
GAZİ ÜNİVERSİTESİ
Gazi
1926

PLC İLE KONTROL EDİLEN MİKRO TİP AKILLI ŞEBEKE SİSTEMLERDE BİLGİ GÜVENLİĞİNİN SAĞLANMASI

Serkan GÖNEN

DOKTORA TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAZİRAN 2018

Serkan GÖNEN tarafından hazırlanan "PLC İLE KONTROL EDİLEN MİKRO TİP AKILLI ŞEBEKE SİSTEMLERDE BİLGİ GÜVENLİĞİNİN SAĞLANMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilgi Güvenliği Mühendisliği Anabilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Ercan Nurcan YILMAZ

Elektrik Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Başkan: Doç. Dr. Hamdi Tolga KAHRAMAN

Yazılım Mühendisliği Anabilim Dalı, Karadeniz Teknik Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Yusuf SÖNMEZ

Elektrik Elektronik Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi İbrahim Alper DOĞRU

Bilgisayar Mühendisliği Anabilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Mehmet Fatih IŞIK

Elektrik Elektronik Mühendisliği Anabilim Dalı, Hitit Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 21/06/2018

Jüri tarafından kabul edilen bu tezin Doktora 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.

Serkan GÖNEN

21/06/2018

PLC İLE KONTROL EDİLEN MİKRO TİP AKILLI ŞEBEKE SİSTEMLERDE BİLGİ GÜVENLİĞİNİN SAĞLANMASI

(Doktora Tezi)

Serkan GÖNEN

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Haziran 2018

ÖZET

Akıllı şebekeler başta olmak üzere kritik altyapıların kontrolünde kullanılan Endüstriyel Kontrol Sistemleri (EKS), gelişen bilim ve teknolojiyle birlikte verimlilik, ekonomi, sürat, coğrafi olarak dağıtık yapıların kontrolü gibi insan hayatını kolaylaştıran etkenler nedeniyle, izole bir ağ mimarisinden dış ağlara, özellikle internete, açık bir mimariye hızlı bir geçiş yapmıştır. Bu geçişle birlikte, EKS'ye özgü protokoller yetersiz kalmış ve karma protokoller (TCP/IP-Modbus, vb.) kullanılmaya başlanmıştır. Bunun sonucunda EKS'ye özgü zafiyetlerin yanında internet ve yeni protokollere özgü zafiyetlerde kontrol sistemlerini tehdit etmeye başlamıştır. İş sürekliliğinin öncelikli olduğu EKS'de, arıza ve/veya kesinti olma ihtimali düşüncesiyle yama/güncellemeler ihmal edilebilmekte, benzer endişeler nedeniyle bu sistemlerin güvenliğine ilişkin değerlendirme yapılmamaktadır. Bu çalışmada EKS'nin en önemli bileşenlerinden biri olan PLC'lerin siber güvenlik analizinin yapılması hedeflenmiştir. Çalışmada oluşturulan sınama ortamında Siemens S-7 1200 (Firmware 2.2) PLC cihazının güvenlik/açıklık analizleri gerçekleştirilmiştir. Öncelikle PLC'lere hedef odaklı saldırılar (MitM, DoS, Başlat/Durdur) gerçekleştirilerek, saldırıların donanımlara ve sisteme olan etkisi incelenmiş, müteakiben sisteme ilave yük getirmemesi için aynalama tekniği kullanılarak yakalanan saldırı paketleri analiz edilmiştir. Tespit çalışmalarında saldırılara özgü patern ve imzalar oluşturularak benzer davranışları sergileyen saldırıların engellenmesi ve sistemin zarar görmemesi hedeflenmiştir. Saldırılardan korunmak amacıyla oluşturulan kural tabloları, bünyesinde çeşitli saldırı tespit ve önleme sistemlerini (Snorby, Snort ve Suricata, vb.) barındıran ve endüstriyel sistemlerde kullanılmayan Debian tabanlı Smoothsec Linux dağıtımına eklenmiştir. Analiz sonuçları, PLC'lerin saldırılara karşı savunmasız olduklarını, ağın sürekli izlenmesi başta olmak üzere, ağ bölümlendirmesi, şifre koruma tekniklerinin uygulanması ve kurumsal bilgi güvenliği farkındalığı sağlanmanın hayati önem taşıdığını göstermiştir. Çalışmanın EKS güvenliğine dikkat çekeceği ve benzer çalışmalara önemli katkılar sağlayacağı değerlendirilmiştir.

Bilim Kodu : 92403

Anahtar Kelimeler : Akıllı şebeke, endüstriyel kontrol sistemleri, PLC, testbed, siber güvenlik, açıklık analizi, saldırı paterni, ağ trafiği analizi, saldırı tespiti, bilgi güvenliği farkındalığı

Sayfa Adedi : 146

Danışman : Doç. Dr. Ercan Nurcan YILMAZ

PROVIDING INFORMATION SECURITY IN MICRO TYPE SMART GRID SYSTEMS CONTROLLED BY PLC

(Ph.D. Thesis)

Serkan GÖNEN

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

June 2018

ABSTRACT

Industrial Control Systems (ICS) used to control critical infrastructures, notably smart grids, have made a rapid transition from an isolated network architecture to an architecture connected to external networks, especially Internet, because of the factors that facilitate human life such as efficiency, economy, speed and controlling geographically distributed structures. With this transition, EKS-specific protocols became insufficient and hybrid protocols (TCP / IP-Modbus, etc.) have begun to be used. As a result, besides the vulnerabilities inherent in the ICS, new vulnerabilities have emerged and began to threaten the control systems. In ICS, where business continuity is prioritized, patches / updates may be neglected due to the possibility of breakdown and / or interruption, and there is no evaluation of the security of these systems due to similar concerns. In this study, carrying out of cyber security analysis of PLCs, one of the most important components of ICS, is aimed. The security / vulnerability analysis of the Siemens S7 1200 (Firmware 2.2) PLC device was performed in the test bed created in the study. Initially, target-oriented attacks (MitM, DoS, Start / Stop) were carried out on the PLCs, the effects of the attacks on the hardware and the system were examined and then the attack packets captured using the mirroring technique to avoid additional load to the system were analyzed. It was aimed to prevent similar attacks and to protect system with creating attack patterns and signatures in detection activities. The rule tables created to protect against attacks were added to the Debian-based Smoothsec Linux distribution, which contains various intrusion detection and prevention systems (Snorby, Snort and Suricata, etc.) and is not used in industrial systems. The results of the analysis show that PLCs are vulnerable to attack, so notably continuous monitoring of the network, network partitioning, application of password protection techniques, and awareness of enterprise information security are crucial. It is assessed that this novel approach will draw attention to security of ICS and provide significant contributions to the research on the security analysis of industrial control systems.

Science Code	:	92403
Key Words	:	Smart grids, industrial control systems, PLC, testbed, cyber security, vulnerability analysis, attack pattern, network traffic analysis, attack detection, information security awareness
Page Number	:	146
Supervisor	:	Assoc. Prof. Dr. Ercan Nurcan YILMAZ

TEŞEKKÜR

Tezin hazırlanması aşamasında bana her türlü desteği veren danışmanım sayın Doç.Dr. Ercan Nurcan YILMAZ'a, değerli katkılarından dolayı çalışma arkadaşlarım Gökçe KARACAYILMAZ ve Erhan SİNDİREN'e, doktora çalışmam boyunca göstermiş olduğu sevgi, anlayış ve sabır ile bana destek olan sevgili eşim Burcu ile çocuklarım Göksu ve Ayperi'ye, desteklerini benden esirgemeyen mesai arkadaşlarıma sonsuz teşekkürlerimi sunmayı bir borç bilirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılan bazı kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklama
ADACS	Otonom bileşen tabanlı politika tanım kontrol sistemlerinde anormal izleme dili (Autonomous component based policy description language for anomaly monitoring in control systems)
AES	İleri kriptolama standartları (Advanced encryption standards)
AMI	**G**elişmiş sayaç altyapısı (Advanced metering infrastructure)
ARP	Adres çözümleme protokolü (Address resolution protocol)
ASPS	Otonom yazılım koruma sistemi (Autonomic software protection system)
BGYS	Bilgi güvenliği yönetim sistemi
BSI	İngiliz standartları enstitüsü (British standards institute)
BT	Bilgi teknolojileri
COTS	Hazır ticari ürün (Commercial off-the-shelf)
CC	Ortak kriterler (Common criteria)
CIM	Genel bilgi modeli (Common information model)
CIP	Kritik altyapısı koruması (Critical infrastructure protection)
CI2CS	Kritik altyapı endüstriyel kontrol sistemleri (Critical infrastructure industrial control systems)
CPNI	Ulusal altyapıları koruma merkezi (Centre for the protection of national infrastructure)
CRC	Döngüsel artık kontrolü (Cyclic redundancy checking)
CSD	Bilgisayar güvenliği başkanlığı (Computer security division)

Kısaltmalar	Açıklama
CSRC	Bilgisayar güvenliği kaynakları merkezi (Computer security resource center)
CTCPEC	Kanada güvenilir bilgisayar ürün değerlendirme kriterleri **(**Canadian trusted computer product evaluation criteria)
DCS	Dağıtık kontrol sistemleri (Distributed control systems)
DDoS	Dağıtık hizmet reddi (Distributed denial of service)
DHCP	Dinamik ana bilgisayar yapılandırma protokolü (Dynamic host configuration protocol)
DHS	İç güvenlik bakanlığı **(**Department of homeland security)
DLP	Veri kaybı engelleme (Data loss prevention)
DNP	Dağıtık ağ protokolü (Distributed network protocol)
DOE	Enerji bakanlığı (Department of energy)
DoS	Hizmet reddi (Denial of service)
DMZ	Yarı güvenli ağ (Demilitarized zone)
EAL	Değerlendirme güvence seviyesi (Evaluation assurance level)
EAP	Genişletilebilir kimlik denetimi protokolü (Extensible authentication protocol)
EISA	Enerji bağımsızlık ve güvenlik antlaşması (Energy independence security act)
EKS	Endüstriyel kontrol sistemleri
EPRI	Elektrik güç araştırma kurumu (Electric power research institute)
ETP	Avrupa teknoloji platformu (European technology platform)
FIPS	Federal bilgi işleme standardı (Federal information processing standard)

Kısaltmalar	Açıklama
FERC	Federal enerji düzenleme kurulu **(**Federal energy regulatory commission**)**
HLA	Üst düzey mimari (High level architecture)
HMAC	Hash tabanlı mesaj doğrulama kodu (Hash-based message authentication code)
HTTP	Köprü metni aktarım protokolü (Hypertext transfer protocol)
ICMP	İnternet denetim iletisi iletişim kuralı **(**Internet control message protocol)
ICS	Endüstriyel kontrol sistemleri (Industrial control systems)
IEEE	Elektrik elektronik mühendisleri kurumu (Institute of electrical and electronic engineers)
ISA	Enstrümantasyon, sistemler ve otomasyon kuruluşu (Instrumentation, systems, and automation society)
IT	Bilgi teknolojileri (Information technologies)
ITACA	İnternet trafik ve içerik analizi (Internet traffic and content analysis)
IP	İnternet iletişim kuralı **(**Internet protocol)
ISML	Endüstriyel durum modelleme dili (Industrial state modelling language)
ISO	Uluslararası standartlar teşkilâtı (International organization for standardization)
ISO / IEC	Standardizasyon organizasyonu / Uluslararası elektroteknik komisyonu (Organization for standardization/international electro technical commission)
ISO / TSAP	Uluslararası standartlar kurumu taşıma hizmeti erişim noktası (International standards organization transport service access point)

Kısaltmalar	Açıklama
ITU	Uluslararası telekomünikasyon birliği (The international telecommunication union)
KPCA	Çekirdek ana bileşen analizi (Kernel principal component analysis)
MAC	Medya erişim kontrolü (Media access control)
MitM	Ortadaki adam (Man in the middle)
MR-ARP	MitM dayanıklı adres çözümleme protokolü **(**MitM-resistant address resolution protocol)
MTTC	Riske atmak için ortalama zaman (Mean time to compromise)
NAN	Komşu alan ağı (Neighborhood area network)
NAC	Ağ erişim kontrolü (Network access control)
NERC	Kuzey Amerika elektrik güvenilirlik şirketi (The North American electric reliability corporation)
NIPP	Ulusal altyapı koruma planı (National infrastructure protection plan)
NIST	Ulusal standartlar ve teknoloji enstitüsü (National institute of standards and technology)
NISTIR	Ulusal standartlar ve teknoloji kurumları arası rapor (National institute of standards and technology interagency report)
NSRM	Ağ güvenliği risk modeli (Network security risk model)
OpenVAS	Özgür açıklık analiz sistemi (Open vulnerability assessment system)
OPNET	Optimize ağ mühendislik araçları (Optimized network engineering tools)
OSSIM	Açık kaynak güvenli bilgi yönetimi (Open source security ınformation management)
PIN	Personel kimlik numarası (Personnel identification number)
PKM	Gizli anahtar yönetimi (Private key management)

Kısaltmalar	Açıklama
RAIM	Gerçek zamanlı izleme, anormallik algılama, etki analizi ve azaltma stratejileri (Real-time monitoring, anomaly detection, impact analysis, and mitigation strategies)
RFC	Yorum istekleri (Requests for comments)
SHA	Güvenli özet algoritması **(**Secure hash algorithm)
SNFG	Yarı ağ-form oyunu (Semi network-form game)
SSEMP	Elektrik piyasası katılımcıları için güvenlik standartları **(**Security standards for electric market participants)
SSL	Güvenli yuva katmanı (Secure sockets layer)
SVM	Destek vektör makineleri (Support vector machines)
TARP	Bilet tabanlı ARP **(**Ticked-based ARP)
TCP	İletim denetimi iletişim kuralı **(**Transmission control protocol)
TCSEC	Güvenilir bilgisayar sistemi değerlendirme kriterleri (Trusted computer system evaluation criteria)
TLS	Taşıma katmanı güvenliği **(**Transport layer security)
UAC	Kimlik doğrulama kodu (User authentication code)
XML	Genişletilebilir işaretleme dili (eXtensible markup language)
WiMAX	Mikrodalga erişimi için dünya çapında birlikte çalışabilirlik (Worldwide interoperability for microwave access)

1. GİRİŞ

İlk çağlarda taşlarla sopalarla savaşan insanlar belirli bir zaman sonra grup, kabile ve devlet düzenine girmiş, savaş aletleri de taş ve sopalardan kılıçlara, kalkanlara ve silahlara dönüşmüştür. Tarihimizin konvansiyonel savaşları (dünya savaşları) ise, farklı örnekleri mevcut olsa da (Kurtuluş Savaşımız) yine muharebe meydanlarında asker, uçak, top, tank gibi sahip olunan unsurların sayıca daha fazla olduğu tarafın kazandığı (simetrik) savaşlardır. Söz konusu savaşlar ülkeler için oldukça maliyetli ve savaşan tarafları her yönden zarara uğratan durumlardır. Ama günümüzde hasım olarak kabul edilen ülkelere zarar vermek için söz konusu savaşlara ve bu savaşlar için ihtiyaç duyulan maliyete ve insan gücüne hiç gerek yoktur. Artık çok az bir maliyetle, iyi motive edilmiş insanlarla hedef ülkenin tespit edilen kritik bir veya birden fazla altyapısına işlevsiz bırakmak amacıyla siber ortamda saldırarak, meydan muhaberesi ile verdirilemeyecek kadar zarara uğratılabilir.

Bilgi ve iletişim alanında yaşanan gelişmeler özellikle internetin de yaygınlaşmasına paralel olarak diğer sektör ve alanlarda da gelişmelere yol açmıştır. İnternetin yaygınlaşması artık tüm olguların elektronik yani ”e-” kavramı üzerinde gerçekleştirilmeye başlanmasına yol açmıştır. Bu gelişmeye paralel olarak, verimlilik, sürat, uzaktan yönetim gibi hayatımızı kolaylaştıran etkenler nedeniyle akıllı şebekeler hayatımızdaki yerini almaya başlamıştır. Akıllı şebekelerde dâhil olmak üzere, toplumlar için hayati önemli olan kritik altyapıların yönetiminde olan EKS (Elektronik Kontrol Sistemleri)’de, bu gelişmelere karşı koyamamış aksine bütünleşmiştir.

EKS’ler, nükleer tesisler, enerji üretimi, su, ulaşım gibi son derece kritik altyapı sistemleri için geleneksel uygulamaların ötesinde yaygın bir kullanım elde etmiştir. İnternet kavramının tüm kontrol sistemlerine dâhil olması ile tehdit ortamı değişmiştir. Mobil ağ üzerinden süreçleri izleme ve kontrol etme konusundaki son ilgi ve yetenekler, sistemlere daha çeşitli noktalardan giriş özelliği eklemiştir. Sonuçta siber güvenlik tehditlerine ve saldırılarına karşı yeterli koruma sağlayabilecek etkili stratejilerin ihtiyaçları ortaya çıkmıştır.

EKS’nin kullanımı, artan endüstriyel süreç otomasyonu, düşük işletme maliyeti ve küresel ekonomideki büyümenin bir sonucu olarak artmıştır. Söz konusu artışa paralel olarak, 2022 yılında yatırımın 13.43 milyar dolara ulaşması beklenmektedir. EKS, 1960'lı yıllarda

kullanılmaya başlandıktan sonra teknolojideki değişimlerle birlikte büyük bir gelişme ve değişim yaşamıştır. EKS, ana birime dayalı istemciden, çevre birimlerinden ana birime veri göndermek için merkezi iletişim protokollerini kullanan istemci / sunucu sistemlerine dönüşmüştür. Nesnelerin İnterneti (IoT), İnternet'e bağlı EKS sensörü ve cihazları çoğalmasıyla birlikte EKS, bağımsız bir sistemden Internet'e bağlı uzaktan erişilebilir bir sisteme dönüşmektedir. Bu süreçle birlikte, EKS bilgisayar korsanları için çekici bir hedef haline gelmiştir [1, 2].

Ölçeklenebilirlik, daha iyi iletişim protokolleri, verimlilik, maliyet etkinliği, bileşenler arasında birlikte çalışabilirlik [3] ve uzaktan erişim dâhil olmak üzere İnternet erişiminin birçok faydası vardır, ancak EKS hiçbir zaman ağ bağlantısı ve güvenlik yönü düşünülerek tasarlanmamıştır [2, 4]. Çünkü EKS'de, güvenlikten ziyade her zaman güvenilirlik ve bir ifadeyle süreklilik üzerinde durulmuş ve özel standartlar kullanılarak koruma sağlanmaya çalışılmıştır [5]. Ancak, 1990'lardan beri kontrol sistemleri bilgisayar ağları ile bütünleşmiş ve aynı zamanda EKS'de daha fazla hazır ticari ürünler (Commercial off the shelves-COTS) kullanılmaya başlanmıştır [6]. Bunun sonucunda, EKS sunucusu ve kullanıcı arayüzlerine artık bir saldırgan için birçok giriş noktası sağlayan İnternet ve hücresel ağlar üzerinden erişilebilir hale gelmiştir. İnternet ve hücresel ağ bağlantısı, güvenlik açıkları olarak bilinen web teknolojileri gibi açık standartların yanı sıra, bir saldırganın SCADA ağları hakkında derinlemesine bilgi sahibi olmasını çok kolay hale getirmektedir. Günümüzde çoğu EKS haberleşme protokolü, mesaj kimlik doğrulaması içermez ve sadece düz metin kullanmaktadır. Bunun sonucunda da örneğin ortadaki adam (Man in the Middle-MitM) saldırısına karşı daha savunmasız hale gelmiştir [7-9]. EKS'nin hibrit protokollerini kullanmasıyla da, TCP / IP protokollerine özgü güvenlik açıkları da EKS için yeni tehdit ortamlarının ortaya çıkmasına neden olmuştur.

SCADA sistemleri üzerindeki siber saldırılar büyük bir artışla devam etmektedir [10]. Genel teknoloji farkındalığı, ücretsiz bilginin yaygın olarak kullanılabilirliği ve kötü niyetli unsurların varlığı, bu tür saldırıları daha kolay ve olası hale getirmektedir. Bu kapsamda, siber saldırının engellenmesi ve siber saldırılara karşı savunmayı güçlendirerek yeterli önlemlerin alınması acil bir ihtiyaçtır. EKS'ye fiziksel erişimin sınırlandırılması, kriptografi, yama yönetimi, kurum ve üretim sistemlerinin ayrılması (ağ bölümlendirmesi) gibi genel siber güvenlik önlemleri, Güvenlik Duvarı ve Erişim Kontrol Listeleri (Access Control List-ACL) uygulanan yöntemlerden bazılarıdır. Bununla birlikte, söz konusu

güvenlik uygulamaları geleneksel bilişim sistemlerinde gösterdiği başarı ve etkiyi EKS sistemlerinde gösterememektedir [11]. Bu nedenle, EKS'ye özgü karakteristikler dikkate alınarak güvenlik önlemleri planlanmalı ve uygulanmalıdır. Örneğin, bilgi teknolojilerinde uygulanan Bilgi Güvenliği karakteristikleri gizlilik, bütünlük ve kullanılabilirlik (Confidentiality, Integrity, Availability-CIA) üçlemesi şeklinde sıralanırken, EKS'de bu sıralama kullanılabilirlik, bütünlük ve gizlilik (Availability, Integrity, Confidentiality-AIC) olarak değişmektedir.

EKS projelerinin, işletmeye alındıktan sonra uzun yıllar boyunca yama ve güncellemeye ihtiyaç duymadan kesintisiz bir şekilde çalışması beklenir [12]. Buda, yöneticilerin yeterli koruma ve sürekli sistem çalışması sağlaması arasındaki bir ikilemi ortaya çıkartır. Yazılım güncellemelerinin ve yamalarının uygulanması, sistemin yürütme ortamına değişmeden çalışmasını sürdürme isteği nedeniyle genellikle ertelenmektedir [13]. Çünkü yamalar ve antivirüs uygulamaları gibi güvenlik önlemleri, iletişimin yavaşlaması ya da sistemin normal çalışmasının engellenmesi başta olmak üzere istenmeyen sonuçlara yol açabilir. Sonuçta, bu sistemlerin operasyonel doğası, sistemi işletmeye alma esnasındaki siber güvenlik testlerini engellemektedir. Bu nedenle, sistemlerin güvenlik durumları belirsizliğini korumaktadır.

Bilinen bir kişi veya kuruluştan olduğu iddia edilen sosyal mühendislik saldırıları, Stuxnet örneğinde olduğu gibi bir sisteme sızmak için kullanılabilir. Çoğu zaman siber güvenlik çalışmaları dışarıdan gelen bir saldırıya odaklanır. Ancak güvenilir ağın içinden bir ihmal veya sabotajdan kaynaklanan bir saldırının da dışarıdan yapılan saldırılara nazaran çok daha tehlikeli sonuçlar doğurabileceği dikkate alınmalıdır. Örnek olarak, beşinci bölümde detayları belirtilen Avustralya Queensland'de yaşanan ve yaklaşık bir milyon litre kanalizasyon atığının park ve nehirlere dökülmesine neden olan kanalizasyon kontrol sistemi üzerindeki saldırının kaynağı hoşnutsuz bir işçi olduğu ortaya çıkmıştır [14]. Benzer diğer bir örnek olan ve siber saldırı dünyasında yeni bir dönemi başlatan Stuxnet'in, ağa USB çubuklarla sızmış olması en önde gelen olasılıklardandır. Stuxnet kontrol sistemlerine saldıran ilk kötü amaçlı yazılım olmuştur ve EKS güvenlik açıklarını öne çıkaran türünün ilk örneğidir. Bu saldırıdan önce, savunmasız olmasına rağmen, izole yapısından dolayı SCADA sistemlerinin aktif olarak hedeflenmediği düşünülmekte idi. Stuxnet, USB cihazları kullanarak yayılmış ve PLC'lerin Ladder lojik kodunu değiştirerek

sisteme saldırmıştır [15, 16]. Bu saldırı teknoloji ve süreç yönetimi kadar insan faktörünün de önemli olduğunu ortaya çıkarmıştır.

Endüstriyel kontrol sistemleri, nükleer tesisler, enerji üretimi, ulaşım, su gibi kritik altyapı sistemleri için geleneksel uygulamaların ötesinde yaygın bir kullanım elde etmiştir. Hal böyle olunca siber güvenlik tehditlerine ve saldırılarına karşı yeterli koruma sağlayabilecek etkili stratejilerin ihtiyacı da ortaya çıkmaktadır.

Bu çalışmada, akıllı şebekelerin merkezinde yer alan ve kritik altyapıların yönetiminde kullanılan EKS'lerin önemli bir bileşeni PLC'lerin güvenlik açıklarına dikkat çekmek için geliştirilen sınama ortamında hedef odaklı saldırılar (Port Tarama, DoS, Ortadaki Adam ve Başlat/Durdur) gerçekleştirilmiştir.

PLC'ler saha donanımları olmaları nedeniyle güvenlik uzmanları/yöneticilerinin fiziki olarak kontrol edebilecekleri donanımlar değillerdir. Bu nedenle, PLC'lere gerçekleştirilen saldırıların tespit edilmesi kolay değildir. Saldırı analizleri sonucunda, PLC'lerin bu saldırılara karşı savunmasız oldukları ve PLC'ler gibi kritik cihazlar için ağ bölümlendirmesi ve şifre korumasının hayati önem taşıdığı göstermiştir.

Çalışmanın tespit aşamasında, içerisinde Snort, Snorby, Barnyard, Sagan gibi ağ güvenliği araçlarını içinde barındıran ve saldırıların tespiti maksadıyla geliştirilen bir Linux dağıtımı olan SmoothSec sistemi kullanılmıştır. EKS'nin en önemli gereksinimi olan sürekliliğe korumak amacıyla, sisteme ek yük getirmeden aynalama tekniği ile tüm paketlerin örneği tespit sistemine aktarılarak analizler gerçekleştirilmiştir. Tespit aşamasında, ağ trafiğinin sürekli izlenmesinin, muhtemel saldırıların tespit edilmesi ve müteakiben önlem alınmasında önemli katkılar sağlayabileceği görülmüştür. Çalışmada kullanılan saldırı tespit sistemleri ve benzeri sistemler ile ağ trafiğinin izlenmesi, sistem normlarının ve eşik değerinin belirlenmesi sonucu norm dışındaki davranışlarda sistem yöneticileri/güvenlik uzmanlarının uyarılması sağlanabilecektir. Bu sayede, EKS'lerin en önemli güvenlik bileşeni olan süreklilik boyutu kapsamında yasal paketlerin geciktirilmeden gönderilmesi ve engellenmemesi sağlanırken, kötücül paketlerin sisteme sızması ve zarar vermesi önlenebilecektir.

Çalışmada ayrıca, toplumlar için hayati önemli olan kritik altyapılar ve akıllı şebekelerin yönetiminde kullanılan EKS'lerin önemli bileşenlerinden olan PLC'lerin açıklık analizine odaklanılmıştır. Bu amaçla, akıllı şebeke altyapısı, haberleşme ağları, akıllı şebeke güvenliği gereksinimleri ve karşılaşılan zorluklar, uluslararası akıllı şebekelerle ilgili güvenlik standartları Bölüm 2'de açıklanmıştır. Bölüm 3'de, en yaygın EKS türleri SCADA ve DCS, bilgi teknolojileri ile EKS arasındaki farklar, EKS'de hazır ticari ürün kullanımı, EKS'de yaşanan güvenlik olayları, EKS'de yama ve güncelleme ve PLC güvenliği ile EKS güvenliğine yönelik yapılan benzer çalışmalara yer verilmiştir. Bilgi güvenliği farkındalığı anketinin yer aldığı EKS çalışanlarında bilgi güvenliği farkındalığına Bölüm 4'de değinilmiştir. PLC açıklık analizine yönelik saldırılar ve saldırıların tespitine yönelik analiz sonuçları ve çıkarımlar Bölüm 5'de sunulmuştur. Bölüm 6'da sonuçlar ve önerilere yer verilmiştir.

2. AKILLI ŞEBEKELERDE SİBER GÜVENLİK

Büyük bir süratle gelişen teknoloji, elektrik dağıtım sistemleri ile haberleşme ağlarını iki yönlü enerji ve bilgi akışının sağlandığı bir formda birleştirerek akıllı şebeke olarak tanımlanan bir altyapıyı oluşturmuştur [17]. Söz konusu bütünleşme sayesinde enerji otomasyon sistemleri eskimiş ve atıl durumdaki teknolojilerden gelişmiş haberleşme teknolojilerine geçmiş, aynı zamanda izole kontrol sistemlerini açık veri ağları haline getirmiştir [18]. Bir akıllı şebeke; yüksek doğrulukla güç akışı kontrolü, kendi kendine onarım sağlayan (self-healing) ve enerji güvenirliliği ve sayısal haberleşmeyi ve kontrol teknolojilerini kullanan, bir elektrik ağının yeni formudur. Yeni teknoloji ürünü haberleşme yeteneklerinin güç şebekelerine kazandırılması vasıtasıyla akıllı şebekeler daha etkin, esnek, yönetimi ve işletimi daha uygun hale gelmiştir. Akıllı sistemler ve ağları için geliştirilen dağıtık anlayış ve geniş bant yetenekleri gibi yeni yetenekler önemli oranda etkinliği ve güvenirliliği sağlamıştır [19]. Akıllı şebekelerin coğrafi geniş yapısı ve kapsamı dikkate alındığında, kritik altyapıların yönetiminde de kullanılan akıllı şebekelerin siber güvenlik açıklıklarının da oldukça fazla olması kaçınılmazdır. Bu nedenle, tüm otorite kurumlarının da kabul ettiği üzere akıllı şebekelerde meydana gelebilecek güvenlik ihlallerinin sonuçları da hayati önemli olacaktır [20].

Genel bir akıllı şebeke haberleşme sistemi, elektrik santrallerini ve alt bileşenlerini yöneten bölgesel kontrol merkezlerinin yatay bileşiminden oluşmaktadır. Bir akıllı şebeke haberleşme sistemi, veri toplama ve elektrik dağıtımının kontrolü işlemlerinin gerçekleştirdiği katmanlı bir mimari yapısına sahiptir. Bölgesel kontrol merkezleri genellikle ölçüm sistemlerini, güç sistemi işletme veri yönetimi, güç pazarı işlemlerini, güç sistemi faaliyetlerini ve veri edinimi kontrolünü desteklerler. Trafo merkezleri; Uzak Yönetim Birimlerini (Remote Terminal Units-RTU's) ve devre şalterlerini, İnsan Makine Arayüzlerini (Human Machine Interface-HMIs), haberleşme donanımlarını (anahtarlayıcılar, yönlendiriciler), log sunucuları, veri toplayıcıları ve protokol ağ geçidini (gateway) içerir. Akıllı Elektronik Cihazları (Intelligent Electronic Device- IEDs), bir dizi dönüştürücü aracı, kılavuz değiştiriciler, devre sonlandırıcıları, faz ölçüm birimlerini (Phase Measuring Units-PMUs) ve koruma rölelerini içeren saha donanımlarıdır [21].

Mevcut siber güvenlik çözümleri, internet gibi kamusal veri haberleşme sistemlerinde çalışan akıllı şebeke haberleşme sistemlerinin ihtiyacını karşılayamamaktadır. Çünkü ticari

ağ sistemleri ile kıyaslandığında, akıllı şebekelerin siber güvenlik hedefleri, amaçları ve yöntemleri tamamen farklıdır. Akıllı şebeke haberleşme sistemlerinde gerçek zamanlı performans ve devam eden süreç özelliklerinin sağlanması gerekmektedir. Bu özellikler genel ticari ağların tasarım gereklilikleri arasında yer almamaktadır. Bu nedenle ticari ağlarda bulunmayan ve akıllı şebeke ağlarının ihtiyacı olan gereksinimlerin de eklenmesiyle akıllı şebekelerde siber güvenlik hedefleri sağlanabilir [22].

Akıllı şebeke haberleşme altyapısı gibi karmaşık sistemlerin güncellemesi de yeni güvenlik açıklıklarının ortaya çıkmasına neden olabilmektedir. Bu nedenle, akıllı şebekelerde dikkat edilmesi gereken hususlardan birisi de güvenli şekilde sistem güncellemelerinde, sistem bileşenleri tarafından doğrulama sorularının (kod, model, seri numarası, vb.) kullanılması gerekmektedir. Baumeister gerçekleştirdiği çalışmada, akıllı şebeke siber güvenliğine yönelik genel bir değerlendirme yapmıştır. Çalışma da, akıllı şebeke bileşenleri 5 kategoride gruplandırılmıştır. Bunlar: Süreç kontrol Sistemi, Akıllı Sayaç Güvenliği, Güç Sistemi Durum Değerlendirme Güvenliği ve Güvenlik Analizleri için Akıllı Şebeke Simülasyonudur [23]. Ancak akıllı şebekeler oldukça büyük karmaşık sistemlerdir ve bu nedenle birçok bileşenine yönelik önemli siber güvenlik tasarımı çalışmasına ihtiyaç duymaktadır.

2.1. Akıllı Şebeke Altyapısı

Bir akıllı şebeke haberleşme sistemi birçok alt sistemden oluşmaktadır. Diğer bir ifadeyle birçok alt ağdan oluşan bir ağdır. Söz konusu alt sistemlerden en önemlilerinden birisi de, akıllı şebeke sistemlerinin merkezinde bulunan EKS çözümüdür. EKS, akıllı şebekelerde sadece bir kontrol sistemi değil, aynı zamanda bir haberleşme sistemidir. Akıllı şebeke sistemlerindeki haberleşme ağları; karasal mobil telsizleri (Land Mobile Radios-LMR), hücresel haberleşme, mikrodalga, fiber optik, güç şebeke haberleşmesi (Power Line Communication-PLC), RS-232/RS-485 seri hatlar gibi kablolu hatları, kablosuz yerel alan ağlarını veya çok yönlü veri ağlarını içerir [24].

Bir EKS, genel olarak algılayıcılar ve diğer donanımlar ile sahadan aldığı bilgileri bir araya getirir, işler, ilgili birimlere iletir, merkezi biriminde görüntüler ve son olarak da ihtiyaç halinde saha donanımlarına kontrol mesajları gönderir. EKS ağları uzak sahalardan verileri alır ve kontrol istasyonu aracılığıyla kontrol mesajları gönderir. Saha bilgileri genellikle Ana Terminal Birimleri (Master Terminal Units-MTU) tarafından görüntülenir.

Günümüzdeki EKS MTU'su yüzlerce Uzak Terminal Birimi (Remote Terminal Unit-RTU) olarak bilinen saha donanımını izleyebilmekte ve kontrol edebilmektedir.

Dağıtım otomasyonu, ortalama gerilim değerlerinin uzaktan kontrolü, yüksek güvenirlilikte tedarik ve düşük maliyetle işlem ve idame EKS ile sağlanmaktadır [25]. EKS için Dağıtık Ağ Protokolü 3 (Distributed Network Protocol 3- DNP 3), Genel Nesne Tabanlı Trafo Aktiviteleri (Generic Object Oriented Substations Events - GOOSE), IEC 61850 ve IEC 608750-5 gibi standartlar geliştirilmiş olsa da, tutarlı güvenlik çözümlerinin uygulanması için yeterli standardizasyon sağlanabilmiş değildir [26].

2.2. Haberleşme Ağları

Akıllı şebekelerde haberleşme ağları, elektrik sistemi otomasyonu uygulamalarını gerçekleştirilebilecek bir ağ yapısında olması gerekmektedir. Bu ağın maliyet-etkin ve güvenilir bir ağ mimarisinde tasarlanması hayati önemlidir. Güngör ve Lampert çalışmalarında, elektrik sistemi otomasyonu için melez ağ mimarisinin fayda ve mahsurlarını incelemişlerdir. Çalışma kapsamında, İnternet tabanlı Sanal Özel Ağlar (VPNs), güç şebekesi haberleşmesi, uydu haberleşmesi ve kablosuz haberleşme (kablosuz algılayıcı ağları, WIMAX ve kablosuz melez ağlar) sistemleri incelenmiştir. Çalışma, heterojen elektrik sistem otomasyonu uygulamalarının gereksinimlerini destekleyen melez ağ mimarisi hakkında özet bir araştırma sağlamaktadır [27].

Farklı ölçek ve yapılardaki akıllı şebeke sistemlerine farklı haberleşme ağı çözümleri uygulanabilmektedir. Örneğin, Gelişmiş Sayaç Altyapısı (Advanced Metering Infrastructure-AMI) çözümleri, kısa yerel kapsamalar veya uzun menzil haberleşme için melez veya uçtan uça yapıda olabilmektedir [28]. Çünkü AMI;

- Akıllı ölçüm sağlar,
- Evdeki uygulamalardan enerji tüketim verilerini toplar,
- Evdeki Enerji Dağılımı hakkında bilgilendirerek karar verme sürecine destek sağlar,
- Komşu Alan Ağı (Neighborhood area Network-NAN) için bir geçit sağlar.

AMI haberleşme vasıtaları ise; kablolu haberleşme için, Ethernet, güç hattı taşıyıcısı (Power Line Carrier-PLC); kablosuz haberleşme için de 802.11, Bluetooth ve ZigBee

teknolojileridir. AMI enerji tüketimine ve ihtiyaçların uygunluğuna göre sistem bileşenlerini gruplara ayırmaktadır. Bu gruplar ve AMI'ye gönderdikleri bilgi mesajları aşağıdaki gibidir;

- 1. Grup: Düşük enerji tüketen donanımlardır (lambalar, laptop şarjı, telefon şarjı, TV, vb.). AMI'ye sadece elektriğe bağlandığında veya bağlantı kesildiğinde mesaj göndermektedir.
- 2. Grup: Yüksek kullanılabilirlik gerektiren yüksek enerji tüketen donanımlardır (fırınlar, ocaklar, buzdolabı). AMI'ye güç kullanım miktarı ve süresini göndermektedir.
- 3. Grup: Düşük kullanılabilirlik gerektiren yüksek enerji tüketen donanımlardır (klimalar, çamaşır makinası ve kurutucu, bulaşık makinesi). AMI'ye belirlenmiş bir miktar ve belirlenmiş bir süre için enerji kullanım talebini göndermektedir. AMI gelene talebe, elektrik fiyatlandırması ve uygunluğa göre evet/hayır cevabını vermektedir.
- 4. Grup: Elektrikli araçlardır (özellikle elektrikli arabalar). AMI, belirlenmiş bir zaman aralığında araçların şarj edilmesini planlamaktadır [29].

Geri taşıma (backhaul) çözüm önerileri ise, fiber, kablosuz geniş bant veya güç şebekesi üzerinden geniş bandı kapsamaktadır. Kablosuz haberleşme çözümleri verilen hizmetin gerekliliğine göre lisanslı veya lisanssız olabilmektedir. Ancak yüksek güvenirlilik gerektiren altyapılarda (özellikle kritik altyapılarda), lisanslı çözümler tercih edilmesi gerekmektedir. Yukarıdaki çözüm önerilerinin çeşitli yönlerden avantajı ve dezavantajı bulunmaktadır ancak tüm çözüm önerilerinin sahip olması gereken temel prensip ise ölçeklenebilir güvenlik çözümüne ihtiyaç duyulmasıdır [30].

2.3. Akıllı Şebeke Kurulumu

Akıllı şebeke kurulumları sıkı güvenlik gereksinimlerini karşılayacak şekilde yapılmalıdır. Tüm kullanıcılar ve şebeke hizmetlerini etkiyebilecek donanımlar için güçlü kimlik doğrulama gerekmektedir. Bu amaçla, çok büyük sayıları (binlerce) bulabilen kullanıcılar ve donanımların güvenliğinin sağlanması için simetrik anahtarların kullanılması ise oldukça maliyetli ve güvensizdir. Bu nedenle geniş ağlar için anahtar ve güven yönetim sisteminin oluşturulması ihtiyacı ortaya çıkmıştır. Çoğunlukla Açık Anahtar Altyapısına dayanan (Public Key Infrastructure-PKI) güven yönetim sistemleri, akıllı şebekelerin güvenliği için oluşturulan standartların ve kılavuzların gereksinimlerini karşılayacak şekilde düzenlenerek kullanılmasıyla kullanıcı doğrulama güvenlik gereksinimi sağlanabilir.

PKI sistemi açık anahtarlar ile kullanıcıların kimliklerini sayısal sertifikalar üzerinden ilişkilendirir. Bu ilişkilendirme (atama) genellikle kayıt otoritesi tarından gerçekleştirilir. Belgelendirme yetkilisi tarafından da kullanıcılara sayısal belgeler dağıtılır. Bu sayede kullanıcı ya da donanım kimlik doğrulaması yaparken bu sayısal belgeleri kullanarak oturum anahtarı oluşturur ve sırasıyla şifreleme ve çözme işlemlerini yapabilir [31].

2.4. Akıllı Şebeke Güvenliği Gereksinimleri

Bir akıllı şebekenin güvenirliliği, kontrol ve haberleşme sistemlerinin güvenirliliğine dayanmaktadır. Haberleşme sistemleri teknolojilerinin de daha iyi kontrol ve yüksek güvenirliliği sağlamak için daha karmaşık hale gelmesiyle birlikte, akıllı şebekeler yeni özellikleri desteklemek için daha yüksek derecede dış ağlara özellikle de internete bağlantı ihtiyacı duymaya başlamıştır. Ancak söz konusu dışa ağlara bağlılık beraberinde siber güvenlik açıklıklarını ve ihlallerinin oluşmasına neden olmaktadır. Bu nedenle, söz konusu bağlantılar, siber güvenlik gereksinimleri kapsamında geliştirilen çeşitli standartların gerekliliklerini yerine getirmeleri gerekmektedir [32].

Elektrik Güç Araştırma Enstitüsü (Electric Power Research Institute-EPRI)'ne göre akıllı şebekelerin düzenlenmesinde karşılaşılan en büyük zorluk sistemlerin siber güvenliğiyle ilgilidir [33]. Akıllı şebeke haberleşme güvenliği kapsamında çalışan çeşitli kuruluşlar ve bu kuruluşlar tarafından oluşturulan çeşitli standartlar bulunmaktadır. Kuzey Amerika Elektrik Emniyet Kurumu- Kritik Altyapı Koruma (North America Electric Reliability Coorporation- Critical Infrastrusture Protection-NERC-CIP) [34], Uluslararası Otomasyon Kurumu (International Society of Automation-ISA) [35], IEEE 1402, Ulusal Altyapı Koruma Planı (National Infrastructure Protection Plan-NIPP) [36] ve Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards and Technology-NIST) [37] başta olmak üzere dünya genelinde birçok kurum ve kuruluş, akıllı şebekelerin siber güvenlik programları konusunda çalışma yapmaktadır.

Bu kuruluşların yanında, akıllı şebekelerin haberleşme sistemlerini geliştirirken aynı kapsamda geliştirilen ISO 17799 (27000 ailesi), Federal Bilgi İşleme Standardı (Federal Information Processing Standard-FIPS) 201, NIST ve diğer kurumların güvenlik standartlarını dikkate alınması, daha güvenli, tutarlı ve ölçeklendirilebilir sistemlerin kurulmasında oldukça önemlidir [38]. Söz konusu standartların içeriği incelendiğinde,

şebekelerin güvenliğinin kimlik doğrulamaya, yetkilendirmeye ve şifreleme (gizlilik) teknolojilerine dayandığı görülmektedir. Özellikle şifreleme teknolojileri oldukça gelişmiş durumdadır. Örneğin FIPS, Gelişmiş Şifreleme Standardı (Advanced Encrpytion Standard-AES) [39] ve Üçlü Veri Şifreleme Standardını (Triple Data Encyrption Standard-3DES) [40] güçlü güvenlik ve yüksek performans sağlaması nedeniyle onaylamaktadır. Ancak şifreleme teknolojilerinin seçimi daha çok korunması gereken haberleşme sisteminin kritikliğine ve risklerine göre değişmektedir. Çünkü gelişen yeni saldırı teknikleri ve saldırganların engin kaynaklara ulaşabilmesi sonucu bu çözüm önerileri de yakın bir gelecekte yeterince koruma sağlamayacaktır. Örneğin NIST 2030 yılı itibariyle 3DES çözümünün tamamen güvensiz hale geleceğini belirtmektedir.

Bu nedenle teknolojik gelişmelere yapılan yatırım kadar bu teknolojilerin güvenlik boyutuna da yatırım yapılması gerektiği unutulmamalıdır. Bu seçimde önemli olan, kurumun riskin kabullenme derecesi ve bilginin kritikliğidir. Maliyet etkinlik faktörü de dikkate alınması gereken diğer bir etkendir.

Kablosuz şebekelerin güvenliği için de IEEE 802.11i [41] ve IEEE 802.16e [42] standartları kullanılabilmektedir. Farklı kablosuz protokollerin güvenlik düzeyi dereceleri de değişmektedir. Kablolu şebekelerin güvenliği ise, VPN'ler, IPSec teknolojileri ve güvenlik duvarlarıyla sağlanmaktadır. Yüksek katman güvenlik mekanizmaları olan Güvenli Kabuk (Secure Shell-SSH) ve SSL/TSL de kullanılabilmektedir [43].

2.4.1. Gizlilik

Akıllı şebeke haberleşme sistemlerinde gizlilik konularını, özellikle ölçüm cihazlarında tutulan kullanıcıların tüketimine ilişkin verilerle birlikte değerlendirmek gereklidir. Çünkü söz konusu tüketim verilerinin detayları kullanıcıların davranışlarını tespit etmeye kadar birçok bilgiye kaynak olabilmektedir. Akıllı şebekelerinin haberleşmesinin kullanıcı mahremiyeti yönünden istenmeyen sonuçları mevcuttur. Akıllı sayaçların gelişmesiyle abonelerin elektrik kullanım bilgisi sayaçlarda depolanmaktadır. Sayaçların ele geçirilmesiyle kullanıcıların tutum ve davranışları hakkında bilgiler kötü niyetli kişilerin eline geçebilecektir [44].

Sadece altyapıları yöneten veya donanımları işleten şirketler potansiyel gizlilik saldırılarının kaynağı değildir. Örneğin, Google Güç Sayacı (PowerMeter) hizmeti akıllı sayaçlar üzerinden gerçek zamanlı kullanım istatistiklerini almaktadır. Bu hizmete üye olan kullanıcılar kendilerine özel bir web sayfası üzerinde yerel kullanımlarını görebilmektedirler. Ancak kullanıcıların yanında bu bilgiler üçüncü taraf olarak nitelendirilen kurum ve kuruluşlar ile de paylaşılmaktadır [45]. Bu verilere yapılacak işlemlerin cezai müeyyidesinin çok düşük ya da hiç olmadığı dikkate alındığında söz konusu verilerin çeşitli kaynaklar tarafından kullanmak üzere hedeflenmektedir.

2.4.2. Erişebilirlik (Kullanılabilirlik)

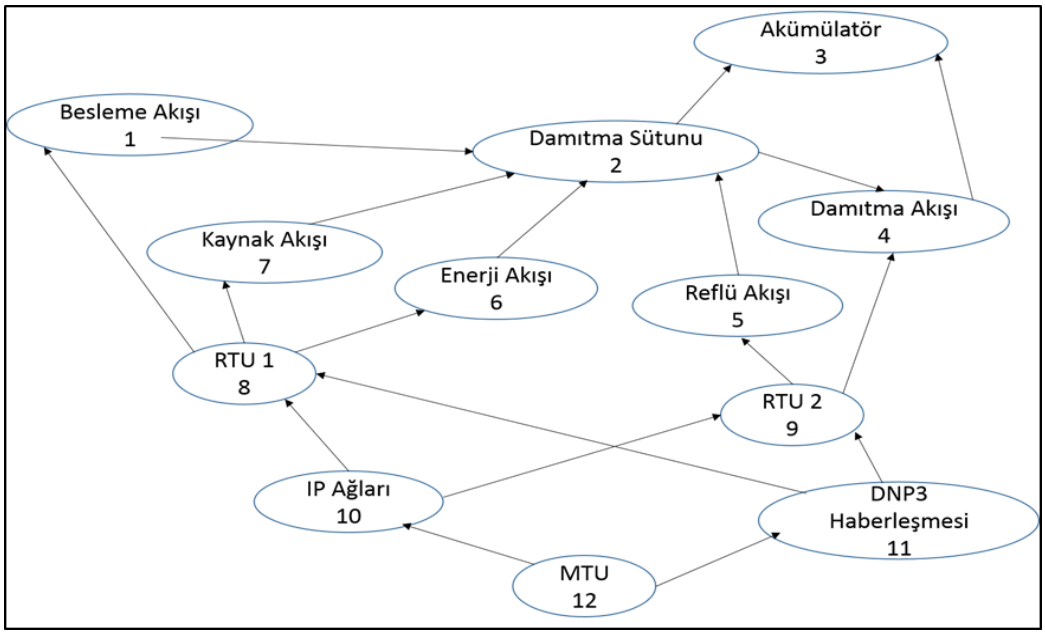
Erişebilirlik yetkisiz personel ya da sistemlerin erişimini engellememesi, dolayısıyla yetkili kullanıcıların sisteme ve izin verilen kaynakları kesintisiz kullanabilmesi olarak tanımlanabilir. Akıllı şebekeler için de, kontrol sistemleri, emniyet sistemleri, operatör iş istasyonları, üretim sistemleri ve haberleşme sistemleri gibi tüm bilgi teknolojileri bileşenlerinin haberleşme sistemleri aracılığıyla bileşenler arasında birbiriyle veya ağ dışındaki başka bir birimle haberleşebilmesi olarak tanımlanmaktadır [46].

Erişebilirliği hedef alan zararlı saldırıların en başında, gecikmeye, tıkamaya ve hatta akıllı şebeke içerisinde bilgi değişimi ihtiyacı bulunan haberleşme düğümlerine ağ kaynaklarına bilgi iletimini kesmeyi hedefleyen Servis Reddi (Denial of Service) ve Dağıtık Servis Reddi (Distributed Denial of Service) saldırıları gelmektedir. Akıllı şebekeler, kritik zaman görevleri nedeniyle DoS saldırılarına karşı oldukça hassastır [46-48].

Yetkisiz giriş yapan (intruder) saldırganlar, akıllı şebekelerde güvenilir ağlar yerine sadece haberleşme kanallarına bağlanmaları yeterli olabilmektedir. Saldırganlar için akıllı şebeke haberleşme ağlarına ve özellikle karıştırma saldırılarına hassas olan kablosuz haberleşme ağlarına DoS saldırısı düzenlemeleri oldukça kolaydır [49, 50]. Bu nedenle, akıllı şebekeler üzerinde DoS saldırılarının etkilerine karşı değerlendirmeler yapmak ve bu tip saldırılara karşı etkin karşı önlemler almak oldukça önemlidir.

Bu kapsamda alınabilecek önlemlerden birisi, sistemi meydana getiren birimlerin belirlenmesidir. Sonra bu birimlerin birbiri ile olan bağlantısının Şekil 2.1'de gösterildiği gibi matris (erişebilirlik) şeklinde oluşturulmasıdır. En son birimlerin kurum/kuruluş

yönünden kritikliklerine ve önem derecelerine göre taktik, operatif ve stratejik seviyelere ayırarak bölümlendirilmesidir. Erişebilirlik matrisi ve seviye bölümlendirmesinin oluşturulması durumda, risk değerlendirme sürecinin tamamlanmasını müteakip risk azaltma sürecinde ilk müdahale edilecek varlıklar tespit edilerek, olası bir risk ya da problem durumunda tepki süresi kısalacak ve sistemin alacağı hasar en aza indirilebilecektir [51]. Erişebilirlik matrisi, hata tespiti için öncelikli hazırlanması gereken süreçlerden birisidir [52]. Yanlış bileşenlerin belirlendiği bir hata matrisi durumunda hata giderme süreci uzayabilmektedir [53].



Şekil 2.1. Erişebilirlik matrisi

2.4.3. Bütünlük

Bütünlük bilginin yetkisiz kişi veya sistemlerce değiştirilmesinin engellenmesidir. Akıllı şebeke haberleşme sistemleri için bütünlük, ürün tarifeleri, algılayıcı değerleri veya kontrol komutları bilgilerinin değiştirilmemesidir. Bu hedef, mesaj enjeksiyonu, mesaj tekrarı veya ağ üzerinde mesajların geciktirilmesi aracılığıyla yapılan değişikliklerin engellenmesini kapsamaktadır. Bütünlüğün ihlali, donanımların veya daha da kötüsü insanların zarar görmesiyle sonuçlanabilecek güvenlik konularına neden olabilmektedir.

Bütünlüğe karşı yapılan saldırılar erişebilirliğe karşı yapılan saldırılara kıyasla daha karmaşıktır. Bütünlük saldırılarının hedefi, kullanıcı bilgileri (fiyatlandırma bilgileri ve

kullanıcı hesap dengesi gibi) olabileceği gibi, ağ faaliyet bilgileri de (voltaj okumaları, donanım çalışma durumu gibi) olabilmektedir. Diğer bir ifadeyle, bu tip saldırılar, akıllı şebekelerdeki kritik veri değişimini engellemek için akıllı şebeke haberleşme sistemindeki orijinal bilgilerin kasten değiştirilmesine teşebbüs edebilmektedir.

Enerji iletim yada dağıtım şebekelerine karşı yapılan saldırılar önemli oranda bütünlüğe yönelik saldırılardır. Y. Liu, P. Ning ve M. Reiter güç şebekesinde sürekli durum değerlendirmesi yaparak sisteme giden verilerin bütünlüğünü bozmaya yönelik hatalı veri enjeksiyonu yaparak durum analizi gerçekleştirmişlerdir. Saldırı sonrasında, saldırganın bir sayacı tehlikeye attığını ve verilerin bütünlüğü değiştirerek izleme merkezine hatalı verileri gönderdiği ve sonuçta da Güç Sisteminin ayarlarının değişmesine sebep olduğu görülmüştür [54].

Akıllı şebeke haberleşme sistemlerinin güvenliğine ilişkin temel gereksinimler olan gizlilik, erişebilirlik ve bütünlük ile birlikte bulunması gereken diğer gereksinimler aşağıda özetle belirtilmiştir.

Kimlik Doğrulama: Haberleşme sistemine doğru katılımcının (geçerli kullanıcı adı), diğer bir ifadeyle sistem tarafından yetki tanınan bir kullanıcının giriş yapıp yapmadığını tespit etmektir. Diğer güvenlik hedefleri ise özellikle de yetkilendirme, yasal ve yasal olmayan kullanıcıları kimlik doğrulama özelliğine dayanarak tespit etmektedir.

İnkar Edememe: İnkar edememe, genellikle hesap verebilme ve şeffaflık (açıklık) hedeflerinin kurulmasını sağlar. Gönderilen veri veya mesajla ilgili tutulan kayıtlar (log) sayesinde kimlik, zaman, vb. bilgilerin inkar edilememesidir. Akıllı şebeke sistemleri kapsamında ise, düzenleme gereksinimleri açısından en önemli hedeflerdendir. Çünkü bu güvenlik gereksinimin ihlali genellikle yasal veya ticari sonuçlara neden olmaktadır.

Denetlenebilirlik: Özellikle bir saldırı gerçekleştiğinde veya saldırı sonrasında sistemde meydana gelen zarar ve değişikliklerin tespitini kapsamaktadır.

Yetkilendirme: Erişim kontrolü olarak da adlandırılmaktadır. İzin verilmeyen kullanıcı ya da sistemlerin, kaynaklara erişiminin engellenmesini kapsamaktadır. Yetkilendirmenin hatalı yapılması ya da ihlal edilmesi güvenlik açıklıklarına neden olabilmektedir.

