İNTERNET MEDYASINDA GİZLİ BELGE YAYINCILIĞININ TEKNİK VE ELEKTRONİK ANALİZİ: WIKILEAKS VE PANAMA BELGELERİ

YÜKSEK LİSANS TEZİ

Salih ERDURUCAN

Danışman:
Doç. Dr. İsmail Hakkı NAKİLCİOĞLU

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ
YÖNETİMİ ANABİLİM DALI

Temmuz 2017

AFYON KOCATEPE ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

İNTERNET MEDYASINDA GİZLİ BELGE YAYINCILIĞININ TEKNİK VE ELEKTRONİK ANALİZİ: WIKILEAKS VE PANAMA BELGELERİ

Salih ERDURUCAN

Danışman:
Doç. Dr. İsmail Hakkı NAKİLCİOĞLU

İNTERNET VE BİLİŞİM TEKNOLOJİLERİ YÖNETİMİ
ANABİLİM DALI

Temmuz 2017

TEZ ONAY SAYFASI

Salih ERDURUCAN tarafından hazırlanan "**İnternet Medyasında Gizli Belge Yayıncılığının Teknik ve Elektronik Analizi: WikiLeaks ve Panama Belgeleri**" adlı tez çalışması lisansüstü eğitim ve öğretim yönetmeliğinin ilgili maddeleri uyarınca 05/07/2017 tarihinde aşağıdaki jüri tarafından **oy birliği** ile Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü **İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı'nda YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman: Doç. Dr. İsmail Hakkı NAKİLCİOĞLU

İmza

Başkan : Doç. Dr. Uçman ERGÜN
Afyon Kocatepe Üniversitesi
Mühendislik Fakültesi

Üye : Yrd. Doç. Dr. Hakan GÜLVEREN
Uşak Üniversitesi
Eğitim Fakültesi

Üye : Doç. Dr. İsmail Hakkı NAKİLCİOĞLU
Afyon Kocatepe Üniversitesi
Güzel Sanatlar Fakültesi

Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
...../...../..... tarih ve
..... sayılı kararıyla onaylanmıştır.

.....
Prof. Dr. Hüseyin ENGİNAR
Enstitü Müdürü

BİLİMSEL ETİK BİLDİRİM SAYFASI

Afyon Kocatepe Üniversitesi

Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlâk kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

05/06/2017

Salih ERDURUCAN

ÖZET

Yüksek Lisans Tezi

İNTERNET MEDYASINDA GİZLİ BELGE YAYINCILIĞININ TEKNİK VE ELEKTRONİK ANALİZİ: WIKILEAKS VE PANAMA BELGELERİ

Salih ERDURUCAN
Afyon Kocatepe Üniversitesi
Fen Bilimleri Enstitüsü
İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı
Danışman: Doç. Dr. İsmail Hakkı NAKİLCİOĞLU

Bu araştırmada, internet medyasında gizli belge yayıncılığının teknik ve elektronik analizi WikiLeaks ve Panama Belgeleri ölçeğinde incelenmiştir. Bu amaçla literatür taramasının yanında teknik özelliklerin analizi, karşılaştırma, muhakeme, tümevarım ve tümdengelim tekniklerinden yararlanılmıştır.

Son yıllarda artış gösteren gizli belge yayıncılığı, internet medyasının sağladığı avantajlar sayesinde kontrol edilemez hale gelmiştir. Gizli belgelerin ele geçirilmesinde iç ve dış tehditler rol almaktadır. Kritik bilgilere sahip kurum ve kuruluşların bilgi ifşalarına karşı etkili ve sürekli güncellenen bir savunma hattı kurmaları gerekmektedir. Çalışanlar güncel bilgi elde etme tekniklerine karşı uyarılmalı, bilgi ifşalarına karşı periyodik olarak eğitilmelidirler. Bilgi işlem birimi, artan dış saldırılara olduğu kadar içeriden gelebilecek kötü niyetli personel saldırılarına da hazırlıklı olmalı, gereksiz yetki seviyelerine, zafiyeti bulunan donanım ve yazılımlara karşı tedbirler almalıdır.

İnternet medyasında gizli belgelerin yayınlanmasını tümüyle engellemek teknik olarak mümkün olmamaktadır. WikiLeaks örneği incelendiğinde; farklı birçok yöntemle engellenmeye çalışılmasına rağmen bunda başarılı olunamayarak belgelerin yayınlanması devam etmiştir. Panama Belgeleri örneğine bakıldığında bazı ülkelerin

belgelerin yayınlandığı web sitesine sansür uyguladığı ancak yayınlamanın önüne geçilemediği görülmektedir. Bu uygulamalar dikkate alındığında gizli belge ve bilgilerin yayınlanmasına teknik olarak engel olunamasa bile bilgilerin ele geçirilmesi engellendiğinde sorunun, kaynağında çözülebileceği öngörülmektedir.

2017, x + 98 sayfa

Anahtar Kelimeler: Gizli belge yayıncılığı, bilgi ifşası, WikiLeaks, Panama Belgeleri, Whistleblowing, TOR, OnionShare, SecureDrop

ABSTRACT

M. Sc. Thesis

TECHNICAL AND ELECTRONIC ANALYSIS OF CONFIDENTIAL DOCUMENT PUBLISHING IN INTERNET MEDIA: WIKILEAKS AND PANAMA PAPERS

Salih ERDURUCAN

Afyon Kocatepe University

Graduate School of Natural and Applied Sciences

Department of Internet and Information Technologies Management

Supervisor: Assoc. Prof. İsmail Hakkı NAKİLCİOĞLU

In this study, the technical and electronic analysis of confidential documents leaks in the internet has been studied with the samples from WikiLeaks and Panama Papers. For this purpose, as well as literature review, techniques like, analysis of the technical properties, comparison, deduction and induction were implemented.

The leaks in the recent years have been out of control through the advantages in the internet media. External and internal threats play part in the leaks of the confidential documents. The departments and governmental bodies with critical information at hand should have continuously-updated defence firewalls. The employees should be warned for the updated leakage techniques and periodically educated. IT departments should be prepared for increasing external threats as well as attacks from the ill-intentioned people within their departments, and take precautions against unauthorized persons, weak software and hardware.

Technically it is impossible to stop all the leakage in the internet. When we study WikiLeaks, we see that it is not possible for the documents to be disseminated even though different precautions were taken. In Panama Papers, we observe that the web sites publishing these were censored, yet could not stop the viral spread. When these practices taken into account, it is viewed that although technically it is impossible to

inhibit disseminating secret documents and information, the problem can be resolved in its source when the information is hindered to be revealed.

2017, x + 98 pages

Keywords: Confidential Document Publishing, Information Disclosure, WikiLeaks, Panama Papers, Whistleblowing. TOR, OnionShare, SecureDrop

TEŞEKKÜR

Bu araştırmanın konusunun belirlenmesi, deneysel çalışmaların yönlendirilmesi, sonuçların değerlendirilmesi ve yazımı aşamasında yapmış olduğu büyük katkılarından dolayı tez danışmanım Sayın Doç. Dr. İsmail Hakkı NAKİLCİOĞLU'na, araştırma ve yazım süresince yardımlarını esirgemeyen Sayın Dr. Ufuk TANYERİ'ne, her konuda öneri ve eleştirileriyle yardımlarını gördüğüm hocalarıma ve arkadaşlarıma şükranlarımı sunarım. Ayrıca bu araştırma boyunca maddi ve manevi desteklerinden dolayı eşime ve aileme teşekkür ederim.

Salih ERDURUCAN

Afyonkarahisar, 2017

İÇİNDEKİLER DİZİNİ

Sayfa

KISALTMALAR DİZİNİ

DDoS	:	Distributed Denial-of-Service Attack Dağıtılmış Hizmet Engelleme Servisi
DLP	:	Data Loss Prevention Veri Kaybı Önleme
ICIJ	:	International Consortium of InvestigateJournalists Araştırmacı Gazeteciler Uluslararası Konsorsiyumu
IETF	:	Internet Engineering Task Force Internet Mühendisliği Görev Gücü
IPS	:	Intrusion Prevention System Saldırı Önleme Sistemi
JWICS	:	TheJoint World Wide Intelligence Communications System Dünya Ortak İstihbarat İletişim Sistemi
NIST	:	National Institute of Standards and Technology Ulusal Standartlar ve Teknoloji Enstitüsü
PGP	:	Pretty Good Privacy Oldukça İyi Gizlilik
SIEM	:	Security Information and Event Management Güvenlik Bilgisi ve Olay Yönetimi
SIPRNET	:	The Secret Internet Protocol Router Network Gizli İnternet Protokolü Yönlendirici Ağı
SMTP	:	Simple Mail Transfer Protocol Basit E-posta İletişim Protokolü
SMTPS	:	Simple Mail Transfer Protocol with Secure Layer Güvenli Basit E-posta İletişim Protokolü
SSL	:	Secure Sockets Layer Güvenli Soket Katmanı
TAILS	:	The Amnesic Incognito Live System Unutkan Gizli Kimlikli Canlı Sistemi
TLS	:	Transport Layer Security Güvenli Taşıma Katmanı
TOR	:	TheOnion Routing Soğancık Yönlendirme
VPN	:	Virtual Private Network Sanal Özel Ağ
VPS	:	Virtual Private Server Sanal Özel Sunucu

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Bilgi ve teknolojinin günümüzdeki artan hızına paralel olarak, son derece önemli olan birçok gizli belge, internet medyası üzerinden, artan bir hızla ifşa edilmektedir. Yakın dönemde birçok şahıs, şirket, kurum hatta hükümete ait gizli belgeler internet medyasında yayınlanmıştır. Bu yayınlar sebebiyle yöneticiler, hatta hükümetler değişmekte, özellikle de toplumun genelini ilgilendiren ifşalar sebebiyle ülkeler arası diplomatik krizler ortaya çıkabilmektedir.

Bilgi ifşalarının önüne geçebilmek için kullanılan yöntemlerin teknik ve elektronik analizlerinin de yapılması gerekmektedir. Bu analizleri yapabilmek için gizli belgelerin veya bilgilerin hangi kanallarla nerelerden elde edildikleri, hangi yöntemler kullanılarak ifşa medyalarına ulaştırıldıkları, hangi ortamlarda hangi tekniklerle yayınlandıkları tespit edilmelidir.

Bu amaçla, dijital kaynakların taranması yoluyla yapılan bu araştırma, iki aşamadan oluşmaktadır:

1. Gizli belge ifşalarında, bilginin kaynaktan yayın noktasına ulaşmasına kadar kullanılan teknik ve yöntemlerin belirlenmesi. Bu aşamada ulusal ve küresel bilgi ifşalarında kullanılan yöntem ve tekniklerin incelenip ortak noktaların ve farklılıkların tespit edilerek model ya da modeller çıkarılması. Genel anlamda gizli belge yayıncılığının sebeplerinin araştırılması ve sonuçlarının değerlendirilmesi.

2. Küresel bilgi ifşalarının sebepleri, sonuçları çerçevesinde özel olarak WikiLeaks ve Panama Belgelerinin teknik ve elektronik açıdan incelenmesi yoluyla bilgi ifşalarının önüne geçilmesi için alınacak önlemlerin somut örnekler çerçevesinde tespit edilerek önerilerde bulunulması.

Araştırma bilgi ifşalarına etki eden psikososyal konulara “neden olması” sebebiyle yüzeysel olarak değinirken odaklanılan bölüm bilgi ifşalarında kullanılan tekniklerdir.

1.1 Araştırmanın Amacı

İnternet medyası üzerinden gizli belge yayıncılığı son yıllarda giderek artmaktadır. Bilgi ifşalarının getireceği avantajlar ve dezavantajlar incelenerek, ifşa çeşitlerinin

belirlenmesi, gizli belge yayıncılığında hangi yöntem ve tekniklerin kullanıldığının tespit edilmesi gerekmektedir. Bu çalışmada, kuruluşların kötü niyetli çalışanlarının içeriden gerçekleştirdiği saldırılara odaklanarak gizli belge ifşalarına karşı alınabilecek tedbirlerin belirlenmesine de yer verilmiştir. Söz konusu önerilerin belirlenebilmesi için de aşağıdaki sorulara cevap bulunmaya çalışılmıştır:

- İfşanın altında yatan sebepler nelerdir?
- Fiziksel ve sanal ortamda bu belgeler nasıl ele geçirilmektedir?
- Hangi kanallarla ve hangi tekniklerle belgeler ifşa ortamına ulaştırılmaktadır?
- İfşacılar, kimliklerinin ortaya çıkmaması için hangi teknik araçları ve yöntemleri kullanmaktadır?
- Belgeler hangi ortamlarda nasıl yayınlanmaktadır?
- Elektronik iletişim yazılımları ve yöntemleriyle belgelerin tümüne ulaşılabilir mi?
- Belge sızdırılmasından kimler, nasıl kazanımlar elde etmektedir?
- Kurumların ifşaları önlemek için alabileceği donanım ve yazılım önlemleri nelerdir?
- Somut örnekler olarak WikiLeaks ve Panama Belgeleri, teknolojik açıdan nasıl değerlendirilmelidir?
- Gizli belge yayıncılığının Türkiye ile ilgili boyutu nedir?

1.2 Araştırmanın Önemi

İnternet medyası üzerinden gizli bilgi ve belge yayıncılığı son yıllarda giderek artmaktadır. Söz konusu durumun getireceği avantajlar ve dezavantajlar değerlendirildiğinde, ifşa kaynaklarının ve toplumun bundan nasıl etkileneceğinin tespit edilmesi önem taşımaktadır.

İfşacıların, gizli bilgileri ele geçirmede ve arzulanan yere ulaştırılmasında izledikleri yöntem ve tekniklerin tespiti, aynı zamanda alınması gereken önlemlerin belirlenmesini de gerektirmektedir. Günümüzde ifşa edilen bilgilerin doğruluğu, ne kadarının açığa çıkarıldığı, yayınlanmasıyla ulusal ve uluslararası politikanın bundan nasıl etkileneceği gibi konuların bilimsel açıdan ve objektif olarak incelenmesine ihtiyaç vardır.

Bu tezde, bilgi ve belge ifşalarındaki ortak noktaların tespiti yapılıp kullanılan yöntem ve tekniklerin çeşitliliği araştırılarak, gelecekteki ifşaların önlenebilmesi için bahsi geçen durumlarda özellikle ulusal düzeyde alınması gereken tedbirlerin neler olduğu ele

alınmaktadır. Buna ek olarak, ifşa edilen bilgilerin hangi ortamlardan hangi yöntemlerle ele geçirildiği, söz konusu bilgilerin, ifşacı kimliği deşifre edilmeyecek şekilde, nasıl ve hangi teknik yöntemler kullanılarak istenilen yerlere ulaştırıldığı incelenmiştir.

Ayrıca, ele geçirilen bilgi ve belgelerin, hangi internet medyalarında, hangi teknik olanaklar kullanılarak kamuya açıldığı, kullanılan yöntemlere, kurumlarca ya da hükümetlerce sansür uygulanıp uygulanmadığı, gerçekleştiği durumlarda başarıya ulaşılıp ulaşılmadığı noktaları üzerinde de durulmuştur. Son olarak tüm bu incelemeler ışığında, bilgi ifşasının Türkiye boyutu ortaya konulurken, somut olarak WikiLeaks ve Panama Belgeleri örnekleri incelemeye konu edilmiştir.

Konu hakkında yapılan literatür taramasında ülkemizde bilgi ifşalarının teknik açıdan değerlendirmesine ait bir çalışma bulunamamıştır. Uluslararası alanda ise bilgi ifşalarında kullanılan tekniklerle ilgili, WikiLeaks ve Panama Belgeleri konusunda kısmi araştırmalar bulunmaktadır. Bu tez çalışması, 2010-2016 yılları arasında yayınlanmış WikiLeaks ve Panama Belgeleri ölçeğinde yapılarak bu alandaki eksiklik giderilmeye çalışılmıştır.

2. LİTERATÜR BİLGİLERİ

Bilgi ifşaları konusu ülkemizde yapılan çalışmaların araştırılmasında üniversite kütüphanelerinin yanı sıra Ulakbim ve YÖK Tez Merkezi'nden yararlanılmıştır. Yurtdışında yapılan çalışmaların araştırılmasında ise elektronik tarama araçları olan veritabanları ile Science Direct, Research Gate, IEEE Xplore, Web of Science gibi indeksler taranmıştır. Bunun yanında internet siteleri de taranarak araştırmada yararlanılmıştır.

Taraması yapılan kaynaklarda özellikle YÖK Tez Merkezinde bulunan çalışmalar bilgi ifşalarının daha çok sosyal boyutunu incelemiştir. Yabancı kaynaklarda ise yine sosyal boyutu daha çok yer alırken teknik anlamda kullanılan teknolojiler parça parça incelenmiştir. Fakat söz konusu çalışmalar arasında bu parçaları bir araya getirerek bir bütün oluşturan araştırma bulunamamıştır. Söz konusu bu çalışmanın bu yönüyle bir eksikliği giderebileceği düşünülmektedir.

İndekslerde bulunan çalışmalar da bilgi ifşalarının hem sosyal hem de teknik kısımlarına değinen çalışmalar bulunmuştur. Chen (2011) ve Dragt (2012) çalışmalarında bilgi ifşalarıyla WikiLeaks arasındaki ilişkileri incelemişlerdir. Hsu and Marinucci (2013) ise bilgi ifşalarında sıklıkla başvurulan TOR ağlarının güçlü ve zayıf yönlerini teknik açıdan değerlendirmişlerdir. Nguyen (2004) kritpo yazılımlarına gerçekten güvenilip güvenilmeyeceğini irdeleyen bir çalışması bulunmaktadır.

WikiLeaks ve Panama Belgeleriyle ilgili yapılan araştırmada ise ifşaların doğası gereği olsa gerek daha çok gazete haberleri ve köşe yazıları bulunmuştur. Bununla birlikte özellikle Panama Belgelerinin yayınlanmasında kullanılan tekniklerin anlatıldığı bir Araştırmacı Gazeteciler Uluslararası Konsorsiyumu (ICIJ) çalışanına ait blog sayfası olan İnt. Kyn. 59 önemli bilgiler vermektedir. İnt. Kyn. 53 ise bilgi ifşalarına karşı alınabilecek tedbirleri incelemiştir.

Ülkemizdeki bilgi ifşalarını teknik açıdan inceleyen çalışmaların yetersiz olması ve taranan veritabanlarındaki WikiLeaks'in kullandığı teknikleri inceleyen çalışmaların eksikliği önemli derecede hissedilmiştir.

3. MATERYAL VE METOT

Bu bölümde araştırmanın modeli, araştırma evreni ve verilerin toplanması yer almaktadır.

3.1 Araştırmanın Modeli

Dijital verilerin taranması yoluyla yapılan bu araştırmada, deneysel olmayan nicel araştırma yöntemleri kullanılmıştır. Metot olarak tarama metodu tercih edilmiştir. Tarama metodu, geçmişte veya halen var olan bir durumu var olduğu şekliyle betimlemeyi, değişkenler arasındaki ilişkiyi karşılaştırmayı amaçlayan ve belli bir zaman diliminde veri toplamaya dayalı bir araştırma yaklaşımıdır (Karaşar 2002)

Araştırmada amaca ulaşılabilmek için araştırma evreni üzerinde çalışılarak, geneli kapsayan bir yargıya varmak üzere öncelikle literatür taraması gerçekleştirilmiştir. tarama metodu uygulanmıştır. Söz konusu araştırmada literatür taraması ve verilere ulaşımda üniversite kütüphaneleri ve internet kaynakları kullanılmıştır.

3.2 Araştırma Evreni

Küresel bilgi ifşalarındaki bilgilerin ele geçirilmesinden yayımlanmasına kadar geçen süreçte kullanılan yöntem ve tekniklerin analiz edilmesinde, bilgi ifşasında kullanılan tekniklerin zirve yaptığı WikiLeaks ve Panama Belgeleri seçilmiştir.

3.3 Araştırma Kısıtları

Araştırma küresel bilgi ifşaları olan WikiLeaks ve Panama Belgeleri ölçeğinde ve yayınlanan kısımlarından 2010 – 2016 yılları arasını kapsamaktadır.

4. BULGULAR

4.1 İnternet Medyasında Gizli Belge Yayıncılığı

Son yıllarda elektronik yayıncılık diğer bir deyişle internet medyası yoğun bir şekilde kullanılmaya başlanmıştır. Elektronik yayıncılık; dijital yayınların veya belgelerin yine elektronik ortamlarda ya da internet ağları aracılığıyla erişime açılması olarak tanımlanmaktadır (Tonta 2000). Özellikle internet kullanımının yaygınlaşması nedeniyle bilgi kaynaklarının sayısında önemli ölçüde artış görülmüştür.

Ele geçirilen gizli bilgilerin, uzmanlar ve gazetecilerce yeniden kontrol edilerek medya aracılığıyla kamuya ulaştırılması olarak da tanımlanan "sızıntı gazeteciliği" yeni bir gazetecilik türü olarak karşımıza çıkmaktadır (Çalışkan 2016).

Geleneksel yayıncılıkta gazeteler günlük süreçlerde tüketilirken, yeni nesil elektronik gazetecilik kolayca arşivlenebilmekte ve yine kolayca sorgulama yapılabilmektedir (Erol 2009).

Elektronik gazeteciliğin getirmiş olduğu bu kolaylıklar, sızıntı gazeteciliğinin etkilerini de artırmaktadır. Yayınlanan gizli belgelerin arşivlenebilmesi ve anahtar kelimelerle sorgular yapılabilmesi nedeniyle yıllar sonra bile ilgi çekmeye devam etmektedir.

4.1.1 Gizli Belge Yayıncılığının Sebepleri

Günümüze kadar gerçekleşen bilgi ifşaları dikkate alındığında, kamu yararı gözetilerek gerçekleştirilen, toplumu ya da siyasi mercileri harekete geçirmeyi amaçlayan, etik dışı veya kanunsuz eylemleri durdurmak üzere gerçekleştirilebileceği gibi çeşitli illegal yöntemler kullanılarak elde edilmiş bilgiler, kişi ya da kurumları veya siyasi hükümetleri zor duruma düşürmek gibi amaçlarla da yayınlanabilmektedir.

WikiLeaks'in binlerce gizli belgeyi yayınlaması kimi otoritelere göre gazetecilik başarısı olarak görülürken kimi çevrelere göre de ulusal çıkarların zarar gördüğü yasadışı bir yayın olarak değerlendirilmektedir (Kumcuoğlu 2011).

Fakat gözden kaçırılmaması gereken nokta, basının kamu yararını gözeterek bilgi ifşası yapmakla görevli olduğudur. Medya, kamu yararına bu bilgileri yayınlayarak, toplumu bilgilendirmekte bu sayede siyasal sistemin denetimini sağlamaktadır (Çaplı 2002).

4.1.2 Gizli Belge Yayıncılığının Yararları ve Zararları

Bilgi ifşalarının faydaları olduğu kadar zararları da olabilmektedir. İfşacı, kurum/kuruluş ve kamu açısından değerlendirildiğinde farklı sonuçlar ortaya çıkmaktadır.

4.1.2.1 İfşacı Açısından Yararları ve Zararları

İfşacı, bilginin ifşa edilmesiyle vicdani ve psikolojik yönden rahatlama hissetmektedir. Bilginin ifşa edilmesiyle etik dışı veya kanunsuz uygulamaların sona ereceği düşünülerek rahatlama meydana gelmektedir. Bilgi ifşası; tehdit, şantaj veya rüşvet karşılığında gerçekleştirilmişse tehdit veya şantajın sona ermesiyle, meşru görülmese de rüşvet karşılığında yapılmışsa maddi çıkar kazanımı elde edilerek fayda sağlanmış olmaktadır (Yılmaz 2009).

İfşacıya kurum/kuruluş içerisinde jurnalci, güvenilmez vs. gibi kötü sıfatlar yakıştırılmaktadır. Bu kişiler, kurum yöneticileri tarafından kötü muameleler, düşük pozisyona atamalar, tehdit gibi olumsuz davranışlara maruz kalabilmektedir (Yılmaz 2009).

4.1.2.2 Kurum/Kuruluş Açısından Yararları ve Zararları

Bilginin ifşa edilmesiyle kurum/kuruluş iç denetim mekanizmaları harekete geçerek haksız ya da kanunsuz uygulamaları sona erdirilebilir. İç denetim mekanizmaları, istismar edilen noktaları tespit ederek kurumun gelecekte daha kaliteli ve güvenli olmasını sağlayabilir (Yılmaz 2009).

Kurum/kuruluş, kamuoyunda itibar kaybı yaşayabilir, kurum/kuruluş dışı denetimler artabilir, bazı yöneticiler pozisyon değişikliğine uğrayabilir, hatta işsiz kalabilir. Ortaya çıkan haksız ya da kanunsuz uygulamaların etkisinin büyük çapta olması durumunda kurum/kuruluş, pazar kaybı nedeniyle ciddi ekonomik kayıplar yaşayabilir veya bunların devlet eliyle tamamen kapatılması söz konusu olabilir (Yılmaz 2009).

4.1.2.3 Kamu Açısından Yararları ve Zararları

İfşacının bilgiyi ifşa etmesiyle kamuoyu yanlış uygulamalardan haberdar olur. Bu durum, toplumsal tepkinin oluşmasını sağlayarak sorunların düzeltilmesini

sağlayabildiği gibi, gizli saklı yapılan işlerin bir gün ortaya çıkacağının düşünülmesini ve potansiyel suç işleme eğiliminde olanların korkarak yanlış işlere tevessül etmelerini de engelleyebilir. Yanlış uygulamalara çözüm bulunamadığında, sessiz kalmak veya görmezden gelmek yerine, halka bilgi verilmesi gerektiği bilinci topluma yerleşebilir.

Ancak halka sistemli ve bilinçli olarak yanlış bilgiler verilmesiyle kamuoyu yanıltılarak provoke edilebilir, toplumsal olaylar tetiklenebilir, sonuçta toplumun sisteme olan inancı ve güveni zedelenebilir. Bu tür durumlar neticesinde bilgi ifşasında bulunarak yolsuzluk, kanunsuzluk gibi etkenlerle mücadele etmek isteyen ifşacılar korkar ve gördüklerini raporlamayan, ihbar etmeyen, hissizleşmiş bireylere dönüşebilir (Yılmaz 2009).

4.2 Bilgi İfşası

90'lı yıllardan başlayarak hızla yaygınlaşan küresel iletişim ağları, yeni medya adı da verilen dijital bir platformu ortaya çıkarmıştır. Yeni medyanın geleneksel medyadan farklı olan yönü, etkileşimli ve multimedya biçimine sahip olmasıdır. Dijital temele sahip olması nedeniyle yeni medya çok sayıda bilgiyi takipçilerine iletebilirken onlardan gelebilecek etkileşimlere de imkân vermektedir. Bu sayede bilginin düz çizgisel iletiminden, hipermetinselliğe geçilmiştir (Binark 2007).

Dijital kodlama, iletişim esnasında taraflar arasında eş zamanlı, yüksek kapasiteli, yüksek hızlı ve çok katmanlı iletişim ortamı sağlamaktadır (İnt. Kyn. 55). Yeni medyanın teknolojik olarak getirdiği bu yüksek imkânlar gizli belge yayıncılığının da yaygınlaşmasına sebep olmuştur. Gizli belgelerin ele geçirilmesinden, kamuoyuna ifşa edilmesi sürecine kadar birçok yeni teknolojik yazılım ve donanım ürünleri kullanılmaktadır.

Whistleblowing, kelime anlamı olarak İngilizce'de "ıslık çalmak" anlamına gelse de daha çok bilgi ifşası anlamında kullanılmaktadır. Kelimenin temelinde, İngiliz polisleri tarafından potansiyel suçluların düdük çalarak ikaz edilmesi yatmaktadır. Bilgi ifşası, organizasyonların içerisinde yaşanan yasadışı, ahlâki veya etik olmayan davranış ya da eylemlerin, diğer kişi ya da kuruluşlara zarar vermeden çözülmek üzere yetki sahibi mercilere bilgilerin aktarılması şeklinde ifade edilmektedir (Aktan 2006).

Başka bir deyişle belirtmek gerekirse, "örgütte iş görenlerin ya da geçmişte çalışmış olan eski personel tarafından, organizasyonda bulunan, yasal olmayan, etik dışı eylemlerin bu olumsuz durumları engelleyebilecek kişi ya da kurumlara bildirilmesi" olarak ifade edilebilir (Miceli and Near 1984).

Aktan (2006), bahsi geçen tanımları değerlendirirken, bilgi ifşalarının özünü oluşturan temel unsurlara değinmiştir.

Buna göre, bilgi ifşaları kamusal ya da özel fark etmeksizin bütün organizasyonlarda yaşanabilecek bir durumdur ve gayrimeşru uygulamaların açığa çıkarılması amacıyla yapılır. Bu durumda üç önemli nokta öne çıkar:

- Organizasyon içindeki davranışlar veya uygulamalar yasalara uygun değildir.
- Organizasyon içi davranışlar veya uygulamalar toplumun ya da en azından ifşacının ahlâk anlayışına aykırı durumdadır.
- Organizasyon içi davranış ve uygulamalar meşruiyet sorgulamasına tâbidir. Diğer bir ifadeyle, organizasyonda karşılaşılan uygulamalar meşru kabul edilemeyecek durumdadır.

Uyar ve Yelgen (2015) ise ifşa edilen bilgiler kapsamında, şirket varlıklarının çalındığını, usulsüzlüklerin görmezden gelinmesi için rüşvet alındığını, şirket ya da kurum varlıklarının kişisel amaçlar için kullanıldığını ve muhasebe kayıtlarının gerçekleri gizlemek üzere değiştirildiğini tespit etmişlerdir.

Söz konusu duruma, denetim görevinin yerine getirilmemesi, kara para aklama, etik ihlallerinin yetkili mercilere bildirilmemesi örnek gösterilebilir. Özellikle toplumun sağlığı, güvenliği ve eğitimi konularında olmak üzere, kurum bünyesinde yaşanan insan hakları ihlâlleri ve cinsel suçlar gibi durumlar daha çok ifşa edilmektedir (Uyar ve Yelgen 2015).

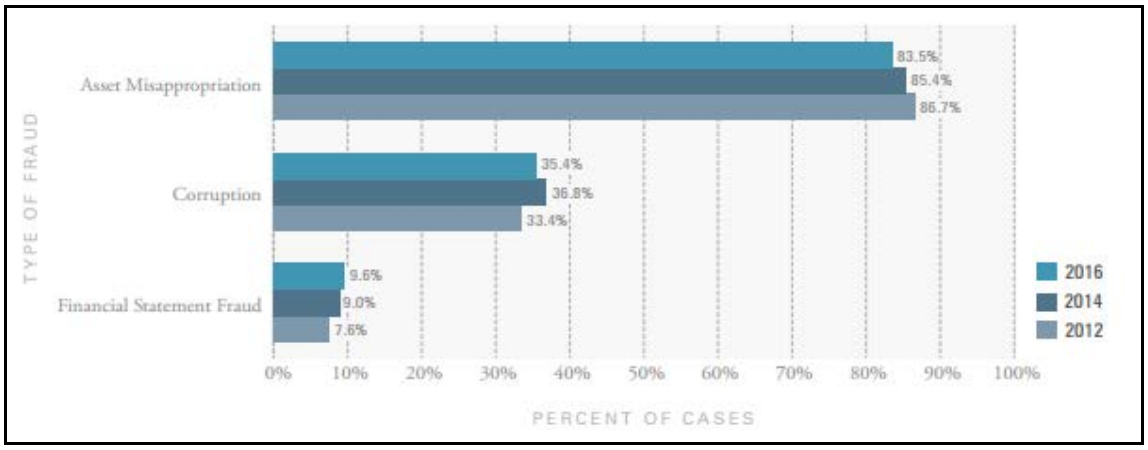
Toplumun hemen hemen her alanında karşılaşılabilecek bir durum olmasının yanında bilgi ifşaları, iş dünyasını da doğrudan ilgilendirmektedir. İş dünyasında yaşanan suistimaller ise genelde üç kategoride incelenmektedir:

- Varlıkların kötüye kullanımı
- Yolsuzluk
- Mali tabloların suistimal edilmesi.

ACFE 2016 Fraud Raporu'na göre (İnt. Kyn. 54), varlıkların kötüye kullanılması en çok karşılaşılan (yüzde 83) suistimal olarak tespit edilmiştir. Bu kadar büyük bir oranda olmasına karşın suistimalin mali boyutu yalnızca 125 bin dolar civarında olmuştur. Fakat yüzde 10 oranına sahip mali tablo suistimali ise 975 bin dolarlık en büyük kaybı oluşturmaktadır.

Yolsuzlukların ortaya çıkartılmasında en yaygın ve tutarlı olan yöntem ise çalışanlar tarafından yapılan ihbarlardır. Tespit yöntemleri bölgesel olarak incelendiğinde, gelişmiş ülkelerde yani raporlama ve denetim kültürünün yerleşik olduğu ülkelerde ihbar etme yöntemi açık ara önde gelmektedir. Ancak Ortadoğu'da ve az gelişmiş ülkelerde ihbar ve iç denetim neredeyse eşit oranlarda görülmektedir.

Bu durumdan; "gelişmiş ülkelerde yapılan yolsuzlukların ortaya çıkarılmasında ihbardan başka etkili bir yöntem bulunmamaktadır, gelişmemiş ya da az gelişmiş ülkelerde ise yapılan yolsuzluklar ihbar edilmese bile profesyonelce yapılmadığı için iç denetimlerle tespit edilebilmektedir" çıkarımı yapılabilmektedir (İnt. Kyn. 1).



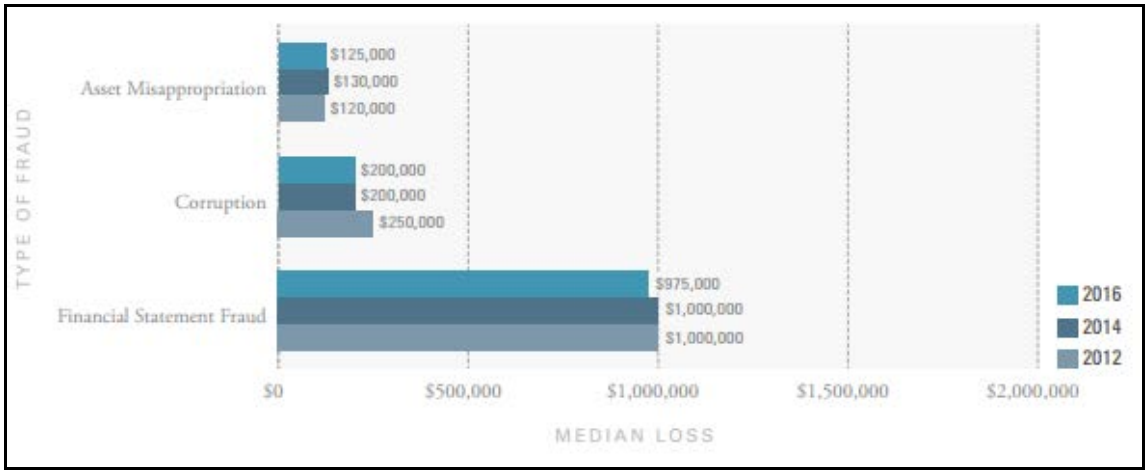
Şekil 4.1 Suistimal türleri ve oranları (İnt. Kyn. 1).

Yine aynı rapora göre kurum ve kuruluşları her yıl gelirlerinin yüzde 5'ini suistimaller nedeniyle kaybetmektedir. Bildirilen ya da tespit edilen suistimallerin mali boyutu, toplamda 6.3 milyar dolar, vaka başına da 2.7 milyon dolar rakamlarına ulaşmaktadır. Bu rakamlar 2014 yılına ait gayri safi milli hâsıla rakamlarıyla birlikte değerlendirildiğinde ortaya çıkan rakam 3.7 trilyon dolar olmaktadır.

Kaybedilen mali kaynakların geri alınabilmesi oldukça uzun zaman ve büyük gayretler gerektirse de bu genelde pek mümkün olmamaktadır. Rapora göre, mağdur kurum ve kuruluşların yüzde 58'i kayıplarının hiçbirini geri alamazken, bunların sadece yüzde 14'lük kısmı tahsil edilebilmiştir. Tespit edilen vakalardaki suçluların yüzde 8,4'ünün cezalandırılabildiği ve ceza verebilmeyi başaran ülkelerin büyük çoğunluğunun gelişmiş ülkeler olduğu da raporda yer almaktadır.

