543-555.

Fleisher, Belton M. (1966); "The effect of income on delinquency," *The American Economic Review*, Sayı 56.1/2, s.118-137.

Fowles R. ve Merva, M. (1996); "Wage Inequality And Criminal Activity," *Criminology*, Sayı 34(2), s.163-182.

Garland, David (1996); "The Limits of The Sovereıgn State Strategies of Crime Control in Contemporary Society," *The British Journal of Criminology*, Sayı 36.4, s.445-471.

Gould E. D., Weinberg B. A. ve Mustard D. (2002); "Crime Rates and Local Labor Opportunities in the United States: 1979-1995," Review of Economic and Statistics, Sayı 84(1), s.45-61.

Edizdoğan, Nihat ve Erhan Gümüş (2013); "Vergi Afları ve Türkiye'de Vergi Aflarının Değerlendirilmesi," *Maliye Dergisi*, Sayı 164, s: 99-119.

Güngör, Kamil (2003); "Ağır Vergi Yükünün Kayıt Dışı Ekonomi Üzerindeki Etkisi ve Türkiye," *Vergi Sorunları Dergisi,* Sayı 172, s.111-128.

Gürünlü, Alma Özlem ve Özgül Vupa (2008); "Regresyon Analizinde Kullanılan En Küçük Kareler ve En Küçük Medyan Kareler Yöntemlerinin Karşılaştırılması," *Dokuz Eylül Üniversitesi, Fen-Edebiyat Fakültesi, İstatistik Bölümü, İzmir, Fen Dergisi, (E-Dergi),* Sayı 3(2) s.219-229.

Güvel, Enver Alper (2004); *Suç ve Ceza Ekonomisi*, Roma Yayınları, Ankara.

Haberturk (2014); "İnternette 22 Sitede Bonzai Satışı Yapılıyor," http://www.haberturk.com/gundem/haber/968196-internette-22-sitede-bonzai-satisi-yapiliyor, (Erişim Tarihi: 02.11.2014).

Haeni, Reto (1997); "Information Warfare: An Introduction," *The George Washington University Cyberspace Policy Institute,* January, s.1-16.

Hekim, Hakan ve Oğuzhan Başıbüyük (2013); "Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları," *Uluslararası Güvenlik ve Terörizm Dergisi,* s.135-138.

Hürriyet (2012); "Türk Kızı Şeniz Sanal Zorba Kurbanı," http://www.hurriyet.com.tr/turk-kizi-seniz-sanal-zorba-kurbani-19693094, (Erişim Tarihi: 02.01.2017).

Hürriyet (2017); "Siber Saldırıların Maliyeti 2.1 Trilyon Dolar," http://www.hurriyet.com.tr/siber-saldirilarin-maliyeti-2-1-trilyon-dolar-40486872, (Erişim Tarihi: 11.09.2017).

Ilgın, Yılmaz (1999); *"Kayıtdışı Ekonomi ve Türkiye'deki Boyutları,"* DPT Yayınlanmamış Uzmanlık Tezleri, Yayın No: DPT 2492, Nisan 1999.

Işık, Osman, Cihat (2013) "Ağ Tabanlı Saldırı Tespit Sistemleri," https://www.slideshare.net/osmncht/ag-tabanl-saldr-tespit-sistemleri, (Erişim Tarihleri: 18.06.2017).

İHA (2014); "Bilişim Suçlarının Dünya Ekonomisine Etkisi," http://www.iha.com.tr/haber-bilisim-suclarinin-dunya-ekonomisine-etkisi-365348/, (Erişim Tarihi: 20.10.2016).

İHS (2016); "Sunucu Nedir Ne işe Yarar?," http://www.ihs.com.tr/blog/sunucu-nedir-ne-ise-yarar, (Erişim Tarihi: 10.06.2016).

İHS (2016a); "Siber Saldırı Mağduru Küçük Şirketlerin %60'ı İflas Ediyor," http://www.ihs.com.tr/blog/siber-saldiri-magduru-kucuk-sirketlerin-yuzde-altmisi-iflas-ediyor/, (Erişim Tarihi: 05.06.2017).

İkiz, Ahmet Salih (2000); *"Kayıt Dışı Ekonomi ve Türkiye'de Ekonomik Büyüme Üzerine Etkileri,"* Yayınlanmamış Doktora Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü, İktisat Anabilim Dalı, İzmir.

İkizler, Metin, ve M. Sinan Başar, (2006); "Spam'ın Zararları ve Spam ile Hukuki Mücadele: ABD Örneği ve Türk ve Avrupa Birliği Hukukları ile Karşılaştırılması," *Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi* Cilt: 8, Sayı: 2, , s.91-114.

İlbaş, Çığır, (2009); *"Bilişim Suçlarının Sosyo - Kültürel Seviyelere Göre Algı Analizi,"* Yayınlanmamış Yüksek Lisans Tezi, Başkent Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

İlbaş, Çığır ve Mehmet Ali Köksal (2011); "Türkiyede Bilişim Suçları (1990 - 2011)," http://www.cigir.com/tr/images/bsraporu.pdf, (Erişim Tarihi: 10.06.2014).

İnternethaber (2017); "Siber Saldırı Mı Var Wanna Cry Nedir Windows Korunma Yolları,"http://www.internethaber.com/siber-saldiri-mi-var-wanna-cry-nedir-windows-korunma-yollari-foto-galerisi-1777092.htm, (Erişim Tarihi: 10.06.2015).

İTÜ BİDB (2013); "Virüs, Solucan ve Truva Atı," http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/vir%C3%BCs-solucan-ve-truva-at%C4%B1, (Erişim Tarihi: 20.10.2015).

İsimtescil (2006); **"**SSL Sertifikaları Hakkında Genel Bilgiler," http://www.isimtescil.net/ssl/ssl-nedir.aspx, (Erişim Tarihi: 10.05.2017).

İSMMMO, (2011); *Suç Ekonomisinin Türkiye Bilançosu,* İstanbul Serbest Muhasebeci Mali Müşavirler Odası Raporu, 2011, s:2011/15

Johnson, Blair T., Lori AJ Scott-Sheldon, and Michael P. Carey (2010); "Meta-synthesis of health behavior change meta-analyses," *American journal of public health* Sayı 100.11 s.2193-2198.

Kagal, L., Paolucci, M., Srinivasan, N., Denker, G., Finin, T. and Sycara, K. (2004); "Towards Authorization, Confidentiality and Privacy for Semantic Web Services," In *Proc of AAAI 2004 Spring Symposium on Semantic Web Services*.

Kahya, Yavuz ve Fatih Irmak (2014); "Kayıtdışı Ekonomi ve Suç Örgütlenmeleri İlişkisinin Sosyolojik Açıdan Değerlendirilmesi," *Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Sayı 18(1): 353, Erzurum.

Kalça, Adem (1995); "Türkiye'de Kayıt Dışı Ekonominin Durumu," *Banka ve Ekonomik Yorumlar Dergisi,* Yıl 32.

Kanlı, Murat (2007); *"Dolaylı Vergiler ve Kayıt Dışı Ekonomi,"* Yayınlanmamış Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü Maliye Anabilim Dalı Maliye Teorisi Bölümü, İstanbul.

Karaarslan, Enis, Abdullah Teke ve Halil Şengonca (2003); "Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması*," Akademik Bilişim, Çukurova Üniversitesi, 1 s.* Adana.

