

SİBER SALDIRILARIN FİRMALARA ETKİLERİ: ZONGULDAK ÖRNEĞİ¹

Yrd. Doç. Dr. Zafer ÖZTÜRK

Bülent Ecevit Üniversitesi, İİBF, (zaferozturk@beun.edu.tr)

Doç. Dr. Mehmet PEKKAYA

Bülent Ecevit Üniversitesi, İİBF, (mehpekkaya@gmail.com)

Muhammed TEMLİ

Batı Karadeniz Kalkınma Ajansı

ÖZET

Günümüzde suç ekonomisinin kapsamı ve hacmi çok önemli boyutlara ulaşmıştır. Gelişen teknolojiyle birlikte birçok suç türü internet ortamına taşınmıştır. Suçlunun mağdura birebir temas etmesini gerektiren birçok suç artık uzaktan işlenebilmektedir. Bu çalışmada Zonguldak ilinde faaliyet gösteren firmaların siber saldırılar nedeniyle uğradıkları maddi zararların ekonomik boyutu ortaya çıkartılmaya çalışılmıştır. Çalışmada, firma ölçekleri büyüdükçe, daha yoğun teknoloji ve bilişim altyapısına ihtiyaç duyulacağı öngörülerek Zonguldak ilinde faaliyet gösteren 20'den fazla personel istihdam eden firmalara anket uygulanmıştır. Firmaların çoğunun saldırılar konusunda yeterli bilgisinin olmadığı kaydedilmiştir. Ayrıca artan bilgi işlem yatırımlarının saldırılar ve verdiği zararlar ile ilişkili olduğu görülmüştür.

Anahtar Kelimeler: Siber Saldırı, Suç Ekonomisi, Siber Suçlar.

EFFECTS OF CYBER ATTACKS ON FIRMS: THE CASE OF ZONGULDAK

ABSTRACT

Today, the scope and volume of the criminal economy has reached very important dimensions. Along with the developing technology, many crime types have been moved to the internet environment. Many crimes, which require the criminal to contact to the victim personally, can now be processed remotely. In this study, it is tried to reveal the economic dimension of the financial losses of companies operating in Zonguldak province due to cyber attacks. In the study, as the scale of the company grows, it is predicted that more intensive technology and information infrastructure will be needed and a questionnaire was applied to the firm that employs more than 20 personnel operating in the province of Zonguldak. It is noted that most of the companies do not have enough knowledge about the attacks. It has also been found that increased information processing investments are associated with attacks and damages.

Keywords: Siber Attack, Crime Economy, Cyber Crime.

¹ Bu çalışma Muhammed TEMLİ'nin "Siber Suçların Ekonomik Boyutu: Zonguldak Örneği" başlıklı yüksek lisans tezinden üretilmiştir. Ayrıca tez çalışması, Bülent Ecevit Üniversitesi BAP birimince desteklenmiştir.

1. Giriş

Kayıt dışı ekonominin ekonomik faktörler başta olmak üzere yaşamın her alanına önemli etkileri mevcuttur. Gelir dağılımından istihdama olan etkisine, vergilerden ekonomik büyümeye kadar ciddi etkileri bulunan kayıt dışı ekonomi olgusu gelişmiş ülkeler ve gelişmekte olan ülkelerde birbirinden farklılık göstermektedir. Az gelişmiş ve gelişmekte olan ülkelerde kayıt dışına yönelmekteki asıl amaç vergiden kurtulmaktır. Gelişmiş ülkelerde ise bireyler ve firmalar vergi kaçırma ile beraber yasal düzenlemelerden kurtulmak içinde kayıt dışına yönelmektedir (Losby vd., 2002). Kayıt dışı ekonomik faaliyetler her an kendini güncelleyen ve teknolojiye hızlı ayak uydurabilen canlı bir konudur. Bu nedenle konu hükümetlerin dikkatini çekmiş akademisyenler tarafından üzerinde çalışmalar yapılmıştır.

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. 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. Suçlunun mağdurla birebir temas etmesini gerektiren birçok suç artık internet aracılığı ile uzaktan işlenebilmektedir. Bu nedenle ekonomik suça neden olan bilişim suçları diğer ismi ile siber suçlar içerik, kapsam ve hacim olarak önemli boyutlara ulaşmıştır. Özetle geleneksel ya da sanal olması fark etmeksizin kanunlar tarafından suç olarak tanımlanmış faaliyetler sonrası elde edilen kazançlar suç ekonomisini oluşturmaktadır.

Siber saldırıların ekonomik yansımalarının zamanla daha da artacağı tahmin edilmektedir. 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 görülmektedir. Bu çalışma, yıllar itibariyle sayısı giderek artan siber saldırıların Zonguldak ilinde sebep olduğu ekonomik zararların boyutunu ortaya çıkarmak amacı ile yapılmıştır. Literatürde bu konuda çalışmalar oldukça sınırlı olduğundan çalışmamız özellikle literatüre bu yönde katkı sağlayacaktır.

