T.C.

ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI

SİBER SUÇLAR VE KURUM GÜVENLİĞİ

DENİZCİLİK UZMANLIK TEZİ

Mithat YILDIZ Denizcilik Uzman Yardımcısı

BİLGİ İŞLEM DAİRESİ BAŞKANLIĞI

Danışman
Alper SINAV
Bilgi İşlem Dairesi Başkanı

Kasım 2014

İçindekiler

ÖNSÖZ

Bu çalışmam süresince her türlü yardım ve fedakârlığı sağlayan, bilgi, tecrübe ve güler yüzü ile çalışmama ışık tutan, tez danışmanım Daire Başkanımız Sayın Alper SINAV'a ve Grup Başmühendisimiz Sayın Özgür GÖRENER'e, Şube Müdürlerimiz Sayın Nejdet GÖKKAYA ve Sayın Asuman KUTLUATA'ya. vermiş oldukları maddi manevi katkılardan dolayı teşekkürlerimi bir borç bilirim.

ÖZET

SİBER SUÇLAR VE KURUM GÜVENLİĞİ
Hazırlayan: Mithat YILDIZ

Bilgi ve iletişim teknolojileri ile internetin yaygınlaşması ve evimizdeki bilgisayarlardan, cep telefonlarına kadar çeşitli cihazların, iletişim ağları aracılığıyla birbirlerine bağlanması, yeni tehditlere ve saldırıların oluşmasına sebep oldu. Bu yeni saldırı türlerinde silah olarak bilgisayar donanımları, yazılımları, virüsler ve zararlı yazılımlar iletişim ağları üzerinden kullanılmaya başlandı.

Siber alan yaygınlaştıkça, güvenlik konusu da önem kazanmaya başladı. Güvenliğe verilen önem artmış olsa da, teknoloji ilerledikçe sistemlerin siber saldırı ve tehditlerle karşı karşıya kalma olasılıkları çok daha yüksek bir orana çıkmış bulunmaktadır. Teknoloji yaşam standartlarımızı yükseltirken, eğer güvenlik önlemlerini önemsemez ve hayata geçirmez isek yeni tehditleri de beraberinde getiriyor.

Bu çalışmada siber suçlar, çeşitleri ve kullanılan zararlı yazılımlar ayrıntılı bir şekilde araştırılmış ve bunlara karşı nasıl önlem alınacağı tezde belirtilmiştir. Ülkemizde siber suçlarla ilgili yapılan yasal düzenlemeler ve siber güvenlikle ilgili yapılan faaliyetler incelenmiş, kamu kurumlarını ve özel sektörü ilgilendiren siber güvenlik standartları hakkında bilgi verilmiştir. Kurumda bilgi güvenliğini sağlamak için yapılması gereken çalışmalara yer verilmiş, teknolojik olarak ne tür önlemler alınabileceği araştırılıp, sunulmuştur.

Ülkemizin siber güvenlik strateji belgesi incelenmiş, 2014-2018 taslağı hakkında bilgi verilmiştir. Kurumda siber güvenlik için yapılması gereken başlıca kontroller değerlendirilerek, kurumumuz için öneriler getirilmiştir.

ABSTRACT

CYBER CRIMES AND SECURITY OF INSTITUTION

Prepared By: Mithat YILDIZ

By information and communication technologies, proliferation of internet and connecting a variety of devices ranging from personel computers at our homes to mobile phones by communication networks have caused new threats and attacks. Computer hardware, software and viruses were started to use as a tool over communication networks in these new kind of attacks.

The security issue also started to gain importance, during the time that cyber domain has became widespread. Even though security is more important than before, depending on developments in technology the probability of that systems exposed to cyber attacks and threats has increased. Technology leads to new threads as well as improving our life standarts, if we do not care about security measures.

In this paper, cyber crimes, sorts of them, and malware in use have been researched in detail and stated how to measure against them. Legal regulations regarding cyber crimes and activities about cyber security has been examined. Beside that the information regarding public institutions and private sector was given in the scope of cyber security standarts. In this respect, the necessity steps providing information security in the institution were explained, and what kind of precautions can be taken by utilizing technology was represented.

Examining cyber security strategy document of our country, information has been given with regard to the draft of period 2014-2018. The recommedations for our institution have been made by evaluating primarily controls to provide cyber security requirements in the institution.

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

SİMGE VE KISALTMALAR CETVELİ

BİT : Bilgi ve İletişim Teknolojileri

TCK : Türk Ceza Kanunu

FSEK : Fikir ve Sanat Eserleri Kanunu

FTP : File Transfer Protocol

SQL : Structured Query Language

MAC : Media Access Control

IP : Internet Protocol

LAN : Local Area Network

ARP : Address Resolution Protocol

DoS : Denial of Service

VPN : Virtual Private Network

DDoS : Distributed Denial of Service

DRDoS : Distrubuted Reflective Denial Of Service

TCP : Transmission Control Protokol

UDP : User Datagram Protocol

ICMP : Internet Control Message Protocol

ISP : Internet service provider

SMS : Short Message Service

SSH : Secure Shell

SSL : Secure Socket Layer

DNS : Domain Name System

HTTP : Hypertext Transfer Protocol

FTP : File Transfer Protocol

TİB : Telekomünikasyon İletişim Başkanlığı

TÜBİTAK: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

URL : Uniform Resource Locator

LOIC : Low Orbit Ion Cannon

IDP : Intrusion Detection & Prevention

RSA : Açık Anahtarlı Şifreleme

IPSec : Internet Protocol Security

ISO : Uluslararası Standartlar Örgütü

OKTEM : Ortak Kriter Test Merkezi

IETF : Internet Engineering Task Force

XSS : Cross Site Scripting

NSA : Amerikan National Security Agency

RAT : Uzaktan Yönetim Aracı

SCADA : Supervisory Control and Data Acqustion

IPS : Intrusion Prevention System

ISTF : Inter Departmental Information Security Task Force

NSD : National Security Database

DHS : Department of Homeland Security

ITU : Uluslararası Telekomünikasyon Birliği

GCA : Global Cybersecurtiy Agenda

ENISA : Avrupa Ağ ve Bilgi Güvenliği Ajansı

BOME : Bilgisayar Olaylarına Müdahale Ekibi

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

USOM : Ulusal Siber Olaylara Müdahale Merkezi

1.GİRİŞ

Bu çalışma ile son yıllarda büyük oranda artış gösteren siber saldırılara karşı Bilgi Sistemlerinin Güvenliğinin nasıl olması gerektiği hakkında bilgi verilerek, belli saldırı senaryolarına karşı nasıl davranılması gerektiği anlatılarak, Bakanlığımız Bilgi Sistemlerinin Güvenliği konusunda yol gösterici bir çalışma olması amaçlanmıştır.

Bu çalışmanın yöntemi olarak siber güvenliğin istenilen seviyede sağlanabilmesi için yapılması gerekenler anlatılacak olup, çalışma kapsamında siber güvenlik, siber uzay, siber suç gibi temel kavramlar, hukuk sistemimize göre bilişim suçlarına giren olaylar, dünya çapında ve devletlerarası problemlere neden olan siber tehditler incelenecektir. Ekler kısmında siber saldırı senaryoları işlenerek alınabilecek tedbirler üzerine çalışma yapılmış olup, Bilgi Sistemlerimize yapılabilecek siber saldırılara karşı alınması gereken önlemler örnekleri ile anlatılmıştır.

Birinci bölümde, temel kavramların tanımları yapılacaktır. Çalışmanın birinci bölümünde anlam birliğinin sağlanması maksadıyla bu konuda en çok karşılaşılan kavramlar ele alınacaktır.

İkinci bölümde, siber suçlardan, siber suçları işlemeye olanak sağlayan siber tehdit araçlarından, zararlı yazılımlardan ve bunlara karşı alınabilecek önlemlerden bahsedilecek, siber uzayda tehdit ve tehlike oluşturan araç ve yöntemler ele alınacaktır. Uluslararası alanda yapılan siber saldırılar hakkında bilgi verilecektir.

Üçüncü bölümde, siber güvenliğin istenilen düzeyde sağlanabilmesi için uyulması gereken politikalar, bilgi sistemi güvenliği için alınabilecek teknolojik önlemler ve siber güvenlik konusunda dünyanın önde gelen ülkelerinin ve uluslararası örgütlerin yapmış oldukları çalışmalar değerlendirilecektir. Siber güvenlik ile ilgili yapılanma ve tedbirler, ülkeler ve uluslararası kuruluşlar bazında ele alınacaktır. Ülkelerin siber güvenlikle ilgili nasıl bir anlayış ve yapılanmaya gittiklerine dair bir özet ortaya konacaktır

Dördüncü bölümde, ülkemizde siber suçlara yönelik yasal düzenlemeler ve siber güvenlik alanında özel sektör ve kamu tarafından yapılan faaliyetler incelenecektir. Ulusal bilgi programları, Ulusal Bilgi Güvenlik Stratejisi Eylem Planı hakkında bilgi verilecektir. Ülkemizde yapılan Siber Güvenlik Tatbikatlarından elde edilen sonuçlar ele alınacaktır. Bölüm sonunda, ülkemizde siber güvenlik alanında yürütülen çalışmalar; planlamalar, yasal düzenlemeler, teknik birimler, gerçekleştirilen ortak tatbikatlar ve düzenlenen çalıştay ve konferanslar bazında ele alınacaktır.

Beşinci bölümde, Uluslararası Siber Güvenlik Standartları incelenecek, ISO 27001'in güncel sürümü hakkında değerlendirme yapılacaktır.

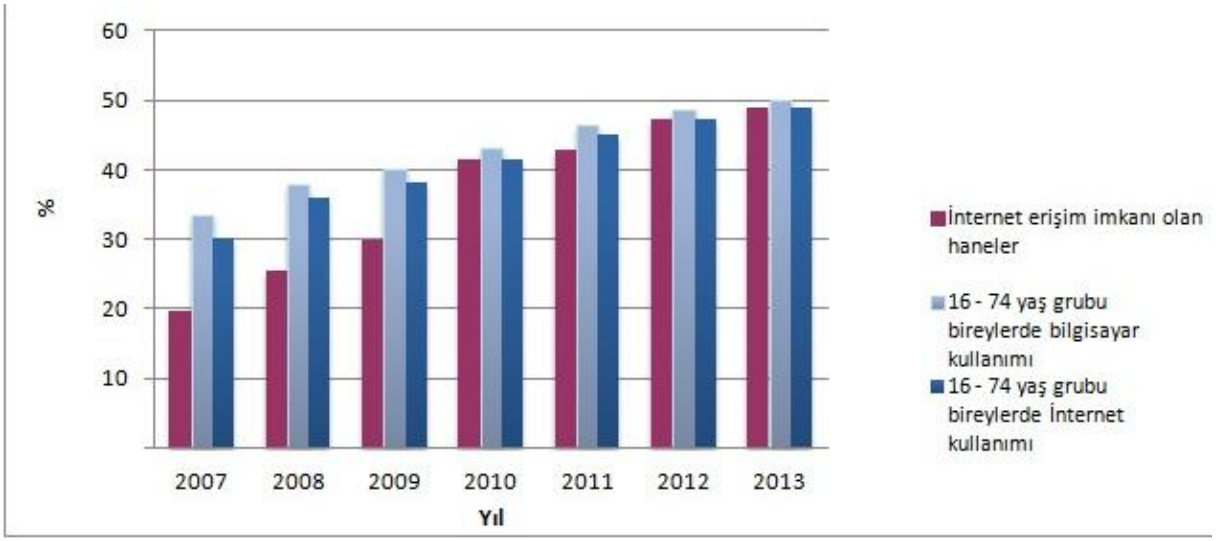
Sonuç bölümünde, kurum güvenliğini sağlamak için yapılması gereken işlemlerle ilgili önerilerde bulunulacaktır ve siber tehditlere karşı kurumlarda güvenli bir siber savunma oluşturabilmek için yapılması gereken kritik kontroller incelenecektir. Ekler kısmında, risk analizi ile örnek saldırılara karşı neler yapılabileceği ayrıntıları ile açıklanmıştır.

Günümüzde bilgisayarın keşfiyle birlikte siber teknolojiler ilerlemekte ve bu ilerlemeyle birlikte bilgisayarın hem faydaları hem de ön görülemeyen zararlarıyla baş başa kalmaktayız. Siber dünyada her türlü medya ortamı, bilgi, makale, program insanoğlunun hizmetine sunulmuştur.

Bilgisayar aritmetik ve mantıksal işlemleri yapabilen ve yaptığı işlemlerin sonucunu saklayabilen ve istenildiğinde geri getiren elektronik bir cihazdır. Bilgisayar kullanım şekline göre iletişim kurmak, bilgi öğrenmek, araştırma yapmak, dış dünya ile irtibat halinde olmak gibi zaman zaman işlerimizi kolaylaştıran lehimize kullandığımız bir araç iken zaman zaman da bilgilerimizin çalındığı, kredi kartı bilgilerimizin kopyalandığı, bulunduğumuz ağa izinsiz sızma girişimlerinin gerçekleştirildiği ya da kullanıcı bilgilerimizin çalındığı bir zararlı siber araca dönüşmektedir.

Siber suçlarda teknolojinin kullanılması kaçınılmazdır. Bir bilgisayar ile internet uzayı bir kredi kartı, elektronik bir cihaz veya cep telefonu ile de bu suçlar işlenebilmektedir. İngilizcede Cyber Crime siber suç olarak tanımlanmaktadır. Sanal ortamlarda yani siber teknolojileri kullanılarak işlenen tüm suçlar "Siber Suçları" oluşturur.

Bilişim teknolojileri bazı klasik suçların daha kolay işlenmesine imkân vermesinin yanında, yeni tip suçların da ortaya çıkmasını sağlamıştır. Günümüzde internetin sağladığı imkânlar sayesinde siber suç işlemek için eskisi kadar teknik bilgi ve beceriye sahip olmaya gerek kalmamıştır. Bununla beraber, bilişim teknolojilerine olan bağımlılığın giderek artması, bireylerin suç mağduru olma riskini artırmasının yanında siber alanı da ulusal güvenliğin önemli bir parçası konumuna getirmiştir. Bu yüzden siber güvenlik son yıllarda en fazla tartışılan konulardan birisi haline gelmiştir.



Şekil-1: Ülkemizde Yıllara Göre İnternet Kullanım Oranları (Tüik)

Ülkelerin bilişim teknolojilerine ve özellikle internete olan bağımlılıkları her geçen gün artmaktadır. Bugün küresel ağ üzerinde günlük 294 milyar e-posta mesajının gönderildiği, bir günde 168 milyon DVD'lik bilginin üretildiği tahmin edilmektedir. Youtube sunucularına günlük 864.000 saatlik video yüklenmekte, Netflix kullanıcıları bir günde 22 milyon saat TV veya sinema seyretmektedirler. Dünya nüfusunun yaklaşık üçte ikisinin internet bağlantısı ve %20'sinin sosyal ağlara üyelikleri bulunmaktadır. Yine dünya nüfusunun %85'i cep telefonu kullanmakta ve bunların %15'i cep telefonlarıyla alışveriş yapmaktadırlar (Klimburg, 2012).

Bu rakamlar bilişim teknolojilerine olan bağımlılığın ne derece arttığını göstermektedir. Bilişim teknolojileri, hayatı kolaylaştırma adına sağladıkları imkânların yanında, güvenlik boyutunda da yeni kaygıların gelişmesine sebep olmuştur. Artık bu yeni dünyada, fiziksel temasa veya mağdurla aynı yerde bulunmaya gerek duymadan hırsızlık, dolandırıcılık gibi suç fiilleri mümkün hale gelmiştir.[1]

2. SİBER SUÇLAR

Bilgi ve İletişim Teknolojileri (BİT) günlük yaşamlarında bilgi ağları ve hizmetlerinin kullanımına bağımlı hale gelen günümüz insanı için giderek daha önemli hale gelmektedir. Bilgi ve iletişim teknolojilerinin hızla gelişmesi ve tüm dünyada yayılması ile kamu ve özel kesim uygulamalarının elektronik ortama aktarılması insanlar için büyük faydalar sağlayan gelişmelerdendir. Ancak bu gelişmelerin kötü niyetli bazı kişilerce suiistimal edilmesi, siber ortamın tehdit, saldırı ve zarar verme gibi amaçlarla kullanılması ile siber saldırılar dolayısıyla kişilerin ve ülkelerin gördüğü zararların büyük boyutlara ulaşması güvenlik anlayışında değişikliklere yol açmış ve bilgi güvenliği konusu bireylerin, kurumların, ülkelerin ve uluslararası kuruluşların en önemli gündem maddelerinden biri haline gelmiştir. Çünkü bilgi oluşturulabilme, depolanabilme, bozulabilme, işlenebilme, kullanılabilme kaybolabilme, çalınabilme ve değiştirilebilme gibi niteliklere sahiptir. BİT'te yaşanan gelişmeler bu özellikleri çok daha kolay uygulanabilir hale getirmiştir. [2]

Herhangi bir suçun elektronik ortam içerisinde işlenebilme imkanı bulunuyor ve bu ortam içerisinde gerçekleştirilen fiil genel olarak hukuka aykırı veya suç olarak tanımlanabiliyorsa (bütün ülkelerin aynı fiili suç olarak yaratmaları gerekmez) bu suçları **siber suçlar** (Cyber Crimes) olarak tanımlayabiliriz. Siber suç bilgisayar veya ağ sistemleri yolu ile ya da bilgisayar veya ağ sistemleri içerisinde veya bilgisayar ve ağ sistemlerine karşı işlenebilir.

Siber suç bir bilişim sistemine izinsiz olarak ve hukuka aykırı olacak şekilde girilmesi ve sonrasında yapılan eylemdir. Bu suçta hedef bir kişi olabileceği gibi kişinin malvarlığı veya

bir sistemin kendisi de olabilir. Örneğin, bir sisteme girerek, zarar verme, verileri silme, şifreleme, ele geçirme, veri ekleme, sistemin kullanımını engelleme, özel hayatın gizliliğine müdahale etme, iletişimi engelleme, iletişimi izinsiz izleme ve kayıt etme gibi eylemler siber suç kategorisinde değerlendirilir.

2.1 İnternet Üst Kuruluna Göre Siber Suçlar

1) Bilgisayar Sistemlerine ve Servislerine Yetkisiz Erişim ve Dinleme

"Erişim" sistemin bir kısmına, bütününe, bilgisayar ağı veya içerdiği verilere, programlara; yine programlar, casus yazılımlar veya virüsler vb. ile ulaşma anlamındadır. Günümüzde özel hayatın gizliliğinin korunması için kanunlarda gerekli müeyyideler konulması ile birlikte dinlemeler ,erişimler ,izinsiz özel ve şirket bilgisayarlarına ve sistemlerine girmek suç olarak kabul edilmiştir.. Günümüzde telefon dinlemeleri veya kişilerin özel mülklerine girmek nasıl savcı izni olmadan mümkün olmamakta ise yine kişiler veya kurumlar arası haberleşmenin bilgisayar üzerinden dinlenmesi veya izinsiz bilgilerin alınması da kişi özel mülkü ya da kişilerin şahsiyetlerine taciz olarak kabul edilmektedir ve suç oluşturmaktadır.

Ülkemizde bu konuda TCK'nin (Türk Ceza Kanunu) 243. maddenin 1. ve 2. fıkrasında açıkça belirtilmiştir. Bu bölümde incelenmesi gereken konulardan biri de casus yazılımlardır. Bu yazılımlar hukuki olarak suç sayılmamaktadır, fakat bu konuda tartışmaya açık bir kavram olduğu da bir gerçektir.

2) Bilgisayar Sabotajı

Bu suç türü iki şekilde karşımıza çıkmaktadır.
1. Bilgisayar teknolojisi kullanarak sistemine sızılan bilgisayardaki bilgilerin silinmesi, yok edilmesi ve değiştirilmesi.
2. Hedef alınan sisteme uzaktan erişerek değil de bilakis fiziksel zarar vererek ya da sistem başında bulunarak bilgisayardaki bilgileri silmek, yok etmek veya değiştirerek zarar verilmesi.

Burada önemli olan mala verilen zarardan ziyade içindeki bilgilere verilen zarar önem arz eder. Yetkisiz erişimin aktif sahası olarak da nitelendirilen "Bilgisayar Sabotajı", yalnız sisteme erişimle kalmamakla birlikte, eriştiği sistem (bilgisayar)„ın içerdiği bilgileri silme veya değiştirme olarak ifade edilir.

Bir bilgisayara veyahut sisteme yetkisiz erişim sağlayanlar; sadece eriştiği bilgileri incelemekle, kopyalamakla kalmıyor, bu bilgileri değiştirebiliyor, silebiliyor ya da bu bilgileri kanun dışı kullanmak isteyenlere satabiliyor. Türkiye'de "Bilgisayar Sabotajı" TCK(Türk Ceza Kanunu)"nun 243/ 3 ile 244/1 ve 2. maddelerine göre suçtur. Virüsler, Wormlar ve Zombiler vb. kötü amaçlı olarak yazılmış kodlardır. Bu tür kötü amaçlı yazılmış kodlar, başkalarına zarar vermediği sürece suç sayılmamaktadır. Fakat bu tür kodlar; kişi ya da kurumlara intikal eder ve zarar verirse suç teşkil etmeye başlar. Yoksa sırf kod yazımı saikten öte bir anlam ifade etmemelidir. Türkiye'de kötü amaçlı kodları yazma bunu yaymaya ilişkin açık bir hüküm bulunmamaktadır.

3) Bilgisayar Yoluyla Dolandırıcılık

Dolandırıcılık genel bağlamda "Hileli davranışlarla bir kimseyi aldatıp, onun veya başkasının zararına olarak, kendisine veya başkasına bir yarar sağlamaya" denmektedir. Bilişim kavramı olarak "Dolandırıcılık" bilgisayar veya iletişim araçlarıyla kişileri şaşırtma, aldatma, kandırma olarak tarif edilebilir. **Bilgisayar Yoluyla Dolandırıcılık suçu;** Kredi kartlarının bir benzerinin yardımcı programlarla oluşturulması yoluyla yetkisiz ve izinsiz erişilen bilgilerin kopyasını almak şeklinde; Finans bilgilerinin tutulduğu programlarla yapılan değişiklik ile istenilen kişinin hesabına istenildiği kadar para aktarmak suretiyle; Kişiler arasında mali alışverişi olan kişilerin adına mail vs. şeklinde iletişim kurarak; kişileri kandırarak, işlenmektedir. Ülkemizde bu tür suçlar TCK(Türk Ceza Kanunu)"da 158.maddenin (1). Fıkrasının (f) bendinde,244.maddenin (3).fıkrasında ve 245.maddesinin (1). Fıkrasında hüküm altına alınmıştır.

4) Bilgisayar Yoluyla Sahtecilik

Klasik olarak tabir edildiğinde, bir şeyin aslına benzetilerek yapılan düzmece olarak tarif edilebilmektedir. Bazen ileri teknoloji ürünü cihazlar kullanılarak, bazen de çok basit web programcılığı (Fakemail, Phishing) yöntemiyle sahtecilik yapılmaktadır. Günümüzde başkalarının adına e-mail göndererek, ticari ve özel ilişkileri zedelenmesini sağlamak, başkalarının adına web sitesi hazırlamak ve bu web sitesinin tanıtım amacıyla başkalarına e-mail ve mesaj göndererek (iletişim kurarak) ve bu mesajlarda da mağdur olan şahsın telefonlarını vererek, sahte para, sahte evrak, sahte bilet vb. basma yönetimiyle bu suç işlenmektedir. Ülkemizde bu tür suçlara yönelik kanunlarda henüz net bir tanımlama yapılmamıştır. Fakat yeni TCK (Türk Ceza Kanunu)'nın 158. maddesinin f bendinin uygulanılabilirliği söz konusudur.

5) Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı

"Kanunla Korunmuş Bir Yazılımın İzinsiz Kullanımı" yazılımların; yasadışı yöntemlerle kopyalanmasını, çoğaltılmasını, satılmasını, dağıtılmasını ve kullanılmasını ifade eder. Ülkemizde 5846 no"lu Fikir ve Sanat Eserleri Kanunu (FSEK) lisanslı yazılımları satın alan kişiye bir adet kopyalama hakkı vermekte, daha fazla kopyanın yapılmasını, satılmasını, yazılımın kiralanmasını yasaklamaktadır.

6) Yasadışı Yayınlar

Yasadışı olarak kabul edilen unsurların bilgisayar sistemleri, ağları, internet aracılığıyla yayınlanması ve dağıtılması olarak ifade edilir. Kanunun yasaklamış olduğu bu materyaller; web siteleri(sayfaları), elektronik postalar, haber grupları, forumlar, iletişim sağlayan her türlü araç, optik araçlar tarafından kayıt yapan tüm sistemler olarak kabul edilir. Yasadışı yayınları üç gruba ayırmak mümkündür. Bunlardan birincisi, vatanın bölünmez bütünlüğüne aykırı olarak hazırlanmış terör içerikli internet siteleridir. Bu tür siteleri hazırlayanların asıl amacı sansür konulmuş Anayasaya aykırı fikirlerini, interneti kullanarak

yaymak, bu sayede de kendilerine taraf toplayarak vatanın bütünlüğünü bozacak düşüncelerini ifade etmektir.

Yasadışı yayınların bir diğeri ise toplumun genel ahlakına, ar ve hayâ duygularına aykırı düşen yayınlardır. Bunlar pornografik görüntü veya yazılar şeklinde olmaktadır. Türkiye'de TCK (Türk Ceza Kanunu)"da 77.102.103 ve 104. maddeleriyle büyük ve çocuk pornografisi yasaklanmıştır. İnternet aracılığıyla fiilen işlenen suçlardan üçüncüsü ise; bir kişiye, kuruma vb. karşı yapılan hakaret ve sövme suçudur. Bu suç türü internet üzerinden başkalarının adına uygun olmayan e-mailler göndererek kişi ya da kurumların itibarını zedelemek suretiyle olabilmektedir. Bir başka yol ise yine kişi ya da kurumların sahip oldukları adın, lakabın web üzerinden satın alınarak, kişi aleyhine yayında bulunmak suretiyle meydana gelebilmektedir. Kısaca 6 Ana başlık altında toplanan Bilişim Suçları Türlerinin birçoğu yasalarımızda suç olarak düzenlenmiş ve bu sayede koruma altına alınmıştır. Lakin günümüz teknolojisinin hızlı ilerlemesi, internetin sürekli yaygınlaşması nedeniyle, bu gün suç türleri arasında sayılmayan yeni birçok zarar amaçlı kullanımlar oluşacaktır.[3]

2.2 Siber Suçlarda Kullanılan Yöntemler ve Siber Saldırılar

Siber alanda saldırı için kullanılan araçlar da siber suçların işlenmesinde öncelikli argümanlardandır. Siber tehditleri değerlendirmek ve engellemek şu nedenlerden dolayı çok zordur (Charney [web], 2009:5-6):

(1) Zararlı faaliyet gösteren birçok aktör bulunmaktadır. Bilgisayarların azalan maliyeti, artan İnternet bağlantısı ve zararlı yazılımların, yazılma ve elde edilme kolaylığı herkesin zararlı yazılım elde edebilmesi ve kullanabilmesini kolaylaştırmıştır. Aslında İnternet suç işlemek için harika bir mekândır çünkü küresel bir bağlantı, kimlik gizleme kolaylığı, izlenme ve takip edilme zorluğu ve hedef konusunda olağanüstü zenginlik sunmaktadır.

(2) İnternette suç işleme konusunda aktörlerin çokluğu kadar suç işleme motivasyonları da oldukça yüksek miktarda bulunmaktadır. Bu motivasyonlar geleneksel suçları içermektedir; pornografi, ekonomik ve askeri casusluk, siber savaş gibi.

(3) Birçok farklı fakat yaygın olarak kullanılan saldırı vektörleri bulunmaktadır. Sistemlerin ve kurumların içerisinden gelen tehditleri bir tarafa bırakırsak uzaktan yapılan ve sistem yapılandırma zayıflıklarını, güvenlik açıklıklarını ve sosyal mühendisliği kullanan saldırılar büyük tehditler oluşturmaktadır. Bu gerçek, kimliklerin tespit edilme güçlüğü ve takip edilebilme zorluğu ile birleştiğinde saldırı tespiti ve saldırganların cezalandırılmasını neredeyse olanaksız hale getirmektedir.

(4) İnternet, ortak kullanılan ve bütünleşik bir alandır. Bu alan vatandaşlar, iş çevreleri ve hükümetler tarafından paylaşılmaktadır ve bu grupları İnternet üzerinde birbirlerinden ayırmak neredeyse imkânsızdır. Tüm bunlara ilaveten, aynı ortam üzerinden eş zamanlı olarak konuşma serbestisi, ticari işlemler, casusluk faaliyetleri ve siber saldırılar gerçekleştirilmektedir.

(5) Bir saldırının potansiyel sonuçlarını tahmin etmek oldukça güçtür. Bilgisayar ağlarının taranması ve yetkisiz erişim gibi faaliyetler bilgi hırsızlığının bir başlangıcı olabileceği gibi veri tabanlarının zarar görmesine ve daha tehlikeli olanı veri tabanlarının değiştirilmesine sebep olabilir. Bütün bunlara ilave olarak sistemlerin birbirlerine karmaşık bir şekilde bağlı olması saldırganın niyetinden çok daha ileriye gidebilen zararlar doğurabilmektedir. Aynı zamanda bazı saldırılar açık olarak görünebilir ve müdahale edilebilir olmasına rağmen bazıları tespit edilemez şekilde gerçekleşmektedir.

2.3 Saldırı türleri

2.3.1 Sniffing

Sniffing temel olarak verinin yolunu kesmek olarak tabir edilebilir. Sniffing ile networkdeki paketler yakalanabilir içeriği okunabilir.

Kelime anlamı koklamak olan *sniffing*, bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi anlamına gelmektedir. Bunu yapmak için internette bol miktarda yazılım bulunmaktadır. Şebeke trafiğinin dinlenmesinde mantık, yönlendiricilere gelen her

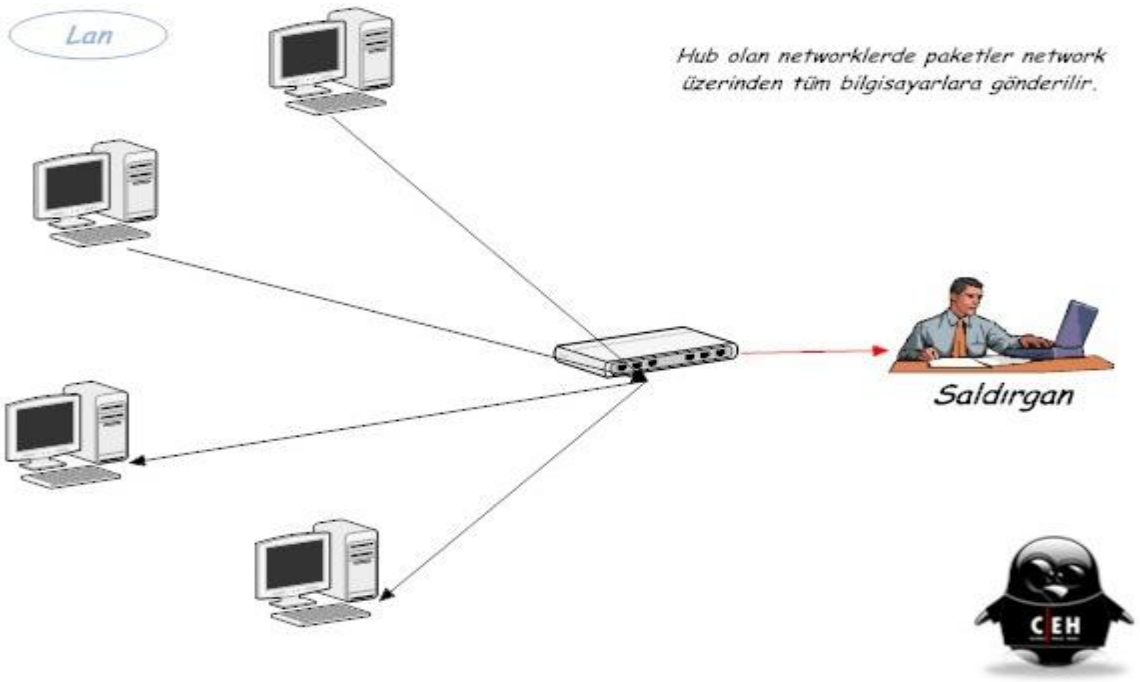
paketin kabul edilmesi dolayısıyla iki bilgisayar arasındaki tüm verilerin yakalanarak saklanmasıdır. Bu, korsanların kullandığı en önemli yöntemlerden birisidir. Bu yöntemden korunmak için bilgisayarlar arasındaki bağlantıların şifreli olması gerekmektedir. Kriptolu paketler de elbette dinlenip ele geçecektir ancak içeriğinden bir şey anlaşılamayacaktır. [4]

Sniffingin Amacı

Şifreleri (email, web, ftp, telnet,SQL) , Email text'ini Transfer edilen dosyaları (e-mail,ftp) yakalamaktır. Sniffing metodu ikiye ayrılır; Pasif Sniffing ve Aktif Sniffing.

2.3.1.1 Pasif Sniffing

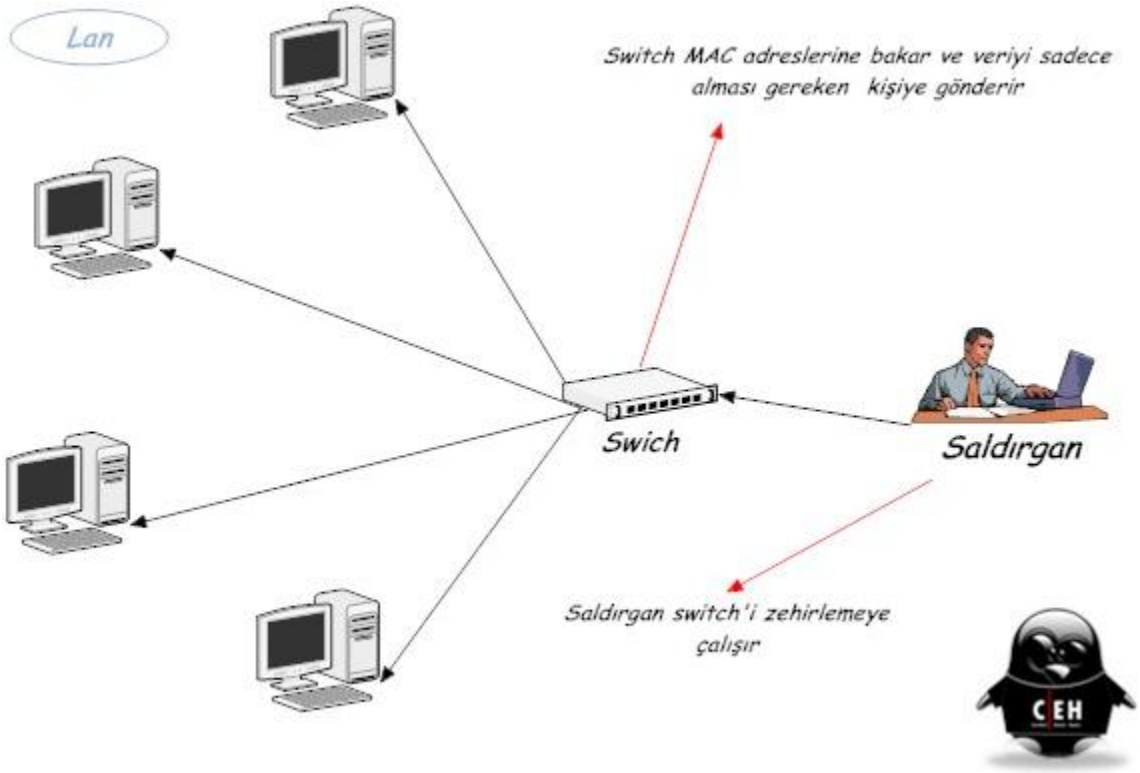
Hub olan sistemler için geçerlidir, Hub olan networklerde paketler tüm bilgisayarlara iletilir. Networkteki veri lan üzerinden tüm bilgisayarlara gönderildiği için sniff etmek kolaydır.



Şekil-2: Pasif Sniffing

2.3.1.2 Aktif Sniffing

Switch olan sistemler için geçerlidir. Switch MAC adreslerine bakar ve veriyi sadece alması gereken kişiye gönderir.



Şekil-3: Aktif Sniffing

Saldırgan switchi zehirlemeye çalışır, binlerce mac adresi gönderip switchin bir hub gibi davranmasına neden olur ve verinin tüm portlardan çıkmasını sağlar. [5]

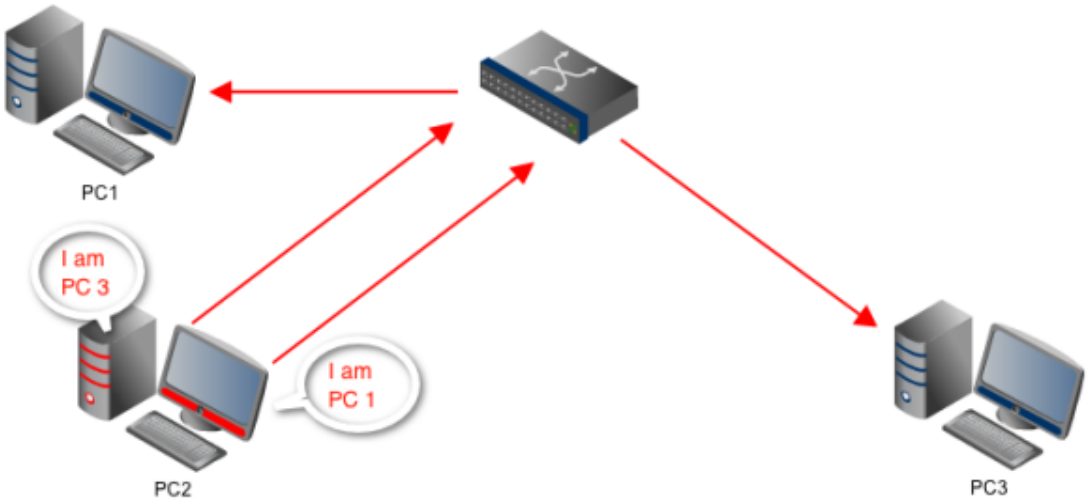
2.3.1.3 ARP Poisoning

Arp veri göndermek için IP adresinin mac adresini çözümlemeye yarayan protokoldür. Arp paketleri taklit edilerek saldırgan kendi makinesine verileri yönlendirebilir. Saldırgan ARP poisoning yaparak iki bilgisayar arasındaki trafiğin ortasına geçebilir. Switche yapılacak flood ile verinin tüm portlara göndermesi sağlanarak sniff yapılabilir.

Adım 1: Saldırgan IP adresinin ve Mac Adresini gateway miş gibi broadcast yaparak duyurur.

Adım 2: Kurbanın internet trafiği saldırgan üzerinden geçmeye başlar ve saldırgan kurbanın tüm internet verilerini yakalar.

Adım 3: Saldırgan trafiği router a yollar.



Şekil-4: ARP Zehirlenmesi

Korunma Yöntemleri

Network kartlarına fiziksel ulaşımı engelleyerek sniffer kurulmasını engellenebilir. Statik IP adresleri kullanın ve arp kayıtlarını statik olarak eklenebilir.

Netwrorkde sniffer olup olmadığını denetleyecek birden fazla araç vardır bunlardan bazıları ;

- Arp Watch
- Promiscan
- Antisniff
- Prodetect

- Network swithlerinde Port güvenliğini sağlayacak özellikler aktif edilmelidir. -Büyük işletmelerde farklı vlan'lar tanımlanabilir.[6]

- Snifferlardan korunmanın en iyi yolu trafiği şifrelemektir. Bunun için Networkte SSH kullanan Ipsec kullanılır. Bu snifferın çalışmasını engellemeyecek fakat yakaladığı verilerin anlaşılmasını engelleyecek veya kırılması için gereken süreyi uzatacaktır.

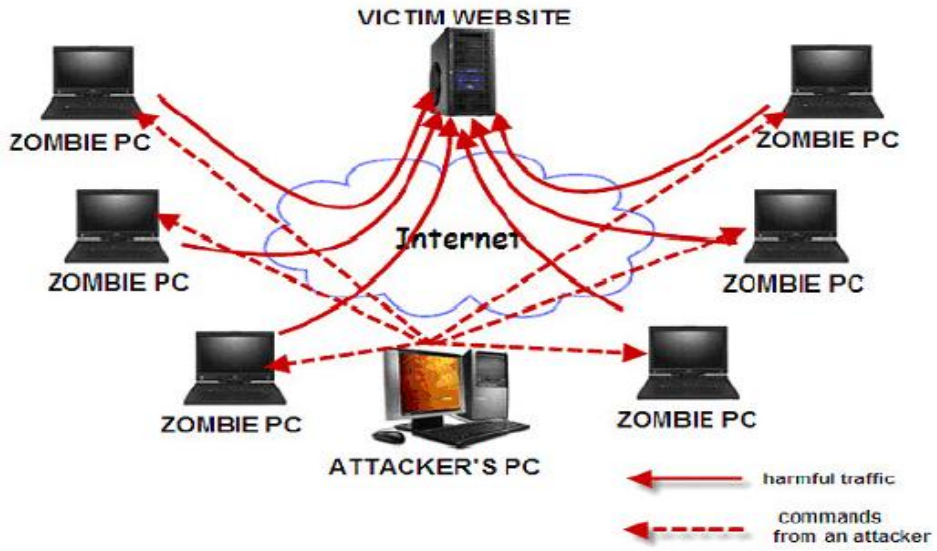
2.3.2 Hizmet Dışı Bırakma (Denial Of Service)

DoS(Denial of Service), hizmeti aksatma veya hizmetin işlevini tamamen yok etme anlamına gelmektedir. İnternet kullanıcılarına ya hiç hizmet veremez ya da çok yavaş bir hizmet sunar.

DDos(Distrubuted Denial of Service) saldırısı ise, saldırganın saldırıya geçmeden önce oluşturduğu makine veya bilgisayar topluluğu ile hedefe saldırmasıdır ve DoS gibi hizmet aksatma veya hiç hizmet veremez hale getirme amaçlanır. Bununla birlikte saldırgan kolay bir şekilde kimliğini belli etmeden gizlenebilir ve saldırganın tespit edilmesi zorlaşır.

1999 yılında Minnesota Üniversitesi öğrencileri tarafından ilki gerçekleştirilen DDoS saldırıları, 2000 yılında Trinoo'nun, CNN, Yahoo, EBay, Datek gibi siteleri hedef alması, 2002 Kök DNS sunucularını hedef alan **DDoS atağı** gerçekleştirilmesi, 2007 yılında Estonya siber saldırıları, 2008 yılında gerçekleştirilen Gürcistan siber saldırısı, 2010 yılında Wikileaks gerçekleştirdiği, TİB, BTK, TÜBİTAK yönelik saldırılar ve 2011 yılında Anonymous'un Malezya, Türkiye, Paypal, Mastercard gibi ülkelere gerçekleştirilmiştir. Bu saldırılar daha önceden tasarladığı birçok makine üzerinden hedef bilgisayara saldırı yaparak hedef sistemin kimseye hizmet veremez hâle gelmesini amaçlayan saldırılardır.

DoS saldırı türünde amaç sınırlı sistem kaynaklarının sınırını aşarak, sistemin devre dışı kalmasını sağlamaktadır.



Şekil 5: DDos Saldırısı

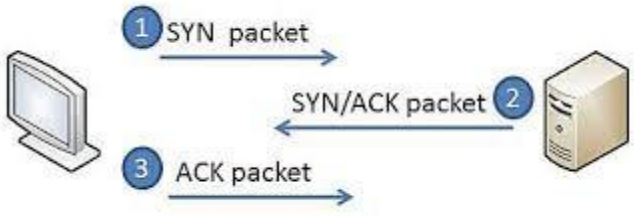
Saldırı DoS saldırısı olursa, yani tek bir IP üzerinden saldırı gerçekleşirse firewall'dan engellenebilir. Fakat DDoS saldırısında çok sayıda makine kullanıldığından, ip tespiti güçleşir ve firewall yakalayamayabilir. Log taşması sonucu firewall devre dışı kalabilmektedir. Bu nedenle DDoS, DoS saldırısına göre daha tehlikeli ve etkilidir. DoS saldırıları siber tehditler arasında 2. Sıraya girebilmektedir.

DRDoS, yani "Distrubuted Reflective Denial Of Service" DDoS'a benzerdir. Tek farkı, daha sık aralıklarla atak yapmak amacıyla ek ağlar kullanmaktadır.

DoS Saldırı Çeşitleri

TCP three handshake tamamlanmadan yapılan bir yöntemdir. Yani istemci bir SYN, sunucuda buna yanıt olarak SYN+ACK paketlerini yollar ve ACK paketini beklemeye koyulur. Buraya kadar herşey güzel. ACK paketi gelmez ise bu bağlantı full-duplex değil "yarı-açık" bir bağlantı olurdu. Ve bu bağlantı çeşidi pek iç açıcı değildir.

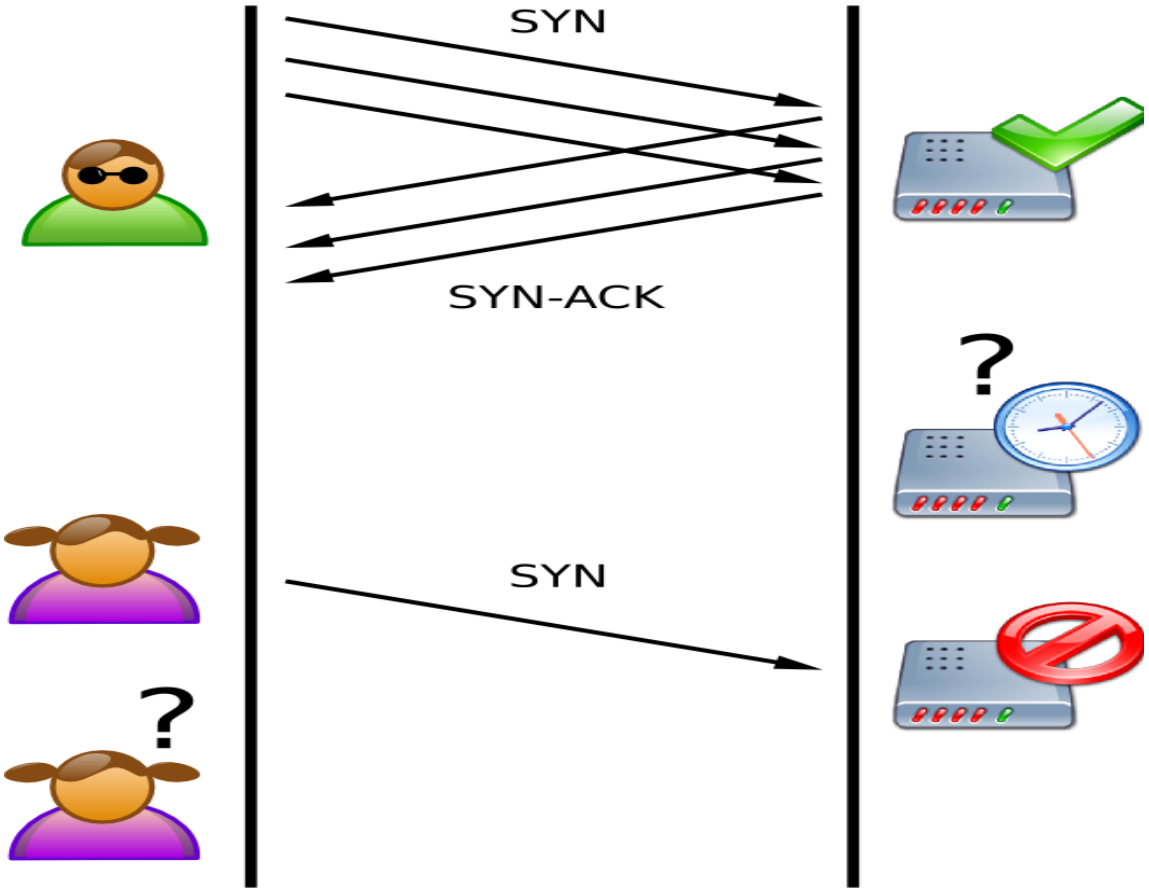
Sunucu SYN+ACK'yi yolladıktan sonra ACK için bekler. Fakat istemci ACK paketini yollamaz ise işler çıkmaza girer. Sunucu beklemeyi bırakmaz. Sürekli bekler.



Şekil-6: TCP three handshake

Sunucu ACK için beklerken, karşıya ACK yerine bir bağlantı talebinde daha bulunduğumuzu varsayalım. Ve yine 3. adım'ı gerçekleştirmeyelim. Yani son ACK'yi yollamayalım. Hatta bunun tekrar tekrar yapılması ile sonuçta **"flood"** oluşur.

Hedef makine, saldırı yapılan makineden yanıt alamayacağından dolayı, SYN-ACK paketini 5 kez tekrar edecektir. Bunun tekrar süreleri, 3, 6, 12, 24 ve 48 saniyedir. Ayırdığı kaynağı boşa çıkartmadan evvel, 96 saniye sonra son bir kez SYN-ACK denemesi yapacaktır. Hepsini topladığınızda, görüldüğü gibi hedef makine ayırdığı kaynakları 3 dakika gibi bir süre tutacaktır. Bu sadece her bir SYN atağı için gerçekleşecek süredir.



Şekil-7: TCP SYN Flood Saldırısı

Saldırgan bu tekniği tekrarlanan bir şekilde gerçekleştirdiği zaman, hedef makine ayırdığı kaynaklardan dolayı kaynak yetersizliğine kadar ulaşır ve artık yeni bir bağlantı karşılayamayacak duruma gelir. Ve bu durumda yetkili kullanıcılar bile makineye bağlanamaz. Yetkililer ne kadar bağlantı iptal ederlerse etsinler, yenileri eklenecektir.

TCP-SYN oturumu host ile client arasında kurulduktan sonra ACK veya PUSH ACK paketleri iletişim için kullanılır. Bu ACK paketleri kurban server'i n kaynaklarını tüketmeye başlarsa **ACK & PUSH ACK Flood** olarak adlandırılan atak gerçekleşmiş olur.

Eğer atak türü kurban nerwork'un bank genişliğini sömürürse, buna **ACK & PUSH ACK Flood** türü olan **Fragmented ACK** denir. Atak'da 1500 byte uzunluğunda paketler kullanılır.

TCP-SYN oturumunu sonlandırmak için **RST veya FIN**(açık olan TCP iletişim handshake oturumunu sonlandırma isteği) server değiştirir. **RST veya FIN** atak esnasında, kurban server **RST veya FIN** paketlerini yüksek oranda kaydeder ve sonuç olarak server'in kaynakları tükenmeye başlar(hafıza, CPU, RAM, vb.). Bu da **RST veya FIN Flood** olarak bilinir. Server bunu karşılayamazsa performansı azalır, isteklere cevap veremez veya kapanır.

2.3.2.1 Land Flood

SYN Flood'a çok benzerdir. Bu atak çeşidinde saldırganlar (hacker) hedef sistemin IP adresini, source (kaynak) IP adresi olarak kullanarak networkü SYN paketleri ile istila ederler. Bu durumda host bilgisayar sanki paketleri kendi kendine göndermiş gibi görünür. Böylece, yukarıda söz ettiğimiz üç aşamalı bağlantı zincirinde(Three Way Handshake), hem dışarıdan paket almış, hem de kaynak kendisi olduğundan kendisine cevap vermiş olur. Böylece hedef sistem bir paket alması gereken birim zamanda iki paket alır ve saldırının boyutu da iki katına çıkar. Yani hedef sistem kendi kendine yanıt vermeye çalışırken sistem kullanılamaz duruma gelir.

2.3.2.2 UDP Flood

UDP, TCP'den en temel farkı belirttiğimiz gibi verinin ulaşıp ulaşmadığını garanti etmez. 3 yollu el sıkışma olmaması ve trafiğin karşı tarafa ulaşıp ulaşmadığını kontrol etmemesinden dolayı daha hızlı çalışır. UDP saldırısı uzaktaki bir bilgisayarın rastgele portlarına çok sayıda UDP paketi göndererek başlatılabilir. Bu durumda saldırıya uğrayan uzaktaki makine:

1. Portu dinleyen bir uygulama var mı diye kontrol eder;
2. Hiçbir uygulamanın o portu dinlemediğini görür;
3. ICMP "Hedefe Ulaşılamıyor" paketi ile cevap verir.

Böylece, çok sayıda UDP paketi gönderilmesi durumunda, mağdur sistem de yanıt olarak çok sayıda ICMP paketi göndermeye zorlanır ve bu da onun diğer istemciler tarafından erişilemez

duruma gelmesine yol açabilir. **Saldırganın UDP paketlerinde sahte IP adresi olabilir, bu durum geri dönen ICMP paketlerinin ona ulaşmamasını** sağlar ve saldırganın bağlantı konumunu anonimleştirir.

Bu saldırı, istenmeyen ağ trafiğini filtrelemek üzere ağ içindeki kilit noktalara güvenlik duvarları kurularak yönetilebilir. Böylece, hedefteki makine UDP paketlerini asla almaz ve kötü niyetli UDP paketlerine asla cevap vermez. Çünkü güvenlik duvarı onları durdurur.

UDP Fragmentation: UDP flood türüdür. Büyük paketler kullanarak (1500 byte) band-genişliğini sömürür. Bu paketler birbirleri ile ilişkisi yoktur ve paketler sunucuda birleştirilmeye çalışılır. Bu paketler birleştirilmeye çalışılırken CPU kaynağı harcanacaktır. Bu sistemin yeniden başlamasını sağlar veya sistemin kapanmasına yol açar.

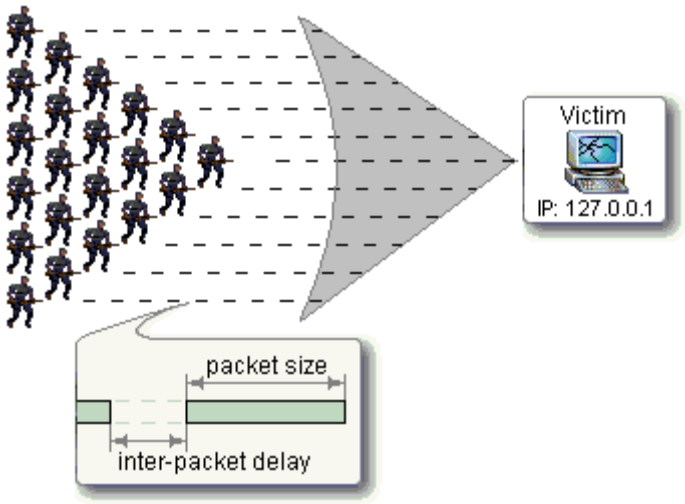
VoIP Flood: Özelleştirilmiş bir UDP Flood türüdür. Kurban VoIP server, yüksek sahte VoIP paketleri ve uzun IP dizilerini kaydeder. Network'u rasgele paket içeriğiyle ve iyileştirilmiş kaynak IP adresi ile istila eder.