Üçüncü-Ortak Koruması: Akıllı şebekeler, en alt bileşenlerinin dahil olduğu bütünsel bir güvenlik anlayışıyla koruma sağlanmalıdır. En zayıf halka teorisi kapsamında bir sistem en zayıf bileşeni kadar kuvvetlidir ve o bileşene yapılan saldırı başarı kazandığı takdirde sistemin en kritik bileşenine de erişim sağlayabileceği dikkate alınarak, özellikle yetkilendirme ve erişim kontrolü hedefleri sağlanarak tüm sistemin güvenliği sağlanmalıdır.

Güven: Geleceğin akıllı şebeke haberleşme sistemlerinin tasarımı çok-katmanlı mimariye dayanmaktadır. Akıllı şebeke sistemlerinin gelişimi, birçok farklı programlama dili ve platformunda geliştirilen yazılım uygulamalarıyla çalışan oldukça fazla güç sistemlerini içermesine neden olmuştur. Yeni geliştirilen sistemlerle eski uygulamaların aynı altyapıda bulunması da bütünleşik bir yapı olmasını engellemektedir. Bu nedenle de, bu kadar karmaşık bir yapıya sahip geniş bir sistemin güvenliğini sağlamak uyum sorunları da eklenince oldukça zor olmaktadır.

Akıllı şebeke haberleşme sistemlerindeki gelişmelere paralel olarak, mutlak ve tek parça siber güvenlik altyapısı geçerli bir seçenek olmaktan çıkmıştır. Bunun yerine, çok katmanlı mimari yapısı, gelişmiş kontrol yöntemleri ve güvenilir yazılım altyapısı ile donanım koruma ve izleme mekanizmaları daha geçerli bir çözüm olarak görülmektedir. Bu özelliklere ilave olarak, ağ mimarisinin sadece belirli bölümlerin güvenli biçimde güncellenmesi yada değişimine imkan sağlayan esnek bir yapıda olması gereklidir [55].

2.5. Akıllı Şebeke Haberleşme Güvenliğinde Karşılaşılan Zorluklar

Akıllı şebekeler, geleceğin elektrik, su, doğal gaz, telekomünikasyon başta olmak üzere kritik altyapı ağlarının ihtiyaçlarına cevap verebilmek için, birbirinden farklı standart ve düzenlemelerle bir araya getirilen bileşenlerden oluşan bir yapıya sahiptir. Ancak söz konusu ihtiyaçlara cevap verebilmek için akıllı şebeke haberleşme sistemi siber güvenlik gereksinimlerinin, mimari gereksinimleri temelinde belirlenmiş olması gerekmektedir.

Güvenli bir akıllı şebeke haberleşme sisteminde karşılaşılan en önemli zorluk, ağlar arası çalışmayı, güvenlik politikalarını ve işlemlerini, güvenlik servislerini, etkinliği, ölçeklenebilirliği ve ticari ağlar ile akıllı şebeke ağ güvenliği arasındaki farklılıkların belirlenmesini kapsamaktadır.

2.5.1. Ağlar arası birlikte çalışabilirlik

Birbirine bağlı akıllı şebeke haberleşme sistemleri birçok uygulama veya donanımdaki güvenlik eksiklikleri nedeniyle oluşan açıklıklara karşı hassas durumdadır. Akıllı şebekelerin siber savunma katmanları kesintilere, duraklamaya, istenmeyen değişikliklere ve sahteciliğe karşı koruma sağlaması gerekmektedir.

Etkinlik, maliyet tasarrufu ve geniş bilgi sistemlerine entegrasyon gibi sebeplerle, akıllı şebekeler artık ayrı haberleşme ağını kullanmamaktadırlar. Bunun yerine, kurumun diğer birimleriyle bilgilerin paylaşıldığı ortak bir ağa hatta İnternete bağlıdırlar. Bu değişiklik akıllı şebeke haberleşme sistemlerinin risk profilinde farklılıklara ve İnternetin genel problemleri ve tehditlerine maruz kalmalarına neden olmuştur. Sonuçta da, genellikle ticari amaçlı kullanılan İnternete bağlantılı olan akıllı şebekeler güç kaynaklarının kesintisine neden olan birçok saldırıya açık durumdadır [44, 45]. Güvenlik tehdit seviyelerindeki bu artış, güvenli ve sorunsuz bir akıllı şebeke haberleşme sistemini temin etmek için daha zorlu bir yönetim ihtiyacını ortaya çıkarmıştır. Bu nedenle, akıllı şebeke ağlarından İnternete yapılan bağlantıların tamamı yüksek güvenlikli olmalıdır. Ayrıca saldırı tespit sistemlerine sadece akıllı şebekelerin İnternete çıkış noktalarında değil aynı zamanda ağ içerisindeki kritik noktalarda ve hassas kablosuz arayüzlerde ihtiyaç vardır [56].

Akıllı şebeke sistemlerinin izole olmaması nedeniyle siber saldırı ihtimali her zaman mevcuttur. Sayısal verilerle uzaktan erişimin avantajları yanında birçok riskleri de vardır. Oluşabilecek açıklıkları en aza indirebilmek için, akıllı şebekelerin haberleşme sistemlerinin sürekli izlenmesi, verilerin incelenmesi gerekli analizlerin yapılması gerekmektedir [57-59].

Bir sistemin veya donanımın kritikliği saldırılarla karşı karşıya kalma eğilimini belirlemektedir. Siber saldırılar incelendiğinde de özel ağların bu tip saldırılarla daha az karşılaştığı görülmektedir [60].

2.5.2. Akıllı şebeke haberleşme güvenlik politikası

Bir akıllı şebekede güvenirlik şebekeyi meydana getiren bileşenlerin faaliyetlerine ve aradaki iletişime bağlıdır [61]. Bir akıllı şebekenin iletişimini engellemek için, saldırganlar

ortamdaki açıklıkları kullanarak sistem bileşenlerine ve özellikle de yönetim birimlerine erişir. Eriştiği sistem bileşenlerini başka bir cihaz gibi yapılandırabilir ve bu sayede sisteme zarar verebilecek veya yanlış bilgiler göndererek sistemi çalışmaz hale getirebilir. Akıllı şebekelere yapılan en basit saldırı türlerinden biriside, saldırganların ele geçirdikleri cihazın sistem kaynaklarını aşırı kullanmasını sağlayarak, diğer bileşenler tarafından kaynakların kullanılmasını engelleyen DoS saldırısıdır. Çünkü son zamanlarda İnternet hizmetlerinin kullanılabilirliğine karşı en önemli tehditlerden birisi DoS ve DDoS saldırılarıdır. Örneğin 2009 yılında DDoS saldırı miktarı % 20 artmıştır ve buna paralel olarak da İnternet Servis Sağlayıcılarının (Internet Service Provider-ISP) ve müşterilerinin ilk problemi köle bilgisayar ağı tabanlı DDoS saldırıları haline gelmiştir [62]. DDoS saldırıları yapısı itibari ile kurbanlar tarafından fark edilebilen saldırılardandır. Her ne kadar farkedebilir saldırılardan olsalarda önemli olan saldırıların hizmetlerin kullanımını engellenmeden en kısa sürede farkedilmesidir veya taşkın etkisi oluşmadan farkedilip önlenmesidir [63].

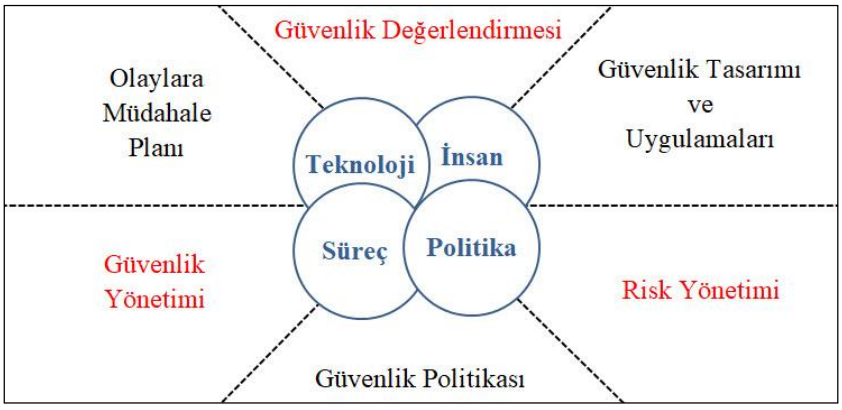
Uluslararası kuruluşlar da dahil olmak üzere gün geçtikçe sayısı artan şekilde birçok kurum, akıllı şebekelerde yer almaktadır. Bu artışa paralel olarak, dağıtık yapı halinde bulunan akıllı şebeke haberleşme sistemine uzaktan erişmek isteyen donanım ve kişilerin sayısı da artacaktır. Bunun neticesinde birleşik varlık yönetime ihtiyaç duyulmaktadır. Bu yapıda bulunan bir yönetimin güvenliğine yönelik çeşitli çözüm önerileri bulunmaktadır. Bunlar arasında, SAML (Security Assertion Markup Language- Güvenlik Onaylama İşaretleme Dili) [64], Güvenli Web Servisleri (WS-Trust) [65] ve PKI [66] çözümleri bulunmaktadır. Sadece satıcıların sunduğu teknik çözümler yeterli olmamakta, bununla birlikte kuruluşların bu çözümlerle tutarlı güvenlik politikaları oluşturması da gerekmektedir. Kurum ve kuruluşlar güvenlik politikalarını ve uygulamalarını oluştururlarken dikkat edilmesi gereken konulardan birisi de birlikte çalışabilirliktir. Birlikte çalışabilirliğin sağlanması için yapılacak çözüm önerilerinden birisi endüstriyel standartların kullanılması ya da yeni standartlarının oluşturulmasıdır [67].

2.5.3. Güvenlik servisleri

Akıllı şebekelerin güvenlik çözümlerinin geliştirilmesi, kurulması ve bütünleştirilmesi kadar, yönetilmesi ve idame ettirilmesi de önemlidir. Güvenlik servisleri, ağ işletmenlerine

akıllı şebeke haberleşme sistemindeki güvenlik risklerinin tanımlanmasında, kontrol edilmesinde ve yönetilmesinde önemli bir yardımcıdır.

EPRI'ye göre, akıllı şebekelerin tüm boyutlarının güvenli olması gerekmektedir [33]. Bu nedenle, siber güvenlik teknolojileri, güvenlik politikaları, risk değerlendirmeleri ve en önemli boyutlardan birisi olan eğitim ve farkındalık olmadan tam anlamıyla bir güvenlik sağlanamaz. Çünkü güvenlik açıklıkları, yapılan çalışmalarda da görülmektedir ki en çok insan faktörüne bağlı olarak ortaya çıkmaktadır [68]. Sistem başındaki insanın aşılması ile antivirüs yazılımları, saldırıları rapor eden sistemlerin aşılması veya güvenlik duvarlarının aşılması çok daha kolay olmaktadır. Çünkü tüm teknolojik düzenlemeler ve güvenlik politikaları geliştirilse ve belirlense bile farkındalığı eksik kullanıcılar bu teknik çözümlerin tamamını etkisiz hale getirecektir [69]. Bilgi güvenliği açıklıkları tam olarak hiçbir zaman tam olarak yok edilememekle beraber, çalışanlarda bilişim güvenliği farkındalığının geliştirilmesi ve bu farkındalığın davranışa dönüştürülmesi sayesinde kabul edilebilir bir düzeye indirilebilir [70]. Akıllı Şebekeye ait Güvenlik Servisleri genel olarak Şekli-2.2.'de belirtilmiştir.



Şekil 2.2. Akıllı şebeke güvenlik servisleri [68]

2.5.4. Etkinlik ve ölçeklenebilirlik

Akıllı şebekeler gibi kritik sistemlerde, sistem erişebilirliği (kullanılabilirlik) yüksek öncelikli gereksinimlerdendir. Bu sebeple, bazı anahtar özelliklere sahip olunması gerekmektedir. Bunlardan ilki, haberleşme kaynaklarının etkin kullanımıdır. Bu sayede tüm kullanıcı isteklerine cevap verilebilecek dengeli bir politika izlenebilecektir. İkincisi, iyi bir hata yönetim sistemine sahip olunmasıdır. Üçüncüsü, yeterli yedekleme sistemlerine

sahip olunarak, tüm sistemin çökmesinin engellenmesi ya da sistemlerin çökmesi durumunda en kısa sürede faal hale getirilmesidir. Dördüncüsü ise; siber saldırıları tespit edip, cevap verebilecek yedekli güvenlik fonksiyonlarını desteklemesidir [61].

2.6. Uluslararası Akıllı Şebekelerle İlgili Güvenlik Standartları

ABD Ulusal standart ve teknoloji kuruluşunun (NIST) yaptığı tanıma göre akıllı şebeke terimi, elektrik iletim sistemlerinin modernizasyonuna karşılık gelmektedir Bu yüzden birbirine bağlı unsurlarının çalışmasını otomatik olarak optimize eder, izler ve olumsuz durumlara karşı korur. Bu tanımda, akıllı şebekeler günümüzün güç sistemlerinden geleceğin bilgi ve iletişim teknolojilerine dayalı güç sistemlerine geçiş olarak tanımlanmıştır. Avrupa Teknoloji Platformu (ETP)'nun tanımına göre de akıllı şebeke, ona bağlı olan tüm kullanıcıların işlemlerini sistem dahil eden, bu sayede devamlı, ekonomik ve güvenli elektrik kaynakları sağlayan bir elektrik ağıdır. Bu tanımda ise akıllı şebeke hedeflenen bir elektrik mimarisidir. Sonuç olarak NIST yönteme vurgu yaparken, ETP ise hedefi tanımlar. Çeşitli uluslararası kuruluşlar akıllı şebekelerin kullanıldığı sektöre ve kritiklik durumlarına göre akıllı şebekeye yönelik tanımlar, öncelikler, gereksinimler, hedefler ve ilkeler belirlemişler [38]. Özellikle elektrik altyapılarında sistemin düzgün çalışması, bilginin korunması, saldırılara karşı korunma yöntemleri gibi konuları düzenlemek amacıyla çeşitli kuruluşlarca oluşturulan bazı güvenlik standartları vardır. Bu standartlar; giriş kontrolü, güvenlik duvarları, saldırı tespit sistemleri, protokol açıklık analizi, kriptografi ve anahtar yönetimi, cihazlar ve işletim sistemleri güvenliği ile güvenlik yönetimi konularını düzenler. Standart oluşturan kuruluşlardan bazıları şunlardır [71, 72] ;

- IEEE (Institute of Electrical and Electronic Engineers- Elektrik Elektronik Mühendisleri Kurumu)
- NIST (National Institute of Standards and Technology- Ulusal Standartlar ve Teknoloji Kurumu)
- CSD (Computer Security Division- Bilgisayar Güvenliği Başkanlığı)
- CSRC (Computer Security Resource Center- Bilgisayar Güvenliği Kaynakları Merkezi)
- ISO/IEC (Organization for Standardization/International Electrotechnical Comission)
- NERC (The North American Electric Reliability Corporation-Kuzey Amerika Elektrik Güvenilirlik Şirketi)

- FERC (The Federal Energy Regulatory Commission-Federal Enerji Düzenleme Komisyonu)
- CPNI (Centre for the Protection of National Infrastructure- Ulusal Altyapıları Koruma Merkezi)
- ISA (Instrumentation, Systems, and Automation Society-Enstrümantasyon, Sistemler ve Otomasyon Kuruluşu)
- EPRI (Electric Power Research Institute –Elektrik Güç Araştırma Kurumu)

Yukarıda belirtilen kuruluşlar tarafından oluşturulan ve uluslararası alanda geçerliliği olan akıllı şebekelere yönelik standartlar hakkında aşağıda kısaca bilgi verilmiştir.

2.6.1. ISO 27000 serisi

ISO 27001 standardı, yaşayan bir bilgi güvenliği kapsamında gerçekleştirilmesi gereken işlevleri tanımlar. ISO 27001 standardı kurumların bilgi güvenliği yönetim sistemi (BGYS) kurmaları için ihtiyaçları tanımlayan tek denetlenebilir BGYS standardıdır [73]. 2005 yılında yayınlanan ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı veya kısa ifadesiyle ISO 27001, 1998 yılında BSI (British Standartds Institute) tarafından yayınlanan BS-7799-2 standardının ISO tarafından kabul edilmiş ve yenilenmiş şeklidir. BSI tarafından yayınlanan BS 7799-1 ise ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. Temmuz 2007 tarihine kadar ISO/IEC 27002 standardı ISO/IEC 17799:2005 olarak adlandırılmıştır. ISO/IEC 27001, BGYS için şart olan gereksinimleri tanımlarken, ISO/IEC 27002 ise, bir sertifikalandırma standardından ziyade BGYS için uygulama esaslarını sunar. Ancak organizasyonlar diğer bilgi güvenliği denetim takımlarını da seçmekte özgürdürler. ISO/IEC 27001, giriş bölümleri dışında 12 ana bölümden oluşmaktadır. Bunlar;

Risk yönetimi: Risk değerlendirme, risk analizi, riski azaltma.

İnsan kaynakları güvenliği: Sistem çalışanlarının eğitilerek bilgi kaybı, dolandırıcılık veya kaynakların kötüye kullanılma riskini azaltmak. Sistem erişimi yönetimi, güvenlik farkındalığı, eğitim ve öğretim.

Güvenlik politikası: Bilgi Güvenliği için geliştirilen prensipler ve aksiyomlar, politikalar, standartlar, rehberler ve prosedürler.

Bilgi güvenliğinin organizasyonu: Bilgi güvenliğinin eşgüdümü ve idamesi için bir yönetim çerçevesinin geliştirilmesi. Yapı, raporlama, irtibat.

Fiziki güvenlik ve çevre güvenliği: Sistemdeki bilgi işlem olanaklarına yetkisiz erişimi önlemek ve bilgilerin kaybolmasını veya çalınmasını engellemek. Fiziki erişim; havalandırma; yangın / su baskını; enerji / güç kaynakları.

İletişim ve operasyon yönetimi: Sistemin uygun ve güvenli kullanımını sağlamak ve kritik olaylara karşı müdahale planları geliştirerek riskleri azaltmak. Arşivleme, yedekleme, loglama, yamalama, izleme, yapılandırma.

Varlık yönetimi: Tüm kritik ve hassas varlıklar için uygun bir koruma düzeyi belirlemek. Envanter, sınıflandırma, sahiplik.

Erişim denetimi: Yetkisiz erişimleri tespit etmek ve ağ sistemlerinin korunması için gerekli kontrol faaliyetlerini sağlamak. Fiziki erişim, ağ erişimi, sistem erişimi, uygulama erişimi, fonksiyon çalıştırma (NAC) .

Bilgi sistemleri edinimi, geliştirme ve bakımı: İşletim sistemlerini ve uygulama yazılımlarını bilgi kaybına karşı güncellemek ve kayıpları engellemek. Gereksinim, tasarım; geliştirme/edinim, test, uygulama, bakım ve destek (DLP).

Bilgi güvenliği ihlali olay yönetimi: Etkin bir bilgi güvenliği sağlamak için olayları zamanında tespit etmek ve gerekli önlemleri almak. Hazırlık, tanımlama, reaksiyon, yönetim ve içerik, çözüm, öğrenme.

İş sürekliliği yönetimi: Doğal afetler, olası arızalar, kritik olaylardan kaynaklanan kesintilere karşı hızlı müdahale için kapasite artırma faaliyetleri gerçekleştirmek. Dirençlilik, afet yedekleme/kurtarma.

Uyumluluk: Mevcut güvenlik politikalarının tüm yasalara ve yönetmeliklere uygun olduğundan ve üst yönetim onayından geçtiğinden emin olmak. Denetim, yasa ve düzenlemeler, güvenlik politikaları-standartları ve teknik uyumluluk [71, 74].

2.6.2. NIST SP 1108, sistem ve akıllı şebeke birlikte çalışabilirlik yol haritası

Standart, NIST FERC'in akıllı şebekeler için belirlediği öncellikler üzerinden başlamıştır ve kendisinin belirlediği konuları eklemiştir. Belirlenen 8 öncelik aşağıdadır:

- Taleplerin karşılanması ve tüketici enerji yeterliliği
- Geniş-alan uygulama farkındalığı
- Enerji depolama
- Elektrik taşıması
- İleri seviye ölçme altyapısı
- Dağıtım şebekesi yönetimi
- Siber güvenlik
- Ağ iletişimi

Enerji Bağımsızlık ve Güvenlik Antlaşmasının (EISA - 2007) gereklerini yerine getirmek ve akıllı şebekelerin kurulumunda başlangıçta gerekli olan standartları belirlemek için NIST 3 safhalı bir plan önermiştir.

- Açık süreçte uygulanabilir standartları ve gereklilikleri, mevcut standartlardaki boşlukları ve öncelikleri belirlemek için paydaşlarla meşgul olmak,
- Uzun dönem çalışabilirliği sağlamak için akıllı şebekelerin karşılıklı kullanılabilirliğini oluşturmak,
- Uyum testi ve sertifikasyonu için bir çerçeve geliştirmek ve uygulamak [75].

2.6.3. IEEE standardı 2030 serisi

IEEE Standard 2030-2011, elektrik güç sistemleri ile bilgi teknolojileri ve enerji teknolojilerinin birlikte kullanılabildiği akıllı şebekeler için bir rehber sağlar. Akıllı şebekelerde IEEE standartlarını içeren birleştirilmiş ilk kapsamlı uygulamadır. 2030 standardını tamamlayıcı ilave 3 standart bulunmaktadır.

- IEEE P2030.1, Elektrik Kaynaklı Taşıma Altyapıları için Rehber
- IEEE P2030.2, Elektrik Güç Altyapılarına Entegre Edilmiş Enerji Depolama Sistemlerinin Birlikte Kullanılabilirliği Hakkında Rehber
- IEEE P2030.3, Elektrik Enerji Depolama Ekipmanları ve Sistemleri için Test Prosedürleri Rehberi [76].

2.6.4. ISO/IEC 15408 standardı

Ortak kriter (Common Criteria-CC), bilgi teknolojisi ürünleri için uluslararası çapta kabul gören bilgi güvenliği değerlendirme kriteridir. Bilgi güvenliği değerlendirme kriterleri olarak kabul edilen Avrupa'daki ITSEC, ABD'deki TCSEC ve Kanada'daki CTCPEC'nin (Canadian Trusted Computer Product Evaluation Criteria) birleştirilmesi sonucu oluşturulmuştur. CC, ISO/IEC 15408 standardında tanımlanmaktadır.

CC Bölüm 1 (Standarda Giriş): CC temel güvenlik değerlendirmelerini verir.

CC Bölüm 2 (Güvenlik Fonksiyonel İhtiyaçları Kataloğu): Bir ürünün sağladığını iddia ettiği güvenlik fonksiyonlarını standart bir yolla ifade etmede kullanılabilecek "sınıf", "aile" ve "bileşenler" i içerir.

CC Bölüm 3 (Güvenlik Garanti İhtiyaçları Kataloğu): Bir ürünün güvenlik özelliklerini nasıl garanti ettiğini standart bir yolla ifade etmede kullanılabilecek "sınıf", "aile" ve "bileşenler" i içerir. Ayrıca EAL (Evluation Assurance Level) seviyelerini tanımlar [71].

2.6.5. ISO/IEC 62351

Enerji sistemleri yönetimi ve bilgi paylaşımı için veri ve iletişim güvenliği konularını kapsar. İletişim protokolleri ile ağ ve işletim sistemlerini ele alır [77]. Uluslararası Elektroteknik Komisyonunun (IEC), TCP/IP protokolü de dahil güç sistemleri denetiminde kullanılan iletişim sistemlerine ait veri aktarım güvenliğini sağlamaya yönelik bir standart çalışmasıdır. Bu standartta ait dokümanlarda açıklıkların giderilmesine yönelik sunulan yöntemlerin teknik ayrıntıları yer almaktadır [74]. Standart aşağıdaki bölümleri içerir:

- Giriş
- Sözlük

- TCP/IP içeren profiller için güvenlik
- MMS içeren profiller için güvenlik
- IEC 60870-5 ve türevleri (DNP) için güvenlik
- IEC 61850 profilleri için güvenlik
- Ağ güvenliği için unsurlar (hedefler) [78].

2.6.6. NERC kritik altyapı koruma

NERC, ilk olarak 2003 yılında Acil Aksiyon Standardı olan "1200 Siber Güvenlik" belgesini yayınlamış ve müteakiben NERC 1300 çalışmasını başlatmıştır. Bu çalışmaların ardından 2006 ve sonrasında NERC, kritik altyapıların korunmasına yönelik daha kapsamlı olan CIP 002-1 ile CIP 009-2 çalışmalarını yayınlamıştır. NERC 1200, iletim ve dağıtım birimlerini kapsayan çalışmalar iken, CIP 002-1 ile CIP 009-2 serisindeki çalışmalar üretim tesislerini de içerecek şekilde genişletilmiştir. ABD Federal Enerji Düzenleme Komisyonu (FERC) tarafından 2006 yılında NERC CIP standartlarının onaylanmasının ardından, CIP standartlarına uyumluluk enerji sektörü için yükümlülük haline gelmiştir [74].

2.6.7. NERC 1200 standardı

FERC, DOE ve DHS tarafından enerji sektörü koordinatörü olarak tanınan NERC tarafından Acil Siber Müdahale Standardı adıyla geliştirilmiştir. Risklerin azaltılması için güvenlik gereksinimlerinin enerji sektöründe kurulmasını sağlar. Taslak aşamasında olan 1300 standardının bu standardın yerine geçmesi beklenmektedir. NERC standartları ve prosedürleri tanımlama ve sertifikasyon için geliştirir. Bunlar tamamlandığında bu standartlar belirtilen faaliyetleri yapan varlıklara (kontrol bölgeleri, iletim şirketleri sahipleri ve operatörleri, üretim şirketleri sahipleri ve operatörleri gibi) uygulanabilmektedir [78].

2.6.8. NERC 1300 standardı

Bir CIP standardı olan NERC 1300'ün amacı, kritik altyapı olarak değerlendirilen altyapılara karşın oluşabilecek riskleri azaltmaktır. Doküman, aşağıda belirtilen ana başlıklar altında kritik konularda kapsamlı bilgiler içerir.

- 1301 Güvenlik Yönetimi Konuları

- 1302 Kritik Siber Varlıklar
- 1303 Personel Konuları ve Eğitimi
- 1304 Elektronik Güvenlik
- 1305 Fiziksel Güvenlik
- 1306 Sistem Güvenlik Yönetimi
- 1307 Olaylara Müdahale Planları
- 1308 İyileştirme Planları. [79].

2.6.9. NERC-CIP-002-CIP-011

NERC 1300 standardı güncellenerek 2006'da hazırlanmıştır ve 3. sürümü 2010'da güncel hali olarak yenilenmiştir. Standart ile sürekli bir kontrol parametresi sağlanması, olay müdahale ve yönetimi, Kritik Siber varlıkların iyileştirilmesi ve çalışır halde tutulması amaçlanmıştır. Standart aşağıdaki konularda düzenlemeler içermektedir:

- Kritik Siber Varlık tanımlama,
- Güvenlik Yönetimi Kontrolleri
- Personel ve Eğitimi
- Elektronik Güvenlik Koruması
- Fiziksel Güvenlik Programı
- Sistem Güvenlik Yönetimi
- Olay Raporu ve Müdahale Planı
- Kritik Siber Varlıklar İçin İyileştirme Planları
- Toplu Elektrik Sistemlerinin Sınıflandırılması
- Toplu Elektrik Sistemlerinin Siber Savunması. [77].

2.6.10. FERC SSEMP

Haziran 2002 yılında yayınlanmıştır. Sonradan ABD'deki tüm elektrik piyasa katılımcıları için zorunlu hale gelmiştir. Bu doküman, elektrik şebekeleri ve personeliyle ilgili donanım, yazılım, veri ve iletişim ağları gibi konularda minimum uyulması gereken standartları belirlemektedir [78].

2.6.11. IEEE 1402 (Elektrik trafo merkezi fiziksel ve elektronik güvenlik kılavuzu)

IEEE tarafından 2000 yılında oluşturulan ve 2008 yılında yeniden gözden geçirilen IEEE 1402-2000 (R2008) standardında çoğunlukla elektik güç üretim ve dağıtım istasyonlarının fiziksel seviyede güvenliği konu edilmekle birlikte, elektronik ortamdan sızmalara da yer verilmektedir. Bu standardın amacı, riskleri azaltmak için hassas şebekelere karşı yetkisiz girişlere, bilgi hırsızlığına, yıkıcı eylemlere karşı fiziksel güvenlik uygulamalarını ve elektrik şebekelerinde farklı güvenlik seviyelerindeki gereksinimleri tanımlamaktır [74].

2.6.12. NIST standardı

Bu standart endüstriyel kontrol sistemlerinin güvenliğini sağlamaya yönelik olarak hazırlanmıştır. Bu standart, Merkezi Denetleme Kontrol ve Veri Toplama sistemleri (SCADA) ve Dağıtık Kontrol Sistemleri (DCS) gibi EKS ve EKS bileşenlerinden Programlanabilir Kontrol Cihazlarını (PLC) içerir. EKS, birbirine bağlı ve karşılıklı çalışabilen bağımsız sistemlerden oluşmaktadır. Bu standart, EKS'ye karşı tehdit ve açıklıkları tanımlar, riskleri azaltmak için tavsiye niteliğinde kurallar içerir. Standartta ele alınan tehditler aşağıda belirtilmiştir.

1. Ağlarda bilgi akışını geciktirerek veya bloke ederek bu sistemlerin çalışmasını bozabilirler.
2. Yetkisiz komut ve yönlendirme yapılarak, hasar eşiğinin aşılması sonucu sistemler kapanabilir, bozulabilir, çevresel etkiler oluşabilir ve sonuçta insan yaşamı zarar görebilir.

Bu yüzden Endüstriyel Kontrol Sistemlerinde kullanılan bu standartların hedefi;

- Sistem ağlarına ve aktivitelerine girişi sınırlandırmak,
- Sistem ağlarına ve cihazlarına fiziksel girişi sınırlandırmak,
- Saldırıdan tekil olarak tüm parçaları korumak,
- Saldırı durumlarında sistemi çalışır halde tutmak,
- Saldırıdan sonra sistemi geri yüklemektir.

Bu standart;

- Güvenlik politikaları, prosedürler ve eğitici materyaller içerir.
- Ulusal güvenlik temelli tehditleri değerlendirerek, güvenlik politikaları ve standartları içerir.
- DMZ ağ mimarisi kullanır.
- Akıllı kimlik kartları gibi modern teknoloji kullanır.
- Sistemin kritik bileşenlerinin hesap izlerini inceler.
- Veri kayıtları ve iletişim için şifreleme teknikleri kullanır [80].

2.6.13. NISTIR 7628 (National institute of standards and technology interagency report)

"Akıllı şebeke kullanımı" konulu çalıştayların sonucunda ortaya çıkmıştır ve kapsamlı siber güvenlik kurallarını içerir. NISTIR 7628 risk değerlendirmesi ve güvenlik analizi konularında aşağıda belirtilen başlıkları içerir [81]:

1. Güvenlik mimarisi stratejisi,
- Siber güvenlik stratejisi
- Mantıksal mimari
- Yüksek seviye güvenlik gereksinimleri
- Kriptografi ve anahtar yönetimi

2. Gereksinimler
- Gizlilik ve akıllı şebekeler

3. Destekleyici analiz ve referanslar
- Açıklık sınıflandırması
- Aşağıdan yukarıya akıllı şebekelerde güvenlik analizi
- Akıllı şebekelerde siber güvenlik konusunda araştırma ve geliştirme konuları
- Standart denetimlerine bakış
- Anahtar güç sistemlerinin güvenlik için kullandığı çözümler [82].

2.6.14. NIST SP 800-53

Federal Bilgi Sistemleri ve Organizasyonları için güvenlik ve gizlilik kontrolleri başlıklı standart; organizasyon varlıklarına, bireylere, diğer kuruluşlara ve ulusa düşman siber ataklara, doğal felaketlere, yapısal hatalara ve insan hatalarına karşı organizasyonun işlevlerini korumak için uygun yöntemleri içerir. Standartta, bu yöntemlerin, kurumların bilgi güvenliği ve gizlilik riskini yönetmede bir kılavuz olarak kullanılabileceği belirtilmiştir. Standart, giriş, önemli konular ve yöntemler adı altında üç bölümden oluşur. Bu bölümler aşağıdaki hedefleri kapsamaktadır:

- Giriş: Amaç ve uygulanabilirlik, hedef kitle, diğer güvenlik kuruluşlarıyla ilişkiler, örgütsel sorumluluklar,
- Önemli konular: Çok yönlü risk yönetimi, güvenlik kontrol yapısı, güvenlik kontrolünün ana hatları, gösterimi, dış servis sağlayıcılar, güven ve güvenilirlik, yenilenme ve büyüme,
- Yöntem: Güvenlik kontrol seçimi ana hatları, ana hatları güvenlik kontrolüne uyarlamak, katman yaratma, kontrol seçim işlemini kayıt altına alma, yeni yöntemler ve yasal sistemler [82].

2.6.15. IEC S63 raporu

Genel olarak akıllı şebeke güvenliği gereksinimleri için statü ve tavsiye niteliğindeki standartları içerir. Endüstriyel güvenlik standartları, giriş kontrolleri, kimlik yönetimi, güvenli ağ, kablolu ve kablosuz bağlantı standartları konularını kapsamaktadır [77].

2.6.16. IEC 1686-2007

Trafo merkezinde kullanılan Akıllı Elektronik Cihazlar için siber güvenlik özellikleri, kabiliyet ve fonksiyonları konusunda standartlar ile kritik altyapıların güvenliği ile ilgili konular hakkında bilgilendirici bir dokümandır [77].

2.6.17. ISA-SP99 üretim ve kontrol sistemleri güvenlik standardı

ISA-SP99 standardı, 2002 yılında hazırlanmış ve 2 teknik rapor halinde yayınlamıştır. Standart, üretimde veya kontrolde kullanılan unsurların ve sistemlerin erişebilirliğini,

bütünlüğünü ve gizliliğini geliştirmeyi kapsamaktadır. Güvenlik kontrol sistemlerini oluşturmayı ve kıstas belirlemeyi hedefler. Teknik raporlar, kontrol sistemlerine özgü veriler, güvenlik standartları ve yayınları içerir [78].

ISA-99, standardı endüstriyel otomasyon ve kontrol sistemleri konusunda yol göstericidir. Risk analizi, farkındalık oluşturma ve karşı önlemler ile siber güvenlik yönetim sistemleri konularını ele alır. Birçok güvenlik teknoloji ürünleri konusunda tavsiye ve rehber niteliğinde bilgiler içerir [77].

2.6.18. NIST 800-82

NIST tarafından hazırlanan NIST 800-82 no.lu "Endüstriyel Kontrol Sistemleri Güvenliği Rehberi" başlıklı çalışmasının amacı, SCADA sistemlerinin ve dağıtık kontrol sistemlerinin, diğer bir ifadeyle endüstriyel kontrol sistemlerinin ve kontrol fonksiyonu sağlayan diğer sistemlerin güvenliğini sağlamaya yönelik bir kılavuz teşkil etmektedir. NIST 800-82 rehberi şu alt başlıklar halinde sıralanmıştır [80] :

- SCADA ve diğer EKS'de alınan fiziksel önemlerin yanı sıra güvenlik ihtiyaçlarının gerekçelerine genel bir bakış,
- Açıklık, tehdit ve olaylar kapsamında EKS ve BT sistemleri arasındaki farklar,
- Yukarıda tanımlanan güvenlik açıkları riskini azaltmak için bir EKS güvenlik programının geliştirilmesi ve dağıtılması,
- Ağ ayrımı uygulamalarını vurgulayarak, EKS'de bulunan tipik ağ mimarilerine güvenlik çözümlerini entegre etmek için öneriler,
- NIST 800-53'te tanımlanan yönetimsel, operasyonel ve teknik kontrollerin özeti.

NIST 800-82, doğrudan bir güvenlik kontrol listesi sunmakla birlikte, aynı zamanda risk değerlendirmesi çalışmaları için yararlanılacak güvenlik gereksinimleri ve çözümleri de sunmaktır. Standart, EKS altyapısında kullanılan donanımsal ve/veya yazılımsal bileşenleri incelemekte, daha güvenli ağ-uygulama servisleri için öneride bulunmakta ve örnekler sunmaktadır. Bu nedenle, pratik inceleme ve düzeltmeler için başvurulabilecek kaynaklar arasında yer almaktadır [32]. NIST 800-82 rehberinde, endüstriyel denetim sistemlerinde ortaya çıkabilecek muhtemel istenmeyen olaylar aşağıdaki şekilde özetlenmiştir [74] :

- Ağda taşınan bilginin engellenmesi veya gecikmesi sonucunda, denetim ve izleme işlemleri aksaması,
- Komut, yönerge ve alarm eşiklerinin yetkisizce değiştirilmesi ile sistem bileşenlerinin kapanması, devre dışı kalması veya hasar görmesi sonucunda çevrenin, çalışanların ve diğer insanların hayatlarının tehlikeye altına girmesi,
- Hatalı bilginin sistem operatörlerine gönderilmesi veya yetkisiz değişikliklerin gizlenmesi ile operatörlerin uygun olmayan komutlar göndermesine sebebiyet verecek durumların oluşturacağı olumsuz etkiler, güvenli sistemlere müdahale ile insanların hayatının tehlikeye düşürülmesi.

3. ENDÜSTRİYEL KONTROL SİSTEMLERİNDE SİBER GÜVENLİK

Endüstriyel Kontrol Sistemleri (Industrial Control Systems- ICS); gaz, su, enerji sistemleri, üretim sistemleri ve ulaşım sistemleri gibi dağıtık bir yapıda bulunan sistemleri uzaktan izleme ve kontrol etmek için kullanılan sistemlerdir. Endüstriyel Kontrol Sistemleri, kritik altyapılarda kullanılanlar da dahil olmak üzere her türlü endüstriyel sistemi kontrol etmek veya işletmek için temel altyapı olarak hizmet eder [80, 83].

EKS, enerji sektöründeki elektrik üretim tesislerinin ve diğer endüstriyel süreçlerin işleyişinde merkezi bir konumdadır. EKS, endüstriyel bir ortamda merkezi sistem kontrol merkezlerine bağlı pompalar, kesiciler, valfler ve diğer sistem algılama, izleme ve kontrol cihazlarını kontrol eden birincil araçtır. Bu kontrol sistemleri, güvenlikle ilgili sistemlerin kontrolünü sağladıkları için endüstriyel operasyonların ayrılmaz bir parçasıdır [84].

Endüstriyel kontrol sistemleri, bir otomasyon sisteminin ihtiyaçlarını karşılamak için uygulanan entegre iletişim ağıdır. EKS ağ bilgi alanı, dijital kontrolörler, alan cihazları, yazılım ve uygulamalar arasındaki iletişim protokollerinin uygulanmasını ve endüstriyel ortamda fiziksel ekipmanların yönetimini içerir [85]. EKS, SCADA ve DCS olarak gruplandırılan endüstriyel kontrol sistemlerinin iki kategorisi için kullanılan şemsiye bir terimdir.

3.1. SCADA

SCADA öncelikle, uzaktaki donanıma üst düzey komutlarla sınırlı olan denetim rolündeki dağıtılmış bir sistemdir. SCADA sistemleri coğrafi olarak dağınık uzak terminal ünitelerinden olaya dayalı verileri elde etmek ve bu verileri bir merkezi insan makine arayüzü (HMI) konsolunda sunmak üzere tasarlanmıştır. Bir SCADA kontrol merkezi, alarmların izlenmesi ve durum verilerinin işlenmesi dahil olmak üzere uzun mesafeli iletişim ağları üzerinden alan siteleri için merkezi izleme ve kontrol gerçekleştirir. Diğer bir ifadeyle, SCADA sistemleri, bir sistemin gözetim ve denetimini sağlayan ve sistemleri uzaktan ve otomatik olarak denetlemek, yönetmek ve izlemek için tasarlanmış bir EKS türüdür. Uzak istasyonlardan alınan bilgilere dayanarak, otomatikleştirilmiş veya operatör tarafından yönetilen denetim komutları, genellikle saha cihazları olarak adlandırılan uzak istasyon kontrol cihazlarına aktarılabilir [86, 87]. Kontrol sistemleri, merkezi olmayan

çeşitli operasyonları izlemek ve kontrol etmek için kullanılan SCADA sistemlerini içermekte olup, bu da esas olarak onu işleten kişinin fiziksel olarak hemen yanında durmadığı anlamına gelmektedir.

SCADA sistemleri, tipik olarak PLC'ler veya diğer ticari donanım modülleri aracılığıyla bir yazılım paketi ile sistem donanımıyla arabirim kurarlar. SCADA sistemleri çoğunlukla santraller gibi endüstriyel ortamlarda veya büyük üretim tesislerinde bulunur. Bir SCADA sisteminde iki temel katman vardır: HMI olan istemci katmanı ve işlemleri yöneten veri sunucusu katmanı. Genel olarak, bu sistemlerin dayanıklılığı veya uzun süreli endüstriyel kullanıma dayanma kabiliyeti, kritik altyapıda neden kullanıldığının kanıtıdır.

Bir SCADA şebekesinin bozulması, bir enerji üretim tesisi için kritik olabilir. SCADA, karmaşık bir siber güvenlik tehdidine karşı savunmasızdır, çünkü süreç izleme ve denetimi tek bir ağda birleştirilmiştir. Bu, saldırgana aynı anda izleme sistemini yerel olarak normal çalışma görünümüyle iletişim kurmak için uzaktan denetim işlevini bozma fırsatı verir [88].

3.2. DCS

DCS, aynı coğrafi bölgede yerel dağıtılmış endüstriyel süreçleri yöneten ve izleyen sistemlerdir. DCS, üretim sürecinin yürütülmesinden toplu olarak sorumlu olan süreç denetleyicilerinin ve operatör istasyonlarının yerel bir ağıdır [89]. DKS, üretim tesisleri, rafineriler, farmasötik işleme tesisleri veya atık su arıtma tesisleri gibi üretim sistemlerinde görev yapmaktadır [80].

Kritik Altyapı Endüstriyel Kontrol Sistemleri (Critical Infrastructure Industrial Control Systems - CI2CS), kontrol sistem konfigürasyonlarında, kızağa monte programlanabilir lojik kontrol cihazları (PLC), SCADA sistemleri ve DCS'yi içerir. Bu kontrol sistemlerinin çalıştığı karşılıklı bağımlı ve sıklıkla birbirine bağlı sistemler, kritik altyapılar için hayati önem taşımaktadır [80].

Endüstriyel kontrol sistemleri, endüstride en çok PLC, HMI, Temel Terminal Birimi (Master Terminal Unit-MTU) ve Uzak Terminal Birimi (Remote Terminal Unit-RTU) gibi birçok alt bileşenlerinden oluşmaktadır [18]. HMI, basitçe, insanların makinelerle nasıl arabirim kurduğudur. Arayüz, düğmeler, monitörler, klavyeler, dip anahtarlar,

dokunmatik ekranlar, potansiyometre gibi bileşenleri içerebilir. İnsan eylemi, sistemlerin tehlikeye düşmesinin başlıca nedenlerinden biridir; çoğu zaman "mızrak phishing (spear phishing)" saldırılarıyla başlar. Eski nesil endüstriyel kontrol sistemlerinde bu bileşenler dış ağlardan bağımsız özel bir iç ağ ile haberleşmekte ve kurumsal iç ağ ve İnternetten, endüstriyel ağa özgü protokoller olan MODBUS, PROFIBUS ve CONTROLNET gibi özel iletişim protokollerini kullanarak tecrit edilmişlerdi. EKS için Dağıtık Ağ Protokolü 3 (Distributed Network Protocol 3- DNP 3), Genel Nesne Tabanlı Trafo Aktiviteleri (Generic Object Oriented Substations Events-GOOSE), IEC 61850 ve IEC 608750-5 gibi standartlar geliştirilmiş olsa da, tutarlı güvenlik çözümlerinin uygulanması için yeterli standardizasyon sağlanabilmiş değildir [26].

Bu nedenle, yalıtılmış halde bulunan endüstriyel kontrol sistemlerinin güvenli olduğu kabul edilerek siber güvenlik boyutu büyük oranda ihmal edilmişti. Ancak, zamanla, üretkenliği ve verimliliği artırmak amacıyla coğrafi olarak birbirinden oldukça uzakta dağınık bir yapıyı kontrol etmek ve izlemek için endüstriyel kontrol sistemi iletişim protokolünün standartları şimdi açık uluslararası standartlara kaydırılmış ve internet veya intranet bağlantısına ihtiyaç duyulmuştur [90]. Ayrıca endüstriyel kontrol sistemi ve kurumsal veritabanları arasında otomasyon süreç değişken verilerini değiştirme gereksinimi EKS içinde Ethernet ve İletim Denetimi Protokolü / Internet Protokolü (TCP / IP) teknolojilerini birleştirmek için katalizör haline gelmiştir. 1990'lı yılların EKS dijital evrimi, bilgi teknolojisi (IT) ve EKS yakınsamasıyla birlikte, endüstriyel ortamda konuşlandırılan Ethernet EKS cihazlarının sayısını artırmıştır [91]. Saldırganlarda, bu standartlar hakkında derinlemesine bilgi edinebilir ve avantajlarını kullanabilir [92]. Bu gelişmelere rağmen güvenlik bugün hala kullanılmakta olan birçok EKS sistemi için sistem tasarımının bir parçası değildir. Bugünün sistemleri artık İnternet ortamına açıktır ve burada hem izlenir hem de kontrol edilir. Bu internet bağlantısının bir sonucu olarak, ağ güvenliği sorunları uzaktan bağlı sistemlerin temel tehdidi olmayı sürdürmektedir [93]. Düşük maliyetli ve yaygın IP cihazlarının patentli çözümlerin yerini alması nedeniyle, siber güvenlik vakaları ve güvenlik açıkları için olasılık artmıştır [94].

3.3. Bilgi Teknolojileri ile EKS Arasındaki Farklar

Ticari uygulamalarda kullanılan EKS ve IT sistemleri arasındaki farklar nedeniyle, BT güvenlik çözümlerini doğrudan EKS içindeki sorunlarla mücadele etmek için kullanabilmek zordur. Örneğin, EKS, olay olmaksızın birkaç yıl süreyle sürekli çalışabilir, ancak çevrimiçi kontrol sistemindeki herhangi bir değişiklik veya güncelleme, proses ve ekipmana beklenmedik zararlara neden olabilir.

Endüstri, oldukça belirgin olan bu güvenlik risklerinin farkındadır. Bununla birlikte, endüstriyel kontrol sistemlerini "güncellemek" oldukça riskli olabilmektedir. Birincil nedeni, özellikle trafik kontrol sistemleri ve enerji santralleri için güvenlik unsurlarının eklenmesiyle istenmeyen uzun bir çalışma zamanı gerekmektedir. İkincisi, mevcut EKS donanımlarının gömülü kodlarını tamamen değiştirmek için yeni güvenlik protokollerinin eklenmesi gerekmektedir. Son olarak, EKS sistem ağları, genellikle EKS'ye özel sistem için özelleştirildiği için genelleştirilmeleri oldukça zordur [93].

Kontrol sisteminin riskini azaltmak için alınacak önlemler, sisteme dahil edilmeden önce dikkatle test edilmelidir [95]. Bu nedenle, siber güvenlik araştırması için canlı bir endüstriyel kontrol sistemi kullanmak yerine bir sınama ortamı geliştirmek önemlidir. EKS, özel yazılım ve donanımları kullanarak tescilli kontrol protokollerini çalıştıran izole sistemler olarak kullanıldığı döneme ilişkin, BT ile olan halka açık protokolleri olan geleneksel IT sistemlerinin aksine farklı gereksinimlerle tasarlanmışlardı. EKS ile Bilgi Teknolojileri Sistemleri arasındaki farklar Çizelge 3.1'de görülmektedir [94].

Endüstriyel tesisler için güvenlik hedefi genellikle fiziksel güvenliğin artırılmasına yöneliktir. Diğer taraftan EKS şebekeleri ile ilgili güvenlik endişeleri, şebeke bağlantısındaki farklılaşması ve dış ağlara açılması nedeniyle artmaya devam etmektedir. EKS ağları, herhangi bir ağdaki gibi, mevcut ağ teknolojisi kullanılarak çoklu erişim noktalarına sahip olabilir. Fiziksel izolasyonun ağ güvenliği ile eşit olduğuna dair bir anlayış da doğru değildir.

Çizelge 3.1. BT ile EKS arasındaki farklılıklar (NIST SP800-82, 2015)

Kategori	Bilgi Teknolojileri Sistemi	Endüstriyel Kontrol Sistemi
Performans Gereksinimleri	a. Gerçek zaman iletişim gereksinimi yoktur (Non Real Time) b. Yanıt tutarlı olmalı c. Yüksek veri aktarımı (High throughput) talep edilir ç. Yüksek gecikme ve gecikmedeki değişim (jitter) kabul edilebilir d. Daha az kritik acil durum etkileşimi e. Sıkı kısıtlanmış erişim kontrolü, güvenlik için gerekli derecede uygulanabilir	a. Gerçek zamanlı iletişim ihtiyacı b. Yanıt zamanı açısından kritik c. Orta Seviye veri iletimi (Modest throughput) kabul edilebilir ç. Yüksek gecikme ve / veya jitter kabul edilemez d. İnsan ve diğer acil müdahaleye tepki kritik önem taşıyor e. EKS'ye erişim sıkı bir şekilde kontrol edilmeli, ancak insan-makine etkileşimine engel olmamalı veya müdahale etmemeli
Kullanılabilirlik (Güvenilirlik) Gereksinimleri	a. Yeniden başlatma (rebooting) gibi işlemler kabul edilebilir b. Kullanılabilirlik eksiklikleri, sistemin operasyonel gereksinimlerine bağlı olarak genellikle tolere edilebilir	a. Yeniden başlatma gibi işlemler, süreçlerin devamlılığı gereksinimleri nedeniyle kabul edilemez. b. Kullanılabilirlik gereksinimleri, yedekli sistemleri gerektirebilir c. Kesintiler günler / hafta önceden planlanmalıdır ç. Yüksek kullanılabilirlik, ayrıntılı ön kurulum (pre-deployment) testi gerektirir
Risk Yönetimi Gereksinimleri	a. Fiziksel dünyanın kontrol edilmesi gereklidir b. Veri gizliliği ve bütünlüğü oldukça önemlidir c. Hata toleransı daha az önemlidir - anlık kesintiler önemli bir risk değildir ç. En önemli risk etkisi iş operasyonlarının gecikmesidir	a. Verilerin yönetimine ihtiyaç duyulur b. İnsanın güvenliği çok önemlidir, bunu sürecin korunması izlemektedir c. Hataya dayanıklılık önemlidir, anlık kesintiler bile kabul edilebilir olmayabilir ç. En önemi risk etkileri yaşam, ekipman veya üretim kaybı, uyumsuzlukların düzenlenmesi ve çevresel etkilerdir
Sistem İşletimi	a. Sistemler, tipik işletim sistemleriyle birlikte kullanılmak üzere tasarlanmıştır b. Otomatik kurulum araçları ile güncellemeler doğrudan gerçekleştirilir	a. Genellikle güvenlik özelliklerini barındırmayan farklı ve muhtemelen tescilli işletim sistemleri b. Yazılım değişiklikleri, özelleştirilmiş kontrol algoritmaları ile yazılım ve donanımların modifiye edilmelerine karşın, yazılım güncellemeleri tedarikçiler tarafından dikkatlice yapılmalıdır.
Kaynak Kısıtlamaları	Sistemler, güvenlik çözümleri gibi üçüncü parti uygulamaların eklenmesini desteklemek için yeterli kaynaklarla desteklenmektedir	Sistemler, tasarlanan endüstriyel süreci desteklemek üzere tasarlanmıştır ve güvenlik yeteneklerinin eklenmesini desteklemek için yeterli bellek ve bilgi işlem kaynakları olmayabilir.

3.4. Hazır Ticari Ürün Kullanımı

EKS ağlarında kullanılan COTS yazılım ve donanımları, EKS güvenlik açıklarına katkıda bulunan bir diğer faktördür. COTS yazılımı ile maliyetler ve tasarım için gereken süre azaltılabilir, ancak güvenlik tehlikeye girebilir [96]. COTS yazılımı, saldırganları cezbedecek bir hedef sağlar, çünkü genellikle güvenlik açısından zayıftır. Devre dışı bırakılabilen, bir saldırgan tarafından sökülüp engellenebilecek başarısız güvenlik mekanizmaları, COTS olmayan cihazların aksine, güvenlik açıkları olarak COTS yazılımında bulunur. COTS dışındaki cihazlar, güvenlik açısından kritik ortamlarda çalıştırılması amaçlandığından genellikle emniyetli olacak şekilde tasarlanmıştır; Bununla birlikte, COTS cihazlarının tasarımcılarında aynı hassasiyet görülmemektedir.

Ülkelerin CI2CS'lerine diğer devletlerin saldırısı devam etmektedir. Çünkü ülkelerin savunması ve güvenliği konusunda en hassas alanlardan birisi EKS'dir. Yakın geçmişte, bu siber zayıf noktalar, daha önce tasarlanmış, güvenlik konusunda çok az güvenliği olan veya olmayan bu eski sistemlerin yerini, en yeni COTS ağ ve sistem donanımı ile entegre olan en güncel COTS yazılımını içeren kontrol sistemleri almaktadır. Otomasyona bağımlı olan belirli endüstrilerde protokolleri ve standartları düzene sokmak için teknolojilerin bu evliliği; her ne kadar kolay ve verimli olsa da, kendi zorluklarını ve güvenlik risklerini ortaya koymaktadır. Ayrıca, ticari amaçlı geliştirilen ürünlerin kullanılması, ModBUS/TCP gibi bütünleşik protokollerin geliştirilmesi sonucunda EKS'lerin daha açık, uzaktan erişilebilir ve çeşitli siber saldırılara karşı zaafiyetli duruma getirmiştir [97, 98]. Bu süreç sonunda önceden tespit edilemeyen yeni açıklıklar ortaya çıkmıştır. Bu açıklıklar;

- Kontrol sistemleri güvenlikten öte, kritik zamanlama gereksinimleri, katı performans ve görev öncelikleri gibi sistemin etkinliğine odaklanılan bir tasarıma sahip olması,
- Sistemi oluşturan kaynak kodlarının çoğunlukla açık olması,
- Uzaktan erişime izin vermesi (VPN, vb.),
- Varsayılan kullanıcı adı ve şifrelerin genellikle değiştirilmemesi ve bu nedenle açık arka kapı bırakılması,
- Sistem bilgi güvenliğinin az düşünüldüğü veya çok az ele alındığı ticari amaçlı geliştirilmiş iletişim protokollerinin uygulanması şeklinde belirtilmektedir [99].

3.5. EKS'de Yaşanan Güvenlik Olayları

EKS'ler birçok kritik altyapının izlenmesinden ve kontrolünden sorumludur. Bu sistemlerde bir oluşacak güvenlik zafiyeti sonuçta saldırganların bu hedeflere karşı iştahlanmasına sebep olur. Sistemin kontrolünün ele geçirilmesi sonucunda, sadece ekonomik zarar değil aynı zamanda insanların yaşantılarında önem arzeden kritik hizmetleri alamamasına ve belkide can kaybına neden olabilir [20].

3.5.1. Hava trafik iletişimi

Mart 1997'de Worcester, Massachusetts telefon şebekesinin bir kısmı çevirmeli modem kullanan bir genç tarafından devre dışı bırakıldı [80]. Saldırı sonrasında, hava durumu servisi, kontrol kulesi, havaalanı itfaiye ve havaalanı güvenliği tüm telefon hizmetlerini kaybetti. Ayrıca, uçuş ilerlemesini izlemek için denetleyicilerin kullandığı bir yazıcı ve kulenin ana radyo vericisinin yanı sıra, pist ışıklarını aktive eden başka bir verici de kapatıldı. Worcester'in yakınında bulunan Rutland'da 600 eve ve işletmelere yönelik telefon hizmeti de saldırıyla engellendi [80].