Siber saldırıların ekonomik büyüklüğünü belirlemek için veriler anket yolu ile elde edilmeye çalışılmıştır. Anket uygulanan 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 anket uygulanarak TÜİK Zonguldak Bölge Müdürlüğü tarafından gerçekleştirilmiştir.

Konulara göre elde edilen anket verilerinden elde edilen bulgular, frekans tabloları ve kontenjans tabloları üzerinden raporlanmıştır. Değişkenler arasında sistematik bir ilişkinin olup olmadığını ki-kare testi üzerinden değerlendirilmiştir.

Çalışmanın birinci bölümünde kayıt dışı ekonomi, nedenleri, türleri ve suç ekonomisi üzerinde durulmuştur. Çalışmanın ikinci bölümünde siber suçlar irdelenerek içerik ve kapsam olarak birçok siber saldırının suç ekonomisi kapsamında olduğu ve aslında siber saldırıların geleneksel suçtan çokta ayrı olmadığı görülmüştür. Üçüncü bölümde Zonguldak'ta yaşanan siber saldırılar ve yatırımlar arasındaki ilişki analiz edilmiştir. Sonuç bölümünde ise daha önceki anlatılan konular çerçevesinde analiz bölümünde çıkan bulgular tartışılmıştır.

2. Kayıt Dışı Ekonominin Nedenleri ve Etkileri

Kayıt dışı ekonomiyi ortaya çıkaran en önemli nedenlerin başında ekonomik nedenler gelmektedir. Kayıtlı çalıştığı işten yeterli ücret alamayan bireylerin ikinci bir işte çalışması ve tarım sektörü gibi emek yoğun alanlarda kadın ve çocukların çalıştırılması kayıt dışı ekonomiyi artırmaktadır (Us, 2004:11). Enflasyonun artması ödenecek vergi miktarını (Karaman, 1999:431), ödenecek faiz miktarını (Özcan, 2003:46-48) ve girdi maliyetlerini değiştirmektedir. Dolayısı ile enflasyonun verdiği zararlar firmalar tarafından ağır rekabet koşullarında kayıt dışı ekonomi ile karşılanmaya çalışılmaktadır.

Ekonomik faaliyetlerin kayıt dışı etkileri hakkında yapılan çalışmalardan görüldüğü üzere iktisatçılar arasında görüş farklılıkları bulunmaktadır. Kimi iktisatçılar ülke ekonomisine zarar verici etkilerinin olduğunu ileri sürerken, farklı görüşte olan iktisatçılar ise sanılanın aksine faydalı etkilerinin olduğunu ileri sürmüşlerdir (Özsoylu, 1994:14).

Özellikle olumsuz etkilerinden bahseden iktisatçılar, kayıt dışı ekonomik faaliyetlerin vergi gelirlerinin azalmasına sebep olduğunu ileri sürmektedir. Vergilerin azalması ise bütçe açıkları oluşturur, oluşan bütçe açıklarının ülkeler tarafından para basılarak karşılanması enflasyon oranlarını yükseltmektedir (Sarıkaya, 2007:47). Kayıt dışı faaliyet yürüten firmalar vergi gibi rekabet üzerinde ciddi etki oluşturan sigorta ve diğer kesintileri de ödemediklerinden dürüst firmalara göre daha düşük maliyetlerle ürün ve hizmet üretebilmekte ve piyasaya daha ekonomik ürünler sunabilmektedir (Sarılı, 2002:12). Dolayısı ile bu tip firmaların satış hacimleri ve karlılıkları artmaktadır (Öğünç ve Yılmaz, 2000:5).

Daha çok olumsuz etkisinden bahsedilse de klasik iktisatçıların ileri sürdüğü *homo economicus* anlayışına göre bireyler kendi çıkarlarını en yüksek düzeye yükseltmek üzerine hareket ederken dolaylı olarak toplum refahını yukarıya çekmektedir (Öztürk, 2006:20). Kayıt dışının olumlu etkisinin temeli olarak gözüken bu yaklaşım, bir takım iktisatçılar tarafından da desteklenmektedir. Bu yaklaşıma göre kayıt dışı ekonomi, özellikle ülkelerin zor zamanlarında, bireylere istihdam sağladığından ekonominin hareketlenmesini sağlayacağı ileri sürülmektedir (İlgin, 1999:45).