Non-Spoofed UDP Flood: Bu atak yapılırken, kurban server sahte UDP paketi olmayan paketleri kaydeder ve gelen UDP paketlerin büyük miktarı istila eder. Atak network kaynaklarını tüketir ve sistem kapanır. Atak sırasında kullanılan IP sahte olmayan BOT'ların IP'sidir.

2.3.2.3 ICMP Flood

Bu saldırı, ICMP (Internet Control Message Protocol) protokolünü hedef almaktadır. Bu sistemin özelliği, saldırının birden çok noktadan yapılması durumunda başarılı sonuç vermesidir. Aksi takdirde çok bir etkisi olmayacaktır. Bu saldırılar özellikle Linux üzerinden yapıldığında başarılı sonuçlar vermektedir ve saldırı için bazı özel komutlar kullanılmaktadır. Örnek olarak **"ping –s ip"** komutuyla 64 kb'lık paketler gönderilebilmektedir. Bu komutun, birçok farklı noktadan gönderilebileceği düşünülürse, oldukça etkili olduğu görülür.

ICMP, genel olarak sistemler arası iletişim ve hata ayıklama amacıyla kullanılan bir protokoldür. Hepimizin siyah ekran, cmd diye tabir ettiği komut satırı açarak yapabildiğimiz ping komutu bu protokol üzerinde çalışmaktadır. Bunun için CMD'ye **"ping –l 65510 ip"** yazmak işi görecektir. İstemci sistemin, hedef sisteme gönderdiği ICMP Echo Request (TYPE 8) paketine karşılık hedef sistem ICMP Echo Reply (TYPE 0) paketi gönderir. Böylece biz, hedef sistemin ulaşılabilir olduğundan emin oluruz. Burada hemen belirtelim, cevap gelmemiş olması sistemin ayakta olmadığını göstermez.



Şekil-8 : ICMP Flood Saldırısı

Bu yapıdan faydalanılarak, saldırgan makineler çok sayıda ICMP Echo Request (type 8) paketi gönderir. Kurban sistem, gelen tüm bu isteklere cevap vermek için çaba harcar ve sistem yorulmaya başlar. Sistem kaynakları bunlara cevap veremez hale gelir ve sistem erişilemez duruma düşer.

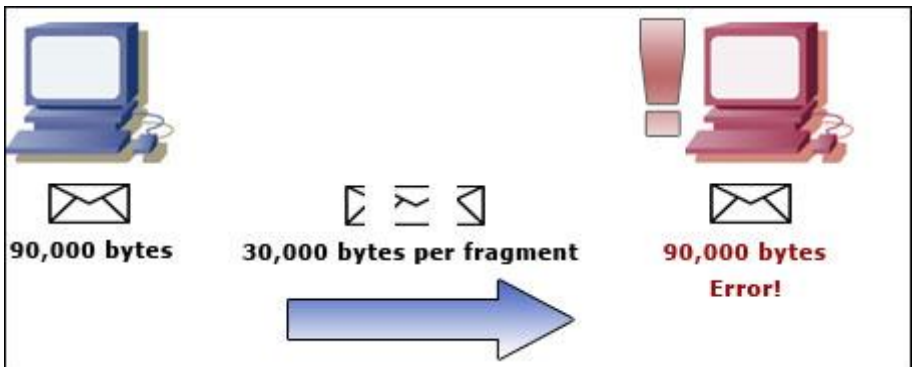
ICMP Fragmentation: Kurban server sahte, büyük ICMP paket parçaları (1500 byte) kaydeder ve bu baketler birleştirilemez. Büyük paket dizinleri ICMP atağın bant genişliğini artırır. Kullanışsız paketlerin birleştirilmesi girişiminde bulunduğunda CPU kaynakları devre dışı kalır. Ve fazla yükleme olduğunda yeniden başlayacaktır.

2.3.2.4 Finger

Finger, belirli bir kullanıcı hakkında bilgi veren programdır, ayrıca kendi sisteminizde veya uzak sistemde giriş yapmış kullanıcıları listelemek için de kullanılır. Genelde kullanıcının tam adını, ne kadar zamandır işlem yapmadan beklediğini, hangi terminal hattından bağlandığını ve terminalin yerini gösterir. Bunlara ilaveten eğer mevcutsa kullanıcıya ait. Plan ve. project dosyalarını görüntüler.

Farklı hostlar üzerinden saldırılacak sunucuya sürekli finger çekiliyorsa bu işlem sonucunda oldukça fazla bant genişliği gitmiş olur. Saldırı birçok farklı noktadan yapıldığından etkisi oldukça büyük olmaktadır.

2.3.2.5 Ping of Death (Ölüm Pingi)

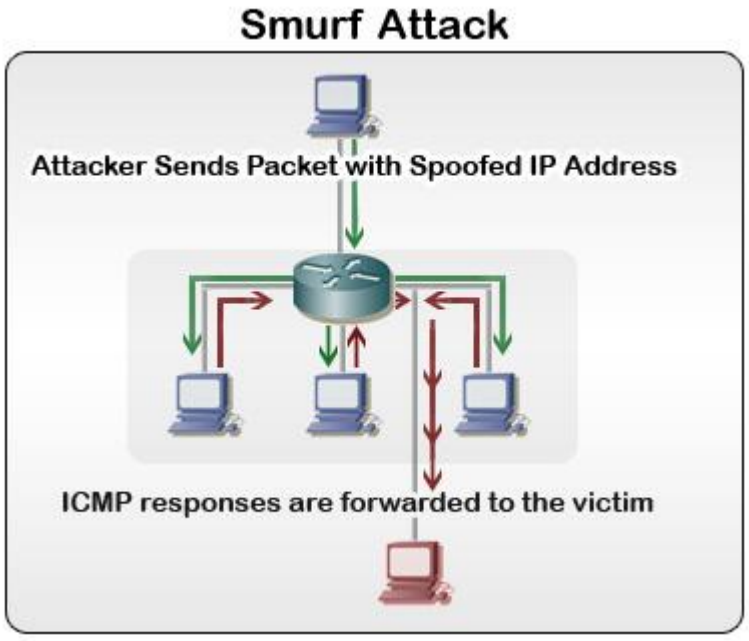


Şekil-9: Ölüm Pingi

Neredeyse bütün işletim sistemleri bu tür bir saldırıya karşı önlemini aldıysa da zamanında çok etkili bir yöntemdi. Bu yöntemin mantığı şöyle çalışır: ICMP protokolü ağda bilgisayarların hata mesajlarını birbirlerine göndermesini ya da 'Ping' gibi basit işlemlerin yapılmasını sağlar. ICMP spesifikasyonunda, ICMP Echo request'lerin data kısmı 216 ile 65,536 byte arasında olmak zorundadır. Eğer bu veri sınırlarının dışına taşmış bir paket kurban sisteme yollanırsa işletim sistemi böyle bir şey beklemediği için çalışamaz duruma gelecektir.

2.3.2.6 Smurf

Smurf atakta, hacker kurbanı birçok "çöp" paketi ile tıkar, kurbanın band genişliği kullanılır. Bir smurf atakta, hackerlar sıkça kullanılan bir İnternet servisini sömürürler-ping(*Internet Control Message Protoco*l). Ping, genelde belirli bir bilgisayar ya da serverin İnternete bağlı çalışır olup olmadığını anlamak için kullanılır. Bir bilgisayar ya da servera bir ping paketi gönderildiğinde, pingi yollayan kişiye bir cevap paketi yollar, "evet burdayım!" demiş olur (Bir networke yollanıldığında networkteki tüm bilgisayarlar cevap verir). Ping edilen network, saldırı hedefi değildir. Bir smurf atakta, hackerlar ping isteklerindeki geri dönüş adreslerini değiştirirler, böylece bu cevap paketleri kendilerine değil de hedeflenen adrese gider. Bunun iki nedeni vardır: hem hedefe saldırır, hem de ping request üzerinde kendi adresi bulunmadığı için yakalanmaktan kendini korur.



Şekil-10: Smurf Saldırısı

Ping istekleri aralıksız bir şekilde networkün "*directed broadcast*" adresine yollanır. Bu adres, geriye, networke bağlı her bilgisayara ping isteklerini yollar-ki bu da birkaç yüz belki de daha fazla bilgisayar eder. Yani bir ağdaki tüm bilgisayarlar işleme karışmış olur.

Bu birkaç yüzden fazla bilgisayarın herbiri ping isteğine cevap yollar. Bilgisayarlar, cevap paketlerini, ping isteğinin üzerinde adresi yazan hedefe yollar. Bunlar hackera gönderilmez çünkü o, önceden ping isteğindeki adresi değiştirmiştir.

Hedef yüzbinlerce ping cevap paketini saniyeler içinde alarak tıkanır-basit bir networkten saniye başı 5Mblik datadan fazlası demektir. Ping paketleri hedefinin tüm bant genişliğini kapladığından, her saniye gelen bu kadar fazla data yüzünden hedef kullanıcıları data alışverişi yapamazlar. E-mail yollayıp alamaz, webde gezemez veya herhangi bir başka Internet servisi kullanamazlar.

Hedefin bu smurf ataklara karşı savunması zordur çünkü ping cevaplama paketleri hackerdan değil, yasal networkten gelir. Hedef, ping cevaplama paketlerinin nereden geldiğini ortaya çıkarmalı, sonra herbir networke bağlanmalı ve onlara ping cevaplama paketlerini kapamalarını söylemelidir. Bunu güçleştiren, hedef sistem kapandığında müşteriler ping isteği yollayıp, onun canlı ve Internete bağlı olup olmadığını öğrenmek ister. Bu nedenle de hedef sistem uygun ping paketlerini, smurf atak paketlerinden ayırabilmekte güçlük çeker.

ISP ler ve Internet routerlara yerleştirmek için smurf koruma özelliği olan yazılımlar kullanılmaktadır. Ancak sadece birkaç şirket bu yazılımı kullanmaktadır.

2.3.2.7 Fraggle

Fraggle da Smurf ile aynı mantığa sahiptir, sadece tek fark olarak UDP paketlerini 7 ile 19 (Unix sistemlerde) numaralı portlara iletir.

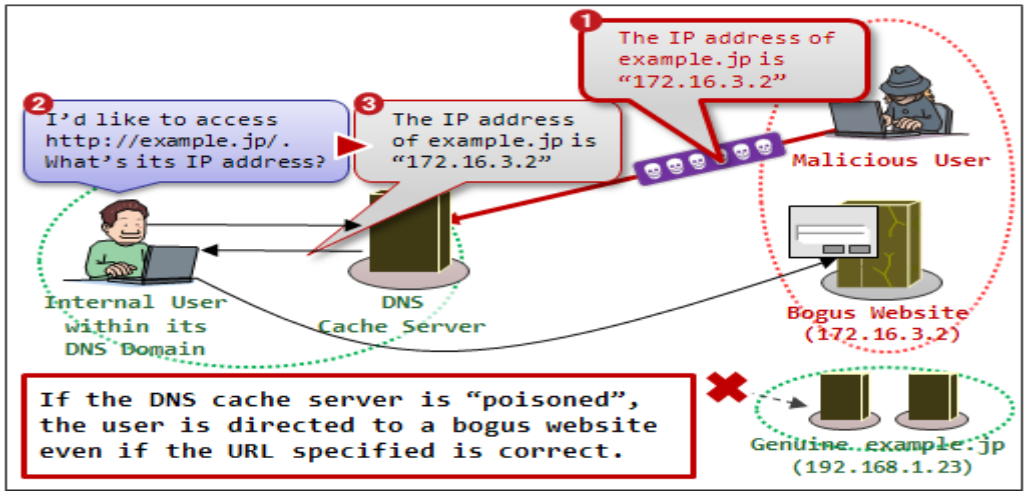
2.3.2 8 DNS Poisoning (DNS Zehirleme)

Alan Adı Sunucuları istemciler ve web sunucuları arasındaki haberleşmenin sağlanması amacıyla kullanılan IP adresinin sayısal değerini, insanın okuyabileceği gibi bir alan adına çeviren sunuculardır.

Bir DNS sunucusu, gerçek olmayan bir veriye sahip olduğunda ve bu veriyi performansı en uygun seviyeye getirebilmek için ön belleğe aldığında, DNS sunucusu bir zehirlenme olduğunu dikkate almaktadır.

Normal olarak ağ tabanlı bir bilgisayar bir ISP veya kullanıcının bilgisayarı tarafından sağlanmış bir DNS sunucusu kullanır. DNS sunucuları önceden elde edilen sorgu sonuçlarını önbellekleyerek cevap performansı duyarlılığını artırmak için genellikle bir organizasyonun ağında dağıtılır. Bir DNS sunucusundaki zehirleme atakları, eğer uygulanabilirse, direk gizliliği ihlal etmiş bir sunucudan veya dolaylı olarak onun aşağı sunucusu veya sunucularından sunularak kullanıcılara etki edebilir.

Bir önbellek zehirleme atağını yapabilmek için, saldırgan DNS yazılımındaki bir kusuru istismar eder. Eğer sunucu doğru bir şekilde güvenilir bir kaynaktan geldiğine emin olmak için doğrulama yapmazsa sunucu doğru olmayan girdileri yerel olarak önbelleklemeyi sonlandıracak ve onları diğer kullanıcılara aynı isteği yaparak sunacaktır.



Şekil-11: DNS Zehirlemesi

Bu teknik kullanıcıları bir siteden saldırganın seçtiği başka bir siteye yönlendirmek için kullanılabilir. Örneğin, bir saldırgan verilen bir DNS sunucusundaki bir hedef websitesi için IP adresi DNS girdilerini onun kontrolündeki sunucunun IP adresiyle değiştirerek zehirler. Sonra hedef sunucusundaki isimlerle eşleşen onun kontrolündeki sunucuda dosyalar oluşturur. Bu dosyalar bilgisayar solucanı veya virüs gibi zararlı içerikler içerebilir. Zehirlenmiş DNS sunucusuna referans edilmiş bilgisayara sahip bir kullanıcı güvenilir olmayan bir sunucudan gelen içeriği kabul ederek kandırılmış olacak ve farkında olmadan zararlı içeriği indirmiş olacaktır. DNS sunucuya, yanlış DNS bilgileri tanıtılarak, istekler değiştirilmiş olan DNS sunucuya iletilir.

2.3.2.9 Buffer Overflows (Hafıza Taşmaları)

Bilgisayarlarda bulunan bufferlar, belli bir kapasiteye sahiptir. Kapasitenin aşıldığı durumlarda kitlenme, reset atma gibi durumlar oluşabilmektedir. Hafıza taşması saldırı tipinde de çok fazla veri gönderilerek trafik yoğunlaşır ve iletişim engellenir. Bu sebeple, saldırganlar büyük boyutta ping göndermeyi tercih etmektedirler.

2.3.2.10 HTTP Fragmentation

Bu saldırıda, server ile BOT arasında geçerli bir HTTP bağlantısı kurulur. Sistem alarm vermeden açılan oturum süresi uzun tutulabilmektedir. Bir çok server tasarlanan uygunsuz time-out mekanizması için, HTTP oturum zamanı, periyodik olarak uzatılabilir. Saldırgan, açılan periyodik uzatılmış oturumlar tarafından web serveri bir miktar Bot'lar ile durdurabilir.

2.3.2.11 Excessive VERB

Atak yapan BOT kurban web server'a geçerli HTTP isteğinde bulunur. Bu istekler web sayfa veya resim gibi büyük boyutlu yanıt GET veya POST istek türleridir. Her bir bot

saniyede 10'dan fazla istek oluşturabilir. Burada server'in band genişliği fazla artmaz. Fakat kurban kaynakları tüketilerek yanıt veremez duruma gelmektedir.

Recursive GET: Bir VERB atak türüdür. Saldırgan bir kaç sayfa veya resim toplar ve GET isteği üretir. Bunu belirlemesi zordur çünkü yasal bir istek oluşturulmuştur.

Radom Recursive GET: Bu atak Recursive GET'nin modifiye edilmiş halidir. Daha çok indeksli olan forum ve haber sitelerinde kullanılır. GET isteklerine rastgele geçerli olabilecek sayfa dizin numaraları eklenir. İstenilen her biri bir öncekinden farklıdır.

2.3.2.12 Faulty Application

Saldırgan uygulamanın zayıf dizaynından veya database ile zayıf etkilişimden kaynaklanan kusuru kullanabilir. SQL injection gibi atak'lar üreterek server'in kaynaklarını sömürebilir(hafıza, CPU, vb.).

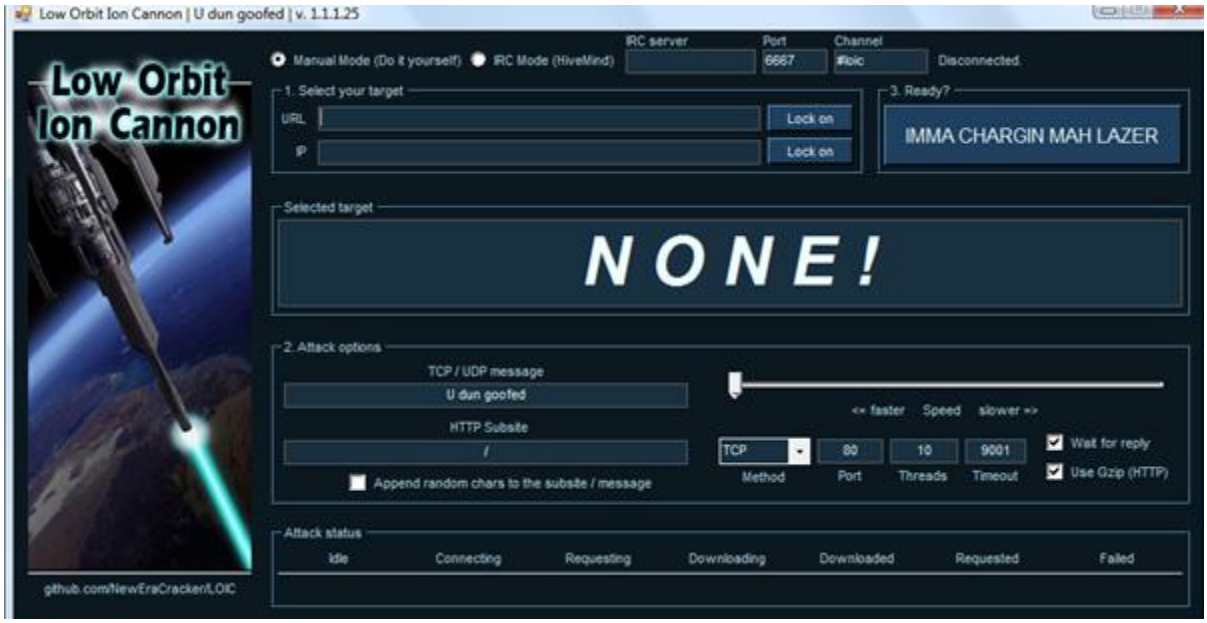
2.3.2.13 Media Data Flood

VoIP ek olarak, UDP flood bir kaç media paketi aldığında oluşur. Atak sırasında, kurban server media veri paket basınlarını yüksek bir veri ve çok uzun bir IP dizisiyle kaydeder. Sistem bunu karşılayamaz ve istila edilmiş olur. Network kaynakları sömürülür ve kapanır. VoIP gibi Media Data flood networku rastgele paketler ve iyileştirilmiş IP adresleri ile baskı uygular. Böylece network bant genişliği tüketilir. [7]

DDos Savunma Yöntemleri

Anonymous tarafından daha önceleri çeşitli nedenlerden Scientology'e, Wikileaks sitesine gelen mali yardımların kesilmesini sağlayan PAYPAL ve Mastercard'a ve Türkiye'deki BTK, TİB gibi birçok kuruma karşı DDoS atağı gerçekleştirmiş ve Anonymous üyelerinin de bu saldırılarda rol alabilmesi için **LOIC** adlı yazılımı geliştirmişlerdi. Bu yazılıım ağ stres testi aracı olarak kullanılabilmektedir. Fakat Anonymous bu aracı DDoS

saldırıları gerçekleştirmek için kullanmaktadır. Low Orbit Ion Cannon yazılımını indiren Anonymous üyeleri belirlenen hedef adreslere DDoS saldırısı yapabilmektediler. Bu saldırılar LOIC ile **HTTP GET, TCP** ve **UDP flood** şeklinde gerçekleştiriliyor.



Şekil-12: Anonymous LOIC Saldırı Yazılımı Arayüzü

Anonymous grubu LOIC aracı ile yapılan saldırıların etkisin arttırmak ve daha fazla gönüllü üye ile saldırıyı gerçekleştirmek için bu aracı web üzerinden çalıştırabilecek hale getirdi. **drive-by-download*** saldırıları gibi herhangi bir web sitesine enjekte edilmiş bir kod ile ya da kullanıcıya içerisinde bu zararlı kodun olduğu bir siteye girdirmek sureti ile saldırı otomatik olarak başlayacak şekilde tasarlanmıştır. Kullanıcı herhangi bir siteden içerisinde LOIC javascript versiyonu enjekte edilmiş bir sitenin linkine tıkladığı andan itibaren DDoS saldırıları devam edecektir.

Siteye giren kullanıcılar üst tarafta bulunan twitleri ya da yazılan mesajları okumaya başladığı andan itibaren alt tarafta bulunan JavaScript kod parçası belirlenen adreslere anlık olarak bağlantı kurmaya başlatmaktadır. Yapılan bu GET istekleri hedef olarak seçilen web sunucuyu cevap veremeyecek duruma sokmaktadır. Son kullanıcı hedef olarak belirtilen

siteye girmeden herhangi bir etkileşime girmeden JS kodunda hedef olarak belirlenen sisteme DDoS atağı gerçekleşmektedir. Sitede o an kaç aktif kullanıcı var ise saldırının boyutu da lineer olarak artmaktadır.

Kullanıcı eğer farkında olmadan bu saldırıya katılmış ise genellikle **msg** alanında herhangi bir değişiklik yapmayacaktır. Ama gönüllü olarak bu saldırıyı gerçekleştiriyor ise **msg** alanının değiştirip gönderebilir. Böyle bir durumda snort imzasını gelen ataklara göre güncellemek gerekir. Fakat bu değişiklik de atağı durdurmak için yeterli olamayabilir. Böyle bir durumda daha ayrıntılı ağ trafiği analizi ile IDS imzaları güncellenebilir. Hedef alınan servislere gelen istekler kısıtlanabilir. Örneğin belirli bir IP adresinden dakikada yapılacak HTTP GET isteklerini sınırlama gibi.

Ayrıca son kullanıcıların bu saldırılara dahil olmalarını engellemek için internet tarayıcılarına NoScript benzeri tarayıcı eklentileri ile saldırıya istemsiz olarak katılımı engellenebilir. İstemci tarafında çalışacak güvenlik yazılımları ile kullanıcının erişim yapacağı sitelere olan istekler limitlenebilir.

Giderek daha karmaşıklaşan bu tür ataklara karşı hem kullanıcıların istemsiz olarak saldırıya katılımını engellemek, hem de kendi sunucularımızı bu tür saldırılardan korumak zorlaşmaktadır. Mümkün olduğu kadar ağ trafiği analiz edilmeli ve bu atağa uygun Güvenlik Duvarı kuralları ve Saldırı Tespit/Engelleme Sistemleri imzaları güncellenmelidir. Son kullanıcılar bu tür ataklara karşı bilgilendirilmelidir.

DOS/DDOS saldırıları internet dünyasının başlangıcından beri önemi gitgide atan bir tehdittir. Güvenlik açıklıkları kapatılsa da TCP/IP Protokolünün yapısı değişmeden bu soruna kesin bir çözüm bulunamayacaktır.

HTTP-GET DDoS Atak Engelleme

- Apache Web Sunucu
- Alan ismi : www.xx.com

Yukarıda belirtildiği gibi üzerinde Apache Web Sunucusu çalışan bir sunucumuz bulunmakta. Web sunucumuz üzerinde çalışmakta olan www.xx.com adresine saniyede binlerce IP adresinden HTTP-GET isteği yapılmaktadır.

Bu durumda Apache belli bir sure sonra bu isteklere yanıt verememeye başlayacaktır. Eğer istekte bulunulan sayfanın bağlandığı bir veritabanı sunucumuz mevcut ise, bu istek veritabanımızın da yanıt verememesine sebep olacaktır.

Peki ne yapacağız?

Öncelikle şunu bilmeliyiz ki; her bir HTTP-GET isteği için ayrı bir bağlantı oluşturulmasına gerek yoktur. Çünkü HTTP/1.1, açılan bir bağlantı içerisinden dilediğimiz kadar istek göndermemize izin verir. Bu bilindiği gibi **Request Pipelining** olarak adlandırılmaktadır. Bu da demek oluyor ki güvenlik duvarımızda (donanımsal ya da yazılımsal) TCP 80 portuna gelen sadece bir HTTP-GET isteği görebiliriz ama aslında bu istek içerisinden binlerce istek alıyor olabiliriz.

- Bir HTTP-GET atağında öncelikle yapmamız gereken şey web sunucumuzun loglarını incelemek olacaktır. Çünkü bu loglar içerisinde bizim IDP (Intrusion Detection & Prevention) sistemimiz üzerinden engelleyebileceğimiz sabit bir data bulabiliriz. Mesela sabit bir HTTP başlığı, referrer veya user-agent tespit edip IDP sistemimiz üzerinden engelleyebiliriz.
- Eğer gelen istekler değişik çerezler ile geliyorsa ve bu alanda yapabileceğimiz ekstra bir şey yoksa ikinci bir önlem olarak, bir dakika içerisindeki web server loglarına bakarak en çok isteği yapan IP adreslerini daha sistemimize ulaşmadan engelleyebiliriz. Ama örneğimizde olduğu gibi farklı kaynaklardan gelen istekleri bu şekilde engellememiz fazla mümkün olamayacaktır. Çünkü karşı karşıya olduğumuz atak türünde saldırılar binlerce farklı IP adresinden gelmekte ve bu IP adresleri sürekli değişmektedir.
- Bir sonraki aşama olarak IDP' miz ya da güvenlik duvarımız üzerinde **TCP Bağlantı Limiti** (Connection Limit) koyarak ve eşik değerini (threshold) düşürerek saniyede gelen bu aşırı HTTP-GET isteklerini daha web sunucumuza ulaşmadan engelleyebiliriz. Bu genellikle etkili olan ve saldırganın başarısını azaltan bir engelleme mekanizmasıdır. Ama bu durumda gelen istek HTTP-GET isteği olduğu için güvenlik duvarımız ya da IDP'miz hangi isteğin

doğru hangi isteğin yanlış olduğunu anlayamayacak ve bu durumda siteye normal olarak ulaşmak isteyen kişilerin isteklerinin de engellenme ihtimali söz konusu olacaktır. Ayrıca bu işlemde bile eğer atak çok büyük ise güvenlik sistemimizden kaçan istekler arka taraftaki web sunucumuza ulaşacak ve sitemizin sağlıklı çalışmasına engel olacaktır.

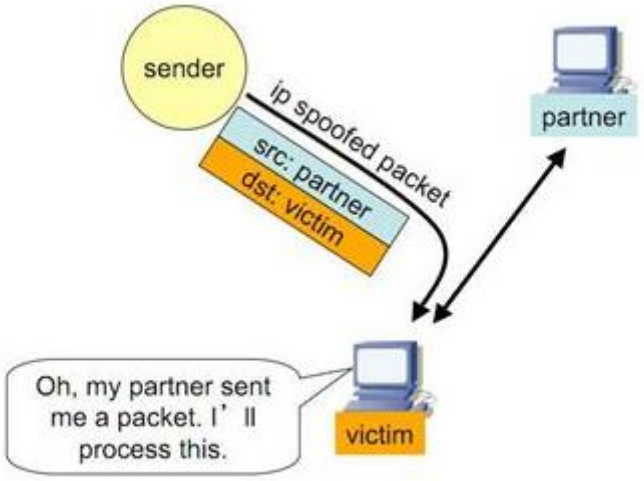
TCP Bağlantı Limitleme işleminin yanı sıra Apache sunucumuz üzerine bir **Ters Vekil Sunucu** (Reverse Proxy) kurup, sayfaların ön belleklenmesini sağlayarak gelen bu isteklerin sunucu tarafında herhangi bir TCP bağlantı açmadan alınmasını sağlayabiliriz. **Nginx** bu amaçla kullanılabilecek faydalı bir yazılımdır.

Bu işlemlerin sonucunda bağlantı limiti (IDP ya da güvenlik duvarı) ile saniyede belirttiğimiz limitin üzerinde gelen istekler engellenecek ve ters vekil sunucumuzun sayesinde gelen istekler daha Apache'ye ulaşmadan ön bellek üzerinden verilecektir. Ters vekil sunucumuzu kurduktan sonra IDP veya güvenlik duvarımız üzerinde yaptığımız bağlantı limiti eşik değerini yukarılara çekerek testlerimizi yapabiliriz. Bu testlerin sonucunda saldırı amaçlı bağlantılar ile sitemize normal yollardan ulaşmak isteyen kullanıcılar arasında bir denge kurulacak ve hatalı engellemelerin önü alınacaktır. [8]

2.3.3 IP Aldatması (IP Spoofing)

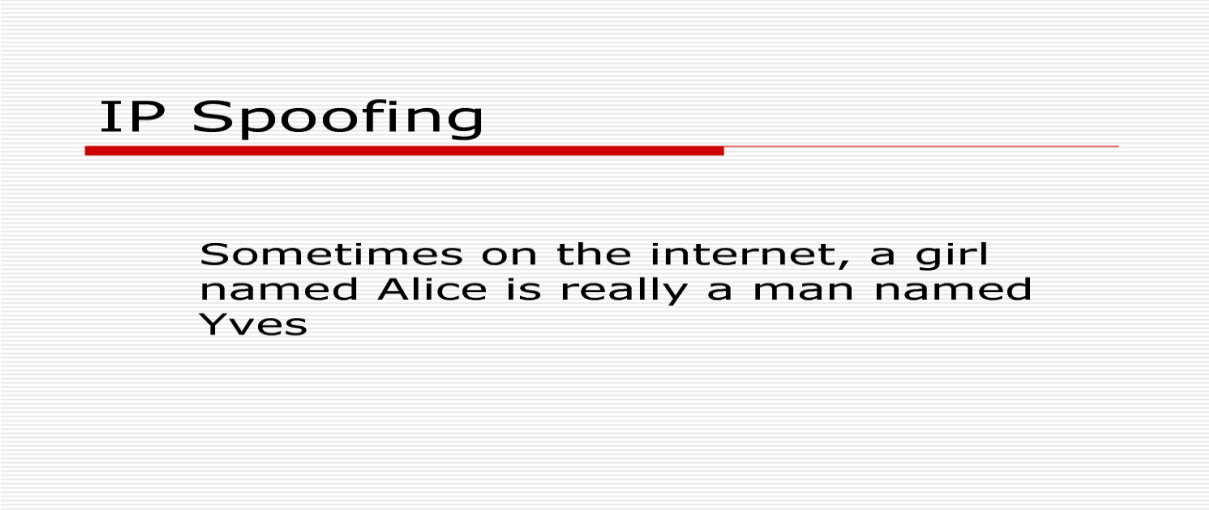
Bilgisayarlar arasındaki bağlantı çeşitli protokoller aracılığıyla sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında bağlanan bilgisayar kendi kimliğini karşı tarafa tanıtır. Bağlanılan bir bilgisayara gerçek IP adresinin gösterilmemesi yani asıl kimliğin gizlenmesine **IP spoofing** (Aldatma) denir. Sahte IP paketi alan bilgisayar, paketin gerçekten gönderilen adresten gelip gelmediğini bilemez. Bu genellikle başkasının IP adresinden mail gönderilmesi veya forumlara mesaj yazılması olarak karşımıza çıkmaktadır. Teoride bu durum mümkün olmakla birlikte pratikte karşıdaki sistem gerçekten ele geçirilmeden başkasının bilgisayarına farklı bir IP'den bağlanma gerçekleşemeyecektir. Günümüzde IP spoofing için kullanılan ticari ve ücretsiz yazılımlar bulunmaktadır. [9]

Aldatma genel olarak bir web sitesini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.



Şekil-13: IP Aldatması

Aldatma genel olarak bir web sit esini işlemez hale getirmek için saldırı esnasında kaynağı gizleme maksadıyla kullanılmaktadır.



Şekil-14: IP Aldatması 2

Genel Anlamda (Spoofing'den) Korunma Yöntemleri

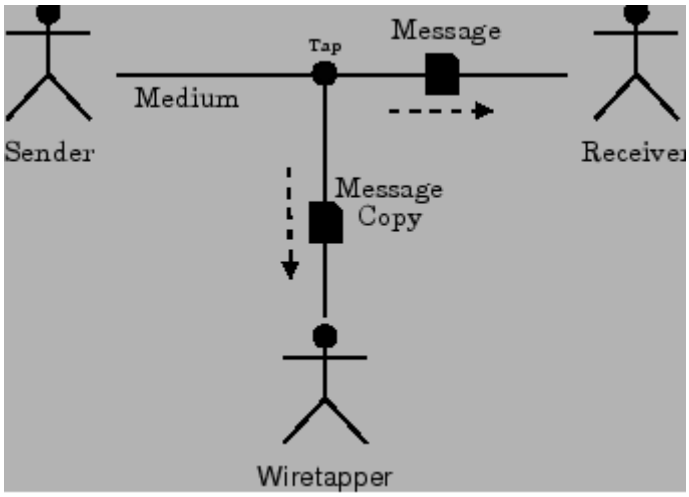
IP Spoofing olayını engelleyebilmek için öncelikli olarak Yönlendiricilerde, Kaynak Yönlendirme fonksiyonunu pasife alınmalıdır. Çünkü kaynak yönlendirme çok kısıtlı ve pek nadir kullanılır. Bu nedenle ağa giren ve çıkan bu trafik engellenmelidir.

Sisteminizde filtre uygulanmalı ve yetkiler kısıtlanmalıdır. Şöyle ki; sistemde IP adreslerini değiştirme hakkı kaldırılmalıdır. Dolayısıyla (IP) Spoofing'in önüne geçilebilir.

Bunlara ek olarak bir takım yazılımları kullanabilirsiniz. Bu yazılımlar Spoofing yapılırken uygulanan metotlara rastladığı zaman size haber verir.

2.3.4 Kabloya saplama yapma

Kabloya saplama yapma, özellikle emniyeti alınmamış iletişim ağı kablolarına özel teçhizat kullanarak fiziksel olarak saplama yapılması ve bağlantı kurulmasıdır.



Şekil-15: Kabloya Saplama

Kabloya saplama yapıldığında, iki taraf arasındaki tüm trafiğin ele geçirilmesi mümkündür.

2.3.5 Kriptografik Saldırılar

Kriptanaliz ve Kriptosistemlere Saldırılar:

Kriptanaliz; uygun anahtarların bilinmeden şifrelenmiş iletişimlerin çözülmesi sanatıdır. En önemli kriptanaliz tekniklerinden bazıları aşağıda verilmiştir:

Cipher-text only (Sadece Şifreli Metin) Saldırısı

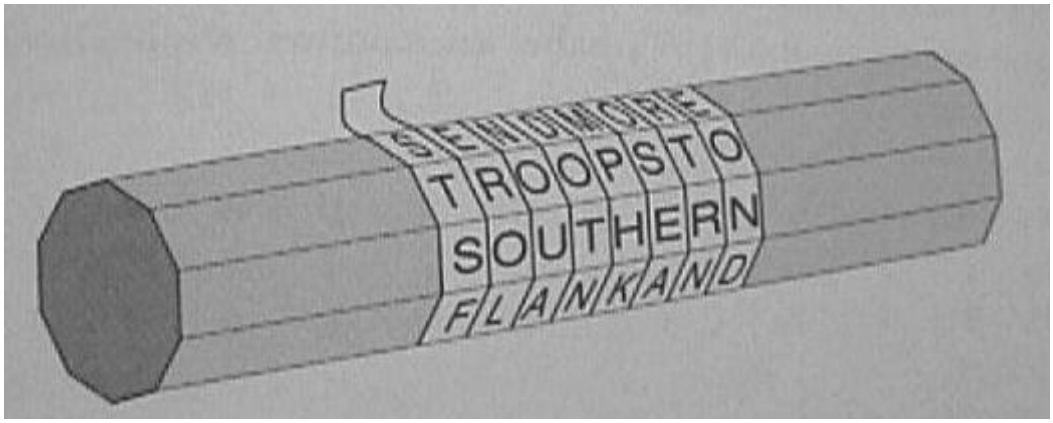
Bu saldırı tipinde, saldırıyı yapan kişi mesajın içeriği hakkında hiç bir şey bilmemektedir ve sadece şifreli-metni kullanarak çalışmalıdır. Uygulamada düz metne (plain text) - pek çok mesaj türü sabit başlık formatlarına olduğundan - ilişkin tahminler yapmak genelde olasıdır. Sıradan mektuplar ve belgeler bile kestirilebilir bir şekilde başlamaktadır. Örneğin, pek çok klasik saldırıda ciphertext'in frekans analizi kullanılmaktadır, ancak modern cipherlara karşı bu yöntem iyi çalışmamaktadır. Buna rağmen mesajlar bazen istatistiksel bir yanlılık içermektedirler.

Bilinen Düz-Metin Saldırısı

Saldırgan ciphertext'in bazı kısımlarından düz metni tahmin edebilir veya bölebilir. Geriye kalan iş bu bilgiyi kullanarak ciphertext bloklarını çözmektir. Bu işlem, veriyi şifrelemek için kullanılan anahtarın belirlenmesi ile yapılabilir. En sık kullanılan Bilinen Düz Metin Saldırısı, blok cipher'lara karşı lineer kriptanaliz saldırısıdır.

Seçilmiş Düz Metin Saldırısı

Saldırgan bilinmeyen anahtar ile şifrelenmiş istediği her metni elde edebilmektedir. Buradaki iş, şifreleme için kullanılan anahtarı belirlemektir. Bu saldırı için iyi bir örnek blok cipherlara karşı uygulanabilen diferansiyel kriptanalizdir. Bazı kripto sistemler, özellikle RSA, seçilmiş-düz metin saldırılarına karşı açıktır. Bu tip algoritmalar kullanıldığında, uygulama (veya protokol) öyle tasarlanmalıdır ki saldırgan istediği düz metni şifrelenmiş olarak elde etmemelidir.



Ortadaki Adam Saldırısı:

Bu saldırı, kriptografik iletişim ve anahtar değişimi protokolleri ile ilgilidir. Fikir şudur; iki kişi güvenli iletişim için anahtarlarını değiş-tokuş ederken (örneğin Diffie-hellman kullanarak), bir düşman kendisini iletişim hattındaki iki kişi arasına yerleştirir. Sonra bu düşman her iki kişi ile ayrı bir anahtar değiş-tokuşu gerçekleştirir. Her iki kişi farklı bir anahtar kullanarak işlerini tamamlayacaklardır ki bu anahtarlar düşman tarafından bilinmektedirler. Bu noktadan sonra saldırgan uygun anahtar ile herhangi bir iletişimi deşifre edebilecek ve bunları diğer kişiye iletmek için diğer anahtar ile şifreleyecektir. Her iki tarafta güvenli bir şekilde konuştuklarını sanacaklardır, ancak gerçekte saldırgan konuşulan her şeyi duymaktadır.

Şekil-16: Ortadaki Adam Saldırısı

Ortadaki-adam-saldırısını engellemenin bir yolu dijital imzaları kullanabilen bir açık anahtar kripto sistemi kullanmaktır. Kurulum için her iki tarafta karşı tarafın açık anahtarını

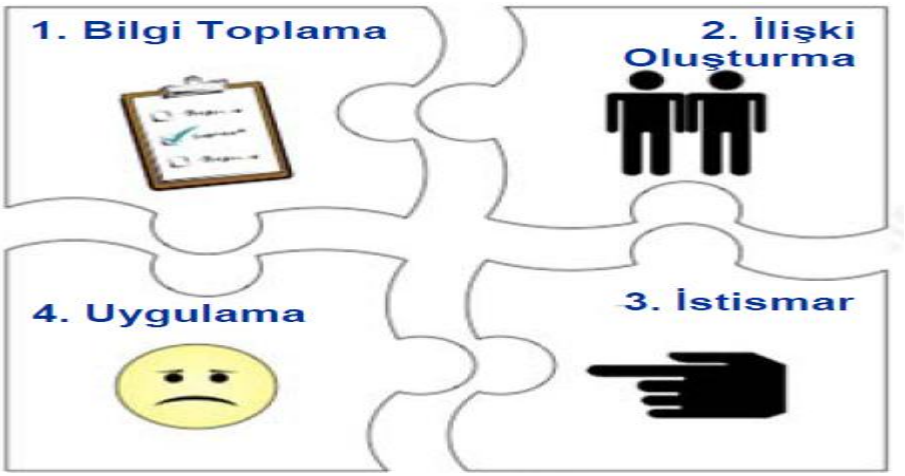
bilmelidir (ki bu bazen açık anahtar kripto sisteminin esas avantajını baltalamaktadır). Paylaşılan gizlilik oluşturulduktan sonra, taraflar kendi dijital imzalarını karşı tarafa göndermelidir. Ortadaki-Adam bu imzaları taklit etmeye çalışacak, fakat imzaların sahtesini yapamayacağı için başarısız olacaktır.

Bu çözüm, açık anahtarların güvenli bir biçimde dağıtımı için bir yolun varlığı halinde yeterlidir. Bu, örneğin, IPSec (Internet Protocol Security) 'de kullanılmaktadır. [10]

IPSec tanımı

İnternet Protocol Security (IPSec) güvenli haberleşmeler sağlamak ve IP ağları üzerinde kişisel gizliliği korumak için standartlar üzerine kurulmuş bir yapıdır. IPSec RFC (Requests for Comments) 2401-2411 de tanımlanmış olan bir IETF (Internet Engineering Task Force) standartıdır. Çoğu ağların güvensiz olduğu ve kablo üzerinde seyahat ederken verileri korumak için ek komponentler gerektirdiği düşüncesinden yola çıkarak IPSec kaynak kimlik tanılama, bütünlük kontrolü ve içerik gizliliği sağlamaktadır. [11]

2.3.6 Sosyal Mühendislik



Şekil-17: Sosyal Mühendislik

Sosyal Mühendislik; temel olarak bilgisayar ya da bilgisayar ağlarındaki açıklıklardan faydalanarak bilgisayar sistemlerine zarar veren yaklaşımların aksine “sosyal mühendislik” yöntemi insanların iletişim, düşünce tarzı, güven ya da kısaca insani zaaflarından

faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi ya da atlatılması şeklinde tanımlanabilir. Sosyal mühendislik yöntemleri; çeşitli yalanlar yolu ile sahte senaryolar üretmek, hedef kişiye kendini güvenilir bir kaynak olarak tanıtmak ya da basit ödüllendirme yöntemleri ile bilgi sızdırmak şeklinde özetlenebilir. [12]

2.3.7 SQL Enjeksiyonu

SQL enjeksiyonu veri tabanından yapılan sorgulama işlemini hedef alan bir saldırı şeklidir. Bu saldırı şeklinde sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir. Bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına

“SELECT * FROM TABLE_PERSONEL WHERE username = '" + kullanıcı adı + "' AND password= '" +şifre+ "'” şeklinde gönderildiğinde (“ ”) işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR "1=) eklinde bir ifade sorguyu

“SELECT * FROM TABLE_PERSONEL WHERE username = '' OR "1=1" AND Password = '' OR "1=1"” haline getirir. Bu durumda sorgudan var olan bütün kayıtlar dönecektir. [13]

2.3.8 Komut Enjeksiyonu

Genellikle komut (shell) enjeksiyon saldırılar SQL enjeksiyon ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler. [14]

2.3.9 HTML Enjeksiyonu

Bu açık, programcıların kodlama sırasında yaptığı hatalı kodlamadan faydalanır. Web yazılımlarında veri tabanına giren verilerin ya da veri tabanından çekilen verilerin bir kontrol mekanizmasından geçirilmemesi açığa neden olmaktadır. XSS olarak da bilinen açıktan faydalanılarak session ve cookie çalması yapılır.

Uygulamalarda sayfaya gönderilen bir isteğe bir cevap döndürülmesi mantığı kullanılır. Sayfaya gönderilen istek sunucuda değerlendirilip bir cevap döndürülür. Ama eğer giriş yaptığınız sayfa kötü amaçlı bir url adresine yönlendirildiyse ya da Truva atı gibi araçlar yerleştirildiyse aldığınız yanıt beklenenden farklı olacaktır. Bu saldırı tipinde amaç web uygulamasına zarar vermek değil daha çok uygulamayın ziyaret eden kullanıcılara erişmektir. [15]

2.3.10 Arka Kapılar (Backdoors)

Bilgisayar üzerinde sıradan incelemelerle bulunamayacak şekilde normal kimlik kanıtlama süreçlerini atlamayı veya kurulan bu yapıdan haberdar olan kişiye o bilgisayara uzaktan erişmeyi sağlayan yöntemler arka kapı olarak adlandırılmaktadır. Bir sisteme sızmak için oldukça zahmetli bir çaba harcayan korsanlar daha sonra aynı sisteme erişmek için daha kolay bir yolu sisteme eklemek isterler. En sık karşılaşılan arka kapı yöntemi hedef sistemde dinleme ajanı iliştirilmiş bir portu açık tutmaktır.

Bu açıdan bakıldığında bu tür bir açığa maruz kalındığından emin olmak için sistemde mevcut bulunan bütün portlar 1'den 65535'e kadar iki kere (bir kez TCP bir kez de UDP için) taranmalıdır. Arka kapılar çoğunlukla Truva atları ile karıştırılabilmektedirler. Her ikisi de hedef sisteme sızmaya yarayan kötü amaçlı yazılımlardan; Truva atı faydalı bir program gibi gözükürken; arka kapı sadece sisteme erişimi sağlayan gizli yapılardır. [16]

Birçok virüs bir bilgisayara bulaştığında mutlaka bir arka kapı açmayı denemektedir. Bu arka kapılar da virüs yayıncısı için çok kolay bir erişim imkânı sağlamaktadır.

Arka kapılar kimi zaman sistemi geliştiren programcı tarafından test edilen sisteme erişmek amacıyla kullanılan fakat daha sonra unutulan açıklar olarak karşımıza çıkmaktadır. Bu durumun bir şekilde farkına varan kötü niyetli kişiler bu yapıları kullanabilirler. Hatta bu tip arka kapılar bazen programcı tarafından kasten bırakılabilmektedir.

Arka kapı konusunda en ünlü iddialardan biri de Microsoft'un Windows işletim sisteminin bütün sürümlerinde NSA (Amerikan National Security Agency) için bir arka kapı yerleştirdiği

iddiasıdır. Bu iddia Microsoft'un bütün sürümlerinde bulunan CryptoAPI yapısında _NSAKey adına ilave bir giriş anahtarın bulunmasıdır. [17]

2.3.11 Oltalama (Phishing)

Phishing kısaca online dolandırıcılık olarak tanımlanabilir. Phishing yönteminde temel amaç internet kullanıcısını kandırarak kullanıcıya ilişkin kredi kartı bilgileri, banka hesap numaralarından, bu hesaba ait online internet şifresine kadar birçok özel bilgileri ele geçirmektir.

Neler Çalınıyor?

Phishing yöntemi kullanarak bilgisayar kullanıcılarını tuzaklarına düşüren dolandırıcılar özellikle aşağıda belirtilen bilgileri çalıyorlar:

1) Kredi Debit/ATM Kart Numaraları/CVV2

2) Şifreler ve Parolalar

3) Hesap Numaraları

4) İnternet Bankacılığına Girişte Kullanılan Kullanıcı Kodu ve Şifreleri

Bu dolandırıcılık işlemi nasıl gerçekleştirilmektedir?

Kullanılan yöntemlerin başında e-posta ile gönderilen sahte mesajlar gelmektedir. Bu e-posta bir ticari kurumdan (bankalar, alışveriş siteleri vb.) geliyormuş gibi bir izlenim yaratır. Bu kullanıcının kendisine ait bilgileri girmesi için kurumun internet adresine ilişkin bağlantıya tıklamasını içeren bir e-posta olabilir. E-posta içeriği kişisel bilgilerin güncellenmesi sistemdeki yeniliklerin hesabınızda aktif olması için şifrenizi girin gibi mesajlardır. Bunu gören kullanıcı e-posta ile gelen mesajdaki bağlantıya tıkladığında kurumun web sitesinin birebir kopyası olan başka bir sayfaya yönlendirilir. Burada girilen şifre gibi özel bilgiler artık başkasının eline geçer. [18]

E-posta kullanım oranının çok yüksek olması bu tür online dolandırıcılık işlemlerinin e-posta yoluyla gerçekleşmesinde temel etmenlerden biridir. E-posta içeriğinde belirtilen bağlantı (genellikle ticari kurumların web sitelerine yönelik sahte gösterim) kullanıcıların aldanmasında büyük rol oynar. İnternet kullanıcısı üyesi olduğu ticari bir kurum sitesine yönlendirildiğini sanıp kendisine belirtilen yönergeleri uygular. Phishing ataklarındaki önemli artış internet gezgin (browser) uygulamalarının (İnternet Explorer, Mozilla Firefox, Opera vb.) güvenlik sorunlarını da ön plana çıkarmıştır.

Örnek olarak http://www.turkiyebankalarkurulu.com adlı bir internet sayfası oluşturulmuştur. Ancak Türkiye Bankalar Birliği'nin resmi internet sitesi olan www.tbb.org.tr adresinden bunun bir internet üzerinden oltalama (phishing) türü dolandırıcılık yapma girişimi olduğu duyurusu yayınlanmıştır. Daha sonra bahse konu site yayından kaldırılmıştır. Bu gibi dolandırıcılık olaylarının engellenebilmesi maksadıyla internet bankacılığında kullanılması gerekli olan kullanıcı adı ve şifre bilgilerine ek olarak 2011 yılında BDDK tarafından zorunlu hale getirilen ve 2010 yılından itibaren uygulanmasına başlanan IBAN numarası ve GSM şebekeleri üzerinden tek kullanımlık şifre düzenlemeleri hayata geçirilmiştir.

Bu dolandırıcılık faaliyetlerine karşı; bankalardan geldiği düşünülen e-postaların içerisindeki linklere tıklanarak bankacılık işlemi yapılmamalıdır. İnternet bankacılığı işlemlerinde banka tarafından sunulan fare ile veri girişi, tuşlar üzerinde bekleyerek veri girişi, değişen karmaşık tuş takımı ve tek kullanımlık SMS ile şifre gönderilmesi gibi çözümleri kullanmak güvenlik açısından önemlidir.

Bu dolandırıcılık tipi sadece bankacılık sitelerinde değil arkadaşlık sitelerinde, sohbet sitelerinde, alışveriş sitelerinde, havayolu sitelerinde ve birçok sitede ortaya çıkabilmektedir. ATM cihazları kullanılırken şüpheci ve dikkatli olunmalıdır. ATM makineleri üzerine mikro kamera kart okuyucu ve sahte tuş takımı (PinPad) düzenekler yerleştirilmesi ile karşılaşılmaktadır. [19]

Phishingten Nasıl Korunulur ?

Unutulmaması gereken nokta her türlü online dolandırıcılık, sahtekarlık ve virüslere karşı en büyük korunma aracı bu konuda bilinçli ve bilgili olmaktır.

1) E-postaya gelen mesajların doğruluğunun ispatlanması. Tanımadığımız kimselerden gelen mesajları silinmesi gerekmektedir. "Aşağıdaki bağlantıya tıklayın" gibi e-posta isteklerine asla yanıt verilmemesi gerekiyor.

2) İşlemleri online yaparken işlem yapılan web sayfasının güvenli olup olmadığını mutlaka kontrol edilmesi lazım. İnternet tarayıcısının üst kısmında bulunan adres bölümünde bulunan adresin "https://" olup olmadığı kontrol edilmelidir. “https://”’in sonunda bulunan “s” harfi bu sayfanın güvenli ve çeşitli şifreleme metotları ile işlem yaptırdığını belirtir.

3) İnternet adresi olarak sayısal rakamlar içeren adresler ile karşılaşıldığında kullanmadan önce mutlaka kontrol edilmeli. Ziyaret edilen web sitelerinde; adresler çoğunlukla adres kısmı ardından firmanın ve şirketin ismine ek olarak com, org, net gibi uzantılar ile biter. Sahte sitelerde çoğu zaman sayısal adresler kullanılmaktadır.

4) E-posta adresine ulaşan e-posta’nın kimden geldiğinden ve doğruluğundan mutlaka emin olunmalıdır.

5) Bankadan gelen kart ekstreleri ve banka hesapları düzenli olarak kontrol edilmelidir. Olası aksiliklerde banka ile kesinlikle irtibata geçilmeli ve zaman kaybedilmemelidir.

6) Sistemin düzenli olarak kontrol edilmesi gerekmektedir. İşletim sisteminin güvenlik yamalarının yüklenmesi, anti-virüs yazılımı varsa devamlı olarak güncellenmelidir.

7) Çeşitli kurumlardaki hesaplar veya birden fazla e-posta adresi kullanılıyorsa kesinlikle her biri için farklı şifreler belirlenmelidir.

8) Belirlenen şifreleri belli aralıklar ile muhakkak değiştirmelidir.[20]

2.3.12 Rootkitler

Çalışan süreçleri dosyaları veya sistem bilgilerini işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren bir program veya programlar grubudur. Amacı yayılmak değil bulunduğu sistemde varlığını gizlemektir. Önceleri çok kullanıcılı sistemlerde sıradan

kullanıcıların yönetim programlarına ve sistem bilgilerine erişimini gizlemek için geliştirilmiş ve kullanılmış olmasına rağmen kötü niyetli kullanımına da rastlamak mümkündür.

Tipine bağlı olmakla birlikte genelde erişim yetkiniz dâhilinde sisteminize kurabileceğiniz rootkit'ler bulmanız mümkündür. Bunun dışında güvenilir bir kaynaktan geldiğine inandığınız bir programı haddinden fazla yetki ile çalıştırmak (Örn: root) zararlı bir rootkit'in sisteme kurulmasına sebep olur. Aynı şekilde çok kullanıcılı bir sistemde kernel vs açıkları kullanılarak sistemde root yetkisi kazanıp rootkit kurulması en yaygın görülen bulaşma şeklidir.

