
GAZİ ÜNİVERSİTESİ
Gazi
1926

KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNDE İÇ TEHDİT ETKİSİ

Uğur ARAS

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2020

Uğur ARAS tarafından hazırlanan "KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNDE İÇ TEHDİT ETKİSİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. İbrahim Alper DOĞRU

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi ……..……..

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. Türksel KAYA BENSGHIR

İşletme Ana Bilim Dalı, Ankara Hacı Bayram Veli Üniversitesi ...……

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Aysun COŞKUN

Bilgisayar Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi ...……

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 30/06/2020

Jüri tarafından kabul edilen bu çalışmanın Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Uğur ARAS
30/06/2020

KRİTİK ALTYAPILARIN SİBER GÜVENLİĞİNDE İÇ TEHDİT ETKİSİ

(Yüksek Lisans Tezi)

Uğur ARAS

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2020

ÖZET

Kritik altyapılar hemen her alanda olduğu gibi bilişim sitemleri aracılığıyla işletilmektedir. Bilgi ve iletişim teknolojilerinin kullanımı, sağladığı birçok fayda olmasına karşın kritik altyapıları siber saldırılara açık hâle getirmektedir. Siber saldırının dışarıdan geleceğiyle ilgili genel bir yanlış kanı bulunmaktadır fakat günümüzde iç tehdit her geçen gün artan bir yere sahiptir. Ayrıca, iç tehdidin zarar vereceği sistemi zaten tanıyor olması ve tespitinin çok daha güç olması gibi kendine has özellikleri bu olguyu çok yönlü bir araştırma konusu haline getirmektedir. Bu çalışmada, siber güvenliğinin sağlanması hayati öneme haiz olan kritik altyapılarda iç tehdit etkisi incelenmiştir. İç tehdidin önemi, nedenleri, motivasyonları, gelişmiş ısrarcı tehdit ile ilişkisi ortaya konduktan sonra iç tehdide karşı alınabilecek önlemler belirtilmiştir. Çalışmada, açık kaynak kodlu bir endüstriyel kontrol sistemleri bal küpü uygulaması ile iç tehdidin tespiti önerilmiştir. Bal küpüne gelen istekler bir SIEM yazılımından izlenerek görünürlük sağlanmıştır. Sistem bir test senaryosu ile sınanarak iç ağda kullanılan bir bal küpü uygulamasının kritik altyapılardaki iç tehdide karşı güvenliği artıracağı tespit edilmiştir.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	İç tehdit, Siber güvenlik, Kritik altyapılar, Bal küpü
Sayfa Adedi	:	123
Danışman	:	Doç. Dr. İbrahim Alper DOĞRU
2. Danışman	:	Prof. Dr. Ercan Nurcan YILMAZ

INSIDER EFFECT ON CYBER SECURITY OF CRITICAL INFRASTRUCTURES

(M. Sc. Thesis)

Uğur ARAS

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2020

ABSTRACT

Critical infrastructures are operated through information systems, as in almost every field. The use of information and communication technologies makes critical infrastructures vulnerable to cyber attacks although it has many benefits. A very common misbelief is that cyber attack will originate from the outside but nowadays the occurance of insider threat is increasing everyday. The insider already knows the system. Besides, it is much more complicated to detect threat, as it is hard to distinguish malicious network traffic from legitimate traffic. These unique features of insider threat make this phenomenon a sophisticated research subject. In this study, we examine insider effect on cyber security of critical infrastructures which is crucial for national security. After describing the importance, causes, motivations of insider threat and relations with APTs, the measures in the literature that can be taken against it are specified. An open source ICS honeypot is proposed to detect the threat. Network visibility is ensured with a SIEM software by monitoring the requests which come to honeypot. The system has been tested with a scenario, and it has been found that a honeypot used in the internal network will increase security against insider threats in critical infrastructures.

Science Code	:	92403
Key Words	:	Insider threat, Cyber security, Critical infrastructures, Honeypot
Page Number	:	123
Supervisor	:	Assoc. Prof. İbrahim Alper DOĞRU
Co Supervisor	:	Prof. Dr. Ercan Nurcan YILMAZ

TEŞEKKÜR

Çalışmalarım boyunca engin bilgi ve tecrübeleriyle bana yol gösteren ve hiçbir zaman desteğini esirgemeyen değerli danışman hocalarım Sayın Prof. Dr. Ercan Nurcan YILMAZ ve Sayın Doç. Dr. İbrahim Alper DOĞRU'ya, yüksek lisans öğrenimim boyunca manevi desteğini daima sürdüren sevgili eşime, 2211 Yurt İçi Lisansüstü Burs Programı desteğiyle eğitimime katkı sağlayan TÜBİTAK'a ve kurumumda yüksek lisans eğitimime destek olan çalışma arkadaşlarım ve değerli amirlerime teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

RESİMLERİN LİSTESİ

Resim **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
ABAC	Attribute Based Access Control
ANSI	American National Standards Institute
BES	Bulk Electric System
BTK	Bilgi Teknolojileri ve İletişim Kurumu
BYOD	Bring Your Own Device
CIWIN	Critical Infrastructure Warning Information Network
CMP	Certificate Management Protocol
CRL	Certificate Revocation Lists
DAC	Discretionary Access Control
DOD	Department of Defense
EAP	Extensible Authentication Protocol
EKS	Endüstriyel Kontrol Sistemleri
ENISA	European Union Agency for Cybersecurity
EPCIP	European Programme for Critical Infrastructure Protection
EPDK	Enerji Piyasası Düzenleme Kurumu
EST	Enrollment over Secure Transfer
ETSI	European Telecommunications Standards Institute
FBI	Federal Bureau of Investigation
FPGA	Field Programmable Gate Array
GDOI	Group Domain of Interpretation
GKRY	Güney Kıbrıs Rum Yönetimi

Kısaltmalar	Açıklamalar
ICS	Industrial Control Systems
IDS/IPS	Intrusion Detection System / Intrusion Prevention System
IEC	International Electrotechnical Comission
IED	Intelligent Electronic Device
IEEE	Institute of Electrical and Electronics Engineers
IIoT	Industrial Internet of Things
IKEv2	Internet Key Exchange version 2
IPMI	Intelligent Platform Management Interface
ISA	International Society of Automation
ISO	International Organization for Standardization
KİT	Kamu İktisadi Teşebbüsü
MAC	Mandatory Access Control
MIB	Management Information Base
MTD	Moving Target Defense
MTU	Master Terminal Unit
NERC	North American Electric Reliability Corporation
NIPC	National Infrastructure Protection Center
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OT	Operasyonel Teknolojiler
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PyPI	Python Package Index
RBAC	Role Based Access Control

Kısaltmalar	Açıklamalar
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrollment Protocol
SIEM	Security Information Event Management
SOME	Siber Olaylara Müdahale Ekibi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UDHB	Ulaştırma Denizlik ve Haberleşme Bakanlığı
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
UKUSA	United Kingdom – United States of America
USB	Universal Serial Bus
USSS	United Stated Secret Service
VPN	Virtual Private Network
XML	Extensible Markup Language

1. GİRİŞ

Bir ülkenin can damarları olarak adlandırılabilecek kritik altyapılar günümüzde her alanda olduğu gibi bilgi teknolojilerine dayanmaktadır. Ulaşımın, elektriğin, iletişimin olmadığı, sağlık hizmetlerinin verilemediği ya da milli savunmaya ait bilgilerin diğer ülkelerin eline geçtiği bir ülke için milli güvenlikten bahsetmek mümkün olmaz. Uzak bir ihtimal gibi görünse de sıralanan bu vakaların yaşanabilmesi çok da zor değildir. Çünkü dijitalleşen dünyanın bir gereği olarak her bir altyapı, kara, hava, deniz ve uzaydan sonra savaşın 5. boyutu sayılan siber uzayda[1] varlık göstermektedir. Dahası siber dünyada bir saldırı gerçekleştirmek, gerçek dünyada bir saldırı gerçekleştirmekten çok daha düşük maliyetli ve daha az risklidir. Ayrıca tespit ve teşhisi de bir o kadar güçtür.

Kritik altyapı bilgi sistemleri geçmişte geniş alana bağlanmayan kapalı sistemler olarak algılandığından siber güvenliğe yönelik önlemler düşünülmemiştir [1]. Ancak Stuxnet ve benzer olaylar kapalı diye düşünülen sistemlere de sızılabileceğini göstermiştir. Dahası günümüzde artık bu sistemler coğrafi olarak farklı yerlerde bulunan diğer sistemlerle de iletişim kurmakta dolayısıyla geniş alana bağlanmakta hatta ağ içinde bazı uç kullanıcılar internete erişim sağlamaktadırlar. Bugüne kadar kritik altyapıların siber güvenliğine yönelik yapılan çalışmalar daha çok dışarıdan gelebilecek tehditleri incelemişlerdir. Bu çalışma bugüne kadar yapılan çalışmalardan farklı olarak kritik altyapıların siber güvenliğine yönelik içeriden gelebilecek insan kaynaklı tehditleri incelemektedir.

Yöntem olarak öncelikle iç tehdidin tanımı, sınıflandırılması, motivasyonları ortaya konmuş ve iç tehdide neden olan etkenler araştırılmıştır. Bu bilgiler ışığında iç tehdide karşı alınabilecek önlemler belirlenmiş, iç tehdidin tespiti ve azaltılmasına yönelik literatürde yapılmış çalışmalar ayrıntılı olarak ele alınmıştır. Yapılan değerlendirmeler neticesinde kritik altyapılarda iç tehdidin tespitine yönelik bir endüstriyel kontrol sistemleri bal küpü önerilmiş ve bir test senaryosu ile bal küpünün etkinliği sınanmıştır.

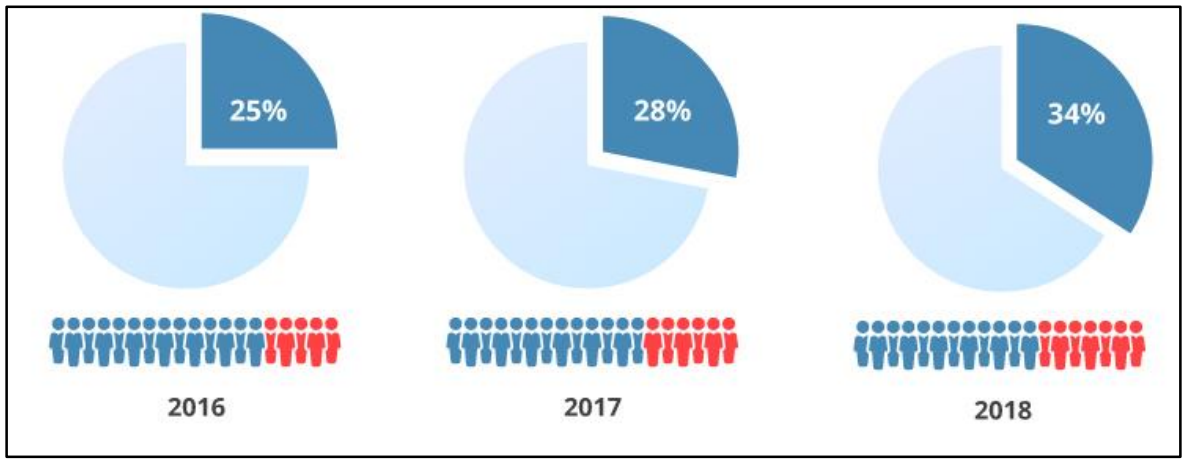
Verizon'un 2019 yılında yapmış olduğu araştırmaya göre 2018 yılında gerçekleşen veri sızıntılarının %34'ü iç tehdit kaynaklıdır [2]. Ponemon Enstitüsünün araştırmasına göre iç tehdit kaynaklı bir olayın ortalama maliyeti 513 000 dolar civarındadır. Yıllık bazda ise iç

[1] NATO, Temmuz 2016'daki Varşova Zirvesi'nde kara, hava ve denizden sonra siber uzayı da yeni bir operasyon alanı olarak kabul etmiştir.

tehdit kaynaklı olaylar bir şirkete 8.76 milyon dolar zarar verebilmektedir [3]. Sadece 2018 yılında yaşanan vakalar bile tarihin en maliyetli iç tehdit kaynaklı veri sızıntıları olmuştur [4].

Oteller zinciri Marriott firmasının rezervasyon sistemi veri tabanından yaklaşık 500 milyon müşteri bilgisi sızdırılmıştır. Firma güvenlik açığını bir iç güvenlik aracı vasıtasıyla öğrenmiştir [5]. Tesla, Martin Tripp isimli işten ayrılmış bir çalışanını şirketin hassas ve ticari sır niteliğindeki bilgilerini yasa dışı olarak ele geçirip 3. taraflara aktarmaktan dolayı mahkemeye vermiştir. Şirket, yaklaşık 1 milyon dolar zarara uğradığını bildirmiştir [6]. Kritik altyapılara bakıldığında ise Hindistan'a ait Punjab National Bank sahte SWIFT transferlerinden dolayı 1,8 milyar dolar dolandırılmıştır. Olay sonrası Gokulnath Shetty isimli bir müdür yardımcısı SWIFT sistemine yetkisiz olarak erişim yetkisine sahip oluğunu itiraf etmiş ve sonrasında tutuklanmıştır [7]. ABD'de bulunan SunTrust bankası, eski bir çalışanının müşteri iletişim listelerini çalması sonucu 1,5 milyona yakın müşteri hesap bilgisinın kurum dışına sızmasına sebep olmuştur [8]. ABD'de bir kişinin AT&T isimli telekomünikasyon şirketindeki çalışanlara, şirket ağına zararlı yazılım yüklemeleri ve telefonların SIM kilitlerini kırmaları için 2012-2017 yılları arasında 1 milyon dolardan fazla rüşvet verdiği ortaya çıkmıştır [9]. İç tehdit kaynaklı olayların büyük bir bölümünün de kurum dışına rapor edilmediği değerlendirilmektedir [10].

2019 yılında iç tehdidin maliyeti 2018'e göre %15 oranında artmıştır. Ayrıca iç tehdit kaynaklı sorun yaşayan firma sayısındaki artış Şekil 1.1'de gösterilmiştir [4].



Şekil 1.1. İç tehditlerden zarar gören şirketlerin oranı [4]

Firmalar ve şirketler yaşanan olaylarda hem maddi kayıplara, hem de itibar kaybına uğramışlardır. 2018 yılında yaşanan iç tehdit kaynaklı vakalar çoğunlukla maddi zarar yaratmış olsalar da kritik altyapılarda meydana gelen iç tehdit kaynaklı sızıntı ve ataklar geçmişte, Snowden ve Manning vakalarında olduğu gibi, ulusal güvenliği tehdit edecek boyutlara da ulaşmıştır.

İç tehdidin tespitinin zor olması, herhangi bir güvenlik tedbirini aşmak zorunda olmaması ve kurum içi bilgiye sahip olması gibi etkenler siber güvenlik açısından büyük bir sorun sahası yaratmaktadır. Bunun yanında, kritik altyapılar gibi hassas tesis ve kurumlarda risk faktörü çok daha büyümektedir. Dolayısıyla kritik altyapı bilgi sistemlerinde iç tehdidi savunmak da yıllardır üzerinde çalışılan önemli bir uğraş alanıdır.

Tehlikenin farkında olan devletler iç tehdidi ve savunma yöntemlerini siber güvenlik stratejilerine, bilgi güvenliği ve siber güvenlik standartlarına dâhil etmişlerdir. ABD İç İşleri Bakanlığı web sitesinde iç tehditlerin azaltılmasına yönelik ayrı bir alan ayırmıştır [11].

İç tehdit, kurum içinde fiziksel ya da mantıksal olarak meşru erişim yetkisine sahip olan kişinin bu yetkiyi bilinçli ya da bilinçsiz olarak kuruma zarar verecek şekilde kullanması olarak tanımlanabilir. Her ne kadar bazı kaynaklar iç tehdidi tanımlarken bilgisiz ve dikkatsiz kullanıcıları içeren grubu tanıma dâhil etmeseler de güncel çalışmalar [12-13] zarar verme kastıyla hareket etmeyen personeli de iç tehdit kapsamına sokmaktadır. İç tehdit tanımıyla ilgili diğer bir sorun ise “içerideki” kavramının kendisiyle alakalıdır. Eski bir çalışan, taşeron personel, kurum dışından destek sağlayan kişi “iç” tehdit olarak tanımlanabilmektedir [14].

Kritik altyapılarda iç tehdide yönelik çalışma yapmanın en önemli sınırlılığı ise konuyla ilgili gerçek veri seti elde etmenin bir hayli zor olmasıdır. Bunun nedeni, iç tehdidin yarattığı trafiğin meşru trafikten ayırt edilmesinin yarattığı güçlüktür. Bu nedenle bazı çalışmalar sentetik veri üretme yoluna gitmişlerdir [15].

Çalışmanın 2. bölümünde kritik altyapı ve kritik altyapı bilgi sistemlerine yönelik kavramsal çerçeve sunulmuş, ayrıca kritik altyapıların korunması ve güvenliğine yönelik standart ve rehberler ele alınmıştır. Bu bölümde ADB, AB ve Türkiye’nin kritik altyapılara yönelik gerçekleştirdiği yasal düzenlemelere ve geçmiş faaliyetlerine yer verilmiştir. 3. bölümde iç

tehdidin tanımı yapılmış, iç tehdide etki eden faktörler ve iç tehdidin motivasyonları anlatılmış, iç tehdidin önemi araştırmalarla ve yaşanmış olaylarla açıklanmıştır. Ayrıca kritik altyapılarda iç tehdidin azaltılmasına yönelik yapılan çalışmalar incelenmiş ve bu bilgiler ışığında iç tehdidin azaltılmasına yönelik önlemlerden bahsedilmiştir. 4. bölümde iç tehditlerin tespiti amacıyla endüstriyel kontrol sistemlerinde çeşitli protokolleri simüle edebilen bir bal küpü uygulaması önerilmiş, bal küpüne gelen trafiğin izlenmesi amacıyla Splunk yazılımı kullanılmış ve önerilen yöntem bir test senaryosu aracılığıyla değerlendirilmiştir. 5. bölümde ise sonuçlar ve önerilere yer verilmiştir.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde kritik altyapı ve kritik altyapı bilgi sistemlerine yönelik tanımlamalar yapılmış, ABD, AB ve Türkiyedeki kritik altyapı bilgi sistemlerinin korunmasına yönelik oluşturduğu yasal mevzuat incelenmiştir. Ayrıca kritik altyapıların korunması ve güvenliğine yönelik standart ve rehberler ele alınmıştır.

2.1. Kritik Altyapılar

Bilgisayar ve bilgisayar ağları o kadar hızlı hayatımıza girmiştir ki elektrik, su, haberleşme, ulaşım ve sağlık gibi günlük hayatımızın olmazsa olmaz ögeleri de teknolojinin gelişimiyle beraber ortaya çıkan tüm kolaylıklardan zaman kaybetmeksizin faydalanmışlardır. Tesis ve altyapıların "dijitalleşmesi" ile beraber daha iyi bir izleme ve kontrol sağlanmış, bu sayede edinilen sağlıklı bilgilerle arıza tespit oranları artmış ve süreçlere müdahale yeteneği kazanılmıştır. Elektrik, su ve doğalgaz gibi üretim, iletim ve dağıtımı bir arada bulunduran şebekeler "akıllı" hale gelmiştir. Tüm bu çabaların asıl amacı şüphesiz ki kullanıcıya daha etkin, kaliteli ve kesintisiz bir hizmet sunabilmektir. Fakat birçok kolaylık sağlamasına rağmen söz konusu altyapıların bilgi ve iletişim teknolojileri ile iç içe geçmesi bu hizmetleri siber saldırılara karşı hassas duruma getirmiştir. Kesintiye uğraması ya da tutarlı çalışmaması durumunda ülke çapında ciddi zararlara yol açabilecek elektrik, su, sağlık, kamu hizmetleri, iletişim, ulaşım, savunma ve güvenlik gibi bilgi teknolojileri ile yönetilen kritik altyapıların güvenliği ulusal güvenlik için de hayati bir konudur.

2.1.1. Tanımı, kapsamı ve önemi

Kritik altyapılar ülkemizde Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ile "işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar" olarak tanımlanmıştır [16].

ABD İç İşleri Bakanlığı "Kritik altyapı, iş görememesi veya yıkımı fiziksel veya ekonomik güvenlik veya halk sağlığı veya asayiş üzerinde ABD için zayıflatıcı bir etkisi olan fiziksel ve siber sistemleri ve varlıkları tanımlar" şeklinde tanımlamıştır [17].

AB ise “Kritik altyapı, hayati toplumsal işlevlerin sürdürülmesi için gerekli olan bir varlık veya sistemdir. Kritik bir altyapının zarar görmesi, doğal afetler, terörizm, suç faaliyeti veya kötü niyetli davranış nedeniyle tahrip olması veya yıkımı, AB'nin güvenliği ve vatandaşlarının refahı için önemli olumsuz etkiye sahip olabilir.” şeklinde tanımlar [18].

2018 yılı itibariyle ABD, AB ve Türkiye’nin kritik altyapı sektörleri Çizelge 2.1’de verilmiştir.

Kritik altyapıların korunması ve güvenliği konularında ABD ve AB gibi diğer birçok ülke de yıllar öncesinden ülke politikalarını oluşturmuş ve gerekli yasal düzenlemelerini yapmışlardır. Bunun sebebi kritik altyapılara yönelik tehditlerin her geçen gün artıyor olması ve aynı zamanda kritik altyapı sistemlerinde meydana gelebilecek zararların ulusal güvenliği de tehlikeye atacak olmasındandır.

ABD İç İşleri Bakanlığı 2015 yılı için endüstriyel kontrol sistemlerine yönelik 300 civarı atağın kurumlar tarafından raporlandığını bildirmiştir. Raporlanmayan atakların ise bunun yaklaşık 3 ya da 4 katı olduğu düşünüldüğünde ülkede günde birden fazla endüstriyel kontrol sistemlerine yönelik atağın meydan geldiği sonucuna ulaşılmaktadır [19].

Çizelge 2.1. ABD, AB ve Türkiye kritik altyapı sektörleri [20,21,16]

ABD	AB	Türkiye
Su ve atık su sistemleri	Su	Su yönetimi
Bilgi Teknolojileri	Bilgi İletişim Teknolojileri	Elektronik Haberleşme
Enerji	Enerji	Enerji
Nakliye Sistemleri	Taşımacılık	Ulaştırma
Finansal Hizmetler	Finans	Bankacılık ve Finans
Savunma Sanayi	Kamu ve Yasal Düzen ve Emniyet	Kritik Kamu Hizmetleri
Kimya	Kimya ve Nükleer Sanayi	
Tarım ve gıda	Gıda	
Sağlık	Sağlık	
Acil Hizmetler	Uzay ve Araştırmalar	
Barajlar		
İletişim		
Nükleer Reaktör, Madde, Atıklar		
Ticari Tesisler		
Kritik Üretim		
Devlet Tesisleri		

ABI Research isimli kuruluşun yaptığı araştırmaya göre kritik altyapıların güvenliğine yönelik yapılan harcamaların 2023 ile beraber dünya çapında 125 milyon doları bulacağı söylenmiştir. Araştırmada bilgi teknolojileri (BT) ile operasyonel teknolojiler (OT) arasındaki güvenlik anlayışı farkını kapatmanın kritik altyapıların güvenliğini sağlamada önemli bir etken olduğu belirtilmiştir. Ayrıca kritik altyapıların siber güvenliğindeki en büyük engelleri, hükümetlerin kritik altyapıların korunmasını siber güvenliğin bir alt dalı olarak algılaması ve konuyla ilgili idari ve yasal düzenlemelerin yapılmasındaki yavaşlık olarak tanımlamıştır [22].

2.2. Kritik Altyapı Bilgi Sistemleri

Kritik altyapılar bankacılıktan sağlığa, enerjinin üretimi, iletimi ve dağıtımından su sistemlerine, ulaşımdan kritik üretim tesislerine kadar çok geniş bir alana yayıldığı için birçok farklı kontrol sistemini ve bilgi teknolojisini barındırmaktadır. Her sektör kendine has ihtiyaçları çerçevesinde farklı bilgi ve iletişim teknolojilerini kullanmaktadır. Söz konusu teknolojilerin kullanımı sektörlere bilgiyi hızlıca iletme ve yayma, süreçler üzerinde kontrol ve izleme, otomasyon, raporlama ve anlık geri bildirim gibi birçok kolaylık sağlıyor olsa da siber tehdit ve riskleri de beraberinde getirmektedir. Ayrıca kullanılan teknolojilerin çeşitliliği, kritik altyapılarda ortaya çıkabilecek tehditlerin de çeşitlenmesine bununla beraber tüm kritik altyapı sektörlerine uygulanabilecek genel geçer bir çözümün belirlenebilmesinin ise zorlaşmasına sebep olmaktadır. Bu yüzden ülkeler genellikle kritik altyapılara yönelik genel kapsamlı bir strateji ya da politika belirledikten sonra her sektör bu strateji ya da politikaya göre kendi özel dokümanını hazırlamaktadır.

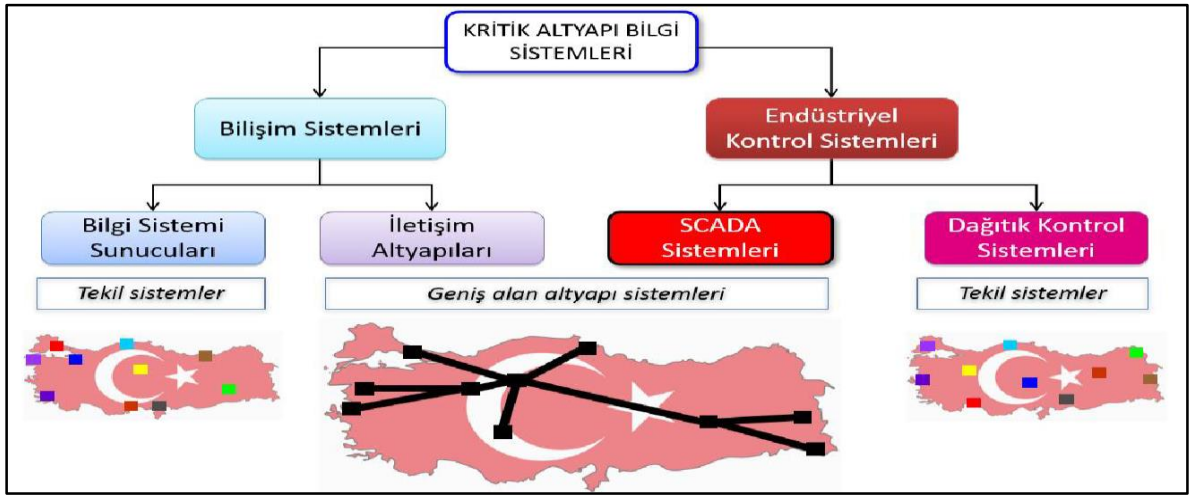
Karabacak [23], kritik altyapılar ile bilgi teknolojileri arasındaki ilişkiyi şu şekilde belirlemiştir:

1. Bilgi teknolojilerini kullanan kritik altyapılar
   - Ulaşım
   - Bankacılık ve finans
   - Sağlık ve Acil Durum Hizmetleri
   - Kritik Kamu Servisleri
2. Tamamen bilgi teknolojilerinden oluşan kritik altyapılar
   - Telekomünikasyon

3. SCADA ile kontrol edilen veya izlenen kritik altyapılar
    - Kritik üretim tesisleri
    - Enerji
    - Barajlar
    - Sulama Sistemleri
    - Elektrik Üretim ve Dağıtım Sistemleri
    - Petrol Rafinerileri
    - Fabrikalar

Kritik altyapıların bir kısmı hizmet vermek için bilinen bilişim sistemlerini kullanırken diğer bir kısmı ise Endüstriyel Kontrol Sistemleri (EKS) olarak adlandırılan özel bilişim sistemleri tarafından izlenmekte ya da yönetilmektedir. Endüstriyel Kontrol Sistemleri, topolojilerine ve içerdikleri bileşenlere göre SCADA (Supervisory Control and Data Acquisition, Merkezi Denetim ve Veri Toplama) ve Dağıtık Kontrol Sistemleri (DKS) olarak ikiye ayrılmaktadır. Bu durumda, bilişim sistemleri açısından, kritik altyapı bilgi sistemlerininin dört farklı kategoride ele alınması Şekil 2.1'de gösterilmiştir [24].

- Bilgi sistemleri, bir kuruma ve paydaşlarına hizmet veren bilgisayar sistemleridir.
- İletişim sistemleri, coğrafi olarak çok geniş bir alana yayılmış bileşenlerden oluşan, pek çok kurum ve kuruluşa iletişim hizmeti sağlayan sistemlerdir.
- SCADA sistemleri, coğrafi olarak çok geniş bir alana yayılmış bir sistemin bileşenlerini merkezi olarak izlemek ve kontrol etmek için kullanılan sistemlerdir.
- Dağıtık kontrol sistemleri, belli bir tesis ve konumla sınırlı bir endüstriyel süreci izlemek ve kontrol etmek için, tesisin tümüne yayılmış kontrol bileşenleri bulunan sistemlerdir.



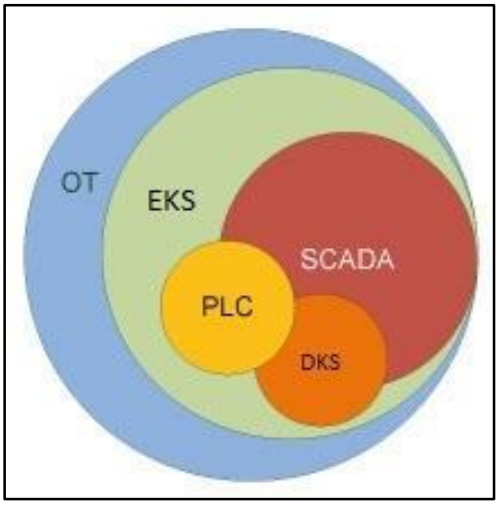
Şekil 2.1. Kritik altyapı bilgi sistemleri [24]

2.2.1. Operasyonel teknoloji, endüstriyel kontrol sistemleri ve SCADA

Operayonel teknoloji (OT) kavramı endüstriyel operasyonları yönetmek için kullanılan ve idari operayonlar dışında kalan bilgisayar sistemleri şeklinde tanımlanmaktadır. Üretim hattı yönetimi, madencilik operasyonları kontrolü, yakıt ve gaz sistemleri izleme gibi sistemler operasyonel sistemlerin içinde sayılmaktadır [25]. Operasyonel teknoloji, fiziksel cihazların çalışmasını izleyen ve kontrol eden bir donanım ve yazılım kategorisi olarak da tanımlanmaktadır [26].

Endüstriyel kontrol sistemleri (EKS), operasyonel teknoloji içindeki büyük bir bölümü ifade etmektedir. Endüstriyel süreçleri izlemek ve kontrol etmek için kullanılan sistemlerin bütünüdür. EKS'ler genellikle erişilebilirlik konusunda hassas olan görev kritik uygulamalardır. Birçok EKS programlanabilir mantıksal kontrolörler (PLC, programmable logic controller) tarafından yönetilen süreç kontrol sistemi ya da bir PLC veya diğer yığın işlem kontrol aygıtları kullanan dağıtık kontrol sistemidir.

EKS'ler çoğunlukla SCADA sistemleri tarafından yönetilirler. SCADA sistemleri operatörlerin bir sistemin durumunu kolayca gözlemlemesi, belirlenen eşik değerlerin dışında çalışmayı belirten herhangi bir alarm üretmesi veya kontrol altındaki süreci yönetmek için sistem ayarlarının girilebilmesi için grafiksel bir kullanıcı ara birimi sağlayan sistemlerdir. Bu sistemler arasındaki ilişki Şekil 2.2'de sunulmuştur [25].

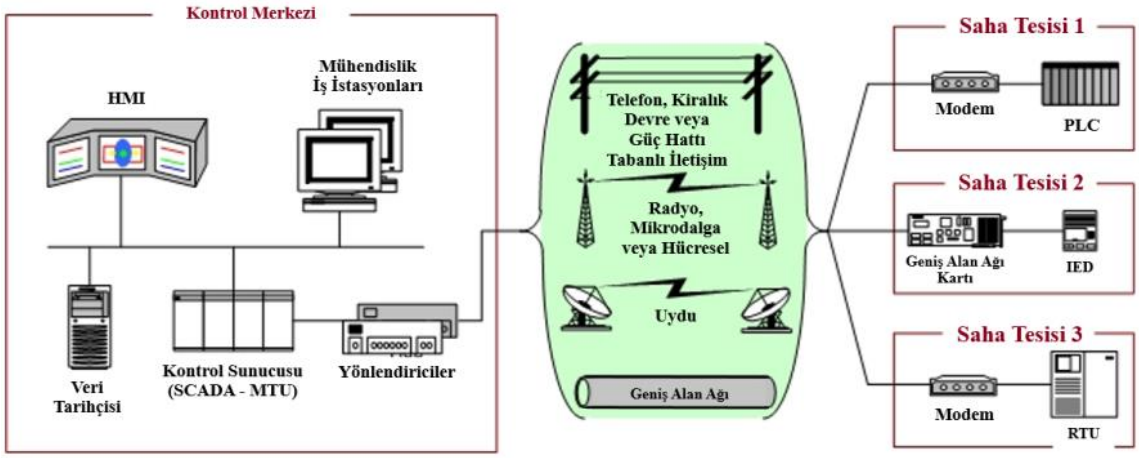


Şekil 2.2. OT, EKS ve SCADA ilişkisi [25]

SCADA sistemleri, merkezi veri ediniminin kontrol kadar önemli olduğu dağıtık varlıkları kontrol etmek için kullanılır. Bu sistemler, su dağıtım ve atık su toplama sistemleri, petrol ve doğal gaz boru hatları, elektrik iletim ve dağıtım sistemleri, demir yolu ve diğer toplu taşıma sistemleri gibi dağıtım sistemlerinde kullanılmaktadır. SCADA sistemleri, veri edinim sistemlerini, veri aktarım sistemleri ve HMI (Human-Machine Interface) yazılımı ile entegre ederek çok sayıda işlem girdisi ve çıkışı için merkezi bir izleme ve kontrol sistemi sunmaktadır. SCADA sistemleri saha bilgilerini toplamak, merkezi bir bilgisayar tesisine aktarmak ve bilgiyi grafiksel veya metinsel olarak operatöre göstermek için tasarlanmıştır, böylece operatörün tüm sistemi gerçek zamanlı olarak merkezi bir konumdan izlemesine veya kontrol etmesine izin verir. Bireysel sistemin karmaşıklığına ve kurulumuna bağlı olarak, herhangi bir bireysel sistemin, işlemin veya görevin kontrolü otomatik olabilir veya operatör komutları ile gerçekleştirilebilir [27].

SCADA sistemleri hem donanım hem de yazılımdan oluşur. Tipik donanım, bir kontrol merkezinde konumlandırılmış bir ana kontrol ünitesine (Master Terminal Unit, MTU), iletişim ekipmanına (örneğin, radyo, telefon hattı, kablo veya uydu) ve aktüatörleri kontrol eden ve/veya sensörleri izleyen bir uzak terminal birimi (Remote Terminal Unit, RTU) veya programlanabilir mantıksal kontrolörden (Programmable Logic Controller, PLC) oluşan bir veya daha fazla coğrafi konumda bulunan tesise sahiptir. RTU veya PLC, yerel süreci kontrol ederken MTU, RTU giriş ve çıkışlarından gelen bilgileri depolar ve işler. İletişim donanımı, MTU ile RTU'lar veya PLC'ler arasında bilgi ve veri aktarımını sağlar. Yazılım, sisteme neyin ne zaman izleneceğini, hangi parametre aralıklarının kabul edilebilir olduğunu ve parametrelerin kabul edilebilir değerlerin dışına çıktığında hangi eylemin başlatılacağını bildirecek şekilde programlanmıştır. Koruyucu bir röle görevinde gibi olan akıllı elektronik aygıt (Intelligent Electronic Device, IED), doğrudan SCADA sunucusuyla haberleşebilir veya yerel bir RTU, verileri toplamak ve SCADA sunucusuna iletmek için IED'leri sorgulayabilir. IED'ler ekipmanı ve sensörleri kontrol etmek ve izlemek için doğrudan bir arayüz sağlar. IED'ler doğrudan SCADA sunucusu tarafından sorgulanıp kontrol edilebilir ve çoğu durumda SCADA kontrol merkezinden doğrudan talimat almadan hareket etmesini sağlayan yerel programlamaya sahiptirler. SCADA sistemleri genellikle sistem mimarisine yerleştirilmiş önemli bir yedekliliğe sahip, hataya dayanıklı sistemler olarak tasarlanmıştır [27].

Şekil 2.3, bir SCADA sisteminin bileşenlerini ve genel konfigürasyonunu göstermektedir. Kontrol merkezi bir SCADA sunucusu (MTU) ve iletişim yönlendiricilerini barındırır. Diğer kontrol merkezi bileşenleri arasında, insan-makine arayüzü (HMI, Human-Machine Interface), mühendislik iş istasyonları ve bir yerel alan ağı ile bağlı olan veri tarihçisi yer alır. Kontrol merkezi, sahadan toplanan bilgileri toplar ve günlüğe kaydeder, bilgileri insan-makine arayüzüne görüntüler ve tespit edilen olaylara göre eylemler oluşturabilir. Kontrol merkezi ayrıca merkezi alarm, trend analizleri ve raporlamadan sorumludur. Saha tesisleri, aktüatörlerin yerel kontrolünü gerçekleştirir ve sensörleri izler. Saha tesisleri ayrıca, saha operatörlerinin genellikle ayrı bir çevirmeli modem veya WAN bağlantısı üzerinden uzaktan teşhis ve onarım yapmasına izin veren bir uzaktan erişim özelliği ile donatılmıştır. Seri iletişim üzerinden çalışan standart ve tescilli iletişim protokolleri telefon hattı, kablo, fiber, mikrodalga, uydu ve radyo frekansı gibi teknikler kullanılarak kontrol merkezi ve saha tesisleri arasında bilgi aktarımı sağlar. MTU-RTU iletişim mimarileri uygulamalar arasında farklılık göstermektedir [27].



Şekil 2.3. SCADA sistemi bileşenleri [27]

Bilgi teknolojileri (BT) ve operasyonel teknoloji (OT) yakınlaşması

Başlangıçta küçük adalar halinde ve herhangi bir geniş alana bağlanmadan nispeten yalıtılmış bir şekilde işletilen operasyonel teknoloji ağları zaman geçtikçe geniş alan bağlantıları ile birbirine bağlanmaya, internete açılmaya ve böylece bilgi teknolojileri ile benzer protokolleri ve standartları kullanmaya başlamışlardır. Endüstriyel kontrol sistemlerine veya operasyonel teknolojiye sahip kurumlarda bulunan bilgi teknolojileri yöneticileri ve personeli operasyonel teknolojiyi içeren ağlar ve cihazların da

güvenliklerinden sorumlu duruma gelmişlerdir [28]. Bugün teknolojinin geldiği noktada nesnelerin interneti (IoT) , akıllı şebekeler ve endüstri 4.0 gibi kavramlarla bilgi teknolojileri ve operasyonel teknolojiler iç içe geçmiş durumdadır. Bunun en belirgin olduğu nokta da endüstriyel nesnelerin interneti (IIoT) kavramıdır denilebilir. Gelecekte BT ve OT yakınlaşmasını gerçekleştirebilmiş şirketlerin ayakta kalabileceği öngörülmektedir [29]. Bununla birlikte bu iki teknolojinin entegrasyonu neticesinde güvenlik hususunun yeniden değerlendirilmesi gerekmektedir. Çünkü operasyonel teknolojiler bir uzak bağlantı sağlayabilmesinden ziyade temelde gerekli işlevi yerine getirebilmek amacıyla tasarlanmışlardır. Dolayısıyla güvenlik zafiyetlerine açık konumdadırlar.

2.2.2. Kritik altyapı kontrol sistemleri ile bilgi sistemleri arasındaki farklar

Kritik altyapılara hizmet eden bilgi sistemleri, bilişim sistemleri ve kontrol sistemlerinden oluşmaktadır. Operasyonel teknoloji kavramı, EKS ve SCADA'yı da içine alarak kritik altyapı kontrol sistemleri için kullanılabilecek en geniş terim olarak düşünülebilir. Bilgi teknolojisi her türlü elektronik veriyi oluşturmak, işlemek, saklamak, güvence altına almak ve değiştirmek için kullanılırken, operasyonel teknoloji fiziksel sürecin izlenmesi ve kontrolü için kullanılır. Dolayısıyla güvenlik açısından bakıldığında bilgi teknolojisi bilgiyi korumaya çalışırken, operasyonel teknoloji fiziksel süreçlerin ve operasyonların yürütülmesini korumak ister.

Örneğin, bilgi teknolojisinde bir bilgisayar ya da sunucuda saldırı ile karşılaşıldığında bir tedbir olarak ağın o bölümü kapatılmaktadır. Buna karşın olası bir atak durumunda OT'nin temel görevi kontrolcüler, akıllı elektronik cihazlar gibi operasyon takımlarının çalışmasını sürdürmektir. Önemli olan sürecin, operasyonun devamını sağlamaktır. Sunuculardaki veri veya tarihsel veriler kaybolabilir. Bu veri daha sonra yedeklerden tekrar sisteme yüklenebilir veya kurtarılabilir. Fakat prosesin aniden durdurulması ekipmanlara zarar verebilir, kalite kaybına yol açabilir, maddi zarar yaratabilir veya en önemlisi operasyon ekibinin yaralanmasına hatta ölmesine sebep olabilir [29].

Bilindiği üzere bilgi güvenliğinin temel unsurları gizlilik, bütünlük ve erişilebilirlik olarak sıralanabilir. Bilgi ve iletişim teknolojilerinin güvenliğinde gizlilik en önemli öncelik sırasına sahiptir ve öncelik sırası bütünlük ve erişilebilirlik şeklinde devam eder. Fakat, operasyonel teknolojilerin güvenliği söz konusu olduğunda bu sıralama tersten işler. Kritik

altyapılarda ve endüstriyel kontrol sistemlerinde süreçlerin yürümesi ve operasyonların devamlılığı en yüksek önceliğe sahiptir. Bu nedenle operasyonel teknolojilerde sıralama erişilebilirlik, bütünlük ve gizlilik şeklinde olduğu Şekil 2.4'te gösterilmiştir [30]. Zhu ve diğerleri [31] yaptıkları çalışmada kritik altyapılarda ve endüstriyel kontrol sistemlerinde kullanılan SCADA sistemlerinin çoğunlukla gerçek zamanlı sistemler olduğunu bu yüzden gerçek-zamanlı işletim sistemleri kullandıklarını söylemişlerdir. Bu maksatla güvenlik unsurlarının başına "vakitlilik" maddesini eklemişlerdir. Ayrıca bilgi ve iletişim teknolojilerinde korunması gereken varlıkların uç sistemlerden ziyade sunucular olduğunu fakat SCADA sistemlerinde veritabanı ya da veri tarihçisi gibi sunucular kadar PLC gibi uç sistemlerin de aynı önemle korunması gerektiğine dikkat çekmişlerdir.

Şekil 2.4. BT ve OT bilgi güvenliği unsurları

Bilgi teknolojileri ile operasyonel teknolojiler arasındaki farklılıklar detaylı olarak Çizelge 2.2'de sunulmuştur [32]. Farklılıklar göz önüne alındığında operasyonel teknolojilerin siber güvenliğinin sağlanmasında da bazı farklılıklar meydana gelmektedir:

- Güvenlik duvarı, saldırı tespit ve önleme sistemleri gibi güvenlik tedbirleri, milisaniye biriminde ölçülen standartlarla hizmet veren sektörlerdeki operasyonel teknolojilerin yavaş çalışmasında ya da aksamasına sebep olabilmektedir.
- Güvenlik için gerekli olan yazılım yamaları ve güncelleştirmeleri, zaman kritik sistemler olan operasyonel teknolojiler için başlı başına bir planlama gerektiren büyük çaplı faaliyetler olabileceğinden bu işlemlerin yapılması zaman ve ekonomik nedenlerden dolayı geciktirilebilir ya da yapılmayabilir. Yöneticiler için yeterli koruma sağlama ve sistemin sürekli çalışması arasında bir ikilem bulunmaktadır. Sonuç olarak ortaya cihaz yazılımları ya da haberleşme sistemi protokolleri uzun zamandır güncellenmemiş dolayısıyla zafiyetlerle dolu sistemler ortaya çıkmaktadır.
- Operasyonel teknolojiler çoğunlukla özel işletim sistemlerini kullansalar da birçok durumda üzerlerinde koştukları işletim sistemleri standart işletim sistemleridir. Dolayısıyla cihazlar bu işletim sistemlerinin açıklıklarını da devralmaktadırlar.