Kayıt dışı ekonominin olumlu ve olumsuz yönlerinin yanı sıra suç teşkil eden ve etmeyen yapısı da bulunmaktadır. Kayıt dışı ekonominin suç teşkil etmeyen yapısı, gerçekleştirilen yasal faaliyetler sonucu elde edilen fakat hukuki boşluklar, denetim mekanizmalarının eksikliği gibi beyan dışında tutulan vergilendirilmemiş kazançlar olarak tanımlanabilir (Mavral, 2001:171). Kayıt dışı ekonominin suç teşkil eden yapısı ise bireylerin veya toplumun iktisadi menfaatlerinin ihlâl edilmesi sonucu orta çıkmakta olup genel olarak ekonomik suçları ifade etmektedir (Tiryaki ve Gürsoy, 2004:54).

Kayıt dışı ekonominin bir alt unsuru olan suç ekonomisi literatürde mafya ekonomisi, yeraltı ekonomisi, yasa dışı ekonomi ve kurşun ekonomisi olarak da adlandırılmaktadır (Altuğ, 1999:3). Suç ekonomisinde önemli olan faaliyetlerin kanunen hukuksuz olmasıdır. Yapılan çalışmanın kanunlara aykırı olmasından dolayı bu faaliyetlerden elde edilen gelirlerde kayıt dışı ve suç olarak kabul edilmektedir (Aktürk, 2005:300). Örneğin uyuşturucunun üretimi, kullanımı, alım satımı, silah kaçakçılığı, organ kaçakçılığı gibi faaliyetler yasaklanmış faaliyetlerdir ve bu alandan kazanılan paralarda suç ekonomisini oluşturmaktadır. Dünyada teknolojik gelişmelerin yaşanması ile birlikte birçok bilişim araçları yaşamımızın bir parçasını olmuştur. Bilgisayar tabanlı cihazlar yeni suç yaklaşımları oluşturmaktadır. Bu sayede birçok suç türü internet ortamına taşınmıştır. Suçlunun mağdura birebir temas etmesini gerektiren birçok suç artık internet aracılığı ile uzaktan işlenebilmektedir. Bu nedenle ekonomik suç içerik, kapsam ve boyut olarak zaman içerisinde genişlemektedir.

3. Siber Suçlar

Dünyada teknolojik gelişmelerin yaşanması ile birlikte bilişim sistemleri hayatımızın her alanına girmiştir. Yeni suç tipleri oluşmakta, suçlular teknolojiye ayak uydurarak yasa dışı faaliyetlerini sürdürmektedirler. Özellikle bilişim sistemlerinin kullanılması ile işlenen suçlarda büyük bir artış görülmektedir. 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 kullanılmaktadır (Dülger, 2004:64-65).

Diğer adi suçlardan daha farklı yaklaşımlar ile karşımıza çıkan bilişim suçları, günümüzde daha çok kredi kartı dolandırıcılığı, banka hesaplarının boşaltılması, kullanıcının bilgisayarındaki verilerin şifreleyerek tekrar aynı kullanıcıya satılması, endüstriyel casusluk, bilgi kaçakçılığı gibi yöntemler (Temli, 2014:80) ile maddi zararlar vermektedir. Ayrıca geleneksel suçlara göre daha zor tespit edilebilmektedir. Adli analiz yöntemleri ve tutulan log kayıtları verileri ile siber suçlar tespit edilebilse dahi çoğu zaman adli işlem yapılamamaktadır. Bu durumun sebepleri şu şekilde sıralanabilir;

1. Siber saldırılar neticesinde firma ya da bireylerin bilgileri çalınsa dahi, firma ya da bireyler verilerinin çalındığını duyurmak istememektedir.
2. Siber saldırıların duyurulması şirketleri özellikle borsa gibi farklı ortamlarda zor duruma düşürdüğünden firmalar saldırıları gizlemeye çalışmaktadır.
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.
6. Doğrudan maddi zarar görmeyen kişiler saldırıyı önemsememekte dolayısı ile genel çözüm üretilmemektedir.

4. Zonguldak İlinde Siber Saldırıları

Siber güvenlik olgusu her geçen gün önemi daha da çok anlaşılan bir konudur. Siber güvenlik çalışmalarına sebep olan siber saldırılar aslında sadece öylesine yapılan, ya da gençlerin eğlenmek için yapmış oldukları bir eğlence aracı değildir. “Bir ara anti virüs ile sistemi taratır gerekirse bilgisayarını yeniden kurarız. Çok önemli değil” algısı ile konuya yaklaşan şirketler artık gerçeğin çok da öyle olmadığını maddi ve manevi kayıplar ile anlamaya başladığı görülebilir. 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, 2016).

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 yazılımının verdiği maddi zararlar 2016 yılında bir milyar doları geçmiştir (Xtrlarge, 2017). Özellikle 2017 yılında ortalığı kasıp kavuran 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). Dünya çapındaki internet trafiğinin ve siber tehditlerin izlenmesine olanak veren bazı platformlar, günümüzde dünya çapında haftada ortalama 124 bin, Türkiye’de ise haftada 18 bin saldırı gerçekleştiğini rapor etmektedir (Kara, 2016).