3.5.2. Maroochy Shire kanalizasyon dağılımı

SCADA sistemleri, kritik altyapı sektörlerinde hayati varlıkları kontrol etmektedir ve kritik altyapıdaki bir sistemin arızalanması felaket olabileceğinden, bu sistemlerin güvenliğinin arttırılması gerekmektedir. Maroochy su ihlali, tehlikeye atılan bir SCADA sisteminin sonuçlarının bir örneğidir. Avustralya Queensland'da yaşanan atık yönetim tesislerinde yaşanan bu saldırı, büyük miktarda atığın kamusal alanlara dökülmesine sebep olmuştur. Bu saldırı, eski bir kurum çalışanı olan Vitek Boden tarafından gerçekleştirilmiştir [14]. Boden'e, Ocak 2000'de Maroochy Shire Konseyi'nde çalışamayacağını söyledikten sonra kanalizasyon sisteminde, pompalar çalışmamaya, alarmlar merkezi bilgisayara ulaşmamaya ve merkezi bilgisayar ile çeşitli pompa istasyonları arasında iletişim kaybı yaşanmaya başlamıştır [100]. Boden, 150 kanalizasyon pompa istasyonunun kontrolünü ele geçirmek için sadece bir diz üstü bilgisayar ve kablosuz modem kullanmıştır. Bu saldırı, 9 Şubat - 23 Nisan 2000 tarihleri arasında, 46 farklı fasılada, iki ay boyunca gerçekleştirilmiştir. Belirli kanalizasyon pompa istasyonları için elektronik verilerin

değiştirilmesi sonucunda nihai olarak yakındaki nehirlerin ve parkların içine toplamda yaklaşık 264.000 galon atık suyun akıtılmasına yol açmıştır [80, 101]].

Boden, SCADA sistemi için kullanılan yapılandırma programını kişisel dizüstü bilgisayarına yüklemiştir. 23 Nisan 2000'de hedeflenen sistemi yönlendirebilen bir kişisel bilgisayarı pompa istasyonunda bir makineyi taklit etmek için kullanmış ve pompalama istasyonlarının dördünde alarmları devre dışı bırakmıştır. Saldırı, işten çıkarılmasına rağmen yetkileri alınmayan içeriden birisi tarafından gerçekleştirilmesi nedeniyle yönetici istasyonları yaşanan olayalar ilişkin uyarı alamamıştır. Bu saldırıyı mümkün kılan çeşitli faktörler vardı. Öncelikle, saldırı gerçekleştirildikten sonra güvenlik önlemleriyle savunulması oldukça zor olan dahili bir saldırıydı. Boden sistemin topolojisini ve nasıl yönlendireceğini biliyordu. Güvensiz radyo sinyallerine müdahale ederek sistemde değişiklikler gerçekleştirdi. En önemli husus, sistem üzerinde uygulanması gereken güvenlik kontrollerinin (kullanıcı girişleri, yetkilendirme, vb.) olmaması nedeniyle bu sistemlere girmeyi başarmasıdır [100].

Maroochy olayı içeriden bir saldırı olmasına rağmen, SCADA ağına ait doğru bilgiler ve ihtiyaç duyulan donanıma sahip herhangi bir saldırgan tarafından benzer bir saldırı gerçekleştirmiş olabilirdi. Maroochy ihlali, sistemi tasarlayan içeriden bir saldırgan tarafından gerçekleştirilmiş olması nedeniyle engellenme şansı düşüktür.

Bilgisayar korsanları kritik altyapı sektörü için tehlikelidir, ancak sistemin özelliklerini bilen hoşnutsuz içerden bir saldırgandan (insider) kaynaklanması durumunda büyük tehlike söz konusudur. Kurumlar genellikle mevcut SCADA sistemlerinin özellikle fiziksel güvenliklerinin çok sıkı olmalarına güvenerek, bu tür bir saldırıya karşı güvende olduklarını düşünmektedirler. Bu nedenle de, bir saldırı ile karşılaştıklarında ciddi kayıp ve zararlara maruz kalmaktadırlar. Bu saldırıda 150 atık su pompası istasyonu 3 aydan fazla süreyle kontrol altına alınamamıştır.

3.5.3. CSX tren sinyalizasyon sistemi

ABD’nin doğu kıyısındaki tren sinyal sistemleri Sobig bilgisayar virüsü tarafından Ağustos 2003’de kapatılmıştır. Jacksonville, Florida karargahında bulunan CSX Corporation'ın bilgisayar sistemine virüsün bulaşması nedeniyle, sinyal alma, gönderme ve diğer sistemler

tamamen kapanmıştır. İçeriği bozulan sinyaller, Florence ile Güney Carolina arasındaki trenlerin durmasına yol açmıştır. Zararlı, Richmond, Virginia'dan Washington'a ve New York'a giden bölgesel tren seferlerini iki saatten, uzun mesafe trenlerini ise dört ila altı saat arasında değişen gecikmelere neden olmuştur [80, 102].

3.5.4. Davis-Besse

ABD Nükleer Düzenleme Komisyonu, Oak Harbor, Ohio'daki boş Davis-Besse nükleer enerji santralinde özel bir bilgisayar ağının, Ocak 2003 - Ağustos 2003 tarihi aralığında Microsoft Yapılandırılmış Sorgu Dili (SQL) sunucusunun Slammer solucanı tarafından enfekte edildiğini bildirmiştir. Bu güvenlik olayı neticesinde, güvenlik izleme sistemi yaklaşık beş saat boyunca devre dışı kalmıştır [80, 103]

3.5.5. ABD kuzeydoğu elektrik kesintileri

First Energy'nin kontrol odası operatörleri, Ağustos 2003'de SCADA sisteminde yer alan bir alarm işlemcisinde oluşan bir problem nedeniyle arıza tespiti yapamadığını, bu nedenle de elektrik şebekesinde oluşan kritik operasyonel değişiklikleri merkeze iletmediğini bildirmişlerdir. Bu durum, şebekenin kontrolsüz bir basamaklama hatasına, yani 265 santral ile ilgili ilave 345kV ve 138kV hatlarının aşırı yüklenmesinden kaynaklanan 61.800 megavat (MW) yük kaybına neden olmuştur [80, 104].

3.5.6. Zotob solucanı

DaimlerChrysler'in ABD'deki otomobil üretim tesisleri, 13'ü Ağustos 2005'de, Zotob adı verilen solucan nedeniyle çevrimdışı kalmıştır. Bu süre zarfında BT işletmenleri, virüs bulaşmış Microsoft Windows sistemlerimi güncelleştirmekte zorlanmışlardır. Indiana, Michigan, Illinois, Wisconsin, Delaware ve Ohio'daki fabrikaların üretimi durmuştur. Solucan Windows XP'nin bazı eski sürümlerini etkilese de, öncelikle Windows 2000 sistemlerini hedef almıştır. Solucanın belirtilerinden en dikkat çekenleri; bilgisayarların kendini sürekli olarak kapatarak, tekrar başlatılması olduğu belirtilmiştir. Zotop ve onun türevi solucanlar nedeniyle DaimlerChrysler'ın yanı sıra, ABD'li birkaç büyük haber kuruluşu, uçak üreticisi Boeing ve ağır ekipman üreticisi Caterpillar Inc.'in bilgisayar sistemlerinde kesintiler yaşanmıştır [105].

3.5.7. Taum Sauk su deposu barajı

Taum Sauk Su Depolama Barajı'ndaki bir felaket arızası, Aralık 2005'de bir milyar galon suyun istem dışı boşaltılmasına neden olmuştur. Olay, Taum Sauk tesisini uzaktan izleyen ve işleten Ozarks Gölü'ndeki Osage tesisindeki göstergelerin barajın değerleri doğru yansıtmaması sonucunda, sisteme aşırı yük bindirilmesi ve geri pompalama operasyonunun devreye alınamamasından kaynaklanmıştır [106].

3.5.8. Stuxnet solucanı

Stuxnet, ilk olarak Temmuz 2010'da sınıflandırılmış ve santraller gibi endüstriyel tesislerin kontrolünü ele geçirmek için EKS'yi hedef aldığı tespit edilmiştir. Zararlının en muhtemel hedefinin endüstriyel casusluk olduğu düşünülmektedir. Stuxnet zararlısı iki farklı saldırı rutinini içermektedir. Her iki saldırı da santrifüj rotorlarına zarar vermeyi amaçlamış, ancak farklı taktikler kullanılmıştır. İlk saldırı santrifüjleri aşırı basınçlandırmaya çalışırken, ikinci saldırı, santrifüj rotorlarını aşırı hızlandırmaya ve kritik (rezonans) hız eşiğine itmeye çalışmıştır [107].

Stuxnet solucanı, ilk sofistike ve potansiyel olarak en tehlikeli EKS saldırılarından birisidir. Stuxnet'ten önceki çoğu zararlı kullanımının hedefi veri sızıntısı iken, Stuxnet'in amacı İran nükleer santrifüjlerini yok etmek ve zararlı kodu belirli Siemens kontrolörlerini tespit ettiğinde döndürülemez bir hasara neden olan saldırıyı başlatmaktır [15].

Stuxnet, daha önce kullanılmış herhangi bir solucandan çok farklıydı, çünkü hedefi kritik fiziki altyapıydı. Slammer, blaster ve conflicker gibi eski solucanlar fiziksel varlıkları etkilemiş olabilir, ancak yarattıkları etki daha çok ağ tıkanıklığına dayanmaktaydı. Stuxnet ise bilgisayar sistemlerinde kalabilir ve arzulanan hedefi bulup saldırana kadar hiçbir şey yapmadan bekleyebilmekteydi. Solucan ilk olarak 2009 yılında keşfedilmiş ve İran'daki Natanz'daki bir uranyum zenginleştirme kompleksinde yer alan kontrol sistemlerini etkilediği ve bunların santrifüjlerine zarar verdiği bildirilmiştir. Saldırganın kim olduğu henüz açık olmamakla birlikte, çoğu kaynak ABD Hükümeti'nin İsrail Hükümeti ile birlikte olduğunu iddia etmektedir [108]. Stuxnet, fiziksel olarak ağa Evrensel Seri Veri Yolu (USB) veya başka bir ortam vasıtasıyla yerleştirilmesi gereken izole bir ağa nüfuz etmiştir. Stuxnet,

en önemli devlet destekli siber saldırılardan birisi olarak bilinir ve hedef sistemde fiziksel hasar oluşturması nedeniyle siber saldırılar kapsamında yeni bir kategori oluşturmuştur.

3.5.9. Heartbleed

Heartbleed, Google Security ve Codenomicon'da çalışan güvenlik mühendisleri ekibi tarafından keşfedilen bir Kavramsal Kanıt (Proof of Concept-PoC) kullanım koduna dayalı güvenlik açığıdır. OpenSSL'de kullanılan özel SSL (Secure Sockets Layer) anahtarları " Taşıma katmanı güvenliği / veri birimi aktarım katmanı güvenliği" (TLS / DTLS) kusurundan dolayı açıklığı vardır. Heartbleed güvenlik açığı ilan edildikten sonra ilk 14 gün içinde tarama ve / veya istismar faaliyetine ilişkin emare tespit eden/ gözlemleyen on iki EKS sahibi / operatörü vardı. Exploit kamuya açıklandığından itibaren tarama ve / veya istismar gerçekleştirdiği bilinen 200'den fazla kaynak IP adresi tespit edilmiştir [109].

3.5.10. Ukrayna güç şebekesi saldırısı

23 Aralık 2015'te, Ukrayna elektrik şebekesinin bir kısmı bilinmeyen bir kaynaktan gelen başarılı bilişim sistemleri korsanlığı (hacking) saldırısından dolayı elektrik kesintisi yaşadı. Saldırı sonrasında 225,000 müşterinin hizmeti kesildi. Ukrayna hükümeti, bu siber saldırıdan Rusya'yı sorumlu tutmuştur. İlk olarak, saldırganlar sistemlere erişim elde etmek için birden fazla teknik kullanmıştır. Bu kapsamda, Mızrak oltalama (spear-phishing) e-postaları, BlackEnergy 3 kötücül yazılımının çeşitleri ve manipüle edilmiş Microsoft Office belgelerini kullanmışlardır. Bu teknikler kullanılarak bilgisayar korsanları EKS ağına erişebildi ve sistemin kontrolünü ele geçirebildiler. İkinci aşamada, saldırganlar sahadaki SCADA sistemleriyle bağlantı kuran sistem üzerindeki kontrolleri kesen ve operatörün sistemin kontrolünü kaybetmesine neden olan HMI saldırısı gerçekleştirmişlerdir. SANS dokümanı, bu saldırıda araçlardan ve uzmanlıktan daha çok "ortamı öğrenmenin ve daha senkronize, çok kademeli, çok bölgeli bir saldırı yürütmek için gerekli uzun vadeli keşif işlemlerini gerçekleştirmenin" saldırganların en güçlü yeteneği olduğunu belirtmiştir [110].

Saldırı esnasında, saldırganlar BlackEnergy 3 kötücül yazılımını gömmek suretiyle Microsoft Excel ve Word belgelerini silah olarak kullanmışlardır. BlackEnergy 3, BlackEnergy kötü amaçlı yazılım ailesindeki üçüncü varyant kötücülüdür.

BlackEnergy'nin ilk varyantı 2007'de keşfedilmiş ve bu sürüm Dağıtık Hizmet Reddi Saldırılarını destekleyen köle bilgisayarlar (Distributed Denial of Service Attacks (DDoS)) üretmek için kullanılmıştır [111]. İkinci türevi, birincisi ile aynı kabiliyete sahipti ve sistem kaynaklarını zayıflatabiliyor ve ağ trafiğini izleyebiliyordu. BlackEnergy 3 ise bu özelliklerin birçoğuna sahiptir, ancak aynı zamanda Microsoft Office kullanan kişileri hedef alabilmektedir. Microsoft Office, dünyadaki hemen her şirkette kurumsal ortamda kullanılmaktadır ve bu nedenle saldırı vektörünün kapsamı oldukça geniştir. BlackEnergy 3, klavye takip (keylogger), şifre çalıcı, sistem yok etme ve ağ tarama gibi çok sayıda eklentiyi içermektedir.

Ukrayna saldırısında, zararlının bulaşma yöntemi, kimlik avı e-postasıydı. Enfekte edilen dosyayı operatörün makinelerine gönderilip, operatör tarafından doküman açıldığında, zararlı kullanıcıya makroların devre dışı bırakıldığını gösteren bir uyarı mesajı ile makroları etkinleştirmeleri istemiştir. Makrolar etkinleştirildiğinde, kötü amaçlı yazılım sistemi ele geçirip BlackEnergy 3 zararlı yazılımını yükleyip onu tehlikeye atabilmiştir.

Saldırgan sistem üzerinde kontrolü sağladığında, saldırının yönetimi ve etkinleştirilmesi süreci başlamıştır. Bu süreçte, kötü amaçlı yazılım bilgisayarlara yüklendikten sonra, saldırganların enfekte sistemlere uzaktan erişmesini sağlayan komuta ve kontrol sistemleri ile bir bağlantı açılmaktadır. Uzaktan erişim elde edildikten sonra, saldırganlar kullanıcı kimlik bilgilerini aldıktan sonra ayrıcalıklı hesaplara erişerek yetki yükseltimi yapmışlardır [112]. Saldırının son evresi ise EKS ağına saldırının gerçekleştirilmesini, yüklenmesini ve yürütülmesini içermektedir. Bu aşamada saldırganlar EKS ağına erişim elde etmek için sanal özel ağ (VPN) kullanmışlardır. Ardından KillDisk yazılımı sayesinde iş istasyonlarını, sunucuları ve bazı HMI'ları silmişler ve iz bilgisi bırakmamak için diğer makinelerde de günlükleri kayıtlarını (log) ve olayları silmişlerdir. Saldırı sonucunda, en az 27 trafo ve 225.000 müşterinin etkilendiği belirtilmiştir [110].

EKS'ye yönelik kasıtlı saldırılar veya SQL slammer solucanı gibi kasıtsız saldırılar nedeniyle kritik altyapılarda meydana gelebilecek önemli kesintiler sadece altyapının kendi değerinden çok daha fazla ulusal çapta ekonomik zarara yol açabilmektedir. Duggan tarafından 2005 yılında gerçekleştirilen bir çalışmada EKS'ye yönelik bir saldırının sonucunda;

- EKS şebekeleri arasındaki bilgi akışının durdurulması veya geciktirilmesi ile kritik zamanlı işlevlerinin yerine getirilmesi engellenebilir,
- Talimatlar, komutlar veya alarmda yetkisiz değişiklikler ile donanıma zarar verebilecek veya devre dışı bırakabilecek ya da kapatabilecek eşik değerler atanabilir (Stuxnet),
- Çevresel olumsuz sonuçlar yaratabilir ve / veya insan hayatını tehlikeye atabilir,
- Sistem operatörlerine yanlış bilgilendirmeler gönderilebilir,
- EKS yazılımı veya yapılandırma ayarları değiştirilebilir,
- İnsan hayatını tehlikeye atabilecek güvenlik sistemlerinin çalışmasına müdahale edilebilir [113].

Endüstriyel Kontrol Sistemlerinin yönettiği altyapıların ülkeler için kritikliği ve hassasiyeti, siber terörizm ve siber savaşın öncelikli hedeflerinden biri haline getirmiştir. Bu nedenle, endüstriyel kontrol sistemlerinde kullanılan protokollerde (ModBUS, Profinet, DNP3, vb.) ve bileşenlerde (PLC, HMI, RTU, MTU, vb.) var olan açıklıkların ortaya çıkarılması için derinlemesine analiz edilmesi hayati önemlidir [114]. Ancak bu sayede tespit edilen açıklıklara önlem alınması ve saldırganlar tarafından tekrar istismar edilmesinin önlenmesi sağlanabilecektir [61, 115, 116].

Endüstriyel kontrol sistemlerinde oluşan açıklıklar Duggan'ın çalışmasında da ele alındığı üzere, saldırganların ağa sızmalarına, kontrol yazılımlarına erişmelerine ve sistemlerin çalışma koşullarını değiştirerek, istenmeyen büyük zararların oluşmasına neden olabilmektedir [33, 113]. Ağın gizli tutulması, kullanılan tüm bağlantıların sadece ilgili kurum ve kuruluşa ait olması, yetkisiz girişlerin (özellikle de İnternet tabanlı) engellenmesi açısından oldukça faydalı olabilecektir. Ancak birbirine bağlı ağların kullanılmasının neredeyse zorunlu olduğu günümüzde söz konusu "izole" bir ağ ile sistemlerin yönetilmesi mümkün değildir [117]. Üst bölümde yer alan EKS'ye yönelik saldırılar, yaşanan güvenlik olaylarına sadece örnek olması amacıyla belirtilmiştir. EKS'ye gerçekleştirilen saldırıların önemli bir bölümü ise kötü ün nedeniyle birçok ülke tarafından kamuoyuna açıklanmamaktadır.

3.6. EKS'de Yama ve Güncelleme

Bilinen güvenlik açıkları olan sistemler tipik olarak yazılım geliştiricileri ve satıcıları tarafından yapılan yazılım yükseltmeleri ile "yamalı" hale getirilmektedir. Güvenlik

yazılımının güncellemelerinin yüklenmesi, endüstriyel sistemlerin güvenliğini sağlamak için çok önemlidir ancak EKS'lerde "düzeltme eklerinin zamanında uygulanması mümkün olamamaktadır. EKS güvenlik yamaları, EKS'nin yönettiği altyapının sürekliliğini sağlamak maksadıyla, uygulanmadan önce sistem hataları veya kesintileri için tamamen sınanması gerekmektedir. Yazılım geliştirici ve satıcıları tarafından desteklenmeyen (end of life) EKS bileşenleri, güvenlik yamaları geliştirilmemesi nedeniyle sömürüye uğrama riski altındadır. 2006 Carnegie Mellon deneysel analizi, yazılım yamaları yayınlandıktan sonra siber saldırıların arttığını ve bunun da, düzeltilmemiş sistemlerin daha fazla sömürü riski taşıdıkları anlamına geldiğini tespit etmiştir [118]. Bunun sonucunda da, EKS sistemleri (Hem SCADA hem de DCS altyapıları) siber saldırganlar tarafından fidye için hırsızlık, hırsızlığa karşı hacking, parasal amaçlı korsanlık, siber terörizm ve siber savaş amaçlı hedef alınmaktadır [119].

EKS sistemlerinde kullanılan yazılımların yamalarına ilişkin Igure, Laughter ve Williams (2006), en yeni ürün bilgisi, güncelleme ve yamalarla düzenli olarak korunması gerektiğini, ancak bu süreçte "en son düzeltme eklerinin" uygun bir inceleme sürecinden sonra uygulanması gerektiğini savunmaktadırlar. Uygun inceleme süreci, yamaların benzer bir EKS üzerinde çevrimdışı olarak test edilmesini gerektirmektedir [97]. Stouffer, Falco ve Scarfone (2011) ise EKS'ye yama uygulanmasının doğru prosedürlerini ve bu prosedürlere uyulmaması durumunda altyapının olumsuz yönde etkilenebileceğini belirtmişlerdir. Çalışmalarında, yamaların güvenlik açığını ortadan kaldırmak için kullanılabileceğini, ancak yama kullanılmasının üretim veya güvenlik risklerine neden olabileceği üzerinde durmuşlardır [80].

İşletim sistemlerinin güvenlik açıkları, üreticiler tarafından düzenli olarak duyurulmaktadır. Yamalar normalde güvenlik açıkları tespit edildikten sonra yayınlanmaktadır, ancak bu yayın süreci için önemli bir zaman gecikmesi gerekebilir veya yamalar ihtiyaç duyulan süre içinde uygulanamayabilir. 2010 yılında tespit edilen Stuxnet'in kullandığı güvenlik açığının yaması 2012 yılında piyasaya sunulmuştur [13, 120].

3.7. PLC Güvenliği

PLC'ler, endüstriyel donanımları ve bilgisayar donanımı ile arayüz oluşturan süreçleri kontrol etmek için kullanılan donanımlardır. Modern PLC'ler, güç kaynağı, mikroişlemci,

dijital ve analog giriş / çıkış ve bir iletişim biriminden oluşan modüler yapıdadır. PLC'ler, belirli proseslerin operasyonel kontrolünü sağlayan EKS'de önemli bir bileşeni oluşturmaktadır. PLC'ler, birçok endüstriyel proseste, sistem veri girişine dayalı önceden programlanmış talimatlar sağlamak için yaygın şekilde kullanılmaktadır. Enerji sektöründe PLC'ler, herhangi bir sistemdeki akışkan hacmi, akış hızı ve basıncı kontrol etmek için sık sık kullanılır. Proses limitlerini belirlemek için girilen parametreler ile PLC, programlamadan sonra insan müdahalesini en aza indirerek sistemin çalıştırılabilmesine imkan sağlar [80, 89]. PLC'ler, sıralama, zamanlama ve sayma olmak üzere önceden belirlenmiş fonksiyonları yerine getirmek için kodlanmış talimatları programlanabilir hafızasında saklayan ve yürüten mikroişlemcileri kullanır [121]. PLC'ler esnek bir yapı sağlar ve değişiklikleri dahil etmek için yeni modüller ile kolayca genişletilebilir. Bir PLC'nin yeniden programlanması oldukça kolaydır ve bu nedenle bir sistemdeki donanımı modifiye etmekten daha maliyetlidir [122].

Kontrol mühendisleri PLC'yi kapalı döngü veya açık döngü işlevselliği, arıza bulma ve alan aygıtı iletişimi için programlamak için yazılım kullanmaktadır. 1993 yılında kar amacı gütmeyen Uluslararası Elektromekanik Komisyon (IEC), IEC 61131 olarak bilinen programlanabilir mantık denetleyicisi programlama standardını yayımladı. Bu standart, kontrol sistemleri, ladder diyagramı, sıralı fonksiyon çizelgesi, fonksiyon blok diyagramı, yapılandırılmış metin ve talimat listesi için beş programlama dilini tanımlamaktadır [85].

Endüstriyel kontrol sistemleri (EKS), üretim ve kontrol sürecinin ayrılmaz bir bileşenidir. Çağımızın modern altyapılarının çoğunluğunun yönetimi bu sistemlere dayanmaktadır. Ancak güvenlik açısından incelendiğinde Endüstriyel Kontrol Sistemlerinin önemli bir bileşeni olan ve yukarıda belirtilen önemli faaliyetleri gerçekleştirerek insan hayatına önemli katkılar sağlayan PLC’lerin dış ağlara ve özellikle de İnternet tabanlı yapılara açık bir mimari içinde bulunduğu görülmektedir. PLC, 1960'lı yılların başından beri kullanımdadır ve başlangıçta otomatik endüstriyel proseslerin güvenilir ve güvenli bir şekilde çalışması için tasarlanmıştır. İlk tasarımların yapıldığı dönemde, internet, tehdit ajanları veya kötücül yazılımlar olmadığı için, güvenli yazılım ve iletişim protokolleri mevcut değildi. Bu nedenle, güvenlik, EKS saha donanımları için bir gereksinim değildi. Bu nedenle, EKS saha cihazları tasarımları gereği güvensizdir ve saha donanımlarının en önemlilerinden olan PLC'ler doğal olarak sömürüye karşı savunmasızdır.

Bir PLC'nin güvenirliliği birçok bileşeninin icraatlarına ve bu bileşenler arasındaki iletişime dayanmaktadır. PLC'lerin temel yapı taşı olduğu EKS'lerin iletişimini engellemek için, saldırganlar siber ortamdaki açıklıklar sayesinde sistem bileşenlerine ve özellikle de yönetim birimlerine erişerek, bu bileşeni başka bir cihaz gibi yapılandırabilir veya bu cihaz sayesinde yanlış veya sahte bilgiler göndererek sisteme önemli zararlar verilebilir.

TCP/IP protokolü kullanılan geleneksel Ethernet ağlarının analizine yönelik çalışmaların sayısı günden güne artmaktadır. Bu çalışmalar sayesinde ağ üzerinde paketlerin yakalanması ve müteakiben de yakalanan paketlerin yorumlanması saldırı esnasında veya hemen sonrasında önlem alınması için oldukça önemlidir. Yakalanan paketler uygun bir şekilde kayıtlandığı sürece saldırıların kaynağının belirlenmesi için tekrar tekrar analiz edilebilirler.

Modern ağ analizinde yaygın olarak kullanılan birçok paket yakalama ve analiz yazılım ve donanımı bulunmaktadır. Söz konusu donanımların çoğunluğu, TCP/IP protokolüne ait paketlerin analizine odaklanmaktadır. Ancak açık kaynak kodlu ve ticari ağ analizi donanımlarının oldukça kısıtlı bir miktarı SCADA başta olmak üzere endüstriyel kontrol sistemlerinde kullanılan ModBUS, DNP3 gibi protokollerin analizine imkan vermektedir.

Bu nedenle çalışmada, EKS'lerin önemli bileşenlerinden birisi olan PLC cihazında kullanılan protokollerin güvenlik açıklıklarından faydalanılarak, söz konusu protokollerdeki güvenliğin nasıl aşıldığını bulmak amacıyla bir test ortamı (Testbed) oluşturulmuştur. Sınama ortamında öncelikle, Ortadaki Adam (Man in the Middle-MitM), Hizmet Reddi (Denial of Service-DoS), Port Tarama ve Başlat/Durdur (Start/Stop) saldırıları ile endüstriyel kontrol sistemlerinin yönetim birimi olan PLC'nin açıklığı değerlendirilmiştir. Müteakiben gerçekleştirilen saldırılara ilişkin paketler yakalanarak analiz edilmiş ve saldırıların paternleri çıkarılmıştır. Bu sayede, ağın saldırılardan en az zararla kurtarılması ve benzer saldırıların engellenmesinde etkili olarak kullanılması hedeflenmiştir.

3.8. Endüstriyel Kontrol Sistemi Güvenliğine Yönelik Yapılan Benzer Çalışmalar

EKS'lerin güvenliğine yönelik çalışmaların bir bölümünde benzetim modellerine dayalı analizlere odaklanılmıştır. Bu kapsamda Giani ve arkadaşları, EKS'lerin incelenmesine yönelik değişik test ortamlarını önermişlerdir. İlk test ortamında Simulink Matworks, ikinci

test ortamında ise Omnet++ DEVS kullanılarak ağ bileşenleri benzetim ortamına aktarılarak saldırılar test edilmiştir [123]. Oman ve Phillips çalışmalarında, benzetim modeli tabanlı test ortamı üzerinden TELNET kaçak girişlerini incelemişlerdir [124]. Byres, Hoffman ve Kube, EKS'lerde kullanılan protokollerin komut satırlarındaki açıklıkların tespitini incelemişlerdir. Çalışma sonucunda yüksek seviyede açıklıklar tespit edilerek, acil çözüm önerilerinin alınması önerilmiştir [125]. Genge, Graur ve Haller, EKS'lerin güvenliği üzerine yaptıkları çalışmada; benzetim sistemi üzerinde derinliğine savunma stratejileri, ağ bölümlendirmesi, ağ güvenlik duvarı yapılandırması, IDS/IPS sistemleri ile anormallik tespit sistemi analiz edilmiştir. Çalışmanın saldırı sonuçları, derinliğine savunmanın kullanılmasının önemini vurgulamıştır [126]. Sayegh, Chehab ve Elhajj ise benzetim sistemleri ile Omron PLC ve HMI donanımları ve bu donanımların kullandığı FINS protokolünün açıklıkları test etmişlerdir [127]. Simülasyon ve modelleme teknikleri karmaşık sistemleri modellemek ve test etmek için faydalıdır. Gerçekçi modellerin geliştirilmesi, henüz var olmayan veya inşa edilmesi çok masraflı olan senaryolar oluşturmaya yardımcı olabilmektedir. Ancak benzetim sistemlerine dayalı çalışmaların en büyük eksikliği, gerçek sistemi tam olarak yansıtmanın zorluğu ve bu nedenle yapılan analizlerin gerçek sistemde de aynı sonuçları vermemesi ihtimalidir.

Endüstriyel Kontrol Sistemlerinin güvenliği kapsamında yapılan çalışmaların diğer bir kısmı ise gizliliğe odaklanmaktadır. Li, Mao, Lai ve Qiu bu kapsamda yaptıkları çalışmada, sıkıştırılmış sayaç okuyucu da rastgele sıra numarası kullanarak gizliliği sağlamayı hedeflemişlerdir [128]. Kalogridis ve diğerleri çalışmalarında, evlerde cihazların kullandığı güç tüketimini gizlemek için, ev yük imzalarını belirten ev elektrik güç yönlendirme şeması kullanmışlardır [129]. Shi ve Perrig bu doğrultuda yaptıkları çalışmalarında, SHA-1 veya HMAC-SHA-1 ve RSA gibi sayısal imzaları da içeren birçok araç kimlik doğrulama ve bütünlüğü sağlayan özet (hash) ve anahtarlanmış özet (keyed hash) araçlarının kullanılmasını önermişlerdir [130]. Yukarıdaki çözüm önerileri genellikle anahtar yönetimini de kapsayan kriptografi teknolojilerine dayanmaktadır. Ancak günümüzdeki endüstriyel kontrol sistemi şebekelerinin milyonlarca donanımı barındıran yüzlerce kurumu kapsadığı dikkate alındığında bu çözüm önerilerinin pratikte uygulanmasının zorluğu daha iyi anlaşılabilmektedir.

Klick, Lau, Marzin, Malchow ve Roth yaptıkları çalışmada, PLC yazılımını olan Statement List (STL)'i kullanarak zararlı kod enjekte etmişlerdir. Bu sayede, PLC üzerinden SNMP (Simple Network Management Protocol-Basit Ağ Yönetim Protokolü) paketleri göndererek endüstriyel kontrol sistemi ağı ile ilgili bilgileri toplamayı ve müteakiben de zararlı kod

enjekte edilen PLC'yi Proxy olarak kullanarak ağın diğer bileşenlerine nüfuz etmeyi hedeflemişlerdir. Çalışmanın sonucunda, PLC'lerin endüstriyel kontrol sistemi içinde zafiyet değerlendirmesinin yapılmasın ve ağa bu donanım üzerinden erişebileceği dikkate alınarak, sürekli izlenmesi önerilmiştir [131].

EKS'lere karşı gerçekleştirilen saldırılara karşı Guan, Graham ve Hieb yaptıkları çalışmada, erişebilirlik matrisi ve seviye bölümlendirmesi ile risk değerlendirme sürecinin tamamlanmasını müteakip risk azaltma sürecinde ilk müdahale edilecek varlıkların tespit edilerek, olası bir risk ya da problem durumunda tepki süresinin kısalması ve sistemlerin alacağı hasarın en aza indirilmesi hedeflenmiştir [132]. Hata tespitinde erişebilirlik matrisi kullanılmadığı durumlarda hata kaynağı olarak yanlış bileşen belirlenebilmekte ve hata giderme süreci uzayabilmektedir [133].

Urias, Van Leeuwen ve Richardson çalışmalarında, yaygın endüstriyel kontrol sistemlerinden olan Denetleme Kontrolü ve Veri Elde Etme (Supervisory Control and Data Acquisition- SCADA) sistemlerinin siber saldırılara karşı daha güvenli hale gelmeleri için açıklıkların tespiti ve bu açıklıkları engellemek için alınması gereken önlemlerin belirlenmesi maksadıyla geliştirilen sınama ortamını ele almışlardır [57].

EKS'ye yönelik yapılan diğer çalışmalar, inceleme odağı, kullanılan araçlar ve uygulama ile simülasyon çerçeveleri, sınama ortamları ve risk değerlendirme teknikleri dikkate alınarak oluşturulan özet tablo Çizelge 3.2'de verilmiştir. Çizelge incelendiğinde; EKS'ye yönelik gerçekleştirilen çalışmaların büyük bir bölümünün simülasyon ve emülasyon sitemlerine yönelik olduğu, gerçek sistemlerin yer aldığı uygulamların ise oldukça sınırlı olduğu görülmektedir. Kritik altyapılar başta olmak üzere, toplum yaşantısı için önemli olan sistemlerin yönetiminde kullanılan EKS'lere yönelik gerçekleştirilebilecek saldırılar sonucunda, sistemlerde meydana gelebilecek zararlar ve alınması gereken tedbirlerin belirlenmesi için gerçek sistem bileşenlerinin analizinin yapılması oldukça önemlidir. Bu nedenle, çalışmanın 4. Bölümünde gerçek sistemlerin yer aldığı sınama ortamına (Testbed) yönelik saldırı ve tespit analizlerine yer verilmiştir.

Çizelge 3.2. EKS güvenlik çalışmaları (İnceleme odağı, kullanılan araçlar ve uygulama ile simülasyon çerçeveleri, test yatakları ve risk değerlendirme teknikleri)

Kategori	Alt kategori	Odak (Hedef Saldırı)	Kullanılan Araçlar	Uygulama	Atıf
Simülasyon Çalışmaları	SCADASiM	Düzenleyici İzleme	ADACS	Su Altyapısı	[133]
	SCADASiM	DDoS, Aldatma (Spoofing) Saldırıları	OMNET++	Akıllı Sayaç, Rüzgar Enerji Santrali	[134]
	MALsim	Güvenlik değerlendirmesi için kötücül simülasyonu	JADE tabanlı MAlsim	Güç Sistemleri	[135]
	Eş Simülasyon (Co-simulation)	Akıllı şebeke bileşen analizi	CIM, GridLab-D, AKKA, EclipseSCADA	Güç Sistemleri	[136]
	Framework	SCADA ve simülasyon entegrasyonu	EngSB	Yazılım Prototipi	[137]
	Framework	Kötü amaçlı yazılım denemesi	MATLAB, Emulab	Bir santralde Stuxnet, Tennessee-Eastman	[3, 97]
Testbed	Simülasyon	DoS	TrueTime (MATLAB/Simulink)	Amerikan Gaz İştirak Raporu No. 12	[138]
	Simülasyon	FINS protokolünün açıklıklar	Donanım, yazılım, anomali tespiti	Omron PLC ve HMI	[126]
	Hibrit (simülasyon, öykünme (emulation) , donanım)	HMI saldırısı için Anomali tabanlı tespit, DoS	Donanım, yazılım, anomali tespiti	Sandia Ulusal Laboratuvarlarında SCADA sistemleri	[117]
	Hibrit (simülasyon, öykünme (emulation) , donanım)	HMI saldırısı için Anomali tabanlı tespit, DoS	OPNET, PowerWorld, ASPS	Arizona Üniversitesi'nde Biyosfer 2 Güç Şebekesi	[2]
	Pedogoji	Modbus, HMI	Donanım, yazılım, Snort	Çeşitli endüstriyel uygulamalar	[2]
	İzinsiz Giriş ve Savunma	Haberleşme protokolleri ve ağlar	Donanım, yazılım, anomali tespiti	PowerCyber testbed	[139]
	İstatistiksel Veri Toplama	DoS, veri kayıtlama	Veri İstatistikleri	Güç Kontrol Sistemleri - Esneklik Testi CESI RICERCA Laboratuvarı	[140]
	Saldırı	DoS, Bütünlük, Oltalama	Simülasyon	Simülasyon tabanlı örnekleme	[59]

Çizelge 3.2. (devam) EKS güvenlik çalışmaları (İnceleme odağı, kullanılan araçlar ve uygulama ile simülasyon çerçeveleri, test yatakları ve risk değerlendirme teknikleri)

Kategori	Alt kategori	Odak (Hedef Saldırı)	Kullanılan Araçlar	Uygulama	Atıf
Testbed	Haberleşme Ağı	DDoS, Ağ	Simulink/Stateflow, HLA, NS2, OPNET, OMNeT++	Tennessee Eastman kimyasal süreç	[141]
	Saldırı	DDoS	SCADA 2, Modbus simülatörü, GNS3	Genel uygulama	[141]
	Sanal Makine	Modbus TCP/IP, DDoS, Hatalı veri enjeksiyonu	Genel Açık Araştırma Emülatörü, Python,	Su deposu sistemi	[142]
	Kaçak Tespiti, Olay Yönetimi	RTU'lar	Snort, Perl, XML	Elektrik trafosu	[123]
Risk değerlen-dirmesi	Olasılık	Risk tahmini	HMM, IIM, RFRM	Genel sistem	[143]
	Modelleme	Kontrol Sistemleri	NSRM	Petrol boru hattı pompa istasyonu	[144]
	Modelleme	Kontrol Sistemleri	Erişebilirlik matrisi	Arıtma sistemi	[131]
	Saldırı Diyagramı	Bayesian ağ	MTTC, CVSS	IEEE RTS79	[145]
	Saldırı Ağacı	Açıklık değerlendirmesi	Açıklık İndeksi	Kontrol Merkezi	[146]
Simülasyon	Saldırı Ağacı	İzinsiz Giriş	Colored Petri Net	SCADA durum çalışması	[147]
	Hatalı sıralama mantık saldırısı	İzinsiz Giriş	MATLAB/ Simulink	Üç tank sistemi	[148]
	Zararlı Yazılım Saldırıları	Modbus	MAlsim	Güç Santrali testbed	[11]
	Test bed	Modbus TCP	Snort, OSSIM OpenVAS, Sebekd	Simüle edilmiş PLC	[149]
	MitM	IEC 60870-5-104	Kali Linux, Snort, WinPP104, Qtester	Yazılım simüle laboratuvarı, testbed	[150]
	Grafik	Modbus	"C" Dili	Tennessee Eastman kimyasal süreç	[151]
	İzleme	Zararlı Komutlar	Gerçek Zamanlı ve simülasyon izlemesi	Su arıtma tesisi	[152]
	Saldırı	DDoS	OPNET	Hidroelektrik	[153]
	Saldırı	Zararlı Yazılım Enjeksiyonu, DoS, MitM	Netlogo	Kurumsal ağa bağlı elektrik şebekesi, NS2	[154]

Çizelge 3.2. (devam) EKS güvenlik çalışmaları (İnceleme odağı, kullanılan araçlar ve uygulama ile simülasyon çerçeveleri, test yatakları ve risk değerlendirme teknikleri)

Kategori	Alt kategori	Odak (Hedef Saldırı)	Kullanılan Araçlar	Uygulama	Atıf
Modelleme	Matematiksel	DoS, Aldatma Saldırıları	Doğrusal dinamik modeller	Su tankı	[155]
	Matematiksel	Model odaklı test	Modelica, Eclipse	Valf ve pompalı tank	[156]
	Oyun teorisi	Siber saldırgan ve operatör arasındaki etkileşimler	Yarı ağ-form oyunu (Semi network-form game-SNFG)	Dağıtım besleyici hattı	[157]
	Bayesian Ağları	Sistem bekası	SCADASim	MitM	[158]
	FNN	Savunma	Faktörlü sinir ağı (Factor neural network)	Genel	[159]
	Framework (Çerçeve), saldırı ağaçları	Modbus, DoS	RAIM	Güç sistemi kontrol ağı	[59]
Saldırı	Saldırı Ağaçları	Modbus/TCP	Saldırı ağaçları	Genel sistem	[160]
	Tekrar Saldırısı	Sensörler	Analitik, simülasyon	Tenessee Eastman problemi	[161]
	Hatalı Veri Enjeksiyonu	AC durum tahmini	Analitik	Su deposu sistemi	[162]
	Hatalı Veri Enjeksiyonu	Bütünlük	Analitik	Akıllı Sayaçlar	[130]
	Hatalı Veri Enjeksiyonu	SNMP	STL	PLC	[54]
Makine Öğrenme	Anomali tabanlı	Bütünlük saldırıları, MITM, Modbus / TCP	WEKA, EPANET, VMs, k-means	Simüle ve gerçek veri setleri, Su dağıtım sistemi	[6]
	Anomali tespit	Telekomünikasyon ağları	SVM	Data setleri	[163]
	Komut satırlarındaki açıklıkların tespiti	EKS Protokollerindeki Sözdizimleri (syntax)	BlackPeer	Genel sistem	[124]
	Özellik Filtreleme	Kötü amaçlı yazılım tespiti	SVM, N-gram analizi	Genel sistem	[164]
	Tek sınıf sınıflandırma	Kötü amaçlı yazılım kaçak girişleri	SVDD, kernel PCA	Gaz boru hattı test yatağı ve su arıtma tesisinden gerçek veriler	[165]
	İtibar sistemi, dağıtılmış ajanlar	Sensörler	Denetimsiz öğrenme	Sensör ağları	[166]

Çizelge 3.2. (devam) EKS güvenlik çalışmaları (İnceleme odağı, kullanılan araçlar ve uygulama ile simülasyon çerçeveleri, test yatakları ve risk değerlendirme teknikleri)

Kategori	Alt kategori	Odak (Hedef Saldırı)	Kullanılan Araçlar	Uygulama	Atıf
Makine Öğrenme	Haberleşme protokolleri	DNP3, gri delik saldırısı	SVM	İz tabanlı simülasyon	[167]
	Analitik	Bulut tabanlı veri analitiği	OpenPlanet, Hadoop, regression tree, Floe, MapReduce, WEKA,VM	Los Angeles Akıllı Şebeke Projesi	[168]
Kaçak Tespit Sistemi Bal Küpleri	Kural tabanlı	IEC 60870-5-104	Derin paket incelemesi, ITACA	Protokol trafik durumu çalışması	[8]
	Filtreleme sistemi	Modbus and DNP311	Güvenlik duvarı	Endüstriyel Ağ Güvenliği Laboratuvarı	[11]
	İzinsiz giriş toleransı, durum makinesi yaklaşımı	SCADA	Donanım	Elektrik iletimi ve dağıtımı için basit SCADA master ve RDU	[12]
	Kritik durum tabanlı	PLC'de Modbus	ISML	Ortak Araştırma Merkezi test ortamı	[169]
	Köle (bot) ağlar	Yeni köle ağların tespiti	Honeyd	Veri izleri	[170]
	Analiz	SCADA'nın korunması, bal küpü teknikleri	Honeywell CDROM	Bal küpü karşıtı teknikler	[16]
	Vekil (proxy) kullanımı	Düşük maliyetli bal küpü teknikleri	Honeyd+, Raspberry Pi	Slammer, Code Red, Blaster	[171]
	Kötücül yazılım	Geniş ölçekli kötücül yazılım	nepenthes	Nepenthes	[172]
	Virüs	Virüs bulma ve hızlı antivirüs yayma	Dinamik dağıtık bağışıklık stratejisi	E-posta ağı	[173]
Kriptoloji	Gizlilik	Akıllı sayaç	Sıra numarası	Veri izleri	[127]
	Gizlilik	Akıllı sayaç	Elektrik güç yönlendirme şeması	Ev yük (payload) imzaları	[128]
	Gizlilik	MitM, Bütünlük	SHA-1, HMAC-SHA-1, RSA		[129]
Saldırı Sonrası	Adli analiz	Akıllı şebekeler	İzler, Leurré.com sistemi	Saldırı ilişkilendirmesi	[4] [170]

4. ENDÜSTRİYEL KONTROL SİSTEMİ ÇALIŞANLARINDA BİLGİ GÜVENLİĞİ FARKINDALIĞI

Çağımızda bilgi teknolojileri günlük yaşantımızın hemen her alanında kullanılmaya başlamıştır. Bu nedenle de, özel bilgilerimiz de dahil olmak üzere tüm bilgilerimiz sayısallaşmaktadır. Bu sayısallaşma, sadece haberleşme yöntemlerimizi değiştirmekle kalmamış, yeni bir çalışma ve yaşam biçimi oluşturmuştur. Bilgi teknolojileri, dolayısıyla sayısallaşma, üretkenlik, verimlilik, zaman kazancı gibi yaşantımıza birçok imkan ve kabiliyetler kazandırmaktadır. Ancak, söz konusu bilgi teknolojilerinin güvenliği sağlanamadığı takdirde, sistemlerde oluşan önemli açıklıklar ve tehditler nedeniyle, telafisi olmayan zararlarla karşı karşıya kalınabilir. Bu nedenle, bilgi teknolojilerinin kullanımında dikkat edilmesi gereken en temel konu güvenliktir. Bilgi teknolojileri ve özellikle bilgi güvenliği konusunda en önemli bileşenlerden birisi de, çoğunlukla göz ardı edilen veya unutulan ancak bilgi güvenliği zincirinin en zayıf halkası olarak tabir edilen insan faktörüdür. Çünkü en güncel, en son teknoloji ürünü güvenlik sistemi donanım ve yazılımlarına sahip olunsa bile, en alt düzey çalışanından en üst düzey yöneticisine kadar bu donanımlarının gereksinimlerini kabul edip, kurumun hedeflerine ulaşılması için gerekliliğine ve yararına inanılmazsa bu kurum için güvenlikten söz edilemez. Çünkü kullanıcılar olarak adlandırılan çalışanlarda yeterli farkındalık oluşturulamadığı için bu donanımlar amaçlandığı biçimde kullanılmadığından yeterli etkinlik ve verim alınamayacaktır. Bu nedenle, çalışmanın bu bölümünde bilgi güvenliği üçlüsünün insan faktörüne odaklanılmıştır.

Bilgi güvenliğine dayalı problemlerin yalnızca teknik yöntemlerle çözümlenebileceği düşüncesi, bilgi güvenliğinin sağlanmasında belki de en önemli unsur olan insan faktörünün ve kullanıcılarının deneyimlerinin göz ardı edilmesine neden olmaktadır. Oysa güvenlik açığı yazılım ya da donanıma dayalı olmaktan çok insan faktörüne bağlı olarak ortaya çıkmaktadır [68]. İnsan faktörünü aşan bir saldırganın antivirüs yazılımlarını, güvenlik duvarlarını ya da saldırıları rapor eden sistemleri aşması çok daha kolay olmaktadır. Çünkü tüm teknolojik düzenlemeler ve güvenlik politikaları geliştirilse ve belirlense bile farkındalığı eksik kullanıcılar tüm bu teknik çözümleri etkisiz hale getirecektir [69]. Bilgi güvenliği risklerinden korunmanın en iyi yolu ise, bilgi teknolojilerine daha fazla yatırım yapmak ve korunma amaçlı teknolojileri daha çok kullanmaktan önce kullanıcıların bilinçlenmesiyle ve ihtiyaç duyulan güvenlik teknolojisinin doğru yer ve zamanda kullanılmasıdır.

Kurumların en değerli varlıkları olan bilginin; gizlilik, bütünlük ve erişilebilirlik nitelikleri bakımından sürekli korunması, bilgi güvenliğinin sağlanması gerekmektedir. Bu bileşenlere kimlik doğrulama, taklit edilememe gibi diğer özellikler eklenebilmektedir. Bilgi güvenliği; en temel olarak bilginin korunması olarak tanımlanmıştır [174]. Diğer bir tanımda ise, bilgi güvenliği, bilginin istenmeyen ya da yetkisiz kişi veya varlıklar tarafından erişilmemesinin, kullanılmamasının, ifşa edilmemesinin, bozulmamasının, değiştirilmemesinin, görülmemesinin, kayıt edilmemesinin ve yok edilmemesinin garanti edilmesi olarak tanımlanmaktadır [175]. Bilgi güvenliği farkındalığı ise, bilişim sistemi kullanıcılarını bilgi güvenliği gereklilikleri ve bireysel sorumlulukları hakkında bilgilendirerek ve bilinçlendirerek yeterli ilgi ve dikkati vermelerinin sağlanması olarak tanımlanmaktadır [176]. 1993 yılında düzenlenen Avrupa Güvenlik Forumu'nda bilgi güvenliği farkındalığı; her bir çalışan ya da kullanıcının bilgi güvenliğinin önemini, kurum için uygun olan bilgi güvenliği derecesini ve bireysel olarak kullanıcıların bilgi güvenliği sorumluluklarını anlama derecesi ve kapsamı olarak tanımlanmıştır [177].

Çoğu endüstriyel kontrol sistemi (akıllı şebekelerde dâhil olmak üzere) kurumu çalışanları ile yöneticileri, değerinin ve korunmasının öneminin farkında olmadığı oldukça hassas bilgileri kontrol etmektedirler. Güvenliği anlayabilmek için öncelikle sahip olunan bilginin değerini ve kurum için ne ifade ettiğini kavramak gerekmektedir. Çünkü birey kendisi için değerli olmayan hiçbir unsuru korumak istemez. Kullanıcılar, tehlikelerin farkında oldukları ve normal iş eğitiminin bir bölümü olarak bilgi güvenliği eğitimi aldıkları sürece, güvenlik kırılmalarının önlenmesine etkin olarak katkı sağlayabilirler [178]. Bu nedenle kritik altyapıları yöneten EKS'de dahil olmak üzere, her kurumun saldırılara karşı koymak için çalışanların sorumluluğu paylaşacağı bir bilgi güvenliği kültürü oluşturması gereklidir. Bilgi güvenliği kültürünün oluşturulmasıyla, riskler hiçbir zaman tam olarak yok edilemese de geliştirilen yazılımsal ya da donanımsal yöntemlerin dışında, bilişim güvenliği farkındalığının gelişmesi veya geliştirilmesi ve bu bilincin davranışa dönüşmesi ile kabul edilebilir bir düzeye indirilebilir [70].

Kullanıcılar bilgilerinin hem güvende olmasını hem de esneklik istemektedirler. Diğer bir ifadeyle kullanıcılar ne verilerinin çalınmasını ne de katı güvenlik önlemleri nedeniyle işlemlerinin aksamasını istemezler. Güvenlik ve kullanılabilirlik arasındaki dengeyi sağlamak kurumların bilgi güvenliği alanında yüzleşmek zorunda olduğu sorunlardan birisidir. Kullanıcıların bu ikilem arasında sürekli yön değiştirdiği bir ortamda saldırganlar

ile güvenlik uzmanları arasındaki mücadele sürekli olarak devam etmektedir. Ancak bu mücadelede sonucu değiştirebilecek en büyük etken insandır. Bu nedenle kullanıcıların bilgi güvenliği farkındalığı, kurumların öncelikli hedeflerinden olmalıdır [179-181].

Çoğu kurumda ihtiyaç duyulan antivirüs yazılımlarını ve güvenlik duvarlarını kuran, sürekli güncelleştirmelerini ve kurumsal bilgilerin yedeklemesini yapan Bilgi Teknolojileri (BT) personeli bulunmaktadır. BT personeli tarafından alınan söz konusu teknik önlemleri detayıyla tüm çalışanların bilmesi gerekli değildir. Ancak alınan önlemlerin gerekliliği ve uygun şekilde kullanılmadıklarında ya da kullanılabilirliği ve iş hızını etkilediği düşüncesiyle devre dışı bırakılmaları durumunda kurumun hangi risklerle karşı karşıya kalabileceği konusunda tüm çalışanlar/kullanıcılar bilinçlendirilmeli ve bu maksatla gerekli eğitimler verilmelidir [182].

Deloitte tarafından 2009 yılında gerçekleştirilen araştırma sonucunda, insan hatası açık farkla (% 86) en büyük güvenlik zayıflığı olarak tespit edilmiş, teknolojik eksiklikler nedeniyle oluşan hatalar ise ile ikinci sırada yer almıştır. Çalışanların kazara ya da kasıtlı olarak parolaları başkalarına söylemesi, güçlü bir parola seçmemesi, şüpheli bir elektronik postayı açması, zararlı içerik bulunduran bir web sayfasına girmesi gibi oldukça basit olarak görülen hatalar en güçlü teknolojilerle alınan güvenlik önlemlerini geçersiz hale getirmektedir. Bunun sonucunda ise ekonomik zararın yanında, aynı zamanda vatandaşların yaşantılarında önemli hizmetlerin aksamasına sebep olabilmektedir [20]. Üçüncü bölümde yer alan EKS'lere yönelik saldırılar sonucunda ülkelerin yaşadığı zararlar bu konudaki önemli örneklerdendir. Örneğin, Ukrayna Güç Tablosu saldırısında, saldırganlar, mızrak e-postalama (spear phishing) e-postaları, BlackEnergy 3 kötücül yazılım varyantları ve kötü amaçlı yazılım içeren Microsoft Office belgelerinin manipülasyonu da dahil olmak üzere insan odaklı zafiyetleri kullanmışlardır [183]. Saldırı sonucunda, Enerji/Nükleer reaktörlerin ve atık sektörlerinin HMI'ları enfekte olmuş ve tespit süresinin gecikmesiyle orantılı olarak, sistemin neredeyse tamamı risk altına girmiştir. İnsan etkileşimi ve hata potansiyeli nedeniyle HMI, özellikle de eski bir işletim sistemine sahipse, bir sistemin en az güvenli bileşeni olarak kullanılabilir [110]. Bu örnekler EKS'nin karşılaştığı birçok güvenlik açığından sadece birkaçıdır. Bu örneklerin çoğu eğitimsiz personel ve sistem bakımı kapsamına girmektedir. Personel, bir saldırının etkilerinin yeterince farkında olmadığında, siber güvenlik uzmanlarının sahip oldukları hassasiyeti ve ilgiyi göstermeyebilirler. Herhangi bir sistemde insan etkileşimi olduğu

sürece, bu etkileşim yüzünden zayıflıklar olacaktır. Kurumlar, insan etkileşimi az olan ortamlarda donanımların arızalanması riskini dengelemeye çalışırken, diğer taraftan da insan arayüzünü sınırlamayı ve/veya personel eğitimini ve farkındalığını geliştirmeyi düşünmelidirler [114]. Çünkü sistemler sertleştikçe, saldırı oluşumu, içeriden yardım almadan sisteme erişmenin zorluğundan dolayı öncelikli olarak dışsallığa değil iç açıkları ve zafiyetleri tespit etme eğilimindedir.