Region	Number of Cases	Percent of Cases	Median Loss (in U.S. dollars)
United States	1038	48.8%	$120,000
Sub-Saharan Africa	285	13.4%	$143,000
Asia-Pacific	221	10.4%	$245,000
Latin America and the Caribbean	112	5.3%	$174,000
Western Europe	110	5.2%	$263,000
Eastern Europe and Western/Central Asia	98	4.6%	$200,000
Southern Asia	98	4.6%	$100,000
Canada	86	4.0%	$154,000
Middle East and North Africa	79	3.7%	$275,000

Şekil 4.2 Vakaların coğrafi dağılımı (İnt. Kyn. 1).



Şekil 4.3 Suistimal türlerine göre kayıp miktarları (İnt. Kyn. 1).

Uyar ve Yelgen (2015)'e göre Bilgi ifşaları temelde iki grupta incelenebilir:

- Birincisi, kurum ya da işletmelerin muhasebe hileleri veya skandallarının çalışanlar tarafından etik dışı bulunması nedeniyle yapılmış olan ifşalardır. Bu ifşalar, genelde kurum bünyesinde yeterli düzeyde ihbar mekanizmasının bulunmaması sebebiyle örgüt

içerisinde çözüm bulunamadığından, bilgilerin kamuoyu baskısı oluşturabilecek mecralara ulaştırılmasını amaçlamaktadır.

- İkincisi ise belirli bir amaç doğrultusunda, kurum çalışanlarının rüşvet, tehdit, şantaj gibi yöntemlerle bilgi sızdırmaya zorlandığı ya da bilgi kaynağına izinsiz, kanunsuz ve benzeri başka illegal yöntemlerle erişilerek elde edilen bilgilerin art niyetli ifşasıdır.

Aktan (2006)'ya göre birinci türden bilgi ifşaları da yöntem açısından iki grupta incelenebilir:

- İçsel bilgi ifşası, raporlamanın veya ifşanın kurum içerisindeki üst yönetime bildirilmesidir.

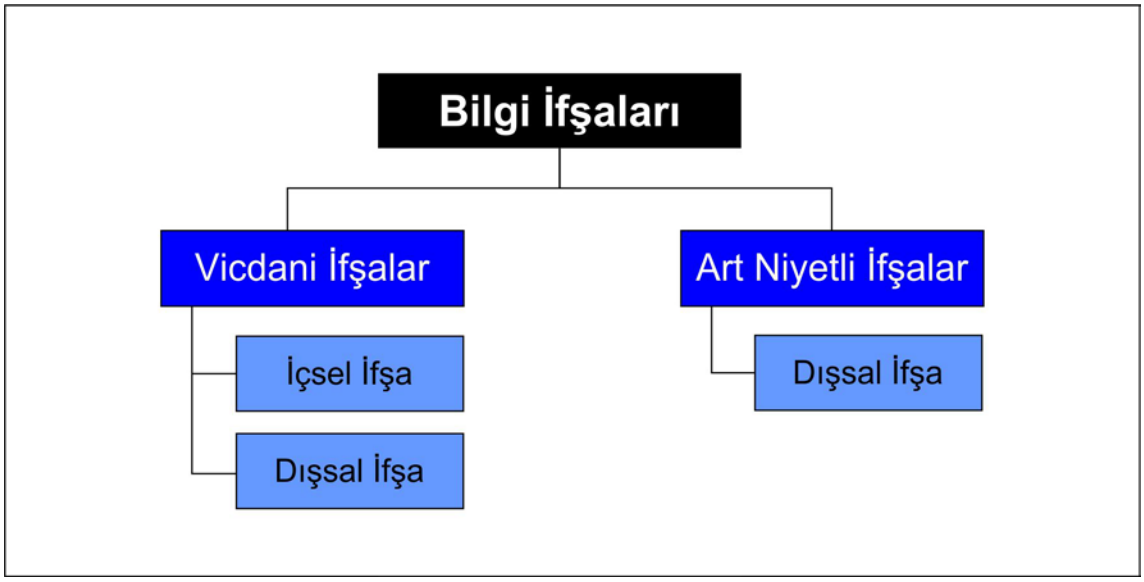
- Dışsal bilgi ifşası ise raporlamanın veya ifşanın kurum dışında, medyaya, adli makamlara ya da siyasi otoriteye yapılmasıdır.

Bilgi ifşalarının meşru görülebilmesi için kuruluş içindeki etik dışı veya kanunsuz uygulamaların özellikle topluma veya çalışanlara karşı etkilerinin olması gerekir.

Bununla beraber söz konusu uygulamaların, kuruma yetkili mercilerce bilgi verilmiş olmasına rağmen düzeltici tedbirlerin alınmamış olması gerekir. Bu noktadan sonra ifşacının, bilgi ifşası karşılığında, kendisine ya da yakın çevresine menfaat sağlamadan yapmış olduğu ifşalar meşru görülebilmektedir (Mercan vd. 2012).

Bilgi ifşacısının; çalışma arkadaşları veya üst düzey yöneticiler gibi birçok etkenle mücadele ederken daha büyük çapta sorunlarla boğuşması, hatta siyasi yönetimle de mücadele etmesi gerekebilir. Bu bağlamda ifşaların başka bir boyutu da sansürdür. İnt. Kyn. 13'e göre "sansür" kelimesi "Her türlü yayının, sinema ve tiyatro eserinin hükûmetçe önceden denetlenmesi işi, sıkı denetim" anlamına gelmektedir.

Şekil 4.4'de bilgi ifşalarının ifşa çeşitlerine göre türleri görülmektedir.



Şekil 4.4 Bilgi ifşalarının ifşa çeşitlerine göre türleri.

Bunun yanında sansür, çeşitli kavramların çeşitli yollarla kontrol altına alınması olarak da tanımlanmaktadır. Sansür genelde hükümetler tarafından toplumu korumak amacıyla ve toplumu ilgilendiren konularda uygulanmaktadır (İnt. Kyn. 22).

4.2.1 WikiLeaks Ve Panama Belgeleri Ölçeğinde Bilgi İfşaları

Kamu ve özel sektördeki bilişim teknolojileri payının artmasıyla; bilgisayar verileri, yüksek düzeydeki gizli bilgiler ve kişisel veriler gibi önemli verilerin depolanması da buna paralel olarak artmaktadır (İnt. Kyn. 17). Özellikle kamusal hizmet verilen kurumlarda bulunan kişisel veriler güncellenerek çoğalmakta, doğal olarak bu verilere göz koyan bilgisayar korsanlarının sayıları da artmaktadır.

Verilerin bulunduğu ortamlardaki güvenlik zafiyetleri bilgisayar korsanları tarafından istismar edilerek yüksek düzeydeki gizli bilgiler ele geçirilebildiği gibi vicdani ya da ahlâki sebeplerle kurum çalışanları tarafından da bilgiler ifşa edilebilmektedir (Tataroğlu 2013).

70'li yıllarda yayınlanan Pentagon Belgeleri örneğinde, belgeleri kendisinin sızdırdığını itiraf eden Daniel Ellsberg: "Bu savaşı durdurmak için siz de hapse girmeyi göze almaz mıydınız?" diyerek kendisini savunmuştur. 2010 yılında WikiLeaks aracılığı ile Afganistan ve Irak savaşlarına ait belgeleri sızdıran Chelsea Manning, casusluktan

yargılandığı dava sırasında kendisini Irak ve Afganistan'da gerçekleştirilen yasadışı uygulamalar nedeniyle vicdan azabı çeken birisi olarak tanıtmıştır.

2013 yılında NSA çalışanı Snowden; devletin yasadışı olarak iletişimi dinlediği ve insansız hava araçlarıyla gerçekleştirilen saldırılardan ötürü tutuklanma ihtimaline rağmen, gizli servise ait birçok gizli bilgiyi sızdırmıştır. Snowden "Çevremde kendim kadar değer verdiğim insanların zarar görmesindense hapse girme riskini almaya ya da kişisel olarak bir negatif sonuca katlanmaya hazırım" demiştir (Çalışkan 2016).

Anonim kaynaklardan sızdırılan bilgileri kamuoyuna ifşa eden kuruluşlardan olan WikiLeaks; Amerika Birleşik Devletleri'ne ait diplomatik misyonlar, elçilik ve 274 farklı konsolosluktan Dışişleri Bakanlığı'na gönderilen gizli belgelerin yayınlandığı sızıntılara, ünlü "Watergate" skandalını çağrıştıran "Cablegate" ismini vermiştir. Bu ismin verilmesinin perde arkasında, istifa ederek ABD başkanlığından ayrılan ilk ve tek başkan olarak tarihe geçen Richard Nixon'ın adının geçtiği "Watergate" skandalı vardır.

WikiLeaks, Cablegate'ı yayınladığı yılın temmuz ayında "Afgan Savaş Günlükleri"ni, ekim ayında ise "Irak Savaş Kayıtları" adı altında "savaş günlükleri" olarak da bilinen sızıntıları yayınlamıştır. Bu sızıntılar sayesinde ABD'nin Afganistan ve Irak savaşı sırasında işlediği savaş suçları, sivil ölümleri ve tutuklulara uygulanan insanlık dışı uygulamalar tüm dünyanın gözleri önüne serilmiştir (Çalışkan 2016).

4.2.2 Küresel Bilgi İfşaları: WikiLeaks

Görünürde bir internet sitesi olan WikiLeaks kendine özgü bir örgütlenmesi olan ve arkasında çok sayıda bilişim uzmanı, gazeteci gibi, alanında uzman sayılacak gönüllüler bulunan bir sistemdir. Dünyanın dört bir yanından destek veren bu gönüllüler internet aracılığı ile bilgilerin ele geçirilmesinden tasnif edilmesine, farklı dillere tercüme edilmesinden yayınlanmasına kadar birçok konuda yardımda bulunmaktadır (Ertem ve Uçkan 2011).

4 Ekim 2006 tarihinde yayına giren WikiLeaks web sitesi "wikileaks.org", ABD'ye kayıtlı bir alan adıdır (İnt. Kyn. 30). Sitenin kurucuları arasında Çinli ve Tibetli muhaliflerin yanı sıra gazeteciler, matematikçiler, kripto uzmanları ve ABD, Tayvan,

Avustralya, Avrupa ve Güney Afrika'dan teknoloji uzmanlarının olduğu ilan edilse de kurucular hiçbir zaman tam olarak tespit edilememiştir (İnt. Kyn. 49).

WikiLeaks'in görünen yüzü, Avustralyalı eski bir bilgisayar korsanı, gazeteci ve aktivist olan Julian Assange aynı zamanda sitenin kurucusu olarak da bilinmektedir (İnt. Kyn. 62). Assange kendisini sitenin danışma kurulu üyesi olarak tanıtmaktadır (İnt. Kyn. 36). Sitenin arayüzü wiki yapısında yani kullanıcıların yorum yapabildiği, etkileşimli bir yapıya sahiptir.

Sitenin kuruluşundan bir yıl sonra WikiLeaks, on üç ülkeye ait 1,2 milyon sızıntı bilgi olduğunu ilan etmiştir. Ekim 2009 tarihinde siteye kayıtlı 1200 gönüllü bulunmaktaydı (Ertem ve Uçkan 2011).

İnt. Kyn. 45'e göre WikiLeaks ilk gizli belgeyi Aralık 2009'da yayınlamıştır. Bu, Somali İslami Dava Birliği lideri Şeyh Hasan Tahir Üveys'in hükümet yetkililerini öldürtmeye karar verdiğini içeren "Gizli Bir Karar" başlıklı gizli bir belgeydi. TOR ağı üzerinden gönderilen Çin kaynaklı belgenin gerçekliğinden emin olamayan WikiLeaks, siteden gönüllülerine çağrı yaparak belgenin analiz edilmesini istemiştir.

İletişimde sitenin wiki yapısında olmasının geri bildirim için büyük kolaylık sağlayacağı öngörülmüştür. Söz konusu belgenin gerçekliği hiçbir zaman kanıtlanamamasına rağmen çıkan haberler sızıntının kaynağının WikiLeaks olduğunu akla getirmiştir. Birkaç hafta sonra anti-kapitalist bir kongre olan Dünya Sosyal Forumu'nda web sitesi hakkında sunum yapmak üzere Kenya'ya giden Assange birkaç ay sonra geri dönerken yanında getirdiği ve Kenya seçimlerine etki edecek belgelerin yayınlanmasıyla WikiLeaks'i geri dönülemeyecek bir yola sokmuştur (İnt. Kyn. 45).

WikiLeaks tarafından 2010 yılının ilkbaharında, Amerika Birleşik Devletleri ordusuna ait altı yıllık gizli askeri bir arşiv yayınlanmıştır (İnt. Kyn. 15). Arşivde Afganistan ve Irak'taki ABD önderliğinde gerçekleştirilen savaşlar ile ilgili gizli belgeler yer almaktadır.

İnt. Kyn. 15'e göre Ocak 2004 - Aralık 2009 dönemini kapsayan 92 bin gizli askeri rapor WikiLeaks tarafından tüm dünyaya ifşa edilmiştir. Belgelerde yer alan ordu mensupları ve müttefiklerine ait bilgilerin ifşa edilmesinin hayati tehlike oluşturmasının

yanı sıra ifşa nedeniyle ABD kaynak ve yöntemlerinin ifşasıyla, ulusal güvenliğin tehlikeye düşmesi ihtimaline karşı Pentagon, birinci önceliği bu konularda tedbir almaya ayırmıştır. Aynı zamanda sızıntının kaynağının tespiti için bir soruşturma da başlatılmıştır.

Bir süre sonra ABD Ordusu, analist olarak görev yapan kıdemli er Bradley Manning'i, çok sayıda yasadışı işlem yapması, gizli verileri sızdırması ve ulusal güvenliği riske atması nedeniyle tutuklamıştır. Manning, Bağdat'ın 40 mil doğusundaki FOB Hammer üssüne götürülerek burada hapsedilmiştir (İnt. Kyn. 15).

Manning; ABD'ye ait bir helikopter hava saldırısının videosunu nasıl sızdırdığı konusunda çevrimiçi konuştuğu eski bir bilgisayar korsanı tarafından ihbar edilmiştir. Manning'e göre, WikiLeaks'e üç bilgi daha sızdırılmıştır. Birincisi 2009'da Afganistan'nın Gerani bölgesinde sivillerin ölüme neden olan hava saldırısıdır. İkincisi WikiLeaks'i, güvenlik tehdidi olarak değerlendiren ve Mart ayında yayınlanan gizli bir askeri belge ve üçüncüsü ise daha önce duyulmamış türden bir ifşadır. Bu ifşada Manning'in "neredeyse suç oluşturacak politik iletişim" şeklinde tanımladığı, ABD'ye ait 260 bin adet diplomatik belge yer almaktadır (İnt. Kyn. 15).

İnt. Kyn. 15'e göre Manning iki ayrı güvenli dizüstü bilgisayardan iki farklı ağa erişebilmiştir. Birincisi Savunma Bakanlığı ve Dışişleri Bakanlığı tarafından kullanılan SIPRNET'tir, bu ağda güvenlik seviyesi "Gizli" ve daha düşük belgeler bulunmaktadır. İkincisi ise istihbarat teşkilatları tarafından kullanılan "the Joint Worldwide Intelligence Communications System" (JWICS diğer adıyla JAYwicks) ağıdır. Söz konusu ağ "Çok Gizli" ve hassas bilgilerin bulunduğu bir ağdır.

Manning bu ağlardan elde ettiği gizli belgeleri, FOB Hammer üssüne girerken yanında getirmiş, üzerinde "Lady Gaga" yazılı, zararsız gibi görünen, boş bir CD'ye kaydederek üs dışına çıkarmıştır. Bu durum tüm anlatılanlar hakkında bir soruyu ortaya çıkarmaktadır: "Manning, hassas ağlara erişmeyi nasıl başarabildi?". Manning'in bu hassas ağlara nasıl bağlandığı tam olarak bilinmemektedir. Bilişim güvenliği açısından değerlendirildiğinde bu kadar hassas verilere erişim yetkisinin bulunmaması gerektiği ortaya çıkmaktadır (İnt. Kyn. 5).

İnt. Kyn. 5'e göre Manning gerçek bir ihtiyaç ya da gereklilik olmaksızın, çeşitli ağlara erişebildiği gibi hassas verilere de erişebilmiştir. Bu durum, iyi tanımlanmış erişim kontrolü politikalarının ve uygulama kontrol mekanizmalarının eksikliğinin, bunun gibi güvenlik sorunlarının temelinde yer aldığı sonucunu ortaya çıkarmaktadır. Devlet kurumları, askeri ve diğer kuruluşlar, faaliyetlerini yönetmek ve çeşitli hizmetleri sunmak için bilgi teknolojisi gücünü giderek daha fazla kullandığından, bilgi güvenliği en büyük endişe haline gelmiştir.

WikiLeaks sızıntıları, hassas verileri etkili bir şekilde güvence altına almanın, kurum ve kuruluşlar için büyük bir sorun olduğunu bir kez daha kanıtlamıştır. Günümüzde, "evden çalışma" (tele-commuting) kavramları giderek kurum ve kuruluşlarda kabul görmektedir. Bu durum, USB bellek ve dizüstü bilgisayarlar gibi dijital depolama aygıtlarının kullanımında artışa neden olmuştur.

Veriler bu cihazlarda bulunduğunda bilgi güvenliğini sağlamak daha da zor hale gelmektedir. Gizli bilgiler mobil aygıtlar yoluyla kötü niyetli kullanıcıların eline kolayca geçebilmektedir (İnt. Kyn. 5).

Siber tehditlerin özel kuruluşlara etkisi, finans veya itibar kaybı ile sınırlı kalmamakta, bazen, kurumsal ya da endüstriyel casusluk durumunda daha büyük zararlar da ortaya çıkmaktadır, hatta devlet kurumlarındaki güvenlik zaafları nedeniyle, ulusal güvenlik bile tehlikeye düşebilmektedir.

Bununla birlikte, tıpkı özel kuruluşlar gibi devlet kurumları da vatandaşlara hizmet verirken bilgi bütünlüğü ve güvenliği ile kamu güvenini oluşturmakla görevlidir. Politik analistlere göre, WikiLeaks'ın küresel siyasi sonuçlarının olması nedeniyle bu tür eylemler ulusal güvenlik için en büyük tehdidi oluşturmaktadır (İnt. Kyn. 5).

WikiLeaks ifşacıların anonimliğini ve takip edilmemelerini sağlamak üzere birtakım şifreleme teknikleri kullanmaktadır. İfşacıların yasal, siyasal, ekonomik veya fiziksel saldırılardan koruması amacıyla karmaşık şifre algoritmaları ve postalama teknolojileri geliştirilmiştir.

WikiLeaks teknik olarak; MediaWiki, OpenSSL, FreeNet, TOR ve PGP'nin kendisi için değiştirilmiş sürümlerini bütünleştirerek kullanmaktadır. WikiLeaks'e göre; sızdırılan

bilgiler birçok örgüt ve yetkili çevreden bireylere kadar ulaştırılır ve sızdırılan bir belgenin sansürlenmesi artık imkânsız hale gelir (İnt. Kyn. 19).

WikiLeaks, Afganistan Savaşı ile ilgili belgeler kapsamında, ayrıca "Sigorta dosyaları" adlı şifrelenmiş bir arşiv yayınlamıştır. 100 bin defadan fazla indirilen AES256 ile şifre koruması bulunan sıkıştırılmış arşivin boyutu 1.4 GB büyüklüğündedir. Spekülatörlere göre, WikiLeaks'e veya sözcüsü Assange'a herhangi bir şey olursa şifrenin dağıtılacağı düşünülmektedir. Spekülatörler, diğer arşivlerden çok daha büyük olan arşivin, 2004 ve 2009 yılları arasındaki Irak savaşıyla ilgili belgeleri içerdiğini düşünmektedir. Bu durum, WikiLeaks'e karşı etkin biçimde harekete geçilmemesinin nedeni olarak da görülmektedir. Assange dosya ile ilgili olarak 504 ABD elçiliği ile ilgili belgenin Murdoch ve News Corp. isimli yayın kuruluşlarında da bulunduğunu söylemiştir (Dragt 2012).

4.2.2.1 WikiLeaks'in Çalışma Modeli

İfşacı, elindeki gizli bilgileri WikiLeaks'e sızdırmak istediğinde anonimlik sağlayan TOR isimli uygulamayı kullanmaktadır. TOR uygulaması ifşacının anonim kalması için gerekli bir dizi prosedürü işleterek hem gizliliği sağlamakta hem de takip edilmeyi engellemektedir.

Söz konusu yöntemle gönderilen ve alınan mesajları şifrelemek amacıyla PGP uygulaması kullanılmaktadır. Bu uygulama sayesinde gönderilen mesaj ele geçirilse bile şifreli bir mesaj olduğu için okunması mümkün olmamaktadır. PGP, 512 ila 4096 bite kadar şifreleme yapabilmektedir. Bu yöntemle ifşacının anonimliği korunurken WikiLeaks için çalışan gönüllülerin de güvenliği sağlanmaktadır (Ertem ve Uçkan 2011).

Gelen bilgilerin doğruluğunu test etmek, çeşitli analizler yapmak ve bireysel zararların oluşmasını engellemek üzere (kimlik bilgilerinin, isimlerin vb. kapatılması gibi) gönüllülerden yararlanılmaktadır. Küçük boyutlu sızıntılarda gönüllülerden yardım alınırken, Irak Savaşı belgelerinde olduğu gibi (400 bin belge) büyük boyutlardaki sızıntıları incelemek ve analiz etmek için özel hazırlanmış yazılımlar ve bilgi işlem gücü kullanılmaktadır (Ertem ve Uçkan 2011).

WikiLeaks tarafından, Kenya'daki yargısız infazlar, Fildişi Sahilleri'ne bırakılan zehirli atıklar, Scientology Tarikatı ve Guantanamo Kampı'ndaki insanlık dışı uygulamalar ifşa edilmiştir. 2010 yılı ise Assange yönetimindeki WikiLeaks'in dünya çapında bilinirliğini artırdığı yıl olmuştur.

WikiLeaks Afganistan ve Irak'ta yaşanan savaş sürecinde ABD tarafından gerçekleştirilen ve kamuoyundan gizlenen kanunsuzlukları ve insanlık dışı uygulamaları içeren binlerce gizli belgeyi belirli bir düzen içerisinde yayımlamıştır. 5 Nisan 2010'da "Collateral Murder" isimli, büyük ses getiren, iki gazetecinin ve sivillerin öldürüldüğünü gösteren video yayınlanmıştır (Adaklı 2012).

Adaklı (2012)'ya göre WikiLeaks tarafından yayınlanan en hassas belgeler tarih sırasına göre şöyledir:

- 5 Nisan 2010: *"Collateral Murder: WikiLeaks reveals Pentagon journalist murder coverup in Iraq"* Temkinli Cinayet: WikiLeaks, Irak'ta gazeteci cinayetini Pentagon'un örtbas ettiğini ortaya koymuştur.
- 25 Temmuz 2010: *"Afghan War Diary, 2004-2010"* 2004-2010 yılları arası Afganistan Savaşı Günlükleri yayınlanmıştır.
- 22 Ekim 2010: *"Iraq War Logs, 2004-2009"* 2004-2009 yılları arası Irak Savaşıyla ilgili kayıtlar yayınlanmıştır.
- 28 Kasım 2010: *"Secret US Embassy Cables (Cablegate), 1966-2010"* 1966 - 2010 yılları arası Büyükelçilik diplomatik yazışmaları yayınlanmıştır.

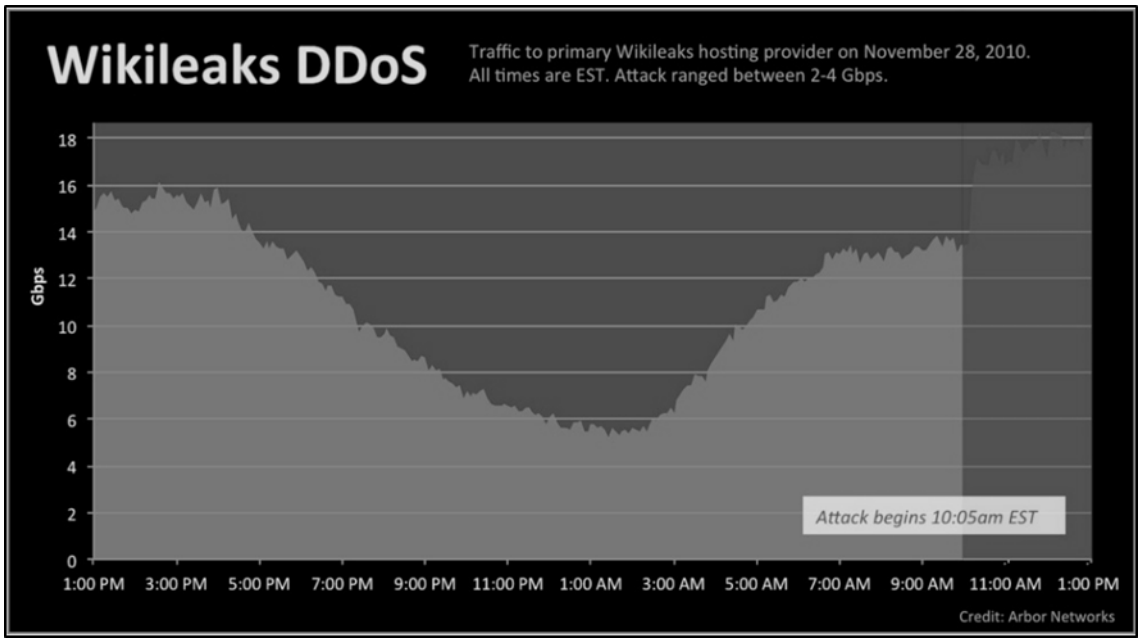
ABD yönetimi; Cablegate ifşası sonrasında Assange'ı itibarsızlaştırmaya, WikiLeaks'i de yayın yapamaz hale getirmeye çalışmış, üniversite öğrencilerinin yanı sıra özellikle yurtdışında bulunan askerler WikiLeaks'e karşı uyarılmıştır. ABD ve batılı ülkeler (özellikle Fransa) yanında, Suudi Arabistan ve Çin gibi ülkeler de WikiLeaks'e yasak getirerek sansürlemeye çalışmışlardır (Erdem 2011).

Takip eden günlerde farklı şirketler ve organizasyonlar da WikiLeaks'e karşı harekete geçmişlerdir. Amazon web hizmetleri WikiLeaks web sitesini yayınlamayı durdururken Aralık ayının başında WikiLeaks içeriklerini sunucularından çıkarmıştır (Sauter 2013).

Sauter (2013)'e göre 3 Aralık 2010 Cuma gecesinden itibaren yaşananlar şöyle gelişmiştir: Cuma gece yarısı civarında çevrimiçi bir WikiLeaks sitesi kalmamıştır. DNS sağlayıcısı olan EveryDNS firması WikiLeaks'e yapılan Şekil 4.5'de etkisi görülen çoklu hizmet reddi (DDoS) saldırıları sebebiyle EveryDNS'in sistem kararlılığının bozulduğu gerekçesi ile hizmet veremeyeceğini açıklamıştır. Şirketin WikiLeaks'e ait DNS kayıtlarını silmesi nedeniyle geçici olarak web sitesi de erişilemez hale getirilmiştir. Google gibi arama motorlarının önbelleği (cache) ya da doğrudan IP adresi yazılarak siteye erişilebilse de bu şekilde devam etmek imkânsızlaşmıştır.

"wikileaks.ch" alan adı üzerinden hizmetin yeniden başlatılması amacıyla WikiLeaks alan adını İsviçre'deki sunuculara taşıyacağını açıklamıştır. Çarşamba gününe gelindiğinde WikiLeaks'e yapılan DDoS saldırıları püskürtülmüştür. WikiLeaks, ikisi Fransa'nın Octopuce firmasınca, diğeri ABD'li Amazon E2 bulut sunucularında bulunan, toplamda üç sunucu sayesinde bu saldırıları atlatmış olsa da EveryDNS'ten sağlanan alan adı hizmeti olmadan siteye URL üzerinden hâlâ erişilemez haldedir (Sauter 2013).

Perşembe gününe gelindiğinde bu kez Amazon web hizmetleri; Milli Güvenlik Komitesi Başkanı Senatör Joe Lieberman'ın çağrısına uyarak WikiLeaks sunucularına ev sahipliği yapmayacağını açıklayarak sistemlerinden çıkartmıştır (İnt. Kyn. 44).



Şekil 4.5 WikiLeaks hosting sağlayıcısına yapılan DDoS saldırı grafiği (İnt. Kyn. 41).

Kısa süre sonra WikiLeaks'e "Bankacılık Ablukası" başlamıştır. Paypal, PostFinance, MasterCard, Visa ve Bank of Amerika WikiLeaks'e yapılan online bağışları geri çevirmeye başlayarak organizasyona giden parasal bağış akışını kesmiştir (Sauter 2013).

"wikiLeaks.org" sitesinin kapanmasının üzerinden 24 saat geçmeden yüzlerce ayna site (orijinal sitenin birebir kopyası) aracılığı ile WikiLeaks yeniden yayına başlamıştır (Erdem 2011). WikiLeaks ve Assange'ın bu saldırılara maruz kalması ve Assange'ın İsveç'te işlediği bir suç nedeniyle, ifşanın hemen ertesinde, 7 Aralık 2010'da tutuklanmasına rağmen geri atmamaları toplumda sempati oluşmasını, binlerce gönüllünün buraya destek vermesini ve Assange'ın bir kahraman olarak görülmesini sağlamıştır (Adaklı 2012).

Sauter (2013)'e göre WikiLeaks'in karşılaştığı sorunlar Anonymous isimli bilgisayar korsanları grubunun dikkatini çekmiştir. Bu grup içerisindeki AnonOps isimli daha küçük bir grubun organizatörlüğünde "Operation Payback" geri ödeme operasyonu ismiyle bilinen hizmet dışı bırakma saldırıları (DDoS) başlatılmıştır.

Çizelge 4.1 PayBack DDoS saldırılarının etkileri (İnt. Kyn. 43).

Site	*Kesinti sayısı*	*Kapalı kalma süresi Saat:Dakika*
thepaypalblog.com	77	8:19
postfinance.ch	55	33:08
e-finance.postfinance.ch	61	33:07
www.aklagare.se	11	13:00
everydns.com	4	0:31
lieberman.senate.gov	8	0:12
advbyra.se	32	5:11
sarahpac.com	8	0:25
TOPLAM	*256*	*94 Saat*

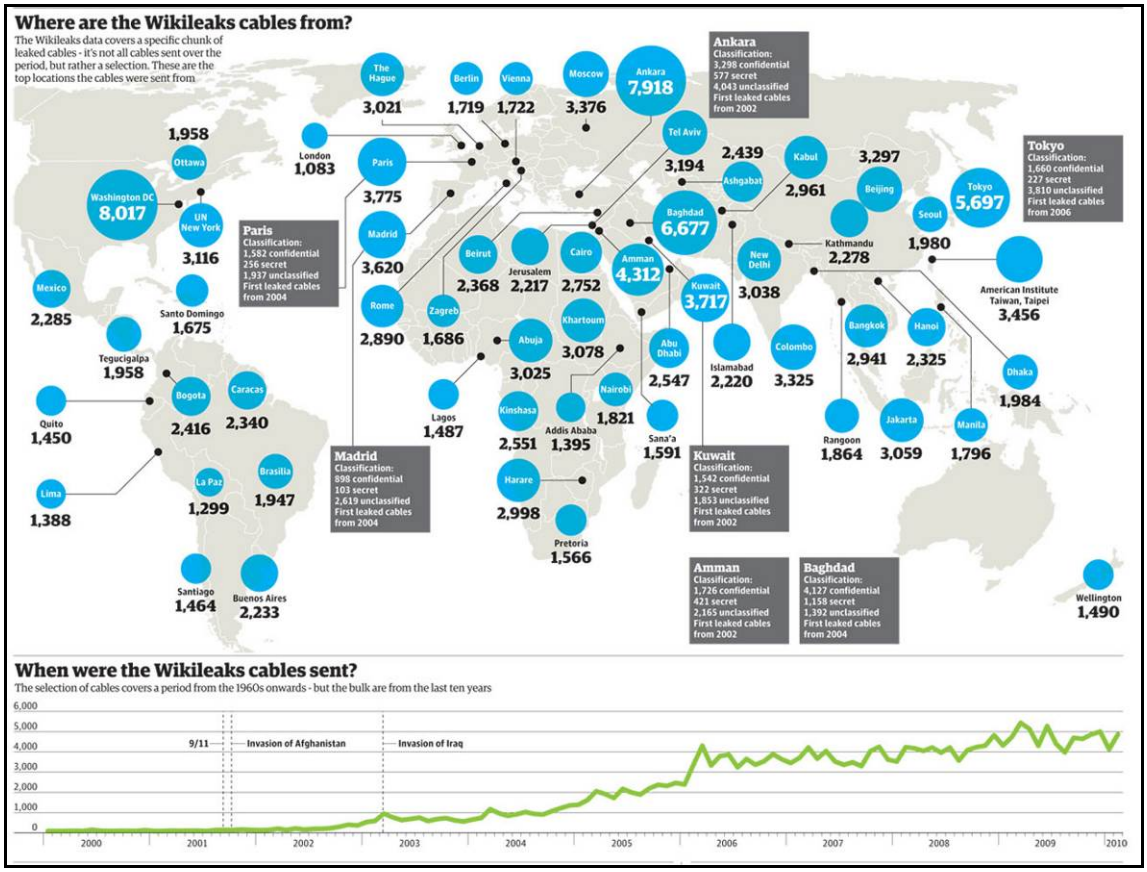
Etkileri Çizelge 4.1'de görülen bu saldırılarda Amerikan Sinema Derneği, telif hakları ve korsanlıkla mücadele gruplarına ait sistemler de hedef alınmıştır. Anonymous'un alt grubu olarak olarak bilinen Anon'lar, WikiLeaks'e ve halka açık yüzü olan Julian

Assange'a karşı yapılanlara cevap vermek üzere Payback operasyonun yelpazesini genişletmiştir.

Anonymous ve AnonOps ilk olarak 6 Aralıkta İsviçre bankacılık hizmeti PostFinance'ı hedef almış, sonrasında dört gün boyunca da İsveç Savcılık Makamı, EveryDNS, Senatör Joseph Lieberman, MasterCard, Visa, Paypal ve "amazon.com" gibi birçok siteye saldırarak bir süreliğine buralara erişimi engellemiştir (Sauter 2013).

Dünya üzerinde ABD'ye ait 274 elçilik, konsolosluk ve diplomatik misyon tarafından Dışişleri Bakanlığı'na gönderilen gizli yazışmaların yayınlandığı Cablegate sızıntıları birçok ülkede geniş yankılar uyandırsa da bunun en güçlü etkisi Kuzey Afrika ve Ortadoğu bölgelerinde olmuştur.

Bu yayınlar, 2010 yılında Tunus'la başlayan, hemen ardından Mısır'la devam eden, sonrasında hemen hemen tüm Arap coğrafyasına yayılan, "Arap Baharı" olarak da adlandırılan bir dizi halk ayaklanmasını tetiklemiştir (Çalışkan 2016).



Şekil 4.6 WikiLeaks sızıntılarında yer alan ülkeler (İnt. Kyn. 40).

4.2.2.2 WikiLeaks Belgelerinde Türkiye

Kasım 2010'da WikiLeaks tarafından yayınlanan, The Guardian, The New York Times ve Der Spigel gibi önemli gazete ve dergiler tarafından haberleştirilen Cablegate dosyaları dünya çapında büyük ilgi görmüş, ülkemizde de dikkatleri çekmiştir. Hükümetin önemli üyeleriyle ilgili iddiaların bulunduğu belgeler, bazı yerel ve ulusal medyanın ideolojik yönelimleri doğrultusunda yeniden kurgulanarak bir mücadele aracı olarak kullanılmıştır (Toruk ve Sine 2012).

İnt. Kyn. 40'a göre Türkiye, 7 bin civarındaki belge ile Cablegate sızıntılarında, ABD'den sonra hakkında en çok belge yayınlanan ikinci ülke olmuştur. Belgeler daha çok, dış politika, finansal faaliyetler, Türk-İran ilişkileri, Türk-ABD ilişkileri, Türk Silahlı Kuvvetleri ve AB katılım süreciyle ilgilidir.