Siber saldırılar tüm dünyada ve ülkemizde artış gösterdiği gibi Zonguldak ilinde de artış göstermektedir. Çalışmada Zonguldak ilinde yaşanan siber saldırıların ekonomik boyutlarının incelenmesi ve değerlendirilmesi amaçlanmıştır. Bu genel amaç doğrultusunda Zonguldak ilinde bulunan firmalar 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.

Verilerin elde edilmesinde anket yöntemi kullanılmıştır. Araştırma Zonguldak ilinde 20 den fazla personel çalıştıran firmalara uygulanmıştır. TÜİK verilerine göre 20’den fazla personel çalıştıran 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 TÜİK tarafından rassal olarak seçilen 20’den fazla personel istihdam eden 336 firmaya yine TÜİK tarafından anket uygulanmıştır. TÜİK’in elde ettiği anket verileri çalışmadaki araştırmacılar tarafından analiz edilmiştir. Örneklem rassal seçildiğinden analizlerden yapılan tüm çıkarsamaların Zonguldak’ı temsil ettiğine karar verilmiştir.

4.1. Zonguldak İlindeki Firmaların Network Yapısı

Tablo 1’de Zonguldak ilindeki firmaların %80,1’inin 10 bilgisayar ya da daha azına sahipken 10 – 20 arası bilgisayarlara sahip firmalar %13,1 olduğu görülmektedir. Örneklemde 20 -100 arasında bilgisayara sahip %5,4 oranında firma bulunmaktadır.

Tablo 1: Firmaların Bilgisayar Sayıları

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

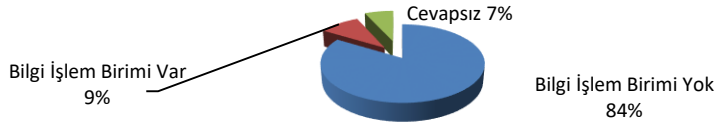
Örneklemden çıkan bir diğer sonuçta firmaların 151’inde sunucu bulunurken bu oran ankete katılanların %44,9’unu oluşturmaktadır. Tablo 2’de görüldüğü gibi networkünde sunucu bulunduran firmaların %37,8’inde 1 sunucu bulunmakta iken %4,8’inde 2 sunucu bulunduğu görülmektedir. 2 den fazla sunucu barındıran firmalar ise %2,4’tür.

Tablo 2: 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 1’de gösterilmektedir. Şekil 1 incelendiğinde firmaların %84’ünde bilgi işlem birimi bulunmadığı, toplamda bilgi işlem birimi olan firmaların oranı ise %9 olduğu görülmektedir.

Şekil 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'te gösterilmiştir.

Tablo 3: 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

Tablo 4'te bilgi işlem için dışarıdan hizmet alım durumu görülmektedir. Tabloya göre firmaların %65,8'i dışarıdan destek aldığı 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.

Tablo 4: Bilgi İşlem Hizmeti İçin Dış Destek Kullanma Durumu

	Hayır	Evet	Toplam	Cevapsız	Genel Toplam
Firma sayısı	99	221	320	16	336
Yüzde	29,5	65,8	95,2	4,8	100

Çalışmada birçok kurum için olmazsa olmaz olarak kabul edilen Firewall kullanım bilgileri sorulmuştur. Firmalardan %61,6'sı firewall kullanmadığını ifade ederken firewall kullanan ve Tablo 5'te 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.

Tablo 5: Firewall Kullanım Çeşitleri

	A. K. K.Fireall	K.Ç. Firewall	D.Ç. Firewall
Firma Sayısı	26	39	45
Yüzde	7,7	11,6	13,4

A.K.K: Açık Kaynak Kodlu, K.Ç.:Kutu Çözüm, D.Ç.: Diğer Çözüm

Zonguldak'ta büyük oranda lisanslı anti virüs yazılımı kullanılmaktadır. Tablo 6 incelendiğinde firmaların %66,78'i bilgisayarlarında lisanslı anti virüs yazılımı kullandığını beyan ederken, %6,31'i lisanslı ve lisanssız anti virüs yazılımı kullanmadığını belirtmiştir. Ayrıca Tablo 6'da, firmaların bilgisayarlarında lisanssız anti virüs kullanım oranı %22,92 olarak izlenirken, firmaların %9,8'i bu soruya cevap vermemiştir.