Çizelge 2.2. Bilgi Teknolojileri ve Operasyonel Teknolojiler arasındaki farklar [32]

	Bilgi Teknolojileri	Operasyonel Teknoljiler
İşlev	Bilgi teknolojileri verilerin depolanması, geri kazanımı, iletimi, değiştirilmesi ve korunmasına odaklanmaktadır.	OT, cihazların izlenmesi ve kontrolü yoluyla süreçlerin kontrolüne veya değişimlerine daha fazla odaklanır.
Kullanım Alanı	İş odaklı	Endüstri odaklı
Erişim	Dış dünya ile bağlantılı.	Çok sınırlı erişim. Ayrıcalıklı erişim hakkına sahip kişilerle sınırlı.
Varlıklar ve çalışanlar	Varlıkların sayısı genellikle çalışanların sayısına eşittir veya yakındır.	Daha otonom. Çalışanlardan daha fazla cihaz.
Frekans değişimi	Sürekli değişen: şirkete katılan yeni çalışanlar (ya da yeni bağlanan cihazlar) ve şirketten çıkan eski çalışanlar (ya da bağlantısı kesilmiş cihazlar)	Daha az değişen ortam (aylar ya da yıllar boyunca hiç değişmeyebilir)
Çevre	Kontrollü, kararlı ve sabit	OT'ler olumsuz hava koşullarına dayanır (aşırı sıcaklıklar veya nem dahil olmak üzere).
Arayüz ve ağ	Web tarayıcısı, klavye, cihaz	Sensörler, kodlu veya dokunmatik ekranlar
Ana öncelik	Veri güvenliği (genellikle gizli veriler)	Çalışma süresi. Temel öncelik süreçlerin devamını sağlamaktır.
Güncellemeler	Yazılım güncellemeleri nedeniyle sabit. Hizmet kesintileri tolere edilebilir ve bazı durumlarda mesai saatleri dışında programlanabilir	Güncellemeler önceden dikkatlice test edilmeli ve genellikle makineleri yeniden başlatmayı veya durdurmayı içermelidir. Sonuç olarak, eski sitemler OT içinde çok sık görülür.
Yaşam döngüsü	Daha kısa yaşam döngüleri (3-5 yıl)	OT sistemleri daha uzun ömürlüdür (15-20 yıl). Sonuç olarak, eski sistemler ve artık desteklenmeyenler çok sık görülmektedir.
Kesinti hassasiyeti	Dakika-günler	Milisaniye-Saniye
Amaç	Mantıksal güvenlik, risk altında yaşam yoktur. Amaç, gizli bilgileri potansiyel risklerden (insan hatası, doğal afetler, siber saldırılar vb.) korumaktır.	Amaç çevreyi, insanları ve altyapıları korumaktır
İşletim sistemi	Standart işletim sistemleri	Özel işletim sistemli, özel amaçlı ekipman (Özel olarak geliştirilmiş yazılım).
Protokoller	HTTP, DNS, SSH, SMTP, SNMP, NTP	DNP3, Modbus, IEC 61850, IEC 608705, EtherCat, BACnet

- Operasyonel teknolojilerin yaşam döngüleri bilgi teknolojilerine göre çok daha uzun olduğundan yazılım ve donanımların desteklenme ömürleri dolabilir ve dolayısıyla yine saldırılara karşı hassas bir sistem meydana gelmektedir.
- Operasyonel teknolojilerin bel kemiğini oluşturan SCADA sistemi, alandaki sensörlerden başlayarak kullanıcı ve kontrol arayüzüne kadar geniş bir alana yayılmaktadır. SCADA sunucuları, siber saldırılara karşı iyi korunmuş olsalar da, saha cihazları için benzer garantiler mevcut değildir. Kablosuz internet, hücresel ve bluetooth teknolojilerini içeren iletişim ağı, saldırganlar tarafından kullanılabilecek çoklu uzak erişim noktaları sağlar. Kablosuz ağlar, özellikle Aircrack-NG gibi paketleri koklayabilen, test edebilen ve çözebilen, serbestçe kullanılabilen araçlara karşı savunmasızdır.
- Özellikle endüstriyel kontrol sistemleri için kullanılan düşük seviyeli ağ protokolleri, bir ana-bağımlı iletişim modeline dayanan basit düz metin mesajları kullanılmaktadır. Bunlar, izole sistemler için ve güvenlikten ziyade hız önceliğiyle tasarlandıklarından dolayı erişim kontrolü ve şifreleme eksikliği barındırmaktadırlar.
- Siber güvenlik çoğu zaman dışarıdan gelen bir saldırıya odaklanır, bu da mantıklıdır, ancak aynı derecede muhtemel ve tehlikeli olan, güvenilir ağın içinden kasıtlı veya kasıtsız bir ihmal veya sabotajdan kaynaklanan bir saldırıdır. Kritik altyapılarda kullanılan bilgi sistemlerinde içeriden gelebilecek bir tehdit daha yıkıcı etkiler doğurabileceğinden bu tarz saldırılara karşı daha hassastır. İnsanın zaaflarından faydalanan sosyal mühendislik saldırıları ise iç tehdide destek olarak ya da yalnız başına kullanılabilir [33].

2.3. Kritik Altyapılarda Siber Güvenlik

Kritik altyapıların ulusal güvenlik açısından hayli önemli bir rol oynadığının farkına varan devletler zamanla kendi kritik altyapılarını tanımlamaya, bunların neler olduğunu belirlemeye ve korumak için önlemler almaya başlamışlardır. Bu maksatla mevcut kurumlarına görevler vermişler, yeni kurumlar oluşturmuşlar, mevzuatlarını belirlemişler ve nihayetinde kritik altyapıların korunmasına yönelik stratejiler geliştirmişlerdir. Önceleri tehdit unsuru olarak fiziksel saldırılar öne çıksa da zaman geçtikçe meydana gelen olaylar odak noktasını siber alana kaydırmıştır. Siber saldırının fiziksel olarak olay yerine gitmeyi gerektirmemesi, bilgi haricinde neredeyse başka hiçbir kaynağa ihtiyaç duymaması ve failinin tespitinin daha zor oluşu gibi sebepler bu hususta önemli rol oynamaktadır.

2.3.1. Geçmişi ve yasal düzenlemeler

Bu bölümde Amerika Birleşik Devletleri, Avrupa Birliği ve Türkiye'ye ait kritik altyapıların geçmişi ve konuyla ilgili yasal düzenlemeleri sunulmuştur.

Amerika Birleşik Devletleri faaliyet ve eylemleri

Kritik altyapılar terimi bilindiği kadarıyla ilk olarak 1996 yılında ABD'nin 13010 sayılı başkanlık kararnamesinde karşımıza çıkmaktadır. Kararname gereği "Kritik Altyapıları Koruma Komisyonu" kurulmuş ve komisyon ABD Başkanı'na ülkenin kritik altyapılarına yönelik tehdit ve açıklıkları raporlamakla görevlendirilmiştir. Kararname kritik altyapı kavramını "Bazı ulusal altyapılar o kadar hayatidir ki, yetersiz olmaları veya yıkılmaları ABD'nin savunması veya ekonomik güvenliği üzerinde zayıflatıcı bir etkiye sahip olacaktır." şeklinde tanımlamıştır. Amerika'nın ilk olarak belirlediği kritik altyapılar; telekomünikasyon, elektrik güç sistemleri, gaz ve petrol depolama ve taşımacılığı, bankacılık ve finans, taşımacılık, su temini sistemleri, acil durum hizmetleri (tıp, polis, yangın ve kurtarma dahil) ve devlet yönetiminin devamlılığını içerir. Kritik altyapılara yönelik tehditler ise iki kategoriye ayrılmıştır;

- fiziksel tehditler, maddi mülke yönelik fiziksel tehditler ve
- siber tehditler, kritik altyapıları kontrol eden bilgi veya iletişim bileşenlerine elektronik, radyo frekansı veya bilgisayar tabanlı saldırılar [34].

Komisyon Ekim 1997'de sunduğu raporda kritik altyapıları tehdit eden acil bir kriz durumu öngörmemiş fakat özellikle siber güvenlik alanında önlem alınmasını gerektirecek sebepler bulmuştur. Bunlar; bilgisayar kullanabilen (dolayısıyla potansiyel saldırgan olabilecek) kişi sayısındaki artış, bilgisayar ağlarında kullanılmakta olan protokollerden gelen zafiyetler ve saldırgan araçlarının birçok internet sitesi sayesinde kolayca erişilebilir olması gibi sebeplerdir. Komisyon, raporunda bir önlem stratejisi bile sunmuştur. Rapora göre;

- özel sektör ile devletin ilgili kurumları arasında koordinasyon ve iletişimi kolaylaştırmak,
- gerçek zamanlı bir saldırı uyarı yeteneği geliştirmek,
- açıklayıcı bir farkındalık ve eğitim programı kurmak ve ilerletmek,
- özellikle saldırı tespitini mümkün kılan teknolojiler olmak üzere teknoloji ve tekniklerin araştırma ve geliştirmesini yaygınlaştırmak gerekmektedir [35].

Komisyonun raporuna dayanarak dönemin ABD başkanı bir direktif yayınlayarak 2003 yılına kadar ülkenin kritik altyapılarını kasıtlı saldırılardan koruyabilme yeteneği hedefi koymuştur [36]. Direktif, korunması gereken altyapıları; bilgi ve iletişim, bankacılık ve finans, su tedariki, havacılık, karayolları, toplu taşıma, boru hatları, demiryolu ve su yoluyla ticaret, acil durum ve kolluk kuvvetleri, acil durum, yangın ve hükümet hizmetlerinin devamlılığı, halk sağlığı hizmetleri, elektrik gücü, petrol ve gaz üretimi ve depolanması olarak belirlemiştir. Direktif ayrıca bu önemli sorunla mücadele için yeni bir yapı kurmuştur. Buna göre;

- ABD'ye yönelik saldırılar net bir şekilde belirlenemeyeceğinden, yalnızca kritik altyapıyı değil, aynı zamanda yabancı terörizmi ve yurt içi kitle imha tehditlerini (biyolojik silahlar dahil) koordine edecek bir Ulusal Koordinatör belirlenecek,
- FBI, DOD, USSS, Enerji, Taşımacılık, İstihbarat Topluluğu ve özel sektörden temsilciler bulunduran FBI'daki Ulusal Altyapı Koruma Merkezi (NIPC) özel sektör ile işbirliği içinde, kurumların birbirleri arasında bilgi paylaşımında bulunmasını sağlayarak kaynaşmasını sağlayacak,
- NIPC ayrıca Federal Hükümetin bir olaya müdahalesini kolaylaştırmak ve koordine etmek, saldırıları azaltmak, tehditleri araştırmak ve yeniden yapılanma çabalarını izlemek için temel yollar sağlayacak,
- özel sektör tarafından ve federal hükümet ile işbirliği içinde bir Bilgi Paylaşım ve Analiz Merkezi'nin (ISAC) kurulması teşvik edilecek,
- ulusal planın politikalarının oluşturulmasına rehberlik etmek için özel sektör liderlerinden ve eyalet/yerel yetkililerden oluşan Ulusal Altyapı Güvence Konseyi kurulacak,
- Kritik Altyapı Güvence Ofisi ise, Ulusal Koordinatörün devlet kurumları ve özel sektör ile ulusal bir plan geliştirmedeki çalışmalarına destek sağlayacak, güvence ofisi ayrıca ulusal bir eğitim ve bilinçlendirme programının ve yasama ve halkla ilişkilerin koordinasyonuna yardımcı olacaktır.

Direktif, bunlarla da yetinmeyip bir de Ulusal Altyapı Güvence Planı yapılmasını istemiştir. Plan, yukarıda sıralanan sektörlerden her biri için oluşturulmuş planları bir araya getirecek, bununla birlikte şunları göz önünde bulunduracaktır:

- Sektörün altyapısının amacına ulaşması için gereken asgari temel yetenekte bir güvenlik açığı değerlendirmesi,
- Sektörün hassasiyetlerini azaltmaya yönelik iyileştirici planlar,
- Uyarı isterleri ve prosedürleri,

- Müdahale stratejileri,
- Hizmetlerin yeniden yapılandırılması,
- Eğitim ve bilinçlendirme programları,
- Araştırma ve geliştirme ihtiyaçları,
- İstihbarat stratejileri,
- Uluslararası işbirliği için ihtiyaçlar ve fırsatlar ve
- Yasal ve bütçe gereksinimleri.

ABD'nin daha 2000'lere varmadan kritik altyapılara bu denli önem vermesi ve caydırıcı tedbirler alabilmek ve farkındalığı artırmak için çalışıyor olması kritik altyapılarda meydana gelebilecek bir tehdidin ülkeye ne kadar büyük zararlar verebileceğini çok önceden görebildiğini göstermektedir.

11 Eylül 2001 saldırıları, başta ABD olmak üzere dünya tarihinde kritik altyapıların güvenliği açısından bir miat kabul edilebilir. Clinton'ın başlattığı kritik altyapıların güvenliğine yönelik çalışmalar 11 Eylül öncesi dönemde Bush yönetimi tarafından da çeşitli düzenlemeler yapılarak sürdürülmüştür. 11 Eylül saldırıları sonrası ise siber güvenlik ile alakalı riskler baki kalmak üzere odak noktasına toplu kayıplara da sebep olabilecek fiziksel tehditleri de yerleştirmiştir. Fakat 2009'da Obama yönetimi kritik altyapılarda siber güvenliği yeniden merkeze koymuştur.

2010 yılına gelindiğinde tüm dünyada kritik altyapıların siber güvenliği açısından dönüm noktası sayılabilecek Stuxnet vakası ortaya çıkmıştır. Bu saldırının ayrıntılarına çalışmanın üçüncü bölümünde değinilmiştir.

Obama yönetimindeki birçok yasa tasarısı yasaya dönüşmeyince 2013 yılında Kritik Altyapıların Siber Güvenliğinin Geliştirilmesi adıyla bir başkanlık kararnamesi yayınlanmıştır [37]. Kararname özellikle kurumlar arası bilgi paylaşımı ve 1 yıl içinde kritik altyapıların siber güvenliği için bir çerçeve hazırlanılması üzerinde durmuştur. Siber güvenlik çerçevesi, kritik altyapı sahiplerinin ve operatörlerinin siber güvenlik risklerini azaltmak için kullanabilecekleri bir dizi standart, metodoloji, prosedür ve süreçler olarak tanımlamıştır. Ulusal Standartlar ve Teknolojisi Enstitüsü ise bunun üzerine 2014 yılında Kritik Altyapıların Siber Güvenliği'nin Geliştirilmesi çerçevesinin ilk versiyonunu yayınlamıştır [38]. Konuyla ilgili yine 2013 yılında yayınlanan direktif ise 16 maddelik

kritik altyapı sektörlerini belirleyerek ABD'nin hâlihazırda tanımlamış olduğu kritik altyapı sektörlerinin temelini oluşturması açısından önemlidir [20].

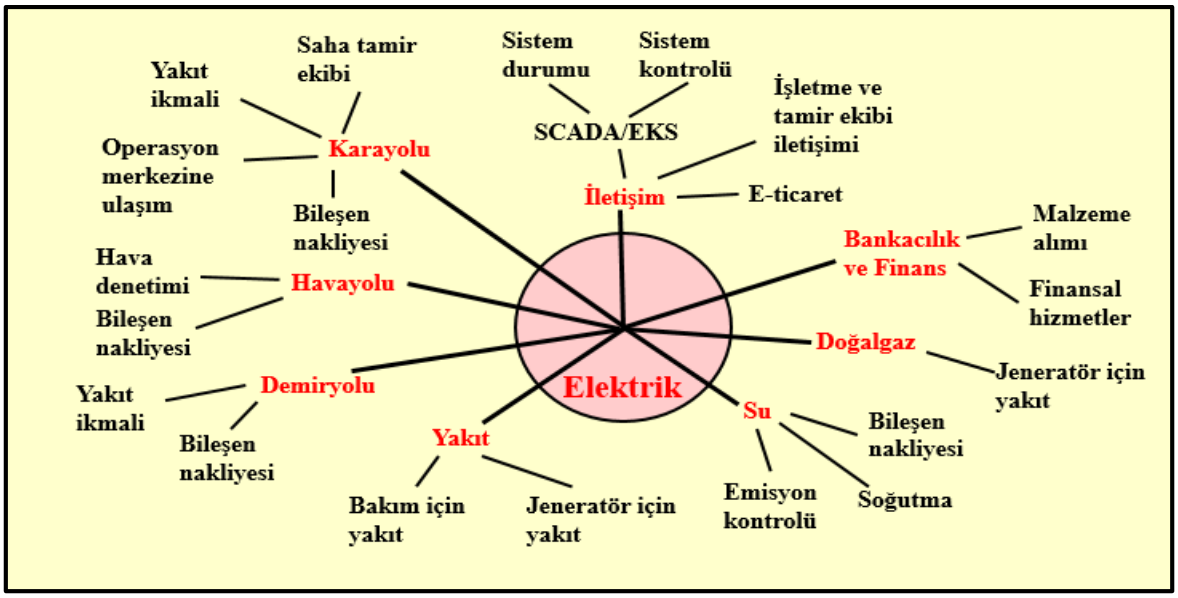
Avrupa Birliği faaliyet ve eylemleri

Avrupa'ya bakıldığında kritik altyapıların korunması ve güvenliği konuları ilk olarak Avrupa Konseyi'nin 2004 yılında kritik altyapıların korunması talebiyle gündeme gelmiştir [39]. 2005 yılında komisyon tarafından yayınlanan belge ile Kritik Altyapıların Korunması Avrupa Programının (European Programme on Critical Infrastructure Protection, EPCIP) temelleri atılmıştır. Belge ile ayrıca Kritik Altyapılar Uyarı Bilgi Ağı Komisyonu (Commission of a Critical Infrastructure Warning Information Network, CIWIN) kurulması çalışmaları desteklenmiştir. Belge içerisinde kritik altyapılara gelebilecek tehditler; kasıtlı terörizm hareketleri, doğal afetler, ihmal, kaza veya bilgisayar saldırıları, zararlı davranışlar olarak belirtilmektedir. Belgede kritik altyapılar tanımı ise şu şekilde yapılmaktadır; kesintiye uğraması veya tahrip edilmesi halinde sağlık, emniyet, güvenlik, ekonomik veya sosyal refah üzerinde ciddi etkilere yol açacak fiziksel kaynaklar, hizmetler, bilgi teknolojileri tesisleri, ağlar ve altyapı varlıklarıdır [21]. Avrupa Komisyonu 2006'da tasarımını son haline getirerek bir direktif olarak yayınlamıştır ve böylece EPCIP resmi olarak hayata geçmiştir [40]. Programın yapı taşlarından birini 2008 yılında Avrupa Konseyi tarafından yayınlanan 2008/114/EC sayılı direktif oluşturmaktadır [41]. Direktif Avrupa kritik altyapılarını tanımlamak ve tasarlamak, bununla beraber kritik altyapıların korunmasını geliştirmeye olan ihtiyacı değerlendirebilmek için genel bir yaklaşım benimsemek amacıyla bir prosedür ortaya koymaktadır. Direktifin ekinde yer alan Avrupa kritik altyapı sektörleri Çizelge 2.3'de verilmiştir.

Çizelge 2.3. 2008/114/EC'ye göre Avrupa kritik altyapı sektörleri [41]

Sektör	**Alt Sektör**
Enerji	Elektrik
	Petrol
	Gaz
Taşımacılık	Karayolu taşımacılığı
	Demiryolu taşımacılığı
	Havayolu taşımacılığı
	Su yolu taşımacılığı
	Okyanus ve kısa mesafeli deniz taşımacılığı, limanlar

Yapılan çalışmalar 2012 yılında üye devletler ve paydaşlarla yakın işbirliği içinde kapsamlı bir şekilde incelenmiştir. Bu incelemenin ilk sonuçları Avrupa Komisyonu'nun yayınladığı bir belge ile özetlenmiştir [42]. Bu incelemenin sonuçları ve mevcut programın diğer elemanlarına dayanarak komisyon 2013'te yeni bir belgeyi kabul etmiştir [43]. Bu belge ile faaliyetler gözden geçirilmiş ve daha pratik bir şekilde icrası maksadıyla 3 ana iş akışı altında ortaya konmuştur; önleme, hazırlıklı olma ve müdahale. Bu yeni bakış açısı AB'de sektörlerin karşılıklı bağımlılıklarını hesaba katarak kritik altyapıları koruma ve dayanıklılığına yönelik ortak araçlar ve ortak bir yaklaşım geliştirmeyi amaçlamaktadır. Sektörler arası bağımlılıklar Şekil 2.5'te gösterilmiştir.



Şekil 2.5. Sektörler arası bağımlılıklar [43]

Avrupa Komisyonu 2007-2012 yılları arasında kritik altyapıların korunması konusuyla alakalı 100'den fazla projeyi desteklediğini de bu belgede belirtmiştir. Bu projelerin en önemlilerinden biri Kritik Altyapıların Korunması için Avrupa Referans Ağının (European Reference Network for Critical Infrastructure Protection, ERNCIP) oluşturulması projesidir. Ağın amacı Avrupanın deneysel yeteneklerinin bağlantılanması aracılığıyla yenilikçi, nitelikli, verimli ve rekabetçi güvenliğin ortaya çıkmasını teşvik etmek olarak belirlenmiştir. Bugün Avrupa Birliğinde kritik altyapılar ve hizmetler ENISA (European Union Agency for Cybersecurity) tarafından şu başlıklar altında yönetilmektedir:

- Kritik bilgi altyapıları
- İnternet altyapısı
- EKS/SCADA

- Akıllı Şebekeler
- Finans
- Sağlık
- Denizcilik

Avrupa Komisyonu'nun 2018 yılındaki bir raporuna göre ise EPCIP'in güncel odak noktalarından birincisi siber güvenlik iken ikincisi iç tehdit etkisi olarak belirlenmiştir [44].

Türkiye faaliyet ve eylemleri

Türkiye'de kritik altyapıların siber güvenliği kavramı bilindiği kadarıyla ilk olarak TÜBİTAK UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) tarafından 2008 yılında hazırlanan ve 2009 yılında Başbakanlığa sunulan sayısal ortam güvenliği politika dokümanında yer almaktadır. Söz konusu dokümanda "Kritik bilgi ve iletişim sistem altyapılarının güvenliği sağlanmalıdır. Ülke içerisindeki kritik bilgi ve iletişim sistem altyapıları, bunların birbirleriyle ilişkileri, kritiklik seviyeleri ve sorumluları tespit edilmelidir. Tespit edilen kritik bilgi ve iletişim sistem altyapıları sanal ortamdan gelebilecek tehditlere karşı korunmalıdır." ifadeleri yer almaktadır [45].

Daha sonra 2012 yılındaki Ulusal Siber Güvenlik Çalışmalarının Koordinasyon ve Yönetimine İlişkin Bakanlar Kurulu Kararı gereğince hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nda ilk defa resmi olarak ve geniş çaplı yer bulmuştur [16]. Planda kritik altyapılara birçok noktada değinilmiş, kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanması, özel sektörle iş birliği yapılması, kritik altyapı sektörlerine özel sektörel SOME'lerin (Siber Olaylara Müdahale Ekibi) kurulması gerektiği belirtilmiştir. Kritik altyapılara ait bilişim sistemlerinin internete bağlı olması, kritik altyapı hizmet ve servislerinin, gerçekleştirilen siber saldırılara ek olarak bilişim sistemlerinin kendi hatalarından, kullanıcı hatalarından ya da doğal afetlerden de olumsuz olarak etkilenmesi ve bu tür olaylara yönelik alınabilecek tedbirler açısından gerekli yeterliliğe sahip olunmaması önemli risk faktörleri olarak göz önüne alınmıştır. Mevcut risk ve tehditleri ortadan kaldırmak için TÜBİTAK ile kritik sektörleri düzenlemek ve denetlemekle sorumlu kurumlar tarafından Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı oluşturulması hedeflenmiştir. TÜBİTAK'ın Kalkınma Bakanlığı 2012 Yatırım Programı içerisinde yer alan "Kritik Altyapılarda Bilgi Güvenliği Yönetimi Projesi" ve UDHB sponsorluğunda

hazırlanan raporlar ülkemizdeki önemli adımlar olsa da 2013-2014 Eylem Planı'nda yer alan Kritik Altyapılarda Bilgi Güvenliği Yönetimi Programı hayata geçmemiştir [46].

Yine 2012'de Ulusal Siber Güvenlik Çalışmalarının Koordinasyon ve Yönetimine İlişkin Bakanlar Kurulu Kararı ile kurulan Siber Güvenlik Kurulu[2] Haziran 2013'te yaptığı toplantıda aldığı kararla Türkiye'deki kritik altyapıları 6 başlık altında toplamıştır:

- Elektronik Haberleşme
- Enerji
- Bankacılık ve Finans
- Kritik Kamu Hizmetleri
- Ulaştırma
- Su Yönetimi

Kritik altyapıların korunması konusu 2016-2019 Ulusal Siber Güvenlik Stratejisi içinde ise ayrı bir alt bölüm olarak yer bulmuştur [47]. Bu bölümde;

- 27001 Bilgi Güvenliği Yönetim Sisteminin zorunlu kılınması,
- sızma testlerinin mecbur hale getirilmesi,
- sistem odalarında bulunması gereken asgari kriterler gibi kritik altyapıların bilgi sistemlerini de kapsayan hususlar yer almıştır.

Halihazırda Türkiye'nin kritik altyapılara özel bir stratejisi bulunmamaktadır. Ancak TÜBİTAK'ın hazırlamış olduğu Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı bu konuda önemli bir temel rehber konumundadır [24].

Ayrıca 2017 yılında yayınlanan "Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği " kritik altyapıların siber güvenliği alanında Türkiye'de yayınlanmış önemli bir mevzuat konumundadır. Yönetmelik enerji piyasasında faaliyet gösteren ve EPDK (Enerji Piyasası Düzenleme Kurumu) tarafından kritik altyapı olarak belirlenen yükümlü kuruluşların EKS'de kullanılan bilişim sistemlerinin tanınması, envanterinin belirlenmesi, risk değerlendirilmesinin yapılması, risklerin işlenmesi ve azaltılması ile EKS'ye yönelik güvenlik kontrollerini içermektedir [48]. Bununla beraber EPDK, 2019 yılında güvenlik analiz ve test metodolojisine yönelik "Enerji Sektöründe

[2] Bu kurul 10.07.2018 tarih 703 no.lu KHK ile kapatılmıştır.

Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları" dokümanını yayınlamıştır [49].

2019 yılında yayınlanan Cumhurbaşkanlığı'na ait Bilgi ve İletişim Tedbirleri Genelgesi endüstriyel kontrol sistemleri ve kritik altyapılarla ilgili önemli maddeler içermektedir. Genelgenin 16'ncı maddesi; "Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır." ibaresini içermektedir. Genelge kritik altyapılarla ilgili aşağıdaki ibareleri içermektedir:

> Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü ve erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve *www.cbddo.gov.tr* adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir [50].

Bununla birlikte tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerin bu rehbere uyması zorunlu kılınmış, rehberin uygulanmasına ilişkin denetim mekanizmasının kurularak en az yılda bir defa uygulamaların denetlenmesi ve sonuçları ile düzeltici faaliyetlerin Dijital Dönüşüm Ofisine iletilmesi talep edilmiştir.

Yine 2019 yılında yayınlanan 11. Kalkınma Planı da kritik altyapıların siber güvenliği konularında önemli maddeler içermektedir. Plana göre;

- kritik altyapılarda bilgi güvenliği yönetim sistemi kurulmasına yönelik usul ve esaslar belirlenerek hayata geçirilecek (Md.474.4),
- kritik önemi haiz enerji altyapısının güvenli bir şekilde işletilmesine yönelik Siber Güvenlik Operasyon Merkezi kurulacak (Md.496.1),
- enerji KİT'lerinde kullanılması amacıyla Milli Akıllı Şebeke Yönetim Sistemi (Milli SCADA) geliştirilmesine yönelik çalışmalar yapılacaktır (Md.496.2) [51].

2.3.2. Kritik altyapıların siber güvenliğine yönelik standart ve rehberler

Kendi ülkelerinde kritik altyapıların ve güvenliğinin düzenlenmesinden sorumlu devlet kuruluşları, özel iştirakler ve uluslararası kuruluşlar kritik altyapıların siber güvenliğine yönelik çabaların koordine edilmesi ve en iyi uygulamaların belirlenerek tüm kritik altyapı sektörlerine yaygınlaşabilmesi amacıyla bir takım standart ve rehberler yayınlamışlardır. Bu alanda dünyada önde gelen kuruluşlar IEC, ANSI, ISO, NIST, IEEE, NERC, ETSI, ENISA olarak sıralanabilir. Türkiye için ise kritik altyapıların siber güvenliğine yönelik standart ve rehber yayınlayan kuruluşlar TSE, BTK ve EPDK'dır. Bu kuruluşların yayınladıkları standart ve rehberlere uyulması kritik altyapıların siber saldırılardan korunmasında kilit rol oynamaktadır.

NIST Kritik Altyapı Siber Güvenliğinin Geliştirilmesi Çerçevesi [52]

ABD'nin 13636 sayılı Yürütme Kararı [37] gereğince ilki 2014'te yayınlanan ve 2018'de 1.1 versiyonu ile güncellenen çerçeve ABD Ulusal Standartlar ve Teknoloji Enstitüsüne aittir. Bu yayında siber güvenlikle ilgili riski yönetmek için yönergeler ve en iyi uygulamalardan oluşan isteğe bağlı bir risk yönetimi çerçevesi ortaya konmaktadır. Yönetici Özeti bölümünde çerçevenin sadece kritik altyapı sektörleri için değil diğer endüstri sektörleri için de kullanılabilecek esnek bir yapıda olduğundan bahsedilmiştir.

Çerçeve, 2015 yılıyla beraber ABD sanayi kuruluşlarının yüzde 30'u tarafından tarafından kullanılmaktaysa da 2020 ile beraber bu oranın yüzde 50'yi bulacağı belirtilmiştir [53]. Diğer veri güvenliği standartlarına benzer şekilde zorunlu olmasa da 2018 yılında yayınlanan bir Başkanlık Kararnamesi [54] federal ajanslar için bu tarz bir çerçevenin kullanılmasını zorunlu kılmaktadır. Benzer bir zorunluluğun tüm sektörlere yaygınlaşması da muhtemel görülmektedir.

Çerçeve, 3 bölümden oluşmaktadır: çekirdek, uygulama katmanları ve profil.

Çekirdek bölümü, kritik altyapı sektörlerinde yaygın olan bir dizi siber güvenlik aktivitesi, istenen çıktılar ve uygulanabilir örneklerini içermektedir. Bölüm, endüstri standartlarını, kılavuzlarını ve uygulamalarını, yönetici seviyesinden uygulama/operasyon seviyesine kadar sunmaktadır. Çekirdek, eş zamanlı ve sürekli devam eden 5 fonksiyondan

oluşmaktadır: tanımla, koru, algıla, karşılık ver, kurtar. Birlikte değerlendirildiğinde, bu işlevler bir kuruluşun siber güvenlik risk yönetimi yaşam döngüsüne ilişkin üst düzey bir stratejik görüş sağlar.

Uygulama Katmanları, bir kuruluşun siber güvenlik riskini nasıl gördüğünü ve bu riski yönetmek için uygulanan süreçleri ele alır. Katmanlar, bir kuruluşun siber güvenlik risk yönetimi uygulamalarının çerçevede tanımlanan özellikleri sergileme derecesini (risk ve tehdide farkında, tekrarlayabilen ve uyabilen gibi) tanımlar.

Profil bölümü, bir kuruluşun belirli bir uygulama senaryosunda standartların, kılavuzların ve uygulamaların çerçeve çekirdeği ile uyumlaştırılması ve elde edilen çıktılar olarak tanımlanabilir. Kuruluşlar, mevcut profilini bir hedef profili ile karşılaştırılarak siber güvenlik duruşunu iyileştirme fırsatlarını belirlemek için kullanmaktadırlar.

Ayrıca NIST tarafından 2019 yılında *çerçeveye* eşlik eden bir de yol haritası dokümanı [55] yayınlanmıştır.

NIST 800-82 Endüstriyel Kontrol Sistemleri Güvenliği Rehberi [27]

Rehber, SCADA sistemleri, Dağıtık Kontrol Sistemleri (DKS) ve Programlanabilir Mantıksal Denetleyicileri (PLC) ve diğer kontrol sistemi yapılandırmaları dahil olmak üzere Endüstriyel Kontrol Sistemlerinin (EKS) kendine has performans ve güvenilirlilik gereklilikleri sağlanırken nasıl güvenli hale getirilebileceğine dair kılavuzluk sağlamaktadır. Doküman, EKS ve tipik sistem topolojilerine genel bir bakış sunmakta, bu sistemlere yönelik tipik tehditleri, açıkları belirlemekte ve ilişkili riskleri azaltmak için önerilen güvenlik önlemlerini ortaya koymaktadır.

Rehber aşağıdaki bölümlerden oluşmaktadır:

- Giriş
- Endüstriyel Kontrol Sistemlerine Genel Bakış
- EKS Risk Yönetimi ve Değerlendirmesi
- EKS Güvenlik Programı Geliştirilmesi ve Yaygınlaştırılması
- EKS Sistem Mimarisi
- Güvenlik Kontrollerinin EKS'ye Uygulanması

IEC 62351 Standartlar Ailesi [56]

IEC 62351 standartları Uluslararası Elektroteknik Komisyonunun (IEC) 57 numaralı teknik komitesine (TC57) ait ve Veri ve İletişim Güvenliği ile alakalı standartlar geliştirmekte olan 15 numaralı çalışma grubu (WG15) tarafından geliştirilmiştir.

IEC 62351, güç sistemi alanındaki otomasyon sistemlerinde güvenliği artırmayı amaçlayan bir endüstri standardıdır. Güç sistemlerinde kullanılan farklı protokoller için bütünlük, kimlik doğrulama ve gizlilik sağlama amacına yönelik hükümler içermektedir.

IEC 62351 standartlar ailesinin içerdiği standartlar ve içerikler aşağıda tanımlanmıştır:

- IEC 62351-1 Standarda giriş
- IEC 62351-2 Terimler sözlüğü
- IEC 62351-3 TCP/IP dahil olmak üzere herhangi bir profil için güvenlik.
  - TLS Şifreleme
  - X.509 sertifikaları aracılıyla Düğüm Kimlik Doğrulama
  - Mesaj Doğrulama
- IEC 62351-4 MMS dahil her profil için güvenlik (örneğin, ICCP tabanlı IEC 60870-6, IEC 61850 vb.).
  - MMS için kimlik doğrulama
  - Taşıma katmanı güvenliğini sağlamak için RFC 1006 ve RFC 793 arasına TLS (RFC 2246) yerleştirilir.
- IEC 62351-5 IEC 60870-5 (ör. DNP3 türevi) dahil olmak üzere herhangi bir profil için güvenlik
  - TCP/IP profilleri için TLS ve seri profiller için şifreleme.
- IEC 62351-6 IEC 61850 profilleri için güvenlik.
  - GOOSE için VLAN kullanımı zorunludur.
  - SNTP için RFC 2030 kullanılacaktır.
- IEC 62351-7 Ağ ve sistem yönetimi ile güvenlik.
  - SNMP tabanlı yöntemlerle ağ ve sistem yönetmek için güç endüstrisine özgü Yönetim Bilgi Tabanını (Management Information Base, MIB) tanımlar.
- IEC 62351-8 Rol tabanlı erişim kontrolü.
  - Rol tabanlı erişim kontrolü (RBAC) ile kullanıcıların ve otomatik ajanların erişim sistemlerini güç sistemlerindeki veri nesnelerine kapsar.

- IEC 62351-9 Anahtar Yönetimi
  - Güvenlik açısından kritik parametrelerin (şifreler, şifreleme anahtarları) doğru ve güvenli kullanımını tanımlar.
  - Şifreleme bilgilerinin tüm yaşam döngüsünü (kayıt, oluşturma, dağıtım, kurulum, kullanım, depolama ve kaldırma) kapsar.
  - Asimetrik kriptografi kullanan algoritmalar için yöntemler
    - Dijital sertifikaların kullanımı (genel/özel anahtar)
    - X.509 sertifikalarıyla PKI ortamının kurulması
    - SCEP/CMP/EST ile sertifika kaydı
    - CRL/OCSP ile sertifika iptali
  - Simetrik anahtarların kullanımı için GDOI ve IKEv2 protokolünü temel alan güvenli bir dağıtım mekanizması.
- IEC 62351-10 Güvenlik Mimarisi
  - BT altyapısının tamamı için güvenlik mimarilerinin açıklanması.
  - İletişim mimarisinin kritik noktalarını belirlemek, örneğin; trafo kontrol merkezi, trafo otomasyonu.
  - Güvenlik gereksinimleri için uygun mekanizmalar (veri şifreleme, kullanıcı doğrulama gibi).
  - BT alanından kanıtlanmış standartların uygulanabilirliği, örn. VPN tüneli, güvenli FTP, HTTPS.
- IEC 62351-11 XML Dosyaları için Güvenlik
  - Orijinal XML içeriğinin bir XML konteynerine gömülmesi
  - XML verileri için yayınlanma tarihi ve erişim kontrolü
  - XML verilerinin doğrulanması için X.509 imzası
  - İsteğe bağlı veri şifreleme [57].

NERC Kritik Altyapıların Korunması (NERC-CIP) Standartları [58]

NERC Kritik Altyapı Koruması (NERC-CIP), büyük elektrik sistemleri için minimum güvenlik gereksinimlerini belirleyen bir standartlar kümesidir. NERC-CIP, güç sistemi güvenliğini ele alan 40 kural ve 100 alt gereksinimden oluşmaktadır.

Standartlar içerisinde, "kritik varlıklar" ve "sorumlu kuruluşlar" kavramları sık sık kullanılmaktadır. Bu yüzden her iki terimin de tanımlarını anlamak önemlidir:

Kritik varlıklar; kontrol sistemleri, veri toplama sistemleri ve ağ donanımlarının yanı sıra sanal makineler veya sanal depolama alanlarını barındıran donanım platformlarından oluşmakla birlikte yalnızca bunlarla sınırlı değildir.

Sorumlu kuruluşlar; güvenilirlik koordinatörleri, dengeleme otoriteleri, değişim otoriteleri, iletim servis sağlayıcıları, iletim sahipleri, iletim operatörleri, jeneratör sahipleri, jeneratör operatörleri, yük servis kuruluşları ve NERC/bölgesel kuruluşlar olarak tanımlanmaktadır.

Halihazırda yürürlükte olan standartlar ve içerikleri aşağıda sunulmuştur.

CIP-002-5.1a - Siber Güvenlik - BES Siber Sistem Kategorizasyonu
Standart, siber güvenlik gereksinimlerinin uygulanması maksadıyla Büyük Elektrik Sistemi (Bulk Electric System - BES) siber sistemlerinin ve bunlarla ilişkili BES siber varlıkların, tanımlanmasını ve sınıflandırılmasını gerektirir. Bu gereksinimler, BES siber sistemlerinin zarar görmesi, tehlikeye atılması veya kötüye kullanılmasıyla ortaya çıkabilecek olumsuz etki ile orantılıdır. BES siber sistemlerinin tanımlanması ve kategorilendirilmesi, BES'te istenmeyen biçimde veya kararsız kullanımına yol açabilecek tehlikelere karşı uygun korumayı desteklemektedir.

Bu standart doğrultusunda kuruluşlar, her bir kritik varlığı tanımlamalı, kategorize etmeli, her bir varlık için zarar görme veya kayıp durumlarının nasıl oluşabileceğini önceliklendirmeli ve nihayetinde varlığın tesise olan genel ilişkisini veya işletme bağımlılığını vurgulamalıdırlar.

CIP-003-6 - Siber Güvenlik - Güvenlik Yönetimi Kontrolleri
Bu standart kuruluşların, BES siber sistemlerini, BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelere karşı korumak için sorumluluk ve hesap verebilirlik sağlayan tutarlı ve sürdürülebilir güvenlik yönetimi kontrollerinin belirlenmesini gerektirmektedir.

Siber güvenlik politikası, liderlik, istisnalar, bilgi koruması, erişim kontrolü, değişiklik kontrolü ve konfigürasyon yönetimi bu standarda dahil edilmiştir. Alt gereksinimlere uyumluluk organizasyona, varlıkların kritikliğine ve etki derecesine göre değişebilmektedir.

CIP-004-6 - Siber Güvenlik - Personel ve Eğitim

Standart, uygun düzeyde bir personel risk değerlendirmesi, eğitimi ve güvenlik bilinci yardımıyla BES siber sistemlerine erişen bireylerden gelebilecek ve istenmeyen şekilde veya kararsız çalışmasına yol açabilecek risklerin en aza indirgenmesini gerektirmektedir.

Kuruluşlar tarafından, kritik siber varlıklara yetkili erişimi olan tüm personelin yeterli derecede kişilik taraması, risk değerlendirmesi, çalışan eğitimi ve güvenlik bilinci programlarına sahip olmasının sağlanması gerekmektedir. Ayrıca, kuruluşun bu tür eğitim ve programları yıllık olarak belgelendirmesini, incelemesini ve güncellemesini gerektirir. Standart bununla birlikte, servis sağlayıcılar ve yükleniciler dâhil olmak üzere bir kimlik bilgisi erişim listesi tutulmasını gerektirmektedir.

CIP-005-5 - Siber Güvenlik - Elektronik Güvenlik Alanı

Standart, BES siber sistemlerinin, BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelere karşı korunmasını desteklemek amacıyla kontrollü bir Elektronik Güvenlik Alanı belirleyerek, BES siber sistemlerine elektronik erişimin yönetilmesini gerektirmektedir.

Bu standart öncelikle çevreye ve uzaktan erişim sırasında karşılaşılan güvenlik açıklarını ele alma çabalarına odaklanmaktadır. Tüm kritik siber varlıkları barındıran çevre korunmalı ve tüm erişim noktaları güvence altına alınmalıdır. Elektronik güvenlik alanı belirlemenin ana bileşenleri arasında; uzak oturum şifrelemesi, çok faktörlü kimlik doğrulama, kötü amaçlı yazılımdan korunma güncelleştirmeleri, yama güncelleştirmeleri ve rollere dayalı erişimi sınırlamak için genişletilebilir kimlik doğrulama protokolü (EAP) kullanma gibi tedbirler bulunmaktadır.

CIP-006-6 - Siber Güvenlik - BES Siber Sistemlerin Fiziksel Güvenliği

Standart, BES siber sistemlerinin, BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelere karşı korunmasını desteklemek için bir fiziksel güvenlik planı belirleyerek fiziksel erişimin yönetilmesini gerektirmektedir.

Standart, fiziksel güvenlik alanını vurgular ve sorumlu kuruluşa bir fiziksel güvenlik programı uygulama görevi vermektedir. Amaç, fiziksel güvenlik bölgesini ele almak ve risk bazlı güvenlik bölgelerine dayanarak siber varlıklara erişimin korunmasını ve kontrol

edilmesini hedefleyen önleyici kontroller oluşturmaktır. Fiziksel güvenlik planı, fiziksel erişim kontrol sistemlerinin korunması, elektronik erişim kontrol sistemlerinin korunması, fiziksel erişim kontrolleri, fiziksel erişim izlemesi, fiziksel erişim kayıtları, saklanan kayıtlara erişim, bakım ve test gibi hususlar CIP-006-6 güvenlik programının gerekliliklerdir.

CIP-007-6 - Siber Güvenlik - Sistem Güvenliği Yönetimi
Standart, BES siber sistemlerini, BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelere karşı korumayı desteklemek için belirli teknik, operasyonel ve prosedürel gerekliliklerin belirlenerek sistem güvenliğinin yönetilmesini gerektirmektedir.

Ayrıca test prosedürleri, portlar ve hizmetler, güvenlik yama yönetimi ve kötü amaçlı yazılım önleme kayıtları gibi güvenlik önlemlerinin belgelendirilmesi gerekliliğini içermektedir.