Farkındalık bölümünün devam eden kısımlarında sırasıyla; ikinci kısımda bilgi güvenliğinin insan boyutu bileşenine yönelik gerçekleştirilen benzer çalışmalar ele alınmıştır. Üçüncü kısımda çalışma kapsamında uygulanan anket uygulamasına, analiz sonuçları ve çıkarımlara yer verilmiş, sonuç kısmıyla bölüm tamamlanmıştır.

4.1. Bilgi Güvenliği Farkındalığına Yönelik Benzer Çalışmalar

Bilgi güvenliği üzerine yapılan çalışmalarda genellikle güvenlik ihlallerine ve bu ihlallerin etkileri üzerine incelemeler yapılmaktadır. Ancak kullanıcıların bu güvenlik ihlalleri hakkında ne düşündükleri, ne bildikleri veya bu ihlallerin sonucunda kendilerini korumak için ne yaptıkları araştırılmamaktadır. Ayrıca bu çalışmaların çoğunluğu sistemlerin işlerliği ve korunmasından sorumlu güvenlik uzmanları tarafından yürütüldüğü için, temel odak noktası teknolojik donanımlar ve yazılımsal koruyucu önlemlerdir. Ancak bu çalışmalarda en önemli bileşen olan insan faktörü kapsam dışı kalmaktadır. Bu nedenle, bilgi güvenliği programının bir bölümü olarak, teknoloji ve süreç ile birlikte insan boyutunun da düşünülmesi gerekmektedir. Çünkü bilgi güvenliği ihlallerinin temelinde mevcut ve herhangi bir şekilde çalışma yaşantıları sona eren geçmişteki çalışanlar bulunmaktadır. Kurum çalışanlarının bilgi güvenliği politikalarını ve düzenlemelerini benimsemeleri ve uygun davranışlar sergilemeleri için bilgi güvenliği kültürünün oluşturulması gerekmektedir. Bilgi güvenliği kültürünün oluşturulması da ancak sürekli izleme, değerlendirme ve etkileme (ikna etme) ile oluşturulabilecektir. Veiga ve Martins'in bilgi güvenliği kültürü üzerine yaptıkları çalışmasında, uluslararası bir finans kurumunda on iki ayrı ülke de sekiz yıllık bir süreçte yaptıkları uygulama sonunda bilgi güvenliği kültürünün oluşumunda, farkındalık ve eğitim bileşenlerinin en önemli iki etken olduğu sonucuna varmışlardır [184]. Bilgi güvenliğinin sadece teknik boyuta dayalı çözümlerle sağlanamayacağını, başarılı bilgi güvenliğinin bilgi istemlerinin kullanımı esnasında uygun kullanıcı davranışlarına bağlı olduğunu Montesdioca ve Maçada da çalışmalarında

belirtmişlerdir. Çalışmanın sonuçları, kullanıcıların bilgi güvenliği uygulamalarının faydalarını algıladıklarını ancak güvenlik kontrollerinin verimliliği azalttığını düşünmeleri nedeniyle istenilen davranışlarda bulunmadıklarını göstermiştir [185].

Bilgi güvenliğine karşı en büyük tehdit, bilgisayar korsanı, kötücül yazılımlar ve donanımlardan daha çok dikkatsiz veya kötü amaçlı kullanıcılar ya da kuruma giriş veya erişim yetkisi olan personelin olduğu ortaya çıkmaktadır. Personel seçimi, eğitim, bilgiyi saklama politikaları ile bilinçli ve uyumlu kişiliğe sahip insanların güvenliğe önemli katkısının olduğu sonucuna ulaşılmıştır [186].

Bilgi güvenliğinin sağlanmasına katkı sağlayan diğer bir bileşen ise bilgi güvenliği alanında kazanımların, tecrübelerin güvenli bir ağ üzerinde paylaşımının yapılarak benzer saldırılardan diğer kurum ve kuruluşların korunmasını sağlamaktır. Tamjidyamcholo ve diğerlerinin bilgi paylaşımının bilgi güvenliğine etkisini konu aldıkları çalışmalarında, güvenlik bilgisi paylaşımının risklerini ve bilgi güvenliği maliyetlerini azalttığı belirtilmiştir. 2008 McAfee tarafından verilen raporda, güvenlik ihlalleri nedeniyle, sadece 1 yılda yaklaşık 1 trilyon dolar maddi kaybın ortaya çıktığı bildirilmiştir. Bu ihlallerin büyük çoğunluğu, içeriden birisi tarafından özellikle de eski çalışanlar tarafından gerçekleştirilmiştir [187]. Sanal topluluklarının özellikle bilgi güvenliğinin sağlanmasına yönelik çalışanların bilgi paylaşımında, tutum, güven ve karşılıklılığın önemli bir şekilde bilgi değişiminde etkili olduğu görülmüştür [188]. Flores, Antonsen ve Ekstedt ise bilgi paylaşımına idari ve ulusal kültür farkının etkisini incelemiştir. Sonuçlar incelendiğinde, öncelikle idari yönetimin risk alma isteği, varlıkları nasıl değerlendirdiği ve faaliyetler üzerindeki kontrol yöntemlerinin bilgi paylaşımını önemli derecede etkilediği sonucuna varılmıştır [189].

Bilgi güvenliği farkındalığı kapsamında yapılan anket çalışmalarında genellikle bilgi güvenliği farkındalığının sadece bir bileşenine (şifre, uygulamalar, politikalar) odaklanılmaktadır. Ancak çok az bir kısmı çalışanların bilgi güvenliği farkındalığının tüm boyutlarını ele almaktadır. Parsons ve diğerleri çalışmalarında insan temelli bilgi güvenliği açıklıklarını ölçmek amacıyla geliştirdikleri Bilgi Güvenliğinin İnsan Boyutu Anketini (Human Aspects of Information Security Questionnaire- HAIS-Q) 500 Avustralya çalışanına uygulamışlardır. Ankette, çalışanların kurumlarının bilgi güvenliği politika ve prosedürleri hakkında yeterli bilgiye sahip olmaları ile bilgi güvenliği konusundaki tutum

ve davranışları arasındaki ilişki incelenmiştir. Çalışmada, internet, elektronik posta, sosyal medya kullanımı, parola yönetimi, olay raporlama, bilgi işleme ve mobil kullanıcı olmak üzere yedi alana odaklanılmıştır [190].

Günümüzde yaşanan siber saldırılar değerlendirildiğinde, saldırganların başarılarındaki ortak noktalardan birisi, kurban olarak nitelendirilen saldırı mağdurlarının yeterli bilinç seviyesine, farkındalığa sahip olmamasıdır. Bu saldırılardan, özellikle sosyal mühendislik saldırılarında farkındalığın önemi çok büyüktür. Bilgisayar ve ağ güvenliği açısından sosyal mühendislik, insan davranışındaki unsurları güvenlik açıkları olarak değerlendirip, bu açıklardan faydalanma yöntemiyle güvenlik süreçlerini aşarak sistem yöneticisi ya da kullanıcıların yetkilerine erişim tekniklerini kapsayan bir terimdir. Tanınmış bir sosyal mühendis olan Kevin Mitnick'e göre güvenlik uzmanları sürekli olarak daha iyi güvenlik teknolojileri geliştirip teknik olarak güvenlik açıklarını istismar etmeyi zorlaştırınca, saldırganlar insan unsurunu istismar etme yoluna daha çok gideceklerdir [191]. Sosyal mühendisliği kullanarak saldırganlar, insani özelliklerdeki ve davranışlarındaki açıklıklardan yararlanarak kurum ve kuruluşlara ait hassas bilgileri elde etmeyi hedeflemektedirler. Sosyal mühendisliğe karşı bilinen tek savunma yöntemi ise etkili bilgi güvenliği farkındalığıdır [192]. Arachchilage ve Love'da yaptıkları çalışmada kullanıcı farkındalığının sosyal mühendislik saldırılarına etkisini incelemişlerdir. Çalışmada, gizli bilgilerin (kullanıcı adı, parola, çevrimiçi bankacılık bilgileri, vb.) elde edilmesi amacıyla gerçekleştirilen oltalama (phishing) saldırısında bilgisayar kullanıcılarının farkındalığının önemine yönelik olarak ortalama bilgisayar eğitimine sahip 161 kullanıcı üzerinde gerçekleştirdikleri anket araştırması sonucunda, kullanıcıların farkındalığı ve bilgi sahibi olmasının saldırının engellenmesine önemli katkısının olduğu görülmüştür [193]. Bilgi güvenliğindeki önemli tehditlerden birisi olan ve tüm teknolojik önlemleri etkisiz hale getiren sosyal mühendislik saldırıları Kruger, Drevin ve Steyn tarafından da incelenmiştir. Çalışanların şüpheli görünen bir elektronik posta almaları durumundaki tutumlarını incelemek amacıyla yaptıkları anket çalışmasında kullanıcıların %37'si postayı açmayacaklarını belirtirken, %13'ü ekte gönderilen dosyayı açabileceklerini belirtmiştir. İlave olarak kullanıcıların %42'si yasal görünen elektronik postanın içerdiği web bağlantısını takip edebileceğini belirtirken, kullanıcıların %30'u bilgisayar performansını artıracağını düşündüğü uygulama dosyasını çalıştırabileceğini belirtmiştir [194]. Sosyal mühendisliğe karşı bilinen tek savunma yöntemi ise etkili bilgi güvenliği farkındalığıdır [195].

Güvenlik olayı, bilgi güvenliği politikalarının, standart güvenlik uygulamalarının ihlali olarak tanımlanmaktadır. Bu nedenle, hizmetlerin engellenmesi, yetkisiz hassas bilgilerin paylaşılması, bilişim sistemlerine veya ağına yapılan saldırılar, istem dışı önemli dokümanların silinmesinin tamamı güvenlik olayı olarak değerlendirilmektedir. Olaylara Müdahale Takımları güvenlik sürecindeki hata veya ihlallere müdahale eden birimlerdir. Olaylara Müdahale Takımları tarafından elde edilen verilerin tüm paydaşlarla paylaşılarak, güvenlik risklerinin kullanıcılar tarafından bilinmesinin ve farkındalığın artırılmasının etkili bilgi güvenliğinin sağlanmasında oldukça önemli bir katkı sağlayacağı sonucuna varılmıştır [196].

Bilgi ve iletişim teknolojilerindeki büyük değişimler ve gelişmeler, kişisel bilgilerin depolanması, işlenmesi ve özellikle de paylaşımını beklenmedik seviyelere getirmiştir [197]. Sosyal teknolojilerin yaygınlaşması, insanlar arasındaki haberleşme, işbirliği, bilgi paylaşımı, çevrim içi ticaret alanında önemli katkılar sağlamıştır [198]. Gizlilik bildirimlerinin önemi Facebook gibi az sayıda site tarafından anlaşılarak, kullanıcılarına kendi gizlilik politikalarını özelleştirme seçeneği sunmaktadır. Ancak bunun yanında Livingstone ve Brake tarafından gerçekleştirilen çalışma sonucu, Facebook kullanıcılarının gizlilik politikasının önemini yeterince algılamadıkları için bu seçeneğin yeterince faydalı olmadığını göstermektedir [199]. Vladlena, Saridakis, Tennakoon ve Ezingeard'ın yaptığı çalışmada da, sosyal medya kullanıcılarının bilgi güvenliği farkındalığına yönelik inceleme yapmışlardır. Araştırma sonuçları, satın alma istekleri ile güvenlik uyarıları ve sosyal ağın güvenlik özellikleri arasında güçlü pozitif bir bağlantı olduğunu göstermiştir. Kullanıcıların TRUSTe, BBBOnline ve Verisign gibi güvenlik etiketleri ile gizlilik/güvenlik bildirileri bulunan web sayfalarının satın alma isteğini olumlu yönde etkilediği sonucuna varmışlardır [200].

Saridakis ve diğerleri bireysel bilgi güvenliği üzerine yaptıkları çalışmalarında sosyal ağ kullanımı ile siber saldırıların kurbanı olma arasındaki ilişki, sosyal medyanın kullanım yoğunluğu, sosyal medya tarafından bilginin kontrolüne yönelik alınan önlemler, siber saldırı riskinin düşük olarak algılanması, yüksek risk alma eğilimi ve bilgi teknolojileriyle ilgili bilgi seviyesi yönünden incelemişlerdir. Çalışma sonucu, sosyal medyayı yoğun olarak kullananların, kişisel bilgilerini paylaşanların ve bilgi paylaşımının riskli olmadığını düşünenlerin, siber saldırıların mağduru olma olasılığının yüksek olduğunu göstermiştir [201].

Bilgi güvenliğinde insan bileşeni, kurum ve kuruluşların siber saldırılara karşı sistemlerin korunmasında da oldukça önemlidir. Söz konusu saldırılara karşı geliştirilen tespit ve

engelleme sistemleri mevcut olsa da, yapılan çalışmalar söz konusu sistemlerin başarısının büyük oranda kullanıcılara bağlı olduğunu göstermektedir. Bu kapsamda, Ben-Asher ve Gonzalez çalışmalarında bilgi güvenliğinin sağlanmasında yaygın olarak kullanılan saldırı tespit sistemlerinin etkili kullanımı için çalışanların bilgi seviyesi ve farkındalığını incelemişlerdir [202].

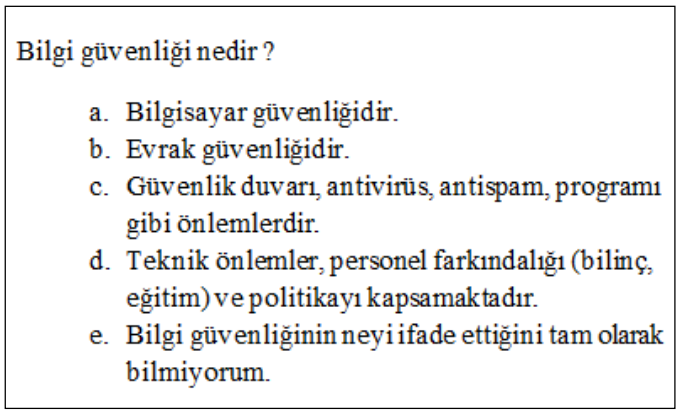
Şirketlerin birleşmesinden sonra yeni kurumda oluşan bilgi güvenliği kültürü bozulmalarına yönelik araştırma yapan Dillon ve diğerleri, çalışmalarında bu kapsamda iki Avrupa şirketi olan AirTelco ve Relicom isimli telekom firmalarının birleşmesini incelemişlerdir. Çalışmada gerçekleştirilen analiz sonucunda kurumların birleşme gibi dönüşüm süreçleri kapsamında dikkat edilmesi gereken bilgi güvenliği ilkeleri tanımlanmıştır [179].

Farooq ve diğerleri, farklı ulus, kültür ve disiplin alanlarında okuyan üniversite öğrencilerinin üzerinde yaptıkları çalışmada, yaş, cinsiyet, eğitim seviyesi, milliyet ve yaşam alanı etkenlerinin bilgi güvenliği farkındalığı ile ilişkisini incelemişlerdir. Yapılan anket çalışması sonucunda, cinsiyet ve eğitim seviyesi ile bilgi güvenliği farkındalığı arasında önemli istatistiksel korelasyon bulunurken, yaş, milliyet ve yaşam alanı arasında bir ilişki bulunmadığı saptanmıştır [203].

4.2. Bilgi Güvenliği Farkındalığı Anketi

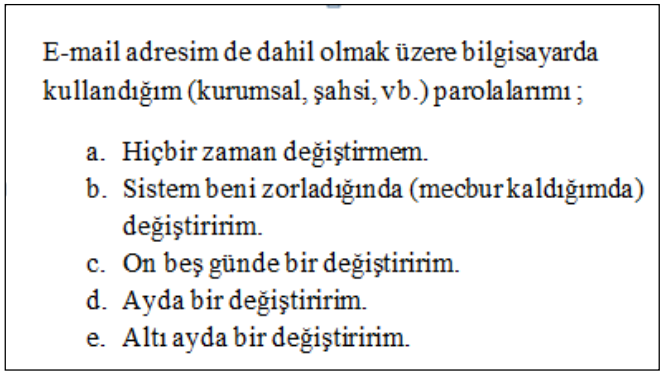
Bu kısımda, çalışma kapsamında geliştirilen ve hedef kitle olarak eğitim seviyesi lisans ve lisansüstü olan endüstriyel kontrol sistemi kurumu çalışanlarına uygulanan anket tanıtılmış müteakiben anket sonuçlarının analiz ve çıkarımlarına yer verilmiştir.

Bilgi güvenliği anketi üç bölümden oluşmaktadır. İlk bölüm, bilgi güvenliğinde önemli olarak düşünülen kavramların tanım bilgisinden oluşmaktadır. Şekil 4.1'de ilk bölümün son maddesinde yer alan "Bilgi güvenliği nedir?" sorusu ve cevapları örnek olarak gösterilmektedir. Bilgi güvenliği hakkında yeterli bilgi seviyesine sahip bireylerin, sadece bilgisayar, doküman ya da güvenlik duvarı, antivirüs, antispam gibi teknik çözümlerin yerine, bilgi güvenliğini bütüncül bir yaklaşım olarak tanımlayan seçenek olan "Teknik önlemler, personel farkındalığı (bilinç, eğitim) ve politikayı kapsamaktadır." seçeneğini işaretlemeleri beklenmiştir.



Şekil 4.1. Tanım bilgisi soru örneği

Anketin ikinci bölümünde verilen bir durum karşısında kullanıcıların tutumlarının ölçülmesinin hedeflendiği çoktan seçmeli sorular bulunmaktadır. Şekil 4.2'de görülen "E-mail adresim de dâhil olmak üzere bilgisayarda kullandığım (kurumsal, şahsi, vb.) parolalarımı" cümle tamamlama sorusuyla kullanıcıların parola yönetim davranışları saptanmaya çalışılmıştır. Mansfield'e göre davranış soruları, bir durum karşısında bireylerin tutum ve davranışlarını hızlı ve kesin bir yolla ortaya çıkarmak için kullanılan en etkili yöntem olarak tanımlanmıştır [204]. Bu bölümde kullanıcılara birden fazla seçeneği seçme özelliği sağlanarak güncel hayattaki tutum ve davranışlarını yansıtmaları amaçlanmıştır.



Şekil 4.2. Çoktan seçmeli soru örneği

Üçüncü bölümde ise kullanıcıların kendilerine belirtilen bilgi güvenliği ile ilgili (25) maddeye 5'li likert ölçeğine göre hazırlanmış 1-5 arası (Kesinlikle Katılmıyorum, Katılıyorum, Kararsızım, Katılıyorum, Kesinlikle Katılmıyorum) değerlerden birisini işaretlemeleri istenmiştir. Bu sayede gerçekleştirilecek analiz çalışmasında katılımcıların verdiği cevaplar sayısal olarak değerlendirilmesi hedeflenmiştir.

Anketin yeni geliştirilmesi nedeni ile 35 kişilik veri üzerinden temel bileşenler analizi yapılmıştır. Analiz sonucunda üçüncü bölümde yer alan 25 maddeden 2 madde güvenilirlik değeri düşük olduğu için çıkartılmış ve Cronbach Alfa değeri (güvenilirlik değeri) 0,691 olarak tespit edilmiştir. Cronbach Alfa değeri kabul edilebilir değerde olup anket 207 kişiye uygulanmıştır.

Anket Google Docs kullanılarak çevrimiçi olarak yüklenmiş ve bağlantı katılımcılara gönderilerek anketi tamamlamaları sağlanmıştır. Anketi toplam 207 katılımcı tamamlamış ancak 7 katılımcının eğitim seviyesi lisansaltı (Lise ve Meslek Yüksek Okulu) olması nedeniyle dikkate alınmamıştır. Kalan 200 katılımcının cevabı üzerinden değerlendirme yapılmıştır. Verilerin toplanılması sürecini müteakip veri analizi için IBM SPSS Statistics 20 paket programı kullanılmıştır.

Çalışmada gerçekleştirilen araştırma kapsamında aşağıdaki hipotezler incelenmiştir.

H1: Eğitim seviyesi ile bilgi güvenliği farkındalığı arasında pozitif bir ilişki vardır.

H2: Kurumdaki iş tecrübesi (çalışma süresi) ile bilgi güvenliği farkındalığı arasında pozitif bir ilişki vardır.

H3:Cinsiyet ile bilgi güvenliği farkındalığı arasında pozitif bir ilişki vardır.

4.3. Bilgi Güvenliği Farkındalığı Anketi Analiz ve Çıkarımları

Çizelge 4.1'de tüm örneklem karakteristikleri görülmektedir. Buna göre katılımcıların %28,5'i kadın ve %71,5'i erkektir. Katılımcıların %4'ü doktora, %28'i yüksek lisans ve %68'i lisans mezunudurlar. Katılımcılarım %7'si 1 yıldan az, %40'ı 1-5 yıl arası, %22,5'i 6-10 yıl arası, %18'i 11-15 yıl arası ve %12,5'i 16 yıl ve üzeri mesleklerinde çalışma sürelerine sahiptirler.

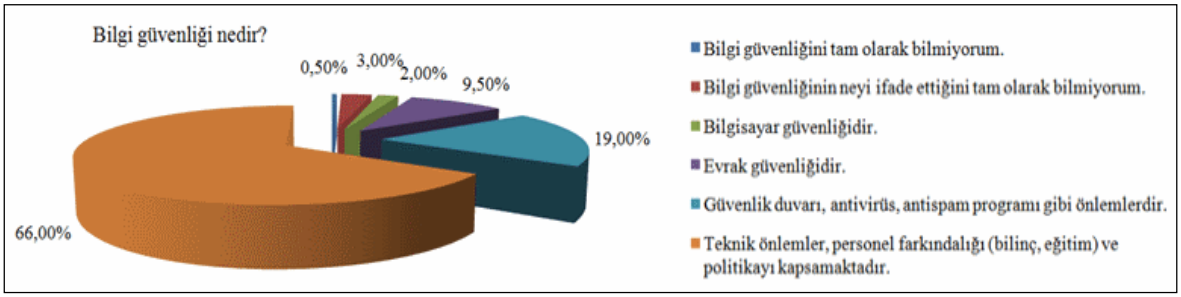
Çizelge 4.1. Örneklem karakteristikleri

Faktörler	Frekans	Yüzde
Cinsiyet		
Erkek	143	71,5
Kadın	57	28,5
Toplam	200	100,0

Çizelge 4.1. (devam) Örneklem karakteristikleri

Faktörler	Frekans	Yüzde
Eğitim Durumu		
Doktora	8	4,0
Lisans	136	68,0
Yüksek Lisans	56	28,0
Toplam	200	100,0
Çalışma Süresi		
1 yıldan az.	14	7,0
1-5 yıl arası	80	40,0
11-15 yıl arası	36	18,0
16 yıl ve üzeri.	25	12,5
6-10 yıl arası	45	22,5
Toplam	200	100,0

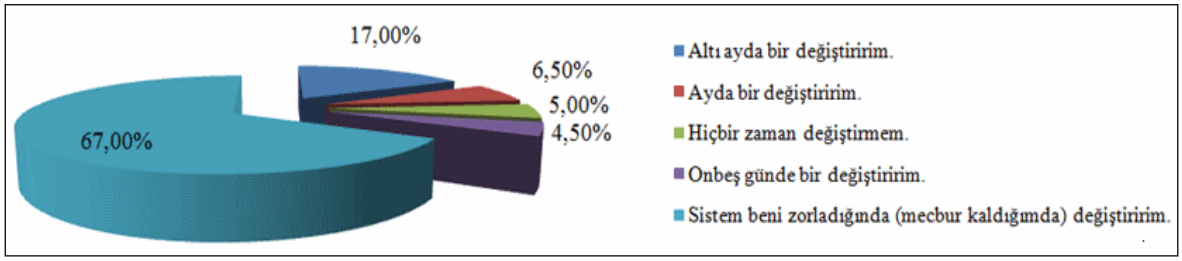
Anketin birinci bölümünde sorulan tanım soruları katılımcıların temel bilgi güvenliği kavramlarının anlaşılma düzeyini belirlemeye yönelik hazırlanmıştır. Birinci bölümün analizi ile ilgili Şekil 4.3'de sunulan soruya göre katılımcıların %66'sı bilgi güvenliğine personel/insan farkındalığını belirten "Teknik önlemler, personel farkındalığı (bilinç, eğitim) ve politikayı kapsamaktadır.” cevabını verirken, %19'u bilgi güvenliğini teknik önlemlerden oluştuğunu belirten "Güvenlik duvarı, antivirüs, antispam programı gibi önlemlerdir." cevabını vermişlerdir. Katılımcıların %4,3'ü ise bilgi güvenliğinin ne anlama geldiğini tam olarak bilmediklerini ifade etmişlerdir.



Şekil 4.3. Bilgi güvenliği nedir?

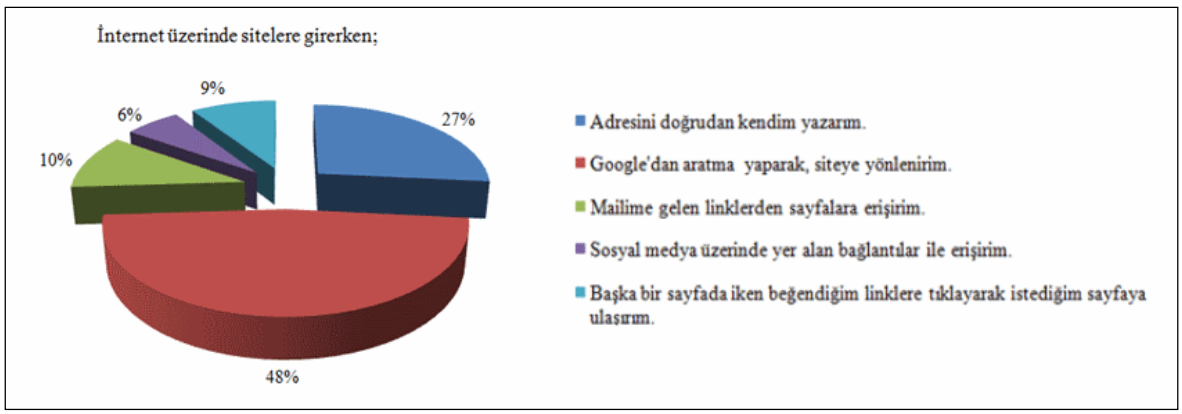
Birinci bölüm genel olarak değerlendirildiğinde katılımcıların büyük bir kısmının kavramlara ilişkin beklenen cevapları verdikleri gözlemlenmiştir.

Anketin ikinci bölümünde yer alan sorular bilgi güvenliği farkındalığının katılımcıların davranışına olan etkilerini belirlemeye yönelik hazırlanmıştır. Bu kapsamda Şekil 4.4'de sunulan soruda katılımcılara kullandıkları hesapların parolalarını değiştirme süresi sorulmuştur. Katılımcıların %67'si "Sistem beni zorladığında (mecbur kaldığımda) değiştiririm." cevabını, %17'si "Altı ayda bir değiştiririm." cevabını, %6,5'i "Ayda bir değiştiririm." cevabını, %4,5'i "On beş günde bir değiştiririm." cevabını, %5'i "Hiçbir zaman değiştirmem." cevabını vermişlerdir.



Şekil 4.4. Katılımcıların parola değiştirme süreleri

İkinci bölümde katılımcıların davranışına olan etkilerini belirlemeye yönelik sorulan sorulardan bir diğeri Şekil 4.5'te sunulmuştur. Sorulan soru kapsamında katılımcıların %48'i sitelere Google arama motorundan arama yaparak, %27'si ise gireceği sitenin adresini doğrudan yazarak girmektedir.



Şekil 4.5. Katılımcıların sitelere giriş yöntemleri

İkinci bölümde yer alan davranış tipi sorulara verilen cevaplar değerlendirildiğinde katılımcıların eğitim seviyelerine rağmen(lisans ve lisansüstü) önemli güvenlik ihlallerine yol açabilecek davranışları(parola değiştirme, internet adresini doğrudan yazmama, vs.) sergiledikleri gözlemlenmiştir.

Anketin üçüncü bölümünden elde edilen ölçek verileri analiz edilerek her bir katılımcı için bilgi güvenliği farkındalığı ortalaması hesaplanmıştır. Bilgi güvenliği farkındalığı ortalaması katılımcıların bilgi güvenliği farkındalığını temsil etmektedir.

Bilgi güvenliği farkındalığının cinsiyete göre anlamlı olarak farklılaşıp farklılaşmadığı test etmek maksadı ile bağımsız örneklem t testi yapılmıştır. Çizelge 4.2'de test sonucu incelendiğinde bilgi güvenliği farkındalığının cinsiyete göre anlamlı olarak farklılaştığı ($t=2,79$, $p<0,05$), erkeklerin bilgi güvenliği farkındalığının (3,56) kadınlardan (3,39) daha yüksek olduğu tespit edilmiştir.

Çizelge 4.2. Bilgi güvenliği farkındalığının cinsiyete göre farklılığı T testi

		Cinsiyet		N	Ortalama	
Bilgi Güvenliği Farkındalığı		Erkek		143	3,5616	
		Kadın		57	3,3928	
		t-test for Equality of Means				
		T	Df	Sig. (2-tailed)	95% Farkın güven aralığı	
					Alt	Üst
Ortalama	Kabul edilen eşit varyanslar	2,794	198	,006	,04962	,28786
	Kabul edilmeyen eşit varyanslar	2,646	92,534	,010	,04207	,29541

Bilgi güvenliği farkındalığının eğitim durumuna göre anlamlı olarak farklılaşıp farklılaşmadığı test etmek maksadı ile tek yönlü ANOVA testi yapılmıştır. Çizelge 4.3'de test sonucu incelendiğinde bilgi güvenliği farkındalığının eğitim durumuna göre anlamlı olarak farklılaşmadığı tespit edilmiştir. Bu sonucun en büyük nedeni ise çalışmada yer alan katılımcıların %68'i lisans, %28'i yüksek lisans ve %4'ü doktora mezunu olup, lisansaltı mezunu katılımcılar dikkate alınmamıştır. Bu hipotez, anketin 1'inci ve 2'nci bölümde yer alan maddelerde ayrıca ölçülmüştür.

Çizelge 4.3. Bilgi güvenliği farkındalığının eğitim durumuna göre farklılığı Anova testi

	Kareler Toplamı	df	Kareler Ortalaması	F	Sig.
Gruplar arası	,110	2	,055	,357	,701
Gruplar içi	30,492	197	,155		
Toplam	30,603	199			

(I) Eğitim Durumu	(J) Eğitim Durumu	Ortalama Fark (I-J)	Std. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
Lisans	Yüksek Lisans	,02046	,06247	,943	-,1271	,1680
	Doktora	-,10454	,14313	,746	-,4425	,2335
Yüksek Lisans	Lisans	-,02046	,06247	,943	-,1680	,1271
	Doktora	-,12500	,14870	,678	-,4762	,2262
Doktora	Lisans	,10454	,14313	,746	-,2335	,4425
	Yüksek Lisans	,12500	,14870	,678	-,2262	,4762

Bilgi güvenliği farkındalığının mesleki tecrübeye göre anlamlı olarak farklılaşıp farklılaşmadığı test etmek maksadı ile tek yönlü ANOVA testi yapılmıştır. Çizelge 4.4'te belirtilen test sonucu incelendiğinde, bilgi güvenliği farkındalığının mesleki tecrübeye göre anlamlı olarak farklılaşmadığı tespit edilmiştir.

Çizelge 4.4. Bilgi güvenliği farkındalığının mesleki tecrübeye göre farklılığı Anova testi

	Kareler Toplamı	Df	Kareler Ortalaması	F	Sig.
Gruplararası	,738	4	,185	1,205	,310
Gruplar içi	29,865	195	,153		
Toplam	30,603	199			

(I) Çalışma Süresi	(J) Çalışma Süresi	Ortalama Fark (I-J)	Std. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
1 yıldan az.	1-5	,04115	,11337	,996	-,2710	,3533
	6-10	-,00801	,11976	1,000	-,3378	,3218
	11-15	-,03313	,12326	,999	-,3725	,3063
	16 yıl ve üzeri.	-,15255	,13063	,770	-,5122	,2072

Çizelge 4.4. (devam) Bilgi güvenliği farkındalığının mesleki tecrübeye göre farklılığı Anova testi

(I) Çalışma Süresi	(J) Çalışma Süresi	Ortalama Fark (I-J)	Std. Hata	Sig.	95% Güven Aralığı	
					Alt Sınır	Üst Sınır
1-5	1 yıldan az.	-,04115	,11337	,996	-,3533	,2710
	6-10	-,04915	,07292	,962	-,2499	,1516
	11-15	-,07428	,07854	,879	-,2905	,1420
	16 yıl ve üzeri.	-,19370	,08967	,199	-,4406	,0532
6-10	1 yıldan az.	,00801	,11976	1,000	-,3218	,3378
	1-5	,04915	,07292	,962	-,1516	,2499
	11-15	-,02512	,08751	,999	-,2661	,2158
	16 yıl ve üzeri.	-,14454	,09762	,576	-,4133	,1242
11-15	1 yıldan az.	,03313	,12326	,999	-,3063	,3725
	1-5	,07428	,07854	,879	-,1420	,2905
	6-10	,02512	,08751	,999	-,2158	,2661
	16 yıl ve üzeri.	-,11942	,10188	,767	-,4000	,1611
16 yıl ve üzeri.	1 yıldan az.	,15255	,13063	,770	-,2072	,5122
	1-5	,19370	,08967	,199	-,0532	,4406
	6-10	,14454	,09762	,576	-,1242	,4133
	11-15	,11942	,10188	,767	-,1611	,4000

Üçüncü bölümde yer alan katılımcıların kurumlarının verdiği eğitimler ile bilgi güvenliği farkındalığı arasında ilişki olup olamadığını belirlemek amacı ile korelasyon testi uygulanmıştır. Çizelge 4.5'de sunulan korelasyon testi incelendiğinde katılımcıların bilgi güvenliği farkındalığı ile kurumlarının verdiği bilgi güvenliği farkındalığı eğitimi arasında anlamlı bir farklılık olduğu tespit edilmiştir.

Çizelge 4.5. Kurumun verdiği eğitim ile bilgi güvenliği farkındalığı arasındaki korelasyon

		Bilgi Güvenliği Farkındalığı	Kurumum yeterli bilgi güvenliği eğitimi vermektedir.
Bilgi Güvenliği Farkındalığı	Pearson korelasyonu	1	,141*
Kurumum yeterli bilgi güvenliği eğitimi vermektedir.	Pearson korelasyonu	,141*	1
*. Correlation is significant at the 0.05 level (2-tailed).			

Üçüncü bölümde yer alan "Cep telefonumda lisanslı güvenlik yazılımı kullanıyorum." maddesiyle "Cep telefonu üzerinden mobil bankacılık ve çevrimiçi alışverişi güvenli olarak yapabiliyorum." maddesi arasında pozitif bir ilişki olması beklenmiştir. Çünkü cep telefonu üzerinde yapılan çevrimiçi alışverişin güvenliği cihazdaki teknik önlemler (antivirüs yazılımı) ile ilişkilidir. Ancak Çizelge 4.6.'da yer alan korelasyon testi incelendiğinde bu maddelerin negatif yönlü ilişkili olduğu görülmektedir. Anketten elde edilen sonuçlara göre katılımcıların çoğunluğu çevrimiçi alışveriş, mobil bankacılık gibi işlemlerini genellikle cep telefonu üzerinden gerçekleştirdiği cevabını verirken, aynı zamanda katılımcıların güncel güvenlik yazılımlarını kullanmadıkları görülmüştür.

Çizelge 4.6. Katılımcıların mobil güvenlik durum farkındalığı analizi

		Cep telefonumda lisanslı güvenlik yazılımı kullanıyorum.	Cep telefonu üzerinden mobil bankacılık ve online alışverişi güvenli olarak yapabiliyorum.
Cep telefonumda lisanslı güvenlik yazılımı kullanıyorum.	Pearson korelasyonu	1	-,147*
Cep telefonu üzerinden mobil bankacılık ve online alışverişi güvenli olarak yapabiliyorum.	Pearson korelasyonu	-,147*	1
*. Correlation is significant at the 0.05 level (2-tailed).			

4.4. Bilgi Güvenliği Farkındalığı Anketi Uygulama Kısıtları

İnternet ortamı kullanılarak verilerin toplanması: Özellikle kelime tipi soruları tarama yaptırarak cevap verebilir. Zaman sınırlamasının olmadığı dikkate alındığında cevaplamaları yaparken başka konularla da ilgilendiği için dikkat dağınıklığı olabilir ve cevaplar gerçeği yansıtmayabilir.

4.5. Bölüm Sonuçları

Bu bölümde, bilgi güvenliği üçlüsünün en önemli ama en az önem verilen boyutu olan insan faktörüne odaklanılmıştır. Çalışmada, lisans ve üstü eğitim seviyesine sahip bireylerin Bilgi Güvenliği Farkındalığı değerlendirilmiştir. Bu kapsamda kullanıcıların bilgi güvenliği

farkındalığına yönelik olarak hazırlanan ve 3 bölüm ve (37) maddeden oluşan bilgi güvenliği farkındalığı anketi 207 kişiye uygulanmış ve 200 geçerli cevap değerlendirmeye alınmıştır.

Çalışmada eğitim seviyesi, iş tecrübesi ve cinsiyet faktörlerinin bilgi güvenliği farkındalığına etkisi incelenmiştir. Analiz sonuçlarında cinsiyet ile bilgi güvenliği farkındalığı arasında pozitif yönde bir ilişki tespit edilmiştir. Pozitif yönde ilişki çıkmasının nedeninin katılımcı sayısına ve ankete katılan bireylere dayalı olarak değişebileceği değerlendirilmektedir.

Eğitim seviyesi ile bilgi güvenliği farkındalığı arasında ise anlamlı bir ilişki tespit edilememiştir. Ayrıca kullanıcıların yüksek eğitim seviyesine sahip olmaları durumunda kavramsal olarak yeterli bilgi seviyesine sahip olmasına rağmen bu bilgileri bilişim sistemlerini kullanırken davranışlarına yansıtmadıkları görülmüştür.

Diğer bir analizde, iş tecrübesi ile bilgi güvenliği arasında anlamlı bir ilişi bulunamamıştır. Bunun en önemli nedeni olarak gerekli eğitim ve bilinçlendirme çalışmalarının yetersiz ve sürekli olmamasından kaynaklandığı görülmektedir. Kurumların bilgi güvenliği politikasına sahip olmaları ve bu alanda kullanıcılarına eğitim vermeleri durumunda kurumsal bilgi güvenliği kültürünün oluşturulmasında ve kullanıcıların bilgi güvenliği konusunda beklenen tutum ve davranışları göstermesinde oldukça etkili olabilecektir. Ancak söz konusu eğitimler konferanslar gibi etkili olmayan yöntemlerle verildiği takdirde beklenen sonuç alınamayabilecektir.

Çağımızın bilgi çağı ve en değerli varlığın bilgi olduğu düşünüldüğünde bilgiye sahip olma ve bilgiyi korunmanın önemi ortaya çıkmaktadır. Günümüzde kurum ve kuruluşlar bilgi güvenliğini, sahip oldukları donanımlarla (güvenlik duvarları, IDS/IPS sistemleri, antivirüs yazılımları, vb.) eşdeğer görmektedirler. Ancak her ne kadar en güncel, en son teknoloji ürünü sistem ve cihazlara sahip olunursa olunsun, bu fiziksel değişimden öteye geçemez. Tam anlamıyla güvenlik ise, fiziksel dönüşümle birlikte kültürel değişiminde sağlanmasıyla mümkün olabilir. Bunun içinde en hassas ve en zayıf boyut olan insan faktörüne gerekli önem verilerek, ihtiyaç duyulan farkındalığın kazandırılması ve yaşayan bir süreç olan etkili eğitim ve bilinçlendirme çalışmaları yapılmalıdır. Bu sayede alınan teknik önlemler ve güvenlik politikalarının etkinlik kazanarak hedeflenen bilgi güvenliği seviyesine ulaşılabilecektir.

4.6. Bilgi Güvenliği Farkındalığı Anketi

Bu anket, aktif bilgi teknolojileri kullanıcılarının bilgi güvenliği farkındalığının ölçülmesine yönelik olarak hazırlanmıştır. Ankette isim ve soy isim istenmemiştir.

Soru 1.Meslekteki çalışma süreniz?

- 1 yıldan az.
- 1-5
- 6-10
- 11-15
- 16 yıl ve üzeri.

Soru 2.Cinsiyetiniz**?**

- Kadın
- Erkek

Soru 3.Eğitim Durumunuz**?**

- Lisans
- Yüksek Lisans
- Doktora
- Diğer

4.6.1. Bölüm 1

Soru 1.Oltalama (phishing) nedir?

- Yasal e-posta gibi görünen ve kişisel bilgilerinizi talep eden bir e-posta mesajıdır.
- İkna yöntemiyle gizli bilgilerin elde edilmesini amaçlayan bir sosyal mühendislik metodudur.
- Kimlik hırsızlığıdır.
- Yukarıdakilerin hepsidir.
- Oltalama (Pishing) nedir bilmiyorum.

Soru 2.İstenmeyen posta (spam) nedir?

- E-posta yada elektronik mesajın bir diğer adıdır.
- Bir pazarlama tekniğidir.
- Talep edilmeyen ya da istenmeyen e-posta mesajıdır.
- Yukarıdakilerin hepsidir.
- İstenmeyen e-posta nedir bilmiyorum.

Soru 3.İlgi güvenliği nedir?

- Bilgisayar güvenliğidir.
- Evrak güvenliğidir.
- Güvenlik duvarı, antivirüs, antispam programı gibi önlemlerdir.
- Teknik önlemler, personel farkındalığı (bilinç, eğitim) ve politikayı kapsamaktadır.
- Bilgi güvenliğinin neyi ifade ettiğini tam olarak bilmiyorum.

4.6.2. Bölüm-2

Soru 1.Bankanızdan gönderilen bir e-posta mesajında sizden bir bağlantıyı (link) tıklayarak kişisel bilgilerinizi güncellemeniz istendiğinde ne yaparsınız? (Birden fazla seçeneği seçebilirsiniz)

- E-posta mesajındaki bankanın logosu adresi ve diğer bütün bilgiler doğru ise istenen bilgileri veririm.
- Bu e-posta mesajını görmezlikten gelirim.
- İş arkadaşlarımda aynı e-posta mesajını almış ve bilgilerini güncellemişse bende aynısını yaparım.
- Bankayı arayıp gönderilen e-posta konusunda bilgi alırım.
- Kurumun bilgi işlem merkezini arayıp bilgi veririm.

Soru 2.Bilgi güvenliği ihlali ile karşılaştığınızda nereye bildirirsiniz? (Birden fazla seçeneği seçebilirsiniz**)**

- Bilgi Sistem Birimine.
- Kolluk Birimleriyle.
- Üst Yöneticime.

- İnternet Sağlayıcısı veya Yazılım Firmasına.
- Nereye bildireceğimi bilmiyorum.

Soru 3. Sadece acil durumlarda olması koşuluyla kullanıcı adınızı ve şifrenizi kiminle paylaşırsınız?(Birden fazla seçeneği seçebilirsiniz)

- Üst Yöneticimle.
- Bilgi Sistem Görevlileriyle.
- Aynı Birimdeki İş Arkadaşlarımla.
- Kararsızım.
- Kolluk Birimleriyle(Savcı, Polis, Jandarma vb.).
- Hiç Kimseyle.

Soru 4. Sosyal paylaşım sitelerinde (Facebook, Instagram, Twittter, vb.) hangi bilgilerinizi paylaşırsınız(birden fazla seçeneği seçebilirsiniz)?

- Ad ve Soyadımı.
- Doğum Tarihimi.
- Akrabalarımı (Dede, Amca, Dayı, Hala, Teyze, vb.).
- Mesleğimi.
- Medeni Halimi (Varsa Eşim ve Çocuklarımın İsimleri).
- Eğitim Durumu.
- Hobilerim ve Fobilerimi.
- Yukarıdakilerden Hiçbirisini.

Soru 5. E-mail adresim de dahil olmak üzere bilgisayarda kullandığım (kurumsal, şahsi, vb.) parolalarımı;

- Hiçbir zaman değiştirmem.
- Sistem beni zorladığında (mecbur kaldığımda) değiştiririm.
- On beş günde bir değiştiririm.
- Ayda bir değiştiririm.
- Altı ayda bir değiştiririm.

Soru 6.İnternet üzerinde sitelere girerken;(birden fazla seçeneği seçebilirsiniz)

- Adresini doğrudan kendim yazarım.
- Google'dan aratma yaparak, siteye yönlenirim.
- Başka bir sayfada iken beğendiğim linklere tıklayarak istediğim sayfaya ulaşırım.
- Mailime gelen linklerden sayfalara erişirim.
- Sosyal medya üzerinde yer alan bağlantılar ile erişirim.

Soru 7.Tarayıcınız (Internet Explorer, Chrome, vb.) ile internette bir sayfaya girdiğinizde bilgisayarınıza virüs bulaştığı ve kaldırmak için OK ikonuna tıklamanız istendiğinde ne yaparsınız? (Biden fazla seçeneği işaretleyebilirsiniz)

- Virüsü temizleyecek programı incelemek için OK ikonuna tıklarım.
- Mesajı "İPTAL" seçeneğinden kapatırım.
- Kutucuğun sağ üst köşesinde bulunan "X" kısmına basarak kapatırım.
- Tarayıcıyı kapatmaya çalışırım.
- Bilgisayarı kapatırım.

Soru 8.Seçeneklerden hangisi uygun parola örneklerindendir?

- Ankara06*
- ankara06*
- Ank06ara*
- Ankara
- Ankara06

Soru 9.Kullanıcı adınızı ve parolanızı unutmamak için ne yaparsınız? (Birden fazla seçeneği seçebilirsiniz)

- Kolay hatırlanabilir parolalar seçerim.
- Kağıda yazıp masaüstü ya da bilgisayarımın yanına veya klavyemin altına yapıştırırım.
- Cep telefonuma kaydederim.
- Tüm parola ve şifrelerimi (iş, mail, bankacılık) aynı yaparım.
- Kısa şifre ve parolalar belirlerim.

- Karakter, büyük/küçük harf ve rakamları hatırlayabileceğim bir kombinasyonla birleştiririm.
- Not defterime yazarım.

4.6.3. Bölüm 3

3ncü Bölüm 5'li likert ölçeğine göre hazırlanmıştır **(***1.'Kesinlikle Katılmıyorum', 2.'Katılmıyorum', 3.'Kısmen Katılıyorum', 4.'Katılıyorum' ve 5. 'Kesinlikle Katılıyorum'***)**

Soru 1. Kişisel bilgilerimin bazılarını internet ortamında paylaşırım.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 2. Kişisel bilgilerimi sosyal medyada(veya internet ortamında) paylaşmanın kendi güvenliğimi etkileyeceğini düşünmüyorum.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 3. İnternet ortamından gelebilecek tehditlerin farkındayım.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 4. Kişisel bilgi güvenliğim hakkında yeterli bilgiye sahibim.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 5. Sosyal medya hesaplarımın parolalarımı yakın çevrem ile paylaşırım.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 6. Parolamı oluştururken doğum yerimi, yılımı, meslek ve medeni bilgilerimi kullanırım.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 7. Sosyal medya ve mail adreslerimi oluştururken kişisel bilgilerimi kullanırım.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 8. Sosyal medya hesaplarımın güvenlik soruları yakın çevre, kişisel bilgilerim, vs.. den oluşur.
1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 9. İnternet ortamında alışveriş yaparım.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 10. Girdiğim sitelerin güvenilir bağlantı olup olmadığına dikkat ederim.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 11. Gelen e-postaların içeriğine ve bağlantılı yönlendirme adreslerine dikkat ederim.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 12. Sosyal medya hesaplarımın başka kişilerin ellerine geçmesi durumunda yapmam gereken işlemleri bilirim.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 13. Kendi bilgi güvenliği açıklarımın kurumuma vereceği zararlar hakkında bilgim var.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 14. Güçlü bir şifre en az 6 karakter uzunluğunda, büyük harf, küçük harf, rakamlar ve alfa-nümerik karakterleri birlikte bulundurmalıdır.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 15. Cep telefonumda lisanslı güvenlik yazılımı kullanıyorum.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 16. İnternet ortamında sörf yaparken (gezinirken) gerektiğinde aile filtresi kullanırım.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 17. Başkalarıyla şifremi paylaşmamam gerektiğini biliyorum, ama ara sıra da olsa iş arkadaşıma işlerin aksamaması için şifremi veriyorum (sadece güvendiğim arkadaşlarıma ve acil durumlarda).

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 18. Sosyal medya hesaplarımda rumuz(takma ad) kullanırım.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 19. Aldığım e-postaların gönderici adreslerine dikkat ederim.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 20. Bilişim suçları ile alakalı yasal mevzuatı bilirim.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 21. Kişisel bilgisayarımda her zaman antivirüs programı yüklü bulunur.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 22. Sosyal medya hesap profillerim herkese açıktır.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 23. Cep telefonu üzerinden mobil bankacılık ve online alışverişi güvenli olarak yapabiliyorum.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

Soru 24. Kafeterya, alışveriş merkezi ve benzeri alanlarda ücretsiz internet hizmetinden faydalanıyorum.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

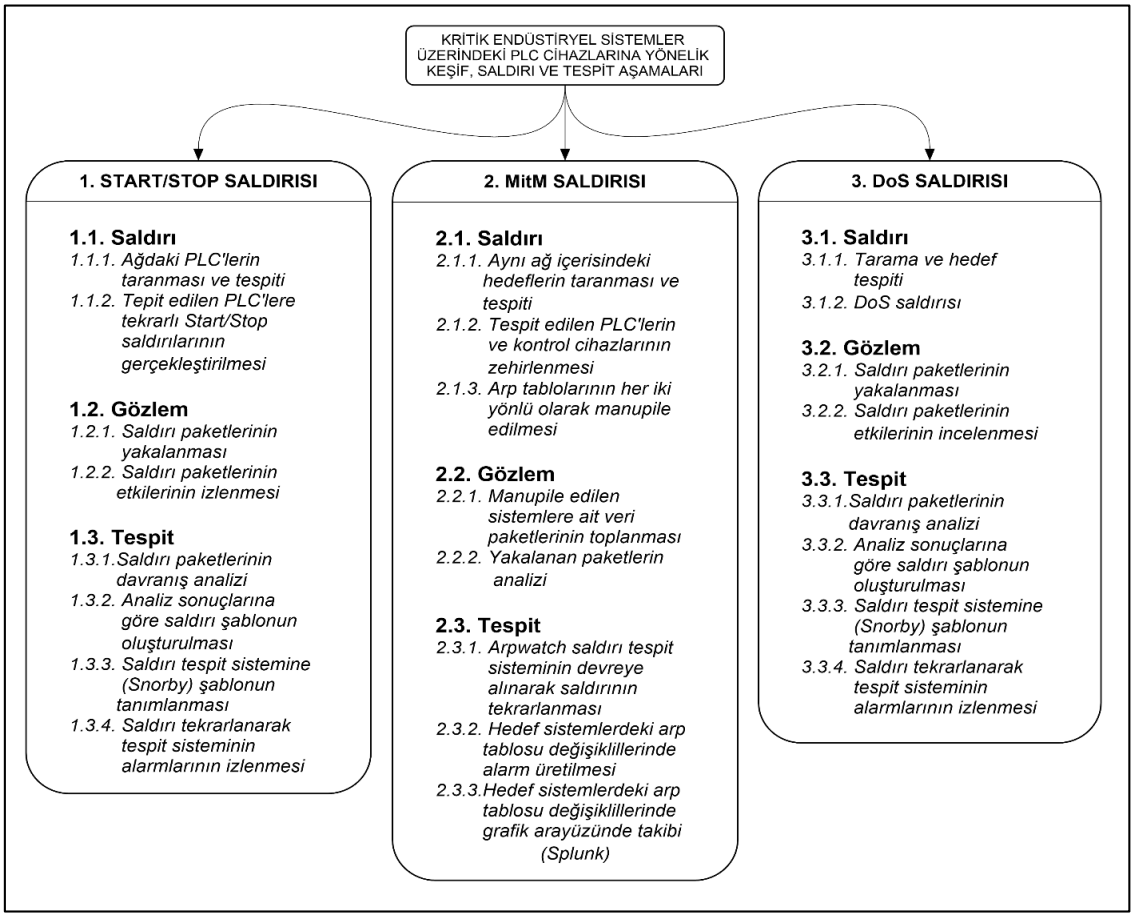
Soru 25. Kurumum yeterli bilgi güvenliği eğitimi vermektedir.

1. Kesinlikle Katılmıyorum. 5. Kesinlikle Katılıyorum.

5. PLC SALDIRI AÇIKLIK ANALİZLERİ VE ÇIKARIMLAR

Endüstriyel Kontrol Sistemlerinin güvenliğine yönelik yapılan çalışmaların çoğunluğunda gerçek bir sisteme yönelik uygulama yapılmamıştır. Bu çalışma da, gerçek bir kontrol sisteminin yer aldığı sınama ortamında testler gerçekleştirilerek, PLC cihazının açıklıklarının tespitine ve çözüm önerilerinin belirlenmesine odaklanılmıştır.

Şekil 5.1'de görüldüğü üzere PLC'ye yönelik gerçekleştirilen analiz çalışmaları üç bölümden oluşmaktadır. İlk aşamada PLC'ye saldırılar gerçekleştirilerek sistem üzerindeki etkileri ölçülmüştür. İkinci aşama, saldırılar sonucunda oluşan paketler yakalanarak analiz edilmesine dayanan gözlem aşamasıdır. Son aşamada ise saldırı tespit sistemleri aracılığıyla saldırılara ilişkin paternler oluşturularak benzer saldırılar gerçekleştirilmesi durumunda saldırıların tespit edilerek sistemin etkilenmemesi hedeflenmiştir.



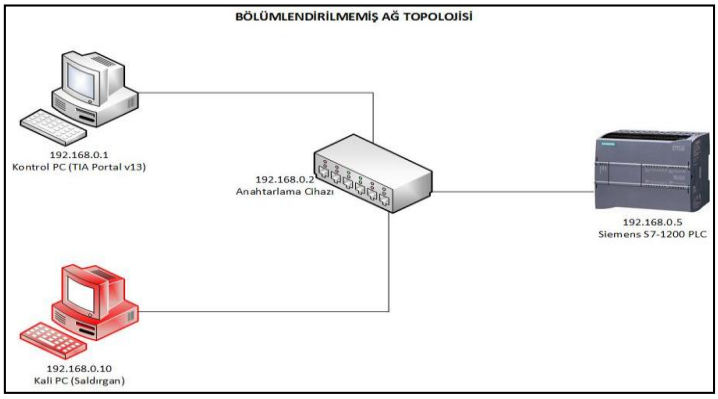
Şekil 5.1. PLC cihazlarına yönelik keşif, saldırı ve tespit aşamaları

5.1. PLC Açıklık Analizi

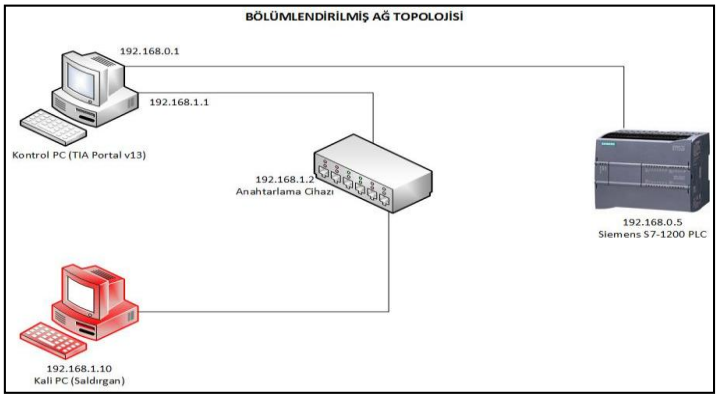
Bu bölümde çalışma kapsamında oluşturulan sınama ortamında gerçekleştirilen açıklık analizi saldırılarının gerçekleştirilmesi, tespiti, paternlerinin oluşturulması ve sonuçları ele alınmıştır. Açıklık analizi testlerinin hedefinde endüstriyel kontrol sistemlerinin önemli bir bileşeni olan PLC cihazlarından yaygın olarak kullanılan Siemens S-7 1200 donanımı yer almaktadır.