Tablo 6: Bilgisayarlarda Anti Virüs Kullanımı

	Bilgisayarlarda lisanssız anti virüs kullanımı		
	Hayır	Evet	Toplam
Bilgisayarlarda lisanslı anti virüs kullanımı	Hayır	19; %6,31	69; %22,92
	Evet	201; %66,78	12; %3,99
	Toplam	220; %73,09	81; %26,91

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

Tablo 7: Sunucularda Anti Virüs Kullanımı

	Sunucularda Lisanssız Anti Virüs Kullanımı		
	Hayır	Evet	Toplam
Sunucularda Lisanslı Anti Virüs Kullanımı	Hayır	12; %12,62	12; %3,99
	Evet	115; %39,20	4; %1,33
	Toplam	127; %51,83	16; %5,32

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 7’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.

Tablo 8: 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

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

4.2. Zonguldak’taki Firmalarda Yazılımsal Altyapı

Firmaların web sitesi ve mobil uygulama kullanım durumları Tablo 9’da gösterilmektedir.

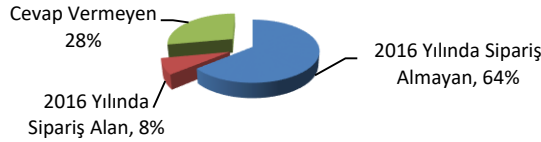
Tablo 9: Firmaların Web Sitesi ve Mobil Uygulama Kullanım Durumları

	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 9’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. 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. Tablo 9’da Zonguldak’taki firmaların %87,2’sinin mobil uygulaması bulunmadığı gözlenirken %4,8’inin ise mobil uygulama kullanmadığı görülmektedir.

Şekil 2: Web Sitesi /Mobil Uygulamalardan Ürün /Hizmet Siparişi Alma Durumu



Şekil 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.

Şekil 3: SSL Kullanım Oranı

Bilginin taşınması sürecinde güvenlik ve gizliliği sağlamak için SSL protokolü

geliştirilmiştir. SSL, sunucu ile istemci arasındaki iletişimin şifreli olarak güvenli bir şekilde yapılmasını sağlamaktadır (İsımtescil, 2016). Şekil 3’te web sitesi ya da mobil uygulamalarında gizlilik mührü veya sertifikası bulunduran firmaların oranının %15,3 olduğu görülmektedir. Firmaların %64,2’si ise SSL kullanmamaktadır.

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 & Aydın, 2007:174).

Tablo 10: E-posta Kullanım Durumu

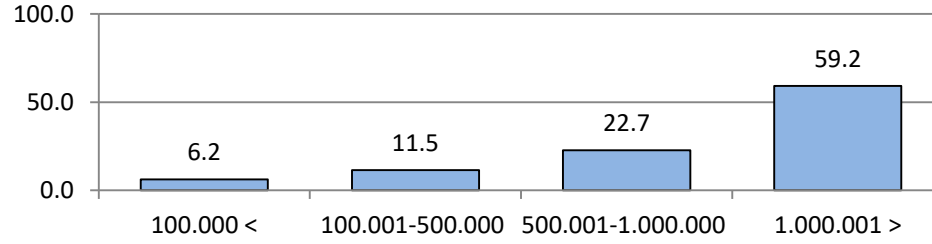
	Hayır	Evet	Toplam	Cevapsız	Genel Toplam
Firma	211	110	321	15	336
Yüzde	62,8	32,7	95,5	4,5	100

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 10'da gösterilmektedir.

4.3. Firmaların Ekonomik Durumu

Ankete katılan firmaların %59,2'si bir milyon liranın üzerinde, %22,7'si 500 bin – 1 milyon arası, %11,5'i 100 -500 bin TL arası, %6,2'si ise 100.000 liranın altında ciroya sahip olduğu Grafik 1'de görülmektedir.

Grafik 1: Girişimlerin Ciro Bilgilerine (TL/yıl) Göre Yüzesel Dağılımı



4.4. Firmaların Karşılaştıkları Siber Saldırıları

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 ortalama 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 11: 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 11'de Zonguldak ilinde yapılan siber saldırı çeşitleri gösterilmektedir. Bu veriler incelendiğinde ilk sırada firmaların e-posta saldırılarıyla karşılaştığı görülmektedir.

Tablo 12: Firmaların e-posta Saldırısına Uğrama Durumu

Saldırı Sayısı	1	2	2+
Firma Sayısı	17	10	10
Yüzde	5,1	3,0	2,9

Tablo 12'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.

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 13: Oltalama Saldırısı ile Karşılaşma Oranı

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

Oltalama saldırısına maruz kalan firmalar ve oranları Tablo 13'te verilmiştir. Zonguldak'ta 2'den fazla saldırıya uğrayan firma sayısı 14 iken 12 firmaya ise 1 defa ortalama saldırısı olduğu kaydedilmiştir.

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 14'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 14: Virüslerinin Sistemi Devre Dışı Bırakma Süresi

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

Virüslerin etkisi incelendiğinde sadece sistemleri devre dışı bırakmadığı maddi zarara da neden olduğu görülmüştür. Örneklemdaki 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.