CIP-008-5 - Siber Güvenlik - Olay Raporlama ve Müdahale Planlaması
Bu standart, olay müdahale gerekliliklerini belirleyerek siber güvenlik olayı sonucunda BES'in güvenilir şekilde çalışmamasına yönelik riskin azaltılmasını gerektirmektedir.

Herhangi bir kritik siber varlık ile ilgili güvenlik olayı, NERC tarafından uygun görülen şekilde tanımlanmalı, sınıflandırılmalı, müdahale edilmeli ve raporlanmalıdır. İlgili kişilerin eylemlerini, rollerini, sorumluluklarını içeren ve olayların nasıl idare edileceği ile yönetim organlarına nasıl rapor edileceğini açıklayan bir olay müdahale planı oluşturulmalıdır. Bu planın yıllık olarak güncellenmesi ve uygulanabilirliği test edilmesi gerekmektedir.

CIP-009-6 - Siber Güvenlik - BES Siber Sistemleri İçin Kurtarma Planları
Bu standart, BES'in devam eden kararlılığını, çalışabilirliğini ve güvenilirliğini desteklemek için kurtarma planı gereksinimlerinin belirlenerek BES siber sistemlerinin gerçekleştirdiği güvenilirlik işlevlerinin kurtarılmasını içermektedir.

Kritik siber varlıkların, felaketten kurtarma en iyi uygulamalarına bağlı kalan kurtarma planları olmalıdır. Bir kurtarma planı, değişiklik kontrolü, yedekleme ve restorasyon işlemleri, test veya yedekleme ortamı gibi hususlar bu standardın gerekliliklerindendir.

CIP-010-2 - Siber Güvenlik - Yapılandırma Değişikliği Yönetimi ve Güvenlik Açığı Değerlendirmeleri

Bu standart, BES Siber Sistemlerinde BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelerden korunmasına yardımcı olmak için yapılandırma değişikliği yönetimi ve güvenlik açığı değerlendirme gerekliliklerinin belirlenerek BES siber sistemlerindeki yetkisiz değişikliklerin önlenmesi ve tespit edilmesini gerektirmektedir.

CIP-011-2 - Siber Güvenlik - Bilgi Koruma

Bu standart, BES siber sistemlerinin, BES'in istenmeyen şekilde veya kararsız çalışmasına yol açabilecek tehlikelerden korunmasına yardımcı olmak için bilgi koruma gereklilikleri belirlenerek, BES siber sistemlerindeki bilgiye yetkisiz erişiminin önlenmesini gerektirmektedir.

CIP-014-2 - Siber Güvenlik - Fiziksel Güvenlik

Bu standart, iletim istasyonlarının, iletim trafo merkezlerinin ve bunların ilişkili birincil kontrol merkezlerini tanımlanmasını ve korunmasını zorunlu kılmaktadır [59].

Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı [24]

2012 yılında TÜBİTAK tarafından hazırlanan ve Ulaştırma Denizcilik ve Haberleşme Bakanlığı tarafından yayınlanan rehber Türkiye'de bu alanda yayınlandığı bilinen ilk rehberdir. Dokümanın içerdiği asgari güvenlik önlemleri şu şekildedir:

- Sistemlerin yetkisiz erişimden korunması
  - Sistem merkezine fiziksel erişimin yönetilmesi
  - Sistemlere bilgisayar ağları aracılığı ile erişimin kısıtlanması
  - Taşınabilir saklama ortamlarının kısıtlanması
- Yetkili personelin sistemlere erişiminin yönetilmesi
  - Sistem yöneticisi ve operatör atama prosedürü
  - Yetkili personelin kullanıcı kimliklerinin yönetilmesi ve güvenli oturum açma prosedürü
  - Kayıt yönetimi ve görevler ayrılığı
  - İşletme prosedürleri, rol ve sorumluluklar
- Sistem tedarik, geliştirme ve bakımının yönetilmesi
  - Uygulama yazılımlarının güvenliğinin yönetilmesi

    - Teknik açıklıkların yönetilmesi
    - Bakım sözleşmesi
- İş sürekliliği önlemleri
    - Yedek sistem merkezi, prosedür ve testler
- Bilişim Sistemleri Güvenliği Yöneticisi ve Personel İstihdamı
    - Güvenlik yöneticisi
    - Personel sürekliliği
    - Personel yetiştirilmesi ve eğitimi
- Dokümantasyon
    - Politika dokümanı
    - Kayıtların yönetilmesi
- Bilgi Güvenliği Olaylarına Müdahale

Enerji Sektöründe EKS Güvenlik Kontrolleri [60]

Türkiye'de kritik altyapıların siber güvenliğine yönelik güncel önemli bir rehberdir. EKS Güvenlik Kontrolleri, enerji güvenliğini tesis etmeye yönelik olarak EPDK tarafından uluslararası örnekler dikkate alınarak geliştirilmiş bir güvenlik kontrolleri bütünüdür. Rehber ile EKS'lerin karşılaştıkları güvenlik risklerinin ortadan kaldırılması, tespit edilmesi, riskin gerçekleşme olasılığının ve olası etkinin düşürülmesi amaçlanmaktadır.

EKS Güvenlik Kontrolleri El Kitabı, EKS sahipleri için bir güvenlik uygulama kılavuzu olmasının yanı sıra, sektörde bulunan EKS'lerin güvenliğinin denetlenmesi için de bir el kitabı olma niteliği taşımaktadır. Bu kontroller baz alınarak yapılacak denetimler ile bir EKS'nin güvenlik seviyesinin ölçülebileceği ve öncelikli gelişim alanları tespit edilebileceği değerlendirilmiştir.

Enerji Sektöründe bulunan EKS'ler için tasarlanmış güvenlik kontrollerini içeren 18 başlık aşağıda sunulmuştur.

- Erişim Kontrolü
- Farkındalık ve Eğitim
- Denetim ve Hesap Verebilirlik
- Acil Durum Planlaması
- Güvenlik Değerlendirmesi ve Yetkilendirme
- Konfigürasyon Yönetimi
- Kimlik Doğrulama ve Yetkilendirme

- Olay Müdahale
- Bakım
- Medya (Ortam) Koruması
- Fiziksel ve Çevresel Güvenlik
- Personel Güvenliği
- Risk Değerlendirme
- Sistem ve Hizmet Edinimi
- Sistem ve İletişim Güvenliği
- Sistem ve Bilgi Bütünlüğü
- Program Yönetimi

Bunların dışında kritik altyapı sektörlerine yönelik olarak TSE'nin ISO standartları kaynak alınarak oluşturulmuş 3 önemli bilgi güvenliği dokümanı bulunmaktadır:

- TS ISO/IEC 27011 Bilgi teknolojisi - Güvenlik teknikleri - Telekomünikasyon kuruluşları için ISO / IEC 27002'ye dayalı bilgi güvenliği denetimleri için uygulama prensipleri,
- TS ISO/IEC 27019 Bilgi teknolojisi - Güvenlik teknikleri - Enerji hizmet endüstrisine özgü proses kontrol sistemleri için ISO / IEC 27002'ye dayalı bilgi güvenliği yönetim kuralları,
- TS EN ISO 27799 Sağlık bilişimi - ISO/IEC 27002 standardını kullanarak sağlıkta bilgi güvenliği yönetimi.

İncelenen standart ve rehberlerde iç tehdide yönelik de birçok güvenlik kontrolü yer almaktadır. Erişim kontrolü, kimlik doğrulama ve yetkilendirme, personel güvenliği, ağ segmentasyonu, farkındalık ve eğitim, şifreleme gibi yöntemler iç kaynaklı tehditlere karşı alınabilecek önlemlerdendir.

3. İÇ TEHDİT ETKİSİ

Bu bölümde iç tehdidin tanımı yapılmış, iç tehdide etki eden faktörler ve iç tehdidin motivasyonları anlatılmış, iç tehdidin önemi araştırmalarla ve yaşanmış olaylarla açıklanmıştır. Ayrıca kritik altyapılarda iç tehdidin azaltılmasına yönelik yapılan çalışmalar incelenmiş ve bu bilgiler ışığında iç tehdidin azaltılmasına yönelik önlemlerden bahsedilmiştir.

3.1. Tanımı ve Kapsamı

"Bir zincir en zayıf halkası kadar güçlüdür" sözüne güvenlik perspektifinden bakıldığında en zayıf halka genellikle insandır.

Literatürdeki önemli sorunlardan biri iç tehdit kavramının uzlaşılmış ortak bir tanımının olmamasıdır. Sadece iç tehdit değil içerideki[3] kavramının da kim ya da ne olduğunu tanımlamak tehdidi belirleyebilmek ve azaltabilmek için önemli görülmektedir. İçerideki kavramının genel bir tanımı "bilgi teknolojilerine meşru erişim yetkisi olan kişi" şeklindedir [11]. Başlangıçta tatmin edici bir tanım gibi görünse de günümüz iş dünyasının dış kaynaklı düzenlemeleri, danışmanlar ve geçici çalışanlar düşünüldüğünde "iç" ve "dış" kavramları arasındaki sınırın ne kadar dinamik olduğu anlaşılabilmektedir. Aşağıda belirtilen senaryoların tamamında "meşru erişim" yetkisi bulunmaktadır ve "içerideki" olarak değerlendirilmektedir:

- İşten çıkarılan fakat sisteme erişim bilgileri geçersiz kılınmamış personel (kurum politikası derhal iptal edilmesi gerektiğini belirtmesine rağmen),
- Bir süre önce organizasyonun sistemlerini tasarlayan ve sisteme nasıl girileceğinin bilgisine sahip yazılım geliştiricisi,
- Oturum açmış bir bilgisayarı yetkili kullanıcının izni olmaksızın kullanan bir "maskeli" saldırgan,
- Hademe (sisteme mantıksal erişim yetkisi olmasa da ayrıcalıklı fiziksel giriş yetkisine sahip).

[3] İngilizcedeki "insider" terimi kurum içinden güvenlik ihlaline neden olan kişi anlamındadır. Türkçedeki birebir karşılığı olan "içerideki" kelimesi ise tam olarak bu anlamı karşılamadığından, aslında "insider threat" kavramına karşılık gelen "iç tehdit" kavramı zaman zaman "insider" yerine de kullanılmıştır.

İçerideki kavramı için literatürde yapılmış çeşitli tanımlamalar aşağıdaki özelliklerin bir ya da birkaçına yapılan vurguya ve yorumuna dayanmaktadır:

- Sisteme erişim, beraberinde sisteme erişimin yetkili mi yetkisiz mi olduğu, yetkili ise yetkiyi kimin tanımladığı, erişimin fiziksel mi yoksa mantıksal mı olduğu,
- Kurumu dışarıdakilere temsil etme yetkisi; içerideki bir aktöre kurum tarafından uygulanan politikalar dışarıdan kesin olarak bilinemeyeceğinden aynı aktör dışarıya karşı tamamen farklı politikalara tabi olduğunu iddia edebilir.
- Bilgi; hâlihazırda kurumla herhangi bir bağlantısı olmayan fakat sistemi tasarlayan kişinin bilgisi,
- Kurum tarafından güvenilme; bireyi güçlendiren bir olgudur.

İçerideki kavramının tanımı "meşru olarak erişim yetkisine, kurum varlıklarından en az birisi hakkında temsil ya da karar yetkisine sahip kişi" olarak yapılabilir. İç tehdit ise "yetkilerini kötüye kullanan ya da sisteme erişimi istismar ile sonuçlanan kişi" olarak tanımlanmaktadır [14].

"Kötüye kullanım" terimi birçok sorunu da beraberinde getirmektedir. Bu durumda doğru ve müsaade edilen kullanımın belirtilmiş olması gerekmektedir. Fakat birçok durumda bu kurallar ve politikalar ya hiç belirlenmemiş ya da net olarak belirtilmemiştir. Bu durum yasal, sosyal ve etik yönlerin ele alınmasını gerektirmekte ayrıca akıllara iç tehdit konusunda altta yatan sistemin rolü nedir, iç tehdidin motivasyonları, riskleri ve sonuçları nelerdir sorularını getirmektedir.

ABD İç İşleri Bakanlığı'na bağlı Siber Güvenlik ve Altyapı Güveliği Ajansı için iç tehdit önemle üzerinde durulan bir konudur. ABD Milli Altyapılar Tavsiye Konseyi ilk raporunda iç tehdidi "Bir şirkete, kuruma veya kuruluşa giriş yetkisine sahip ya da bunlarla ilgili içeriden bilgiye sahip olan ve bu yetki ve bilgiyi o işletmenin güvenlik, sistem, hizmet, ürün veya tesislerinin zarar görmesine neden olabilecek zayıflıklarından faydalanmak için kullanan bir veya daha fazla kişi" olarak tanımlanmaktadır [61].

Carnegie Mellon Üniversitesi uzun yıllar yaptığı çalışmalar sonucunda iç tehdidi *"*kurumun varlıklarına erişim yetkisine sahip bir bireyin bu yetkiyi, kötü niyetli ya da kasıtsız bir

şeklide, kurumu olumsuz olarak etkileyecek biçimde kullanma potansiyeli" olarak tanımlamaktadır [13].

İç tehditle ilgili büyük sorunlardan bir diğeri konuyla ilgili gerçek verinin çok az olmasıdır. Çünkü bir iç tehdidin kurumsal ya da organizasyonel bir sistemde yapmaması gereken bir şeyi yapmaya çalışıyor olmasını tespit edebilmek siber ve organizasyonel güvenlik açısından önemli bir sorundur. Tespit edebilmenin güç olmasının sebebi ise iç tehdidin oluşturduğu trafiğin normal trafikten ayırt edilmesinin çok zor olmasından kaynaklanır. Bununla birlikte içeriden gelen tehditler dışarıdan gelen tehditlerin bilmediği bilgilere ve sahip olmadığı yeteneklere sahiptirler ve bunun sonucunda ciddi zararlara yol açabilirler. Tüm bu unsurlar iç tehdit etkisini başa çıkılması en zor problemlerden yapmaktadır [14].

3.1.1. İç tehdidin sınıflandırılması

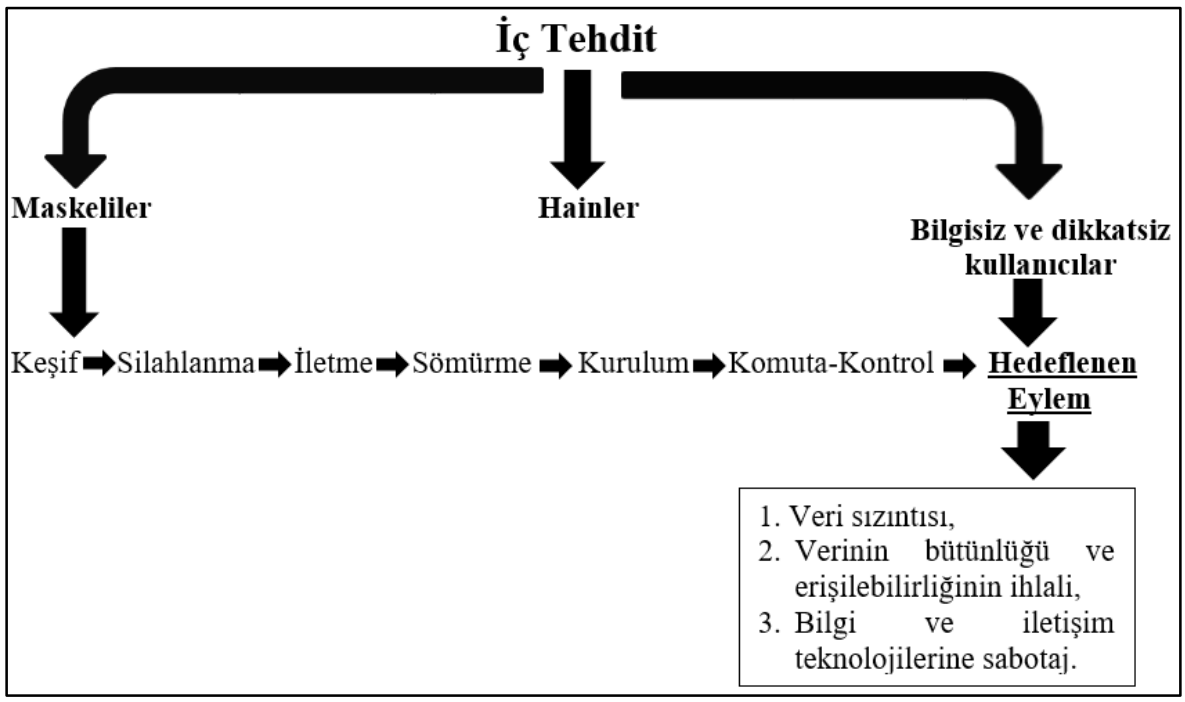
İç tehdit için literatürde çeşitli sınıflandırmalar bulunmaktadır. Predd ve diğerleri [62] iç tehdidi kişinin karakteristik özelliklerine (motivasyonu, bilgisi), kuruma (politikaları), sisteme (sistemin tehdidi kolaylaştırmadaki rolü) ve çevreye (hukuk ve etik ilkeler) göre sınıflandırmıştır. Bishop ve diğerleri [63] ise iç tehdidin kendisi ve erişim ayrıcalığından oluşan bir kaynağa göre sınıflandırmışlardır. Böylece iç tehdidin derecesini bilmek mümkün olabilmektedir.

Sınıflandırma yaparken iç tehdidin türünü belirleyen önemli faktörler bulunmaktadır. Motivasyon, bu faktörlerden biridir. İç tehditle ve onun sonuçlarıyla başa çıkarken önemli bir etkendir. Masum eylemden başlayıp, eğlence, teknik mücadele, suça yönelik niyetler ve casusluğa kadar uzanan geniş bir yelpazeyi kapsayabilmektedir. Aksi beklense de şaşırtıcı şekilde bu motivasyonların her biri benzer yıkıcı etkiye sahip olabilirler. Bu da tabi ki iç tehdidi çok daha önemli ama bir o kadar da karmaşık hale getirmektedir.

İç tehdidin tespiti ile alakalı bilinen ilk çalışmalardan biri [64] iç tehdide neden olan kişileri temel olarak 2 sınıfta toplamıştır: hainler ve maskeliler. Hain, bir kuruluş içindeki sistemlere ve bilgi kaynaklarına erişim hakkı verilmiş ancak eylemleri politikaya aykırı olan ve amacı bazı bilgi varlıklarının gizlilik, bütünlük veya erişilebilirliklerini olumsuz yönde etkilemek olan meşru bir kullanıcıdır. Hain, kötü niyetli eylemlerini sürdürürken kendisine verilen meşru kimlik bilgilerini kullanmaktadır. İç tehdide neden olan kişilerin en bilinen

örneklerinden maskeli ise meşru bir kullanıcının kimliğini çalmayı başarabilen ve kötü niyetli amaçlar için başka bir kullanıcının "kılığına bürünen" bir saldırgandır. Kredi kartı hırsızları, maskelilerin en iyi örneklerindendir. Hırsızlar, bir banka müşterisinin kredi kartı bilgilerini ele geçirir ve bu bilgileri bir maske olarak kurbanın kendisiymiş gibi kullanarak para çalar. Burada hainler grubuna girenlerin maskelilere nazaran kurumla ilgili daha fazla bilgiye sahip olduğu söylenebilmektedir.

Daha yeni bir çalışma [12] ise bu sınıflandırmaya kötü niyetli olmayan fakat bilgisizlik ya da dikkatsizlik sonucu zararlara yol açan kullanıcıları da eklemişlerdir ve sonuç olarak iç tehdide neden olan kişileri 3 ana sınıf altında toplamışlardır. İç tehditlerin sınıflandırılması Şekil 3.1'de gösterilmiştir.



Şekil 3.1. İç tehditlerin sınıflandırılması [12]

Hainler ile bilgisiz ve dikkatsiz kullanıcılar grupları hâlihazırda kurum içinde olduklarından ve kurum içi bilgiye sahip olduklarından hedeflerinde doğrudan ulaşabilmektedirler. Oysa maskeli iç tehditler meşru erişim yetkisine sahip olsalar da kurum içi bilgileri zayıf olduğundan keşif, zararlı kodun iletilmesi, istismar gibi aşamalarda yarattığı trafik dışarıdan gelen tehditlere benzer şekildedir. Böylece maskeli iç tehditlerin tespitine yönelik emareler doğduğundan bu gruba giren saldırganların belirlenmesi diğer gruplara nazaran daha muhtemel konumdadır.

3.1.2. İç kaynaklı saldırıların sınıflandırılması

Genel olarak 3 tip içeriden gelen saldırı türü belirtilebilir:

- Erişim yetkisinin kötüye kullanımı, teknik önlemler kullanarak tespit edilmesi ve engellenmesi en zor saldırı türüdür zira tanım gereği içerideki zaten meşru erişim yetkisine sahiptir.
- Savunmayı atlatma, saldırgan zaten sistemin içinde olduğundan sistemi kurcalamak için daha fazla imkâna sahiptir. Teknik ve teknik olmayan önlemlerin birlikte kullanımına ihtiyaç bulunmaktadır.
- Erişim kontrolü hataları, içerideki herkes tüm sistem kaynaklarına erişim sağlayamamalıdır. Teknik bir sorundur ve önlemesi basit olmakla birlikte, erişim kontrolü hatalarının tespiti, erişim yetkisinin kötüye kullanımının tespitindeki aynı nedenlerden dolayı zordur [64].

İç kaynaklı saldırıların en çok sebep olduğu zararlar ise;

- veri sızıntısı
- verinin bütünlüğü ve erişilebilirliğinin ihlali,
- bilgi ve iletişim teknolojilerine sabotaj olarak sıralanabilir [12].

Genel olarak en tehlikeli hedeflerden olan veri sızıntısı “verinin bir bilgisayardan yetkisiz olarak kopyalanması, taşınması veya alınması” olarak tanımlanabilir. Kurumsal bilginin yetkisiz bir şekilde kullanımı, özel veya hassas verinin istemeden ortaya çıkması ve fikri mülkiyetin çalınması gibi biçimlerde ortaya çıkabilmektedir.

Veri bütünlüğünün veya erişilebilirliğinin ihlali ikinci büyük tehdittir. Böyle bir tehdit, “verinin doğru bir kopyasının artık kurumun erişemeyeceği biçimde ortadan kaybolması veya hasarı” olarak tanımlanabilir. Bu tehdide ilişkin; kullanıcıları şaşırtmak için dosya uzantılarını değiştirmek, hassas verileri şifrelemek/deşifre etmek ve dosyalara müdahale etmek gibi yöntemler bulunur. Fidye yazılım bu tehdit için en iyi örnektir. Fidye yazılımlar kurbanın bilgisayarındaki dosyaları şifreler ve şifrenin tekrar çözülebilmesi için ödeme talep edebilmektedir.

Saldırganın bir diğer hedefi bilgi ve iletişim teknolojilerine sabotaj yapmak olabilir. Kuruma ya da kişiye doğrudan verilecek bir zarar olarak tanımlanabilir. Örnek olarak içeriden ele

geçirilmiş bir bilgisayar ağı (botnet) ile başlatılacak bir DDoS saldırısı dışarıdan gelecek sıradan bir saldırıya göre çok daha ciddi sonuçlar doğurabilmektedir [12].

İç tehdidin kritik altyapılarda yaşanan vakalarda öncelikli hedefi bilgi ve iletişim teknolojilerine, tesisin ya da kurumun fiziksel varlıkların sabotaj olmuştur. Kritik altyapı hizmetleri durmaksızın devam etmesi gereken hizmetler olması sebebiyle en büyük potansiyel hedef de süreçlere müdahale etmek ve sistemin istenmeyen şekilde çalışmasını sağlayarak maddi kayba yol açmak yönündedir. Bununla beraber veri sızıntısı, özellikle ulusal emniyet ve güvenliği sağlayan kurumlara yönelik öncelikli hedef konumundadır.

3.1.3. İç tehdidin motivasyonları ve karakteristiği

Potansiyel bir iç tehdit ile zararlı bir eylem arasında duran 3 temel öge bulunmaktadır. Bunlar; motivasyon, fırsat ve yetenektir [65]. Aslında tehdidin yol açacağı zarar miktarı doğrudan motivasyon ile bağlantılı değildir. Çünkü bazen dışarıdan küçük ve anlamsız gibi görünen bir motivasyon kaynağı yıkıcı etkilere sebep olabilmektedir [14]. Fakat iç tehdidin tespitine giden yollardan biri motivasyon kaynağının belirlenmesinden geçmektedir.

"Kırgın" çalışanlar, kurum içinden zarara sebep olanlarla ilgili geçmişte en çok vurgu yapılan grup olmasına karşın iç tehdide neden olan kişilerin büyük çoğunluğunu oluşturduğu ifadesi basmakalıp bir tespit olarak görülmektedir. Hedef kitlenin bu denli basitleştirilmesi yanlış kişilere odaklanılmasına sebep olabilmektedir [65]. 2008 yılında yapılan bir çalışma kırgın çalışanlar ile iç tehdit arasında herhangi bir bağlantının bulunmadığını tespit etmiştir [61]. Motivasyonun analiz edilebilmesi için karmaşık psikolojik araştırmalara ihtiyaç bulunmaktadır ve analiz yöntemi kişiden kişiye değişmektedir. Shaw ve diğerleri zararlı iç tehdit davranışına etki eden 6 kişisel karakter özelliği belirlemişlerdir [66]:

- Yanlış yetki duygusu; intikam ile sonuçlanan onay ya da statü eksikliği,
- Kişisel ve sosyal hayal kırıklıkları; öfke, yabancılaşma, otoriteden hoşnutsuzluk ve intikam eğilimi,
- Bilgisayar bağımlılığı; agresif yalnızlar, takımın zayıf oyuncuları, ağları keşfetme, güvenlik kodlarını kırma, güvenlik uzmanlarına saldırma ve meydan okuma isteği duyanlar,
- Sadakat yoksunluğu; işveren/kurumdan ziyade mesleği ya da bilgisayar uzmanlığı ile özdeşleşmek,

- Empati eksikliği; davranışın diğerleri üzerindeki etkisini değerlendirememek veya dikkate almamak.

ABD Milli Altyapılar Tavsiye Konseyi, kötü niyetli iç saldırganların, motivasyonunu etkileyen ve ihanete yol açan nedensel bir deneyime veya mekanizmaya sahip oldukları sonucuna varmaktadır [61]. Bu deneyimler 3 ana kaynak altında toplanabilmektedir:

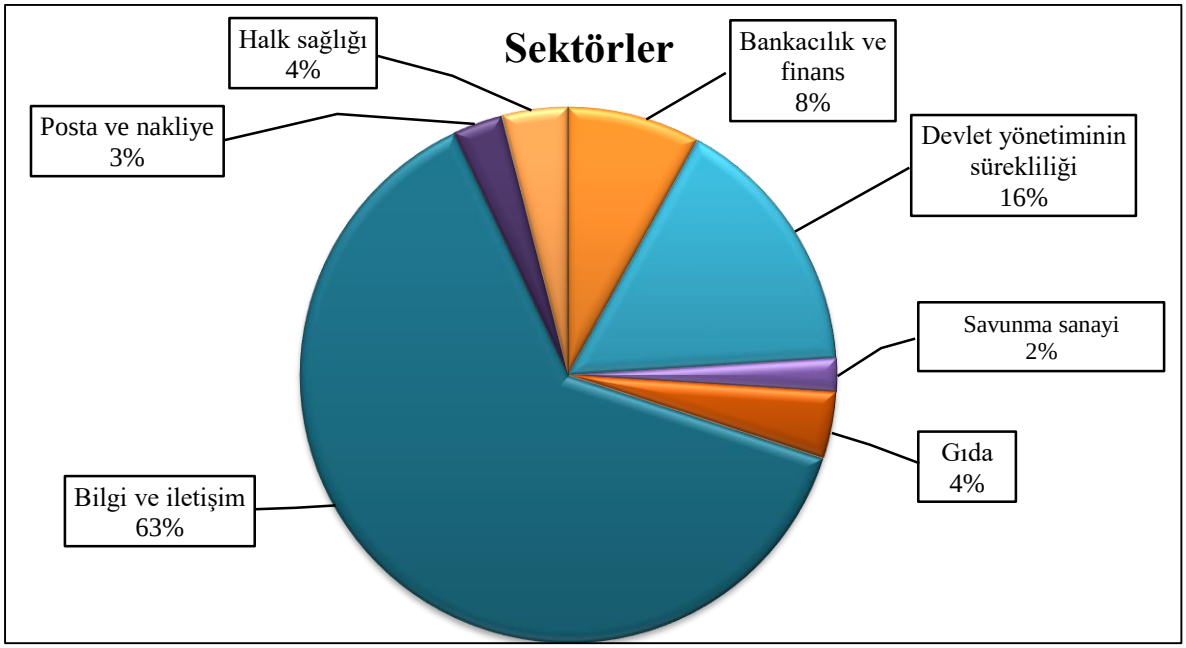
- Kurumdaki konumları ya da kendilerine verilen değer konusunda sürekli büyüyen, şiddetlenen fakat farkına varılmamış hoşnutsuzluk,
- Dışarıdaki hasım tüzel kişiler veya gruplar tarafından işe alınma,
- Kötü niyetli bir tehdit aktörünün güvenilir bir pozisyona sızması.

2005 yılından beri iç tehdit ile alakalı çalışmalar yapan Carnegie Mellon üniversitesi iç tehdit konusunda dünyada muhtemelen en çok veriye sahip olan kurum konumundadır. 2019 itibariyle 1500'den fazla vakayı ele almıştır. 2005 yılında yayınlanan ve ABD Gizli Servisi ile ortak yürütülen bir çalışmanın ürünü olan İç Tehdit Çalışması 1996-2002 yılları arasında kritik altyapı sektörlerinde meydana gelen 49 iç tehdit olayını inceleyen ilk rapordur [67]. Rapor, iç tehdidin birincil hedefinin organizasyonun bazı bölümlerini sabote etmek olduğu olayları incelemiştir. Birincil amacı maddi kazanç olanlar genellikle bankacılık ve finans sektörünü hedef almıştır ve farklı bir raporda ele alınmıştır.

Çalışmada iç tehdide neden olan kişilerin %86'sının hedeflenen kurumda daha önce teknik bir konumda bulunan eski bir çalışan olduğu görülmüştür. Bunların %90'ına işe alındıklarında sistem yöneticisi ya da sisteme ayrıcalıklı erişim yetkisi verilmiştir. Kurumlara bakıldığında ise yaşanan olayların kritik altyapı sektörlerine dağılımı Şekil 3.2'de gösterilmiştir [67].

İç tehdide neden olan kişilerin motivasyonlarına bakıldığında ise temel bulgular şu şekildedir:

- İç tehdit içeren eylemlerin %92'sini işle ilgili olumsuz bir olay tetiklemiştir.
- İç tehdide neden olan kişilerin %85'inin olaydan önce işle ilgili bir şikâyeti bulunmaktadır.
- Olayların %84'ünün motivasyon kaynağı intikam duygusu olarak tespit edilmiştir [67].

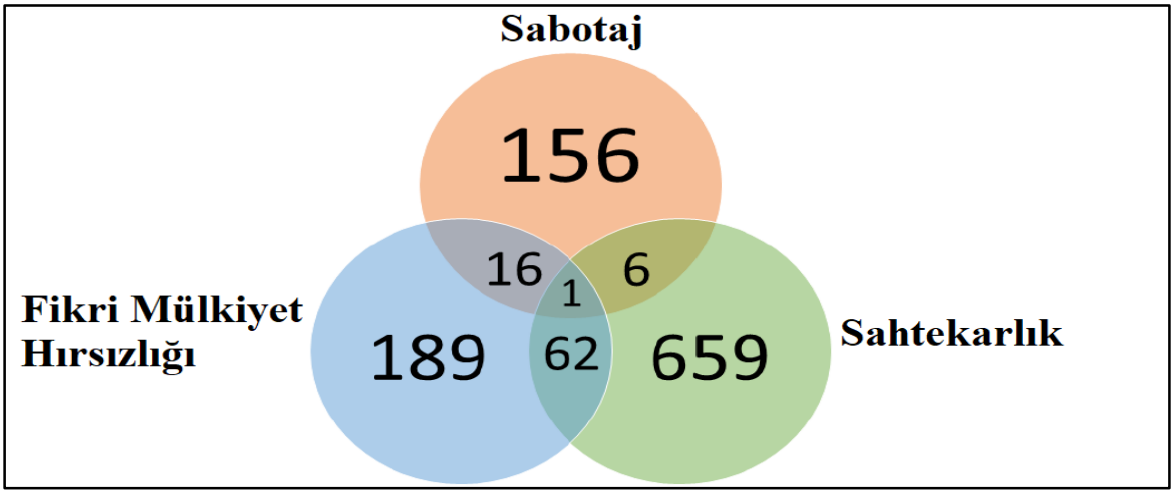


Şekil 3.2. İç tehdit kaynaklı siber olayların kritik altyapı sektörlerine dağılımı

İç tehditle ilgili bilgileri toplamaya devam eden Carnegie Mellon Üniversitesi günümüzde çalışmalarını hala sürdürmektedir. Elde ettiği verilerle iç tehdidi azaltmaya yönelik ortak hareket tarzı belirlemeyi amaçlayan bir rehber yayınlamaya başlamıştır. Altıncı basımı Aralık 2018'de yayınlanan rehberde 21 maddelik bir yol haritası belirlenmiştir ve yeni vakalar incelendikçe güncellenmeye devam etmektedir [13]. Rehberde 1500'den fazla olay içerisinde 1154 zararlı iç tehdit aktivitesi tespit edilmiştir. Zararlı iç tehdit eylemlerinde gözlemlenen 4 temel eğilim aşağıda sunulmuştur.

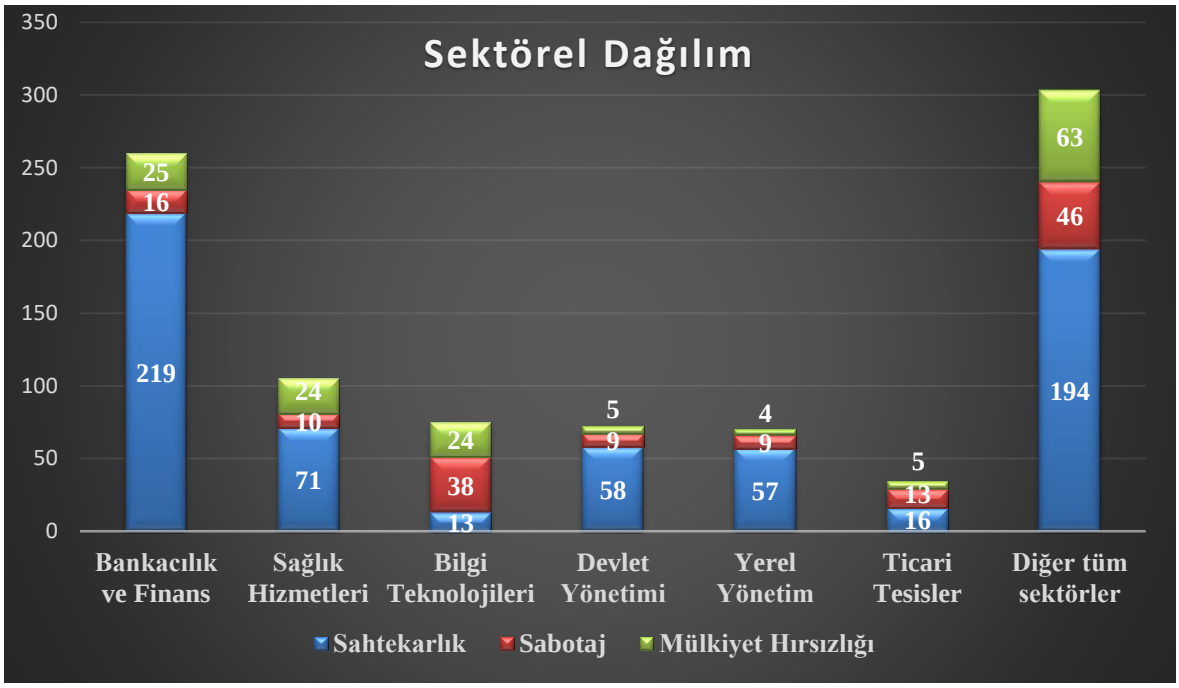
- Bilgi teknolojisi sabotajı, içeriden bir kişinin, bir kuruluş veya bireye zarar vermek için bilgi teknolojilerini kullanmasıdır.
- Fikri mülkiyet hırsızlığı, içeriden bir kişinin, kuruluştan fikri mülkiyeti çalmak için bilgi teknolojilerini kullanmasıdır. (Bu kategori dış destek içeren endüstriyel casusluğu da kapsamaktadır).
- Sahtekârlık, içeriden bir kişinin, kişisel kazanç sağlamak için bir kuruluşun verilerini (programlar veya sistemler değil) yetkisiz bir şekilde değiştirmek, silmek ya da bir kimlik suçuna (örneğin kimlik hırsızlığı veya kredi kartı sahtekârlığı) yol açan bilgileri çalmak amacıyla bilgi teknolojilerini kullanmasıdır.
- Diğer; fikri mülkiyet hırsızlığı, sahtekârlık veya bilgi teknolojileri sabotajı kategorilerine girmeyen durumlardır.

Diğer sınıfına giren olaylar haricinde iç tehdit eğiliminin dağılımı Şekil 3.3'de sunulmuştur.



Şekil 3.3. İç tehdit kaynaklı olayların eğilim dağılımı [13]

İncelenen olaylar neticesinde iç tehditten en çok zarar gören sektörler Şekil 3.4'de sunulmuştur.



Şekil 3.4. İç tehdit kaynaklı olaylarda en çok zarar gören sektörler [13]

3.2. İç Tehdit Etkisi ve Önemi

İç tehdit, Avrupa Birliği'nin siber güvenlikten sorumlu ajansı ENISA tarafından hazırlanan "2018'in 15 Siber Tehdidi" raporunda en çok maruz kalınan 15 siber tehditten biri olarak yer almaktadır [68]. Raporda iç tehdit etkisi, "yetkili erişim hakkını isteyerek ya da

istemeyerek organizasyonun güvenliğine zarar verecek şekilde kullanan kişinin yarattığı etki" olarak tanımlanmıştır. İç tehdit etkisinin normal aktiviteden ayrılmasının zor olmasından dolayı organizasyonlar ve hükümetler tarafından önemli bir risk faktörü olarak değerlendirildiğinden bahsedilmiştir. İç tehdit etkisiyle mücadele edebilmek için ise teknik, sosyolojik ve sosyo-teknik alanlarının bir arada kullanıldığı bir yöntem önermiştir. Rapor iç tehdidin yaratacağı zararı en aza indirgemek için şu yöntemler önerilmektedir:

- İç tehdide yönelik güvenlik politikası,
- Kimlik ve erişim yönetiminin kullanımı,
- Kimlik yönetimi çözümleri ve rol tabanlı erişim yönetimi,
- Güvenlik istihbaratı çözümleri,
- Veri temelli davranış analiz araçları,
- Ayrıcalıklı kimlik yönetimi çözümleri,
- Eğitim ve farkındalık aktiviteleri,
- Denetim ve kullanıcı izleme planları,
- Eğitim ve farkındalık aktivitelerinin uygulanması.

Dünya üzerinde siber güvenlikle alakalı genel yanlış kanı tehdidin sadece dışarıdan geleceği yönündedir. Bu yüzden de güvenlik cihazları yatırımları, konfigürasyonları, izleme ve kontroller dışarıdan gelebilecek bir tehdide yönelik planlanır ve icra edilir. Araştırmalar, siber sahtekârlığın %70'inin dış suçlular yerine içeridekiler tarafından yapıldığını, güvenlik kontrollerinin ve izlemenin %90'ının dış tehditlere odaklandığını göstermektedir [69].

İngiltere'de yapılan bir çalışma kurumların iç tehdit algısıyla alakalı çarpıcı bazı verileri gözler önüne sermektedir [70]:

- Kurumların %52'si herhangi bir güvenlik risk değerlendirmesinde bulunmamışlardır;
- Kurumların %67'si gizlilik dereceli bilginin USB yoluyla sızdırılmasını önlemek için hiçbir önlem almamaktadır;
- Kurumların %78'inde şifrelenmemiş diskleri çalınmış bilgisayarlar bulunmaktadır.
- Kurumların %84'ü giden e-postaları gizlilik dereceli bilgi açısından taramamaktadır.

Oysa ki kötü niyetli bir iç tehdit dışarıdan gelebilecek saldırılara karşı bazı avantajlara ve daha fazla yıkım potansiyeline sahiptir. İç saldırganların, tesislere veya bilgiye erişimde meşru giriş hakları hatta sık sık da ayrıcalıklı yetkileri bulunur. Bununla birlikte tesisteki kritik varlıkların yerleri hakkında ve kurumun işleyişi hakkında bilgi sahibidirler. İç

saldırganlar kurumun sadece politika ve prosedürlerini bilmekle kalmayıp açıklıklarını da bilmektedirler. Hatta bazı durumda güvenliği tasarlayan kişilerdir. Dolayısıyla ne zaman, nereye saldıracaklarını ve izlerini nasıl yok edebileceklerini çok daha iyi bilmektedirler. Bir dış saldırgan kurumla ilgili birçok bilgi toplaması gerekirken, iç saldırgan hedefini belirleyebilmekte ve dış saldırganın karşılaştığı hiçbir güvenlik engeli ile uğraşmak zorunda olmamaktadır. Dış saldırganlar için çok katmanlı bir korumaya karşı saldırıya geçmektense bir iç tehdit kaynağı yerleştirmek çoğu zaman daha maliyet-etkin ve hızlı bir çözümdür [65].

ABD Ulusal İç Tehdit Merkezi, ABD Gizli Servisi, CSO Dergisi tarafından yürütülen ve Forcepoint'in sponsor olduğu 2017 ABD Siber Suçlar Anketi, elektronik suç olaylarının %20'sinin içeriden kaynaklandığının tespit edildiğini ya da iç kaynaklı olmasından şüphelenildiğini ortaya koymuştur. Ankette ayrıca ankete katılanların %30'unun içeriden gelen saldırıların neden olduğu zararın dış kaynaklı saldırılardan daha şiddetli olduğunu düşündüğü ortaya çıkmıştır. Ankete göre, iç tehdidin neden olduğu en yaygın olaylar şu şekildedir (azalan sırada):

- Özel veya hassas bilgilerin istemeden ifşası,
- Müşteri kayıtlarının tehlikeye düşmesi veya çalınması,
- Çalışan kayıtlarının tehlikeye düşmesi veya çalınması,
- Özel veya hassas bilgilerin kasıtlı olarak açıklanması ve
- Gizli belgelerin (örneğin ticari sırlar veya fikri mülkiyet) tehlikeye düşmesi veya çalınması [71].

Yaşanan olaylar iç tehdidin, kuruluşlar için finansal kayıplar, ticari faaliyetlerde olumsuz etkiler ve itibarın zedelenmesi gibi etkilere sahip olabileceğini göstermiştir. Yapılan çalışmada [67] kurumların %81'inin iç tehdit aktörlerinin neden olduğu saldırılar sonucu olumsuz ekonomik etkiler yaşadığı görülmüştür. McAfee ise veri ihlallerinin %43'ünün iç kaynaklı olduğunu (kötü niyetli ya da kasıtsız) belirtmektedir [72].

Ponemon Enstitüsü tarafından yayımlanan 2018 İç Tehditlerin Maliyeti: Global Kuruluşlar adlı çalışma, küresel çapta içeriden gelen tehditlerin verdiği zararın 12 ayda ortalama 8,76 milyon dolar olduğunu ortaya koymaktadır [3]. Araştırmacılar, Kuzey Amerika, Avrupa, Orta Doğu, Afrika ve Asya-Pasifikteki 1000'i aşkın çalışanı olan 159 organizasyondaki 717 BT ve BT güvenlik uzmanıyla mülakat yapmışlardır. Son 12 ayda tüm kuruluşlarda toplam 3.269 iç tehdit vakası tespit edilmiştir. Araştırmanın diğer öne çıkan sonuçları şunlardır:

- Her türden iç tehdit artış göstermektedir. 2016'dan bu yana, çalışan veya yüklenici ihmalini içeren ortalama olay sayısı yüzde 26, suçlu ve kötü niyetli içerdekiler için yüzde 53 artmıştır. Kimlik bilgileri hırsızlığı olaylarının sayısı son iki yılda yüzde 170 oranında artmıştır.
- Araştırma, iç tehditlerin tespit edilmesi ve yönetilmesinin zor olmaya devam ettiğini göstermektedir; bir olay ne kadar uzun sürede çözülürse, kuruluşlar için o kadar maliyetli olmaktadır. İç tehditleri içeren olayların ortalama süresi 72 gündür. Olayların sadece %16'sı tespit edilmiş ve 30 gün içinde durdurulabilmiştir.
- Finansal kuruluşlar, iç tehdit maliyetleri açısından yıllık ortalama 12,05 milyon dolarla başı çekmektedir. Enerji ve kamu hizmetleri 10,23 milyon dolarla ikinci sıradadır. İmalat örgütleri, iç tehditle ilgili olayları karşılamak maksadıyla yıllık ortalama 8,86 milyon dolar maliyete maruz kalmıştır.
- En yüksek yıllık iç tehdit maliyeti 11 milyon dolarla Kuzey Amerikadadır. Ardından 7 milyon dolarla Avrupa ve Orta Doğu gelmektedir ve bunları yıllık 6 milyon dolarla Asya-Pasifik izlemektedir.