WikiLeaks sadece 2010 yılında değil, farklı zamanlarda da Türkiye'yi ilgilendiren konularda belgeler yayınlamıştır. Özellikle 8 Nisan 2013'de PlusD ismiyle 2 milyon civarında diplomatik içerikli belge yayınlanmıştır. PlusD: Public Library of US Diplomacy kelimelerinin ilk harflerinden türetilmiş bir kelimedir (İnt. Kyn. 2). PlusD sızıntılarında özellikle 1973-76 yılları arasındaki diplomatik yazışmalar bulunmaktadır.

Bu belgelerde dönemin siyasi aktörlerine ve siyasi tablosuna ait yorumların yanında, Türk-Arap dünyası ilişikleri ve Kıbrıs sorunuyla ilgili 38 bin civarında belge yer almıştır (İnt. Kyn. 3). Bunun yanında WikiLeaks'te farklı yıllara, farklı zaman dilimlerine ait belgeler de yayımlanmaya devam edilmektedir.

4.2.3 Küresel Bilgi İfşaları: Panama Belgeleri

2013 yılındaki İsveç sızıntısı (SwissLeaks) ve 2016 yılındaki Panama Belgeleri (Panama Papers) sızıntıları küresel finans sisteminde güvenli bir limanın kalmadığını göstermiştir.

Panama merkezli, dünyanın dördüncü büyük offshore firması olan Mossack Fonseca'ya ait veri tabanından sızdırılan 11.5 milyon belge, Uluslararası Gazeteciler Konsorsiyumu Konseyi (ICIJ) tarafından tüm dünyaya servis edilmiştir.

İnt. Kyn. 63'e göre sızıntıya firmanın Panama merkezli olması nedeniyle "Panama Belgeleri" ismi verilmiştir. Belgeler Alman gazetesi Süddeutsche Zeitung tarafından, açıklanmayan bir kaynaktan elde edilmiştir. Daha sonra ICIJ, bu belgeleri The Guardian ve BBC de dâhil olmak üzere geniş bir uluslararası ortak ağ ile paylaşmıştır.

Ortaya çıkan belgeler, zenginlerin gizli offshore şirketleri aracılığıyla vergi cennetlerinde kullanabileceği sayısız yolu göstermektedir. On iki ulusal lider, denizaşırı vergi cennetlerini kullandığı bilinen 143 siyasetçi, bunların aileleri ve dünyadaki yakın ortakları belgelerde yer almaktadır (İnt. Kyn. 63).

Panama Belgeleri'nde: Rusya Devlet Başkanı Vladimir Putin ile ilişkilendirilen Sergei Roldugin, Pakistan Başbakanı Navaz Şerif, Arjantin Başbakanı Mauricio Macri, Gürcistan eski Başbakanı Bidzina Ivanishvili, İzlanda Başbakanı Sigmundur Davíd Gunnlaugsson, Irak eski Başbakanı Ayad Allawi, Ürdün eski Başbakanı Ali Abu al-Ragheb, Katar Eski Başbakanı Hamad bin Jassim bin Jaber Al Thani, Katar Eski Emiri Hamad bin Khalifa Al Thani, Sudan Eski Başkanı Ahmad Ali al-Mirghani, Suudi Arabistan Kralı Salman bin Abdulaziz bin Abdurrahman al-Saud, Abu Dhabi Emiri ve Birleşik Arap Emirliği Başkanı Khalifa bin Zayed bin Sultan Al Nahyan, Ukrayna eski devrik lideri Pavlo Lazarenko, Ukrayna Başbakanı Petro Poroshenko, Azerbaycan Cumhurbaşkanı İlham Aliyev (eşi ve çocukları aracılığıyla yapılan işlemler nedeniyle), Suriye Cumhurbaşkanı Beşar Esad (kuzenleri olan Rami ve Hafez Maklhlouf üzerinden yaptığı işlemler nedeniyle), İngiltere Başbakanı David Cameron (babası Ian Cameron nedeniyle), Çin Halk Cumhuriyeti Eski Başbakanı Li Peng (kızı Li Xiaolin nedeniyle), Moğolistan eski Başbakanı Sükhbaataryn Batbold ve halen Avustralya Başbakanı olan Malcolm Turnbull güçlü oyuncular olarak belgelerde yer almaktadır (İnt. Kyn. 28).

Offshore; kıyı bankacılığı olarak da adlandırılan, serbest bölgelerde faaliyet gösteren ve ulusal bankacılık sisteminin dışında tutulan ve buna göre de muafiyetler tanınan bir tür uluslararası bankacılıktır (Çeker 2006).

İnt. Kyn. 61'e göre kıyı bankacılığı, hesap sahibinin yerleşik olduğu ülke dışında bir yerde kurulu olanlardan seçilmektedir. Bu gibi yerlerde genellikle vergi oranları ve bürokratik işlemler çok azdır, denetim ise ya hiç yoktur ya da çok az uygulanmaktadır. Bu tip yerlerde yargı denetiminin de düşük seviyede olması, kara para, haksız kazanç ya

da kanunsuz yollardan elde edilen kazançlar veya haklı bir kazanç olsa dahi vergisi ödenmemiş gelirler için güvenli bir liman oluşturmaktadır.

Kocaman (2016)'a göre bir yıllık dünya ticaretinde dolaşan para miktarı 72 trilyon dolardır. Bu miktarın yarısı offshore merkezlerinde işlem görmektedir. Ülkelerinde vergi kaçıran büyük şirketler, ailesinden ya da eşinden para saklayan zenginler, geleceklerini sağlama almaya çalışan siyasetçiler, rüşvet paralarını gizlemeye çalışan üst düzey bürokratlar, yurtdışı operasyonları yöneten gizli servisler gibi paranın izini kaybettirmeye çalışanlar için offshore hesaplar vazgeçilmez bir liman olarak görülmektedir. Vergi kaçırmada en çok tercih edilen 15 yöntemi ise şöyle sıralamıştır.

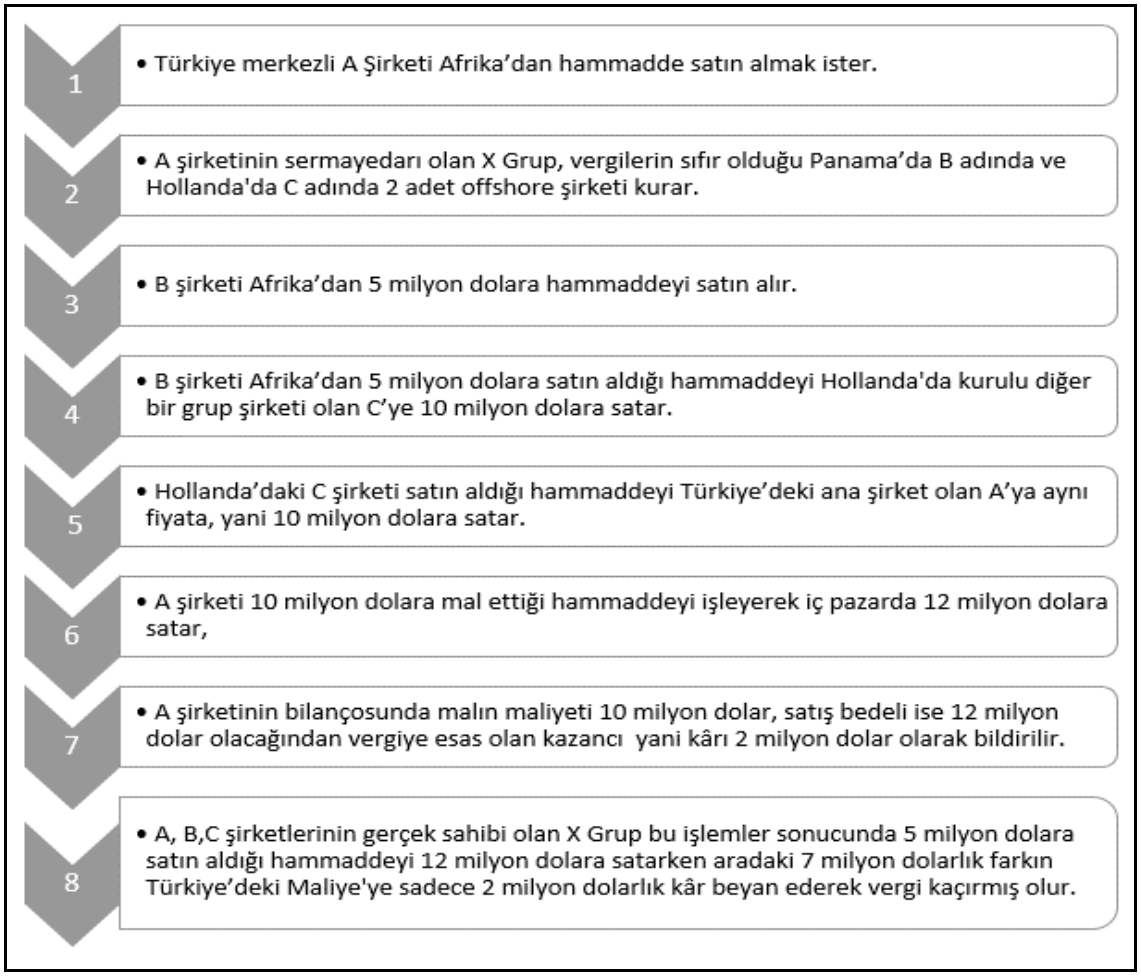
- Leasing anlaşmaları
- Yurtdışındaki grup şirketinden borçlanmak
- Acente anlaşması yapmak
- Grup şirketleri arasında ticari aktivite sağlamak
- Yurtdışındaki inşaat işlerine tedarik sağlamak
- Borsada yabancı görünümlü hisse senedi ve tahvil alım satımı yapmak
- Fikri mülkiyet, marka hakları ve bayiler adına ülke dışına ödemeler yapmak
- Sigortacılık faaliyetlerine para transferi gerçekleştirmek
- İthalat-ihracat işlemlerinde kârı, vergisiz ülkede bırakmak
- Kâr payı ödemelerinde vergiden kaçınmak
- Offshore'da şirket birleşmeleri ve satınalma işlemleri yapmak
- Proje hizmetleri ve Ar-Ge ödemelerini Offshore'a kanalize etmek
- Lojistik firmaları aracılığıyla aktarımlarda bulunmak
- Yurtdışında imalat yaptırmak
- Kurumsal yapılanma yöntemi kullanmak

Kıyı bankacılığında hesap açmak için çeşitli nedenler olsa da bunların en bilinenleri aşağıda açıklanmıştır:

- Kişi ve kurumların varlıklarını siyasi risklere karşı korumak. (Kıyı bankalarının bulunduğu yerler siyasal risklerin en düşük olduğu bölgelerdir.)

- Kişi ve kurumların varlıklarını gizlemek. (İki tür gizlilik söz konusu olabilir: İlk olarak varlığın devletten saklanması, ikinci olarak da aileden veya akrabalardan saklanması.)
- Kişi ve kurumlara hakkında açılacak davalara karşı varlıkları korumak. (Aleyhte açılabilecek tazminat davası gibi davalarda bu hesaplardaki varlıklar önceden bilinemediğinden davaların sonuçlarından korunmuş olunur.)

Büyük şirketler ticaret yaparken elde edecekleri kazançların vergisini azaltmak yani vergi kaçırmak için farklı yöntemler kullanabilmektedir. Ancak bu farklı yöntemler içerisinde öne çıkan, Şekil 4.7'de anlatılan yöntemdir.



Şekil 4.7 Sekiz adımda vergi kaçırma yöntemi (İnt. Kyn. 32).

Şekil 4.7'de yer alan yöntemde işleyiş şu şekilde olmaktadır:

Türkiye'de kurulmuş ve normal ticaretini yapan A şirketi, Afrika'dan satın aldığı ve Türkiye'de satmayı planladığı hammaddeyi, bir offshore şirketi olan B aracılığıyla 5

milyon dolara satın alır. B şirketi 5 milyon dolara aldığı hammaddeyi başka bir offshore şirketi olan C firmasına 10 milyon dolara satar. Ancak bulunduğu ülkede vergiler sıfır olduğu için vergi kaybı olmaz. C firması ise 10 milyon dolara aldığı hammaddeyi aynı fiyata Türkiye'deki A firmasına satar. A firması 10 milyon dolara satın aldığı hammaddeyi 12 milyon dolara iç piyasa sürer. A firması 10 milyon dolara alarak 12 milyon dolara sattığı ticaretten elde ettiği kâr üzerinden yani 2 milyon dolar üzerinden vergisini öder. Aradaki 7 milyon dolarlık kazancın vergisi, ülkemizin kasasına girmesi gerekirken her üç firmanın da sahibi olan A şirketinde kalır.

AB listelerinde yer alan ve kıyı bankacılığında en çok kullanılan merkezler; Andorra, Lihtenştayn, Guernsey, Monako, Morityus, Liberya, Seyşeller, Brunei, Hong Kong, Maldivler, Cook Adaları, Nauru, Niue, Marshall Adaları, Vanuatu, Anguilla, Antigua ve Barbuda, Bahamalar, Barbados, Belize, Bermuda, İngiliz Virgin Adaları, Cayman Adaları, Grenada, Montserrat, Panama, St. Vincent ve Grenadines, StKitts ve Nevis, Turks ve Caicos, Amerikan Virgin Adaları'dır. Bunların dışında da kıyı bankacılığı hizmeti veren birçok merkez bulunmaktadır.

4.2.3.1 Panama Belgelerinin Boyutları

2015 yılında gizli bir kaynak tarafından Panama'lı Off-Shore şirketi olan Mossack Fonseca'ya ait 11,5 milyon belge sızdırılmıştır. Bugüne kadar gerçekleşen en büyük doküman sızıntısı olarak kabul edilen belgelerde; politikacılar, iş adamları ve bürokrasiye ait kara para aklama, ambargoların delinmesi, vergi kaçakçılığı ve yasa dışı ekonomik faaliyetler yer almaktadır (Kılınç 2016).

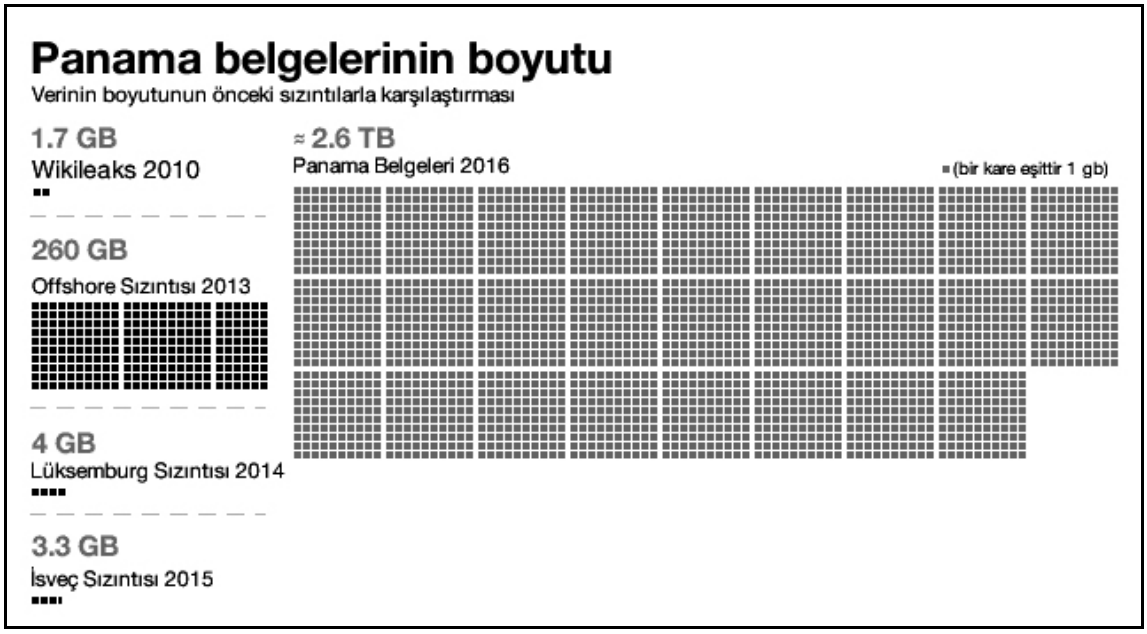
Mossack Fonseca; Panama ticaret siciline kayıtlı, fakat dünyanın farklı bölgelerinde bulunan 42 ülkede işlem yapan, yaklaşık 600 personeli bulunan ve offshore şirketlerine hukuki danışmanlık yapan uluslararası bir şirkettir. Şirket özellikle İsviçre, Kıbrıs ve Virgin Adaları gibi vergi cenneti olarak bilinen ülkelerde faaliyet göstermekte ve bu alanda hizmet veren en büyük dördüncü şirket olarak bilinmektedir. 1970'li yıllardan günümüze kadar tutulan 11,5 milyon doküman 2,6 TB'lık veri olarak sızdırılmıştır (İnt. Kyn. 34).

2014 yılının sonlarında Süddeutsche Zeitung gazetesinin yazarlarından Bastian Obermayer'e gelen "Merhaba, ben John Doe. Elimdeki verilerle ilgilenir misiniz?

Birkaç şartla bu verileri sizinle paylaşabilirim. Hayatım tehlikede. Sadece şifreli kanallar üzerinden konuşacağız. Asla buluşmayacağız. Belgelerden çıkarılacak haberlerin seçimine tamamen siz karar vereceksiniz." mesajı tarihin en büyük sızıntısının başlangıcı olmuştur (İnt. Kyn. 33).

John Doe (ABD'de, gerçek kimliği belirlenemeyen, ya da yasal gerekçelerle gizli tutulması gereken kişiler ve kimliği saptanamayan cesetler için kullanılan bir takma isimdir) isimli kullanıcıdan alınan mesaj sonrasında 2,6 TB'lık veri sızıntısı gerçekleştirilmiştir.

Panama Belgeleri'ni sızdıran John Doe takma isimli ifşacı Mayıs 2016 tarihinde "Devrim Dijitalleştirilecek" başlıklı bir açıklama yayınlayarak dokunulmazlık zırhı verilmesi şartıyla savcılara yardım edebileceğini bildirmiştir. Açıklamada kendisinin hiçbir istihbarat örgütü ya da devlet adına çalışmadığını, ifşa için motivasyonunun "gelir adaletsizliği" olduğunu ifade etmiştir (İnt. Kyn. 4).



Şekil 4.8 Panama Belgeleri'nin diğer sızıntılarya karşılaştırılması (İnt. Kyn. 33).

İnt. Kyn. 59'a göre 2.6 TB'lık 11.5 milyon adet belge incelenebilmesi ve sorgu yapılabilir hale getirilebilmesi için birtakım işlemlerden geçirilmesi gerekmiştir. Bu işlemlerde özellikle açık kaynak kodlu yazılımlar, isteğe göre düzenlenebilmesi sebebiyle tercih edilmiştir. Öncelikle farklı ülkelerde yerleşik olan gazetecilerin

birbirleriyle iletişim kurabilmeleri için Oxwall isimli açık kaynak kodlu bir sosyal ağ aracı kullanılmıştır.

Facebook benzeri bu sosyal ağda, son gelişmelerin takip edilebileceği bir haber akışı, forum yazılarının eklenebileceği bir forum alanı ve katılımcıların kendi aralarında sohbet edebilecekleri bir mesajlaşma bölümü de bulunmaktadır. Bu iletişim ortamı, her bir gazetecinin, bulduğu farklı bilgileri birleştirebilmesi ve daha büyük fotoğrafı görülebilmelerini sağlama açısından yararlı olmuştur. İletişim güvenliği için HTTPS protokolünü kullanan iki aşamalı bir doğrulama sistemi kullanılmıştır. Elde edilen bilgilerin birçoğunu e-postalar oluştururken, taranmış belgeler, PDF dosyaları gibi işlenmesi gereken çok fazla veri de sistemde yer almıştır.

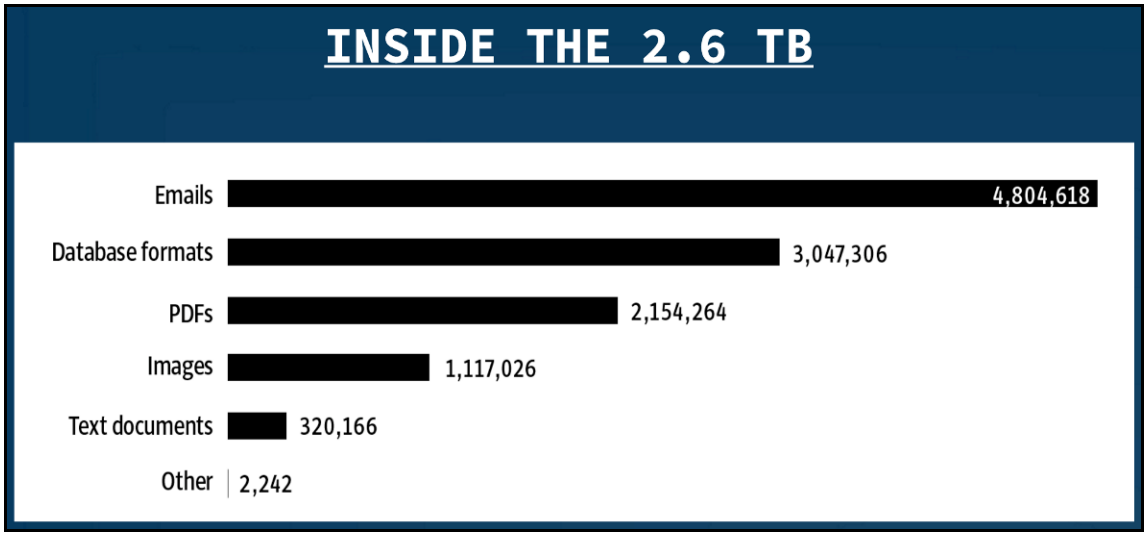
Bu belgelerin işlenebilmesi için yine açık kaynak kodlu Optik Karakter Tanıma (OCR) yazılımları olan Apache Tika ve Tesseract kullanılmıştır. Bu yazılımlar, paralel işlem yürütülebilmesi için bulut üzerindeki 30-40 civarında sunucu üzerinde konumlandırılmışlardır. Belgelerin tanınıp tanınmayacağını belirleyecek küçük bir uygulama da geliştirilmiştir. Bu uygulama belgeyi tanıyamadığında OCR yazılımına gönderirken, diğer belgeleri Apache Solr isimli belge arama platformuna aktarmaktadır.

Apache Solr temeline dayanan bir indeks oluşturularak, kütüphaneler için geliştirilmiş açık kaynak kodlu bir yazılım olan Project Blacklight arayüz olarak kullanılmıştır. Gelişmiş arama için birtakım iyileştirmeler yapılarak, yakınlık gibi daha ayrıntılı sorgulamalara olanak sağlanmıştır. Bu noktada açık kaynak kodun büyük faydaları olmuştur. 2.6 TB'lık veri içerisinde belgelerden başka Mossack Fonseca'nın dahili veri tabanı da bulunmaktadır.

Bu veri tabanı üzerinde yeniden çalışılarak Microsoft SQL üzerinde yeni bir veri tabanı oluşturulmuştur. 21 bölge ve 210 binden fazla şirketin ve bunların arkasındaki kişilerin nasıl ilişki içerisinde olduklarının tam olarak anlaşılabilmesi için birtakım görselleştirmelere ihtiyaç duyulmuştur. Bu grafikselleştirilmiş raporlama işi için Linkurious isimli yazılımdan yararlanılmıştır.

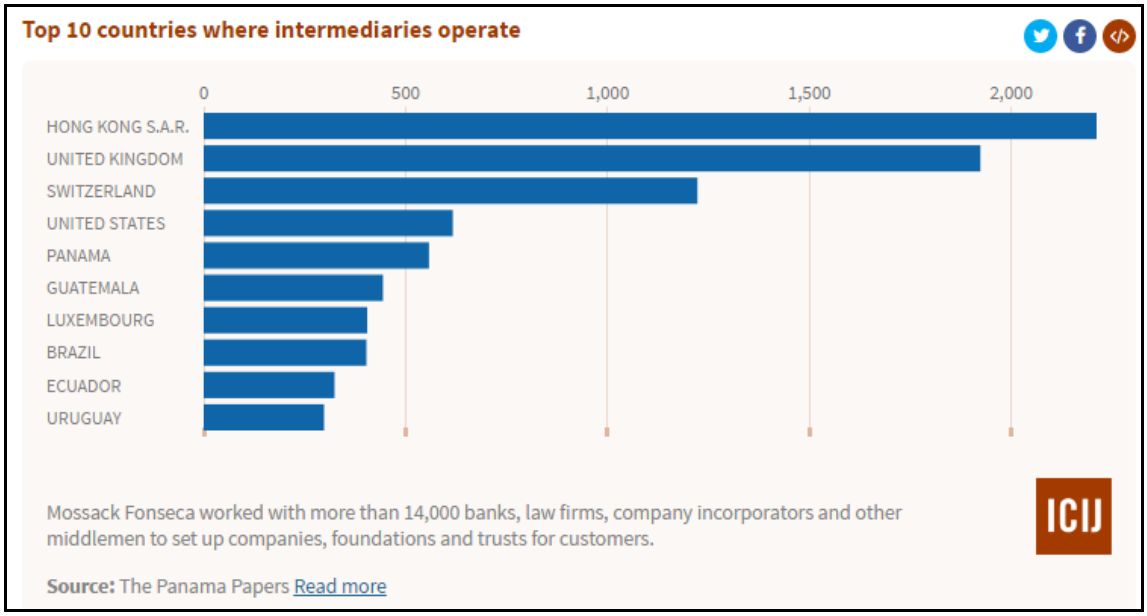
Bu yazılım için bir sunucuya lisans alınmış ve Neo4j isimli grafik veri tabanı ile birlikte çalıştırılmıştır. Linkurious üzerinde gazetecilerin giriş çıkış yapabileceği özel bir bölüm

de bulunmaktadır. Başlangıçta SQL üzerinde bulunan Panama Belgeleri veri tabanı yine açık kaynak kodlu bir yazılım olan Talend yardımıyla çok kolay bir şekilde Neo4j veri tabanına taşınmış ve Linkurious ile görsel raporlamalar alınması sağlanmıştır.



Şekil 4.9 Panama Belgeleri'ndeki verilerin türleri ve boyutları (İnt. Kyn. 59).

Gazeteci Bastian Obermayer, gizli belgeleri sızdıran kişiyi ya da kimliğini bilmediğini, kendisinin şifreli kanallar üzerinden iletişim kurduğunu, her iletişim kurduklarında doğru kişiyle bağlantı kurup kurmadıklarını anlayabilmek için önceden belirlenmiş soru-cevap ile başladıklarını belirtmiştir (İnt. Kyn. 33).



Şekil 4.10 Panama Belgeleri'ndeki aracıların faaliyet gösterdiği ilk 10 ülke (İnt. Kyn. 4).

Mossack Fonseca'nın 40 yıl boyunca gerçekleştirdiği işlemleri içeren belgelerde, aralarında eski ve halen görevde bulunan 12 ülke lideri, 143 politikacı, işadamları, spor dünyasından ünlü isimler ve yöneticiler, sinema yönetmenleri gibi birçok önemli görevdeki kişi ve kuruluşa ait vergi kaçakçılığı veya kara para aklama gibi kanunsuz işlemler ifşa edilmiştir.

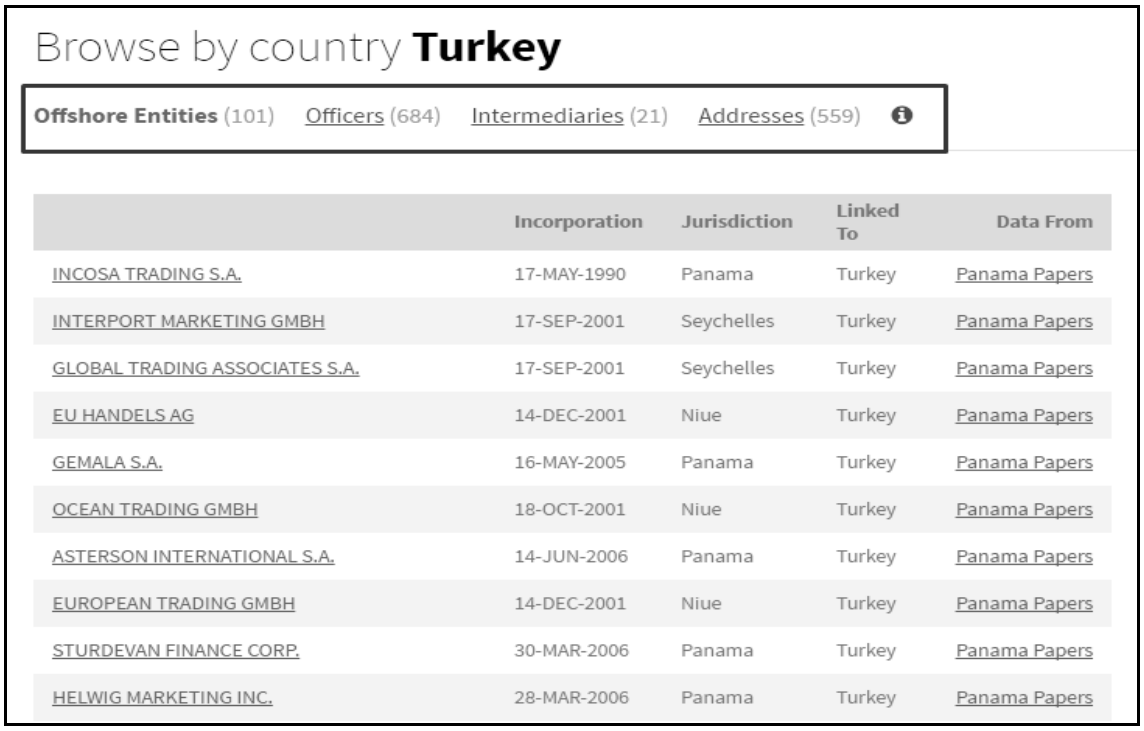
Şekil 4.11'de yer alan, güçlü oyuncular olarak da adlandırılan liderler arasından İzlanda Başbakanı Sigmundur Davíd Gunnlaugsson, belgelerin yayınlanmasından sonra istifa etmek zorunda kalmıştır. Rusya Devlet Başkanı Putin'in, yakın arkadaşına ait hesaplar üzerinden vergi kaçırdığı iddiaları üzerine Kremlin açıklama yapmak zorunda kalmıştır. Belgelerde Çin Devlet Başkanı Şi Cinping'in kayınbiraderinin isminin de geçmesi üzerine Çin'de Panama Belgeleri'yle ilgili haberler sansürlenmiştir (İnt. Kyn. 33).

Şekil 4.11 Panama Belgeleri'ndeki siyasi bağlantılar (İnt. Kyn. 4).

Panama Belgeleri'ni yayınlayan Uluslararası Araştırmacı Gazeteciler Konsorsiyumu'nu finansal olarak destekleyenler listesinde; George Soros, ABD Hazine Bakanlığı, Almanya ve İngiltere gibi ülkelerin bulunması, akıllara, sızıntının arkasında iki amacın olduğunu getirmektedir. Birincisi, büyük şirketlerin vergi kaçırması nedeniyle ismi geçen ülkelerde vergi gelirlerinin azalmasına neden olmasıdır. İkincisi ise küresel anlamda tek süper güç olan ABD'nin kendi menfaatlerine zarar veren ülkelere karşı giriştiği finansal bir savaş olarak değerlendirilmektedir (Kocaman 2016).

4.2.3.2 Panama Belgeleri'nde Türkiye

Mossack Fonseca'dan sızdırılan ve Panama Belgeleri olarak da bilinen offshore kayıtlarının Türkiye ile ilgili kısmı, kamuoyuna açıklanan ikinci bölümde yer almaktadır. Türkiye'den, aralarında ülkemizin en büyük şirketlerinin de bulunduğu toplamda 684 kişi, 101 şirket ve 21 aracı kuruluşun ismi yayınlanan sızıntılarda yer almaktadır (İnt. Kyn. 29). Açıklanan belgelerde Çalık Holding, Doğan Holding, Koç Holding ve Zorlu Holding gibi Türkiye'nin önde gelen büyük şirketlerin olması dikkatleri çekmektedir (İnt. Kyn. 6). Belgelerin yayınlandığı site üzerinden ülke seçilerek arama yapıldığında Şekil 4.2'de bir kısmı görülen bilgiler yer almaktadır.



Browse by country **Turkey**

Offshore Entities (101) Officers (684) Intermediaries (21) Addresses (559)

	Incorporation	Jurisdiction	Linked To	Data From
INCOSA TRADING S.A.	17-MAY-1990	Panama	Turkey	Panama Papers
INTERPORT MARKETING GMBH	17-SEP-2001	Seychelles	Turkey	Panama Papers
GLOBAL TRADING ASSOCIATES S.A.	17-SEP-2001	Seychelles	Turkey	Panama Papers
EU HANDELS AG	14-DEC-2001	Niue	Turkey	Panama Papers
GEMALA S.A.	16-MAY-2005	Panama	Turkey	Panama Papers
OCEAN TRADING GMBH	18-OCT-2001	Niue	Turkey	Panama Papers
ASTERSON INTERNATIONAL S.A.	14-JUN-2006	Panama	Turkey	Panama Papers
EUROPEAN TRADING GMBH	14-DEC-2001	Niue	Turkey	Panama Papers
STURDEVAN FINANCE CORP.	30-MAR-2006	Panama	Turkey	Panama Papers
HELWIG MARKETING INC.	28-MAR-2006	Panama	Turkey	Panama Papers

Şekil 4.12 Panama Belgeleri'nde yer alan Türkiye ile bağlantılı kişi ve kuruluşlar (İnt. Kyn. 28).

Kocaman (2016)'a göre ICIJ Başkanı Gerard Ryle, Türkiye'de yayınlanan bir televizyon programında 11.5 milyon belge arasında Türkiye'yi ilgilendiren belgelerin henüz hiç birine dokunulmadığını, bu yüzden ne çıkacağını bilmediğini söylemiştir. Belgelerin yayınlanmamasına gerekçe olarak, Türkiye'deki bir medya kuruluşu ile belgeleri değerlendirmek üzere irtibata geçtiklerini, ancak medya kuruluşunun kendileriyle çalışmayı reddettiğini belirtmiştir.

Ryle belgelerin açıklanıp açıklanmayacağı ile ilgili soruya; birlikte çalışabilecekleri Türk gazeteciler olmadan haber yapmak istemediklerini, çünkü kimin ve neyin önemli olup olmadığını Türk gazeteciler olmadan ortaya çıkarmanın aylar sürebileceğini öne sürerek yayınlanmayacağını söylemiştir (Kocaman 2016).

İnt. Kyn. 47'ye göre İngiltere, İrlanda, Yeni Zellanda, Panama ve Belize gibi offshore cennetlerinde bulunan 350 şirketten Türkiye'deki iki firmaya 10 aylık bir süreçte 6,2 milyar lira değerinde para transfer edilmiştir. Üçü Türk, birisi İran bankası aracılığı ile gerçekleştirilen para transferleriyle ilgili olarak Maliye Bakanlığı vergi incelemesi başlatmıştır. Türkiye'deki iki firmaya 6.2 milyar TL değerinde Euro ve Dolar gönderen tabela şirketlerinden birçoğunun, Panama Belgeleri'nde yer alan firmalar olması ilgiyle karşılanmıştır.

Söz konusu şirket bilgilerinin, Panama Belgeleri'nde yayınlanan belgeler ile örtüşmesi de dikkatleri çekmiştir. Maliye Bakanlığı bu şirketleri, vergi kaçırıp kaçırmadıklarının ortaya çıkarılması amacıyla incelemeye almıştır. Bu kadar yüksek bir meblağın hangi amaçlarla transfer edildiği ve herhangi bir suç unsuru taşıyıp taşımadığının ortaya çıkarılması amacıyla Mali Suçları Araştırma Komisyonu (MASAK) tarafından inceleme başlatılmıştır (İnt. Kyn. 47).

Söz konusu firmaların 6.2 milyar liralık para transferine aracılık ederek yüzde 1'lik bir komisyon almaları halinde 62 milyon TL kazanç elde edecekleri, bu rakam üzerinden yüzde 20 oranında vergi tahakkuk etmesi halinde 12.4 milyon TL'lik bir vergi kaybının oluştuğu hesaplanmıştır (İnt. Kyn. 47).