Firmalarda ana bilgisayarlara yapılan siber saldırılar incelendiğinde 13 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 15'de görülmektedir. Bir firmanın 7 gün, 1 firmanın 5 gün, 5 firmanın ise 1 gün siber saldırılar nedeni ile hizmetinin aksadığı kaydedilmiştir.

Tablo 15: Ana Sunucuya Yapılan Saldırı Sayıları

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

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.

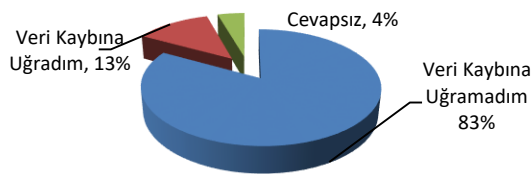
13 firmanın mobil uygulamalarına ya da web sitelerine siber saldırı olduğu kaydedilen örnekleimde Tablo 16'de görüldüğü gibi firmaların %1,8'ine 1 kez, %1,2'sine 2 kez ve %0,3'ün 10 kez saldırıyla karşılaştığı tespit edilmiştir. Firmaların 5 tanesinin toplamda 10 gün sistemleri durduğundan hizmet verememiştir. Ayrıca firmaların biri 1.600 TL ve bir diğeri ise 4.000 TL olmak üzere doğrudan maddi zarara uğradığı da tespit edilmiştir.

Tablo 16: Mobil Uygulamalar ve Web Sitesi Saldırı Sayıları

Saldırı Sayısı	1	2	3	10	Toplam
Firma Sayısı	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. Şekil 4'te görüldüğü gibi firmaların %13'ü harddisk bozulması nedeni ile veri kaybına uğramıştır.

Şekil 4: 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.

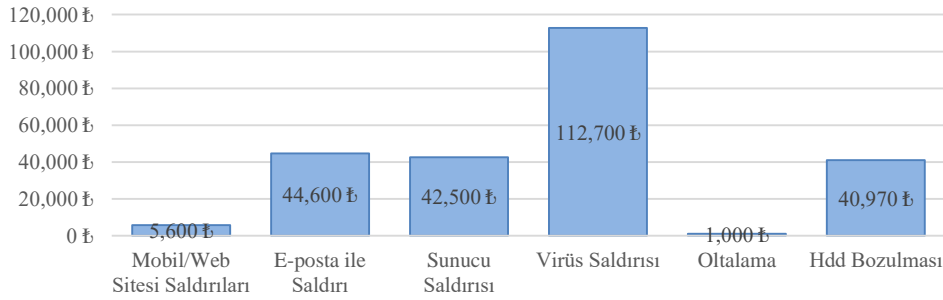
Tablo 17: Uygulanan Güvenlik Yöntemleri

	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

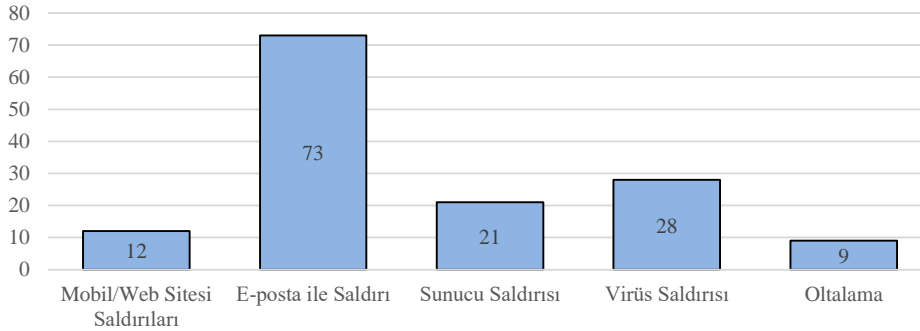
Firmalarda güçlü parola ve kimlik doğrulama (Örneğin: minimum 8 karma karakter, maksimum 6 ay süre, şifrelenmiş iletim ve depolama) uygulanıp uygulanmadığı sorulduğunda 200 firma ile büyük oranda uygulandığı görüldü de 119 firmanın uygulamadığı Tablo 17’de görülmektedir. Ayrıca firmaların %11,6’sının 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.

Grafik 2: Örnekteki Firmaların 2016’da Siber Saldırlardan Uğradığı Zarar (TL)



Firmaların farklı siber saldırılar karşısında uğradıkları toplam zararlar Grafik 2’de gösterilmiştir. Grafik 2 incelendiğinde firmaları en büyük zarara uğratan saldırı türünün virüs saldırıları olduğu görülmektedir. Tüm saldırılar sonucunda Zonguldak’ta 2016 yılında firmaların uğradığı toplam zarar 247.370 TL’dir.