Adından da anlaşılabileceği gibi Rootkit iki parçadan oluşmaktadır; Root= Unix sistemlerinde her şeyi yapma yetkisine sahip olan kullanıcı ya da kullanıcı yetkisi Kit = Bu yetki sahibi olabilmek için kullanılan gerekli araç kutusu şeklinde ifade edilebilir.

Bunu yaparken sistem araçları ile yer değiştirmiş olmaları tanınmalarını engellemekte ve arka planda hiçbir kullanıcının ya da tarayıcının fark edemeyeceği biçimde çalışmalarını sağlamaktadır. Bu özellikleri zararlı yazılımları yazan programcılar (hacker) tarafından çok cazip bulunmakta ve ilk başlarda kötü amaçlarla kullanılmayan bu yazılımlardan yanlış kimselerin elinde çok tehlikeli olabilecekleri için günümüzde kötü niyetli yazılımlar olarak bahsedilmektedir. [21]

2.3.13 Casus Yazılım (Spyware)

Bu programlar kullanımı masum görünen ve genelde internetten “bedava” diye reklamını görüp indirilen programlar ile bilgisayarlara bulaşan programcıklardır. Çoğunlukla dikkat edilmeyen EULA (Son Kullanıcı Lisans Sözleşmesi) içerisinde (programla birlikte kurulacağı belirtilir ve “I Agree” kabul edildiğinde her şeyi kabul edilmiş olunuyor) bulunur.
Tam anlamı ile virüs olarak adlandırılamayan bu programların temel amaçları kuruldukları bilgisayarda bilgi toplamak ve bu bilgileri bu programları yaratan kişilere göndermektir.
Bu spyware/casus programların bilgisayar sistemlerine tehlikesi casusluk derecelerine göre değişir.

Casusluk yaptıkları konular nispeten masum olarak adlandırılabilecek olan “hangi siteye gidiyor, ne kadar orada kalıyor” gibi bilgilerden daha ciddi olan bilgisayarın veya

sistemin kurulum şifreleri veya kullanılan kredi kartı bilgilerini edinerek bunları program yazıcılarına postalamaya kadar varabilen her türlü casusluk örneklerini kapsayabilirler. Sörf bilgilerini genelde google toolbar, alexa toolbar veya diğer benzeri toolbar ismiyle dağıtılan internet explorer eklentileri biriktirirler. Bu şekilde hangi sitelerin ziyaret edildiğini ölçerek ziyaret edilen sitelere puan veya benzeri değerlendirmeler verirler. Sonra bu verileri arama sitelerinde sonuçları sıralamak için kullanabilirler. Aynı şekilde GetRight, Gator ve benzeri internetten dosya indirmeye yarayan programlar da bu tür spyware içerirler. Ancak bunu kendileri tabiî ki kabul etmezler çünkü bu programları kurarken kabul ettiğiniz kullanım kurallarına göre bu veri aktarımını kabul ettiğinizi bildirdiğiniz için bunun casusluk olmadığını gönüllü veri paylaşımı olduğunu belirtirler.

Spyware veya casus programların daha tehlikeli olan türevleri ise bilgisayar veya internet ayarlarınızı kendi istedikleri gibi değiştirirler ve kendi istedikleri sitelere yönlendirirler bazıları bununla da yetinmeyip internet başlangıç sayfasını kendi istedikleri gibi değiştirirler hatta bazen bilgisayarda karşınıza nereden geldiğini bilmediğiniz ve anlayamadığınız reklam içerikli pencereler çıkarırlar. Bunlara Adware'de denir çünkü her ne kadar bir önceki casus programlar gibi casusluk yapıyor olsalar da bunun yanında ayrıca bir de bilgisayarınızda reklama yönelik oynamalar yapmaktadırlar. [22]

Tabi bunlardan daha da tehlikeli olanları da vardır. Mesela bu türün en tehlikelileri olarak nitelendirilmesi mümkün olan Dialer programları bunlardandır. Telefon hattı üzerinden internete bağlananlar için bu dialer programlar bilgisayarın internet bağlantı ayarlarını değiştirerek ödemeli bir telefon hattına yönlendiren programlardır. Bu dialer programlar bulaştığı esnada her zamanki gibi internete bağlanırken telefon faturası gelince şoke olursunuz çünkü faturanız birden belki de 10 katı ile artmıştır. Bunun nedeni bu bilgisayara bulaşan dialer programlar internete bağlandığınız numarayı biraz önce belirttiğimiz gibi ücretli bir yurtdışı hattı veya 900 lü bir hat ile değiştirip sizi her internete girişinizde bu ücretli hatlar aracılığı ile internete bağlamıştır.

2.3.14 Virüsler

Virüs, bilgisayar dünyasında on yıllardır karşılaşılan bir terimdir. Bu terim genellikle zararlı yazılımları ifade eden kapsayıcı genel bir ifade olarak kullanılmıştır, ancak bu kullanım yanlıştır. Her tür zararlı yazılım virüs olarak ifade edilemez. Virüs diğer dosyalara bulaşarak yayılan özel bir zararlı yazılım türünü ifade etmektedir.

Kayıtlara geçen ilk virüs 1986 yılında ortaya çıkan IBM-PC tabanlı "*Brain*" ismi verilen bir *boot sector* virüsüdür. [23]

Bilgisayarlara zarar vermek üzere hazırlanmış programlardır. E-postalar ve dosyalar ile bilgisayarlara bulaşan virüsler bilgisayarların çalışmasını engelleyebilmekte bilgilerin kaybolmasına, bozulmasına veya silinmesine neden olabilmektedir. Ayrıca bilgisayarları yavaşlatabilmektedirler. Bunlar bilgisayar belleğine yerleşen, çalıştırılabilen programlara kendini ekleyebilen, yerleştiği programların yapısını değiştirebilen ve kendi kendini çoğaltabilen programlardır.

Virüslerin sistemleri yıkıcı etkileri bulunmaktadır. Virüsler bir dosyanın açılması, bir e-postanın okunması veya virüs bulaşmış bir programın çalıştırılması gibi yöntemlerle yayılmaktadır.

Bir sistemdeki olası virüs belirtileri şunlardır:

- İnternette bir işlem ya da faaliyet yapılmayan zamanlarda veri trafiğinin devam etmesi: Buna göre başka kişi veya kullanıcılar sistemde aktif olabilirler ve kötü niyetli bir çalışma yapıyor olabilirler.
- Sistemde yapılandırılmış bir güvenlik duvarı olduğu taktirde bazı uygulamaların internetten bağlanma girişimleri
- İnternet sitelerinde dolaşırken reklam pencerelerinin açılması
- Bilgisayarın işlemez hale gelmesi
- Telefonlardaki kötü amaçlı yazılımlar

Bir sisteme virüs bulaşması durumunda güncel bir anti-virüs programıyla sistemi taramak gerekmektedir. Virüsler başlıca üç bölümden meydana gelmişlerdir. Bunlar sırasıyla kopyalama bölümü, gizleyici bölümü ve etki bölümüdür.

Kopyalama bölümü ile virüs kendisini çalıştırılabilir dosyalara (.EXE file) ilave eder.

Gizleyici bölümü kendini gizleme görevi yapar. Anti-virüs programlarının tespit etmemesi için saklanır. Etki bölümü ise asıl işlemi gerçekleştirir. Örneğin dosyaların yapısını bozmak, silmek, değiştirmek, hard-diskin bir kısmına ulaşamamak gibi işlemleri yapar.

Genel olarak virüsleri tahrip edici ve sisteme rahatsızlık verici olarak ikiye ayırabiliriz. Tahrip edici virüsler verilerin veya programların bir kısmına veya tamamına zarar verip sistemin çalışmasını engellerken sisteme rahatsızlık verici virüsler ise geçici bir süre sistemin çalışmasına engel olan virüslerdir.

Bilgisayar virüslerinin yol açtığı zararlar küçük gibi gözükse de toplamda çok büyük zararlara yol açabilmektedirler. 3 Mayıs 2000 günü tüm dünyada yayılan ve elektronik postaya ekli olarak gelen "I Love You" veya "Love Bug" virüsü çok kısa bir zamanda 55 milyon bilgisayara ulaşmış ve bunların 2,5-3 milyonuna bulaşarak 8,7 milyar dolar zarara neden olmuştur.

2.3.15 Truva Atları

Faydalı bir fonksiyonu varmış gibi görünen fakat aynı zamanda gizli ve güvenlik mekanizmalarını aşabilecek potansiyel zararlı fonksiyon içer en ve bazen bir sistem biriminin meşru olarak yetkilendirilmesini istismar eden bir bilgisayar programı olarak tanımlanmaktadır. [24].

Genellikle ücretsiz olarak sunulan yazılımlarla birlikte sisteme bulaşmaktadırlar. Truva atlarından korunmanın en iyi yolu kaynağı bilinmeyen yazılımların sisteme yüklenmemesidir.

Truva atı çeşitli zararlar vermek için dizayn edilmiş olsa da zararsız da olabilir. Truva atları sistemde nasıl gedik açabildiğine ve nasıl tahribat yaptığına göre sınıflandırılır. Truva atları 7 farklı amaca hizmet edebilir. Bunlar:

- Uzaktan Erişim
- E-posta Gönderme
- Veri yıkımı

- Proxy Truva (zararlı bulaşmış sistemi saklama)
- Ftp Truva (zararlı bilgisayardan dosya ekleme ya da kopyalama)
- Güvenlik yazılımını devre dışı bırakma
- Hizmetin reddi servis saldırıları (DoS Saldırıları)
- URL truva (zararlı bulaşmış bilgisayarı sadece pahalı bir telefon hattı üzerinden internete bağlama)

Bazı örnekler;

- Veriyi silme ya da üzerine yazma
- Ustaca dosyalara zarar verme
- Bilgisayar kamerasını açarak kullanıcının görüntüsünü kaydetme
- Dosyaları internetten çekme veya internete aktarma
- Kurbanın bilgisayarına uzaktan erişime izin verme. Buna RAT (Uzaktan yönetim aracı) denir.
- Diğer zararlı yazılımları üzerinde toplama. Bu noktada Truva atı dropper ve vector diye ikiye ayrılır.
- DDoS saldırısı yapabilmek veya spam e-posta göndermek için zombi bilgisayar ağı kurma
- Bilgisayar kullanıcısının alışkanlıklarını başka insanlara gizlice rapor etme kısacası casusluk
- Arkaplan resmi oluşturma
- Klavye tuşlarını şifreleri ve kredi kartı numaraları gibi bilgileri çalabilmek için kaydetme (keylogging)
- Suç aktivitelerinde kullanılabilecek banka ya da diğer hesap bilgileri için oltalama

- Bilgisayar sistemine arka kapı yerleştirme
- Optik sürücünün kapağını açıp kapama
- Spam posta göndermek için e-posta adreslerini toplama
- İlgili program kullanıldığında sistemi yeniden başlatma
- Güvenlik duvarını veya anti-virüs programına müdahale etmek veya devre dışı bırakma

2.3.16 Solucanlar (*Worms*)

Solucanlar da, tıpkı virüslerde olduğu gibi, kendini bir cihazdan başkasına kopyalamak üzere tasarlanmışlardır, ancak bunu kendi başlarına gerçekleştirmektedirler. Öncelikle bilgisayarda dosya veya veri transferi yapan fonksiyonların denetimini ellerine geçirip bir kez sisteme bulaştıktan sonra kendi kendine yollarına devam edebilirler. Solucanların en göze batan tehlikesi, büyük miktarlarda çoğalma yetenekleridir. Kullanıcıların veri ve dosya alışveriş yöntemlerini kullanarak kendilerini, irtibat halinde olunan tüm bilgisayarlara, tüm e-posta adreslerine gönderebilmektedirler. Bu da ağ trafiğinin önemli derecede yavaşlamasına neden olabilmektedir. Bir solucan yeni çıktığında, daha güvenlik yazılımları tarafından tanınmadığı için ilk etapta ağ trafiğini önemli oranda yavaşlatabilmektedir. [25]

Solucanlar genel olarak kullanıcı müdahalesi olmadan yayılmakta ve kendilerinin birebir kopyalarını ağdan ağa dağıtmaktadırlar. Solucanlar yayılmak için bir taşıyıcı programa veya dosyaya ihtiyaçları olmadığı için sistemde bir tünel de açabilmekte ve başkasının, bilgisayarınızın denetimini uzaktan eline geçirmesine olanak sağlayabilmektedir.

Karıştırılan terimler oldukları için virüsleri, Truva atları ve solucanlardan ayıran özelliği burada vurgulamakta fayda bulunmaktadır: Truva atları zararsız birer yazılım gibi görünmekte ve bir sistemde istismar edeceği bir durum ortaya çıktığında (bilgisayarın İnternete bağlanması gibi) devreye girmekte, diğer zamanlarda sisteme herhangi bir müdahalede bulunmamaktadır. Solucanlar ise ağda kendilerini yayabilen kendi başlarına birer

programdırlar. Bunların aksine virüs, bulaşmak için kendine ye tenbir program değildir. Kendini başka dosyalara ilave ederek yayılır ve eğer virüslü dosya açılmazsa virüs başka ortamlara yayılamaz.

İnternetteki solucan örnekleri

İnternette sörf yaparken karşımıza çıkan küçük pencerelerde ilgi çekici şeyler bulunmaktadır. Bunlara tıkladığımızda İnternet Explorer solucan virüsü taşıyan dosyalar indirir. Tıkladığımız andan itibaren virüs bilgisayarımızda etkinleşir. Bazı penceredeki yazıların örnekleri;

- Tebrikler 250 sms kazandınız telefonunuza indirmek için tıklayınız.
- Tebrikler Amerika'ya gitme hakkını yakalamak için ücretsiz çekiliş kazandınız.
- Tebrikler Amerika kapınızda.
- Visa kartınıza bonus kazandınız.
- Sitemize giren 1.000.000. kişisiniz. Bizden hediye şarkı kazandınız.
- Bugün şanslı gününüzdesiniz. Bizden para ödülü kazandınız.
- Tebrikler bizden saat kazandınız.

Tübitak tarafından 2011 yılında yapılan bir açıklamada son yılların en büyük saldırılarından biri olan ve tüm dünyada 15 milyon bilgisayara bulaştığı tahmin edilen "Conficker" adlı solucanın zayıf şifreler sahip kullanıcı hesapları aracılığıyla ağ üzerindeki paylaşımlarla ve solucanın bulaştığı bilgisayarlara takılan taşınabilir bellekler vasıtasıyla yayıldığı belirtilmiştir.

2.3.17 Bot

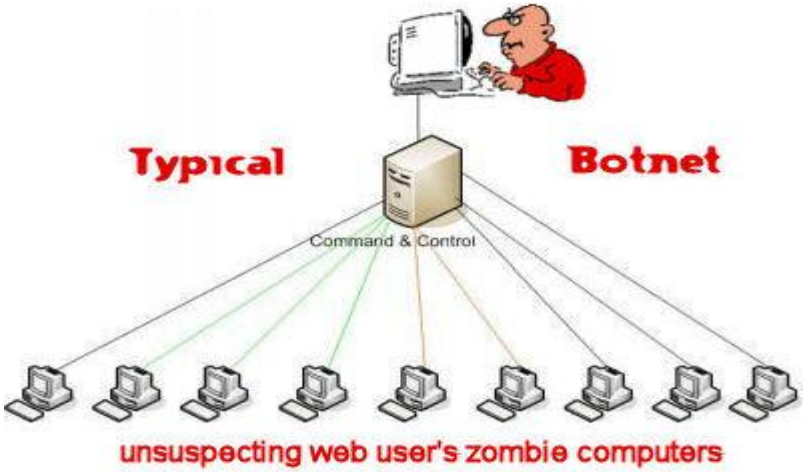
Bot bilişim dünyasında "robot" anlamında kullanılan yaygın bir terimdir. Pek çok bilgisayar işlemini yarı-otomatik olarak yapabilen robotlar bilişimin tüm alanlarında kullanılır. En ünlü oldukları alan arama motorları tarafından kullanıldıkları endeksleme teknolojisidir. Akıllı ajan teknolojilerinin İnternet ile birlikte hızla yaygınlaşması İnternet robotu ya da kısaca bot olarak adlandırılan ve özel olarak İnternet üzerinde hareket göstermek

üzere geliştirilen bir ajan yazılımı grubunu ortaya çıkarmıştır. Bu grupta esasen web tabanlı arama motorlarının çekirdeklerinde yer alan örümcek yazılımları ve özel amaçlı tarayıcı yazılımlar gibi değişik türler de yer alır. Kesin bir çizgi olmamakla birlikte Çek dilinde iş anlamına gelen robota kelimesinden türeyen robot kelimesinin kısaltılmışı olan bot kavramı akıllı ajan yazılımlarının İnternet üzerinde etkinlik gösterenlerine verilen bir ad olmuştur. Belki de bu adlandırmada gerçek dünyada robot davranışı olarak adlandırılabilecek türden davranışların sanal dünyadaki karşılığı olmaları beklentisi etkili olmuştur. [26]

Günümüzde pek çok değişik bot türünden söz edilmektedir. Ticari veri madenciliği, e-posta, oyun, kamusal haber grubu, sohbet, alışveriş, hisse senedi, yazılım vb. gibi hedeflenen bilgi türüne göre adlandırılan pek çok bot türü mevcuttur. Bu türlerin hemen hepsi karakteristik olarak otonom bilgi ajanları/arabirimleri olarak ve özellikle İnternet üzerinde faaliyet göstermek üzere tasarlanmış ve geliştirilmiş yazılım türleridir.

2.3.18 Zombi Ordular (Botnetler)

Zombi bilgisayarlar ya da botnetler bu tehdit grubunun en tehlikeli olanları olarak kabul edilebilir. Burada önemli olan nokta,bilgisayar kullanıcısının hiçbir haberi olmaksızın bilgisayarının çok ciddi suçlar işlenmesinde kullanılabilmesidir. Bu tür bilgisayarlar robot veya bot şeklinde de ifade edilmektedir.



Şekil-18: Basit Bir Bot-Net

Zombi ordunun bir parçası haline gelen bilgisayarlarda buna sebep olan nokta, genellikle bu tür bilgisayarların firewall denilen güvenlik duvarlarının olmamasıdır. Günümüzde bant genişliğinin artmasıyla beraber herhangi bir korunmaya sahip olmayan bir bilgisayar kolaylıkla bir botnet'in parçası haline gelebilir. Bir botnet, genellikle açık bır akılan bir kapıdan (port) bir bilgisayara, daha sonra aktif hale gelecek şekilde, Truva atı bırakılması sonucu oluşturulmaktadır. Botnet'in parçası haline gelen bilgisayarlar mesela bir web sitesine aynı anda yönlendirilerek bu siteyi hizmet veremez hale getirmek için kullanılabilmektedir. [27]

2.3.19 Klavye İşlemlerini Kaydeden Programlar (Keyloggers)

Keylogger'lar kısaca klavye işlemlerini kaydeden programcıklardır. Bu programcıklar, farkına varılmadan klavyede dokunulan her tuşu kaydedip, fırsatını bulduklarında daha önce belirlenen adreslere bunları göndermektedirler. Özellikle bankacılık işlemlerinde klavyeden şifre girilmemesi, rakamlara tıklanarak veya rakamların üzerlerinde beklenerek şifreler girilmesi ve ayrıca cep telefonu ile SMS şifreleri yoluyla ilave güvenlik desteği sunulabilmesine rağmen İnternet üzerinden ticaret yapan birçok site, alıcıların kredi kartı bilgilerini girmesi için güvenlik seviyesi yüksek bu tür platformlar oluşturmamaktadır. Bu da klavyeden girilen bu bilgilerin nasıl kolayca başkalarının eline geçebileceğini göstermektedir. Bu durum, sadece alışveriş ve bankacılık işlemleriyle sınırlı değildir. Klavye işlemlerini kaydeden bu tür yazılımlar nedeniyle, e-posta ve sosyal paylaşım siteleri gibi kullanıcıların özel bilgilerinin yer aldığı web sit elerine ait kullanıcı adları ve şifrelerin ne kadar büyük tehlike altında olduğu anlaşılabilmektedir. Günümüzde sosyal medya ve çevrimiçi (online) oyunların ne kadar yaygın olduğu ve bunlar yüzünden meydana gelen cinayet ve intiharların ne kadar çok arttığı göz önünde bulundurulursa keylogger'ların meydana getirdiği asıl tehlike gerçek manasıyla anlaşılabilir.

Bu yazılımlar, aynı zamanda aldatan bir eşi takip etmede, işverenlerin çalışanlarını izlemesinde veya bir çocuğun bilgisayarda neler yaptığının gözlenmesinde kullanılabilmektedir. Bu programlar, maksatlı kişiler tarafından bilgisayarlara doğrudan

fiziksel erişim sağlanarak veya İnternete bağlı olan bir bilgisayardaki açıklıklar kullanılarak sistemlerin içerisine kurulabilir. [28]

Keylogger'lar küçük programcıklardır ancak bunlar sadece yazılım olarak değil donanım olarak da var olabilmektedirler ve kullanıcılar ve sistemler bunların farkına varamamaktadırlar. Bu tür klavye hareketlerini kaydeden donanımlar fiziksel olarak klavye ile bilgisayar arasına monte edilmekte ve bilgisayar kasasının arka kısmına gizlenmektedir. Yapılan araştırmalarda ne kullanıcılar, ne de sistemler bu kaydedicileri fark etmiştir. Hazırlanmaları ve kurulumları çok basit olan bu tür cihaz ve yazılımların varlıklarına karşı dikkatli olunması gerekmektedir.

2.4 DÜNYADA SİBER SALDIRI ÖRNEKLERİ

Soğuk Savaş sırasında Rusya ve ABD'nin karşılıklı casusluk faaliyetleri yaptığı biliniyordu. Moskova, 1982 yılında Kanada'da bir şirketten doğalgaz boru hatlarını kontrol etmek için kullanılan bir yazılımı çalmaya başladı. Bunu fark eden Amerikalılar ise, operasyonu durdurmak yerine yazılımın içine virüs yerleştirdiler. Rusların çaldığı yazılım bir süre sonra virüs tarafından bozuldu, boru hatlarındaki akışı anormal seviyelere çıkartı ve borunun patlamasına neden oldu. Sonuçta o güne kadar uzaydan görülen en büyük (nükleer olmayan) patlama yaşandı. Bu olay tarihe ilk siber saldırı olarak geçti. [29]

ABD, 1992 yılında daha savaş başlamadan Irak devletinin tüm telekomünikasyon alt yapı şebekesini bir tuşla çökertmiştir. Oysa Saddam iletişim alt yapısını en son teknoloji ile yenilmek için çok büyük paralar harcamıştı. Hatta o yıllarda dünyadaki en son teknolojik gelişmelerin uygulandığı sayısal haberleşme sistemleri Irak'ta kurulmuştu. Tüm askeri birliklerin birbirleri ile olan iletişimi bir tuşla çökertilmiştir. Hem de çok uzaklardan, bir tuşa basılarak uzaydaki uydu üzerinden bir komut gönderildi ve tüm iletişim sistemlerinin çalışması aynı anda bloke edildi. 2003 yılında ABD Irak'ı işgal etmeyi planlarken Irak Savunma Bakanlığı'nda çalışan binlerce kişi, işgalden hemen önce bilgisayar ekranlarında Amerikan Merkez Komutanlığı'ndan gelen bir mesaj gördüler. Mesajda, "Yakın bir zamanda Irak'ı işgal edebiliriz. Sizlere zarar vermek istemiyoruz. Başınıza bir şey gelmesini

istemiyorsanız savaş başladığında evlerinize gidin" diyordu. Birçok kişi hatta askerler bu mesajı ciddiye alıp tankları terk edip evlerine gitti. ABD böylece Irak tanklarını kolaylıkla imha edebildi.

Siber saldırı ve savunma sistemlerinde en güçlü olduğu tahmin edilen ülkelerden biri olan Çin'in, ABD'nin askeri ve Avrupa'nın teknoloji sırlarını elde etmeye çalıştığı iddia edilmektedir. Amerikan askeri araç ve silahlarının üreticisi Lockheed Martin'in gizli bilgilerine eriştiği iddia edilen Çin'in siber istihbarat uzmanlarının, F-35 savaş jetlerinin tüm planlarını ele geçirdikleri iddia edilmektedir.

1- 1998 *Solar Sunrise* Vakası

Şubat 1998'de ABD Savunma Bakanlığı ağı bir grup saldırıya maruz kalmıştır. Saldırı yöntemi olarak *UNIX* tabanlı işletim sistemi olan *Solaris*'teki bir açık kullanılmıştır. Saldırganlar önce sistemde bu açığın var olup olmadığını kontrol etmişler, mevcut olduğunu fark edince de bu açıktan faydalanıp sisteme, bilgi toplama maksatlı bir program yerleştirmişler ve daha sonra toplanan bilgileri almak için geri gelmişlerdir (Hildreth, 2001). ABD'nin değişik bölgelerindeki askeri ve devlet kurumlarının sistemlerine girildiği tespit edilen saldırılar aynı güvenlik açığı kullanılarak dünyada daha birçok ülkeye karşı gerçekleştirilmiştir.

2- 1999 Kosova Vakası

NATO tarafından 1999 yılında gerçekleştirilen Kosova operasyonu içerisinde yer alan siber saldırı olayları, Dünya üzerinde gerçekleşen ilk geniş kapsamlı İnternet Savaşı olarak kabul edilmektedir (Geers [web], 2012).

NATO uçakları Sırbistan'ı bombalamaya başladığı andan itibaren "Black Hand" vb. Sırp yanlısı birçok hacker grubu NATO'nun internet altyapısına saldırmaya başlamıştır (Geers [web], 2012).

Operasyon boyunca saldırganlar NATO internet altyapısına, hizmet dışı bırakma ve virüslü e-postalar (25 farklı virüs tespit edilmiştir) yoluyla saldırmışlardır. ABD'de Beyaz Saray'ın web

sitesinin ana sayfası değiştirilmiştir. İngiltere ise bir miktar veri tabanı bilgisini kaybettiğini kabul etmiştir (Geers [web], 2012).

3- 2001 Çin - ABD Siber Savaşı

1999 yılında ABD'nin Belgrad'daki Çin elçiliğini yanlışlıkla bombalamasının ardından ABD ve Çin arasındaki ilişkiler gerilmiştir (Geers [web], 2012). 2001 yılının Nisan ayında bir Çin savaş uçağı ile ABD'ye ait bir keşif uçağının Çin'in güneyinde çarpışmasından sonra Çinli hackerlar tarafından ABD hükümet sitelerine yoğun bir saldırı başlamıştır (Gürkaynak ve İren, 2011). Çinli hackerlar Mayıs başında başlayan tatil boyunca ABD sitelerine saldırı düzenlenmesi için çağrıda bulunmuşlardır (Tang [web], 2001). Çinli hackerlar ABD hükümetine ait yaklaşık 1200 siteye saldırı düzenlemişlerdir (Gürkaynak ve İren, 2011).

4- 2000 Avustralya Atık Sistemi SCADA Vakası

Daha önce bir yazılım geliştirme şirketinde çalışmakta iken işinden ayrılan Avustralyalı bir hacker Queensland atık işleme tesislerinin kontrol sistemine sızmış ve 264.000 galon işlenmemiş atığı yakındaki nehir ve parklara yönlendirmiştir (CIIP [web], 2009). Avustralya'nın Moroochy eyaletinde 2000 yılında iki ay içerisinde arıtma tesisinden kanalizasyon suları en az 40 kez parklara, nehirlere ve Hyatt Regency otelinin zeminine salınmıştır. Bu kirli sularla Morochy'deki marina yaşamı yok olmuştur (CIIP [web], 2009).

5- Hainan Adası olayı

1 Nisan 2001 de Bir Çin jeti ile ABD casus uçağı Güney Çin Denizi'nde çarpışınca, 80.000 den fazla bilgisayar korsanı ABD'ye karşı saldırı başlattı. Bu olay The Newyork Times gazetesince "World Wide Web War 1" olarak tanıtılmıştır.

ABD'de "2003 Northeast Blackout" olarak bilinen ve sekiz eyalette 50 milyon kişiyi çaresiz bırakan, bazı bölgelerde iki gün süren ve 11 kişinin ölümü ve 6 milyar dolar zarar ile sonuçlanan ABD tarihinin en büyük elektrik kesintisinin sebeplerinden birinin elektrik dağıtım sisteminde kullanılan yazılım olduğunun saptandığı bildirilmiştir

6- 2001 *Code Red* Vakası

Code Red ilk defa Temmuz 2001'de ortaya çıkan ve birçok türü bulunan bir solucandır. Bu solucan ABD'de Microsoft'un IIS Web sunucularında bulunan bir güvenlik açığından faydalanmış ve yaklaşık olarak 300.000 bilgisayarı etkilemiştir. Solucanın yapısı ayın 1 – 19 arasında kendisini çoğaltacak, 20 – 27 arasında belirli bir siteye Hizmet Dışı Bırakma (*DoS*) saldırısı gerçekleştirecek ve 27'sinden ay sonuna kadar da bilgisayarda sessiz bir şekilde uyuyacak şekilde programlanmıştır. Bu solucanın ilk türleri belirli tarihlerde Beyaz Saray'a Hizmet Dışı Bırakma saldırısı düzenleyecek şekilde programlanmıştır. Beyaz Saray'ın sistemi saldırılardan titizlikle korunsa da diğer sitelerin hizmet veremez hale getirilip ana sayfalarının "Çinliler Tarafından Hacklendi" mesajı ile değiştirilmesinin önüne geçilememiştir (Frontline [web], 2003).

7- 2002 *Titan Rain* Vakası

Titan Rain: 2002 yılından itibaren ABD Savunma Bakanlığına Çin tarafından yapılan siber faaliyetlerin genel adıdır. 2006 yılında Pentagon iletişim ağında günlük yaklaşık olarak 3 milyon tarama yapıldığı ve bunun kaynağı olarak Çin ve ABD'nin ilk iki sıradaki ülke olduğu rapor edilmiştir.

Bu saldırılarda Çinliler tarafından NIPRNet sunucularından 10 – 20 terabayt veri indirildiği düşünülmektedir (Carr ve Shepherd, 2010:4). Bu faaliyetlerin sonrasında gerçekleşmiş olan vakalar da bu isimle anılmaya devam edilmiştir.

2008 yılında, ABD Savunma Bakanlığı iletişim ağına bağlı bilgisayarlarda 46.880 zararlı faaliyet tespit edilmiştir. Titan Rain saldırıları sadece ABD devlet sitelerini değil, devletle işbirliği yapan özel sektörü de hedef almıştır.

8- 2003 Ohio Nükleer Tesis Vakası

2003 yılının Ocak ayında ABD'nin Ohio Eyaletindeki bir nükleer tesisin özel ağına "*slammer*" adı verilen bir solucan bulaşmış ve nükleer tesisin güvenlik izleme sistemini yaklaşık beş saat süreyle devre dışı bırakmıştır (Poulsen [web], 2003).

Nükleer tesis, başlıklarından birindeki bir delik nedeniyle 2002 yılı Şubat ayından bu vaka gerçekleşene kadar geçen sürede devre dışı olduğu için tesisin bu solucandan zarar görmediği

belirtilmiştir. Vaka Nükleer Düzenleme komisyonuna tesisi işleten First Enegy Corp. tarafından Nisan ayında rapor edilmiştir. Rapora göre "*slammer*" solucanı sisteme rutin bir faaliyet sırasında ismi verilmeyen bir yüklenicinin ağına girmesiyle başlayan bir süreç sonucunda bulaşmıştır. Solucan sistemin normalden daha düşük bir şekilde faaliyet göstermesi sonucu fark edilmiştir. Davis-Besse tesisinin sistemine bulaşan bu solucan işlevinin bozulması durumunda yüz binlerce hayatı tehlikeye sokabilecek bir nükleer tesisisin bile siber güvenlik açısından tehlikelere ne kadar açık olabileceğini göstermesi açısından önem arz etmektedir.

2003 yılı Ekim'inde ABD'deki en yoğun limanlardan biri olan Houston Limanı'nda yer alan bilgisayar ağı saldırıya maruz kalmış ve limanda hizmetler bir müddet aksamıştır

9- 2006 – *Wikileaks* Vakası

2006 yılında İnternet sitesi ismini kaydettiren ve 2007 yılı Ocak ayında, elinde yayınlanmak üzere 1,2 milyon doküman olduğunu bildiren *Wikileaks* dünya üzerinde çok ses getirmiş bir sitedir. Birçok ülkeye ait gizli belgeleri bu tarihten itibaren yayınlamaya başlamıştır ve günümüzde bu faaliyetlerine devam etmektedir (Domscheit-Berg, Klopp ve diğerleri, 2011:xi). Dünyada geniş yankılar uyandıran bu haber sızıntıları "Wikileaks Gazeteciliği" olarak bilinen yeni bir gazetecilik teriminin doğmasına neden olmuştur.

Bu şekliyle *Wikileaks* dijital çağda gazetecilik tarihinde ortaya çıkmış en büyük fenomenlerden biri haline gelmiştir. Ortaya çıkardığı haberler, Johnson zamanında Vietnam Savaşı'nın başlatılmasıyla ilgili yalanlarla karşılaştırılır hale gelmiştir (Beckett ve Ball, 2012). Ortaya koymuş olduğu haberler, gazetecilik yöntemlerinin ve ülkelerin siber güvenliklerinin sorgulanır hale gelmesine neden olmuştur.

10- 2007 Estonya Vakası

İkinci Dünya Savaşında Estonya, Sovyetler Birliği ile birlikte Almanya'ya karşı savaşmıştır. Savaş sona erince Rusya, Estonya'da, Rusya tarafından Estonya'nın Nazi istilasından korunması için verilen mücadeleyi simgeleyen bir heykel dikmiştir.

Bu heykel 26 Nisan 2007 tarihinde Estonya tarafından yerinden kaldırılmıştır. Heykelin kaldırılması üzerine ülkede ayaklanmalar çıkmıştır. Bu olayı takip eden günlerde devlete ait internet sayfaları ele geçirilmiştir. Daha sonraki günlerde daha organize bir şekilde gerçekleştirilen saldırılar sonucu ülkenin ulusal bilgi sistemleri, internet hizmet sağlayıcıları ve bankaları çok büyük zarar görmüştür. Ülkenin internet sistemi çökme tehlikesiyle karşı karşıya gelmiştir. Estonya'nın 1,3 milyon olan nüfusunun 1 milyondan fazlası sayısal kimliğe sahiptir. Nüfusunun %66'sının internet kullanıcısıdır. Evlerin %55'inde internet bağlantısı vardır ve vergi beyanlarının %80'i internet üzerinden yapılmaktadır. Bankacılık işlemlerinin %97'sinin çevrim içi olarak gerçekleştirildiği, sağlık kayıtlarının tamamının sayısal ortamda tutulduğu da göz önünde bulundurulduğunda Estonya'ya verilen zararın boyutları tahmin edilebilecektir (Bakır, 2011:16).

11- 2008 Rusya – Gürcistan Vakası

2008 Ağustos ayında Rus ordusunun Güney Osetya'ya girmesi ile eş zamanlı olarak Gürcistan'ın altyapı ve hükümet sitelerine Siber saldırı düzenlenmesi ikinci büyük siber savaş vakası olarak kabul edilmektedir. (Coleman [web], 2008)

8 Ağustos 2008'de Rusya'nın Gürcistan'a saldırısının ardından Gürcistan'a ait internet sitelerine Hizmet Engelleme saldırıları düzenlenmiştir. Fiziki saldırılarla eş zamanlı olarak gerçekleştirilen siber saldırılar gerçek dünyada meydana gelen sorunların anında sanal dünyaya da yansıyabileceğini göstermektedir. Gürcistan ve Rusya arasındaki siber savaş kamuoyunu şekillendirme maksadı da taşımaktadır. İki tarafça da gerçekleştirilen *DoS* saldırılarına ilave olarak sahte siteler oluşturulmuş, bu sitelerde yoğun propaganda faaliyeti gerçekleştirilmiştir (Gürkaynak ve İren, 2011:271).

Saldırıda *Voip* iletişim sistemine zarar verilmiş Gürcistan Dışişleri Bakanlığı sitesinde Saakashvili'nin fotoğrafının yanına Adolf Hitler fotoğrafı yerleştirilmiştir (Coleman [web], 2008).

12- Stuxnet, Duqu, Flame, Gauss

2010 yılı ve öncesindeki siber saldırılarda genellikle servis dışı bırakma, spam mail yollama, web sitesi içeriği değiştirme/yönlendirme ile provokasyon yapma ve halkı yanıltma amacıyla saldırılar kullanılırdı. Bu tehditlerden daha tehlikeli sonuçlar doğurabilecek ve ileri siber casusluk tehditlerinin kullanılarak sistemlere gerçek hasar verebilecek zararlı yazılımlar ortaya çıktı. Özellikle endüstriyel sistemler gibi kritik alt yapıları hedef alan zararlı yazılımlar İran'ın nükleer faaliyetlerini durdurma/kontrol altına faaliyetlerinin hemen arkasından geldi. Siber casusluk, istihbarat ve siber sabotaj için oluşturulmuş bu yazılımlar çok büyük bütçeler, devlet desteği ile organize çalışılarak hedef olarak belirlenmiş sistemlere yönelik yazılıyordu.

Şekil-19: Stuxnet, Duqu, Flame, Gauss

Endüstriyel sistemleri yönetmek için kullanılan sistemler Supervisory Control and Data Acqustion kelimelerin baş harflerinden oluşan SCADA terimi ile Türkçede "Merkezi Denetim ve Veri Toplama" olarak karşılık bulur.

2006 yılında Amerikan askeri ve istihbarat yetkilileri gizli bir siber savaş programı hazırladılar. Bu programın amacı İran'ın uranyum zenginleştirme programını durdurmaktı. Kod adı "Olimpiyat oyunları" olan bu program ile Amerikan Ulusal laboratuvarlarında İran'ın Natanz kentindeki var olan nükleer santrallerinin sanal bir kopyası çıkartıldı. Amerikan NSA ve İsrail UNIT8200 adlı istihbarat kurumlarının beraber çalışarak hazırlandıkları proje ile o

ana kadar görülmüş en karmaşık zararlı yazılımı oluşturuldu. 2010 yılında yaklaşık 1000 santrifüj, ki bu sayı İran'daki çalışır durumda olan santrifüj sayısının 1/5'ine denk gelmektedir, hedef alınıp donanımları çalışılamaz hale getirilmiştir.

Stuxnet ilk defa haziran ayının ortalarında anti virüs üreticileri arasında çok da popüler olmayan Belarus menşeli küçük bir firma olan Virus BlokAda [VIRUSBLOKADA]tarafından tespit edildi. İlk incelemeler virüsün standart bir solucan olmadığını zaten gösteriyordu. Fakat stuxnet'in teknik analizi yapılırken işin boyutu farklı noktalara geldi. Özellikle solucanın çok karmaşık yapısı, kullandığı taktikler ve hedefi göz önüne alınınca, siber savaş adı altında yıllarca dillendirilen senaryoların aslında çok da gerçek dışı olmadığı ortaya çıktı. Stuxnet zararlı yazılımından yaklaşık 130.000 bilgisayarın etkilendiği belirtilmektedir. Ayrıca dünya üzerinde Stuxnet bulaşan bilgisayarların %60'ı İran'da yer almaktadır.

Stuxnet'in keşfinden bir sene sonra Duqu adı verilen yeni bir zararlı yazılım daha keşfedildi. Endüstriyel sistemler hakkında bilgi toplamak için oluşturulan bu zararlı yazılım muhtemelen stuxnet öncesi istihbarat sağlamak amacıyla oluşturulmuştur. Böylece Stuxnet'in daha etkin çalışması sağlanmıştır.

Birer sene aralıklarla tespit edilen siber silahlara bir yenisi daha eklenmişti: Flame en büyük en karmaşık siber casusluk yazılımı olarak ortaya çıkan bu yazılım senelerce siber ortamda bilgi toplarken kendisini devamlı güncellemesi ile anti virüs tarayıcıları tarafından tespit edilememiştir. 2012 yılında tespit edildiğinde diğer zararlı yazılımların aksine çok büyük (20MB boyutunda) olması, modüler olması diğer zararlı yazılımlardan kendisini ayırıyordu. Stuxnet ve duqu örneklerinde olduğu gibi geliştiricileri tarafında dahi bilinmeyen açıklıkları kullanarak uzun süre faaliyet göstermiştir. [30]

2012 yılında çıkan yeni siber silahlardan birisi de Gauss'tu. Bu zararlı yazılım yine Ortadoğu'yu hedef almış fakat bu sefer endüstriyel kontrol sistemleri yerine finansal bilgileri hedef alıyordu.

13- Flame

Flame, Siber Casusluk için kullanılan ve hedefe yönelik atak yapabilmek için tasarlanan, çok karmaşık bir saldırı kitidir. Hem arka kapı, hem bir Truva atı, hem de solucan

gibi farklı zararlı yazılımların özelliklerini barındıran bir yapıda çalışmaktadır. Ortadoğu'da özellikle akademik kurum ve devlet sistemlerini hedef almaktadır. [31]

Nasıl yayılır?

Bu zararlının ilk yayılma yöntemi olarak, mail üzerinden oltalama saldırıları kullanılarak veya çeşitli web sitelerine zararlı kod yükleyip, bu zararlı yazılımın indirilmesini sağlanması ile gerçekleştirildiği düşünülmektedir.

Flame'in ana hedefi Ortadoğu'dur, ayrıca çeşitli kaynaklarda GMT+2 saat diliminde olan ülkelerin hedef alındığı belirtilmiştir. Enfekte olan PC'ler yerel ağa bağlı diğer bilgisayarların ve taşınabilir bellekler ile daha fazla bilgisayarın etkilenmesine sebep olmuştur. Başka bilgisayarlara yayılmak için stuxnet tarafından da kullanılan açıklıklar kullanılmıştır.

3. SİBER GÜVENLİK

Günümüzde hızla artan siber tehditler nedeniyle, birçok ülke güvenlik politikalarının içerisinde önemli bir başlık olarak siber güvenliğe yer vermeye başlamıştır. Bu ülkelerden bazıları ekonominin, sosyal yaşamın ve milli güvenliğin sanal dünya ile giderek iç içe girmesi sebebiyle, siber güvenlik alanına büyük yatırımlar yaparak bu alanda çalışacak kadroları yetiştirmek için çeşitli stratejiler geliştirmektedirler. Bunların dışındaki ülkeler ise daha geriden gelişmeleri takip ederek, başarılı örnekleri saptadıktan sonra onları kendilerine uyarlayarak kamu ve özel sektördeki ağların güvenliğini sağlamaya çalışmaktadır.

Siber güvenliğin en üst düzeyde sağlanabilmesi için;

- Siber güvenlik politikası oluşturulmalıdır,
- Devletin çatısı altında uygulayıcı kurumlar oluşturulmalıdır.
- Daha sonrasında uyum içerisinde çalışabileceği bir mekanizma kurulmalıdır,
- Bu yapıların esnek ve hızlı bir biçimde çalışmalarını sağlayabilecek hukuki altyapı oluşturulmalıdır.
- Ülkemizde bu alanda hem kamu hem de özel sektörde çalışacak nitelikli personel ihtiyacının karşılanabilmesi için üniversitelere düşen roller düzenlenmelidir.
- En son gelişmeleri takip edip siber güvenlik alanında en ileri düzeyde savunma yapabilmek için AR-GE merkezleri kurulmalıdır.

3.1 Güvenlik Prensipleri

Bilişim Güvenliğinin birçok boyutu olmasına karşın yedi prensipten söz edilebilir: Gizlilik, Veri Bütünlüğü, Süreklilik, İzlenebilirlik, Kimlik Sınaması, Güvenilirlik, İnkâr Edememe.

3.1.1 Gizlilik (Confidentiality)

Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik hem kalıcı ortamlarda (disk tape vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik bilgisayar başında

çalışan bir kullanıcının ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.

Şekil-20: Bilgi Güvenliği Temel Prensipleri

3.1.2 Veri Bütünlüğü (Data Integrity)

Bu hizmetin amacı veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri haberleşme sırasında izlediği yollarda değiştirilmemiş araya yeni veriler eklenmemiş belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: Bozulma Sınaması ya da Düzeltme Sınaması.

Bozulma Sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenmiştir. Düzeltme Sınaması'nda ise Bozulma Sınaması'na ek olarak eğer veride değişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenmektedir.

3.1.3 Süreklilik (Availability)

Bilişim sistemleri kendilerinden beklenen işleri gerçekleştirirken hedeflenen bir performans vardır. Bu performans sayesinde müşteri memnuniyeti artar ve elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti bilişim sistemlerini kurum içinden ve dışından gelebilecek performansı düşürücü tehditlere karşı korumayı hedefler. Süreklilik hizmeti sayesinde kullanıcılar erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden zamanında ve güvenilir bir şekilde ulaşabilirler. Sistem sürekliliği yalnızca kötü amaçlı bir "hacker"ın sistem performansını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir.

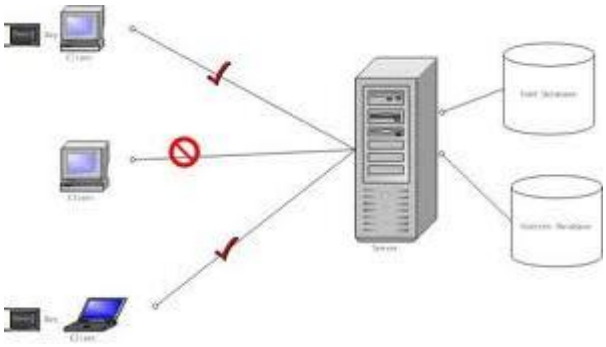
3.1.4 İzlenebilirlik ya da Kayıt Tutma (Accountability)

Bu hizmetin hedefi sistemde gerçekleşen olayları daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay dendiğinde bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak, göndermek ya da icq ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır.

3.1.5 Kimlik Sınaması (Authentication)

Ağ güvenliği açısından kimlik sınaması; alıcının göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması sadece bilgisayar ağları ve sistemleri için değil fiziksel sistemler için de çok önemli bir hizmet haline

gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır.



Şekil -21: Kimlik Sınaması

3.1.6 Güvenilirlik (Reliability - Consistency)

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik sistemden ne yapmasını bekliyorsak sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.

3.1.7 İnkâr Edememe (Non-repudiation)

Bu hizmet sayesinde ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Bu hizmetler zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir denilebilir.

3.2 Bilgi Sistemleri Güvenliği

Bilgi sistemleri güvenliği erişilebilirlik, gizlilik ve bütünlük ilkeleri çerçevesinden düşünüldüğünde çok geniş bir yelpazede konuyu içeren bir alandır. Bu üç temel ilkenin hepsinin bir arada sağlanması ise bu geniş çalışma alanının her konu baslığında gerekli çalışmanın yapılması zorunluluğunu ortaya çıkarır. Örnek verilmek istenirse, bütünlüğü bozulmuş bir hasta veya finans bilgisinin erişilebilir olmasının ve gizliliğinin bir anlamı kalmamaktadır.

Güçlü bir güvenlik altyapısı kurabilmek için bu üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir yaklaşımla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde bilgisayar ve bilişim güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Diğer bir deyişle bir kurumun kurumsal bilişim güvenliğini sağlamak amacıyla sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır.

3.2.1 Kurumsal Bilgi Güvenliği Önlem Türleri

Kurumsal bilgi güvenliği, bilginin üretildiği işlendiği ve saklandığı her ortamda sağlanmak zorundadır. Bunun için mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları dikkate alınmalıdır.

Bilgi güvenliğine yönelik olarak alınabilecek önlemleri genel olarak 3 başlık altında toplamak mümkündür:

1. Yönetsel önlemler
2. Teknolojik önlemler
3. Eğitim

Kurumsal bilgi güvenliği yönetim, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve bu üç unsur arasında tamamlayıcılık olmadığı sürece etkin bir güvenlikten bahsedebilmenin mümkün olamayacağı yönetilmesi zorunlu olan canlı bir süreçtir. [32]

Bu üç önlem türünün her biri başarıya ulaşmak için diğer iki önlem türü ile tam ve eksiksiz çalışmalıdır. Bu üç önlem türü birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Bir kurumun bilgi güvenliği bu üç önlem türünün birlikte çalışmasıyla sağlanabilmektedir.

3.2.1.1 Yönetsel Önlemler

Yalnız teknolojik önlemlerle (anti-virüs "firewall" sistemleri kripto vb.) iş süreçlerinde bilgi güvenliğini sağlama olanağı yoktur. Bilgi güvenliği süreçlerin bir parçası olmalı ve bu bakımdan bir iş anlayışı yönetim ve kültür sorunu olarak ele alınmalıdır. Her kurum mutlaka bireysel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dokümante etmek ve çalışanlarına iş ortaklarına paydaşlarına aktarmak zorundadır. Tüm çalışanlar bilgi güvenliği konusunda bilinçli olmalı, erişebildikleri bilgiye sahip çıkmalı, özenli davranmalı, üst yönetim tarafından yayınlanan "Bilgi Güvenliği Politikası" şirket açısından bilgi güvenliğinin önemini ortaya koymalı, sorumlulukları belirlemeli, çalışanlarını bilgilendirmeli ve Bilgi Güvenliği sistemi iş ortaklarını (müşteri tedarikçi taşeron ortak firma vb.) da kapsamalıdır.

Yönetsel Önlemler güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi bilgi güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından belirlenenlerin yazıya dökülmesi yani prosedür, yönerge ve talimatlar gibi dokümanların oluşturulması gelmelidir. [33]

Üst yönetimin desteği olmadan kurumsal tabanda bir işi gerçekleştirmek hayli zordur. Bu nedenle üst yönetim ile güvenlik yönetimi arasında açık bir iletişim kanalı kurulmalı ve her iki yönde de kusursuz bir bilgi akışı sağlanmalıdır. Bu sayede yürütülen güvenlik yönetim programı üst yönetimden ihtiyacı olan desteği alır, üst yönetim de gerektiğinde devreye girerek gerekli stratejik kararları verir. [34]

Yönetsel önlemler kapsamında yapılması gereken temel işlemler şunlardır:

1.Risk yönetimi

2. Güvenlik politikaları

3. Standartlar, yönergeler ve prosedürler

4. Güvenlik denetimleri

Risk yönetimi

Risk sözlük anlamı olarak zarara uğrama tehlikesidir; öngörülebilir tehlikeleri ifade eder. Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliğini, ticari müesseseler içinse öncelikle karlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. [35]

Bir sistemin nasıl korunacağına karar vermeden önce onu hangi tehlikelere karşı korumak gerektiği bilinmelidir. Coğrafyanın karakteristiğinden teknik hatalara, intikam almak isteyen eski çalışanlardan "hacker"lara kadar tüm riskler göz önünde tutulmalıdır. Doğrudan ve dolaylı maliyetler dikkate alınmadığında bir kurum için kağıt üstünde "çok güvenli" bir güvenlik altyapısı kurmak kolaydır. Ancak kurumun hedefi kendisi için "yeterli, etkin ve yönetilebilir" bir güvenlik altyapısını oluşturmak olmalıdır. Bu yeterlilik düzeyini belirlemekte risk analizi önemli bir role sahiptir. Risk analizi yardımıyla kurumlar karşı karşıya bulundukları riskleri öncelik sırasına koyabilir ve her bir riske karşı alınacak önlemlerin ve tedbirlerin getireceği maliyetleri değerlendirebilirler. Risk yönetimi riskin tümüyle engellenmesi değil sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için kurumun varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, kontrol altında tutmak ve izlemek gereklidir.

Burada önemle üzerinde durulması gereken konu etkinliktir. Risklerin ortadan kaldırılması veya azaltılması için kontrollerin oluşturulması gereklidir ancak çok fazla kontrol sebebiyle iş yapılamaz duruma gelinmesi de kurumlar için bir risk faktörü olabilmektedir. Risk yönetimi prosedürleri oluşturulurken getiriler ve etkinlik iyi değerlendirilmelidir.
Risk analizi, risklerin gerçekleşme olasılıklarının gerçekleşmeleri durumunda yol açacakları kayıpların doğru bir şekilde belirlenmesi ve buna göre uygun tedbirlerin devreye sokulmasıdır. Risk analizinin üç temel amacı vardır:

- Risklerin belirlenmesi
- Tehditlerin potansiyel etkisinin belirlenmesi

-Riskin gerçekleşmesi durumunda getireceği zararla bu riskten korunmak için seçilecek tedbir arasında ekonomik bir denge kurulması.

Risk değerlendirmesi çalışmasında aşağıdaki esaslar göz önünde bulundurulmalıdır:

a) Bilgi varlıklarının (ekipman, yazılım vb.) ya da iş varlıklarının ve aktivitelerinin tanımı ve değerinin tespit edilmesi;

b) Bu varlıklara karşı içeriden veya dışarıdan gelebilecek tehditlerin belirlenmesi;

c) Bu tehditlerin oluşma olasılığının belirlenmesi;

d) Bu tehditlerin kurumdaki etkilerinin belirlenmesi;

e) Tehditlerin engellenmesi veya kabul edilebilir bir seviyeye indirilmesi için gerekli ek kontrollerin belirlenmesi;

f) Ek kontrollerin uygulanması için aksiyonların planlanması.

Risklerin yukarıda belirtildiği şekilde tanımlanması ve önceliğinin belirlenmesinin yanı sıra; bu risklerin azaltılması ya da ortadan kaldırılmasına yönelik kontrol ve çözüm alternatifleri; maliyet uygulanabilirlik ve yararlılık ilkeleri doğrultusunda değerlendirilmeli gerekli önlemler planlanarak uygulanmalıdır.

Güvenlik Politikaları

Kurumsal bilgi güvenliği politikası, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uymaları gereken kuralları içeren kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden resmi bir belge niteliğindedir.

İyi bir bilgi güvenlik politikası öncelikle uygulanabilir olmalıdır. Politika kullanıcıların ve sistem yöneticilerinin eldeki olanaklarla uyabilecekleri kurallar ve ilkelerden oluşmalıdır. Politika yeterli düzeyde yaptırım gücüne sahip olmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer yaptırımları uygulayabilecek güçle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri açıkça tanımlanmalıdır. Kullanıcılar, sistem yöneticileri ve diğer ilgililerin sisteme ilişkin sorumlulukları ve yetkileri kuşku ve çelişkilere

yer bırakmayacak biçimde açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar açıklanmalıdır. Güvenlik politikasının kapsamı da nitelikleri kadar önemlidir. Kurumun sahip olduğu bilgi varlıkları ve ihtiyaçları doğrultusunda kapsam belirlenmelidir. Bilgi varlıklarının tamamı kapsam dâhilinde olabileceği gibi belirli ortamlarda saklanan bilgi varlıkları da belli bir yerleşim birimindeki bilgi varlıkları da kapsamı oluşturabilir. Güvenlik politikaları kurumun üst düzey yönetimi tarafından desteklenmeli ve çalışanlar tarafından benimsenmelidir. Güvenlik politikası kullanıcılar tarafından uygulanabilir ve anlaşılabilir, güvenlik yöneticileri tarafından yönetilebilir olmalıdır.