Karaman, Fazıl (1999); "Ekonomik ve Sosyal Boyutla Türkiye'de Kayıt dışı Ekonomi," *Yeni Türkiye,* Cilt:5, Sayı:27, Mayıs-Haziran 1999.

Karasar, Niyazi (1991); *Bilimsel Araştırma Yöntemi*, Nobel Yayınları, Ankara.

Karatay, Özcan (2009); *"Kayıt Dışı Ekonominin Ülke Ekonomisine Etkileri ve Toplumsal Maliyeti,"* Yayınlanmamış Doktora Tezi, Sivas Cumhuriyet Üniversitesi Sosyal Bilimler Enstitüsü, Sivas.

Kaspersky (2016); "Kaspersky Lab Türkiye'de Security Awareness Training (Güvenlik Farkındalığı Eğitimi)," http://www.kaspersky.com/tr/about/news/press/2016/kasper sky-lab-turkiyede-security-awareness-training-guvenlik-farkindaligi-egitimi-urunlerini-duyurdu, Erişim Tarihi: 08.03.2015).

Kaspersky, (2014); "Solucan, Virüs veya Solucanı Nedir? ," http://www.kaspersky.com/tr/internet-security-center/threats/viruses-worms, (Erişim Tarihi: 20.10.2016).

Kayaokay, Kübra (2014); "Terörizm ve Siber Terör," http://kubrakayaokay.blogspot.com.tr/2014/03/turkceye-franszca-terreur-sozcugunden.html, (Erişim Tarihi: 15.10.2016).

Keçeci, Orçun (2012); "Siber Suçlar ve Siber Terörizm," http://goo.gl/ASxX4e, (Erişim Tarihi: 6.08.2016).

Kılıçdaroğlu, Kemal (2000); "Suç Ekonomisini Önleme Yargı Cephesi ve Sorunları," *Vergi Dünyası Dergisi,* Sayı 225, s.5-18.

Kiveko, (2017); "İngilterede Siber Saldırıların Maliyeti," https://kiveko.org/ingilterede-siber-saldirilarin-maliyeti-30-milyar/, (Erişim Tarihi: 07.05.2017).

Kocasakal, Ümit (2005); "Ekonomik Suçluluk," *Güncel Hukuk Dergisi*, Sayı:23.

Kulaksızoğlu, Adnan (1999); *Ergenlik Psikolojisi*, Remzi Kitabevi, 2.Baskı İstanbul.

Kuplay, Ömer (2007); "Bilişim Suçları ve Hukuku," *Çağın Polisi Dergisi* 66.Sayı.

Kurt, Levent (2005); *Açıklamalı-İçtihatlı Tüm Yönleriyle Bilişim Suçları ve Türk Ceza Kanunundaki Uygulaması*, Seçkin Yayıncılık, Ankara, 2005.

Lashkari, Habibi Arsah, and Omar Bin Zakaria (2009); "Shoulder Surfing attack in graphical password authentication," *International Journal of Computer Science and Information Security*, Cilt. 6, No:2.

Losby, J. L., Else, J. F., Kingslow, M. E., Edgcomb, E. L., Malm, E. T., ve Kao, V. (2002); "Informal economy literature review," *ISED Consulting and Research*.

Latham, Shinder (1998); "Zimbabwe's Informal Sector," *Monthly Lab., Sayı 121* s.72.

Mavral, Ülker (2001); "Karapara Kayıtdışı Ekonomi İlişkisi ve Türkiye'ye Yansımaları," *Vergi Denetmenleri Derneği Yayını*, Ankara.

Mavral, Ülker (2003); "Kara Para, Kayıtdışı Ekonomi İlişkisi ve Türkiye" ye Yansımaları," *Maliye ve Hukuk Yayınları,* 2. Baskı, Ankara.

McEachen, John C., ve John M. Zachary (2007); "IDS for Networks," *Network Security: Current Status and Future Directions*, s.83-97.

Merritt, Marian (2014); "Kimlik Hırsızlığı Temel Bilgiler," http://tr.norton.com/identity-theft-primer/article, (Erişim Tarihi: 11.12.2014).

Microsoft, (2009); "Kendinizi Conficker'dan Koruyun," http://www.microsoft.com/tr-tr/security/pc- security/conficker.aspx, (Erişim Tarihi: 19.10.2014).

Microsoft (2014); "Bilgisayar Virüsü Nedir," http://www.microsoft.com/tr-tr/security/pc-security/virus-whatis.aspx, (Erişim Tarihi: 19.10.2014).

Milliyet (2006); "Çocuk Pornosunun Yüzde 20'si Bebek Görüntüleri," http://www.milliyet.com.tr/2006/10/20/pazar/paz02.html, (Erişim Tarihi: 12.10.2014).

Milliyet (2012); "İnternet Bankacılığı Kullananlar Dikkat," http://www.milliyet.com.tr/internet-bankaciligi-ni-kullananlar-dikkat-/ekonomi/ekonomidetay/14.12.2012/1641786/default.htm, (Erişim Tarihi: 10.10.2014).

Milliyet (2013); "ABD'yi Karıştıran İntihar," http://www.milliyet.com.tr/abd-yi-karistiran-intihar/dunya/detay/1763540/default.htm, (Erişim Tarihi: 02.01.2017)

Muğla Emniyet Müdürlüğü (2013); "Solucan "Worm" Nedir?," http://www.mugla.pol.tr/fethiye/Sayfalar/Solucan-Nedir.aspx, (Erişim Tarihi: 20.10.2014).

Nas, Şahin (2014); *"Kayıt Dışı Ekonomi ve Türkiye Örneği,"* Yüksek Lisans Tezi, T.C. Çukurova Üniversitesi Sosyal Bilimler Enstitüsü İktisat Ana Bilim Dalı.

Nato Dergisi, (2014); "Yeni Tehditler: Siber Boyut," http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/TR/index.htm, (Erişim Tarihi: 19.10.2014).

Ntvmsnbc (2010); "70 Milyonun Kimliği Çalındı," http://www.ntvmsnbc.com/id/25118140/, (Erişim Tarihi: 9.01.2015).

Ntvmsnbc (2014); "Kredi Kartı Dolandırıcılığında 10 Yöntem" http://arsiv.ntvmsnbc.com/news/195214.asp, (Erişim Tarihi: 09.01.2015).

Odabaşı, H. Ferhan ve Ömer Uysal (2006); "Bilgisayar Etiği Öğretiminde Kullanılan Yöntemler," *VI. International Education Technology Conference*, s. 1639-1652.

Öcal, Oğuz (2010); "*Suçun Sosyal ve Ekonomik Belirleyicileri: Kayseri Örneği,"* Yayınlanmamış Doktora Tezi, Erciyes Üniversitesi Sosyal Bilimler Enstitüsü, Kayseri.

Öğünç, Fethi ve Gökhan Yılmaz (2000); "Estimating the Underground Economy in Turkey," *Research and Monetary Policy Department, Central Bank of the Republic of Turkey*.

Önal, Huzeyfe (2012); "Dos ve DDos Saldırıları Savunma Yolları ve Çözüm Önerileri," http://docplayer.biz.tr/9747357-Dos-ddos-saldirilari-savunma-yollari-ve-cozum-onerileri-huzeyfe-onal-huzeyfe-onal-bga-com-tr.html, (Erişim tarihi: 20.10.2016).