Cybersecurity Insiders'ın yayınlamış olduğu 2019 İç Tehdit Raporunda yer alan önemli bulgular ise şu şekildedir [73];

- kurumların %70'i iç tehdit bağlantılı saldırıların daha sık olduğunu kabul etmektedirler,
- %68'i iç tehdit saldırılarına aşırı derecede veya orta derecede açık olduklarını hissetmektedirler,
- %39'u bulut depolama ve dosya paylaşımı uygulamalarının iç tehdide karşı en hassas uygulamalar olduklarını belirtmişlerdir,
- kurumların %85'i iç tehdidin gerçek zararını belirleyebilmenin orta zorlukta veya çok zor olduğunu bildirmişlerdir,
- %56'sı buluta göç etme sebebiyle iç tehdidi tespit edebilmenin daha zor olacağına inanmaktadır.

Verizon'un 2019 Veri İhlali Araştırma Raporu 41.686 güvenlik olayını analiz etmiş ve bunların 2.013'ünün veri ihlali olduğunu doğrulamıştır [2]. Raporda iç tehdit ve iç tehdit aktörleriyle ilgili önemli veriler şu şekildedir;

- ihlallerin üçte birinde iç tehdit aktörü bulunmaktadır,
- tüm siber güvenlik vakalarının %20'si ayrıcalığın kötüye kullanımından kaynaklanmıştır,

- ihlallerin %29'unda çalınmış ya da ele geçirilmiş kullanıcı adı ve parola bilgileri bulunmaktadır.

NATO'nun Siber Güvenlik Mükemmeliyet Merkezi'nin İç Tehdit Tespit Çalışması ise iç tehdidin önemini dünyayı sarsan olayları ve baş aktörlerini sunarak anlatmıştır [74]. Bu olayların tamamında güvenilir bir şahıs kuruma büyük zararlar vermiştir. Örneğin, Stuxnet saldırıları nükleer madde ayrımı görevini yapan santrifüjleri kontrol eden programlanabilir mantıksal kontrolörleri (PLC) sabote ederek İran nükleer programını durdurmuştur [75]. Bu tür tesisler genellikle geniş alan bağlantısı ve katı erişim politikaları olmayan yerel alan ağlarını kullanmaktadırlar. Bu nedenle, en mantıklı sonuç, içeriden bir insanın sisteme kötü amaçlı yazılım yüklemesidir.

Yükleniciler, Edward Snowden vakasında olduğu gibi, kritik sistemleri geliştirmek veya sürdürmek için sıklıkla kullanılmaktadırlar. Snowden, Merkezi İstihbarat Ajansı (CIA) bünyesinde sistem yöneticiliği yapmıştır. Daha sonra en büyük müşterilerinden biri Ulusal Güvenlik Ajansı (NSA) olan Dell ve Booz Allen Hamilton'da sistemleri yönetmek (ve tasarlamak) amacıyla çalışmıştır. Sonuç olarak, birkaç yıl boyunca topladığı yüksek gizlilik dereceli verilere erişebilmiştir. Tüm belgeleri 2013 yılında gazetecilere açıklamış ve ardından The Guardian, Der Spiegel, The Washington Post ve The New York Times gibi medya yayın organlarında yayınlanmıştır [76].

Snowden olayından önce ise, 2010 yılında, Chelsea Elizabeth Manning (eski adıyla Bradley Edward Manning) Irak ve Afganistan'daki savaş kayıtlarını, gizli bilgileri yayınlamaya adanmış bir site olan Wikileaks'e göndermiştir. Materyallerin arasında, bir Apache saldırı helikopterinin Bağdat'taki gazetecilere saldırdığı bir "dost ateşi" olayını belgeleyen tartışmalı bir video da bulunmaktadır [77-78].

ABD'nin Vietnam'daki politik ve askeri müdahaleleri ile alakalı çok gizli bir çalışma olan "Pentagon Papers"ı yayınlayan Daniel Ellsberg, Snowden ve Manning ile karşılaştırılabilir [79-80]. Ellsberg çalışmanın yazımında bulunmuştur ancak savaşa karşı çıkmıştır. Bunlardan başka, Estonya Savunma Bakanlığı'nın güvenlik departmanının eski şefi Herman Simm, yabancı bir ulus için casusluk yapmakla suçlanmıştır [81]. Suçunu kabul etmiş ve 2009 yılında hapis cezasına çarptırılmıştır [82]. Diğer bir örnek, ABD Ordusu psikiyatrı olan ve 13 kişinin öldürülmesinden sorumlu Nidal Malik Hassan'dır. Hassan, katliamdan önce

bilinen bir El Kaide üyesi ile e-posta alışverişinde bulunmuş ve FBI tarafından soruşturulmuştur [83]. Fakat önleyici bir tedbir alınmamıştır.

3.2.1. İç tehdide etki eden faktörler

Carnegie Mellon Üniversitesi'nin gerçekleştirmiş olduğu ve literatürde önemli bir yere sahip olan İç Tehdit Çalışması [67] üzerinden gerçekleştirilen bir diğer çalışma [84] iç tehdide sebep olan etkenlerle ilgili "büyük resmi" görmemizi sağlamıştır. İncelenen olayların analizi sonucu iç tehdide etki eden 7 temel gözlem yapılmıştır:

Gözlem 1: İç tehdide neden olan aktörlerinin birçoğunda BT sabotajı gerçekleştirme riskine katkıda bulunan kişisel eğilimler mevcuttur. Bu kişisel eğilimler gözlemlenebilir bazı karakter özellikleri ile teşhis edilebilmektedir:

- Ciddi zihin sağlığı bozuklukları
- Sosyal beceri ve karar verme yeteneği eksikliği
- Kural ihlallerinin bulunduğu bir geçmişe sahip olma.

Gözlem 2: BT sabotajına yeltenen iç tehdit aktörlerinin çoğu, beklentilerinin karşılanmaması sebebiyle kuruma küskünlerdir.

Olaylarda gözlenen karşılanmayan beklentiler arasında yetersiz maaş/ikramiye, terfi eksikliği, çevrim içi faaliyetlerin kısıtlanması, şirket kaynaklarının kullanımına getirilen kısıtlamalar, işyerinde mahremiyet ihlali, azalan yetki/sorumluluklar, haksız iş gereksinimleri algısı ve iş arkadaşlarıyla zayıf ilişkiler yer almaktadır.

Gözlem 3: Çoğu durumda stresli olaylar, kurumsal yaptırımlar dahil olmak üzere, kurum içi sabotaj olasılığına katkıda bulunmuştur.

Vakalarda gözlenen stresli olaylar, zayıf performans değerlendirmeleri, kabul edilemez davranışlara yapılan uyarılar, aşırı devamsızlık nedeniyle uzaklaştırılma, düşük performans sebebiyle daha alt bir pozisyonda görevlendirilme, sınırlı sorumluluklar ve internet erişimi, maaş veya ikramiye konusundaki hoşnutsuzluklar, kıdem tazminat paketlerinin eksikliği, işe alınan yeni denetçiler, boşanma ve ailede ölümdür.

Gözlem 4: BT sabotajı olaylarında davranışsal emareler sıklıkla mevcutken kurum tarafından göz ardı edilmiştir.

İncelenen olaylarda gözlenen davranış emareleri arasında uyuşturucu kullanımı, iş arkadaşlarıyla çatışmalar, saldırgan veya şiddet içeren davranışlar, şirket hesaplarından uygunsuz satın almalar, ruh hali değişimleri, kötü iş performansı, işe gelmeme veya gecikme, cinsel taciz, vasıfla ilgili yanıltıcı davranışlar, kıyafet düzenlemesi ihlalleri ve temizliğe önem vermeme sayılabilir. Davranışsal belirteçlerin çoğu, açık kurumsal politika ve kuralların doğrudan ihlalidir.

Gözlem 5: Birçok olayda kuruluşlar teknik emareleri tespit edememişlerdir.

Vakalarda gözlenen teknik emareler arasında bilgisayar korsanlığı araçlarının indirilmesi ve kullanılması, yedek oluşturulamaması, belge yönetim sistemlerine veya yazılımına erişimde yaşanan sorunlar, müşterilerin veya iş arkadaşlarının sistemlerine yetkisiz erişim, işten çıkarılma sonrasında sisteme erişme, işte uygun olmayan internet erişimi ve kurulumları ve arka kapı hesaplarının kullanılması yer almaktadır.

Gözlem 6: İç tehdit aktörleri, saldırılarını gerçekleştirmek, kimliklerini ve eylemlerini gizlemek amacıyla yönetimin bilmediği erişim yollarını kullanmış veya yeni erişim yolları oluşturmuşlardır. İç kaynaklı saldırganların çoğunluğu işten çıkarılma sonrasında faaliyete geçmişlerdir.

Analiz edilen vakalardaki birçok kişi, işten çıkarılma öncesinde saldırıyı ayarlamak maksadıyla teknik adımlar atmak için ayrıcalıklı sistem erişim yetkisini kullanmıştır. Örneğin, arka kapı hesapları oluşturulmuş, şifre kırıcı yazılımlar, uzaktan ağ yönetim araçları ve organizasyon sistemlerine erişmek için modemler kurulmuştur. Ayrıca işten çıkarılmada uygulanan etkisiz güvenlik kontrollerinden faydalanılmıştır. Bu adımların çoğu, bilinmeyen erişim yollarının oluşturulmasına veya kullanılmasına neden olmuştur.

Gözlem 7: Fiziksel ve elektronik erişim kontrollerinin eksikliği BT sabotajını kolaylaştırmıştır.

Olaylarda gözlenen erişim kontrolü güvenlik açıkları, çalışanların oturum açtıktan sonra başıboş bıraktıkları bilgisayarlardan, kuruluş tarafından bilinemeyen hesaplar oluşturma yeteneğinden, yazılım kodunun kuruluşun onayı veya bilgisi olmadan üretim sistemlerine dâhil edilebilmesinden ve işten çıkarma sırasında uygulanan elektronik ve fiziksel erişimin engellenmesi önlemlerinin yetersizliğinden oluşmaktadır.

İç tehdide neden olan, ortaya çıkmasına sebep olan etkenlerin belirlenebilmesi ve etki eden faktörlerin doğru anlaşılması iç tehdidin tespitine ve önlenmesine giden yoldaki en önemli adımdır. Bu faktörlerin kaynağı sadece kurumun içi ve şahsın kendisi değildir. Çevresel etmenler de iç tehdide etki eden önemli faktörlerdendir [65].

İç tehdide etki eden teknik ve sosyal faktörler

Teknolojinin gelişimi sosyal davranışları ve etkileşimleri de değiştirmektedir. Sosyal medyanın yaygınlaşması ve mobil iletişim teknolojilerinin kullanımı bilgi güvenliği için bir mücadele sahası durumundadır. Gün geçtikçe daha çok çalışan işlerini daha etkin bir biçimde yerine getirmek amacıyla iş yerinde BT uygulamaları ve cihazlarının özgürce kullanımını ifade eden "teknolojik demokrasi"yi talep eder olmuştur [85]. Bugün artık kişisel gizliliğin korunduğu, devletlerin ya da iş yerinin denetiminden bağımsız "özgür internet" kavramı ortaya çıkmış durumdadır. Doğrudan cep telefonu ve internetin olduğu bir dünyaya doğan Y kuşağı artık orta kademe yönetici kadrolarını işgal etmeye başlamışlardır [86]. Bu yüzden teknoloji ve güvenlik şirketleri hem özgürlüğün hem de denetimin sağlanabildiği "kendi cihazını getir" (Bring Your Own Device, BYOD) teknolojileri oluşturmuşlar, kurum ve kuruluşlar da güvenlik politikalarını bu yönde belirlemeye başlamışlardır.

Fakat, güvenlik tedbirleri iş yerindeki sosyal ve teknolojik değişimlere uyum sağlayamamaktadır. Taşınabilir veri cihazları, iç tehdit kaynaklı bilgi sızıntılarını kolaylaştırmaktadır: Araştırmalar [87], çalışanların %89'unun haftada en az bir kez kişisel bir taşınabilir cihazı şirket ağına bağladığını ve İngiltere'deki işletmelerin yarısından fazlasının taşınabilir bellek cihazlarının kullanımını yönetecek kontrol mekanizmalarına sahip olmadıklarını göstermiştir.

İç tehdide etki eden mesleki ve ekonomik faktörler

Günümüzün giderek artan rekabet ortamında, çoğu kuruluş bir dönüşüm yaşamaktadır ve taşeronlaştırma bu dönüşümü başarmanın yaygın yollarındandır. Kuruluşların kritik sistemlerine uzun süreli erişim sağlayan üçüncü taraf personel sayısı hızla artmaktadır. Tek bir taşeronlaştırma işlemi yüzlerce 'yabancı' kişinin durumunu 'içerideki' şeklinde değiştirebilmekte ve bir şirketin çalışanları ile üçüncü taraf personel arasındaki farkı bulanıklaştırabilmektedir. Çünkü bu personel, kuruluşun tam zamanlı çalışanları ile aynı düzeyde mantıksal ve fiziksel erişim yetkilerine sahip olabilmektedir.

McAfee ekonomik durgunluğun, siber suçluların, masum iç tehdit aktörlerini kendileri ve kuruluşları hakkında hassas bilgileri ifşa etmeye zorlamak için verimli bir zemin oluşturduğuna inanmaktadır [88]. Araştırmalar ayrıca, ekonomik iklim kötüleştikçe, işten çıkarıldığında veya ihtiyaç fazlası duruma geldiğinde, rekabet avantajı ve kurumsal güvenliği korumak için kritik olan özel veri ve bilgileri alabileceklerini söyleyen katılımcıların sayısında keskin bir artış olduğunu ortaya koymaktadır [89].

İç tehdide etki eden kültürel faktörler

Organizasyonlar değişen şartlara ayak uydurabilmek için sürekli bir dönüşüm içindedirler. Fakat bu dönüşüm doğru yönetilmezse çalışanlarda korku, belirsizlik ve şüpheye sebep olabilir ki bu da güvenliğe karşı olan davranışları etkileyebilmektedir.

Bölgesel kültüre bakıldığında ise örneğin batılıların Hindistan'daki kast sistemi ve hiyerarşik uygulamalarını, örneğin kültürel, dini ve toplumsal baskıları anlamaları genellikle zordur. İşte gereken kurallar her zaman sayısız nesiller boyunca yerleşmiş davranışlardan daha az önemli olmaktadır [65].

3.3. Gelişmiş Israrcı Tehdit (GIT) ve İç Tehdit

Siber güvenlik için yüklü yatırımlar yapmış bir kuruma sızmak maksadıyla birçok güvenlik ürününü aşmak yerine, kurum içinden bir kişiyi kullanmak çoğu zaman maliyet ve zaman açısından daha etkin olmaktadır. Bu nedenle siber suç örgütleri ve Gelişmiş Israrcı Tehdit

grupları sıklıkla içeriden destek almaktadırlar bu nedenle GIT'leri tanımak ve yöntemlerini bilmek iç tehdidi tespit edebilmek amacıyla önem arz eder.

3.3.1. Gelişmiş ısrarcı tehdit

Kritik altyapılar gibi tehlikeye düşmesi halinde bir devletin güvenliğinde büyük zararlara yol açabilecek altyapılara yönelen siber saldırganlar hedeflerine ulaşabilmek maksadıyla bolca zaman ve para harcamaktan çekinmemektedirler. Güçlü destek ve kaynaklara sahip olmalarının yanında sinsi, kesintisiz ve karmaşıktırlar. Bu yüzden tespitleri zor, hedeflerine ulaşmakta kararlı ve bilgi, tecrübe düzeyleri yüksektir. Dolayısıyla zarara yol açma ihtimalleri daha yüksek ve verdikleri zarar miktarı da büyüktür. Tüm bu sebepler GIT'leri bütün siber sistemler için en yüksek risk grubuna sokmaktadır. Yaşanan olaylar da giderek artan bir tehdit olduklarını göstermektedir.

ABD Ulusal Standartlar ve Teknoloji Enstitüsü [90], GIT için şu tanımı kullanmıştır: "Yüksek bilgi ve tecrübe ile önemli kaynaklara sahip olan hasım bunları kullanarak çoklu saldırı vektörleri (siber, fiziksel gibi) ile amaçlarına ulaşmak için kendisine uygun fırsatlar oluşturur. Buradaki amaçlar genellikle, sürekli olarak bilgi toplamak ve/veya bir misyonun, programın veya kuruluşun kritik yönlerini sekteye uğratmak veya engellemek ya da gelecekte bunu yapacak bir konumda bulunabilmek maksadıyla hedeflenen kuruluşların bilgi teknoloji altyapısında bulunmak ya da buradaki varlığını genişletmektir." GIT;

- amaçlarını gerçekleştirmek için uzun süre takipte kalır,
- hedefin savunma sistemine karşı koyabilmek için ona uyum sağlar,
- belirlenen amacı gerçekleştirmek için gerekli olan etkileşim seviyesini sağlar ve onu korur [91].

Her ne kadar farklı amaçları gerçekleştirmeye yönelik olsalar da GIT'ler benzer yapılara ve işleyişe sahiptirler. GIT'leri hedeflerine ulaşırken kullandıkları ve saldırı evrelerini tanımlayan yönteme siber ölüm zinciri (cyber kill chain) denilmektedir.

Siber ölüm zinciri bir siber saldırının evrelerini ortaya koymaktadır. Bu evreler bilgi toplamadan sisteme sızmaya kadarki süreci kapsamaktadır. Gelişmiş ısrarcı tehditleri analiz edebilmek amacıyla saldırının aşamalarını belirlemek, önlem almak için gerekli yöntemlerin geliştirilmesine olanak sağlar. Siber ölüm zinciri aynı zamanda savunmasız veya savunması

zayıf bir ağın güçlendirilmesine yardımcı olmak için bir yönetim aracı olarak da kullanılabilmektedir. Tipik bir siber ölüm zincirinin aşamaları aşağıda açıklanmıştır [92].

Siber ölüm zinciri

Keşif/Bilgi Toplama

Siber ölüm zincirinin ilk aşaması keşif aşamasıdır. Bu aşamada saldırgan hedefi teknik ve teknik olmayan bir bakış açısıyla dışarıdan değerlendirir. Saldırganın amacı, hangi kaynaktan daha fazla fayda sağlayabileceğini saptamaktır. Saldırgan, istismar edebileceği güvenlik açıklarını arar. Bunu yaparken aktif ve pasif bilgi toplama olarak adlandırılan iki çeşit bilgi toplama yöntemini kullanabilir. Port taraması ya da zafiyet taramaları bu aşamada kullanılabilecek yöntemlerdendir.

Silahlanma

Bu aşamada tehdit aktörü, bir önceki aşamada keşfedilen güvenlik açıklarına özel olarak hazırlanmış kötü amaçlı yazılımlar geliştirir. Keşif aşamasında toplanan istihbarat temelinde, saldırganın silahlanma aşamasında nasıl bir yol izlemesi gerektiğine karar vermesi için kullanılır. Bu aşamaya kısaca silahın belirlendiği aşama diyebiliriz.

Teslimat/İletme

Siber ölüm zinciri metodolojisinin üçüncü aşaması, zararlı kodun, kurbanı sömürmek için hedef bilgisayara iletilmesidir. 2018 Verizon Veri İhlali Araştırma Raporundan gelen araştırma ve analizler, ağ saldırılarının büyük ölçüde, kurumun iç çalışanları hedef alınan oltalama saldırılarından kaynaklandığını göstermektedir.

Bilgi toplama aşamasında toplanan verilere dayanarak, bir kuruma özel araştırılmış ve hazırlanmış oltalama saldırısı ile zararlı yazılım kuruma bulaştırılabilmektedir. Hedefli oltalama (spear phishing) olarak adlandırılan saldırı tipinde hedefin kim olacağı da bilgi toplama aşamasında belirlenir ve en zayıf halka hedef olarak seçilir. Çoğunlukla Microsoft Word veya Adobe PDF belgesi gibi bir ek içerir ve bu ek kurum içi ağa erişilmesine sebep olacak ilk adımı oluşturur.

İstismar (Sömürme)

Sömürü aşamasında, kötü amaçlı yazılım kodu hedef ağda, uzaktan veya otomatik olarak yürütülür ve hedeflenen bilgi sistemine erişimi sağlamak için mevcut güvenlik açıklarından yararlanır.

Kurulum

Sistemin sömürülmesi başarılı olduktan sonra, kötü amaçlı yazılım kodu kendisini hedeflenen bilgi sistemine yüklemeye çalışacaktır. Bu noktada ağ erişimi varsa, zararlı yazılım, dışarıdan güncellemeler ve yazılımlar indirmeye başlayacaktır. Bu güncellemeleri kendini daha fazla gizlemek ve iz sürülemez hale getirmek için kullanabilir.

Komuta ve Kontrol

Bu aşama C2 (Command and Control) olarak adlandırılabilir. Bu aşama saldırganın iletişim kodlarını hedef ağa yerleştirdiği aşamadır. Bu yazılım, saldırganın ortamdaki tehdit kodunu tamamen yönetmesine ve saldırganın ağda daha derin bir şekilde hareket etmesine, veri göndermesine ve arkasında bıraktığı izleri yok etmesine olanak sağlar.

Hedeflenen Eylem

Hedef sistem ele geçirildikten sonra, saldırgan amacına ulaşmak için çeşitli eylemler gerçekleştirir. Veri çalma, değiştirme ve silme, bulunduğu yerden başka bir sisteme sıçrama, gibi eylemler örnek gösterilebilir. Asıl hedefine ulaşmak için yapması gereken tüm eylemlerin yapıldığı son aşamadır.

3.3.2. Gelişmiş ısrarcı tehdit ve iç tehdit ilişkisi

Gelişmiş ısrarcı tehdit sadece yukarıda tanımlanan kendi özellikleri itibariyle dahi büyük bir risk faktörü iken iç tehdit ile birleşmesiyle beraber sorun ikiye katlanmaktadır. Bu ilişkinin temel sebebi iç tehdit unsurlarının genellikle maddi çıkar motivasyonu ile hareket etmesidir. GIT'ler ise yüksek kaynaklara sahiptirler ve mümkün olduğu kadar tespit edilmeden ilerlemek istemektedirler. Tespit edilmeden hedefe ulaşmanın önemli yollarından birisi ise içeriden değerli bilgileri alabilmektir. Bu nedenle GIT'ler genellikle iç tehditlerden faydalanmaktadırlar [93].

Bununla beraber GIT'ler ve iç tehditler geleneksel saldırı yöntemlerinden ayrılan bazı benzer özelliklere sahiptir [94]:

- Saldırıları ayrıntılı planlama gerektirir ve tespitten kaçınmak için uzun bir sürece yayılmaktadırlar. İç tehdit unsurları mevcut güvenlik kontrollerinin farkında olduklarından, saldırılarının planlanmasında GIT'lere göre potansiyel bir avantaja sahipler. İç tehdidin ayrıcalıklı bir pozisyonda (bir yöneticinin konuşlandırılmış güvenlik mekanizmaları hakkında bilgi sahibi olması ve potansiyel olarak onları kontrol etmek için erişim haklarına sahip olması gibi) bulunması durumunda avantaj daha büyüktür. Bununla birlikte, mevcut tecrübeler GIT'lerin altyapı hakkında önceden bilgi sahibi olmadan da algılamadan kaçınırken hedeflerine ulaşmayı başardıklarını göstermiştir.
- Her iki grup da sosyal mühendislik ve aldatma dahil olmak üzere hedeflerine ulaşmak için tüm olası saldırı yollarını araştırmak için önemli miktarda zaman harcamaya isteklidir. GIT grupları, önemli kaynaklara (finansal, teknik, istihbarat) erişimi olan yüksek vasıflı kişilerden oluşan ekiplere sahiptirler. Kötü niyetli iç tehditler, çoğunlukla yalnız çalışsalar da, Manning ve Snowden olaylarında olduğu gibi, teknik olarak iyi gelişmiş olabilmektedir.
- Her ikisi de nüfuz edilen altyapıya erişimi korumak ve verilerin kurum dışına taşınmasını mümkün olduğu kadar sürdürmek istemektedirler.

GIT ve iç tehdit arasında sayılan benzerlikleri kuran çalışma [94], GIT'lerin şantaj ya da rüşvetle iç tehditleri kendilerine hizmet etmek amacıyla zorlamaları sebebiyle kötü niyetli iç tehdit unsurlarının GIT'lerin bir alt grubu olarak görülmesi gerektiğini belirtmektedir.

3.4. Kritik Altyapılarda İç Tehdidin Yer Aldığı Siber Saldırılar

Siber savaş ve siber saldırılarda kritik altyapılar saldırganlar için öncelikli hedef konumunda yer almaktadır. Kritik altyapılarda meydana gelen birçok saldırı bulunsa da bu saldırılardan iç tehdit etkisi bulunanlar ele alınmıştır. Operasyonel teknolojiler ve endüstriyel kontrol sistemleri, bilgi ve iletişim teknolojilerine nazaran daha kapalı sistemler olduğu için saldırganlar tarafından iç tehdit aktörleri daha çok kullanılmaktadır. Bu yüzden de kritik altyapılarda meydana gelen saldırılarda iç tehdit etkisi bulunma ihtimali yüksektir.

3.4.1. Stuxnet

Stuxnet öncesinde de kritik altyapılarda birçok siber saldırı meydana gelmiştir. Fakat Stuxnet, karmaşıklığı, hedefe yönelik olması, kullandığı yöntemler ve verdiği zarar ile kritik altyapılar için bir dönüm noktası olmuştur. Belirtilen özellikleri nedeniyle de devlet destekli olduğu düşünülmektedir.

İlk olarak Haziran 2010'da Virusblokada isimli bir firma tarafından raporlanmıştır. Sonrasında yapılan incelemeler solucanın sofistike yapısını ortaya çıkarmıştır [95]. Stuxnet solucanı, sorunsuzca ilerleyen 3 aşamadan oluşmaktadır:

Öncelikle kendini çoğaltmak ve yayılmak için Microsoft Windows makineleri hedeflemektedir. Bu esnada daha sonradan çalıntı olduğu tespit edilen bir dijital sertifika ile beraber sisteme kendini güvenilir bir kaynaktan gibi göstermekte ve saldırı tespit sistemlerinden bu şekilde kaçınabilmektedir. Sistemler arasında çoğunlukla USB cihazı ile taşınmaktadır. Stuxnet solucanının şimdiye kadar 4 adet sıfırıncı gün açığı kullandığı tespit edilmiştir ki bu açıklıkların 2'si solucanın yerel ağ içinde kendi kendine yayılması amacıyla diğer ikisi bulaştığı sistemlerde hak yükseltme amacıyla kullanılmıştır. Tek bir sıfırıncı gün açığını keşfedebilmek bile hayli yüksek teknik donanım gerektirdiğinden 4 farklı sıfırıncı gün açığının bir arada bulunması güçlü kaynaklara işaret etmektedir.

Daha sonra ortamda bir SCADA yazılımı olan Siemens Step7'nin varlığını araştırmaktadır. Step7 İran nükleer santrallerinde de kullanılan bir endüstriyel kontrol sistemleri yazılımıdır [96].

Son olarak, sistem içerisindeki PLC'leri kontrol ederek istenmeyen biçimde çalışmasına neden olmaktadır. Stuxnet solucanının hedeflediği SCADA yazılımının ve PLC'lerin İran'ın Natanz'daki uranyum zenginleştirme tesisinde bulunması, dünya genelinde %60'ı aşan bir oranda İran'ı etkilemesi ve solucanın 2009 yılında ilk olarak İran'da ortaya çıkmış olması Stuxnet'in hedefinde İran'ın olduğunu kanıtlamaktadır [97].

Stuxnet nihayetinde PLC'lerin kontrolünü ele aldığında tesiste bulunan santrifüjlerin devre dışı kalmasını sağlayacak kadar hızlı dönmesine sebep olmuş, böylece birçok santrifüjü çalışmaz duruma getirerek İran nükleer programına büyük maddi zarar vermiştir.

Santrifüjlerin hızlı dönmesine sağlayan Stuxnet aynı zamanda HMI'ya da sürecin normal ilerlediği bilgisini göndererek kendini uzun süre gizlemiştir.

Stuxnet kullandığı yöntem ve sisteme sızma evreleri açısından bir GIT uygulamasıdır [91]. Ayrıca Stuxnet herhangi bir geniş alan ya da internet bağlantısı olmayan kapalı bir ağa sızdığından dolayı kapalı ağların güvenli olduğu algısını da yok etmiştir. Tüm bu özellikler yani Stuxnet'in bir GIT uygulaması olması ve kapalı bir ağa sızması akıllara iç tehdit varlığını getirmekedir. Nitekim, 2019'da yayınlanan bir haber bu düşünceyi doğrulamaktadır. Habere göre ABD ve İsrail İran'daki tesise sızmak için Hollandalılardan yardım istemiştir. Hollandalı istihbarat birimi AIVD ise aslen İranlı bir mühendis olan ve kendi görevlendirdiği bir kişiyi tesise sokmayı başarmıştır. Sonrasında bu kişi Natanz'daki sistemlerle ilgili kritik bilgileri temin etmiş ve Stuxnet zararlı yazılımını barındıran USB cihazını sistemde kullanmak suretiyle solucanın hedefine ulaşmasını sağlamıştır [98-99].

3.4.2. Maroochy Shire kanalizasyon döküntüsü

Mart 2000'de Avustralya Queensland'da yaşanan olay bir iç saldırganın kritik altyapılara yönelik gerçekleştirebileceği bir saldırının ne kadar basit ve etkili olabildiğini göstermesi açısından önemlidir. Olayda yaklaşık 1 milyon litre kanalizasyon parklara, nehirlere ve bir otelin bahçesine taşmıştır [100].

Hunter Watertech (HWT) firması, 1997-2000 yılları arasında Maroochy Shire atık su sistemindeki 142 pompa istasyonuna kendi ürünü olan PDS Compact 500 RTU/PLC cihazının monte edilmesi projesini yürütmektedir. Vitek Boden de HWT firmasında saha denetçisi olarak çalışmaktadır. Boden, yaşanan bir anlaşmazlık sonucu 3 Aralık 1999 tarihinde firmasından istifa etmiştir. Bu olaydan sonra Boden, Maroochy Shire Konseyi'ne yaptığı ilk iş başvurusunda, daha sonra başvurması cevabını almış, bir süre sonra tekrar başvurduktan sonra ise red cevabı almıştır.

Bu tarihten sonra atık su sisteminde kullanılan ve PDS Compact 500 cihazlarının bulunduğu SCADA sisteminde iletişim kaybı, pompaların kontrolünün kaybolması, yanlış alarmlar ve pompa istasyonlarının ayarlarında değişiklik gibi ilginç hatalar yaşamaya başlamıştır. Vitek Boden, sadece bir dizüstü bilgisayar ve radyo vericisi kullanarak 28 Şubat - 23 Nisan 2000 tarihleri arasında toplamda 142 adet atık su pompa istasyonunu ele geçirebilmek amacıyla

46 girişimde bulunmuştur. Boden, 23 Nisan 2000 tarihinde 19:30 - 21:00 saatleri arasında 4 numaralı pompa istasyonunu kimliğini kullanarak 4 farklı pompa istasyonunun alarmlarını kapatmış ve pompa istasyonlarının görevini yapmasını engellemiş, böylece 1 milyon litre (264 000 galon) atık suyun kamusal alana saçılmasına sebep olmuştur [101].

Boden bu olayı bir intikam olarak gerçekleştirmiştir. Sonucunda ise 2 yıl hapis cezası ile cezalandırılmıştır. Maroochy Shire olayı önceden sistemi ve işleyişini bilen bir iç saldırganın dış kaynaklı saldırganlara karşı ne tür üstünlükleri olduğunu göstermektedir.

3.4.3. Manning vakası

Chelsea Elizabeth Manning (önceki adıyla Bradley Edward Manning) ABD ordusunda istihbarat uzmanı bir askerdir. ABD ordusunun 2004-2009 yılları arasında Afganistan ve Irak Savaşlarında tutmuş olduğu kayıtlar ve raporların bulunduğu 750 000 gizli veya hassas bilgiyi sızdırdığından dolayı Mayıs 2010'da görev yaptığı Irak'ta tutuklanmıştır. Belirtilen bilgiler içerisinde dost ateşi ile hayatını kaybeden askerler, ABD'nin 2007 yılında Bağdat'ta birçok sivilin kaybına da yol açan hava saldırısı ve 2009 yılında Afganistan'da gerçekleştirdiği çarpıcı görüntülere sahip Garani hava saldırısı da bulunmaktadır. Manning'in sızdırdığı belgeler Nisan 2010 ile Nisan 2011 arasında Wikileaks web sitesi ile The Guardian, The New York Times ve Der Spiegel gazeteleri tarafından yayınlamıştır. Manning internet üzerinden sohbet ederken sızdırdığı bilgileri eski bir hacker olan Adrian Lamo'ya itiraf etmiştir. Lamo da Amerikalı yetkililere haber vererek Manning'in tutuklanmasını sağlamıştır.

Manning'in geçmişinde de bilgisayarlar ile yakından ilgili olduğu ve ABD ordusuna katıldığı dönemde cinsiyet kimliği ile ilgili sorunlar yaşadığı bilinmektedir. İstihbarat uzmanı olarak görev yaptığından gizli bilgilere erişimi bulunmaktadır. Manning, ölüm cezasını gerektiren düşmana yardım suçu dâhil 22 suçtan yargılanmıştır ve 14 Ağustos 2013 tarihinde 35 yıl hapse mahkûm edilmiştir [102].

3.4.4. Edward Snowden

Snowden, sistem yöneticisi olarak görev yapmış eski bir CIA çalışanıdır. 2009 yılında CIA'den istifa ettikten sonra Dell ve Booz Allen Hamilton firmalarında çalışmıştır. 2013

yılına kadar bu firmalar bünyesinde siber güvenlik analisti olarak NSA ve CIA'ya danışmanlık ve teknik destekte bulunmuştur. 5 Haziran 2013'te Hong Kong'ta bulunduğu sırada NSA'den sızdırdığı birçok gizli belgeyi ifşa etmiş ve belgeler The Guardian ve The Washington Post tarafından yayınlanmıştır. Gizli belgelerin ifşası ile PRISM internet izleme programını, Beş Göz olarak da bilinen UKUSA[4] anlaşmasını ve birçok ticari ve uluslararası ortaklığı açığa çıkarmıştır [103]. PRISM programı ise Facebook, Google, Microsoft, Yahoo, AOL, Paltalk, Skype ve Apple gibi sosyal medya ve teknoloji bilgilerinden topladığı bilgilerle kişilerin özel hayatlarına ulaşarak bilgilerini alabilmekte ve kişisel hesaplarına doğrudan erişebilmektedir [104].

Snowden ifşalar sırasında ayrıcalıklı kullanım hakkına sahiptir ve NSA verilerine sınırsız erişim hakkı bulunmaktadır [103].

Tanık olduğu olaylar vicdanını yaralamış, onu rahatsız etmiş ve bunun bir insan hakları ihlali olduğunu değerlendirmiştir. Bu yüzden de gördüklerini herkese duyurma kararını vermiştir. Snowden'ın bilgi sızdırmadaki en büyük motivasyonu halk adına yapılan fakat halka karşı olan eylemler konusunda halkı bilgilendirmektir. Amacı ise insanların kullandıkları teknolojiler konusunda bilinçlenmelerini sağlamaktır [104].

Snowden, Hong Kong'dan Rusya'ya geçmiş ve burada geçici sığınma altına alınmıştır. İfşa ettiği belgeler sonucu kişisel verilerin gizliliği ve ulusal güvenlik konularında birçok tartışma yaşanmıştır.

3.4.5. Avrupa Birliği diplomatik ağına sızılması

18 Aralık 2018 tarihli New York Times haberine göre Avrupa Birliği'nin diplomatik iletişim ağı 3 yıldan uzun süredir saldırganların elinde ve binlerce diplomatik mesaj elde edilmiştir [105]. Haberde, söz konusu bilgisayar korsanlığı tekniğinin Çin ordusununki ile benzerlik gösterdiği iddia edilmektedir. Olayın araştırılması maksadıyla haberin dayandırıldığı Area1 firmasına ait rapor incelenmiştir [106].

[4] Birleşik Krallık, ABD, Kanada, Avustralya ve Yeni Zelanda arasında elektronik istihbarat alanında iş birliği yapılmasını öngören çok taraflı bir anlaşma.

Raporda Çin Hükümet destekli Stratejik Destek Gücü (Strategic Support Force)'nün saldırıyı gerçekleştirdiği ve hedefinde uluslararası kuruluşlar, Dış İşleri Bakanlıkları, Ekonomi Bakanlıkları, ticari birliktelikler ve düşünce kuruluşlarının da bulunduğu 100'den fazla organizasyonun bulunduğu belirtilmiştir.

COREU adlı ağ 28 AB ülkesi, AB Konseyi ve AB Komisyonu gibi birimler arasında işlemektedir. Başarılı bir şekilde erişimin sağlanması oltalama yoluyla GKRY Dış İşleri Bakanlığı üzerinden olmuştur. Ağ yöneticisi ve kıdemli uzmanların kullanıcı adı ve parolaları ele geçirilmiş böylece ağa doğrudan giriş sağlanabilmiş ve ayrıcalıklı hesap yetkilerine sahip olunmuştur. Daha sonra PlugX zararlı yazılımı ile ağda kalıcı bir arka kapı oluşturulmuş ve binlerce diplomatik mesaj ve belge saldırganların bilgisayarına aktarılmıştır.

Raporun saldırıyla ilgili değindiği 3 temel nokta bulunmaktadır:

- Oltalama, saldırganların bilgisayar ağlarına sızmak için kullandığı baskın yöntem olma durumunu sürdürmektedir.
- Siber saldırılar çığ gibi büyüyen bir kartopundan çok montaj hattına benzemektedir. Yani saldırılar karmaşık olmaktan çok ısrarcı ve yaratıcı olarak tanımlanabilir. Siber saldırıların çok az bir kısmı mühendislik gerektirebilecek teknik bilgi ve donanıma ihtiyaç duymaktadır. Bunun yerine bariz olmayan hedefleri belirleyebilmek ve oltalamadaki yaratıcılık daha etkili bir yöntem olarak kullanılmaktadır.
- Siber aktörler, dijital güvenlik zincirindeki en zayıf halkayı bulmak için devamlı olarak hayal güçlerini kullanmaktadırlar. Çünkü, açık olan bir yan kapıdan girmek kilitli olan ön kapıyı kırmaya çalışmaktan çok daha kolaydır. Raporda bahsedilen açık yan kapı ise çoğu zaman insandır.

3.5. Kritik Altyapıların Siber Güvenliğinde İç Tehdidin Tespiti ve Önlenmesine Yönelik Yapılan Çalışmalar

İç tehdit öncelikle ABD olmak üzere birçok ülkeye, birçok devlet kurumuna ve özel kuruma zarar vermiştir. Bu yüzden sadece akademik literatürde değil özel siber güvenlik araştırmacılarınca ve çeşitli kurumlarca da üzerinde durulan bir konudur. Tehdidin iç kaynaklı olması, saldırganın ya da kuruma istemeden de olsa zarar veren kişinin kurumun bilgi sistemlerine hâlihazırda meşru giriş yetkisinin bulunması, genel olarak dış kaynaklı

tehditlere duyarlı birçok güvenlik sistemini etkisiz kılmaktadır. Ayrıca kötü niyetli bir iç saldırgan kurumdaki hassas kaynakları, kurumun işleyiş ve düzenini, alınan güvenlik önlemlerini - ve belki de bunların nasıl atlatılabileceğini - de bildiğinden dış kaynaklı saldırgana göre çok daha büyük bir risk faktörü konumundadır. Bu hususlar iç tehdidi araştırılması, incelenmesi ve tehdide karşı etkili tespit ve savunma yöntemleri geliştirilmesi gereken zorlu bir mücadele alanı haline getirmektedir.

Gao ve diğerleri [107] SCADA sistemi üzerine bir takım komut ve yanıt zerki saldırısı ve hizmet dışı bırakma saldırısı gerçekleştirmişlerdir. Kimlik doğrulama ve yetkilendirmenin olmadığı bu tarz sistemlerde, Maroochy Shire kanalizasyon döküntüsü olayında olduğu gibi, bir iç saldırganın bu tarz saldırıları gerçekleştirme ihtimali hayli yüksektir. Saldırılar ticari bir SCADA kontrol sistemine gerçekleştirilmiş ve saldırıyla ilgili trafik bilgileri SCADA ağ işlemleri veri kayıtçısı kullanılarak elde edilmiştir. Elde edilen trafik bilgisi yapay sinir ağları temelli bir saldırı tespit sistemini eğitmek ve geçerliliğini test etmek için normal olarak çalışan bir SCADA kontrol sisteminin trafik bilgisi ile birlikte kullanılmıştır. Saldırı tespit sistemi olarak Snort kullanılmıştır. 3 aşamalı yapay sinir ağları temelli saldırı tespit sistemi yetkisiz yanıtların tespiti için kontrol edilen sisteminin fiziksel bir takım özelliklerinden faydalanmaktadır. Sonuç olarak, saldırı tespit sistemi yetkisiz yanıtların tespiti için tatmin edici sonuçlar üretmiştir. Araştırmacılar gelecek çalışmalar için doğrulun artırılmasına yönelik girdi özelliklerinin geliştirilmesini ve yineleme saldırılarının (replay attack) tespitine yönelik özelliklerin tespit edilmesini önermişlerdir.

Kim [108] iç tehdit kaynaklı saldırıların tespitine yönelik olarak hâlihazırda kullanılan erişim kontrolü, kimlik yönetimi ya da kayıt tutma sistemleri gibi birçok farklı sistemin yerine bir donanım ve TCP tünellemesi yapabilen bir yazılım içeren bütünleşik bir sistem önermiştir. Bu sistemin sunuculardaki kritik bilgiyi korumak için sunucu ile kullanıcı arasında bir ağ geçidi gibi konumlandırılabileceğini belirtmiştir. Böylece sunucuya Telnet, FTP gibi yöntemlerle bağlanan kullanıcılar kontrol edilebilecek ve akıllı paket filtreleme yöntemleri ile hassas bilginin kaçırılması engellenebilmektedir. Ayrıca gerçekleştirilen tüm işlemler bütünleşik sistem vasıtasıyla kayıt altına alınabilecektir.

Formby ve diğerleri [109], özellikle enerji ve güç sistemlerinde kullanılan akıllı elektronik aygıtlar (intelligent electronic device, IED) için kullanılabilecek kimlik doğrulamalı giriş kontrolü ve diğer güvenlik izlemeleri sağlayabilecek bir fiziksel ağ katmanı önermiştir.

IED'ler üzerinde USB, seri port, RJ-45 ve Ethernet gibi portlar bulunmaktadır. Araştırmacılar kritik arayüz kilidi adını verdikleri cihaza saldırı tespit sistemi, USB takip sistemi ve antivirüs gibi çeşitli güvenlik araçları yükleyerek söz konusu IED'leri ve arayüzleri kontrol altına almayı hedeflemişlerdir. Yüklenen güvenlik araçları vasıtasıyla kullanıcılar ile IED'ler arasında bir ağ arayüzü oluşturan kritik arayüz kilitleri, kullanıcı kimlik doğrulama, güncelleme ve bakım, dosyaların güvenilirlik ve bütünlük kontrolü ile trafik izlemesi gibi güvenlik tedbirleri sağlayabilmektedir. Fakat kritik altyapı tesisleri, ağ ya da veri giriş arayüzü barındıran birçok cihazın bulunduğu büyük endüstriyel kontrol sistemleri için bahsedilen yöntemin ölçeklenebilir olmadığı değerlendirilmektedir.