Bilgi güvenliği politikaları her kuruluş için farklılık gösterse de genellikle çalışanın sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını, dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadelerdir. Yönetimin kurumsal bilgi güvenliği hakkında aldığı ayrıntılı kararları da içerir.

Kurumsal Bilgi Güvenlik Politikası Çeşitleri

Kurumsal bilgi güvenlik politikaları kurumların hassasiyetleri doğrultusunda farklılıklar gösterebilir. Bilgi güvenliğinin temel unsurlarından hangisi kurum için daha önemli durumda ise o unsura önem verilerek politika hazırlanabilir. Kurumsal bilgi güvenliği politikası kuruma özgü olmalıdır ve kurumun ihtiyaçlarına yönelik olmalıdır.
Gizlilik politikası: Elimizde bir miktar bilgi olsun ve bir grup insan bu bilgiye ulaşabilsin bu bilgi bu grubun dışındakiler için gizli bilgidir. Gizlilik açısından güvenlik politikası yetkisi olmayanlara bilgi sızmasının ne zaman söz konusu olduğunu tanımlar.

Bütünlük politikası: Elimizde bir miktar bilgi olsun ve bir grup bu bilginin bütünlüğüne güvensin o zaman bu bilgi bu gruba göre bütünlüğü olan bilgidir. Burada söz konusu bir kaynak da olabilir o zaman o kaynağa güvenen grup için o kaynak bütünlüğe sahiptir. Bütünlük açısından güvenlik politikası bilginin hangi durumda hangi yolla ve/veya kimler tarafından değiştirebileceğini tanımlar. Buna bütünlük politikası denir.

Kullanılabilirlik politikası: Elimizde bir miktar bilgi olsun ve bir grup bu bilgiyi kullanabilsin o zaman bu bilginin bu grup tarafından kullanılabilir olduğu söylenir. Kullanılabilirlik açısından güvenlik politikası hangi servislerin ne şartlar altında söz konusu kullanıcılar tarafından kullanılabileceğini tanımlar. Buna kullanılabilirlik politikası denir.

Askeri-yönetimsel güvenlik politikası: Bu çeşit politikalarda ilk amaç gizliliktir. Güvenilirlik ve erişilebilirlik de önemlidir ancak birinci planda gizlilik gelir. Diğer ikisinin üstesinden gelinebilir ancak gizliliğin delinmesinin sonuçları çok ağır olur.

Ticari güvenlik politikası: Bu çeşit politikalarda ilk amaç güvenilirliktir. Bunun isminin ticari olmasının nedeni ticari uygulamalarda amaç, verilerin değiştirilmesini engellemektir. Politika dokümanları kuralların farklı ve yanlış anlaşılmasını önlemek, ilgilileri eğitmek, muhtemel sorunları önceden tespit edebilmek, kriz durumlarında hızlı hareket edebilmek gibi faydalar sağlar. Yasal boşlukların olduğu durumlarda kuruluşun saldırganlardan korunabilmesi için politika dokümanları yasal destek oluşturur. Uygulanacak olan yasal ve ahlaki mahremiyet koşulları açıklanmalıdır.

Elektronik mesajların ve dosyaların okunması, kullanıcı işlemlerinin kaydedilmesi gibi kullanıcıların davranışlarının izlenmesine dönük işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır.
Güvenlik politikaları güvenli bir sistemin nasıl olması gerektiğini tanımlar. Güvenlik politikaları oluşturulurken sisteme gelebilecek bütün tehditler göz önünde bulundurulmalıdır. Ayrıca güvenlik tehditleri zamanla değiştiğinden güvenlik politikaları da devamlı kontrol edilip güncellenmelidir. Güvenlik politikalarının etkin olarak kullanılabilmesi için kullanıcıları da güvenlik politikaları konusunda bilgilendirmek gerekmektedir.
Politikalar içerisinde; gerekçelerin ve risklerin tanımlandığı, kapsadığı bilgi varlıkları ve politikadan sorumlu olan çalışanların ve gruplarının belirlendiği, uygulanması ve yapılması gereken kuralların ihlal edildiğinde uygulanacak cezai yaptırımların, teknik terimlerin tanımlarının ve düzeltme tarihçesinin yer aldığı bölümden oluşmalıdır. [36]

Güvenlik Denetimleri

Bilgi güvenlik denetimi maliyete ve bir güvenlik olayının diğer bütün zararlarına uğramaksızın kurumun bilgi güvenliğini belirlemesi için en iyi yollardan biridir.
Güvenlik denetimleri sürekli devam eden etkin güvenlik politikalarının tanımlanması ve korunması sürecinin parçasıdırlar. Güvenlik denetimlerinin cevaplaması gereken anahtar sorular vardır:

• Şifreleri kırmak zor mu?
• Paylaşılan verilere kimin eriştiğini kontrol etmek için ağ cihazları üzerinde yer alan erişim kontrol listeleri var mı?
• Veriye kimin eriştiğini kaydeden denetleme günlükleri var mı?
• Denetim günlükleri yeniden gözden geçiriliyor mu?
• İşletim sistemleri için güvenlik ayarları endüstri güvenlik uygulamalarına uygun kabul edildi mi?
• Her bir sistem için bütün gereksiz uygulamalar ve bilgisayar hizmetleri elimine edildi mi?
• Bu işletim sistemleri ve ticari uygulamalar var olan seviyeyle uyuşuyor mu?
• Yedekleme ortamları nasıl saklanıyor? Kim ona erişebiliyor? Güncelleniyor mu?

Bunlar bir güvenlik denetiminde değerlendirilebilecek, değerlendirilmesi gereken soru türlerinden yalnızca birkaçıdır. Dürüstçe ve dikkatlice bu soruların cevaplanmasıyla kurum gerçekçi olarak önemli bilgilerinin güvenliğinin nasıl olduğunu değerlendirebilir.
Bilgi güvenliği bilgi teknolojilerinden daha fazlasını içerir ve sistemi kullanan insanlar da dikkatsizce güvenlik boşlukları açabilir. Bir güvenlik denetimi, bilgi teknolojileri altyapısı ve ekip davranışları içinde problemli alanları ortaya çıkarmayı ve dikkat çekmeyi amaçlar. Her denetim sonuç olarak bütün olası riskleri belirlemeye çalışmalıdır.

3.2.1.2 Teknolojik Önlemler

Güvenliği Sınıflandırmak

Mantıksal Güvenlik

Mantıksal güvenlik bilgi sistemlerinin iletişim ağları vasıtası ile maruz kalabileceği tehditleri kapsamaktadır.

Fiziksel Güvenlik

Fiziksel güvenlik ise bilgi sistemlerini barındıran fiziksel altyapının güvenliğini tarif etmektedir. Fiziksel güvenliğin kapsamına sunucu ve istemci donanımları, sistem odası, sistem odasının bulunduğu bina, güç hatları gibi bileşenler girer.

Çevre Güvenliği

Çevre güvenliği ise fiziksel güvenlikle bir düşünülebilir, ayrıldığı nokta ise bilgi sistemini barındıran bina veya kampus alanının sınırlarında alınacak güvenlik önlemleridir.

Mantıksal Güvenlik

Mantıksal güvenlik iki alt guruba ayrılabilir:
Uygulama Güvenliği
Altyapı Güvenliği

Uygulama güvenliği, uygulamayı geliştiren yazılım ekibinin sorumluluğunda olan bir alandır. Burada yazılımcıların yazdıkları uygulama için geliştirme sırasında gerekli olan güvenlik seviyesine göre gereken önlemleri almaları beklenir.

Altyapı güvenliği ise bilgi sistemlerinin diğer sistemler ve kullanıcılar ile iletişim kurması esnasında alınabilecek önlemleri kapsar. Bu önlemler altyapı üzerinden geçen trafik üzerinde veya pasif olarak güvenlik personeline bilgi sağlayacak şekilde olabilir. Bir bilgi sistemi katmanlı olarak düşünülürse yapılan sınıflandırmaların Şekil 1 de hangi katmanlara denk geldiği görülebilir.

Bilgi Sistemi Uygulamaları, Hizmetler	Uygulama Güvenliği
Veritabanları	
Hazır yazılımlar	
İşletim Sistemi	Alyapı Güvenliği
İç Network	
İnternet	
Fiziksel Ekipman, Personel, Tesis	Fiziksel Güvenlik

Şekil-22: Bilgi Sistemleri Katmanları

3.2.1.2.1 Güvenlik Yazılımları

Kamu ve özel sektör kurum ve kuruluşları, güvenlik ihtiyaçlarına göre aşağıda kısaca özetlenmiş olarak verilen güvenlik yazılımlarını kullanabilirler. Güvenlik yatırımlarının kurumların ihtiyaçlarını karşılayacak şekilde yapılması önemlidir. İhtiyaçtan daha az veya daha fazla yapılan yatırım ve çabalar her zaman maddi ve manevi zararlar ile sonuçlanacaktır.

1- Güvenlik Duvarı (Firewall): Güvenlik duvarları üzerlerinden geçen trafik için erişim kuralları belirlemek ve uygulamak amacı ile kullanılırlar. Üzerlerinde bulunan kural tablosu yardımı ile istenmeyen yere doğru giden belirli nitelikte trafiğin geçişi engellenebilir. Ana ağ segmentleri (veya bölümleri) içinde kullanılabilmeleri sayesinde segmentler arasında erişim kuralları uygulanabilir. Dış dünya ile bağlantıyı güvenlik duvarları sağladığından mobil kullanıcıların şifreli olarak bağlantı kurmalarına olanak sağlayarak açık ağlardan geçerken verinin gizliliğinin korunmasına yardımcı olur. [37]

2-Atak Önleme Sistemi (Intrusion Prevention System, IPS): Atak önleme sistemleri korunmak istenen ağ segmentlerinin bağlantıları üstüne konularak zararlı trafiğin kesilmesi sağlanır. IPS sistemleri trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği

ararlar ve bulduklarında, paket düşürme, TCP bağlantısını sonlandırma gibi eylemlerde bulunabilirler. Bu özelliklere ek olarak servis dışı bırakma saldırılarına karşı, istatistiksel ve manüel verilmiş sınırları işleterek koruma sağlayabilirler. [38]

3-Web Uygulama Güvenlik Duvar (Web Application Firewall): Web uygulama güvenlik duvarları IPS lere benzer bir görev üstlenir. Web hizmetlerinin çok yaygın kullanılması sebebi ile üretilen bu sistemler web hizmetlerine ve web sunucularına gelebilecek saldırıları önleyecek trafik imzaları bulundururlar. Bu özelliklerine ek olarak yazılım geliştirilirken önlem alınmamış konularda ek koruma getirebilirler. Web arayüzünde bilgi girişi yapılan alanlar üzerinde istenilen kontrollerin veya girdi doğrulamasının yapılması bir örnek olarak verilebilir.

4-Veritabanı Güvenlik Duvarı (Database Firewall): Veri tabanı güvenlik duvarları veri tabanına gelen sorguları inceler ve olası zararlı aktiviteleri tespit edebilir. Kullanıcı davranışlarını öğrenerek profil dışına çıkma durumlarında uyarı üretebilirler. Web ve veri tabanı güvenlik duvarının beraber kullanımı ile kullanıcıların web üzerinde yaptıkları işlemlerin veri tabanı üzerinde yarattığı iz düşümü takip edilebilir. Bu sayede uygulamaların veri tabanına bağlandığı tek bir kullanıcı yerine gerçek kullanıcıların kimlik bilgileri ile eşleştirme yapılarak veri tabanı operasyonları gerçek kişilere bağlanabilir.

5-E-Posta Güvenliği (E-mail Security Gateway): Kurum sistemlerine dışarıdan gelen spam ve zararlı kodların önlenmesinde kullanılırlar. Ağ seviyesinde internete açık bir şekilde mail sunucu (Mail transfer agent, MTA) görevi ile de kullanılabilir. Aynı zamanda mail sunucuların üzerinde çalışan çeşitleri de vardır.

6-Yük Dengeleyici (Load Balancer): Yük dengeleyiciler erişilebilirliği en üst seviyede tutmak için yoğun istek gelen sunucular arasında yük paylaştırırlar. Eğer bu bir web sunucu ise SSL(secure sockets layer)'i kendi üstlerinde sonlandırarak sunucuları kriptolama yükünden kurtararak performans artışı sağlarlar.

7-URL Filtresi ve Antivirus (Web Security Gateway): Kurum ağında çalışan istemcilerin internet erişimlerini düzenlemek amacı ile kullanılırlar. Bazı sitelere erişimin engellenmesi hem güvenlik hem de kurum politikası gereği istendiği durumlarda erişimi engelleyebilirler. Bu işlevi yaparken vekil sunucu şeklinde çalışıyorlarsa gelen trafik üzerinde zararlı yazılım taraması da yapabilirler.

8-Web Cache Vekil Sunucusu (Caching Proxy Server): Cache sunucuları URL filtreleri ile aynı sistemde olabildikleri gibi ayrı olarak da kullanılabilir. İnternetten çok defa aynı dosyanın indirilmesi durumunu engellemek amacıyla çok indirilen dosyaları üzerlerinde tutarak internet bant genişliği tasarrufu sağlarlar. Bu da erişilebilirliği artıracaktır.

9-Transparan İçerik Yönlendiriciler (Transparent Redirection): Karmaşık ve büyük ağ yapılarında istemcilerin URL filtre gibi trafiğin yönlendirilmesi gereken yerlerde kullanıcı sistemleri üzerinde ayar yapılmadan gönderilmesini sağlayabilirler. Bu özellik ile kullanım kolaylığı sağlarken aynı zamanda da ayarların eksik yapılması ihtimalini ortadan kaldırarak her kullanıcının istenen vekil sunucuları kullanmasını garanti altına alırlar.

10-Zafiyet Tarama Sistemleri (Vulnerability Scanner): Böyle bir sistem işletim sistemleri üzerindeki ve işletim sisteminde çalışan uygulamalar üzerindeki zafiyetleri otomatik taramalar ile bulur. Aynı zamanda yama eksikleri veya kurum politikasına aykırı yapılandırılmış sistemleri de tespit edebilir.

11-Risk Analiz ve Önceliklendirme Sistemi (Risk Management Systems): Zafiyet tarama sistemlerinden sistem zafiyetlerini, güvenlik duvarı, ağ anahtarları ve yönlendiricileri gibi cihazlardan da yapılandırma ayarlarını toplayarak bir ağ modeli oluşturur. Oluşturulan ağ modeli üzerinden risk analizi yapılır ve önceliklendirilir. Bu sayede kısıtlı personel kaynaklarının nerelerde ilk önce kullanılması gerektiği ve en çok risk altında bulunan sistemler gibi bilgiler elde edilir

12-Kayıt Toplama ve Korelasyon Sistemi (Security Information and Event Management, SIEM): Birçok güvenlik sistemi üzerlerinde meydana olaylar için çeşitli

ortamlarda olay kayıtları tutarlar. Bu olay kayıtları her sistemin üzerinde olduğundan diğer sistemlerdeki olaylar ile ilişkilendirme işlemi çok zor olmaktadır. SIEM sistemleri dağıtık halde olan bu kayıtları bir yerde toplayarak korelasyon yapılabilir hale getirirler. Yazılan mantıksal kurallar sayesinde gerçek zamanlı korelasyon yapılabilir ve normalde tespit edilemeyen güvenlik olayları tespit edilebilir.

13-Ağ erişim kontrolü (Network Access Control): Ağ erişim kontrolü sistemleri kurum politikalarına uymayan sistemlerin ağa dâhil olmalarını engellemek amacı ile kullanılır. Bu sayede yabancı sistemlerin ve güvenlik durumu uygun olmayan sistemlerin iç ağı tehdit etmesi önlenir.

14-Sıfır Gün Zararlı Yazılım Tespit Sistemi (Zero Day Malware Protection System, Malware sandboxing): İmza tabanlı zararlı yazılım tespit sistemleri (Antivirüs) imza veri tabanlarında olmayan zararlı yazılımları yakalayamamaktadır. Günümüzde artan bir hacimde zararlı yazılımlar yazıldığından imza veritabanlarında yer almaları uzun süreler almaktadır ve bu arada geçen zamanda sistemler savunmasız kalmaktadırlar. Bu sistemler genelde şüpheli yazılımları ağ seviyesinde yakalayarak test sistemlerinde çalıştırırlar (Sandboxing). Çıkan sonuçlara göre imzasız olarak zararlı tespit edilen yazılımlar engellenebilir.

15-Ağ izleme ve Performans Analiz Sistemi (Network Performance Management): Böyle bir sistem ağ trafiği üzerinden uygulama ve ağ performansı hakkında bilgi toplar. Bu sayede performans kaybı olaylarında bilgilendirme yapabilir ve bu durumlarda sorunun kaynağı ile alakalı detaylı bilgiyi ilgili personele sağlar.

16-Veri Kaçaklarını Önleme Sistemi (Data Loss Prevention): Sistemler üzerinde bulunan hassas verinin izinsiz kurumlar dışına çıkartılmasına engel olur. Hem ağ hem de istemci seviyesinde çalışan modelleri vardır. İstemci üzerinde çalışan sistemlerde taşınabilir medya gibi kaynaklardan kaçakların önlenmesi için aygıt kontrolü yapan bileşenleri bulunur. Yazıcılar, CD-DVD yazıcı ve okuyucular, USB depolama cihazları örnek olarak verilebilir.

17-Ağ Tabanlı Adli Bilişim Sistemi (Network Forensics): Bu sistemler pasif olarak ağ trafiğini yakalayarak trafik üzerinde derin paket incelemesi yapabilme olanağı sağlarlar. Bu sayede sistemde meydana gelen olaylar ve sorunlar detaylı şekilde incelenebilir. Trafik kayıt edildiği için veri kaçaklarını önleme sistemlerine kaçak olması durumunda çıkan verinin niteliği hakkında bilgi sağlayarak yardımcı olurlar.

18-Tek Yönlü Veri Transfer Cihazları (One Way Data Transfer *)*: Genelde internete kapalı ağlara veri transferi yapılırken dışarı veri sızıntısını engellemek amacı ile kullanılırlar. Donanım tabanlı ürünler iki tarafa da kullanılan protokol çalışırmış gibi gösterirken donanım üzerinde bir yön haricinde ters yöne veri iletişimi fiziksel olarak engellerler.

19-İstemci Güvenlik Ürünleri (Endpoint Security): İstemci üzerinde çalışan güvenlik ürünleri ağ seviyesinde çalışanlara destek olacak şekilde ek bir katman olarak görev yaparlar. Antivirus, IPS, Veri kaçakları önleme yazılımı, disk şifreleme örnek olarak verilebilir. [39]

3.3 Siber Güvenlik Politikalarına Ve Uygulayıcı Kurumlara Dünyadan Örnekler

3.3.1 Hindistan

Hindistan yaklaşık 1.173.000.000 kişilik nüfusu ile Çin'den sonra dünyanın en kalabalık 2.ülkesi olmasının yanı sıra, Çin ile birlikte yakın gelecekte güç dengelerini önemli oranda değiştireceği tahmin edilen, dünyada politik ve stratejik anlamda en önemli ülkelerden birisidir.

Yoğun nüfusunun yanında, bilişim sektöründeki gelişmeler ve yatırımlar sebebiyle Hindistan, siber güvenlik alanına birçok ülkeden daha fazla önem vermeye başlamış ve bununla ilgili olarak çeşitli düzenlemelere gitmiştir. Bilişim sistemlerine ve bilgi güvenliğine karşı giderek büyüyen tehditleri karşılayabilmek için, Hindistan Devleti Inter Departmental Information Security Task Force (ISTF) isimli kuruluşu oluşturmuş ve Ulusal Güvenlik Konseyi (National Security Council) ile birlikte en üst düzeyde yetkilendirmiştir. Böylece kapsamlı bir Ulusal Siber Güvenlik Politikasının inşasına başlanmıştır. Bu çerçevede ISTF'nin yaptığı öneriler

doğrultusunda aşağıdaki konu başlıklarıyla ilgili devlet düzeyinde çalışmalar yapılmaya başlanmıştır

- Ulusal bilgi güvenliği tehdit algılamalarının saptanması
- Kritik altyapıların korunması
- Bilgi güvenliğinin sağlanması için gerekli yasal düzenlemelerin hazırlanması
- Siber güvenlik konusunda farkındalık yaratılması ve ilgili personelin eğitimi
- Siber güvenlik konusunda araştırma ve geliştirmelerin desteklenmesi ve bu çalışmalara özel sektörün ve üniversitelerin de dahil edilmesi

Bu çalışmaların yanında, Hindistan Devletine ait ağların ve kritik altyapıların korunması için Bilgi Güvenliği Çerçeve Politikası hazırlanmıştır. Ulusal çapta yürütülen bir Bilgi Güvenliği Farkındalığı ve Eğitimi Kampanyası düzenlenmiştir ve bu kampanya devam etmektedir. Siber uzayın güvenli tutulabilmesi için uygulanacak eylem planı da aşağıdaki gibi belirlenmiştir:

- Adli bilişim sistemlerinin geliştirilmesi ve saldırı analizlerinin 7/24 esasına göre yapılması
- Ulusal açıdan kritik önemde olan altyapıların, ağların ve bilişim sistemlerinin korunması
- Erken saptama ve uyarı sistemlerinin geliştirilmesi
- Ekonomiye zarar verebilecek düzeydeki organize siber saldırılara karşı koruma sağlanması
- Kritik sektörlerdeki firmaların bilişim sistemlerinin güvenliklerini en üst düzeyde sağlayabilmeleri için onlara AR-GE desteğinin verilmesi.

Siber güvenliğin sağlanmasına yönelik oluşturulan bu stratejinin yanı sıra, Hindistan Ulusal Güvenlik Konseyi Danışma Kurulu (National Security Council Advisory Board) sunduğu bir raporda, Amerika Birleşik Devletleri'nin oluşturduğu gibi merkezi bir siber komutanlığın kurulmasını önermiştir.

CERT-In 2010 yılında "Siber Saldırılar ve Siber Terörizme Karşı Kriz Yönetimi Planı" oluşturmuş ve bu planın tüm devlet bazında ve kritik sektörlerde uygulamaya geçirilmesi için

çalışmalarına devam etmektedir. Bunun dışında kritik sektörlerde ve devlet kurumlarında siber saldırılara karşı direncin daha sağlam olması ve güvenlik omurgasının güçlendirilmesi için, kritik sektörlerde iş yapan firmalara, Hindistan Devleti tarafından, ISO 27001 Bilgi Güvenliği Yönetimi Standardı çerçevesinde iş organizasyonlarını yeniden oluşturmaları konularında bilgilendirmelerde bulunulmakta ve bu dönüşüm teşvik edilmektedir.

Hindistan'da yaklaşık 246 firma ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardına uygunluk sertifikasına sahiptir ve bu firmalar genellikle bilgi teknolojileri, telekomünikasyon ve bankacılık gibi sektörlerde yer alan firmalardır.

CERT-In kanalıyla, devlet kurumlarına ve özel sektördeki firmalara düzenli aralıklarla penetrasyon testleri uygulanmakta ve böylece bilişim sistemlerinin hangi noktalarında açıkları olduğu saptanarak bunlara yönelik önlemler alınmaktadır. CERT-In Hindistan Bilgi Teknolojileri Departmanına ulusal siber güvenlik stratejisi ve ulusal bilgi güvenliği yönetimi politikası oluşturulması konularında danışmanlık yapmaktadır. CERT-In gelecek için yol haritasını çizerken, sadece olaylara karşı müdahale mekanizmasının siber güvenliği sağlamada tam olarak yeterli olmayacağını, aynı zamanda proaktif bir siber güvenlik politikası oluşturularak gerçek zamanlı bilgi paylaşımına dayalı bir sistemin oluşturulması gerekliliğini saptamıştır. Böylece siber güvenlikle ilgili olay gerçekleşmeden belirli risk parametrelerine ulaşılacak ve gerçek zamanlı bilgi paylaşımına dayalı olarak olay engellenebilecektir.

Hindistan Hükümeti Basın Bilgi Bürosu, yaptığı yazılı bir açıklamada, Hindistan Siber Güvenlik Politikası kapsamında, hassas düzeyde ve devletin güvenliğini ilgilendiren gizli bilgilerin, internete bağlı olan bilgisayarlarda kesinlikle tutulmadığını açıklamıştır.

Özellikle Hindistan Dışişleri Bakanlığı'nın, yurtdışındaki misyonlarıyla yaptığı iletişim ve yazışmalar için özel güvenlik standartları geliştirilmiş, bu çerçevede görev yapan bütün personel özel bilgi güvenliği eğitimlerinden geçirilmiş ve bu eğitimler düzenli olarak belirli zaman aralıklarıyla devam ettirilmektedir. National Informatics Center (NIC) isimli Hindistan Devletine bağlı kuruluş, Hindistan çapında ağ omurgasını sunmakta ve denetlemekte, ayrıca

Hindistan Federal Devleti ve bünyesindeki federe devletlere, daha küçük idari birimlere ve belediyelere e-devlet hizmetleri sunulması konusunda destek vermektedir. Bu yüzden NIC altyapısının güvenliği Hindistan Devleti için kritik önemdedir.

Bütün bu sayılanların dışında, Ulusal Güvenlik Veri Tabanı (National Security Database-NSD) isimli bir oluşum kurulmuş ve bünyesinde siber güvenlik ile ilgili ve ulusal kritik altyapıların ve bilişim sistemlerinin korunmasıyla ilgili çalışan güvenilir ve donanımlı uzmanların listesi oluşturulmuştur. Bu veri tabanı sayesinde ülkedeki kritik sektörlerde görev yapmak isteyen kişilerin de belli testlerden ve güvenlik soruşturmalarından geçmeleri sağlanmakta ve böylece özel sektörde de bilgi güvenliği açısından insan kaynaklı hataların en aza indirilmesi hedeflenmektedir. Daha yüksek pozisyonlarda ve önemli noktalarda çalışmak isteyen uzmanların, Ulusal Güvenlik Veri tabanı bünyesindeki konumu ve eylemlerine bakılmakta ve ona göre karar verilmektedir. [40]

3.3.2 Amerika Birleşik Devletleri

Amerika siber uzayın oluşturduğu yeni gerçeklere kurumsal tepki veren önder ülkelerden biri olarak görülmektedir. Devlet olarak siber uzayın kurulmasına destek çıkarak ve kullanımını teşvik ederek diğer ülkelere örnek olmuştur. Özellikle Avrupa ve Asya'daki ülkelere siber sorunlar ile başa çıkılması konusunda örnek teşkil ederek bir rol model haline gelmiştir. Her ne kadar Amerika siber tehlike ve tehditlere karşı muhafaza sistem ve altyapısına sahip en güçlü ülkelerden biri olarak görülse de şu anda uygulanmakta olan programlar, sistem ve altyapıların günümüzdeki tehlikelere karşı halen yeterli olmadığı bilinmektedir. Aslında, en son yayınlanan siber güvenlik politika raporunda "Amerika'nın büyümekte olan tehditlere karşı kendini koruyabileceği şüphe götürmektedir." İbaresi yer almaktadır.

Hatta raporda daha da ileri gidilerek federal hükümetin giderek büyüyen bu probleme karşı şu anda ve hatta gelecekte de verimli bir şekilde hareket edebilecek bir organizasyona sahip olmadığı ve siber güvenlik ile ilgili sorumlulukların geniş bir federal departman ve kurumlar yelpazesine dağıtıldığı ve bu kuruluşların kendi aralarında birbiriyle ortak düşen

sorumluluklarının olduğu ve hiçbirisinin direkt olarak karar verme ve aksiyona geçme yetkisine sahip olmadığının gözlemlendiği açıkça belirtilmiştir.

2001 yılındaki olaylardan sonra Amerika, internet güvenlik politikasının tekrar gözden geçirilmesi konusunda kapsamlı bir çalışma başlattı. Bir takım Amerikan başkanı direktifleri aracılığı ile gelişmekte olan DHS (Department of Homeland Security) birimi siber internet güvenliğinin sağlanması için tüm sorumluluğu üzerine almıştır. Bu karar 2003 yılında sunulan "Ulusal Siber Uzay Güvenliğini Sağlama Stratejisi" dokümanında da resmiyete dökülmüş ve siber savunmanın sağlanması açısından iki taraflı bir yaklaşımın ortaya çıkmasına sebep olmuştur. CERT/CC işbirliği ile DHS organizasyonu içerisinde bulunan Ulusal Siber Güvenlik Birimi altında ulusal bir CERT organizasyonu (US-CERT) kurulmuştur. Bu kuruluşun amacı federal sivil ağları (.gov uzantılı) korumak olarak belirlenmiştir. Bir takım federal kurumların çalışmalarını koordine etmek amacıyla DHS'den bir acil çıkış planı ve uyarı sistemi geliştirmesi istenmiş ve ulusal çapta bir siber atağın ortaya çıkması durumunda 19 federal kuruluşun çalışmalarını koordine etme ve yönetme yetkisi verilmiştir.
Yayınlanan bu dokümanda özel sektörün gelişen bir siber tehdide karşılık vermek açısından daha iyi ekipman ve yapıya sahip olduğu vurgulanmış ve ulusal güvenlik birliğinin oluşturulması için ayrıca bir yaklaşımın ortaya çıkarılması konusunun üzeri çizilerek belirtilmiştir.

Sonuç olarak, her ne kadar DHS daha önce göz ardı edilmiş bir savunma alanı hakkında sorumluluğu üzerine almış olsa da inter savunma stratejisi konusunun ayrı bir alan olarak belirlenmesi hususunda herhangi bir çalışma ortaya çıkmamıştır. 2008 yılında Amerika siber politikası tekrar yenilenerek ve "Kapsamlı Ulusal Siber Güvenlik Girişimi" (Comprehensive National Cybersecurity Initiative, CNCI) başlıklı bir direktif hazırlanarak Başkan Bush tarafından imzalandı. Bu doküman bir takım büyük çaplı politika değişikliklerini içermekteydi. İlk olarak, Yönetim ve Bütçe Ofisi (Office of Management and Budget) DHS'den federal kuruluşlar ve dış sağlayıcılar arasında bulunan ağ bağlantılarının 4 ay içerisinde 4000'den 50'ye düşürülmesini istedi.

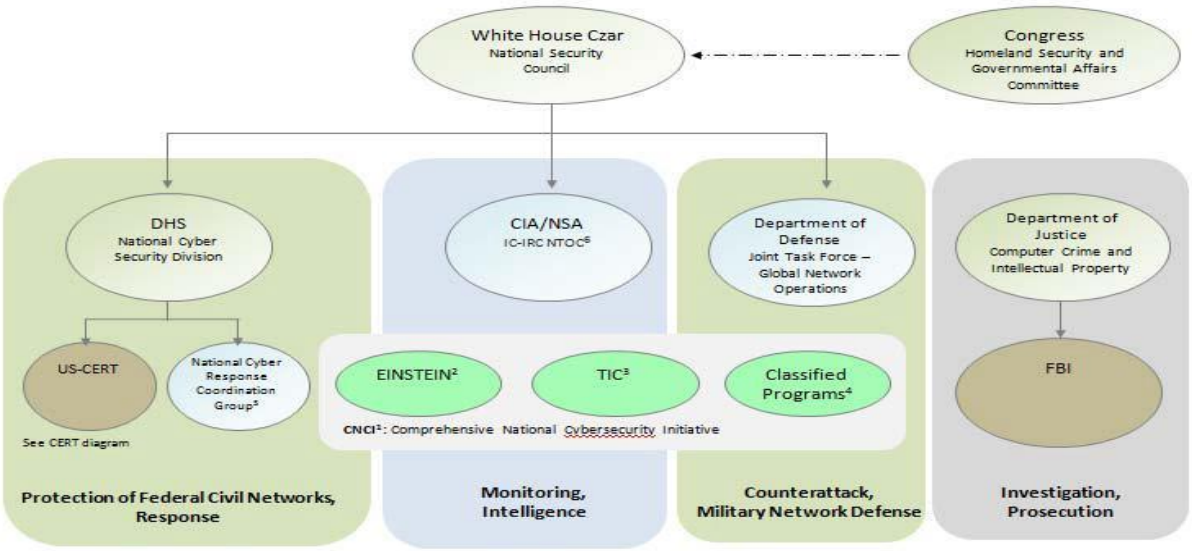
İkinci aksiyon ise, opsiyonel bir DHS programı olan ve federal web sitelerinden web sitelerine olan internet trafiğini gözlemleyen EINSTEIN adlı programın yetkisinin Ulusal Güvenlik Birimi'ne (National Security Agency) aktarılmasıydı. Bu programın yeni versiyonunda ise trafiğin yanı sıra içeriklerin de yakalanması ve takip edilmesi ve proaktif olarak federal ağların yanı sıra muhtemelen özel ağların da gözlemlenmesi gibi özellikler yer almaktaydı.

Son olarak, bu doküman konu hakkında AR-GE yatırım ve çalışmalarının artırılması, siber karşı istihbarat çalışmalarının koordine edilmesi ve hükümet kuruluşları arasında bilgi paylaşımının teşvik edilmesi gibi provizyonları da içermekteydi.

Obama'nın başkanlığında da, var olan CNCI planı desteklenmiş ve çalışmalar hakkında daha fazla şeffaflık olması gerektiği belirtilmiştir. Buna ilaveten, Beyaz Saray yeni bir çalışma ile siber politikasını tamamen revize etmiştir. Oluşturulan son raporda Beyaz Saray içerisinde bir Siber Güvenlik Ofisi'nin kurulması tavsiye edilmiştir. Oluşturulacak bu yapıda bir Siber Çar'ın lider olarak görev alması ve Ulusal Güvenlik Konseyi'nin bir üyesi olması ve Başkan'a kolay ve hızlı erişim ayrıcalığına sahip olması gerektiği belirtilmiştir.

Her ne kadar bu ofisin tek başına politika belirleme yetkisi olmasa da, kurumdan federal departmanların çalışmalarını koordine etmesi ve ortak politika belirleme tavsiyelerinde bulunarak federal hükümet içerisindeki tüm siber güvenlik ile ilgili aktiviteler hakkında yetki, rol ve sorumlulukların netleştirilmesinde yardımcı olarak oluşan iletişim ve politika açığı için bir köprü görevi görmesi istenmiştir.

Geçmişte yaşanan siber vakalarda ortak bir federal tepkinin olmadığı fark edilerek, kuruluşlar arasında var olan ortak sorumluluk alanlarının ortadan kaldırılması ve hükümet ağı içerisinde siber savunma ile ilgili spesifik rol ve sorumlulukların belirlenmesi tavsiye edilmiştir.



Şekil-23: ABD Ulusal Siber Güvenlik Birimi

Yukarıda tavsiye edilen organizasyon şeması yer almaktadır. Bu şemaya bakıldığında Beyaz Saray'da görevlendirilen ve Ulusal Güvenlik Konseyi üyesi olan ve kongreye bağlı olarak çalışan bir Çar başkanlığında 4 ana iş kavramı altında federal kuruluşların birbirleriyle olan bağlantıları resmedilmeye çalışılmıştır. Federal Sivil Ağların Korunması ve Tepki Konması süreci içinde DHS içerisinde yer alan Ulusal Siber Güvenlik Biriminin (National Cyber Security Division) liderliğinde US-CERT ve Ulusal Siber Tepki Koordinasyon Grubu (National Cyber Response Coordination Group) gibi kuruluşların çalışması öngörülmüştür. Ulusal Siber Tepki Koordinasyon Grubu ulusal çapta etki yaratabilecek bir siber saldırı durumunda 19'dan fazla federal kuruluş arasında koordinasyonun sağlanması ile görevlidir. US-CERT (United States Computer Emergency Readiness Team) ise daha önce var olan CERT/CC (Computer Emergency Readiness Team Coordination Center) yerine görevlendirilmiştir.

İzleme ve İstihbarat sürecinde ise Merkezi İstihbarat Ajansı (Cetral Intelligence Agency, CIA)

ve Ulusal Güvenlik Ajansı (National Security Agency, NSA) işbirliği altında İstihbarat Toplumu Vaka Tepki Merkezi (Intelligence Community-Incident Response Center, IC-IRC) ve Ulusal Güvenlik Kuruluşu Tehdit Operasyonları Merkezi(NSA/CSS Threat Operations Center, NTOC) gibi kuruluşlar görev almaktadır.

Karşı atak ve Ordu Ağı Savunması sürecinde ise Savunma Departmanı'na bağlı (Department of Defense) Birleşik İş Gücü – Global Ağ Operasyonları (Joint Task Force – Global Network Operasyonları) başkanlığında çalışmalar yürütülmektedir. [41]

3.3.3 Çin

Çin Askeri Stratejisi'nde siber güvenlik, Çin Halk Kurtuluş Ordusu'nun (Peoples Liberation Army – PLA) üzerine çok büyük yatırımlar ve çalışmalar yapması gereken çok önemli bir alan olarak tanımlanmıştır.

Çinli askeri stratejistlere göre siber güçler, savaş konseptinde güçlü asimetrik fırsatları da beraberinde getirmektedir.Çin Halk Cumhuriyeti, siyasi organizasyonu ve ideolojisi sebebiyle ülkenin güvenliği yanında siber güvenliği de büyük oranda ordunun denetimine bırakmış durumdadır. PLA'nın GSD (General Staff Department) 3. ve 4. Departmanları, ülkenin bilişim altyapısının korunmasından sorumludurlar. Bu birimler hava, kara, deniz kuvvetleri ve milis kuvvetlerin ilgili siber güvenlik birimleriyle birlikte Çin sınırları içerisindeki tüm iletişim trafiğini izlemektedirler. PLA GSD 3. Departmanı ayrıca, Çin ordusunun sahip olduğu bilişim altyapısının ve ağların da güvenliğinden sorumludur. 3. Departman altında 12 adet operasyonel büro vardır. Bunun yanında 3 adet araştırma enstitüsü de ülkenin siber güvenliğinin geliştirilmesi amacıyla aralıksız AR&GE faaliyetleri yürütmekte ve Çin'in önde gelen üniversitelerinin de desteği alınmaktadır. Resmi olmayan bir rapora göre, PLA GSD'ye bağlı 3. Departman bünyesinde 130.000 civarında personel görev almaktadır.

PLA bünyesinde dünyadaki en hızlı süper bilgisayar sistemlerinden bazıları bulunmaktadır. Jiangnan Bilgisayar Teknolojileri Araştırma Enstitüsü (Jiangnan Computer Technology Research Institute) adıyla da bilinen 56. Araştırma Enstitüsü Çin'deki en eski ve büyük

araştırma ve geliştirme organizasyonudur. Çok önemli süper bilgisayar yatırımları yapmakta ve bu süper bilgisayarlarla Çin'deki diğer bilgisayar merkezlerine ve PLA bünyesindeki organizasyonlara destek vermektedir. Burada yer alan süper bilgisayarlar sayesinde, diğer ülkelerin kullandıkları karmaşık kodları ve şifreleri kırma çalışmaları hızlanmıştır.

Her ne kadar Çin, bazı batılı ülkeler için ticari espiyonaj ve siber saldırılar konusunda tehdit olarak kabul edilse ve siber suçlular için devlet desteği sağlayan bir ülke olarak adlandırılsa da, siber güvenliğini iyileştirmek ve bunun için gerekli tedbirleri almak amacıyla birçok adım atmıştır. Kaspersky'nin 2010 birinci çeyrek raporunda, 2009'un dördüncü çeyreğinden bu yana. cn uzantılı üst seviye domainlerden kaynaklı kötü niyetli yazılım yüzdesinin %32,8'den %12,84'e düştüğü saptanmıştır. Bunun temel sebeplerinden birisi ise Çin'in. cn domainler üzerindeki yeni kısıtlamalarıdır. Bu kısıtlamaya göre, .cn uzantılı bir adresi satın almak için hükümet veri tabanında kayıtlı bir işletme ve başvuru sırasında işletme lisansı ve devlet kimlik numarası gösterilmesi gerekmektedir. Çinli operatörlerin genellikle büyük çaptaki siber saldırılara sebep olduğu iddia edilmektedir. Çin Devleti'nin bu iddiaya yanıtı ise, aslında Çin Devleti'nin de sürekli saldırı altında olması ve bu saldırıların genellikle başka ülkelerdeki girişimciler tarafından yapılıyor olmasıdır.

Çin Komünist Partisi'nin resmi gazetesine göre, Çin hükümeti hackleme suçlarının mahkemeler tarafından nasıl değerlendirildiği konusunda sıkı yaptırımlar getirmek için çalışmaktadır. Çin ayrıca online bilgi güvenliği ve siber suçların azaltılması gibi konulardaki hukuki yaptırımlarda değişiklikler yapılmasını önermiştir. 2010 yılında Çin, kullanıcıları siber veri hırsızlığı hakkında korumak amaçlı regülasyonlar getirmiş ve Çinli telekom şebekesi operatörü şirketlerin botnet'lere karşı savaşması ve domain alanları kaydı sırasında sahte isim veya kimlik kullanılmasını önlemek amaçlı ek regülasyonlar yürürlüğe koymuştur.

Çin, bunun yanında siber suçlara karşı farkındalığın oluşturulması ve gerekli hukuki takiplerin yapılması için çalışmalarda bulunmuştur. Öte yandan, Çinli güvenlik araştırmacılarının Çin'deki güvenlik şirketlerinde çalışmaya başlamaları Çinli hacker'ların devlet sponsorluğunda çalıştığı iddialarını ortaya çıkarmıştır fakat işin gerçek boyutu Çinli araştırmacıların hükümet için çalışarak kariyerlerini yasallaştırmak istemeleridir. Çin'deki

güvenlik endüstrisi halen başlangıç safhalarında olmakla beraber, birçok hacker kendilerine yasal yollardan iş bulamadıklarından dolayı bu tarz suçlar işleyerek para kazanmaya çalışmaktadır. Getirilen yeni kanunlar bu yeni jenerasyon hacker'ları hedef almış ve 2009 yılında uygulanan yeni bir kanun ile hackleme araçlarının dağıtım ve paylaşımı suç olarak kabul edilmiştir.

Çin, bilgi ve siber savaş alanlarında lider konuma gelme hedefini açık olarak beyan etmiş ve bu konular hakkında 20 yıldan bu yana teoriler, doktrinler ve politikalar yayınlamaktadır. 1990'ların ortasından bu yana Çin ordusu "bilgileştirme" konsepti altında modernleşme programı uygulayarak bilgi teknolojileri ve siber uzay alanlarında etkin güç haline gelmeyi planlamaktadır.

Çin hükümeti ayrıca "Altın Kalkan" adlı, politik anlamda hassas verilerin ülke dışına çıkması veya içeri girmesini önleyen meşhur bir filtreleme sistemi uygulamaktadır. Batıda bu filtre "Büyük Çin Firewall" u olarak adlandırılmaktadır. Bu Altın Kalkan gelecekte bir siber savaş çıkması durumunda Çin'e avantaj sağlayabilecek düzeyde gelişmiş yeteneklere sahiptir. [42]

3.3.4 Estonya

2007'de Estonya'ya yönelik gerçekleştirilen siber saldırılar, ülkenin siber yeteneklerini ve politikalarını ciddi şekilde sorgulamasına neden olmuştur. Olaylar neticesinde Estonya'da siber savunma faaliyetleri Savunma Bakanlığı gözetiminde gerçekleştirilmektedir. Bunun yanı sıra, ülkede Defence League (Savunma Ligi) adı verilen bir organizasyon da, ülkenin siber savunma yeteneklerini geliştirmek için çalışmalarda bulunmaktadır. Defence League'e bağlı olarak çalışan Cyber Security Alliance, 3 ana başlıkta görevlerini icra etmekle sorumludur. Bu görevler;

- Estonyalıların elektronik yaşamlarını koruma altına alma,
- IT uzmanları yetiştirme,
- Siber Savunma hakkında halkı bilgilendirme faaliyetlerinde bulunma olarak sıralanabilir.

Belirlenen siber güvenlik politikalarının uygulanabilmesi için oluşturulan Kamu kurumları ve STK'lar, kurumlar arası ilişkiler, özel sektör ve Kamu kurumları arasındaki ilişkiler Ülkenin Siber Savunma stratejileri, 2007 olayından sonra Cyber Security Strategy Committee (Siber Güvenlik Strateji Komitesi) adı verilen bir oluşum tarafından hazırlanmıştır. Komite başkanlığı ve yürütücülüğü Savunma Bakanlığı tarafından yapılmakla birlikte, Dışişleri Bakanlığı, İçişleri Bakanlığı, Eğitim ve Araştırma Bakanlığı, Adalet Bakanlığı ve Ekonomi Bakanlığı da komisyon üyeleri arasında yer almaktadır. Bu komitenin faaliyetleri neticesinde alınan kararlar, bu komiteye bağlı olarak oluşturulan Siber Güvenlik Konseyi tarafından uygulanmaktadır. Siber Dünya'da Estonya'nın zaaflarını gidermeye yönelik faaliyetlerin temel amacı, ülkenin siber saldırılara karşı savunma yapabilmesini sağlamak ve kritik altyapılara yönelik atakların en kısa sürede çözüme kavuşturularak etkisini minimize etmek olarak belirtilebilir. Bu hedeflerden yola çıkarak ülkenin; güvenlik ölçütlerinde çok katmanlı yapıya geçmesi, bilişim güvenliğinde uzmanlığını geliştirmesi, siber güvenliği geliştirecek yönetsel reformlara imza atması ve uluslararası işbirliğini artırmaya çalışması ilkelerini benimsediği söylenebilir. Estonya, üyesi olduğu NATO çatısı altında Bilişim Güvenliği alanında uluslararası işbirliğinin önemini gören ve bu alanda aktif rol alan ülkelerden biridir. Bu işbirliği, kendi savunma yetkinliğinin artmasının yanı sıra NATO üyesi diğer ülkelere de önemli katkılarda bulunmasını sağlamaktadır. Bir NATO kuruluşu olarak 2008 yılında Tallinn kentinde faaliyete geçen Cyber Defence Centre of Excellence (Siber Savunma Mükemmeliyet Merkezi), üye ülkeler arasında işbirliğini artırma, bilgi paylaşımı sağlama ve siber güvenlik alanında araştırmalar yapma hedefine yönelik faaliyetlerde bulunmaktadır.
Merkezin destekçileri olan ülkeler; Estonya, Almanya, Macaristan, İtalya, Letonya, Litvanya, Slovakya ve İspanya olarak sıralanabilir.

İlgili kurumların görevlendirmelerine dayanak olan hukuki mevzuatlar, kurumların görev ve yetki sınırlarının çerçevesi Estonya'nın siber güvenlik konusunda oluşturmaya çalıştığı hukuki altyapı ve mevzuatlar, temel olarak 3 hedefi gözetmektedir. Bunlar;

- Estonya'nın kabul ettiği Siber Güvenlik Stratejisi'ne uyum sağlayan ve bu stratejik hedefler için ihtiyaç duyulan kanuni değişikliklerin yapılması
- Kritik bilgi altyapılarının korunmasına yönelik mevzuatların hazırlanması ve yürürlüğe konması,

- Estonya'da geliştirilen ve düzenlenen mevzuatların, uluslararası platformda ve özellikle AB üye ülkelerinde tanıtılması, benzer mevzuatların bu ülkelerde yapılmasının sağlanmasıdır.

Çalışmaların en başında ülkenin genel durumu incelenmiş, Siber Güvenlik Stratejisine uyumlu olan ve olmayan, ihtiyaç duyulan ve çalışmaları engelleyen kanun ve yönetmelikler tespit edilmiştir. Bu çalışmaların sonunda görülmüştür ki, Estonya'da hali hazırda yürürlükte olan yönetmelikler, merkezileştirilmeyen ve hatta birbiriyle çakışan hükümler içermektedir. Örnek vermek gerekirse, yürürlükte olan ve elektronik servislerin daha liberal ve serbestçe kullanılmasını yaygınlaştırmaya yönelik mevzuatlar bulunmasına rağmen yürürlükte olan bir diğer mevzuat kişisel veri koruması hükümlerinin oldukça kapalı ve sıkı şekilde denetlenmesini salık vermektedir. [43]

3.3.5 Fransa

Fransa'da siber güvenlik ile ilgili temel kurum 2009 yılında kurulan Ulusal Bilgi Sistemleri Güvenlik Ajansı'dır. Bu kurumun görev alanları arasında siber saldırıları tespit ve karşı cevap, araştırma ve geliştirme faaliyetleri vasıtasıyla siber saldırıların önlenmesi ve hükümete ve kritik önemi haiz kurumlara bilgi sağlamak bulunmaktadır.
Bu kurum doğrudan Başbakana bağlı olarak Milli Güvenlik Genel Sekreterliği gözetimi altında faaliyetlerini yürütmektedir. Siber güvenliğin yanı sıra Fransa, ayrıca uzmanlaşmış kurumlar bünyesinde siber saldırı kabiliyetlerini de geliştirmektedir.

Hem kara kuvvetleri hem de hava kuvvetleri bünyesinde elektronik saldırı üniteleri bulunmaktadır. Ayrıca Fransız istihbarat teşkilatı da siber saldırı unsurlarını yakından takip etmektedir.

Şubat 2011'de, Ulusal Bilgi Sistemleri Güvenlik Ajansı bilgi sistemlerinin savunması ve güvenliğiyle ilgili ulusal strateji planını yayınlamıştır. Mezkûr strateji temel olarak 4 ana prensibi içermektedir:

1. Siber güvenlik alanında uluslararası bir güç konumuna erişmek,
2. Bilgi egemenliğini temin etmek suretiyle Fransa'nın karar alma inisiyatifini korumak, (Burada özellikle kritik kararlar almak durumunda olan hükümet yetkililerinin birbiriyle iletişimlerinin gizliliğinin temin edilmesi amaçlanmaktadır.)
3. Kritik önemi haiz ulusal altyapıların siber güvenliğinin temin edilmesi
4. Siber ortamda gizliliğin ve güvenliğin sağlanmasıdır.

Fransa yukarıda belirtilen amaçlara ulaşmak için aşağıdaki uygulamaların hayata geçirilmesi gerekliliğini kararlaştırmıştır. Bu uygulamalar;

1- Sağlıklı kararlar almak için güvenliği temin edilecek ortamın iyi araştırılması,
2- Saldırıları tespit edip onlara karşılık verilmesi, zarar görmesi muhtemel kişilerin uyarılması ve onlara yardım edilmesi,
3- Siber özerkliğin sağlanması için Fransa'nın; ilmi, teknik, endüstriyel ve beşeri becerilerinin arttırılıp devam ettirilmesi,
4- Devletin ve kritik altyapı hizmetini sunan hizmet sunucularının bilgi sistemlerinin güvenliğinin temin edilmesi,
5- Kuralların teknolojideki yeniliklere uyum sağlayabilecek nitelikte düzenlenmesi,
6- Bilgi sistemlerinin güvenliği, siber suçlarla mücadele ve siber güvenlik hususlarında Fransa'nın uluslararası işbirliklerinin geliştirilmesi, (Bu amaçla Almanya ve Amerika Birleşik Devletleri ile özel olarak anlaşma imzalanmış, ayrıca AB ve NATO bünyesinde de uluslararası işbirliği yapılmıştır.)
7- Fransa'da yaşayan bireylerin bilgi sistemi güvenliğiyle ilgili hususları daha iyi kavrayabilmesi adına bunların düzenli olarak bilgilendirilip, konuyla ilgili ikna olmalarının sağlanmasıdır.

Fransa'da konuyla ilgili hukuki düzenlemeler temel olarak şunlardır:

- E-Devlet Kanunu,
- 8 Kasım 2005 tarihli Kamu Kurumları ile Bireyler ve Kamu Kurumları arasındaki Elektronik Etkileşime dair Yönetmelik,

- 6 Ocak 1978 tarihli Bilgi Teknolojileri ve Özgürlükler Kanunu -belirtmek gerekir ki bu kanuna göre veri güvenliğinin temini amacıyla Ulusal Enformatik ve Özgürlükler Komisyonu kurulmuştur-
- E-ticaret mevzuatı,
- E-iletişim mevzuatı,
- Siber suçlara karşı mücadeleyi amaçlayan 5 Ocak 1988 tarihli Godfrain Kanunu -bu kanun alanında bir ilk olma özelliği taşımaktadır-
- E-kimlik mevzuatıdır [44]

3.3.6 İsrail

Siber tehdit ve siber saldırı konusunda en iyi güvenlik ve savunma stratejisine sahip ülkelerden biri de İsrail'dir. İsrail'in gelişmiş siber saldırı yetenekleri vardır ve ofansif bir strateji benimsemişlerdir. Ordu içinde "Birim 8200" adı verilen Subay, MOSSAD ajanları ve emekli askerlerden oluşan bölüm MOSSAD'ın içindeki özel birimle birlikte İsrail'in siber saldırı gücünü oluşturmaktadır.

İsrail, siber savunma ve istihbarat faaliyetini yaparken "C4ISR adlı" bir sistemler bütünü de kullanmaktadır. Tam Açılımı Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance: Komuta, Kontrol, Muhabere, Bilgisayar, İstihbarat, Gözetleme, Keşif; yani sağlıklı bir muharebe yürütülmesi için gerekli olan fonksiyonlar ve sistemlerin tümü denebilir. Bir keşif İHA'sı da C4ISR sistemidir, istihbarat uydusu da, askeri haberleşme sistemi gibi sistemler içerir.

İsrail'in siber güvenlik stratejisi içerisinde ülke içindeki bilgisayarların güvenliğini sağlamak ise iç istihbarat kurumu Şin Bet'in görevidir. Başbakan Netanyahu'nun da siber tehdidi "Füzelerle yapılacak bir savaş kadar tehlikeli" olarak yorumladığı ve bu düşünceyle ordu içinde özel bir birim kurduğu ifade edilmektedir.

“Birim 8200” aynı zamanda yetişmiş donanımlı personel temini konusunda akademik bir rol üstlenmekte ve eğittiği personeli istihbarat ve siber güvenlik konusunda çeşitli birimlerde görevlendirmektedir.