5.1.1. Deneysel sınama ortamı

Çalışmanın ilk aşaması olan saldırı aşamasında, endüstriyel kontrol sistemlerine yönelik en önemli saldırılardan Port Tarama, DoS, MitM ve Başlat/Durdur saldırıları Kali Metasploit, Ettercap ve Armitage saldırı araçları ile Wireshark trafik analizi kullanılarak Şekil 5.2'de belirtilen bölümlendirilmemiş ve Şekil 5.3'de belirtilen bölümlendirilmiş ağ topolojilerindeki deneysel ağlara gerçekleştirilmiştir.



Şekil 5.2. Bölümlendirilmemiş ağ topolojisi (Saldırı aşaması)



Şekil 5.3. Bölümlendirilmiş ağ topolojisi (Saldırı aşaması)

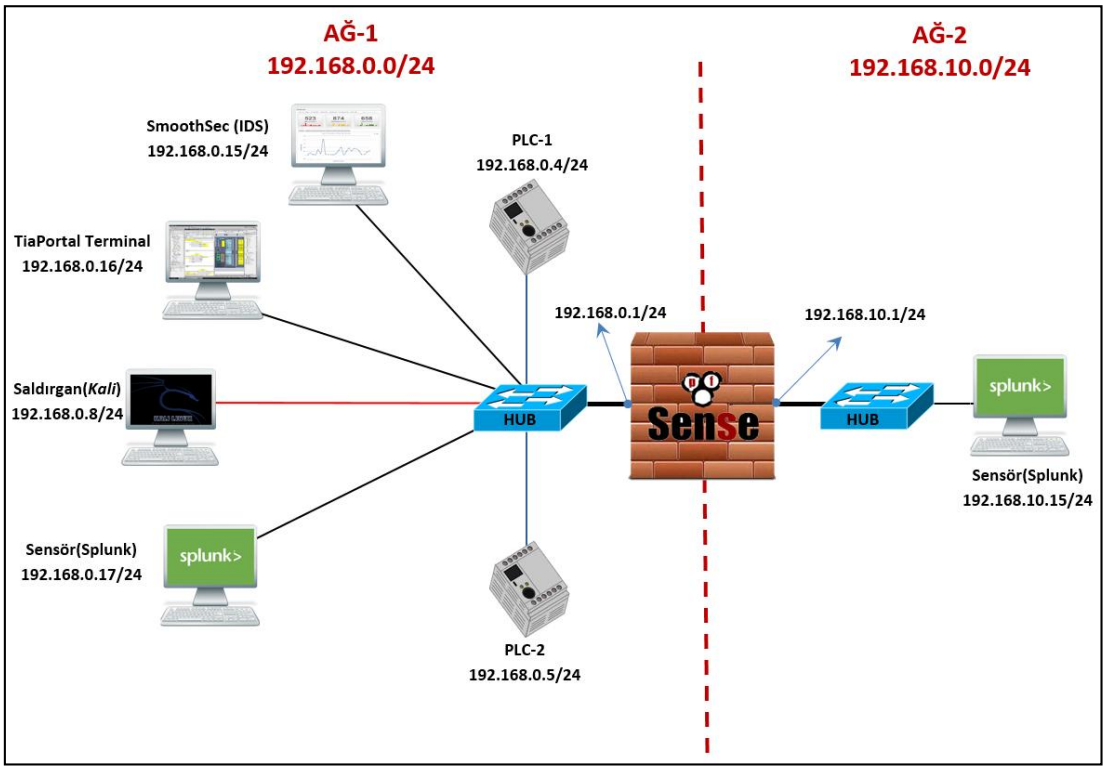
Bu aşamada sadece saldırılara odaklanılmışmış, tespite yönelik herhangi bir araç kullanılmamıştır. Sınama ortamında, bir adet S-7 1200 PLC donanımı, PLC'nin uzaktan yönetim ve kontrolünün gerçekleştirildiği üzerinde TIA Portal yönetim yazılımı bulunan bir adet yönetim bilgisayarı, Kali Linux işletim sistemi kurulu bir adet saldırgan kişisel bilgisayar yer almaktadır. Cihazların bağlantıları fiziksel olarak gerçekleştirilmiş, kullanılan saldırı araçları için Kali işletim sistemi Vmware sanallaştırma yazılımı üzerine kurulmuştur. Kali, sayısal analiz ve penetrasyon testleri için tasarlanmış açık kaynak işletim sistemidir. Saldırıların cihaz üzerindeki etkilerinin tespit edilmesi maksadıyla kullanılan tespit yazılımları için de ayrı bir bilgisayar kullanılmıştır.

Ağ bölümlendirmesi/izolasyonu (segmentation), geleneksel bilgi teknolojileri ve ağlarında hayati öneme sahip donanımların ya da uygulamaların daha iyi korunması ve ağın diğer bölümlerinden izole edilmesinde sıklıkla kullanılan güvenlik önlemidir. Çalışmada, bölümlendirilmiş ağ topolojisinde, PLC'leri Şekil 5.3'de gösterildiği gibi diğer bileşenlerden yalıtmak için ayrı bir ağda yapılandırılmıştır. STUXNET örneğinde olduğu gibi tüm sisteme zarar vermemek için, bölümlendirme yapılan ağda PLC'ler ayrı alt ağlarda olmalıdır. Ağ segmentasyonu, hayati donanım ve uygulamaları korumak için ağın diğer bölümlerinden izole etmek için geleneksel bilgi teknolojileri ağlarında sıklıkla kullanılan bir güvenlik önlemidir [53]. Ağ bölümlemesinin ana amacı, siber saldırılara karşı direnç de dahil olmak üzere fiziksel süreçlerin esnekliğini ve direncini arttırmaktır. Ağ bölümlemesi, aynı alt ağda meydana gelen siber saldırıların etkilerini en aza indirmenin bir yolu olarak kullanılan bir yöntemdir [205]. Fiziksel kısıtlamalar, coğrafi olarak dağınık cihazlar ve özellikle kritik servislerin korunması için gerçekleştirilmektedir [5].

Şekil 5.2 (bölümlendirilmemiş) ile Şekil 5.3 (bölümlendirilmiş) karşılaştırıldığında, Şekil 5.2'de sadece bir ağın (192.168.0.0/24) olduğu görülmektedir. Diğer taraftan, Şekil 5.3'de ise 192.168.0.0/24 ve 192.168.1.0/24 adres aralığına sahip iki farklı ağ bulunmaktadır. Bölümlendirilmiş ağ topolojisinde PLC'ler 192.168.0.0/24 ağında, ağın diğer bileşenleri ise 192.168.1.0/24 ağında konuşlandırılmıştır. PLC'lerin diğer bileşenlerden ayrılmasının nedeni, onları kritik önem taşıyan donanımlar olarak korumaktır.

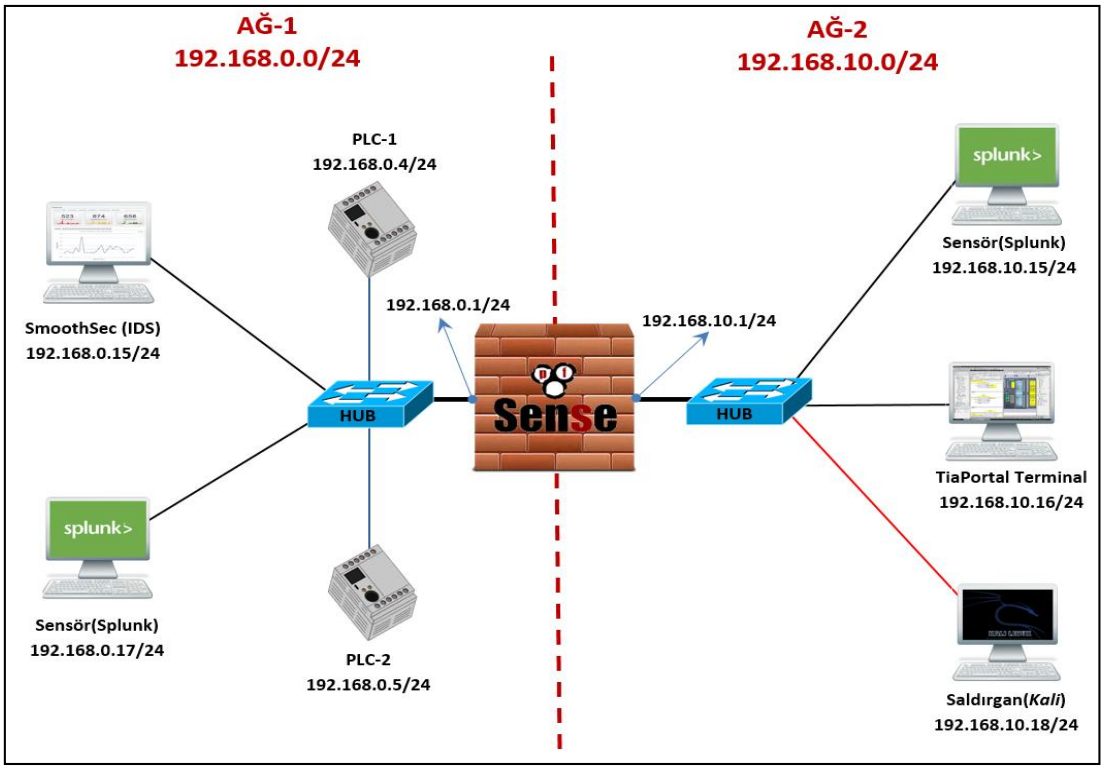
5.1.2. Saldırıların tespiti

Analizlerin ikinci aşamasında ise ilk aşamada gerçekleştirilen saldırı paketlerinin izlenmesi, depolanması, paket analizi yapılması, saldırı paternlerinin oluşturulması ve bu paternlere ilişkin tespit sistemlerine (smoothsec ve splunk) saldırı kurallarının girilerek, müteakip bir zamanda yapılacak benzer saldırıların tespit edilmesi hedeflenmiştir. Bu kapsamda, Şekil 5.4'de yer alan bölümlendirilmemiş ağ topolojisinde tüm saldırı ve tespit sistemleri 192.168.0.0/24 ağında yer almaktadır. Bu ağ topolojisi, Şekil 5.2'de yer alan topolojiye analiz aşamasında gerçekleştirilen saldırılardan Hizmet Reddi (DoS), Başlat/Durdur (Start/Stop), Port Tarama (Port Scan) başta olmak üzere ağa yapılacak saldırıların tespitine yönelik, SmoothSec IDS yazılımı (sensör) ve MitM saldırı yöntemi içinde Splunk log yönetim yazılımının eklenmesiyle genişletilmiş biçimidir.



Şekil 5.4. Bölümlendirilmemiş ağ topolojisi (Tespit)

Şekil 5.5'de görülen bölümlendirilmiş ağ topolojisinde ise 2 adet PLC, Splunk log izleme ve yönetim bilgisayarı ile SmoothSec IDS yazılımı bilgisayarı ağ-1'de (192.168.0.0/24) TIA Portal yönetim bilgisayarı, Kali Linux bilgisayarı, Splunk log izleme ve yönetim bilgisayarı ağ-2'de (192.168.10.0/24) yer almaktadır. Bu topoloji de Şekil 5.3'de yer alan topolojiye tespit sistemlerinin eklenmesiyle oluşturulmuştur.



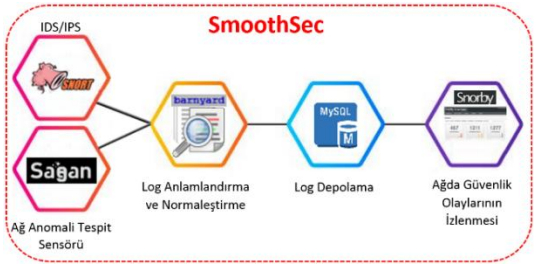
Şekil 5.5. Bölümlendirilmiş ağ topolojisi (Tespit)

Güvenlik ve güvenilirlik, ticari ya da endüstriyel herhangi bir ağın en temel gereksinimlerindendir. Ancak ağ teknolojisindeki hızlı ilerlemelerle saldırılar savunmalara kıyasla daha karmaşık hale gelmiştir. Güvenlik duvarları ve yönlendirici tabanlı paket filtreleme genel bir ağ güvenlik topolojisinin temel unsurları olmasına rağmen, kendi başlarına yeterli değildir. Dolayısıyla, ağın yetkisiz erişimden korunması için, İzinsiz Giriş Tespit Sistemi (IDS) ve İzinsiz Giriş Önleme Sistemi (IPS) çözümleri ön plana çıkmaktadır.

Saldırı tespiti, bir sistemin veya ağın şüpheli etkinliklerini izlemek ve raporlamak için kullanılan bir aktivitedir. Saldırı tespit sistemi ise bir sisteme veya bir ağa müdahaleleri tespit eden bir yazılım veya donanım veya her ikisinin birleşimi olabilir [206]. Aktif IDS, saldırıları ve karşı önlemleri engellemeye ya da en azından yöneticileri uyarmaya çalışır. Pasif IDS, sadece saldırı ayrıntılarını günlüğe kaydettirir veya denetim için izler oluşturur. Bir IPS ise ağ trafiğini tarayan ve bir uygulamanın veya sistemin yetkisiz erişimi gibi durumlarda istismarını önleyen bir ağ güvenliği veya tehdit önleme teknolojisidir. IPS, tehlikeli içeriği analiz etmek için güvenlik duvarının arkasında bulunur. IDS tarayıp ve raporlarken; IPS aktif olarak analiz edebilir ve ağ trafiğinde işlem yapar [207].

Saldırıları tespit etmek için imza tabanlı ve anormalliğe dayalı olmak üzere iki temel yaklaşım mevcuttur. İmza tabanlı tespit fonksiyonel olarak geleneksel antivirüs tarayıcıyla aynıdır. Her saldırı olayı için olay kütüphanesinden bilinen bir imza arar. Daha sistematik ve daha güvenli bir çözüm uygulamak için anormalliğe dayalı tespit düşünülmelidir. Anomaliliğe dayalı tespitte öncellikle bir ağın gelen trafiği taranır. Bütün yasal (normal) trafik filtrelenir ve anormal davranış sergileyen trafik paketleri izlenir. Her iki yaklaşımın artı ve eksileri vardır. Bilinen imzaların bulunduğu veritabanıyla imza tabanlı IDS daha güvenilirdir ve sistem eşleşen kalıpları aldığında daha iyi çalışır, ancak yeni saldırıları tespit edemez. Öte yandan, anormalliğe dayalı IDS, yanlış alarmların sayısını arttırmanın dezavantajlarının yanında bilinmeyen (özellikle sıfırıncı gün) saldırıları tespit edebilmektedir.

Ticari ağlar için kullanılan IDS kurallarının büyük çoğunluğu Endüstriyel kontrol sistemleri ve diğer kontrol sistemleri için geçerli olmamaktadır. Geleneksel IDS/IPS sistemlerinin temel çalışma mantığı; paketlerin atılması ya da aynı paketler için yönlendirmenin iptali ile erişimlerin engellenmesine dayanmaktadır. Ancak bu çalışma yöntemi endüstriyel kontrol sistemleri için kabul edilebilir değildir. Endüstriyel altyapıların gereksinimleri nedeniyle, SCADA gibi endüstriyel kontrol sistemlerinde donanımlar ve kontrolcüler arasında düzenli ve sürekli bir haberleşme gereklidir. Bu haberleşmede meydana gelen en küçük bir kesinti, en iyi ihtimalle sistemin çalışmasının durması başta olmak üzere önemli felaketlere yol açabilmektedir. Bu nedenle EKS'ye özgü kural setlerinin oluşturulması gerekmektedir. Çalışmada sınama ortamında PLC'nin bulunduğu ağ üzerinde gerçekleştirilen aktif saldırıların tespitine yönelik olarak Şekil 5.6'da görülen Smoothsec sistemi kullanılmıştır. SmoothSec; Snort, Snorby, Barnyard, Sagan gibi ağ güvenliği araçlarını içinde barındıran ve saldırıların tespiti maksadıyla geliştirilen bir Linux dağıtımıdır. SmoothSec aracılığıyla elde edilen verilerin daha sonra tekrar analizi için veritabanına kaydetmek üzere veritabanı kurulumu yapılmıştır.



Şekil 5.6. Saldırı tespitinde kullanılan SmoothSec sistemi

Tespit sisteminin mevcut sisteme ilave yük getirmemesi ve sistemin işlerliğini etkilememesi için aynalama tekniği kullanılarak ağ üzerinde akan paketlerin bir kopyası sensörlere aktarılarak analizler gerçekleştirilmiştir. Smoothsec'in bileşenlerinden biri olan Snort IDS'e girilen örnek bir kural, Şekil 5.7’de gösterilmiştir. Önceki bölümde belirtildiği gibi, SmoothSec, EKS'ye özel yapılandırmalar ve kural dizileri gibi endüstriyel kontrol sistemindeki saldırıları tespit etmek için Şekil 5.7'nin ilk satırında gösterildiği gibi Başlat \ Durdur saldırısına özgü kural girilmiştir. Algılama kurallarını elde etmek için, Şekil 5.1'de gösterilen aşamalar uygulanmıştır. Bu kapsamda, başlangıçta, saldırı gerçekleştirilmiş ve bu çalışmada Wireshark olan paket analizörü yoluyla analiz için saldırı paketleri ele geçirilmiştir. Daha sonra, saldırının imzası, Şekil 5.7'de ikinci sırada belirtilen port 102'nin sürekli olarak izlenmesi sonucunda ortaya çıkarılmıştır. Son olarak, saldırı, Smoothsec'e girilen kuralın doğrulanması için tekrar edilmiştir.

<table>
<tr><th>Kural Adı</th><th>Kural</th><th>Öncelik</th></tr>
<tr><td>SET PLC START/STOP</td><td><code>alert tcp any any ->any 102 (msg: ”Request CPU functions/set PLC CPU START/STOP”; content:”|03 00 00 43 02 f0 80 72|”; classtype: policy-violation; sid:201800001; rev:1;)</code></td><td>Yüksek (1)</td></tr>
<tr><td>DATA FLOW FROM/TO PLC</td><td><code>alert tcp any any ->any 102 (msg: ”Data flow from/to PLC”;classtype: misc-activity; sid:201800002; rev:1;)</code></td><td>Düşük (3)</td></tr>
<tr><td>ET POLICY Unallocated IP Space Traffic</td><td><code>alert ip any ->$HOME-NET any (msg: ”ET POLICY Unallocated IP [0.0.0.0/18, 192.0.0.0/24, 192.0.2.0/24, 198.18.0.0/15, 198.51.100.0/24, 203.0.113.0/24] Space Traffic – Bogon Nets“; threshold:typelimit, trackby-src,count 1, seconds 360; classtype:bad-unknown; sid:2002749; rev:14;)</code></td><td>Orta (2)</td></tr>
<tr><td>ET SCAN ICMP PING IPTools</td><td><code>alert icmp $EXTERNAL_NET any -> $HOME-NET any (msg: ” ET SCAN ICMP PING IPTools”; itype:8, icode 0; content: ”|A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7 A7|”; fast_pattern: only; reference: url,www.ks-soft.net/ip-tools.eng/ index.htm; reference: url,doc,emergingthreats.net/2000575; classtype: misc-activity; sid:200575; rev:8;)</code></td><td>Düşük (3)</td></tr>
</table>

Kural Eylemi | Protokol | Kaynak IP/Port | Hedef IP/Port | Kural Opsiyonu | Değişken | Payload Algılama

Şekil 5.7. Snort IDS’e Başlat/Durdur saldırı paketlerinin tespit için kural girilmesi

Snort, 1998'de Martin Roesch tarafından oluşturulan açık kaynak kodlu bir IDS'tir. IP ağlarında gerçek zamanlı trafik analizi yapılabilir. Snort ayrıca, işletim sistemi parmak izi (fingerprint) girişimleri, ara bellek taşmaları (buffer overflow), gizli port taramaları gibi çeşitli saldırıları tespit etmek için kullanılabilir. Snort esas olarak dört bileşenden oluşur: veri koklayıcılar (sniffer), ön işlemci, algılama motoru ve günlük (log) ve alarm sistemi [208]. Snort, algılamanın doğası gereği, Snort imza eşleşmesine bağlıdır. Bu nedenle, yeni imzalar için ağın sürekli izlenerek anormal paketlerin imzaları çıkarılmalıdır [209].

Bu kapsamda, öncelikle mevcut yapıda başlat ve durdur işlemlerinde gerçek sistemin göndermiş olduğu paketler tespit edilerek incelenmiştir. Müteakiben başlat/durdur işlemlerinde cihaz bağımsız olarak gönderilen paketler ayrıştırılmıştır. Ayrıştırılan paketler tespit sistemine (Snort) entegre edilmiş ve cihaza gönderilen başlat/durdur komutlarının tespiti sağlanmıştır. Bu sayede iç ve dış tehditlere karşı normlar belirlenerek, sapmaların tespitine yönelik çalışma gerçekleştirilmiştir. Son olarak, saldırılara karşı olan normlar ve saldırının imzası, Şekil 5.8'de gösterildiği gibi yakalanan saldırı paketlerini Wireshark üzerinden analiz ederek elde edilmiştir.

```
00 0c 29 fa 99 e5 00 1c  06 06 10 f1 08 00 45 00   ..)...........E.
00 46 01 93 00 00 1e 06  19 c3 c0 a8 0a 12 c0 a8   .F..............
00 04 86 2b 00 66 00 03  60 d9 ab a3 13 3b 50 18   ...f.+..`....;P.
10 00 35 56 00 00 03 00  00 1e 02 f0 80 72 02 00   ..5V.........r..
0f 32 00 00 04 f2 00 00  00 08 34 00 00 00 00 00   .2........4.....
72 02 00 00                                        r...
```

Nitelik	İçerik (Hexadecimal/Decimal)
Saldırı imzası	0300001e02f08072
Sıra numarası	237
Kimlik	0x0193 (403)
Kaynak	192.168.10.18
KaynakPort	34347
Hedef	192.168.0.4
Hedef Port	102
Tür	IPv4 (0x0800)
Bayraklar	PSH,ACK
Sürüm	4
Veri	7202000f32000004f2000000083400000000072020000

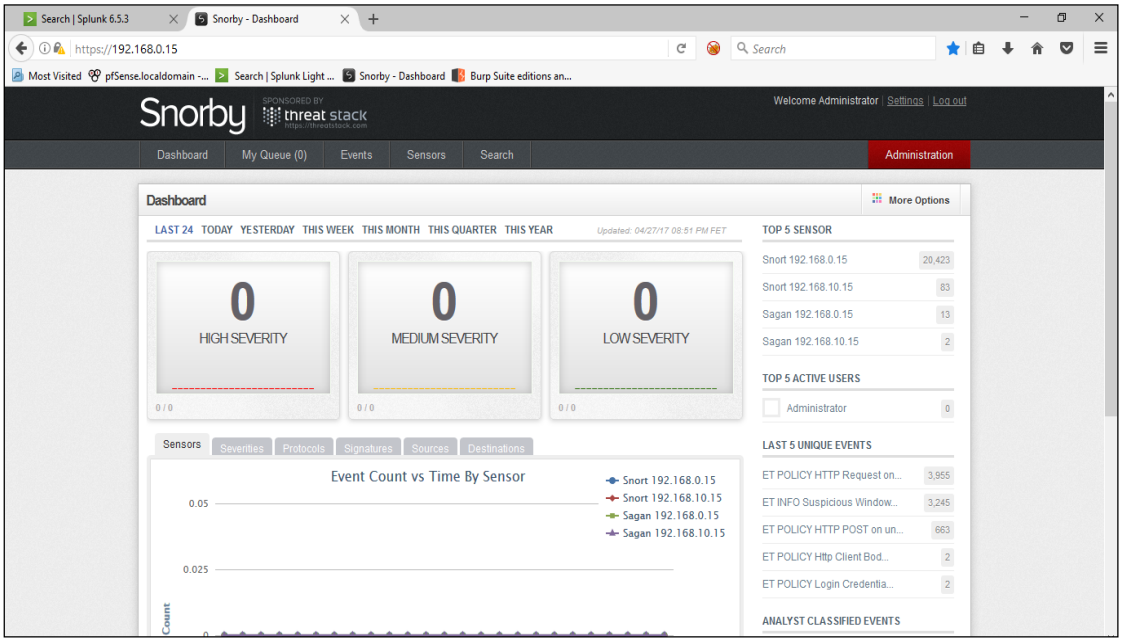
Şekil 5.8. Başlat / Durdur saldırı paketi örneği ve paket özellikleri tablosu

Snort IDS sistemine başlat/durdur saldırı kuralının tanımlanması sonucunda, IDS sistemi saldırı gerçekleştiği takdirde tespit etmesi ve alarm üretmesi hedeflenmiştir. Ancak görselleştirilmiş olan Snorby ekranında Şekil 5.9'da belirtilen kural tanımının yapılmaması durumunda, ekranda sadece kural numarası görülecektir. Bu da sistem yöneticisi tarafından alarmın hangi sebeple üretildiğini anlamasını zorlaştıracaktır. Bu nedenle, Şekil 5.9'da belirtilen kural numarasına isim tanımı yapılarak sistem yöneticisinin tespit sistemi tarafından üretilen alarmın kaynağını belirlemesi ve bu sayede hızlı reaksiyon vererek önlem alması kolaylaştırılmıştır.

```
#v1
# sid-msg.map autogenerated by PulledPork - DO NOT MODIFY BY HAND!
9          || SET PLC START/STOP
100000102 || GPL GAMES Halocon Denial of Service Empty UDP Packet || bugtraq,122
81
100000103 || GPL GAMES Breed Game Server Denial of Service Empty UDP Packet || b
ugtraq,12262
100000104 || GPL GAMES Amp II 3D Game Server Denial of Service Empty UDP Packet
|| bugtraq,12192
100000119 || GPL WEB_CLIENT Internet Explorer URLMON.DLL Content-Encoding Overfl
ow Attempt || url,www.microsoft.com/technet/security/bulletin/MS03-015.mspx || c
ve,2003-0113 || bugtraq,7419
100000136 || GPL DELETED GNU imapd search format string attempt || cve,2005-2878
 || url,www.osvdb.org/displayvuln.php?osvdb_id=19306
100000139 || GPL WEB_SERVER WEB-IIS Remote IIS Server Name spoof attempt loopbac
k IP || cve,2005-2678
100000149 || GPL EXPLOIT WEB-MISC Jboss % attempt || url,www.osvdb.org/displayvu
ln.php?osvdb_id=17403 || cve,2005-2006 || bugtraq,13985
100000152 || GPL DELETED MDaemon authentication protocol decode
100000153 || GPL IMAP MDaemon authentication multiple packet overflow attempt ||
 bugtraq,14317
100000155 || GPL DELETED MDaemon authentication overflow single packet attempt |
| bugtraq,14317
100000158 || GPL VOIP SIP INVITE message flooding
"sid-msg.map" 18326L, 2730068C                                1,1           Top
```

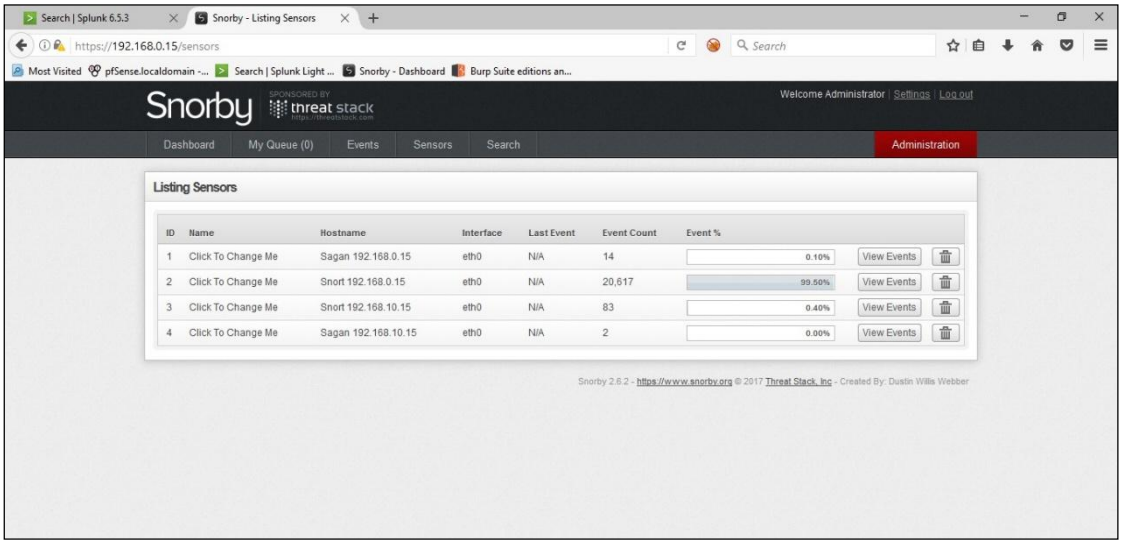
Şekil 5.9. Snort IDS'e Başlat/Durdur saldırı paketlerinin tespitinde girilen kuralın isimlendirilmesi (SID)

Test ortamında gerçekleştirilecek saldırılar öncesinde, SmoothSec tarafından yönlendirilen ağ trafiğinin analizi Snorby'e ait izleme ekranında, olayların yüksek, orta ve düşük seviye olmak üzere üç kategoriye ayrıldığı, ayrıca başlangıçta tüm değerlerin '0' olduğu görülmüştür (Şekil 5.10).



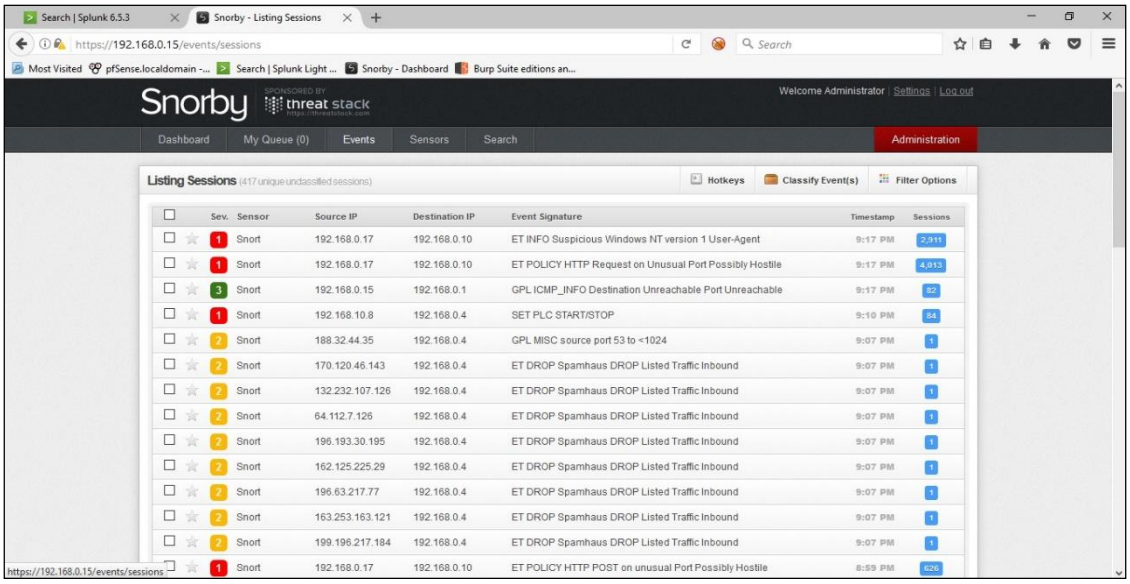
Şekil 5.10. Saldırılar öncesi Snorby yönetim ekranı

Test ortamı üzerinde yer alan bölümlendirilmiş ağ topolojisi üzerinde Şekil 5.11'de görüldüğü üzere Snort ve Sagan Sensörleri olmak üzere iki tip IDS Sensorü bulunmaktadır. Snort sensörleri, farklı ağlardan gelen trafiği izleyerek daha önceden tanımlanmış olan kural dizilerine uyması durumunda saldırıları ve ağdaki anomalileri tespit ederek, ağ güvenliği için kullanılmaktadır. Öte yandan, Sagan sensörleri, ağ anomalilerini ve ağ ve bileşenlerini izleyerek tanımlanan kurallara uygun olarak değişiklikleri algılar. Özellikle saldırıların sadece dışarıdan gelmediği ve içeriden yapılan saldırıların çok daha yıkıcı olduğu düşünüldüğünde, iç ağın Sagan IDS tarafından izlenmesinin önemi ortaya çıkmaktadır. Yukarıda belirtilen görevler kapsamında, tabloda yer alan sensörler tarafından sunulan IDS isimlerinin ve dolayısıyla uyarı kaynağının ayırt edilmesi, güvenlik uzmanlarının anormal ağ faaliyetlerine hızlı bir şekilde tepki vermesini kolaylaştıracaktır. Örneğin, Snort tabanlı bir uyarı tetiklendiğinde, güvenlik politikasına göre dışarıdan gelen tehditler için ihtiyati tedbirler alınması yönelik hızlı reaksiyon verilebilir. Diğer taraftan, iç ağın konfigürasyonunun değiştirilmesi, yeni bir cihaz eklenmesi gibi Sagan tabanlı bir uyarı alındığında, operatör tarafından yasal veya yetkisiz bir şüpheli işlem olup olmadığını kontrol edip, engellemeye veya izin vermeye yönelik hızlı bir şekilde aksiyon uygulanabilir.



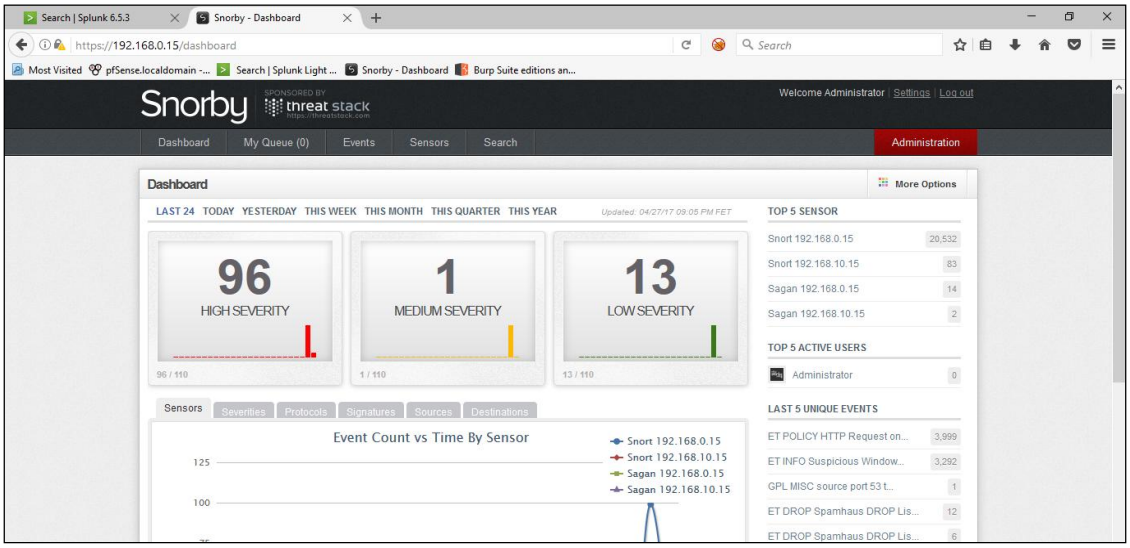
Şekil 5.11. Saldırıların tespitinde kullanılan sensörler

Saldırılara ilişkin detaylı bilgi almak amacıyla Snorby izleme ekranında yer alan olaylar (events) sekmesi altındaki oturum listesi (listing sessions) incelenmektedir. Şekil 5.12'de sunulan ekran görüntüsü incelendiğinde, tespit edilen olayların ortaya çıktığı zamana göre sıralandığı görülmektedir.



Şekil 5.12. IDS sensörleri tarafından yakalanan paketlerin olaylara dönüştürülmesi

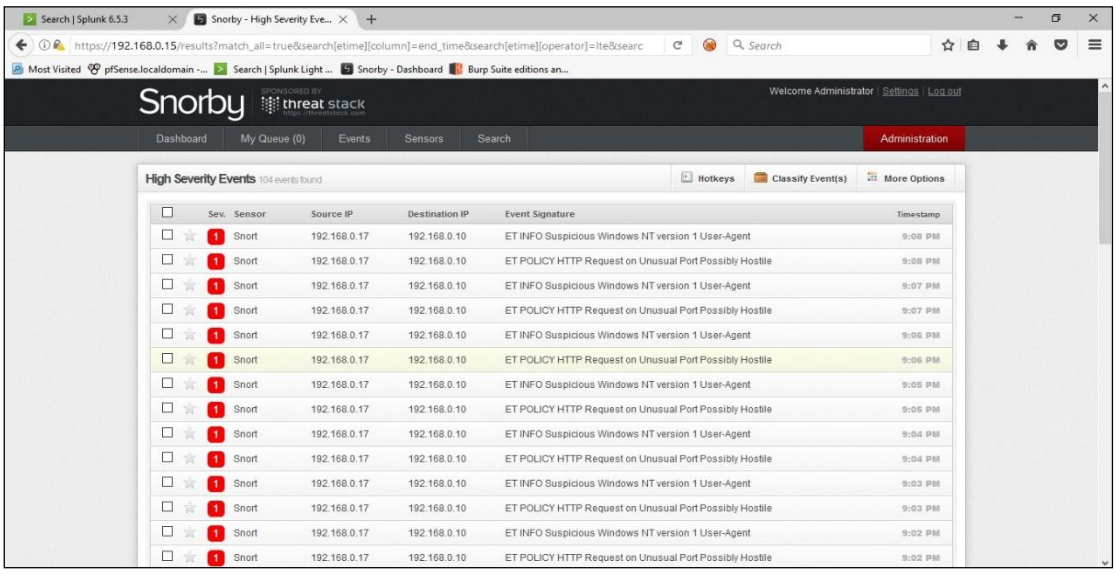
Test ortamında MitM saldırısını tespit etmek amacıyla kullanılan Splunk log izleme ve yönetim sistemi devreye alındığında ağ trafiğinde tespit edilen yüksek seviye olay sayısının '96' adet olduğu Şekil 5.13'de görülmektedir. Aynı işlem tekrarlandığında olay şablonun değişmediği ve paket sayısının 96 olduğu görülmüştür.



Şekil 5.13. Ağ paketlerinin analizi sonrası olay sayıları

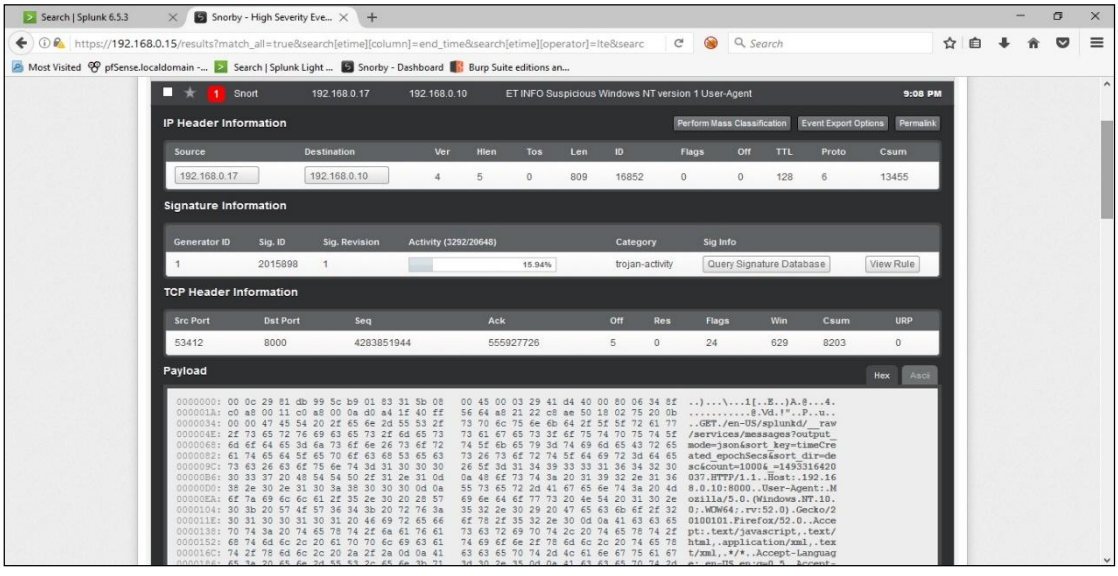
Şekil 5.13'de sunulan yüksek seviyeli olayların listesini içeren Şekil 5.14'deki ekran görüntüsü incelendiğinde, saldırının kaynak IP adresinin Splunk log izleme ve yönetim sistemi yüklü olan bilgisayara ait olduğu görülmektedir. Bu kapsamda; saldırı olarak Snorby IDS tarafından tespit edilen olayların Splunk log izleme ve yönetim bilgisayarına

ait olağan ağ trafiği olduğu, bu nedenle üretilen alarmların false-pozitif olduğu değerlendirilmiştir (EKS ağ trafiğinin izlenmesi ve ağ paketlerin doğru olarak değerlendirilmesinin önemi ortaya çıkmaktadır).



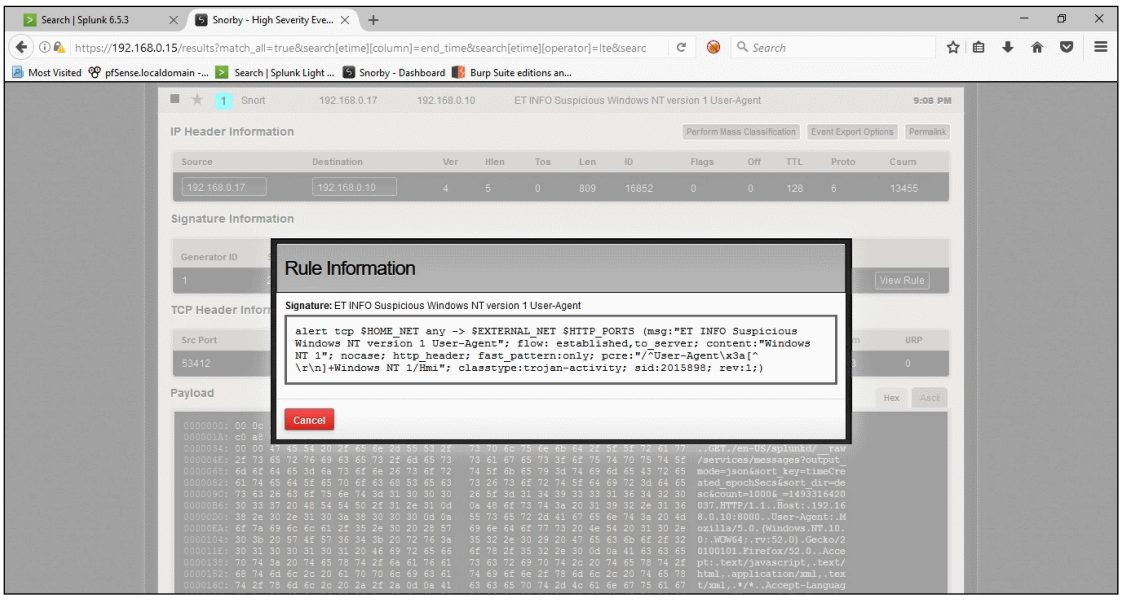
Şekil 5.14. Yüksek olayların detayı

Snorby üzerinde yüksek seviyeli olaylarda listesinde görüntülenen ve 'ET INFO Suspicious Windows NT version 1 User-Agent' olarak tanımlanan (Şekil 5.15) olaya ait paket incelendiğinde, Snorby IDS'in ortaya çıkan şüpheli trafik paketlerini tanımlayabildiği görülmektedir.



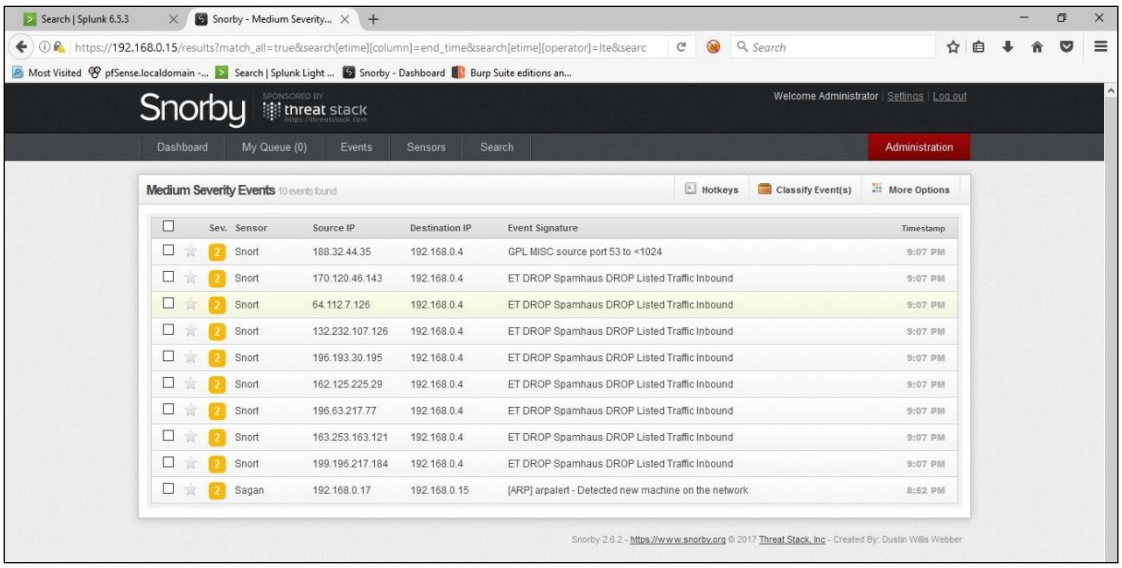
Şekil 5.15. Yüksek seviyeli olay paket içeriği

Genel olarak IDS sistemleri, üzerinden akan ağ trafiğini incelerken kütüphanesinde bulunan ve saldırı imzalarını içeren şablonlar ile gelen paketleri karşılaştırır. IDS üzerinde önceden ayarlanmış olan eşik değerleri doğrultusunda ortaya çıkan eşleşmelerin sonucunda alarm üretir. IDS sistemlerine ait saldırı imzalarını içeren kütüphaneler sürekli olarak güncellenmektedir. Bu çalışmada saldırıların sonucunda elde edilen saldırı şablonları temel alınarak saldırı imzaları oluşturulmuştur. IDS sistemleri üzerinde oluşturulan saldırı imzalarının söz konusu kütüphanelere kural bilgisi olarak (Rule Information) eklenmesi ile daha sonra meydana gelmesi muhtemel benzer saldırıların otomatik olarak tespit edilmesi hedeflenmiştir. Şekil 5.16'da yüksek seviyeli olayların tespitine ilişkin bir kural bilgisi örnek olarak görülmektedir.



Şekil 5.16. Yüksek seviyeli olayın tespit edilmesini sağlayan kural

Sagan Sistem Anomali Tespit Sensörü tarafından orta seviyeli olarak tanımlanan olayları içeren Snorby IDS'e ait ekran görüntüsü Şekil 5.17'de sunulmuştur. Ağ topolojisine yeni eklenen bir bileşenin, ağ yöneticilerinin bilgilendirilmesi maksadıyla orta seviyeli bir olay olarak listelendiği görülmektedir.



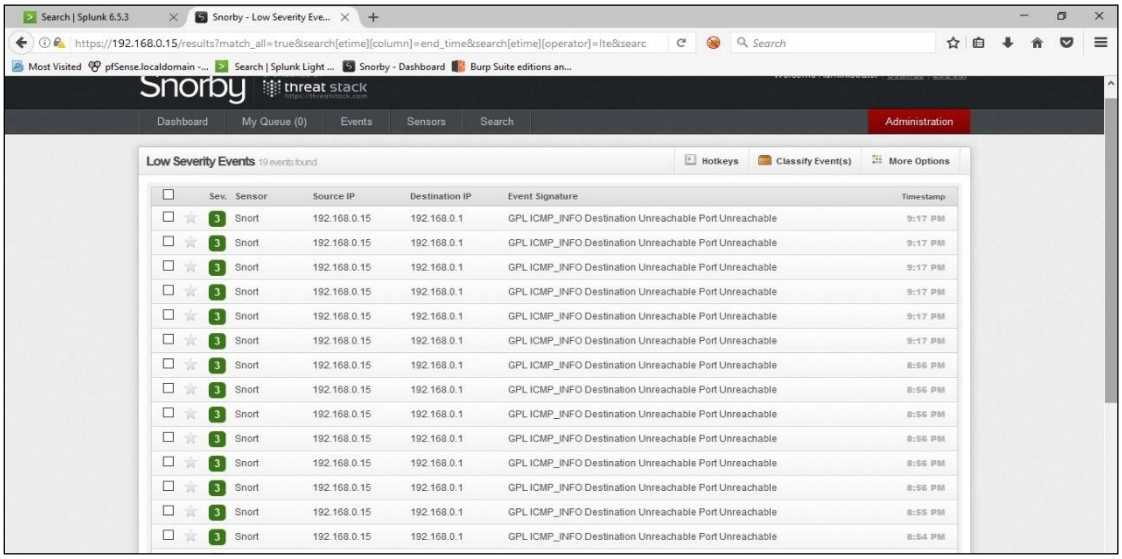
Medium Severity Events 10 events found

☐		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
☐	☆	2	Snort	188.32.44.35	192.168.0.4	GPL MISC source port 53 to <1024	9:07 PM
☐	☆	2	Snort	170.120.46.143	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	64.112.7.126	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	132.232.107.126	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	196.193.30.195	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	162.125.225.29	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	196.63.217.77	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	163.253.163.121	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Snort	199.196.217.184	192.168.0.4	ET DROP Spamhaus DROP Listed Traffic Inbound	9:07 PM
☐	☆	2	Sagan	192.168.0.17	192.168.0.15	[ARP] arpalert - Detected new machine on the network	8:52 PM

Snorby 2.6.2 - https://www.snorby.org © 2017 Threat Stack, Inc - Created By: Dustin Willis Webber

Şekil 5.17. Orta seviyeli olay örneği

IDS tarafından düşük seviyeli olarak tanımlanan olayların listelendiği Snorby'e ait ekran görüntüsü ise Şekil 5.18'de görülmektedir. Liste incelendiğinde, SmootSec'in yüklü olduğu kaynak bilgisayar ile PfSense güvenlik duvarı (hedef) arasındaki ağ trafiğinde meydana gelen olayların bilgilendirme maksadıyla listelendiği görülmektedir.

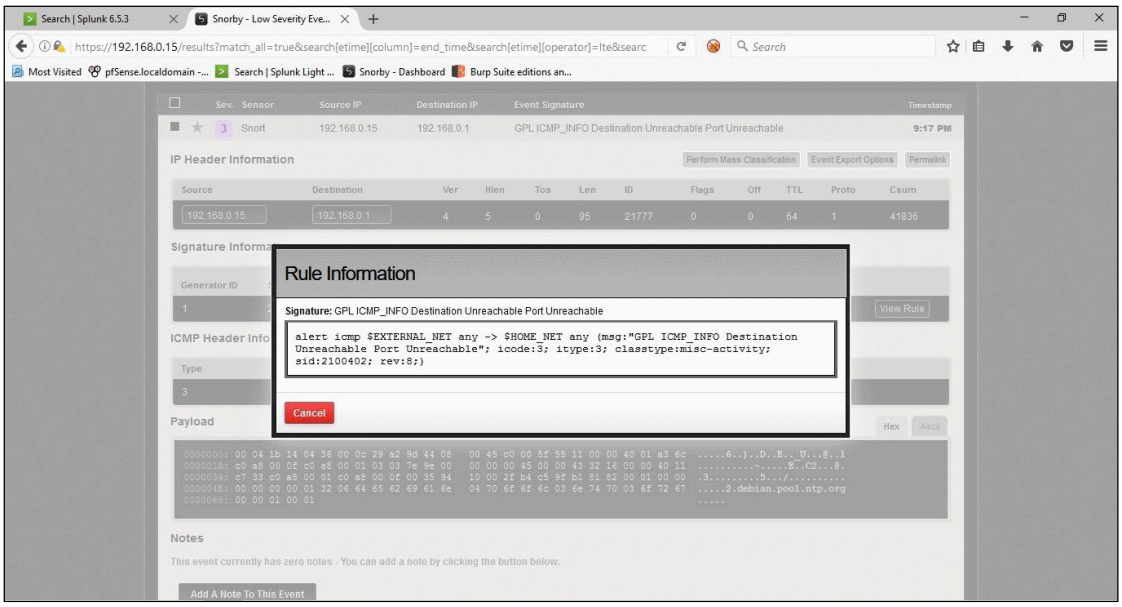


Low Severity Events 19 events found

☐		Sev.	Sensor	Source IP	Destination IP	Event Signature	Timestamp
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	9:17 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:56 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:55 PM
☐	☆	3	Snort	192.168.0.15	192.168.0.1	GPL ICMP_INFO Destination Unreachable Port Unreachable	8:54 PM

Şekil 5.18. Düşük seviyeli olay örneği

Şekil 5.19'da listelenen düşük seviyeli bir olaya ait kural bilgisi incelendiğinde, kuralın kaynak ile hedef IP adresi arasındaki iletilen ICMP paketlerini içeren ağ trafiğine ait olduğu görülmüştür.