Grafik 3: Örnekteki Firmaların 2016’da Siber Saldırlardan Uğradığı Zarar (Gün)



Aynı şekilde, farklı siber saldırılar sonucunda firmaların uğradıkları iş gücü kaybı Grafik 3’te gösterilmiştir. Grafik 3 incelendiğinde en fazla işgücü kaybının 73 gün ile virüs saldırıları sonucu yaşandığı görülmektedir. Zonguldak’ta firmaların 2016 yılında saldırılar sonucu toplam işgücü kaybı 143 gün olarak tespit edilmiştir.

4.5. Kontenjans Tabloları ve Belirlenen Bazı İlişkiler

Ki- kare testi bağımsız guruplar için iki kategorik değişken arasında bir ilişkinin olup olmadığını test etmek için yaygın kullanılmaktadır. Ki-kare testinin varsayım olarak gerekli kıldığı şekilde verilerimiz kategorik değişkenlerden oluşmaktadır. Test ile beklenen ve gözlemlenen frekanslar üzerinden hipotezdeki iddia edilen ilişki incelenir. Kontenjans tabloları 2x2 olup kategorik değişkenlerle ilişki araştırılması ve ki-kare test istatistiği hesaplamasında bir hücrenin beklenen değeri (frekansı) 5’ten küçük ise ki-kare istatistiği yerine bu durumlarda daha robust görülen Fisher’s test istatistiği ile karar verilmiştir. İlişki inlemelerinde araştırılan alternatif hipotezler aşağıdadır.

H1: Firmalarda kullanılan firewall cihazlarının varlığı ile ana sunuculara yapılan saldırılar arasında ilişki vardır.

Ki-kare testinde p değeri 0,021 olduğundan, istatistiksel olarak %5 anlamlılıkta H0 hipotezi reddedilerek, Firewall kullanımı ile e-posta saldırısına uğrama arasında ilişki olduğuna karar verilmiştir. Ki-kare istatistiğine en büyük katkı² iki soruya da evet cevabı veren grupta beklenen değer 4,98 iken gözlemlenen değer 9 olarak kaydedilmiş olmasıdır. Post hoc testi ile ilgili 4. Hücrenin ki kare istatistiğine 3,24 katkı yaptığı 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 18: Firewall Bulunması ve Ana Bilgisayarlara Saldırısı Arasındaki İlişki

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

Tablo 18 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 19'da ki-kare testinde p değerinin 0,019 olması, firmada firewall cihazının bulunması ile e-posta saldırıları arasında istatistiki olarak 0,05'te anlamlı bir ilişkinin ($p=0,019<0,05$) varlığını desteklemiştir.

Tablo 19: 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
Firewall Kullanımı	Evet	Gözlem	59	20	79
		Beklenen Sayı	65,4	13,6	79
		% Firewall	74,7	25,3	100
Toplam		187	39	226	

Tablo 19'da 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: Kurumsal e-posta kullanan firmalarda, firewall kullanımı ile e-posta saldırılarına uğrama 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 olduğuna karar verilmiştir.

² Ki-kare istatistiğine katkı: Çapraz tabloda her hücre için beklenen ve gözlenen değerlerden, $(G_i - B_i)^2/B_i$ skorlar toplamı 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 20: 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 20’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. Yapılacak çıkarsamalarda, firewall kullananların saldırıları gözlemleyebilme imkânının olması da dikkate alınmalıdır.

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

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

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

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

H4, H5, H6 ve H7 iddiaları, çalışmamızda araştırılmış, ancak bu iddiaların doğru olmadığına istatistiksel olarak 0,05 anlamlılıkta (yapılan ki kare testlerine ait p değerleri sırasıyla 0,457; 0,736; 0,798; 0,484’dür) karar verilmiştir. Dolayısı ile bu analizlerde ilgili değişkenler arasında ilişki gözlenmediğinden, kontenjans tabloları raporlanmamıştır.

5. Sonuç

Her geçen gün artan siber saldırıların birden çok etkisi görülmektedir. Yapılan teorik ve pratik çalışmalar siber saldırıların sadece mühendislik olarak değil diğer bilimlerden de incelenmesi gerektiğini göstermiştir. 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.

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. Bu ve benzeri nedenler ile siber saldırı sayıları ve yaşanan maddi zararlar olduğundan daha az kaydedilmesine ilişkilendirme modellerinin daha zayıf olmasına neden olmuştur.

Zonguldak ilindeki firmaların network yapısına bakıldığında çok büyük olmadığı görülmektedir. Anketten elde edilen verilere göre firmaların büyük kısmının bilişim alanında 10 bilgisayar ya da daha düşük donanım bulunduğu kaydedilirken firmaların yarıya yakınının bilişim alanında en az bir adet sunucu bulunmaktadır.