İsrail’in siber savunma ve siber güvenlik politikasına göre; ordu ve sivil otoriteler gerekli teknik alt yapısı ve tam donanımlı eğitimli personeliyle, internet üzerinden gelebilecek siber tehditlere karşı her an hazır durumdadırlar. Negev çölündeki üs bölgesinde ileri teknoloji ekipmanlar ve antenler tüm dünyadaki internet ve data trafiğini sürekli takip etmektedirler.

İsrail gerek jeopolitik konumu gerekse de ulusal güvenlik politikaları gereği, siber savaş ve siber tehditler ile mücadeleyi istihbarat faaliyetleri ve askeri hareket kabiliyetiyle birleştirmiştir. İsrail’in kritik hükümet sistemleri herhangi bir siber tehditten etkilenmemesi için intranet gibi, internetten bağımsız olarak çalışabilen ve genellikle hassas ve gizli bilgileri taşıyan ağlar üzerinde çalışır. Günümüzde birçok ülke hala gizli ve kritik ulusal sistemlerini internet tabanlı sistemlerde tutmaktadır ve sırf bu yüzden internet üzerinden gelebilecek her türlü siber saldırı tehditlerine her an açık durumdadırlar. İsrail kritik sistemlerini intranet sistemleri üzerinde tutarak nispeten dışarıdan gelen tehditlere karşı kendini kapamış durumdadır. İnternet güvenlik şirketi McAfee’nin desteklediği bir araştırma sonucuna göre İsrail, Finlandiya ve İsveç sanal saldırılara karşı en hazırlıklı ülkelerdir. [45]

3.3.7 NATO – Kuzey Atlantik Antlaşması Örgütü

3.3.7.1 NATO’nun Siber Savunma Politikası

21. Yüzyılda güvenlik anlayışı, geleneksel tanımların oldukça dışına çıkmış durumdadır. Günümüzün modern toplumları ve ekonomileri tamamen elektronik ağlar ve kablolarla birbirine bağlanmış, iletişimlerini bilgisayar ve akıllı elektronik cihazlar üzerinden sağlar duruma gelmiştir. Kullanımı gittikçe yaygınlaşan bilişim sistemleri, kritik altyapıların ve toplumların fiziksel güvenliğini dahi etkileyecek seviyeye gelmiştir. İşte bu durum, siber güvenliğin tehdit düzeyinin ne denli önemi haiz olduğuna dair fikir vermektedir. NATO’nun 2010 Stratejik Konsept’inde Siber Güvenlik konusu “ … siber saldırılara karşı yeteneğimizi

geliştirerek saldırıları tespit etme, koruma ve engelleme alanlarında çalışmalar yapma..” pasajıyla vurgulanmıştır. İşte bu arka plan hazırlıkları 2010 Lizbon Zirvesinde aksiyon planına dönüşmüş, NATO’nun ihtiyacı olan Siber Savunma Politikası dokümanı hazırlanmasına karar verilmiştir. Konsept dokümanı alınan bu kararla 2011 Mart’ında hazır edilmiş, sonrasında 8 Haziran 2011’de NATO Savunma Bakanlarının onayıyla uygun görülerek yürürlüğe girmiştir.

Hedefler

- NATO’nun temel görevlerini yerine getirmesi esnasında siber güvenlik unsurlarını dikkate alması ve NATO yapıları ile iş süreçlerinde bu unsuların tam entegrasyonunun sağlanması,
- NATO ve üye ülkelerin siber saldırılara karşı etkin savunma yapabilmesi,
-NATO’nun kendi ağlarının merkezi kontrolü ve savunmasıyla birlikte siber savunma yetkinliklerinin geliştirilmesi,
- NATO’nun bütün temel işlevlerini kapsayacak siber savunma ihtiyaçlarının tespiti ve hayata geçirilmesi,
- Uluslararası organizasyonlar, sivil toplum kuruluşları, üye ülkeler, akademik çevreler ve özel sektör ile ortak çalışma ve fikir alışverişi yürüterek siber savunma yetkinliklerini geliştirmesi,

NATO’nun Siber Savunma Politikası kapsamında değerlendirilen hususlar olarak öne çıkmaktadır.

3.3.7.2 Ana hatlarıyla NATO Siber Savunma Politikası

Temel Noktalar

NATO, üye ülkelerle iş birliği içinde yürüttüğü temel ve kritik işlemlerin kesintisiz gerçekleştirilmesine büyük önem vermektedir. Bu önem, Siber Savunma Politikası’nın da omurgasını oluşturmakta ve temel hedef olarak “NATO’nun kendi iletişim ve bilgi sistemlerinin her türlü siber saldırıya karşı korunması” ilkesi benimsenmektedir. Bu temel hedef doğrultusunda varılmak istenen gayeye ulaşabilmek için her geçen gün çeşitlenen siber

saldırılara karşı bilgi birikimini geliştirmek ve kendi sistemlerini bu bilgi birikimiyle destelemek, NATO'nun üzerinde önemle durduğu noktalar arasında yer almaktadır. Hedefler NATO, siber saldırı anında etkili cevap verme mekanizmalarını geliştirme hedefinin yanı sıra planlama ve yetkinlik boyutlarında da ciddi çalışma içindedir. Bunu sağlayabilmek için bütün üye ülkelerle birlikte organize hareket etmesi NATO'nun olmazsa olmaları arasındadır denilebilir. İşte bu noktada, NATO Defense Planning Process (NDPP) yapısı devreye girerek ulusal savuma mekanizmalarının NATO ile haberleşmesini sağlar. Bu yapı ile NATO üye ülkelerin ağlarıyla tam entegre biçimde büyük bir haberleşme altyapısı kullanır ve koordinasyon başarıyı getirir.

3.3.8 ITU (Uluslararası Telekomünikasyon Birliği)

Gelişim Tarihçesi:

2003-2005: WSIS (World Summit of the Information Society) ICT kullanımlarına güven duyulması konusunda aksiyonların tek sorumlusunu ITU olarak görevlendirdi.

2007: ITU Genel Sekreterliği, siber güvenlik konusunda uluslararası bir kapsam yaratmayı hedefleyen GCA (Global Cybersecurtiy Agenda) dokümanlarını yayınladı.

2008 – 2010: ITU üyeleri GCA dokümanını uluslararası birlikteliği sağlayacak içerik olarak kabul ettiler ve onayladılar. Siber güvenlik tehditlerine karşı verilecek mücadelede uluslararası bir platform yaratma ihtiyacı doğmuş ve global standartların oluşturulması için ITU görevlendirilmiştir.

ITU 3 ana sektörden oluşur: Radyo İletişim Sektörü (ITU-R), Standartlar Sektörü (ITU-T), Telekomünikasyon Geliştirme Sektörü (ITU-D).

ITU Standart Çalışmaları: IT standart belirleme çalışmaları özel sektörü ve devlet kurumlarını bir araya getirmesi ve güvenlik politikaları ile güvenlik standartlarının uyumluluğunu sağlaması anlamında tekil bir göreve sahiptir. Standartların netleştirilmesi güvenlik

konusundaki kırılımların doğru adreslenmesi adına çok önemli protokollerdir. Özellikle IP tabanlı sistemler, NGN sistemlerinde seriş kalitesi, şebeke yönetimi, mobilite, faturalandırma süreçleri hakkında uluslararası platformlar tasarlanması hedeflenir. Bu hedef doğrultusunda ITU tarafından belli başlıklarda farklı tavsiye kararları yayınlanmıştır. Bu kararların içerikleri aşağıdaki gibidir;

H.235.x Tavsiye Kararları: IP tabanlı multimedya uygulamalarına ait altyapıları düzenleyen ve gizlilik hizmetleri sağlayan kararlardır. Multimedya uygulamaları üzerinden iletişim kuran kullanıcıların onay ve yetki süreçlerinde verilerinin siber tehditlere karşı korunması sağlanmaktadır.Gerçek zamanlı şifreleme metotları ile güvenlik katmanları oluşturulmaktadır.

J.170 Tavsiye Kararları: IP Cablecom mimarisi için güvenlik düzenlemelerini içerir ve televizyon operatörlerine güvenli IP hizmetleri sağlama konusunda yönlendirir.

X.805 Tavsiye Kararları: Bu kararlar tüm iletişim şebekeleri için baştan sona güvenlik sağlamayı hedeflemektedir. Bu adımda şebeke saldırılarına karşı tedbirleri, hırsızlık ve fraud, gizli dinlemeler, yetkilendirme için telebiometri, telekomünikasyon süreçlerinde güvenlik gibi pek çok farklı konuyu içermektedir.

X.509 Tavsiye Kararları: ITU tarafından geliştirilen en önemli standartlar olarak bilinen ve günümüzde kullanımı olan tüm şebekede elektronik yetkilendirme standartlarıdır. Tüm dijital sertifika sistemlerinin temeli olan Açık Anahtar Altyapısının (PKI) referansları bu standart sayesinde belirlenir. Web arayüzleri ve sunucular arasındaki entegrasyonlarda transfer edilen datanın güvenliğini sağlayan şifreleme anahtarlarının güvenilir yapısını sağlamaktadır. Ek olarak maillerin onaylanması ve güvenliğini sağlayan dijital sertifikayı destekler.

ITU-T X.1205 Tavsiye Kararları: En son onaylanan "Siber Güvenlik Genel Açıklamaları" olarak bilinen kararlardır. Siber güvenlik konularına ve siber tehditlerin sınıflandırmalarına ait tanımları içerir. Siber güvenlik ortamının normlarını ve risklerini tartışır, olası stratejileri belirler, güvenli iletişim tekniklerini inceler.

3.3.8.1 Itu'nun Siber Güvenlik Araçları

1- IMPACT Security Assurance Division

IMPACT, BİT uzmanları ile işbirliği yaparak, küresel "Best Practice" kılavuzları hazırlamaktadır. Aynı zamanda, talep edilmesi halinde, devlet kurumları veya kritik önem taşıyan altyapı şirketlerinin sistemleri üzerinde bağımsız güvenlik denetimleri gerçekleştirmektedir. Ek olarak, siber güvenlik için bağımsız, uluslararası olarak tanınan bir sertifikasyon kurumu olarak da görev yapmaktadır.

2- ITU National Cybersecurity/CIIP SelfAssessment Tool

ITU Ulusal Siber Güvenlik/ CIIP Öz Değerlendirme Aracı, ITU üye devletlerinin siber güvenlik ve CIIP (Critical Information Infrastructure Protection – Kritik Bilgi Altyapısı Koruması) konusundaki politikalarını belirlemeye yardımcı olmayı amaçlayan bir araçtır.

3- ITU Toolkit for Promoting a Culture of Cybersecurity

Bu araç, gelişmekte olan ülkelerde, siber güvenlik konusunda KOBİ'lerin, tüketicilerin ve son kullanıcıların bilinçlendirilmesi için atılabilecek adımları gösterecek bir kılavuz oluşturmaktadır.

4- ITU Botnet Mitigation Toolkit

Gelişmekte olan ülkelerin büyüyen botnet (zombi bilgisayar ordusu) sorunu ile başa çıkabilmelerini sağlayacak bir araçtır. Botnetlerin bulunması ve etkilerinin sonlandırılmasına hizmet eder.

3.3.9 Avrupa Birliği (Ab)

Siber Güvenlik konusunda AB'de temel adımlar

- 1 Eylül 2005: Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tam anlamıyla faaliyete başladı.

- Mayıs 2007: Çevirim içi terörizmi gözlemlemek için Avrupa Polis Ofisi (Europol) tarafından 'Webi (ağı) Kontrol Et" isimli güvenlik portalı kuruldu.
- Nisan 2010: AB bakanları, merkezi siber suç ajansına ihtiyacın araştırılması için Komisyon'a çağrıda bulundu.

Konular

2020 itibariyle internet güvenliği öncelikli konulardan birini teşkil ediyor. AB'nin internet güvenliği ajansı ENISA, bilgi ağlarını güvenlik altına almaya çalışmakta, fakat şu anki durumda ajans başa çıkmasını sağlayacak yasal dayanağı olmayan bir merkez konumundadır. Örneğin 2008'de ajans mobil iletişimin güvenlik tehditlerine karşı ne kadar savunmasız olduğu konusunda bir bildiri yayınlamıştır.

Siber suçlarla mücadelede Europol de aktif çalışmalar içindedir. Kurum, çocuk pornografisi gibi sınır ötesi siber suçların engellenmesinde yürütme organlarına yardım adına faaliyet gösteren çeşitli çalışma gruplarını denetlemektedir. Buna karşın, gittikçe artan bir kullanıcı sayısının sosyal paylaşım sitelerinde bilgilerini paylaşmaları, siber suçun çoğalmasına zemin hazırlamaktadır.

ENISA'nın izlediği internet güvenliği konuları şu şekilde: spam, botnet, e-dolandırıcılık, kimlik hırsızlığı, menkul kıymetler borsasında hackerlar, yazılım konusundaki hassasiyetler ve kimi cihazlardaki güvenlik eksikliğidir. Kasım 2010'da ENISA tarafından siber güvenlik alıştırması yapılmış ve 27 üye yanında İsviçre, Norveç ve İzlanda ülkelerinin katılımı sağlanmıştır Bu alıştırmadan çıkan en ciddi sonuç hukuksal olarak bir işbirliğine ihtiyaç olduğudur.

AB idaresinin bildirdiği üzere siber suçun AB'ye maliyeti yıllık 750 milyar Euro ile uyuşturucu trafiğinin maliyetini de aşarak küresel GSMH'nin % 1'i olarak kayda geçmiştir. Komisyon aynı zamanda Avrupa'da siber atağa karşı bir anında müdahale sistemi kurma çabasındadır. Buna ek olarak komisyonun hedefleri arasında bilgisayarlar için bir acil yanıt takımı (Certs) kurma planı ve ENISA'nın rolünü arttırmak da vardır. [46]

4. ÜLKEMİZDE SİBER GÜVENLİĞE YÖNELİK YASAL DÜZENLEMELER ve SİBER GÜVENLİK FAALİYETLERİ

Günümüzde teknolojinin gelişmesiyle orantılı olarak bilişim sistemleri kullanılarak işlenen suçlarda da artış yaşanmaktadır. Siber suç, suçun fail ya da failleri tarafından bilişim sistemi kullanılarak başka bir bilişim sisteminin güvenliğini, buna bağlı verileri ya da kullanıcısına yönelik işlenen suçtur.

Tanımda bahsedilen bilişim sistemleri, 5237 sayılı TCK'nın (Türk Ceza Kanunu) 243. maddesinin gerekçesine göre "…verileri toplayıp yerleştirdikten sonra bunları otomatik işlemlere tabi tutma olanağını veren manyetik sistemlerdir" şeklinde tanımlanmıştır [2]. Siber suçlar genel olarak, bilişim sistemi aracılığıyla başka bir bilişim sistemine yönelik olarak işlenebilir. Bunun dışında diğer iletişim araçlarıyla (telefon, faks… vb.) işlenen suçlar (örneğin; telefonla aldatarak veri hırsızlığı) niteliği itibariyle bilişim sistemi sayılamayacağından; siber suçlar kapsamında da yer almamaktadır.

Siber suçlar genel olarak; 5237 sayılı TCK'nın Onuncu Bölümü'nde 243 ile 246. maddeler arasında düzenlenmiştir. Ayrıca 5651 sayılı Kanun ve 5846 sayılı FSEK'in (Fikir ve Sanat Eserleri Kanunu) ilgili maddelerinde ve diğer kanunlarda çeşitli siber suçlar tanımlanmıştır.

Siber suçlar takibi şikâyete bağlı olan suçlardır. Yani suçun cezaî yaptırımının sağlanabilmesi için ilgili makamlara bu suç bildirilmelidir. Aksi takdirde bu suç hakkındaki adlî işlemler başlamayacaktır. Takibi şikâyete bağlı olan suçlar da şikâyet süresinde yapılmalıdır. Şikâyet süresi, siber suçun faili ve bu suçun fiilinin öğrenilmesinden itibaren altı aydır. Şikâyet süresinde yapılmadığı takdirde, işlenen siber suçun soruşturulması ve kovuşturulması yapılamamaktadır.

Ceza hukukunun suçun kanuniliği ve kanunsuz suç ve ceza olmaz ilkeleri doğrultusunda Türk hukukundaki yaygın olarak işlenen siber suçları şu şekilde sıralayabiliriz:

Kullanıcıların sanal kimliklerine ilişkin suçlar (Örneğin; Facebook veya Twitter gibi, sosyal medya hesaplarının çalınması, ilgili hesaplara zarar verilmesi ya da fotoğraf, video gibi verilerin çalınması, ilgili verilerin izinsiz kullanılması; banka hesaplarının çalınması).

- Dijital olarak depolanmış verilerde sahtekârlık ve söz konusu verilerin değiştirilmesi, silinmesi.
- Bilgisayar virüslerinin ve diğer zararlı yazılım unsurlarının (Örneğin; Spam, Worm gibi tehdit oluşturan unsurlar) dağıtılması – bulaştırılması.
- Bilgi teknolojileri sistemlerine yönelik saldırılar.
- Diğer siber suçlar (Örneğin; çocuk pornografisi ya da sanal ortamdaki telif haklarının ihlali).

4.1 Siber Suçlara Karşı Türk Hukukundaki Cezaî Yaptırımlar

Bir önceki bölüm altında da ifade edilen; Türkiye'de yaygın durumdaki siber suçlar karşısında, hukukî bağlamda izlenecek işlem adımlarını ve ilgili cezai yaptırımları şöyle açıklamak mümkündür:

4.1.1 Kullanıcıların Sanal Kimliklerine İlişkin Suçlar

Gerek ülkemizde, gerekse dünya çapında işlenen en yaygın siber suçlardan birisi, kullanıcıların Internet ya da daha genel anlamda dijital ortamdaki sanal kimliklerinin çalınması ya da kötüye kullanılması doğrultusunda ortaya çıkmaktadır. Bu tarz siber suçları kısaca sanal kimliklere ilişkin suçlar olarak ifade etmemiz mümkündür.

Daha detaylı olarak ilgili suçlar, -özellikle günümüzde oldukça sık karşılaşılan- banka veya kredi hesaplarının kötüye kullanılması olacağı gibi, Internet ortamındaki Facebook benzeri sosyal medya platformlarında kullanılan kimliklerin (profil) çalınması ve kötüye kullanılması şeklinde ortaya çıkabilmektedir. Bu noktada; sanal kimliklerin çalınması, kullanıcıların farkına varamadıkları casus yazılımlar ile (Örneğin; keylogger yazılımları) yapılabildiği gibi,

donanımsal ve yazılımsal açıklardan faydalanarak ya da kişiler üzerinde sosyal mühendislik yaklaşımları uygulanarak da yerine getirilebilmektedir.

Daha önce de bahsedildiği üzere, takibi şikâyete bağlı olan suçlardan olan bu tarz siber suçlara karşı çeşitli adımların izlenmesi, sonuca ulaşma noktasında kişilere faydalı olmaktadır. Bu bağlamda, burada bahsi geçen sanal kimliğe ilişkin suçlara karşı etkili ve sağlıklı çözüm elde etmek adına şu adımların izlenmesinde fayda bulunmaktadır:

▪ Güvenli bir bilgisayardan ilgili hesabın kurtarılması denenmeli; eğer kurtarma işlemi başarılı olmazsa, hesabın olduğu Web sitesinin ilgili birimlerine şikâyette bulunulmalıdır.

Adli işlem yapılabilmesi için şahsi müracaat yapılması şarttır. Bu noktada; işlemin eksiksiz başlaması için, ilgili emniyet şubelerinde ya da savcılıkta temin edilebilecek örnek müracaat formu doldurulmalıdır (Söz konusu form, ilgili emniyet müdürlüğünün Web sitesinden de elde edilebilmektedir).

Form el yazısıyla doldurup imzalandıktan sonra; form ile birlikte suçun işlendiği yerdeki polis merkez amirliğine, Cumhuriyet Başsavcılığı'na ya da Siber Suçlarla Mücadele Şube Müdürlüğü'ne müracaat edilmelidir.

Bu suçu işleyen kişi TCK'nın 243. Maddesine göre 1 yıla kadar hapis veya adli para cezası ile cezalandırılmaktadır. Ek olarak; bilgisayar sistemindeki verilerinin silinmesi ya da değiştirilmesi halinde ise, suçun faili için bu suçun cezası altı aydan iki yıla kadar hapis cezasıyla sonuçlanmaktadır.

Açıklanan siber suç, banka veya kredi hesaplarının kötüye kullanılması yönünde ise; siber suçu işleyen kişi, 5237 sayılı TCK'nın 245. Maddesi hükümlerince cezalandırılmaktadır. Böyle bir suçla karşılaşılması hâlinde yapılması gerekenleri ise kısaca şu şekilde sıralayabiliriz:

▪ İlgili banka ile görüşüp şüpheli görülen harcamanın / harcamaların ekstresi temin edilerek, kişiye ait olmayan harcamalar belirlenmeli; gerekirse bağlı doküman çıktıları elde edilmelidir.

4.1.2 Bilgisayar Virüslerinin Ve Diğer Zararlı Unsurların Dağıtılması – Bulaştırılması

Bir bilgisayara, Internet'ten indirilen dosyalar ya da başka bir yerden kopyalanmış dosyalar aracılığıyla virüs yazılımı bulaşabilmektedir. Ancak buna benzer unsurların bilgisayara bulaşmış olması, suçun oluşması için yeterli değildir. Bu zararlı unsurların suç oluşturabilmesi için, bilgisayarda kanundaki yazılı neticeleri doğuracak fiillerin gerçekleşmesi gerekmektedir.

Örneğin, bilgisayara bir Worm (solucan) zararlı yazılımı bulaştıktan sonra, bilgisayardaki verilerde bir zarar oluşmuyor ya da kişiye yönelik herhangi bir problem ortaya çıkmıyor; sadece bilgisayarın performansında yavaşlama söz konusu ise; bu durum bir siber suç olmayacaktır. Ancak, bilgisayarın işleyişi engelleniyorsa, siber suç işlenmiş olacak (TCK m.244/f.1) ve bu nedenle ilgili makamlara başvurarak, gerekli adlî işlemlerin başlatılmasının önü açılmış olacaktır.

4.1.3 Bilgi Teknolojileri Sistemlerine Yönelik Saldırılar

Bu siber suç türü, doğrudan bilgisayara karşı işlenen ve seçimlik hareketli bir suç olup, TCK'nın ilgili maddelerinde nitelikli hâlleriyle birlikte düzenlenmiştir.

Buna göre:
5237 sayılı TCK'nın 244. Maddesinin 1. fıkrasına göre, bir bilişim sisteminin işleyişini engelleyen veya bozan kişi, bir yıldan beş yıla kadar hapis cezası ile cezalandırılmaktadır.

TCK'nın 244. Maddesinin 2. fıkrasına göre, bir bilişim sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişi, altı aydan üç yıla kadar hapis cezası ile cezalandırılmaktadır.

TCK'nın 244. Maddesinin 3. fıkrasına göre, bu fiillerin bir banka veya kredi kurumuna ya da bir kamu kurum veya kuruluşuna ait bilişim sistemi üzerinde işlenmesi halinde, verilecek ceza yarı oranında artırılmaktadır.

TCK'nın 244. Maddesinin 4. fıkrasına göre, bilgi teknoloji sistemlerine yönelik saldırı fiillerin işlenmesi suretiyle kişinin kendisinin veya başkasının yararına haksız bir çıkar sağlamasının başka bir suç oluşturmaması hâlinde, iki yıldan altı yıla kadar hapis ve beş bin güne kadar adlî para cezasına hükmolunmaktadır.

4.1.4 Diğer Siber Suçlar

Diğer siber suçlardan başlıca hukuka ve genel ahlâka aykırı verilerin bulundurulması suçuna değinilmelidir. Bu bağlamda, ilgili verilerin bulundurulması ve yayınlanması durumunda; TCK m.226'da düzenlenmiş olan "müstehcenlik suçu" işlenmiş olacaktır.

Böyle bir siber suç ile karşılaşıldığı takdirde, ilgili suçun ihbar edilmesi gerekmektedir. Ancak suçu işleyen kişiye karşı etkili bir çözüme ulaşılması için şu adımların takip edilmesi gerekmektedir:

- Müstehcen – pornografik içeriğin olduğu Web sayfasının ekran görüntüsü alınmalı,
- Tespit edilen; örneğin çocuk pornografisi görüntüsü yer alan Web sayfasının adres bilgisi not alınmalı,
- İşlemin eksiksiz başlaması için hazırlanan örnek müracaat formu elle doldurulup imzalanmalı ve formda, şikâyet edilecek Web sitesinin – sayfasının adresini eksiksiz belirtmeye dikkat edilmelidir.
- Aynı zamanda, ilgili Web sitesini – sayfasını Telekomünikasyon İletişim Başkanlığı İnternet Bilgi İhbar Merkezi'nin; "ihbarweb. org.tr" Web adresine ya da bulunulan yerdeki Siber Suçlar Şube Müdürlüğü'nün ihbar hattı adresine Web site – sayfa adres bilgisi ve ekran görüntüsü ile ihbar etmek mümkündür.

Özellikle 5237 sayılı TCK'nın, siber suçlarını sadece dört madde olarak düzenlemesi; her geçen gün gelişen teknoloji ve ortaya çıkan yeni tehditler düşünüldüğünde, yeni oluşan siber suçların suçun kanunîlik ilkesi kapsamında cezasız kalmasına yol açabilmektedir. Buna göre, siber suçlarıyla mücadelede alınması gereken önlemler bağlamında; ceza hukuku normlarıyla bu konuyla ilgili kamu düzenin ihlali olarak görülen eylemlerin suç tipi olarak tanımlanması, siber suçların kapsam ve niteliği ayrıntılı bir şekilde açıklanması ve gerekli yasal düzenlemelerin yapılması, açıkların ortadan kaldırılması adına etkili olacaktır.

Uygulama aşamasında, işlenen bir siber suçun faili, siber suçların nitelikli hâlleri ayrıntılı düzenlenmediği ve sadece takdiri indirim nedenleriyle (faile uygulanarak yapılan yargılama sonunda hükmolunan ceza, iki yıl veya daha az süreli hapis cezası olduğu için), "hükmün açıklanmasının geri bırakılması" kararı verilerek (5271 sayılı CMK m.231'e göre) [6] gerektiğinden daha az ceza alabilmektedir. Bu durum, mevcut kanunların işlenen suçun cezasının belirlenmesinde yetersiz olmasından kaynaklanmaktadır. Bu nedenle daha detaylı düzenlemelerin, ilgili kanunlar altında gerçekleştirilmesi son derece önemlidir. [47]

4.1.5 5651 Sayılı Kanun

5651 Sayılı Kanun Maddesinin Amacı

Kanun maddesi internet erişiminin kontrol altına alınmasını amaçlamaktadır. Bu sayede internet üzerinden işlenen bilişim suçlarının önemli ölçüde önüne geçilmekle beraber suç unsuru içeren herhangi bir olay sonrasında suçlu ya da sorumluların tespit edilerek suçsuzdan kolayca ayrılmasını sağlamak. Ayrıca kullanıcıların internet üzerinden aldatılmalarını ve yasal içerikte olmayan kötü amaçlı içeriklerden korunması amaçlanmaktadır.

5651 Sayılı Kanun Maddesi İle İlgili Anlaşılması Gerekenler?

1. 5651 sayılı kanun maddesi kamu kurumları, özel şirketler ve kullanıcılar için bir öneri niteliği taşımamaktadır. İlgili kanun maddesinin gereklerinin yerine getirilmesi zorunlu

kılınmıştır. Kanun maddesini yerine getirmeyen tüm erişim sağlayıcılar için kanuni yaptırımlar söz konusudur. Bunları uyarı, para cezası, hapis, kapatma ve yayından kaldırma gibi sıralayabiliriz.

2. Kanun maddesince alınması istenen tedbirler tamamıyla kullanıcıların çıkarlarını gözetmekte olup, uygulanmadığı takdirde kullanıcıya maddi zararlar açabileceği gibi bu kaybın yanı sıra kamu kurumları ve özel firmalar için prestij kaybına da sebep olabilmektedir.

Yukarıda özet olarak verilen 2 maddeyi inceledikten sonra kanun esasları ile ilgili detaylara bir göz atalım.

Kanun maddesi kimleri kapsamaktadır?

İster ücretli, ister ücretsiz birden fazla kullanıcıya bir veya birden fazla internet bağlantısı üzerinden erişim hizmeti sağlayan tüm kurum ve kuruluşları kapsamaktadır. Kanun maddesi kendi içerisinde ikiye ayrılmaktadır ve kapsamları farklılık göstermektedir.

a) İnternet erişimini hizmet amaçlı veya işlerinin devamlılığını sağlamak için çalışan ya da ziyaretçilerine kullandıran kurum ve kuruluşlar.

- Kamu kurumları
- Özel şirketler
- Hastaneler
- Okullar
- Alışveriş merkezleri vb. gibi kurumlar

b) İnternet erişimini kazanç elde etmek amacıyla kullanıcıların hizmetine sunan işletmeler.

- İnternet Cafeler
- Oteller
- Ücretli kullanımın söz konusu olduğu Cafe vb. gibi işletmeler.

Yukarıda yazıldığı gibi hizmet veya kazanç amaçlı kurum ve işletmelerin kullanıcılarına kullandırmakta olduğu internet erişim hizmetinin kanun kapsamı dâhilinde kontrol altına alınması istenmektedir. Erişim sağlayıcısının kanun maddesi ile ilgili genel yükümlülüklerini şöyle sıralayabiliriz:

1.Kullanıcıların yasal içerikte olmayan WEB sayfalarına erişimlerinin engellenmesi.

2.Erişim log ve kayıtlarının tutulması.(Zaman ve Tarih Mührü ile)

3.Networklerine bağlı kullanıcıların iç IP loglarının tutulması.

4. Eğer bir Web sayfası mevcut ise ve bu Web sayfasını kendi sunucularında barındırıyor ise dışarıdan gelen erişim log ve kayıtlarının tutulması.

Kullanıcılar internet teknolojisi sayesinde Web sayfaları üzerinden bilgi paylaşımı, eğlence, iletişim kurmak, hizmet vermek ve kendilerini tanıtmak gibi birçok ihtiyacını karşılamaktadır. Artık hayatımızın olmazsa olmazları arasında yer alan internet ortamı faydalarının yanı sıra birçok tehdidi de beraberinde getirmiştir. Kötü amaçlı kişi veya kişiler haksız kazanç elde etmek için kullanıcıların kişisel bilgilerini çalarak çıkar amaçlı kullanmaktadırlar. Kullanıcı bilgileri ile kullanıcıları dolandırmak, bilgilerini pazarlayarak haksız kazanç elde etmek ya da işledikleri bir suçu habersiz masum kullanıcılar işlemiş gibi göstererek kendilerini gizlemektedirler. İlgili kanun maddesi tüm bu olumsuzlukları minimuma indirmeyi amaçlamaktadır. Bu sebeple internet ortamında tamamıyla savunmasız bulunan kullanıcıların hizmet aldıkları kurumlar tarafından koruma altına alınmasını istemektedir. Kanun maddesinde istenen bu yaptırım hizmet veren kurumlarında müşterilerini korumak ve daha iyi hizmet verebilmek için uygulamaları gereken bir yaptırımdır.

Kanun maddesi tam olarak yasal içerik taşımayan kullanıcıların bilgilerinin çalınmasına sebebiyet verebilecek sahte web sayfaları, yasal olmayan propagandaların bulunduğu, sitelerin, suç unsuru içeren tüm web sayfalarının engellenmesini ve kullanıcıların bilinçli veya bilinçsiz bir şekilde bu web sayfalarına erişimlerinin engellenmesini istemektedir.

Fakat büyük bir hızla hemen her gün yayınlanan web sayfalarının kontrol altına alınması neredeyse imkânsız olduğundan henüz kara listeye alınmayan bir web sayfası üzerinden işlenebilecek olası suçlarında daha sonra takip edilebilmesi ve kim tarafından nasıl gerçekleştirildiğinin bilinmesi amacıyla web sayfalarına erişen tüm kullanıcıların kayıtlarının (loglarının) zaman tarih mührü ile tutulmasını ve saklanmasını istemektedir. İster yasal içerikte olsun ister olmasın tüm erişimlerinin kayıtlarının tutulması gerekmektedir ve bu kayıtların 6 ay ila 2 yıl arasında süre ile saklanması istenmektedir. [48]

4.1.6 5809 sayılı Elektronik Haberleşme Kanunu

5809 sayılı Elektronik Haberleşme Kanunu daha önce 5803 sayılı Kanun olarak 01.08.2008 tarihinde TBMM'de kabul edilmiş ve yayımlanmak üzere Cumhurbaşkanlığına gönderilmiştir. Ancak, Cumhurbaşkanlığı tarafından 59, 60, 66 ve 67 nci maddeleri yönünden yeniden görüşülmesi istemi ile TBMM'ye iade edilmesi üzerinde tekrar görüşülerek 5809 sayılı Kanun olarak kabul edilmiş ve 10.11.2008 tarihinde yürürlüğe girmiştir. Elektronik Haberleşme Kanunu, Avrupa Birliğine uyum çalışmaları çerçevesinde gelişen teknolojinin beraberinde getirdiği sorunları çözme amacıyla çıkartılmış olan yasalardan birisidir.

15.01.2004 tarih ve 5070 sayılı Elektronik İmza Kanunu ile elektronik imzanın geçerliliği kabul edilmiş ve anılan kanunun 17'nci maddesi ile sahte elektronik sertifika yapılması ve kullanılması suç olarak kabul edilmiştir.

4. 2 Türkiye Siber Güvenlik Faaliyetleri

4.2.1 Strateji Eylem Planları

Ülkemizde siber güvenlik konusunda birçok çalışma yapılmış ve yapılmaya devam edilmekle birlikte daha alınacak çok yol olduğu değerlendirilmektedir. Bu konuda yapılan çalışmaları, yasal çalışmalar, ulusal bilgi güvenliği kapısı, TR-BOME Bilgisayar Olaylarına Müdahale Ekibi, Bilgi Toplumu Stratejisi Eylem Planı (2006 - 2010), Kişisel Verilerin Korunması Kanunu Tasarısı, Ulusal Sanal Ortam Güvenlik Politikasının oluşturulması, siber

güvenlik tatbikatları, siber güvenlik çalıştay ve konferansları ve TSK'nın yürüttüğü faaliyetler şeklinde sayabiliriz (BTK [web], 2012a).

4.2.2 Ulusal Bilgi Güvenliği Programı

2005 yılında oluşturulan Bilgi Toplumu Stratejisinin 88nci maddesinde "TÜBİTAK - Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne" (UEKAE) "Ulusal Güvenlik Programı"nı yürütme sorumluluğu verilmiştir. Bu programın ana hedefleri ve yürütülen çalışmalar şunlardır (TUBİTAK BİLGEM [web], 2012):

Hedefler

(a) Kamuda yer alan kurumların bilgi güvenliği konusunda bilinçlenmelerini sağlamak ve bilgi noksanlıklarının giderilmesi ve kurumlar için güncel olan bilgi güvenliği uyarılarının düzenli olarak yayınlanması

(b) "Bilgisayar Olayları Müdahale Ekibi - Koordinasyon Merkezi'nin kurulması ve etkin olarak çalıştırılması

(c) Kamu kurumlarında bilgi güvenliğinin sağlanması maksadıyla alınması gereken tedbirlerin ortaya çıkarılması

(ç) Kamu alanında faaliyet gösteren kurumları hedef alan tehditlerin tespit edilmesi

Çalışmalar

(a) Örnek olarak belirlenen kamu kurumları için "Bilgi Güvenliği Yönetim Sistemi" kurulumu danışmanlık hizmeti verilmesi ve kurumların bilgi sistemlerinde yer alan güvenlik sorunlarının belirlenmesi

(b) "Bilgisayar Olayları Müdahale Ekibi - Koordinasyon Merkezi'nin kurulması ve akabinde kamu kuruluşlarına "Bilgisayar Olayları Müdahale Ekipleri" kurulması maksadıyla danışmanlık hizmeti sunulması

(c) Kamu kurumlarında bulunan bilgi sistemlerinin siber alan üzerinden maruz kalacağı tehditlerin tespit edilmesi maksadıyla "sanal ortam savunma sistemi" kurulması

(ç) "Ulusal Bilgi Güvenliği Kapısı'nın kurulup işletilmesi

(d) Kamu kuruluşlarında bilgi güvenliğinin değişik boyutları ile alakalı uygulamalı eğitim hizmeti verilmesi

(e) Bilgi güvenliği konusunda rehber doküman ve teknik makaleler hazırlanması

4.2.3 Ulusal Bilgi Güvenliği Kapısı

Ulusal Bilgi Güvenliği Programının bir alt projesi olan ve amacı "Bilgi güvenliği ile ilgili güncel uyarılar, bilgilendirici rehberler ve teknik yazılar yayınlamak" olan "Ulusal Bilgi Güvenliği Kapısı"nın kurulması ve işletilmesi, TÜBİTAK-UEKAE tarafından gerçekleştirilmektedir. İçerik olarak her şahıs ve kurumun katkı yapabildiği bu kapının ülkemizde ihtiyaç duyulan bilgi güvenliği konusundaki bilgi birikimini meydana getirmek adına çok önemli bir fonksiyonu gerçekleştirmesi umulmaktadır (TUBİTAK BİLGEM [web], 2012).

4.3 Ulusal Siber Güvenlik Stratejisi ve 2013 – 2014 Eylem Planı

Bakanlar Kurulunun 11.6.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20.10.2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmişti. İlgili karar kapsamında hazırlana Eylem Planı 2013-2014 döneminde gerçekleştirilmesi planlanan işleri tanımlamakla beraber, bu yılları aşan periyodik faaliyet ile eğitim ve bilinçlendirme çalışmaları gibi sürekli yürütülmesi gereken faaliyetlere de yer verilmektedir.

Bu karar kapsamında Kritik alt yapılar;
"İşlediği bilginin gizliliği, bütünlüğü ve erişilebilirliği bozulduğunda,
* Can kaybına,
* Büyük ölçekli ekonomik zarara,

* Ulusal güvenlik açıkların ve kamu düzeninin bozulmasına,
yol açabilecek bilişim sistemlerini barındıran altyapılar," olarak tanımlanmıştır.

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın kabulü; Ulaştırma, Denizcilik ve Haberleşme Bakanlığının 18.2.2013 tarihli ve 412 sayılı yazısı üzerine, Bakanlar Kurulu'nca 25/3/2013 tarihinde kararlaştırılmıştır.

Özetle;

EYLEM PLANININ AMACI

a) Kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına,
b) Kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına,

c) Siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçun adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına, yönelik bir altyapı oluşturmaktır.

EYLEM PLANI KAPSAMI;

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, kamu bilişim sistemlerini ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerini kapsar.

EYLEM PLANININ GÜNCELLEMESİ

Ulusal Siber Güvenlik Stratejisi gelişen teknoloji, değişen şartlar ve ihtiyaçlar göz önünde bulundurularak kamu ve özel sektörden gelecek talepler doğrultusunda en az yılda bir kez olmak üzere ulusal düzeyde sağlanacak eşgüdüm ile güncellenecektir.

SİBER GÜVENLİK RİSKLERİ,

Dikkat çekici maddeler;

5) Siber güvenliğin ulusal düzeyde bütün vatandaşlarca topyekûn sağlanabileceği gerçeğine rağmen bu konudaki ulusal bilincin yetersiz olması.

9) Kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması.

10) **Kurumlarda bilgi güvenliği yönetim altyapılarının yeterli düzeyde olmaması.**

11) **Siber güvenlik konusunda kurumsal ve kişisel seviyede yeterli bilgi ve bilinç seviyesine ulaşılamamış olması.**

12) **Siber güvenlik konusunda kurumların üst düzey yöneticilerinin yeterli bilince sahip olmamaları veya siber güvenlik konusunda yeterince sahiplenmemeleri.**

13) Siber güvenlik konusunda kurumların yapılanmalarının yetersiz olması ve siber güvenliğin, kurumların sadece bilgi işlem birimlerinin sorumluluğunda görülmesi.

14) Bilgi işlem birimlerinde çalışanların siber güvenlik konusunda yeterli bilgi seviyesine ve tecrübeye sahip olmaması.

15) Siber güvenlik olaylarının detaylı araştırılması ve ihlal ile ortaya çıkan suçun soruşturulması alanlarında az sayıda yeterli personel bulunması.

16) Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınmaması.

17) Siber güvenliğin, geliştirilen veya tedarik edilen bilişim sistemlerinin vazgeçilmez bir unsuru olarak ele alınmaması, buna bağlı olarak kamu kurumlarının bilgi ve iletişim teknolojileri alanındaki ürün ve hizmet tedariklerinde siber güvenliğin yeterli seviyede göz önünde bulundurulmaması.

18) **Donanım ve yazılım alanında yerli üretimin yeterli düzeyde olmaması**.

EYLEM PLANI İLKELER

Dikkat çekici maddeler;

13) Siber güvenlik gereksinimlerinin karşılanmasında yerli ürün ve hizmet kullanımı teşvik edilir, bunların geliştirilmesi için araştırma ve geliştirme projeleri desteklenir, inovasyon (yenileşim) anlayışı esas kabul edilir. [49]

STRATEJİK SİBER GÜVENLİK EYLEMLERİ

Adli Süreçlere Yardımcı Olacak Çalışmaların Yürütülmesi

Uluslararası hukuk kuralları çerçevesinde, siber saldırılara maruz kalan tarafların haklarının korunabilmesi için, saldırı kaynağının tespiti ve saldırılan sistemler ile bu sistemlerden hizmet alan taraflarda hangi boyutta etki oluştuğunun belirlenmesi gerekir. Bu bilgilerin üretilmesi için ulusal siber ortamın günün teknolojisine uygun ve güvenilir kayıt mekanizmaları ile donatılması gerekmektedir.

Ulusal Siber Olaylara Müdahale Organizasyonunun Oluşturulması

Kısa vadede; siber ortamda ortaya çıkan tehditlerin hızla belirlenmesi, yaşanabilecek olayların etkilerini azaltmaya veya ortadan kaldırmaya yönelik önlemlerin geliştirilmesi ve paylaşılması için ulusal ve uluslararası düzeyde etkin bir şekilde çalışacak **Siber Olaylara Müdahale Organizasyonu oluşturulacak, böylece kurum ve kuruluşların siber güvenlik olaylarına müdahale yeteneği kazanması sağlanacaktır**. Ülkemizi etkileyebilecek tehditlere karşı, 7/24 müdahale esasına göre çalışacak "Ulusal Siber Olaylara Müdahale Merkezi (USOM)" kurularak, USOM'un koordinasyonunda çalışacak sektörel "Siber

Olaylara Müdahale Ekipleri (SOME)" oluşturulacaktır. Sektörel SOME'ler siber olaylara müdahalenin yanı sıra kendisine bağlı SOME'lere ve ilgili olduğu sektöre özel bilgilendirme ve bilinçlendirme faaliyetleri yürütülecektir. Kurum ve kuruluşlar bünyesinde de sektörel SOME'lerin koordinasyonunda çalışacak SOME'ler kurulacaktır. USOM ve SOME'ler olaylara müdahale ederken suç soruşturmasına destek sağlayacak verilerin sağlanması için adli makam ve kolluk birimleri ile koordineli hareket edeceklerdir. USOM ulusal temas noktası olarak diğer ülkelerin eşdeğer makamlarıyla ve uluslararası kuruluşlarla yakın işbirliği yapacaktır.

Ulusal Siber Güvenlik Altyapısının Güçlendirilmesi

Kısa ve orta vadede tüm kurumlar, kurumsal bilişim sistemlerinin siber güvenliğini destekleyecek geniş kapsamlı altyapı projeleri gerçekleştirilecektir. Öncelikli olarak kritik altyapılara ait bilişim sistemleri olmak üzere kurumsal siber güvenliğin sağlanması için çalışmalar yapılacaktır. Kritik altyapılara ait bilişim sistemleri, kritiklik seviyeleri, birbirleriyle ilişkileri ve sorumlulukları belirlenecektir. Kritik altyapılara ait bilişim sistemlerinin siber güvenliği, teknolojik önlemlerin yanı sıra idari tedbir ve süreçlerle de sağlanacaktır. Bunun için kurumlarda idari ve teknolojik içerikli eğitimler aracılığıyla üst düzey yöneticiler başta olmak üzere tüm çalışanların siber güvenlik konusunda yetkinlik düzeyi arttırılacaktır. Kurumsal siber güvenliği sağlama konusunda gerekli yetkinliğe sahip olmayan kurumlar teknolojik ve idari boyutta sağlanacak hizmetlerle desteklenecektir.

Siber Güvenlik Alanında İnsan Kaynağının Yetiştirilmesi ve Bilinçlendirme Faaliyetleri

Orta ve uzun vadede siber güvenlik alanında yeterli sayıda ve yetkin insan kaynağı oluşturulmasına yönelik çalışmalar yapılacaktır. İlk, orta, lise öğrenimi ve yaygın eğitim ile yükseköğretimde siber güvenlik konusunun yer alması için düzenlemeler yapılacaktır. Bilişim sistemleri denetçilerinin, teknoloji eleştiricilerinin, sistem yöneticilerinin ve ilgili tüm tarafların siber güvenlik bilincinin arttırılması ve üstlerine düşen sorumluluklar konusunda bilgilendirilmeleri amacıyla etkinlikler gerçekleştirilecektir. Kurumsal iç denetim süreçlerinde siber güvenliğe ilişkin denetim adımlarının yeterli seviyede ele alınması için çalışmalar yapılacaktır. Ayrıca, siber güvenlik bilincini oluşturmak ve geliştirmek üzere tüm

vatandaşlara yönelik bir eğitim platformu oluşturulacak ve bu eyleme hizmet eden girişimler desteklenecektir.

Siber Güvenlikte Yeterli Teknolojilerin Geliştirilmesi

Orta ve uzun vadede siber güvenlik konusunda ülkemizin sahip olduğu teknik birikim, olanak ve kabiliyetler arttırılacaktır. Kamu ve özel sektörün araştırma ve geliştirme gereksinimlerinin karşılanmasına yönelik tüm eylemlerde işbirliği içerisinde çalışması sağlanacaktır. Kurumların bilişim sistemlerinde yerli olarak geliştirilmiş ürünleri tercih etmeleri, yerli ürünlerin mevcut olmadığı durumlarda ise güvenlik değerlendirmesi yerli olarak gerçekleştirilmiş sertifikalı ürünleri tercih etmeleri teşvik edilecektir.

4.4 Siber Güvenlik Tatbikatları

Ülkemizde ilki 2008 yılında ikincisi ise 2011 yılında olmak üzere iki siber güvenlik tatbikatı yapılmıştır. ABD'deki *CyberStorm*, NATO bünyesinde yapılan Cyber *Coalition* ve AB bünyesinde gerçekleştirilen *Cyber Europe* isimli tatbikatlardan, yazılı senaryoların yanında gerçek saldırıları da içermesiyle ayırt edilen bu tatbikatlara birçok kamu kurumu ve özel sektör kuruluşu katılmıştır (TUBİTAK UAKAE [web], 2012).

Bu tatbikatlardan ilki olan "BOME 2008" 8 kamu kurumunun katılımıyla 20-21 Kasım 2008 tarihinde TR-BOME tarafından gerçekleştirilmiştir. Daha kapsamlı olan ikinci siber güvenlik tatbikatı 2011 yılında 41 kurumun katılımıyla 25 ila 28 Ocak 2011 günleri arasında gerçekleştirilmiştir. Tatbikat ile "siber savaş tehdidine karşı hazırlıklı olmak, kurumların bilgi sistemi güvenliği olaylarına müdahale yeteneği ile kurumlar arası koordinasyon yeteneğini tespit etmek, kurumlar arası iletişimi artırmak, bilgi ve tecrübe paylaşımını ve siber güvenlik bilincinin artırılmasını sağlamak" amaçlanmıştır (TUBİTAK UAKAE [web], 2012).

İcra edilen tatbikatta elde edilen bulgular şu şekilde özetlenmektedir

(1) "Bilgi Güvenliği Yönetim Sistemi Eksikliği

Bazı katılımcılarda Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) bulunmadığı ve katılımcıların yazılı politikalarının, özellikle bilgi güvenliği politikasının, prosedür ve talimatlarının olmadığı, risk analizlerinin yapılmadığı, bir bilgi güvenliği ihlali gerçekleştiğinde bu olayın nasıl yönetileceğine ve böyle bir olayla bir daha karşılaşmamak için gerçekleştirilmesi gereken düzeltici/önleyici faaliyetlerin nasıl belirleneceğine dair yerleşik bir bilgi güvenliği kültürünün bulunmadığı gözlemlenmiştir.

(2) Sistem Yöneticilerinin Teknik Yetersizliği

Bazı katılımcıların sistem yöneticilerinin yeterli teknik bilgi birikimine sahip olmadıkları, sistemde bir problem meydana geldiğinde bu problemle teknik olarak nasıl başa çıkacaklarını bilemedikleri, dolayısıyla problemlerin olması gerekenden daha uzun sürede çözüldüğü tespit edilmiştir.

(3) Saldırı Tespit Sistem ve Süreçlerinin Yetersizliği

Bazı katılımcılarda düzenli olarak gerçekleştirilen saldırılara karşı önlem almak amacıyla saldırı tespit sistemlerinin kullanılmadığı, saldırı tespit sistemlerinin bulunduğu bazı katılımcılarda ise söz konusu sisteme ait uygulamanın ürettiği kayıtların etkin olarak incelenemediği, dolayısıyla saldırıların tespit edilmesi noktasında sıkıntılar yaşandığı gözlemlenmiştir.

(4) Sosyal Mühendislik Saldırılarına İlişkin Bilinç Yetersizliği

Bazı katılımcıların, yaşanan güvenlik olaylarına sadece teknik çözüm arayışında oldukları, güvenlik zincirinin en önemli halkasını oluşturan insan faktörünü göz ardı ettikleri tespit edilmiştir.

Katılımcıların genel olarak çalışanlarına, sosyal mühendislik saldırılarına karşı düzenli olarak farkındalık eğitimleri vermedikleri, bazı katılımcılarda bu tip saldırıları engellemek amacıyla kullanıcılara düzenli olarak uyarı e-postaları gönderme ve kurum içerisinde belirli yerlere çeşitli bilgi güvenliği uyarıları asma gibi bilgi güvenliğini hatırlatıcı yöntemlerin etkin olarak kullanılmadığı gözlemlenmiştir. Ayrıca bazı katılımcılarda personelin bu tür saldırılara karşı bağışıklığını arttırmak için periyodik

olarak sosyal mühendislik testlerinin yapılmadığı gözlemlenmiştir.

(5) Güncel Olmayan Anti Virüs Sistemleri

Bazı katılımcılarda merkezi anti virüs sunucuların imza dosyalarının düzenli olarak güncellenmediği, dolayısıyla merkezi anti virüs sunucusundan güncellemeleri alan uç birimler üzerinde kurulu olan anti virüs yazılımlarının imza dosyalarının da periyodik olarak güncellenmediği tespit edilmiştir.

(6) Sistem Yöneticilerinin Güvenlik Boyutunda Yetersizliği

Bazı katılımcılarda sistem yöneticilerinin bilgi güvenliği konusunda gerekli yetkinliğe sahip olmadıkları, ayrıca katılımcıların özel ilgi grupları, diğer uzman güvenlik forumları ve STK'lar ile iletişim içinde olmadığı gözlemlenmiştir.

(7) Kurum İçi Koordinasyonun Yetersizliği

Bazı katılımcılarda kurum içinde birimler arası koordinasyonun yetersiz olduğu, bazı birimlerde personel yedekliliğinin sağlanamadığı, dolayısıyla bir bilgi güvenliği olayı gerçekleşmesi durumunda gerekli adımların zamanında atılamadığı ve ilgili mercilerle temasın hiç sağlanamadığı ya da geç sağlanabildiği tespit edilmiştir.

(8) Erişim Kontrol Politikasının Bulunmaması

Bazı katılımcılarda, erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikasının bulunmadığı, bunun bir sonucu olarak personelin kendileriyle ilgili olmayan bilgi ve hizmetlere de erişebildiği tespit edilmiştir.

(9) Sistem Tasarımı Aşamasında Güvenliğin Göz Ardı Edilmesi

Bazı katılımcılarda, sistem tasarım aşamasında güvenliğin bir temel tasarım prensibi olarak ele alınmadığı, bu durumun güvenlik olaylarının yaşanmasını tetiklediği ve yaşanan güvenlik olaylarına etkin müdahaleyi zorlaştırdığı tespit edilmiştir.

(10) Kablosuz Ağlardan Kaynaklanan Riskler

Bazı katılımcılarda, saldırgan tarafından yayıma sunulan kablosuz erişim noktasının tespitinin yapılamadığı ve personelin bu yetkisiz erişim noktası üzerinden hizmet alabilecek durumda oldukları gözlemlenmiştir.

(11) İş Sürekliliği Planlarının Bulunmaması

Bazı katılımcıların, sistem kesintisine yol açan bilgi güvenliği olayı yaşanması durumunda iş faaliyetlerindeki kesintileri önlemek ve önemli iş süreçlerinin devamlılığını sağlamak amacıyla tesis edilmiş bir iş sürekliliği planına sahip olmadıkları tespit edilmiştir.

(12) Port Tarama Saldırılarının Algılanmaması

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerine yapılan "Port Tarama" saldırısını algılayamadıkları tespit edilmiştir.

(13) Dağıtık Servis Dışı Bırakma Saldırılarının Olumsuz Sonuçları

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerine yapılan "Dağınık Servis Dışı Bırakma" (DDoS) saldırısı sonucunda kurumların çoğunun hizmetlerinin kesintiye uğradığı, hizmet kesintisi yaşamayanların İnternet Servis Sağlayıcılarından (İSS) bu tür saldırılardan korunmak amacıyla hizmet satın aldıkları tespit edilmiştir. Bu durum, bilgi güvenliğinin sağlanmasında kurumlar arası iletişime, işbirliğine ve koordinasyona verilmesi gereken önemi ortaya koymaktadır.

(14) Web Uygulamalarında Bulunan Açıklıklar

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerinde çalışmakta olan web uygulamalarında çeşitli açıklıklar bulunduğu tespit edilmiştir. Uygulama geliştirirken güvenliği temel ihtiyaç olarak göz önünde bulunduran, ek olarak web uygulamalarını bağımsız kurum/kuruluşlara denetlettiren katılımcıların web uygulamalarında nispeten daha az açıklık bulunduğu görülmüştür.

(15) Kayıt Dosyalarının Analizinin Gerçekleştirilememesi

Bazı katılımcılarda tatbikat kapsamında yapılan saldırılar sırasında oluşturulmuş

saldırı kayıt dosyalarını analiz ederek saldırının ne zaman, nasıl, kim tarafından gerçekleştirildiğini belirleyemediği tespit edilmiştir. Özel bir bilgi güvenliği birimine sahip olan katılımcıların nispeten daha başarılı oldukları görülmüştür.