Lüksemburg, Malta ve Bahreyn gibi vergi cennetlerinde bulunan 11 Türk bankası, offshore hesaplarında 142 milyar civarındaki bir parayı yönetmektedir. Bu rakamlar

ülkemizin GSMH'sının yüzde 5'inden fazlasına karşılık gelmektedir. Türkiye'deki büyük firmalardan birçoğunun offshore şirketleri bulunmaktadır. Offshore cennetlerinde kurulmuş fakat Türkiye'de yabancı şirket olarak faaliyet gösteren on binlerce şirket bulunmaktadır (Kocaman 2016).

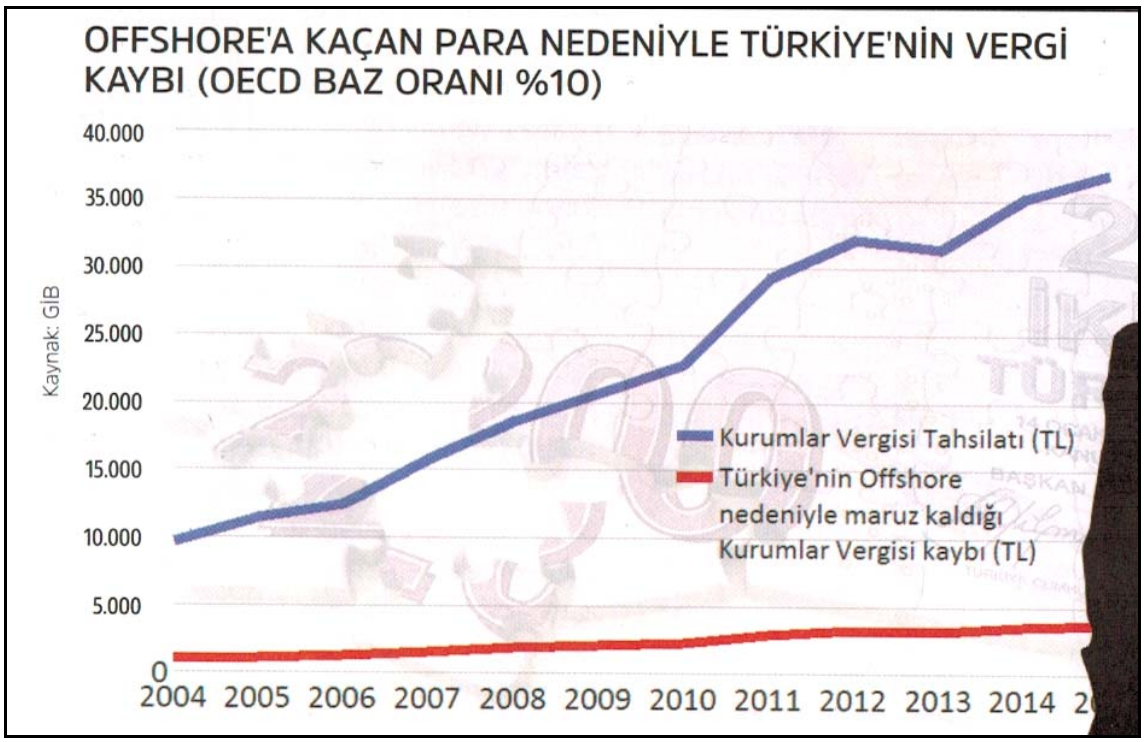
Kurumlar vergisini OECD ortalamasının altına, yüzde 20'ye indiren Türkiye; yerli yabancı sermayenin ülke ekonomisine girişini sağlarken, büyük şirketler de kârlarını üç ilâ beş kat arasında artırmışlardır. Ancak bu durumun aksine, büyük firmalardan elde edilen kurumlar vergisinin toplam vergi gelirleri içerisindeki payı son 10 yılda yüzde 1,6 oranında azalmıştır. İşçi ve memur maaşlarından kesilen gelir vergisinin payı ise yüzde 3,6 oranında artış göstermiştir.

Çizelge 4.2 Offshore merkezli ve Türkiye'de faaliyet gösteren şirket sayısı (Kocaman 2016).

Offshore Merkezi	*Şirket Sayısı*
İngiltere*	2.895
Hollanda*	2.564
ABD*	1.604
İsviçre	763
Lüksemburg	426
KKTC	408
BAE	383
İrlanda	351
İsrail*	335
Kanada*	320
İngiliz Virgin Adaları	176
Singapur	94
Hong Kong	72
Bahreyn	57
Malta	52
Panama	39
Cayman Adaları	32
İngiliz Jersey Adaları	32
Belize	22
Yeni Zelanda*	21
İzlanda	19
Marshal Adaları	16
Bahamalar	12
Bermuda	10
Cebeli Tarık	10
Diğer offshore ülkeleri	92
TOPLAM	*10.785*

OECD'nin yaptığı tespite göre Türkiye ve benzeri ülkelerde yüzde 4 ila yüzde 10 arasında kurumlar vergisi kaçağı ortaya çıkmaktadır. yüzde 10 rakamı baz alındığında, basit bir hesaplamayla toplam vergi kaybı 9 milyar TL'yi bulmaktadır. Bu miktar Yavuz Sultan Selim Köprüsü'nün maliyetinin üç katına denk gelmektedir.

Eski bakanlardan Ali Babacan tarafından 2013 yılında yapılan açıklamaya göre, yurt dışında tutulan Türk sermayesi 130 milyar dolar büyüklüğündedir. 50 milyar dolarlık kısmı ABD'nin vergi cennetlerinden Delaware eyaletindedir. Türkiye bu paraların ülkeye girişini sağlamak amacıyla iki kez "vergi barışı" düzenlemiştir. 2009'daki vergi barışında 48 milyar lira kayıt altına alınarak 1,9 milyar liralık vergi geliri elde edilmiştir (Kocaman 2016).



Şekil 4.13 Offshore hesapları nedeniyle Türkiye'nin vergi kaybı (Kocaman 2016).

4.3 Gizli Belge Yayıncılığında Kullanılan Yöntem ve Teknikler

Dünyayı sarsan gizli belge yayınlarına bakıldığında (Pentagon Belgeleri, WikiLeaks, Snowden ve Panama Belgeleri gibi) bu tür sızıntıların genellikle kurum içerisinde çalışanlar tarafından gerçekleştirildiği görülmektedir. Çalışanların gizli belgeleri ele geçirmelerinde farklı metotlar uygulansa da belgelerin yayınlanmasında kullanılan teknikler çoğu zaman birbirine benzer nitelikler taşımaktadır.

Gizli belge yayıncılığı, geçmiş yıllarda korkusuz gazeteciler ya da yayın kurumları aracılığıyla gerçekleştirilirken günümüzde sunmuş olduğu olağanüstü imkânlar sebebiyle "internet medyası" aracılığı ile yürütülmektedir.

Gizli belge yayıncılığında kullanılmak üzere ifşacı ile alıcı arasında güvenli iletişimi sağlamak üzere sızdırma platformları geliştirilmiştir. Bu platformlar erişim güvenliğini denetlerken platformdaki verilerin yetkisiz erişimlerden korunmasını da sağlamaktadır. Bunun yanında ifşacıya ve alıcısına kimlik bilgilerinin açığa çıkmaması için gerekli güvenlik tedbirleri sunulmakta, bu tedbirler dikkate alınmadan bağlanmak istendiğinde erişim engellenmektedir.

Platform, ifşacı ve alıcı arasındaki iletişimin anonim olmasını sağlayan şifreli güvenlik uygulamaları da sunmaktadır. Anonimleştirme uygulamalarında en çok tercih edilen sistem TOR ağıdır (Çalışkan 2016).

Günümüzün en popüler iki gizli belge yayıncısı WikiLeaks ve ICIJ (Panama Belgeleri'ni yayınlayan kuruluş); belge gönderimi için benzer metotları kullanmaktadırlar. Her iki kuruluş da belge sızıntılarını TOR ağı üzerindeki, resmi web sitelerinde yayınladıkları bir adres aracılığı ile kabul etmektedir. İfşacılar, TOR sisteminin güvenliğine ek olarak isterlerse bu kuruluşlara ait PGP anahtarları ile mesajları şifreleyerek gönderebilmektedirler.

ICIJ, WikiLeaks'ten farklı olarak SecureDrop sistemini de kullanmaktadır. Söz konusu sistem şöyle işlemektedir: İfşacı ICIJ'ın SecureDrop hizmetinin yüklü olduğu sunucuya bağlanır, sistem, kullanıcıdan hiçbir bilgi almadan, benzersiz bir kullanıcı hesabı oluşturur ve en az yedi kelimelik bir güvenlik anahtarı üretir. İfşacı, bilgileri sisteme yüklediğinde sistem bu belgeleri güvenli bir şekilde depolar.

Muhabir, ifşacının gönderdiği bilgileri bilgisayarına indirip gerekli incelemeleri yaptıktan sonra ihtiyaç duyarsa ifşacı ile ek bilgi/belge vs. için iletişim kurabilir, ancak bu noktada muhabir, ifşacının kimliğiyle ilgili olarak kullanıcı adından başka hiçbir bilgiye ulaşamaz. İfşacı istemediği sürece kendisine ait hiçbir bilgi muhabirler tarafından öğrenilemez. Bu yazılım bağımsız güvenlik uzmanları tarafından incelendiğinde herhangi bir kritik düzeyde güvenlik açığı tespit edilememiştir.

Kullanmak isteyen kuruluşlar için bu yazılım ücretsiz olarak dağıtılmaktadır (İnt. Kyn. 48).

ICIJ, iletişim amacıyla elektronik forma ilâve olarak bir posta adresi de eklemiş durumdayken WikiLeaks web tabanlı bir chat linkini yayınlamıştır (erişimin yapıldığı tarih itibariyle chat sayfasına ulaşılamamıştır). Fakat WikiLeaks'in TOR üzerinden kurulacak iletişimi tavsiye ettiği görülmektedir (İnt. Kyn. 20; İnt. Kyn. 29).

Gizli belgeler; SecureDrop, TOR, Multihop VPN yazılımları sayesinde ifşacının kimliği ortaya çıkmadan ifşa noktalarına ulaştırılabilmekte ve bu belgeler ifşa noktasında kamunun erişimine açılmaktadır. Ancak gizli belgeler, WikiLeaks ya da ICIJ gibi profesyonel anlamda kamu bilgilendirmesi yapan kuruluşlara gönderildiğinde, birtakım incelemeler, tasnifler ve ifşadan dolayı zarar görebilecek görevlilerin kimliğinin gizlenmesi gibi işlemlerden geçmektedir (İnt. Kyn. 51).

Standart elektronik iletişim yazımlarıyla yayınlanan bu bilgilere erişim sağlanabilirken, bazen sızıntılardan hoşnut olmayan hükümetler ifşanın yapıldığı sitelere sansür uygulayabilmektedir. Ancak bu gibi durumlar için WikiLeaks, ayna siteler oluşturmak ve P2P ağları kullanmak gibi çözümler üreterek sansüre rağmen bilgileri kamuoyunun erişimine açık tutabilmiştir (Munro 2015).

Gizli belge yayıncılığı, değişen teknolojiyle birlikte sürekli olarak gelişmektedir. Ülkemizde ve dünyada gerçekleştirilen bilgi ifşaları incelendiğinde, gizli belge yayıncılığında kullanılan teknolojilerin benzerlik gösterdiği anlaşılmaktadır. Gizli belge yayıncılığında kullanılan teknolojilerden en sık kullanılanları şöyle sıralanabilir:

4.3.1 Soğan Projesi (TOR)

Soğan Projesi (The Onion Router) (TOR), anonim olarak internette gezinmeyi sağlayan, açık kaynak kodlu ve ücretsiz hizmet olarak sunulan bir tür VPN uygulamasıdır. Bu uygulamadan yararlanan kullanıcılar en az üç farklı sunucu üzerinden geçerek internete erişmektedir. Bu durum, kullanıcıların takip edilme riskini azaltan en büyük etkendir. (Sağıroğlu vd. 2015)

TOR projesi 1995 yılında Amerikan deniz araştırmaları laboratuvar çalışanları tarafından ABD gizli servislerinin iletişim hizmetlerinde gizliliği sağlamak amacıyla

başlatılmıştır (İnt. Kyn. 23). Günümüzde ise gönüllülerin sunucularına veya kişisel bilgisayarlarına yükleyerek oluşturduğu bağımsız bir yapı olarak kullanıcılarına anonimlik sağlamaktadır. (Karaarslan vd. 2014)

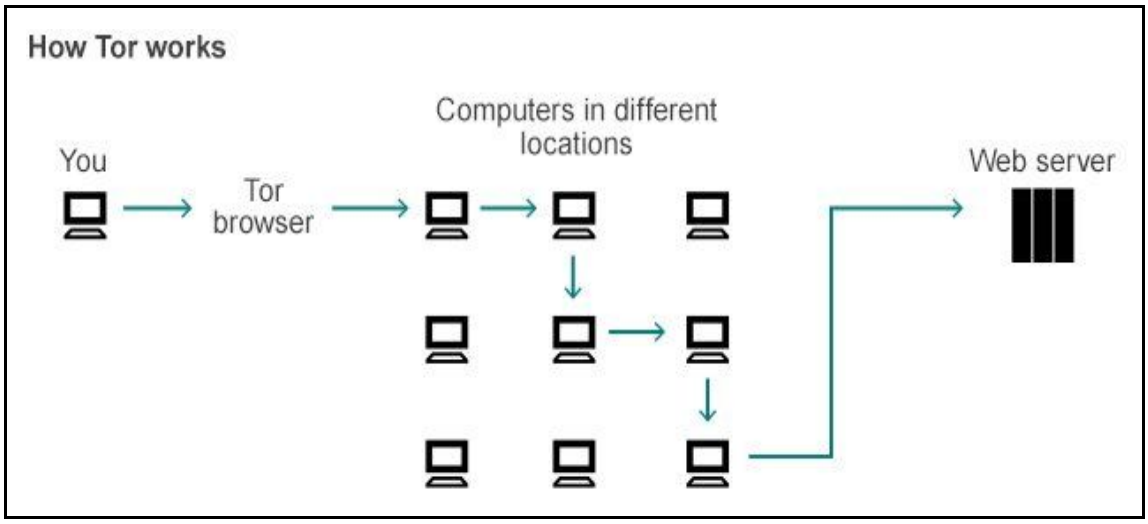
TOR sisteminin nasıl çalıştığına gelince... Kullanıcı, TOR tarayıcı aracılığıyla bir web sitesine bağlanmak istediğinde TOR ağına giriş, TOR ağından çıkış ve aradaki yönlendiriciler rastgele (random) seçilmektedir. TOR ağında kullanılan yönlendiriciler kendilerine gelen ve giden verileri şifreleyerek göndermektedir.

Söz konusu veriler şifreli olarak rastgele seçilen farklı bir yönlendiriciye iletilmektedir. Verileri alan yönlendirici de aynı protokolleri uygulayarak yine farklı bir yönlendiriciye teslim etmekte, bu sayede veriler farklı yönlendiricilerden geçtikten sonra erişilmek istenen asıl sunucuya ulaşmaktadır (Karaarslan vd. 2014).

TOR ile özel bir ağ yolu oluşturmak için kullanıcının yazılımı veya istemcisi, ağdaki yönlendiriciler vasıtasıyla art arda şifreli yönlendirici devresi oluşturmaktadır. Devre her defasında bir sıçrama genişletilmekte ve yol boyunca her yönlendirici yalnızca hangi yönlendiriciye veri teslim ettiğini ve hangi veri paketini verdiğini bilmektedir. Yönlendiriciler veri paketinin tam yolunu hiçbir zaman bilmemektedir.

İstemci, izlenmemek için devre boyunca her bir atlama için ayrı bir şifreleme seti oluşturmaktadır. Bir devre kurulduktan sonra, birçok türde veri değiş-tokuş edilebilmektedir. Sunucular, devrede birden fazla atlamayı görmediğinden, ne bir izleyici ne de izlemek isteyen yönlendirici, kaynak ve hedef arasındaki bağlantıları analiz edememektedir (Hsu and Marinucci 2013).

TOR ağı, basit ancak veri izlerinin takip ve analiz edilmesini engelleyecek bir yapıda oluşmaktadır. TOR; doğrudan doğruya tek noktadan sunucuya erişmemektedir. Bu durum, takip edilmek istemeyen bir kişinin yaptığı gibi, ara sokaklardan geçen, kıvrımlı, takip edilmesi zor bir yol izlemeye benzemektedir.



Şekil 4.14 TOR ağı çalışma şeması. (İnt. Kyn. 16)

Bunun yanında, periyodik olarak izler silinmektedir. Veriler hem şifreli, hem rastgele, hem de farklı yönlendiriciler üzerinden gelip gittiği için kullanıcıyı izlemek isteyen gözlemci, verilerin nereden gelip nereye gittiğini takip edememektedir.

4.3.1.1 TOR Sisteminin Hedefleri

TOR sistemi kullanıcılarının gizliliğini hedeflemektedir. Ancak bunu gerçekleştirmek için ağa bağlı çok sayıda yönlendirici bulunması gerekmektedir. Ağa bağlanan yönlendirici sayısını artırabilmek için kurulabilirlik, kullanabilirlik, basitlik gibi özellikler hedeflenerek geliştirmeler yapılmıştır.

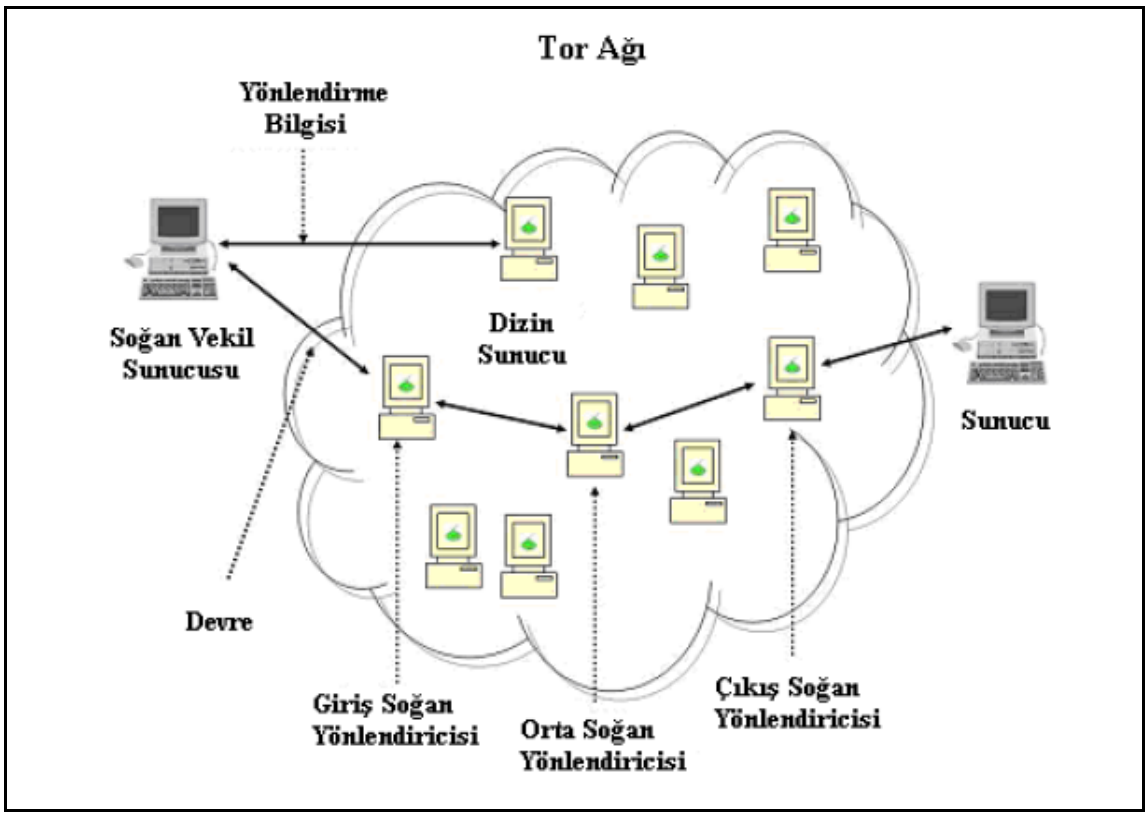
TOR'un yapısında ne kadar fazla yönlendirici olursa o kadar iyi anonimlik sağlanacağından, kullanım kolaylığı ön plana alınarak basit ara yüzler üretilmiştir. TOR kullanımı artırmak için Windows, Linux, MacOS X, BSD-Style, Unix, Solaris gibi işletim sistemleriyle de uyumlu uygulamalar geliştirilmiştir. TOR yine kullanımı artırabilmek için veri trafiğinde yaşanabilecek gecikmeleri azaltmayı da amaçlamıştır (Yüksel 2010).

4.3.1.2 TOR Sisteminin Bileşenleri

TOR ağı; kullanıcılar, yönlendiriciler, vekil sunucuları, köprüler ve dizin sunucuları gibi bileşenlerden oluşmaktadır. TOR'un gönüllüler tarafından desteklenen bir sistem olması nedeniyle isteyen kullanıcılar istediklerinde bir yönlendirici çalıştırabilmektedir.

Yönlendirici çalıştırmak isteyen kullanıcıları teşvik edici bazı özellikler de kazandırılmıştır.

Örneğin kullanıcı isterse kendisine yönlendiricinin bant genişliğini kısıtlama ve çıkış politikalarını yapılandırabilme yetkileri verilirken uygulamaya dinamik IP (İnternet Protokolü) ile çalışabilme özelliği de katılmıştır (İnt. Kyn. 14).



Şekil 4.15 TOR bileşenleri (İnt. Kyn. 16).

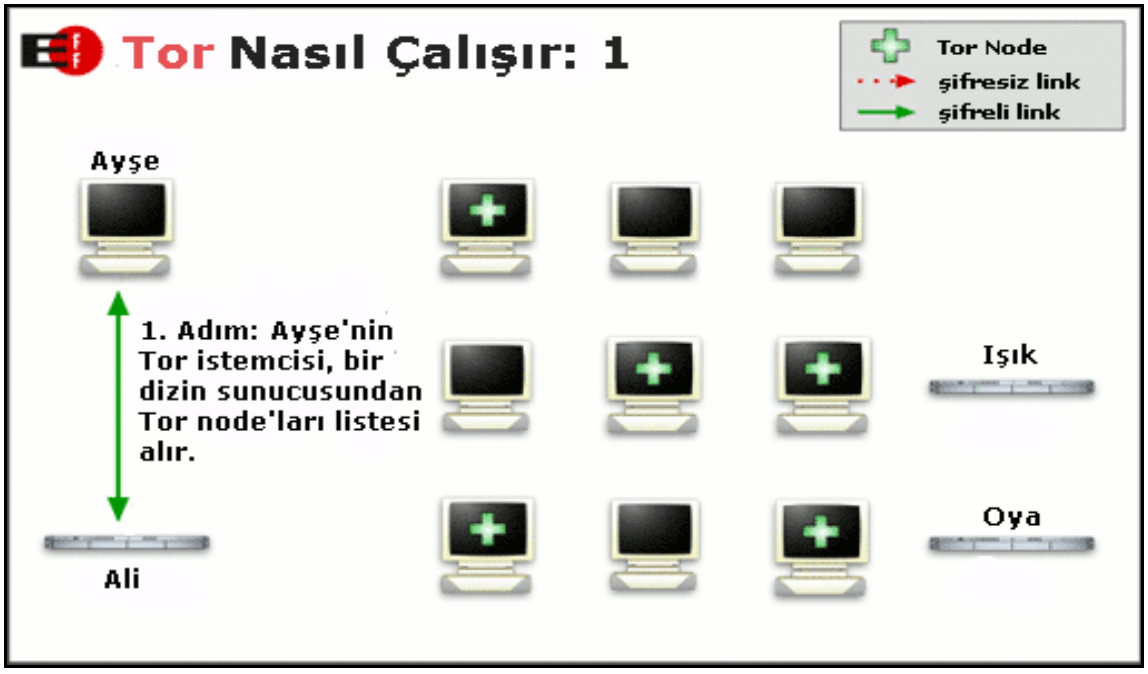
TOR istemcilerinin ve yönlendiricilerinin yapılandırılması amacıyla kullanılan "torrc" isimli bir dosya bulunmaktadır. Bu dosya sayesinde istenilen düzenlemeler kolaylıkla yapılabilmektedir. Kullanıcıların tercihine bırakılan düzenlemeler TOR Project resmi sitesindeki el kılavuzu sayfasında bulunmaktadır (İnt. Kyn. 16).

Kullanıcı şayet istemci değil, yönlendirici olmak isterse bilgisayarında TOR yönlendirici portu açması gerekmektedir. Özellikle ülkemizde DSL yönlendiriciler oldukça yoğun kullanılmaktadır. Bu sebeple TOR yönlendiricisi çalıştırabilmek için mutlaka NAT (Network Address Translator) sunucusu üzerinden de gerekli yönlendirmeler yapılması gerekmektedir (M. İ. Yüksel, 2010).

4.3.1.3 TOR Çalışma Sistemi

TOR, kullanıcıların anonimliğini sağlamak üzere geliştirilmiş bir sistem olmasına rağmen aslında doğrudan kullanıcıyı gizlemeye çalışmaz, TOR'un asıl amacı kullanıcılar ile hedef arasındaki bağlantıyı gizlemektir. Bunun için veri paketleri, Anonymizer vb. uygulamalarda olduğu gibi tek bir nokta üzerinden bağlantı kurmaz. TOR ağına kayıtlı yönlendiriciler arasından rastgele seçilen birkaçı üzerinden bağlantı gerçekleşir. Bu durumda herhangi bir noktada bulunan herhangi bir gözlemci, veri paketlerinin nereden gelip nereye gittiğini tespit edememektedir (Yüksel, 2010)

Şekil 4.15'de görüldüğü üzere TOR ağını kullanarak anonim olmak isteyen kullanıcı (Ayşe), istemci aracılığıyla dizin sunucularından, TOR ağında o anda aktif bulunan yönlendiricilerin bir listesini alır. Alınan liste istemci bilgisayarda "cached-consensus" isimli bir dosyada tutulmaktadır.



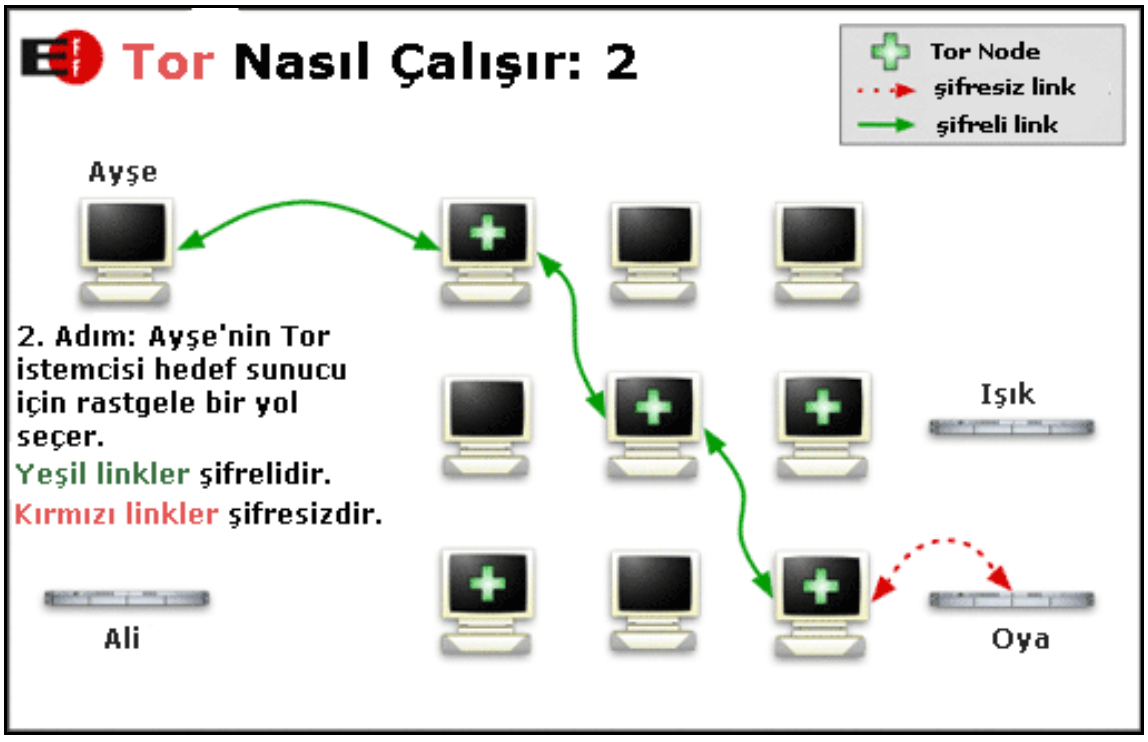
Şekil 4.16 Dizin sunucusundan yönlendirici listesi çekilmesi. (İnt. Kyn. 16)

Ayşe, Ali isimli dizin sunucusundan almış olduğu listeyi kullanarak varsayılan üç adet rastgele yönlendiriciyi seçer ve seçilenler üzerinde bir devre kurar. Devre her bir zamanda bir yönlendirici genişleyerek tamamlanır. Devrede bulunan yönlendiriciler veriyi aldığı ve verdiği yönlendirici dışındaki devreyi oluşturan diğer hiçbir

yönlendiriciyi bilmez, bu sayede verinin sunucuya ulaşırken kullanmış olduğu yol tam olarak bilinemez.

İstemciler ilk olarak; dizin sunucusu, devrede bulunan yönlendiriciler ve düğümler arasında şifreleme anahtarları oluşturur. Burada tek bir şifresiz nokta bulunur, bu da son düğümde oluşmaktadır. Yani Ayşe'nin göndermiş olduğu veriler Oya isimli sunucuya giderken sadece son düğüm ile Oya isimli sunucu arasında şifrelenmeden gönderilmektedir (Yüksel 2010).

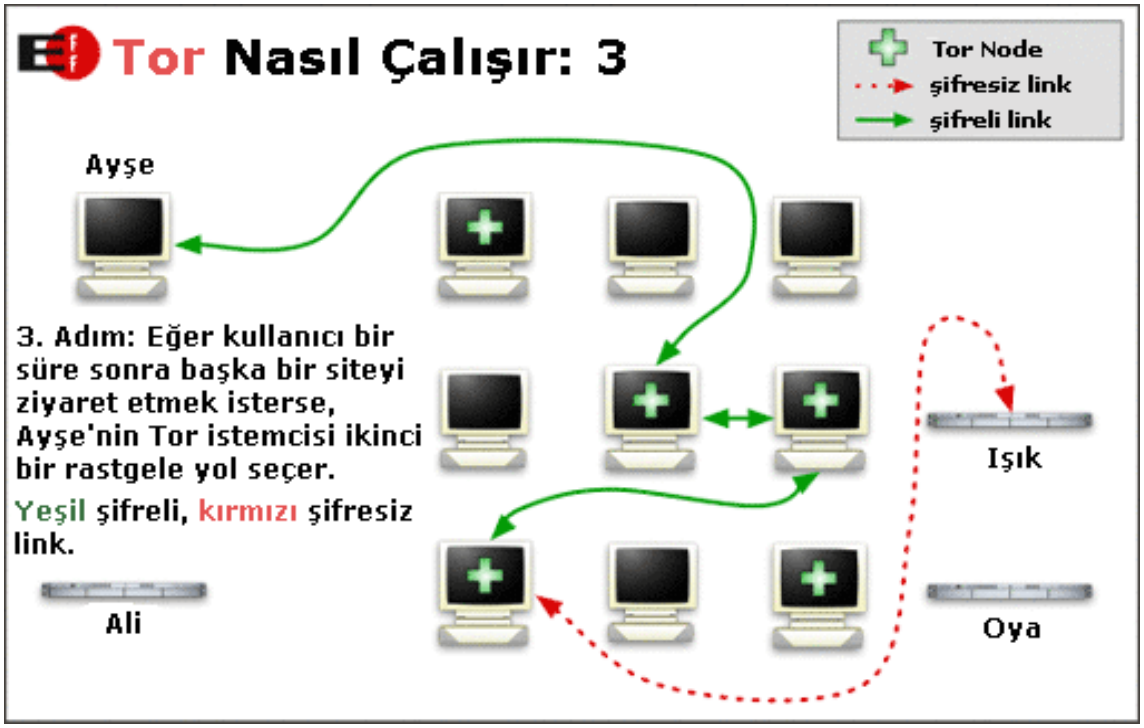
Bu devredeki son yönlendirici ExitNode olarak isimlendirilmektedir. ExitNode olan yönlendirici kendisi üzerinden geçen veri trafiğini okuyabilir, bu nedenle bu noktada dinleme (eaves dropping) yapılabilmektedir. Bu sebeple tüm bağlantılarda uçtan uca şifreleme kullanılması güvenliği sağlayabilecektir.



Şekil 4.17 Devre kurulumu (İnt. Kyn. 16).

İstemcinin (Ayşe) rastgele seçmiş olduğu yönlendiriciler üzerinden kurulan bu devre üzerinde farklı türlere ve uygulamalara ait veriler taşınabilmektedir. İstemci başka bir sunucu ile iletişim kurmak istediğinde yeni bir devre kurulmaktadır.

Bunun dışında anonimliğin artırılması için belirli aralıklarla (varsayılan 10 dakika) yeni devreler kurulur ve iletişim artık bu yeni devreler üzerinden sağlanır. Kullanıcı kurulmuş devre üzerinden bir sunucuya bağlanıp on dakika dolduğunda yeni bir devre kurularak iletişim bu yeni devre üzerinden sürdürülür. Bu şekilde bir önceki devre ile yeni kurulan devre arasında ilişki kurulması engellenmiş olur.



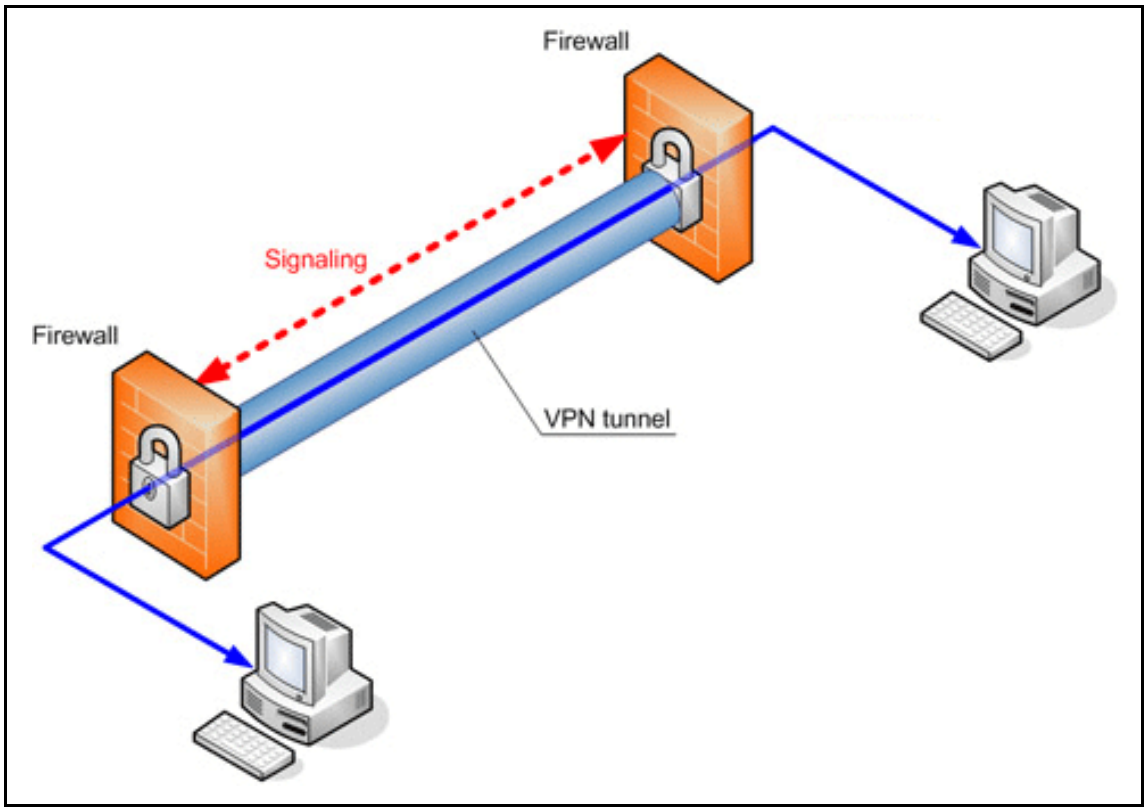
Şekil 4.18 Farklı bir hedefe yeni bir devre üzerinden bağlantı kurulması (İnt. Kyn. 16).