Yılmaz ve diğerleri [110], yaptıkları çalışmada gerçek PLC cihazları kullanarak kurum içinden hizmet dışı bırakma saldırıları gerçekleştirmişler ve sonuçlarını analiz etmişlerdir. Hizmet dışı bırakma saldırıları bilgi ve iletişim teknolojilerine nazaran zaman açısından çok daha hassas olan endüstriyel kontrol sistemleri açısından daha yıkıcıdır. Saldırı sonuçlarının analizinde EKS'ye ayrıcalıklı erişim yetkisine sahip kullanıcıların mutlaka izlenmesi ve kontrol altında tutulması önerilmiştir.

Mylrea ve diğerleri [111], iç tehdit ve karmaşık siber-fiziksel tehditlere karşı bir İç Tehdit Siber Güvenlik Çerçevesi web aracı önermişlerdir. Araç, kurumların iç tehdit ve zafiyetlerini tanımlamasına, korunmasına, tespit edebilmesine, karşı koyabilmesine ve kurtarılmasına yardımcı olabilecek 30 en iyi önlemi içermektedir. Çalışma, 2 kullanım senaryosu vasıtasıyla bu aracın etkinliğini ve geçerliliğini test etmektedir. Web aracı kontrol listeleri ve risk değerlendirmeleri kullanarak kurumlar için kapsamlı bir rapor sunabilmekte ve sonucunda kurumsal siber güvenlik açısından geliştirilmesi gereken yönleri ortaya koyabilmektedir.

Lamba ve diğerleri [112], iç tehditleri belirleyebilmek için kullanıcıların yazılımlarda bıraktığı izlerden faydalanarak oluşturulacak grafik modelinden faydalanılabileceğini belirtmişlerdir. Kurumun yazılım sistemlerinde gezinen kullanıcılar bilindiği gibi kendilerine has izler bırakmaktadırlar. Çalışma, bu izlerden oluşan aktivite ve kayıtların davranışsal yollara dönüştürülebileceğini böylece bir kümeleme algoritması kullanarak bu davranışların hangilerinin anormal olarak belirlenebileceğini ifade etmiştir. Fakat, sistemdeki normal olmayan davranışlar bu şekilde belirlenebilecek olsa da tehdit olarak

nitelendirilebilmesi için organizasyon ve yazılım mimarisi bakımından ilave özelliklere ihtiyaç bulunmaktadır.

Bir diğer çalışma [113], iç tehditten korunmak amacıyla sosyal (insanlar ve kurumu içeren), mantıksal (teknik) ve fiziksel seviyeleri bulunan üç-katmanlı bir güvenlik mimarisi önermiştir. Çalışmaya göre iç tehditleri önlemek, tespit etmek ve gerektiğinde kurtarma yapabilmek için belirtilen seviyelerin tamamının kapsandığı bütüncül bir mimari gerekmektedir. Araştırmacı, bu güvenlik mimarisinin finansal sektörleri ve kritik altyapılarda da geniş kullanım alanı bulabileceğini değerlendirmektedir.

Başka bir çalışma [114], iç tehdit sorunu ile mücadele etmek amacıyla yeni bir kimlik doğrulama faktörü olarak "nerede olduğun" özelliğini kullanmayı önermiştir. Bilindiği üzere kullanıcıların kimlik doğrulaması "neye sahip olduğun" (kimlik, giriş kartı, sertifika vb.), "neyi bildiğin" (parola, kişisel bilgiler vb.) ve "ne olduğun" (parmak izi, retina gibi biyolojik özellikler) olmak üzere 3 temel faktör kullanılarak yapılmaktadır. Çalışma, kullanıcıların bileklik benzeri bir etiketi sürekli yanlarında bulundurmasını gerektiren Gerçek Zamanlı Konumlandırma Sistemi kullanılmasını önermektedir. Bu sayede anlık konum bilgisinin gücünden faydalanılarak diğer 3 faktörün barındırdığı zafiyetlerin önüne geçilebileceği böylece uygun bir iç tehdit önlem sistemi oluşturulabileceğini öne sürmektedir.

Nasr ve Varjani [115], yaptıkları çalışmada kritik altyapılarda iç kaynaklı saldırıların tespit edilmesi amacıyla SCADA alarmlarından faydalanılmasını önermiştir. SCADA sisteminde meydana gelen alarmlar incelenerek sistemin normal davranışını tespit eden ve sonrasında bu normal davranışın dışına çıkan davranışları zararlı olarak adlandıran yeni bir istatistiksel anomali tespit sistemi ortaya koymuşlardır. Çalışma sistemin normal davranışını belirlemek için operatörlerin izlenmesini şart koşmamış bunun yerine bazı eşik değerler belirlenebileceğini, bu eşik değerlerin dışında üretilen alarmların da anomali olarak değerlendirilebileceğini belirtmiştir. Önerilen yöntem birkaç alt istasyon barındıran bir SCADA simülasyonunda 2 farklı iç tehdit saldırısı ile değerlendirilmiş ve anomalilerin tespit edilebildiği gözlemlenmiştir.

Virvilis ve diğerleri yaptığı çalışmada [94] ise özellikle kritik altyapılara yönelen GIT ve iç tehditlerin ortak karakteristik özelliklerini göz önünde bulundurarak her iki gruba karşı da kullanılabilecek aldatma tekniklerinden faydalanılmasını önermiştir. Kurumun iç ve dış

kaynaklarını korumayı sağlayabilecek bu teknikler çok yönlü saldırıların erkenden tespit edilmesini sağlayabilmektedir. Çalışma, ayrı ayrı saldırı hazırlığı (bilgi toplama) ve sömürme/veri sızıntısı aşamalarında kullanılabilecek birçok aldatma yöntemi belirlemiştir.

Ghafir ve diğerleri [116] çalışmalarında özellikle kötü niyetli olmayan iç tehditleri hedef alan güvenlik farkındalığı eğitimini önermişlerdir. Bilindiği gibi, kötü niyetli olmayan iç tehditler hatalı ve dikkatsiz kullanıcılardan oluşmaktadır. Meydana gelebilecek saldırılar ise oltalama, yemleme ve başkasının yerine geçme gibi sosyal mühendislik yöntemlerinden faydalanabilmektedir. Çalışma, bu yöntemlere karşı kullanıcıların eğitilmesini sağlayan içerik tabanlı bir masaüstü uygulaması sunmaktadır. Uygulama 4 farklı durumda (Facebook sitesi açıldığında, yüklü e-posta uygulaması kullanıldığında, .exe uzantılı bir dosya çalıştırıldığında ya da 5 dakika boyunca bilgisayar kullanılmadığında) ortaya çıkan pop-uplar üretmektedir. Bu diyalog kutuları ve pop-uplar çeşitli modüllerle ilgili (parola güvenliği, bilinmeyen bağlantılara tıklamama, kaynağı bilinmeyen e-postalardaki ekleri açmama gibi) uyarılar üretmektedir. Uyarıya verilen tepkiye göre veri tabanında bir kullanıcı profili oluşmakta ve sistem yöneticileri tarafından kullanıcılar bu şekilde eğitilmekte ve takip edilmektedir.

İç tehdidin kullanabileceği en kolay ve en etkili yol olarak değerlendirdikleri USB bellek için yeni bir yöntem öneren bir diğer çalışma [117], bu amaçla FPGA kartından yararlanmıştır. ZedBoard isimli bir kart kullanan araştırmacılar, kartın mantıksal bölümünde USB iletişimini yakalayan bir yazılım kullanarak zararlı davranışlarını tespit etmeyi ve engellemeyi hedeflemişlerdir. Elde edilen paketler ile USB cihazın üretici numarası, cihaz numarası, USB adresleri ve istemci bilgileri elde edilebilmektedir. Bu sayede sistem yöneticisi tarafından cihaz ya da üretici bazlı olarak USB cihazlarına izin verilebilmekte ya da engellenebilmektedir. İşletim sistemi bağımsız olarak çalışan sistem FPGA donanımına ihtiyaç duymaktadır.

Hareketli hedef koruması (Moving Target Defense, MTD) isimli yeni bir güvenlik konseptini içeren bir başka çalışma [118] iç tehditle mücadelede proaktif bir tutum takınmayı önermiştir. Hareketli hedef koruması, birçok farklı siber saldırıdan korunmak için bilgi teknolojileri altyapısının dinamik bir biçimde şekil değiştirmesi olarak açıklanabilir. Böylece saldırganın muhtemel atak yüzeyi genişleyecek dolayısıyla hedef analiz maliyeti yükselecektir. MTD konseptine bağlı olarak geliştirilen dinamik makine mutasyonu

(Dynamic Host Mutation, DHM) mimarisinde 3 temel bileşen bulunmaktadır. Bunlar; ağ adresi mutasyonu, parmak izi mutasyonu ve tuzak düğüm noktası oluşturmadır. Ağ adresi mutasyonu ile ağdaki makinaların ve servislerin IP adresi, port numarası, bulundukları platform ve yazılım bilgisi gibi temel bilgileri değişime uğramaktadır. Parmak izi mutasyonu ile saldırganın iç ağdaki kritik sunuculara erişmesini engellemek amaçlanmaktadır. Bu maksatla ağda sahte trafik yaratılarak iç saldırganın trafiği analiz ederek sunuculara ulaşmasının önüne geçilmesi hedeflenmektedir. Tuzak düğüm noktaları ise saldırganın - iç ağda olsa bile - kritik sunucuyu ağ taraması sonucu bulabilmesinin engellenmesi amacıyla kullanılmaktadır. Bu bilgiler bir kimlik doğrulama mekanizmasıyla meşru istemciler arasında paylaşılmaktadır. Böylece kurum içinden başka bir kişinin hesabını ele geçirmiş olan bir maskeli iç saldırgan ağ taraması, trafik incelemesi gibi yöntemlerle ya da cihazların parmak izi bilgilerini kullanarak kritik sunucuya ulaşamayacaktır.

3.6. İç Tehdide Karşı Alınabilecek Önlemler

Kurum içinden gelen tehditlere karşı alınabilecek önlemler sosyal, teknik ve sosyo-teknik önlemlerin bütününden oluşmaktadır. Kaynağı doğrudan insan olan ve kuruma küskün kişiler ile intikam almak isteyen eski çalışanlar gibi grupları barındıran iç tehdidi sadece teknik önlemlerle engellemek mümkün değildir. Kurumsal idare başta olmak üzere insan kaynakları, hukuk müşavirliği ve fiziksel güvenlik ile ilgili birimlerin ortak çaba göstermesi gerekmektedir. Bununla beraber literatürde yapılan çalışmalar, rafta hazır ürünler ve ticari hazır yazılımlar da iç tehdide karşı birçok özel araç içermektedir.

Çalışmanın bu bölümünde iç tehdidin azaltılmasına yönelik hem tüm önlemleri içeren bir rehber sunulmuş hem de güncel iç tehdit algılama, önleme ve müdahale araçlarından bahsedilmiştir.

3.6.1. İç tehdidi azaltma rehberi

Uzun yıllardır ABD Gizli Servisi ile ortak bir şekilde iç tehditle alakalı çalışmalar yürüten Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü 1500 iç tehdit vakasını inceleyerek bilindiği kadarıyla bu alandaki en kapsamlı ve uzun soluklu çalışmayı yürütmektedir. Bu yüzden ulaştığı sonuçlar ve önerdiği yöntemler açısından literatürde

önemli bir yere sahiptir. Bu kapsamda 2018'in sonunda 6. baskısını yayınlamış oldukları rehber [13] iç tehdidin azaltılmasına yönelik kapsayıcı bir yol gösterici konumundadır.

Rehber, kurumun aşağıda belirtilen birimleri için iç tehdidin azaltılması maksadıyla sunulmuş bilgiler ve öneriler içermektedir:

- İnsan Kaynakları
- Hukuk Müşavirliği
- Fiziksel Güvenlik
- Veri Sahipleri
- Bilgi Teknolojileri
- Yazılım Mühendisliği
- Yönetim
- Bilgi Güvenliği

Rehberdeki öneriler karar vericilerin beraber çalışarak iç tehditleri tespit etmesi, engellemesi ve müdahale etmesi amacıyla tasarlanmıştır. Bu rehberde [13] yer alan 21 en iyi uygulama, açıklamaları ile sunulmuş ve her uygulamayla ilgili kurumsal birimler Çizelge 3.1'de gösterilmiştir.

Kritik varlıklar tanımlanmalı ve korunmalıdır

Bir iç tehdit programının en temel işlevi kurumdaki varlıkların tanımlanmasıdır. Kritik varlıklar, yok edildiğinde, değiştirildiğinde ya da bozulduğunda kurumun ana görev ve iş fonksiyonları üzerinde ciddi olumsuz etkiler yaratacak varlıklardır. Kritik varlıklar, fiziksel ya da mantıksal olabilirler ve tesisler, sistemler, ekipman, personel ve teknolojiyi içerebilirler. Kritik varlıkların sık sık göz ardı edilen bir tarafı ise fikri mülkiyettir. Fikri mülkiyet; kuruma ait yazılım, müşteri bilgisi, şemalar ve iç üretim süreçlerini içerebilmektedir.

Kritik varlıklar tanımlandıktan ve önceliklendirildikten sonra, kuruluş kritik sistemler veya verilerle en sık etkileşimde bulunan veya diğer personel için tehdit oluşturabilecek yüksek riskli kullanıcıları tanımlamalıdır. Bu, kurumun potansiyel içerideki tehditleri başarıyla tespit etmek için en iyi yaklaşımları belirlemesine yardımcı olacaktır.

Çizelge 3.1. İç tehdidin azaltılmasına yönelik en iyi uygulamalar [13]

S.No.	Uygulama	İnsan Kaynakları	Hukuk Müşavirliği	Fiziksel Güvenlik	Veri Sahibi	BT	Yazılım Mühendisi
1	Kritik varlıklar tanımlanmalı ve korunmalıdır.	√	√	√	√	√	√
2	Resmi bir iç tehdit programı geliştirilmelidir.	√	√	√	√	√	√
3	Güvenlik politikası ve dokümanları açıkça belirtilmeli ve tutarlı biçimde uygulanmalıdır.	√	√	√		√	
4	Şüpheli ve yıkıcı davranışlar işe alımdan itibaren izlenmeli ve gerektiğinde yaptırım uygulanmalıdır.	√	√	√	√	√	√
5	Çalışma ortamındaki olumsuz durumlar öngörülmeli ve yönetilmelidir.	√	√	√	√	√	
6	Risk değerlendirmesinde içeriden ve iş ortaklarından gelebilecek tehditler göz önünde bulundurulmalıdır.	√	√	√	√	√	
7	Sosyal medya paylaşımları konusunda ihtiyatlı olunmalıdır.	√	√	√	√	√	
8	Yapısal yönetim ve iç kaynaklı stresin ve hataların azaltılmasına yönelik görevler.	√	√	√	√	√	√
9	Kötü niyetli ve kasıtsız iç tehdit farkındalığı düzenli olarak icra edilen güvenlik eğitimine dâhil edilmeli ve tüm çalışanların katılımı sağlanmalıdır.	√	√	√	√	√	√
10	Parola ve hesap yönetimi politikaları ve yöntemleri sıkı biçimde uygulanmalıdır.	√	√			√	
11	Ayrıcalıklı hesaplar üzerinde sıkı erişim kontrolü ve izleme politikaları uygulanmalıdır.	√	√			√	

Çizelge 3.1. İç tehdidin azaltılmasına yönelik en iyi uygulamalar [13] (devam)

S.No.	Uygulama	İnsan Kaynakları	Hukuk Müşavirliği	Fiziksel Güvenlik	Veri Sahibi	BT	Yazılım Mühendisi
12	Çalışanları eylemlerini izlemeye yönelik çözümler hayata geçirilmeli ve birçok veri kaynağından gelen bilgiler ilişkilendirilmelidir.	√	√	√	√	√	√
13	Mobil cihazlar dâhil tüm uç noktalardan gelen uzak bağlantılar izlenmeli ve kontrol edilmelidir.				√	√	
14	Hem ağ hem de çalışanlar için bir normal davranış referans değerleri elde edilmelidir.				√	√	
15	Görevlerin ayrılığı ve en az ayrıcalık ilkeleri uygulanmalıdır.	√	√	√	√	√	√
16	Bulut hizmetleri için özellikle erişim kısıtları ve izleme yeteneklerinin yer aldığı güvenlik sözleşmeleri tanımlanmalıdır.		√	√	√	√	
17	Sistem değişikliği kontrolleri kurumsallaştırılmalıdır.				√	√	√
18	Güvenli yedekleme ve kurtarma süreçleri yürütülmelidir.				√	√	
19	Yetkisiz veri sızıntılarına karşı "kapılar" kapatılmalıdır.			√	√	√	
20	İşten çıkarmaya yönelik kapsayıcı bir süreç geliştirilmelidir.	√	√	√	√	√	
21	İş gücünü kurumla birlikte hareket ettirebilmek için olumlu teşvikler benimsenmelidir.	√	√	√	√	√	√

Resmi bir iç tehdit programı geliştirilmelidir

Resmi bir iç tehdit programı, iç tehdit sorununu ele almak için belirlenmiş bir kaynak sağlamaktadır. Kurumların iş gücüne duydukları güven, yasa dışı faaliyetlerini gizlemek için genellikle belirli yöntemler kullanan kötü niyetli iç saldırganlara karşı kurumları savunmasız

bırakabilmektedir. Kurumlar yalnızca özelleşmiş ve orantılı uygulamalar yaparak, kurum içindekilerin yarattığı kendine has tehdidi etkili bir şekilde tespit edebilmekte, önleyebilmekte ve bunlara müdahalede bulunabilmektedirler. Kötü niyetli olsun ya da olmasın iç kaynaklı olayları azaltmak amacıyla bir süreç geliştirmek için en iyi zaman, olayın ortaya çıkmasından önce değil, olayın meydana gelmesinden öncesidir. Bir olay meydana geldiğinde, önceki olayların incelemesinden sonra ortaya çıkan sonuçlara göre süreç uygun şekilde değiştirilebilmektedir.

Güvenlik politikası ve dokümanları açıkça belirtilmeli ve tutarlı biçimde uygulanmalıdır

Tüm kurumsal politika ve prosedürlere dair tutarlı ve net bir mesaj, çalışanların yanlışlıkla kuruma zarar verme veya bir haksızlık algısı nedeniyle kuruluşa veya çalışanlarına saldırma olasılığını azaltmaktadır. Kurumlar, politikaların adil olmasını ve herhangi bir ihlal için cezalandırılmanın orantısız olmamasını sağlamalıdır.

Şüpheli ve yıkıcı davranışlar işe alımdan itibaren izlenmeli ve gerektiğinde yaptırım uygulanmalıdır

Kurumlar, kötü niyetli içeriden kaynaklanan faaliyet riskini azaltmak için proaktif olarak şüpheli veya rahatsız edici çalışanlarla ilgilenmelidir. Bir kurumun iç tehditleri azaltma yaklaşımı işe alım sürecinde başlamalıdır. Potansiyel çalışanlar hakkındaki geçmiş kontroller, önceki ceza mahkûmiyetlerini ortaya çıkarmalı, kimlik bilgilerini ve geçmiş istihdamı doğrulamalı ve önceki işverenlerinden iş yeri sorunları ile ilgilenme konusundaki yeterliliği ve yaklaşımı konusunda elde edilen bilgileri içermelidir. Kurumlar, bir geçmiş kontrol politikası oluştururken yasal gereklilikleri (örneğin, adaya bildirim ve adayın rızası) göz önünde bulundurmalıdır.

Çalışma ortamındaki olumsuz durumlar öngörülmeli ve yönetilmelidir

Çalışan sorunlarıyla başa çıkabilmek için açıkça tanımlanmış ve iletilmiş kurumsal düzenlemeler, politikaların tutarlı bir şekilde uygulanmasını kolaylaştırmakta ve olumsuz işyeri sorunları ortaya çıktığında riski azaltmaktadır.

Kurumlar, politikalarını ve uygulamalarını yeni çalışanlara ilk günlerinde iletmelidir. Bu tür

politikalar ve uygulamalar işyeri davranışları, kıyafet kuralları, kullanım politikaları, çalışma saatleri, kariyer gelişimi, uyuşmazlık çözümü ve diğer işyeri konularını içermektedir. Bu tür politikaların tek başına varlığı yeterli değildir. Yeni çalışanlar ve deneyimli çalışanlar, bu tür politikaların ve bunların ihlal edilmesinin sonuçlarının farkında olmalıdırlar. Kurumlar uyumlu bir çalışma ortamı sağlamak için politikalarını sürekli olarak uygulamak zorundadır. Politikaların tutarsız bir şekilde uygulanması, işyerinde düşmanlığa yol açmaktadır. Analiz edilen iç tehdit vakalarının çoğunda, kurum içindeki tutarsız uygulama veya algılanan adaletsizlikler küskünlük ve kırgınlıklara neden olmuştur. Çalışanlar genellikle gözde elemanların kuralların üstünde olduğunu ve özel muamele gördüklerini hissetmektedirler. Bu durumun yarattığı hoşnutsuzluğun, iç tehditlerin BT'yi sabote etmesine veya bilgi çalmasına neden olduğu görülmüştür.

Risk değerlendirmesinde içeriden ve iş ortaklarından gelebilecek tehditler göz önünde bulundurulmalıdır

Kurumlar kritik varlıklarını korumak amacıyla, yetkili güvenilir iş ortakları da dahil olmak üzere, içeriden ve dışarıdan gelen tehditlere karşı kapsamlı ve risk bazlı bir güvenlik stratejisi geliştirmelidir. Sadece büyük paydaşlar değil kurumun tüm çalışanları, sistemin ele geçirilmesinin, kritik verilerin kaybedilmesinin veya ifşa olmasının risklerini bilmelidir. İşyerindeki şiddet olaylarının etkisini hem fiziksel olarak hem de yasal olarak anlamalıdır.

Sosyal medya paylaşımları konusunda ihtiyatlı olunmalıdır

Sosyal medya sitelerini kullanan iç tehditler kasıtlı ya da kasıtsız olarak kurumun kritik varlıklarını tehlikeye atabilirler. Kurumlar çalışanların, iş ortaklarının ve yüklenicilerin sosyal medyayı nasıl kullanmaları gerektiği hakkında eğitim, politika ve prosedürler belirlemelidir.

Sosyal medya siteleri, insanların kendileriyle ilgili bilgileri başkalarıyla kolayca paylaşmalarını sağlar. Bir kullanıcının sosyal medya profilinden veya herhangi bir popüler arama motorunu kullanarak yapılan bir aramadan doğum günleri ve aile üyelerinden ticari kuruluşlara ve hobilere kadar her şey hakkında bilgi edinilebilir. Bu bilgi, sosyal medyayı kullanan çalışanları, sosyal mühendislik için muhtemel hedef durumuna getirmektedir.

Facebook ve LinkedIn gibi sosyal medya siteleri, belirli bir şirkette kimin çalıştığını belirlemek için kullanılabilmektedir. Kötü niyetli kullanıcılar bu bilgileri bir kuruluşa karşı hedefli e-posta saldırısı gerçekleştirmek için kullanabilmektedir.

Bu siteler ayrıca, bir kuruluş içinde kimin iç kaynaklı saldırıya karşı daha hassas veya iç kaynaklı bir saldırıya katılmaya daha istekli olabileceğini belirlemek için de kullanılabilmektedir. Örneğin, bir sosyal paylaşım sitesindeki bir çalışanın, işi veya şirketi hakkında olumsuz yorumlar yayınlaması, saldırganlar tarafından çalışanın hoşnutsuz olduğu dolayısıyla kötü niyetli bir iç tehdit olmaya aday olduğu şeklinde yorumlanabilmektedir.

Yapısal yönetim ve iç kaynaklı stresin ve hataların azaltılmasına yönelik görevler

Kurumlar, iş gücünün psikolojisini ve liderlerinin onlara getirdiği talepleri anlamalıdır. Bunlar anlaşıldığında, kurumun olumlu sonuçlara elverişli bir çalışma ortamı yaratması gerekmektedir.

İnsan davranışı, özellikle yüksek stresli ortamlarda birden fazla görevi tamamlamak için acele edenler tarafından yapılacak hatalar için elverişlidir. Hataların ötesinde, işyerinde yüksek düzeyde stres olması kötü niyetli faaliyet için daha fazla potansiyel yaratmaktadır. Çalışanlar işi bitirmek için acele ettiğinde daha fazla hata yapmakta, endişeleri göz önünde bulundurulmamış gibi hisstmekte ve potansiyel olarak yönetim ve organizasyonlarına yönelik olumsuz tutumlar geliştirmektedirler. Kötü niyetli ve kasıtsız iç tehdit olasılığını azaltmak için kurumlar, çalışanların stres düzeyini azaltabilecek araçları göz önünde bulundurmalıdır.

Kötü niyetli ve kasıtsız iç tehdit farkındalığı düzenli olarak icra edilen güvenlik eğitimine dahil edilmeli ve tüm çalışanların katılımı sağlanmalıdır

Kuruluştan geniş bir anlayış ve katılım olmadan uygulanan teknik veya yönetimsel kontroller uzun ömürlü olmamaktadır. Kötü niyetli ve kasıtsız iç tehdit farkındalığını içeren periyodik güvenlik eğitimi, organizasyonda istikrarlı bir güvenlik kültürünü desteklemektedir.

Parola ve hesap yönetimi politikaları ve yöntemleri sıkı biçimde uygulanmalıdır

Katı şifre ve hesap yönetimi politikaları ve uygulamaları, kötü niyetli iç tehditlerin otomatik ve otomatik olmayan kontrol mekanizmalarını atlatmak için kurumun kullanıcı hesaplarını ele geçirmesini engelleyebilmektedir.

Bir kuruluş içeriden gelen tehditlere karşı ne kadar uyanık olursa olsun, kuruluşun kullanıcı hesapları ele geçirildiğinde, iç tehditlere saldırı önleme mekanizmalarını aşma fırsatı doğmaktadır. Kullanıcı hesabı ve şifre yönetimi politikaları ve uygulamaları, içeriden birinin kurumun sistemlerini yasa dışı amaçlarla kullanılabilme yeteneğine engel olmak için kritik öneme sahiptir. Uygun bilgisayar hesabı yönetimi ile birlikte iyi ayarlanmış erişim kontrolü, kuruluşun tüm kritik elektronik varlıklarına erişimin bireysel çalışanlara atfedilmesini sağlamaktadır.

Ayrıcalıklı hesaplar üzerinde sıkı erişim kontrolü ve izleme politikaları uygulanmalıdır

Sistem yöneticileri ve teknik veya ayrıcalıklı kullanıcılar, kötü niyetli faaliyetlerde bulunma ve gizlenme konusunda teknik yetenek, erişim ve gözetim ile ilgili yeteneklere sahiptir.

CERT Ulusal İç Tehdit Merkezi'nin araştırmasına göre, sabotaj yapan iç saldırganların büyük bir kısmı ve gizli veya özel bilgi çalanların yarısından fazlasının mağdur kurumlarda teknik görevlerde bulunduğu tespit edilmiştir.

Çalışanların eylemlerini izlemeye yönelik çözümler hayata geçirilmeli ve birçok veri kaynağından gelen bilgiler ilişkilendirilmelidir

Etkili iç tehdit programları, kurumdaki birçok farklı kaynaktan bilgi toplamakta ve analiz etmektedir. Fakat, tüm ağ etkinliklerini günlüğe kaydetmek, bir kurumu kötü niyetli iç kaynaklı faaliyetlerden korumak için yeterli değildir. İçeriden gelen tehditleri analiz etmek için kullanılan veri kaynaklarının sayısı arttıkça, bir kurumun iç tehditler hakkında daha fazla ilgili uyarı üretme ve bilinçli kararlar alma yeteneği de artmaktadır. Toplanması, bir araya getirilmesi, ilişkilendirilmesi ve analiz edilmesi gereken veri büyüdükçe, farklı kaynaklardan gelen verilerin potansiyel iç tehdit faaliyetlerin bir göstergesi olan alarmlara dönüştürülmesini sağlayan araçlara olan ihtiyaç artmaktadır. Çalışanların eylemlerini

izleyen çözümler, risk bazlı bir yaklaşım kullanılarak uygulanmalı ve önce kurumun kritik varlıklarına odaklanmalıdır.

Mobil cihazlar dahil tüm uç noktalardan gelen uzak bağlantılar izlenmeli ve kontrol edilmelidir

Uzaktan erişim, iç saldırganların daha az risk alarak saldırması için cazip bir fırsat sunar. Kuruluşlar, çalışanların temelde bir veri bağlantısı olan herhangi bir yerden çalışmasına olanak tanıyan mobil bir iş gücüne doğru ilerlemektedir. Bu nedenle daha fazla kullanıcı şirket bilgi sistemlerine uzaktan erişmek için akıllı telefonlar ve tablet bilgisayarlar gibi ek teknolojileri kullanmaktadırlar. Kurumlar, çalışanları tarafından kullanılan uzaktan erişim teknolojilerinin ve bu teknolojilerin kurumsal sistemler ile verileri hangi potansiyel tehditlere maruz bıraktığının farkında olmalıdır.

İç saldırganlar sıklıkla kurumun sağladığı meşru erişimi kullanarak, çalıştıkları sırada veya işten çıkarıldıktan sonra uzaktan saldırı gerçekleştirirler. Uzaktan erişim çalışan verimliliğini büyük ölçüde artırabilirken, kritik verilere, süreçlere veya bilgi sistemlerine uzaktan erişim yetkisi dikkatle verilmelidir. İç saldırganlar kötü niyetli faaliyetlerin evden yapılmasının daha kolay olduğunu kabul etmektedirler çünkü iş arkadaşlarının kötü niyetli eylemlerini gözlemlemesi endişesi ortadan kalkmaktadır.

Hem ağ hem de çalışanlar için bir normal davranış referans değerleri elde edilmelidir

Bir kuruluş kritik varlıklarıyla ilgili bilgi bakımından zengin veri akışlarını tanımlayıp bir araya getirdikten sonra, veriler üzerinde analiz yapmaya başlayabilmektedir.

Her kuruluş, bant genişliği kullanımı, kullanım düzenleri ve protokoller gibi özellikler açısından benzersiz bir ağ topolojisine sahiptir ki bu özellikler güvenlik olayları ve anormallikleri izlerken kullanılabilmektedir. Aynı şekilde, kuruluşlardaki tüm çalışanların tipik çalışma saatleri, kaynak kullanım kalıpları ve kaynak erişim kalıpları da dâhil olmak üzere kendi benzersiz özellikleri vardır. Normal ağ ve çalışan davranışlarından sapmalar, içeriden gelen tehditler de dâhil olmak üzere olası güvenlik olaylarını işaret edebilmektedir. Normal davranıştan sapmaları tespit edebilmek için kuruluşların önce normal ağ ve çalışan davranışının karakteristik özelliklerini belirlemesi gerekmektedir.

Görevlerin ayrılığı ve en az ayrıcalık ilkeleri uygulanmalıdır

Görevlerin ayrılığı, bir çalışanın başkaları ile işbirliği yapmadan bilgi hırsızlığı, dolandırıcılık veya sabotaj gerçekleştirme olasılığını sınırlandırmak için işlevleri birçok kişi arasında bölmeyi gerektirir. Birçok kuruluş, "iki kişi kuralı"nı uygular. Bu kural, bir görevin başarılı bir şekilde yapılabilmesi için iki kişinin bir arada bulunması gerekliliğidir. Kurumlar, görevlerin ayrılmasını sağlamak için teknik veya teknik olmayan kontrolleri kullanabilirler. Yüksek meblağlı çeklerin imzalanması için iki banka yetkilisinin gerekmesi örnek olarak verilebilir. Çalışanların başka bir çalışanla iş birliği yapmaları gerekiyorsa kötü niyetli eylemlerde bulunma olasılığının daha düşük olduğu ortaya konmuştur.

Bulut hizmetleri için özellikle erişim kısıtları ve izleme yeteneklerinin yer aldığı güvenlik sözleşmeleri tanımlanmalıdır

Kuruluşlar, bulut servis sağlayıcıları ile yapılan anlaşmalarda veri erişim kontrolü ve izlenmesi ile ilgili hükümler bulundurmalıdırlar.

Bulut bilişim, kuruluşların maliyetleri düşük tutarken çeşitli altyapı cihazlarına ve hizmetlerine hızlı bir şekilde ayak uydurmalarını sağlar. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) bulut bilişimi "yapılandırılabilir bilgi işlem kaynaklarından (ör. ağlar, sunucular, depolama, uygulamalar) oluşan ortak bir havuza her yerden, kullanışlı, isteğe bağlı erişime olanak sağlayan bir modeldir. Erişim sağlanan kaynaklar asgari yönetim çabası gerektirir ve asgari servis sağlayıcı etkileşimi ile hızlı bir şekilde yayınlanabilirler" şeklinde tanımlamaktadır [119].

Ponemon Enstitüsü tarafından yapılan bir araştırmada, "bulut sağlayıcıların çoğunluğu, bulutun güvenliğini sağlamanın kendilerinin değil müşterilerin sorumluluğu olduğuna inanmaktadır. Ayrıca, sistemlerinin ve uygulamalarının, müşterilere sunulmadan önce güvenlik tehditleri açısından her zaman değerlendirilmediğini" belirtmektedirler [120]. Kuruluşlar, bulut hizmet sağlayıcılarının kuruluşun bilgilerinin güvenliğini sağlama konusunda sorumluluk aldığı kabulüne dayanmamalıdırlar.

Sistem değişikliği kontrolleri kurumsallaştırılmalıdır

Kurumlar, arka kapılar, klavye kayıt cihazları, mantık bombaları ve diğer kötü niyetli kod veya programların yerleştirilmesini önlemek için sistem ve uygulamalardaki değişiklikleri kontrol etmelidir. Değişim kontrolleri projenin tamamında uygulanmalı ve zaman içinde ve projelerin tüm aşamalarında devam etmelidir.

Değişim kontrolleri, bilgisayar ve ağ sistemlerinde yapılan tüm değişikliklerin doğruluğunu, bütünlüğünü, yetkilendirmesini ve belgelenmesini sağlayan güvenlik denetimleridir. Mağdur kurumların sistemlerinde yapılmış yetkisiz değişikliklere dayanan çeşitli iç kaynaklı sızmalar, daha güçlü değişim kontrollerine olan ihtiyacı ortaya koymaktadır. Daha güçlü değişiklik kontrolleri geliştirmek için kuruluşların temel yazılım ve donanım yapılandırmalarını tanımlamaları gerekmektedir. Farklı kullanıcıların (örneğin, muhasebeci, yönetici, programcı ve resepsiyonist) farklı bilgi işlem ve bilgi ihtiyaçları göz önüne alındığında, bir kurum birkaç temel konfigürasyona sahip olabilmektedir. Temel konfigürasyonlar hash özeti, aygıt kimlikleri, seri numaralı konfigürasyon dosyaları gibi yollarla karakterize edildikten sonra bu bilgilerde meydana gelen değişiklikler izlenmelidir.

Güvenli yedekleme ve kurtarma süreçleri yürütülmelidir

Tüm önlemlere rağmen, içeriden başarılı bir saldırı gerçekleştirilmesi yine de mümkündür. Kurumlar, güvenli yedekleme ve kurtarma işlemlerini uygulayarak ve periyodik olarak test ederek bu olasılığa hazırlanmalı ve kurumsal esnekliği arttırmalıdır.

Önleme, içeriden gelebilecek saldırılara karşı ilk savunma hattıdır. Fakat, kararlı iç tehditler yine de bir sistemi tehlikeye atmanın yollarını bulabilmektedir. Kuruluşların etkin yedekleme ve kurtarma süreçleri yürütmesi gerekmektedir; böylece bir sistem ele geçirilirse işletme operasyonları minimum kesintiyle sürdürülebilmektedir.

Yetkisiz veri sızıntılarına karşı "kapılar" kapatılmalıdır

Kuruluşlar, bilgi sistemlerinin veri sızmalarına karşı nere(ler)de hassas olduğunu anlamalı ve azaltma stratejileri uygulamalıdır.

Bilgi sistemleri, USB sürücülerden diğer çıkarılabilir ortamlara, yazıcılardan e-postalara kadar bilgi paylaşmanın birçok yolunu mümkün kılmaktadır. Her tip cihaz, veri sızıntısını önleme konusunda farklı zorluklara sahiptir. Hassas bilgilerin iç tehditler tarafından ele geçirilmesi riskini azaltmak için kurumlar, verinin sistemden nerede ve nasıl çıkarılabileceğini tanımlamalıdır.

İşten çıkarmaya yönelik kapsayıcı bir süreç geliştirilmelidir

Kurumlarda eski çalışanlarından gelebilecek zarar riskini azaltan bir işten ayrılma prosedürü bulunmalıdır. İşten ayrılma prosedürleri, eski çalışanın hesaplarının kapatılmasını, ekipmanlarının toplanmasını ve diğer personele bildirilmesini içermelidir. Düzgün işeyen bir hesap ve envanter yönetimi süreci, bir çalışan şirketten ayrıldığında ortaya çıkabilecek iç tehdit riskini azaltmada yardımcı olabilmektedir. Çalışanların işten çıkarılması, çalışanın tekrar geri dönerek iş yeri şiddet olayına teşebbüs etmesine yol açabilecek hoşnutsuzluğunun azaltılması yönünde tutarlı ve saygılı bir şekilde yapılmalıdır.

İş gücünü kurumla birlikte hareket ettirebilmek için olumlu teşvikler benimsenmelidir

Kurumsal desteği artıran işgücü yönetim uygulamaları olumlu teşvikler olarak adlandırılmaktadır, çünkü bir çalışanı kuruluşun çıkarları için hareket etmeye ikna etmeye çabalamaktadırlar. Çalışanların, olumlu teşvikler yoluyla kuruluşun çıkarlarına dâhil olmaya teşvik edilmesi, iç tehdit riskini azaltmaktadır. İşgücü değerlerini ve tutumlarını kurumun hedefleri ile uyumlu hale getiren olumlu teşvikler, zorlama işlevlere dayanan geleneksel güvenlik uygulamalarının geliştirilmesinde bir temel oluşturmaktadır. Teşviklerin ve zorlama işlevlerin bir araya gelmesi, içeriden tehdit savunmasının etkinliğini ve verimliliğini arttırmaktadır.

3.6.2. Kritik altyapılarda iç tehdidin tespiti ve önlenmesine yönelik teknik önlemler

Teknik önlemler tek başlarına yeterli olmasa da, iç tehdidin tespiti ve önlenmesinde önemli bir sac ayağı konumundadır. Çalışanların ve kullanıcıların sosyal, davranışsal ve psikolojik analizlerine ve analizlerden çıkan sonuçların yorumlanmasına dayanan önlemlerin incelenmesi bu çalışmanın kapsamı dışındadır.

Bilinen özelliklerinden dolayı iç tehdide karşı tedbir almak araştırmacılar ve hem özel hem de kamu sektöründeki yöneticiler için uzun yıllardır önemli bir mücadele alanıdır. İç tehdidin tespiti ve önlenmesine yönelik teknik tedbirlerin sınıflandırılmasına yönelik de literatürde önemli çalışmalar bulunmaktadır [121-122]. Bu çalışmalar ışığında alınabilecek teknik önlemlere ait sınıflandırma Çizelge 3.2'de sunulmuştur.

Çizelge 3.2. Kritik altyapılarda iç tehdide karşı alınabilecek teknik önlemler

Teknik önlem	Açıklama	Yapılan Çalışmalar
Saldırı tespit sistemleri (IDS)	Anomali ya da imza tabanlı tespit sistemleridir. Örn. Snort, Suricata vb.	[107, 110, 115]
Erişim kontrolü ve kimlik yönetim sistemleri	Kimlik doğrulama ve yetkilendirmeyi içerirler. Kullanıcı hesap ve parola yönetim uygulamalarını barındırırlar.	[109, 114, 123, 124, 125]
Güvenlik olay yönetim sistemleri (SIEM)	Çeşitli kaynaklardan toplanan kayıtların analizi ve yorumlanmasıdır. SIEM olarak adlandırılır. Örn. Splunk, OSSEC, OSSIM, Elasticsearch vb.	[112, 126, 127]
Uç nokta koruma ve veri kaçağı önleme sistemleri	Uç noktalarda bulunan ajanlar vasıtasıyla ya da ağ temelli konumlandırılmaktadırlar. Hassas verinin kurum dışına çıkmasını engellemek ve zararlı yazılıma karşı mücadele etmek amacıyla kullanılmaktadırlar.	[128, 129]
Balküpleri ve tuzak kayıtlar	Kötü niyetli kullanıcıyı kendine çekerek tespit edebilmeyi hedeflerler. Endüstriyel kontrol sistemlerinde kullanılan balküpleri; Conpot, T-pot, Honeynet vb.	[94]
Diğer	Active Directory, grup politikası (GPO), segmentasyon, ayrıcalıklı hesap yönetimi, makine öğrenmesi, farkındalık ve eğitim vb.	[132-134]

Saldırı tespit sistemleri (IDS)

Literatürdeki çalışmaların büyük bölümü saldırı tespit sistemlerine dayanmaktadır [107, 110, 115]. Saldırı tespit sistemleri uç nokta tabanlı ya da ağ tabanlı olarak konumlandırılabilmektedir. Bu sayede ağdaki trafiği inceleyerek zararlı davranışları tespit etmektedirler. Tespit yöntemi anomali ya da imza tabanlı olarak ikiye ayrılmaktadır. Anomali tabanlı saldırı tespiti ağ trafiğindeki "normal" davranıştan sapmaları tespit etmektedir. Bu maksatla önce "normal" diye nitelendirilebilecek baz trafik tespit edilmelidir. Baz olarak alınan trafikteki bant genişliği, veri kullanımı, kullanılan protokoller ve zaman

bilgisi önemli kriterler arasındadır. Bu verilerde meydana gelebilecek ani sapmalar iç tehdidin tespitinde kullanılabilmektedir. Fakat hatalı alarmlar üretilmesine karşın kriterler çok iyi belirlenmeli ve baz trafik doğru bir şekilde tespit edilmelidir. İmza tabanlı yöntemde ise endüstriyel kontrol sistemlerinde geçmişte meydana gelmiş bilinen saldırıların (ExplReadRam, ExplExec, ExplWriteRam gibi) imzaları ile mevcut trafik bilgisi karşılaştırılmaktadır.

Günümüzde saldırı tespit sistemleri ile yapılan çalışmalar veri madenciliği, istatistiksel modeller (eşik değeri belirlenmesi, Markov modeli vb.) ve yapay sinir ağlarını da beraber kullanmaktadırlar [107].

Erişim kontrolü ve kimlik yönetim sistemleri

Erişim kontrolü içeriden gelen saldırıları önlemenin önemli bir yoludur. İdeal erişim kontrolü ilkesi, aynı anda kullanıcıya bir dizi kurala göre erişimi kısıtlarken, gerekli görevleri yerine getirmek için yeterli yetkileri verir. Kurallar, en az imtiyaz, hak yükseltme (kullanıcının belirli hakları edinebilmesine izin verme) ve görevlerin ayrılması (temelde eylemleri ayrı görevlere bölme ve görevi tamamlamak için her bir eylemi yapacak birden çok kişinin bulunması) ilkelerine dayanmaktadır.

Erişim kontrolü, bazı kimlik bilgilerine dayanarak elektronik kaynaklara erişimi sağlayan veya sınırlayan bir mekanizmadır. Bu mekanizmanın iki bileşeni vardır:

- Kimlik doğrulama, kim ya da ne olduğunuzu, hangi referanslara sahip olduğunuzu gösterir. Genellikle “neyi bildiğiniz” (örneğin bir şifre), “neye sahip olduğunuz” (örneğin, cep telefonu) ve “ne olduğunuz” (biyometrik veri) özelliklerinin bir kombinasyonunu sunmak olarak tanımlanır. Ayrıca bazı yöntemler, “nerede olduğunuz” (örneğin belirli bir yer) gibi bir dördüncü kriteri de dikkate almaktadır [114].
- Yetkilendirme, sağlanan kimlik bilgilerinin istenen türde bir erişim sağlamak için yeterli olup olmadığını sistemin belirlemesidir [14].