Önder, İzzettin (1992); "Vergiye Psikolojik Direniş," *Görüş,* s.50-52.

Önder, Merve (2012); *"Türkiye'de Kayıt Dışı Ekonomi ve Uluslararası Uygulamalar Işığında Çözüm Önerileri,"* Yayınlanmamış Mesleki Yeterlilik Tezi, Maliye Bakanlığı Strateji Geliştirme Başkanlığı.

Özcan, Süleyman Emre (2003); *"Devlet İç Borçlanması ve Türkiye'de Devlet İç Borçlanmasının Sürdürülebilirliği,"* Yayımlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Özçelik, Özer (2005); *"Teorik Ve Kavramsal Perspektiften Kayıtdışı Ekonomi Sorunu, Ölçümü Ve Çözüm Önerileri,"* Yayınlanmamış Yüksek Lisans Tezi, Dumlupınar Üniversitesi, Sosyal Bilimler Enstitüsü İktisat Anabilim Dalı. Kütahya.

Özdemirci, Fahrettin ve Cengiz Aydın (2007); "Kurumsal Bilgi Kaynakları ve Bilgi Yönetimi," *Türk kütüphaneciliği,* Sayı 21, 2 s.164 – 185.

Özgenç, İzzet (2007); *Kaçakçılıkla Mücadele Kanunu,* Seçkin Yayıncılık, İstanbul.

Özsoylu, Ahmet Fazıl (1994); "Kayıtdışı Ekonominin Etkileri, Kim Kazanıyor, Kim Kaybediyor," *Ekonomik Forum Dergisi,* s.14.

Özsoylu, Ahmet Fazıl (1996); *Türkiye'de Kayıtdışı Ekonomi*, Bağlam Yayıncılık, İstanbul.

Özsoylu, Ahmet Fazıl (1998a*); 2000 li Yıllara Doğru Türkiye'nin Önde Gelen Sorunlarına Yaklaşımlar, TÜGİAD*, İstanbul.

Özsoylu, Ahmet Fazıl (1998b); *Suç ekonomisi ve Mafya, Ekonomik Forum, TOBB Yayını*, Sayı 11, Ankara.

Öztürk, Bahri (2004); *Ceza Hukuku Genel ve Özel*, Turhan Kitapevi, 2. Bası, Ankara.

Öztürk, Nazım (2006); "Ekonomide Devletin Değişen Rolü," *Amme idaresi Dergisi,* Cilt: 39, Sayı 1, s:17-38.

Pazarlıoğlu, M. Vedat ve Timur Turgutlu, (2007); "Gelir, İşsizlik ve Suç: Türkiye Üzerine Bir İnceleme," *Finans Politik & Ekonomik Yorumlar Dergisi,* Sayı 44.513, s.63-70.

Pekkaya, Mehmet ve Sabire Başaran (2011); "Konaklama İşletmeleri Hizmet Kalitesi Boyutları Önem Derecelerinin AHP ile Belirlenmesi Ve İşletmelerin Hizmet Kalitesine Göre TOPSIS ile Sıralanması," *Mali Ufuklar,* Sayı 5(15), 111-136.

Pekkaya, Mehmet ve Mesut Aktogan (2014); "Dizüstü Bilgisayar Seçimi: DEA, TOPSIS ve VIKOR ile Karşılaştırmalı bir Analiz," *AİBÜ-İİBF Ekonomik ve Sosyal Araştırmalar Dergisi*, Cilt:10, Sayı 1 s:157-178.

Pekkaya, Mehmet (2016); "Hizmet Kalite Standartları Temelli Hastanelerin ÇKKV ile Değerlendirilmesi," *17. International Symposium on Econometrics, Operations Research and Statistics,* s:974-981.

Pekkaya, Mehmet ve Fatma Akıllı (2013); "Statistical Analysis and Evaluation of Airline Service Quality By Servperf-Servqual Scale," *Ekonomik ve Sosyal Araştırmalar Dergisi,* 9(1), 75-96.

Pocor, Fausto (2004); "New challenges for international rules against cyber-crime," *Crime and Technology,* Springer Netherlands, s.29-38.

Sabah (2011); "Dünyanın En Tehlikeli Virüsleri," http://www.sabah.com.tr/fotohaber/teknoloji/dunyanin-en-tehlikeli-virusleri/31171, (Erişim Tarihi: 19.10.2015).

Sancak, Serdar (2008); *"Saldırı Tespit Sistemleri Tekniklerinin Karşılaştırılması,"* Yayınlanmamış Yüksek Lisans Tezi, Gebze Yüksek Teknoloji Sosyal Bilimler Enstitüsü, Kocaeli.

SANS (2013); "Hedef Odaklı Oltalama Saldırıları (Spear Phishing)," *Bilgisayar Kullanıcıları İçin Aylık Güvenlik Farkındalığı Bülteni,* https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201307_tr.pdf (Erişim Tarihi:15.10.2016).

Sarıkaya, Hatice Elanur (2007); *"Kayıt Dışı Ekonominin Ekonomik Büyümeye Etkisi: Türkiye Örneği (1980-2005),"* Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, SBE.

Sarılı, Mustafa Ali (2002); "Türkiye'de Kayıt Dışı Ekonominin Boyutları, Nedenleri, Etkileri ve Alınması Gereken Tedbirler," *Bankacılar Dergisi* Sayı 41 s.32-50.

Scorzafave, Luiz Guilherme ve Milena Karla Soares (2009); "Income inequality and pecuniary crimes," *Economics Letters,* Sayı 104.1 s.40-42.

Schineider, Friedrich (2013); "Shadow Economy of 31 European and 5 other OECD Countries from 2003 to 2013," http://www.econ.jku.at/members/schneider/files/publications/2013/shadeceurope31_jan2013.pdf, (Erişim Tarihi: 24.12.2015).

Schmidt, Klaus M. ve M. Schnitzer (2003); "Public Subsidies for Open Source? Some Economic Policy Issues of the Software Market," *Harvard Journal of Law and Technology.*

Sofaer, Abraham D. ve Seymour E. Goodman (2001); "The Transnational Dimension of Cyber Crime and Terrörism," *CA:Hoover Institution Press, Stanford.*

Soyaslan, Doğan (1998); *Kriminoloji,* Ankara Üniversitesi Hukuk Fakültesi Yayınları, 2. Baskı, Ankara.

Starteknoloji (2013); "Tüm Zamanların En Zararlı 5 Virüsü," http://haber.stargazete.com/teknoloji/tum-zamanlarin-en-zararli-5-virusu/haber-808951, (Erişim tarihi: 19.10.2015).

STM (2017); *2016 Ekim – Aralık Dönemi Siber Tehdit Durum Raporu,* STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.

Süer, C., (2011); "En Tehlikeli 10 Bilgisayar Virüsü," http://shiftdelete.net/en-tehlikeli-10-bilgisayar-virusu-28544?p=7, (Erişim Tarihi : 19.10.2015).

Şahinaslan, Önder, Ender Şahinaslan ve Mesut Razbonyalı (2013); "Eğitim Kurumlarına Yönelik Sızma Test Metodolojisi," *Akdeniz Üniversitesi, Hukuk Fakültesi, Akademik Bilişim, Bildiri.* Antalya.