4.3.2 Sanal Özel Ağlar

Sanal Özel Ağlar (VPN); herkesin erişimine açık durumda bulunan internet aracılığıyla, özel bir ağ oluşturularak bağlanılan ve güvenli veri transferi gerçekleştirmeye yarayan bir ağ bağlantı çeşididir (Aydoğdu 2014). VPN teknolojisiyle farklı ağlara uzaktan erişim sağlanabilmektedir. VPN aracılığıyla farklı bir ağa bağlanan cihazlar, bu ağa sanal bir ağ uzantısı oluşturarak bağlanmakta, bu yüzden bağlanılan ağa sanki fiziksel olarak bağlıymış gibi veri alışverişinde bulunabilmektedir.

VPN dağınık yapıdaki özel iletişim ağlarında bulunan bilgilere, kamuya açık bir ağ olan internet aracılığı ile bağlandığı sırada iletimdeki verilerin üçüncü kişiler tarafından ele geçirilmesinin önlenmesi gerekmektedir. VPN teknolojisi veri iletişimini basit, ekonomik ve güvenilir biçimde sağlayan bir tünelleme teknolojisini kullanmaktadır.

VPN teknolojisinde iletişim maliyetlerinin düşürülmesi amacıyla kamuya açık internet ağı kullanılmaktadır. Bu iletişim omurgası kamuya açık olmasına rağmen veri iletişimi bir noktadan diğer noktaya kadar özel bir tünel kullanılarak şifrelenmektedir. Bu tünelden çıkış noktası, sadece karşı noktada bulunan güvenli yönlendiriciler veya ağ güvenlik sunucularıdır (firewall server).



Şekil 4.19 Sanal özel ağ çalışma esası (İnt. Kyn. 37).

VPN teknolojisinin dört farklı tipi bulunmaktadır (Demir 2010). Bunlar;

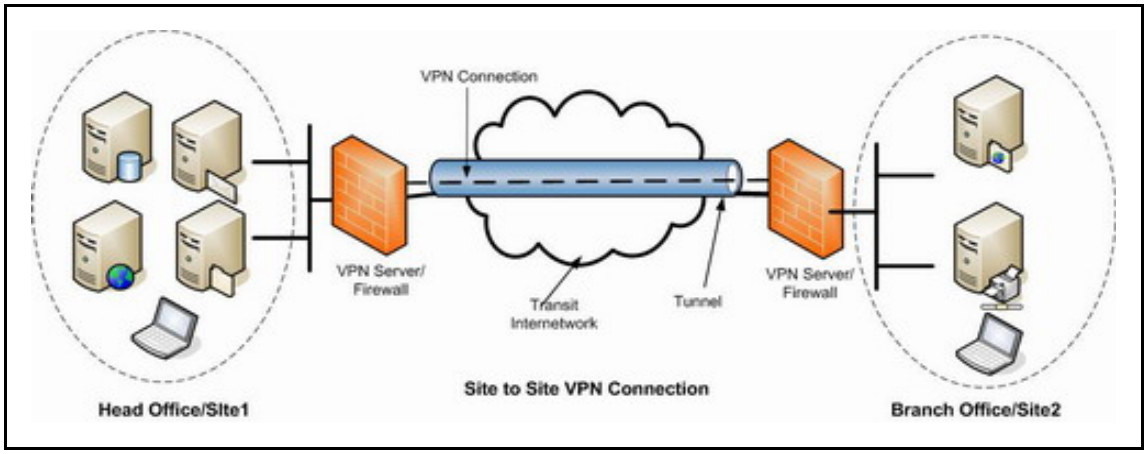
- Noktadan Noktaya VPN (Site to Site VPN)
- Uzak Erişim VPN (Remote Access VPN)
- Güvenlik Duvarı VPN (Firewall VPN)
- Kullanıcıdan Kullanıcıya VPN (User to User VPN)

VPN teknolojisi, verinin şifrelenmesi ve sarmalanması (encapsulation) ilkesiyle çalışmaktadır. VPN tipleri de bu işlemlerin uygulandığı noktaya göre temelde ikiye ayrılmaktadır. Bu temeller taşıma ve tünel modu olarak adlandırılmaktadır. Taşıma modu iki cihaz arasında kaynak ve hedef cihazlarına gerçek IP adresleri ile kurulmaktadır. Bu durum gizliliğe engel teşkil etmektedir.

İnternet üzerinden geçen veri paketleri dinlenerek kaynak ve hedef cihazların IP adresleri tespit edilebilmektedir. Tünel modu, taşıma modunda olduğu gibi cihazdan cihaza değil, ağdan ağa gerçekleştirilmelidir (Demir 2010). Veriler ve üstbilgi kapsüllenip çapraz geçişlere izin veren bilgiler içerecek şekilde oluşturulmaktadır. Veri paketlerinde bulunan veri başlıklarının önüne yeni başlıklar eklenerek ağda gerçekleştirilecek dinlemelere karşı gizlilik sağlanmaktadır (Aydoğdu 2014).

4.3.2.1 Noktadan Noktaya VPN

Noktadan Noktaya VPN, farklı bir lokasyonda bulunan ağ kullanıcılarının, merkez lokasyonda bulunan veri kaynaklarına erişimini sağlamak üzere iki nokta arasında sanal özel bir ağ kurulması olarak tanımlanmaktadır. VPN sunucusu bağlı olduğu ağa erişim imkânı verirken, istekleri karşılayan diğer VPN sunucusu VPN istemcisinin kimlik doğrulamasını yapar, böylece karşılıklı doğrulama sağlanmış olur (Aydoğdu 2014).



Şekil 4.20 Noktadan noktaya VPN (İnt. Kyn. 37).

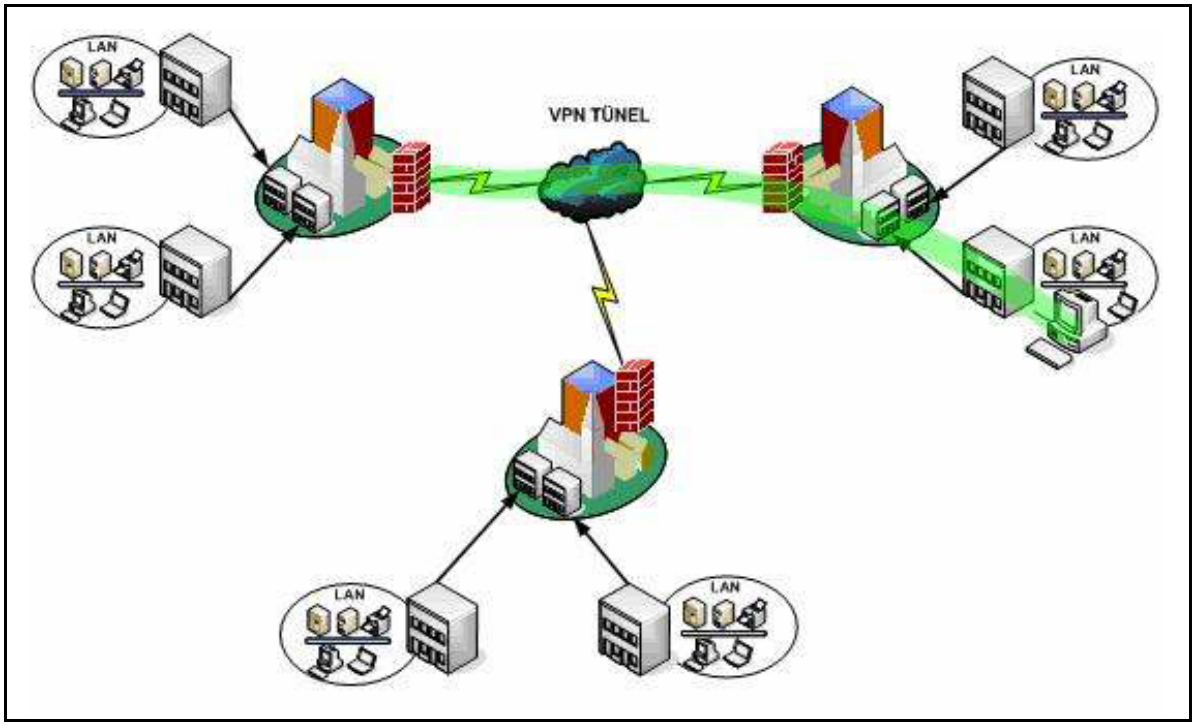
Aydoğdu (2014)'ya göre VPN'lerin kullanım amacına göre üç farklı tür bulunmaktadır. Bireysel kullanımlar için Access VPN, şirketler, üniversiteler, kurum ve kuruluşlar için ise Intranet VPN ve Extranet VPN'ler kullanılmaktadır. VPN'lerin kullanım amaçları şöyle belirtilebilir:

- Ofis dışında bulunulan zamanlarda ofis ağına bağlanarak projelere ve kişisel dokümanlara erişebilmek.

- Farklı lokasyonlarda bulunan bir şirketin ya da kurumun, şubeleri arasındaki veri iletişimini yüksek güvenlik protokolleri kullanarak sanki fiziksel olarak aynı ağdaymış gibi gerçekleştirmesine imkân sağlamak.
- Güvenlik protokollerine bağlı olarak bağlanılan ağ üzerindeki veri kaynaklarına erişebilmek.

4.3.2.2 Uzak Erişim VPN

Uzak Erişim VPN, çeşitli sebeplerle ofis dışında bulunan kullanıcıların, bulundukları noktadan ofis ağında bulunan kaynaklara erişme imkânı sağlamaktadır. VPN, istemciyle sunucu arasında doğrudan doğruya, yani noktadan noktaya bağlanmaktadır. Uzak Erişim VPN bağlantıları diğer türlere göre daha düşük bant genişliğine sahip kullanıcılar için tercih edilmektedir. Uzak erişim VPN teknolojisinde Tünel Modu kullanılmaktadır (Demir 2010).



Şekil 4.21 Uzak Erişim VPN (Demir 2010).

4.3.2.3 Güvenlik Duvarı VPN

Güvenlik duvarı VPN'leri, temel olarak L2L (Lan to Lan) ve uzak erişim VPN'lerin özelliklerine güvenlik ve firewall fonksiyonlarının eklenmiş hali olarak tanımlanmaktadır. Bu VPN'ler genelde, cihazın bağlı olduğu kurumun güvenlik

politikalarının güvenlik ve firewall fonksiyonlarına ihtiyaç duyması halinde kullanılmaktadır. Bu fonksiyonlar;

- Korumalı (stateful) filtreleme
- Uygulama katmanında filtreleme
- Adres transfer politikaları olarak açıklanabilmektedir (Demir 2010).

4.3.2.4 Kullanıcıdan Kullanıcıya VPN

Her iki kullanıcıdaki cihazlar güvenlik duvarları, SYSLOG sunucuları, TFTP (Kolay Dosya Transfer Protokolü) sunucu ve yönlendiriciye **telnet** ya da **putty** gibi yazılımlarla bağlanan kullanıcılar için geliştirilmiştir. Bu VPN teknolojisinde Taşıma Modu kullanılmaktadır (Demir 2010).

4.3.3 Çok İyi Mahremiyet (PGP)

Phill Zimmermann tarafından geliştirilen Çok İyi Mahremiyet (Pretty Good Privacy) (PGP) sahip olduğu kripto algoritmalarının güçlü olmasıyla bilinen güvenli bir e-posta yazılımıdır. Ticari kullanımlar haricinde ücretsiz olarak kullanıma sunulmuştur (Levi 2004).

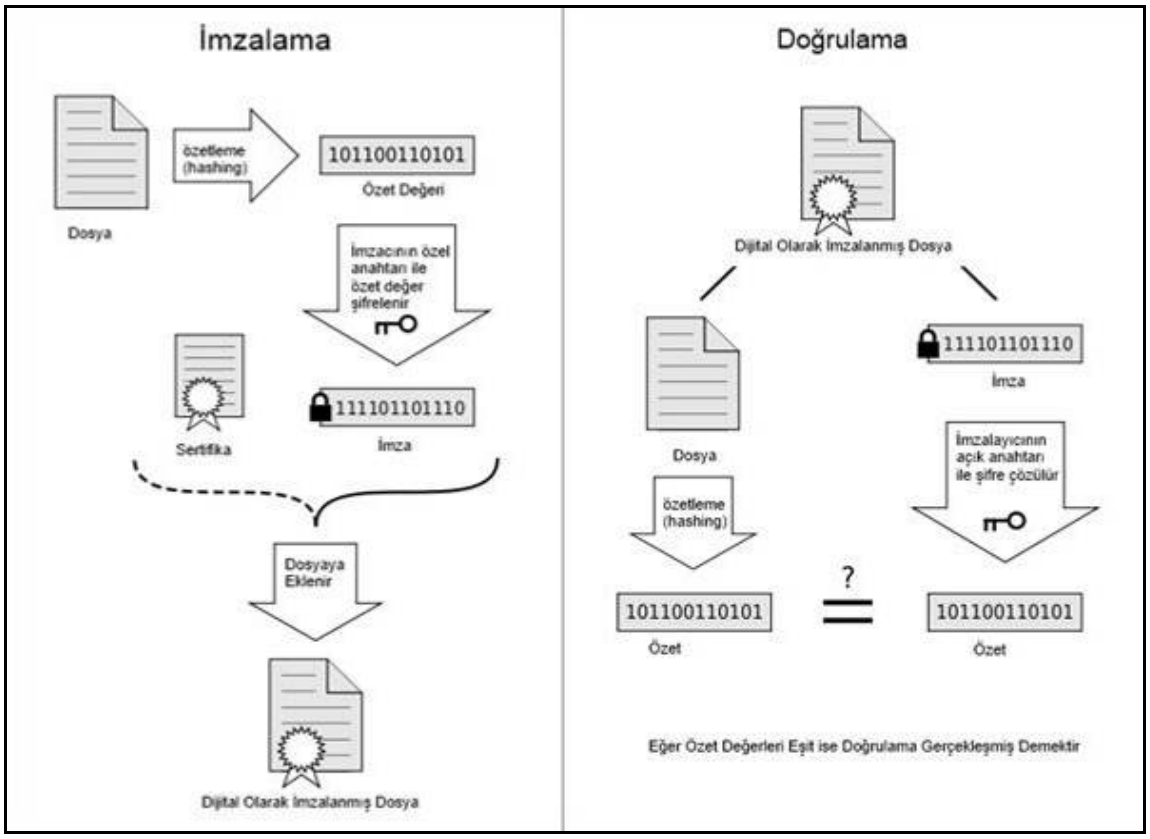
PGP, veri iletişiminde kullanılan kimlik doğrulama ve gizliliği sağlayan şifreleme ve şifreyi çözme yöntemi olarak tanımlanmaktadır (İnt. Kyn. 25). PGP genelde iletişim güvenliğini artırmak amacıyla dosyaları imzalama veya şifreleme, sabit disk ve dizin şifreleme, metin ve e-posta şifrelemek amacıyla kullanılmaktadır (Poşul ve Aksoy 2013). PGP'nin başarılı olmasında iki önemli etken bulunmaktadır. İlki, ücretsiz dağıtılması, diğeri ise şifreleme tekniğinin güçlü algoritmalar içermesidir.

Kullanıcı dostu bir uygulama olmamasına rağmen PGP, bu iki etken sayesinde önemli bir kullanıcı sayısına ulaşabilmiştir. Bu sistemin bir başka özelliği, isteyen kullanıcıların kendilerine ait bir güven mekanizması kurabilmeleridir. Fakat böyle bir çalışma için kullanıcının şifre algoritmaları ve güvenlik konularında az-çok bilgi sahibi olması gerekmektedir (Levi ve Özcan 2002).

PGP'nin çalışma mantığı temelde şu yönteme dayanmaktadır: Mesajı gönderen, mesajı alacak kişinin açık anahtarı ile yazdığı mesajı şifreleyerek karşı tarafa gönderir. Bu esnada mesaj üçüncü kişilerin eline geçse bile şifreli olduğundan mesaj içeriğinde neler

olduğu anlaşılamamaktadır. Mesaj alıcıya ulaştığında, mesaj sahibi sadece kendisinde bulunan özel anahtarla şifreli mesajı çözerek mesajı doğru bir şekilde okuyabilmektedir.

PGP, 512 bit ile 4096 bit arasında değişen RSA ve DSA anahtar boyutu için seçenekler sunmaktadır. Anahtar ne kadar büyük olursa, şifrelemenin RSA / DSA bölümü de o kadar güvenli hale getirilmektedir. Anahtar boyutunun, programın çalışma süresinde büyük bir değişiklik oluşturduğu tek yer, anahtar üretimi aşamasında olmaktadır. 1024 bitlik bir anahtar, 384 bitlik bir anahtara göre 8 kat daha uzun sürede üretilebilmektedir. Bu işlem, başka bir anahtar çifti oluşturmak istenmediği sürece tekrarlanmasına gerek olmayan bir kerelik bir işlemdir (İnt. Kyn. 9).



Şekil 4.22 PGP çalışma mantığı. (İnt. Kyn. 38)

4.3.4 Güvenli Soket Katmanı (SSL)

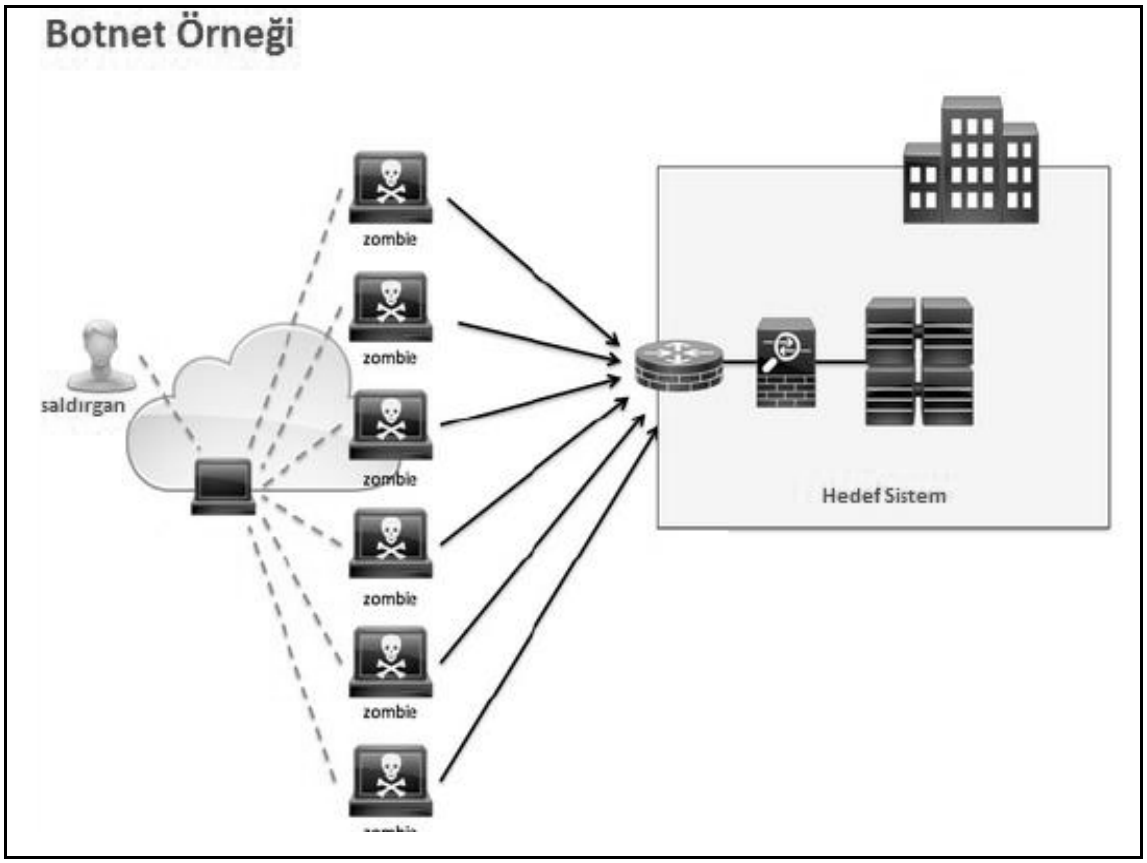
Güvenli soket katmanı (SSL) Netscape firması tarafından 1994 yılında geliştirilmiştir. İlk olarak Transport Layer Security (TLS) olarak bilinen fakat daha sonra Güvenli Soket Katmanı anlamına gelen ve kısaca SSL adıyla anılan güvenli veri iletişimi sağlayan bir protokoldür. 1995 yılında SSL 2.0 ve 1996 yılında günümüzde de kullanılmaya devam

eden SSL 3.0 sürümleri piyasaya sürülmüştür. 1999 yılında IETF tarafından SSL 3.0'ı temel alan TLS 1.0, 2006'da TLS 1.1, 2008'de ise TLS 1.2 yayınlanmıştır.

2015 yılından bu yana geliştirilmeye devam eden TLS 1.3 henüz yayınlanmamıştır. İlk zamanlarda sadece HTTP trafiğini şifrelemek amacıyla geliştirilmiş olmasına rağmen bugün TCP protokolünü kullanan tüm trafiği şifrelemek amacıyla da kullanılmaktadır (Yüksel 2007).

4.3.5 Dağıtık Hizmet Engelleme (DDoS)

Dağıtık hizmet engelleme saldırısı olarak bilinen, Distributed Denial of Service Attack'ın kısaltılmışı olan DDoS; özellikle web sunucularının yayınlarının engellenmesi amacıyla hizmet sunamaz hale gelinceye kadar tüm bant genişliğinin tüketilmesi esasına dayanan bir saldırı türüdür. DDoS'ta amaç bilgi hırsızlığı ya da sızma girişimi yapmak değil, hizmeti kullanılamaz hale getirmektir (Koçaslan 2015).



Şekil 4.23 DDoS saldırı için botnet ağı örneği (Koçaslan 2015).

DDoS saldırıları genelde iki tip uygulanmaktadır:

- Bant genişliğini tüketmeyi amaçlayan DDoS saldırıları
- Sistem kaynaklarını tüketmeyi amaçlayan DDoS saldırıları

Saldırganlar birinci yöntemde hedefteki ağı gereksiz fakat normal veri paketleriyle doldururlar, hedef ağdaki bant genişliği dolduğunda, hedefe gerçekten erişmek isteyen kullanıcıların hizmete ulaşmaları engellenmiş olur.

İkinci yöntemde ise hedefteki sistemin kaynaklarını tüketmek amacıyla, bozuk paketler ya da ağ protokollerini kötüye kullanan veri paketleri kullanılarak saldırıda bulunulur. Bu paketler, normal veri paketlerine göre daha fazla kaynağın tükenmesine neden olur, çünkü sistem bu veri paketlerini işlemeye çalışırken işlemci ve bellek gibi kaynaklarını sömürerek hizmet veremeyecek duruma gelir (Erhan vd. 2013).

4.3.6 Veri Sızıntısı Engelleme (VSE)

Topaloğlu (2012)'na göre, Veri Sızıntısı Engelleme (VSE), kurum ya da kuruluşların sahip oldukları gizlilik seviyesi yüksek verilerin, herhangi bir sebeple kurum ya da kuruluş dışarısına çıkarılmasını engellemek üzere tasarlanmış, birden fazla aşamaya sahip bir sistemdir. Yoğunlukları ve karmaşık yapılarıyla bilinen siber tehditler sürekli artmaktadır.

Artan siber saldırılar bir şirketin işletme faaliyetlerinde veya operasyonel tedarik zincirinde ciddi aksamalara, itibar kaybına veya hassas müşteri bilgilerine ve fikri mülkiyet haklarına zarar verebilmektedir (İnt. Kyn. 35). Siber güvenlikte alınması gereken tedbirler kurumdan kuruma farklılık gösterse de verilerin önem düzeyi arttıkça güvenlik önlemleri alınması da aynı oranda artmaktadır.

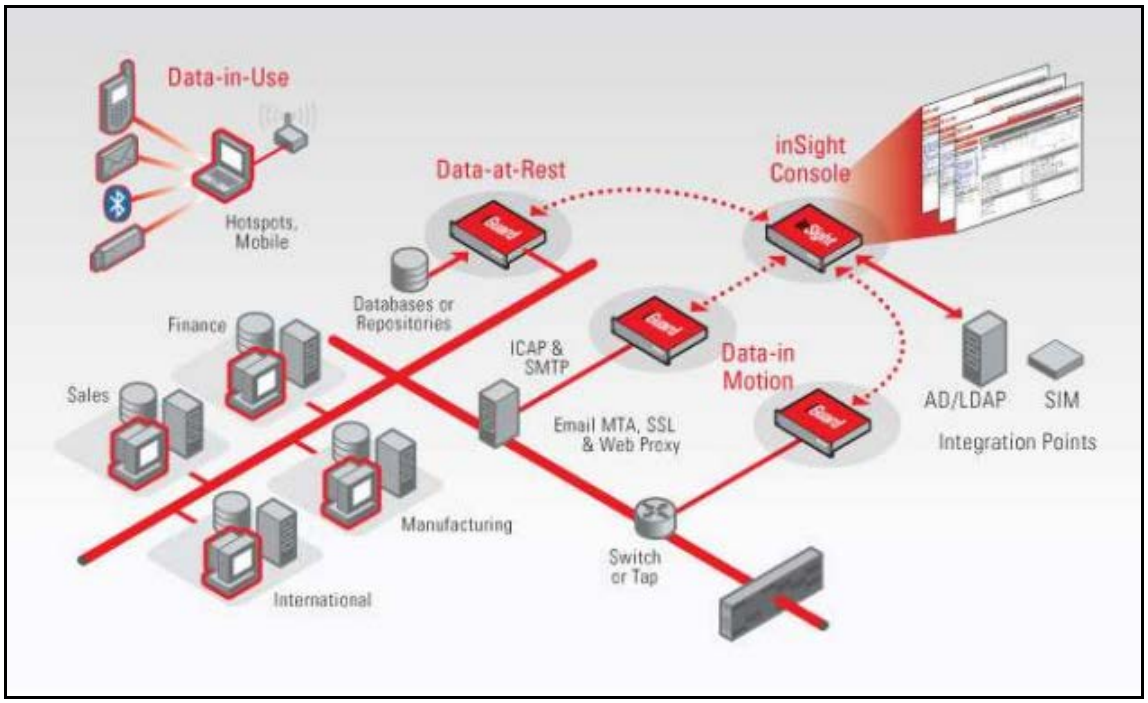
Siber güvenlik alanında "Data Loss Prevention" (DLP) olarak da bilinen bu uygulamalar, farklı bakışlar nedeniyle "veri sızıntısı önleme", "veri kaybı önleme", "veri kaçağı önleme", "veri sızıntısı engelleme", "veri kaybı engelleme" veya "veri kaçağı engelleme" olarak isimlendirilebilmektedir. Özünde ise DLP, hassas verilerin yetkisiz olarak erişimini veya izinsiz olarak başka ortamlara taşınması ya da iletilmesini izleyen ve korunmasını sağlayan bir veri güvenliği teknolojisidir.

Veri güvenliği ölçeğinde değerlendirildiği zaman, bilgi güvenliği denildiğinde, veri sızıntısı engelleme teknolojileri yardımıyla, imha edilinceye kadar veriyi bulunduğu depolama alanlarında, ağ içerisinde ve kullanıcı noktasında koruma altına almak anlaşılır. Topaloğlu (2012)'na göre DLP teknolojileri söz konusu sebepler nedeniyle üç farklı yapıda değerlendirilmektedir:

- **Kullanımdaki veriler:** Kullanıcının sürekli erişim halinde bulunduğu verilerin güvenliğinin sağlanması, uç noktada istemci tarafına kurulan bir ajan uygulama sayesinde gerçekleşmektedir. Sunucuda bulunan kurallar, ajan uygulamasını sürekli olarak güncelleyip değişen politikalara uyumlu hale getirilmesini sağlayarak yetkisiz bilgi iletimini engellemektedir. Bununla birlikte en zayıf halkanın insan olduğu prensibi dikkate alınarak kullanıcılara bilgi güvenliği konularında belli periyodlarda eğitim verilmelidir.

- **Durağan veriler:** Depolama ortamlarında bulunan veriler durağan halde bulunmaktadır. Bu tür veriler, bilgilerin, veri tabanlarının ya da dosya yedeklerinin bulunduğu alanda korunmaktadır. Kurumlarca durağan verilerin sınıflandırılmasını yapılmalı, unutulan fakat kritik bilgiler ihtiva eden veri tabanları veya dosyalar mutlaka sunucu tarafında yapılandırılmış olan kurallar içerisine dahil edilmeli, olası sızıntılar engellenmelidir.

- **Hareket halindeki veriler:** Ağ üzerinde iletilen veriler hareket halindeki veriler olarak adlandırılır. DLP uygulamaları, hareket halinde bulunan verileri analiz ederek herhangi bir sızıntının olup olmadığını algılayabilmektedir. Hareket halinde bulunan verilerin durağan verilere göre algılanması ve tehdit anında durdurulması daha zordur. Verilerin ağ içerisinde bir noktadan başka bir noktaya iletimi esnasında sunucu tarafında yapılandırılmış olan kurallara göre izin verilmekte veya engellenmektedir. Ağa katılması gereken misafir kullanıcılar kritik verilerin bulunduğu ağlarda çok daha büyük tehlike oluşturmaktadır. Sunucudaki protokoller buna göre yapılandırılmalı, zorunlu olmadıkça misafir katılımlarına izin verilmemelidir.



Şekil 4.24 Genel kabul görmüş DLP mimarisi (İnt. Kyn. 57).

4.3.7 SecureDrop

SecureDrop açık kaynak kodlu, ifşacı ile gazeteciler arasında güvenli bir iletişim kurulmasını sağlayan Python dili ile hazırlanmış bir yazılımdır. İlk olarak Aaron Swartz ve Kevin Poulsen tarafından DeadDrop adı altında tasarlanmış ve geliştirilmiştir. Aaron Swartz'ın ölümü sonrasında The New Yorker gazetesi çalışanları tarafından StrongBox ismiyle geliştirilmeye çalışılmıştır.

Basın Özgürlüğü Vakfı (The Freedom of the Press Foundation) tarafından Ekim 2013'te DeadDrop projesi devralınarak SecureDrop ismiyle geliştirilmeye başlanmıştır. Vakıf daha sonra ProPublica, The Intercept, The Guardian ve The Washington Post gibi gazetelere SecureDrop kurulumu için yardımda bulunmuştur (İnt. Kyn. 26).

SecureDrop, TOR ağını kullanarak, ifşacı ve gazeteciler arasında anonim bir iletişim kurulmasını sağlamaktadır. Bu iletişim için TOR ağında bulunan gizli servisler kullanılmaktadır. TOR ağı üzerinden SecureDrop web sitesine erişen ifşacıya, rastgele üretilmiş bir kod adı verilir ve kod adıyla ifşa edilmek istenen bilgi ya da belgeler araştırmacı gazetecilere gönderilir.

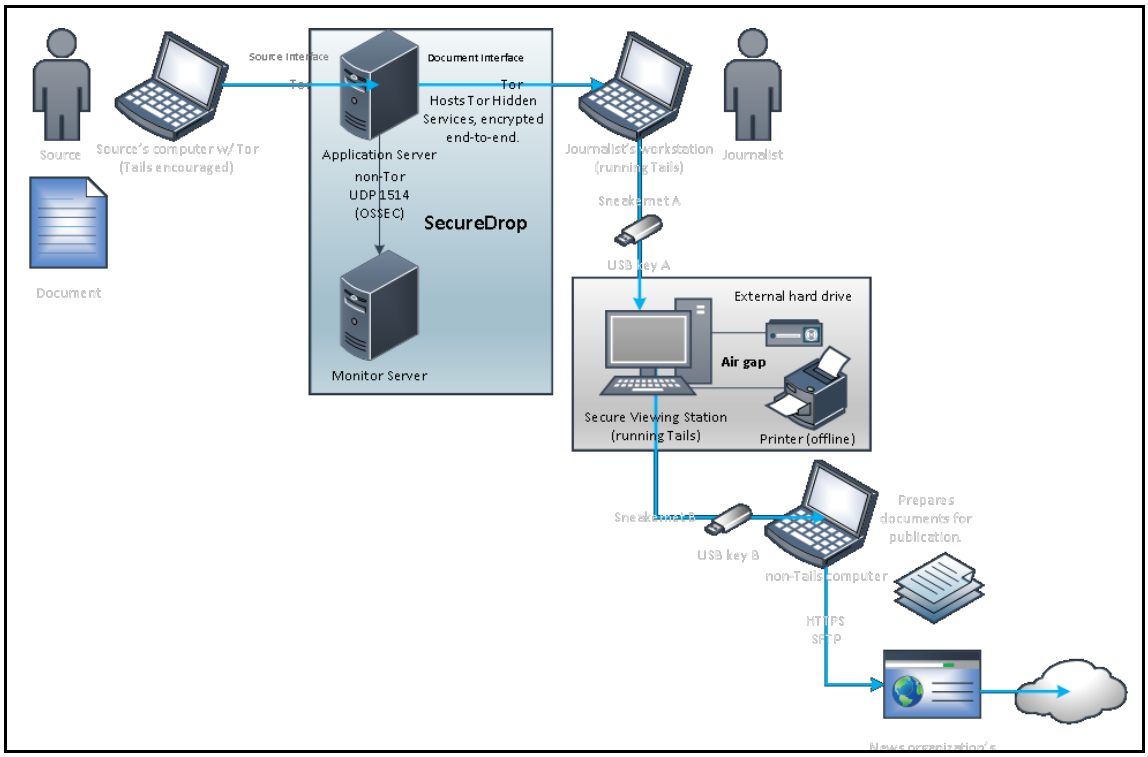
Tekrar iletişim kurmak isteyen ifşacının, rastgele üretilen kod adını unutmaması gerekmektedir. Haber kuruluşları kendilerine ait ayrılmış sunucuları kullanmaktadır (İnt. Kyn. 26).

SecureDrop iki fiziksel sunucu kullanmak üzere tasarlanmıştır. Mesajları ve belgeleri depolayan kamuya açık bir sunucu ile kamuya açık sunucunun güvenliğini kontrol eden ikinci bir sunucu bulunmaktadır. Kamuya açık sunucuda; mesaj ve belgeleri web üzerinden kabul eden ve güvenli depolama için GPG ile şifreleyen Python ile geliştirilmiş bir web uygulaması bulunmaktadır.

Söz konusu sunucuya sadece TOR'un gizli servislerine erişebilmek için gereken TOR tarayıcı ile bağlanılabilmektedir. Bu sayede ifşacı, kimliğini SecureDrop sunucusundan ve birçok ağ dinleyicisinden gizleyebilmektedir. SecureDrop uygulaması içerisinde ve etkileşimde bulunduğu çevrede TOR, GnuPG şifreleme, Apache, OSSEC, Grsecurity, Ubuntu ve TheTails işletim sistemiyle birlikte çalışmaktadır. Web uygulamasının ürettiği benzersiz rastgele kod ile giriş yapan ifşacı, medya kuruluşundan cevap olarak gelen mesajları okuyabilmekte, yeni mesajlar veya yeni belgeler ekleyebilmektedir.

Gelen ve giden cevapların tamamı, en son gelen en üstte olacak şekilde, gazeteci ve ifşacı tarafından görülebilmektedir. Bu ortam karşılıklı iletişim için herhangi bir e-posta adresi gerektirmediğinden diğer yöntemlere göre çok daha güvenli olmaktadır. Gazetecinin ifşacı hakkında bildiği tek şey, benzersiz rastgele üretilmiş kod adıdır (İnt. Kyn. 10).

Gazeteciler, SecureDrop aracılığı ile gelen bilgilere erişebilmek için iki USB bellek ve iki kişisel bilgisayara ihtiyaç duymaktadır. İlk kişisel bilgisayar TOR ağı üzerinden SecureDrop sunucusuna erişerek ifşacının göndermiş olduğu şifreli belgeleri ilk USB belleğe indirmektedir. İkinci kişisel bilgisayar; internet bağlantısı bulunmamakla birlikte her yeniden başlatıldığında izleri temizleyen bir yapıya sahip olan Tails işletim sistemi ile çalışmaktadır.



Şekil 4.25 SecureDrop çalışma mimarisi (İnt. Kyn. 10).

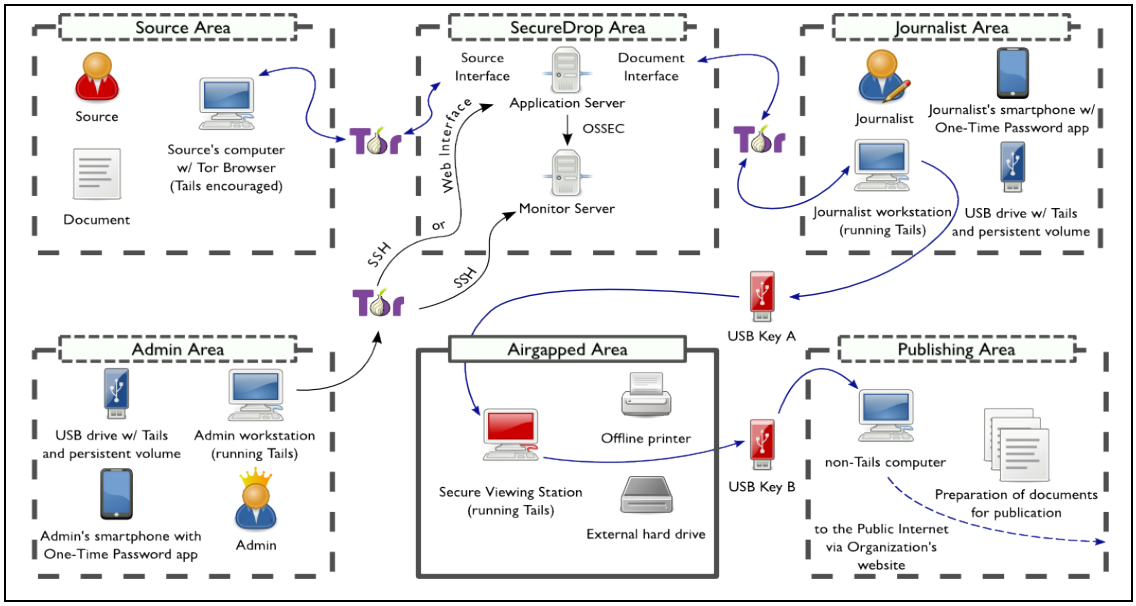
İkinci USB bellekte ise şifreyi çözen kod bulunmaktadır. Birinci ve ikinci USB belleklerin her ikisi de ikinci kişisel bilgisayara takılarak, ifşacıdan gelen verilerin şifreleri çözebilmektedir. Bu sayede sızdırılan veriler gazeteciye eksiksiz bir şekilde ulaştırılırken ifşacının bilgileri gizli tutulmuş olmaktadır (İnt. Kyn. 10).

Basın Özgürlüğü Vakfı, SecureDrop kaynak kodlarının ve güvenlik ortamının, her önemli sürümün yayınlanmasından önce bağımsız bir üçüncü tarafça denetleneceğini ve sonuçlarının yayınlayacağını ilan etmiştir. SecureDrop uygulaması üç özel bilgisayardan oluşmaktadır (İnt. Kyn. 39):

- **Güvenli İzleme İstasyonu (Secure Viewing Station):** USB Bellek üzerinde çalışan TheTails işletim sistemi ile çalışan kişisel bilgisayardır. Bu bilgisayarda internet bağlantısı bulunmamakta, ifşacıdan gelen şifreli verilerin şifresinin çözülerek incelenebilmesi sağlanmaktadır.
- **Uygulama Sunucusu (Application Server):** İki parçalı ve TOR gizli servislerini çalıştıran Ubuntu sunucusudur. Bu sunucudaki ilk parça, ifşacının, gizlilik içerisinde ifşa etmek istediği verileri şifreleyerek sunucuya yüklemesini sağlamaktadır. Yani ilk bölüm TOR gizli servislerini kullanarak ifşacılar için özel olarak hazırlanmış bir

arayüze sahiptir. İkinci bölüm ise gazetecilerin ifşacılar ile iletişim kurabileceği, şifrelenmiş verileri USB belleğe alabilmelerini sağlayan kimlik doğrulamalı ve TOR gizli servislerini kullanan doküman arayüzüdür.

- **İzleyici Sunucu (Monitor Server):** Uygulama sunucusuna yapılacak saldırıları tespit etmekte ve sunucunun durumu hakkında bilgilendirici e-postalar göndererek sistem yöneticisini uyarmaktadır. Bu işlem için OSSEC isimli IPS yazılımı kullanılmaktadır.



Şekil 4.26 SecureDrop altyapısı (İnt. Kyn. 10).

Günümüzde SecureDrop kullanan birçok basın kuruluşu bulunmaktadır. Herhangi bir kuruluşa SecureDrop ile bilgi göndermek istendiğinde, kuruluşun web sitelerinde yayınlanan "soğancık (onion)" adresi SecureDrop web sitesinde ilan edilen adresle karşılaştırılarak, devam etmeden önce adreslerin eşleştiği doğrulanmalıdır. Yayınlanan adreslerin bazıları Çizelge 4.3'de yer almaktadır.

Bilgisayar korsanlarının basın kuruluşlarının meşru kimliğiyle maskelenmiş, kötü amaçlı bir SecureDrop örneği ile ifşacıları kandırmaya çalışma ihtimaline karşı bu tedbir alınmalıdır (İnt. Kyn. 11).

Çizelge 4.3 Basın kuruluşlarına ait soğancık (onion) adresleri (İnt. Kyn. 11).

Organizasyonun adı	*Uygulama tarihi*	*Web konumu*
The New Yorker	15 Mayıs 2013	https://projects.newyorker.com/strongbox/ Tor: strngbxhwyuu37a3.onion
Forbes	29 Ekim 2013	https://safesource.forbes.com/ Tor: bczjr6ciiblco5ti.onion
Bivol	30 Ekim 2013	https://www.balkanleaks.eu/ Tor: dtsxnd3ykn32ywv6.onion
ProPublica	27 Ocak 2014	https://securedrop.propublica.org/ Tor: pubdrop4dw6rk3aq.onion
The Intercept	10 Şubat 2014	https://firstlook.org/theintercept/securedrop/ Tor: y6xjgkgwj47us5ca.onion
San Francisco Bay Guardian	18 Şubat 2014	https://bayleaks.com/ Tor: wd5x5eexdqcjrqfa.onion
The Washington Post	5 Haziran 2014	https://www.washingtonpost.com/wpstat/securedrop/securedrop.html Tor: vbmwh445kf3fs2v4.onion
TheGuardian	6 Haziran 2014	https://securedrop.theguardian.com/ Tor: 33y6fjyhs3phzfjj.onion
The Globe and Mail	04 Mart 2015	https://sec.theglobeandmail.com/securedrop/ Tor: n572ltkg4nld3bsz.onion
Radio Canada	20 Ocak 2016	https://sourceanonyme.radiocanada.ca/ Tor: w5jfqhep2jbypkek.onion
Canadian Broadcasting	29 Ocak 2016	https://securedrop.cbc.ca/ Tor: ad2ztmbv5vmbj7ic.onion
The Associated Press	18 Ekim 2016	https://securedrop.ap.org/ Tor: 3expgpdnrrzezf7r.onion
The New York Times	15 Aralık 2016	https://www.nytimes.com/tips#securedrop Tor: nytimes2tsqtnxek.onion
BuzzFeed News	21 Aralık 2016	https://contact.buzzfeed.com/ Tor: 6cws3rcwn7aom44r.onion
USA Today	22 Şubat 2017	https://newstips.usatoday.com Tor: usatodayw7vu5egc.onion

4.3.8 GlobaLeaks

GlobaLeaks, güvenli ve anonim ifşacılık girişimlerine imkân tanıyan, açık kaynaklı ve ücretsiz bir yazılımdır (İnt. Kyn. 27). Çevrimiçi olarak konuşma özgürlüğünü destekleyen İtalyan merkezli bir sivil toplum kuruluşu olan "Şeffaflık ve Dijital İnsan Hakları için Hermes Merkezi" tarafından geliştirilmiştir.

Proje, Fabio Pietrosanti tarafından başlatılmış ve ilk kez 15 Aralık 2010'da yapılan bir hactivist toplantısında paylaşılmıştır. GlobaLeaks gizli belgeleri yayınlayıcı değildir, gizli belgelerin ifşacı tarafından belirlenen medya kuruluşlarına anonim bir şekilde ulaştırılmasını sağlamak üzere geliştirilmiş bir çerçevedir (Chen 2011).

Bilgi ifşasının güvenli ve kolay olması için gerekli basitlikte tasarlanmış, anonim ihbarlara imkân sağlayan bir yapıdadır (İnt. Kyn. 31). Kullanıcı dostu olacak şekilde hazırlanan yazılım, ihtiyaçlara göre özelleştirilebilmektedir. GlobaLeaks birçok kullanım şeklini hedeflemektedir ve bu nedenle bir çerçeve olarak tasarlanmıştır.

Esneklik düşünülerek tasarlanan GlobaLeaks günümüzde 60'tan fazla projede yer almakta olup bu yazılım AGPL lisansını kullanmakta ve yazılım geliştirmek ve iyileştirmek için birlikte çalışan kullanıcıların, gönüllülerin ve katkıda bulunanların oluşturduğu açık bir topluluk tarafından yetkilendirilmektedir.

Birçok işletim sistemi ile çalışabilmesine rağmen GlobaLeaks tarafından önerilen, Ubuntu Xenial 16.04 LTS işletim sistemidir. Sistem, Python 2.7 ve AppArmor desteği gerektirmektedir. Söz konusu uygulamalar, Ubuntu 14.04 ve sonrası sürümlerde önceden kurulu olarak geldiği için bu işletim sistemi önerilmektedir.

Güvenlik ve kaynak kullanılabilirliği için, GlobaLeaks'in özel bir sunucuya ihtiyacı bulunmaktadır. Kurulacak mimariye bağlı olarak, GlobaLeaks'e tahsis edilecek bir veya iki sunucu gerekebilmektedir. Bu sunucuların VPS sunucu olmaması güvenlik açısından çok önemlidir. İki sunucudan her birinin barındırılması için farklı veri merkezlerinin kullanılması tavsiye edilmektedir.

Barındırma sağlayıcısının ve GlobaLeaks sunucusunun fiziksel konumu güvenlik açısından önem arz etmektedir. VPS'lerde bulunan zafiyetlerden dolayı bazı riskler bulunmaktadır. GlobaLeaks, sunucu durumuyla ilgili uyarı bildirimlerini işlemek için e-posta hizmetini kullanmaktadır. Bu sebeple ilgili bildirimleri alıcılara göndermek için kullanılacak bir e-posta hesabına ihtiyaç duyulmaktadır. Bu e-posta hesabının kullanıma hazır olması ve SMTP sunucusunun e-postanın güvenli bir şekilde iletilmesini sağlamak üzere SMTPS veya SMTP/TLS'yi desteklemesi gerekmektedir (İnt. Kyn. 31) .

4.3.9 GNU Privacy Guard (GPG)

GNU Privacy Guard (kısa yazılımı GnuPG veya kısaca GPG), PGP şifreleme tekniğine cevap olarak 90'lı yılların sonlarında geliştirilmiştir. GPG, PGP'yi genişleten ve bir internet standardı olan OpenPGP'nin tam bir uygulamasıdır. GPG, GNU Genel Kamu Lisansı (GNU GPL) kapsamında ücretsiz yazılım olarak yayınlanmıştır. Kaynak koda tam erişim imkânı sunnmaktadır.

Alman Federal Ekonomi ve Teknoloji Bakanlığı, GPG'nin daha da geliştirilmesi için fon sağlamaktadır. GPG oldukça önemli bir kullanıcı kitlesine sahiptir: Debian, MandrakeSoft, Red Hat ve SuSE gibi çoğu GNU/Linux dağıtımında bulunmaktadır. GPG'nin ilk kararlı sürümü 7 Eylül 1999'da yayınlanmıştır (Nguyen 2004).

4.3.10 Tails İşletim Sistemi

Tails; DVD, SD Kart veya USB flash bellek gibi taşınabilir ortamlara kurulabilen, anonim bir şekilde bilgisayar kullanabilmeyi sağlayan, Linux türevli bir işletim sistemidir. Özellikle iki nokta arasındaki iletişimi, iz bırakmadan gerçekleştirmesi nedeniyle tercih edilmektedir. Anonim olarak internette gezinmeyi sağlayan Tor2Web, ifşacıların sızıntı platformlarına ve TOR servislerine bağlanabilmelerini kolaylaştırmaktadır.

Kişisel bilgiler ve parolalar gibi gizliliği yüksek verilerin iletiminde güvenli veri katmanı (SSL) yaygın olarak kullanılırken, ifşacılar ile ifşa noktasındaki gazeteciler arasında gerçekleştirilen iletişim PGP veya GnuPG kullanılarak şifrelenmektedir (Çalışkan 2016).

Tails; bellekte çalışan bir işletim sistemi olması sayesinde gizli bir şekilde internette gezinmeyi sağlamaktadır. Açık kaynak kodlu, Linux temelinde, kullanıcıların gizliliklerini ve anonimliklerini koruyan bir işletim sistemidir. Gizliliğin çok önemli olduğu durumlarda bilgisayarın sabit sürücüsünün sökülmesi ve sadece USB bellek üzerinde çalışan Tails işletim sisteminin kullanılması önerilmektedir.

Bilgisayar kapatıldığında tüm kişisel veriler temizlendiği için herhangi bir iz kalmamaktadır. Ayrıca dizüstü bilgisayar gibi taşınabilir aygıtların çalınması riskine karşı bilgilerin de güvende olması sağlanmaktadır (İnt. Kyn. 60).

Debian Linux işletim sisteminin bir türevi olan Tails aracılığı ile yapılan tüm bağlantılar TOR ağından geçmek zorunda kalır. Bir uygulama doğrudan internete bağlanmak istediğinde güvenliği sağlamak amacıyla bağlantı engellenmektedir (Farina et al. 2015).

Tails, üzerinde; dosyaları, e-postaları ve anlık mesajlaşmaları şifrelemeye yarayan araçlarla, web tarayıcısı, anında mesajlaşma istemcisi, e-posta istemcisi, ofis paketi, görüntü ve ses düzenleyici gibi uygulamaları bulundurmaktadır (İnt. Kyn. 12).

4.3.11 TrueCrypt

TrueCrypt; TrueCrypt Vakfı tarafından geliştirilen açık kaynak kodlu bir şifreleme çözümüdür. İlk sürümü, Şubat 2004'te piyasaya sürülmüştür. TrueCrypt ücretsiz olarak dağıtılmaktadır. Yazılım aşağıdaki özellikleri taşımaktadır (İnt. Kyn. 50):

- Bir dosyada sanal bir şifreli disk oluşturur ve onu gerçek bir disk gibi kullanmaktadır.
- USB flash bellek veya sabit disk gibi bir kayıt ortamını veya depolama aygıtını şifrelemektedir.
- Windows'un yüklü olduğu bir bölümü veya sürücüyü şifrelemektedir.
- Şifreleme otomatik, gerçek zamanlı ve şeffaf bir yapıdadır.
- Birisi tarafından parolayı söylemeye zorlanılması durumunda, iki seviyeli, akla yatkın bir inkâr edilebilirlik sağlamaktadır. Bunlar gizli bölüm (steganografi) ve rastgele veriden ayırt edilemeyen TrueCrypt bölümüdür.
- Şifreleme algoritmaları: AES-256, Serpent ve Twofish'tir. Çalışma şekli ise XTS ile uyumludur.

Bir flash bellekte veya taşınabilir bir depolama aygıtında veri taşırken, mevcut masaüstü makinelere TrueCrypt'i yüklemek uygun veya mümkün olamamaktadır. Taşınabilir depolama aygıtının tamamı TrueCrypt birimi değilse bile bu bir sorun teşkil etmemektedir.

TrueCrypt'in Traveler Disk kurulumu kullanılarak, truecrypt.exe, korunan bilgiye erişmek için kullanılan kişisel bilgisayara TrueCrypt'i yüklemeden, şifrelenmiş verilere erişilebilmeyi sağlamaktadır. Kullanıcı isterse, TrueCrypt'i bir flaş bellek üzerinde otomatik olarak çalışacak şekilde yapılandırabilmektedir.

TrueCrypt anahtar dosyalarının kullanılmasını desteklemektedir. Anahtar dosyalarını, tuş vuruşlarını kaydeden (keylogger) saldırılarına karşı koruyabilmektedir. Şayet bir saldırgan girilen şifreyi bir keylogger aracılığı ile yakalasa bile, anahtar dosyası olmadan bağlantı kuramamaktadır. Sistem, kaba kuvvet saldırılarına (bruteforceattacks) karşı koruma sağlayabilmektedir.

Bu durum özellikle birim şifresi zayıf olduğunda önemli hale gelmekte, çok kullanıcılı, paylaşımlı erişimlerin yönetilmesine izin verebilmektedir. Bu durumda şifreli birimi takmadan önce tüm anahtar dosyaları sahiplerinin anahtar dosyalarını sunmaları gerekmektedir (İnt. Kyn. 50).

4.3.12 Soğan Paylaşımı

Soğan Paylaşımı (OnionShare), kullanıcıları için güvenli dosya aktarımları sağlamak için TOR'un anonimliğini güçlendiren bir dosya paylaşım uygulamasıdır. Her iki kullanıcı da TOR tarayıcısını kullanması nedeniyle farklı yönlendiricilerden geçmesine rağmen, dosya aktarımları doğrudan yükleyiciden alıcıya doğrudur.

OnionShare, Python ile geliştirilmiş, sınırlı bir web sunucusu olarak yerel sistemde dosya paylaşımı oluşturmaktadır. Bu web sunucusu daha sonra TOR tarayıcısının yerleşik işlevselliğini kullanarak TOR Gizli Servisi olarak ilan edilmiştir (Farina et al. 2015).

Uygulama, bir referans olarak kullanılmak üzere paylaşılan dosya için benzersiz bir isim oluşturmak üzere 16 karakterlik ".onion" adresi ve dosya adı için yine rastgele karakterler üretmektedir. Farina vd. (2015)'e göre, soğan paylaşımı tarafından gerçekleştirilen işlemler üç adımda tamamlanmaktadır:

- Birinci adımda yükleyici, TOR ağına soğan paylaşımına giriş noktası sağlamak için işlem başlattığında kullanıcılar için varsayılan geçici (temp) klasörde geçici bir dizin oluşturulmaktadır. Soğan paylaşımındaki rastgele oluşturulmuş isimler aynı prosedürü takip ederken bir dizi kural uygulanır. Bunlar:

a) İşletim sistemi tarafından rastgele bir dizi bayt oluşturulur. Bunların 8'i dizin ya da ana bilgisayar adı için kullanılırken 16'sı ise paylaşım URL'sinin dosya adı bölümü için kullanılmaktadır.

b) Bu rastgele baytlar SHA-256'dır ve elde edilen karmanın en sağdaki 16 karakteri çıkarılmaktadır.
c) Oluşturulan bu başlık, daha sonra base32 olarak kodlanır, tüm karakterler küçük harfe dönüştürülür ve paylaşım yolu ya da adında kullanılamayacak olan karakterler ("=" işareti vb.) kullanılmışsa kaldırılır.

- İkinci adımda, birinci adımın sonucu olarak ortaya çıkan veri <host>.onion/<dosyaadı> biçiminde kullanılarak bir URL şeklinde tanımlanır. Bu URL'ler TOR tarayıcının giriş düğümlerini tanıtan URL'dir ve DHT'ye kaydolmaktadır.

- Üçüncü adımda yükleyici, URL'yi belirli bir zaman diliminde (varsayılan olarak 24 saat) kullanması gereken indiriciye göndermektedir. Bu dosyanın imzası, zaman damgasıyla eşleşmezse bu işlem bir kütüphane tarafından kontrol edilir. Bunun yanında süre sınırı olan soğan paylaşımı, değeri 1'den başlayan bir karşıdan yükleme sayacı da kullanmaktadır. Başarıyla başlatılan karşıdan yükleme sayısı bu sayacı eşleştirdikten sonra bağlantı artık geçerli sayılmaz ve dosya imzasıyla birlikte gelen tüm URL'ler reddedilir (Farina *et al*. 2015).

4.3.13 Eşler Arası Ağlar (P2P)

Eşler arası (Peer-to-Peer) (P2P) protokolü, ilk olarak 1999 yılında geliştirilen Napster isimli paylaşım yazılımına dayanmaktadır (Çaylı vd. 2007). Bu uygulamada Peer-to-Peer ağ yapısı dosyaları paylaşmak için kullanılmıştır. Diğer bir deyişle MPEG Layer3 (mp3) sıkıştırılmış ses dosyalarının paylaşımı için kullanılırken eşler arasında çoklu ortam iletişimi kurmak için de kullanılmıştır (Schollmeier 2001).

Uygulama merkezi, istemciler tarafından paylaşılan dosyaların listesini bir sunucuda tutmaktadır. İstemci, uygulama aracılığı ile sorgulama yaptığında, sunucuda bulunan listeden arama gerçekleştirilerek arama sonucunda bulunan sonuçlar istemci bilgisayara gönderilmektedir (Çaylı vd. 2007). İnternetin yaygınlaşması ve kullanıcıların kolaylıkla dosyaları paylaşabilmesi telif hakkı sahibi yapımcıların zarar etmesine neden olmuş, harekete geçen hak sahiplerinin dava açması sonucunda Napster uygulamasının sunucuları kapatılmıştır.

Tek merkezden kontrol edilen sistem durdurulduğunda P2P geliştirilerek ikinci nesil uygulamalar yazılmıştır. Söz konusu uygulamalar günümüzde de kullanılmaktadır. P2P ağ protokolünde yapılan iyileştirmeler, geleneksel sunucu-istemci iletişiminin de gelişmesine, yaşanan dar boğazların aşılmasına ön ayak olmuştur.

Bu bakımdan P2P iletişimi yararlı ve istenen bir yöntem olmaktadır. Ancak bu protokol aracılığı ile paylaşılan dosyalar büyük boyutlara ulaştığında bağlantı hızıyla orantılı olarak P2P, ağda ciddi yavaşlamalara sebep olmakta ve ağ kaynaklarını sömürmektedir (İnt. Kyn. 56).

4.3.14 BitTorrent

P2P ağlarında gerçekleştirilen yenilikler sonrasında eski bir bilgisayar korsanı olan Bram Cohen yeni bir yazılım geliştirmiştir. Bu uygulama, geçmişteki P2P yazılımlarından oldukça farklı bir yapıya sahiptir. Bir dosyanın HTTP protokolü ile transfer edilmek istenmesi halinde tüm yük barındırma (hosting) sunucusunda olmaktadır.

Uygulamanın ilk adımı internet üzerinde yapılacak arama sonucunda, istenen dosyaya ait .torrent uzantılı dosyanın indirilmesidir. Büyüklüğü 50 KB civarında bulunan bu dosya sayesinde istemciler, torrent yazılımlarını kullanarak aynı dosyayı paylaşan kişilerin oluşturduğu kümeye dâhil olmaktadır (İnt. Kyn. 56).

BitTorrent ile birden çok kullanıcı aynı dosyayı aynı anda indirirken dosyanın parçalarını da birbirlerine yüklemektedirler. Bu, indiren kullanıcılara yükleme sebebiyle oluşan kaynak maliyetinin pay edilmesini sağlamaktadır. Yani indirmeyi tamamlayan kullanıcılar (indirme tam olarak bitmese bile) yeni indiren kullanıcılara indirdiği parçalardan göndererek yükün paylaşılmasını sağlamaktadır (Cohen 2003).

İnt. Kyn. 56'a göre kümeye dâhil olan her kullanıcı dosyadan indirdiği kadarını diğer kullanıcılara göndermekle yükümlüdür. Kullanıcıların yükümlü oldukları göndermeleri yapıp yapmadığını ve diğer işlemleri kontrol eden bir izleyici (tracker) sunucu bulunmaktadır.

Bir kümenin oluşabilmesi için dosyanın tamamına sahip en az bir kullanıcının (seeder) olması gereklidir. Bu yöntem, bir dosyanın kısa sürede birçok bilgisayara ulaşmasını

sağlamaktadır. Tek bir merkezi sunucusu bulunmadığı için paylaşıma düşen bir dosyanın erişimden çıkarılması neredeyse imkânsızdır.

4.4 Gizli Belge Yayıncılığına Karşı Alınabilecek Tedbirler

İnt. Kyn. 5'e göre en üst düzey bilgi güvenliğine ulaşmak, özel ve resmi kurumlar için vazgeçilmez bir hedeftir. Ancak, bu hedefe ulaşabilmek için geçilmesi gereken iki ana engel bulunmaktadır;

Dış Saldırılar: Kuruluşlar çeşitli şekillerde farklı kişilerle iletişim kurmaktadır. Bazen stratejik bilgilerin ve BT kaynaklarının, kurum içindeki diğer bölümler, dış dünyadaki ajanslar veya vatandaşlarla paylaşılması gerekebilmektedir. Hassas verilere erişebilen çalışan sayısının çoğalması ve giderek artan sayıda sade vatandaşın özel ya da resmi kurum ve kuruluşların hizmetlerine erişebilmek amacıyla bilgi teknolojisine yönelmesi dış tehlikeleri artırmaktadır.

Devlet kurumları, doğası gereği çok büyük miktarda hassas veri/bilgi barındırmaktadır. Bu bilgi yoğunluğu, devlet kuruluşlarını, veri problemlerine ve amatör veya uzman bilgisayar korsanlarından gelen siber saldırılara açık hale getirmektedir.

İç Tehditler: Birkaç yıl öncesine kadar organizasyonların BT alt yapısında dış tehditlere karşı klasik tedbirleri almak yeterli olmaktaydı. Bugün ise bilgi güvenliğinin boyutları değişmiş durumdadır. Bilgi güvenliğine yönelik tehdit her zaman dışarıdan kaynaklanmamakta, organizasyonların kendi içinde de tehditler oluşabilmektedir. Küskün personel, saf veya açgözlü çalışanlar, teknoloji konusunda meraklı kişiler ve görevden atılanlar art niyetle hareket ederek ayrıcalıklı erişim yetkilerini kötüye kullanabilmektedir.

Kurumsal bilgi güvenliği, sadece BT bölümünün sorumluluğunda değildir, aksine tüm birimler arasında koordine edilerek en yüksek düzeyde ele alınması gereken bir konudur. İnt. Kyn. 53'e göre alınacak tedbirlerin altı farklı kurumsal birimi doğrudan ilgilendirdiği vurgulanmıştır. Bu birimler şunlardır:

- İnsan kaynakları birimi
- Hukuk birimi
- Fiziki güvenlik birimi

- Veritabanı yöneticileri
- Bilgi teknolojileri birimi
- Yazılım birimi

Bu altı grup, önerilen tedbirlerin çoğunu paylaşmaktadır, bu nedenle bir kuruluştaki bu grupların altısının birlikte çalışması önemlidir. Örneğin, insan kaynakları, çalışan bir personel kuruluştan ayrıldığında; BT, veritabanı yöneticileri, fiziki güvenlik ve hukuk birimleri birlikte çalışmalıdır. Söz konusu rapor, mevcut veya eski bir çalışanın ortaya çıkardığı geleneksel tehdide ek olarak, içerdeki tehdidin aşağıdaki yönlerini de değerlendirmeye almaktadır (İnt. Kyn. 53):

- Dışsal Tehditlerle Gizli Anlaşma: Bilgileri çalan veya bilgileri değiştiren çalışanların birçoğu organize suç şebekeleri ve yabancı kuruluşlar ya da yabancı hükümetler de dâhil olmak üzere dış tehditlerle gizli anlaşmalar yapabilmektedir.

- İş Ortakları: Sistemlere ve verilere erişim yetkisine sahip olan güvenilir iş ortaklarının çalışanlarının işleyebileceği suçlar da dikkate alınmalıdır.

- Birleşme ve Satın Almalar: Kuruluşların başka bir kuruluş tarafından satın alınması nedeniyle iç tehdit riski artmaktadır. Çalışanlar, stresli ve gelecek kaygısının ağır bastığı iş ortamında kaldıkları için organizasyonlarda iç tehdit riski artış göstermektedir.

- Kültürel Farklılıklar: Kültürel farklılıklar da çalışanların davranışlarını etkileyebilmektedir. Yurt dışına gönderilen ya da yurt dışında uzun bir süre geçiren çalışanlar kurum içerisinde uyum sağlamakta zorluk yaşayabilmektedir.

İç tehditler; teknik, davranışsal ve örgütsel sorunlardan kaynaklanabilir. Bu yüzden iç tehditlere karşı kapsamlı politikalar geliştirilmeli, prosedürler uygulanmalı ve teknolojiler kullanılmalıdır. Bir örgütte kurumsal yönetim, insan kaynakları, hukuk, fiziki güvenlik, bilgi teknolojileri, veri tabanı yöneticileri ve yazılım birimleri, kendi alanlarıyla ilgili önlemleri almalıdır. Kurum çapında karar vericiler, içerdeki tehdit sorununun önemini ve genel kapsamını iyi kavramalı ve bunu kurumun tüm çalışanlarına iletmelidir.

İnt. Kyn. 53'e göre, içsel tehdit oluşturan davranışlar; fikri mülkiyet hırsızlığı, BT sabotajı, dolandırıcılık, casusluk ve kazara oluşan tehditlerden korunmak için kurum ve kuruluşların uygulamaları gereken önemli tedbirler vardır. ISO 27001, ISO 27002, NIST gibi standartların yönergeleri ile Carnegie Mellon Üniversitesi tarafından dördüncü sürümü 2012'de hazırlanan "İçeriden Gelecek Tehditleri Azaltmak İçin Ortak Hassas Yönergeler" (Common Sense Guide to Mitigating Insider Threats) teknik raporu birlikte değerlendirildiğinde, alınması gereken önlemlerin Çizelge 4.4'de yer alan başlıklar altında incelenmesi gerektiği düşünülmüştür. Söz konusu tedbirler, kuruluşların içsel tehditlere karşı hangi adımları atmaları gerektiğini gösterirken, hangi uygulamada hangi birimlerin birlikte hareket edeceklerini de ortaya koymaktadır. Tabloda hangi birimin hangi tedbirler ile ilgisi belirtilmiştir. Her birim kendisini ilgilendiren konularda tedbirleri alması gereksiz iş yükünü azaltırken yetersiz güvenlik tedbirinin de oluşmasını engelleyebilecek bir yapıda bulunmaktadır.

Çizelge 4.4 Tüm örgüt grupları için uygulanacak önlemler ve öneriler (İnt. Kyn. 53).

	Uygulama - Öneri	*İ. K. Birimi*	*Hukuk Birimi*	*Fiziki Güvenlik*	*VT Birimi*	*BT Birimi*	*Yazılım Birimi*
1	Kurum çapında risk değerlendirmelerinde içeriden ve iş ortaklarından gelen tehditleri göz önünde bulundurun.	✓	✓	✓	✓	✓	
2	Politikaları ve kontrolleri açıkça belgeleyin ve tutarlı şekilde uygulayın.	✓	✓	✓		✓	
3	Tüm çalışanlar için periyodik güvenlik eğitiminde içeriden gelebilecek tehdit bilincini yerleştirin.	✓	✓	✓	✓	✓	✓
4	İşe alım sürecinden başlayarak, şüpheli veya zarar verici davranışları izleyin ve raporlayın.	✓	✓	✓	✓	✓	✓
5	Çalışma ortamında oluşabilecek olumsuz konuları belirleyin ve iyi yönetin.	✓	✓	✓	✓	✓	
6	Kritik verilerinizi ve varlıklarınızı listeleyin.	✓	✓	✓	✓	✓	✓
7	Sıkı şifre ve hesap yönetimi politikalarını uygulayın.	✓	✓			✓	
8	Görev ayrımı yapın ve erişim yetkisini belirleyin.	✓	✓	✓	✓	✓	✓
9	Bulut hizmetleri için erişim kısıtlamaları ve izleme yetkileri konusunda güvenlik kuralları tanımlayın.		✓	✓	✓	✓	
10	Sıkı erişim kontrolleri ve ayrıcalıklı kullanıcıları izleme politikaları oluşturun.	✓	✓			✓	✓
11	Sistem değişikliğiyle ilgili uygulamaları kurallara bağlayın.				✓	✓	✓
12	Çalışan eylemlerini izlemek için bir güvenlik bilgi ve olay yönetimi (SIEM) sistemi kullanın.	✓	✓	✓	✓	✓	✓
13	Mobil cihazlar da dâhil olmak üzere tüm uç noktalardan yapılan uzaktan erişimi izleyin ve kontrol edin.				✓	✓	
14	Kapsamlı bir çalışan işe son verme prosedürü geliştirin.	✓	✓	✓	✓	✓	
15	Güvenli yedekleme ve kurtarma süreçlerini uygulayın.				✓	✓	
16	“Kötü Niyetli Çalışan Tehditleri” programı geliştirin.	✓	✓	✓	✓	✓	✓
17	Normal ağ davranışları için ölçütler oluşturun.				✓	✓	
18	Sosyal medya konusunda özellikle dikkatli olun.	✓	✓	✓	✓	✓	
19	Verilerin kuruluş dışına yetkisiz çıkarılmasına açık kapı bırakmayın.			✓	✓	✓	

Çizelge 4.4'da yer alan uygulamaları, bilgi güvenliği açısından değerlendirerek tek tek yorumlamak gerekirse;

"Kurum çapında risk değerlendirmelerinde içeriden ve iş ortaklarından gelen tehditleri göz önünde bulundurma" önerisi, kuruluşların, yetkili kullanıcı erişimi olan güvenilir iş ortakları da dâhil olmak üzere kritik varlıklarını, kurum içi ve dışı tehditlere karşı korumak amacıyla kapsamlı, risk temelli bir güvenlik stratejisi geliştirilmesini gerekli kılmaktadır. Sadece büyük paydaşlar değil, organizasyonun çalışanlarının tamamı, sistem güvenliğinden ödün verme ve kritik verilerin kaybolması gibi risklere maruz kalınacağını bilmelidir.

Bununla beraber kuruluşun, kurumsal riski doğru bir şekilde değerlendirebilmek için tehdit ortamını tam olarak tanıması gerekmektedir. Risk; tehdit, savunmasızlık ve görevlerin birleşimi olarak tanımlanmaktadır. Kuruluş çapında risk değerlendirmeleri; kuruluşların kritik varlıklarını, bu varlıklara yönelik olası tehditleri tespit etmelerine ve varlıklar tehlikeye girdiğinde gerekli tepkiyi vermelerine yardımcı olmaktadır.

Kuruluşlar, tehditlerle mücadele etme ve örgüt görevlerini yerine getirme arasındaki dengeyi belirleyen genel bir ağ güvenlik stratejisi geliştirmeli ve güncellemek için değerlendirmenin sonuçlarını kullanmalıdır. Çok fazla güvenlik kısıtlamasına sahip olmak, kuruluşun görevlerini yerine getirmesini engelleyebilir, çok az güvenlik tedbirlerine sahip olmak ise güvenlik ihlaline sebep olabilir.

"Politikaları ve kontrolleri açıkça belgeleyin ve tutarlı şekilde uygulayın" önerisi, tüm organizasyon politikalarının ve prosedürlerinin tutarlı ve açık bir mesaj içermesi, çalışanların yanlışlıkla kuruluşa zarar verme veya algılanan bir haksızlığın örgüt dışına sıçrama olasılığını azaltma amacıyla verilmektedir. Kuruluşlar, politikaların adil olmasını sağlamalı ve herhangi bir ihlâl cezasının orantısız olmadığından emin olmalıdır.

Kuruluşlar, güvenlik politikaları ve denetimleri için şunları sağlamalıdır:

• Politikanın arkasındaki mantık da dâhil olmak üzere, özlü ve tutarlı belgeler bulunmalıdır.

• Uygulamalarda tutarlılık sağlanmalıdır.

• Politikalar konusunda periyodik olarak eğitimler verilmeli ve bunların gerekçesi anlatılarak politikaların uygulanması konusunda kararlı olunmalıdır.

"Tüm çalışanlar için periyodik güvenlik eğitiminde içeriden gelebilecek tehdit bilincini yerleştirin" önerisi, güvenlik eğitimleri, çalışanları, sadece kötü niyetli personeli tanımak üzere değil, kişisel davranışları da güvenlik politikaları doğrultusunda geliştirmeye teşvik etmelidir. Çalışanların politikaları ihlâl eden her tür davranışı kontrol altında tutulmalıdır. Örneğin:

• Organizasyonu tehdit eden veya içeriden gelebilecek zararları övmek,
• İstifa ya da işten ayrılma sonrasındaki kısa sürede büyük miktarda veri indirmek.
• Kuruluşun kaynaklarını başka bir yan iş için kullanmak veya çalışanlarla birlikte rekabet edecek başka bir iş kurmak için tartışmak.
• Çalışanların şifrelerini elde etmeye çalışmak veya güvenilir bir ilişkiden yararlanıp hilekârlık veya sömürü yoluyla erişim yetkisi sağlamak (genellikle "sosyal mühendislik" olarak adlandırılır).