Temel formunda erişim kontrolü, sistem kaynaklarına erişimi olan kullanıcıları tanımlamaktadır. Erişim kontrol yöntemleri isteğe bağlı erişim kontrolü (DAC), zorunlu erişim kontrolü (MAC) ve rol tabanlı erişim kontrolü olarak (RBAC) üçe ayrılabilir. İsteğe bağlı erişim kontrolünde veriye erişimde bulunacak kişileri verinin sahibi belirlerken,

zorunlu erişim kontrolünde yetkilendirme, merkezî bir otoritenin düzenlemelerine göre belirlenmektedir. Rol tabanlı erişim kontrolü daha ayrıntılı bir yaklaşımdır. RBAC, kaynaklara erişimi olan bir kuruluşta kullanıcılar yerine "roller" tanımlar. Daha sonra erişim yetkisi için kullanıcılar rollere atanır. En az ayrıcalık ve görevlerin ayrılığı gibi ilkeleri uygular. Bu yöntemlerin dışında ortaya çıkan bir diğer yöntem özellik tabanlı erişim kontrolü (ABAC) ya da grup tabanlı erişim kontrolü (GBAC) olarak adlandırılır [123]. Bu yöntemde ise kullanıcılar çalıştıkları zaman aralığı, pozisyon ya da konum bilgisi gibi özelliklere bağlı olarak atandıkları grubun kaynaklarına erişirler. Diğer yöntemlere göre daha dinamik bir yöntemdir.

Bu kapsamda kritik altyapılarda özellikle SCADA yazılımlarına her kullanıcı kendi hesap bilgileri ile giriş sağlamalı, erişimler kontrol altında bulundurulmalı, kayıt altına alınmalı ve HMI cihazları kullanıcı profillerine göre yetkilendirilmelidir. SCADA sunucusu ve veri tarihçilerine erişim sınırlı sayıda kişide bulunmalı, her kullanıcı kendi hesap bilgileri ile giriş sağlamalı ve yapılan işlemler kayıt altında tutulmalıdır. Özellikle geniş alana ya da internete erişim sağlayan cihazlarda mutlaka erişim kontrolü uygulanmalı, yetkisiz kişilerce kullanılamamalıdır [124]. Literatürde kritik altyapılarda operatörlerin davranışlarına endeksli olarak oluşturulan güven tabanlı erişim kontrol sistemi çalışmaları da bulunmaktadır [125].

Güvenlik olay yönetim sistemleri

Bilgi teknolojilerinde olduğu gibi operasyonel teknolojilerdeki cihazlar da yapılan işlemler sonucunda log kaydı üretmektedirler. Bu kayıtlar kaynak kullanım bilgileri, işletim sistemi kayıt dosyaları, dosya ve klasör erişim bilgileri, hata raporları ve güvenlik cihazlarına ait kayıtları içerebilmektedir. Tüm bu kayıtları tek bir merkezde toplayarak analiz eden, yorumlayabilen ve alarm üretebilen sistemler ise SIEM (security information and event management) olarak adlandırılmaktadır. Operasyonel teknolojilerin, bilgi teknolojilerine göre bu konudaki dezavantajı ise zaman-kritik sistemler olmasıdır. Kayıt dosyalarının toplanması sistemlerde fazladan kaynak tüketimine neden olduğundan cihazların ağır çalışmasına sebep olabilmektedir. Bu nedenle kritik altyapılarda ve endüstriyel kontrol sistemlerinde alınan güvenlik tedbirleri PLC, RTU, HMI, IED gibi cihazların yükünü artırmamalıdır.

Bununla beraber SIEM sistemleri kullanılarak kullanıcı aktiviteleri izlenebilmekte ve buna dayalı kullanıcı davranış analizleri (user activity monitoring) yapılabilmektedir [112]. Örneğin, normalde gündüz vardiyasında çalışan bir operatörün gece saatlerinde ağda yarattığı trafik, bir kullanıcının bilinen kullanım kalıbının dışında büyük boyutlu bir dosya transfer işlemi ya da bir çalışanın daha önce hiç kullanmadığı bir yazılımı indirmesi ve kurması gibi davranışlar kötü niyetli girişimlerin göstergesi olabilir. Kullanıcı davranışlarını izlemek amacıyla aşağıda sunulan parametreler kullanılmaktadır:

- Trafik bilgisi (tüketilen bant genişliği, kullanılan protokoller),
- Oturum açma-kapama saatleri,
- Ziyaret edilen web siteleri,
- Kullanılan araçlar,
- Oturum açılan bilgisayarlar,
- Giriş yapılan dahili sunucu vb.

SIEM'ler sıklıkla diğer yöntemler ile beraber kullanılırlar [126-127].

Uç nokta koruma ve veri kaçağı önleme sistemleri

Dünyayı sarsan Snowden ve Manning vakalarında olduğu gibi birçok kritik altyapı kurumu veri sızıntısı yaşamışlardır. Kritik altyapılarda meydana gelen veri sızıntıları ulusal güvenliği tehdit etmekle beraber fikri mülkiyet hırsızlığı gibi olaylar da büyük maddi kayıplara neden olmaktadır.

Uç nokta koruma ve veri kaçağı önleme sistemleri genellikle uç noktalarda bulunan bir ajan yazılım vasıtasıyla kullanıcı aktivitelerini takip eder ve bir merkezi sunucuya bilgi gönderirler. Bu aktiviteler dosya transfer işlemleri, harici bellek kullanım işlemleri, dosya yükleme ve indirme işlemleri gibi eylemlerden oluşabilir. Bu sistemler ayrıca uç noktalarda zararlı yazılımların tespiti ve engellenmesi maksadıyla antivirüs ve işletim sistemi zaafiyetlerini tarayan yazılımlar da barındırabilmektedirler.

Kritik altyapılarda bulunan kritik verilerin erişimlerinin kontrol edilmesi, dolaşımdaki verinin takip edilmesi ve kuruma veri giriş/çıkışı olabilecek noktalarla ilgili net politikaların belirlenmesi iç kaynaklı sızıntıların önlenmesine yönelik alınabilecek önemli tedbirlerdir.

Ayrıca hassas veriler şifrelenerek kötü niyetli kişilerin eline geçmesi engellenebilmektedir [128].

Uzun yıllardır iç tehdit üzerinde araştırmalarını sürdüren Carnegie Mellon Üniversitesi bu konuda hazırladığı teknik dokümanda [129], OpenDLP adlı açık kaynak veri kaçağı önleme sisteminin kullanımından bahsetmiştir. Taşınabilir USB belleklerin denetimi amacıyla Active Directory grup politikalarının (GPO) kullanımını önerilmiş ve her iki kaynaktan da üretilecek kayıtların bir arada değerlendirilmesi gerektiği vurgulanmıştır.

Bal küpleri ve tuzak kayıtlar

Bu yöntem özellikle aktif keşif aşamasındaki saldırganı kendine çekerek tespit edilmesini ve saldırının daha başlamadan sonlandırılmasını hedeflemektedir. Bu yüzden, bazı tuzak kayıtlar, bal küpü uç noktalar ve aldatıcı veriler kullanmaktadırlar. Yapılan çalışmada [94] aldatma yöntemleri saldırı hazırlığı safhası ve sömürme/veri sızıntısı aşaması olarak iki ana başlıkta toplanmıştır.

Saldırı hazırlığı safhası

DNS bal kaydı, bir bal küpü tekniği olarak kurumun DNS sunucusunda gerçekte kullanılmayan sahte DNS kayıtları oluşturulmasıdır. Saldırganlar bilgi toplama aşamasında, bu adresleri ele geçirip aktif keşif aşamasına geçtiklerinde, aslında var olmayan bu adreslere gelen istekler için alarm üretilerek saldırı öncesinde keşif yapılabilmektedir.

Web sunucu bal kaydı, kurumun web sitesi üzerinde üretilecek görünmez linkler yardımıyla oluşturulmaktadır. Arama motoru botları tarafından okunan ve web sunucusunda indekslenmesi istenmeyen klasörleri barındıran robots.txt dosyası üzerinde oluşturulabilecek ve aslında var olmayan sahte klasörler (/admin, /login gibi) ile normal kullanıcıların erişmeyeceği alanlara erişim olması durumunda alarm ürettirilerek daha keşif aşamasında saldırı tespiti yapılabilmektedir. Ayrıca sahte HTML yorumları da (<!-- test hesabı:admin, parola:password --!> gibi) bu yöntem için ek olarak kullanılabilmektedir [94].

Sömürme/veri sızıntısı aşaması

İnternette kara delikler olarak da adlandırılan, kurumun sahip olduğu IP aralığında bulunan fakat hiçbir sunucu ya da istemci bilgisayarın bulunmadığı ağlar "kara ağlar" olarak isimlendirilmektedir. Bu ağlara meşru bir kullanıcı yanlış bir IP adresi girmesi sonucu da bağlanabilir fakat ağa gelen yoğun istekler şüpheli davranış olarak sınıflandırılmalıdır.

Bal dosyaları, kurumun dosya sunucuları ya da ağdaki herhangi bir konumda saldırgan için çekici görünebilecek ama aslında hassas bilgi barındırmayan dosyalar yaratılabilmektedir. Bu tarz dosyalar ya mevcut bir dosyanın değiştirilmesi ile ya da inandırıcılığı yüksek bir içerik kullanılarak oluşturulabilmektedir. Örneğin dosya ismi password.docx ya da yeni_yatirimlar.pdf olabilir. Ayrıca yem dosya oluşturulurken sahte damgalar (GİZLİ, ÇOK GİZLİ gibi) kullanılarak inandırıcılık artırılabilmektedir. Dosya sistemi izlemesi ya da bir kod parçacığı kullanılarak bu tarz erişimler kayıt altına alınmakta ve alarm üretilmektedir. Böylece içeriden de olsa bir veri sızıntısı önceden tespit edilebilmektedir [94].

Bal küpleri ayrıntılı olarak çalışmanın 5. bölümünde açıklanmıştır.

Diğer

Kritik altyapılar hem bilgi teknolojisi hem de operasyonel teknoloji ağlarını bir arada bulundururlar. Operasyonel teknoloji güvenliğinin sağlanması ise öncelikle bilgi teknolojilerinden geçmektedir. Çünkü saldırganlar operasyonel teknolojilere ulaşmak için bilgi teknolojilerini bir atlama noktası olarak kullanmaktadırlar [130].

Bu durumun bir örneği 2015'te Ukrayna'da 225 000 kullanıcının elektriğinin kesilmesine sebep olan siber saldırıda görülmüştür. Saldırganlar hedefli oltalama saldırısı ile önce bilgi teknolojilerine sızmış, ardından BlackEnergy 3 zararlı yazılımını kullanarak tuş kayıt ediciler sayesinde kullanıcı hesap bilgilerini elde etmiş ve operasyonel teknoloji ağlarına sızmışlardır [131].

Bu maksatla kritik altyapılarda mutlaka ağ segmentasyonu uygulanmalıdır. BT ve OT ağları ayrı segmentler halinde konumlandırılmalı ve mutlaka güvenlik duvarı ile ayrılmalıdır. Bu maksatla Purdue Üniversitesi tarafından geliştirilen ve ISA (International Society of

Automation) tarafından endüstriyel kontrol sistemlerine uyarlanan Purdue Model kritik altyapılarda kullanılabilecek örnek bir modeldir (EK-1). Purdue modelde kritik altyapı bilgi ve operasyonel teknolojileri 6 ağ segmentine ayrılmıştır [132]:

- Kurumsal DMZ
- Yerel Kurumsal Ağ
- Kontrol DMZ
- Supervisory
- Lojik (Kontrol)
- Saha & Enstrümanlar

Bu segmentler arası geçişlerde mutlaka güvenlik duvarı bulundurulmalı ve sadece müsaade edilen kullanıcı, makine ve servislerin geçişi mümkün olmalıdır. Böylece örneğin kurumsal ağda yetki sahibi bir kullanıcı, kontrol ağında bulunan bir HMI'ya müdahale edemeyecektir. Dolayısıyla kurum içindeki kötü niyetli kullanıcıların yetkisiz erişim olanakları azaltılmış olacaktır.

Bununla beraber kritik altyapıların özellikle kurumsal ağ tarafında uygulanacak Active Directory benzeri dizin hizmetleri ile hem erişim kontrolü ve kimlik yönetimi sağlanabilir hem de oluşturulacak grup ilkeleri (GPO) ile çok esnek ve hassas bir şekilde istenen kısıtlamalar uygulanabilir. Grup ilkeleri ile iç kaynaklı saldırılara yönelik kullanıcıların;

- CD/DVD ve USB gibi taşınabilir depolama ortamları kullanımı kısıtlanabilir; eğer kısıtlanmak istenmiyorsa kullanımlarının denetlenmesi amacıyla olay kayıtlarından (event logs) faydalanılabilir,
- İstenmeyen herhangi bir yazılım çalıştırması engellenebilir (AppLocker),
- Maskeli saldırganlara karşı belirli bir süre oturumu açık kalan kullanıcıların hesaplarının kilitlenmesi sağlanabilir,
- Kullanıcılara parola karmaşıklık ilkeleri uygulanabilir ve belirli sürelerle değiştirmeleri sağlanabilir,
- Oturum açma yetkisi belirli saat aralığı ile kısıtlanabilir,
- Ağdaki herhangi bir klasörü bilgisayarına ataması engellenebilir.

Alınabilecek bu tedbirler ile birçok iç kaynaklı saldırının önüne geçmek mümkün olabilmektedir.

Bununla beraber kritik altyapılardaki iç tehditlere karşı literatürde makine öğrenmesi ve bilişsel zeka yöntemlerinin de kullanılabileceğini belirten çalışmalar da mevcuttur [133-134].

Endüstriyel kontrol sistemleri gibi çok katmanlı mimarilerde derinlemesine güvenlik (depth-in-defense) anlayışı önem kazanmaktadır. Derinlemesine güvenlik, alınan siber savunma tedbirlerinin herhangi bir yoldan atlatılabileceği kabul edilerek her katmanda, o katmanın özelliklerine ve bulundurduğu varlıklara göre özel önlemler almaktır [132].

İnsan kaynaklı tehditleri azaltabilmenin en önemli yollarından biri de kullanıcıların farkındalık sahibi olmaları ve düzenli olarak eğitilmeleridir. Eğitimlerin asıl amacı kullanıcıda davranış değişikliği yaratabilmektir. Kullanıcıların pasif olarak dinleyecekleri eğitimler yerine, kendilerinin de katılabileceği tatbikat (oltalama vb.) tarzı faaliyetler daha etkili olmaktadır. Farkındalık ve eğitimler sadece bilgisiz ve dikkatsiz kullanıcılara yönelik gibi görünse de güvenlik ihlallerinin neticesinde doğacak sorumlulukların belirtilmesi kötü niyetli kullanıcılara karşı da caydırıcılık sağlamaktadır.

4. UYGULAMA VE ANALİZ

Yapılan çalışmada kritik altyapılarda ve endüstriyel kontrol sistemlerinde kullanılabilecek bir bal küpü uygulaması önerilmiştir. Önerilen yöntemde, kurum içinde konumlandırılan bal küpü uygulaması gerçek bir PLC gibi ağ paketlerine yanıt vermekte, aynı zamanda trafik bilgisi için log üretmektedir. Üretilen kayıtlar daha sonra bir SIEM uygulaması olan Splunk'a gönderilerek burada sonuçlar analiz edilmekte ve muhtemel saldırgana ait bilgiler elde edilmektedir. Ayrıca Splunk üzerinde gerçekleştirilen ayrıntılı sorgular ile alarmlar ve ayrıntılı raporlar üretilmektedir.

Önerilen yöntemin test edilmesi amacıyla faklı EKS protokolleri üzerinde test senaryoları geliştirilmiş ve sonucunda bal küpü uygulamasının iç tehditlere karşı kullanım etkinliği değerlendirilmiştir.

4.1. Bal Küpleri

Bal küpleri gerçek sistemin özelliklerini taklit ederler ve saldırganları kendilerine çekerek saldırıların keşif aşamasında tespit edilebilmesini hedeflemektedirler. Bal küplerinde üretilen log kayıtlarından faydalanılarak saldırganların teknik, taktik ve prosedürleri (TTP) ortaya çıkarılabilmektedir [135]. Bu nedenle bal küplerinin sahip olması gereken iki önemli özellik bulunmaktadır: ikna edicilik ve cezbedicilik. Bal küpü, saldırgan tarafından tuzak olarak anlaşılmamalı fakat aynı zamanda saldırganı da üzerine çekebilecek gerekli açıklıkları barındırmalıdır.

Bal küpleri literatürde düşük-etkileşimli ve yüksek-etkileşimli olmak üzere ikiye ayrılmaktadır [136]. Aralarındaki fark, saldırganın bal küpü üzerinde neler yapabileceği ile ilgilidir.

Yüksek etkileşimli bal küpleri genellikle gerçek cihaz, işletim sistemi ve uygulamaları kullanmaktadırlar. Yüksek-etkileşimli bal küpünün faydası, saldırgan gerçek sistemde uygulayabileceği her şeyi yüksek-etkileşimli bal küpünde de uygulayabilecektir. Böylece saldırganın tüm davranışları yakalanabilecek ve analiz edilebilecektir. Fakat bu tip bal küpleri saldırganın sızma girişimleri sonucu kolayca zarar görebilirler. Bu durumda yeniden

kurulmaları gerekir. Hatta nadiren olsa da bazı ataklar bal küpünün geri döndürülemez şekilde kullanım dışı kalmasına neden olabilmektedir [135].

Düşük-etkileşimli bal küpleri ise genellikle Linux gibi bilinen bir işletim sistemi üzerine kurulmaktadırlar. Gerçek sistemin tüm özelliklerini ihtiva etmese de saldırganın etkileşime geçmesini sağlayan altyapıyı bünyelerinde barındırmaktadırlar. Avantajlarından biri de kolay kurulmalarıdır. Honeyd, bu tipte bal küpüne bir örnek olarak verilebilir. Düşük-etkileşimli ve yüksek-etkileşimli bal küplerinin özellikleri Çizelge 4.1'de sunulmuştur [136].

Çizelge 4.1. Bal küpü tipleri [136]

Düşük etkileşimli	Yüksek etkileşimli
Gerçek işletim sistemi ve hizmetleri taklit eder.	Gerçek işletim sistemi ve hizmetler kullanılır.
Yüklenmesi ve kurulumu kolaydır. Genellikle bilgisayar üzerine yüklenebilen bir yazılımdır.	Kurulumu ve kullanımı karmaşıktır.
Saldırganın yapıp yapamayacağı şeyler taklit edilen hizmetler tarafından belirlendiğinden düşük risk taşır.	Saldırganlar gerçek işletim sistemine müdahale edebildikleri için risk yüksektir.
Asıl işlem verisinin bir bölümünü ve sınırlı etkileşim verisi ele geçirir.	Yeni araçlar, iletişim yolları ya da saldırganın tuş vuruşları gibi çok daha fazla bilgiyi ele geçirebilir.

4.1.1. Kritik altyapılarda kullanılabilecek bal küpleri

SCADA HoneyNet Project

SCADA ağlarına yönelik bilinen ilk bal küpü Cisco Systems çalışanı iki kişi tarafından ortaya konmuştur. PLC benzetimi yapan ve honeyd ile beraber çalışan bir modül hedeflemişlerdir. FTP, http, Modbus TCP ve Telnet gibi protokolleri içermektedir [137].

PLC HoneyNet Project

Bir başka bal küpü ağı projesi, bir araştırma ve danışma şirketi olan Digital Bond tarafından geliştirilmiştir. Proje kapsamında PLC bal küpü olan ve trafiği toplayan bir güvenlik duvarı bal küpünden oluşan iki adet sanal makine bulunmaktadır [135]. Digital Bond tüm içeriğini

Dale Peterson adlı araştırmacının sitesine taşıdığından dolayı bu çalışmanın yapıldığı sırada söz konusu proje erişilebilir değildir [138].

Conpot

Conpot, dağıtımı, değiştirilmesi ve genişletilmesi kolay, düşük etkileşimli ve açık kaynak kodlu bir endüstriyel kontrol sistemleri (EKS) bal küpüdür. Birçok EKS protokolünü barındırmakta ve bu sayede saldırganı ikna edebilecek büyük ve karmaşık bir yapı yaratılabilmektedir. Aldatıcı yetenekleri geliştirmek ve aynı zamanda saldırı yüzeyini arttırmak için özel bir insan-makine arayüzü oluşturma imkânı sağlanmıştır. Protokoller eksiksiz olarak temsil edildiği için, Conpot'a insan-makine arayüzü kullanılarak erişilebilir ya da gerçek donanımlarla genişletilebilir. Conpot, Honeynet Projesi çatısı altında geliştirilmektedir [139].

Conpot bu çalışmanın gerçekleştirildiği sırada (versiyon 0.6.0) 6 farklı şablon içermektedir.

- IPMI: Basit bir IPMI (akıllı platform yönetim arayüzü) cihazı yaratır.
- IEC-104: IEC 60870-5-104 standardına dayanan bir Siemens S7-300 cihazı oluşturur.
- Kamstrup 382: Kamstrup 382 modeli bir akıllı sayaç emülasyonudur.
- Proxy: Vekil bilgisayar işlevi sunan örnek şablondur.
- Default: Siemens S7-200 cihazının benzetimini yapar. http, SNMP, Modbus, S7comm protokollerini barındırır.
- Guardian AST: Guardian AST gaz tankı sensörü benzetimidir.

SCADA ve endüstriyel kontrol sistemlerine yönelik bal küpü çalışmaları Çizelge 4.2’de sunulmuştur [140].

4.2. Deney Ortamı

İcra edilen çalışmada bal küpü olarak Conpot (versiyon 0.6.0) kullanılmıştır. Bal küpü Ubuntu 18.04 işletim sistemi üzerine kurularak SCADA ağı içinde konumlandırılmıştır. Bal küpü bilgisayarı Windows 10 Professional konak bilgisayarı üzerinde VMware Workstation Pro sanallaştırma programı kullanılarak sanal makine şeklinde oluşturulmuştur. Sanal makinanın ağ ayarı bridged seçilerek fiziksel ağa doğrudan bağlanması ve konak bilgisayardan farklı bir IP adresine sahip olması sağlanmıştır. Böylece bal küpü uygulaması

Çizelge 4.2. Kritik altyapılarda bal küpü çalışmaları

Çalışma	Bal küpü	Test Yatağı	Yöntem	Bulgular
[135]	Conpot	Syslog, Splunk	SNMP, MODBUS, HTTP	Geçmişte «hava boşluklu» olarak tasarlanan SCADA ağında bal küpü uygulaması değerlendirilmiştir.
[136]	Digital Bond Honeynet	Vmware, Snort	Telnet, FTP, SNMP, HTTP, Modbus, VxWorks Debugger	Bal küpü kurulumu aktif bir şekilde incelenmiş fakat düşük etkileşim sağlanmıştır.
[140]	Conpot	Amazon Micro Instance	SNMP, MODBUS, HTTP	Conpot etkili bir SCADA bal küpü olmasının yanında, analiz konusunda geliştirilmelidir.
[141]	Özel	Snort	HTTP	Hedefli saldırılara yönelmiş ve saldırganın yerini doğru bir şekilde tespit etmiştir.
[142]	Linux tabanlı	Vmware	HTTP, HTTPS, SNMP, ISO-TSAP	Siemens PLC'nin etkin bir simülasyonu olmakla beraber yüksek etkileşimli ortamda saldırgan davranışlarını da kayıt etmiştir.
[143]	CryPLH	Vmware	HTTP, HTTPS, SNMP, ISO-TSAP	Linux kullanılarak Siemens PLC etkili bir şekilde taklit edilebilmiştir.
[144]	Honeynet	Amazon EC2, Snort	Modbus, ICCP, DNP3, IEC-104, SNMP (v1/2/3), TFTP, XMPP'den faydalanan bal küpü ağı	Shodan ile bulunan uçlardan faydalanılarak diğer uçlara ulaşılmıştır.

ağdaki kullanıcıların bakış açısından konak bilgisayardan bağımsız bir cihaz görünümünde olmaktadır. Gerçekleşen iletişime bağlı olarak bal küpünde üretilen kayıtlar (log) daha sonra bir SIEM ürünü olan Splunk'a gönderilmektedir. Çalışmada Splunk Enterprise (versiyon 8.0.0) kullanılmıştır. Splunk Windows 10 Professional üzerinde kurulmuştur.

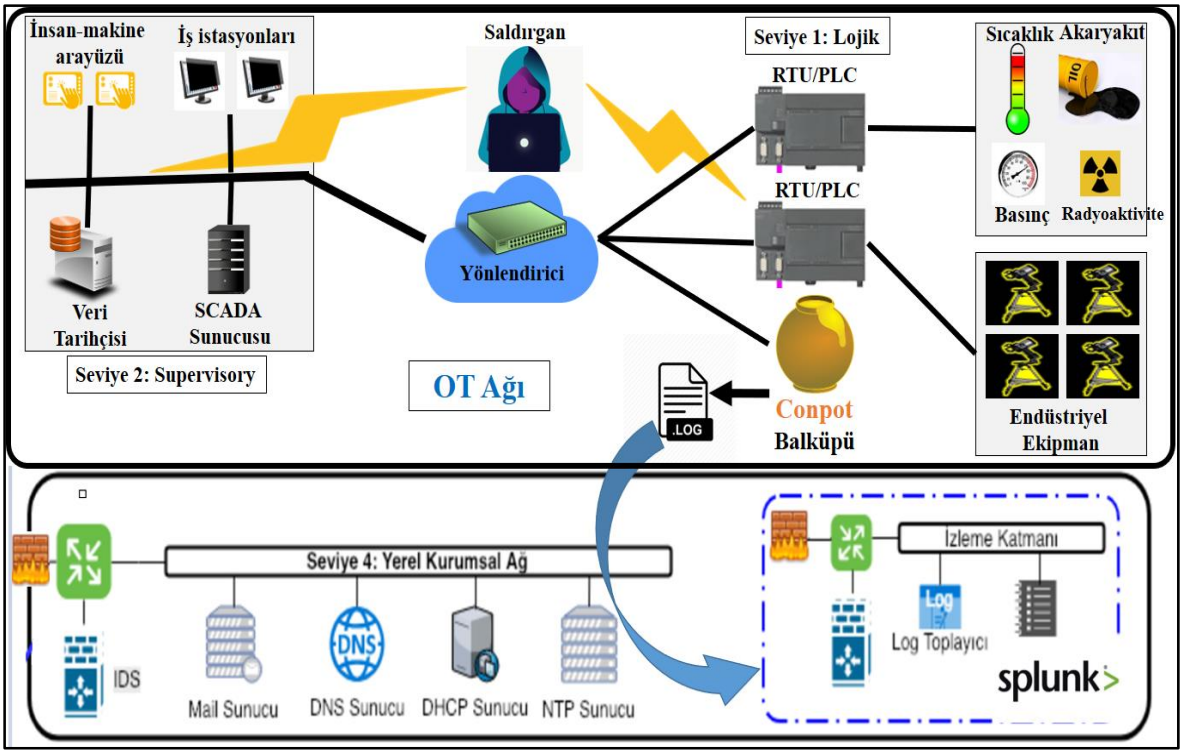
Test senaryolarını gerçekleştirmek amacıyla saldırı bilgisayarında Ubuntu 18.04 işletim sistemi kullanılmıştır. Ağ taramaları nmap aracı kullanılarak gerçekleştirilmiştir. Saldırıların gerçekleştirilmesi maksadıyla ScadaStrangeLove tarafından geliştirilen Plcscan yardımcı

programı ve Metasploit Framework sızma testi aracında bulunan modbusclient istismar kodu kullanılmıştır. Deney elemanları Çizelge 4.3'te sunulmuştur.

Çizelge 4.3. Deney elemanları

Deney Elemanı	Araç	Versiyon	İşletim Sistemi
Bal küpü	Conpot	0.6.0	Ubuntu 18.04 (Sanal)
SIEM	Splunk Enterprise	8.0.0	Windows 10 Professional
Saldırgan	Nmap modbusclient plcscan	-	Ubuntu 18.04

Yapılan çalışmada bal küpü tipik endüstriyel kontrol sistemi ağı içerisinde konumlandırılmıştır. Dolayısıyla operasyonel teknolojilerin bulunduğu ağda RTU ve PLC cihazların yer aldığı Lojik seviyede bulunmaktadır (EK-1). SIEM ürünü olan Splunk ise bilgi teknolojilerinin bulunduğu ağda ve Yerel Kurumsal Ağ segmentinde yer almaktadır. Bal küpüne gelen isteklerin bulunduğu log dosyalarının Splunk'a aktarılması için kurum içi güvenlik duvarında gerekli izinler sağlanmıştır. Deney ortamını gösteren topoloji Şekil 4.1'de gösterilmiştir.



Şekil 4.1. Deney ortamı ve test senaryosu topolojisi

4.2.1. Conpot kurulumu

İşletim sistemi üzerinde Conpot uygulaması kurulmadan önce bazı bağımlılıkların yüklenmesi gerekmektedir. Bu maksatla aşağıdaki komutlar çalıştırılır [145-147].

```
$ sudo apt-get install git libsmi2ldbl smistrip libxslt1-dev
python3.6-dev libevent-dev default-libmysqlclient-dev
```

Linux üzerindeki araçların ihtiyaç duyduğu *python* bağımlılıklarını birbirinden ayırabilmek için *virtualenv* aracından faydalınılır.

```
$ virtualenv --python=python3.6 conpot
```

Ortam aktif hale getirilir.

```
$ source conpot/bin/activate
```

Bağımlılıklar ve ortamda bulunan araçların güncellenmesi sağlanır.

```
$ pip install --upgrade pip
$ pip install --upgrade setuptools
$ pip install cffi
```

Python paket ambarı (PyPI) kullanılarak Conpot yüklenir.

```
$ pip install conpot
```

Uygulama kurulumu test edilir. Conpot bal küpü uygulaması çalıştırılır ve mevcut şablonlar (templates) aşağıdakikomut ile görüntülenebilmektedir.

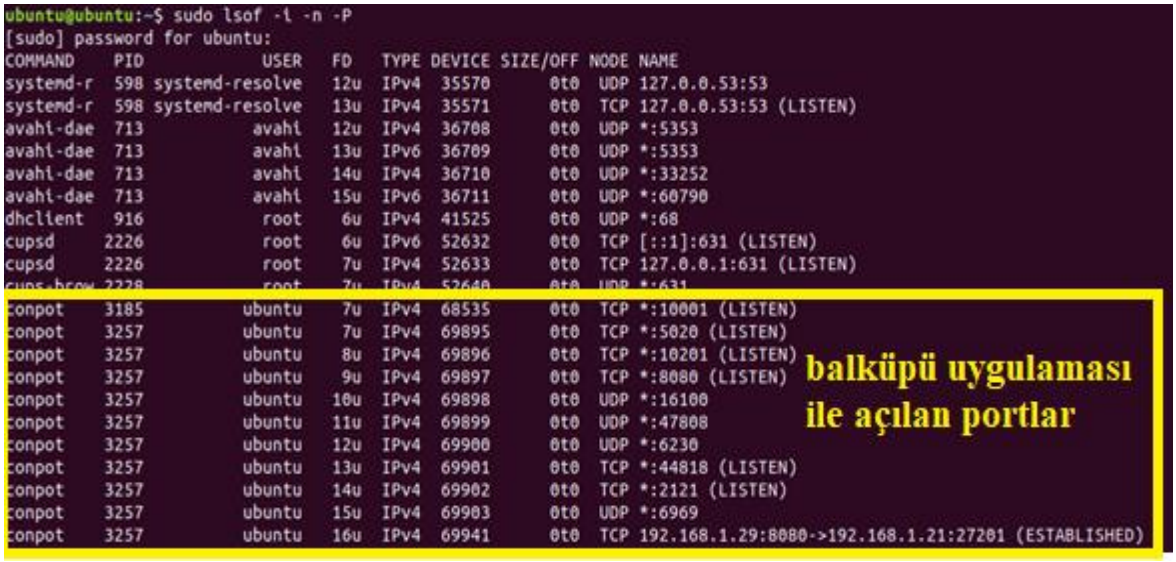
```
$ conpot -f
$ conpot –f –t default
```

komutu ile *default* şablon başlatılır. Hizmete açılan servisler ve portlar Resim 4.1'de görülmektedir.

```
2020-02-18 20:32:55,339 Modbus server started on: ('0.0.0.0', 5020)
2020-02-18 20:32:55,340 S7Comm server started on: ('0.0.0.0', 10201)
2020-02-18 20:32:55,341 HTTP server started on: ('0.0.0.0', 8800)
2020-02-18 20:32:55,560 SNMP server started on: ('0.0.0.0', 16100)
2020-02-18 20:32:55,563 Bacnet server started on: ('0.0.0.0', 47808)
2020-02-18 20:32:55,564 IPMI server started on: ('0.0.0.0', 6230)
2020-02-18 20:32:55,564 handle server PID [11979] running on ('0.0.0.0', 44818)
2020-02-18 20:32:55,564 handle server PID [11979] responding to external done/disable signal in object 140710598
608
2020-02-18 20:32:55,565 FTP server started on: ('0.0.0.0', 2121)
2020-02-18 20:32:55,565 Starting TFTP server at ('0.0.0.0', 6969)
```

Resim 4.1. Conpot default şablonunun başlatılması

Bal küpü bilgisayarı üzerinde farklı bir *terminal* açılarak hizmete açılan servisler ve portlar Resim 4.2'de gösterilmiştir.




```
ubuntu@ubuntu:~$ sudo lsof -i -n -P
[sudo] password for ubuntu:
COMMAND    PID            USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
systemd-r  598 systemd-resolve   12u  IPv4  35570      0t0  UDP 127.0.0.53:53
systemd-r  598 systemd-resolve   13u  IPv4  35571      0t0  TCP 127.0.0.53:53 (LISTEN)
avahi-dae  713           avahi   12u  IPv4  36708      0t0  UDP *:5353
avahi-dae  713           avahi   13u  IPv6  36709      0t0  UDP *:5353
avahi-dae  713           avahi   14u  IPv4  36710      0t0  UDP *:33252
avahi-dae  713           avahi   15u  IPv6  36711      0t0  UDP *:60790
dhclient   916            root    6u  IPv4  41525      0t0  UDP *:68
cupsd     2226            root    6u  IPv6  52632      0t0  TCP [::1]:631 (LISTEN)
cupsd     2226            root    7u  IPv4  52633      0t0  TCP 127.0.0.1:631 (LISTEN)
cups-brow 2228            root    7u  IPv4  52640      0t0  UDP *:631
conpot    3185          ubuntu    7u  IPv4  68535      0t0  TCP *:10001 (LISTEN)
conpot    3257          ubuntu    7u  IPv4  69895      0t0  TCP *:5020 (LISTEN)
conpot    3257          ubuntu    8u  IPv4  69896      0t0  TCP *:10201 (LISTEN)
conpot    3257          ubuntu    9u  IPv4  69897      0t0  TCP *:8080 (LISTEN)
conpot    3257          ubuntu   10u  IPv4  69898      0t0  UDP *:16100
conpot    3257          ubuntu   11u  IPv4  69899      0t0  UDP *:47808
conpot    3257          ubuntu   12u  IPv4  69900      0t0  UDP *:6230
conpot    3257          ubuntu   13u  IPv4  69901      0t0  TCP *:44818 (LISTEN)
conpot    3257          ubuntu   14u  IPv4  69902      0t0  TCP *:2121 (LISTEN)
conpot    3257          ubuntu   15u  IPv4  69903      0t0  UDP *:6969
conpot    3257          ubuntu   16u  IPv4  69941      0t0  TCP 192.168.1.29:8080->192.168.1.21:27201 (ESTABLISHED)
```

Resim 4.2. Bal küpü bilgisayarında açık portların görüntülenmesi

4.2.2. Conpot bal küpü uygulamasının deney ortamı için yapılandırılması

Resim 4.1'de görüldüğü gibi Conpot uygulaması Modbus, Bacnet, S7comm gibi endüstriyel kontrol sistemleri protokollerini başlatmıştır. Fakat uygulama bu protokolleri standart portlarında başlatmamaktadır. Bu maksatla uygulamanın bulunduğu bilgisayarda port yönlendirme yapılarak özellikle Modbus ve S7comm protokollerinin standart portları olan 502 ve 102 portlarında hizmet vermesi sağlanmıştır. Yapılan işlem bal küpü uygulamasının inandırıcılığını artıracak ve saldırganın bal küpüne ulaşmasını kolaylaştıracaktır. Port yönlendirme amacıyla iptables aracı kullanılmıştır.

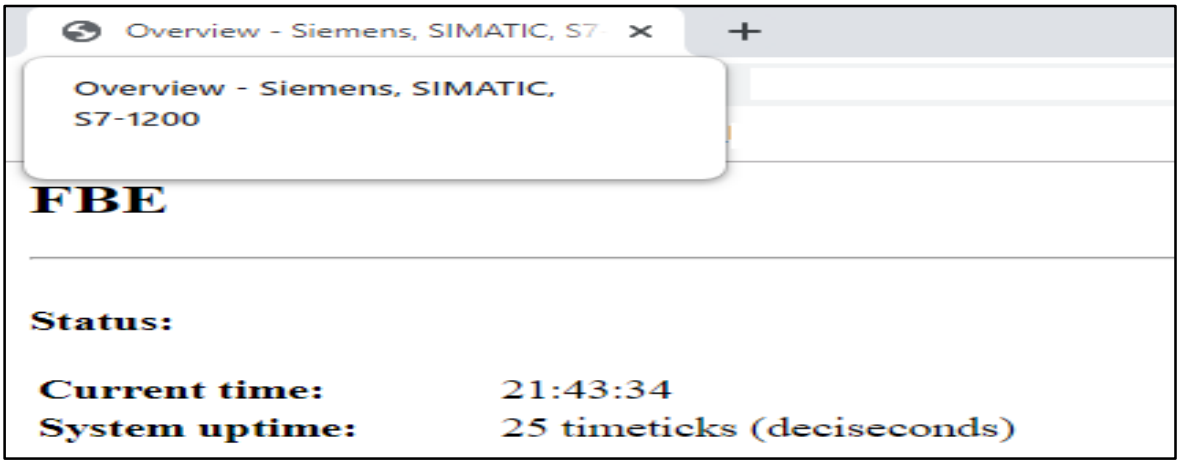
```
$ sudo iptables -t nat -I PREROUTING -p tcp --dport 102 -j
REDIRECT --to-ports 10201
$ sudo iptables -t nat -I OUTPUT -p tcp -o lo --dport 102 -j
REDIRECT --to-ports 10201
$ sudo iptables -t nat -I PREROUTING -p tcp --dport 502 -j
REDIRECT --to-ports 5020
$ sudo iptables -t nat -I OUTPUT -p tcp -o lo --dport 502 -j
REDIRECT --to-ports 5020
```

Deney ortamında Conpot uygulamasındaki default şablonu (template) kullanılacaktır. Fakat şablonda kullanılan Siemens S7-200 PLC cihazının eski bir cihaz olduğu değerlendirildiğinden ve saldırgan tarafından fark edilmemesinin sağlanması gerekçesiyle

cihaza ait konfigürasyon bilgileri daha yeni bir cihaz olan S7-1200'e ait bilgiler ile değiştirilmiştir. Uygulamanın açık kaynak kodlu olması mevcut endüstriyel kontrol sistemine uyum sağlama konusunda esneklik sağlamaktadır.

Siemens S7-200 ile alakalı bilgiler ve tanımlamalar S7-1200 ile değiştirilmiştir. İletişim protokolü modülü, işlemci (CPU) ve diğer modül bilgileri xml dosyasının düzenlenmesi sonucu S7-1200'e göre yapılandırılmıştır. Tesis adı ve sistemin adı isteğe göre yapılandırılabilir.

PLC'ye ait güncellenen bilgiler tarayıcı görüntülenerek test edilmiştir. PLC'nin S7-1200 olarak ve sistem adının FBE olarak görüntülendiği Resim 4.3'te görülmektedir.



Resim 4.3. Güncellenen PLC bilgilerinin tarayıcıda görüntülenmesi

4.2.3. Splunk kurulumu ve yapılandırılması

Splunk, birçok kaynaktan gelen log kayıtlarını gerçek zamanlı olarak analiz edebilen, kendine özel sorgu diliyle sorgulama yapmaya izin veren ve ayrıntılı raporlamalar sunabilen bir SIEM ürünüdür. Windows üzerinde Splunk .msi uzantılı bir dosya yardımı ile kurulmakta ve web arayüzü aracılığıyla yönetilmektedir [148]. Kurulum yapıldıktan sonra 8000 portu üzerinden yönetim arayüzüne ulaşılmaktadır.

Kurulum tamamlandıktan sonra Conpot bal küpü uygulamasına ait log dosyalarının gerçek zamanlı olarak izlenmesi sağlanmıştır. Bu maksatla, bal küpü uygulamasının olduğu bilgisayar ile Splunk kurulu bilgisayar arasında dosya paylaşım sistemi oluşturulmuştur. Böylece Splunk uygulaması üzerinden ilgili dosya "Add Data" seçeneği ile tanımlanmış ve

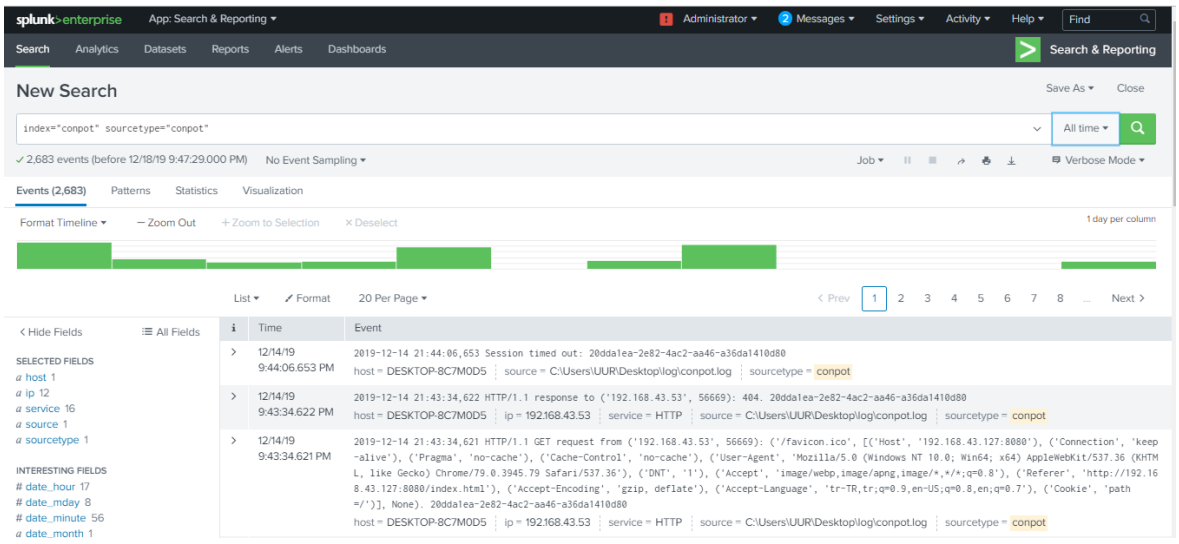
gerçek zamanlı olarak izlenmesi, analiz edilmesi ve sorgu yapılabilmesi sağlanmıştır.

Splunk üzerinde log dosyası girilirken belirlenmesi gereken en önemli etken “index” seçeneğidir. “Index” verilerin kayıt edildiği dizinlerdir. Farklı log dosyaları farklı “index” seçenekleri ile birbirinden ayrılmaktadır. Örneğin web sitesine ait veriler ile güvenlik kayıtları ayrı “index” alanlarında bulunabilir. Böylece sorgular daha hızlı ve amaca yönelik olmaktadır. Ayrıca her “index” için farklı kullanıcı yetkilendirmeleri yapılabilmekte ve saklanma süreleri farklı olarak belirlenebilmektedir. Yapılan çalışmada Splunk üzerinde “conpot” isimli bir “index” oluşturulmuştur ve Conpot log dosyaları bu alanda tanımlanmaktadır.

Belirlenmesi gereken bir diğer önemli husus da “sourcetype” seçeneğidir. Bu seçenek verinin ne şekilde yorumlanması gerektiğini belirler. Splunk log dosyasının tipine göre veriyi belirli alanlara ayırmaktadır. İsteğe bağlı olarak boşluk ya da tırnak işareti gibi belirteçler kullanılarak verinin nasıl yorumlanacağı özel olarak girilebilir. Resim 4.4’te görüldüğü üzere Conpot log dosyalarını zaman ve olay bilgisi şeklinde doğru bir şekilde yorumlamıştır.