(16) Yasal Mevzuata İlişkin Bilgi Eksikliği

Bazı katılımcıların, siber güvenliğe ilişkin ulusal mevzuatımız hakkında yeterli bilgiye sahip olmadıkları, dolayısıyla tatbikatta uygulanan yazılı senaryolarda yer alan yasal mevzuatta bilişim suçu olarak tanınan fiilleri adli mercilere bildirmedikleri tespit edilmiştir."

4.5 T.C Ulaştırma Denizcilik Ve Haberleşme Bakanlığı, Bilgi Güvenliği Derneği, Türkiye Barolar Birliği İşbirliği İle Düzenlenen Siber Güvenlik Hukuku Çalıştayı Sonuç Bildirgesi

Çalıştay sonucunda elde edilen çıktılar ve ülkemiz için yapılması gereken hususlar ile ilgili öneriler aşağıda balıklar halinde verilmiştir.

1. Günümüzde kişi, kurum ve kuruluşlara ait bilgi varlıklarının hacminin ve çeşitliliğinin geçmişe oranla ciddi artışlar gösterdiği. Artık bilgi varlıklarımızın çok büyük ölçüde sayısallaştığı ve bu durumunun gerek kamu gerekse özel iş süreçlerini kolaylaştırdığı. Geçmişte mümkün olmayan yeni servisleri mümkün hale getirdiği. Ancak bütün bunların yanı sıra hayatımızın birçok yönünü ve evresini kapsayan siber uzay altyapısının güvenliğinin sağlanması konusunun ciddi bir problem olduğunun taraflarca kabul edildiği ve gerekli eylemlerin ivedilikle hayata geçirilmesi gerektiği.

2. Başta Kamu olmak üzere tüm kurum ve kuruluşların birçok hizmetlerini internet ortamında sunmaya başlamasıyla birlikte bu ortamda yaşanacak olumsuzlukların kişisel, sosyal ve ekonomik hayatımızı önemli ölçüde etkilediği. Etkili tedbirler alınmadığı takdirde gelecekte yaşanabilecek olumsuzlukların daha da artacağı. Oluşabilecek siber güvenlik vakalarının hem

maddi hem de manevi zararlar verebileceği. Bu tür zararlarının büyük ölçüde engellenebilmesi için ilgili tüm taraflara görevler düştüğü.

3. Ülkemizde bilişim ve internet ortamında işlenen suçlar ile ilgili mevcut mevzuat değerlendirildiğinde, 5237 sayılı "Türk Ceza Kanunu", 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun", 5070 sayılı "Elektronik İmza Kanunu" gibi kanunlar ve ilgili yönetmeliklerle siber güvenlik hukuku altyapısının desteklendiği fakat sadece bu düzenlemelerle günümüz ihtiyaçlarının tümüyle karşılanmasının mümkün olmadığı.

4. Siber güvenlik hukuku mevzuat çalışmalarında, hukukçu, teknik kişi, sosyolog-psikolog gibi sosyal bilimci vb. farklı disiplinlerinden oluşan mesleki uzmanların katkı vermesinin hukuki ve teknik altyapı uyumluluğunun sağlanması noktasında önem arz ettiği.

5. Bireyleri ve toplumu siber güvenlik vakalarının muhtemel olumsuzluklarından korumak için, mevzuat, standart, eğitim ve denetleme unsurlarının tümünü içerecek kapsamlı bir altyapının ilgili taraflarının katkı ve katılımıyla oluşturulması gerektiği.

6. Siber güvenliğin sağlanması ve vatandaşlarının her türlü veri ve bilgilerinin korunmasının yasal güvence altına alınabilmesi için hukuk bütünlüğü içinde ilgili yasa ve yönetmelikleri içeren mevzuatın siber alandaki günümüz ihtiyaçlarını kapsayacak biçimde hazırlanması gerektiği.

7. Siber varlıkların sınırlarının ve bu varlıklar arasındaki iletişimin ulusal sınırları aştığı. Siber ortamda saldırgan ve mağdurların çoğu durumda farklı ülkelerde yer alabildiği. Dolayısıyla siber güvenlik alanında, uluslararası birlikte çalışılabilirlik mekanizmalarının ve sözleşmelerin önem kazandığı. Önümüzdeki günlerde uluslararası işbirliklerinin daha da arttırılmasına ihtiyaç olduğu.

8. Türkiye'nin Avrupa Konseyi Üyesi 47 ülke tarafından imzalanan "Siber Suçlar Sözleşmesini" imzaladığı ve yürürlüğe girmesi için T.B.M.M onayını beklediği. Bu

sözleşmenin Meclis tarafından onaylanmasına müteakip iç hukuka uyarlanması gerektiği. Bu sözleşme kapsamınca özellikle vatandaşların kişisel verilerinin diğer ülkelerle paylaşımı hususundaki düzenlemelerin dikkatlice irdelenmesi gerektirdiği.

9. Yasalaşmayı bekleyen "Kişisel Verilerin Korunması Yasa Tasarısının" farklı görüşlerin, yaklaşım ve kaygılarını da dikkate alarak kapsamlı şekilde değerlendirmesi gerektiği, bu konudaki yasal boşluğun bir an önce giderilmesine ihtiyaç olduğu.

10. Kişisel verilerinin korunmasıyla ilgili yasal düzenlemelerde, vatandaşlarının gizli kalması gereken kişisel veri ve bilgisine erişimde, istisnai durumlar olarak tanımlanan ve tanımlanacak olan hususların açık kriterlere bağlanmasına ihtiyaç olduğu. Bu yasal düzenlemelerde ülkemizde vatandaşların en önemli kişisel verilerinden olan genetik ve DNA bilgilerin gizliliğinin sağlanması konularının göz önünde bulundurulması gerektiği.

11. Siber güvenlik ve kişisel verilerin korunması hususundaki yasal mevzuat çalışmalarında katılımcılık ve şeffaflık ilkelerinin gözetilmesi gerektiği ve bu düzenlemelerinin hem idarenin hem de halkın talep ve menfaatlerini azami ölçüde gözetmesinin beklendiği.

12. Kamu kurumları ile bankacılık, telekomünikasyon vb. hizmet sunucu özel kuruluşlarının kullandıkları bilişim altyapılarının, önceden belirlenmiş ve yasal düzenlemelerdeki ihtiyaçlara cevap veren standartlara sahip olması gerektiği. Bu bağlamda öncelikli olarak uluslararası güvenlik standartlarından da faydalanılarak ulusal siber altyapı güvenliği standartlarının belirlenmesine ve uygulanmasına ihtiyaç olduğu.

13. Mevzuatta tarifi yapılmayan ve/veya içtihada bağlanmayan siber suçlarının, adli süreçlerde sorumluluğunun belirlenmesi ve dağıtılması hususlarının zorlaştırdığı; mevcut Türk Ceza Kanununda tarifi yapılmayan suç ve taraf tanımlarının yapılarak bu konudaki eksikliklerin giderilmesinin adli süreçlerin hızlı ve sağlıklı ilerlemesi açısından önem arz ettiği.

14. Fikri ve Sınaî Haklar Yasasında, yazılımların eser olarak tanımlandığı ve aynı yasanın 16. Maddesinde yazılımlarının değiştirilmesi hakkının manevi haklar kapsamında

değerlendirildiği ve bu durumun özellikle kullanılan yazılımlarının güvenlik amaçlı olarak değiştirilmesi önünde engellere sebebiyet verdiği. Bu problemin özellikle yabacı menşeli savunma sınaî yazılımları için çok ciddi bir problem olarak ortada durduğu ve çözüm beklediği.

15. Başta A.B.D ve batı Avrupa ülkeleri olmak üzere siber suçlarla mücadele için çok ciddi mali kaynaklarının ayrıldığı, siber güvenlik politika ve strateji belgeleri oluşturulduğu; Ülkemizde bu yönde eksiklikler olduğu ve bu eksikliklerin ivedilikle giderilmesine ihtiyaç olduğu.

16. Kamu kurum ve kuruluşlarının siber güvenlik alanında bilgi, beceri ve imkânları arasında ciddi farklılıklar olduğu; kurumlar arası bu alandaki bilgi ve tecrübelerinin paylaşılması ve giderilmesi gerektiği.

17. Başta bankalar olmak üzere, ticaret ve hizmet hayatının önemli kuruluşların, şeffaflığı sağlamak ve hizmet alıcıları bilgilendirmek için yaşanan bilgi güvenliği açıklarını hesap sahipleri ile veya kamuoyu ile paylaşmaları gerektiği.

18. Ülkemizde siber güvenlik hukuku konusunda daha fazla uzman yetiştirilmesine ihtiyaç olduğu ve bu konuda üniversitelerin ve kurumların gerekli eğitim, sertifikasyon ve tez çalışmaları yapılmasına imkân sağlamasının daha çok faydalar getireceği ve sürecin sağlıklı olarak yönetilmesine büyük katkılar sağlayacağı.

19. Ülke ekonomisi, kamu refahı ve güvenliği için çok önem arz eden su, elektrik, gaz, telekomünikasyon ve finans gibi sektörlerin kullandığı bilişim ve otomasyon altyapılarının AB Ülkelerinde ve ABD'de "Kritik Altyapılar" olarak nitelendirildiği. Bu tür altyapıların sürekli ve güvenli hizmet verebilmesi için ulusal güvenlik, risk değerlendirme ve denetleme standartlarının belirlenmesine ihtiyaç olduğu. Kamu, özel ayrımı yapmadan ülke Kritik Altyapının korunması için hukuki ve teknik düzenlemelerin ayrıca ve ivedilikle ele alınması gerektiği; bu konuda yürütülecek bilimsel çalışmaların desteklenmesinin faydalar getireceği.

20. Ulusal siber güvenliğin en önemli hukuki altyapısını oluşturacak olan "Ulusal Siber Güvenlik Yasa Tasarısının" ivedilikle gündeme alınması ve yasalaştırılmasının son derece önemli olduğu.

21. Bütün bunların yanı sıra; Ulusal Bilgi Güvenliği konusunda politika belirlemek, strateji geliştirmek, Siber Güvenlik alanında her türlü koordinasyonu sağlamak, planlanma ve uygulamaları gerçekleştirmek, Siber savunma gücünü oluşturmak, Ulusal anlamda bütün kritik altyapı ve ülke varlıklarını savunmak, gerektiğinde müdahale etmek ve toplu saldırılar karşısında gerekli koordinasyonu sağlamak amacıyla BOME, C-SIRT gibi birimleri de içerisine alan bir "Siber Güvenlik Ulusal Koordinasyon Kurulunun" ivedilikle hayata geçirilmesi, kararları alınmıştır.[50]

4.6 Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri

1. Giriş

Dayanak

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanı, "**Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı**'nın 6'ncı ana eylem maddesi olan "Kamu Bilgi Güvenliği Programı" kapsamında hazırlanmıştır. İlgili eylem maddesi Tablo-1'de verilmiştir.

No	Eylem	Alt Eylem	Bitirilme Tarihi	Sorumlu (S) ve İlgili (İ) Kuruluşlar
6	**Kamu Bilgi Güvenliği Programı**	- ***Kamu kurumlarının uyması gereken asgari güvenlik kriterleri dokümanının hazırlanması***	***Ağustos 2013***	- TÜBİTAK (S) - Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (İ) - USOM (İ)
		- Sistem yöneticilerine ve ilgili diğer teknik personele öncelikli ihtiyaçlar uyarınca periyodik siber güvenlik eğitimlerinin ilkinin verilmesi, eğitim alan personelin yeterliliklerinin tespiti	İlki tamamlanmıştır.	
		- Kurum bazında yapılması zorunlu kılınacak yıllık güvenlik test ve denetimlerinin ilkinin, önceliklendirilecek kamu kurumları için ilgili kurumlarla mutabakat sağlanarak gerçekleştirilmesi	Aralık 2013	
		- Bilişim sistemleri güvenliğine ilişkin sıkılaştırma dokümanları ve standartların yayınlanması ve güncellenmesi	Sürekli	- TÜBİTAK (S)

Tablo-1: Eylem Planı'nın 6. maddesi

Bilişim Sistemleri ve Kamu Kurumları

Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bilgi ve iletişim sistemleri hayatımızın her alanında önemli rol oynamaktadır. Kamu kurumlarına ilave olarak enerji, su, ulaşım, haberleşme ve finansal hizmetler gibi kritik altyapı sektörlerinde faaliyet gösteren kurum ve kuruluşlar da bilgi ve iletişim sistemlerini yoğun olarak kullanmaktadır.

Sözü edilen sistemler, verilen hizmetin kalitesini ve hızını artırmakta, dolayısıyla hem ilgili kurumun daha verimli çalışmasını sağlamakta hem de vatandaşlarımızın yaşam standardının yükseltilmesine katkıda bulunmaktadır.

Kurumlarımızın hizmet sunumlarında bilgi ve iletişim sistemlerini her geçen gün daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması hem ulusal güvenliğimizin, hem de rekabet gücümüzün önemli bir boyutu haline gelmiştir. Bilgi ve iletişim sistemlerinde bulunan güvenlik zafiyetleri, bu sistemlerin hizmet dışı

kalmasına veya kötüye kullanılmasına, can kaybına, büyük ölçekli ekonomik zarara, kamu düzeninin bozulmasına ve/veya ulusal güvenliğin ihlaline neden olabilecektir. Bu tür durumların önüne geçebilmek amacıyla kamu kurumlarının sahip olması gereken asgari güvenlik kuralları belirlenmeli ve belirlenen kurallar ivedilikle hayata geçirilmelidir.

1.2 Amaç

Bu dokümanın amacı, ülkemiz kamu kurumlarında alınması gereken asgari bilgi güvenliği kriterlerini belirlemektir.

1.3 Kapsam

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanında yer alan kriterler, ülkemizdeki tüm kamu kurumlarını kapsamaktadır.

1.4 Güncelleme

"Kamu Kurumlarının Uyması Gereken Asgari Bilgi Güvenliği Kriterleri" dokümanı ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak güncellenecektir. Ayrıca Ulusal Siber Güvenlik Politikalarında yapılacak güncellemeler, bu dokümanda güncelleme ihtiyacı doğurabilecektir.

2. Kamu Kurumlarının Sınıflandırılması

Kamu kurumlarına uygulanması gereken asgari bilgi güvenliği kriterlerini belirlemeden önce kamu kurumlarının kategorilere ayrılması ve her bir sınıfa hitap edecek asgari kriterlerin belirlenmesi gerekmektedir.

Ülkemizin kamu kurumları iki kategoriye ayrılabilir.

Her kamu kurumu, öncelikle aşağıdaki tanımları göz önünde bulundurarak hangi kategoride yer aldığına karar vermelidir.

Kritik Bilgi Sistemi:

Bir bilgi sisteminin bozulması veya yetkisiz erişimle karıştırılması halinde;

a. Enerji, su, acil yardım hizmetleri, gıda tedariki ve benzeri hayati hizmetlerin durması sonucunda can kaybı oluşması veya bazı bölgelerin boşaltılması,

b. Para piyasalarının durması, ulaştırma sistemlerinden birinin durması veya diğer nedenlerle ulusal ekonominin ciddi düzeyde zarara uğraması,

c. Ulusal güvenliğin sekteye uğraması söz konusu oluyorsa o bilgi sistemi kritiktir.

Kritik Kamu Kurumları: Bünyesinde *"**kritik bilgi sistemi**"* bulunduran kamu kurum ve kuruluşları.

Diğer Kamu Kurumları: Bünyesinde *"**kritik bilgi sistemi**"* bulundurmayan kamu kurum ve kuruluşları.

Tüm kamu kurumlarının bulunduğu listeye Başbakanlık Devlet Teşkilatı Veritabanı (http://dtvt.basbakanlik.gov.tr/AnaSayfa.aspx) internet sitesinden ulaşılabilir.

3. Uluslararası Standartlar ve Bilgi Güvenliği Kriterleri

3.1 Standartlar

Kamu kurumları için asgari bilgi güvenliği kriterleri belirlenirken, bu konuda uluslararası platformda akla gelen ilk standartlar olan ISO/IEC 27001 ve ISO/IEC 27002'den faydalanılmıştır

ISO/IEC 27001 standardı bilgi güvenliği yönetim sürecini tanımlamakta, standartta yer alan Ek-A'da ise güvenlik önlemleri ve açıklamaları özet halinde yer almaktadır.

ISO/IEC 27002 standardında ise, ISO/IEC 27001 standardı Ek-A'da yer alan güvenlik önlemlerinin detaylı açıklamaları ve iyi uygulamaları yer almaktadır. Bu standartlara ilave olarak, farklı sektörler için hazırlanmış olmakla birlikte tüm kurum ve kuruluşlara faydalı olacak güvenliği standartları da mevcuttur. NIST'in süreç kontrolü ile uğraşan ya da iletişim

sektöründe yer alan kurumlar için hazırladığı bilgi güvenliği dokümanları bu faydalı örnekler arasında gösterilebilir.

Benzer şekilde ISO/IEC 27032 Siber Güvenlik Standardı, önemi giderek artan siber güvenlik konusunda fikir verme açısından faydalıdır ISO/IEC 27002 standardının iletişim ve enerji sektörlerinde yer alan kurumlar için özelleştirilmiş güvenlik önlemlerini içeren türevleri de tüm kurumlara bilgi güvenliği konusunda fikir verebilecek dokümanlardır.

3.2 Öncelikli Güvenlik Önlemleri

ISO/IEC 27002 standardı 11 başlık altında 133 güvenlik önlemine yer vermekle birlikte, bunlardan 10 tanesinin öncelikli olduğunu belirtmektedir. Bu önlemler ISO 27002 referansları ile birlikte aşağıda belirtilmiştir:

1. Bilgi Güvenliği Politikası (5.1.1)
2. Bilgi Güvenliği Sorumluluklarının Atanması (6.1.3)
3. Bilgi Güvenliği Eğitimleri (8.2.2)
4. Yazılım Uygulamalarında Güvenlik (12.2)
5. Teknik Açıklık Yönetimi (12.6)
6. İş Sürekliliğinin Yönetilmesi (14)
7. Bilgi Güvenliği Olaylarının Yönetilmesi (13.2)
8. Veri Koruma ve Kişisel Bilgilerin Mahremiyeti (15.1.4)
9. Kurumsal Kayıtların Korunması (15.1.3)
10. Fikri Mülkiyet Hakları (15.1.2)

4. Bilgi Güvenliği Kriterleri

Bu başlık altında ülkemiz kamu kurumlarının sahip olması gereken asgari bilgi güvenliği kriterleri açıklanmaktadır. Kriterler belirlenirken 2. ve 3. bölümlerde yer alan tanım ve başlıklar esas alınmıştır.

4.1 Kamu Kurumlarının Sağlaması Gereken Kriterler

Bilgi güvenliği kriterleri bu dokümanda iki başlık altında toplanmıştır: Önlemler ve Bilgi

güvenliği süreci. Bilgi güvenliği önlemleri güvenlik duvarı, sistem odasının emniyeti, yedekleme gibi politika ve prosedürler aracılığı ile uygulanacak tedbirlerdir. Bilgi güvenliği süreci ise, önlemlerin kurumdaki risklere uygun şekilde belirlenmesini, ardından önlemlerin izlenmesini, iç tetkik ile tüm önlemlerin gözden geçirilmesini ve yönetim tarafından Düzenleyici ve Önleyici Faaliyetlerin belirlenmesini öngören bir iş sürecidir. Kamu kurumlarının sağlaması gereken kriterler belirlenirken ISO/IEC 27001 standardına ilave olarak diğer uluslararası standartlar, TÜBİTAK SGE'nin kurumsal deneyimi ve Ulusal Siber Güvenlik Tatbikatlarında elde edilen sonuçlar göz önünde bulundurulmuştur. Aşağıdaki tabloda kamu kurumlarının sağlaması gereken bilgi güvenliği kriterleri belirtilmekte, dokümanın izleyen bölümlerinde ise bu kriterler açıklanmakta ve somutlaştırılmaktadır.

4.2 Bilgi Güvenliği Süreci

Bilgi güvenliği yönetiminde kurumların odaklanması gereken esas nokta, olabildiğince çok güvenlik önleminin kurumda uygulanması değil, uygulanan güvenlik önlemlerine sahip çıkılmasıdır. ***Sahip çıkma kurum üst yönetiminin bilgi güvenliğini kurumsal bir süreç olarak benimsemesi***, süreci oluşturan adımları gerçekleştirmek için gereken insan kaynağını ve maddi kaynağı sağlaması ile mümkün olabilmektedir.

Bilgi güvenliğine sahip çıkma, aynı zamanda ISO/IEC 27001 standardında tarif edilen "Risk Analizi ve Tedavisi", "İç Tetkik ve Gözden Geçirme", ve "Düzeltici/Önleyici Faaliyetler" adımlarının gerçekleştirilmesi ile mümkün olabilmektedir.

Risk Analizi ve Tedavisi

Kurum, çalıştırdığı bilgi kritik sistemleri başta olmak üzere bilgi varlıklarını belirler, bu bilgi varlıklarında bulunan açıklıkları ve bu açıklıklara yönelebilecek tehditleri değerlendirir. Gerçekleştirilen değerlendirme sonucunda risk tedavisini gerçekleştirir. Risk analizi ve tedavisi işlemi yılda bir kez tekrarlanır.

İç Tetkik ve Gözden Geçirme

Bilgi güvenliği süreci uyarınca yapılan çalışmalar yılda bir kez kurum yönetimi tarafından atanan ve bilgi güvenliği çalışmalarına katılmayan tetkikçiler tarafından denetlenir. İç tetkik

sonucu bir rapor halinde kurum yönetimine arz edilir ve kurum yönetimi tarafından değerlendirilir.

Kurum yönetimi iç tetkik sonucunu ve diğer verileri değerlendirerek bilgi güvenliği sürecini kapsam, etkinlik, yasal yükümlülüklere uyum ve benzeri açılardan değerlendirir, gerçekleştirilmesi gereken düzeltici ve önleyici faaliyetleri belirler.

Düzeltici/Önleyici Faaliyetler

Yönetim gözden geçirmesi ve benzeri mekanizmalar tarafından belirlenen sorunların tekrar etmemesi için "kök sebep"ler belirlenir ve bu kök sebeplerin ortadan kaldırılması için düzeltici faaliyet gerçekleştirilir. Diğer kurumların yaşadığı sorunlar veya değişen riskler göz önünde bulundurularak önleyici faaliyetler belirlenir ve gerçekleştirilir. Düzeltici/önleyici faaliyetler kayıt altına alınır ve koyulan güvenlik hedeflerini sağlama açısından takip edilir.

5. Genel Değerlendirme ve Sonuç

20.10.2012 tarihli Resmi Gazete'de yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile 5809 sayılı Elektronik Haberleşme Kanunun eklenen EK MADDE 1 – (Ek: 6.2.2014-6518/106 md.) çerçevesinde Siber Güvenlik Kurulu'nun kurulmuş olması, ülkemiz için büyük bir kazanç olarak değerlendirilmektedir. Bu Karar ve Kanun, ülkemiz siber güvenliği olgunluk seviyesinin gelişmiş ülkelerin seviyesine çıkmasına vesile olacaktır. Bu adımın atılmasına müteakip hazırlanan eylem planı ise bu kapsamda itici güç arz etmektedir. Eylem planındaki maddelerin gerçekleştirilmesiyle, ülkemizin siber güvenlik konusunda dünyada başı çeken ülkelerden birisi olması kaçınılmazdır.

Eylem Planı uyarınca hazırlanan bu dokümanda, ülkemiz kamu kurumlarının uyması gereken asgari bilgi güvenliği kriterleri belirlenmiştir. Bu kapsamda öncelikle kamu kurumları kendi içlerinde sınıflandırılmış, kritik bilgi sistemi bulunan ve bulunmayan kamu kurumlarının sağlaması gereken kriterler belirlenmiştir. Bilgi güvenliği kriterleri belirlenirken uluslararası alanda en çok kullanılan bilgi güvenliği standartlarından ve TÜBİTAK SGE'nin kurumsal birikiminden faydalanılmıştır. Bu arada, bilgi güvenliği standartlarının yaşayan dokümanlar

olduğu da unutulmamalıdır. Örneğin ISO 27001 Bilgi Güvenliği Yönetim Sistemi Gereksinimleri standardının güncellenmesi beklenmektedir

Bu dokümanda belirlenen bilgi güvenliği önlemlerinin ve yapılandırmalarının, kamu kurumlarının sınıflandırılmasının ardından, ivedilikle hayata geçirilmesinin, ülkemiz siber güvenliğine katkı yapması beklenmektedir.

Son olarak, asgari güvenlik önlemlerinin kurumdaki belli başlı açıklıkları kapatma konusunda etkili olacağı, ancak bütün açıkların kapatılmasını *sağlamayacağı* unutulmamalı, kurumsal bilgi güvenliğinin en üst düzeyde gerçekleştirilmesi gereken noktalarda detaylı risk analizini ve tedavisini içeren bilgi güvenliği süreçleri oluşturulmalı ve çalıştırılmalıdır.[51]

4.7 Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ

BİRİNCİ BÖLÜM
Amaç ve Kapsam

MADDE 1 − (1) Bu Tebliğin amacı ve kapsamı, Siber Olaylara Müdahale Ekiplerinin kuruluş, görev ve çalışmalarına ilişkin usul ve esaslarını belirleyerek, hizmetlerin etkin ve verimli bir şekilde yürütülmesini sağlamaktır.

Dayanak
MADDE 2 − (1) Bu Tebliğ, 20.10.2012 tarihli ve 28447 sayılı Resmî Gazete'de yayımlanan 2012/3842 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Kararın 5 inci maddesinin birinci fıkrasının (ç) bendi ile üçüncü fıkrası ve 25.3.2013 tarihli ve 2013/4890 sayılı Bakanlar Kurulu Kararıyla yürürlüğe konulan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi ve 655 sayılı Ulaştırma, Denizcilik ve Haberleşme Bakanlığının Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararnamenin 29 uncu

maddesinin yedinci fıkrası ile 30 uncu maddesine dayanılarak hazırlanmıştır.

Tanımlar
MADDE 3

(1) Bu Tebliğde geçen;

a) Bilişim Sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmet, işlem, veri ve bunların sunumunda yer alan sistemleri,

b) Endüstriyel Kontrol Sistemi: Geleneksel bilişim teknolojileri dışında, programlanabilir mantıksal denetleyiciler aracılığı ile üretim, ürün işleme ve dağıtım kontrolleri gibi endüstriyel işlemler için kullanılan bilgi sistemleridir. Bu sistemler Veri Tabanlı Merkezi Kontrol ve Gözetleme Sistemi (SCADA) ile coğrafi olarak Dağınık Kontrol Sistemleri (DKS) şeklinde gruplanmaktadır.

c) Kritik Altyapılar: İşlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran altyapıları,

ç) Kritik Sektörler: Kritik altyapıları bünyesinde barındıran sektörleri,

d) Kurul: Siber Güvenlik Kurulunu,

e) Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya teşebbüste bulunulmasını,

f) Siber Olaya Müdahale: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemlerde tutulan veya işlenen verilerin gizlilik, bütünlük ve erişilebilirliğinde meydana gelme riski

bulunan veya meydana getiren siber olayın kaynağını, nedenlerini ve sonuçlarını tespit ederek siber olayın devam etmesini, tekrarını veya zarar vermesini önleyen çalışmaları,

g) SOME: Siber Olaylara Müdahale Ekibini,

ğ) USOM: Ulusal Siber Olaylara Müdahale Merkezini, ifade eder.

İKİNCİ BÖLÜM

SOME'lerin Kuruluşu, Yapısı, Görev ve Yükümlülükleri, USOM'la İlişkileri

Kurumsal SOME'lerin Kuruluşu

MADDE 4

(1) Kurumsal SOME'ler Bakanlıkların bünyesinde, hizmet gereklerine göre, Bakanlık birimlerini, bağlı, ilgili ve ilişkili kurumlarını kapsayacak şekilde kurulur. Ancak Bakanlık koordinesinde Bakanlık birimleri, bağlı, ilgili ve ilişkili kurum ve kuruluşları altyapılarının önem ve büyüklüğüne göre kendi bünyelerinde bir kurumsal SOME kurabilirler.

(2) Diğer tüm kamu kurum ve kuruluşları kendi bünyelerinde kurumsal SOME kurabilirler.

(3) Bakanlıkların merkez birimleri, bağlı, ilgili ve ilişkili kurum ve kuruluşlarının yanı sıra 10.12.2003 tarihli ve 5018 sayılı Kamu Malî Yönetimi ve Kontrol Kanununa ekli I, II, III ve IV sayılı cetvellerde yer alan kurum ve kuruluşlar da kendi bünyelerinde kurumsal SOME kurabilirler.

(4) Kurumsal SOME'lerin kuruluşunun eşgüdümü Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından yürütülür.

(5) Sektörel SOME'lerin bulunduğu sektörlerdeki özel kurumlar ve diğer kuruluşlar kendi bünyelerinde kurumsal SOME kurabilirler.

Kurumsal SOME'lerin Görev ve Sorumlulukları

MADDE 5

(1) Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler.

(2) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar.

(3) Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini varsa birlikte çalıştığı sektörel SOME ile eşgüdüm içerisinde yürütürler. Durumdan gecikmeksizin USOM'u haberdar ederler.

(4) Kurumsal SOME'ler bir siber olayla karşılaştıklarında, USOM ve birlikte çalıştığı sektörel SOME'ye bilgi vermek koşulu ile öncelikle söz konusu olayı kendi imkân ve kabiliyetleri ile bertaraf etmeye çalışırlar. Bunun mümkün olmaması halinde varsa birlikte çalıştığı sektörel SOME'den ve/veya USOM'dan yardım talebinde bulunabilirler.

(5) Kurumsal SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.

(6) Kurumsal SOME'ler kurumlarına yapılan siber olayları raporlar ve gecikmeksizin USOM ve birlikte çalıştığı sektörel SOME'ye bildirirler.

(7) Kurumsal SOME'ler USOM ve/veya birlikte çalıştığı sektörel SOME tarafından iletilen

siber olaylara ilişkin alarm, uyarı ve duyuruları dikkate alarak kurumlarında gerekli tedbirleri alırlar.
(8) Kurumsal SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştığı sektörel SOME'lere ve USOM'a bildirirler.

Sektörel SOME'lerin Kuruluşu

MADDE 6

(1) Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulur.
(2) İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde sektörel SOME kurulabilir.
(3) Kritik sektörlerde, sektörel SOME kurulması zorunludur. Kritik sektörlerin listesi Kurul tarafından belirlenir, ilgililere duyurulur ve güncellenir.
(4) Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümü Bilgi teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülür.

Sektörel SOME'lerin Görev ve Sorumlulukları

MADDE 7

(1) Sektörel SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik faaliyetlerini USOM'la koordineli şekilde yürütürler.
(2) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olayları gecikmeksizin USOM'a bildirirler.
(3) Sektörel SOME'ler siber olaylara ilişkin USOM tarafından iletilen alarm, uyarı ve duyuruları dikkate alarak birlikte çalıştıkları SOME'lerde gerekli tedbirlerin alınmasına yönelik çalışmaları yürütürler.

(4) Sektörel SOME'ler birlikte çalıştıkları SOME'lerin yapılanması konusunda düzenleyici faaliyetleri yürütürler.
(5) Sektörel SOME'ler ilgili oldukları sektörde, bilgilendirme, bilinçlendirme ve eğitim faaliyetleri ile siber güvenlikle ilgili kabiliyetlerinin geliştirilmesi ve önlemlerin alınması konusunda gerekli düzenleyici faaliyetleri yürütürler.
(6) Sektörel SOME'ler 7/24 erişilebilir olan iletişim bilgilerini belirleyerek birlikte çalıştıkları SOME'lere ve USOM'a bildirirler.
(7) SOME'ler 7/24 erişilebilir olan iletişim bilgilerini Sektörel SOME'lere ve USOM'a bildirirler.
(8) Sektörel SOME'ler birlikte çalıştıkları SOME'lerde yaşanan siber olaylarda imkânları ölçüsünde gerekli desteği sağlarlar. Sektörel SOME'ler, imkânlarının yetersiz olması durumunda USOM'dan destek alırlar.
(9) Sektörel SOME'ler siber olaya müdahale ederken suç işlendiği izlenimi veren bir durumla karşılaştıklarında gecikmeksizin durumu kanunen yetkili makamlara bildirirler. Durumu gecikmeksizin USOM'a da bildirirler.
(10) Sektörel SOME'ler gerekmesi durumunda birlikte çalıştıkları SOME'ler arasındaki işbirliğini koordine ederler.

Kurumsal ve Sektörel SOME'lerin Yapısı
MADDE 8

(1) SOME'lerin Bakanlık ve diğer kurumlar içinde nasıl yapılandırılacağı, hangi birim içinde çalışacağı, Bakanlığın veya kurumun diğer birimleri ile ilişkileri, bilişim ve endüstriyel kontrol sistemlerinin yapısı da dikkate alınarak ilgili Bakanlık veya kurum tarafından belirlenir ve kurum içerisinde uygun yöntem ile duyurulur.

(2) SOME'ler kurumların bilişim ve endüstriyel kontrol sistemlerinin büyüklük ve kritikliği dikkate alınarak meydana gelebilecek siber olaya müdahale edebilecek yeterlilikte personel ve teçhizatla desteklenirler.

(3) SOME'ler; bilgi güvenliği, bilişim ağları, yazılım ve sistem uzmanlığı gibi alanlarda bilgili ve tecrübeli personel öncelikli olmak üzere ilgili bakanlık ve kurumların belirleyeceği personelden teşkil edilir.

(4) Mevcut ve olası siber olayların niteliği ve yoğunluğuna göre USOM tarafından bu yapıların geliştirilmesi önerilebilir.

(5) SOME'ler iletişim kanallarını 7/24 açık tutarlar.

(6) SOME'ler siber olaylara imkânları dâhilinde 7/24 esasına göre müdahale ederler.

(7) SOME'ler, ilgili kurumların teşkilat yapılarına ve hizmet gereklerine göre farklı birim personelinden oluşturulabilir.

SOME'lerin USOM'la İlişkisi
MADDE 9

(1) SOME'lerin USOM ile ilişkilerini varsa birlikte çalıştıkları sektörel SOME'ler üzerinden yürütmesi esastır.

(2) Birlikte çalıştıkları bir sektörel SOME olmayan kurumsal SOME'ler, faaliyetlerini doğrudan USOM ile koordineli yürütürler.

(3) Siber olaylar ile ilgili olarak diğer ülkelerin eşdeğer makamları ve uluslararası kuruluşlarla işbirliği USOM tarafından yerine getirilir.

(4) USOM gerekli gördüğü durumlarda kurumsal SOME'ler ve sektörel SOME'ler ile doğrudan çalışma yürütebilir.

(5) Kurumsal/Sektörel SOME'ler siber olayların tespiti, önlenmesi, zararlarının en aza

indirilmesi gibi konularda USOM tarafından geliştirilen veya yürütülen projelerin gerçekleştirilmesinde USOM ile işbirliği içerisinde hareket ederler.

Eğitim

MADDE 10

(1) Kurumsal SOME'ler, USOM ve/veya birlikte çalıştıkları sektörel SOME'lerin planladığı eğitimlere katılım sağlar.

(2) Sektörel SOME'ler, USOM'un planladığı eğitimlere katılım sağlar.

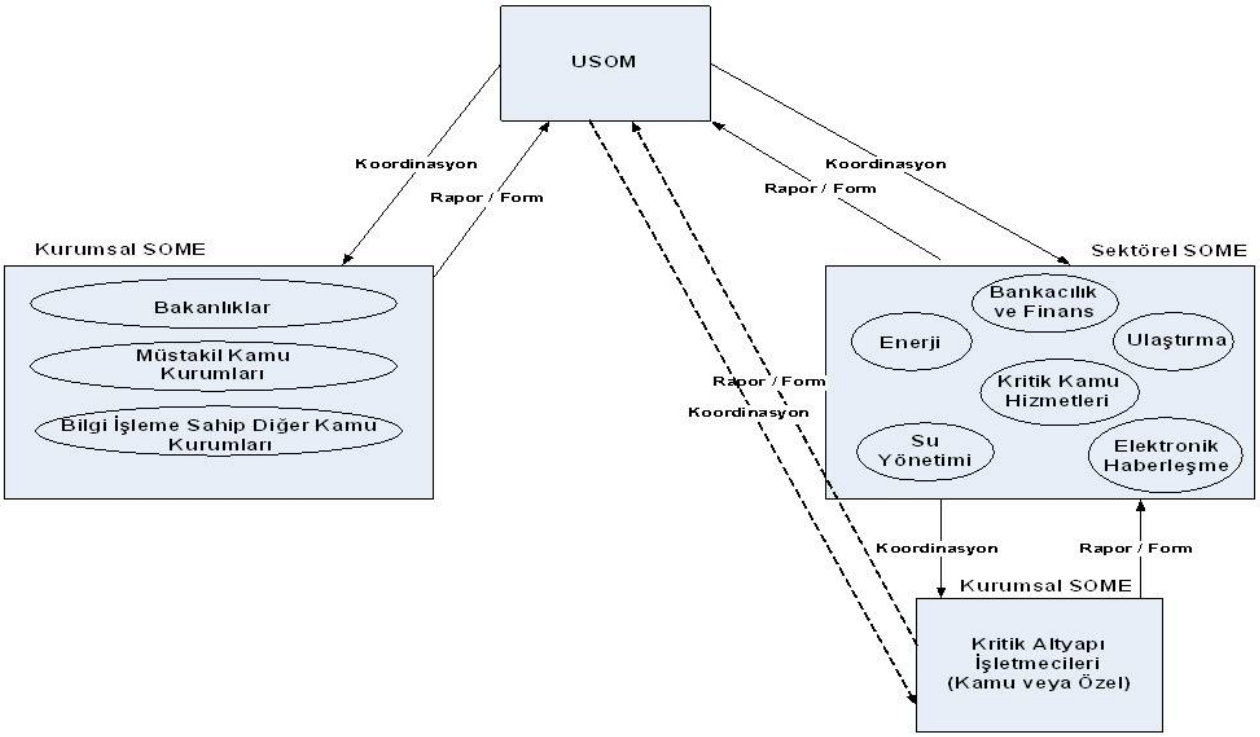
USOM, ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına kurulmuştur. İnternet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilecektir.

Siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri de yapacak olan USOM, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlayacaktır.

USOM'a bağlı olarak çalışacak, sektör ve kurum bazında kurulacak olan Siber Olaylara Müdahale Ekipleri'nin kısaltmasıdır. Sektörleri yönetecek somelere SEKTÖREL SOME, Kurumları yönetecek somelere ise KURUMSAL SOME ile adlandırılmaktadır. Sektörel ve Kurumsal SOME'ler kendi aralarında ve USOM ile koordinasyon ve işbirliği içindedir.

Sektörel SOME'ler düzenleyici ve denetleyici kurumların bünyesinde kendi sektörlerinde faaliyet gösteren kurum, kuruluş ve işletmeleri kapsayacak şekilde kurulur. İhtiyaç duyulması halinde, düzenleyici ve denetleyici kurumların yetki alanı dışında kalan diğer sektörlerde ilgili olduğu Bakanlık bünyesinde sektörel SOME kurulabilir. Kritik sektörlerde, sektörel SOME

kurulması zorunludur. Kritik sektörlerin listesi Kurul tarafından belirlenir, ilgililere duyurulur ve güncellenir. Düzenleyici ve denetleyici kurumlardaki sektörel SOME'lerin eşgüdümü Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yürütülür.



Şekil-24: USOM-SOME

Kurumsal SOME'ler kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapmak veya yaptırmakla yükümlüdürler. Kurumsal SOME'ler, siber olayların önlenmesi veya zararlarının azaltılmasına yönelik olarak, kurumlarının bilişim sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda öneri sunarlar. [52]

USOM internet sitesine http://www.usom.gov.tr/ adresinden ulaşılabilmektedir.

Siber Güvenlik Kurulu

MADDE 11

(1) Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma, Denizcilik ve Haberleşme Bakanının başkanlığında Dışişleri, İçişleri, Milli Savunma, Ulaştırma Denizcilik ve Haberleşme Bakanlıkları Müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur.

Bakanlar Kurulu Kararı ve Siber Güvenlik Kurulunun Kuruluşu

Bakanlar Kurulunca alınan 11.6.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20.10.2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Söz konusu Bakanlar Kurulu Kararı uyarınca; "Siber güvenlikle ilgili olarak alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Ulaştırma Denizcilik ve Haberleşme Bakanının başkanlığında, Dışişleri, İçişleri, Milli Savunma, Ulaştırma Denizcilik ve Haberleşme bakanlıkları müsteşarları, Kamu Düzeni ve Güvenliği Müsteşarı, Milli İstihbarat Teşkilatı Müsteşarı, Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşan Siber Güvenlik Kurulu kurulmuştur.

5809 sayılı Kanun maddesine aşağıdaki Siber güvenlik Kurulu ile ilgili "EK MADDE 1" eklenmiş ve 19.02.2014 tarihli ve 28918 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir.

(1) Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir.

(2) Kurulun görevleri şunlardır:

a. Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak.

b. Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak.

c. Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek.

ç. Kanunlarla verilen diğer görevleri yapmak.

(3) Siber Güvenlik Kurulunun çalışma usul ve esasları Başbakanlıkça çıkartılacak yönetmelikle belirlenir.

Siber Güvenlik Kurulu Toplantıları

Bakanlar Kurulu Kararı ile oluşturulan Siber Güvenlik Kurulu'nun ilk toplantısı 21.12.2012 tarihinde; Ulaştırma, Denizcilik ve Haberleşme Bakanı Binali Yıldırım'ın başkanlığında yapılmıştır. Toplantıya; Dışişleri, İçişleri, Milli Savunma, Ulaştırma, Denizcilik ve Haberleşme Bakanlıkları, Kamu Düzeni ve Güvenliği ile MİT müsteşarları, Genelkurmay Bakanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı, Bilgi Teknolojileri ve İletişim Kurumu Başkanı, Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı, Mali Suçları

Araştırma Kurulu Başkanı, Telekomünikasyon İletişim Başkanı ile Ulaştırma Denizcilik ve Haberleşme Bakanlığı yetkilileri katılmıştır.

20.12.2012 tarih ve 2012/1 sayılı Kararda "Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesi" ile "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı"nın yürürlüğe konulmuştur. Kararın ekinde 5 karar yer almıştır:

1.Kamu kurum ve kuruluşlarının güvenli bir ağ üzerinden haberleşmesi konusunda, Haberleşme Genel Müdürlüğü tarafından çalışma başlatılması,

2.İnternet Değişim Noktalarının yurtiçinde oluşturulması için alınması gereken tedbirleri ve çözüm önerilerini de içeren hususlarda Haberleşme Genel Müdürlüğü ile Bilgi Teknolojileri ve İletişim Kurumu tarafından bir raporun hazırlanması,

3.2007 yılında NATO ile TÜBİTAK arasında imzalanan Siber Savunma Mutabakat Muhtırasının Genelkurmay Başkanlığı tarafından güncellenerek Bakanlığımız koordinasyonu ile imzalanması,

4.Siber güvenlik terminolojisi ve sözlüğünün oluşturulmasının Eylem Planı içerisinde yer alması,

5.Siber Güvenlik Kurulunca oluşturulacak alt çalışma gruplarında kurumların karar almaya yetkili temsilcilerinin katılımının sağlanması.[53]

4.8 Siber Güvenlik İnisiyatifi

Siber Güvenlik İnisiyatifi; İnternet Geliştirme Kurulu çatısı altında, sektör paydaşlarının katılım sağladığı ve hedefi siber güvenlik alanında çalışmalar yaparak, tüm paydaşların görüşlerini toplayarak, kurumlar arasında fikir alışverişini ve işbirliğini sağlayarak, ortak fikirler ortaya çıkararak, yaptığı çalışmaları Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'na sunmaktır. Siber Güvenlik İnisiyatifinin faaliyetlerinden bazıları; vatandaş ve küçük işletmeleri siber güvenlik konusunda bilinçlendirme, farkındalık oluşturma, koruma tedbirlerini oluşturma ve anlatma, pozitif içerik üretimi, veri merkezlerinin

ISS'lerin minimum güvenlik kriterlerini belirleme, sektörel risk analizi, siber güvenlik standartlarını belirleme, raporlar ve kılavuzlar yayınlamak olarak sıralanabilir. [54]

Siber Güvenlik İnisiyatifi Çalışma Grupları

1. Farkındalık, Eğitim ve Rapor Çalışma Grubu
- **a.** Ev Kullanıcıları için Farkındalık ve Eğitim
- **b.** Öğrenciler için Farkındalık ve Eğitim
- **c.** KOBİ'ler için Farkındalık ve Eğitim
- **d.** Kamu Kurumları ve Kurumsal İşletmeler için Farkındalık
- **e.** ISS ve Veri Merkezleri için Farkındalık

2. Siber Olaylarla ilgili Mevzuat ve Koordinasyon Çalışma Grubu
- **a.** Mevzuat
- **b.** Kamu, Özel Sektör İşbirliği ve Uluslararası Koordinasyon
- **c.** Adli Bilişim ve Delillendirme (auditing)
- **d.** Adli Makamlar ve Kolluk Kuvvetleri ile Koordinasyon

3. Ulusal Siber Olaylara Müdahale Organizasyonu Çalışma Grubu
- **a.** SOME'lerin Yapısı ve Buralarda Çalışacak Personel Nitelikleri
- **b.** Kritik Altyapılarda Bilgi Güvenliği Yönetimi
- **c.** Risk Analizi ve Acil Eylem Planları Hazırlanması
- **d.** Siber Tatbikatlar

4. Teknik Araştırmalar ve Standartlar Çalışma Grubu
- **a.** Network Güvenliği ve Ürünlerin Sertifikasyonu
- **b.** İşletim Sistemleri ve Güvenlik Seviyesinin Belirlenmesi
- **c.** Yazılım Güvenliği ve Standartlarının Belirlenmesi
- **d.** Mobil Cihazlar Güvenlik
- **e.** Bulut Bilişim Standartları
- **f.** Veri Merkezleri İçin Standardizasyon Çalışması Yapılması

5. Siber Tehditlerle Mücadele Çalışma Grubu

Siber Güvenlik İnisiyatifi Üyeleri

	KURUM
1	Kaspersky Lab
2	PricewaterhouseCoopers Türkiye
3	Adeo
4	Netaş
5	Isaca Istanbul
6	Merkezi Kayıt Kuruluşu
7	Eset Türkiye
8	KPMG Türkiye
9	BT Yön
10	Accenture
11	Turktrust
12	Issa Türkiye
13	Bilgi Güvenliği Akademisi
14	IDC Türkiye
15	Oracle Türkiye
16	Comodo Türkiye
17	Websense Türkiye
18	Bilge Adam
19	Paloaltonetworks Türkiye
20	Ernst&Young Türkiye
21	Dataserv Bilgi Teknolojileri
22	Symantec Türkiye
23	Deloitte Türkiye
24	Ericsson Türkiye
25	Google Türkiye
26	Koçsistem
27	Cisco Türkiye
28	Panda Security Türkiye
29	Bilgi Güvenliği Derneği
30	IPTV Derneği
31	TÜBİDER
32	EDER
33	Bilişim Güvenliği ve Bilişim Suçlarına Karşı Müdahele Derneği
34	Turkcell
35	TTNET
36	TUDOF
37	Grid Telekom
38	Vodafone İletişim Hizmetleri ve Vodafone Net
39	MOBİSAD
40	TESİD
41	YASAD
42	Kredi Kayıt Bürosu
43	TİEV
44	Millenicom
45	Huawei Türkiye

46	Lostar Bilgi Güvenliği
47	Türk Telekom
48	TÜBİSAD
49	TÜTED
50	ZTE Türkiye
51	TİD
52	Avea
53	MOBİLSİAD
54	Superonline
55	Microsoft Türkiye
56	İnternet Medya ve Bilişim Federasyonu
57	Turksat
58	Bilgisayar Mühendisleri Odası
59	Trendmicro
60	Biznet Bilişim
61	Dsmart
62	Webrazzi

Tablo-2: Siber Güvenlik İnisiyatifi Çalışma Grubu

4.9 Tatbikatlar

BTK tarafından yürütülen siber güvenlik ile ilgili çalışmaların en önemlileri arasında siber güvenlik tatbikatları yer almaktadır. Siber güvenliğin sağlanmasına yönelik girişimler içerisinde uzmanlık seviyesinin geliştirilmesi, bilgi güvenliği standartlarının uygulanması ve kullanıcı eğitimlerinin yanı sıra, siber güvenlik konusunda farkındalığın arttırılmasına yönelik çalışmalarda siber güvenlik tatbikatları önemli bir yer tutmaktadır.

Tatbikatların amacı;

- Katılımcıların siber saldırılara karşı koyma yeteneklerini geliştirmeyi,
- Katılımcıların siber saldırılara karşı kurum içi ve kurumlar arası koordinasyonlarını geliştirmeyi,
- Siber güvenlik konusunda ulusal farkındalık seviyesini arttırmayı hedeflemektedir.

Farkındalık Çalışmaları

Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 23. maddesi kapsamında ve kurumların talepleri doğrultusunda siber güvenlik konusunda farkındalığın arttırılması amacıyla sunumlar yapılmaktadır. Söz konusu sunumlarda;

- Kamu kurum ve kuruluşları bünyesinde tutulan verilerin veya kurumsal alanda gizli kalması gereken verilerin güvenliğinin sağlanması hususlarında bilgilendirmeler yapılmakta, dünyada bu konulardaki genel eğilim,
- Kurumumuzun düzenleme ve denetleme yetkisinde olan elektronik haberleşme sektörüne yönelik siber güvenlik mevzuat çalışmaları,
- Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının 4 üncü maddesi ile kurulan Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) yapısı ve faaliyetleri anlatılmaktadır.

4.10 Projeler

Bilgi Teknolojileri ve İletişim Kurumu tarafından siber güvenliğin sağlanmasına yönelik olarak son yıllarda yürütülmekte olan çalışmalar, 5809 sayılı Elektronik Haberleşme Kanunu ile kendisine verilen yetkilere dayanmakta ve BTK'nın ülkemizi temsilen üyesi bulunduğu Uluslararası Telekomünikasyon Birliği'nin (ITU) çalışmalarına paralellik arz etmektedir.

Uluslararası Telekomünikasyon Birliği, Telekomünikasyon Standardizasyon Sektörü (ITU-T) Çalışma Grubu 17'nin (SG17), 2013-2016 çalışma periyodundaki birinci toplantısı 17-26 Nisan 2013 tarihleri arasında, ikinci toplantısı 26 Ağustos 2013 - 4 Eylül 2013 tarihleri arasında, üçüncü toplantısı 15-24 Ocak 2014 tarihleri arasında İsviçre'nin Cenevre kentinde yapılmıştır.

20 Ekim 2012 tarihinde yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar" ile Türkiye'de siber güvenliğin ulusal düzeyde koordinasyonunun sağlanması konusunda önemli adım atılmıştır.

Projeler

- **Siber Tehditleri Önleme Projesi (STOP)**

  Siber tehditleri tespit amacıyla bal küpü sistemi kurulması, siber saldırı raporlama sisteminin kurulması ve geliştirilmesi, siber tehditlerle ilgili veri üretilmesi ve siber tehditlerin önlenmesine ilişkin gerekli mekanizmaların geliştirilmesine yönelik bir projedir.

- **Spam E-postalarla Mücadele Projesi**

  2009 yılında BTK önderliğinde internet servis sağlayıcı ve yer sağlayıcı firmaların katılımıyla birlikte, siber güvenliğe yönelik tehdit oluşturan ve internet kaynaklarını gereksiz meşgul eden istem dışı e-postaların engellenmesine yönelik bir pilot proje yürütülmüştür.

  Söz konusu pilot projenin başarılı olması sonrasında ise öngörülen Çözüm tüm Türkiye geneline 3 faz halinde yaygınlaştırılmıştır.

  Proje sonrasında, istem dışı e-posta yayan **IP sayısı % 99** oranında azalmış, istem dışı e-posta yayan ülkeler sırlamasında ülkemiz gerilere düşmüş, dolayısıyla uluslararası alanda imajı güçlendirilmiştir. [55]

5.SİBER GÜVENLİK STANDARTLARI

5.1 Temel Güvenlik Standartları

5.1.1 Ortak Kriterler

Okbs Genel Bakış

Ortak Kriterler bilgi teknolojileri ürün ve/veya sistemlerinin güvenlik seviyelerinin tespit edilmesi ve bağımsız laboratuvarlarda test edilebilmesi için geliştirilmiş olan, temelini TCSEC ve ITSEC standartlarından alan ve Uluslararası Standartlar Organizasyonu'nun (ISO) 1999 yılında Uluslararası Bilgi Teknolojileri Güvenlik Değerlendirme Standardı olarak kabul ettiği (ISO 15408) güvenlik standardıdır. Türkiye Eylül 2003 tarihinde bu standardı kabul eden ülkelerin imzaladığı Ortak Kriterler Tanıma Sözleşmesini imzalayarak sertifika üretici ülkelerin değerlendirmelerini kabul etmiş, TSE Belgelendirme Merkezi bünyesinde kurulan Ortak Kriterler Belgelendirme Sistemini hayata geçirmiştir.

Ortak kriterler birbirleriyle ilişkili üç ayrı bölümden oluşmaktadır.

Ortak Kriterler Standartı

Ortak Kriterler standardı üç (3) bölümden oluşmaktadır. Birinci bölümde Ortak Kriterler standardına giriş yapılır ve genel model anlatılır. İkinci bölümde BT ürünü veya sistemi güvenlik gereksinimleri belirlenirken kullanılacak ve genel bir dil oluşturulması için Ortak Kriterler formatından belirtilmiş güvenlik fonksiyonel gereksinimleri bulunmaktadır. Üçüncü bölümde ürünün veya sisteminin garanti iddiasının belirlenebilmesi için Ortak Kriterler formatından belirtilmiş güvenlik garanti gereksinimleri bulunmaktadır.

Bölüm 1, Giriş ve Genel Model, Ortak kriterlere giriş niteliğindedir. Bu bölüm BT güvenlik değerlendirmelerinin temel konsept ve prensiplerini tanımlar niteliktedir ve genel bir değerlendirme modeli sunmaktadır. Bölüm aynı zamanda BT güvenlik hedeflerinin oluşturulması, BT güvenlik gereksinimlerinin seçilmesi ve tanımlanması ve ürünlerin veya sistemlerin üst düzey spesifikasyonlarının yazılması konusunda bilgiler içermektedir. Ayrıca

standardın bütün bölümlerinin bütün potansiyel kullanıcılar için nasıl kullanılacağı bu bölümde tanımlanmaktadır.