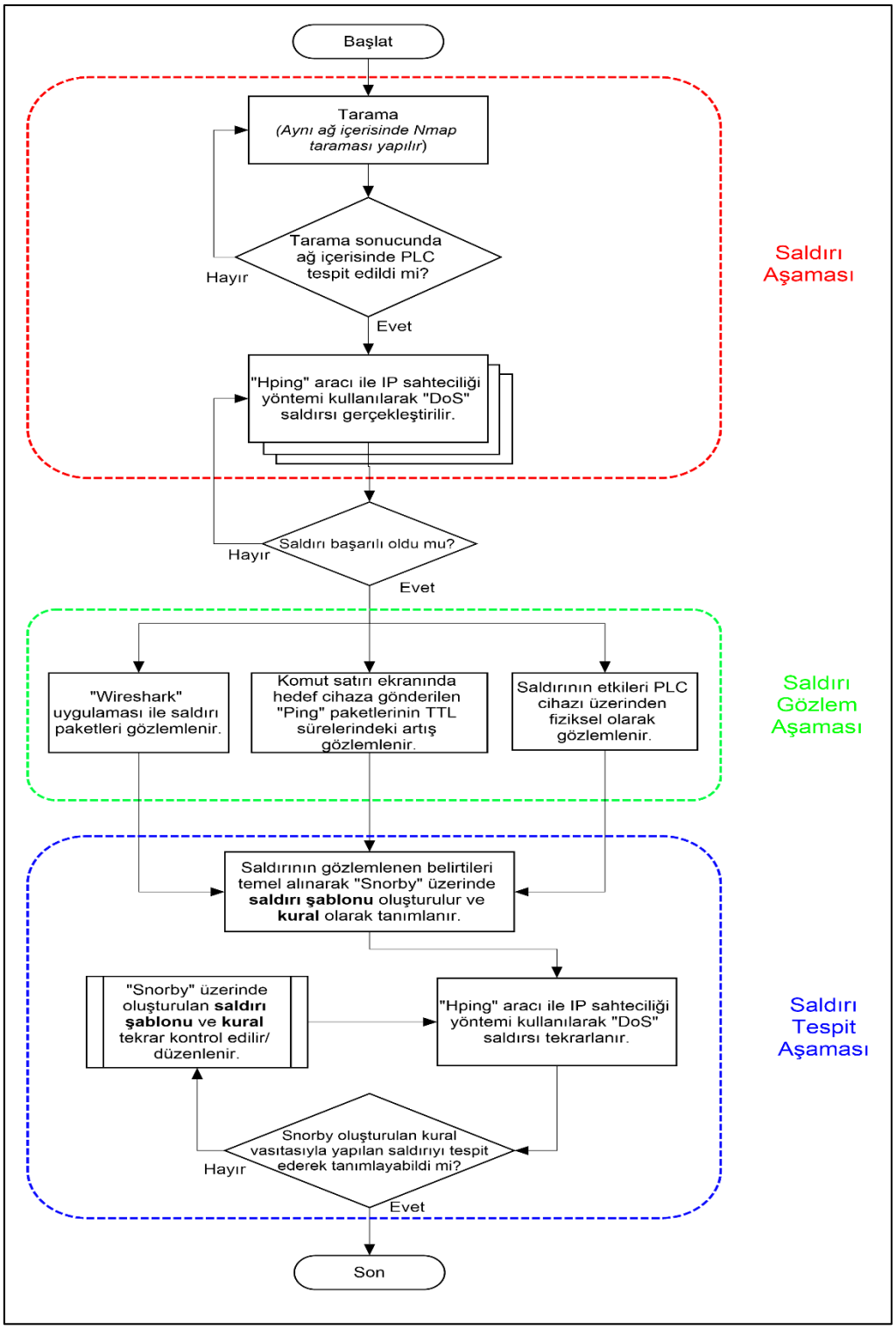


Şekil 5.19. Düşük seviyeli olayın tespit edilmesine yönelik IDS kuralı

5.1.3. Hizmet dışı bırakma saldırısı (DoS)

Saldırı analizleri kapsamında ilk olarak Hizmet Reddi saldırısı gerçekleştirilerek Şekil 5.20'de belirtilen aşamalar doğrultusunda saldırıya ilişkin sistemde gerçekleşen değişikliklerin incelenmesi, saldırı paketlerinin yakalanması ve analizi ile snort tabanlı kütüphaneye Şekil 5.7 ve Şekil 5.8'de belirtildiği üzere kural setlerinin girilmesiyle snorby aracılığıyla nihai hedef olan saldırının tespiti gerçekleştirilmiştir.

DoS ve DDoS saldırılarının temel amacı, ağın, bilgisayar sistemlerinin ve donanımlarının bant genişliği, hafıza ve disk alanı gibi kaynaklarının kaldırabileceğinden daha fazla yük bindirilmesinin sağlanarak; sistemin kullanılamaz hale getirilmesidir. Dağıtık Hizmet Engelleme saldırılarında ise (DDoS, Distributed Denial of Service), DoS'tan farklı olarak saldırı tek bir kaynaktan değil de birden fazla kaynaktan (genellikle ele geçirilmiş köle bilgisayarlardan) kurbana doğru yapılmaktadır [210]. DoS saldırıları ağ ve uygulama katmanı seviyesinde yapılmaktadır. Ağ katmanı seviyesindeki en yaygın DoS saldırı türleri; TCP taşkını (flood), UDP taşkını, ICMP ve SYN taşkınıdır. Uygulama katmanı seviyesinde ki DoS saldırıları ise; HTTP/HTTPS taşkını ve FTP taşkınıdır [211].



Şekil 5.20. Hizmet dışı bırakma (DoS) saldırısı keşif, saldırı ve tespit aşamaları

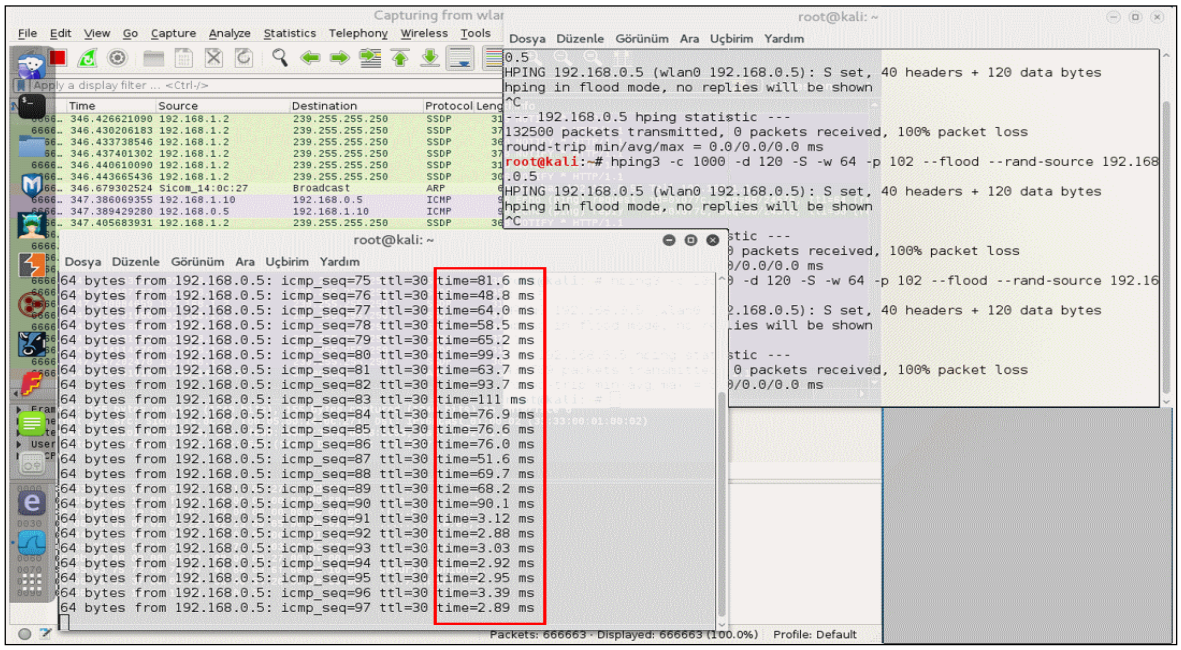
DoS ve DDoS saldırıları, yapılan çalışmalarda farklı gruplarda sınıflandırılmaktadır. Bhuyan ve diğerleri DDoS saldırılarını; kaynak sonlandırmalı, kurban sonlandırmalı, aradaki (intermediate-orta) ağ ve dağıtık olmak üzere 4 grupta sınıflandırmaktadır. Çalışmada, DDoS saldırısını kaynağında tespit etmeye yönelik kaynak sonlandırmalı

savunma mekanizması geliştirmişlerdir. Mekanizma zararlı paketleri tespit ederek olası bir taşkını engellemeye yöneliktir. Ancak bu işlem kurban tarafında yapılmamaktadır. Bunun için bir filtre veya sınırlandırma oranı girilerek kurbanlara ulaşmadan engellemeye çalışılmaktadır [211]. Bu mekanizmanın temel zorlukları ise; kurban düğüm ile herhangi bir ilişki bulunmadığından kurbana ulaşan zararlı trafik izlenememektedir. İkinci olarak, kaynak geniş bir ölçeğe dağıtıldığı için odaklanma yapılamamaktadır. Üçüncü olarak da tanımlamalar kaynak sonlandırma noktalarında yapıldığı için sık sık hatalı uyarılar verebilmektedir. Mirkovic ve Reiher'in yaptığı D-WARD çalışması kaynak sonlandırmalı DDoS savunma sistemidir [212]. Bu yöntemin önemli bir eksikliği, saldırganların kaynak adreslerini taklit ederek veya gizleyerek DDoS saldırılarını daha karmaşık hale getirmesi durumunda, diğer bir ifadeyle kaynağın tespit edilememesi ya da yanlış tespit edilmesi halinde yetersiz kalmasıdır.

DoS ve DDoS saldırılarının diğer bir gruplandırılması da tespit mekanizmalarına göre yapılmaktadır. LEE ve diğerleri çalışmalarında, gelen paketlerin kaynak IP adreslerinin dağılımını kullanarak DDoS saldırılarının tespitine yönelik bir model önermişlerdir. Bu modelde, düşük ek yük, kısa tespit gecikmesi ve yüksek tespit oranı hedeflenmiştir [213]. Peng ve diğerleri de, bu ikinci yöntemi uygulamışlar ve çalışmalarında gelen IP paketlerinin izlenmesine dayalı bir tespit mekanizması önermişlerdir. Bu mekanizma, yeni kaynak IP adreslerini kullanarak basit bir tespit modeli oluşturmaktadır [48].

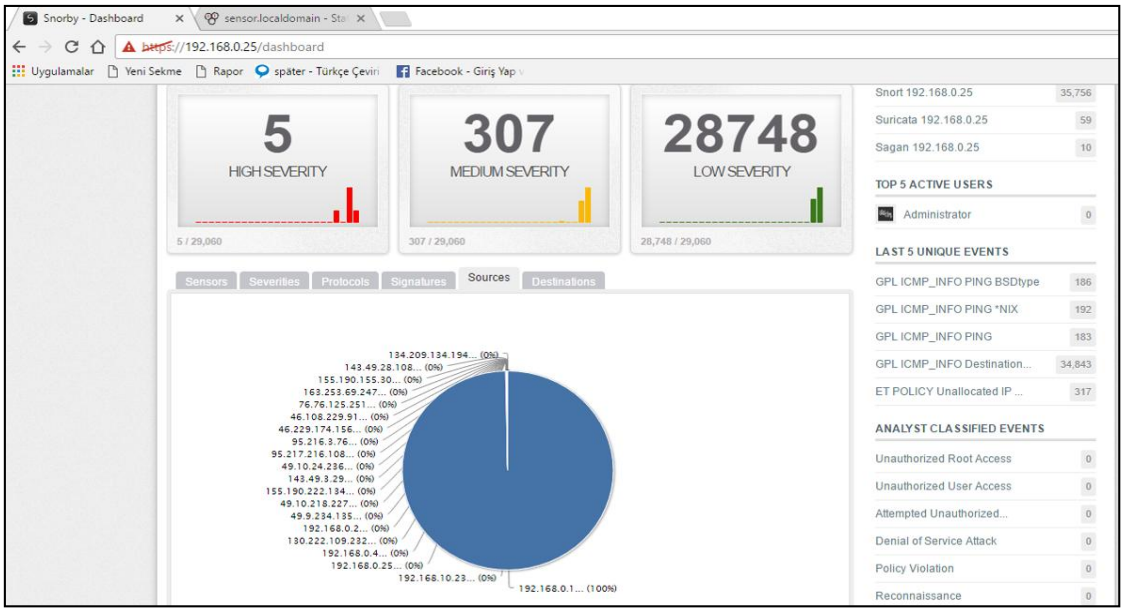
Ticari ağlarda olduğu gibi EKS'ye yönelik önemli tehditlerden de birisi Servis Reddi saldırısıdır. DoS saldırısı ile EKS sisteminin belirli bir kaynağa erişiminin veya kaynağın amacı doğrultusunda kullanımının engellenmesidir [214]. Endüstriyel kontrol sistemlerinde kritik olan sistemlerin izlenmesinin veya ihtiyaç duyulduğunda gerekli düzenlemelerin yapılmasının engellenmesi Servis Reddi'nin önemli sonuçlarındandır [46]. DoS saldırıları nihayetinde kurbanlar tarafından fark edilebilen saldırı türlerindendir. Ancak önemli olan nokta, bu saldırıları mümkün olan en kısa sürede, hizmetlerin kullanımı engellenmeden veya taşkın etkisi oluşmadan tespit etmektir [63]. DoS saldırısı çoğunlukla diğer saldırılara göre daha az tehlikeli görünse de endüstriyel kontrol sistemleri ve yönettiği kritik altyapılar için bazı durumlarda diğer birçok saldırı türünden daha tehlikeli hale gelebilmektedir. Örneğin baraj kapağının zamanında kapatılamadığı bir olayda hizmet reddi önemli felaketlere yol açabilmektedir.

PLC protokollerindeki diğer bir önemli açıklık da herhangi bir IP/MAC adresinden veya düğüm noktasından gelen tüm sorgu paketlerine PLC'nin cevap vermesidir. Bu doğrultuda, çalışmada Hping programı kullanılarak, PLC cihazının ağa bağlantısının yapıldığı PROFINET portuna (102) gerçekleştirilen DoS saldırısı sonucu Şekil 5.21'de görülmektedir. Saldırı sonucunda, cihaza gönderilen ping paket süreleri saldırı devam ettiği sürece oldukça (90 ms civarı) artmıştır. Bu nedenle, DoS saldırısının sürecinde büyük miktarda istek paketlerinin art arda gönderilmesi nedeniyle, PLC'nin TIA Portal üzerinden komut edilmesi engellenmiş ve istenilen değişiklikler gerçekleştirilememiştir.



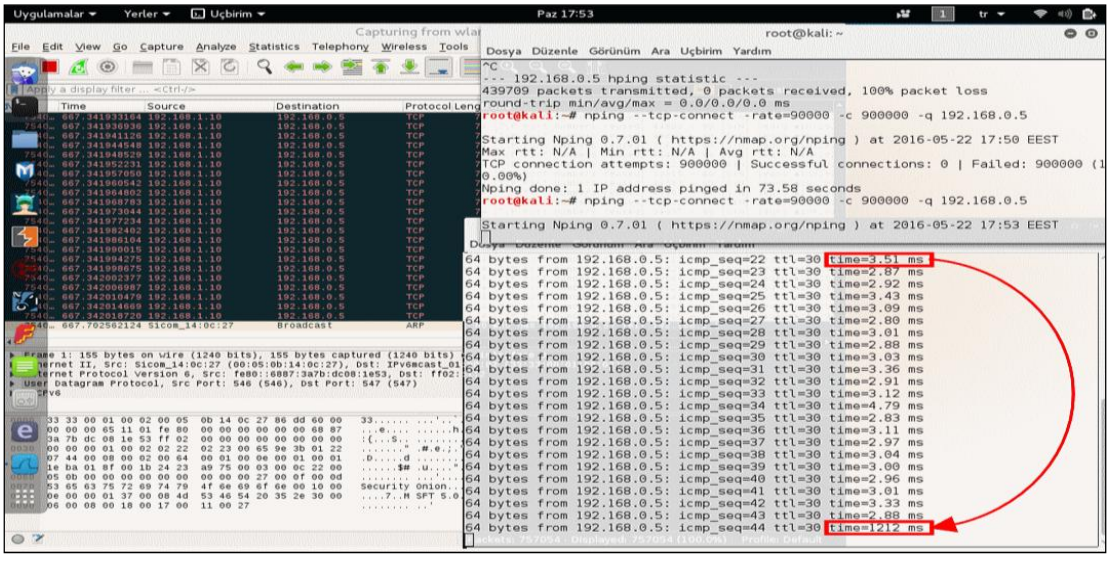
Şekil 5.21. Bölümlendirilmemiş ağda hizmet dışı bırakma saldırısı

DoS saldırısı sonrasında az sayıda saldırgan bilgisayar ile saldırı yapılmasına rağmen paket trafiğinde dalgalanmaların olduğu görülmektedir. IEEE 1646-2004 trafo merkezlerinin otomasyon haberleşmesindeki gecikme standardına göre yüksek hızlı mesajların 2 ms ile 10 ms arasında iletilmesi gerekmektedir [215]. Bu kapsamda, DoS saldırısı nedeniyle kritik zamanlı kontrol sistemi trafiğindeki değişmeler özellikle de yüksek hızlı mesaj dağıtımı ihtiyaçları dikkate alındığında önemli problemlere yol açabilecektir. Tek kaynaktan yapılan saldırılarda büyük oranda paket aynı IP adresinden geldiği için tespiti kolay olmaktadır ancak IP sahteciliği yapılarak farklı IP adreslerinden yapılan DoS saldırılarının tespiti aynı oranda kolay olmamaktadır. Şekil 5.22'de Hping3'ün IP sahteciliği özelliği (IP Spoofing), ile saldırı kaynağı olarak atanmamış IP adreslerinin (bogon) rastgele tahsis edildiği (rand source) görülmektedir.



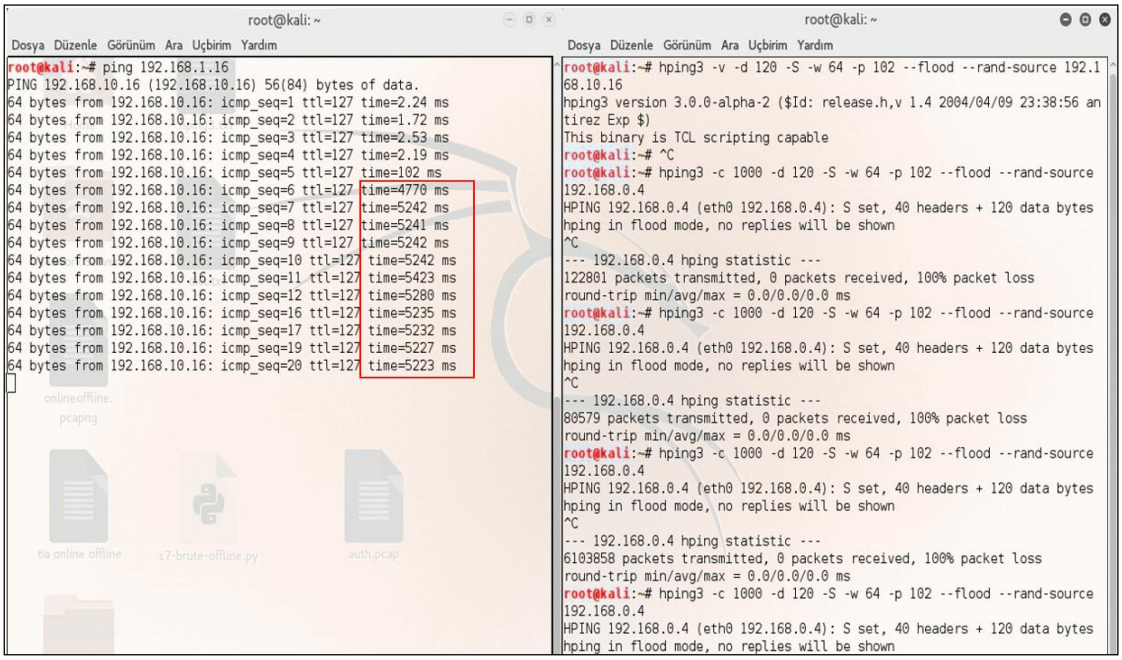
Şekil 5.22. Hizmet dışı bırakma saldırısı paketlerine ait kaynak IP adresleri

DoS saldırısı ağ bölümlendirilmesinin yapıldığı topoloji üzerinde tekrar test edilmiştir. Şekil 5.23'de görüldüğü üzere, bölünmemiş ağ topolojisine yapılan DoS saldırısında olduğu gibi PLC cihazının Ping tepki süresi, saldırı devam ettiği sürece önemli ölçüde artmıştır. DoS saldırısı durdurulduğunda ping tepki süresi 1212 ms olarak ölçülmüştür. DoS saldırısı doğrudan IP hedefli olduğu için IP adresi tespit edildiği takdirde farklı bir ağ içerisinde olsa dahi başarıyla gerçekleştirilebildiği tespit edilmiştir. PLC'nin IP adresini saptamak için Nmap aracı gibi herhangi bir port tarama aracı kullanılabilir. (Bu süreç Başlat / Durdur saldırısı bölümünde tartışılmıştır).

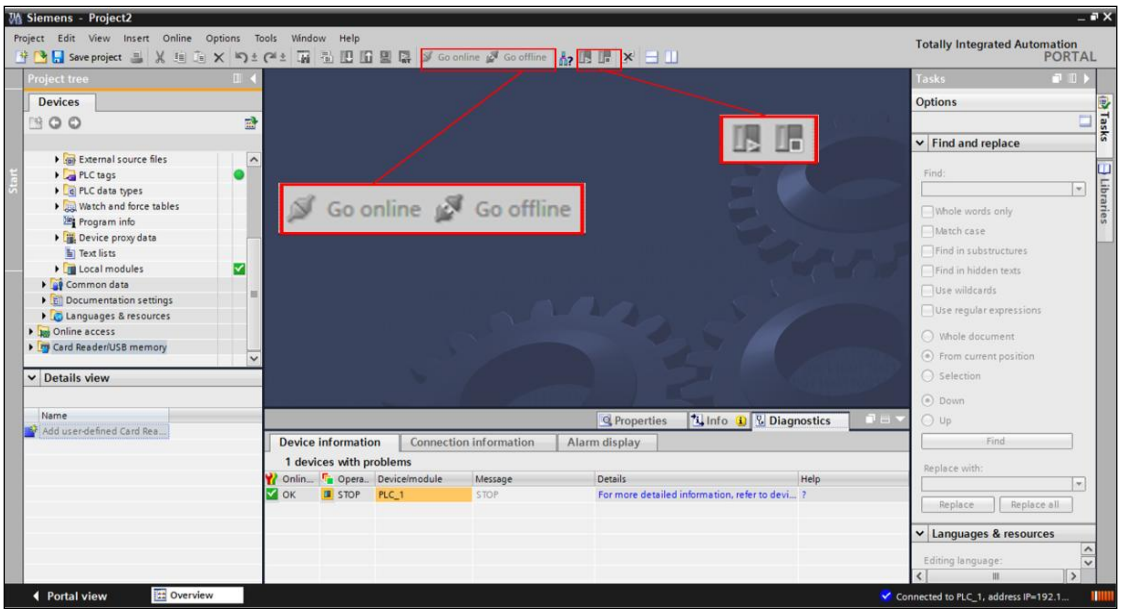


Şekil 5.23. Bölümlendirilmiş ağda hizmet dışı bırakma saldırısı

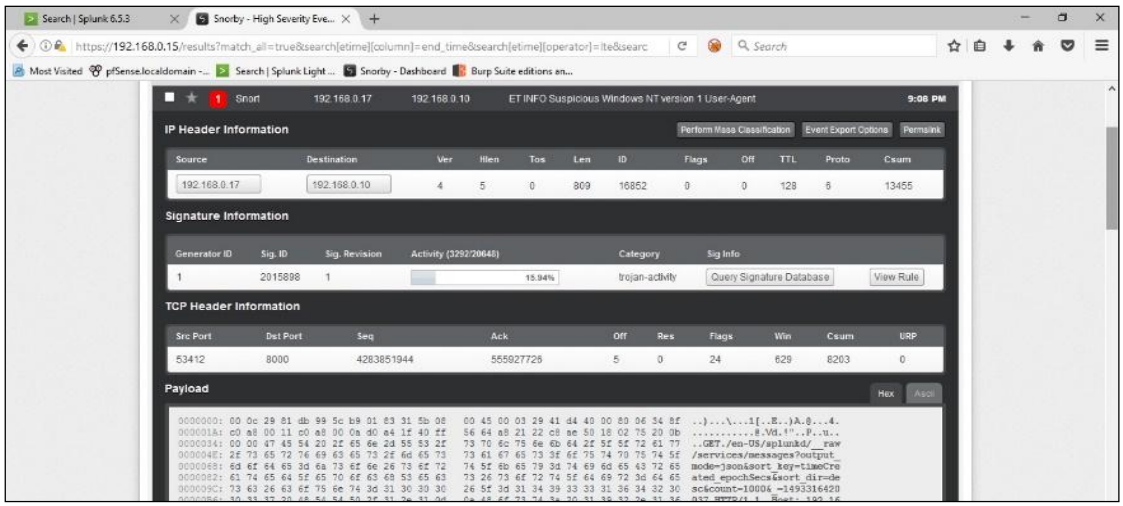
DoS saldırısı, kontrol bilgisayarı olan TIA Portala da gerçekleştirilmiştir. Şekil 5.24'de gösterildiği gibi, saldırı devam ettiği sürece, ping yanıt süresi yaklaşık 2 ms'den 5280 ms'e yükselmiştir. Ayrıca, Şekil 5.25'de görüldüğü üzere TIA Portalda yer tüm kontrol fonksiyonları devre dışı kalmış ve PLC TIA Portal üzerinden kontrol edilememiştir.



Şekil 5.24. TIA Portal'a gerçekleştirilen DoS saldırısı ve cevap süreleri (Bölümlendirilmiş ağda)

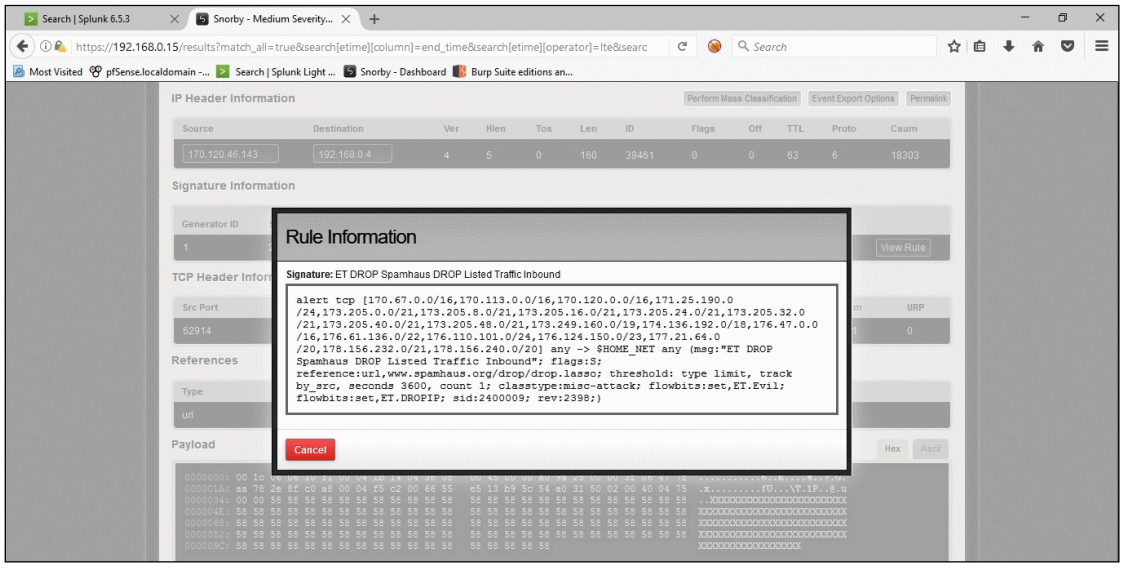


Şekil 5.25. DoS saldırısı sonrası TIA Portal ekranı (Bölümlendirilmiş ağda)



Şekil 5.26. DoS saldırısı sonrasında tespit edilen olay paketleri

Orta seviyeli olaylar kategorisinden spam olarak uyarı verilen pakete ait içerik Şekil 5.26'da görülmektedir. Şekil incelendiğinde, DoS saldırılarına ait paketlerin orta seviyeli bir olay olarak listelendiği görülmektedir. Şekil 5.27'de listelenen orta seviyeli olaya ait kural bilgisi incelendiğinde ise farklı kaynak IP adreslerinden gelen ve aynı şablondaki ağ trafiği paketleri olduğu görülmüştür. Listelenen olaylar genel olarak değerlendirildiğinde dağıtık hizmet reddi (DDoS) saldırısına yönelik paketler olduğu anlaşılmaktadır.

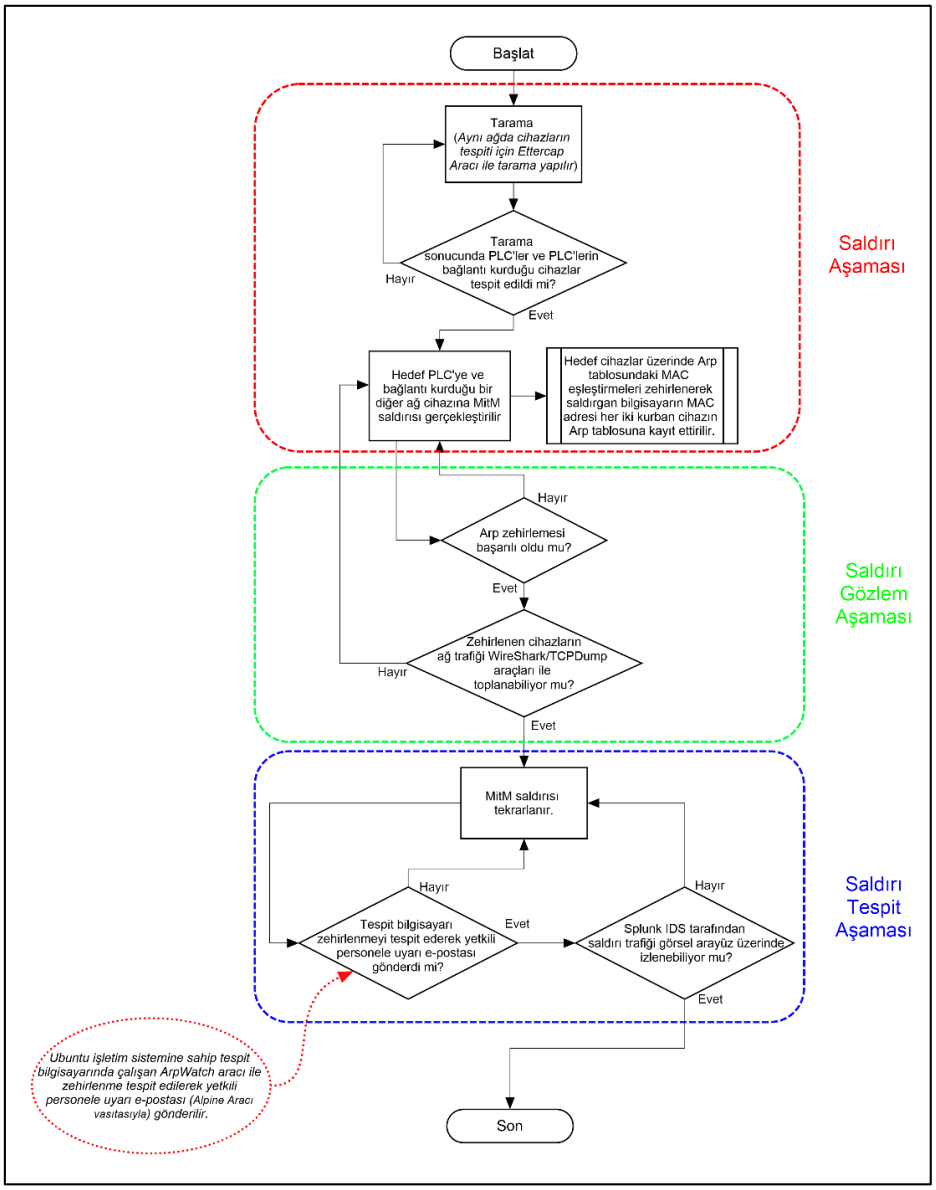


Şekil 5.27. DoS saldırısına ait paketlerin tespit edilmesinde kullanılan kural

DoS saldırısı sonuçlarından görüldüğü üzere, saldırı hem kontrol bilgisayarı TIA Portala hem de PLC'ye başarılı bir şekilde gerçekleştirilmiş ve her iki sistem de etkisiz hale gelmiştir.

5.1.4. MitM saldırısı

Saldırı analizlerinin ikinci kısmında MitM saldırısı gerçekleştirilmiş ve Şekil 5.28'de belirtilen aşamalar takip edilmiştir. Bu kapsamda, öncelikle ağ taranarak MitM saldırısının gerçekleştirilmesi için ARP zehirlenmesi yapılacak hedef PLC ile PLC'nin haberleştiği bilişim sistemi tespit edilmesi, ikinci olarak saldırı gerçekleştirilerek PLC'nin haberleşmesinde araya girilerek hassas bilgilerin elde edilmesi, son olarak da ARP tablosunun sürekli kontrolüne dayalı uyarı sistemi ve splunk saldırı tespit sisteminin görsel log ekranının kullanılması ile de benzer bir saldırı anında sistemin zarar görmemesi hedeflenmiştir.



Şekil 5.28. Ortadaki adam (MitM) saldırısı keşif, saldırı ve tespit aşamaları

MitM saldırısı temel olarak, bir saldırgan ve iki kurban (victim) bilgisayar olmak üzere üç sistemden oluşmaktadır. Saldırı; saldırganın ilk mağdur sisteme, ikinci mağdur sistem olduğunu; ikinci mağdur sisteme de ilk mağdur sistem olduğunu belirten sinyaller göndermesiyle başlar. Bu sayede Ortadaki Adam etkisiyle ilk mağdur tüm paketlerini saldırgana gönderir, saldırgan da bu paketleri ikinci mağdura kendi üzerinden iletir. Sahte bağlantı kurulduğunda, mağdur ağ bağlantısını normal olarak kullandığını düşünmektedir.

MitM saldırıları en yaygın olarak Adres Çözümleme Protokolünün açıklıklarından faydalanılarak, ARP zehirlemesi olarak ifade edilen MAC adres bilgilerinin değiştirilmesiyle gerçekleştirilmektedir. İntranet ve İnternet ağlarının yaygınlaşmasına paralel olarak, güvenlik açıklıkları da artmıştır. Özellikle ARP protokolündeki açıklıklar nedeniyle, ARP hileciliğinde büyük bir artış yaşanmaktadır. ARP protokolündeki açıklığın tespitinin üzerinden yaklaşık 30 yıl geçmiştir. Ancak sistemlere zarar verme de hala yaygın olarak kullanılan yöntemlerden birisidir. Bu sonuç ise alınan güvenlik önlemlerinin yetersiz kaldığını göstermektedir [216]. Özellikle günümüzde yaygınlaşan mobil olarak ağa katılımın ve ağdan ayrılmanın ne kadar kolay olduğu düşünüldüğünde, ARP zehirlenmesi ve MitM saldırısının önlenmesinin zorluğu anlaşılmaktadır.

Nam, Djraev ve Park; ARP zehirlemesinden dolayısıyla MitM saldırısından korunmak için MR-ARP (MitM-Resistant Address Resolution Protocol) tekniğini önermişlerdir [216]. Bu teknik kablolu ağlarda, düğümler sabit olduğu için başarılı olabilmektedir. Ancak kablosuz ve mobil ağlarda düğümler sürekli yer değiştirdiğinden başarı oranı oldukça düşük kalmaktadır. MitM saldırılarına karşı korunmak için, Pansa ve Chomsiri MAC-IP veritabanını merkezi olarak kullanan DHCP sunucularının kurulumuna yönelik bir yöntemi çözüm olarak tespit etmişlerdir. Bu yöntemde, her bir kullanıcı arasında MAC adreslerinin iletiminin gerçekleştirilmesi için yeni bir DHCP önerilmektedir [217]. Ancak yaygın olarak kullanılmasına rağmen DHCP'nin yönetimi ve konfigürasyonu oldukça zordur ve bu nedenle uygulanabilir bir yöntem değildir.

ARP hilesinin yapılabilmesinin en büyük nedeni düğümler arasında MAC adresi değişimi yapılırken kimlik doğrulamasının yapılmamasıdır. Bu nedenle tüm ARP paketleri bilgisayar korsanlarının saldırısına uğrayabilir. Hong, Oh ve Lee çalışmalarında, bu saldırıları engellemek maksadıyla, ARP protokolünü korumak için AES ve RSA kriptolama teknikleri kullanılan bir model tasarlamışlardır. Modelde, istemci isteğini MAC dağıtıcısına

ilettiğinde, MAC dağıtıcısı genel RSA anahtarını (açık anahtar) dağıtmaktadır. Buna karşılık istemci AES anahtarını oluşturmaktadır ve bunu açık anahtarla şifrelemektedir. ARP istekleri ve cevap paketleri sürücüler tarafından engellenerek, ARP zehirlenmesi saldırısının etkisizleştirilmesi hedeflenmiştir [218]. Bu koruma yönteminde, istemci tarafı korunmakla birlikte ağ geçidi kısmı tam olarak korunamamakta ve ARP zehirlenmesi saldırılarına karşı hassas durumdadır. Bu nedenle böyle bir saldırı yapıldığında ağ geçidi tüm istemcilere ağın saldırı altında olduğu mesajını iletmektedir. Lootah, MCDaniel ve Enck ise; ARP zehirlenmesine engel olmak amacıyla kriptografi yöntemlerinden yaralanmışlardır. Çalışmada, en yaygın bilinen kriptografi- tabanlı yaklaşımlarından olan Bilet-Tabanlı ARP (Ticked-based ARP(TARP)) kullanılmıştır [219]. Bu çözüm önerisi, ticari ağlara özgü başarı sağlayabilse de EKS'de kriptoloji kullanımın zorluğu dikkate aldığında uygulanmasının çok da mümkün olmadığı anlaşılmaktadır.

Asokan, Niemi ve Nyberg'in çalışmalarının odak noktası ise, TLS tüneli içinde HTTP kimlik doğrulamanın kullanılmasıdır [220]. Ancak bu yöntem tek başına açıklıkları ortadan kaldırmamaktadır. Bu nedenle, istemci kimlik doğrulama protokolünde ve tünel protokolünde kriptolama teknikleri kullanılmaktadır. Oppliger, Hauser ve Basin, SSL/TLS protokolünde sunucuya erişim yapan kullanıcıya ait Kullanıcı Kimlik Doğrulama Kodu (User Authentication Code-UAC) ile kimlik doğrulama yapmasına yönelik bir model önermişlerdir. Modelin amacı; sunucunun sahte kullanıcıyı tanıyarak düşürmesidir [221]. UAC kullanımında, sistemin zararlı yazılımlardan korunmuş olması gereklidir. Aksi takdirde Truva Atı (Trojen) gibi kötücül yazılımlarla yetkili kullanıcıların bilgileri ele geçirilebilir ve sistem saldırılara açık hale gelebilir.

Mobil ağlardaki MitM saldırılarının engellenmesine yönelik yaptıkları çalışmada, Bıçakçı ve diğerleri; Mobil-ID olarak adlandırılan mobil kimlik doğrulama protokolü kullanılması ve kullanıcılardan kaynaklanan hataların güvenlik döngüsü dışında bırakmasıyla MitM saldırılarını önlemeye yönelik bir model önermişlerdir. Çalışmaları, kullanıcının PIN'ini (Personnel Identification Number- Personel Kimlik Numarası) girmesiyle özel anahtarın aktifleşmesine dayanmaktadır. Kullanıcı bir servise girmek istediğinde, servis genel anahtarı gönderip, kullanıcıdan özel anahtarla aktifleştirmesini istemektedir. Geleneksel olarak, MitM saldırılarının kullanıcı kimlik doğrulaması ile engellenemeyeceği ancak sunucu kimlik doğrulaması ile engellenebileceği belirtilmektedir [222]. Bu çözümdeki

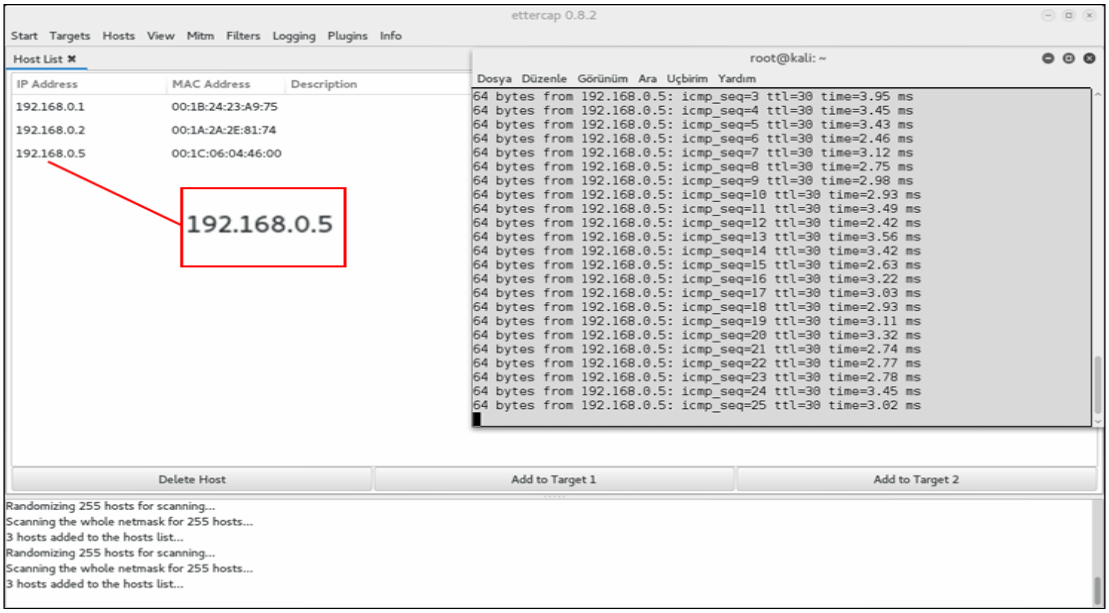
hassas taraf ise, sunucu genel anahtarı güvenilir üçüncü bir taraf tarafından onaylanmasıdır. Bu nedenle, bu üçüncü taraf güvenilir bir kurum/kuruluş olması önemlidir.

Yukarıda belirtilen yöntemler incelendiğinde bütün önlemlerin bilgisayar sistemlerine yönelik olduğu görülmektedir. Ancak söz konusu çözümlerin EKS'de kullanılması sistemler üzerindeki değişikliklerin anlık olarak takip edilmesinin kritikliği önemi değerlendirildiğinde mümkün olmamaktadır. Bu kapsamda, çalışmanın öncelikli hedefi EKS'nin kesintisiz çalışması sağlarken ağ içerisinde MitM saldırısı gerçekleştirilmesi durumunda, saldırının en kısa zamanda tespit edilerek, saldırgan bilgisayarın sisteme müdahalesinin engellenmesidir.

Bir haberleşme altyapısı olarak İnternet büyük çoğunluğu TCP/IP açıklıklarından kaynaklanan birçok tehdide maruz kalmaktadır. Bunun yanında EKS ve özellikle SCADA protokolleri kendi açıklıklarına da sahiptir. Örneğin Modbus/TCP haberleşmesi açık bir şekilde iletilmektedir ve tesis bilgisi, ağ adresleri gibi önemli bilgiler ele geçirilip manipüle edilebilir. Döngüsel Artık Kontrolü (Cylic Redundancy Checking-CRC), veri senkronizasyonu ve çoklu veri biçimlerini içermesine rağmen DNP3 protokolü de güvenlik açıklıklarına sahiptir. DNP3'ün bir türevi olan Güvenli DNP3 oturum anahtarı ile mesaj kaynağını doğrulayan sorgu-cevap (challange-response) kimlik doğrulama sistemini kullanmaktadır ancak pratikte yaygınlaşmamıştır. Bu nedenle endüstriyel kontrol sistemi ağlarında iletilen veri paketleri çoğunlukla şifrelenmediği için ağa erişen ve yeterli donanıma sahip kötü niyetli herhangi birisi ağa ilişkin paketleri ele geçirip içeriğini okuyabilir veya değiştirip tekrar gönderebilir. Siemens PLC'leri programlamak için Simatic TIA Portal yazılımı kullanılmaktadır. TIA Portal ile PLC arasındaki haberleşme ISO-TSAP (International Standards Organization Transport Service Access Point- Uluslararası Standartlar Kurumu Taşıma Hizmeti Erişim Noktası) protokolüne dayanmaktadır. Bu protokolde, PLC'ler ile yapılan haberleşmede veriler herhangi bir şifreleme kullanılmadan açık bir şekilde iletilmektedir [80].

Çalışmada MitM saldırısı öncelikle Şekil 5.2'de görülen topolojideki bölümlendirme yapılmayan ağa gerçekleştirilmiştir. Saldırının ilk aşaması olan tarama aşamasında ağ üzerinde bulunan PLC'lerin adreslerinin tarama sonucunda elde edilmesi hedeflenmiştir. Şekil 5.29'da görüldüğü üzere tarama sonucunda elde edilen ağ adreslerinden 192.168.0.5 IP numarası PLC cihazına aittir.

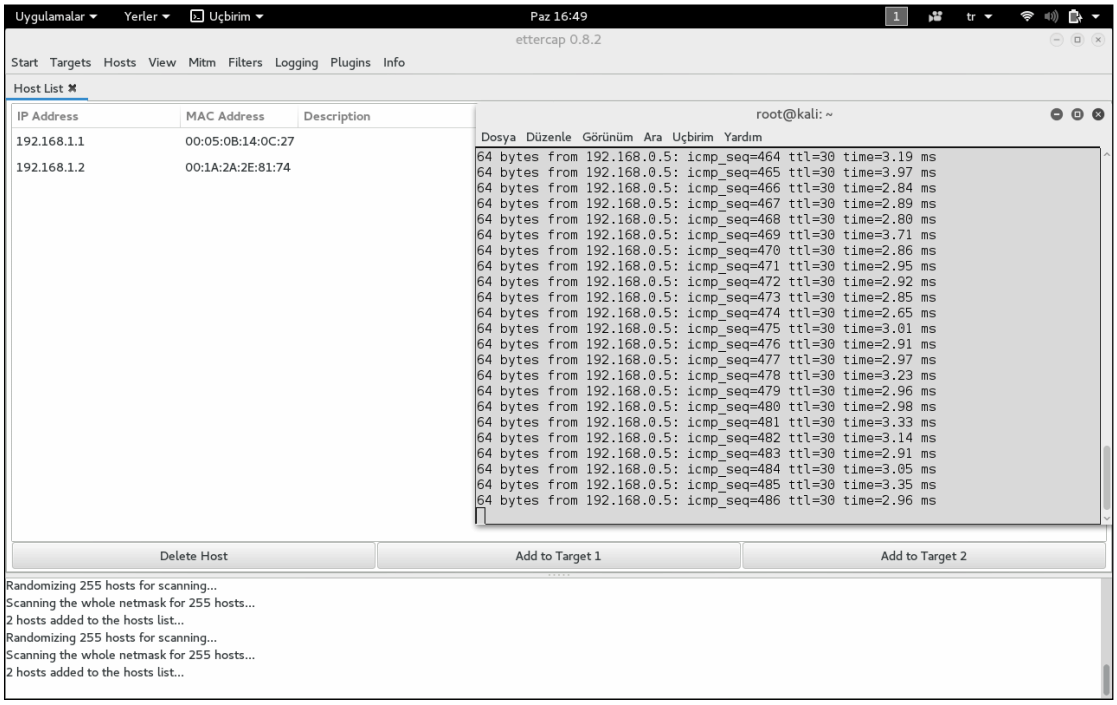
Bölümlendirilmemiş ağda gerçekleştirilen MitM saldırısı sonucunda, PLC cihazına ait Şekil 5.30'da görülen ve her bir cihaz için farklı olan; sunucu oturum kimliği, cihaz seri numarası, cihaza ait model bilgisi ile donanım (firmware) versiyon bilgisi elde edilmiştir. Bu bilgiler kullanılarak açık kaynak araştırması ile cihaza ait önemli açıklık bilgileri bulunabilmektedir. PLC'ye ait bilgilerin yanında ağ üzerinde akan trafiğin yakalanması ile kullanıcılara ait özel bilgilerde elde edilebilmektedir. Endüstriyel kontrol sistemlerinde elektrik kullanım bilgisi akıllı sayaçlarda depolanmakta ve dağıtılmaktadır. Bu nedenle MitM saldırısı ile kolaylıkla ele geçirilmesi halinde kullanıcıların tutum ve davranışları hakkındaki bilgilerin istenmeyen kişilerce kullanılabilmesine yol açabilecektir.



Şekil 5.29. Bölümlendirilmemiş ağ topolojisinde gerçekleştirilen MitM saldırısı

Şekil 5.30. MitM saldırısında elde edilen PLC cihazı bilgileri (Bölümlendirilmemiş ağ)

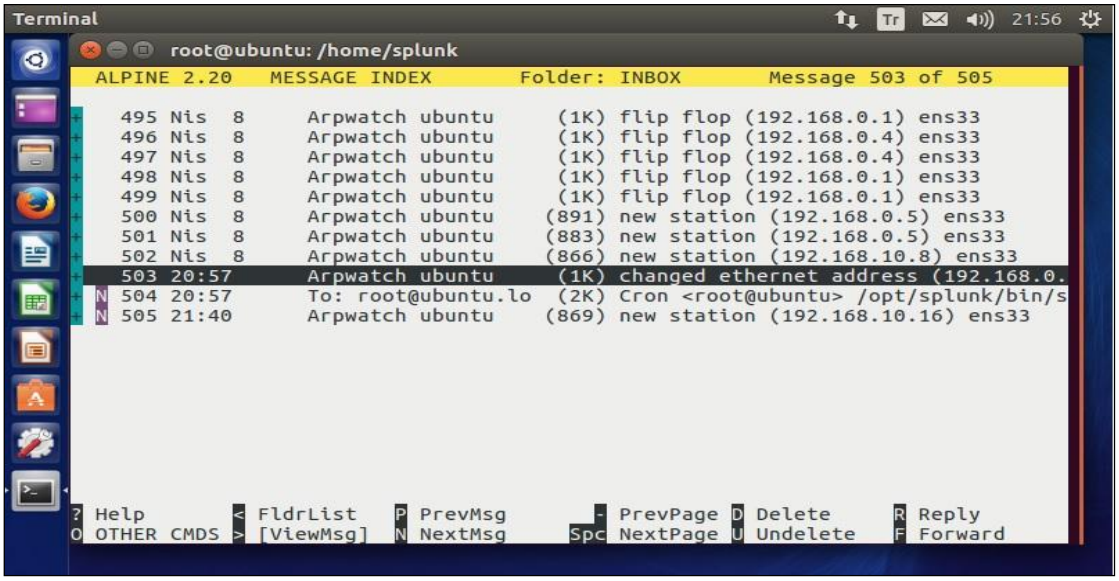
Sınama ortamında MitM saldırısı ikinci olarak Şekil 5.3'de görülen topolojideki bölümlendirme yapılan ağa gerçekleştirmiştir. Şekil 5.31'de görülen ekran görüntüsünde saldırı sonucunda ağ taraması ile elde edilen hedefler incelendiğinde PLC cihazının IP numarasının farklı bir IP grubunda olması nedeniyle tespit edilemediği ve bu nedenle bölümlendirme yapılan ağda PLC'ye MitM saldırısının gerçekleştirilemediği görülmektedir.



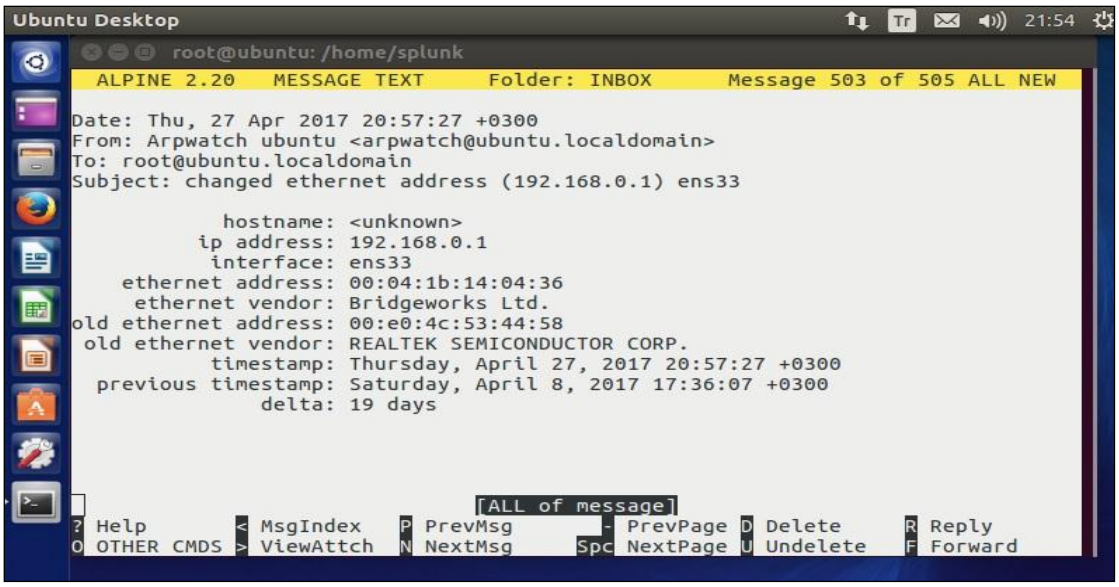
Şekil 5.31. Bölümlendirilmiş Ağ Topolojisinde Gerçekleştirilen MitM Saldırısı

MitM saldırısının tespit aşamasında, Ubuntu (Linux) işletim sistemi üzerinde kurulu olan Arpwatch uygulaması ile ağ üzerinde bulunan cihazlara ait MAC adresleri toplanarak ARP Tablosu oluşturulmuştur. Tablo içerisinde herhangi bir değişiklik (ekleme, değiştirme, vb.) olması durumunda istenilen kullanıcıya (root) uygulamanın (Arpwatch) SMTP Server (send mail özelliği) aracılığıyla e-posta göndermesi sağlanmıştır. Alınan e-postalar Şekil 5.32'deki konsol tabanlı çalışan e-posta istemcisi (Alpine) ile görüntülenmiştir.

Şekil 5.32'de belirtilen saldırı uyarı e-postalarından 503 numaralı uyarı paketinin içeriği Şekil 5.33'de görülmektedir. Paket genel olarak değerlendirildiğinde, saldırganın ağ cihazı (Hub) ile PLC arasına girerek 00:e0:4c:53:44:58 MAC adresine sahip 192.168.0.1 IP adresli ağ cihazının MAC adresini kendi MAC adresi olan 00:04:1b:14:04:36 ile değiştirdiği tespit edilmiştir.