Şener, Kemal (2013); "Bilişim Suçları Hangi Yollarla İşlenir," http://www.kemalsener.av.tr/bilisim-suclari/bilisim-suclari-hangi-yollarla-islenir.html, (Erişim Tarihi: 17.04.2015).

Şişman, Yener (1999); "*Ekonomik Faaliyetlerde Enformelleşme ve Türkiye'de Enformel Ekonomik Faaliyetlerde Çalışanlara Yönelik Sosyal Politikalar: Eskişehir'deki Seyyar Satıcılar Üzerine Bir Alan Araştırması,*" Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Eskişehir.

Tandoğan, Safai (2007); *"Öz-Düzenlemeli Harita (SOM) Kullanarak DDOS Saldırılarının Sınıflandırılması,"* Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Fen Bilimleri, Eskişehir.

Tanzi, Vito (1984); "Yeraltı Ekonomisi" çev. Mustafa Açıkalın, *Maliye Dergisi,* Sayı:70, Temmuz - Ağustos.

Tapan, Burak (2015); "Dünyanın En Popüler Şifresi," http://www.gazetevatan.com/dunyanin-en-populer-sifresi-123456-1030630-pazar-vatan/, (Erişim Tarihi: 14.10.2015).

TASAM (2004); *Siber Terörizm Raporu*, Türk Asya Stratejik Araştırmalar Merkezi (TASAM) Yayını, Sayı 2014:2.

Temli, Muhammed (2014); "Siber Güvenlik ve Alınabilecek Kurumsal Tedbirler," *Batı Karadeniz Kalkınma Ajansı, BAKKA Bülten* 4. Sayı s:80.

Terzioğlu, Pınar (2016); "Türkiye'de en çok karşılaşılan beş siber saldırı çeşidi," http://blog.trendmicro.com.tr/turkiyede-en-cok-karsilasilan-bes-siber-saldiri-cesidi/, (Erşim Tarihi: 14.10.2016).

Tiryaki, Tercan ve T. Gürsoy (2004); "Ekonomik Suç Kavramı ve Sigortacılık Suçlarının Bu Açıdan Değerlendirilmesi," *Sayiştay Dergisi,* s.53-69.

Toptaş, Ülker (1998); "*Türkiye'de Kayıtdışı Ekonominin Nedenleri*," TES-AR Yayınları, Sayı:26, Ankara.

TSE (2013); *Sızma Testi Teknik Kriterleri Programı*, Türk Standartları Enstitüsü TSE -2013, Sürüm1 s.21.

Tulum, İsmail (2006); "*Bilişim Suçları ile Mücadele*," Yayınlanmamış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Anabilim Dalı, Isparta.

Tunç, Mehmet (2017); *"Kayıt Dışı İstihdamla Mücadelede Geliştirilen Stratejiler Uygulanan Politikalar ve Gelişmiş Ülke Örnekleri,"* Türkiye İş Kurumu Genel Müdürlüğü Uzmanlık Tezi, Ankara.

Tütüncü, Asiye (2013); *"Kayıtdışı Ekonomi ve Türkiye'de Kayıtdışı Ekonomi Boyutunun Tahmini,"* Yayınlanmamış Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Ekonometri Anabilim Dalı Ekonometri Programı.

Ulak-CSIRT (2009); "Honeypot (Balküpü) Çalışma Grubu," http://csirt.ulakbim.gov.tr/gruplar/bal.uhtml, (Erişim Tarihi: 03.03.2015).

US, Vuslat (2004); *"Kayıt Dışı Ekonomiyi Tahmin Yöntem Önerisi: Türkiye Örneği,"* Tartışma Metni, Türkiye Ekonomi Kurumu.

Uyanık, Namık Kemal (2001); *Bir Bölüm Finansal İşlemler ve Vergilendirilmeleri,* Türkiye Bankalar Birliği Yayınları, İstanbul.

Uydacı, Mert (2004); "Pazarlamada Elektronik Posta Kullanımı," *Ege Academic Review Sayı* 4.1 s.79-84.

Uzunay, Yusuf (2005); "Dijital Delil Araştırma Süreci," 2. *Polis Bilişim Sempozyumu, Ankara Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü,* Ankara.

UNECE (1993), "*Review of Concepts and Definations for Use in Statistics of Hidden and Informal Economy*," Joint OECD/UNECE Meeting of National Account Expert, Paris, s.1.

UDHB (2014); *"Kurumsal SOME Kurulum ve Yönetim Rehberi,"* Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Haberleşme Genel Müdürlüğü.

Ünver, Mustafa, Cafer Canbay ve Ayşe Gül Mirzaoğlu (2009); "*Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,"* Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara.

Ünver, Mustafa ve Cafer Canbay(2010); "Ulusal ve Uluslararasi Boyutlariyla Siber Güvenlik," *Elektrik Mühendisliği Dergisi, Sayı* 438, s. 94-103.

Wikimedia, "Ddos Attack," https://commons.wikimedia.org/wiki/File:Ddos-attack-ex.png, (Erişim Tarihi: 07.11.2017).

Wikipedia (2012); "Solucan(Virüs)," http://tr.wikipedia.org/wiki/Solucan_(vir%C3%BCs), (Erişim Tarihi: 20.10.2015).

Wikipedia (2014); "İnternet," http://tr.wikipedia.org/wiki/%C4%B0nternet, (Erişim Tarihi: 20.10.2015).

Wikipedia (2014); "Bilgisayar," http://tr.wikipedia.org/wiki/Bilgisayar, (Erişim Tarihi: 20.10.2015).

Wikipedia (2016); "Süper Bilgisayar," https://tr.wikipedia.org/wiki/S%C3%BCper_bilgisayar, (Erişim Tarihi: 25.01.2016).

Wikipedia (2016b); "Bilgisayar Virüsü," http://tr.wikipedia.org/wiki/Bilgisayar_vir%C3%BCs%C3%BC, (Erişim tarihi: 19.10.2014).

Witte, Ann D. ve Helen Tauchen (1993); "Work and Crime: An Exploration Using Panel Data," *The Economic Dimensions of Crime*. Palgrave Macmillan UK, s.176-191.

Wong, Kenneth ve Phet Sayo (2004); "Free/Open Source Software- a General Introduction," *UNDP-APDIP, Kuala Lumpur, MY.*

Worldometers (2016); "Dünya Üzerindeki İnternet Kullanıcı Sayısı," http://www.worldometers.info/tr/, (Erişim tarihi: 25.12.2016).

Xtrlarge (2017); "2016'da Online Fidye Yazılımları ile 1 Milyar Dolar Zarar," https://www.xtrlarge.com/2017/03/14/2016-online-fidye-yazilim-milyar-zarar/ (Erişim Tarihi:18.09.2017).

Yavuzer, Haluk (1996); *Çocuk ve Suç*, Remzi Kitabevi, 1996, İstanbul.

Yenidünya, Ahmet Caner ve Olgun Değirmenci (2003); *Mukayeseli hukukta ve Türk hukukunda bilişim suçları*, Legal.

Yenisafak (2003), "Küresel Utanç: Kadın ve Bebek Ticareti," http://www.yenisafak.com.tr/arsiv/2003/agustos/04/d2.html, (Erişim tarihi: 02.11.2014).

Yetim, Sedat (1999); *Türkiye'de Vergi Kaçakçılığı ve Kayıt Dışı Ekonomi*, Türkiye Bankalar Birliği.