Bölüm 2, Güvenlik Fonksiyonel Gereksinimleri, değerlendirme hedefinin güvenlik fonksiyonel gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik fonksiyonel bileşenleri kümesi bu bölümde listelenmektedir. Standardın ikinci bölümü fonksiyonel bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır.

Bölüm 3, Güvenlik Garanti Gereksinimleri, değerlendirme hedefinin güvenlik garanti gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik garanti bileşenleri kümesi bu bölümde listelenmektedir. Standardın üçüncü bölümü garanti bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır. Bu bölüm aynı zamanda Koruma Profillerinin ve Güvenlik Hedeflerinin değerlendirme kriterlerini ve değerlendirme garanti seviyelerini oluşturan garanti bileşenlerini de içermektedir.

Ortak kriterlerin bu üç bölümünün desteklenmesi açısından teknik gerekçeleri ve kılavuz dokümanlarını da içeren birçok doküman yayınlanmıştır. [56]

Neden Ortak Kriterler Kullanılmalıdır?

Ortak Kriterler, Kanada, Fransa, Hollanda, İngiltere, Almanya ve Amerika Birleşik Devletleri' nin ulusal güvenlik organizasyonları ve standartlar enstitüleri ile birlikte ortak bir çalışma sonucunda hazırlanmıştır ve bu ülkelerde kullanılan güvenlik değerlendirme kriterlerinin yerine kullanılması amaçlanmıştır. Ulusal organizasyonlar, Uluslararası Standartlar Örgütü (ISO) ile birlikte çalışarak Ortak Kriterlerin biçimsel bir standart haline getirilmesini sağlamıştır. Sonuç olarak Ortak Kriterlerin 2.1 sürümü ISO tarafından ISO 15408 olarak kabul edilmiştir. ISO'nun Ortak Kriterleri kabul etmesiyle bu standart dünyada güvenlik spesifikasyonları ve değerlendirmelerinde yaygın olarak kullanılmaya başlanmıştır.

5.1.1.1 Ortak Kriter Uygulamaları

Ortak Kriterler genelde aşağıdaki durumlarda kullanılır ve uygulanır.

Bir ürünün veya sistemin güvenlik özelliklerinin tespit ederken,

Bir ürün veya sistem için güvenlik özellikleri eklerken,
Bir ürünün veya sistemin güvenlik özelliklerini değerlendirirken,
Güvenlik özellikleri olan bir ürün veya sistem satın alınırken.

5.1.1.2 Türkiye'de Ortak Kriterler Yapısı ve Faaliyetler

Uluslararası alanda Ortak Kriterler yapısı, ülkede var olan bir sertifikasyon makamı ve ona bağlı lisanslı Ortak Kriterler laboratuvarı/laboratuvarları tarafından sağlanmaktadır.
Ülkemizde de benzer şekilde bir yapı mevcuttur. Sertifikasyon Makamı olarak Türk Standartları Enstitüsü (TSE, www.tse.org.tr), lisanslı Ortak Kriterler laboratuvarı olarak TÜBİTAK-UEKAE OKTEM (Ortak Kriter Test Merkezi) görev almaktadır. Her bir proje sonucunda, test edilen BT ürününe veya sistemine ilişkin TÜBİTAK-UEKAE OKTEM tarafından hazırlanan Değerlendirme Teknik Raporu, TSE'ye gönderilir. TSE yetkili teknik personelleri değerlendirme teknik raporunu değerlendirir ve sonucun olumlu olması durumunda ilgili BT ürünü veya sistemini Ortak Kriterler standardına uygun olarak sertifikalandırır.

Mevcut durumda OKTEM, ülkemizde TSE tarafından lisanslı tek Ortak Kriterler laboratuvarıdır. OKTEM, 1 yıllık periyotlarla TSE tarafından Ortak Kriterler Belgelendirme Sistemi'ne uygun olarak ve Türk Akreditasyon Kurumu (TÜRKAK) tarafından ISO 17025 standardına uygun olarak denetlenmektedir.

OKTEM, şu ana kadar 7 (yedi) BT ürününün Ortak Kriterler değerlendirmesini tamamlamıştır. Bu ürünler ve ilgili garanti iddiaları aşağıda belirtilmiştir.[57]

Ürün Adı	Garanti İddiası
Silgi Yazılımı v1.0	EAL 1
ISDN Configuration Management Center Yazılımı v1.0.1	EAL 4

ISDN Configuration Management Center Yazılımı v1.0.2	EAL 4
AKİS Yazılımı v1.0	EAL 4+ (ALC_DVS.2)
EGA Sertifika Tanzim ve Yönetim Bileşeni Yazılımı v 0.0.2.19	EAL 3+ (AVA_VAN.3, ADV_TDS.3, ADV_IMP.1, ADV_FSP.4, ALC_TAT.1)
LABRİS Güvenlik Duvarı Yönetim Merkezi Yazılımı v1.6.7.b	EAL 4+ (ALC_FLR.2)
Elektronik Sertifika Yönetim Altyapısı v 1.0	EAL 4+ (ALC_FLR.2)

Tablo-3: Ortak Kriterler değerlendirmesini tamamlanan ürünler

OKTEM'de Ortak Kriterler değerlendirmesi devam eden ürünler ve ilgili garanti iddiaları aşağıda belirtilmiştir.

Ürün Adı	**Garanti İddiası**
AKİS V1.2i	EAL 4+ (AVA_VAN.5)
AKİS V1.2n	EAL 4+ (AVA_VAN.5)
Ulusal Akıllı Kart Tüm Devresi (UKT23T64H4) sürüm 4	EAL 5+ (ALC_DVS.2)
Kurumsal Kart Erişim Cihazı (KEC) Uygulama Yazılımı sürüm 1.26.03	EAL 4+ (ALC_DVS.2)

Tablo-4: Ortak Kriterler değerlendirmesini devam eden ürünler

EAL1: Fonksiyonel olarak test edilmiştir.

EAL2: Yapısal olarak test edilmiştir.

EAL3: Metodik olarak test edilmiştir.

EAL4: Metodik olarak tasarlanmış, geliştirilmiş ve gözden geçirilmiştir.

EAL5: Yarı resmi (semi-formally) tasarlanmış ve test edilmiştir.

EAL6: Yarı resmi tasarım doğrulaması yapılmış ve test edilmiştir.

EAL7: Resmi tasarım doğrulaması yapılmış ve test edilmiştir.

5.1.2 ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi

Bilgi, kuruluşunuzun faaliyetleri ve belki devamı için büyük bir önem taşır. ISO/IEC 27001 Belgesi değerli bilgi varlıklarınızı yönetmenize ve korumanıza yardımcı olur.

ISO/IEC 27001, Bilgi Güvenliği Yönetimi Sistemi (ISMS) gereksinimlerini tanımlayan tek uluslararası denetlenebilir standarttır. Yeterli ve orantılı güvenlik denetimleri seçilmesini sağlamak için tasarlanmıştır.

ISO 27001 Kurumların risk yönetimi ve risk işleme planlarını, görev ve sorumlulukları, iş devamlılığı planlarını, acil durum olay yönetimi prosedürleri hazırlamasını ve uygulamada bunların kayıtlarını tutmasını gerektirir. Kurum tüm bu faaliyetlerin de içinde yer aldığı bir bilgi güvenliği politikası yayınlamalı ve personelini bilgi güvenliği ve tehditler hakkında bilinçlendirmelidir. Seçilen kontrol hedeflerinin ölçülmesi ve kontrollerin amacına uygunluğunun ve performansının sürekli takip edildiği yaşayan bir süreç olarak bilgi güvenliği yönetimi ancak yönetimin aktif desteği ve personelin katılımcılığıyla başarılabilir.

Bu, bilgi varlıklarınızı korumanıza ve ilgili taraflara, özellikle de müşterilerinize güven vermenize yardımcı olur. Bu standart, Bilgi Güvenliği Yönetimi Sisteminizi oluşturmak, uygulamak, işletmek, izlemek, incelemek, sürdürmek ve geliştirmek için süreç yaklaşımını benimser.

ISO 27001 Kimi ilgilendirir ?

ISO/IEC 27001, dünyanın hangi Ülkesinden veya hangi sektörden olursa olsun büyük küçük tüm kuruluşlara uygundur. Bu standart, finans, sağlık, kamu ve BT sektörleri gibi bilginin korunmasının büyük öneme sahip olduğu alanlarda özellikle gereklidir. [58]

ISO/IEC 27001, BT taşeron şirketleri gibi bilgiyi başkaları adına yöneten kuruluşlar için de oldukça önemlidir, müşterilere bilgilerinin koruma altında olduğu güvencesini vermek için kullanılabilir.

ISO/IEC 27001 İle ilgili Terim ve Kavramlar

Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımın dayalı tüm yönetim sisteminin bir parçası.

Risk analizi: Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı.
Risk değerlendirme: Risk analizi ve risk derecelendirmesini kapsayan tüm proses.

Risk derecelendirme: Riskin önemini tayin etmek amacıyla tahmin edilen riskin verilen risk kriterleri ile karşılaştırılması prosesi.
Risk yönetimi: Bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler.
Risk işleme: Riski değiştirmek için alınması gerekli önlemlerin seçilmesi ve uygulanması prosesi.
Uygulanabilirlik bildirgesi: Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kurmanın Yararları

• **Bilgi varlıklarının farkına varma:** Kuruluş hangi bilgi varlıklarının olduğunu, değerinin farkına varır.
• **Sahip olduğu varlıkları koruyabilme:** Kuracağı kontroller ile koruma metodlarını belirler ve uygulayarak korur.
• **İş sürekliliği:** Uzun yıllar boyunca işini garanti eder. Ayrıca bir felaket halinde, işe devam etme yeterliliğine sahip olur.

• **İlgili taraflar ile barış halinde olma:** Başta tedarikçileri olmak üzere, bilgileri korunacağından ilgili tarafların güvenini kazanır.
• Bilgiyi bir sistem sayesinde korur, tesadüfe bırakmaz.
• Müşterileri değerlendirirse, rakiplerine göre daha iyi değerlendirilir.
• Çalışanların motivasyonunu arttırır.
• Yasal takipleri önler.
• Yüksek prestij sağlar.

ISO 27001 Bilgi Güvenliği Sistemi Kurma Aşamaları :

• Varlıkların sınıflandırılması,
• Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi,
• Risk analizi,
• Risk analizi çıktılarına göre uygulanacak kontrolleri belirleme,
• Dokümantasyon oluşturma,
• Kontrolleri uygulama,
• İç tetkik,
• Kayıtları tutma,
• Yönetimin gözden geçirmesi,
• Belgelendirme**.**

2013 yılı başlarında taslak sürümleri yayınlanan ISO 27001 ve ISO 27002 Bilgi Güvenliği Yönetim Sistemi Standartlarının 25.09.2013 tarihinde yeni sürümleri yayınlandı. Standardın 2013 sürümü (İngilizce) ISO-Uluslararası Standardizasyon Örgütü sayfasından satın alınabilmektedir.

Arka Plan

ISO/IEC 2700_ Standart-Ailesi Bilgi Güvenliği ve Bilgi Güvenliği Yönetim Sistemi ile ilgilidir. Aşağıda sayılan standartlar bilgilendirici ve normatif dokümanlardır:

ISO/IEC 2700<u>0</u>: Bilgi Güvenliği konusuna genel bir bakış açısı içeren Standart, 46 anahtar tanım ve terimi açıklamaktadır.

ISO/IEC 27001: Bilgi Güvenliği Standartları arasında çekirdek doküman hükmünde olan bu doküman Bilgi Güvenliği Yönetim Sistemi için gerekli olan gereksinimleri içermektedir. Dokümanın Ek kısmında da gerekli kontroller ve amaçları listelenmiştir.

ISO/IEC 27002: 27001 EK-A kısmındaki kontrollerinin iyi uygulamaları için bir kılavuz görevi gören bu standart tamamlayıcı açıklamalar içermektedir.

ISO/IEC 2700_,-4,-5 ve -7: Bilgi Güvenliği Yönetim Sistemi kurulumu için en önemli konulara yönelik hazırlanmış olan bilgilendirici kılavuzlardır. Örnek: 27005 Bilgi Güvenliği Risk yönetimi.

Hangi Dokümanlar ve Kayıtlar gereklidir?

Yeni sürümde hangi maddeler hangi dokümantasyonu gerektirmektedir? Hangi kayıtlar tutulmalıdır? Hangi dokümanlar ve kayıtlar standartta zorunludur? Aşağıdaki tablolar bu soruları cevaplamak için oluşturulmuştur.

ISO 27001:2013 Standart maddesi	Doküman
4.3	BGYS Kapsamı
5.2 ve 6.2	Bilgi Güvenliği Politikası ve Hedefleri
6.1.2	Risk Analizi ve Risk Değerlendirme Metodolojisi
6.1.3 (d)	Uygulanabilirlik Bildirgesi
6.1.3 (e) ve 6.2	Risk Tedavi Planı
8.2	Risk Değerlendirme Raporu
A.7.1.2 ve A.13.2.4	Roller ve Sorumluluklar
A.8.1.1	Varlık Envanteri
A.9.1.1	Erişim Kontrol Politikası
A.12.1.1	BT Yönetimi İçin İşletme prosedürleri
A.14.2.5	Güvenli Sistem Mühendisliği Prensipleri
A.15.1.1	Tedarikçi Zinciri güvenlik Politikası
A.16.1.5	Olay Yönetimi Prosedürü
A.17.1.2	İş Sürekliliği Prosedürü
A.18.1.1	Sözleşmelerden, Düzenlemelerden ve Yasalardan Kaynaklanan Yükümlülükler

Tablo -5: ISO 27001 Zorunlu Dokümanlar

EK-A da yer alan kontrollerden bazıları kurum ilgili riskleri içermiyorsa seçilmeyebilir. Aşağıdaki Tablo BGYS kurulması ve uygulanması esnasında tutulması gereken zorunlu bilgi kayıtlarını göstermektedir.

ISO 27001:2013 Standart Maddesi	Kayıtlar
7.2	Eğitim, Kabiliyetler, ve Tecrübe Kayıtları
9.1	Ölçme ve İzleme Sonuçları
9.2	İç Tetkik Programı
9.2	İç tetkik Raporu
9.3	Yönetim Gözden Geçirme Raporu
10.1	Düzeltici Faaliyet Kayıtları ve Sonuçları
A.12.4.1 ve A.12.4.3	Kullanıcı işlem ve Faaliyet Kayıtları, Hatalar ve İhlal Olayları

Tablo-6 : ISO 27001:2013, Zorunlu Kayıtlar

Yukarıdaki zorunlu dokümanların haricinde genelde kullanılan, bilgi güvenliği seviyesini ve etkinliğini artırabilecek dokümanlarda aşağıdaki tabloda gösterilmiştir.

ISO 27001:2013 Standart maddesi	Doküman
7.5	Doküman Kontrol Prosedürü
7.5	Yönetim kayıtlarının Kontrolü
9.2	İç Tetkik Prosedürü
10.1	Düzeltici Faaliyet Prosedürü
A.6.2.1	Kişisel cihaz Kullanım Politikası
A.6.2.1	Mobil Cihaz ve Uzaktan erişim politikası
A.8.2.1,A.8.2.2, A.8.2.3	Bilgi Sınıflandırma Politikası
A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1 A.9.4.3	Parola Politikası
A.8.3.2, A.11.2.7	Güvenli İmha Politikası
A.11.1.5	Güvenli Ortamlarda çalışma politikası
A.11.2.9	Temiz Masa ve Temiz Ekran Politikası
A.12.1.2, A.14.2.4	Değişiklik Yönetimi Prosedürü
A.12.3.1	Yedekleme Politikası
A.13.2.1, A.13.2.2, A.13.2.3	Bilgi Değişim Prosedürü

Tablo-7: Zorunlu olmayan fakat hazırlanmasında fayda olan Dokümanlar

BÖLÜM 6. SONUÇ VE ÖNERİLER

Günümüz internet dünyasında siber suçlar kişi, kurum ve kuruluşları gerek günlük işlerle gerek eğitim faaliyetleriyle gerekse özel ve kamu kurum faaliyetleriyle ilgili olarak tehdit eden hayati öneme sahip hakkında binlerce inceleme ve araştırma faaliyetleri yapılan bir unsur haline gelmiştir.

Bu kapsamda kurumlar için alınması gereken tedbirler ve önlemler aşağıdaki gibi sıralanmıştır.

6.1 E-Posta Güvenlik Tedbirleri

E-posta kurumun en önemli iletişim kanallarından biridir ve bu kanalın kullanılması kaçınılmazdır. Bunun yanı sıra e-posta basitliği ve hızı nedeni ile yanlış kullanıma veya gereğinden fazla kullanıma açık bir kanaldır. Kurumda E-posta güvenliğinin sağlanabilmesi için alınması gereken tedbirleri şu şekilde sıralayabiliriz.

- Kurumun e-posta sistemi taciz, suistimal veya herhangi bir şekilde alıcının haklarına zarar vermeye yönelik öğeleri içeren mesajların gönderilmesi için kullanılmamalıdır. Bu tür özelliklere sahip bir mesaj alındığında ilgili birim yöneticisine haber verilmesi ve daha sonra bu mesajın tamamen silinmesi gerekmektedir.
- Mesajların gönderilen kişi dışında başkalarına ulaşmaması için gönderilen adrese ve içerdiği bilgilere azami biçimde özen gösterilmesi gerekmektedir.
- Spam, zincir e-posta, sahte e-posta vb. zararlı e-postalara yanıt yazılmamalıdır.
- Kullanıcıların kullanıcı kodu/şifresini girmesini isteyen e-postaların sahte e-posta olabileceği dikkate alınarak herhangi bir işlem yapılmadan silinmelidir.
- Gizli ve hassas bilgi içeren elektronik postalar kriptolanarak iletilmelidir.
- Kurum çalışanları kurumsal e-postaların kurum dışındaki şahıslar ve yetkisiz şahıslar tarafından görülmesi ve okunmasını engellemekten sorumludurlar.
- Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve derhal silinmelidir.

- Virüs, solucan, Truva Atı veya diğer zararlı kodlar bulaşmış olan bir e-posta kullanıcıya zarar verebilir. Bu tür virüslerle bulaşmış e-postalar Anti-virüs sistemleri tarafından analiz edilip temizlenmelidir.

6.2 Şifre Güvenlik Tedbirleri

Şifreleme bilgisayar güvenliği için önemli bir özelliktir. Kullanıcı hesapları için ilk güvenlik katmanıdır. Zayıf seçilmiş bir şifre ağ güvenliğini tümüyle riske atabilir. Bütün sistem seviyeli şifreler (örnek root administrator enable vs) ve bütün kullanıcı seviyeli şifreler (örnek e-posta web masaüstü bilgisayar vs.) belirli periyotlarla değiştirilmelidir. Tavsiye edilen değiştirme süresi en az 6 ayda birdir.

- Sistem yöneticisi her sistem için farklı şifreler kullanmalıdır.
- Kullanıcı şifresini başkası ile paylaşmaması kâğıtlara ya da elektronik ortamlara yazmaması konusunda eğitilmelidir.
- Şifre seçimleri yapılırken alfa-nümerik karakterler seçilmeli ve en az 8 karakter olmalıdır.

6.3 Anti-Virüs Güvenlik Tedbirleri

- Kurumun bütün PC tabanlı bilgisayarları anti-virüs yazılımına sahip olmalıdır ve belli aralıklarda düzenli olarak güncellenmelidir. Ayrıca anti-virüs yazılımı otomatik olarak güncellenmelidir.
- Anti-virüs güncellemeleri bu iş için adanmış Sunucular vasıtası ile yapılmalıdır. Sunucular internete online bağlantısı olmalı ve otomatik olarak veritabanlarını güncelleyebilmelidir. Bilinmeyen kaynaklardan gelen diskler ve CD-Rom'ları daima virüslere karşı tarama yapılmalıdır.
- Kritik veri ve sistem konfigürasyonları düzenli aralıklar ile yedeklenmeli ve güvenli bir yerde saklanmalıdır.
- Virüs bulaşan makineler tam olarak temizleninceye kadar ağdan çıkarılmalıdır.
- Hiçbir kullanıcı herhangi bir sebepten dolayı anti-virüs programını sisteminden kaldıramamalıdır.

6.4 Sunucu Güvenlik Tedbirleri

Kurumun sahip olduğu sunucularının temel güvenlik konfigürasyonları için bazı standartlar vardır.

- Sunucular üzerinde kullanılmayan servisler ve uygulamalar kapatılmalıdır.
- Servislere erişimler loglanmalı ve erişim kontrol metotlarıyla koruma sağlanmalıdır.
- Sistem yöneticileri gerekli olmadığı durumlar dışında “Administrator" ve “root” gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalıdır. Gerekli olduğunda önce kendi hesapları ile log-on olup daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
- Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL, IPSec, VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
- Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdırlar.
- Sunucuların yazılım ve donanım bakımları üretici tarafından belirlenmiş aralıklarla, yetkili uzmanlar tarafından yapılmalıdır.
- Sistem odalarına yetkisiz girişler engellenmelidir. Sistem odalarına giriş ve çıkışlar erişim kontrollü olmalı ve bilgisayar sistemine kayıt edilmelidir.

6.5 Ağ Yönetimi Tedbirleri

Kurumun bilgisayar ağında yer alan bilgilerin ve ağ altyapısının güvenliği, gizlilik, bütünlük ve erişilebilirlik kavramları göz önüne alınarak sağlanmalıdır. Uzaktan erişim hususunda özel önem gösterilmelidir. Yetkisiz erişimle ilgili tedbirler alınmalıdır. Ağın güvenliği ve sürekliliğini sağlamak amacıyla bir takım kontroller gerçekleştirilmelidir.

- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için özel kontroller uygulanmalıdır.
- Ağ servisleriyle ilgili standartlarda erişimine izin verilen ağlar ve ağ servisleri ve ilgili yetkilendirme yöntemleri belirtilmelidir.

- Gerek görülen uygulamalar için portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmalıdır.
- Sınırsız ağ dolaşımı engellenmelidir.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden teknik önlemler alınmalıdır (ör. Firewall)
- Ağ erişimi, VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmalıdır.
- Ağ bağlantıları periyodik olarak kontrol edilmelidir.
- Gerek görülen uygulamalar için elektronik posta tek yönlü dosya transferi, çift yönlü dosya transferi, etkileşimli erişim, güne ve günün saatine bağlı erişim gibi uygulama kısıtlamalarıyla ağ erişimi denetimi yapılmalıdır.
- Ağ üzerindeki firewall'lar üzerinde ilgili konfigürasyon dokümanlarında belirtilen servisler dışında tüm servisler kapatılmalıdır Firewall olarak kullanılan cihazlar başka bir amaç için kullanılmamalıdır.
- Bilgisayar ağıyla ilgili sorumlulukları desteklemek amacıyla ağ dokümantasyonu hazırlanmalı ağ cihazlarının güncel konfigürasyon bilgileri saklanmalıdır.
- Bilgisayar ağı üzerinde gerçekleşen işlemler takip edilmeli, loglar saklanmalıdır.

6.6 Kablosuz İletişim Tedbirleri

Kurum bünyesinde kablosuz iletişim sağlanması için kullanılan erişim cihazları (Access Point) ve kartları güvenlik tedbirleri belirlenmediğinde saldırganlar için büyük bir giriş kapısıdır. Bu durum bilgi sistemlerini tehdit altında bırakacaktır ve bilgi güvenliği konusunda zafiyet oluşacaktır. Kablosuz iletişim için alınması gereken tedbirler şu şekildedir.

- Kurumun bilgisayar ağına bağlanan bütün erişim cihazları ve ağ arabirim kartları (örnek PC Card) Bilgi İşlem birimi tarafından kayıt altına alınmalıdır. Erişim cihazları periyodik olarak güvenlik testlerinden geçirilmelidir. Ancak Mac adresleri kayıtlı olan cihazlar bilgisayar ağına erişebilmelidir.
- Erişim cihazlarındaki firmware'leri düzenli olarak güncellenmelidir. Bu donanım üreticisi tarafından çıkarılan güvenlik ile ilgili yamaların uygulanmasını sağlar.

- Erişim cihazlarını kolayca erişilebilir bir yerde olmaması gereklidir. Çünkü cihaz resetlendiğinde fabrika ayarlarına geri dönebilmekte ve güvenlik açığı oluşturabilmektedir.
- Cihaza erişim için güçlü bir şifre kullanılmalıdır. Erişim şifreleri varsayılan ayarda bırakılmamalıdır.
- SSID numaraları yayınlanmamalıdır. Böylece sniffer tarzı cihazların otomatik olarak bu numaraları çözmesi engellenecektir.
- Varsayılan SSID isimlerini kullanılmamalıdır. SSID ayarı bilgisi içerisinde kurumla ilgili bilgi olmamalıdır mesela kurum ismi ilgili bölüm çalışanın ismi vs.
- Erişim Cihazları üzerinden gelen kullanıcılar Firewall üzerinden ağa dâhil olmalıdırlar.
- Hem kullanıcılar hem de erişim cihazları statik ip adresleri kullanmalıdır. Aynı zamanda donanım adresleme (örnek mac adresleme) kullanılmalıdır.

6.7 Kriz ve Acil Durum Yönetimi Tedbirleri

Kurumun bilgi güvenliliği ve iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde, gerekli müdahale yapabilmelerine yönelik standartları belirlemektedir. İzlenen olayın uygun şekilde raporlanması ve belirlenen önlem ve acil durum faaliyetlerinin uygulanması önemlidir.

Kurum çalışanlarının bilgi güvenliği veya iş sürekliliği ile ilgili acil bir durum oluştuğunda sorumlulukları dahilinde gerekli müdahaleyi yapabilmelerine yönelik tedbirler aşağıda belirtilmiştir.

- Bahse konu acil durum senaryoları yaşanmadan önce uygun acil durum hareket planının yapılması esastır. Bilgi güvenliğine yönelik tehlike senaryolarından bazıları sistemlere yapılacak direkt saldırılar, zararlı kod içeren programların, kişilerin sisteme sızması, bilginin hırsızlığı dışarıdan veya içeriden gerçekleştirilebilecek saldırı öncesi taramalar olarak tanımlanabilir.
- Acil durum sorumluları atanmalı ve yetki ve sorumlulukları belirlenmeli ve dokümante edilmelidir.

- Bilgi sistemlerinin kesintisiz çalışabilmesi için gerekli önlemler alınmalıdır. Örneğin uygulama veya veri tabanı sunucularında donanım ve yazılıma ait problemler oluştuğunda yerel veya uzak sistemden yeniden kesintisiz (veya makul kesinti süresi içerisinde) çalışma sağlanabilmelidir.
- Acil durumlarda kurum içi işbirliği gereksinimleri tanımlanmalıdır.
- Acil durumlarda sistem log'ları incelenmek üzere saklanmalıdır.
- Güvenlik açıkları ve ihlallerinin rapor edilmesi için kurumsal bir mekanizma oluşturulmalıdır.
- Bir güvenlik ihlali yaşandığında ilgili sorumlulara bildirimde bulunulmalı ve bu bildirim süreçleri tanımlanmış olmalıdır.

6.8 Kimlik Doğrulama ve Yetkilendirme Tedbirleri

Kurumun bilgi sistemlerine erişimde kimlik doğrulaması ve yetkilendirme tedbirleri şu şekildedir.

- Bilgi sistemlerine erişecek tüm kullanıcıların kurumsal kimlikleri doğrultusunda hangi sistemlere hangi kimlik doğrulama yöntemi ile erişeceği belirlenmeli ve dokümante edilmelidir.
- Tüm bilgi sistemleri üzerindeki kullanım hakları periyodik olarak gözden geçirilmeli ve gereksinimler ve gerekli minimum yetkinin verilmesi prensibi doğrultusunda revize edilmelidir.
- Erişim ve yetki seviyelerinin sürekli olarak güncelliği temin edilmelidir.
- Sistemlere başarılı ve başarısız erişim 156oğları düzenli olarak tutulmalı tekrarlanan başarısız log-on girişimleri incelenmelidir.
- Kullanıcılar kendilerine verilen erişim şifrelerini gizlemeli ve kimseyle paylaşmamalıdır.
- Sistemlere log-on olan kullanıcıların yetki aşımına yönelik hareketleri izlenmeli ve yetki ihlalleri kontrol edilmelidir.

- Kullanıcı hareketlerini izleyebilmek üzere her kullanıcıya kendisine ait bir kullanıcı hesabı açılmalıdır.

6.9 Veri Tabanı Güvenlik Tedbirleri

- Kritik verilere her türlü erişim işlemleri (okuma değiştirme silme ekleme) loglanmalıdır. Log kayıtlarına idarenin izni olmadan kesinlikle hiçbir şekilde erişim yapılamamalıdır. Manyetik kartuş, DVD veya CD ortamlarında tutulan log kayıtları en az 5 (beş) yıl süre ile güvenli ortamlarda saklanmalıdır.
- Veritabanı sistem logları tutulmalı ve gerektiğinde idare tarafından izlenmelidir.
- Veritabanı sistemlerinde tutulan bilgiler sınıflandırılmalı ve uygun yedekleme politikaları oluşturulmalı, yedeklemeden sorumlu sistem yöneticileri belirlenmeli ve yedeklerin düzenli alınması kontrol altında tutulmalıdır.
- Bilgilerin saklandığı sistemler fiziksel güvenliği sağlanmış sistem odalarında tutulmalıdır.
- Veritabanı sistemlerinde oluşacak problemlere yönelik bakım onarım çalışmalarında yetkili bir personel bilgilendirilmelidir.
- Bilgi saklama medyaları kurum dışına çıkartılmamalıdır.
- Sistem dokümantasyonu güvenli şekilde saklanmalıdır.
- İşletme sırasında ortaya çıkan beklenmedik durum ve teknik problemlerde destek için temas edilecek kişiler belirlenmelidir.
- Veritabanı sunucusuna ancak zorunlu hallerde root veya admin olarak bağlanılmalıdır.
- Bağlanacak kişilerin kendi adına kullanıcı adı verilecek yetkilendirme yapılacaktır.
- Bütün kullanıcıların yaptıkları işlemler loglanmalıdır.
- Veritabanı yöneticiliği yetkisi sadece bir kullanıcıda olmalıdır.
- Veritabanında bulunan farklı şemaların kendi yetkili kullanıcısı dışındaki diğer kullanıcıların erişmesi engellenmelidir.
- Veritabanı sunucularına internet üzerinden erişimlerde VPN gibi güvenli bağlantılar tesis edilmelidir.

- Veritabanı sunucularına kod geliştiren kullanıcı dışında hiçbir kullanıcı bağlanıp sorgu yapamamalıdır. İstekler arayüzden sağlanmalıdır

6.10 Yazılım Geliştirme Tedbirleri

Yazılım geliştirme üzerindeki kontroller kurumların günlük operasyonlarını yürütmek için kullandıkları yazılımların oluşturulması esnasında kullanılan kontrol mekanizmalarıdır. Programların geliştirilmesi esnasında uygulanması gereken kontroller yazılımların kontrollü bir şekilde geliştirilmesini sağlamayı hedeflemektedir. Bu şekilde güvenlik kriterlerinin hem yazılımın geliştirilmesi aşamasında hem de geliştirilen yazılım uygulamaya alındıktan sonra gözetilmesi sağlanır. Bu tedbirler yazılım geliştirme hakkındaki kriterleri ortaya koymaktadır.

- Sistem yazılımında mevcut olan kontroller kullanılacak yeni bir yazılım veya mevcut sistem yazılımına yapılacak olan güncellemeler ile etkisiz hale getirilmemelidir.
- Yönetim, sadece uygun yazılım projelerinin başlatıldığından ve proje altyapısının uygun olduğundan emin olmalıdır.
- İhtiyaçlar uygun bir şekilde tanımlanmalıdır.
- Sistem geliştirmede ihtiyaç analizi, fizibilite çalışması, tasarım geliştirme, deneme ve onaylama safhalarını içeren sağlıklı bir metodoloji kullanılmalıdır.
- Hazırlanan sistemler mevcut prosedürler dahilinde, işin ve iç kontrol gerekliliklerini yerine getirdiklerinden emin olunması açısından test edilmeli ve yapılan testler ve test sonuçları belgelenerek onaylanmalıdır.
- Yeni alınmış veya revize edilmiş bütün yazılımlar test edilmeli ve onaylanmalıdır.
- Eski sistemlerdeki veriler tamamen doğru olarak ve yetkisiz değişiklikler olmadan yeni sisteme aktarılmalıdır.
- Uygulama ortamına aktarılma kararı uygun bilgilere dayalı olarak ilgili yönetim tarafından verilmelidir.
- Yeni yazılımların dağıtımı ve uygulanması kontrol altında tutulmalıdır.
- Yazılımlar sınıflandırılmalı, etiketlenmeli ve envanterleri çıkarılarak bir yazılım kütüğünde muhafaza edilmelidir.

6.11 Kurumlarda Güvenlik için 20 Kritik Kontrol

Herhangi bir kurum veya kuruluşun bilgi sistemlerinde sağlam ve güvenilir bir siber savunma sağlayabilmesi için Amerika'da bulunan SANS Enstitüsü'nce 20 kritik güvenlik kontrolü yayınlanmıştır. 2011 yılında İngiltere'de devlet kurumları ve kritik altyapılarda bu kontrollerin uygulanacağı duyurulmuştur. 2012 yılında da ABD Siber Güvenlik Komutanı ve NSA Başkanı Keith Alexander, bu kontrollerin güvenilir bir siber savunma oluşturmak için çok önemli olduğunu söylemiştir.

Bu kontroller aşağıda listelenmiştir.

1- Donanım Envanteri

Envanter yönetim yazılımları ile sisteme eklenen tüm donanım envanterinin güncel halinin tutulmasını sağlayan bir sistemin kurulması ve sürdürülmesidir. Ağa yeni eklenen donanımların otomatik olarak algılanmasını sağlayan yazılımlar kullanarak izinsiz bağlanan donanımları tespit ederek sistem yöneticisine bildirilmesidir.

2- Yazılım Envanteri

Yetkisiz yazılım kurulmasını önleyecek şekilde, sadece izin verilen programların çalışmasını sağlayacak ve sistemde kullanılan yazılımları otomatik olarak tespit eden yazılım araçlarının kullanılması. Sunucularda, dizüstü bilgisayarlarda, ağ ve sistemlerde kullanılan yazılımların güncel olarak tutulmasıdır.

3- Mobil Cihazlar, dizüstü bilgisayarlar, iş istasyonları ve Sunucuların Donanım ve Yazılımlarının Güvenli bir şekilde Yapılandırılmaları

Donanımların ve yazılımların kurulumunda güvenli olarak konfigüre edilmesi, kurulum parametrelerinin belgelendirilmesi ve konfigürasyon yönetim araçlarının kullanılmasıdır. Düzenli aralıklarla, sistem konfigürasyonunun kontrolü, problem halinde tespiti ve raporlanarak çözümünün yapılması.

4- Ağ Donanımları Kontrolü

İletişim ağıyla alakalı tüm mimari, erişim kontrol listelerinin, ağ cihaz ayarlarının yazılı olarak kaydedilmesi ve güncel yapılandırılma ile olması gereken ayarların karşılaştırılması. Ağdaki DNS ayarlarının periyodik olarak kontrolünün sağlanması, IP adreslerinin loglanması ve DHCP ayarlarının düzgün olarak yapılandırılmasıdır.

5- Zararlı Yazılımlara (Malware) Karşı Savunma

Güncel anti-virüs, anti- rootkit ve anti-malware yazılımlarının ağdaki bütün bilgisayarlara ve serverlara kurulması. Kullanıcıların tarafından yapılacak saldırıları engelleyebilmek amacıyla sunucu tabanlı saldırı önleme sisteminin kurulması. Bilgisayarlara takılan USB gibi taşınabilir aygıtların auto-run özelliklerinin İşletim Sistemi tarafında kapatılması gibi önlemlerdir.

6- Uygulama Yazılımlarının Güvenliği

Uygulama yazılımlarının çalıştığı sunucu ve veri tabanının parametrelerinin güvenli şekilde ayarlanması, gerek kurumdaki ilgili personel tarafından geliştirilen gerekse satın alınan yazılımların güvenlik testleri yapılarak arka kapı veya Truva atı tarzı zararlı yazılımları bulundurmamasının tespiti gibi önlemlerdir.

7- Kablosuz Erişim Denetimi

Kablosuz iletişim cihazlarının yetkisiz olarak sisteme bağlanmasının engellenmesidir. Belirli yerlerde kablosuz iletişimin kullanımının sağlanması ve bu iletişim noktalarının güvenlik ve yönetim yazılımlarının güvenli olması kontrolleri. Kablosuz saldırı tespit sistemlerinin alınması ve kablosuz iletişimin şifreli olarak kullanılmasıdır.

8- Veri Kurtarma Kapasitesi

Önemli sistem dosyalarının ve verilerin düzgün bir şekilde yedeklenmesinin sağlanması. Hızlı ve güvenilir şekilde yedekten geri dönmeyi sağlayacak sistemlerin kurulması, yedeklerin kriptolu bir şekilde tutulması gibi kontrollerdir.

9- Güvenlik Becerilerini Değerlendirme ve Uygun Eğitimler ile Zafiyet olan Alanları Giderme

Sistem yöneticileri ile güvenlikten sorumlu personelin güncel eğitimler ile becerilerinin geliştirilmesi olası saldırı ve tehditlere karşı nitelikli eleman ihtiyacını gidermektir.

10- Güvenlik Duvarları, Router ve Switch gibi Ağ cihazlarının Güvenli bir şekilde yapılandırılmaları

Ağ cihazlarının konfigürasyonlarının periyodik olarak kontrol edilmesi, yönlendirme bilgilerinin kontrolü, geniş alan ağı, yerel alan ağı, sanal ağ bağlantılarının kontrollerinin yapılmasıdır.

11- Ağ Bağlantı Noktaları (Port), Protokoller ve Servislerin Kontrolü

Güvenlik duvarı ve filtreleme sistemlerinin ağa bağlı bütün cihazlara kurulumunun yapılması, router ve switch lere gereksiz erişimin engellenmesi, güvenlik duvarında port taraması yapılarak sadece gerekli olan port ve protokollere izin verilmesidir.

12 - Sistem Yönetici Yetkilerinin Kontrolü

Personele yaptığı işe göre yetki verilmesi, sistemden birinci derecede sorumlu olmayan personele, makamından dolayı fazla yetki verilmemesi, yetkili personelin yetkilerinin kontrol edilmesi, personelin işi bırakması gibi durumlarda yetkilerinin iptal edilmesi gibi kontrollerdir.

13- Sınır Savunma

Güvenlik duvarları, ağ geçitleri, Proxylerin kullanılması, serverlara erişimin sınırlı tutulması, saldırır tespit ve önleme sistemlerinin kurulumunun yapılarak, sisteme yapılan saldırıların önlenmesi ve anormal ağ trafiğinin tespit edilmesi, gerekli olmayan sunucu ve servislere erişimin kapatılması ağ geçitleri ile zararlı yazılımların bilgisayarlara bulaşmadan engellenmesi gibi kontrollerdir.

14- Logların Güvenli Olarak Kaydedilmesi, Yönetilmesi Ve İzlenmesi

Sistemlerle ilgili tutulması gereken önemli logların tespit edilerek, bunların dokümante edilmesi ve belirli aralıklarla kontrolünün sağlanması, logların yeterli bilgiyi (kullanıcı adı, uygulama, tarih, yapılan işlem) içerdiğinin kontrol edilmesi, logların arşivlenmesi, log analiz programları ile raporlar çıkarılarak sistemlerin güvenliğini tehdit edebilecek davranışların belirlenmesidir.

15- Güvenlik Eğitimleri

Kurumdaki bütün çalışanlara temel güvenlik eğitimlerinin verilmesidir.

16- Kullanıcı Hesabı Denetimi

Sistemde boşta bulunan, herhangi bir nedenden dolayı kullanılmayan kullanıcı hesaplarının tespit edilerek kapatılması, kullanıcı oluşturma, yetkilendirme, silme gibi kullanıcı hesabı yönetimiyle ilgili işlemlerinin kayıt altına alınmasıdır.

17- Veri Koruma

Kritik bilgilerin bulunduğu bilgisayarlarını hard-disklerinin kriptolanması, Veri Kaçağı Önleme Sisteminin kurulması, e-posta güvenliğinin sağlanması, ağı kullanarak paylaşım yapılan verilerin kriptolu olarak iletilmesini sağlayan sistemlerin kurulması, ağın izlenerek dosya transferlerinin, uzun süre açık kalan bağlantıların, anormal şekilde kullanılan port ve protokollerin tespit edilmesini sağlayan sistemlerin kurulmasıdır.

18- Bilgisayar Olaylarına Müdahale

Bilgisayar Olaylarına Müdahalenin kimler tarafından ve nasıl yapılacağının belirlenmesidir. Kurulacak ekibe gerekli eğitim ve teknik donanımın sağlanması, bilgisayarlara müdahale edilme durumunda ilgili personelin irtibat bilgilerinin kayıt altına alınması ve bilgisayar olaylarına müdahale tatbikatlarının yapılmasıdır.

19- Güvenli Ağ Mühendisliği

İletişim ağının yönetilebilirliği ve güvenliğine, mimari yapısına hâkim olunması, ağın mümkün olduğu kadar alt VLAN'lara bölünerek, erişim kısıtlamalarının yapılmasıdır.

20- Güvenlik Analizi ve Sızma(Penetration) Testleri

Sistemdeki yazılım ve donanım bileşenlerinin güncel ayarlarının olması gereken ayarlara uygunluğunun periyodik olarak test edilmesi, sistem güvenliğinin belirli aralıklarla analiz edilerek raporlanması, sızma testleri gerçekleştirilerek zafiyetlerin tespit edilmesidir.

6.12 Eğitim

Bilgi güvenliğinin sağlanmasında ne kadar önlem alınmış olsa da insan faktörü göz ardı edilirse hiçbir önlem sonuç vermeyecektir. Çünkü bilgi güvenliği bilinci ve farkındalığı olmayan insanlar bu güvenlik sürecini aksatacaktır.

Bilginin korunmasına çalışıldığı günden bu yana insanlar güvenlik sürecinin en zayıf tarafını oluşturmuşlardır. Birçok teknik ve yönetsel güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan kullanılarak çeşitli yöntemlerle kolaylıkla aşılabilmektedir. "Gücünüz en zayıf halkanız kadardır" ilkesi bilgi güvenliği için de geçerlidir.

Yapılan araştırmalar göstermiştir ki bilgi güvenliği ihlali olayları genellikle kurum çalışanları tarafından yapılmıştır. Bunlardan çoğu bilinçsiz davranışların sonucudur. Nadir de olsa kötü niyetli çalışanların bilgiyi dışarıya sızdırması kötü amaçlı kullanımı veya yok etmesi de söz konusudur.

Kurumsal bilgi güvenliğinin sağlanmasında insan faktörü önemli bir yere sahiptir. Yeterli bilinç, farkındalık ve eğitim düzeyine sahip olmayan kurum çalışanları ile kurumsal bilgi sistemleri üzerinde yetkileri olan ve yerel saldırgan olarak adlandırılan iyi niyetli olmayan üst derecede bilgiye sahip olan çalışanlar kurumsal bilgi güvenliğini tehdit eden faktörlerdir. Bu nedenle günümüzde saldırganlar teknolojik olmayan ve engellenmesi daha zor olan sosyal yöntemleri tercih etmektedirler. İnsan faktörünü kullanmak teknik yöntemlere göre daha tehlikeli sonuçların oluşmasını sağlayan önemli ve güncel bir saldırı aracıdır. Bu saldırı türünü kullanan saldırganlar sosyal mühendis olarak adlandırılmaktadır.

Sosyal mühendislik insan doğasında varolan başkalarına güvenme ve yardım etme eğiliminin başka şekilde elde edilmesi zor olan şeylerin ele geçirilmesi amacı ile kullanılmasıdır. Sosyal mühendislerin amaçları bilgiye erişim yetkisi olan kullanıcılar aracılığıyla güvenlik teknolojilerinin atlatılmasını (by-pass) sağlamaktır. İnsanlar, başkalarının maksatlı olarak kendilerini tuzağa düşürmeyecekleri veya kullanmayacaklarını düşünme eğiliminde olsalar da bu yöntem en sık kullanılan saldırı yöntemlerindendir. Bu yöntem kolay ve hızlı olduğu için saldırganlar tarafından tercih edilmektedir. En yaygın sosyal mühendislik yöntemleri başka birisiymiş gibi davranma, kompliman, aciliyet ve yetkilendirme alınmış duygusu yaratmadır. Bu nedenlerle kullanıcıların sosyal mühendisliğe karşı korunmasını hedefleyen bir eğitim stratejisi izlenmelidir. Bilgi güvenliği hususunda çalışanlara eğitim verilerek yeterli bilince ve bilgiye sahip olması ile bu zafiyet giderilebilmektedir.

Bilgi güvenliğini sağlamak için en önemli unsur olan insan faktörünün bilgi güvenliği konusunda eğitimi şarttır. Bu eğitim kurumun hayati fonksiyonlarını yerine getirebilmesini sağlayan, bilginin nasıl korunacağını, neden korunması gerektiğini öğretmelidir. Çalışanlar hatalı davranışlarının kurum bilgi güvenliği üzerinde yaratabileceği etkiyi anlamalıdır.[59]

Eğitimin temel hedefi, çalışanları kurumsal bilgi güvenliği hususundaki görev ve sorumlulukları hakkında bilinçlendirmektir. Ayrıca güvenlik ve güvenlik kontrollerinin önemi hakkında kollektif bir bilinç oluşturulması amaçlanmaktadır.

Kurumdaki tüm personelin bilgi güvenliğinin yarar ve öneminin farkına varması ve bu hususta bilinçlendirilmesi sağlanmalıdır. Çalışanların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması kritik öneme sahiptir.
Bilgi güvenliği ve bu hususstaki eğitimler çalışanlar tarafından eski köye yeni adet getirilmesi olarak algılanabilmektedir. Kullanıcılara göre kurum güvenlik önlemleri olmaksızın gayet iyi çalışmaktadır ve yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişikliklerdir. Çünkü alışkanlıkların değişmesi söz konusudur. Ancak kullanıcı odaklı eğitimlerle bu bakış açısı değiştirilebilir. Bilgi güvenliği, bilgi işlem işi olarak algılandığından çalışanlar güvenlik Bilgi Teknolojilerinin problemi olduğuna kendisi ile ilgili olmadığına inanmakta ve bu konuda bir sorumluluğu olmadığını düşünmektedir. Oysa bilgi güvenliği sadece Bilgi Teknolojilerinin ve bilgi işlem biriminde çalışanların değil tüm personelin sorumluluğudur.

Eğitimler herkese aynı biçimde ve aynı içerikte verildiğinde istenilen sonucu vermemektedir. Eğitim verilmeden önce eğitim gereksinimi belirlenip, sınıflandırma yapılıp her sınıfa özgü bir anlatım biçimi ve içerik belirlendiğinde daha etkin bir sonuç elde edilmektedir. Yeni teknolojinin kuruma katılması genellikle kullanıcı davranışlarının değişmesi veya yeni bir bakış açısına sahip olmasını gerektirir.

Ancak teknoloji bazen eğitimden hızlı veya bağımsız olarak ilerlemektedir. Dolayısıyla eğitimsiz olarak yeni teknolojinin kullanıma alınması söz konusu olursa bilgi güvenliğinde bir zafiyet oluşacaktır.

Bu noktadan hareketle eğitimin bir kereye özgü bir faaliyet olmaması gerektiği anlaşılmaktadır. Ancak ilk baştaki ilgi ve heyecanın kaybedilmemesi gerekmektedir. Aksi halde eğitimlerde bilgi güvenliği de bir angarya olarak görülecektir. İletişime öncelik verilerek eğitim alan insanların ihtiyaçları ve beklentileri doğrultusunda düzenli ve tutarlı programlar oluşturulması ve ilerletilmesi suretiyle ilgi canlı tutulabilmektedir.

Ancak unutulmaması gereken husus eğitim ile ancak iyi niyetli ve bilinçsiz kullanıcıların bilgi güvenliği ihlalini gerçekleştirmesinin önüne geçilebileceğidir. Eğitim kötü niyetli çalışanlara karşı alınacak önlemler arasında yer almamaktadır. İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bir eğitim programıyla riskin kabul edilebilir bir seviyeye indirilmesi sağlanabilmektedir.

EKLER

Risk Yönetimi

Risk, Fransızca risque olarak dilimize geçmiş olup sözlük anlamı "Riziko, zarara uğrama tehlikesi" şeklindedir. Risk (riziko), bir olayın gerçekleşme olasılığı ve olaydan etkilenme olanağı olarak tanımlanmaktadır. Genellikle risk olumsuz bir durum yani tehlike olarak değerlendirilir. Bu nedenle risklerin olumsuz etkilerinden zarar görmemek için olasılıklar göz önüne alınarak, önlemler almaya yönelik, çalışma ve planlama faaliyetlerini içeren ve risk yönetimi olarak anılan bir disiplin ortaya çıkmıştır. Risk, gelecekte oluşabilecek potansiyel problemlere, tehdit ve tehlikelere işaret eden, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşamama, kayba ya da zarara uğrama olasılığı olarak da tanımlanabilir.

Risk Yönetimi ise bir kurumun ya da kuruluşun çalışabilirliği, ticari kuruluşlar içinse öncelikle kârlılığını olumsuz yönde etkileyebilecek risk faktörlerinin belirlenmesi, ölçülmesi ve en alt düzeye indirilmesi sürecidir. Risk yönetiminde, riskin tamamıyla ortadan kaldırılması mümkün değildir. Sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesi amaçlanmaktadır. Başarılı bir risk yönetimi için, kuruluşların bilgi varlıklarına ve hedeflerine yönelik risklerin belirlenerek, analiz edilmesi, tanımlanan risklerin denetim altında tutularak izlenmesi gereklidir. Riski yönetmenin en doğru yolu, gerçekleşme olasılığı ve gerçekleştiğinde vereceği zarar en yüksek olan riskleri azaltacak bilgi teknolojisi risk yönetim sürecinin oluşturulmasıdır.

Tehditlerin Belirlenmesi

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır:

Doğal tehditler: Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler.

Çevresel tehditler: Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.

İnsan kaynaklı Tehditler: İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs. Tehdit değerlendirmesi sırasında hiçbir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir. Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir.

Açıklıkların Belirlenmesi

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir. Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde anket, birebir görüşme, dokümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir.

Risk Derecelerinin Tanımı

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçekleşmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir.

Risk Derecesi	Risk Açıklaması ve yapılması gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Bilgi Güvenliği İhlal Olayları Raporlama, Müdahale ve Kanıt Toplama

Aşağıdaki başlıklar ISO 27001 standardı temel gereksinimleri göz önünde bulundurularak hazırlanmıştır.

İhlal Olayları Raporlama

Bilgi güvenliği ihlal olayı tespiti sonrası olayla ilgili deliller toplanacak ve müdahale için sınıflandırılacaktır. Müdahaleden önce kayıtların toplanması, bozulması engellenecek şekilde saklanması ve yetkisiz erişime karşı korunmalıdır.

Kayıtlar ve içreği hakkında hazırlanan rapor en az aşağıdakileri içerir;

- Toplanan kanıtlar
- Kanıt türü
- Kanıt saklama yeri
- Kanıt tarihi ve zamanı
- İlgili Düzeltici Faaliyet kayıtları
- İhlal olayı tespit tarihi ve zamanı

Olayların öncelikledirilmesi için olayın etkisini kapsamını ve sınıflandırılması belirlemek amacıyla veriler incelenir. Bilgi güvenliği olayı için dikkat edilmesi gereken durumlar şunlardır:

İhlal Olayları Müdahale

Kontroller veya bildirilen durumlar ile tespit edilen ve delilleri toplanan tüm olaylar için diğer işlemlerden önce olaya sebep olan zafiyet düzeltilir.

Zafiyetlerin kapatılmasından sonra mutlaka kontroller tekrarlanır ve zafiyetin kapandığı onaylanır. Delilleri tahrip edecek veya bozacak hiçbir açıklık için kapatma işlemi gerçekleştirilmez.

Risk seviyesi çok yüksek olaylar için sistemler tamamen kapatılır veya diğer sistemlere erişimi engellenir.

Bilgi güvenliği ihlal olayına yapılan müdahaleler takip edilerek olay yönetimi, deneyim edinme ve önlem alma amacıyla kayıt altına alınır. Bilgi güvenliği ihlali kapsamında tespit edilen olayları yönetmek için düzeltici faaliyet başlatılır.

İhlal Olayları Kayıt ve Kanıt Toplama

Olayın tespiti ve sorumlunun belirleneceği kayıtların bütünlüğünün bozulmadığı kontrol edilir. Bütünlüğü kanıtlanamayan kayıtlar için işlemler yapılmaz.

- Bilgi güvenliği ihlal olayları için toplanan deliller 2 yıl boyunca silinmez.
- Sorumlu tespiti ile ilgili durumlarda kamera varsa mutlaka kamera kayıtları saklanır.
- Erişim kayıtları.
- Kontrol kayıtları.
- Sistem güvenlik yazılımları tarafından tutulan kayıtlar.
- Sorunların çözülmesi için gerekli maliyet kayıtları
- Bilgi güvenliği olaylarının değerlendirilmesi için ihtiyaç gösterebilecek ve gelecekteki olayların sıklığı, hasar ve maliyet sınırlarını belirleyecek kayıtlar.

Yakın Zamanda Kurumumuza Yapılan Siber Saldırılar ve Alınması Gereken Önlemler

1.Siber Olay Analizi

Genişbant hizmetleri ile ilgili bilgilerin yer aldığı ve Haberleşme Genel Müdürlüğü tarafından Tübitak'a yaptırılarak Bakanlığımız sunucularında "**genisbant.udhb.gov.tr**" alan adıyla hizmet vermekte olan genişbant portaline gidildiğinde siteden farklı bir siteye yönlendirmenin olduğu 01.12.2014 tarihinde 16:00 civarında tespit edilmiştir.

Teknik ekiplerimizce derhal siteye tüm erişimler durdurularak analizlere başlanmış ön analizler neticesinde sitenin veritabanında çeşitli saldırı yöntemleri ile bazı kullanıcı kayıtlarının oluşturulduğu ve veritabanındaki linklerinde değiştirilerek başka sayfaya yönlendirmelerin yapıldığı gözlemlenmiştir.