4.3. Test Senaryosu

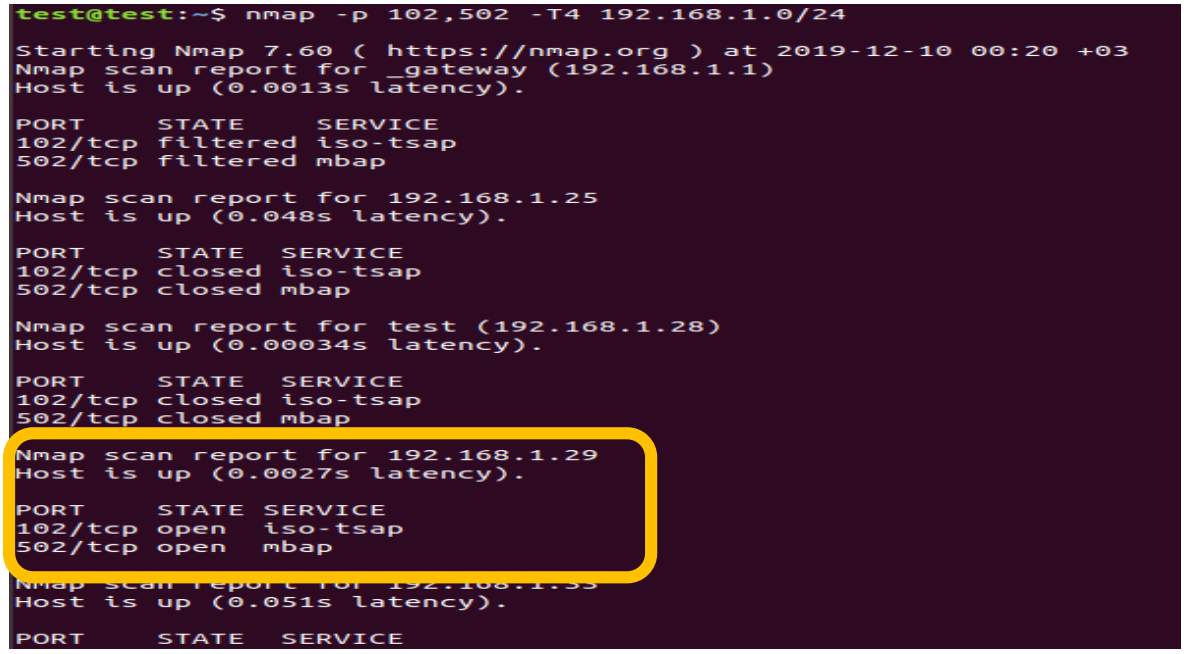
3. bölümde açıklandığı üzere bir siber saldırı keşif/bilgi toplama aşaması ile başlamaktadır.



Resim 4.4. Bal küpüne gelen isteklerin Splunk üzerinde gerçek zamanlı izlenmesi

Saldırgan her ne kadar içeride olsa da ulaşması gereken cihazların IP adresi ya da birim numarası gibi bilgilerine ihtiyaç duymaktadır. Bu maksatla pasif bilgi toplama aşamasını tamamladıktan sonra aktif keşif aşaması kapsamında port taraması gerçekleştirecektir.

PLC/RTU cihazlarının bulunduğu ağda S7comm ve Modbus protokollerine ait portlarda nmap tarama aracı kullanılarak IP taraması yapılmış ve bu portlarda hizmet veren bir cihaz Resim 4.5'te görülmektedir. Saldırganın tespit ettiği cihaz aynı ağda konuşlanmış bal küpü uygulamasıdır.

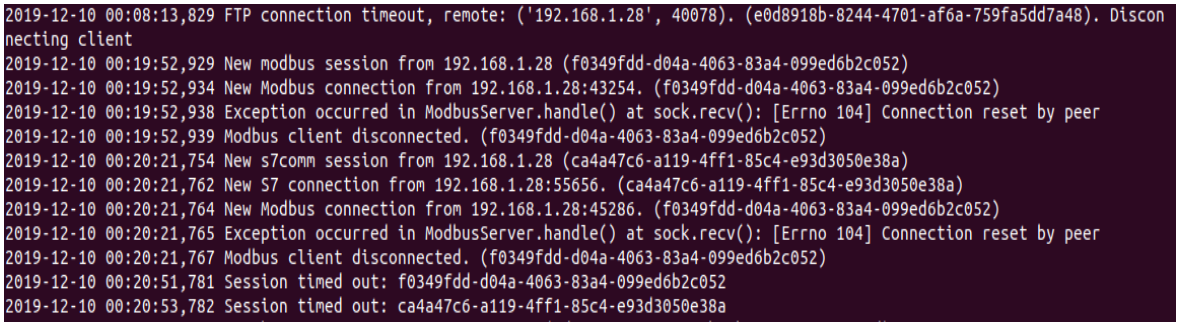


Resim 4.5. IP taraması

PLC olabilecek bir cihaz keşfedildikten sonra cihazda hizmet veren tüm servislerin tespiti için keşfedilen cihaz özelinde tüm portlar taranmıştır. Gerçekleştirilen port taraması sonucu açık olduğu tespit edilen portlar ve servisler Resim 4.6'da gösterilmiştir.

Resim 4.6. Port taraması

IP taraması ve port taraması bal küpü uygulamasında trafik yarattığından dolayı log kaydı oluşturmuştur. Gelen istekler ve verilen cevaplara ait verileri gösteren kayıtlar Resim 4.7'de sunulmuştur. Bu veriler eş zamanlı olarak Splunk uygulamasında görüntülenebilmektedir ve gerçek zamanlı izlenebilmektedir.



Resim 4.7. Bal küpü uygulamasına gelen istekler ve verilen cevaplar

Çalışan servisler, protokoller, açık portlar ve IP adresi bilgileri saldırgan tarafından tespit edilmiştir. Bu aşamadan sonra toplanan bilgiler ile elde edilen açıklıklar istismar edilmiştir. Bu maksatla Metasploit Framework sızma testi aracında bulunan modbusclient istismar kodu kullanılmıştır. Gerçekleştirilen saldırının, ele geçirilen ya da değiştirilen verinin daha iyi anlaşılabilmesi amacıyla kısaca Modbus protokolü veri yapısından ve diğer özelliklerinden bahsedilmiştir

Modbus veri modeli, bir dizi ayırt edici özelliklere sahip tablosal bir yapıdan meydana gelmektedir ve veriler bu dört tablo içerisinde saklanır. İki tablo dijital çıkış (coil, bobin) değerlerini ve dijital giriş (kontak) değerlerini açık/kapalı (on/off) formatında tek bit olarak saklar. Diğer iki tablo da saklayıcı kaydedicileri (analog çıkışlar, holding register) ve giriş kaydedicileri (analog girişler, input register) değerlerini nümerik formatta 16 bit (word) olarak saklar. Her tablo 9999 değer saklayabilir [149]. Bu tablosal yapı Çizelge 4.4'te gösterilmiştir.

Çizelge 4.4. Modbus veri yapısı [149]

Coil/contact/register numarası	**Veri Boyutu (Bit)**	**Özellik**	**Tablo Adı**
1-9999	1	Okuma/Yazma	Dijital Çıkışlar (Coil)
10001-19999	1	Okuma	Dijital Girişler (Contact)
30001-39999	16	Okuma	Giriş Kaydedicileri
40001-49999	16	Okuma/Yazma	Saklayıcı Kaydediciler

Modbus veri yapısında tutulan değerler EKS için önem arz etmektedir. Örneğin tek bit saklayabilen yazmaçlar bir vananın ya da rölenin açık-kapalı gibi durumlarını tutuyorken, 16-bit yazmaçlar bir depoda bulunması gereken minimum ya da maksimum su değerini, bir nükleer elektrik santrali santrifüjünün dönme hızını veya bir doğalgaz tesisindeki basınç miktarının eşik seviyesini gösteriyor olabilmektedir. Bu nedenle bu değerlerin elde edilmesi ya da değiştirilmesi büyük önem arz etmektedir [150].

Metasploit Framework sızma testi aracında bulunan modbusclient kodunu kullanarak istismarı gerçekleştirebilmek için öncelikle gerekli parametreler girilmiştir. PLC üzerindeki veri modelinde 1-10 arasındaki adres değerler (dijital çıkışlar – coils) Resim 4.8'de görülebilmektedir.

```
msf5 auxiliary(scanner/scada/modbusclient) > set RHOSTS 192.168.1.29
RHOSTS => 192.168.1.29
msf5 auxiliary(scanner/scada/modbusclient) > set action READ_COILS
action => READ_COILS
msf5 auxiliary(scanner/scada/modbusclient) > set DATA_ADDRESS 1
DATA_ADDRESS => 1
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.29

[*] 192.168.1.29:502 - Sending READ COILS...
[+] 192.168.1.29:502 - 10 coil values from address 1 :
[+] 192.168.1.29:502 - [1, 0, 1, 0, 1, 1, 1, 0, 0, 0]
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

Resim 4.8. Dijital çıkış (coils) değerlerinin okunması

Daha sonra aynı adres aralığında yazma işlemi gerçekleştirilmiştir. Bilindiği üzere dijital çıkışlar (coils) hem okuma hem de yazma yapabildiği için gerçekleştirilen işlem başarılı olmuştur ve 1-10 adres aralığının tamamının bit bazında 1 olarak değiştirilmesi Resim 4.9'da gösterilmiştir. Gerçekleştirilen manipülasyon duruma göre tüm vanaların açılması anlamına gelebilmektedir.

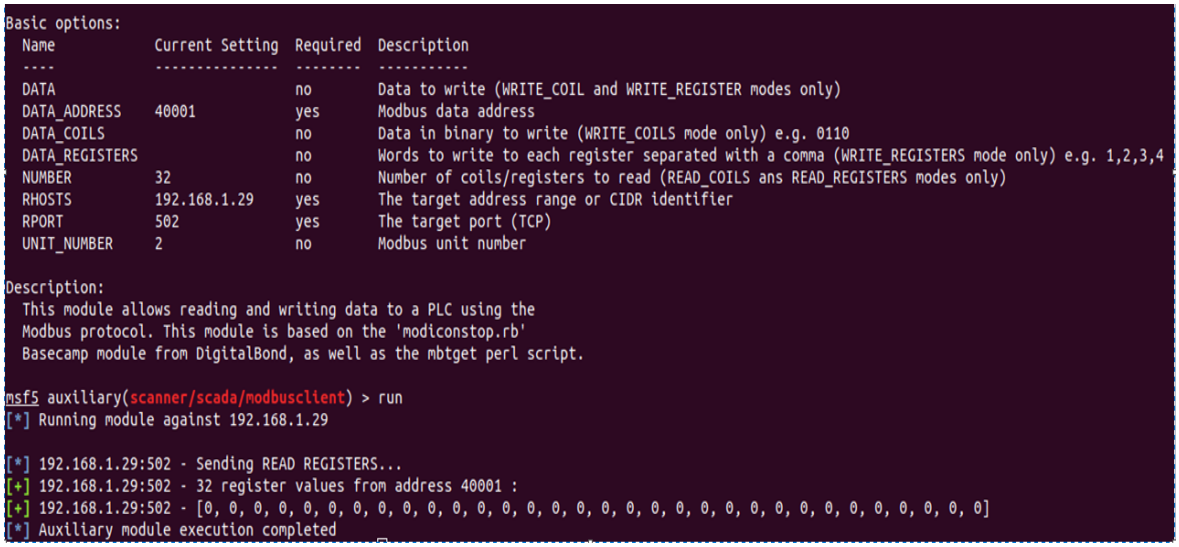
```
msf5 auxiliary(scanner/scada/modbusclient) > set DATA_COILS 1111111111
DATA_COILS => 1111111111
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.29

[*] 192.168.1.29:502 - Sending WRITE COILS...
[+] 192.168.1.29:502 - Values 1111111111 successfully written from coil address 1
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) > set action READ_COILS
action => READ_COILS
msf5 auxiliary(scanner/scada/modbusclient) > run
[*] Running module against 192.168.1.29