"İşe alım sürecinden başlayarak, şüpheli veya zarar verici davranışları izleyin ve raporlayın" önerisi doğrultusunda, bir organizasyonun kötü niyetli çalışan tehdidini azaltma girişimi, işe alım sürecinde başlamalıdır. Bu çerçevede, şüpheli çalışanların geçmiş denetimleri yapılmalı, varsa daha önceki cezai mahkûmiyetleri ortaya çıkarılmalı, kredi notu kontrolü yapılmalı, kimlik belgeleri ve geçmiş istihdamı doğrulanmalıdır.

Bununla beraber işyerinde yaşanan sorunlarla baş edilebilmesi için kişinin yetkinliği ve davranışlarıyla ilgili olarak önceki işverenlerden bilgi alınmalıdır. Kuruluşlar, çalışanın kritik, gizli bilgilere ya da güvenlik sistemine erişimini kayıt altına almak üzere riske dayalı bir karar sürecini kullanmalı, herhangi bir suçun niteliğini ve süresini dikkate alarak, sistem kayıt bilgilerini yasal olarak kullanabilmelidir.

"Çalışma ortamında oluşabilecek olumsuz konuları belirleyin ve iyi yönetin" önerisi kuruluşların, politikalarını ve uygulamalarını yeni çalışanlara ilk günlerinde bildirmesini gerekli kılar. Bu tür politikalar ve uygulamalar, kabul edilebilir işyeri davranışları, kıyafet kuralları, kabul edilebilir kullanım politikaları, çalışma saatleri, kariyer gelişimi,

çatışma çözümü ve diğer işyeri sorunlarını da içermelidir. Bu politikaların tek başına uygulanması yeterli değildir.

Yeni çalışanlar ve deneyimli çalışanlar, bu politikaları ihlal etmenin sonuçlarının farkında olmalıdır. Kuruluşlar, uyumlu bir çalışma ortamı sağlamak için tutarlı bir şekilde politikalar izlemelidir. Politikaların tutarsız olarak uygulanması, işyeri içinde husumet duygularının ortaya çıkmasına neden olabilmektedir. İş arkadaşları genelde bazı çalışanların kuralların üstünde olduğunu ve özel muamele gördüklerini düşünebilirler. Bu tür anlaşmazlıklar, çalışanların içeriden BT'yi sabote etmesine veya bilgi hırsızlığına yol açabilmektedir.

"Kritik verilerinizi ve varlıklarınızı listeleyin**"** önerisi, organizasyonların içeriden gelebilecek saldırılar da dâhil olmak üzere tüm saldırılardan korunmak için bir risk değerlendirmesi yapılmasını içermektedir. Risk değerlendirmesi, bir organizasyona sistemlerinin nasıl işlediği, hangi verilerin kimler tarafından kullanıldığı ve nerede depolandığı hakkında bilgi verebilmektedir. "National Institute of Standards and Technology (NIST)"e göre, risk değerlendirme çerçevesi altı adımda yapılmaktadır:

1. Bilgi sistemi ve bu sistem tarafından işlenen, saklanan ve iletilen bilgileri bir etki analizini temel alarak sınıflandırmak
2. Bilgi sistemi için bir başlangıç güvenlik kontrol seti oluşturmak. Risk analizine ve yerel koşulların organizasyon açısından değerlendirmesine bağlı olarak güvenlik kontrolü için en alt seviyeyi belirlemek ve bunu güçlü tutmak.
3. Güvenlik kontrollerini uygulamak ve bu kontrollerin bilgi sistemi ve çalışma ortamındaki dağılımını belgelemek.
4. Kontrollerin doğru bir şekilde uygulanma derecesini belirlemek, güvenlik kontrollerini, amaca uygun şekilde çalışma ve sistemin güvenlik gereksinimlerini karşılama açısından değerlendirmek.
5. Bilgi sisteminin çalışmasına izin vermeden önce, bu sisteminin işletilmesinden doğacak riskin kabul edilebilir olduğuna karar vermek. Bunun için organizasyonlar, varlıklar, kişiler, diğer kuruluşlar ya da dış çevreler için risk oranları ve düzeyleri belirlemek.
6. Güvenlik kontrolünün etkinliğini değerlendirmek, sistem veya çalışma ortamındaki değişiklikleri belgelemek, ilgili değişikliklerin güvenlik etki analizlerini yapmak ve

sistemin güvenlik durumunu raporlamak da dâhil olmak üzere, bilgi sistemindeki güvenlik kontrollerini sürekli olarak izlemek ve değerlendirmek.

"Sıkı şifre ve hesap yönetimi politikalarını uygulayın" önerisiyle kurumlar kötü niyetli çalışan tehdidine karşı ne kadar dikkatli olursa olsun, kullanıcı hesaplarından taviz verilmesi durumunda, çalışanların saldırı önleme mekanizmalarından kaçabileceğine dikkat çekilmektedir. Kullanıcı hesabı ve parola yönetimi politikaları, çalışanların kuruluşun sistemlerini yasadışı amaçlarla kullanma becerilerini engellemek açısından kritik önem taşımaktadır. Doğru yapılandırılmış hesap yönetimi ile iyi belirlenmiş erişim kontrolü, kuruluşun tüm kritik elektronik varlıklarına erişimin güvenli olmasını sağlayacaktır.

İnt. Kyn. 53'e göre kötü niyetli çalışanların, özel hesapları veya gizli bilgileri ele geçirmek için kullandıkları bazı taktikler ise şunlardır:

• Sosyal mühendislik çalışması veya çalışanların açıkça şifrelerini paylaşması nedeniyle özel hesapların şifrelerini ele geçirme.

• Çalışanlar tarafından bilgisayarlarında veya e-postalarına kaydedilmiş, düz metin dosyası halinde saklanan şifreleri ele geçirme.

• Hesap isimlerini ve parolaları, yapışkan notlar, açıkta bırakılan kâğıtlar veya kolayca erişilebilen nesneler (klavye, telefon veya fare altlığı, ajandalar vs.) aracılığıyla ele geçirme.

• Yetkili kullanıcı oturumu açık bırakılmış bir bilgisayarı kullanarak şifreleri öğrenme.

• Şifre kırıcılar yardımıyla parolaları ele geçirme.

• Tuş vuruşlarını kaydeden uygulamalarla şifrelere ulaşma.

• Bir kullanıcının şifresini yazarken gözleme yoluyla parola öğrenme.

"Görev ayrımı yapın ve erişim yetkisini belirleyin" önerisi, görevlerin ayrılmasının, bir çalışanın diğer çalışanlarla işbirliği yapmadan bilgi çalmasını, dolandırıcılık veya sahtekârlık yapma olasılığını azaltmak üzere işlevlerin birden fazla kişiye dağıtılmasını içermektedir. Birçok organizasyon, iki kişi kuralını kullanmaktadır; bu kuralın başarılı bir şekilde uygulanabilmesi için bir işlem yerine getirilirken yetkili iki kişinin birlikte hareket etmesi gereklidir. Örneğin, veri kasasını açmak için farklı kişilerde bulunan iki anahtarın bir araya gelmesi gibi.

Kuruluşlar, görev ayrımını uygulamak için teknik veya teknik olmayan yöntemleri kullanabilirler. Örnek vermek gerekirse, iki banka yetkilisinin yüklü vezne ödemeleri

öncesinde ödeme işlemini onaylamaları gereklidir. Genel olarak, çalışanların başka bir çalışanla birlikte işlem yapması gerektiğinde, kötü niyetli eylemleri yapma eğilimleri azalmaktadır.

"Bulut hizmetleri için erişim kısıtlamaları ve izleme yetkileri konusunda güvenlik kuralları tanımlayın" önerisinde, bulut hizmetinin alındığı kurumlarla güvenlik konusunda güçlü anlaşmaların yapılmasına dikkat çekilmektedir.

Kuruluşlar hizmet aldıkları kurumun, bilgileri güvence altına alma sorumluluğunu üstlendiğini varsaymamalıdır. Bulut sağlayıcılarıyla, verileri güvenli bir şekilde depoladığı, ağa erişebilecek kullanıcıların ve yetkilerinin izlenebilmesi için gerekli kayıtların tutulduğu, hizmetin sonlanması durumunda da veri izlerinin akıbetinin ne olacağının belirlendiği yazılı bir anlaşmanın yapılması zorunludur.
Kuruluşlar için dört çeşit bulut hizmeti mevcuttur, her kuruluşun kendisine uygun olan hizmeti seçmesi önemli bir konudur.

1. Özel bulut (Yalnızca bir organizasyon için çalışır)
2. Bulut topluluğu (Çeşitli kuruluşlar tarafından paylaşılır)
3. Genel bulut (Herhangi bir müşteriye açıktır)
4. Melez bulut (Bağlı olan iki veya daha fazla bulut sahibi tarafından kullanılabilir)

"Sıkı erişim kontrolleri ve ayrıcalıklı kullanıcıları izleme politikaları oluşturun" önerisiyle tüm kullanıcıların işlem kayıtlarının tutulması konusuna dikkat çekilmektedir. Yapılan araştırmalara göre, sabotaj yapan kötü niyetli çalışanların çoğunluğu ile gizli veya kişiye özel bilgileri çalanların yarısından fazlası teknik görevlerde bulunmuştur. Kötü amaçlı eylemleri gerçekleştirmenin ve gizlemenin teknik olarak gelişmiş yöntemleri şunlardır:

• Script veya programları yazmak ya da indirmek
• Arka kapı hesapları oluşturmak
• Uzaktan sistem yönetim araçları kurmak
• Sistem günlüklerini değiştirmek
• Virüs yerleştirmek
• Şifre kırıcılarını kullanmak.

“Sistem değişikliğiyle ilgili uygulamaları kurallara bağlayın” önerisinde; bilgisayar ve ağ üzerindeki tüm değişikliklerin doğruluğunu, bütünlüğünü, yetkilendirilmesini ve belgelenmesini takip etmek üzere güvenlik kontrolü kurulması yer almaktadır. Mağdur örgütlerin, sistemlerinde yetkisiz değişiklik nedeniyle çok çeşitli sorunlar yaşamaları, değişim kontrollerinin daha güçlü yapılmasının gerekliliğini ortaya koymaktadır.

Sistem değişiklik denetimleri geliştirmek için kuruluşlar temel yazılım ve donanım yapılandırmalarını tanımlamalıdır. Bir kuruluş, farklı kullanıcıların farklı bilgi işlem ve bilgi ihtiyaçlarına göre (örneğin; muhasebeci, yönetici, programcı veya tasarımcı) farklı birkaç temel konfigürasyona sahip olabilmektedir. Kuruluşlar farklı konfigürasyonları tanımlamalı, donanım ve yazılım bileşenlerinin ayırt edici özelliklerini belirlemelidir.

“Çalışan eylemlerini izlemek için bir güvenlik bilgi ve olay yönetimi (SIEM) sistemi kullanın” önerisinde ise çalışanların eylemlerinin günlüğe kaydedilmesi ve olayların birbiriyle olan bağlantısının anlaşılabilmesi için bir uygulamadan yararlanılması tavsiye edilmektedir.

Çalışanların tüm çevrimiçi etkinliklerinin kayıt altına alınması, kuruluşu kötü niyetli etkinliklerden korumak için yeterli olmamaktadır. Olayları birbiriyle ilişkilendirmek, daha etkili uyarılar alınmasını ve daha iyi isabetli kararlar üretilmesini sağlayacaktır. Günlükler, düzenli ve rastgele bir incelemeye tabi tutulmadıkça anomaliler saptanamamaktadır; bu yüzden günlükler, anomalilerin tespiti ile değerli hale gelmektedir.

Bir görevlinin çok sayıda günlük dosyasını gözle incelemesini beklemek gerçekçi değildir. Bununla birlikte, sistemlerde anormal aktivitelerle ilgili ilâve bir güvenlik katmanı sağlamak için kayıt toplama ve korelasyon teknolojileri kullanılmaktadır. Tek bir kayıttan anlaşılamayacak bir saldırı örneğini diğer düzensiz faaliyetler aracılığıyla tanımlamak mümkün olabilmektedir.

“Mobil cihazlar da dâhil olmak üzere, tüm uç noktalardan yapılan uzaktan erişimi izleyin ve kontrol edin” önerisiyle, uzaktan erişimin kontrol altına alınmasına dikkat çekilmektedir. Kötü niyetli çalışanlar saldırmak için daha az dikkat çeken, uzaktan erişimi fırsat olarak görebilmektedirler.

Kuruluşlar, personellerinin, bir internet bağlantısının bulunduğu her yerde çalışabilmesini sağlayan mobil bir iş gücüne doğru ilerlemektedir. Bu aynı zamanda, daha fazla kullanıcının iletişim araçlarını kullanmasına ve kurumsal bilgi sistemlerine uzaktan erişmek üzere akıllı telefonlar, tabletler ve bilgisayarlar gibi ek teknolojilerden yararlanmasına izin verilmesi anlamına gelmektedir. Kuruluşlar, çalışanlarının kullandığı uzaktan erişim teknolojilerinden, örgüt içinde eriştikleri sistemlerden ve hangi verilere eriştiklerinden haberdar olmalıdır.

Dizüstü bilgisayarları, ev-iş istasyonları, tablet bilgisayarlar ve akıllı telefonlar uzaktan erişimi mümkün kılan teknolojiyi içermektedir.

Kötü niyetli çalışanlar, çoğu zaman kuruluş tarafından sağlanan meşru erişim hakkını kullanarak, gerek görevli iken gerekse işten ayrılma sonrasında kuruluşlara uzaktan saldırabilmektedir. Uzaktan erişim, çalışan verimliliğini büyük ölçüde artırmaktadır, ancak kritik verilere, süreçlere veya bilgi sistemlerine erişim konusunda dikkatli olunmalıdır. Çalışanlar, işyerindeki gibi, kötü niyetli eylemleri fiziksel olarak gözlemleyen birisi var olmadığı için kurum dışından kötü amaçlı faaliyetlerde bulunmanın daha kolay olacağını düşünebilirler.

“Kapsamlı bir çalışan işe son verme prosedürü geliştirin” önerisinde; kuruluşların, eski çalışanlardan zarar görme riskini azaltan bir fesih işlemi tavsiye edilmektedir. Fesih işlemleri, eski çalışanın hesaplarının kapanmasını, ekipmanının toplanmasını ve kalan personelin bilgilendirilmesini sağlamalıdır. Doğru hesap ve envanter yönetimi süreçleri, bir çalışanın şirketten ayrılması durumunda organizasyonun içeriden alınan tehdit riskini azaltmasına yardımcı olabilmektedir.

Bir çalışanın işten ayrılmasına hazırlanmak amacıyla kuruluşlar, çalışanın son gününden önce bir dizi işlem yürütmelidir. Kuruluşlar, fesih işleminin tüm yönlerini kapsayan politikalar ve prosedürler geliştirmelidir. Fesih kontrol listesi, bir çalışanın işten ayrılmadan önce tamamlanması gereken işlemlerin bitirilip bitirilmediğinin kuruluş tarafından izlenmesine yardımcı olmaktadır.

Fesih kontrol listesinde, en azından, çalışana verilmiş görevlerin tamamlanıp tamamlanmadığı, görev tamamlanmamışsa görevin tamamlanması hususunu kimin

kontrol edeceği, görevi tamamlaması gereken kişinin isim ve imza satırı bulunmalıdır. Tamamlanan kontrol listesi, çalışan kuruluştan çıkmadan önce İK'na teslim edilmelidir.

"Güvenli yedekleme ve kurtarma süreçlerini uygulayın" önerisinde herhangi bir veri kaybı durumundaki kurtarma süreçlerine dikkat çekilmektedir. Bir organizasyonun tüm önlemlerine rağmen, içeriden birinin kuruma saldırması yine de mümkündür. Kuruluşlar bu gibi durumlar için hazırlanmalı, güvenli yedekleme ve kurtarma süreçlerini uygulayarak, bu süreçleri ve alınan yedeklerin doğruluğunu periyodik olarak test etmelidir.

Önleme, kötü niyetli çalışanların saldırılarına karşı ilk savunma hattı olarak bilinmektedir. Bu tür çalışanlar yine de sistemin güvenliğini aşmanın yollarını bulabilmektedirler. Kurumlar, etkili bir yedekleme ve kurtarma işlemini planlamalı ve işletmeye başlamalıdır. Böylece sistem güvenliğinin aşılması durumunda, faaliyetler en kısa sürede tekrar başlayabilecektir. Etkin yedekleme ve kurtarma mekanizmaları, kurumlara aşağıdaki avantajları sağlamaktadır:

• Yedek verilerden yararlanarak sistemi yeniden ayağa kaldırma süresi günlerce sürmek yerine, birkaç saate indirilebilmektedir.
• Mevcut yedekleme olmadığında uzun sürecek elle veri girişi yapma yükü ortadan kalkmaktadır.
• Yedeği bulunmayan bilgileri yeniden oluşturmak için gereken süre azalmaktadır.
• Veri kaybı nedeniyle yaşanacak itibar kayıplarının önüne geçilmektedir.

Yedekleme ve kurtarma stratejilerinde aşağıdaki hususlara dikkat edilmesi veri güvenliğinin artırılmasına yardımcı olabilir:
• Yedek depolama alanına kontrollü erişim.
• Fiziksel ortama kontrollü erişim (örneğin hiç kimse hem çevrimiçi verilere hem de fiziksel yedekleme ortamına erişmemelidir).
• Yedekleme işleminde değişiklikler yapıldığında, görevler ayrılmış olmalı ve "iki kişi" kuralı mutlaka uygulanmalıdır.
• Yedekleme ve kurtarma yöneticilerinin görevleri birbirinden ayrılmalıdır.

“Kötü Niyetli Çalışan Tehditleri programı geliştirin” önerisinde, kuruluşların art niyetli çalışan tehdidine özel dikkat göstermesi gerektiği ifade edilmektedir. Kötü niyetli çalışanlar, kuruluşların işgücüne verdiği güveni, yasadışı faaliyetlerini gizlemek için kullanarak kuruluşu savunmasız bırakabilmektedir.

Kuruluşlar; orantılı ve dikkatli bir tutuma, kötü niyetli çalışanların tehditlerini başarılı bir şekilde tespit edebilir, önleyebilir ve bunlara karşı harekete geçebilir. Kötü niyetli çalışanların, bilgi çalma eylemlerini önlemek amacıyla bir süreç geliştirmek için vakit kaybedilmemelidir.

Bir olay meydana geldiğinde, süreç önceki olaylardan edinilen tecrübelere göre uygun şekilde güncellenip yönetilmelidir. Kötü niyetli çalışan tehditleri programı, vizyonu belirlenmiş, görev ve sorumluluk çerçevesi iyi çizilmiş, kurumsal çapta bir program olmalıdır. Programa katılan tüm bireylerin uzmanlık eğitimleri almaları gereklidir. Program, soruşturmalar yapmak, araştırmacılarla temasta olmak ve kovuşturma talebinde bulunmak için ölçü ve ölçütlere sahip olmalıdır.

Soruşturmaların, mahremiyet ve gizliliği sağlamak üzere kontrol edilmesi, grubun güvenilirliğini artıracaktır. En önemlisi, programın başarılı olabilmesi için mutlaka yönetimin desteğini alması gerekmektedir.

“Normal ağ davranışları için ölçütler oluşturun” önerisinde ise her organizasyonun bant genişliği kullanımı, kullanım biçimleri ve protokolleri gibi özellikleri belirlemek üzere objektif ölçütler konulması anlamına gelmektedir. Bu kriterler, normal ağ davranışında yaşanan sapmalar, içeriden gelen tehditler de dâhil olmak üzere olası güvenlik olaylarını izleme ve önlemede etkili olacaktır.

Bununla birlikte, BT yöneticilerinin ağdaki sorunları daha kolay anlayabilmesi için görsel raporlar verebilen araçlardan yararlanmaları uygun olacaktır. Çeşitli araçlar ve yazılım paketleri, ağ sistemleri hakkında bilgi toplamakta ve bir ağ topolojisi geliştirmesine yardımcı olmaktadır.

İzlenecek temel veri noktaları şunları içermelidir:

• Cihazlar arasındaki iletişim:

- Bir iş istasyonu ile iletişim kuran cihazlar. Bunlar yapılandırmaya, departmana ve yere bağlı olarak değişir, ancak belirli bir iş istasyonu yalnızca önceden belirlenmiş bir sunucu grubu ile iletişim kurmalıdır.
- Bir sunucunun iletişim kurduğu aygıtlar. Bunlar yapılandırmaya, departmana ve yere bağlı olarak değişir; ancak belirli bir sunucu yalnızca önceden belirlenmiş bir aygıt grubuyla iletişim kurmalıdır.
- Tüketilen bant genişliği. Çalışma saatleri boyunca ve sonrasında bant genişliği kullanımı arasındaki farkları göz önünde bulundurmak gerekir.

• Sanal özel ağ (VPN) kullanıcıları:

- Erişim zamanı
- Tüketilen bant genişliği
- Kaynak IP adresleri ve coğrafi konum bilgileri
- Kullanılan kaynaklar

• Portlar ve protokoller

• Normal güvenlik duvarı ve IDS uyarıları: Normal uyarılar, iş süreçleri değiştiğinde ortaya çıkmaktadır (Ör. Web sitesi trafiğinin artması).

“Sosyal medya konusunda özellikle dikkatli olun” önerisinde, çalışanların sosyal medya kullanımlarına karşı dikkatli olunması tavsiye edilmektedir.

Sosyal medya sitelerinde kullanılan içerikler, kasten veya istemeden kuruluşların bilgi sistemlerini ve verilerini tehdit edebilmektedir.

Kuruluşlar; çalışanlar, iş ortakları ve yüklenicilerin sosyal medyayı nasıl kullanmaları gerektiği konusunda eğitim, politika ve prosedürler oluşturmalıdır.

Sosyal medya siteleri, insanlara kendilerini kolayca ifade edebilecekleri ve bilgi paylaşımı yapabilecekleri bir ortam sunmaktadır. Kişilerin özel yaşamlarından iş dünyası üyeliklerine ve hobilerine kadar her konuda bilgi, bir kullanıcının sosyal medya profilinden veya herhangi bir popüler arama motoru yardımıyla rahatça elde edilebilmektedir.

Bu bilgiler, çalışanları olası sosyal mühendislik girişimlerine açık hale getirmektedir. Sosyal ağlar, bir organizasyon içinde, kimin içeriden gerçekleştirilecek bir saldırıya daha yatkın veya istekli olabileceğini belirlemek için de kullanılabilmektedir.

Örneğin, sosyal paylaşım sitelerine katılan bir çalışan kendi işi veya şirketi hakkında olumsuz yorumlar yayınlarsa, saldırganlar bunu, çalışanın hoşnutsuzluğunun ve muhtemelen kötü niyetli çalışan saldırısında bulunmaya açık olduğunun bir işareti olarak değerlendirebilir.

Saldırganlar, bir kuruluşun personel yapısını haritalamak ve daha sonra hedefli saldırılarda bulunmak için yüksek değerli (C düzeyinde yöneticiler, finansal personel vb.) çalışanları belirlemek için bu siteleri kullanılabilmektedir.

"Verilerin kuruluş dışına yetkisiz çıkarılmasına açık kapı bırakmayın" önerisiyle, kuruluşların bilgi sistemlerinin veri sızıntısına karşı savunmasız olduklarından hareketle riskleri azaltma stratejilerini uygulamak gerektiğine atıfta bulunulmaktadır.

Bilgi sistemleri, USB bellek sürücüleri, yazıcılar ya da hafızası bulunan çıktı birimleri gibi harici birçok donanımı ve e-posta gibi yazılımları kullanmaktadır. Her cihaz türü, beraberinde veri sızıntısıyla ilgili sorunları da taşımaktadır. Söz konusu tedbirlerde bu tür donanımların göz ardı edilmemesi önerilmektedir.

Hassas bilgilerin sızdırılması riskini azaltmak için, verilerin nerede ve nasıl depolanabileceği bilinmelidir. Çalışanların, kötü niyetli veya istemeden veri çıkarma riskini azaltmak için kuruluşlar veri çıkış noktalarını tespit etmeli ve gerekli tedbirleri almalıdır.

Birçok teknoloji ve hizmet, veri çıkış noktası haline gelebileceğinden, bir kuruluş kendi sistemine bağlanan tüm cihazların yanı sıra sistemlerine gelen tüm fiziksel ve kablosuz bağlantıları göz önüne almalıdır.
Bilgilerin kuruluş dışarısına çıkarılmasında kullanılan araçlar ve yöntemlerden bazıları şunlardır:

- Bluetooth
  - Kablosuz dosya aktarımları
- Taşınabilir medya
  - USB flaş bellekler
  - CD ve DVD'ler
  - Hafızalı ve akıllı telefonlar
  - Medya kartları (kompakt flaş, SD kartları, vb.)
  - Veri saklama özelliğine sahip projektörler
  - Kameralar ve video kayıt cihazları
  - USB sürücüler (flaşsız)
  - Mikrofonlar
  - Web kameraları
- Veri iletim noktaları
  - İnternet bağlantısı
  - Güvenilir iş ortaklarıyla bağlantılar
- İnternet hizmetleri
  - FTP, SFTP, SSH
  - Anlık mesajlaşma ve internet sohbeti (GChat, Facebook Sohbet vb.)
  - Bulut hizmetleri (çevrimiçi depolama, e-posta vb.)
- Yazıcılar, faks makineleri, fotokopi makineleri ve tarayıcılar.

Verilerin haklı bir sebeple kurum dışına çıkarılması gerektiği durumlar için "veri aktarım prosedürü" oluşturulmalıdır. Bu prosedür, kullanıcının yapılan iş gereği sistemden kopyalanması gereken dosyaları tanımlamasıyla başlamalıdır.

Kullanıcı tarafından, dosya adları, dosyaların yeri, transferin nedeni, verinin kime ait olduğu, verinin önem derecesi ve istekte bulunanın imzasını listeleyen bir veri aktarım formu doldurulur. Çalışanın formu doldurmasının ardından, yönetici, dosyaların istek ve içeriğini gözden geçirir ve aktarımı onaylar veya geri çevirir. Ardından, veri sahibi isteği inceler ve aktarıma onay verir veya reddeder. İki aşamalı onay sonrasında, istenen dosya, iş birimi tarafından, dış kayıt ortamına aktarılır ve güvenirliği teyit edilmiş çalışana teslim edilir.

Bu işlem, birden fazla kişi tarafından USB flaş sürücülere erişim gereksinimini ortadan kaldırmakta ve sistemden çıkarılan verileri denetlemenin bir yolunu oluşturmaktadır.

Çalışanlar kullandıkları verileri dışarı çıkarmak için veri aktarım prosedürünü uygulamak yerine, e-posta veya bulut hizmetleri gibi çevrimiçi araçlara yönelebilmektedir. Bu nedenle, verileri filtrelemek ve bu tür çıkış noktalarında DLP yöntemini kullanmak gibi önlemler alınmalıdır.

Bilgisayar korsanlığı sonucunda elde edilen bilgi sızıntılarının yüzde 80'i çalışanların bilgi güvenliği politikasını bilmemesinden kaynaklanmaktadır (Oğuz ve Cevahir 2010). Kurumlar için en kritik varlık olan bilgi ise sadece bilgi teknolojileri aracılığıyla işlenmemekte, birçok farklı noktada kritik bilgiler bulunabilmektedir.

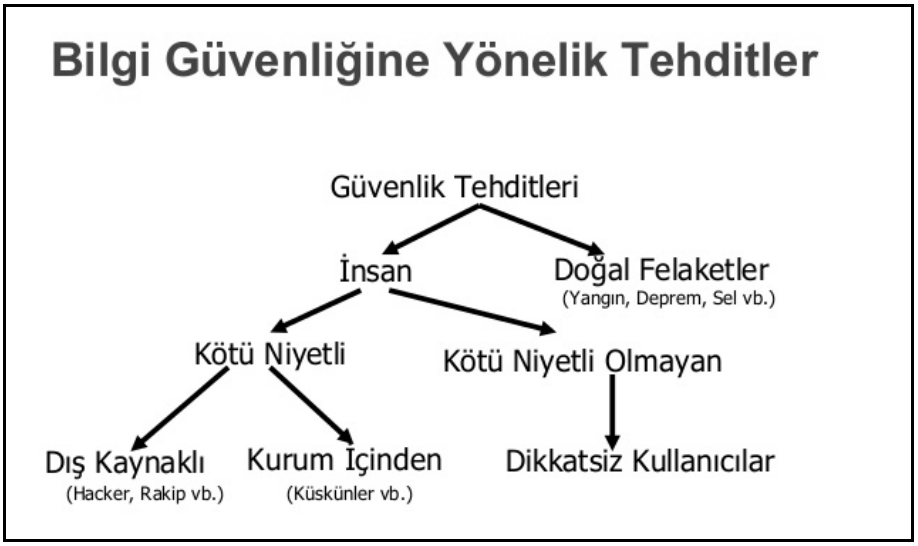
Bu sebeple bilgi güvenliği denilince akla sadece bilişim alt yapısı ve onun güvenliği gelmemelidir. Kurumsal olarak tüm birimleri kapsayan bir güvenlik politikası oluşturulmalıdır (Alagöz ve Allahverdi 2011).

Bilginin kolay işlenebilmesi amacıyla dijital ortama taşınması, beraberinde birçok güvenlik riskini de getirmektedir. Kâğıda basılı halde tutulan bilgilerin, dijital ortamlarda depolanan verilere göre, meraklı gözlerden daha güvende olduğuna şüphe yoktur.

Basılı gizli belgelerin bulunduğu ortama yabancı kişilerin girişi engellendiğinde temel güvenlik sağlanabilirken, dijital ortamda tutulan bilgilere; bırakın aynı odada olmayı, aynı şehirde ya da aynı ülkede olmadan bile erişilebilir, bu bilgiler kopyalanabilir, değiştirilebilir, hatta yok edilebilir. Bilginin güvenliği bu kadar saldırıya açık durumdaysa alınacak tedbirler de elbette bir o kadar çok ve ayrıntılı olmak zorundadır.

Bilgi işleme teknolojilerindeki hızlı gelişmeler; bilgilerine yönelik tehditleri de her geçen gün artırmaktadır. Buna karşın geçerliliği uluslararası kurum ve kuruluşlarca kabul edilmiş ve halen geliştirilmeye devam eden; ISO 27001, ISO 27005, COBIT, PCI, SOX ve BASEL II gibi standartlar ve kurallar risk yönetimini zorunlu tutmaktadır (Şahinaslan vd. 2010).

Güvenlik standartlarında ifade edildiği gibi, bilgi güvenliğine yönelik tehditler Şekil 4.26'da da görüldüğü üzere, öncelikle insani ve doğal afetler olarak iki gruba ayrılmaktadır. İnsan faktörü de kötü niyetli olanlar ve olmayanlar olarak iki gruba ayrılabilir. Kötü niyetli olmayanlar dikkatsiz kullanıcılar olarak tanımlanırken, eğitim ile bu sorunun aşılabileceği düşünülmektedir. Kötü niyetli kullanıcılar ise kurum içinden ve dış kaynaklı olarak iki gruba ayrılmaktadır.



Şekil 4.27 Bilgi güvenliğine yönelik tehditler (İnt. Kyn. 46).

4.4.1 ISO 27001 Bilgi Güvenliği Yönetim Sistemi

ISO 27001 Bilgi Güvenliği Yönetim Sistemi, bir standartlar dizgesi olup ilk kez 1995 yılında İngiltere'de hazırlanan BS (British Standarts) 7799 isimli standart üzerine kurulmuştur ve zaman içerisinde güncellemeler geçirmiştir. 1998 yılında "Part 2" olarak yayınlanan sürümü ISO/IEC tarafından geliştirilerek ISO 27001 sürümüne evrilirken, "Part 1" ISO 27002 olarak uluslararası kullanıma sunulmuştur (İnt. Kyn. 58).

ISO 27001, kurumsal bilgi varlıklarının tamamının incelenerek bu bilgilere yönelik risklerin analizinin yapılmasını gerekli tutmaktadır (İnt. Kyn. 7). ISO 27002 ise bilgi güvenliği sürecinde alınması gereken tedbirleri içeren bir kurallar bütünü olarak tanımlanmaktadır (İnt. Kyn. 8).

Ülkemizde Avrupa Birliği Uyum Kriterleri ile gündeme gelen Bilgi Güvenliği Yönetim Sistemi standartları, Türk Standartları Enstitüsü (TSE) tarafından; ISO/IEC 27001

“Bilgi Güvenliği Yönetim Sistemi” standardı olarak tanımlanmış olup gerekli koşulları sağlayan kurum ve kuruluşlar belgelendirilmektedir (Vural ve Sağıroğlu 2008).

ISO 27001’e göre “Bilgi, bir kurumun en önemli değerlerinden biridir ve sürekli korunması gerekir”. Bu bağlamda bilginin güvenliği için bazı hususlara dikkat etmek gerekmektedir. Bilgi güvenliği; bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması olarak tanımlanmaktadır. Bir başka deyişle gizlilik, bütünlük ve erişilebilirlik, bilgi güvenliğinin temel taşı olarak değerlendirilmektedir (Doğantimur 2009).

Gizlilik (Confidentiality): Erişme yetkisi olmayanlar tarafından bilgiye erişilememesidir.
Bütünlük (Integrity): Bilginin değiştirilmediğinin ve hiçbir kısmının silinmediğinin yani tam olduğunun teyit edilmesidir.
Erişilebilirlik (Availability): Erişim yetkisi bulunanların, istedikleri anda bilgiye ulaşabilmeleridir.

Bilgi güvenliği, bu üç özelliğin bir arada, ayrılmaz bir bütün olarak sağlanması olarak düşünülmektedir. “Erişilebilirlik” gizli bilgilere istenildiği anda, belirli güvenlik kontrollerinden geçen kullanıcıların erişmesine izin verirken, “Gizlilik” erişim yetkisi olmayanların gizli belgelere erişimini engellemektedir. “Bütünlük” ise erişilen bilgilerin eksik olmadığının ya da değiştirilmediğinin güvencesini vermektedir (Doğantimur 2009).

Bilgiler; üretim, iletim, işleme veya depolama sırasında çok farklı ortamlarda bulunabilmektedir. Kurumlar çalışanlarına hangi bilgilerin hangi tür ortamlarda bulunacağı konusunda bilgilendirmede bulunmalıdır. Bilgilerin yer alabileceği ortamlar şunlardır:

• **Fiziksel ortamlar:** Basılı evraklar, çalışma panoları, fakslar, çöp kutuları, dolaplar vs.
• **Elektronik ortamlar:** Bilgisayarlar, sunucular, mobil cihazlar, diskler, disketler, e-postalar, hafıza kartları, CD/DVD vb. manyetik ortamlar.
• **Sosyal ortamlar:** Arkadaş grupları, telefon görüşmeleri, toplu taşıma araçları gibi ortamlarda yapılan sosyal aktiviteler.

• **Tanıtım platformları:** Web siteleri, sunular, tanıtım videoları, broşürler, reklamlar gibi görsel ortamlar.