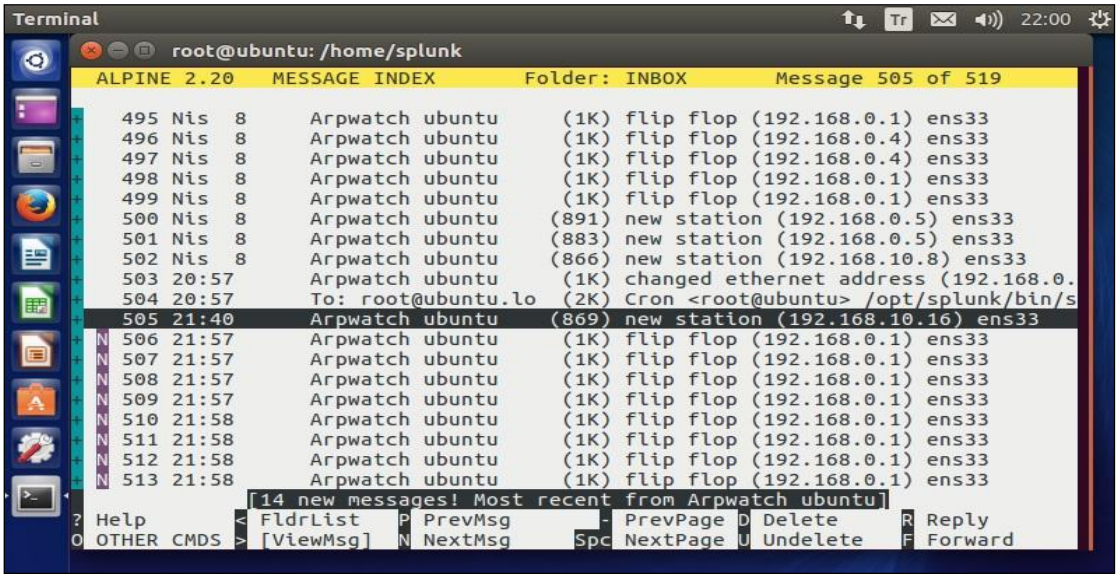


Şekil 5.32. MitM Saldırısının Tespitine Yönelik Linux Alpine Ekranı

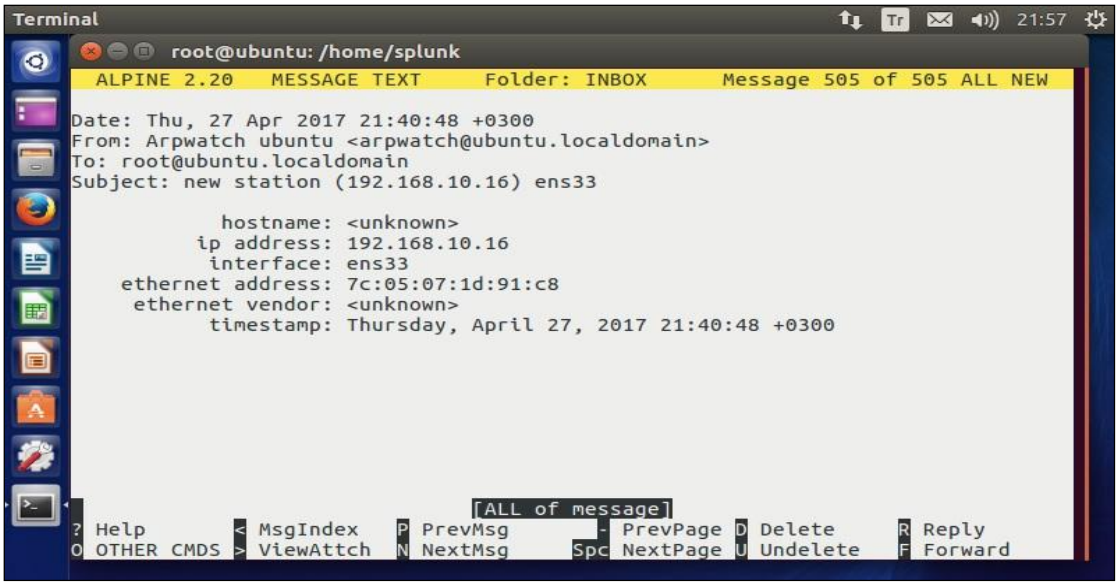


Şekil 5.33. MitM Saldırısının Tespitine Yönelik Paket İçeriği

Arpwatch uygulaması ARP tablosundaki tüm değişikliklerde uyarı üreterek ağ yöneticilerinin incelemesine sunmaktadır. Bu kapsamda, Şekil 5.34'deki ekran görüntüsü MitM saldırısına ait bir uyarı olmayıp ağa yeni eklenen bir donanımın MAC adresini ARP tablosuna yazdırmasına yönelik bir uyarıdır. Ancak bu uyarı türü de ağ yöneticileri için oldukça önemli bir bilgi olup, yasal olmayan ağa girişlerinin tespitinde oldukça etkili olarak kullanılabilmektedir. Örneğin, Şekil 5.35'de yer alan ağa yeni eklenen bileşene yönelik uyarı paketi içeriğinde bileşenin IP (192.168.10.16) ve MAC (7c:05:1d:91:c8) adresleri görülmektedir.

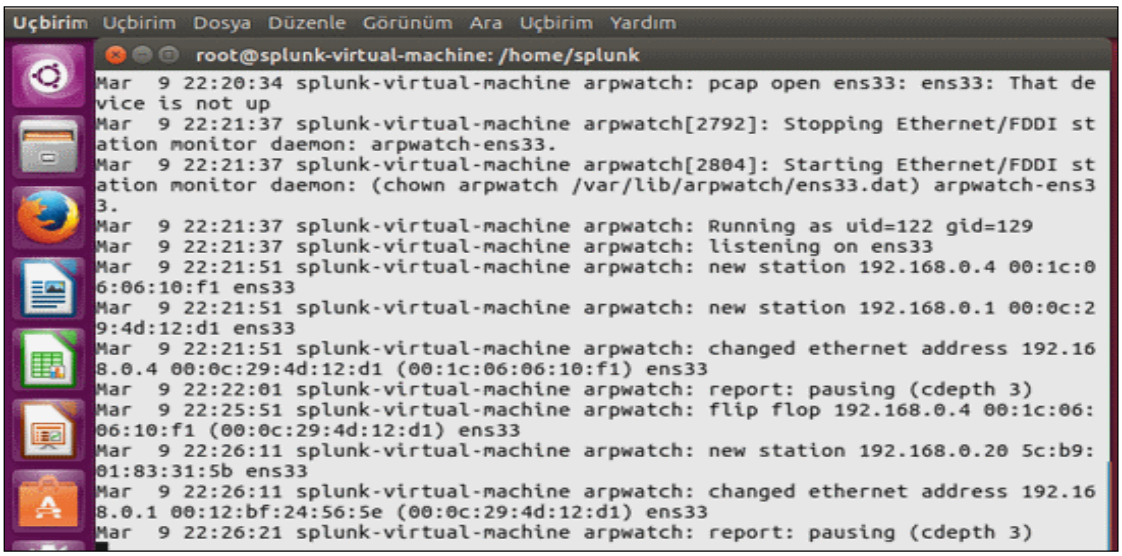


Şekil 5.34. Ağa Yeni bir terminalin eklenmesiyle ARP tablosu değişimi

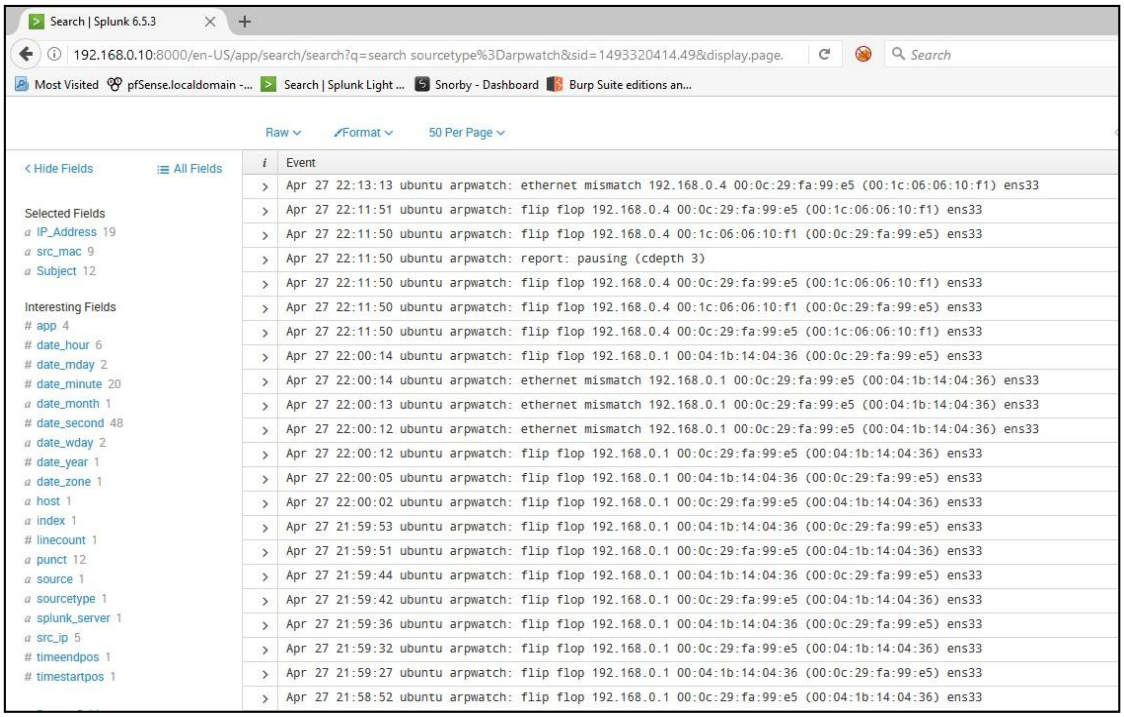


Şekil 5.35. Ağa yeni bir terminalin eklenmesiyle ARP tablosu değişimi paket içeriği

MitM saldırısının tespitine yönelik oluşturulan uyarılar Şekil 5.36'da görüldüğü üzere Linux konsol ekranında listelenebileceği gibi, Şekil 5.37'de yer alan Splunk IDS sisteminin sensörlerinin Ubuntu işletim sistemi ile uyumlandırılması ve MitM uyarı loglarının aktarılması ile daha görsel ve fonksiyonel olarak da takip edilebilmektedir.



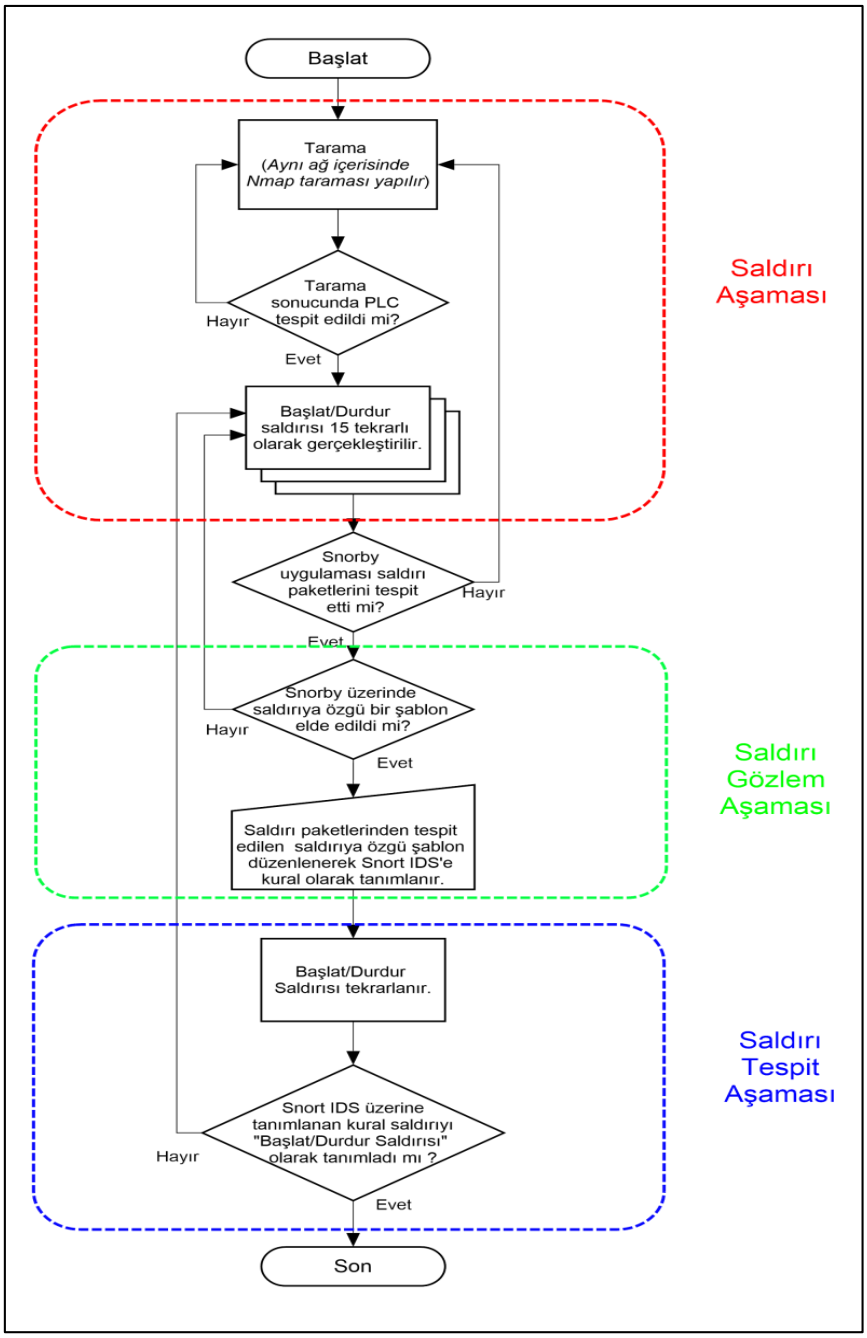
Şekil 5.36. MitM saldırısı sonrası ARP tablosundaki değişimlerin konsol ekranı



Şekil 5.37. MitM saldırısı sonrası ARP tablosundaki değişimlerin Splunk log yönetim ekranı

5.1.5. Başlat/Durdur (Start/Stop) saldırısı

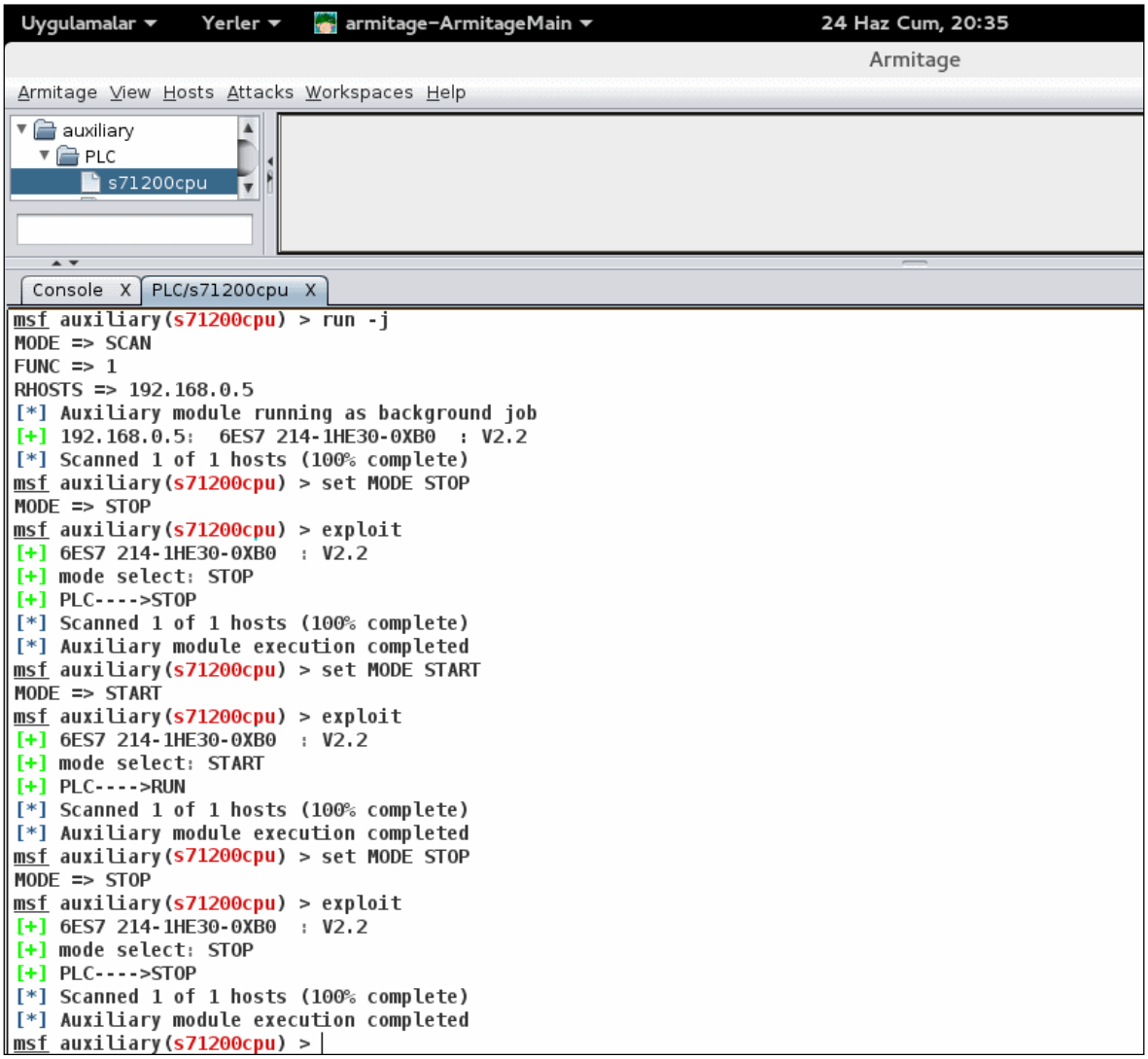
Saldırı analizlerinin son kısmında ise PLC'lere yapılabilecek en önemli ve etkili saldırılardan olan Başlat/Durdur saldırısı Şekil 5.38'de belirtilen aşamalar doğrultusunda gerçekleştirilmiştir. Bu kapsamda, öncelikle Başlat/Durdur saldırısı gerçekleştirilerek saldırıya ilişkin sistemde gerçekleşen değişikliklerin incelenmesi, müteakiben saldırı paketlerinin yakalanması ve analizi ile snort tabanlı kütüphaneye Şekil 5.7 ve Şekil 5.8'de görüldüğü üzere Başlat/Durdur saldırı paketlerinin paternlerinin kural setlerine girilmesiyle Snorby aracılığıyla saldırının tespit edilmesi hedeflenmiştir.



Şekil 5.38. Başlat/Durdur saldırısı keşif, saldırı ve tespit aşamaları

Başlat/Durdur saldırısı aşaması kapsamında, bölümlendirilmemiş ağda bulunan ve okuma/yazma parolası olmayan PLC cihazına, Şekil 5.39'de görüldüğü üzere öncelikle tarama (scan) atağı gerçekleştirilerek, MitM saldırısı sonrasında Wireshark ile elde edilen cihaza ait bilgilerden model bilgisi ile donanım versiyon bilgisi (firmware) elde edilmiştir. Ağ üzerinde bulunan PLC'leri taramak için, Nmap başta olmak üzere herhangi bir port tarama aracı kullanılarak, "~ nmap —script mms-identify.nse —script-args='mmsidentify.timeout= 500' -p 102 <host>" komutu ile 102. portun taranması yeterli

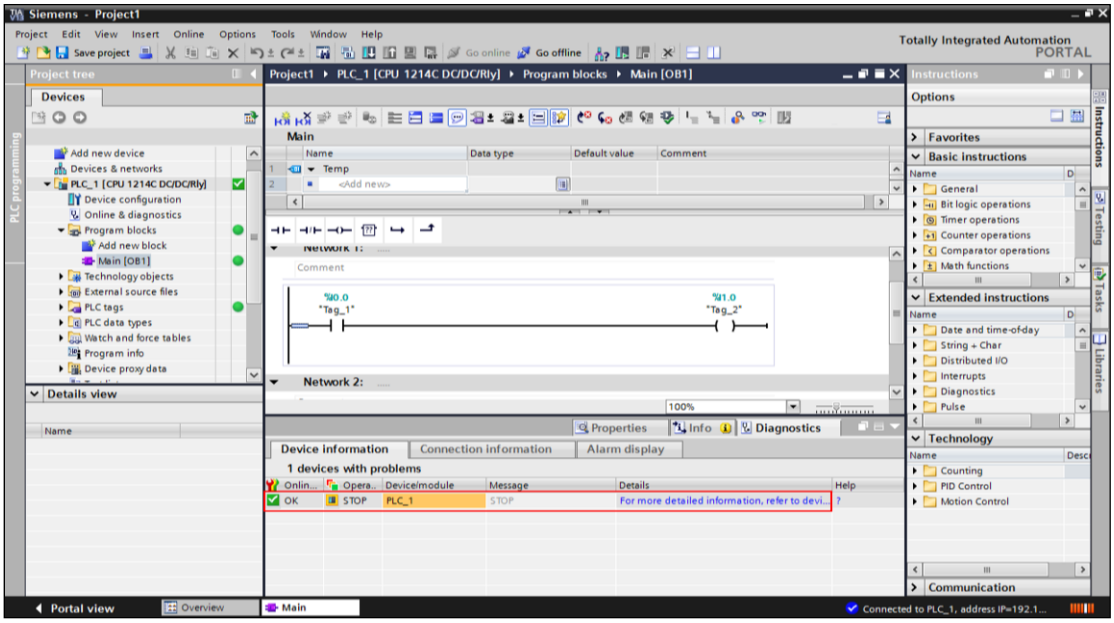
olabilmektedir. Bu sayede ağ üzerinde mevcut olan PLC cihazları ve cihazlara ait IP bilgileri elde edilerek, bu cihazlara yönelik diğer saldırılar gerçekleştirilebilecektir. Bu çalışmada, ağ nmap aracı ile tarandıktan sonra PLC-1 ve PLC-2 donanımlarına ait "192.168.0.4" ve "192.168.0.5" IP adresleri tespit edilmiştir.



Şekil 5.39. Bölümlendirilmemiş ağda Başlat/Durdur saldırısı

PLC'lerin yer aldığı EKS ağı tarandıktan ve ağdaki PLC'ler tespit edildikten sonra, PLC'lere başlat/durdur saldırısı gerçekleştirilmiş ve saldırıların sisteme etkisi izlenmiştir. Saldırı kapsamında, herhangi bir PLC ile bir etkileşim olup olmadığını anlamak için tarama paketi gönderilmiş ve cevap beklenmiştir. PLC'den başarılı taama cevabı geldikten sonra, durdurma komutu aktif olan PLC'ye gönderilmiş ve cihaz durdurulmuştur. Bu komutun sistem üzerindeki etkisini doğrulamak için TIA Portal yönetim ara yüzündeki değişiklik de

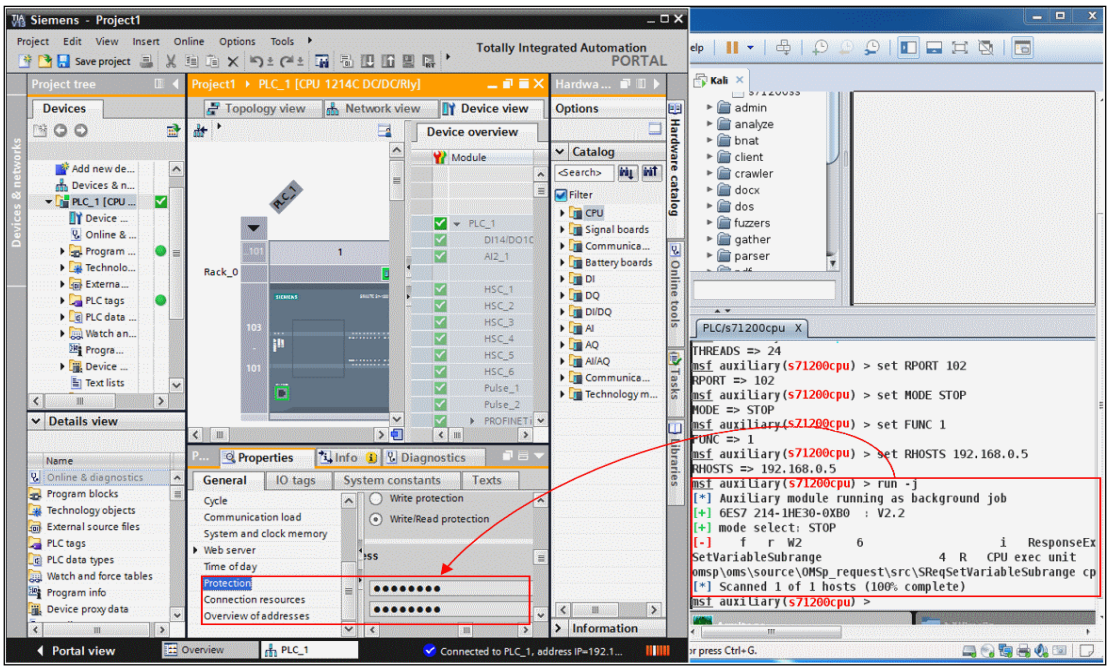
takip edilmiştir. Şekil 5.40'da gösterildiği gibi, durdurma saldırısı gerçekleştirilirken, TIA Portal'da durdurma komutu aktif hale gelmiştir.



Şekil 5.40. Bölümlendirilmemiş ağda Başlat/Durdur atağı (Okuma/Yazma koruması pasif)

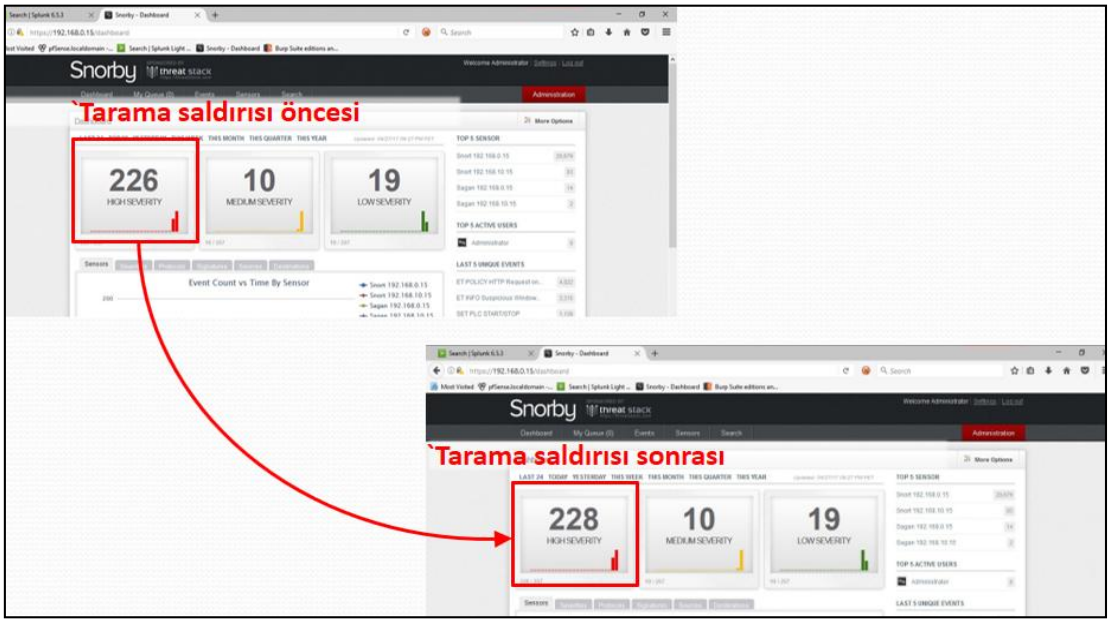
Üçüncü aşamada Başlat/Durdur saldırısı tekrarlı modda gerçekleştirilmiştir. TIA Portalı yazılımı, 10 tekrarlama olarak belirlenen saldırı döngüsü sırasında PLC'ye komuta edememiştir. Tekrar sayısının 1000 tekrar (ya da daha yüksek) gibi yüksek bir değere ayarlanması durumunda, PLC TIA Portal ile uzun süre kontrol edilemez ve yalnızca yeniden başlatma ile PLC'ye yeniden komuta edebilir. Başlat/durdur saldırısı sonucunda, özellikle tekrarlı modda, PLC görevini yerine getirememiştir. Bu bağlamda, PLC'nin anlık tepki verme gereksinimleri dikkate alındığında, başlat/durdur saldırısı nedeniyle kontrol sistemlerinin ağ trafiğinde meydana gelen gecikmenin, önemli sorunlara yol açabileceği görülmüştür.

Başlat/Durdur saldırısının dördüncü aşamasında, PLC'nin okuma/yazma şifresi TIA Portal programı vasıtasıyla etkinleştirilmiş ve PLC'ye Başlat/Durdur saldırısı tekrarlanmıştır. Şekil 5.41'de gösterildiği gibi, PLC'nin okuma/yazma parolasının etkinleştirilmesi halinde, Başlat/Durdur saldırısı sonucunda yalnızca tarama aşaması başarıyla tamamlanmış ancak cihaz durdurma için şifre istediğinden durdur saldırısının başarısız olduğu görülmüştür.



Şekil 5.41. Bölümlendirilmemiş ağda Başlat/Durdur atağı (Okuma/Yazma koruması aktif)

Bölümlendirilmiş ağ topolojisinde Başlat / Durdur atağı denenmesi sonucunda ise okuma/yazma parolasının pasif olması halinde saldırının başarıyla gerçekleştirilebildiği gözlenmiştir.

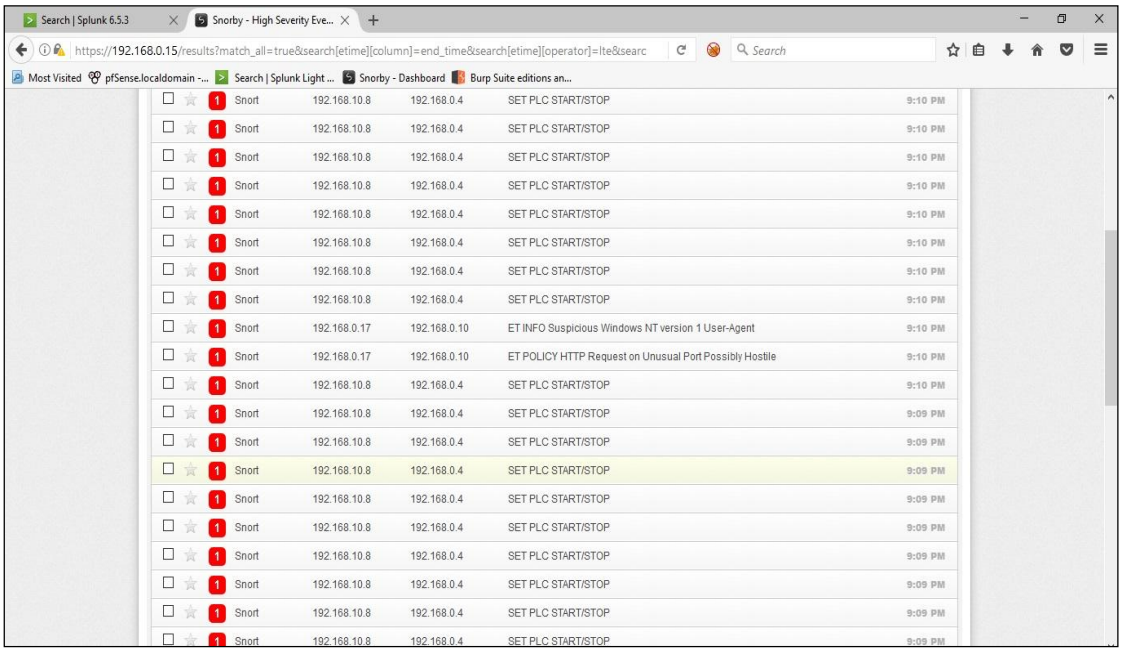


Şekil 5.42. Tarama saldırı aşamasında yüksek seviyeli olay miktarındaki değişim

Başlat / Durdur saldırısının tespit aşamasında, PLC'ye ilk saldırı adımı olan tarama saldırısı gerçekleştirildiğinde, Şekil 5.42'de görüldüğü üzere yüksek seviyeli olay sayısının 226'dan

228’e çıktığı görülmüştür. Artışa neden olan ilk paket, aktif durumda PLC'yi araştıran sorgu paketi iken, ikincisi ise yanıt paketidir. Tarama saldırısının başarılı bir şekilde gerçekleştirildiği bilgileri aldıktan sonra Başlat / Durdur saldırısının gerçekleştirilebileceği anlaşılmıştır.

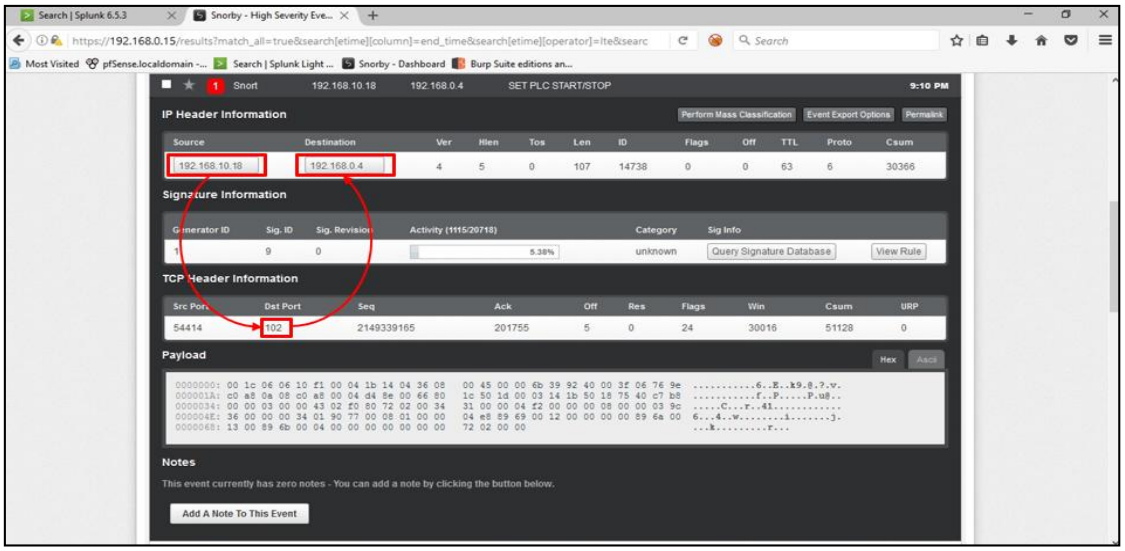
Başlat/Durdur saldırısı tespitinin ikinci aşamasında PLC’ye tekrarlı modda saldırı gerçekleştirildiğinde, Snorby tarafından saldırı imzaları (Bkz. Şekil 5.7 ve Şekil 5.8) ile eşleşen paketler yüksek seviyeli olaylar listesinin yer aldığı Şekil 5.43’de görülmüştür. Şekil 5.43’de yer alan liste incelendiğinde, saldırı tekrarlı olarak uygulandığında toplam “`2n + 2`” kadar olay sayısının arttığı tespit edilmiştir. Bu formülasyonda, n tekrar sayısıdır. Örneğin; 10 tekrarlı bir başlat/durdur saldırısı için toplam 22 adet olay listelenmektedir. 22 olayın, 2 adedi ise “tarama saldırısına”, 10 adedi illegal ``Başlat`` isteklerine ve 10 adedi ise illegal ``Durdur`` isteklerine ilişkindir.



Şekil 5.43. Başlat/Durdur saldırı olay paketleri

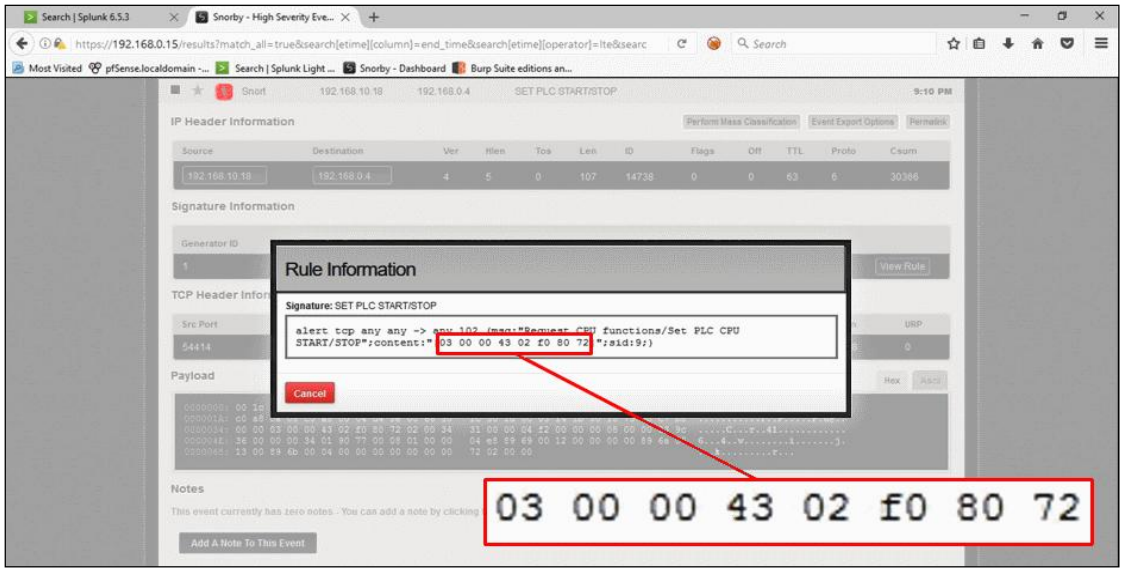
Yüksek seviyeli olaylar listesinde görüntülenen olaylar içerisinde listelenen ve “SET PLC START/STOP” olarak tanımlanan olaya ait paket incelendiğinde, Snorby’nin ortaya çıkan şüpheli paketlerin kaynak ve hedef IP adresleri ile iletişim portunun tanımlanabildiği görülmektedir. Bu kapsamda, Şekil 5.44’de belirtilen paketin 192.168.10.18 IP adresine sahip Kali Linux saldırgan bilgisayarından 192.168.0.4 IP adresine sahip PLC cihazına 102. porttan yapılan Başlat/Durdur saldırısı olduğu görülmektedir.

Kaynak ve hedef IP adreslerini ve kullanılan port numarasını belirlemek, ağ güvenliği uzmanlarına büyük kolaylık sağlayabilir. Başlat/durdur komutlarının yetkili bir kullanıcı (örn., TIA Portal) veya kötü niyetli bir saldırgan tarafından gerçekleştirilip gerçekleştirilmediği belirlenebilir. IP sahtekarlığı veya içeriden birisi (insider) saldırısı dışında, bu bilgiler yetkisiz erişime daha hızlı bir tepki vermeyi sağlayacaktır.



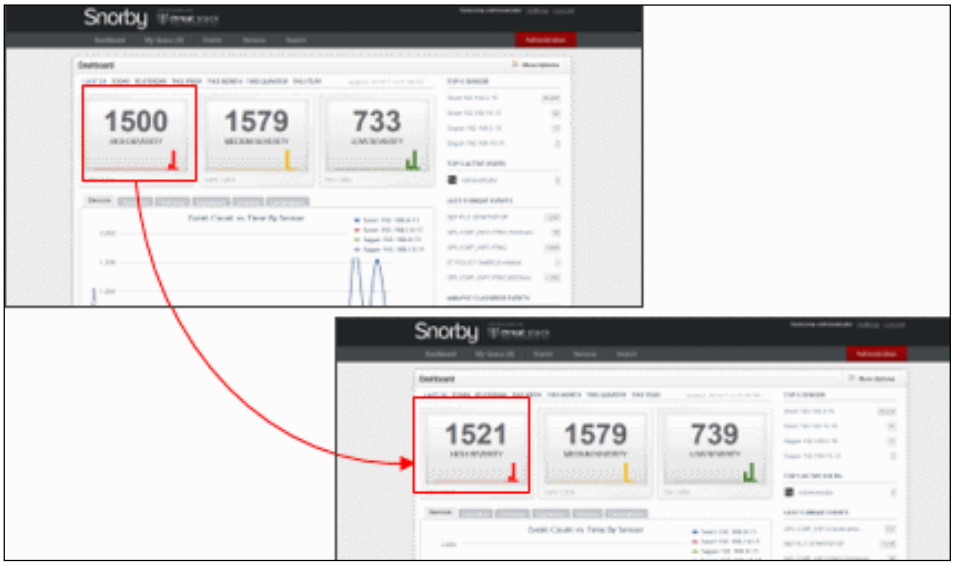
Şekil 5.44. Başlat/Durdur saldırısı olay paketi analizi

Şekil 5.45'de gösterilen listelenmiş bir üst düzey olayın kural bilgisi incelendiğinde, olay paketlerinin Şekil 5.7 ve Şekil 5.8 ile Snorby'de tanımlanan başlat/durdur saldırı paketleri olduğu anlaşılmaktadır.



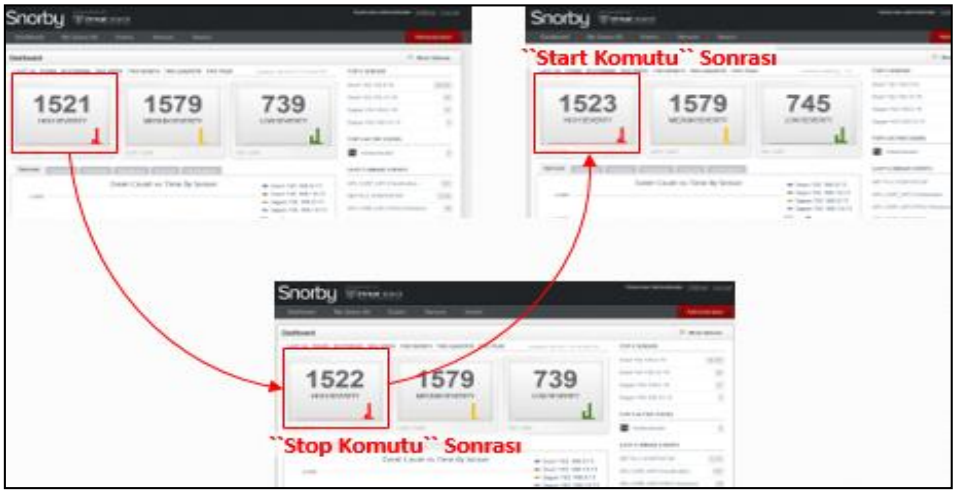
Şekil 5.45. Başlat/Durdur saldırı olay paketinin tespitine ilişkin kural

PLC'lerin kontrolü ve yönetiminin sağlandığı TIA Portal üzerinden PLC'ye çevrim içi/çevrim dışı isteklerinin gönderilmesi sonucunda ise Şekil 5.46'da görüldüğü üzere, yüksek seviyeli olay sayısı 1500'den 1521'e (15 çevrim içi + 6 çevrim dışı) çıktığı görülmüştür.



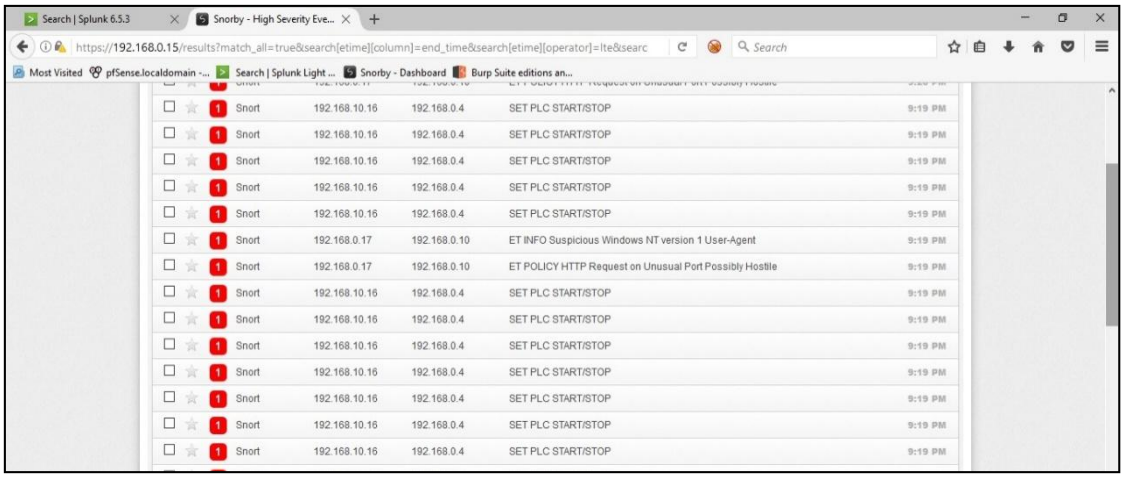
Şekil 5.46. TIA portal üzerinden gönderilen çevrim içi ve çevrim dışı komutları sonrası olay sayısının değişimi

Çevrimiçi halde bulanan PLC'ye TIA Portal üzerinden durdur isteği gönderildiğinde, Şekil 5.47'de görüldüğü üzere, yüksek seviyeli olay sayısının 1521'den 1522'ye, başlat isteği PLC'ye gönderildiğinde ise 1522'den 1523'e (1 durdur paketi + 1 başlat paketi) çıkmıştır.



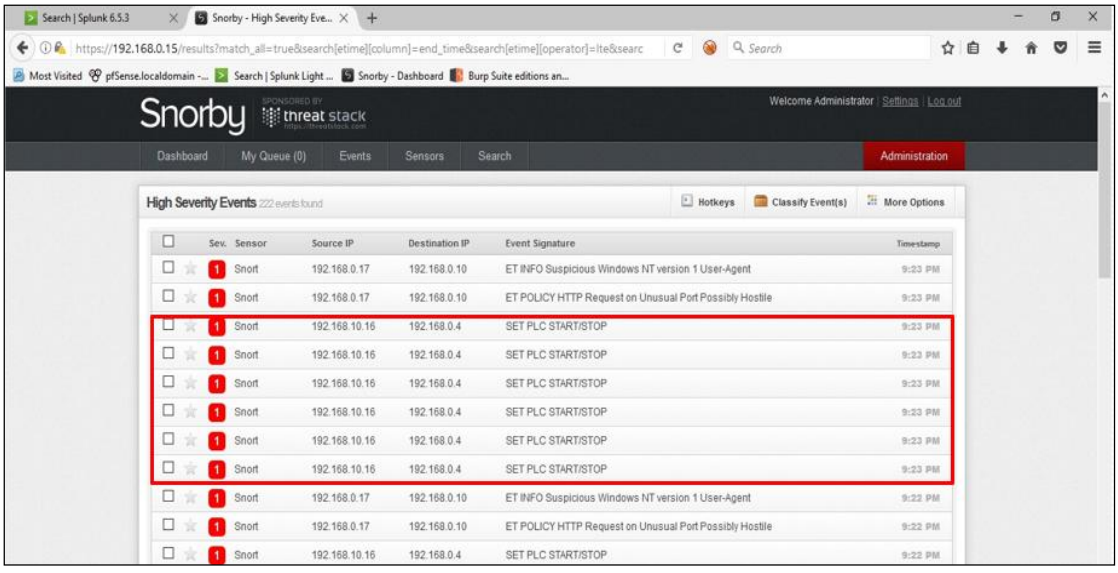
Şekil 5.47. TIA portal üzerinden gönderilen Durdur ve Başlat komutları sonrası olay sayısının değişimi

TIA portal yönetim ara yüzü vasıtasıyla PLC'nin çevrim içi (go online) olması için gönderilen komut, Snorby tarafından davranış şablonunun Başlat/Durdur saldırısı ile benzer olması nedeniyle yüksek seviyeli olaylar listesinde görüntülenmektedir. Olayın davranış şablonu incelendiğinde, PLC cihazının çevrim içi hale getirilmesi için gönderilen komutun "15" benzer paketten oluştuğu tespit edilmiştir (Şekil 5.48).



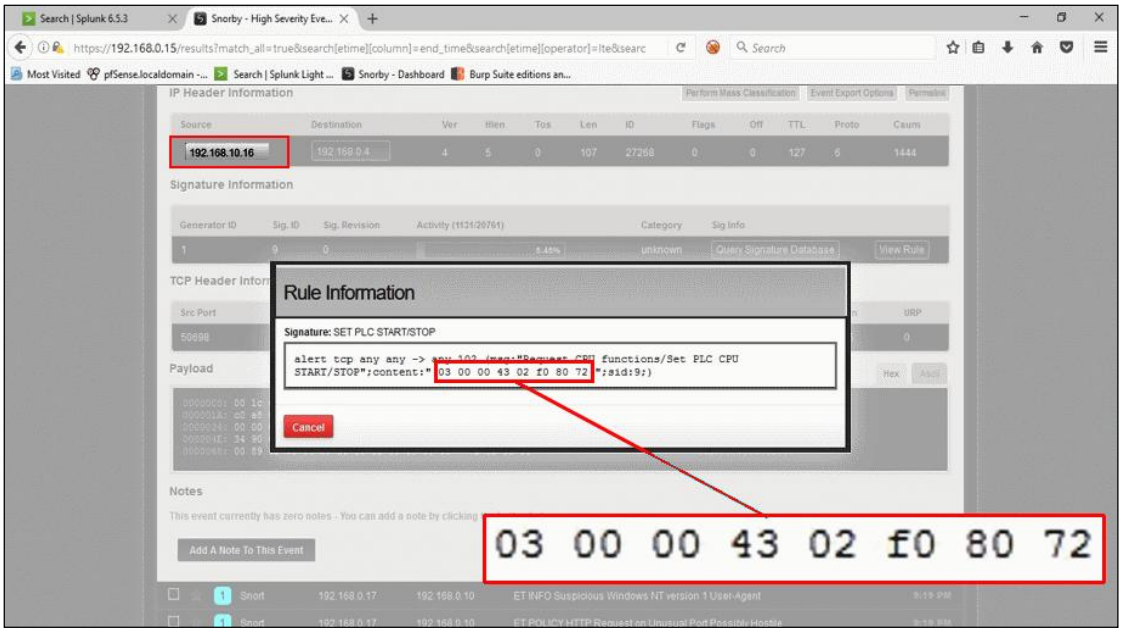
Şekil 5.48. TIA Portal üzerinden çevrimiçi (Go online) komutuna ilişkin paketler

PLC'ye TIA portal yönetim ara yüzü vasıtasıyla çevrim dışı (go offline) olması için gönderilen komuta ilişkin Şekil 5.49'da belirtilen paket içerikleri incelendiğinde ise "6" benzer paketten oluştuğu tespit edilmiştir. Saldırı paketlerini yasal paketlerden ayırmak için sürekli izlemenin ve kalıpların oluşturulmasının önemi ortaya çıkmaktadır.



Şekil 5.49. TIA Portal üzerinden çevrimdışı (Go offline) komutuna ilişkin paketler

PLC'ye TIA portal yönetim ara yüzü vasıtasıyla çevrim içi (go online) olması için gönderilen komutun tespit edilmesinde kullanılan kural bilgisinin yer aldığı Şekil 5.50 incelendiğinde, başlat/durdur saldırısına ait kural bilgisi ile aynı içeriğe sahip olduğu görülmektedir. Paketin kaynak adresi incelendiğinde ise TIA Portal Yönetim arayüzünün kurulu olduğu bilgisayara ait olduğu anlaşılmaktadır.



Şekil 5.50. TIA Portal çevrim içi komutuna ait olay paketinin tespitine ilişkin kural

Bir kontrol bilgisayarı olan TIA Portal tarafından gönderilen yetkili başlat/durdur paketlerinin yakalanması, IDS sisteminin yanlış pozitif (false-positive) alarmı olarak düşünülebilir. Bununla birlikte, başlat/durdur işleminin hassasiyeti değerlendirildiğinde, IDS sistemi, sistem tarafından yetkilendirilmiş olsa bile trafiği tespit etmeli ve kaydetmelidir. Böylece sistem, sürekli olarak ağ trafiğini izleyerek ve saldırı paternleri oluşturarak gerçek bir saldırı ile yasal bir komutu ayırt edebilmelidir. Tespit aşamasının analizinde görüldüğü gibi, farklı kaynaklardan (TIA Portal ve saldırgan PC'ler) yapılan taleplerin paterni sürekli izleme süreci ile elde edilebilir. Dolayısıyla, bu modeller benzer saldırıları önlemek için herhangi bir güvenlik aygıtına (güvenlik duvarı, ağ erişim denetimleri-NAC, e-posta ağ geçidi (e-mail gateway), vb.) kara (black-yasaklı) listelerine girebilir.

5.2. Analiz ve Çıkarımlar

Analizler kapsamında gerçekleştirilen saldırılar ve başarı durumları Çizelge 5.1'de görülmektedir. Çizelge 5.1 değerlendirildiğinde, saldırı uygulaması üç gruba ayrılabilir. İlk iki grup, ağ topolojisinin segmentasyonuna (bölümlü ve bölünmemiş) ve üçüncüsü ise okuma / yazma şifresinin etkin veya pasif hale getirilmesiyle ilgilidir.

Sınama ortamında ilk olarak bölümlendirmenin yapılmadığı ağa gerçekleştirilen saldırılarda, saldırıların tamamı başarılı olmuş ve PLC gibi Endüstriyel Kontrol sistemlerinin önemli bir bileşeninin önemli açıklıklara sahip olduğu görülmüştür. İkinci aşamada ise saldırılar bölümlendirmenin yapıldığı ağ topolojisine gerçekleştirilmiştir. Bölümlendirmenin yapıldığı ağ topolojisine sahip ağa yapılan saldırıların sonucunda ise MitM saldırısı hariç diğer saldırılar başarıyla gerçekleştirilmiştir. MitM saldırısının sonucunda, ağda iletilen verilerin açık bir şekilde iletilmesi ve sistemde oluşabilecek olumsuz etkiler dikkate alındığında, ağ bölümlendirmesinin önemi daha iyi anlaşılmaktadır.

Saldırı analizinin son aşaması olan üçüncü aşamasında, PLC'ye başlat/durdur saldırısı gerçekleştirilmiştir. Analiz kapsamında öncelikle TIA Portal programı tarafından PLC'ye okuma/yazma koruma şifresi aktive edildiğinde Başlat/Durdur saldırısının gerçekleştirilemediği ancak diğer saldırıların başarılı olduğu görülmüştür. Sistemlerin çalışmaması gerektiği bir anda çalıştırılması ya da çalışması gerektiği bir anda durdurulması hayati önemli sonuçlar doğurabilecektir. Bu test sonucunda, okuma/yazma parolasının aktif edilmesinin ve sadece yetkili personel tarafından bilinmesinin, sonuç olarak parola yönetimin etkin bir şekilde uygulanmasının önemi görülmüştür.

Sistem yöneticileri, TIA Portal uygulamasının yüklü olduğu kontrol bilgisayarlarına daha kolay erişebilir ve bu nedenle, TIA Portala yönelik saldırılar çok daha kolay ve hızlı tespit edilebilir ve gerekli tedbirler alınabilir. Ancak, PLC'lere yapılan saldırıları tespit etmek çok daha uzun sürebilmektedir. Çünkü PLC'ler uzakta bulunan RTU ve IED gibi alan cihazları oldukları için, saldırılar belirtilerini sistem yöneticilerin fark etmesi mevcut altyapılarda çok zordur. PLC'lere yönelik siber saldırılar STUXNET örneğinde de yaşandığı üzere sıklıkla saldırıdan sonra hayati sonuçlar meydana geldiğinde fark edilmektedir. Bu amaçla, çalışmada saldırı sonuçlarının çok daha yıkıcı olması nedeniyle PLC'ler saldırı senaryolarında hedef olarak seçilmiştir.

Saldırıların tespitine ilişkin analizler değerlendirildiğinde, aynalama (mirroring) yöntemi ile ağda akan trafiğin tamamı analiz etmek paket analiz yazılımı ile yakalanmış ve ağdaki anomaliliklere yönelik paketlerin içerikleri değerlendirilmiştir. Aktif saldırıların tespiti kapsamında; Smoothsec sistemine kural olarak girilmesi ile de Başlat/Durdur saldırısı başarılı bir şekilde tespit edilerek, yüksek seviyeli olay kısmında yer almıştır. IP sahteciliği yapılarak Bogon IP adresleri üzerinden gerçekleştirilen DoS saldırısı da yine Smoothsec sistemi ile başarılı bir şekilde tespit edilerek, orta seviyeli olay kısmında görüntülenmiştir.

Pasif bir saldırı olarak nitelendirilen Ortadaki Adam saldırısına yönelik olarak ise Ubuntu işletim sistemi üzerine kurulu olan arpwatch uygulaması ile ağ üzerindeki herhangi bir cihaza ilişkin paketlerin dinlenmesi amacıyla arp zehirlemesi yapılması durumunda arpwatch uygulaması aracılığı ile sistem yöneticisine e-posta atılması, konsol üzerinden veya Splunk log yönetim arayüzü üzerinden görüntülenmesi sağlanmıştır.

Çizelge 5.1. Saldırı/tespit sonuçları

Saldırı Türü	Bölümlendirilmemiş Ağ Topolojisi	Bölümlendirilmiş Ağ Topolojisi	Okuma/Yazma Korumalı PLC	SmoothSec	Splunk
Port Tarama	✓	✓	✓	✓	-
DoS	✓	✓	✓	✓	-
MitM	✓	X	✓	-	✓
Başlat/Durdur	✓	✓	X	✓	-

5.3. Analiz Sonuçları

Çalışmanın PLC analizi bölümünde, kritik bir cihazın önemli bilgileri, EKS'nin iletişim protokollerinde paketlerin iletilmesi ya da alınmasında çoğunlukla şifreleme kullanılmaması nedeniyle, Kali Linux işletim sistemi ve Wireshark gibi ücretsiz erişilebilir analiz programları kullanılarak elde edilebilmiştir. Korumasız endüstriyel protokollerin açıklıklarına yönelik gerçekleştirilecek hedefli saldırılar nedeniyle ciddi fiziksel tehlikeler ortaya çıkabilir. PLC'nin güvenlik açıklarına dikkat çekmek için sınama ortamında MitM, DoS, Port Tarama ve Başlat/Durdur saldırıları gerçekleştirilmiştir. Saldırıların sonuçları, PLC'lerin bu saldırılara karşı savunmasız olduklarını ve PLC'ler gibi kritik cihazlar için ağ bölümlendirmesi ve şifre korumasının hayati önem taşıdığını göstermiştir. Saldırıların tespit

aşamasına yönelik analiz sonuçları ise PLC'lere yönelik haberleşme trafiğinin sürekli izlenmesinin, gerçekleştirilebilecek muhtemel saldırıların tespit edilmesi ve önlem alınmasında önemli katkılar sağlayabileceğini göstermiştir.