Yıldız, Rıfat, Oğuz Öcal ve Ertuğrul Yıldırım (2011); "Suçun Sosyoekonomik Belirleyicileri: Kayseri Üzerine Bir Uygulama," *Erciyes Üniversitesi İktisâdi ve İdarî Bilimler Fakültesi Dergisi,* Sayı 36, s.15-31.

Yılmaz, Gülay Akgül (2006); *Kayıt Dışı Ekonomi ve Çözüm Yolları*, Serbest Muhasebeci Mali Müşavirler Odası, İstanbul.

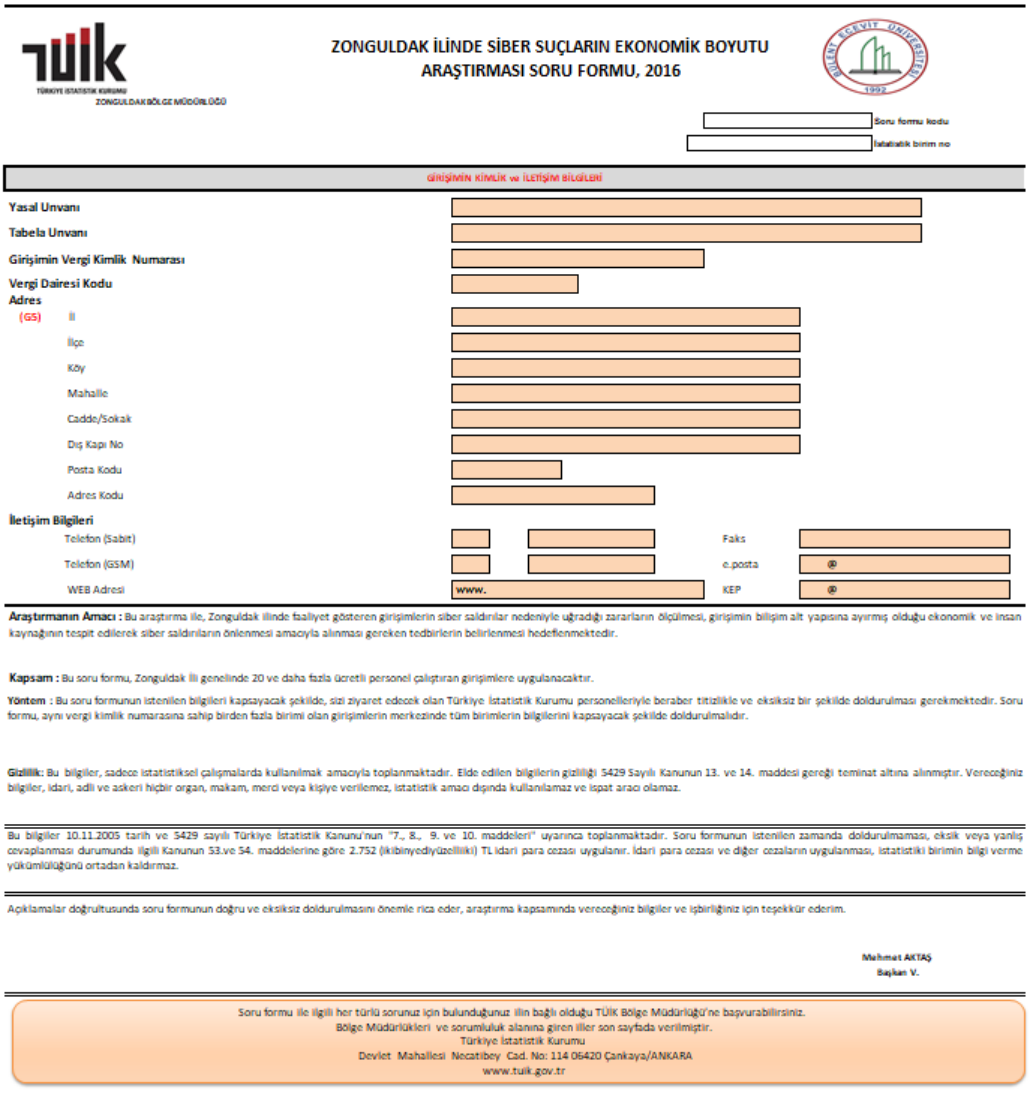
Yılmaz, Onur (2009); "Web Uygulamalarına Yönelik Saldırılar," *WGT E-Dergi 2. Sayı*.

Yılmaz, Murat (2014); "Bilişim suçları", http://www.olympos.org/article/author/view/57, (Erişim tarihi: 01.08.2014).

Yücebaş, Önder (2010); *Suç Ekonomisi Ve Terörün Finansmanı*, Turhan Kitabevi, Ankara.

EKLER

Ek 1: Zonguldak İlinde Siber Suçların Ekonomik Boyutu Araştırması Soru Formu



TÜİK
TÜRKİYE İSTATİSTİK KURUMU
ZONGULDAK BÖLGE MÜDÜRLÜĞÜ

ZONGULDAK İLİNDE SİBER SUÇLARIN EKONOMİK BOYUTU ARAŞTIRMASI SORU FORMU, 2016

BÜLENT ECEVİT ÜNİVERSİTESİ 1992

Soru formu kodu

İstatistiki birim no

GİRİŞİMİN KİMLİK ve İLETİŞİM BİLGİLERİ

Yasal Unvanı	
Tabela Unvanı	
Girişimin Vergi Kimlik Numarası	
Vergi Dairesi Kodu	
Adres	
(GS) İl	
İlçe	
Köy	
Mahalle	
Cadde/Sokak	
Dış Kapı No	
Posta Kodu	
Adres Kodu	
İletişim Bilgileri	
Telefon (Sabit)	Faks
Telefon (GSM)	e.posta @
WEB Adresi www.	KEP @

Araştırmanın Amacı : Bu araştırma ile, Zonguldak ilinde faaliyet gösteren girişimlerin siber saldırılar nedeniyle uğradığı zararların ölçülmesi, girişimin bilişim alt yapısına ayırmış olduğu ekonomik ve insan kaynağının tespit edilerek siber saldırıların önlenmesi amacıyla alınması gereken tedbirlerin belirlenmesi hedeflenmektedir.

Kapsam : Bu soru formu, Zonguldak İli genelinde 20 ve daha fazla ücretli personel çalıştıran girişimlere uygulanacaktır.

Yöntem : Bu soru formunun istenilen bilgileri kapsayacak şekilde, sizi ziyaret edecek olan Türkiye İstatistik Kurumu personelleriyle beraber titizlikle ve eksiksiz bir şekilde doldurulması gerekmektedir. Soru formu, aynı vergi kimlik numarasına sahip birden fazla birimi olan girişimlerin merkezinde tüm birimlerin bilgilerini kapsayacak şekilde doldurulmalıdır.

Gizlilik: Bu bilgiler, sadece istatistiksel çalışmalarda kullanılmak amacıyla toplanmaktadır. Elde edilen bilgilerin gizliliği 5429 Sayılı Kanunun 13. ve 14. maddesi gereği teminat altına alınmıştır. Vereceğiniz bilgiler, idari, adli ve askeri hiçbir organ, makam, merci veya kişiye verilemez, istatistik amacı dışında kullanılamaz ve ispat aracı olamaz.