Yeterli güvenlik tedbirleri alınmadığı ve kritik bilgilerin güvenliği sağlanamadığı takdirde;

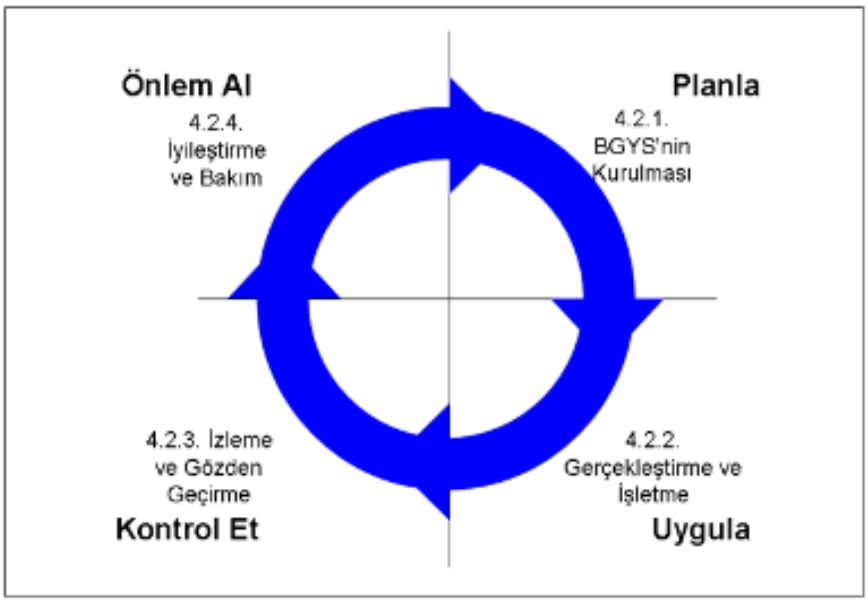
- Mağduriyetlerin yaşanması.
- Kaynakların tüketilmesi,
- İşin yavaşlaması ya da tamamen durması,
- Kurumsal imaj kaybı,
- Üçüncü şahıslara yapılacak olan saldırıların mesuliyeti gibi zararların ortaya çıkması

söz konusu olmaktadır.

ISO/IEC 27001 ve ISO/IEC 27002 standartlarında PUKÖ (Planla - Uygula - Kontrol et - Önlem al) modeli uygulanmaktadır. Marttin and Pehlivan (2010)'a göre bu modelde:

- Planla: BGYS'nin kurulması için gereken; güvenlik politikaları, amaçlar, hedefler, süreçler ve prosedürlerin belirlenmesi aşamasıdır.
- Uygula: BGYS'nin işletilmesi yani politika, kontrol, süreç ve proseslerin uygulanmasıdır.
- Kontrol et: BGYS'nin kontrol edilme sürecidir. Bu aşamada BGYS'nin değerlendirilmesi, performans ölçümlerinin yapılması ve bu sonuçların bir rapor haline dönüştürülmesi sürecidir.
- Önlem al: BGYS'nin işletilmesine devam edilebilmesi için gerekli hazırlıkların yapıldığı, yönetim tarafından yapılan kontrollerin sonuçlarına göre düzeltici ve önleyici tedbirlerin alındığı süreçtir.

Kesintisiz bir süreç olması nedeniyle bilginin BGYS'de sürekli bir döngü içerisinde bulunması gerekmektedir. PUKÖ modeli BGYS'nin sürekli bir döngü içerisinde nelerin yapılacağına karar verilmesini, verilen kararın uygulanmasını, çıktının kontrol edilmesini ve eksik ya da hatalı sonuçların giderilerek iyileştirilmiş işleyişin devreye alınmasını hedeflemiş bir modeldir. (Marttin ve Pehlivan 2010)



Şekil 4.28 PUKÖ - Planla, Uygula, Kontrol et, Önlem al döngüsü (Marttin ve Pehlivan 2010).

4.4.2 Veri Sızıntısı Engelleme (DLP) Yazılımları

Sosyal yaşamda mobilitenin artmasıyla birlikte, günümüzde veriler daha önce hiç olmadığı kadar hareket halindedir. Bu hareket, geçmişte şan şöhret gibi sebeplerle motive olan bilgisayar korsanlarının itici gücü, özellikle finansal sebeplere dönüşmesi nedeniyle parlak hedefi haline gelmiştir. Hedeflerin bireysel, kurumsal veya ulusal olması korsanlar açısından para miktarından dışında bir farklılık arz etmediği için günümüzde veri sızıntılarını engellemek, hedefler açısından ciddi bir sorun olmaya devam etmektedir.

Verileri sızdırmayı amaçlayanlar sadece bilgisayar korsanları değildir. Birçok devletin istihbarat örgütleri yerli-yabancı kurumların gizli bilgilerini ele geçirmeyi amaçlayan çalışmalarda bulunmaktadır. WikiLeaks'in 7 Mart 2017'de açıkladığı 8 bin civarındaki belgede, ABD istihbarat örgütü CIA'in akıllı telefonların ve televizyonların mikrofon özelliklerini kullanarak ortam dinlemesi yapabildiği ve bu cihazların kameralarından görüntü alabildiğine ilişkin bilgiler yayınlanmıştır.

Yayınlanan belgelere göre CIA'in yazılım açıklarını kullanarak, Android, iOS ve Windows tabanlı telefonlardaki belgelere erişebildiği, ayrıca Windows, MacOS ve Linux işletim sistemine sahip bilgisayarlara da sızabildiği ortaya konulmuştur. Belgelere göre CIA'in, devlet imkânlarının sağlamış olduğu büyük avantajları da

kullanarak tespit ettiği güvenlik açıklarını muhatap kurumlara bildirmediği, bu açıkların bilgisayar korsanlarının da eline geçmesi halinde çok ciddi güvenlik sorunlarının ortaya çıkacağı düşünülmektedir (İnt. Kyn. 21).

"Veri Sızıntısı" (Data Loss) olarak da adlandırılan olayın engellenebilmesi yani bilgi güvenliğinin sağlanabilmesi amacıyla hazırlanmış çözümler bulunmaktadır. Bu çözümlere farklı özellikleri nedeniyle ya da çeşitli nedenlerle aşağıdaki gibi değişik isimler verilmiştir (Kanagasingham 2008):

- İçerik İzleme ve Filtreleme - Content Monitoring and Filtering (CMF)
- Veri Kaybı Önleme - Data Loss Prevention (DLP)
- Veri Sızıntısı Önleme - Data Leak Prevention (DLP)
- Çıkarma Önleme Sistemi - Extrusion Prevention System (EPS)
- Bilgi Sızıntısı Önleme - Information Leak Prevention (ILP)
- Bilgi Kaçak Tespiti ve Önleme - Information Leak Detection and Prevention (ILDP)
- Bilginin Korunması ve Kontrolü - Information Protection and Control (IPC)

Farklı isimler verilse de yapılan işin türü dikkate alınarak bu ürünlerin tümüne genel olarak Veri Sızıntısı Engelleme (Data Loss Prevention - DLP) adı verilmektedir. DLP çözümleri genel olarak kritiklik düzeyi daha önceden tanımlanmış olan verileri; ağ kullanımında, manyetik ortamlarda veya veri tabanları üzerindeyken izlemek amacıyla, daha önceden belirlenen kurallara göre koruma görevini yerine getirecek donanım ve yazılımlardan oluşan sistemler olarak tanımlanmaktadır (Kanagasingham 2008).

DLP sistemlerinin geliştirilmesinde ve ticari olarak pazarlanmasında önemli etkenlerden birisi, kurumların sahip olduğu gizli belgelerin sızdırılmasından kaynaklanacak yasal sorumluluklardır. Bununla birlikte, her kurum, içerisinde bulunduğu sektörün düzenleyici kurumları tarafından veri güvenliğini sağlama konusunda zorunlu tutulabilmektedir. Finans sektöründeki GLBA, BASEL II ve PCI (Payment Card Industry) Standartları veya sağlık sektöründe HIPAA gibi mevzuat örnek olarak gösterilebilir.

DLP yazılımlarıyla korunmakta olan kurumda gizli bilgileri dışarı sızdırmak isteyen bir çalışan, gizli bir belgeyi e-posta aracılığıyla kurum dışına çıkarmak istediğinde istem ağ geçidindeki protokolleri geçemeyecek ve bu teşebbüs sistem kayıtlarına işlenecektir.

Yine benzer şekilde, anlık mesajlaşma programları (MSN, Skype vb.) aracılığı ile bilgi çıkarma girişimi olduğunda ağ geçidi üzerinden bilginin çıkışına izin verilmeyecek ve bu girişim sistem kayıtlarına işlenecektir. Ağ üzerinden gizli belgeyi dışarı çıkaramayan çalışan, USB bellek, CD/DVD gibi medyalar aracılığı ile bunu denediğinde, yine DLP yazılımı sayesinde engellenerek, sistem kayıtlarına işlenecektir.

Bu kez gizli belgenin bir bölümünü yeni bir belgeye kopyalayarak dışarı çıkarmak istediğinde de DLP devreye girerek sızıntının oluşmasını engelleyecektir. Çünkü DLP çözümleri, belgelerin içeriğini de etiketlediği için gizli belgenin bir bölümü yeni oluşturulmuş bir dosyada olsa bile sistem, sızıntıyı fark ederek engelleyecektir. Kimlik numaraları ya da kredi kartı numaraları gibi belirli bir örüntüye sahip bilgiler de DLP yazılımları sayesinde sızıntılara karşı koruma altına alınabilmektedir.

Ancak bu kadar güvenilir sistemin zayıf bir yönü de bulunmaktadır. DLP sistemleri belirli örüntüyü ya da daha önceden tanımlanmış belgeleri ve içeriğini tanıyabilirken, çalışanın bilgileri kendi cümleleriyle ifade ettiği ya da tahrif ederek sızdırmak istediğinde sistem başarısız olabilmektedir.

Bu gibi durumlar için veri madenciliği yöntemleriyle desteklenmiş DLP sistemlerinin zayıf yönleri kapatılabilmektedir (İnt. Kyn. 43).

5. TARTIŞMA VE SONUÇ

Gizli belge yayıncılığının son yıllarda artmasının farklı sebepleri bulunmaktadır. Çalışanlar veya eski çalışanlar kurumların uygulamalarından duydukları vicdani rahatsızlıklar nedeniyle veya ekonomik çıkar elde etmeyi amaçlayarak gizli bilgileri ifşa etmektedir.

Vicdani sebeplerle yapılan ifşalar çeşitli sebeplerle kısmen de olsa mazur görülebilmektedir. Ancak ifşalar, bazı kritik görevlilerin veya masum vatandaşların kimliklerinin ya da gizli bilgilerinin ortaya çıkması gibi olumsuz durumlara da sebep olabilmektedir. Kurumların kendi iç bünyelerinde kuracakları kontrol mekanizmalarıyla vicdani sebeplerle kurum dışına yapılacak gizli bilgi ifşaları büyük ölçüde engellenebilmektedir.

Problemin çok daha ciddi olan boyutu ise vicdani bir durum olmadan, tehdit, şantaj veya rüşvet karşılığı yapılan art niyetli bilgi ifşalarıdır. Bu tür ifşalar genelde kurumun mevcut ya da eski çalışanları tarafından yani içeriden yapılan saldırılarla gerçekleştirilmektedir.

Gizli belge yayıncılığında belgelerin ele geçirilmesinde uygulanan bir başka yöntem ise kurum dışından yapılan ve siber korsanlık olarak da adlandırılan, sistemlerde bulunan açıkların veya zafiyetlerin istismar edilmesidir. Bilişim alt yapısındaki donanım ve yazılım zafiyetlerinin, gizli bilgilerin kurum dışına sızdırılmasında önemli rolü bulunmaktadır.

Küresel bilgi ifşaları incelendiğinde sızıntı kaynakları belirtilmemiştir. Fakat medyaya yansıyan önemli sızıntıların kurum çalışanları tarafından yapıldığı, bir kısmının ise bilgisayar korsanlarınca dışarıdan yapılan saldırılar neticesinde elde edildikleri görülmektedir. Elde edilen gizli belgelerin yayınlanmasında da farklı yöntemler bulunmaktadır.

WikiLeaks örneğine bakıldığında, bilgilerin hükümetler tarafından sansürlenmemesi için P2P ağlar dâhil olmak üzere, dosya paylaşımında yararlanılan birçok tekniğin kullanıldığı görülmektedir. Belgelerin yayınlanmasından önce incelenmesi ve kritik bazı

bilgilerin kapatılması amacıyla (isimler, kimlik numaraları vs.) gönüllülere ve ifşa amacıyla kamuya açılmasında MediaWiki yapısının kullanıldığı görülmektedir.

Elde edilen gizli belgelerin elektronik ortamda sorgulanabilmesi için veriler önce OCR yazılımlarıyla tarama işleminden geçirilmekte, sonrasında ise bir veri tabanına aktarılmaktadır.

Panama Belgeleri örneğinde ise gazetecilerin iletişimi için bir tür sosyal medya programı olan Oxwall isimli yazılım kullanılmıştır. Gelişmiş sorgulamalarda kullanmak üzere imaj haldeki dokümanların taranması için OCR yazılımları (Apache Tika ve Tesseract) ve bunların kurulu olduğu sunucular kullanılmıştır. Sorgulama yapabilmek için Apache Solr isimli bir belge arama yazılımından da yararlanılmıştır. Project Blacklight ise sorgulama arayüzünde kullanılmıştır.

Belgelerin tamamının tek bir veri tabanında birleştirilmesi için Microsoft SQL yazılımından yararlanılmıştır. Veri tabanındaki veriler ile taranan belgelerdeki veriler birleştirilerek OffshoreLeaks isimli yeni bir veri tabanı oluşturulmuştur. Daha sonra SQL üzerindeki bu veri tabanı yine açık kaynak kodlu bir yazılım olan Talend yardımıyla Neo4j veri tabanına dönüştürülmüştür.

Grafiksel ilişkilendirme için Neo4j isimli veri tabanı kullanılmıştır. Raporlama ve görselleştirme aracı olarak ise Linkurious isimli yazılım kullanılmıştır. Oluşturulan grafiksel veri tabanı 950 bin düğüm ve 1.2 milyon kenara sahip 4 GB büyüklüğündedir.

WikiLeaks ve ICIJ ifşada bulunmak isteyenlere web sitesi üzerinde özel bir giriş alanı tanımlamıştır. Her iki kuruluşun sayfasındaki bu alanlara erişebilmek için TOR tarayıcısını kullanmak gerekmektedir. WikiLeaks büyük boyutlarda dosya yüklemek gerektiğinde; ifşacıyı, anonim dosya yükleyici bir siteye yönlendirmektedir.

Her iki örnekte de ifşa edilen verilere, özel bir yazılıma gerek duymadan bir internet tarayıcısı ile erişilebilmektedir. Ancak bazı ülkelerde bu sitelere erişim engellenmektedir. Bu ülkelerden erişim sağlayabilmek için VPN türünde yazılımlar ya da TOR tarayıcısı kullanmak gerekmektedir.

Wikileaks ve Panama Belgelerinin yayınlanmasına kadar olan süreçte kullanılan teknolojiler ile kullanılan sunucu teknolojisi Çizelge 4.5'de görüldüğü gibidir. Söz konusu teknolojiler zaman içerisinde değiştirilmekte ya da güncellenmektedir.

Çizelge 5.1 WikiLeaks ve Panama Belgeleri'nde kullanılan teknolojiler.

	WikiLeaks	*Panama Belgeleri*
İşletim sistemi	Tails	Tails
Tarayıcı	TOR anonim ağı	TOR anonim ağı
Sızıntı aracı	Web form	Securedrop
Şifreleme	PGP	GPG
Gönüllü iletişimi	Mediawiki (Web 2.0)	Oxwall (Web 2.0)
Protokol	https	https
OCR	Bilinmiyor	Apachetika / Tesseract
Veri tabanı	Bilinmiyor	Neo4j
Sunucu	nginx	CloudFront
Sunucu Konumu	Norveç/Hollanda/Rusya	A.B.D.

Küresel bilgi ifşalarından WikiLeaks ve Panama Belgeleri örnekleri incelendiğinde önemli bilgi ifşalarında bilgi kaynağının, kurum veya kuruluş çalışanları olduğu, ancak bazı ifşaların ise kurum dışından bilgisayar korsanlığı yöntemlerine dayandığı görülmektedir. Bu durum bilgi güvenliğinin hem kurum içinden hem de kurum dışından gelebilecek saldırılar dikkate alınarak yapılandırılmasının önemini ortaya koymaktadır.

Bilgi güvenliği ortam dinlemesinden iletişim dinlemesine, basılı evrak sızıntısından elektronik belge sızıntısına kadar kritik bilginin bulunduğu her ortam düşünülerek yapılandırılmalıdır.

Teknolojinin sürekli gelişmesi, kullanılan cihazların akıllanması ve internete bağlanabilir olması, bilgi ifşalarının boyutunu artırmıştır. Kurum ve kuruluşlar bilgi ifşaları gerçekleştirilmeden tedbirlerini almalı, örgütsel etik ortamını oluşturarak, vicdanları yaralayıcı olaylar yaşansa bile, bunları içsel bilgi ifşası yoluyla çözüme kavuşturarak dışsal bilgi ifşasının oluşmasını engellemelidir.

Kurumların öncelikli görevi, kişisel ya da örgütsel çıkarlar değil, kamu yararı olmalıdır. Kurumlar, örgütsel yapılarını ve etik iklimini kamu yararını göz önüne alarak kurduklarında; bunun güvenlik, sağlık, ekonomi ve çevre yönünden etkileri olumlu yönde artacaktır. Bu sayede bilgi ifşalarının vicdani sebeplerle gerçekleşmesi engellenebilecektir.

İster vicdani sebeplerle, isterse korsan yöntemlerle yapılsın, bilgi bir kez ifşa edildiğinde bunun yayılmasını engellemek neredeyse imkânsızdır. Küresel bilgi ifşaları örneği incelendiğinde yüksek teknolojiye sahip birçok devlet ve kurum ifşa edilen bilgilerin yayılmasını durdurmayı başaramamıştır. Bu sebeple hassas bilgilerin ele geçirilmemesi için bunların çok ciddi bir şekilde korunması gerekmektedir.

Bilgi ifşalarını önlemek üzere kurum içerisinde bilişim güvenliği politikaları oluşturulmalı, kurum için en uygun BGYS standartları sağlanmalıdır. Politikalar günün şartlarına göre sürekli olarak güncellenmeli, tespit edilen eksiklikler tamamlanmalıdır. Sistem içerisinde bulunan tüm yazılımların güncellemeleri eksiksiz yapılmalı, kırık lisanslı yazılımlardan kaçınılmalıdır.

Kuruma yapılacak saldırılarda kritik bilgilerin illegal kopyalanması, silinmesi ya da değiştirilmesi gibi istenmeyen durumlar için DLP çözümleri konumlandırılmalı, gerekli politikaların doğru bir şekilde yapılandırılması sağlanmalıdır.

Bilişim donanımları üzerinde mutlaka güvenilir bir antivirüs yazılımı kurulmalı, antivirüs politikaları düzgün bir şekilde yapılandırılmalı ve antivirüs ile ilgili karar yetkileri kullanıcıya bırakılmamalıdır. Kurum içerisinde bulunan donanımlardaki gereksiz çıktı birimleri devre dışı bırakılmalı, hatta bunlar donanımsal olarak ortamdan çıkarılmalıdır.

Ağ geçidinde bir güvenlik duvarı doğru yapılandırılmış bir şekilde mutlaka konumlandırılmalıdır. Bilişim alt yapıları periyodik olarak kontrol edilmeli, sonradan ilâve edilecek donanım ve yazılımların tehdit oluşturup oluşturmadıkları, bunları kullanan kişilerin yetkilerinin bulunup bulunmadığı gibi hususlar kontrol edilmelidir.

Bilgi güvenliğinde en zayıf halkanın “insan” olduğu unutulmamalı, kurum personeli hizmet içi eğitim programlarıyla bilgi güvenliği konusunda sürekli bir eğitime tabi tutulmalıdır.

Bu konu ile ilgili bundan sonra yapılacak çalışmalarda; kötü niyetli çalışanlar dışında, çeşitli bilgisayar korsanlığı yöntemleriyle gizli bilgilerin ele geçirilmesinde ve bu tür bilgi ifşalarında kullanılan tekniklerin analizi yapılabilir.

6. KAYNAKLAR

Adaklı, G. (2012). Hakim Güçlere ve Hakim Gazeteciliğe Meydan Okuyan Bir Girişim: Wikileaks. *Ankara Üniversitesi SBF Dergisi* **66**-1: 189-192.

Aktan, C. C. (2006). Organizasyonlarda Yanlış Uygulamalara Karşı Bir Sivil Erdem, Ahlaki Tepki ve Vijdani Red Davranışı: Whistleblowing. *Mercek Dergisi* **1**: 12-15.

Alagöz, A., ve Allahverdi, M. (2011). Kurumsal Bilgi Güvenliği Ve Muhasebe Bilgi Sistemi. *Muhasebe ve Vergi Uygulamaları Dergisi*, **3**: 47-64.

Aydoğdu, N. (2014). Sanal Özel Ağ (VPN) Bağlantı Mantığı (VPN Teknolojisi) ve Token Güvenliğinin Pin Kodu ile Arttırılması. Yüksek Lisans Tezi, T.C. Beykent Üniversitesi.

Binark, M. (2007). Yeni Medya Çalışmalarında Yeni Sorular ve Yöntem Sorunu. Mutlu Binark (der.) içinde. *Yeni Medya Çalışmaları Dergisi* 21-44.

Chen, N. (2011). Wikileaks and its Spinoffs: New models of journalism or the new media gatekeepers. *Journal of Digital Research & Publishing*, **1**: 157-167.

Cohen, B. (2003). Incentives build robustness in BitTorrent. *Workshop on Economics of Peer-to-Peer systems*, **6**: 68-72.

Çalışkan, B. (2016). Kitlesel Gözetime Karşı Kolektif Bir Üretim Biçimi Olarak Sızıntı Gazeteciliği. *Galatasaray Üniversitesi İletişim Dergisi* **25**: 127-154.

Çaplı, B. (2002). *Medya ve Etik*. İmge Kitabevi, Ankara, Türkiye.

Çaylı, A., Akyüz, A., Efe, E., ve Üstün, S. (2007). P2P ile Mücadele ve KSU-NET Örneği. *IX*. Akademik Bilişim Konferansı Bildirileri, Kütahya. 31 Ocak – 02 Şubat, 321-324

Çeker, M. (2006). Offshore Hesaplar ve Bankaların Sorumluluğu. *Çukurova Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* **10**:95-107.

Demir, F. (2010). Güvenli Veri İletiminde Kullanılan VPN Tiplerinin Uygulaması ve Performans Analizi. Yüksek Lisans Tezi. İstanbul Teknik Üniversitesi.

Doğantimur, F. (2009). ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği. TC Maliye Bakanlığı Strateji Geliştirme Başkanlığı Mesleki Yeterlilik Tezi, Ankara.

Dragt, J. (2012). American Power on the Internet: The Conceptualization of Power in the Debates about Online Piracy and Wikileaks. Yüksek Lisans Tezi, Utrecht University.

Erdem, B. K. (2011). Radikal Demokrasi Kuramı Bağlamında Yeni Medyanın Geleceği: "Wikileaks Örneği". *İstanbul Üniversitesi İletişim Fakültesi Hakemli Dergisi*, **40**: 5-24.

Erhan, D., Anarım, E., Kurt, G. K., ve Koşar, R. (2013). DDoS Saldırılarının Trafik Özellikleri Üzerindeki Etkisi. 21. Signal Processing and Communications Applications Conference, (SIU) Sabancı Üniversitesi İstanbul 24-26 Nisan 2013 372.

Erol, A. (2009). Dünyada ve Türkiye'de Elektronik Yayıncılık. Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi Isparta.

Ertem, C., ve Uçkan, Ö. (2011). Wikileaks Yeni Dünya Düzenine Hoşgeldiniz: Nesil Basım Yayın Gıda Ticaret ve Sanayi A.Ş. İstanbul

Farina, J., Scanlon, M., Kohlmann, S., Khac, N.-A. L., and Kechadi, M. (2015). HTML5 Zero Configuration Covert Channels: Security Risks and Challenges. Annual ADFSL Conference on Digital Forensics, Security and Law, 452:135-150.

Hsu, D. F., and Marinucci, D. (2013). Advances in Cyber Security Technology, Operations and Experiences. Fordham University Press. New York. USA.108-256

Karaarslan, E., Eren, M. B., ve Koç, S. (2014). Çevrimiçi Mahremiyet: Teknik ve Hukuksal Durum İncelemesi. Türkiye'de İnternet Konferansı Bildirisi, İzmir. 27 - 29 Kasım 2014. 187-195

Karaşar, N. (2002). Bilimsel Araştırma Yöntemi. Ankara: Nobel Yayın Dağıtım, 81-86.

Kılınç, D. (2016). 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun'un 9/A Maddesi Çerçevesinde Özel Hayatın Korunması. *Gazi Üniversitesi Hukuk Fakültesi Dergisi*, **20-2**: 577-623.

Kocaman, Y. (2016). Offshore'un Dayanılmaz Hafifliği. *Derin Ekonomi*, **12**: 48-56.

Koçaslan, M. D. (2015). DDoS Saldırıları ve Korunma Yöntemleri Üzerine Simülasyon Uygulamaları. Yüksek Lisans Tezi. Beykent Üniversitesi.

Kumcuoğlu, İ. (2011). Mahremiyet mi Kamu Çıkarı mı? Değişen Gazetecilik Kodları, Wikileaks ve Medya Etiği. II. Medya ve Etik Sempozyumu, 55-61.

Levi, A. (2004). Nasıl bir E-posta güvenliği? *Bilişim Güvenlik.* Mart/Nisan 2003, 38-40

Levi, A., ve Özcan, M. (2002). Açık Anahtar Tabanlı Şifreleme Neden Zordur? Bilişim 2002, TBD 19. Bilişim Kurultayı İstanbul, 3 - 6 Eylül 2002, 41-45.

Marttin, V., ve Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir İnceleme *Mühendislik Bilimleri ve Tasarım Dergisi,* **1**, 49-56.

Mercan, N., Altınay, A., ve Aksanyar, Y. (2012). Whistleblowing (Bilgi İfşası, İhbar) ve Yolsuzlukla Mücadelede İç Denetimin Değişen ve Gelişen Rolü. *Organizasyon ve Yönetim Bilimleri Dergisi,* **4(2)**: 167-176

Miceli, M. P., and Near, J. P. (1984). The relationships among beliefs, organizational position, and whistle-blowing status: A discriminant analysis. *Academy of Management journal,* **27(4)**: 687-705.

Munro, I. (2015). Organizational resistance as a vector of deterritorialization: The case of WikiLeaks and secrecy havens. *Organization,* **23(4)**: 567-587. Doi: 10.1177/1350508415591362

Nguyen, P. Q. (2004). Can we trust cryptographic software? Cryptographic flaws in GNU Privacy Guard v1. 2.3. International Conference on the Theory and Applications of Cryptographic Techniques. Advances in Cryptology - EUROCRYPT 2004. Berlin : 555-570

Oğuz, B., ve Cevahir, H. K. (2010). BT Yönetiminde Bilgi Sızıntısı ve Ağ Tabanlı Çoklu Protokol Bilgi Sızıntısı Engelleme. 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, Ankara 5-6 Şubat.

Sağıroğlu, Ş., Ceyhan, E. B., ve Maraş, R. (2015). E-Postalarda Adli Bilişim ve Karşı Adli Bilişim Teknikleri. Internatıonal Conference On Informatıon Securıty And Cryptology (ISCTurkey). 70-77

Sauter, M. (2013). Distributed Denial of Service Actions and the Challenge of Civil Disobedience on the Internet. Yüksek Lisans Tezi. MIT Massachusetts Institute Of Technology University.

Schollmeier, R. (2001). A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications. Peer-to-Peer Computing, 2001. Proceedings. First International Conference on. Linkoping, Sweden 27-29 Ağustos

Şahinaslan, E., Kandemir, R., ve Kantürk, A. (2010). Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme. 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, Ankara 5-6 Şubat

Tataroğlu, M. (2013). Mahremiyet Sorunlarının Önlenmesinde Mahremiyet Etki Değerlendirmesi (MED). *Yönetim ve Ekonomi*, **20(1)**: 263-290

Tonta, Y. (2000). Elektronik yayıncılıkta son gelişmeler. *Bilgi Dünyası*, **1**(1): 89-132.

Topaloğlu, M. (2012). Özel Anlamlı İfade İçeren Verilerde Sızıntı Önleme İçin Bir Mimari Tasarım ve Gerçekleştirilmesi. Doktora Tezi. Trakya Üniversitesi. Edirne

Toruk, İ., ve Sine, R. (2012). Haber Söylem Üretimindeki İdeolojik Etki: Wikileaks Haberleri. *Selçuk Üniversitesi Türkiyat Araştırmaları Dergisi*, **1(31)**: 351-378.

Uyar, S., ve Yelgen, E. (2015). Bilgi İfşasi (Whistleblowing) ve Denetim. *Journal of Management and Economics Research*, **13(1)**: 85-106 Doi: 10.11611/jmer412

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartlari Üzerine Bir Inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, **23(2)**: 507-522

Yılmaz, E. G. (2009). Kurumsal iletişim ve prensiplere dayalı kurumla uyuşmazlık davranışı: Whistleblowing. Uluslararası Davraz Kongresi, Isparta

Yüksel, M. İ. (2010). Tor Anonimleştiricisinde Sınırlı Kaynak Kullanarak Trafik Analizi Gerçekleştirimi. Yüksek Lisans Tezi, Ege Üniversitesi.

Yüksel, Z. (2007). Ağ Güvenliği ve Güvenlik Duvarında VPN ve NAT Uygulamaları. Yüksek Lisans Tezi. Yıldız Teknik Üniversitesi. İstanbul

İNTERNET KAYNAKLARI

1) https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations, 06.02.2017

2) https://search.wikileaks.org/plusd/about, 09.04.2017

3) http://www.bbc.com/turkce/haberler/2013/04/130408_wikileaks_turkiye, 09.04.2017

4) https://panamapapers.icij.org/20160506-john-doe-statement.html, 09.04.2017

5) https://www.manageengine.com/products/passwordmanagerpro/preventing-wikileaks-type-incidents-white-paper.html, 14.05.2017

6) http://www.bbc.com/turkce/haberler/2016/05/160510_panama_turkiye, 09.04.2017

7) https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en, 17.03.2017),

8) https://www.iso.org/standard/54533.html, 20.03.2017

9) http://www.pgp.net/pgpnet/pgp-faq/pgp-faq-keys.html, 04.04.2017

10) https://securedrop.org/faq#how_works, 07.05.2017

11) https://securedrop.org/directory, 07.05.2017

12) https://tails.boum.org/doc/index.en.html, 09.05.2017

13) http://www.tdk.gov.tr/index.php?option=com_gts&kelime=SANS%C3%9CR, 05.01.2017

14) http://www.torproject.org/overview.html.en#overview, 09.02.2017

15) https://www.symantec.com/content/en/us/enterprise/white_papers/b-avoiding-a-repeat-of-wikileaks_WP_21141461.en-us.pdf , 12.05.2017

16) https://www.torproject.org/tor-manual.html, 06.03.2017

17) http://www.tbd.org.tr/, 12.02.2017

19) www.wikileaks.org/wiki/Wikileaks:About/tr , 03.04.2017

20) https://wikileaks.org/#submit, 01.03.2017

21) https://wikileaks.org/ciav7p1/, 08.03.2017

22) https://tr.wikipedia.org/wiki/Sans%C3%BCr, 19.01.2017

23) https://tr.wikipedia.org/wiki/Tor_(anonim_a%C4%9F), 05.02.2017

25) https://en.wikipedia.org/wiki/Pretty_Good_Privacy, 26.02.2017

26) https://en.wikipedia.org/wiki/SecureDrop, 07.05.2017

27) https://en.wikipedia.org/wiki/GlobaLeaks, 08.05.2017

28) https://panamapapers.icij.org/the_power_players/, 12.05.2017

29) https://www.icij.org/securedrop, 01.03.2017

30) http://whois.domaintools.com/wikileaks.org, 03.04.2017

31) https://www.globaleaks.org/, 08.05.2017
32) https://www.ekovizyon.com.tr/dunya/%EF%BB%BF%EF%BB%BF8-adimda-vergiden-kacinma-ya-da-vergi-kacirma, 12.05.2017
33) http://www.aljazeera.com.tr/al-jazeera-ozel/panama-belgelerinin-yarattigi-etki-sasirtici, 07.04.2017
34) http://www.bbc.com/turkce/haberler/2016/04/160404_panama_7_soru, 06.04.2017
35) https://www.us-cert.gov/sites/default/files/publications/DHS-Cybersecurity-Questions-for-CEOs.pdf, 13.03.2017
36) http://www.theage.com.au/news/Technology/Chinese-cyberdissidents-launch-WikiLeaks-a-site-forwhistleblowers/2007/01/11/1168105082315.html, 03.04.2017
37) https://teknodestek.com.tr/vpn-nedir-ne-ise-yarar-kullanim-alanlari-nedir/, 02.02.2017
3). https://www.bilgiguvenligi.gov.tr/gizlilik/pretty-good-privacy-pgp-sifreleme.html, 10.05.2017
39) https://docs.securedrop.org/en/stable/overview.html, 07.05.2017
40) http://rethinkingvis.com/visualizations/68, 22.04.2017
41) http://www.pbs.org/newshour/rundown/can-wikileaks-be-stopped/, 29.04.2017
42) http://infosecisland.com/blogview/10121-WikiLeaks-Denial-of-Service-Wars-Continue-to-Escalate.html, 10.05.2017
43) https://www.sans.org/reading-room/whitepapers/dlp/data-loss-prevention-32883, 14.03.2017
44) https://www.nbr.co.nz/article/wikileaks-offline-faces-triple-threat-134238, 09.04.2017
45) http://www.newyorker.com/magazine/2010/06/07/no-secrets, 21.04.2017
46) https://www.slideshare.net/EmreERKIRAN/iso-27001-bilgi-gvenlii-ynetim-sistemi, 01.03.2017
47) http://www.yenisafak.com/politika/turk-leaks-573440, 08.03.2017
48) https://freedom.press/news-advocacy/how-we-plan-on-keeping-securedrop-as-secure-as-possible/, 01.03.2017
49) https://www.newscientist.com/article/mg19325865.500-how-to-leak-a-secret-and-not-get-caught/, 05.05.2017
50) http://searchmobilecomputing.techtarget.com/tip/TrueCrypt-reviewed-Free-utility-for-mobile-encryption, 05.04.2017

51) http://www.tandfonline.com/doi/abs/10.1080/01436597.2012.728324, 05.05.2017
52) https://www.bilgiguvenligi.gov.tr/gizlilik/pretty-good-privacy-pgp-sifreleme.html, 12.02.2017
53) http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf, 12.05.2017
54) https://tr.linkedin.com/pulse/acfe-2016-fraud-raporu-dr-%C3%BCnal-%C5%9Ferifler-smmm-spk-kgk-bdl, 05.05.2017
55) http://sk.sagepub.com/reference/hdbk_mediastudy/n8.xml, 25.04.2017
56) http://csirt.ulakbim.gov.tr/dokumanlar/p2p_ile_yasamak.pdf, 15.03.2017
57) https://www.bilgiguvenligi.gov.tr/veri-kacagi-onleme/veri-kacagi-onleme-dlp-ve-veri-madenciligi-3.html, 05.05.2017
58) https://www.crcpress.com/How-to-Achieve-27001-Certification-An-Example-of-Applied-Compliance-Management/Arnason-Willett/p/book/9780849336485, 15.03.2017
59) https://neo4j.com/blog/icij-neo4j-unravel-panama-papers/, 06.05.2017
60) http://www.tcij.org/sites/default/files/u11/InfoSec%20for%20Journalists%20V1.3.pdf, 11.04.2017
61) http://www.mahfiegilmez.com/2016/04/ky-offshore-bankaclg.html, 02.04.2017
62) http://www.theaustralian.com.au/national-affairs/defence/rudd-government-blacklist-hacker-monitors-police/news-story/53c647d56c2d928d20cc70c9257f0026, 04.04.2017
63) https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers?CMP=twt_gu, 24.03.2017

ÖZGEÇMİŞ

Adı Soyadı : Salih ERDURUCAN

Doğum Yeri ve Tarihi : Ankara 1974

Yabancı Dili : İngilizce

İletişim (Telefon/e-posta) : serdurucan@gmail.com / salih.erdurucan@ankara.edu.tr

Eğitim Durumu (Kurum ve Yıl)

Lise : Beypazarı Endüstri Meslek Lisesi (1989-1992)

Önlisans : Mustafa Kemal Üniversitesi, İskenderun MYO (1992-1994

Lisans : Hoca Ahmet Yesevi Üniversitesi, Mühendislik Fakültesi Yönetim Bilişim Sistemleri, (2012-2015)

Yüksek Lisans : Afyon Kocatepe Üniversitesi, Fen Bilimleri Enstitüsü, İnternet ve Bilişim Teknolojileri Yönetimi Anabilim Dalı, (2015-2017)

Çalıştığı Kurum/Kurumlar ve Yıl : Ankara Üniversitesi, Nallıhan MYO, (2015- Dvm)