[*] 192.168.1.29:502 - Sending READ COILS...
[+] 192.168.1.29:502 - 10 coil values from address 1 :
[+] 192.168.1.29:502 - [1, 1, 1, 1, 1, 1, 1, 1, 1, 1]
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/scada/modbusclient) >
```

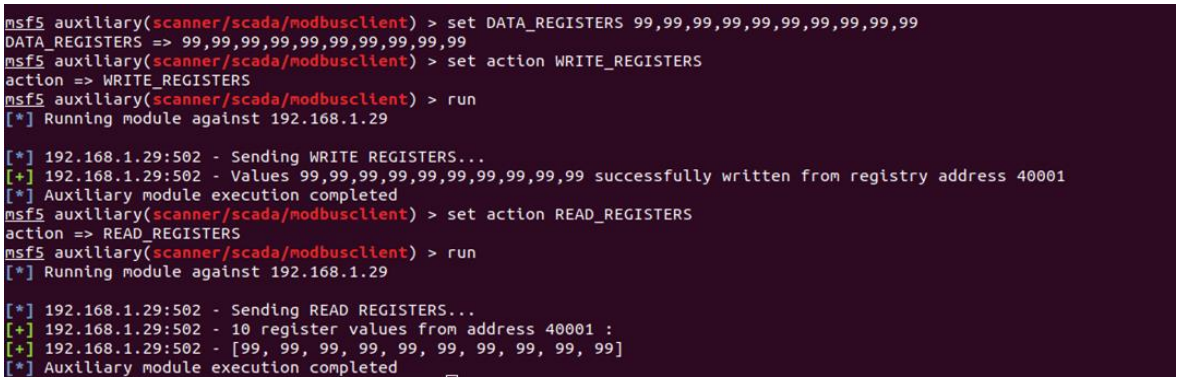
Resim 4.9. Dijital çıkış (coils) değerlerinin değiştirilmesi

Dijital çıkış değerleri değiştirildikten sonra saldırgan tarafından 30001-39999 ve 40001-49999 adres aralığında olduğu bilinen 16-bitlik yazmaç değerleri hedeflenmiştir. Yapılan denemelerden sonra 40001 adresinden başlayarak 32 saklayıcı kaydedici değeri okunmuştur ve hâlihazırda tamamına "0" değeri atandığı Resim 4.10'da görülmektedir.



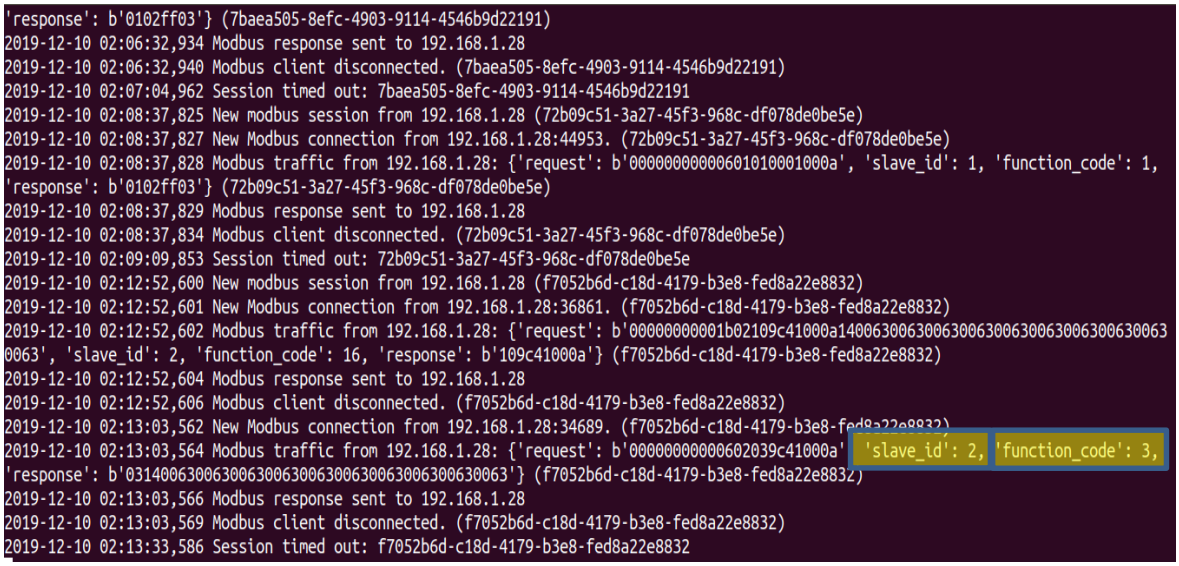
Resim 4.10. Saklayıcı kaydedici (holding registers) değerlerinin okunması

Son olarak 40001 adresinden başlayarak 10 saklayıcı kaydedici değeri "99" değeriyle değiştirilmiştir ve bu işlemin de başarılı olduğu Resim 4.11'de görülmektedir.



Resim 4.11. Saklayıcı kaydedici (holding registers) değerlerinin değiştirilmesi

Saldırganın PLC olduğunu düşünerek gerçekleştirdiği saldırı sonucu bal küpünde üretilen log kayıtları Resim 4.12'de sunulmuştur.



Resim 4.12. Saldırı sonucu Conpot uygulamasında oluşan log kayıtları

Bal küpünde üretilen log kayıtlarında Modbus protokolüne ait "slave_id" ve "function_code" değerleri, ayrıca değiştirilmesi amacıyla gönderilen değerler görülebilmektedir.

Modbus seri hat haberleşme protokolünde bir ana cihaz (master) ve sayısı 247'yi bulabilen bağımlı cihazlar (slave) yer almaktadır. Kayıt verilerinde yer alan "slave_id" bağımlı cihazı tanımlamaktadır. Böylece talebin hangi bağımlı cihaza gönderildiği görülebilmektedir.

Fonksiyon kodları ise bağımlı cihazların yapacakları ya da yaptıklarını işlemleri ifade eder. Modbus protokolünde yaygın olarak kullanılan fonksiyon kodları Çizelge 4.5'de listelenmiştir [149].

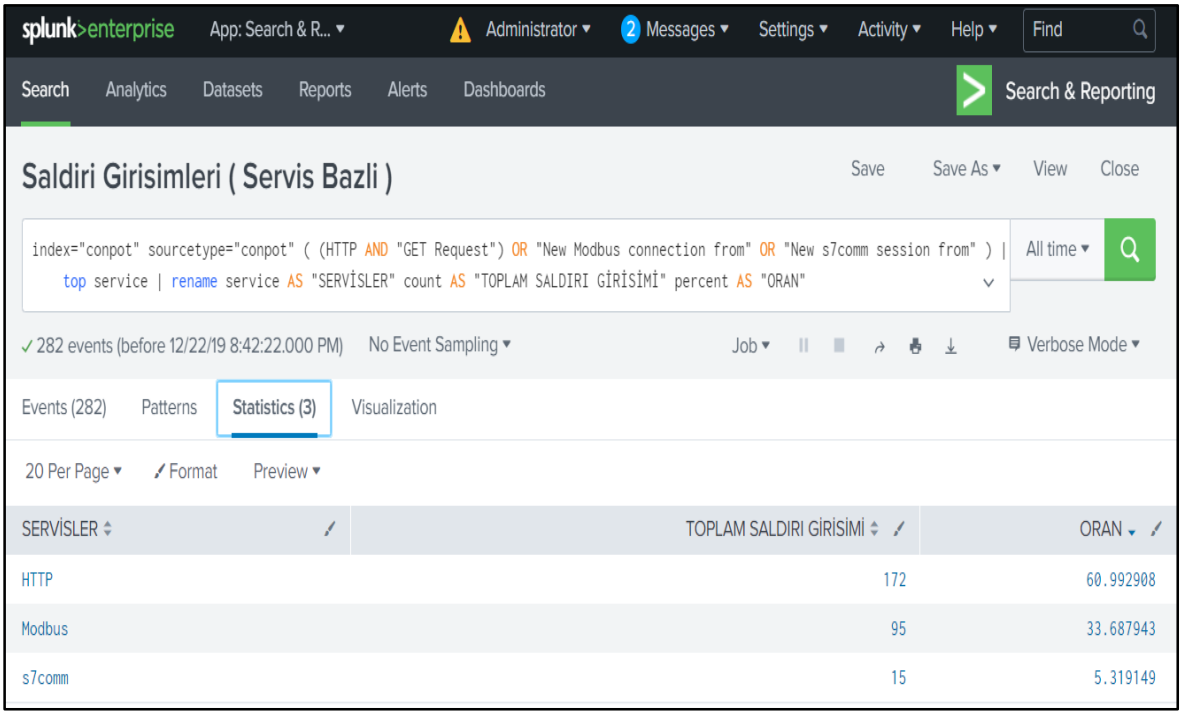
Çizelge 4.5. Modbus protokolünde yaygın olarak kullanılan fonksiyon kodları [149]

Fonksiyon Kodu	**Görevi**	**Açıklama**
01 (01 hex)	Okuma	Dijital çıkışları (bobin, coil) okuma
02 (02 hex)	Okuma	Dijital girişleri okuma
03 (03 hex)	Okuma	Saklayıcı kaydedicileri okuma
04 (04 hex)	Okuma	Giriş kaydedicilerini okuma
05 (05 hex)	Tekli Yazma	Tek bir bobine yazma
06 (06 hex)	Tekli Yazma	Tek bir tutucu kaydediciye yazma
15 (0F hex)	Çoklu Yazma	Birden fazla bobine yazma
16 (10 hex)	Çoklu Yazma	Birden fazla tutucu kaydediciye yazma

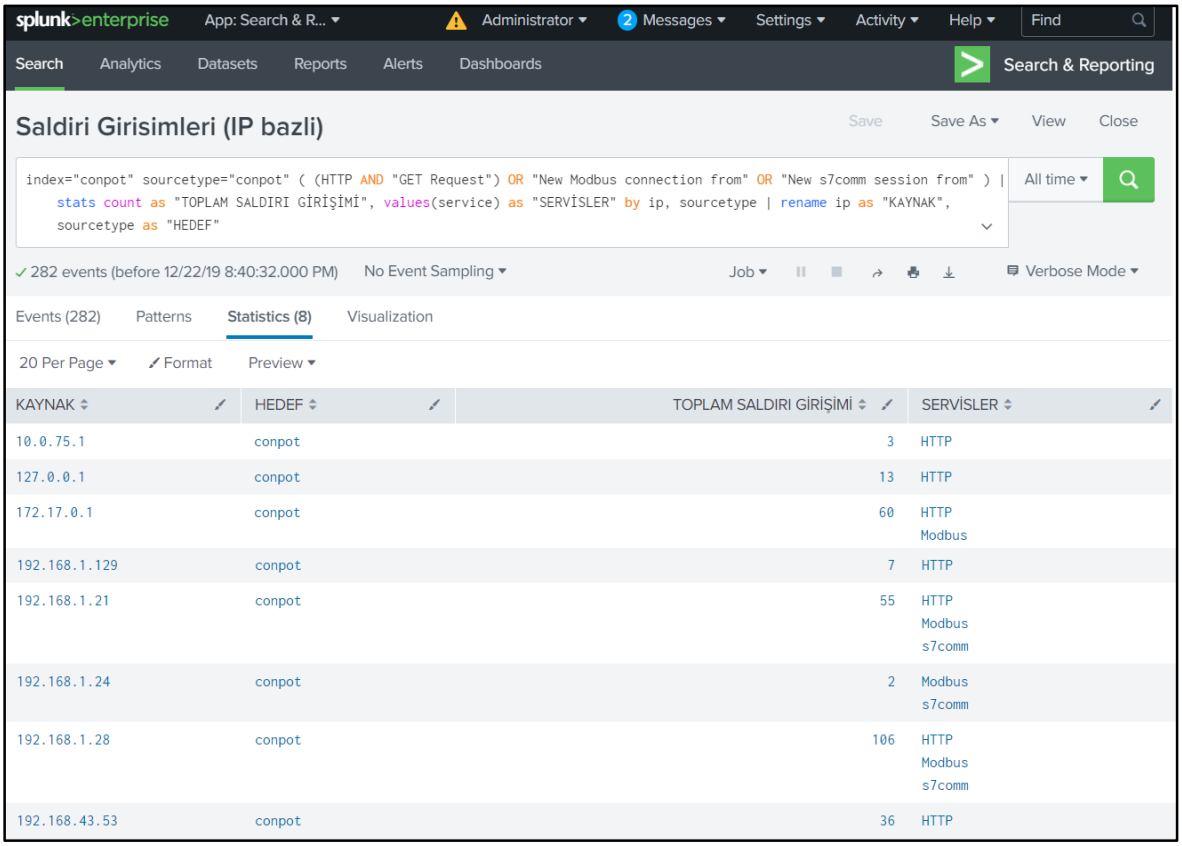
4.4. Saldırı Tespiti

İcra edilen test senaryosu dışında çeşitli kaynaklardan IP/port taramaları ya da HTTP isteklerinde bulunulmuştur. Kurum içi ağda konumlandırılan Conpot bal küpü uygulaması standart ağ trafiğine dâhil olmadığından, gelen isteklerin tamamı zararlı olarak algılanmaktadır. Splunk uygulamasına gelen log kayıtları üzerinde sorgular gerçekleştirilerek saldırı girişimleri tespit edilmiştir. En çok istek alan servisler ve her bir servis için toplam saldırı girişimi sayıları Resim 4.13'de, saldırı gerçekleştiren kaynak IP adresleri, saldırı girişimi sayısı ve hangi servise saldırı gerçekleştirdikleri Resim 4.14'de sunulmuştur. Tüm saldırı girişimleri ile alakalı ayrıntılı log kayıtlarına "Events" sekmesinden ulaşılabilmektedir.

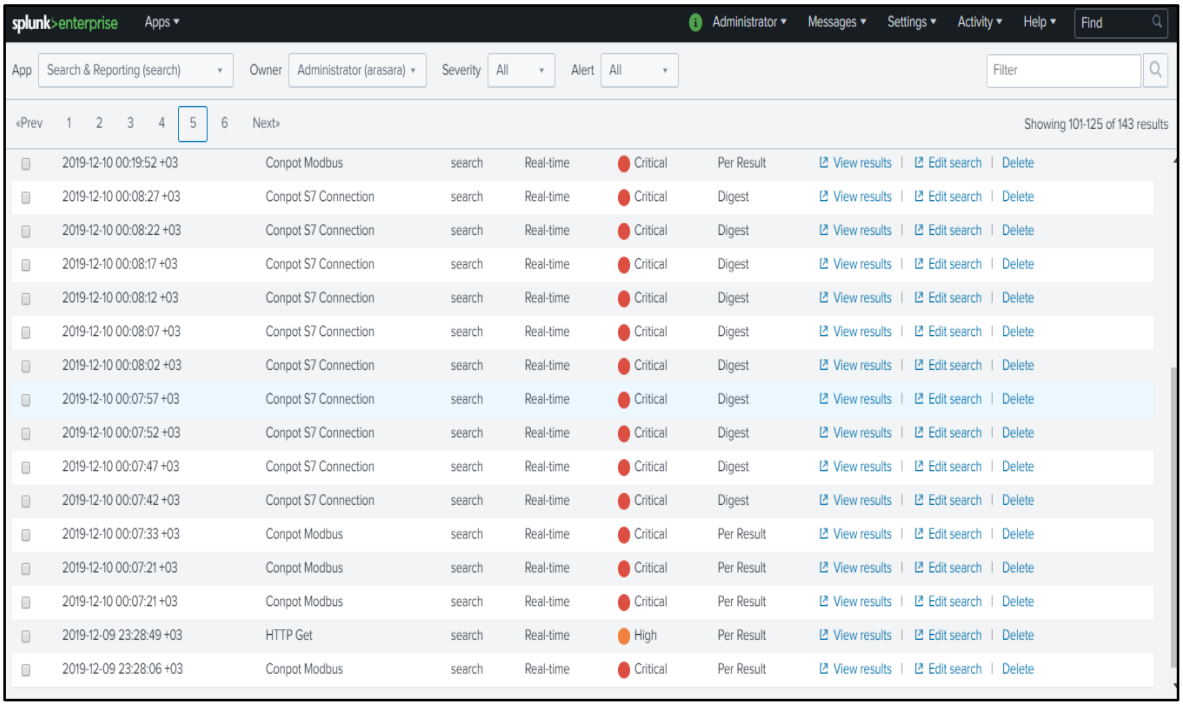
Sorgular vasıtası ile tespit edilen saldırı girişimleri için alarmlar oluşturulmuş ve her bağlantı talebi yapıldığında alarmın tetiklenmesi sağlanmıştır. Modbus ve S7comm için gelen bağlantı taleplerine yönelik alarm seviyesi "Kritik", HTTP için gelen bağlantı taleplerine yönelik alarm seviyesi ise "Yüksek" olarak belirlenmiştir. Tetiklenen alarmlar Resim 4.15'de gösterilmiştir. İsteğe bağlı olarak Splunk uygulaması tetiklenen alarm ile ilgili e-posta da gönderebilmektedir.



Resim 4.13. Servis bazlı saldırı girişimleri (istatistiksel)

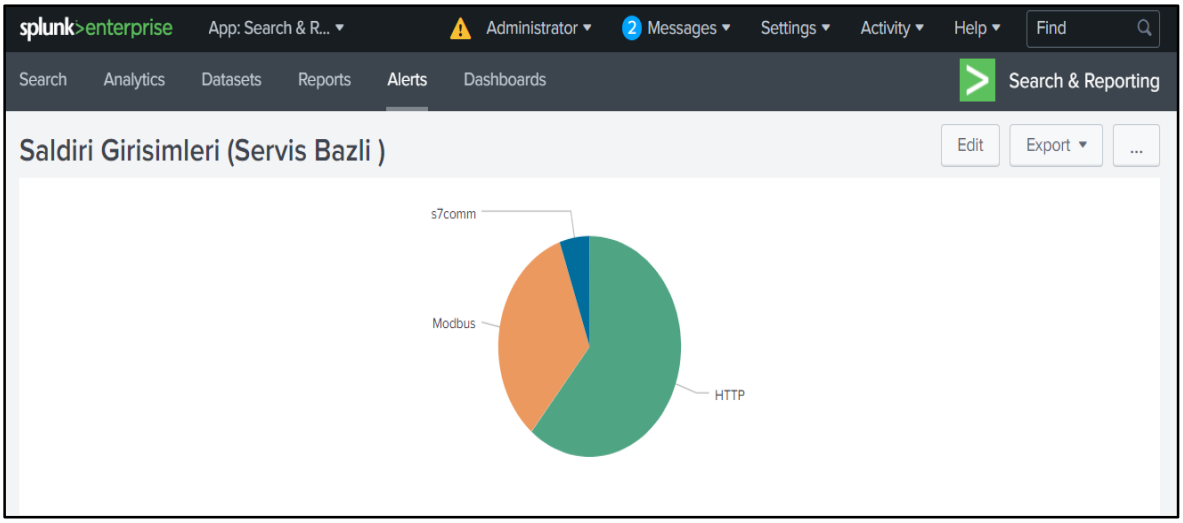


Resim 4.14. IP bazlı saldırı girişimleri (istatistiksel)



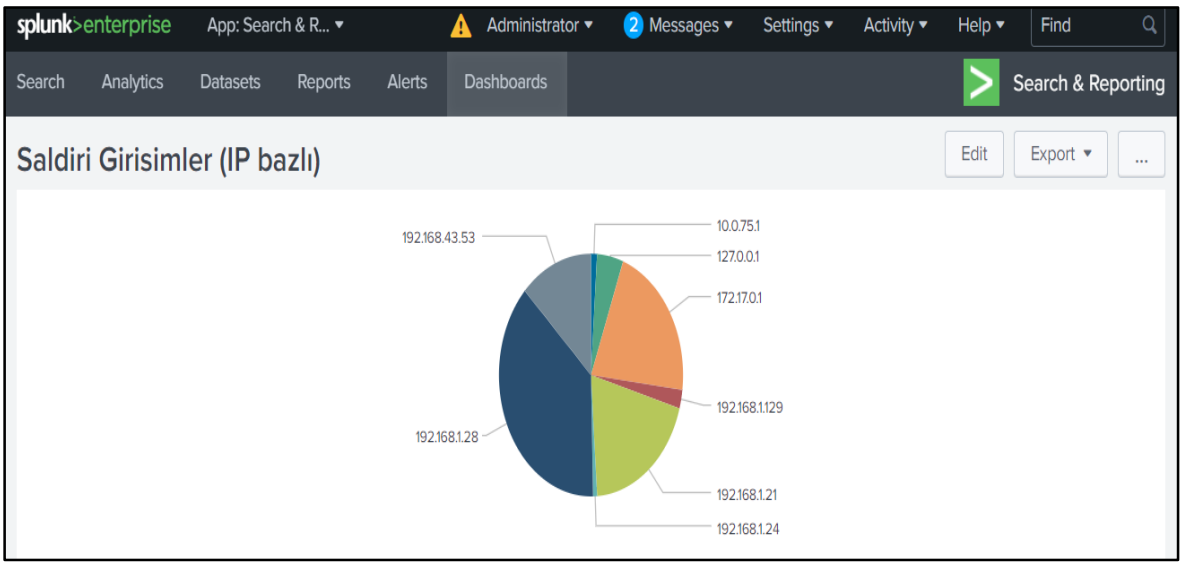
Resim 4.15. Tetiklenen alarmlar

Son olarak Splunk uygulama arayüzündeki görselleştirme özelliğinden faydalanılarak saldırı girişimlerine yönelik paneller oluşturulmuş ve bu sayede mevcut tehditlerin servis ya da kaynak IP adresi özelinde dağılımları Resim 4.16 ve Resim 4.17'de gösterilmiştir.



Resim 4.16. Servis bazlı saldırı girişimleri (grafik)

Grafiksel gösterim, elde edilen log kayıtlarını görselleştirerek anlaşılabilir hale getirmesi ve bir bakışta tehdit analizi sağlaması açısından önemli bir özelliktir. Siber güvenlik operasyon merkezlerince de istenmekte ve izlemeyi kolaylaştırmaktadır.



Resim 4.17. IP bazlı saldırı girişimleri (grafik)

4.5. Değerlendirme ve Analiz

Yapılan çalışmada bir EKS ağı içerisinde Conpot bal küpü uygulaması konumlandırılmış ve uygulamaya gelen istekler bir SIEM uygulaması olan Splunk'a gönderilerek yorumlanmış, saldırı girişimlerinin ve saldırı kaynaklarının tespiti sağlanmıştır. Ayrıntılı sorgulamalar ile istatistiki bilgiler elde edilmiş ve görselleştirme yapılarak log verileri anlaşılabilir hale getirilmiştir.

Bal küpü uygulamaları saldırıyı henüz keşif/bilgi toplama aşamasında tespit etmeyi hedeflemektedirler. 2018 yılında IBM sponsorluğunda ve bağımsız araştırma kurumu Ponemon Institute tarafından gerçekleştirilen araştırmaya göre [151], bir veri sızıntısının tespit edilebilmesi için geçen ortalama süre 197 gündür. Bu açıdan bakıldığında bal küpü uygulamasının erken tespit ve saldırıya müdahale açısından bir hayli önemli olduğu söylenebilir.

Literatürde kritik altyapılara yönelik olarak gerçekleştirilen bal küpü uygulamaları genellikle internet ortamında konumlandırılmış ve dışarıdan gelebilecek tehditlere karşı yem olarak kullanılmıştır [135,136,140-144]. Fakat kurum dışında konumlandırılan ve herkesin ulaşabileceği bir bal küpü uygulamasının birçok hatalı sonuç yaratacağı değerlendirilmektedir. Çünkü internet ortamında birçok meşru ya da meşru olmayan bot ya da örümcek (crawler) makine bulunmaktadır. Google, Shodan gibi kuruluşlara ait bu makinalar düzenli olarak internette bulunan tüm IP bloklarını tarayarak açık port ve servisleri hatta bu servislerde çalışan yazılımların versiyon bilgilerini tespit etmektedirler. Bu ve benzeri sebeplerle internet ortamında konuşlandırılmış bir bal küpüne her gelen isteğin zararlı olarak algılanması doğru görünmemektedir. Gelen isteklerin içerisinden zararlı olanları tespit edebilmek ise bir hayli zordur. Oysa iç ağda konumlandırılmış bir bal küpü uygulamasına meşru bir trafik gelme ihtimali çok daha düşüktür. Bu nedenle bal küpü hatalı sonuç üretmeyecek ya da çok az üretecektir. Bu nedenle, Conpot bal küpü uygulamasının çalışmanın gereği olarak iç ağda kullanımının gayet yerinde ve faydalı olduğu değerlendirilmektedir.

Fakat bal küpü uygulamalarının iç tehditlere karşı kullanımında dikkat edilmesi gereken bazı önemli özellikler bulunmaktadır. Öncelikler bal küpleri doğru ağda ve segmentte konumlanmalıdırlar. PLC ya da RTU cihazını temsil eden bir bal küpü SCADA sunucusu,

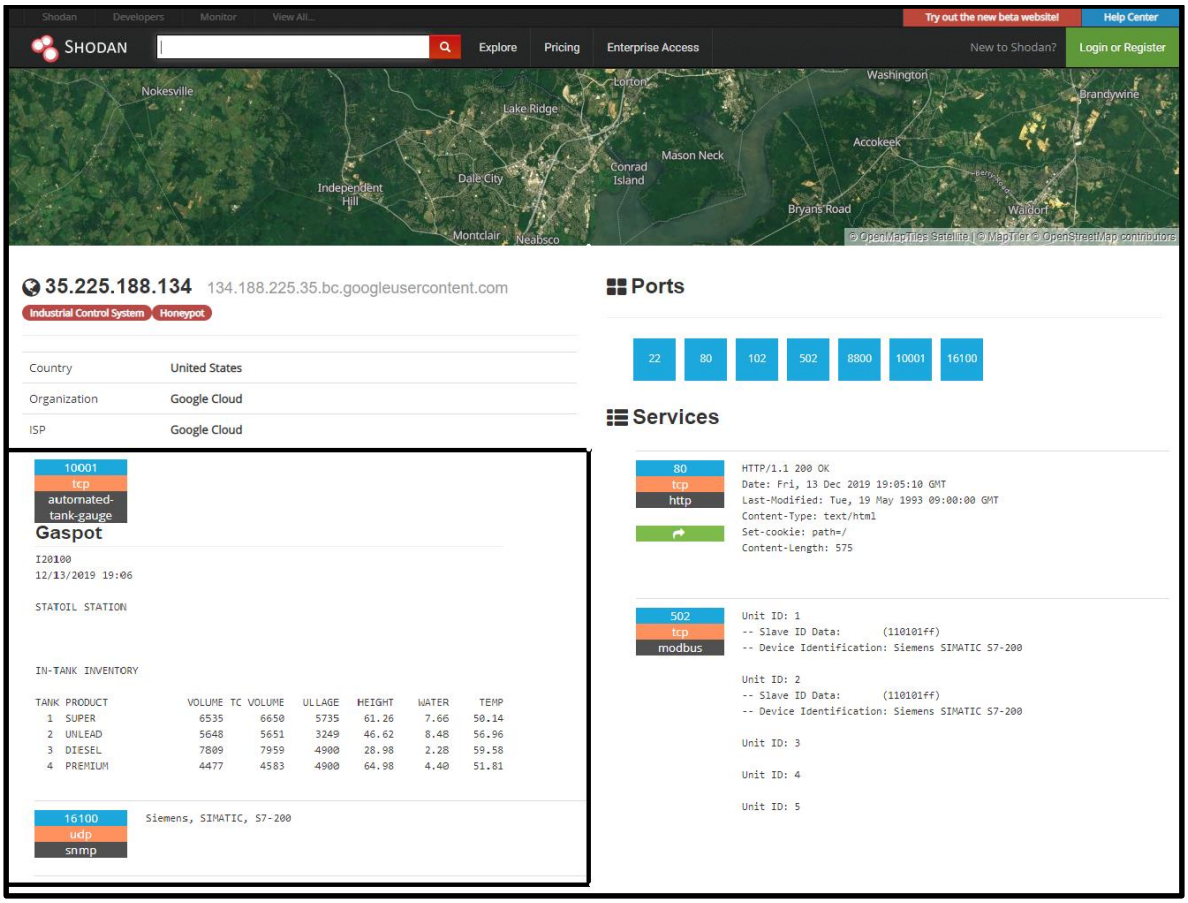
veri tarihçisi ve HMI'ların bulunduğu ağda değil yine RTU ve PLC'lerin bulunduğu ağda konumlandırılmalıdır. Bununla birlikte bal küpü saldırgan gözünden bakıldığında inandırıcı olmalı ve aynı zamanda saldırganı kendine çekebilecek açıklıkları da üzerinde barındırmalıdır.

Gerçekleştirilen IP/port taramalarında görüldüğü üzere Conpot hizmete sunduğu protokoller için ilgili portu açmaktadır. Test senaryosunda Modbus isteklerine de beklendiği şekilde cevap verdiği görülmüştür.

Conpot bal küpü uygulamasının geçerliliğini ve bir saldırganın gözünden nasıl görünebileceğini test etmek amacıyla Google Cloud Platform üzerinde Ubuntu 18.04 bir makine oluşturulmuş ve üzerine Conpot bal küpü uygulaması kurulmuştur. Harici IP ile yapılandırılarak internet üzerinden erişilebilir olması sağlanmıştır. Conpot default şablon ile çalıştırılmış ve port yönlendirme uygulanmıştır. Google Cloud Platform güvenlik duvarı ayarları kullanılarak ilgili portlara dış dünyadan gelen istekler için izin verilmiştir. Daha sonra Shodan aracı ile dış dünyada hizmete sunulan bal küpü uygulamasına isteğe bağlı tarama işlemi gerçekleştirilmiştir. Sonuç olarak Shodan üzerinde de gerekli portların açık olduğu, endüstriyel kontrol sistemi olarak tanımlandığı ve hizmete sunulan servis bilgilerinde "Siemens SIMATIC S7-200" ibaresi görülmüştür. Ancak birden fazla EKS protokolünü aynı IP üzerinden hizmete sunduğundan ve PLC bilgilerinde yer alan "Mouser Factory, Technodrome" gibi hazır bilgiler nedeniyle bal küpü olduğu anlaşılmıştır. Shodan port taraması sonucu Resim 4.18'de gösterilmiştir.

Conpot düşük-etkileşimli bir bal küpü uygulaması için Modbus ve S7comm gibi EKS protokollerini gerçekçi olarak taklit edebilmektedir. Bu yönüyle teknik kapasitesi düşük bir saldırgan için yeterli gelebilmektedir. Ancak teknik kapasitesi daha yüksek bir saldırgan için şablonlar ve PLC'ye ait bilgiler kuruma uygun hale getirilmelidir. Ayrıca kurumda hizmet veren servislerin dışında bir servis Conpot bal küpü uygulaması üzerinde açık bırakılmamalıdır.

Sonuç olarak; bal küpü uygulamalarının kritik altyapılarda, endüstriyel kontrol sistemleri özelinde iç ağa yönelik olarak kullanılması iç tehdit kaynaklı saldırıların tespitinde fayda sağlayacağı değerlendirilmektedir. Bu maksatla bal küpünün kuruma özel olarak uyarlanması ve mutlaka bir SIEM ürünü ile beraber kullanılması önem arz etmektedir.



Resim 4.18. Shodan port taraması sonucu

Conpot bal küpü uygulamasının açık kaynaklı olması uyarlanabilirlik açısından gerekli esnekliği sağlamaktadır. Ayrıca, mevcut cihaz ve sistemler üzerinde fazladan yük de getirmemesinden dolayı, bal küpü uygulamalarının SCADA/EKS gibi zaman-kritik sistemler için uygun olduğu saptanmıştır. Gelecek çalışmalara yönelik olarak; bal küpü log kayıtlarını yorumlamakta kullanılan SIEM sitemlerine SCADA/EKS ağında bulunan diğer sunucu ve güvenlik ürünlerine (SCADA sunucusu, veri tarihçisi, HMI vb.) ait log kayıtları da eklenerek korelasyon kuralları ile daha doğru ve geçerli sonuçlar elde edilebileceği değerlendirilmektedir.

5. SONUÇ VE ÖNERİLER

Kritik altyapılar kapsamına giren tüm hizmetler ve işletilen süreçler; anlık takip ve kontrol, otomasyon ve merkezi kontrol, kolay müdahale, zaman ve kaynak tasarrufu gibi sebeplerle zamanla dijital altyapıya geçiş yapmışlardır. Birçok sektör, bilişim sistemlerini belirtilen amaçlar doğrultusunda bir araç olarak kullanırken telekomünikasyon gibi bazı sektörler ise tamamen bilişim sisteminden oluşmaktadırlar. Kritik altyapı bilişim sistemlerinin geçmişte kapalı bir yapıda olmaları ve zaman-kritik sistemler olmalarından ötürü öncelikle süreçlerin aksamadan yürütülebilmesine yönelik tasarlanmışlardır. Bu nedenle güvenlik hususu ikinci planda kalmış hatta bazen hiç düşünülmemiştir. Fakat Stuxnet vakası, kapalı sistemlerin de güvenli olmadığını göstermesi açısından tüm dünya için bir dönüm noktası olmuştur. Dahası çeşitli kritik altyapı sektörleri coğrafi olarak dağıtık yerleşkelerini birbiriyle haberleştirebilmek için geniş alanı ve internet altyapısını kullanmaya başlamışlardır. Bu hususlar güvenlik zafiyetlerini ve ülkelerin bu konudaki çekincelerini daha da artırmıştır. Nitekim yıllar geçtikçe kritik altyapılara yönelen siber saldırıların sayısında ve yarattığı etkide meydan gelen artış hassasiyetlerin ne kadar yerinde olduğunu ispatlamıştır. Bu sebeple ABD'nin öncülüğünde birçok devlet zamanla kritik altyapıların bilişim sistemleri güvenliği ve siber saldırılardan korunmasına yönelik yasal mevzuat oluşturmuş, siber güvenliğin sağlanmasına ve kritik altyapı sektörlerinin bu konuda denetlenmesine yönelik kurumlar oluşturmuşlardır. Türkiye'de de kritik altyapıların savunması ve güvenliğine yönelik bir kurumun oluşturulmasının bu konudaki çabaların ortak bir merkezden koordine edilmesi açısından faydalı olacağı değerlendirilmektedir.

Kritik altyapı sektörlerine yönelik olsun ya da olmasın meydana gelen siber saldırıların yalnızca dışarıdan gelebileceği ile ilgili genel bir yanlış kanı bulunmaktadır. Bu durum kurum ve kuruluşların gerçekleştirdiği siber güvenlik yatırımlarının büyük bölümünün dışarıya karşı olmasından net bir şekilde anlaşılabilmektedir. Oysa ister kötü niyetli ister dikkatsiz ve bilgisiz kullanıcı kaynaklı olsun içeriden gelebilecek tehditlerin firma, kurum ve kuruluşlarda yol açtığı maddi ve manevi kayıp çok fazladır. Ayrıca sosyal mühendislik ve gelişmiş ısrarcı tehdit gruplarının taktik ve yöntemleri iç tehditlerin siber saldırılardaki yerini her geçen gün artırmaktadır. Çünkü dışarıdan bir siber saldırıda bulunmak yerine kurum içinden bir kişinin kullanılması önemli bazı avantajlara sahiptir. İçeriden bir kişi hem fiziksel hem de mantıksal olarak zaten meşru erişim yetkisine sahiptir. Dolayısıyla

siber saldırganlar keşif yapmaya, sızma girişiminde bulunmaya ya da güvenlik tedbirlerini atlatmaya ihtiyaç duymayacaktır. Kısacası iç tehditler, siber saldırganlara engelleri aşmaya çalışmak yerine engelin etrafından dolaşma imkânı tanımaktadır. Hatta ayrıcalıklı erişim yetkisine sahip bir iç tehdide ulaşılması durumunda hak yükseltme saldırısında bulunulmasına da ihtiyaç kalmayacaktır. Bu kişi kurumun kritik varlıkları ve kurumun işleyişini de bilmektedir. Dolayısıyla saldırganların sömüreceği ve çıkar sağlayacağı noktalar konusunda da doğrudan bilgi sahibidir. Kurumun iç dinamiklerini bilmek sadece ne zaman nereye saldırılacağı konusunda yardımcı olmaktan öte siber saldırıların izlerinin nasıl daha iyi silinebileceği ve çeşitli güvenlik tedbirlerinden nasıl kaçınılacağı konusunda da yardımcı olmaktadır. En önemlisi iç kaynaklı bir siber tehdidi keşfetmek, dışarıdan gelebilecek bir saldırıya karşı çok daha zordur. Tüm bu hususlar iç tehditleri siber saldırganlar için mükemmel bir araç konumuna getiriken kurum için de savunulması en zor tehditlerden biri yapmaktadır.

Kritik altyapılar zaten siber saldırganlar için önemli bir hedef durumundadır. Sekteye uğraması ya da hiç işlememesinin ülkeye büyük ekonomik zararlar hatta can kaybına sebep verebilecek olması hassasiyeti, iç tehdidin yıkıcı etksisiyle birleştiğinde, iç tehdidin kritik altyapılarda savunulması gerekliliği hayati öneme haiz olmaktadır. İnsan kaynaklı bir zafiyet olması sebebiyle iç tehdidin yalnızca teknik önlemlerle engellenebiliyor olması mümkün değildir. Bu nedenle iç tehdide yönelik olarak sosyal, teknik ve sosyo-teknik önlemlerin bir arada kullanılması zorunludur. Bu yüzden kurumların insan kaynakları, hukuk müşavirliği, fiziki güvenlik ve bilgi teknolojilerinden sorumlu birimlerinin birlikte çalışmaları gerekmektedir. Sosyal önlemlerde güvenlik soruşturması, arşiv araştırması, kişilik testleri ve çalışan hakları gibi hususlar yer almaktadır. Kritik altyapılarda iç tehdidin azaltılması özelinde rehber, prosedür ve idari tedbirlerin bulunması ve uygulanması da sosyo-teknik önlemler açısından sıralanabilir. Bilişim sistemlerinde rafta hazır ya da özel güvenlik ürünlerin kullanılması teknik önlemlere dâhildir. Çalışmanın konusu gereği bu çalışmada teknik önlemlere yönelik bir çözüm sunulmuştur.

Yapılan çalışmada iç tehditlerin bilindiği kadarıyla en çok kullanılan türü olan maskeli iç tehditler hedeflenmiştir. Maskeli iç tehdit, meşru bir kullanıcının kimliğini çalmayı başarabilen ve kötü niyetli amaçlar için başka bir kullanıcının "kılığına bürünen" bir saldırgandır. İçeriden bir kişinin erişim yetkisini ele geçirmenin yanında, kurumun iç yapısı hakkında bilgiye sahip değildir. Siber ölüm zincirinin adımlarını gerçekleştirmek zorunda

olsa bile, büyük ihtimalle tespit edilmeden bilişim sitemi üzerindeki faaliyetlerini gerçekleştirebilecektir. Çünkü içeriden bir kullanıcının yarattığı anomaliteyi, normal kullanıcı davranışından ayırt edebilmek bir hayli güçtür. Bunu aşabilmek maksadıyla iç tehdidin bir kritik altyapı bilişim sisteminde keşfedilmesine yönelik olarak açık kaynak bir bal küpü uygulaması kullanılmıştır. Bilindiği üzere balküpleri, üzerlerinde bulundurdukları açıklıklarla saldırganları kendine çeken tuzak sistemlerdir. Conpot bal küpü uygulaması, yaygın kullanılan endüstriyel kontrol sitemleri protokollerini barındırmakta ve saldırganın gözünden bir PLC gibi görünmektedir. Uygulama içinde PLC'ye ait şablon dosyasında yapılan değişikliklerle saldırganın gözünden daha gerçekçi ve inandırıcı görünmesi sağlanmıştır. Uygulama tüm erişim talepleri için log kaydı oluşturmaktadır. İzleme ve takip hususunu kolaylaştırmak ve geliştirmek amacıyla bir SIEM uygulaması olan Splunk aracı kullanılmıştır. Conpot uygulamasından alınan log kayıtları Spunk üzerinde görüntülenerek bal küpüne gelebilecek bağlantı girişimleri izlenmiştir. Bir test senaryosu ile sistemin tespit yeteneği test edilmiş, gerçekleştirilen tarama ve saldırılar gözlemlenmiştir. Splunk üzerinde detaylı sorgu cümlecikleri yazılarak saldırı gerçekleştirilen servis ve kaynak IP gibi muhtemel saldırgana yönelik bilgiler ayrıntılı olarak listelenmiş, ayrıca grafikler oluşturularak iç ağda görünürlük artırılmış ve görsellik kazandırılmıştır.

Kritik altyapıların siber güvenliğine yönelik yapılmış çalışmalarda literatürde bal küpünü kullanan çalışmalar bulunmaktadır. Gerçekleştirilen çalışmada mevcut çalışmalardan farklı olarak bal küpü iç ağda konumlandırılarak daha sağlıklı sonuçlar elde edilmiştir. Önceki çalışmalarda balküpleri dış ağda ve internet ortamında konumlandıklarından meşru ya da meşru olmayan tüm bot ve örümceklerin taramalarına da açıktırlar. Shodan benzeri birçok sistem interneti düzenli aralıklarla taramakta, bulduğu IP'ler üzerinde çalışan servisleri, versiyon bilgisini ve mevcut versiyona yönelik açıklıkları listeleyebilmektedir. Bu durumun gerçek saldırganın tespitine yönelik olarak birçok I. tip hata (false-pozitive) meydana getireceği değerlendirilmektedir. Oysa iç ağda konumlandırılmış bir bal küpüne kötü niyetli olmayan bir girişimde bulunulması ihtimali çok daha zayıftır. Dolayısıyla gelen trafiğin tamamı zararlı olarak nitelenebilmektedir.

Bununla birlikte özellikle EKS'nde kullanılacak güvenlik ürünleri PLC ya da RTU gibi cihazlara fazladan trafik yükü bindirmemelidir. Çünkü EKS/SCADA sistemleri zaman açısından hassas sistemlerdir ve bu cihazlara gelebilecek ekstra yük sistemin kararsız

çalışmasına hatta devre dışı kalmasına sebep olabilmektedir. Bu açıdan bal küpü sistemleri EKS/SCADA sistemleri açısından kullanışlı ve uygun bir güvenlik tedbiridir.

Bal küpü sistemlerinin en önemli özelliği keşif aşamasında saldırıyı tespit etmesidir. İç tehdit vakalarının sadece %16'sının ilk 30 gün içinde tespit edilebildiği göz önünde bulundurulduğunda saldırı henüz gerçekleşmeden tespit edebilmek büyük avantaj sağlayacaktır. Bu açıdan bakıldığında bal küpü sisteminin kullanımı savunma gücü açısından hayli getiri sağlamaktadır.

Çalışmanın en önemli sınrlılığı kritik altyapılarda iç tehdide yönelik gerçek verinin özellikle de trafik verisinin bulunmamasından kaynaklıdır. Yapılan araştırmalar sonucunda ulaşılabilen trafik verisi de suni ortamda üretilmiş veridir. Gelecek çalışmalara yönelik olarak, endüstriyel kontrol sistemi içerisindeki diğer sunuculardan (SCADA sunucu, etki alanı sunucusu, veri tarihçisi vb.) alınan log kayıtlarının da SIEM üzerinde bal küpünden gelen veriyle eşleştirilerek daha doğru ve sağlıklı sonuçlar elde edilebileceği değerlendirilmektedir.

KAYNAKLAR

1. Bologna,S., Fasani, A. And Martellini M. (2013). Cyber Security and Resilience of Industrontrol Systems and Critical Infrastructures, In: Martellini M. (eds) *Cyber Security*. Springer Briefs in Computer Science. Springer, Cham.

2. Verizon (2019). 2019 Data Breach Investigations Report.

3. Ponemon Institute (2018). 2018 Cost of Insider Threats: Global, *Research Report.*

4. İnternet: Insider Threat Statistics for 2019: Facts and Figures. URL: https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures Son Erişim Tarihi: 17 Aralık 2019.

5. İnternet: Marriott Hack Hits 500 million Starwood Guests. URL: https://www.bbc.com/news/technology-46401890 Son Erişim Tarihi: 17 Aralık 2019.

6. İnternet: Tesla Accuses Insider of Stealing Gigabytes of Data. URL: https://www.bankinfosecurity.com/tesla-lawsuit-alleges-insider-stole-gigabytes-data-a-11118 Son Erişim Tarihi: 17 Aralık 2019.

7. İnternet: Mitigating the Insider Threat: Lessons From PNB Fraud Case URL: https://www.bankinfosecurity.com/mitigating-insider-threat-lessons-from-indian-fraud-case-a-10674 Son Erişim Tarihi: 17 Aralık 2019.

8. İnternet: SunTrust said employee worked with outside criminal when info on 1.5M clients was breached URL: https://www.usatoday.com/story/tech/2018/04/20/many-1-5-million-accounts-may-have-been-compromised-suntrust-banks/535687002/ Son Erişim Tarihi: 18 Aralık 2019.

9. İnternet: Pakistani Man Bribed AT&T Insiders to Plant Malware and Unlock 2 Million Phones. URL: https://amp.thehackernews.com/thn/2019/08/sim-device-unlocking-malware.html?__twitter_impression=true Son Erişim Tarihi: 18 Aralık 2019.

10. İnternet: WRIT 2018. URL: https://www.ieee-security.org/TC/SPW2018/WRIT/ Son Erişim Tarihi: 20 Aralık 2019.

11. İnternet: Insider Threat Mitigation. URL: https://www.cisa.gov/insider-threat-mitigation Son Erişim Tarihi: 24 Aralık 2019.

12. Liu, L., Vel, O., Han Q. and Xiang Y. (2018). Detecting and Preventing Cyber Insider Threats: A Survey. *IEEE Communications Survey & Tutorials*, 20(2), 1397-1417.

13. CERT National Insider Threat Center (2018). Common Sense Guide to Mitigating Insider Threats, Sixth Edition. *Technical Report, CMU/SEI-2018-TR010*. Software Engineering Institute, Carnegie Mellon University.

14. Hunker, J. and Probst, C.W. (2011). Insiders and insider threats - An overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*. Vol. 2, 4-27.

15. Glasser, J. and Lindauer B. (2013). Bridging the gap: A pragmatic approach to generating insider threat data, *IEEE Security and Privacy Workshops*, 98-104.

16. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı.

17. İnternet: Infrastructure Security. URL: https://www.dhs.gov/topic/critical-infrastructure-security Son Erişim Tarihi: 25 Temmuz 2019.

18. İnternet: Critical Infrastructure. URL: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en Son Erişim Tarihi: 25 Temmuz 2019.

19. Mansfield-Devine, S. (2017). Going Critical: Attacks against National Infrastructure, *Network Security*, 2017(11), 16.

20. United States and Obama, B. (2012). Presidential Policy Directive-21: Critical Infrastructure Security and Resilience. Washington: U.S. G.P.O.

21. Comission of the European Communities (2005). Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final, 6-7.

22. İnternet: Closing the IT and OT Security Gap Will Drive US$125 Billion Critical Infrastructure Security Spending by 2023. URL: https://www.abiresearch.com/press/closing-it-and-ot-security-gap-will-drive-us125-billion-critical-infrastructure-security-spending-2023/ Son Erişim Tarihi: 27 Temmuz 2019.

23. Karabacak B. (2011). Kritik Bilgi Altyapıları ve Siber Güvenlik, *Siber Güvenlik Konferansı*, Bilişim Sistemleri Güvenliği Bölümü, 9.

24. TÜBİTAK (2012). Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı, 7.

25. İnternet: OT, ICS, SCADA – What's the difference? URL: https://www.kuppingercole.com/blog/williamson/ot-ics-scada-whats-the-difference Son Erişim Tarihi: 28 Temmuz 2019.

26. İnternet: Bilgi Teknolojileri ve Operasyonel Teknolojiler Arasındaki Farklar. URL: http://ozdenercin.com/2018/10/22/bilgi-teknolojileri-ve-operasyonel-teknolojiler-arasindaki-farklar/ Son Erişim Tarihi: 29 Temmuz 2019.

27. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., and Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security, *NIST*, NIST.SP.800-82r2, 2-5 - 2-7.

28. İnternet: IT and OT convergence - two worlds converging in Industrial IoT. URL: https://www.i-scoop.eu/internet-of-things-guide/industrial-internet-things-it-ot/ Son Erişim Tarihi: 02 Eylül 2019.

29. İnternet: IT / OT Yakınlaşması. IT nedir? OT nedir? URL: https://otomasyonadair.com/2016/07/13/it-ot-yakinlasmasi-it-nedir-ot-nedir/ Son Erişim Tarihi: 11 Eylül 2019.

30. Vavra, J. and Hromada, M. (2015). An Evaluation of Cyber Threats to Industrial Control Systems, *International Conference on Military Technologies*, 369-373.

31. Zhu, B., Anthony, J. and Sastry S. (2011). A Taxonomy of Cyber Attacks on SCADA Systems, *2011 IEEE Internatıonal Conferences on IoT, and Cyber, Physical and Social Computing*, 380-386.

32. İnternet: Information Technologies (IT) vs Operational Technologies (OT). URL: https://randed.com/information-technologies-it-vs-operational-technologies-ot/?lang=en Son Erişim Tarihi: 13 Eylül 2019.

33. Sajid, N., Patel, S. and Patel, D. (2017). Assessing and Augmenting SCADA Cyber Security - A Survey of Techniques. *Computers & Security*, Vol. 70, 436-454.

34. Exec. Order No. 13010, 3 C.F.R. 37345 (July 15, 1996).

35. President's Comission on Critical Infrastructure Protection (1997). Critical Foundations Protecting America's Infrastructure, *Report of the PCCIP*, Washington, 1-99.

36. Presidential Decision Directive 63, Protecting America's Critical Infrastructure (1998).

37. Exec. Order No. 13636, 3 C.F.R. 11739 (February 12, 2013).

38. Moteff J.D. (2015). Critical Infrastructures: Background, Policy, and Implementation. *CRS Report*, RL30153, Washington DC, 3-35.

39. Krassnig C. (2011). European Programme on Critical Infrastructure Protection (EPCIP), *1st International Workshop on Regional Critical Infrastructures Protection Programmes*, Milan, 1-16.

40. Comission of the European Communities (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final, 1-13.

41. The Council of the European Union (2008). Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. *Official Journal of the European Union*, 345/75-82.

42. European Comission (2012). Comission Staff Working Document on the Review of the European Programme on Critical Infrastructure Protection, Brussels.

43. European Comission (2013). Comission Staff Working Document on a new approach to the European Programme on Critical Infrastructure Protection Making European Critical Infrastructures More Secure, Brussels, 1-17.

44. Kuczynski M. (2018). European Programme on Critical Infrastructure Protection (EPCIP), 11th Meeting of the Community of Users. Brussels, 1-21.

45. Karabacak B. (2011). Kritik Altyapılar: Dünya ve Türkiye Özeti, *BİLGEM*, 3(5), 29.

46. T.C. Başbakanlık Afet ve Acil Durum Yönetimi Başkanlığı (2014). Kritik Altyapıların Korunması Yol Haritası. Eylül, 2014, 11.

47. T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi, 1-20.

48. Enerji Piyasası Düzenleme Kurumu (2017). Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği. *Resmi Gazete,* Sayı:30123, 1-4.

49. Enerji Piyasası Düzenleme Kurumu (2019). Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde İçin Güvenlik Analiz ve Test Usül ve Esasları. *Resmi Gazete,* Sayı:30763, 1-11.

50. Cumhurbaşkanlığı (2019). Bilgi ve İletişim Güvenliği Tedbirleri, Resmi Gazete Sayı:30823, Genelge 2019/12, 1-2.

51. Türkiye Cumhuriyeti Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı (2019). On Birinci Kalkınma Planı (2019-2023), 116-121.

52. Barrett, M.P. (2018). Framework for Improving Critical Infrastructure Cybersecurity, version 1.1, Technical Repot, *NIST*, CSWP.04162018.

53. İnternet: NIST Releases Update Cybersecurity Framework. URL: https://digitalguardian.com/blog/nist-releases-update-cybersecurity-framework Son Erişim Tarihi: 22 Ekim 2019.

54. İnternet: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. URL: https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/ Son Erişim Tarihi: 25 Ekim 2019.

55. İnternet: NIST Roadmap for Improving Critical Infrastructure Cybersecurity, version 1.1. URL: https://www.nist.gov/system/files/documents/2019/04/25/csf-roadmap-1.1-final-042519.pdf Son Erişim Tarihi: 30 Ekim 2019.

56. Cleveland, F. (2012). IEC TC57 WG15: IEC 62351 Security Standards fort he Power System Information Infrastructure, IEC, 1-34.

57. İnternet: IEC 62351 URL: https://en.wikipedia.org/wiki/IEC_62351 Son Erişim Tarihi: 30 Ekim 2019.

58. İnternet: CIP Standards URL: https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx Son Erişim Tarihi: 01 Karsım 2019.

59. İnternet: What you need to know about NERC CIP Cybersecurity? URL: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/what-you-need-to-know-about-nerc-cip-cybersecurity-standards/ Son Erişim Tarihi: 01 Karsım 2019.

60. Enerji Piyasası Düzenleme Kurumu (2017). Enerji Sektöründe EKS Güvenlik Kontrolleri v1.0, *EPDK,* 4-70.

61. Noonan, T. and Archuleta, E. (2008). Final Report and Recommendations: The Insider Threat to National Infrastructures, NIAC, 11.

62. Predd, J., Pfleeger, S. L., Hunker, J. and Bulford, C. (2008). Insiders behaving badly, *IEEE Security and Privacy*, Vol. 6, 66–70.

63. Bishop, M., Engle, S., Peisert, S., Whalen, S. and Gates C. (2009). Case studies of an insider framework. *Proc. of the 42nd Hawaii International Conference on System Sciences (HICSS'09), Hawaii, USA*, IEEE, 1–10.

64. Salem, M.B., Hershkop, S. and Stolfo, S.J. (2008). A Survey of Insider Attack Detection Research. In: S.J. Stolfo, S.M. Bellovin, A.D. Keromytis, S. Hershkop, S. Smith and S. Sinclair (eds) *Insider Attack and Cyber Security: Beyond the Hacker*, Springer 2008, 69-90.

65. Colwill C. (2009). Human Factors in Information Security: The Insider Threat – Who can you trust these days?, *Information Security Technical Report*, 14, 186-196.

66. Shaw, E., Post, J. and Ruby, K. (1999). Inside the Mind of the Insider. *Security Management Magazine*.

67. Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T. and Rogers, S. (2005). Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors. US Secret Service and CERT Coordination Center, *Special Report*, Software Engineering Institute, Carnegie Mellon University, 1-67.

68. İnternet: Top 15 Cyber Threats in 2018. URL: https://etl.enisa.europa.eu/#/ Son Erişim Tarihi: 14 Eylül 2019.

69. Internet: Beware the Insider. URL: http://www.silicon.com/management/cio-insights/2008/04/17/beware-the-insider-security-threat-39188671/ Son Erişim Tarihi: 25 Eylül 2019.

70. Department for Business Enterprise and Regulatory Reform (2008). Information Security Breaches Survey, *BERR Technical Report*, UK, 3.

71. Internet:. State of Cybercrime: Security Events Decline But not the Impact. URL: https://www.csoonline.com/article/3211491/secu-rity/state-of-cybercrime-2017-security-events-decline-but-not-the-impact.html Son Erişim Tarihi: 25 Eylül 2019.

72. McAfee (2015). Grand Theft Data, Data exfiltration study: Actors, tactics, and detection. *Report*, McAffee, 1-13.

73. Cybersecurity Insiders (2019). 2019 Insider Threat Report, *Nucleus Cyber*, 2019, 1-21.

74. Kont, M., Pihelgas, M., Wojtkowiak, J., Thinberg, L. And Osula A. (2015). Insider Threat Detection Study, *NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)*, Talinn, Estonia, 9-10.

75. İnternet: The Real Story of Stuxnet. URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet Son Erişim Tarihi: 02 Ekim 2019.

76. İnternet: The Snowden Saga: A Shadowland of Secrets and Light. URL: http://www.vanityfair.com/news/politics/2014/05/edward-snowden-politicsinterview Son Erişim Tarihi: 02 Ekim 2019.

77. İnternet: Who is Bradley Manning. URL: http://www.washingtonpost.com/lifestyle/magazine/who-is-wikileaks-suspect-bradleymanning/2011/04/16/AFMwBmrF_print.html Son Erişim Tarihi: 02 Ekim 2019.

78. İnternet: Manning-Lame chat logs revealed. URL: http://www.wired.com/2011/07/manning-lamo-logs/ Son Erişim Tarihi: 05 Ekim 2019.

79. İnternet: Daniel Ellsberg, Biography. URL: http://www.biography.com/people/daniel-ellsberg-17176398 Son Erişim Tarihi: 06 Ekim 2019.

80. İnternet: Extended biography. URL: http://www.ellsberg.net/bio/extendedbiography Son Erişim Tarihi: 06 Ekim 2019.

81. İnternet: The case of Herman Simm. URL: http://vm.ee/sites/default/files/content-editors/web-static/319/Herman_Simm.pdf Son Erişim Tarihi: 10 Ekim 2019.

82. İnternet: Judicial Decisions. URL: https://www.kapo.ee/eng/judicial-decisions.html Son Erişim Tarihi: 12 Ekim 2019.

83. İnternet: Profile of Major Nidal Malik Hasan. URL: http://www.homelandsecurityus.com/archives/3262 Son Erişim Tarihi: 12 Ekim 2019.

84. Moore, A., Cappelli, D. And Trzeciak R. (2008). The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures, *Technical Report, CMU/SEI-2008-TR009, ESC-TR-2008-09,* Software Engineering Institute, Carnegie Mellon University, 3-7.

85. Economist Intelligence Unit (2009). Power to the people? Managing technology democracy in the workplace, *EIU Report,* 2-26.

86. İnternet: Flinders, K. (January, 2010). Employees will choose their own computers in 2010, *Computer Weekly,* URL: http://www.computerweekly.com/Articles/2010/01/19/239999/Employees-will-choose-theirown-computers-in-2010.htm Son Erişim Tarihi:17 Ekim 2019.

87. İnternet: Kavanagh, J. (April, 2006). Security special report: the internal threat, *Computer Weekly,* URL: http://www.computerweekly.com/Articles/2006/04/25/215621/security-special-report-the-internal-threat.htm Son Erişim Tarihi: 17 Ekim 2019.

88. İnternet: Virtual Criminology report, http://resources.mcafee.com/content/NAMcAfeeCriminologyReport Son Erişim Tarihi: 25 Ekim 2019.

89. İnternet: Mohamed, A. (January, 2009). Security Trends for 2009, *Computer Weekly*. URL*:* http://www.computerweekly.com/Articles/2009/01/20/234316/security-trends-for-2009.htm Son Erişim Tarihi: 17 Ekim 2019.

90. NIST (2011). Managing Information Security Risk: Organization, Mission, and Information System View, Joint Task Force Transformation Initiative, NIST Special Publication, 800-39.

91. Söğüt, E. ve Erdem, O.A. (2015) Gelişmiş Israrcı Tehditler ve GIT Örneklerinin Karşılaştırılması. *VIII. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı: Siber Güvenlik ve Kritik Altyapılar*, Ankara, 1-2.

92. İnternet: Siber Ölüm Zincirini Anlamak. URL: https://www.bgasecurity.com/2019/06/siber-olum-zincirini-anlamak-bolum-6/ Son Erişim Tarihi: 15 Eylül 2019.

93. Hu, P., Li, H., Fu, H., Cansever, D. and Mohapatra, P. (2015). Dynamic Defence Strategy against Persistent Threat with Insiders. *2015 IEEE Conference on Comuter Communications (INFOCOM)*, 747-755.

94. Virvilis, N., Serrano, O., and Vanautgaerden B. (2014). Changing the Game: The art of deceiving Sophisticated Attackers. *6th International Conference on Cyber Conflict*, NATO CCD COE Publications, Talinn, Estonia, 90-91.

95. İnternet: W32.Stuxnet Dossier, Symantec, version 1.4 URL: https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/security-response-w32-stuxnet-dossier-11-en.pdf Son Erişim Tarihi: 02 Kasım 2019.

96. İnternet: The Real Story of Stuxnet. URL: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet Son Erişim Tarihi: 02 Kasım 2019.

97. Karabacak B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri, *Siber Güvenlik Çalıştayı*, Bilgi Güvenliği Derneği, Ankara, 1-9.

98. İnternet: Revealed: How a secret Dutch mole aided the U.S.-Israeli Stuxnet cyberattack on Iran. URL: https://news.yahoo.com/revealed-how-a-secret-dutch-mole-aided-the-us-israeli-stuxnet-cyber-attack-on-iran-160026018.html Son Erişim Tarihi: 03 Kasım 2019.

99. İnternet: Stuxnet hakkındaki efsaneler son buldu: Nasıl bulaştırıldığı ortaya çıktı. URL: https://siberbulten.com/siber-guvenlik/stuxnet-hakkindaki-efsaneler-son-buldu-nasil-bulastirildigi-ortaya-cikti/ Son Erişim Tarihi: 03 Kasım 2019.

100. İnternet: Maroochy Shire Sewage Spill, The Repository of Industrial Security Incidents. URL: https://www.risidata.com/Database/Detail/maroochy-shire-sewage-spill Son Erişim Tarihi: 07 Kasım 2019.

101. Sayfayn, N. and Madnick, S. (2017) Cybersafety Analysis of the Maroochy Shire Sewage Spill, Working Paper CISL# 2017-09, Sloan School of Management, Massachusetts Institute of Technology, 5-6.

102. İnternet: Chelsea Manning. URL: https://en.wikipedia.org/wiki/Chelsea_Manning Son Erişim Tarihi: 05 Kasım 2019.

103. İnternet: PRISM (surveillance program). https://en.wikipedia.org/wiki/PRISM_(surveillance_program) Son Erişim Tarihi: 05 Kasım 2019.

104. Bulut, S. (2019). Söylemin Kapatılma ve Açımlama Savaşımında Edward Snowden, *Etkileşim Dergisi*, 2(3), 128-140.

105. İnternet: European Diplomatic Cables Hacked. URL: https://www.nytimes.com/2018/12/18/us/politics/european-diplomats-cables-hacked.html?action=click&module=Top%20Stories&pgtype=Homepage Son Erişim tarihi:27 Aralık 2018.

106. Falkowitz, O.J. and Darche B. (2018). Phishing Diplomacy, *Security Report*, , Area 1, 650.491.9371, Redwood City, CA, USA, 1-22.

107. Gao, W., Morris, T., Reaves, B. and Richey, D. (2010). On SCADA Control System Command and Response Injection and Intrusion Detection, *2010 eCrime Researchers Summit*, Dallas, TX, 1-9.

108. Kim, J. (2011). Development of Integrated Insider Attack Detection System using Intelligent Packet Filtering, 2011 First ACIS/JNU International Conference on Computers, Networks, Systems and Industrial Engineering, Jeju Island, 65-69.

109. Formby, D., Jung, S.S., Walters, S. and Beyah, R. (2014). A Physical Overlay Network for Insider Threat Mitigation of Power System Devices, *2014 IEEE International Conference on Smart Grid Communications*, Venice, Italy, 970-975.

110. Yılmaz, E.N., Ciylan, B., Gönen, S., Sindiren, E. and Karacayılmaz, G. (2018). Cyber Security in Industrial Control Systems: Analysis of DoS Attacks against PLC and the Insider Effect, *2018 6th International Istanbul Smart Grids and Cities Congress and Fair (ICSG)*, İstanbul, 81-85.

111. Mylrea, M., Gourisetti, S., Larimer, C. and Noonan, C. (2018). Insider Threat Cybersecurity Framework Webtool & Methodology: Defening Against Complex Cyber-Phsical Threats, *2018 IEEE Symposium on Security and Privacy Workshops*, San Francisco, CA, USA, 207-216.

112. Lamba, H., Glazier, T., Schmerl, B., Pfeffer, J. and Garlan, D. (2015). Detecting Insider Threats in Software Systems using Graph Models of Behavioral Paths, *Proceeding of th 2015 Symposium and Bootcamp on the Science of Security*, Article No.20, Urbana, Illionis, USA, 1-2.

113. Blackwell, C. (2009). A Security Architecture to Protect against the Insider Threat from Damage, Fraud and Theft, *Proceedings of the 5th Annual Workshop on Cyber*

Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Article No. 45, Tenessee, USA, 1-3.

114. Choi, S. and Zage, D. (2012). Addressing Insider Threat using "Where You Are" as Fourth Factor Authentication, *2012 IEEE International Carnahan Conference on Security Technology (ICCST),* Boston, MA, USA, 147-149.

115. Nasr, P.M. and Yazdian-Varjani, A. (2014). Alarm Based Anomaly Detection of Insider Attacks in SCADA System, *2014 Smart Grid Conference*, 1-3.

116. Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S. and Baker, T. (2018). Security Threats to Critical Infrastructure: The Human Factor, *The Journal of Supercomputing*, October 2018, 74(10), 4986-5002.

117. Erdin, E., Aksu, H., Uluagac, S., Vai, M. and Akkaya, K. (2018). OS Independent and Hardware-Assisted Insider Threat Detection and Prevention Framework, *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, Los Angeles, CA, 926-932.

118. Park, K., Woo, S., Moon, D. and Choi, H. (2018). Secure Cyber Deception Architecture and Decoy Injection to Mitigate the Insider Threat, *Symmetry 2018*, 10(1), 14.

119. Mell, P. and Grance, T. (2011). The NIST Definition of Cloud Computing, NIST, SP 800-145 Draft, 1-7.

120. Ponemon Institute (2011). Security of Cloud Computing Providers Study. Ponemon Institute, LLC.

121. Zeadally, S., Yu, B., Jeong, D. and Liang, L. (2012). Detecting Insider Threats: Solutions and Trends, *Information Security Journal: A Global Perspective*, 21(4), 183-192.

122. Sanzgiri, A., and Dasgupta, D. (2016). Classification of Insider Threat Detection Techniques, Conference CISR'16, Oak Ridge, TN, USA, 1-4. 122, 114

123. Bishop, M., and Gates, C. (2008). Defining the Insider Threat, *Proceedings of the Cyber Security and Information Intelligence Research Workshop*.

124. Sinclair, S. and Smith, S. (2008). Preventative Directions for Insider Threat Mitigation via Access Control. In: S.J. Stolfo, S.M. Bellovin, A.D. Keromytis, S. Hershkop, S. Smith and S. Sinclair (eds) *Insider Attack and Cyber Security: Beyond the Hacker*, Springer 2008, 165-192.

125. Nasr, P.M. and Yazdian-Varjani, A. (2018). Toward Operator Access Management in SCADA System: Deontological Threat Mitigation, *IEEE Transactions on Industrial Informatics*, 14(8), 3314-3324.

126. Gao, Y., Xie, X., Parekh, M. and Bajramovic, E. (2016). SIEM: Policy-based Monitoring of SCADA Systems, Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016, 559-570. 126, 118

127. Lemay, A., Sadighian, A. and Fernandez, J. (2016). Lightweight Journaling for SCADA Systems via Event Correlation, *Critical Infrastructure Protection X*, *IFIP Advance Information and Communication Technology*, Volume:485, 99-115.

128. Blackwell, C. (2010). A Security Architecture to Protect against Data Loss, *1st International Conference on Information Security and Digital Forensics*, City Univ London, United K,ingdom, 102-110.

129. Silowash, G. and King, C. (2013). Insider Threat Control: Understanding Data Loss Prevention (DLP) and Detection by Correlating Events from Multiple Sources, *Technical Note, CMU/SEI-2013-TN-002,* Software Engineering Institute, Carnegie Mellon University, 1-16.

130. İnternet: İlbiz, H. (2019). Kritik Altyapılarda Secure Dizayn ve Güvenlik Konsepti. https://roothfy.com/kritik-altyapilarda-secure-dizayn-nasil-olmali/ Son Erişim Tarihi: 09 Aralık 2019.

131. Lee, R.M., Assante, M.J., Conway, T. (2016). Analysis of the cyber attack on the Ukrainian power grid, *Electricity Information and Analysis Center, SANS ICS*, 5-6.

132. İnternet: Aydemir, M. (2019). Endüstriyel Kontrol Sistemleri İçin Purdue Katmanlı Güvenlik Mimarisi. URL: https://www.biznet.com.tr/wp-content/uploads/2019/01/Biznet_Bilisim_Purdue_Model_v2.pdf Son Erişim Tarihi: 09 Aralık 2019.

133. Beaver, J.M., Borges-Hink, R.C. and Buckner, M.A. (2013). An Evaluation of Machine Learning Methods to Detect Malicious SCADA Communications, *12th International Conference on Machine Learning and Applications*, Volume:2, 45-59.

134. Punithavathani, D.S., Sujatha, K. and Jain, J.M. (2014). Surveillance of anomaly and misuse in critical networks to counterinsider threats using computational intelligence, *Cluster Computing*, Volume:18, 435–451.

135. Scott, C. (2014). Designing and Implementing a Honeypot for a SCADA Network. *SANS Institute InfoSec Reading Room,* 1-39.

136. Wade, S. M. (2011). *SCADA Honeynets*: *The attractivenss of honeypots as critical infrastructure security tools for the detection and analysis of advanced threats*, Doctoral dissertation, Iowa State University, 1-67.

137. İnternet: Pothamsetty, V. and Franz, M. (2004). SCADA HoneyNet Project: Building Honeypots for Industrial Networks. URL: http://scadahoneynet.sourceforge.net/ Son Erişim Tarihi: 10 Aralık 2019.

138. İnternet: Digital Bond Archives. URL: https://dale-peterson.com/digital-bond-archives/ Son Erişim Tarihi: 10 Aralık 2019.

139. İnternet: Honeynet Project, Conpot. URL: https://www.honeynet.org/projects/active/conpot/ Son Erişim Tarihi: 10 Aralık 2019. 139

140. Jicha III A.F. (2016). SCADA Honeypots – An In-depth Analysis of Conpot. Master's Paper, Department of Management Information Systems, Eller College of Management, The University of Arizona, 1-21.

141. Wilhoit, K. (2013). The SCADA That Didn't Cry Wolf. *Blackhat 2013*, 1-24.

142. Buza, D. I., Juhasz, F., and Miru, G. (2013). Design and implementation of critical infrastructure protection system. *Budapest University of Technology and Economics*, 1-58.

143. Buza, D. I., Juhasz, F., Miru, G., Felegyhazi, M., & Holczer, T. (2014). CryPLH: Protecting Smart Energy Systems from Targeted Attacks with a PLC Honeypot. *Springer International Publishing Switzerland*, 1-12.

144. Serbanescu, A. V., Obermeier, S., and Yu, D. (2015). ICS Threat Analysis Using a Large-Scale Honeynet. *BCS Learning & Development Ltd.*, 1-11.

145. İnternet: Conpot. URL: http://conpot.org/ Son Erişim Tarihi: 15 Aralık 2019.

146. İnternet: Github, Conpot. https://github.com/mushorg/conpot Son Erişim Tarihi: 15 Aralık 2019.

147. İnternet: Installation on Host using virtualenv. URL: https://conpot.readthedocs.io/en/latest/installation/install.html Son Erişim Tarihi: 15 Aralık 2019.

148. İnternet: Splunk. URL: https://www.splunk.com/ Son Erişim Tarihi: 10 Aralık 2019.

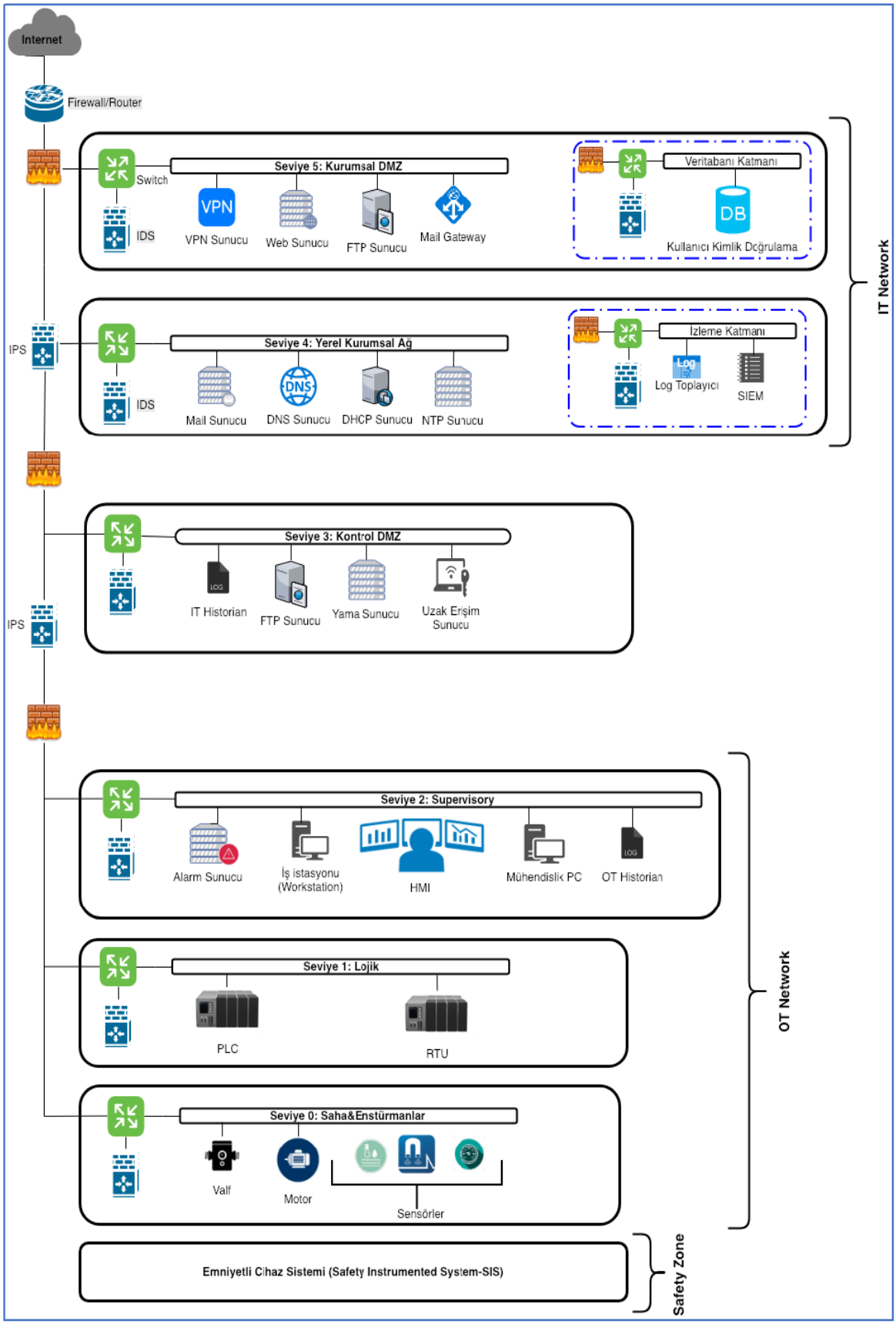
149. Akkaya Ş. (2015). *Fpga Tabanli Modbus Ağ Geçidi Tasarimi*, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, 7-28, 45-59.

150. Yılmaz, E.N., Doğru, İ.A. and Aras, U. (2018). Analysis of Modbus Protocol Vulnerabilities with ModbusPal Simulator, In Salman, S., Karapınar, R., Kavak, D. and Kılıçer, A. (Eds.), *Current Academic Studies in Engineering Sciences-2018*, Vol.1, 184-202.

151. Ponemon Institute (2018). 2018 Cost of Data Breach Study: Impact of Business Continuity Management, Research Report, 5.

EKLER

EK-1. Purdue Model



Şekil 1.1. Purdue Model

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ARAS, Uğur
Uyruğu : T.C.
Doğum tarihi ve yeri : 27.03.1987, Muş
Medeni hali : Evli
Telefon : 0 (312) 417 51 90
e-mail : ugur.aras1@gazi.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Yüksek Lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam ediyor
Lisans	Kara Harp Okulu / Sistem Mühendisliği	2009
Lise	Işıklar Askeri Lisesi	2005

İş Deneyimi

Yıl	**Yer**	**Görev**
2009-Halen	Türk Silahlı Kuvvetleri	Subay

Yabancı Dil

İngilizce

Yayınlar

1. Yılmaz, E.N., Doğru, İ.A. and Aras, U. (2018, 16-17 Kasım). *Analysis of Modbus Protocol Vulnerabilities with ModbusPal Simulator*, V. Uluslararası Multidisipliner Çalışmalar Sempozyumu, Ankara.

Hobiler

Spor, Film, Müzik

GAZİ GELECEKTİR...