Bu bilgiler 10.11.2005 tarih ve 5429 sayılı Türkiye İstatistik Kanunu'nun "7., 8., 9. ve 10. maddeleri" uyarınca toplanmaktadır. Soru formunun istenilen zamanda doldurulmaması, eksik veya yanlış cevaplanması durumunda ilgili Kanunun 53.ve 54. maddelerine göre 2.752 (ikibinyediyüzelliiki) TL idari para cezası uygulanır. İdari para cezası ve diğer cezaların uygulanması, istatistiki birimin bilgi verme yükümlülüğünü ortadan kaldırmaz.

Açıklamalar doğrultusunda soru formunun doğru ve eksiksiz doldurulmasını önemle rica eder, araştırma kapsamında vereceğiniz bilgiler ve işbirliğiniz için teşekkür ederim.

Mehmet AKTAŞ
Başkan V.

Soru formu ile ilgili her türlü sorunuz için bulunduğunuz ilin bağlı olduğu TÜİK Bölge Müdürlüğü'ne başvurabilirsiniz.
Bölge Müdürlükleri ve sorumluluk alanına giren iller son sayfada verilmiştir.
Türkiye İstatistik Kurumu
Devlet Mahallesi Necatibey Cad. No: 114 06420 Çankaya/ANKARA
www.tuik.gov.tr

SORU FORMUNUN DOLDURULMASINA YÖNELİK AÇIKLAYICI BİLGİLER

Bu Araştırma Zonguldak İlinde faaliyet gösteren 20 ve daha fazla çalışanı olan girişimlerden örnekleme yöntemi ile tespit edilen girişimlere uygulanmaktadır. Soru formu, birden fazla birimi olan girişimlerin merkezlerinde, bağlı tüm yerel birimlerin bilgilerini kapsayacak şekilde **bilişim teknolojilerinden sorumlu bir yönetici** tarafından doldurulmalıdır.

Soru formunun doldurulmasına ilişkin genel açıklamalar

I. Bu soru formunda yer alan 'kullanım' ifadeleri 'sahiplik' ifadesine karşılık gelmemektedir. Örneğin, bilgisayarın girişim bünyesinde kullanılıyor olması (kiralama vb. yollarla) bilgisayar kullanımı ile ilgili sorulan soruların yanıtlanabilmesi için yeterlidir.

II. Sorulan teknolojiler, girişim adına başka kişi ya da girişimler tarafından kullanılıyorsa, (örneğin teknoloji, işlemi girişim adına yapan ancak girişim dışında faaliyet gösteren bir muhasebeci tarafından yapılıyorsa), cevaplayıcı girişimin ilgili teknolojiyi kullanmadığı anlaşılmalıdır. Ancak bazı durumlarda teknoloji hem cevaplayıcı birim, hem de başka bir kişi ya da girişim tarafından kullanılıyor olabilir. Bu durumda aşağıdaki kriterler esas alınmalıdır:

a. Çoğu kez web hizmetler dışarıdan satın alınır / kiralanır ve yönetilir. Bu durumda, yukarıda belirtilen kriterden farklı olarak girişimin söz konusu web sitesinin içeriği üzerinde "kontrol ve sorumluluk" hakkının olması yeterlidir.

b. E.ticaret konusunda da benzer durumlar olabilir. Örneğin hizmet online marketler üzerinden (bu siteler başka bir girişime aittir) yapılsa bile, cevaplayıcı birimin kendine ayrılmış bölümde ürünlerini pazarlaması ve satış yapması, e.ticaret için yeterlidir.

III. Soru formunda yer alan bazı tanımlar aşağıda verilmiştir.

Girişim: Birinci derecede karar alma özerkliğini kullanarak, mal veya hizmet üreten bir organizasyon biçimidir. Girişim bir veya birden fazla faaliyet yürütebilir. Girişim ve yasal birim arasındaki ilişki şu tanımla doğrudan ifade edilir: Bir girişim ya yasal birime ya da yasal birimlerin birleşimine karşılık gelmektedir.

Bilgisayar: Masaüstü bilgisayar, laptop, tablet bu çalışma kapsamında bilgisayar olarak değerlendirilmelidir. Yazarkasalar, POS cihazları, akıllı telefon (smartphone) ve bilgisayar kontrollü makineler bilgisayar kapsamında değildir.

web: World Wide Web (kısaca WWW veya web), birbiriyle bağlantılı, İnternet üzerinde çalışan ve "www" ile başlayan adreslerdeki sayfaların görüntülenmesini sağlayan servistir.

Mobil uygulama : Smartphone (akıllı telefon), tabletler gibi cihazlara özel olarak kodlanmış ve tasarlanmış yazılımlardır.

e.ticaret: İşletmeler, haneler, kişiler, kamu veya özel sektör kurum ve kuruluşları arasında bilgisayar ağları üzerinden bir malın alışı veya satışının gerçekleşmesi olarak tanımlanmaktadır. e.posta ile alınan siparişler kapsam dışındadır.

Siber saldırı : Bilgisayar ve internet alanında uzmanlaşmış hacker diye tabir edilen gruplarının banka, polis, jandarma, devlet, şahıs, girişim vb. sitelere veya bilgisayarlara zarar vermek amacı ile yaptıkları saldırılardır. Bu saldırılar neticesinde bilgisayara ya da sitelere solucanlar, trojenler sokarak ya da açıklar aranıp bulunarak bilgiler ele geçirilebilir veya var olan bilgiler yok edilebilir.

Gizlilik Mührü veya sertifikası : Sunucu ile istemci (yani kullanıcı) arasındaki veri akışının şifrelenmesidir.

Bölüm I . Bilgisayar ve İnternet Durumu

1. **Girişiminizde kaç bilgisayar bulunmaktadır?**

   (Masaüstü bilgisayar, laptop, tablet dahil, cep telefonları hariç tutulmalıdır.)

   (C1) ☐ Adet

2. **Girişiminizin internet erişimi var mı?**

   (C2) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 31'e geçiniz.

3. **Girişiminizde ana bilgisayar *(sunucu, server)* var mı?** *(Sanal sunucular dahil edilecektir.)*
   Sanal Sunucu *: Bir fiziki sunucunun sanal olarak bölünmesiyle elde edilen sunucu.*

   (C3) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 4'e geçiniz.

   3.1. Sayısı **(C3.1)** ☐ Adet

4. **Girişiminizde bilgi işlem birimi var mı?**

   (C4) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 5'e geçiniz.

   4.1. Bilgi İşlem Biriminde 2016 yılında ortalama çalışan personel sayısı **(C4.1)** ☐ Kişi

   4.2. Bilgi İşlem Birimi için 2016 yılı içerisinde gerçekleştirilen harcama **(C4.2)** ☐ TL

5. Bilgi işlem işleriniz için dışarıdan destek alıyor musunuz?

(C5) Evet ☐ 1 Hayır ☐ 2

Bölüm II . İnternet Güvenliği

6. Güvenlik duvarı (firewall) kullanıyor musunuz?

Güvenlik Duvarı (Firewall) *: Bilgisayarınıza ya da bilgisayar ağınıza yetkisiz veya istemediğiniz kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır.*

(C6) Evet ☐ 1 Hayır ☐ 2 ➡ Soru 8'e geçiniz.