6. SONUÇ

Bu çalışmada, kritik altyapıların yönetiminde kullanılan ve toplum hayatı için çok önemli olan ve akıllı şebekelerin merkezinde yer alan EKS'nin zafiyetleri analiz edilmiştir. Analizler kapsamında, EKS'nin önemli bir bileşeni olan PLC'ler hedef cihazlar olarak seçilmiştir. Çünkü PLC'ler coğrafi olarak dağıtılmış saha cihazlarıdır, bu nedenle bu saldırıların fiziksel olarak tespit edilmesi çok zordur. Bu kapsamda, PLC'lerin güvenlik açıklarına dikkat çekmek için sınama ortamında gerçekleştirilen hedef odaklı saldırılar (MitM, DoS, Port Tarama ve Başlat/Durdur) gerçekleştirilmiştir. Saldırı analizi sonuçları, PLC'lerin bu saldırılara karşı savunmasız olduklarını ve PLC'ler gibi kritik cihazlar için ağ bölümlendirmesi ve şifre korumasının hayati önem taşıdığını göstermiştir. Ayrıca, EKS protokollerinde çoğunlukla şifreleme kullanılmaması nedeniyle, trafik analizörleri vasıtasıyla PLC'lere yönelik önemli bilgiler elde edildiği görülmüştür.

Sınama ortamında Siemens S-7 1200 PLC cihazları kullanılmıştır. Bununla birlikte, benzer uygulamalar beşinci bölümde açıklanan saldırı, gözlem ve tespit aşamalarını takip ederek diğer marka ve modellere uygulanabilir. Bu sistemlerin hızlı gelişimi, hazır ticari ürünlerin (COTS) kullanımı ve ModBUS / TCP veya Profinet / TCP gibi hibrit entegre protokollerin geliştirilmesi ve üretkenliği ve verimliliği arttırmak için internet veya intranet bağlantısı kullanılması, PLC'ler dahil olduğu EKS ve bileşenlerini çeşitli siber saldırılara karşı savunmasız hale getirmiştir. Bu nedenle, çalışmanın analiz aşamalarını diğer marka ve model PLC'lere uygulayarak, bu PLC'lerin güvenlik açıklarını bulmak ve bunları kullanmak mümkündür.

Çalışmanın tespit aşamasında ise içerisinde Snort, Snorby, Barnyard, Sagan gibi ağ güvenliği araçlarını içinde barındıran ve saldırıların tespiti maksadıyla geliştirilen bir Linux dağıtımı olan SmoothSec sistemi kullanılmıştır. EKS'nin en önemli gereksinimi olan sürekliliği korumak amacıyla, sisteme ek yük getirmeden aynalama tekniği ile tüm paketlerin örneği tespit sistemine aktarılarak analizler gerçekleştirilmiştir. Analizlerin tespit aşaması, ağ trafiğinin sürekli izlenmesinin muhtemel saldırıların tespit edilmesi ve müteakiben önlem alınmasında önemli katkılar sağlayabileceğini göstermektedir. İmza tabanlı engelleme sistemleri ile (mevcut antivirüs ve IPS sistemleri) bilinen siber saldırılara karşı büyük oranda başarı sağlanıp sistemin güvende olduğu düşünülse de, söz konusu sistemler her saniye ortaya çıkan yeni kötücül (malicious) yazılımlara ve özellikle sıfırıncı

gün açıklıklarına karşı yeterince etkili olamamaktadır. Bu nedenle, ağ trafiğinin izlenmesi, sistem normlarının ve eşik değerinin belirlenmesi sonucu norm dışındaki davranışlarda çalışmada kullanılan saldırı tespit sistemleri ve benzeri sistemler ile sistem yöneticileri/güvenlik uzmanlarının uyarılması sağlanabilecektir. Bu sayede, EKS'lerin en önemli güvenlik bileşeni olan süreklilik boyutu kapsamında yasal paketlerin geciktirilmeden gönderilmesi ve engellenmemesi sağlanırken, kötücül paketlerin sisteme sızması ve zarar vermesi önlenebilecektir. Analizlerin en önemli boyutu, sürekli izleme, normale uygun olmayan (anormal) paketlerin tespiti, saldırı imzasının ve paterninin oluşturulması ve benzer atakların tespiti için uyarı üretilmesi diğer PLC'lere de başarılı bir şekilde uygulanabilir. Böylece, bu açıklıklara karşı önlemler almak ve saldırganların yeniden istismar etmesini önlemek mümkün olacaktır. Çalışmada gerçekleştirilen deneyler; endüstriyel kontrol ağlarına özgü güncel IDS kural dizilerinin eklenmesi şartıyla, derinliğine savunmanın bir bileşeni olarak açık kaynak kodlu IDS'lerin kullanılmasının endüstriyel ağların siber güvenliğine önemli katkılar sağlayacağını göstermiştir.

Akıllı şebekelerde dahil olmak üzere haberleşme sistemleri güvenliğinin önemli bir bileşeni ve genellikle dikkate alınmayan ya da unutulan unsuru insan bileşenidir. Bir zincirin en zayıf halkası kadar kuvvetli olduğu dikkate alındığında, bilgi güvenliği zincirinin de en zayıf bileşeni (halkası) kullanıcılar olarak da adlandırılan insan boyutudur. Bu amaçla, personel güvenliği, yetkilendirmeler, eğitim ve farkındalık teknolojik önlemler ve kurum güvenlik politikaları kadar dikkate alınması gereken kurumsal hedeflerden olmalıdır. Bu sayede alınan teknik önlemler ve güvenlik politikaları etkinlik kazanarak hedeflenen bilgi güvenliği seviyesine ulaşılabilecektir.

Sonuç olarak, günlük yaşantımızda bize büyük faydalar sağlayan EKS'nin güvenliği gözle görülür problemler karşımıza çıkana kadar unutulan ya da umursanmayan önemli bir husustur. Çağımızın en değerli varlığının bilgi olduğu, bilgeye sahip olanın güce, üstünlüğe sahip olduğu dikkate alındığında, bireyler, kurumlar ve ülkeler arasındaki mücadelenin de bilgiye (özellikle de kritik bilgiye) hakim olma, bilgiyi elde etme üzerine olacağı görülmektedir. Sözkonusu hakimiyeti sağlamak için sistemin açıklıklarını bilmek ve ihtiyaç duyulan önlemleri zamanında olmak gerekmektedir. Bu amaçla, kritik altyapıların güvenlik açıklarını belirlemek için, gerçek sistemleri örnekleyen bir sınama ortamı oluşturmak hayati önem taşır. Endüstriyel kontrol sistemlerinin en önemli fonksiyonu olan iş sürekliliği dikkate alınarak ve bu amaçla mevcut sisteme ilave yük getirmeden sürekli izlenebilirliği

gerçekleştirilerek, söz konusu sınama ortamı üzerinde yapılacak güvenlik analizleri sonucunda edinilen bilgilere göre iyileştirme prosedürleri uygulandığı takdirde, kritik altyapıların siber saldırılardan en az hasarla kurtulması ve mümkün olan en kısa zamanda tekrar faal hale getirilmesi sağlanabilecektir.

KAYNAKLAR

1. Shancang, L., Theo, T. ve Honglei, L. (2016). The Internet of Things: a security point of view. *Internet Research*, 26(2), 337-359.

2. Mallouhi, M., Al-Nashif, Y., Cox, D., Chadaga, T., ve Hariri, S. (2011). *A testbed for analyzing security of SCADA control systems (TASSCS)*. ISGT 2011, Anaheim, CA, United States, 1-7.

3. Genge, B., Siaterlis, C., Nai Fovino, I., ve Masera, M. (2012). A cyber-physical experimentation environment for the security analysis of networked industrial control systems. *Computers & Electrical Engineering*, 38(5), 1146-1161.

4. Erol-Kantarci, M. ve Mouftah, H. T. (2013). Smart grid forensic science: applications, challenges, and open issues. *The Institute of Electrical and Electronics Engineers Communications Magazine*, 51(1), 68-74.

5. Zhu, B., Joseph, A. ve Sastry, S. (2011). *A Taxonomy of Cyber Attacks on SCADA Systems*. International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 380-388.

6. Almalawi, A., Yu, X., Tari, Z., Fahad, A., ve Khalil, I. (2014). An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems. *Computers & Security*, 46, 94-110.

7. Pidikiti, D. S., Kalluri, R., Kumar, R. K. S., ve Bindhumadhava, B. S. (2013). SCADA communication protocols: vulnerabilities, attacks and possible mitigations. *Computer Society of India's Transactions on Information and Communication Technologies*, 1(2), 135-141.

8. Yang, Y., McLaughlin, K., Littler, T., Sezer, S., ve Wang, H. F. (2013). *Rule-based intrusion detection system for SCADA networks*. 2nd IET Renewable Power Generation Conference (RPG 2013), Beijing, China, 1-4.

9. Jain, P. ve Tripathi, P. (2013). SCADA security: a review and enhancement for DNP3 based systems. *Computer Society of India's Transactions on Information and Communication Technologies*, 1(4), 301-308.

10. İnternet: Dell Security (2016). Annual Threat Report. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.netthreat.co.uk%2Fassets%2Fassets%2Fdell-security-annual-threat-report-2016-white-paper-197571.pdf&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

11. Nai Fovino, I., Carcano, A., Masera, M., ve Trombetta, A. (2009). An experimental investigation of malware attacks on SCADA systems. *International Journal of Critical Infrastructure Protection*, 2(4), 139-145.

12. Kirsch, J., Goose, S., Amir, Y., Wei, D., ve Skare, P. (2014). Survivable SCADA Via Intrusion-Tolerant Replication. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid*, 5(1), 60-70.

13. Pauna, A. ve Moulinos, K. (2013). Window of exposure… a real problem for SCADA systems? *Recommendations for Europe on SCADA patching*. The European Union Agency for Network and Information Security (ENISA), 1-19.

14. Slay, J. ve Miller, M. (2008). *Lessons Learned from the Maroochy Water Breach*. International Conference on Critical Infrastructure Protection (ICCIP), Hanover, NH, United States, 73-82.

15. Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *The Institute of Electrical and Electronics Engineers Security & Privacy*, 9(3), 49-51.

16. Disso, J. P., Jones, K. ve Bailey, S. (2013). *A Plausible Solution to SCADA Security Honeypot Systems*. Eighth International Conference on Broadband and Wireless Computing, Communication and Applications, Compiegne, France, 443-448.

17. Gellings, C. W., Samotyj, M. and Howe, B. (2004). The future's smart delivery system (electric power supply). *The Institute of Electrical and Electronics Engineers Power and Energy Magazine*, 2(5), 40-48.

18. Farhangi, H. (2010). The path of the smart grid. *The Institute of Electrical and Electronics Engineers Power and Energy Magazine*, 8(1), 18-28.

19. Amin, S. M. ve Wollenberg, B. F. (2005). Toward a smart grid: power delivery for the 21st century. *The Institute of Electrical and Electronics Engineers Power and Energy Magazine*, 3(5), 34-41.

20. Clements, S. ve Kirkham, H. (2010). *Cyber-security considerations for the smart grid*. The Institute of Electrical and Electronics Engineers PES General Meeting, Providence, RI, United States, 1-5.

21. Hauser, C. H., Bakken, D. E. ve Bose, A. (2005). A failure to communicate: next generation communication requirements, technologies, and architecture for the electric power grid. *The Institute of Electrical and Electronics Engineers Power and Energy Magazine*, 3(2), 47-55.

22. Fan, J. ve Borlase, S. (2009). The evolution of distribution. *The Institute of Electrical and Electronics Engineers Power and Energy Magazine*, 7(2), 63-68.

23. Baumeister, T. (2010). Literature Review on Smart Grid Cyber Security; *Department of Information and Computer Sciences University of Hawaii*, Honolulu, HI, 1-34.

24. Lo, C. H. ve Ansari, N. (2012). The progressive smart grid system from both power and communications aspects. *The Institute of Electrical and Electronics Engineers Communications Surveys & Tutorials*, 14(3), 799-821.

25. Hong, S. and Lee, M. (2010). *Challenges and Direction toward Secure Communication in the SCADA System*. 8th Annual Communication Networks and Services Research Conference, Montreal, QC, Canada, 381-386.

26. Patel, S. C. ve Yu, Y. (2007). Analysis of SCADA security models. *International Management Review*, 3(2), 68-76.

27. Gungor, V. C. ve Lambert, F. C. (2006). A survey on communication networks for electric system automation. *Computer Networks*, 50(7), 877-897.

28. Liu, E., Chan, M. L., Huang, C. W., Wang, N. C. ve Lu, C. N. (2010). *Electricity grid operation and planning related benefits of advanced metering infrastructure*. 5th International Conference on Critical Infrastructure (CRIS), Beijing, China, 1-5.

29. Aravinthan, V., Namboodiri, V., Sunku, S. ve Jewell, W. (2011). *Wireless AMI application and security for controlled home area networks*. The Institute of Electrical and Electronics Engineers Power and Energy Society General Meeting, Detroit, MI, United States, 1-8.

30. Parikh, P. P., Kanabar, M. G. ve Sidhu, T. S. (2010). *Opportunities and challenges of wireless communication technologies for smart grid applications*. The Institute of Electrical and Electronics Engineers PES General Meeting, Providence, RI, United States, 1-7.

31. Metke, A. R. ve Ekl, R. L. (2010). Security technology for smart grid networks. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid,* 1(1), 99-107.

32. Dzung, D., Naedele, M., Hoff, T. P. V. ve Crevatin, M. (2005). Security for ındustrial communication systems. *Proceedings of the The Institute of Electrical and Electronics Engineers,* 93(6), 1152-1177.

33. Von Dollen, D. (2009). NIST on the Smart Grid Interoperability Standards Roadmap *EPRI*, (SB1341-09-CN-0031), United States, 1-184.

34. Zafirovic-Vukotic, M., Moore, R., Leslie, M., Midence, R., ve Pozzuoli, M. (2009). *Secure SCADA network supporting NERC CIP*. The Institute of Electrical and Electronics Engineers Power & Energy Society General Meeting, Calgary, AB, Canada, 1-8.

35. Guerrero, J. M., Vasquez, J. C., Matas, J., Vicuna, L. G. d., ve Castilla, M. (2011). Hierarchical Control of Droop-Controlled AC and DC Microgrids; A General Approach Toward Standardization. *The Institute of Electrical and Electronics Engineers Transactions on Industrial Electronics,* 58(1), 158-172.

36. IEEE. *Guide for Electric Power Substation Physical and Electronic Security* IEEE Standard 1402-2000 (6643126), (2000).

37. Dumont, D. (2010). *Cyber security concerns of Supervisory Control and Data Acquisition (SCADA) systems*. IEEE International Conference on Technologies for Homeland Security (HST), Waltham, MA, United States, 473-475.

38. Rohjans, S., Uslar, M., Bleiker, R., González, J., Specht, M., Suding, T. ve Weidelt, T. (2010). *Survey of Smart Grid Standardization Studies and Recommendations*. First The Institute of Electrical and Electronics Engineers International Conference on Smart Grid Communications, Gaithersburg, MD, United States, 583-588.

39. National Institute of Standards and Technology (NIST) (2001). Advanced Encryption Standard (AES)-FIPS 197; *FIPS*, (0704-0188), Gaithersburg, MD,USA. 1-51.

40. National Institute of Standards and Technology (NIST). *Data Encryption Standard (DES)*, (1999).

41. IEEE. *Standard for information technology-Telecommunications and information exchange between systems-Local and metropolitan area networks-Specific requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control (MAC) Security Enhancements* IEEE Standard 802.11i-2004, (2004).

42. IEEE. *Standard for Local and Metropolitan Area Networks Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands and Corrigendum 1*, IEEE Standard 802.16e-2005 and IEEE Std 802.16-2004/Cor 1-2005 (Amendment and Corrigendum to IEEE Std 802.16-2004), (2006).

43. Bendahmane, A., Essaaidi, M., Moussaoui, A. E., and Younes, A. (2009). *Grid computing security mechanisms: State-of-the-art*. International Conference on Multimedia Computing and Systems, Ouarzazate, Morocco, 535-540.

44. McDaniel, P. ve McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy*, 7(3), 75-77.

45. Allan, K. (2009). Power to the people [power energy saving]. *Engineering & Technology*, 4(18), 46-49.

46. Varalakshmi, P. ve Selvi, S. T. (2013). Thwarting DDoS attacks in grid using information divergence. *Future Generation Computer Systems*, 29(1), 429-441.

47. Mirkovic, J. ve Reiher, P. (2004). A taxonomy of DDoS attack and DDoS defense mechanisms. *SIGCOMM Comput. Commun. Rev.*, 34(2), 39-53.

48. Peng, T., Leckie, C. ve Kotagiri, R. (2004). *Information sharing for distributed intrusion detection systems*. Third International IFIP-TC6 Networking Conference, Athens, Greece, 771-782.

49. Strasser, M., Pöpper, C., Capkun, S., ve Cagalj, M. (2008). *Jamming-resistant Key Establishment using Uncoordinated Frequency Hopping*. IEEE Symposium on Security and Privacy (sp 2008), Oakland, CA, United States, 64-78.

50. Pöpper, C., Strasser, M. ve Capkun, S. (2009). *Jamming-resistant broadcast communication without shared keys*. The 18th Conference on USENIX Security Symposium, Montreal, Canada, 231-248.

51. Chen, W. H. (2012). Online fault diagnosis for power transmission networks using fuzzy digraph models. *The Institute of Electrical and Electronics Engineers Transactions on Power Delivery*, 27(2), 688-698.

52. Hashimoto, Y., Toyoshima, T., Yogo, S., Koike, M., Jing, S., ve Koshijima, I. (2012). Conceptual Framework for Security Hazard Management in Critical Infrastructures. I. A. Karimi and R. Srinivasan (Eds.), *Computer Aided Chemical Engineering*. London: Elsevier, 1266-1270.

53. Cheng, H., Tikkala, V. M., Zakharov, A., Myller, T., ve Jamsa-Jounela, S. L. (2011). Application of the enhanced dynamic causal digraph method on a three-layer board machine. *The Institute of Electrical and Electronics Engineers Transactions on Control Systems Technology*, 19(3), 644-655.

54. Liu, Y., Ning, P. ve Reiter, M. K. (2011). False data injection attacks against state estimation in electric power grids. *ACM Trans. Inf. Syst. Secur.*, 14(1), 1-33.

55. Kuntze, N., Rudolph, C., Cupelli, M., Liu, J., ve Monti, A. (2010). *Trust infrastructures for future energy networks*. The Institute of Electrical and Electronics Engineers PES General Meeting, Providence, RI, USA 1-7.

56. Kent, S. (2000). On the trail of intrusions into information systems. *The Institute of Electrical and Electronics Engineers Spectrum*, 37(12), 52-56.

57. Urias, V., Leeuwen, B. V. ve Richardson, B. (2012). *Supervisory Command and Data Acquisition (SCADA) system cyber security analysis using a live, virtual, and constructive (LVC) testbed*. MILCOM 2012 - 2012 IEEE Military Communications Conference, Orlando, FL, United States, 1-8.

58. Morris, T., Srivastava, A., Reaves, B., Gao, W., Pavurapu, K., ve Reddi, R. (2011). A control system testbed to validate critical infrastructure protection concepts. *International Journal of Critical Infrastructure Protection*, 4(2), 88-103.

59. Ten, C. W., Manimaran, G. ve Liu, C. C. (2010). Cybersecurity for critical ınfrastructures: attack and defense modeling. *ıeee transactions on systems, man, and cybernetics - part a: Systems and Humans*, 40(4), 853-865.

60. Dong, W., Yan, L., Jafari, M., Skare, P., ve Rohde, K. (2010). *An integrated security system of protecting Smart Grid against cyber attacks*. Innovative Smart Grid Technologies (ISGT), Gothenburg, Sweden, 1-7.

61. Jensen, M., Sel, C., Franke, U., Holm, H., ve Nordström, L. (2010). *Availability of a SCADA/OMS/DMS system; A case study*. The Institute of Electrical and Electronics Engineers PES Innovative Smart Grid Technologies Conference Europe (ISGT Europe), Gothenberg, Sweden, 1-8.

62. Arun, R. K. P. ve Selvakumar, S. (2009). *Distributed Denial-of-Service (DDoS) Threat in Collaborative Environment - A Survey on DDoS Attack Tools and Traceback Mechanisms*. The Institute of Electrical and Electronics Engineers International Advance Computing Conference, Patiala, India, 1275-1280.

63. Peng, T., Leckie, C. ve Ramamohanarao, K. (2007). Survey of network-based defense mechanisms countering the DoS and DDoS problems. *Association for Computing Surveys*, 39(1), 1-42.

64. Komura, T., Nagai, Y., Hashimoto, S., Aoyagi, M., and Takahashi, K. (2009). *Proposal of Delegation Using Electronic Certificates on Single Sign-On System with SAML-Protocol*. Ninth Annual International Symposium on Applications and the Internet, Bellevue, WA, United States, 235-238.

65. Cai, Y. and Tang, S. (2008). *Security Scheme for Cross-Domain Grid: Integrating WS-Trust and Grid Security Mechanism*. International Conference on Computational Intelligence and Security, Suzhou, China 453-457.

66. Perlman, R. (1999). An overview of PKI trust models. *The Institute of Electrical and Electronics Engineers Network,* 13(6), 38-43.

67. Thomas, R. J. (2009). Putting an action plan in place. *The Institute of Electrical and Electronics Engineers Power and Energy Magazine,* 7(4), 26-31.

68. Öztemiz, S. ve Yilmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. *Bilgi Dünyası,* 14(1), 87-100.

69. Shaw, R. S., Chen, C. C., Harris, A. L., ve Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education,* 52(1), 92-100.

70. Vural, Y. ve Sağıroğlu, Ş. (2007). *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler*. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansında sunuldu, Ankara.

71. Çifci, H. (2013). *Her yönüyle siber savaş*. Ankara: TÜBİTAK, 224-228.

72. Kiuchi, M. ve Serizawa, Y. (2009). *Security technologies, usage and guidelines in SCADA system networks*. ICCAS-SICE, Fukuoka, Japan, 4607-4612.

73. Cardenas, A. A. ve Moreno, R. (2012l). *Cyber-Physical Systems Security for the Smart Grid*. the Cybersecurity in CyberPhysical Systems Workshop (NISTIR 7916), Gaithersburg, MD,USA, 189-214.

74. Özbilen, A. (2012). *TCP/IP tabanlı dağıtık endüstriyel denetim sistemlerinde güvenlik ve çözüm önerileri.* Doktora Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.

75. National Institute of Standards and Technology (NIST). *NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 1.0*, 1108, (2010).

76. Basso, T. ve Deblasio, R. (2011). *IEEE Smart Grid Series of Standards IEEE 2030 (Interoperability) and IEEE 1547 (Interconnection)*. Grid-Interop, Phoenix Arizona, United States, 1-11.

77. Falk, R. ve Fries, S. (2011). Smart Grid Cyber Security – An Overview of Selected Scenarios and Their Security Implications. *PIK - Praxis der Informationsverarbeitung und Kommunikation,* 34(4), 168-175.

78. Carlson, R., Dagle, J., Shamsuddin, S., ve Evans, R. (2005). A summary of control system security standards activities in the energy sector. *National SCADA Test Bed (NSTB)*, 1-41.

79. North America Electric Reliability Council. *NERC Standard 1300 — Cyber Security*, (2004).

80. Stouffer, K. A., Falco, J. A. ve Scarfone, K. A. (2011). Guide to Industrial Control Systems (ICS) Security-SP 800-82; *National Institute of Standards and Technology (NIST)*. 1-155.

81. Chan, A. C. F. ve Zhou, J. (2013). On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. *The Institute of Electrical and Electronics Engineers Communications Magazine*, 51(1), 58-65.

82. Smart Grid Interoperability Panel Cyber Security Working Group (2010). Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security *NIST Special Publications*, 154, 1-19.

83. İnternet: Shaw, W. T. (2004). SCADA system vulnerabilities to cyber attack. *Electric Energy Online*. URL: http://www.webcitation.org/query?url=http%3A%2F%2Fwww.electricenergy online.com%2Fshow_article.php%3Fmag%3D%26article%3D181&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

84. Ghanaim, A. ve Frey, G. (2011). *Modeling and control of closed-loop networked PLC-systems*. American Control Conference, San Francisco, CA, United States, 502-508.

85. Galloway, B. ve Hancke, G. P. (2013). Introduction to Industrial Control Networks. *IEEE Communications Surveys & Tutorials*, 15(2), 860-880.

86. Campbell, R. J. (2015). Cybersecurity issues for the bulk power system. *Congressional Research Service*, 1-39.

87. Bobat, A., Gezgin, T. ve Aslan, H. (2015). The SCADA system applications in management of Yuvacik Dam and Reservoir. *Desalination and Water Treatment*, 54(8), 2108-2119.

88. Miller, B. ve Rowe, D. (2012). *A survey SCADA of and critical infrastructure incidents*. the 1st Annual conference on Research in information technology, Calgary, Alberta, Canada, 51-56.

89. Sharma, K. L. S. (2011). 12 - Types of automation systems. *Overview of Industrial Process Automation*. London, UK: Elsevier, 153-164.

90. Motta Pires, P. S. ve Oliveira, L. A. H. g. (2006). *Security Aspects of SCADA and Corporate Network Interconnection: An Overview*. International Conference on Dependability of Computer Systems, Szklarska Poreba, Poland, 127-134.

91. Alcaraz, C., Fernandez, G. ve Carvajal, F. (2012). Security Aspects of SCADA and DCS Environments. J. Lopez, R. Setola, and S. D. Wolthusen (Eds.), *Critical Infrastructure Protection: Information Infrastructure Models, Analysis, and Defense*. Berlin, Heidelberg: Springer, 120-149.

92. Byres, E. ve Lowe, J. (2004). *The myths and facts behind cyber security risks for industrial control systems*. VDE Congress, VDE Association for Electrical, Electronic and Information Technologies, Berlin, 213-218.

93. Chabukswar, R., Sinópoli, B., Karsai, G., Giani, A., Neema, H., ve Davis, A. (2010). *Simulation of Network Security Attacks on SCADA Systems*. First Workshop on Secure Control Systems (SCS), Stockholm, Sweden, 1-8.

94. Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., ve Hahn, A. (2015). Guide to Industrial Control Systems (ICS) Security; *NIST,* (SP 800-82r2), Gaithersburg, MD,USA. 1-247.

95. Chen, D., Peng, Y. ve Wang, H. (2013). *Development of a Testbed for Process Control System Cybersecurity Research*. 3rd International Conference on Electric and Electronics (EEIC 2013) Hong Kong, China, 158-161.

96. Stamp, J. E. ve Campbell, P. L. (2004). A classification scheme for risk assessment methods (SAND2004-4233); *Sandia National Laboratories,* (SAND2004-4233), USA. 1-29.

97. Igure, V. M., Laughter, S. A. ve Williams, R. D. (2006). Security issues in SCADA networks. *Computers & Security*, 25(7), 498-506.

98. Hentea, M. (2008). Improving security for SCADA control systems. *Interdisciplinary Journal of Information, Knowledge, and Management,* 3(1), 73-86.

99. Rautmare, S. (2011). *SCADA system security: Challenges and recommendations*. Annual IEEE India Conference, Hyderabad, India, 1-4.

100. Abrams, M. and Weiss, J. (2008). Malicious Control System Cyber Security Attack Case Study–Maroochy Water Services, Australia; *The MITRE Corporation*, Australia. 7-10.

101. İnternet: Smith, T. (2001). Hacker jailed for revenge sewage attacks. *The Register*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.theregister.co.uk%2F2001%2F10%2F31%2Fhacker_jailed_for_revenge_sewage%2F&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

102. İnternet: Hancock, D. (2003). Virus Disrupts Train Signals. *CBS News*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.cbsnews.com%2Fnews%2Fvirus-disrupts-train-signals%2F&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

103. İnternet: Poulsen, K. (2003). Slammer worm crashed Ohio nuke plant network. *SecurityFocus*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.securityfocus.com%2F news%2F6767&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

104. U.S.-Canada Power System Outage Task Force (2006). Fi*nal Report on the Implementation of the Task Force Recommendations;* Natural Resources Canada-U.S. Department of Energy, Canada-USA. 1-62.

105. İnternet: Lemos, R. (2005). Worm spreading through Microsoft Plug-and-Play flaw. *SecurityFocus*. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.security focus.com%2Fnews%2F11281&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

106. Federal Energy Regulatory Commission (2005). Commission conducts investigation of Taum Sauk Dam breach; *Federal Energy Regulatory Commission,* (P-2277), 1-2.

107. Lagner, R. (2013). A Technical Analysis of What Stuxnet's Creators Tried to Achieve -To Kill a Centrifuge; *The Langner Group,* Arlington, Hamburg, Munich.

108. Porche, I. R., Sollinger, J. M. ve McKay, S. (2011). *A Cyberworm that Knows no Boundaries.* RAND (W74V8H-06-C-0002). Santa Monica, CA, USA. 1-55.

109. Department of Homeland Security (2014). Siemens Industrial Products OpenSSL Heartbleed Vulnerability; *ICS-CERT,* (ICSA-14-105-03B).

110. Lee, R. M., Assante, M. J. ve Conway, T. (2016). Analysis of the Cyber Attack on the Ukranian Power Grid; *E-ISAC* Washington, DC, USA. 1-29.

111. Nazario, J. (2007). BlackEnergy DDoS Bot Analysis; *Arbor Networks*, Burlington, MA, USA. 1-11.

112. Assante, M. J. ve Lee, R. M. (2015). The ındustrial control system cyber kill chain. *SANS Institute InfoSec Reading Room,* 1, 1-24.

113. Duggan, D., Berg, M., Dillinger, J., ve Stamp, J. (2005). Penetration Testing of Industrial Control Systems; *Sandia National Laboratories,* (SAND2005-2846P), Albuquerque, New Mexico. 1-7.

114. Johnson, R. E. (2010). *Survey of SCADA security challenges and potential attack vectors*. International Conference for Internet Technology and Secured Transactions, London, UK, 1-5.

115. Nicholson, A., Webber, S., Dyer, S., Patel, T., ve Janicke, H. (2012). SCADA security in the light of Cyber-Warfare. *Computers & Security,* 31(4), 418-436.

116. Sandaruwan, G. P. H., Ranaweera, P. S. ve Oleshchuk, V. A. (2013). *PLC security and critical infrastructure protection*. The Institute of Electrical and Electronics Engineers 8th International Conference on Industrial and Information Systems, Peradeniya, Sri Lanka, 81-85.

117. Byres, E. J. (2000). Designing secure networks for process control. *The Institute of Electrical and Electronics Engineers Industry Applications Magazine,* 6(5), 33-39.

118. Arora, A., Nandkumar, A. ve Telang, R. (2006). Does information security attack frequency increase with vulnerability disclosure? An empirical analysis. *Information Systems Frontiers,* 8(5), 350-362.

119. Elms, E. R., LaPrade, J. D. ve Maurer, M. L. (2008). Hacking of Corporate information Systems: Increasing threats and Potential Risk Management Techniques. *Chartered Property Casualty Underwriter eJournal*, 61(2), 1-9.

120. August, T., August, R. ve Shin, H. (2014). Designing user incentives for cybersecurity. *Commun. Association for Computing Machinery*, 57(11), 43-46.

121. İnternet: Storr, W. (2014). Basic Electronics Tutorial: Closed Loop System. URL: http://www.webcitation.org/query?url=https%3A%2F%2Fwww.electronics-tutorials.ws%2F systems%2Fclosed-loop-system.html&date=2018-06-07, Son Erişim Tarihi: 20.05.2018.

122. Bolton, W. (2015). Chapter 1 - Programmable Logic Controllers. *Programmable Logic Controllers (Sixth Edition)*. Boston: Newnes, 1-22.

123. Giani, A., Karsai, G., Roosta, T., Shah, A., Sinopoli, B., ve Wiley, J. (2008). A testbed for secure and robust SCADA systems. *Special Interest Group on Embedded Systems Review*, 5(2), 1-4.

124. Oman, P. ve Phillips, M. (2007). *Intrusion Detection and Event Monitoring in SCADA Networks*. International Conference on Critical Infrastructure Protection (ICCIP), Hanover, NH, United States, 161-173.

125. Byres, E., Hoffman, D. ve Kube, N. (2006). *On Shaky Ground – A Study of Security Vulnerabilities in Control Protocols*. 5th International Topical Meeting on Nuclear Plant Instrumentation, Controls, and Human Machine Interface Technology (NPIC & HMIT), Albuquerque, NM, United States, 782-788.

126. Genge, B., Graur, F. ve Haller, P. (2015). Experimental assessment of network design approaches for protecting industrial control systems. *International Journal of Critical Infrastructure Protection*, 11, 24-38.

127. Sayegh, N., Chehab, A., Elhajj, I. H., ve Kayssi, A. (2013). *Internal security attacks on SCADA systems*. Third International Conference on Communications and Information Technology (ICCIT), Beirut, Lebanon, 22-27.

128. Li, H., Mao, R., Lai, L., ve Qiu, R. C. (2010). *Compressed Meter Reading for Delay-Sensitive and Secure Load Report in Smart Grid*. First IEEE International Conference on Smart Grid Communications, Gaithersburg, MD, United States, 114-119.

129. Efthymiou, C. ve Kalogridis, G. (2010). *Smart Grid Privacy via Anonymization of Smart Metering Data*. First The Institute of Electrical and Electronics Engineers International Conference on Smart Grid Communications, Gaithersburg, MD, United States, 238-243.

130. Shi, E., Perrig, A. ve Doorn, L. V. (2005). *BIND: a fine-grained attestation service for secure distributed systems*. The Institute of Electrical and Electronics Engineers Symposium on Security and Privacy (S&P'05), Oakland, CA, United States, 154-168.

131. Klick, J., Lau, S., Marzin, D., Malchow, J. O., ve Roth, V. (2015). *Internet-facing PLCs as a network backdoor*. The Institute of Electrical and Electronics Engineers Conference on Communications and Network Security (CNS), Florence, Italy, 524-532.

132. Guan, J., Graham, J. H. ve Hieb, J. L. (2011). *A digraph model for risk identification and mangement in SCADA systems*. The Institute of Electrical and Electronics Engineers International Conference on Intelligence and Security Informatics, Beijing, China, 150-155.

133. Mahoney, W. ve Gandhi, R. A. (2011). An integrated framework for control system simulation and regulatory compliance monitoring. *International Journal of Critical Infrastructure Protection*, 4(1), 41-53.

134. Queiroz, C., Mahmood, A. ve Tari, Z. (2011). A Framework for Building SCADA Simulations. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid*, 2(4), 589-597.

135. Leszczyna, R., Nai Fovino, I. ve Masera, M. (2010). Simulating malware with MAlSim. *Journal in Computer Virology*, 6(1), 65-75.

136. Bytschkow, D., Zellner, M. ve Duchon, M. (2015). *Combining SCADA, CIM, GridLab-D and AKKA for smart grid co-simulation*. IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, United States, 1-5.

137. Novák, P., Šindelář, R. ve Mordinyi, R. (2014). Integration framework for simulations and SCADA systems. *Simulation Modelling Practice and Theory*, 47, 121-140.

138. Farooqui, A. A., Zaidi, S. S. H., Memon, A. Y., ve Qazi, S. (2014). *Cyber Security Backdrop: A SCADA testbed*. The Institute of Electrical and Electronics Engineers Computers, Communications and IT Applications Conference, Beijing, China, 98-103.

139. Hahn, A., Kregel, B., Govindarasu, M., Fitzpatrick, J., Adnan, R., Sridhar, S. ve Higdon, M. (2010). *Development of the PowerCyber SCADA security testbed*. The Sixth Annual Workshop on Cyber Security and Information Intelligence Research, Oak Ridge, Tennessee, United States, 1-4.

140. Dondossola, G., Garrone, F. ve Szanto, J. (2009). *Supporting cyber risk assessment of Power Control Systems with experimental data*. The Institute of Electrical and Electronics Engineers/PES Power Systems Conference and Exposition, Seattle, WA, United States, 1-3.

141. Nazir, S., Patel, S. ve Patel, D. (2017). Assessing and augmenting SCADA cyber security: A survey of techniques. *Computers & Security*, 70, 436-454.

142. Tesfahun, A. ve Bhaskari, D. L. (2016). A SCADA testbed for investigating cyber security vulnerabilities in critical infrastructures. *Automatic Control and Computer Sciences*, 50(1), 54-62.

143. Ralston, P. A. S., Graham, J. H. ve Hieb, J. L. (2007). Cyber security risk assessment for SCADA and DCS networks. *ISA Transactions*, 46(4), 583-594.

144. H., H. M. ve Y., H. Y. (2009). A Comprehensive Network Security Risk Model for Process Control Networks. *Risk Analysis*, 29(2), 223-248.

145. Zhang, Y., Wang, L., Xiang, Y., ve Ten, C. W. (2015). Power System Reliability Evaluation With SCADA Cybersecurity Considerations. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid*, 6(4), 1707-1721.

146. Ten, C. W., Liu, C. C. ve Govindarasu, M. (2007). *Vulnerability Assessment of Cybersecurity for SCADA Systems Using Attack Trees*. The Institute of Electrical and Electronics Engineers Power Engineering Society General Meeting, Tampa, FL, United States, 1-8.

147. El Bouchti, A. ve Haqiq, A. (2012). *Modeling cyber-attack for SCADA systems using CoPNet approach*. The Institute of Electrical and Electronics Engineers International Conference on Complex Systems (ICCS), Agadir, Morocco, 1-6.

148. Li, W., Xie, L., Deng, Z., ve Wang, Z. (2016). False sequential logic attack on SCADA system and its physical impact analysis. *Computers & Security*, 58, 149-159.

149. Mahboob, A. ve Zubairi, J. A. (2013). *Securing SCADA systems with open source software*. High Capacity Optical Networks and Emerging/Enabling Technologies, Magosa, Cyprus, 193-198.

150. Maynard, P., McLaughlin, K. ve Haberler, B. (2014). *Towards Understanding Man-in-the-middle Attacks on IEC 60870-5-104 SCADA Networks*. 2nd International Symposium for ICS & SCADA Cyber Security Research, St Polten, Austria, 1-11.

151. Genge, B. ve Siaterlis, C. (2014). Physical process resilience-aware network design for SCADA systems. *Computers & Electrical Engineering*, 40(1), 142-157.

152. Li, F., Shen, L., Si, Y., ve Niu, J. (2009). *A Method to Enhance SCADA Systems Survivability through Simulation Technology*. International Conference on Measuring Technology and Mechatronics Automation, Zhangjiajie, Hunan, China, 175-178.

153. Markovic-Petrovic, J. D. ve Stojanovic, M. D. (2013). *Analysis of SCADA system vulnerabilities to DDoS attacks*. 11th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services (TELSIKS), Nis, Serbia, 591-594.

154. Ciancamerla, E., Minichino, M. ve Palmieri, S. (2013). *Modeling cyber attacks on a critical infrastructure scenario*. Fourth International Information, Intelligence, Systems and Applications (IISA) Conference Piraeus, Greece, 1-6.

155. Cardenas, A. A., Amin, S. ve Sastry, S. (2008). *Research Challenges for the Security of Control Systems*. the 3rd Conference on Hot Topics in Security (HotSec), San Jose, CA, United States, 1-6.

156. J. G, S., Pop, A., Fritzson, P., ve Wildman, L. (2008). *Towards ıntegrated model-driven testing of SCADA systems using the eclipse modeling framework and modelica*. 19th Australian Conference on Software Engineering (aswec 2008), Perth, WA, Australia, 149-159.

157. Backhaus, S., Bent, R., Bono, J., Lee, R., Tracey, B., Wolpert, D., Xie, D. ve Yildiz, Y. (2013). Cyber-physical security: A game theory model of humans ınteracting over control systems. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid*, 4(4), 2320-2327.

158. Queiroz, C., Mahmood, A. ve Tari, Z. (2013). A probabilistic model to predict the survivability of SCADA systems. *The Institute of Electrical and Electronics Engineers Transactions on Industrial Informatics*, 9(4), 1975-1985.

159. Yang, L., Cao, X., Li, J., Wang, A., Tan, W. ve Yu, Z. (2012). *Research on FNN-based security defence architecture model of scada network*. The Institute of Electrical and Electronics Engineers2nd International Conference on Cloud Computing and Intelligence Systems, Hangzhou, China, 1367-1371.

160. Byres, E. J., Franz, M. ve Miller, D. (2004). *The Use Of Attack Trees in Assessing Vulnerabilities in SCADA Systems*. International Infrastructure Survivability Workshop (IISW'04), Lisbon, Portugal, 1-9.

161. Mo, Y., Chabukswar, R. ve Sinopoli, B. (2014). Detecting ıntegrity attacks on SCADA systems. *IEEE Transactions on Control Systems Technology*, 22(4), 1396-1407.

162. Hug, G. ve Giampapa, J. A. (2012). Vulnerability Assessment of ac state estimation with respect to false data ınjection cyber-attacks. *The Institute of Electrical and Electronics Engineers Transactions on Smart Grid*, 3(3), 1362-1370.

163. Jiang, J. ve Yasakethu, L. (2013). *Anomaly Detection via One Class SVM for Protection of SCADA Systems*. International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, Beijing, China, 82-88.

164. Kane, P. O., Sezer, S., McLaughlin, K., ve Im, E. G. (2013). SVM training phase reduction using dataset feature filtering for malware detection. *The Institute of Electrical and Electronics Engineers Transactions on Information Forensics and Security*, 8(3), 500-509.

165. Nader, P., Honeine, P. ve Beauseroy, P. (2014). ${l_p} $-norms in one-class classification for ıntrusion detection in SCADA systems. *The Institute of Electrical and Electronics Engineers Transactions on Industrial Informatics*, 10(4), 2308-2317.

166. Moya, J. M., Araujo, A., Banković, Z., De Goyeneche, J. M., Vallejo, J. C., Malagón, P., Villanueva, D., Fraga, D., Romero, E. ve Blesa, J. (2009). Improving security for SCADA sensor networks with reputation systems and self-organizing maps. *Sensors*, 9(11), 9380-9397.

167. Torrisi, N. M., Vuković, O., Dán, G., ve Hagdahl, S. (2014). *Peekaboo: A gray hole attack on encrypted SCADA communication using traffic analysis*. The Institute of Electrical and Electronics Engineers International Conference on Smart Grid Communications, Venice, Italy, 902-907.

168. Simmhan, Y., Aman, S., Kumbhare, A., Liu, R., Stevens, S., Zhou, Q. and Prasanna, V. (2013). Cloud-based software platform for big data analytics in smart grids. *Computing in Science & Engineering*, 15(4), 38-47.

169. Carcano, A., Coletta, A., Guglielmi, M., Masera, M., Fovino, I. N. ve Trombetta, A. (2011). A multidimensional critical state analysis for detecting ıntrusions in SCADA systems. *The Institute of Electrical and Electronics Engineers Transactions on Industrial Informatics*, 7(2), 179-186.

170. Pham, V.-H. ve Dacier, M. (2011). Honeypot trace forensics: The observation viewpoint matters. *Future Generation Computer Systems*, 27(5), 539-546.

171. Winn, M., Rice, M., Dunlap, S., Lopez, J. ve Mullins, B. (2015). Constructing cost-effective and targetable industrial control system honeypots for production networks. *International Journal of Critical Infrastructure Protection*, 10, 47-58.

172. Baecher, P., Koetter, M., Holz, T., Dornseif, M. ve Freiling, F. (2006, September). *The Nepenthes Platform: An Efficient Approach to Collect Malware*. 9th International Symposium Recent Advances in Intrusion Detection Hamburg, Germany, 165-184.

173. Goldenberg, J., Shavitt, Y., Shir, E. ve Solomon, S. (2005). Distributive ımmunization of networks against viruses using the 'honey-pot'architecture. *Nature Physics*, 1(3), 184-188.

174. Vural, Y. ve Sağıroğlu, Ş. (2018). Kurumsal Bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi,* 23(2), 507-522.

175. Laudon, K. C. ve Laudon, J. P. (2004). *Management ınformation systems: Managing the digital firm plus* (8 ed.). New Jersey, USA: Prentice Hall Press, 588.

176. Al-Hamdani, W. A. (2006). *Assessment of need and method of delivery for information security awareness program*. 3rd Annual Conference on Information Security Curriculum Development - InfoSecCD '06, Kennesaw, GA, United States, 102-108.

177. Kruger, H. A. ve Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289-296.

178. Thomson, K. ve Van Niekerk, J. (2012). Combating information security apathy by encouraging prosocial organisational behaviour. *Information Management & Computer Security*, 20(1), 39-46.

179. Dhillon, G., Syed, R. ve Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. *Computers & Security*, 56, 63-69.

180. Bulgurcu, B., Cavusoglu, H. ve Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and ınformation security awareness. *MIS quarterly*, 34(3), 523-548.

181. Weiguo, S., Gareth, H., Michael, F., Farzin, D., ve Shengyong, C. (2012). Reliable and secure encryption key generation from fingerprints. *Information Management & Computer Security*, 20(3), 207-221.

182. Kearney, P. (2010). *Security: The human factor*. Cambridgeshire, UK: IT Governance, 62.

183. Parmar, B. (2012). Protecting against spear-phishing. *Computer Fraud & Security*, 2012(1), 8-11.

184. Da Veiga, A. ve Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162-176.

185. Montesdioca, G. P. Z. ve Maçada, A. C. G. (2015). Measuring user satisfaction with information security practices. *Computers & Security*, 48, 267-280.

186. Shropshire, J., Warkentin, M. ve Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, 49, 177-191.

187. Tamjidyamcholo, A., Bin Baba, M. S., Tamjid, H., ve Gholipour, R. (2013). Information security – Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language. *Computers & Education*, 68, 223-232.

188. Tamjidyamcholo, A., Bin Baba, M. S., Shuib, N. L. M., ve Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, 43, 19-34.

189. Rocha Flores, W., Antonsen, E. ve Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110.

190. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., ve Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165-176.

191. Mitnick, K. D. ve Simon, W. L. (2009). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers*. Indianapolis, IN, USA: John Wiley & Sons, 288

192. Gardner, B. (2014). Chapter 1 - What Is a Security Awareness Program? *Building an Information Security Awareness Program*. Boston, MA, USA: Syngress, 1-8.

193. Arachchilage, N. A. G. ve Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312.

194. Kruger, H., Drevin, L. ve Steyn, T. (2007). *Email Security Awareness — a Practical Assessment of Employee Behaviour*. Fifth World Conference on Information Security Education, West Point, NY, United States, 33-40.

195. Hansman, S. ve Hunt, R. (2005). A taxonomy of network and computer attacks. *Computers & Security,* 24(1), 31-43.

196. Ahmad, A., Maynard, S. B. ve Shanks, G. (2015). A case analysis of information systems and security incident responses. *International Journal of Information Management,* 35(6), 717-723.

197. Conger, S., Pratt, J. H. ve Loch, K. D. (2013). Personal information privacy and emerging technologies. *Information Systems Journal,* 23(5), 401-417.

198. Aral, S., Dellarocas, C. ve Godes, D. (2013). Introduction to the Special Issue—Social Media and Business Transformation: A Framework for Research. *Information Systems Research,* 24(1), 3-13.

199. Sonia, L. ve R, B. D. (2010). On the Rapid Rise of Social Networking Sites: New Findings and Policy Implications. *Children & Society,* 24(1), 75-83.

200. Benson, V., Saridakis, G., Tennakoon, H., ve Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. *International Journal of Human-Computer Studies,* 80, 36-44.

201. Saridakis, G., Benson, V., Ezingeard, J.-N., ve Tennakoon, H. (2016). Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users. *Technological Forecasting and Social Change,* 102, 320-330.

202. Ben-Asher, N. ve Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior,* 48, 51-61.

203. Farooq, A., Isoaho, J., Virtanen, S., ve Isoaho, J. (2015). *Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors*. The Institute of Electrical and Electronics Engineers Trustcom/BigDataSE/ISPA, Helsinki, Finland, 352-359.

204. Mansfield, R. S. (1996). Building competency models: Approaches for HR professionals. *Human Resource Management,* 35(1), 7-18.

205. Peng, Y., Xiang, C., Gao, H., Chen, D., ve Ren, W. (2015). *Industrial Control System Fingerprinting and Anomaly Detection*. International Conference on Critical Infrastructure Protection (ICCIP 2015), Arlington, VA, United States, 73-85.

206. Genge, B. ve Siaterlis, C. (2012). *An Experimental Study on the Impact of Network Segmentation to the Resilience of Physical Processes*. 11th International IFIP TC 6 Networking Conference, Prague, Czech Republic, 121-134.

207. Gaddam, R. ve Nandhini, M. (2017). *An analysis of various snort based techniques to detect and prevent intrusions in networks proposal with code refactoring snort tool in Kali Linux environment*. International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, India, 10-15.

208. Zihao, F., Sujuan, Q., Xuesong, H., Pei, P., Ye, L., ve Liming, W. (2016). *Snort improvement on Profinet RT for Industrial Control System Intrusion Detection*. 2nd The Institute of Electrical and Electronics Engineers International Conference on Computer and Communications (ICCC), Chengdu, China, 942-946.

209. Nivethan, J. (2016). *A Framework for SCADA/ICS Security*. Ann Arbor, MI, USA: ProQuest LLC, 39.

210. Richey, D. J. (2016). *Leveraging PLC ladder logic for signature based IDS rule generation.* Doctoral Dissertation, Mississippi State University, Mississippi State.

211. Bhuyan, M. H., Kashyap, H. J., Bhattacharyya, D. K., ve Kalita, J. K. (2014). Detecting distributed denial of service attacks: methods, tools and future directions. *The Computer Journal*, 57(4), 537-556.

212. Mirkovic, J. ve Reiher, P. (2005). D-WARD: a source-end defense against flooding denial-of-service attacks. *The Institute of Electrical and Electronics Engineers Transactions on Dependable and Secure Computing*, 2(3), 216-232.

213. Lee, S. M., Kim, D. S., Lee, J. H., ve Park, J. S. (2012). Detection of DDoS attacks using optimized traffic matrix. *Computers & Mathematics with Applications*, 63(2), 501-510.

214. Silberschatz, A., Galvin, P. B. ve Gagne, G. (2012). Chapter 15: Security. *Operating System Concepts* (9 ed.). Hoboken, NJ, USA: JohnWiley&Sons, 673-674.

215. Budka, K. C., Deshpande, J. G., Doumi, T. L., Madden, M., ve Mew, T. (2010). Communication network architecture and design principles for smart grids. *Bell Labs Technical Journal*, 15(2), 205-227.

216. Nam, S. Y., Djuraev, S. ve Park, M. (2013). Collaborative approach to mitigating ARP poisoning-based Man-in-the-Middle attacks. *Computer Networks*, 57(18), 3866-3884.

217. Lootah, W., Enck, W. ve McDaniel, P. (2007). TARP: Ticket-based address resolution protocol. *Computer Networks*, 51(15), 4322-4337.

218. Pansa, D. ve Chomsiri, T. (2008). *Architecture and Protocols for Secure LAN by Using a Software-Level Certificate and Cancellation of ARP Protocol*. Third International Conference on Convergence and Hybrid Information Technology, Busan, South Korea, 21-26.

219. Hong, S., Oh, M. ve Lee, S. (2013). Design and implementation of an efficient defense mechanism against ARP spoofing attacks using AES and RSA. *Mathematical and Computer Modelling*, 58(1), 254-260.

220. Asokan, N., Niemi, V. ve Nyberg, K. (2005). *Man-in-the-Middle in Tunnelled Authentication Protocols*. 11th International Workshop on Security Protocols, Cambridge, UK, 28-41.

221. Oppliger, R., Hauser, R. ve Basin, D. (2006). SSL/TLS session-aware user authentication – Or how to effectively thwart the man-in-the-middle. *Computer Communications*, 29(12), 2238-2246.

222. Bicakci, K., Unal, D., Ascioglu, N., and Adalier, O. (2014). *Mobile Authentication Secure against Man-in-the-Middle Attacks*. 2nd The Institute of Electrical and Electronics Engineers International Conference on Mobile Cloud Computing, Services, and Engineering, Oxford, UK, 273-276.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : GÖNEN, Serkan

Uyruğu : T.C.

Doğum tarihi ve yeri : 11/07/1979 Ankara

Medeni hali : Evli

Telefon : 0505 351 12 01

e-posta : serkangonen@gazi.edu.tr

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Doktora	Gazi Üniversitesi / Fen Bilimleri Enstitüsü / Bilgi Güvenliği Mühendisliği	Devam Ediyor
Yüksek lisans	Kara Harp Okulu / Teknoloji Yönetimi	2006
Lisans	Kara Harp Okulu	2002
Lise	Maltepe Askeri Lisesi	1998

İş Deneyimi

Yıl	**Yer**	**Görev**
2002- devam ediyor	Jandarma Genel Komutanlığı	Subay (Bilgi Sistemleri, Siber Güvenlik)

Yabancı Dili

İngilizce

Yunanca

Yayınlar

SCI ve SCI-E Kapsamındaki Yayınlar

1. Yılmaz, E. N. ve Gönen, S. (2018). Attack Detection/Prevention System Against Cyber Attack in Industrial Control Systems. *Computers & Security*, 77, 94-105

Hakemli ve Alan İndeksli Dergilerde Yayınlar

1. Yılmaz, E. N., Ulus, H. İ. ve Gönen, S. (2015). Bilgi Toplumuna Geçiş ve Siber Güvenlik. *International Journal Of Informatics Technologies*, 8(3), 133.

2. Gönen, S., Ulus, H. İ. ve Yılmaz, E. N. (2016). Bilişim Alanında İşlenen Suçlar Üzerine Bir İnceleme. *International Journal Of Informatics Technologies,* 9(3), 229.

Ulusal ve Uluslararası Sempozyumlarda Sunulan Bildiriler

1. Yılmaz, E. N. ve Gönen, S. (25-26 Ekim 2016). *Endüstriyel Kontrol Sistemlerinde Siber Güvenlik: PLC Güvenliği Üzerine Bir İnceleme*. 9'uncu Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Siber Güvenlik ve Nesnelerin İnterneti, Orta Doğu Teknik Üniversitesi, Ankara.

2. Yılmaz, E. N. ve Gönen, S. (21-22 Eylül 2017). *Endüstriyel Kontrol Sistemi Çalışanlarında Bilgi Güvenliği Farkındalığı*. 1'nci Ulusal Elektrik Enerjisi Dönüşümü Kongresi. Fırat Üniversitesi, Elazığ.

3. Yılmaz, E. N. ve Gönen, S. (21-22 Eylül 2017). *4650 kVA Kurulu Güce Sahip Bir Enerji Dağıtım Sisteminin ETAP Programı ile Analizi*. 1'nci Ulusal Elektrik Enerjisi Dönüşümü Kongresi, Fırat Üniversitesi, Elazığ.

Hobiler

Yüzme, Kitap Okumak, CTF Çözümleri, Sızma Testi Araçları

GAZİ GELECEKTİR..