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

Firmalardan sadece %27,4’ü firewall kullanırken, bu firmaların %30,2’si açık kaynak kodlu, %43,8’i kutu çözüm güvenlik duvarı kullandığı örneklerden 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.

Zonguldak'ta 2016 yılında farklı siber saldırılar sonucunda 143 gün hizmet aksaması yaşanmış ve siber saldırının maddi zararlar verdiği analiz edilmiştir. Ayrıca firmaların siber saldırılar nedeni ile toplam 247.370 TL doğrudan maddi zarara uğradığı görülmüştür.

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 kullanımının 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 daha kapsamlı çalışmaların yapılması uygun olacaktır.

Kaynakça

- Aktürk, E. (2005). Türkiye'de kayıt dışı ekonomi: Sebepleri ve çözüm önerileri, *Ekev Akademi Dergisi*, 23, 285 – 300.
- Altuğ, O. (1999). *Kayıtdışı ekonomi*, İstanbul: Türkmen Kitabevi.
- Çavuşoğlu, H., & Pekkaya, M. (2015). Siyasal propaganda araçlarının seçmen tercihine etkisi: Zonguldak örneği, *Eskişehir Osmangazi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(3), 91- 115.
- Dülger, M. V. (2004). *Bilişim suçları*, Ankara: Seçkin Yayınları.
- 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).
- İlgın, Y. (1999). *Kayıtdışı ekonomi ve Türkiye'deki boyutları*, DPT Yayınlanmamış Uzmanlık Tezleri, Yayın No: DPT 2492, Nisan 1999.
- İHS. (2016). *Siber saldırı mağduru küçük şirketlerin %60'ı iflas ediyor*. <http://www.ihs.com.tr/blog/siber-saldiri-magduru-kucuk-sirketlerin-yuzde-altmisi-iflas-ediyor/>, (Erişim Tarihi: 05.06.2017).
- 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).
- Kara, B. (2016). *Türkiye'de haftada 18 bin siber saldırı yaşanıyor*. <http://www.teknolojioku.com/haber/turkiyede-haftada-18-bin-siber-saldiri-yasaniyor-36749.html> (Erişim Tarihi 22.09.2017).
- Karaman, F. (1999). Ekonomik ve sosyal boyutla Türkiye'de kayıt dışı ekonomi, *Yeni Türkiye*, 5(27).
- Losby, J. L., Else, J. F., Kingslow, M. E., Edgcomb, E. L., Malm, E. T., & Kao, V. (2002). Informal economy literature review, *ISED Consulting and Research*, http://www.kingslow-assoc.com/images/Informal_Economy_Lit_Review.pdf, (Erişim Tarihi 22.09.2017).
- Mavral, Ü. (2001). *Karapara Kayıtdışı Ekonomi İlişkisi ve Türkiye'ye Yansımaları*, Ankara: Vergi Denetmenleri Derneği Yayını.
- Öğünç, F., & Yılmaz G. (2000). *Estimating the underground economy in Turkey*, Research and Monetary Policy Department, Central Bank of the Republic of Turkey.
- Özcan, S. E. (2003). *Devlet İç Borçlanması ve Türkiye'de Devlet İç Borçlanmasının Sürdürülebilirliği*, Yayınlanmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.
- Özsoylu, A. F. (1994). Kayıtdışı ekonominin etkileri, kim kazanıyor, kim kaybediyor, *Ekonomik Forum Dergisi*, TOBB 2, 14-17.
- Öztürk, N. (2006). Ekonomide devletin değişen rolü, *Amme idaresi Dergisi*, 39(1), 17-38.
- Sarıkaya, H. E. (2007). *Kayıt dışı ekonominin ekonomik büyümeye etkisi: Türkiye örneği (1980-2005)*. Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi, SBE.
- Sarılı, M. A. (2002). Türkiye'de kayıt dışı ekonominin boyutları, nedenleri, etkileri ve alınması gereken tedbirler, *Bankacılar Dergisi*, 41, 32-50.

- Temli, M. (2014). Siber güvenlik ve alınabilecek kurumsal tedbirler, *Batı Karadeniz Kalkınma Ajansı, BAKKA Bülten* 4.
- Temli, M. (2017). *Siber suçların ekonomik boyutu: Zonguldak örneği*. Yayımlanmamış Yüksek Lisans Tezi, Bülent Ecevit Üniversitesi, SBE.
- Tiryaki, T., & Gürsoy, T. (2004). Ekonomik suç kavramı ve sigortacılık suçlarının bu açıdan değerlendirilmesi, *Sayıştay Dergisi*, 55, 53-69.
- Us, V. (2004). *Kayıt dışı ekonomiyi tahmin yöntem önerisi: Türkiye örneği*, Tartışma Metni, Türkiye Ekonomi Kurumu.
- 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).