7. Ne tür güvenlik duvarı (firewall) kullanıyorsunuz? *(Her satırda bir kutuyu işaretleyiniz.)*

		Evet	Hayır
Açık kaynak kodlu güvenlik duvarı *(Kullanıcıya yazılımı değiştirme imkanı sağlayan yazılımlardır.)*	(C7.1)	☐ 1	☐ 2
Kutu çözüm güvenlik duvarı *(Ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir.)*	(C7.2)	☐ 1	☐ 2
Telekom, ttnet gibi firmaların sunmuş olduğu hizmet	(C7.3)	☐ 1	☐ 2

8. Bilgisayarlarınızda anti virüs programı kullanıyor musunuz? ***(*** *Her satırda bir kutuyu işaretleyiniz.)*

		Evet	Hayır
Lisanslı anti virüs programı	(C8.1)	☐ 1	☐ 2
Lisanssız (veya ücretsiz) anti virüs programı	(C8.2)	☐ 1	☐ 2

9. Ana bilgisayarınızda (sunucu, server) anti virüs programı kullanıyor musunuz? *(Bölüm I Soru 3'e evet cevabı veren girişimler tarafından cevaplandırılacaktır. Soru 3'de hayır cevabı verenlere soru 10 sorulacaktır. Her satırda bir kutuyu işaretleyiniz.)*

		Evet	Hayır
Lisanslı anti virüs programı	(C9.1)	☐ 1	☐ 2
Lisanssız (veya ücretsiz) anti virüs programı	(C9.2)	☐ 1	☐ 2

10. Girişiminizde IDS-IPS ve DDOS saldırı engelleyici kullanıyor musunuz?

IDS *: Intrusion Detection Systems: Kötü niyetli ağ hareket ve bağlantılarının tespiti için kullanılan sistem. Amacı kötü niyetli ağ hareketlerinin önlenmesidir.*

IPS *: Intrusion Prevention Systems: Kötü niyetli ağ hareket ve bağlantılarının önlenmesi için kullanılan sistem.Amacı kötü niyetli ağ hareketlerinin önlenmesidir.*
DDOS : *Belli bir sunucunun hizmet bekleyen kullanıcılara hizmet vermesini engellemek amacıyla yapılan saldırılardır.*

(C10) Evet ☐ 1
Hayır ☐ 2
Bu konuda bilgim yok ☐ 3

Bölüm III . Girişimde Var Olan Uygulamalar (Bu bölümdeki soruları 2016 yılını referans alarak yanıtlayınız.)

11. Girişiminizde aşağıdaki uygulamalardan hangileri mevcuttur? *(Her satırda bir kutuyu işaretleyiniz. Web sitesi ve mobil uygulamalar olmayan girişimler için Soru 15'e geçiniz.)*

		Evet	Hayır
Web Sitesi	(C11.1)	☐ 1	☐ 2
Mobil uygulamalar	(C11.2)	☐ 1	☐ 2

12. Girişiminiz 2016 yılında web sitesi ya da mobil uygulamalar üzerinden ürün/ hizmet siparişi aldı mı? *(Bölüm III. Soru 11'in herhangi bir şıkkına evet cevabı veren girişimler tarafından cevaplandırılacaktır.)*

(Online mağazalar, kendi web siteniz ya da mobil uygulamalar üzerinden alınan siparişleri dahil ediniz. E.posta, telefon ve faks ile alınan siparişleri hariç tutunuz.)

(C12) Evet ☐ 1 Hayır ☐ 2 ➡ Soru 14'e geçiniz.

13. Girişiminizin 2016 yılında web sitesi ya da mobil uygulamalar üzerinden aldığı siparişlerin toplam cironuz içindeki payı ne kadardı?

%(C13) ☐

14. Web sitesi ya da mobil uygulamarınızın güvenliği ile ilgili olarak gizlilik mührü veya sertifikası (SSL, TSL, vb.) **var mı?**

(C14) Evet ☐ 1 Hayır ☐ 2

15. Girişiminizin Adını Taşıyan Kurumsal Mail Sunucunuz var mı? *(xxxx@tuik.gov.tr , xxxxx@bakka.gov.tr , xxxx@beun.edu.tr gibi)*

(C15) Evet ☐ 1 Hayır ☐ 2

Bölüm IV . Girişimin Uygulamalarına Yapılan Siber Saldırılar ve Sebep Olduğu Kayıplar (Bu bölümdeki soruları 2016 yılını referans alarak yanıtlayınız.)

16. Mobil uygulamalarınız veya web sitenize herhangi bir siber saldırı oldu mu?

(C16) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 17'e geçiniz.

16.1. Saldırı sayısı (C16.1) ☐ kez

16.2. 2016 yılında uygulamalarınız kaç gün devre dışı kaldı (C16.2) ☐ gün

16.3. 2016 yılındaki maddi kaybınız (C16.3) ☐ TL

17. E-mail yoluyla saldırıya uğradınız mı? (Soru 15'e evet cevabı veren girişimler tarafından cevaplandırılacaktır.)

(C17) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 18'e geçiniz.

17.1. Saldırı sayısı (C17.1) ☐ kez

17.2. 2016 yılında uygulamalarınız kaç gün devre dışı kaldı (C17.2) ☐ gün

17.3. 2016 yılındaki maddi kaybınız (C17.3) ☐ TL

18. Ana bilgisayarınıza (sunucu, server) siber saldırı oldu mu? *(Bölüm I Soru 3'e evet cevabı veren girişimler tarafından cevaplandırılacak)*

(C18) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 19'a geçiniz.

18.1. Saldırı sayısı (C18.1) ☐ kez

18.2. 2016 yılında kaç gün devre dışı kaldı (C18.2) ☐ gün

18.3. 2016 yılındaki maddi kaybınız (C18.3) ☐ TL

19. Bilgisayar Virüsleri, Truva atı, Solucan gibi zararlı yazılımlar ile çalışanlardan kaynaklı (şifresini başkasına verme, başkasının şifresini kullanma, dikkatli davranmama gibi) nedenlerden dolayı siber saldırıya uğradınız mı?

(C19) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 20'ye geçiniz.

19.1. Saldırı sayısı (C19.1) ☐ kez

19.2. Sunmuş olduğunuz hizmet veya sisteminiz kaç gün devre dışı kaldı (C19.2) ☐ gün

19.3. 2016 yılındaki maddi kaybınız (C19.3) ☐ TL

20. Girişiminiz, oltalama (phishing) saldırıları veya sosyal mühendislik olarak tabir edilen telefon ya da e-posta ikna yöntemleriyle saldırıya uğradı mı?

(C20) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 21'e geçiniz.

20.1. Saldırı sayısı (C20.1) ☐ kez

20.2. Sunmuş olduğunuz hizmet veya sisteminiz kaç gün devre dışı kaldı (C20.2) ☐ gün

20.3. 2016 yılındaki maddi kaybınız (C20.3) ☐ TL

21. Hard disk bozulması nedeni ile veri kaybı yaşadınız mı?

(C21) Evet ☐ 1 Hayır ☐ 2

22. Hard disk bozulması nedeni ile maddi zarara uğradınız mı?

(C22) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 23'e geçiniz.

22.1. Maddi zarar (C22.1) ☐ TL

23. Aşağıdaki uygulamalardan dolayı zarara uğradınız mı? *(Her satırda bir kutuyu işaretleyiniz.)*

23.1. Lisanssız yazılım kullanımı (C23.1) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 23.2'ye geçiniz.

23.1.1. Maddi zarar (C23.1.1) ☐ TL

23.2. Endüstriyel casusluk (C23.2) Evet ☐ 1 Hayır ☐ 2 ➞ Soru 24'e geçiniz.

23.2.1. Maddi zarar (C23.2.1) ☐ TL

Bölüm V . Siber Saldırılara Karşı Alınan Güvenlik Önlemleri (Bu bölümdeki soruları 2016 yılını referans alarak yanıtlayınız.)

24. Siber saldırılara müdahale ekibiniz (SOME) var mı?

(C24) Evet ☐ 1 ➡ Soru 26'ya geçiniz. Hayır ☐ 2

25. SOME birimi kurmayı planlıyor musunuz?

(C25) Evet ☐ 1 Hayır ☐ 2

26. Girişiminizde resmi olarak tanımlanmış ve düzenli olarak gözden geçirilen planlı bir bilgi ve iletişim teknolojisi (BİT) güvenliği politikası var mı?

(C26) Evet ☐ 1 Hayır ☐ 2 ➡ Soru 29'a geçiniz.

27. Aşağıda belirtilen risklerden hangisi / hangileri BİT güvenliği politikanızda yer aldı? *(Her satırda bir kutuyu işaretleyiniz.)*

		Evet	Hayır
Beklenmeyen bir olay veya saldırı nedeniyle verilerin bozulması ya da kaybolması	(C27.1)	☐ 1	☐ 2
Başka siteye yönlendirilerek şifre çalınması	(C27.2)	☐ 1	☐ 2
İstenmeden güvenli verilerin açıklanması	(C27.3)	☐ 1	☐ 2
Dışarıdan saldırı nedeniyle BİT hizmetlerinin verilememesi	(C27.4)	☐ 1	☐ 2

28. BİT güvenliği ile ilgili olarak aşağıda belirtilen olaylardan girişiminize ait sistemler etkilendi mi?
(Her satırda bir kutuyu işaretleyiniz.)

		Evet	Hayır
Donanım veya yazılım hataları nedeniyle verinin bozulması ya da kaybolması sonucunda BİT hizmetlerinin verilememesi	(C28.1)	☐ 1	☐ 2
Başka siteye yönlendirilerek şifre çalınması	(C28.2)	☐ 1	☐ 2
İstenmeden güvenli verilerin elektronik ortamda açıklanması	(C28.3)	☐ 1	☐ 2
Dışarıdan saldırı nedeniyle BİT hizmetlerinin verilememesi	(C28.4)	☐ 1	☐ 2
Kötü amaçlı yazılım veya yetkisiz erişim nedeniyle verinin bozulması veya kaybolması	(C28.5)	☐ 1	☐ 2

29. Aşağıda belirtilen dahili güvenlik yöntemleriden hangileri girişiminiz tarafından uygulandı? *(Her satırda bir kutuyu işaretleyiniz.)*

		Evet	Hayır
Güçlü parola ve kimlik doğrulama (Örneğin: minimum 8 karma karakter, maksimum 6 ay süre, şifrelenmiş iletim ve depolama)	(C29.1)	☐ 1	☐ 2
Donanım belirtici yardımıyla kullanıcı tanımlama ve kimlik doğrulama *(Örneğin : Akıllı kartlar)*	(C29.2)	☐ 1	☐ 2
Biometrik yöntemlerle kullanıcı tanımlama ve doğrulama	(C29.3)	☐ 1	☐ 2
Farklı mekanlarda veri yedekleme	(C29.4)	☐ 1	☐ 2
Güvenlik olaylarının analizi için listeme faaliyetleri	(C29.5)	☐ 1	☐ 2

Bölüm VI . Girişimin Web Sitesi ve Mobil Uygulamaları İçin Yapmış Olduğu Harcamalar ve Girişimin Ekonomik Büyüklüğü

30. Web sitesi veya mobil uygulamalar için 2016 yılında harcama yaptınız mı?

(C30) Evet ☐ 1 Hayır ☐ 2 ➡ Soru 31'e geçiniz.

30.1. Harcama tutarı (C30.1) ☐☐☐☐☐☐☐☐☐ TL

31. Girişimin 2016 yılı cirosu için aşağıdaki uygun seçeneklerden birini işaretleyiniz.

100.000 TL veya daha az	(C31.1)	☐ 1
100.001-500.000 TL arası	(C31.2)	☐ 2
500.001-1.000.000 TL arası	(C31.3)	☐ 3
1.000.001 TL veya daha fazlası	(C31.4)	☐ 4

32. Girişiminizde 2016 yılı Kasım ayı itibariyle ücretli çalışan personel sayısı için aşağıda uygun seçeneklerden birini işaretleyiniz.

1-19	(C32.1)	☐ 1
20-49	(C32.2)	☐ 2
50-99	(C32.3)	☐ 3
100-249	(C32.4)	☐ 4
250+	(C32.5)	☐ 5

ÖZGEÇMİŞ

Muhammed TEMLİ, 1980 yılında Karabük'te doğmuştur. İlk, orta ve lise öğrenimlerimi Karabük'te tamamlamasının ardından üniversite hayatına 19 Mayıs Üniversitesi Samsun Meslek Yüksek Okulu Bilgisayar Programcılığında başlamıştır. Devamında Anadolu Üniversitesi Çalışma Ekonomisi ve Endüstri İlişkileri bölümünü bitirip Bülent Ecevit Üniversitesi İktisat Fakültesi bölümünde yüksek lisans yapmıştır.

Profesyonel Meslek Hayatına 2000 yılında e-devlet projelerinin en önemlilerinden biri olan Mernis Projesi ile başlamıştır. 2010 yılına kadar alanının iki büyük firması olan Meteksan Sistem ve Koç Sistem firmalarında 100'e yakın ulusal ve uluslararası projelerde uzman, saha sorumlusu ve saha koordinatörü olarak görevler almıştır. 2010 yılından itibaren Batı Karadeniz Kalkınma Ajansı'nda Bilgi İşlem Sorumlusu ve Siber Olaylara Müdahale Ekibi Personeli olarak görev yapmakta olup, Bülent Ecevit Üniversitesi'nin farklı bölümlerinde kendi uzmanlık alanı ile ilgili dersler vermiştir.

Ülkenin önemli ulusal bilişim projelerinde görev alarak çeşitli sertifikalara sahip olan Temli, halen siber güvenlik konusunda akademik çalışmalar yapmaktadır. Evlidir. İki çocuk babasıdır ve mesleki düzeyde İngilizce bilmektedir.

Alınan Bazı Eğitim ve Sertifikalar

Certified WhiteHat Hacker C.E.H (60 Saat)

Siber Güvenlik Eğitimi (60 Saat)

CPTE: Certified Penetration Testing Engineer (30 Saat)

MS 6231 Maintaining a Microsoft SQL Server 2008 R2 Database (30 Saat)

MS 6232 Implementing a Microsoft SQL Server 2008 R2 Database (30 Saat)

Configuring, Managing and Troubleshooting Microsoft Exchange Server 2010 (30 Saat)

CISCO IP V6 (30 Saat)

Alınan Başarı Belgesi

Zonguldak Valiliği Başarılı Çalışma Belgesi

İletişim:

muhammedtemli@gmail.com