Ancak eldeki imkanlar ölçüsünde yapılan log incelemeleri ve analizler neticesinde tam olarak saldırının gerçek tarihi ve ilgili sitede yapılan değişikliklerle ilgili detaylı bilgilere erişilememiş olup detaylı analiz için Haberleşme Genel Müdürlüğü ilgilileri vasıtasıyla TÜBİTAK Siber Güvenlik Enstitüsünden destek talep edilmiştir.

TÜBİTAK Siber Güvenlik Enstitüsü ekibince siber güvenlik olayına 8-9 Aralık 2014 tarihleri arasında ivedilikle müdahale edilmiştir. Ekibin detaylı incelemesi neticesinde bahse konu siber güvenlik olayının bir "yetkisiz" içerik değiştirme (web defacement) saldırısı olduğu, saldırgan ilgili web sitesinde bulunan sıfırıncı gün açıklığından faydalanarak veritabanına

yerleştirdiği kod parçacığı sayesinde siteyi propaganda amacıyla oluşturduğu internet ortamında bulunan bir adrese yönlendirdiği tespit edilmiştir.

TÜBİTAK Siber Güvenlik Enstitüsü ekibince yerinde gerçekleştirilen çalışmalarında öncelikle saldırı izlerine ait kayıt bilgileri, uygulama kodları ve veritabanı incelenmiştir. Saldırıya uğramış uygulama ve veritabanı, saldırının etkileri giderilerek saldırı öncesi çalışabilir haline geri döndürülmüştür. Sonrasında yapılan incelemelerde saldırganın saldırıyı gerçekleştirme yöntemi tespit edilmeye çalışılmıştır. Aynı saldırı, test ortamında test edilip saldırının başarı ile sonuçlandığı anlaşılmıştır. Saldırının kaynağının Suriye kökenli, facebook ve twitter adreslerini kullanan "Dr.SHA6H" takma adlı bir saldırgan olduğu tespit edilmiştir.

Saldırıya maruz kalan uygulamanın Drupal isimli açık kaynak kodlu bir içerik yönetim sistemi kullandığı tespit edilmiştir. Bu aşamadan sonra içerik yönetim sistemine yönelik saldırılar gerçekleştirilmiştir. Yapılan incelemeler sonucu saldırganın "CVE: 2014-3704" kodlu zafiyeti kullandığı anlaşılmıştır. Bu zafiyet kodunun kullanıldığı IIS olay kayıtlarından da tespit edilmiştir.

Saldırganın bu saldırıyı 22 Kasım 2014 tarihinde gerçekleştirdiği, fakat söz konusu zafiyetin olayın açığa çıktığı tarihten önce de denendiği ve başarılı olunduğu anlaşılmıştır.

Etkilenen Sistemler	
IP Adresleri	İç IP: 172.16.0.5 Dış IP: 212.174.131.5
Sunucu Adları	genisbant
Sistem Rolü (Örneğin: DNS sunucu, yönlendirici, e-posta sunucu, uygulama sunucusu, vb.)	Uygulama Sunucusu
Etkilenen Sistemler (İşletim Sistemi, Veritabanı, Sunucular)	Windows Server 2008 R2, IIS 8.5, MySQL 5.5
Var olan Koruma Sistemleri (Örneğin: Güvenlik duvarı, saldırı tespit sistemi, antivirus yazılımı, vb.)	Checkpoint Firewall, Checkpoint IDS blade, F-Secure Antivirus

Saldırı Kaynağı	
Asıl Saldırı Kaynağı IP Adresi	83.96.94.25
Muhtemel Saldırı IP Adresleri	103.6.196.200, 58.97.141.85, 162.253.145.147, 60.49.94.145, 194.63.239.236, 175.141.118.144, 103.6.196.29, 62.248.35.176, 180.149.12.195, 111.243.251.162, 78.160.193.176
IP Adresleri Ülke Bilgisi	Malezya, Kuveyt, Bangladeş, Tayvan, Yunanistan, Türkiye
İlgili Diğer Bilgiler (Twitter, Facebook vb.)	https://www.facebook.com/Dr.SHA67 ?fref=photo https://twitter.com/DrSHA67/media Saldırgan Takma Adı: Dr.SHA6H

Tavsiyeler	
1	Saldırıya maruz kalan sistemdeki veritabanı için kayıt tutma mekanizması aktif edilmelidir.
2	Saldırıya maruz kalan uygulama sunucu için ileri düzey kayıt tutma (IIS Advanced Logging) seçeneği aktif edilmelidir.
3	Tüm uygulama sunucuları ve veritabanı gibi sistemlerin düzenli olarak yedeği alınmalıdır.
4	Tüm bilişim sistemleri güvenlik sıkılaştırma (hardening) işlemi yapılarak üretim ortamında kullanılmalıdır.
5	Düzenli olarak tüm sistemler üzerinde açıklık taraması yapılıp karşılaşılan açıklıklar sıkılaştırılmalıdır.
6	Düzenli olarak yamalar ve güncellemeler kontrollü olarak tüm sistemlere uygulanmalıdır.
7	Düzenli olarak tüm sistemlere sızma testleri yaptırılmalıdır.

2. Siber Olay Analizi

01.12.2014 tarihinde Saat 17:00 civarında güvenlik duvarı sistemlerinden siber saldırı alarmı alınmıştır. Yapılan ön incelemede Bakanlığımız web sayfasının olduğu 212.174.131.32 IP numaralı sunucuya DDOS (Servis Durdurma) saldırısı yapıldığı gözlemlenmiştir. Bu aşamada öncelikle güvenlik duvarındaki güvenlik önlemleri arttırılmış, akabinde internet hizmeti sağlayan ve ayrıca ekstra kurumsal güvenlik hizmeti aldığımız Türk Telekom A.Ş.'nin güvenlik grubu ile irtibata geçilmiştir. Saldırının Bakanlığımız sistemlerine ulaşmadan Türk

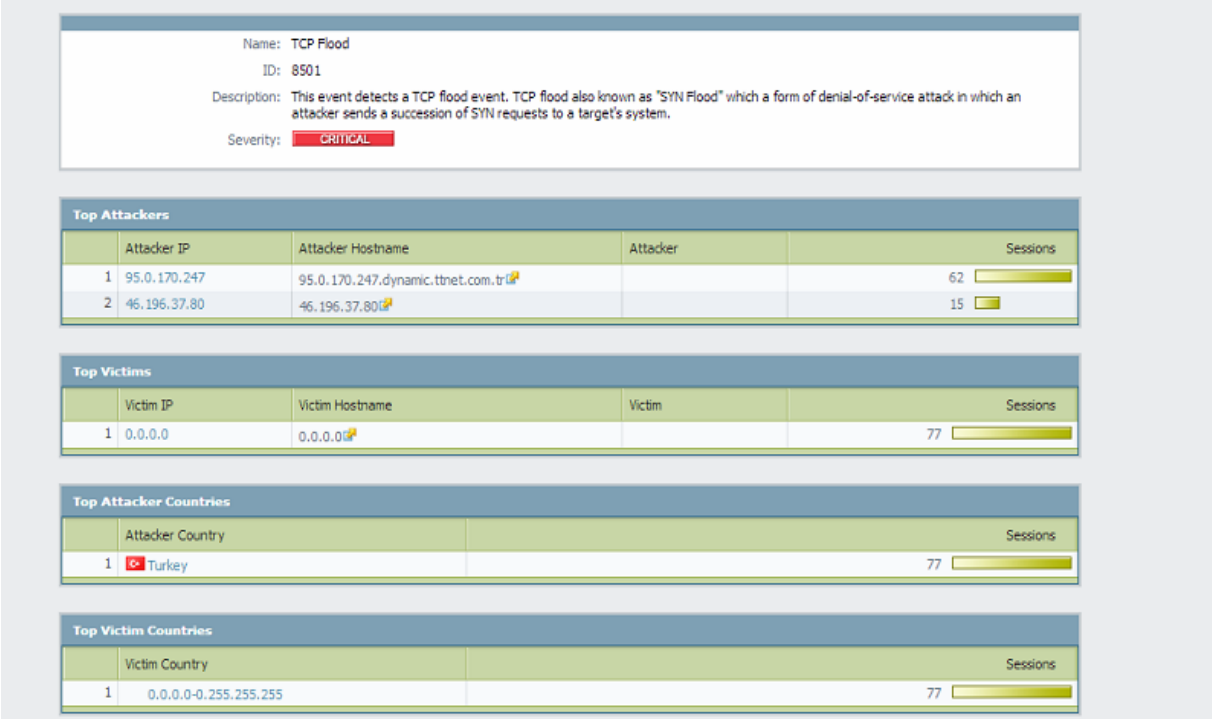
Telekom A.Ş. sistemlerinde kesilmesi sağlanmıştır. Türk Telekom A.Ş. sistemlerinden elde edilen bilgiler ve yapılan detaylı analizler aşağıda özetlenmiştir.

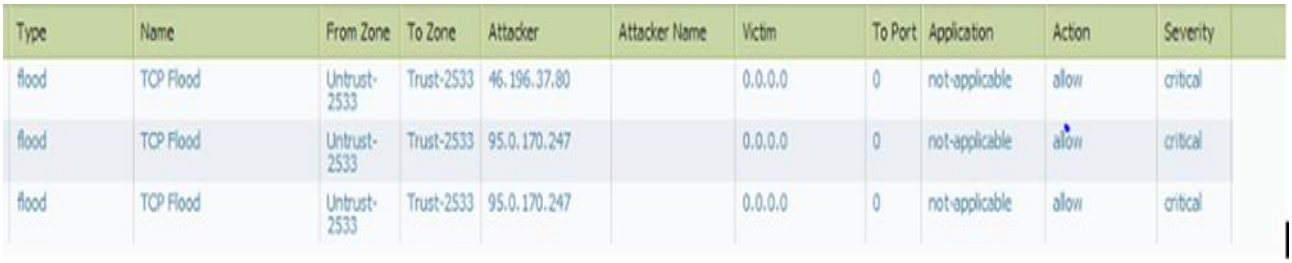
Source address	Source Host Name	Destination address	Destination Host Name	Threat/Content Name	ID	Action	Repeat Count
95.0.170.247	95.0.170.247	0.0.0.0	0.0.0.0	TCP Flood	8501	allow	62
46.196.37.80	46.196.37.80	0.0.0.0	0.0.0.0	TCP Flood	8501	allow	15

yapılan istekler analiz edildiğinde, saldırının iki IP'den yapıldığı tespit edilmiştir.

- 95.0.170.247 (Çalışma ve Sosyal Güvenlik Bakanlığına ait)
- 46.196.37.80 IP'si (Türksat'a ait).

Web sitesi IP 'sine doğru 3 adet flood trafiği gözlemlenmiştir.
Flood olduğu için saldırı yapılan ip görünmemekle birlikte trafik loğunda 212.174.131.32 nolu ip adresine doğru olduğu(trafiğin) gözlemlenmiştir.





Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
flood	TCP Flood	Untrust-2533	Trust-2533	46.196.37.80		0.0.0.0	0	not-applicable	allow	critical
flood	TCP Flood	Untrust-2533	Trust-2533	95.0.170.247		0.0.0.0	0	not-applicable	allow	critical
flood	TCP Flood	Untrust-2533	Trust-2533	95.0.170.247		0.0.0.0	0	not-applicable	allow	critical

Olay Tanımı	
Olayın Tespit Edildiği Tarih / Zaman	01 Aralık 2014 17:00
Olayın Gerçekleştiği Tarih / Zaman	01 Aralık 2014 17:00-19:00
Olay Türü **(Örneğin: DDOS, Web defacement, virus, vb.)**	DDOS (Distributed Denial of Service) (Dağıtık Hizmet Engelleme)
Kaynak Adresler	95.0.170.247 46.196.37.80
Saldırı Yöntemi **(Örneğin: Açıklığın sömürülmesi, ele geçirilen hesap, vb.)**	DDOS (Distributed Denial of Service) (Dağıtık Hizmet Engelleme)

Etkilenen Sistemler	
IP Adresleri	212.174.131.32
Sunucu Adları	www.udhb.gov.tr
Sistem Rolü **(Örneğin: DNS sunucu, yönlendirici, e-posta sunucu,**	Web Sunucusu

uygulama sunucusu, vb.)	
Etki Seviyesi	WEB sunucusuna saldırı süresince zaman zaman erişilememe durumu oluşmuş ancak Bakanlık ve Türk Telekom IDS/IPS sistemlerinin devreye girmesi ile saldırı bertaraf edilmiştir.
Var olan Koruma Sistemleri (Örneğin: Güvenlik duvarı, saldırı tespit sistemi, antivirus yazılımı, vb.)	Checkpoint Firewall, Checkpoint IDS blade, F-Secure Antivirus, Türk Telekom Güvenlik hizmeti.

3. Hatalı Nat-Pmp Uygulamalarından Kaynaklanan Güvenlik Açıklığı

Genel Bilgi

NAT-PMP, güvenilir bir yerel sunucu ile dış ağ arasındaki trafiği yönlendirmek amacıyla genellikle yönlendirici (router) gibi bir ağ adresi dönüştürme (NAT) cihazının kullanıldığı bir protokol olarak tanımlanmaktadır. RFC 6886, sayılı IETF dokümanına göre NAT ağ geçidinin dış IP adresine gelen veya dış ağ arayüzü aracılığıyla alınan port adresleme (port mapping) taleplerine cevap vermemesi gerekmektedir. Buna ilave olarak port mapping taleplerinin iç sunucunun kaynak adresine yönlendirilmesi gerekmektedir. NAT-PMP cihazların hatalı yapılandırma veya başka bir nedenle bu koşulları yerine getirmemesi durumunda, söz konusu cihazlar kötü amaçlı port adreslemelerine izin verebilmekte veya cihaz bilgilerinin açığa çıkmasına yol açabilmektedir.

Etki

Söz konusu güvenlik açıklığına yönelik bir siber saldırı sonucunda, saldırganlar tarafından NAT cihazı bilgilerinin ele geçirilmesi, cihazdaki port adreslemesinin manipüle edilmesi, iç ve özel trafik bilgileri ile servislere erişim sağlanması veya sunucu hizmetlerinin engellenmesi mümkün olabilmektedir.

Çözüm

Kullanılan cihazların tedarikçileriyle irtibata geçilerek, cihazların mevcut güvenlik açıklığından etkilenme durumunun öğrenilmesi ve NAT-PMP cihazlarında doğru yapılandırmaların kullanılması önem arz etmektedir. Ayrıca güvenlik duvarlarında, güvenilmeyen adreslerden port 5351/UDP'ye olan erişimlerin engellenmesini sağlayacak

kurallar tanımlanması ile kullanımı zorunlu haller haricinde, cihazlar üzerinde NAT-PMP protokolünün pasif hale getirilmesi tavsiye edilmektedir.

4. Ssl 3.0'deki Poodle Güvenlik Açıklığı

Genel Bilgi

SSL 3.0'ın OpenSSL'in 1.0.1i sürümünün de dahil olduğu birden fazla uygulamasında CBC modunun kullanımı desteklenmektedir. SSL 3.0'de CBC modu kullanıldığında padding oracle saldırısına hedef olabilecek bir güvenlik açığı bulunmaktadır.

Buna ilave olarak birçok yeni TLS istemcilerinin, eski sunucularla haberleşebilmesi amacıyla halen SSL 3.0 protokolünü de desteklediği bilinmektedir. Bu durumda man in the middle saldırısı yapan bir saldırganın bir sistemde mevcut protokolü SSL 3.0'e indirgeyerek padding oracle saldırısı için hedef haline getirmesi mümkün olabilmektedir. Bu saldırı türü genellikle "POODLE" (Padding Oracle On Downgraded Legacy Encryption) olarak adlandırılmaktadır.

Etki

Saldırı sonucunda SSL 3.0 protokolünü CBC modunda kullanıldığı şifreli haberleşme İçeriğine yetkisiz erişim sağlanabilmektedir.

Çözüm

Söz konusu açıklık ile ilgili olarak Open SSL'in 1.0.1j, 1.0.0o ve 0.9.8zc sürümleri için güvenlik güncellemesi yayınlanmıştır. Protokolün diğer uygulamalarının söz konusu güvenlik açıklığından etkilenme durumu konusunda tedarikçi firmalarla irtibata geçilmesi tavsiye edilmektedir.

SSL 3.0'ün devre dışı bırakılmasının mümkün olmadığı durumlarda TLS istemci ve sunucularında TLS_ FALLBACK_SCSV şifreleme mekanizması kullanılarak man-in-the-middle saldırıları aracılığıyla protokol sürümlerinin indirgenmesi engellenebilir.

5. 24.11.2014 - Wordpress Tarafından Yeni Güvenlik Güncellemesi Yayınlandı

Genel Bilgi

WordPress'in halen kullanımda olan bazı sürümlerinde "cross-site scripting" türünde bir güvenlik açıklığı bulunmaktadır.

Etki

Söz konusu güvenlik açıklığı nedeniyle siber saldırganlar tarafından bir sitenin ele geçirilmesi, kullanıcıların şifre değişikliğine yönlendirilmesi ve eski kullanıcı hesaplarının ele geçirilmesi ihtimal dahilindedir. Güvenlik açıklığından Word Press 3.9.2. ve önceki sürümleri etkilenmektedir.

Çözüm

Kullanıcıların konu ile ilgili olarak WordPress tarafından yayınlanan güvenlik bültenini (WordPress Maintenance and Security Release) inceleyerek sistemlerinde gerekli güncellemeleri yapmaları tavsiye edilmektedir.

Kurumumuza Yapılabilecek Olası Saldırı Senaryoları ve Yapılması Gereken İşlemler

SENARYO 1

Enjeksiyon İçeriği

1. Ütopya Büyükşehir Belediyesi'nin sistem yöneticisi, 23-25 Ocak 2015 tarihleri arasında kurumumuza ait IP havuzuna ait bir IP'den 130 spam e-postanın kendi kurumlarının farklı kullanıcılarına yollandığını tespit etmiştir.

2. Ütopya Büyükşehir Belediyesi'nin sistem yöneticisi, söz konusu spam e-posta saldırısının önlenmesi, detaylarının ortaya konması ve failleri ile ilgili kurumumuzdan bilgi istemiştir.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Söz konusu saldırı ihbarının gerçekliği nasıl doğrulanmıştır ?

2. Sözü edilen spam e-posta saldırısının gerçekten sizin kurumdan yapılıp yapılmadığının tespiti nasıl yapılmıştır ?

3. Söz konusu faaliyeti gerçekleştiren kişi veya kişiler nasıl tespit edilmiştir ?

4. Bu faaliyetin devam etmemesi için ne tür tedbirler alınmıştır ?

5. Benzeri faaliyetlerin bir daha gerçekleştirilememesi için ne tür tedbirler alınmıştır ?

6. Faaliyetle ilgili tespitlerden sonra nasıl bir hukuki ve idari süreç çalıştırılmıştır ?

Yapılması Gereken İşlemler

1- Saldırı ihbarının gerçekliği resmi yazı ve mail yolu ile tespit edilmelidir.

2- 23-25 Ocak tarihleri arasında kurumumuz mail sunucusundan ilgili kurumun mail sunucusuna giden mail trafiği izlenerek tespit edilmelidir.

3- Mail Güvenlik sistemi loglarından saldırıyı gerçekleştiren makinaların ipleri belirlenerek tespit edilmelidir.

4- Spam yapan makinalar güvenlik yazılımlarıyla taranarak temizlenmiştir. Bilinçli saldırı yapan kullanıcılar hakkında idari ve hukuki süreç başlatılmalıdır.

5- Mail güvenlik sistemi güncellemeleri ve yamaları geçilmiştir. Yerel güvenlik araçları güncellenmelidir.

Mail sisteminin benzeri bir olay karşısında Mail sistemi yöneticisine e-mail ve sms yoluyla uyarı göndermesi sağlanmalıdır.

6- Tüm kullanıcılar iç duyuru sistemiyle uyarılmalıdır. Güvenlik politikasına dahil olmayan ve olmak istemeyen kullanıcılar idari olarak uyarılmalıdır.

SENARYO 2

Enjeksiyon İçeriği

1. Kurumumuzun bilgi işlem biriminde veritabanı yöneticisi olarak çalışan personel birim müdürüyle yaptığı sert tartışmalar sonrasında kurumdan ayrılma kararı almıştır.

2. 20 Ocak 2015 tarihinde işten ayrılan veritabanı yöneticisi, 19 Ocak 2015 tarihinde işten ayrılmadan önce veritabanı üzerinde zamanlanmış görev tanımlamış ve bu görevle veri tabanında 2014 yılına ait muhasebe verilerinin 23 Ocak 2015 tarihinde silinmesini sağlamıştır.

3. 27 Ocak 2015'de 2014 yılı muhasebe kayıtlarına ait rapor almaya çalışıldığında bu verilerin silindiği görülmüştür.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Veri tabanında hangi verilerin silindiği nasıl tespit edilmiştir ?

2. Silinen verilerin kurtarılması için ne yapılmıştır ?

3. Silinmiş verinin tekrar kullanılır hale gelmesi ne kadar sürede sağlanmıştır ?

4. Verilerin kaybının sebebi nasıl araştırılmıştır ?

- **a.** Veri silmenin yöntemi nasıl bulunmuştur ?

b. Silme işleminden sorumlu olan hesap ve silme tarihi tespit edilebilmiş midir ?

c. Eğer saldırganın kullandığı hesap tespit edildiyse saldırganın kimliğine ulaşılabilmiş midir ? (Ortak hesap mı kullanılıyor yoksa kişiye özel hesap mı ?)

5. Kurtarma işleminde geri kazanılamayan veri var mıdır ? (yedekleme yapılan zamanlar göz önünde bulundurulacaktır.)

6. Hukuki bir süreç işletilmiş midir ?

a. Suç duyurusu ve ekleri nelerdir ?

Yapılması Gereken İşlemler

1- Veritabanı sunucusu üzerindeki sistem logları incelenerek çalıştırılan script bulunmalı ve ilgili script incelenerek veritabanındaki muhasebe kayıtlarına ait verileri silmek için yazılıp yazılmadığı tespit edilmelidir.

Ayrıca Veritabanı logları incelenerek geriye doğru çalıştırılan sorgular ve komutlarla da doğrulanmalıdır..

2- 2014 Yılında alınan veritabanı yedeğinden muhasebe kayıt geri dönülmelidir.

3- Veritabanı yöneticisi ve uygulamacılar çalışarak 24 saat içerisinde 2014 yılına ait verileri kullanabilir hale getirmelidir.

4- Veritabanı ve sistem üzerindeki loglar ve ilgili script incelenerek tespit edilmelidir.

a- Veritabanı yöneticisinin çalıştırdığı script ve veritabanı logları incelenerek silme yöntemi bulunmalıdır.

b- Veritabanı loglarından ve sistem loglarından silme işleminden sorumlu olan hesap ve silme sorgusu tespit edilmelidir.

c- Saldırganın kullanıdığı hesab tespit edilmekle birlikte ortak hesap olduğu için saldırganın kimliği doğrulanamaz.

Ancak Saldırganın çalışmak için veritabanı sunucusuna bağlandığı ip üzerinden saldırganın kulandığı bilgisayara ulaşılabilinir.

5- Yedekler, günlük, haftalık, aylık ve 6 Aylık olmak üzere ayarlanırsa kurtarma işleminde geri kazanılamayan veri olmamalıdır. 6 Ay öncesi veriler güvenli bir yerde muhafaza altına alınmalıdır.

6- Verilerin silindiği ve saldırganın kimliği belirlendiği, yapılan fiil ile bilişim araçları vasıtasıyla kamu kurumuna ait verilerin imha edilmesi durumu söz konusu olduğundan, ilgili hakkında savcılığa suç duyurusunda bulunulmalıdır.

a- Suç duyurusu dilekçesine sistemden alınan kayıtlar, yapılan fiilin kayıt örneği ve yapılan fiil sonucunda oluşan zarara air ekran görüntüleri ile gerek duyulması halinde durumun tespitini ve delilleri güvene almak için yapılan noter tespitine ait dokümanlar eklenmelidir.

SENARYO 3

Enjeksiyon İçeriği

1. Bir kurum çalışanı tarafından, bilgi işlem birimine, kendisine gelen şüpheli bir e-posta ile ilgili ihbarda bulunulmuştur.

2. Kurum çalışanı, maaş hesabının bulunduğu bankanın müdürünün adına bir e-posta hesabıyla gönderilmiş olarak görünen bir mesaj aldığını ve mesajın ekinde zip uzantılı bir dosyanın bulunduğunu iletmiştir.

3. Mesajda, "Yeni yıldaki maaş promosyonlarınızı ve hesaba geçeceği tarihi ekteki dosyada bulabilirsiniz." ifadesi yer almaktadır**.**

4. Kurum çalışanı ekteki dosyayı açmış ama bu bilgiye ulaşamamıştır.

5. Kurum çalışanı bu durumu şüpheli bulup bilgi işlem birimini aramıştır.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır

1. Bu olay bir saldırı olarak değerlendirilmiş midir ?

2. Gönderilen e-postanın zararlı kod içeren eklentiye sahip olup olmadığı nasıl tespit edilmiştir ?

(Eklentinin zararlı kod içerdiği ve kurumsal olarak kullanılan anti virüs tarafından tespit edilemediği varsayılacaktır.)

3. Zararlı kodun bulaştığı sistemlerin temizlenmesi için hangi çalışmalar yapılmıştır ?

4. Kurum dışı üçüncü taraflardan bu konuda destek alınmış mıdır ?

5. Zararlı kod içeren eklentiyi açan kurum çalışanının güvenliğini sağlamak için neler yapılmıştır ?

6. Benzer bir duruma maruz kalmış olabilecek kurumun diğer çalışanları tespit edilmiş midir ?

Bu çalışanların tespiti nasıl gerçekleştirilmiştir ? Söz konusu çalışanların güvenliğini sağlamak için neler yapılmıştır ?

7. Diğer çalışanların benzer bir saldırıya maruz kalma ihtimaline karşı ne tür önlemler alınmıştır ?

Yapılması Gereken İşlemler

1- Bu olay bir siber saldırı olarak değerlendirmelidir.

2- İlgili dosya, dosya analizi yapan web sayfalarına gönderilerek taratılmalı ve zararlı kod olup olmadığı anlaşılmalıdır.

3- Zararlı kodun bulaştığı sistemlerin ağ erişimi kesilmelidir.

Anlaşmalı olduğumuz antivirüs şirketine dosya gönderilip analiz yapılarak çözüm bulunması istenmelidir.

Zararlı koda karşı çözümü olan antivirüs firmalarından biriyle anlaşılıp sistemlerin temizlenmesi sağlanmalıdır.

4- İlgili probleme çözümü olan bir firmadan destek alınmalıdır.

5- İlgili kurum çalışanının bilgisayarı temizlenene kadar ağ erişimi kesilmelidir.

Banka hesapları ile ilgili güvenlik bilgilerini değiştirme hususunda uyarıda bulunulmalıdır.

6- Kurum içi duyuru sistemiyle olay diğer kullanıcılara duyurularak diğer mağdur kullanıcılar tespit edilmeye çalışılmalıdır.

Mail güvenlik sisteminde saldırgan kaynaktan gelen tüm e-mailler taratılarak kime geldiği belirlenmeye çalışılmalı tüm e-mailler taratılarak ilgili eke sahip olan e-maillerin kime geldiği tespit edilmelidir.

7- Kurum içi duyuru sistemiyle tüm kullanıcılar benzer olay ve olaylara karşı uyarılmalıdır. Anlaşmalı olunan antivirüs sisteminin güncellemesiyle birlikte tüm makinalar merkezi olarak taratılmalıdır.

SENARYO 4

Enjeksiyon İçeriği

1. İnternet üzerinden kurumumuz adına gönderilmiş olarak görünen e-postalar gözlemlenmeye başlamıştır.

2. Kurumumuzdan gönderilmiş olarak görünen e-postalarda, kullanıcıların web sayfanızdan indirecekleri yazılımla sisteminizden faydalanabilecekleri belirtilmiştir.

3. Sahte e-postadaki bağlantı ile ulaşılan web sayfası kurumumuzun sayfasının kopyalanmış halidir.

4. Sahte sayfa Kamanga ülkesinden yayın yapmaktadır.

5. Sayfa üzerinden indirilmesi istenen yazılım zararlı kod içermektedir ve kullanıcıların kişisel bilgilerini çalmayı amaçlamaktadır.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Kullanıcıların/Vatandaşların zarar görmemesi için hangi işlemler yapılmıştır ?

2. Zararlı yazılım ile ilgili bir çalışma yapılmış mıdır ?

3. Sayfaya erişimin önlenmesi için neler yapılmıştır ?

Yapılması Gereken İşlemler

1- Yapılan oltalamayla ilgili olarak tüm kullanıcılara iç duyuru sistemi yoluyla, vatandaşlara da internet sitesi üzerinden duyuru yapılmalıdır. Öncelikle yerel kullanıcıların sayfaya erişimi güvenlik duvarından önlenmelidir. Vatandaşların erişimi Bilgi Teknolojileri Kurumuna yapılan başvuruyla önlenmelidir.

2- Zararlı yazılım, analiz sayfalarında analiz ettirilerek varlığından diğer antivirüs firmalarının haberdar olmaları sağlanmaya çalışılmalıdır. Zararlı yazılımın bağlantı kurmaya çalıştığı IP adresleri belirlenmelidir.

3- Yerel kullanıcılardan, ilgili IP adreslerine ve web sayfasına yapılan istekler güvenlik duvarı üzerinden engellenmelidir. Vatandaşların korunması için zararlı yazılım ve ilgili web sitesi hakkında Bilgi Teknolojileri Kurumuna bilgi verilip, erişimin engellenmesi istenmelidir.

SENARYO 5

Enjeksiyon İçeriği

1. Kurumun bulunduğu bölgede bakım çalışmaları nedeni ile bir günlük bir elektrik kesintisi yaşanacağı elektrik dağıtım şirketi tarafından duyurulmuştur.

2. Kurum elektrik kesintilerine karşı kesintisiz güç sistemi (KGS) ve jeneratöre sahip olduğundan herhangi bir hazırlık yapmamıştır.

3. Elektrik kesintisi gerçekleştiği zaman KGS devreye girmiştir. KGS'nin dayanma süresi 1 saattir. Elektrik kesintisinden kısa bir süre sonra devreye girmesi gereken jeneratör sistemi devreye girmemiştir.

4. Jeneratör devreye alınamadığı takdirde en geç bir saat içinde sistem odasında bulunan tüm donanımlar enerji olmadığı için kapanacaktır.

5. Yapılan arıza tespit çalışmaları sonucunda jeneratörün yakıtının bulunduğu, aküsünün sağlam olduğu fakat motorda mekanik bir sorun olduğu tespit edilmiştir.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Elektrik kesintisi sonrasında jeneratörün devreye girmediği ne kadar süre sonra ve nasıl anlaşılmıştır ?

2. Jeneratörün arızasının tespit edilmesi için hangi çalışmalar gerçekleştirilmiştir ?

3. Jeneratör arızasının mekanik problemlerden kaynaklandığı tespit edildikten sonra hangi işlemler yapılmıştır ?

a. Arızanın giderilmesi için gerçekleştirilen faaliyetler iş sürekliliği planına göre mi yapılmıştır ?

b. Bir saat içinde sorun çözülemedi ise sistemlerin güvenli kapatılması için herhangi bir işlem yapılmış mıdır ?

Yapılması Gereken İşlemler

1- Elektrik kesintisi duyurusu önceden yapıldığı için gerekli hazırlıklar yapılmalıdır. Bu itibarla KGS ve jeneratör sistemi gözlem altına alınmıştır. Kesinti başladıktan sonra jeneratörün devreye girmesi gereken sürede yani 1-2 dakika içinde devreye girmediği görüldüğü zaman jeneratör sisteminde bir arıza olduğu anlaşılmalıdır.

2- Öncelikle gözle gerekli kontroller yapılmalı ve sistemdeki arıza tespit edilmeye çalışılmalıdır. Yakıt, akü, enjektörler, ilk hareket sistemi v.b. mekanik sistemlerin dıştan kontrolü yapılmaya çalışılmalıdır.

3- Arızanın mekanik olması ve motordan kaynaklanıyor olması durumunda, bu arızayı giderecek durumda olunmadığı için jeneratörün bakımından ve arızasından sorumlu firmaya derhal haber verilmelidir.

a- Gerekli girişimler iş sürekliliği planına göre yapılmalıdır..
b- KGS sisteminin kapanmasından önce kullanıcılar uyarılarak sistemlerin güvenli şekilde kapatılması sağlanmalı, ayrıca ana sistem üzerinde de bu yolda gerekli hazırlıklar yapılmalıdır.

SENARYO 6

Enjeksiyon İçeriği

1. Kurum içinde kablosuz ağ kuruludur ve yayınlanan SSID dikkat çekmemesi için "kablosuz_ag" olarak belirlenmiştir.

2. Bir kurum çalışanı "Kurum_Adı" kablosuz ağ ismi (SSID si) ile bağlanılabilinen bir erişim noktası (access point) tespit ettiğini bilgi işleme birimine bildirmiştir.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Söz konusu erişim noktasının yeri ve kullandığı İnternet hattı nasıl tespit edilmiştir? (Kurum yakınındaki bir noktada farklı bir İnternet hattı kullanıldığı ve buraya erişim noktası bağlandığı varsayılacaktır.)

2. Kurum çalışanlarının bu bağlantıyı kullanıp kullanmadıkları nasıl tespit edilmiştir?

3. Bu tür bir yetkisiz bağlantının kurum çalışanlarına zarar vermemesi için hangi önlemler alınmıştır?

Yapılması Gereken İşlemler

1- İhbar eden kullanıcının odasına gidilerek şüpheli ağa dahil olunup, internet çıkış IP'si üzerinden servis sağlayıcısı belirlenmelidir. ISS'den gelen cevapla erişim noktasının adresi ve yeri bulunmalıdır.

2- El konulan accespoint, modem vb. cihazlar üzerindeki DHCP loglarındaki MAC adresleri ile kurum kullanıcılarının MAC adresleri karşılaştırılarak şüpheli ağa dahil olan kurum kullanıcıları tespit edilmelidir.

3- Kurum çalışanlarına Kurum SSID'sinin "kablosuz_ag" olduğu, başka ağlara dahil olmamaları konusunda duyuru yapılmalıdır. Kurum binalarının etrafına diğer yayınların kurum içine yapılmasını, kurum yayınının da dışarıya yapılmasını engelleyici cihazlar yerleştirilmelidir.

SENARYO 7

Enjeksiyon İçeriği

1. Kurumumuzun resmi web sayfasının İçeriği yetkisiz kişilerce gerçekleştirilen saldırı sonrasında değiştirilmiştir.

2. Giriş sayfanıza saldırgan tarafından eklenen yazıda kurum çalışanlarınıza ve kurumumuzdan hizmet alan vatandaşlara ait bilgilerin ele geçirildiği ve yakında bu bilgilerin İnternet üzerinden yayımlanacağı görülmektedir.

3. 25 Ocak 2015 tarihinde saat 13.35'te bilgi işlem biriminizi arayan kurum içi bir kullanıcının sayesinde durumdan haberdar olunmuştur.

4.Kurumumuzun uğradığı saldırıyla ilgili ulusal basın yayın organlarında 25 Ocak 2015 tarihinde saat 15.23'te haberler çıkmaya başlamıştır.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Bilgi işlem birimine kurum içi kullanıcı tarafından ihbar geldikten sonra olay nasıl doğrulanmıştır?

2. Sayfanın ele geçirildiği belirlendikten sonra yapılan teknik faaliyetler nelerdir?

a. Sistemin ne zaman ele geçirildiği nasıl tespit edilmiştir?

b. Sistemin nasıl ele geçirildiği tespit edilmeye çalışılmış mıdır? Neler yapılmıştır?

c. Veri sızması olup olmadığı nasıl tespit edilmiştir?

3. Sayfanın tekrar uygun içerikle erişilebilir olması nasıl, ne kadar sürede sağlanmıştır?

4. Diğer sistemlerin zarar görmesi nasıl önlenmiştir?

5. İlgili olayda hukuki olarak bir çalışma yapılmış mıdır?

a. Suç duyurusu ve ekleri nelerdir?

Yapılması Gereken İşlemler

1- Web Sayfa İçeriği yerel ağdan ve dış ağdan kontrol edilmeli, üzerindeki bilgilerin değiştirildiği teyit edilmelidir.

2- Güvenlik, Sistem ve uygulama logları üzerinde incelemeler yapılmalıdır.

a. Web sunucusu üzerindeki uygulama loglar incelenerek tespit edilmelidir.

b. Güvenlik sistemleri üzerindeki loglar incelenerek saldırı türü tespit edilmelidir.

c. Web Sunucusu üzerindeki güvenlik ve uygulama logları incelenerek veri sızması olduğu tespit edilmelidir.

3- Saat 14:00'da Saldırıyla ilgili olarak uygulamacı personel haberdar edilerek, yapılan değişik bildirilmelidir. İlgili personel tarafından 14.15'de müdahale edilmeli. 14.45'de içerik düzeltilmiş olmalıdır.

4- Web sunucusu DMZ (*demilitarized zone*) alanında olduğu için diğer sistemlerde erişimi hali hazırda kısıtlıdır. Bu kısıtlama güvenlik sistemleriyle sağlandığından ilgili güvenlik sistemi diğer sistemlere yapılan saldırıyı engellemiş olmalıdır.

5- Bilgi İşlem Dairesi tarafından Hukuk Müşavirliğine saldırı konusunda yazı yazılmalıdır.

Hukuk Müşavirliğine; yapılan saldırının niteliği, meydana getirdiği etki, saldırı sonucu ekranlarda görünen ekran görüntüsünü gösteren renkli çıktı(screenshoot) ve saldırıyı yapanlara ait tespit edilmiş IP numaraları, eventlog kayıtları tutanak ile yazı ekinde gönderilmelidir. Yapılan saldırı "internet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun" ve "Türk Ceza Kanunu" ve diğer ilgili mevzuata göre suç teşkil etmektedir. Hukuk Müşavirliğince alınan yazı ve eklerine göre yapılan fiilin suç teşkil ettiği için, gelen veriler düzenlenen suç duyurusu

dilekçesine eklenerek Nöbetçi Savcılığa bildirilmeli ve saldırganların cezalandırılması ile birlikte saldırının devam etme olasılığına karşı durumun Telekomünikasyon İletişim Başkanlığına da bildirilmesi gerekmektedir. Saldırının ulusal güvenlik açısından büyük tehlike arz edebileceği durumu da göz önüne alınarak delillerin kaybolmasını önlemek üzere noter tespiti yapılmalıdır.

SENARYO 8

Enjeksiyon İçeriği

1. Kuruma ait dış dünyaya ve kuruma hizmet veren DNS sunucusuna, farklı kaynaklardan sahte kaynak IP adreslerine sahip UDP istekleri gönderilmiştir.

2. Sunucu, yoğun trafikten dolayı normal DNS sorgu isteklerinin önemli bir kısmına cevap verememektedir.

3. Bu durum DNS sunucuya yapılan bir UDP seli dağıtık servis dışı bırakma saldırısıdır.

4. Normal kullanıcıların kurumun web sitesine erişimi büyük oranda aksamıştır.

5. Kurum kullanıcılarının İnternet çıkışlarında da büyük oranda aksamalar yaşanmaktadır.

6. Kurum çalışanlarının e-posta gönderme ve almalarında önemli oranda aksamalar yaşanmıştır.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. DNS sunucusunun servis verememesindeki temel darboğazın kaynağını nasıl tespit edilmiştir?

2. DNS servisinin tekrar çalışabilir hale getirilmesi için neler yapılmıştır ?

3. Saldırının önlenmesi için neler yapılmıştır ?

4. Saldırının kaynağını tespit edilebilmiş midir ?

Yapılması Gereken İşlemler

1- Güvenlik sistemleri üzerindeki loglar izlenerek DNS sunucusuna dns flooding yapıldığı tespit edilmelidir.

2- Dış DNS Servisinin IP adresi lokalden ve ULAKBİM üzerinden değiştirilerek yapılandırılmalıdır.

3- ISS'e saldırı hakkında çağrı açılarak güvenlik duvarı üzerinden ilgili ip'ye gelen istekler Reject edilmelidir.

4- Saldırıda kullanılan ipler tespit edilmeli ve saldırının kaynağı hakkında ISS'den bilgi alınmalıdır.

SENARYO 9

Enjeksiyon İçeriği

1. İnternet üzerinden yayılmaya başlayan yeni bir solucan ortaya çıkmıştır.

2. Bu solucan yayılmak için Microsoft sistemleri üzerinde bulunan, iki hafta önceki güncellemelerde yaması yayınlanan bir açıklığı kullanmaktadır.

3. Solucan aşağıdaki yollarla yayılmaktadır:

a. Enfekte olan bilgisayar üzerindeki e-posta adreslerine kendini yollayarak,

b. Erişim yetkisi olan Windows paylaşımlarını tespit edip bu paylaşımlara kendini kopyalayarak.

4. Solucan kendini e-posta kullanarak yayarken, her e-posta için rastgele bir dosya adı kullanmaktadır ve dosya uzantısı olarak 10 tane farklı uzantıdan birini seçmektedir.

5. Solucan, e-postalarda konu olarak 100'den fazla konu içeren bir listeden seçim yapmaktadır.

6. Solucan, e-postaların mesaj kısmı için yaklaşık 100 farklı konunun bulunduğu geniş bir listeden seçim yapmaktadır.

7. Anti virüs üreticileri bu solucanla ilgili uyarıları yayınlamışlardır fakat anti virüs üreticileri virüse ait imzaları yayınlamadan önce, solucan kurum sistemlerine bulaşmıştır.

8. Virüs bulaştığı bilgisayarların Windows güncellemelerini ve anti virüs güncellemelerini almalarını önlemektedir.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Bu olaya müdahale ederken solucanın bulaştığı tüm sistemler nasıl tespit edilecektir?

2. Solucanın yayılmasını önlemek için hangi önlemler alınacaktır?

3. Solucanın bulaştığı sistemler üzerinde hangi çalışmalar yapılacaktır?

4. Sistemler zararlı yazılımdan temizlendikten sonra kurum içerisinde bir bilgilendirme yapılacak mıdır?

5. Solucan saldırısına müdahale ederken kurum dışından yardım alınacak mıdır?

6. Kurum dışından yardım alınması durumunda üçüncü kişilerle/kurumlarla hangi esaslara göre irtibata geçileceği belli midir?

Yapılması Gereken İşlemler

1- Microsoft Sistemlerden iki hafta önceki yamayı geçmeyenler, Domain Controller üzerinden tespit edilmelidir.

2- Tespit edilen sistemlere ilgili yama geçirilerek , Merkezi Antivirüs sistemi üzerinden antivirüs güncellenmelidir.

3- Solucanın bulaştığı sistemlerin sabit diskleri, update-yama vs leri yüklenmeli ve temiz bir bilgisayar tarafından taratılarak temizlenmelidir.

4- Temizlenmeden önce bilgilendirme yapılmalıdır.

5- Güvenlik firması tarafından yardım alınmalıdır.

6- Gizlilik sözleşmesi imzalanmış bir firmayla irtibata geçilmeli, sözleşmeli firma yok ise ilgili firma ile gizlilik sözleşmesi imzalanmalıdır.

SENARYO 10

Enjeksiyon İçeriği

1. Bir kurum çalışanı tarafından bilgi işlem birimi aranarak kendisine şüpheli bir telefon geldiği bildirilmiştir.

2. Kurum sabit hattına gelen telefonda, şüpheli kendini bilgi işlem biriminde yeni çalışmaya başlayan bir kişi olarak tanıtmıştır.

3. Sistemde güncelleme yaptıklarını belirterek kurum kullanıcısının etki alanına girerken kullandığı kullanıcı adı ve parolayı istemiştir.

4. Kurum kullanıcısı kendine ait olan kullanıcı adı ve parolayı telefondaki şüpheliye vermiştir. Daha sonra bu durumu şüpheli bulup bilgi işlem birimini aramıştır.

Tepki mesajında aşağıdaki soruların cevapları bulunmalıdır.

1. Bu olay bir saldırı olarak değerlendirilmiş midir?

2. Telefon konuşmasındaki kişinin bir saldırgan olup olmadığı, kimliği nasıl tespit edilmiştir?

3. Parolasını veren kurum çalışanının güvenliğini sağlamak için neler yapılmıştır?

4. Benzer bir duruma maruz kalmış olabilecek kurumun diğer çalışanları tespit edilmiş midir? Bu çalışanların tespiti nasıl gerçekleştirilmiştir?

Söz konusu çalışanların güvenliğini sağlamak için neler yapılmıştır?

5. Diğer çalışanların benzer bir saldırıya maruz kalma ihtimaline karşı ne tür önlemler alınmıştır?

Yapılması Gereken İşlemler

1- Bu olay saldırı olarak değerlendirilmelidir.

2- Gelen telefonun yerelden mi? yoksa dışardan mı? olduğu kontrol edilmelidir.

Yerel ağdan olduğu durumda; ilgili personelle iletişime geçilerek hakkında idari ve hukuki soruşturma başlatılmalıdır.

Dışardan olduğu durumda; ilgili telefon görüşmesini yapanın bulunması için savcılığa suç duyurusunda bulunulmalıdır.

3- İlgili kullanıcının kullanıcı adı ve parolası değiştirilip, eski kullanıcı adı ve parolası silinmelidir.

4- Konuyla ilgili olarak tüm kurum personeline mail/sms gönderilerek böyle bir durumla karşılaşanlar tespit edilmelidir.

Tespit edilen personelin kullanıcı adı ve şifresi değiştirilmelidir.

5- Konuyla ilgili olarak tüm kurum personeline mail/sms gönderilerek böyle bir saldırının varlığından haberdar edilmelidir.

Ayrıca domain controller tarafındaki kullanıcı adı ve şifre politikası güncellenmelidir.

KAYNAKLAR

1. VURAL Y. SAĞIROĞLU Ş. Kurumsal Bilgi Güvenliği ve Standartları Üzerine bir inceleme Gazi Üniv. Müh. Mim. Fak. Der. Cilt :23 No: 2 2008.
2. Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü Tübitak-UEKAE-BGYS-001 Sürüm 1.002007 ÖNEL D. DİNÇKAN A. Bilgi Güvenliği Yönetim Sistemi Kurulumu 7-9 Gebze
3. Her Yönüyle Siber Savaş, Hasan Çifci, TÜBİTAK Popüler Bilim Yayınları, Haziran 2013
4. Cybersecurity: The Essential Body Of Knowledge by Dan Shoemaker and Wm. Arthur Conklin (May 17 2011
5. Cybersecurity: Public Sector Threats and Responses (Public Administration and Public Policy) by Kim J. Andreasson (Dec 20 2011
6 . AKGÜL Mustafa. *Türkiye interneti'nin ve internet Kurulunun Kısa Tarihi* Türkiye Bilişim Derneği 2001
7. James Graham and Ri chard Howard, et all , ***Cyber Security Essentials***, Boca Rat on, Auerbach Publi cat i ons, 2010, pp. 198, 199
8. Tan. H. "Kurum ve Kuruluşların Bilgi Sistemi Güvenliği ve Bir Uygulama"
9. James A. Lewis – Katrina Timlin, "Cybersecurity and Cyberwarfare", Center For Strategic and International Studies, 2011,p. 14.
10. Chen Zhou, "A Review of China's Military Strategy," China Armed Forces 1:1 (2009): 19.
11. Estonia Ministry of Defense, Cyber Security Strategy Committee, Cyber Security Strategy, Talin 2008
12. "France Country Report", European Network and Information Security Agency, 2010, <www.enisa.europa.eu/act/sr/files/country-reports/France.pdf>, pp. 5, 23.
13. NATO and Cyber Defence, Rex B. Hughes, Ap:2009nr1/4
14. Siber Güvenlik Raporu Mayıs 2012

15. 5237 sayılı Türk Ceza Kanunu, Beta Yayınları, 2013.

16. Evik V., Sınar H., Erman B., Kurt G., 'Bilişim Hukuku', Güncel Hukuk Dergisi, 2013, s. 17-18.

17. Centel N., Zafer H., Çakmut Ö., 5271 sayılı Ceza Muhakemesi Kanunu, 2013.

18. "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı", T.C. Resmi Gazete, 20 Haziran 2013. http://www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf

19. TS ISO/IEC 27001: Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler, TSE, Mart 2006

20. ISO/IEC 27032: Bilgi Teknolojisi – Güvenlik Teknikleri – Siber Güvenlik Kılavuzu, Temmuz 2012

21. "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar", Resmi Gazete, http://www.resmigazete.gov.tr/eskiler/2012/10/20121020-181.pdf, Ekim 2012

22. Kalkınma Bakanlığı, Bilgi Toplumu Stratejisi ve Eylem Planı (2006-2010) Nihai Değerlendirme Raporu, 2013

İnternet Kaynakları

1. http://utsam.org/images/upload/attachment/cilt4/Sayi2

2. http://eturksoft.com/Adepo/Haber/Dosya/772.pdf

3. http://www.abuyum.com/Assets/Content/file/pdf/bilisimsuclari.pdf

4. BGA, **"Günümüz Internet Dünyası nda IP Spoofi ng"**, <http:/ /blog.bga. com.tr / network-securit y/ gunumuz-internet -dunyasinda-ip-spoofi ng>, 03.05.2012

5. http://www.cehturkiye.com/index.php/2008/06/28/sniffing-ve-korunma-yollari/sniffing-ve-korunma-yollari.html

6. http://www.mustafakaya.com.tr/sniffing-ve-korunma-yollari.html

7. http://blog.btrisk.com/2014/05/dos-turleri.html

8. https://www.bilgiguvenligi.gov.tr/ag-guvenligi/yeni-nesil-ddos-saldirilari-ve-savunma-yontemleri-i.html

9. BGA, "Günümüz Internet Dünyasında IP Spoofing", <http://blog.bga.com.tr /network-security/gunumuz-internet-dunyasinda-ip-spoofing>, 03.05.2012.

10. http://80.251.40.59/science.ankara.edu.tr/ozbek/kripto1.htm

11. http://dokumanistan.blogspot.com.tr/2012/07/internet-protocol-security.html

12. Bican, C. 2008. Sosyal Mühendislik Saldırıları, Ulusal Bilgi Güvenliği Kapısı. http://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html

13. www.iscturkey.org/iscold/ISCTURKEY2013/files/paper81.pdf

14. www.iscturkey.org/iscold/ISCTURKEY2013/files/paper81.pdf

15. www.iscturkey.org/iscold/ISCTURKEY2013/files/paper81.pdf

16. www.cyber-warrior.org/Dokuman/Default.Asp?Data_id=4670

17. http://telekom.com.tr/blog/arka-kapilar-backdoors

18. http://www.olympos.net/belgeler/turkiyede-phishing-126266.html

19. http://eturksoft.com/Adepo/Haber/Dosya/772.pdf

20. https://sisli.iem.gov.tr/?page_id=210&uyari_id=1

21. http://www.langturk.com/rootkit-nedir/

22. http://serkanaltintas.blogspot.com.tr/2011_01_01_archive.html

23. James Graham and Richard Howard, et all, Cyber Security Essentials, Boca Raton, Auerbach Publications, 2010, pp. 198, 199

24. Richard Kissel (Ed.), Glossary of Key Information Security Terms, National Institute of Standards and Technology, 2011, <http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>, 08.03.2012, p. 196

25. <http://windows.microsoft.com/trTR/windows-vista/Viruses-frequently-asked-questions>,17.04.2012.

26. http://tr.wikipedia.org/wiki/Bot_(robot)

27. SearchSecurity İnternet Sitesi, Botnet (Zombie Army), <http://searchsecurity.techtarget.com/definition/botnet>, 17.04.2012.
28. Kishore Subramanyam and Charles E. Frank et all, "Keyloggers: The Overlooked Threat to Computer Security", <http://www.keylogger.org/articles/kishore-subramanyam/keyloggers-the-overlooked-threat-to-computersecurity-html#.T6GcbOs9XmQ>,03.05.2012.
29. http://www.ckk.com.tr/ders/communication.pdf
30. https://www.bilgiguvenligi.gov.tr/siber-savunma/5.-boyutta-savas-siber-savaslar-ii.html
31. http://www.bilgiguvenligi.gov.tr/zararli-yazilimlar/flame-en-buyuk-en-karmasik-siber-casusluk-yazilimi.html
32. http://www.btd.gazi.edu.tr/article/viewFile/1041000047/1041000045
33. Bilişim Güvenliği Sürüm 1.1,Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003
34. Bilişim Güvenliği Sürüm 1.1,Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003
35. Bilişim Teknolojilerinde Risk Yönetimi, TBD Kamu –BİB Kamu Bilişim Platformu VIII.
36. http://www.sgb.gov.tr
37. http://www.emo.org.tr/ekler/3f3c315eef29de0_ek.pdf
38. http://www.emo.org.tr/ekler/3f3c315eef29de0_ek.pdf
39. http://www.emo.org.tr/ekler/3f3c315eef29de0_ek.pdf
40. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
41. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
42. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
43. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
44. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)

45. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
46. Siber Güvenlik Raporu(Taslak10-090512)-SiberGuvenlikCalismaGrubu.doc (Mayıs, 2012)
47. http://www.tbb.org.tr/content/upload/dokuman/801/bilisim_hukuku.pdf
48. http://www.beyaz.net/tr/tabdetay/5651-sayili-kanun.html
49. www.resmigazete.gov.tr/eskiler/2013/06/20130620-1-1.pdf
50. http://www.iscturkey.org/iscold/SiberGuvenlikHukukCalistayi/SonucBildirgesi.pdf
51. http://www.siberstrateji.com/wp-content/uploads/2013/10/Ulusal-Siber-Guvenlik-Stratejisi-ve-2013-2014-Eylem-Plani.doc
52. www.resmigazete.gov.tr/eskiler/2013/11/20131111-6.htm
53. http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/siberguvkurulu.php
54. http://www.siberguvenlik.org.tr/
55. http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/tatbikatlar.php
56. https://www.tse.org.tr/upload/tr/dosya/icerikyonetimi/551/17102014094159-1.pdf
57. https://www.bilgiguvenligi.gov.tr
58. http://www.kascert.com/
59. http://www.sgb.gov.tr/MaliyeUzmYrdArasRaporlari

ÖZGEÇMİŞ

Doğum Tarihi: 01/12/1983

Doğum Yeri: Kırıkkale

Lise: (1994-2001) Kırıkkale Anadolu Lisesi

Lisans: (2001-2009) Gebze Yüksek Teknoloji Enstitüsü(GYTE) Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü

Çalıştığı Kurum

(Nisan 2009- Mayıs 2010 – ETL Proje Grubu) RDC Partner

(Haziran 2010- Devam Ediyor) T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı