TCP / IP TABANLI DAĞITIK ENDÜSTRİYEL DENETİM SİSTEMLERİNDE GÜVENLİK VE ÇÖZÜM ÖNERİLERİ

Alper ÖZBİLEN

DOKTORA TEZİ
ELEKTRİK EĞİTİMİ

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

AĞUSTOS 2012
ANKARA

Alper ÖZBİLEN tarafından hazırlanan "TCP / IP TABANLI DAĞITIK ENDÜSTRİYEL DENETİM SİSTEMLERİNDE GÜVENLİK VE ÇÖZÜM ÖNERİLERİ" adlı bu tezin doktora tezi olarak uygun olduğunu onaylarım.

Prof. Dr. İlhami Çolak
Tez Danışmanı,Elektrik-Elektronik Mühendisliği Anabilim Dalı
Prof. Dr. Şeref SAĞIROĞLU
Tez Danışmanı, Bilgisaray Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından oybirliğiyle Elektrik Eğitimi Anabilim Dalında doktora tezi olarak kabul edilmiştir.

Prof. Dr. Ziya AKTAŞ
Bilgisaray Mühendisliği Anabilim Dalı,Başkent Üniversitesi

Prof. Dr. İlhami ÇOLAK
Elektrik-Elektronik Mühendisliği Anabilim Dalı,G.Ü.

Prof. Dr. Güngör BAL
Elektrik-Elektronik Mühendisliği Anabilim Dalı, G.Ü.

Prof. Dr. M. Reşit TOLUN
Bilgisaray Mühendisliği Anabilim Dalı, TED Üniversitesi

Prof. Dr. Mustafa ALKAN
Elektrik-Elektronik Mühendisliği Anabilim Dalı, G.Ü.

Tarih : 07/08/2012

Bu tez ile Gazi Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu Doktora derecesini onamıştır.

Prof. Dr. Şeref SAĞIROĞLU …….....
Fen Bilimleri Enstitüsü Müdürü

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Alper ÖZBİLEN

TCP / IP TABANLI DAĞITIK ENDÜSTRİYEL DENETİM SİSTEMLERİNDE GÜVENLİK VE ÇÖZÜM ÖNERİLERİ
(Doktora Tezi)

Alper ÖZBİLEN

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
Ağustos 2012

ÖZET

Su, elektrik, doğal gaz ve petrol gibi toplumların refahı, emniyeti ve ülke ekonomileri için önemli kaynakların üretim, iletim ve dağıtım sistemleri literatürdekritik altyapılar olarak tanımlanmaktadır. Bu altyapıların ortak özelliği, Dağıtık Denetim Sistemlerini (DDS) veya Merkezi Yönetim, Denetleme ve Veri Toplama (SCADA) sistemlerini sahadaki fiziksel iş süreçlerini otomatize etmekte kullanmalarıdır. Geçmişten farklı olarak, bilgi teknolojileri ve denetim sistemlerine dayanan kritik altyapılarını yalnızca fiziki tedbirlerle korumak günümüzde artık mümkün değildir. Son dönemde SCADA/DDS sistemlerinde özel tasarım bileşenler yerine, standart ve genel amaçlı donanım ve yazılımlar sıklıkla kullanılmaya başlanmıştır. Ayrıca, bu sistemlerin çoğu farklı şekillerde ve farklı amaçlar için internet veya diğer harici ağlara bağlanabilmekte ve uzaktan işletilebilmektedir. Son yıllarda bu sistemlere yöneliksiber saldırılar arttığından,bu sistemlerin açıklarını araştırmak ve gidermek için farklı ülkelerde akademik ve devlet destekli çalışmalar başlatılmıştır.

Bu çalışma kapsamında, ülkemizde denetim sistemlerine dayalı üretim, iletim ve dağıtım yapan kritik altyapıların güvenliğine katkılar sağlamak ve çözüm önerileri getirmek,DDS sistemlerin güvenlik gereksinimlerini belirlemek, ülkemizdeki kurumsal uygulamaları izlemek ve neticesinde gerçekçi ve uygulanabilir çözümler önerebilmek için literatür incelemeleri ve örnek

durumçalışmaları yapılmıştır. Literatürde sunulanve örnek durum çalışmalarından elde edilen veri, bilgi ve bulgulardan yararlanılarak, ülkemizdekidenetim sistemlerine dayalı kritik altyapılara yönelik güvenlik açıklıklarıincelenmiştir. Ayrıca, farklı işletmeciler için tanımlıistenmeyen olaylara göre muhtemel açıklıklarının kritikliğini belirleyen bir yaklaşım geliştirilmiştir.

Sonuç olarak, bu tez çalışmasında, kritik altyapılarda kullanılan DDS sistemlerine ilişkin yönetim, işletme ve teknik boyutları dikkate alanbütüncül bir güvenlik yaklaşımının geliştirilmesi hedeflenmiş, güvenlik risklerinin iyileştirilmesi ve bugünün güvenlik gereksinimlerinin karşılanması için karar vericilere, araştırmacılara ve işletmecilere yönelik ulusal ve kurumsal bazda kullanılabilecek ve uygulanabilecek stratejileri ve planları kapsayan güvenlik dokümanları oluşturulmuştur.Bu tez çalışması sonucunda ortaya konulan strateji dokümanı ve kurumsal eylem planının, denetim sistemlerine dayalı kritik altyapı güvenliğinin sağlanmasınakatkılar sağlayacağı değerlendirilmektedir.

Bilim Kodu : **703.1.014**
Anahtar Kelimeler : **Kritik altyapılar, denetim sistemleri, SCADA, DDS, güvenlik, risk değerlendirme, iyileştirme yaklaşımları, strateji ve politikalar, güvenlik dokümanları**
Sayfa Adedi : **201**
Tez Yöneticileri : **Prof. Dr. İlhami ÇOLAK Prof. Dr. Şeref SAĞIROĞLU**

SECURITY AND SOLUTIONPROPOSALS FOR TCP/IP BASED DISTRIBUTED INDUSTRIAL CONTROL SYSTEMS

(Ph.D. Thesis)

Alper ÖZBİLEN

GAZİ UNIVERSITY

INSTITUTE OF SCIENCE AND TECHNOLOGY

August 2012

ABSTRACT

Water, electricity, natural gas and oil production, transmission and distribution systems which are important in terms of social welfare,security and economy are defined as critical infrastructure in literature. One of the common features of these infrastructures is to use Distributed Control Systems (DCS) or Supervisory Control and Data Acquisition (SCADA) systems to automate physical processes in industrial plants. Unlike the past, the critical infrastructures based on information technology and control system technology could not be defended by solely physical protection. Recently, standard and general purpose hardware and software are frequently used in SCADA/DCS products instead of custom designed andproprietarycomponents. In addition, most of these systems could be connected to internet or other external networks in some ways and allow remote access and operations. In the last years, increases in cyber attacksto SCADA/DCS have more attentions because of its criticalfunctionalities. That is why academics and government sponsored studies have been started in some countries.

In this study, it is aimed to contribute and propose solutions to security of critical infrastructures that are used for production, transmission and distribution based on control systems. Case studies and literature reviews have been conducted to determine security requirements, observe institutional practices in Turkey, and propose realistic and applicable security solutions. Vulnerabilities of critical infrastructures in Turkey are determined with the

help of data obtained from case studies. In addition an approach illustrating the criticality level of security vulnerabilities based on unwanted incidents for different operators is proposed.

As a result,we have aimed to develop an integrated security aspect which gives importance to managerial, operational and technical dimensions related to DCS systems. In this context, several security documents have been created in terms of improvement of security risks and to supply the needs of decision makers, researchers and operators. These strategy and action plan documents could be used in national or organizational platforms.It is evaluated that the present study will make contributions to security of critical infrastructures based on control systems

Science Code : 703.1.014
Key Words : Critical infrastructure, control systems, SCADA, DCS, security, risk assessment, improvement approach, strategy and politics, security documents
Page Number: 201
Adviser : Prof. Dr. İlhami ÇOLAKProf. Dr. Prof. Dr. Şeref SAĞIROĞLU

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren tez danışmanlarım Sayın Prof. Dr. İlhami ÇOLAK ve Sayın Prof. Dr. Şeref SAĞIROĞLU'na, teşekkürü bir borç bilirim. Bu süreçte destek ve katkılarını gördüğüm,Tez İzleme Komitesi Üyeleri Sayın Prof. Dr. Mehmet Reşit TOLUN ve Sayın Prof. Dr. Güngör BAL hocalarıma şükranlarımı sunarım.

Güvenlik nedeniyle isimlerini burada anamasam da bu çalışmanın meydana gelmesinde ve tamamlanmasında en büyük katkı sahiplerinden olan ülkemizin iki önemli işletmecisinin kıymetli yönetici ve çalışanları ile güvenlik taramaları için bana her türlü teknik imkânlarını sunan ASES Bilgi Güvenlik Teknolojileri yönetici ve çalışanlarına da teşekkürlerimi sunarım.

Son olarak, çalışmalarım esnasında başta eşim olmak üzere kendilerine yeterince vakit ayıramadığım herkese anlayışları ve destekleri için müteşekkirim.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmadakullanılmışbazı kısaltmalar, açıklamaları ile birlikte aşağıdasunulmuştur.

Kısaltmalar	Açıklama
3G	Üçüncü Nesil Mobil Telekomünikasyon Hizmetleri
AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
AGA	Amerikan Gaz Birliği (American Gas Association)
ARP	Adres Çözümleme Protokolü (Address Resolution Protocol)
ATM	Hücre Anahtarlamalı Devre (Asynchronous Transfer Mode)
BCIT	İngiliz Kolombiya Teknoloji Enstitüsü (British Columbia Institute Of Technology)
BDDK	Bankacılık Düzenleme ve Denetleme Kurumu
BGYS	Bilgi Güvenliği Yönetim Sistemii
BIOS	Temel Giriş-Çıkış Sistemi (Basic Input-Output System)
BOOTP	Önyükleme Protokolü (Bootstrap Protocol)
BSI	İngiliz Standartlar Enstitüsü (British Standartds Institute)
BT	Bilgi Teknolojileri
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CDMA	Kod Bölmeli Çoklu Erişim (Code Division Multiple Access)
CIP	Kritik Altyapı Koruma (Critical Infrastructure Protection)
CIWIN	Kritik Altyapı Erken Bilgi Ağı (Critical Infrastructure Warning Information Network)
CSSP	Denetim Sistemleri Güvenlik Programı (Control Systems Security Program)

Kısaltmalar	Açıklama
DB	Veritabanı (Database)
DDS	Dağıtık Denetim Sistemleri
DCS	Dağıtık Denetim Sistemleri (Distributed Control Systems)
DNS	Alan Adı Sunucusu (Domain Name Server)
DNP	Dağıtık Ağ Protokolü (Distributed Network Protocol)
DOS	Hizmet Durdurma/ Servis Engelleme Saldırısı (Denial Of Service)
EDH	Ephemeral Diffie-Hellman Anahtar Değişim Algoritması
EDS	Endüstriyel Denetim Sistemleri
EPCIP	Kritik Altyapıları Korumak için Avrupa Programı (European Programme For Critical Infrastructure Protection)
EPDK	Enerji Piyasası Düzenleme Kurulu
FERC	ABD Federal Enerji Düzenleme Komisyonu (Federal Energy Regulatory Commission)
FR	Paket Anahtarlamalı Veri Devresi (Frame Relay)
GPRS	Genel Paket Radyo Veri Hizmeti (General Packet Radio Service)
GSM	Mobil İletişim için Küresel Sistem (Global System For Mobile Communications)
HMI	İnsan-Makine Arayüzü (Human-Machine Interface)
HTTP	Hiper Metin Aktarım Protokolü (Hypertext Transfer Protocol)
ICS	Endüstriyel Denetim Sistemleri (Industrial Control Systems)
IEC	Uluslararası Elektroteknik Komisyonunu (International Electrotechnical Commission)
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü (The Institute of Electrical and Electronics Engineers)
INL	Idaho Ulusal Laboratuarı (Idaho National Laboratory)

Kısaltmalar	Açıklama
IP	İnternet Protokolü (Internet Protocol)
ISA	Enstrümantasyon, Sistem ve Otomasyon Topluluğu (Instrumentation, Systems and Automation)
ISAKMP	İnternet Güvenliği Birliği ve Anahtar Yönetimi Protokolü (Internet Security Association And Key Management Protocol)
ISID	Endüstriyel Güvenlik Olayları Veritabanı (Industrial Security Incident Database)
ISO	Uluslararası Standartlar Organizasyonu (International Organization For Standardization)
L2TP	İkinci Katman Tünelleme Protokolü
LTE	Dördüncü Nesil Mobil Telekomünikasyon Erişim Tekniği (Long Term Evolution)
MAC	Ortam Erişim Denetimi (Media Access Control)
MTU	Master Terminal Birim (Master Terminal Unit)
NERC	Kuzey Amerika Elektrik Emniyeti Kuruluşu (North American Electric Reliability Corporation)
NIST	ABD Ulusal Standartlar ve Teknoloji Enstitüsü (National Institute of Standards And Technology)
OCTAVE	İşlevsel Kritik Tehdit, Varlık ve Açıklık Değerlendirmesi (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
OI	Operasyonel Etki (Operational Impact)
OSI	Açık Sistem Arabağlantısı (Open Systems Interconnection)
PCSRF	Süreç Denetimi Güvenlik Gereksinimleri Forumu (Process Control Security Requirements Forum)
PDU	Protokol Veri Birimi (Protocol Data Unit)

Kısaltmalar	Açıklama
PLC	Programlanabilir Mantıksal Denetleyici (Programmable Logic Controller)
PPTP	Noktadan Noktaya Tünelleme Protokolü (Point-To-Point Tunneling Protocol)
RD	Risk Değerlendirmesi
RTU	Uzak Uç Birim (Remote Terminal Unit)
SCADA	Merkezi Yönetim, Denetleme ve Veri Toplama Sistemi (Supervisory Control And Data Acquisition)
SHA	Güvenli Sağlama Protokolü (Secure Hash Algorithm)
SPP	Sistem Koruma Profili (The System Protection Profile)
SQL	Yapılandırılmış Sorgu Dili (Structured Query Language)
SSEMP	Elektrik Piyasası Katılımcıları için Güvenlik Standardı (Security Standart For Electric Market Participants)
STOE	Sistem Hedef Değerlendirme (System Target of Evaluation)
TCP	Aktarım Denetim Protokolü (Transport Control Protocol)
UI	İstenmeyen Olay (Unwanted Incident)
VPN	Sanal Özel Ağ (Virtual Private Network)
WiMax	Mikrodalga Erişim için Dünya Çapında Birlikte Çalışabilirlik (Worldwide Interoperability for Microwave Access)
xDSL	Sayısal Abone Hatları (Digital Subscriber Line)

1. GİRİŞ

Bilgi ve iletişim teknolojilerinde ilerleme, beraberinde birçok alanın gelişmesini ve ilerlemesini sağlamıştır. En önemli vasıtası internet olmak üzere, sayısallaşmanın ve her yerden erişilebilirliğin yaygınlaşması farklı sektörlerdeki iş yapış ve hizmeti sunuş şekillerini de değiştirmiştir. Bu bağlamda bilgi ve iletişim teknolojilerinin, diğer sektörlerin değişimi ve gelişimi yönünde lokomotif görevi gördüğünü söylemek mümkündür. Ancak bu değişim beraberinde yalnızca yeni imkân ve fırsatları değil önceden var olmayan güvenlik zafiyet ve risklerini de getirmiştir.

Bunlarla sınırlı olmamakla birlikte, enerji, su, ulaşım, sağlık, bankacılık, nükleer/kimyasal tesisler ve haberleşme altyapıları ABD (Amerika Birleşik Devletleri) ve AB (Avrupa Birliği) ülkeleri başta olmak üzere birçok ülke için kritik sektörler olarak belirlenmiş ve bu sektörlere ilişkin altyapılar ise ülke kritik altyapıları olarak nitelendirilmiştir. Kritik altyapı tanımlamalarındaki ortak özellik, bu kapsamdaki altyapıların zarar görmeleri veya işlevsiz kalmaları durumunda ülke ekonomilerinin, kamu can ve mal emniyetinin, ortaya çıkan durumdan ötürü tehlikeye düşmesi veya olumsuz etkilenmesidir [1-5].

Elektrik, doğalgaz, petrol, su üretim, iletim ve dağıtım altyapıları ile birçok modern endüstriyel üretim tesisleri ülkeler için kritik altyapılar olmakla birlikte, bunları diğer altyapılardan farklı kılan ortak özellikleri sahadaki fiziki süreç ve unsurlarını "denetim sistemleri" marifetiyle izlemeleri ve yönetmeleridir. Dolayısıyla, bu tür kritik altyapılardaki denetim sistemlerine yönelik yetkisiz erişim ve müdahaleler, sadece sayısal ortamlardaki değil gerçek dünyadaki kritik fiziki varlıklar üzerinde de yetkisiz erişim ve müdahaleleri mümkün kılacaktır.

Birçok kritik tesis ve altyapıyı izlemek ve yönetmekte kullanılan "Dağıtık Denetim Sistemleri (DDS)" veya literatürde ve endüstride sıkça kullanıldığı haliyle "SCADA sistemleri" tasarlanırken henüz internet dünya geneline yaygın olmadığı gibikablolu ve kablosuz erişim teknolojilerinde bugünkü imkânlarla kıyaslanamayacak ölçüde kısıtlıydı [6]. DDS ağlarda diğer BT (Bilişim Teknolojileri) ağlarından izole

yapıdaydı [7].Üstelik kullanılan işletim sistemi ve uygulamaların güvenlik açıklıkları da kapalı ağlarda çalıştırılmanın verdiği yanıltıcı güven algısı nedeniyle yeterince dikkate alınmamaktaydı. Ancak günümüz koşullarında "mutlak kapalı ağ yapıları" neredeyse kalmamış olup, tüm ağ ve sistemler için, internet başta olmak üzere dış dünyadan gelecek tehditlere karşı sürekli ve sürdürülebilir tedbirler almak gerekli hale gelmiştir.

Günümüzde bilgi ve iletişim teknolojilerinde kullanılan altyapı bileşenlerinde hızlı bir tek tipleşmenin yaşandığı gözlenmektedir. Artık özel tasarım işletim sistemi, iletişim protokolü ve ağ arayüzleri yerine internet odaklı, genel amaçlı ve hazır ürünler üzerine tasarımların geliştirildiği ve piyasaya arz edildiği görülmektedir. Günümüz DDS bileşenleri de birçok alanda olduğu gibi hazır donanım ve yazılım bileşenleri üzerinde geliştirilmektedir [7]. Örneğin, BTağlarındaki veri haberleşmesinde neredeyse tamamen Ethernet arayüzünün ve IP (Internet Protokolü) protokolünün kullanıldığı günümüzde, endüstriyel denetim sistemlerine özel arayüz ve protokol tasarımı yapılmasını beklemek gerçekçi bir yaklaşım değildir. Nitekim DDS sistem üreticilerinin yeni nesil ürünleri incelendiğinde, aynı haberleşme arayüzlerini ve IP protokolünü kullandığı görülmektedir [8]. Dolayısıyla BT altyapısı için geliştirilen ve kullanılan donanım, işletim sistemi, ağ arayüzü ve protokollerinin kullanılmaya başlandığı DDS altyapılarına yönelik güvenlik açıklıkları BT altyapılarında var olanlarla büyük ölçüde benzerlik göstermektedir. Ancak gördükleri işlev ve uğrayacakları saldırılar sonucunda ortaya çıkacak etkiler açısından taşıdıkları siber güvenlik riskleri önemli farklılıklar arz etmektedir.

Farklı ülkelerde DDS altyapıların siber güvenliğine ilişkin akademik ve devlet destekli çalışmalaryürütüldüğü gözlenmektedir. Son yıllarda DDS sistemlere yönelik siber saldırılardaki artış ile birlikte konuya olan dikkatin de arttığı söylenebilir. Ülkemizde ise, denetim sistemlerine dayalı üretim, iletim ve dağıtım yapan kritik altyapıların güvenliğine ilişkin kısıtlı sayıda çalışma bulunmaktadır. Ancak Türkçe literatürde, 2008 yılından bu yana devam eden bu tez çalışması sürecinde üretilen yayınlar [9-12] dışında, konunun Ünver ve ark. [4], Karabacak [5] ile Kara ve ark. [13] tarafından da ele alındığı, tüm bu çalışmaların ülkemizde kritik altyapı ve

denetim sistemlerinin güvenliğine ilişkin farkındalığın oluşmasına katkılar sağladığı gözlenmiştir. Türkçe literatürde eksiklik devam etmekte olup, bu tez çalışması, ülkemizde hissedilen bu eksikliği bir ölçüde gidermeyi veböylece güvenli altyapıların oluşturulmasına katkılar sağlamayıamaçlamaktadır. Bu amaca ulaşılabilmesi için, öncelikle dünyadaki benzer çalışmaların incelenmesine, literatürdeki güvenlik açıklıkları ve olaylarının irdelenmesine ve Türkiye'deki mevcut durumunun araştırılmasına ihtiyaç duyulmuştur. Bu bağlamda yapılan literatür incelemeleri ve saha araştırmalarından elde edilen veri, bilgi ve bulgulardan yararlanarak, güvenlik açıklıklarının ve açıklık kaynaklarının belirlenmesi ve giderilmesine yönelik çalışmalar yürütülmüştür.

Bu çalışmada öncelikle, iş süreçlerini DDS ile izleyen ve yöneten kritik altyapılara yönelik uygulanabilir, gerçekçi ve kapsamlı bir güvenlik yaklaşımı geliştirmek için literatürde yer alan yaklaşımlar ve farklı ülke uygulamaları incelenmiştir. Devamında, iki farklı ve önemli kritik altyapı işletmecisiyle çalışmalar yürütülmüş ve buradan elde edilen veri, bilgi, deneyim ve sınama/araştırma sonuçlardan yararlanılarak, önceden tanımlı istenmeyen olaylara dayalı olarak olası tüm güvenlik açıklıklarının kritiklik sıralamasını bulmakta kullanılabilecekyaklaşım geliştirilmiş ve böylece giderilmesi öncelikli açıklıkların belirlenmesi hedeflenmiştir. Ayrıca, olasıtüm güvenlik açıklıklarını gidermeye yönelik olarak, ülkeler ve işletmeler özelinde uygulanması önerilen güvenlik iyileştirmeleri, yönetimboyutunda, işletmeboyutundave teknik boyutta ele alınmıştır. Türkiye incelemesi ve saha çalışmalarındaki gözlemlere dayalı olarak önerilerde bulunulmuştur. Bu öneriler ayrı birer belge olarak EK-3 (Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi), EK-4 (Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi) ve EK-5'de (42 Kritik İyileştirme Adımı-Kontrol Listesi) sunulmuştur. EK-1 'Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları' belgesi ise farklı araştırmacıların benzer çalışmalarında yararlanabilmesi için eksiksiz verilmiştir. Öte yandan, saha incelemelerinde elde edilen somut açıklık bulgularını ve işletmeciye özel önerileri içeren EK-2 belgesinin tam hali ise yayımlanmamıştır.

İkinci bölümde DDS altyapıları ve bileşenleri genel olarak incelenmiştir. Ayrıca kullanılabilecek erişim ortam ve teknikleri ile endüstride sıkça kullanılan iletişim protokollerine yer verilmiş, Modbus protokolü özelinde, endüstriyel iletişim protokollerinin yapısı ve gelişim süreci ele alınmıştır.

Üçüncü bölümde, siber güvenlik risk değelerlendirmesine ilişkin temel kavram ve tanımlara yer verilmiş, literatürdeki mevcut yöntem ve yaklaşımlardan bazıları incelenmiştir.

Dördüncü bölümde, literatürde yer alan önemli güvenlik olaylarına yer verilmiş, AB ve ABD örneğinde kritik altyapıların siber saldırılara karşı korunması hususunda yürütülen önemli bazı çalışmalara değinilmiştir. Ayrıca ABD'de yürütülmüş iki önemli çalışma sonrasında yayımlanan raporlarda yer alan önemli açıklık bulguları ileriki tartışmalara zemin oluşturması bakımından burada sunulmuştur.

Beşinci bölümde, odak noktası dağıtık denetim sistemleri kullanan kritik altyapılar olmak üzere, çeşitli bilgi ve bilgi sistemleri güvenliği standartları, rapor ve rehber niteliğindeki dokümanları incelenmiş, farklı alt başlıklarda bu dokümanların birbirleriyle karşılaştırılmasına yer verilmiş, böylece mevcut standartların güçlü, birbirlerinden farklı ve eksik yanlarının da ortaya konulabilmesi hedeflenmiştir.

Altıncı bölümde, yürütülen saha çalışmalarında nelerin hedeflendiği, inceleme yönteminin başlangıçta neye göre ve nasıl tarif edildiği, ne şekilde sürdürülebildiği ve nerede hangi inceleme araçların kullandığı açıklanmıştır.İncelemeler sonrasında elde edilen somut açıklıkların hangi eksiklik ve kusurlardan kaynaklandığı burada sunulmuştur.

Yedinci bölümde DDS sistemler için varlıklar, güvenlik açıklıkları, saldırı hedef ve biçimleri tanımlanmıştır. Ayrıca iki örnek durum incelemesi için tanımlı istenmeyen olaylara bağlı kalarak, her bir Örnek Durum için olası tüm açıklıkların önem sıralamasının yapılmasına imkân veren ve her bir açıklık için nicel bir kritiklik değeri belirleyebilen bir hesaplama yaklaşımı önerilmiştir.

Son olarak sekizinci bölümde, saha gerçekleri, öncelikleri ve eksiklikleri dikkate alınarak ülkeler ve işletmeler özelinde uygulanması önerilen güvenlik iyileştirmeleri yönetim boyutuyla, işletme boyutuyla ve teknik boyutta ele alınmıştır. Yönetim boyutunda yapılması gerekenler güvenlik iyileştirmeleri Türkiye özelinde tartışılmış, gözlenen mevcut eksiklik ve problemlerin giderilmesine yönelik çözüm önerileri bu bölüm içerisinde sunulmuştur.

Bu çalışma kapsamında, farklı üretim ve dağıtım noktalarındaki iş süreçlerini otomatize etmek için bilgi ve iletişim teknolojilerine dayalı denetim sistemlerini yoğun olarak kullanan kritik altyapı ve tesislerin siber güvenliği ele alınmıştır. Olası güvenlik açıklıkların giderilmesine yönelik çözüm önerileri araştırılmış, saha ihtiyaç ve gerçekleriyle uyumluluk kriterleritemel alınaraksadece güvenlik açıklıklarını değil açıklık kaynaklarını da giderecek biçimde bütüncül bir çözüm yaklaşımının ortaya konumasıhedeflenmiştir. Karar vericiler ve işletmeciler için EK-3 ve Ek-4'de sunulan siber güvenlik strateji, eylem planı belgeleri üretilmiş ve ilgililerinin kullanımına sunulmuştur.

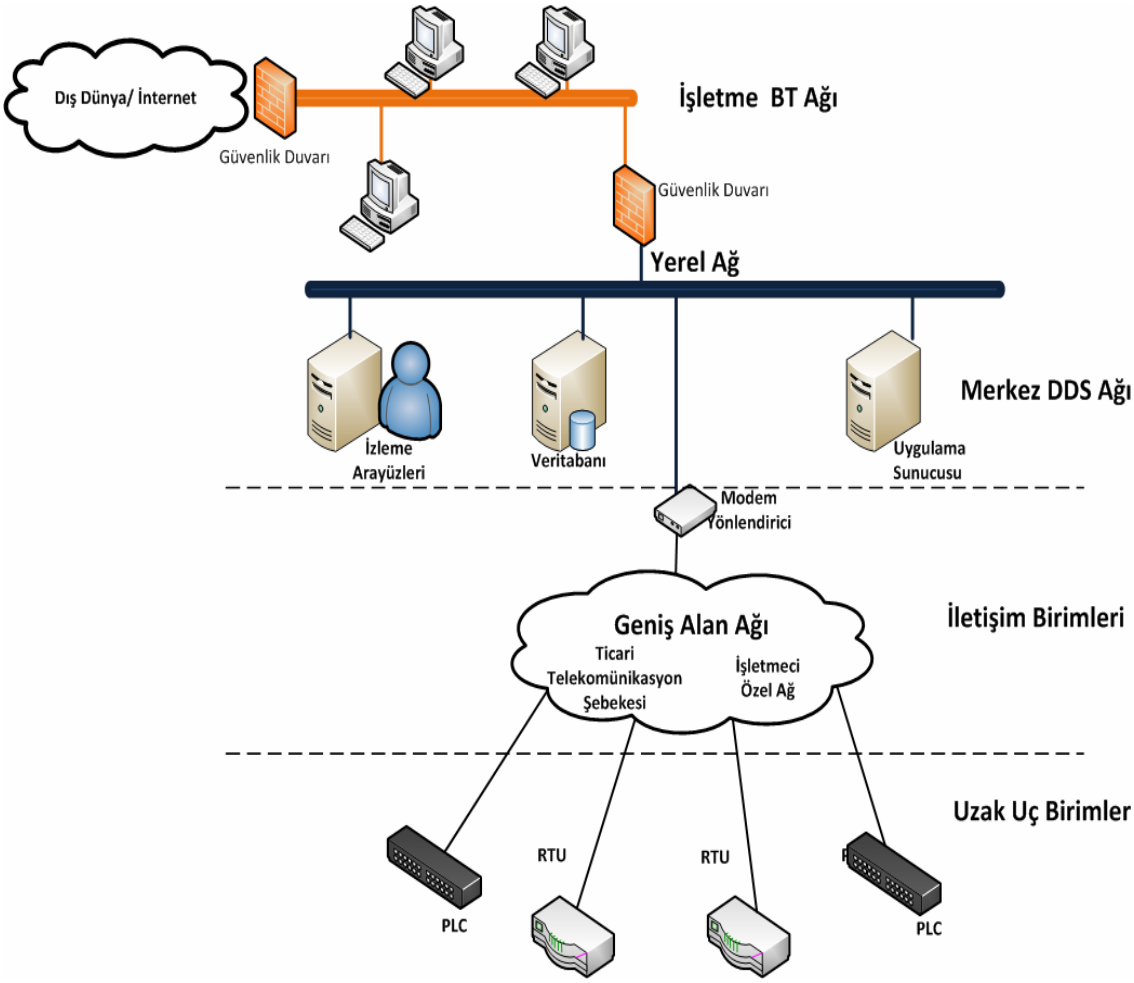
2. DAĞITIK DENETİM SİSTEMLERİ VE ALTYAPI BİLEŞENLERİ

Dağıtık Denetim Sistemleri (DDS), çeşitli üretim, iletim ve dağıtım altyapılarındaki süreçleri izlemek ve yönetmek için uzaktan yönetilebilen denetim birimlerinin doğrudan veya dolaylı olarak bağlı olduğu bir merkez üzerinden kumanda edildiği altyapılara verilen genel bir isimdir. Denetlenen alanın farklı coğrafi noktalarda konuşlanmış bileşenlerden oluşması nedeniyle de dağıtık ifadesi kullanılmaktadır. Örneğin belirli bir bölge veya ülke ölçeğinde hizmet veren elektrik iletim ve dağıtım şebekeleri yüzlerce ayrı noktada binlerce süreç veya cihazın uzaktan yönetimi ile gerçekleştirildiği için bu tür izleme ve kumanda etme sistemleri, dağıtık denetim sistemleri olarak adlandırılmaktadır.

SCADA, benzer şekilde belirli bir alandaki üretim tesislerinde ve/veya geniş bir coğrafyadaki dağıtım tesislerinde süreç ve kaynaklarının yönetiminde kullanılan denetim sistemlerinin en çok bilinen adı olarak nitelendirilebilir. Farklı birçok kaynak incelendiğinde, "DDS" ifadesinin SCADA ile eşdeğer kullanıldığı veya "merkezi denetim birimi birkaç alana bölünmüş SCADA" sistemi anlamında kullanıldığı görülmektedir. Bu çalışma kapsamında DDS ifadesi SCADA tanımının yerine veya birlikte kullanılacaktır. Yine literatürdeki farklı kaynaklarda kullanıldığı şekliyle, "Endüstriyel Denetim Sistemleri" ifadesine de yer yer başvurulacaktır.

DDS sistemler temel olarak aşağıdaki üç bileşenden oluşurlar. Bunlar, Merkez Birim, Uzak Uç Birim ve İletişim Birimleridir [14].

Şekil 2.1'de SCADA/DDS ağ ve bileşenlerine ait genel bir görünüş yer almaktadır. Bu şekilde yer alan bileşenler takip eden altbaşlıklarda açıklanmıştır.



Şekil 2.1. SCADA/DDS ağı ve bileşenleri

2.1. Merkez Birim

"Yönetici Birim" veya "Ana Kumanda ve İzleme Birimi" olarak da adlandırılabilir. Sahadaki tüm uç birimlerinin kumanda edildiği, izlendiği, ölçüm sonuçlarının alındığı ve saklandığı birimdir.

Merkez Birimde, işlemci, bellek, disk ve ağ arayüzlerinden oluşan bilgisayar donanımları; genel veya özel amaçlı işletim sistemleri ve bu işletim sistemlerinin üzerinde izleme, denetleme, depolama ve raporlama yazılımları bulunabilir [14]. DDS altyapı mimarisine bağlı olarak birden fazla ve birden farklı yönetici/ana birim kullanılabilir.

Merkez birim yazılımları, genel olarak şu iki temel fonksiyonu yerine getirmek üzere tasarlanır. Birincisi, uzak uç birimlerden alarm ve verileri toplayıp işlemek ve bunları raporlamak üzere saklamaktır. İkincisi ise, uçlardan toplanan verileri değerlendirerek tekrar uç birimlere gönderilmek üzere uygun komutlar üretmektir [14].

Merkez Birim, hem nihai karar alma hem de sistemin hafızasını tutması bakımından altyapının en önemli birimidir. Burada meydana gelebilecek bir arıza veya saldırı tüm şebekeyi etkileyecek kapsama sahiptir.

Merkez Birimdeki doğrudan varlıklar aşağıda verilen alt başlıklarda sıralanmıştır. Sunucu donanımları,

- İş istasyonu donanımları,
- İşletim sistemleri,
- Uygulama yazılımları ve
- Veri tabanları.

Şekil 2.1'de de gösterildiği üzere, DDS merkez birimin aynı zamanda doğrudan veya bir güvenlik duvarı üzerinden işletme iş ağına bağlı olması yer yer görülebilen bir durum olup böyle bir bağlantı merkez birimin ve dolayısıyla tüm altyapının güvenliği üzerinde önemli olumsuz etkileri bulunmaktadır.

2.2. Uzak Uç Birimler

Uzak Uç Birimler, sahada izlenmesi ve yönetilmesi gereken süreçleri uzaktan yönetmek için kullanılan uç birim cihazlardır. Bu cihazlar genellikle karar verme mekanizmalarına sahip olmayıp, donanımsal ve yazılımsal bileşenleri kısıtlıdır. Uç birim cihazlar çoğunlukla, gerçek zamanlı ve önceden tanımlı işlemleri yürütmek üzere tasarlanmışlardır.

Uzak uç birimler, merkezin gözü, kulağı ve eli gibi çalışırlar. Sahadan topladıkları verileri işler ve ilgili verileri merkez birime aktarırlar. Benzer şekilde merkezden aldıkları komutları da sahaya iletirler [15].

Birer uç birim cihaz olarak RTU ve PLC'lerin farklı kaynaklarda eş anlamlı olarak kullanıldığı görülebildiği gibi kimi kaynaklarda farklı yönleriyle de ele alınabilmektedir. Örneğin pazarın önemli oyuncularından Motorola, RTU için gerçek zamanlı olmayan işletim sistemi kullanan birim, PLC içinde gerçek zamanlı işletim sistemi kullanan saha birimi ayrımını yapmaktadır [16]. Ghosh [17] ise günümüz birçok RTU ekipmanını, standart bilgisayar donanımlarını ve programlanabilir mantıksal denetleyiciler (PLC) üzerine oluşturulduğunu ifade etmektedir. Daha farklı kaynaklarda PLC ve RTU ürün ve tanımlamaları için başka benzerlik ve farklılıklara da rastlamak mümkündür. Ancak bu çalışmada RTU ile elektriksel sinyalleri ve adreslenebilir giriş çıkışları kullanarak sahadan veri toplayan ve merkezden aldığı komutları sahadaki birimlere ileten; aynı zamanda merkez ile bir iletişim protokolü üzerinden ve uzak alan bir iletişim kanalı kullanarak haberleşen DDS uç birim cihazları kast edilmektedir. Bu nedenle, çalışmada PLC ifadesi daha kapsayıcı olan RTU ifadesi ile birlikte kullanılacaktır. Farklı bir tanım olarak 'saha birimleri' ise, RTU'lar ile birlikte sensörleri ve mekanik birimleri de içerecek biçimde kullanılacaktır.

2.3. İletişim Birimleri

İletişim birimleri, merkez ve uç birimler arasındaki haberleşmeyi sağlayan erişim ortamları, arayüz ve teknikleri ile iletişim protokollerini kapsar.

İletişim birimde yer alan varlıklar şu şekilde sıralanabilir:

- Ağ anahtarları,
- Modemler,
- Yönlendiriciler,

- Ağ geçitleri / Protokol-ortam dönüştürücüler,
- Kablolu veya kablosuz erişim ortamları,
- Endüstriyel iletişim protokolleri.

Aşağıda, güvenli iletişim açısından iletişim birimlerinin iki önemli unsuru olan erişim ortam ve teknikleri ile endüstriyel iletişim protokolleri alt başlıklarda ele alınmıştır.

2.3.1. Erişim ortamı ve teknikleri

Merkez ve uç birimler arasındaki veri akışını mümkün kılan uzak alan haberleşmesini sağlamak için farklı erişim şekillerine dayanan iletişim teknikleri kullanılabilir. Günümüzde, işletmenin coğrafi dağınıklık durumu ile edinilebilen iletişim teknik ve servislerinin sağladıkları imkânlara bağlı olarak farklı DDS işletmecilerinin farklı iletişim tekniklerinin tercih ettiği görülmektedir. Bu teknik ve servisleri en genel haliyle kablolu veya kablosuz; ticari veya özel erişim altyapıları olarak nitelendirmek mümkündür.

Veri iletişimi için bugünkü iletişim tekniklerinin tümünü DDS altyapıları için de kullanmak mümkündür. Ancak kullanılacak iletişim tekniklerinin düşük band genişliğine karşın çok sayıda nokta ihtiyacını makul fiyatlarda karışılıyor olması ve güncel güvenlik gerekliliklerini sağlıyor olması gerekir.

Bugün için Türkiye'de ve gelişmiş ülkelerin çoğunda veri iletişimi için ticari servis olarak sunulan devre tabanlı kiralık hatlar, paket temelli FR, hücre temeli ATM, noktadan noktaya bağlantı imkânı da sağlayabilen xDSL gibi kablolu iletişim teknikleri DDS haberleşmesi için de kullanılabilecektir. Benzer şekilde kablosuz GSM, GPRS, CDMA ve WiMAX şebekeleri de DDS altyapısındaki merkez ve uç bileşenlerin haberleşmesi için erişim teknikleri arasındadır. Ayrıca saha çalışmalarında görüldüğü üzere DDS işletmeleri, iletişim giderlerini kısmak veya ticari erişim sağlayıcılara bağımlı kalmamak için kendi erişim altyapılarını kurma ve kullanma yoluna da gidebilmektedir. Bu açıdan işletmeciler için en elverişli yol

kiralanabilir özel tahsisli frekans bandlarını kullanmaktır. İşletmenin faaliyet alanına bağlı olarak kendi kablo altyapısını kurması veya mevcut enerji hatlarını kullanması da olası erişim imkânları içerisindedir.

Uzak alan haberleşmesi için hangi erişim tekniği kullanılırsa kullanılsın, yerel alanda tıpkı BT sistemlerde olduğu gibi DDS sistemlerin saha birimlerinde bugün için hala kullanılan seri iletişim (RS-232, RS 485, RS 422) şekilleri tamamen terk edilerek uçtan uca IP (Internet Protokolü) kullanan ve Ethernet ağ bağlantı arayüzüne sahip cihazlar kullanılacaktır [8].

Merkez Birimlerin fiziki sınırları belli ve genel olarak korunaklı iken, haberleşme ortamları herkese açık (kablosuz) veya bir kısım insanların erişimine açık (kablolu) durumdadır. Bu yönüyle, erişim biçiminin kablolu veya kablosuz oluşu, kullanılan erişim tekniğinin veri gizleme ve bütünlük kontrolü gibi güvenlik fonksiyonlarına sahip olup olmadığı, DDS iletişiminin ve dolayısıyla tüm altyapının güvenliğiyle ilişkilidir. Erişim tekniğinin sağladığı güvenlik fonksiyonlarına ilaveten, kullanılan iletişim protokolünün güvenliğinin de ayrıca tartışılması gerekir.

2.3.2. Endüstriyel iletişim protokolleri

DDS sistemlerde Merkez-Uç Birim haberleşmesinde ağırlıklı olarak kullanılan iletişim protokolleri Çizelge 2.1.'de yer almaktadır.

Çizelge 2.1. DDS İletişim Protokolleri [18]

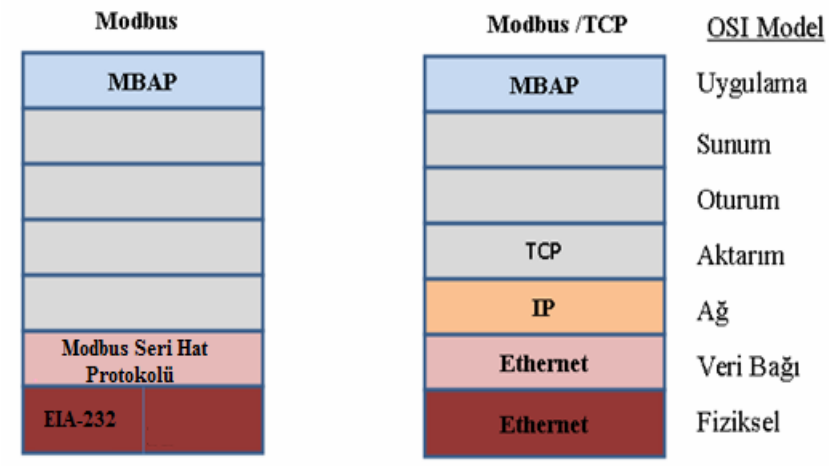
DDS İletişim Protokolü	**Organizasyon / Standart Adı**
Ethernet /IP	Open DeviceNet Vendors Association www.odva.org
ControlNet	ControlNet International www.controlnet.org
PROFIBUS	IEC Standart 11674 ve 61158 www.profibus.org
MODBUS TCP/IP	MODBUS-IDA www.modbus.org
DNP3	IEC Technical Committee 57 Working Group 03 Standart
Foundation Fieldbus	The Fieldbus Foundation Open Standart Protocol www.fieldbus.org

Çizelge 2.1.'de yer alan endüstriyel iletişim protokolleri arasından Modbus, örnek olarak seçilmiş ve aşağıda daha yakından incelenmiştir. Böylece, Modbus özelinde olsa da, endüstriyel protokollerin yapısı ve zaman içerisinde değişen ihtiyaçlara göre ortaya çıkan çeşitliliklerine kısaca değinilmiştir.

Modbus, ilk kez 1979 yılında Modicom firmasınca tasarlanan ve bugün otomasyon pazarında önemli bir standart haline gelen endüstriyel haberleşme protokolüdür. Hem üreticiler hem de açık kaynak topluluklarınca sürekli geliştirilen ve desteklenen bir protokol olmayı da başarmıştır [9].

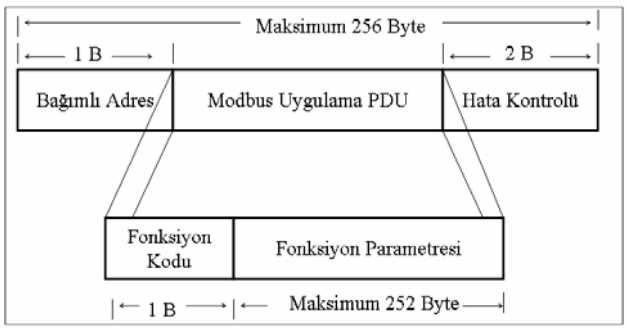
Modbus, esasen iki katmanlı olan ve istemci-sunucu mimarisinde seri link üzerinde çalışan bir protokoldür. Bugün ise farklı fiziksel katmanlarda çalışabilen farklı Modbus türleri mevcuttur. Bunlardan ikisi, MODBUS Seri ve MODBUS TCP'dir.

Şekil 2.2.'de bu üç türün OSI katmanlarına göre sınıflandırılması görülmektedir.



Şekil 2.2. OSI katmanlarına göre MODBUS Seri ve MODBUS TCP karşılaştırması [19]

İki birim (istemci-sunucu veya yönetici-bağımlı) arasında gönderilen mesajın çerçevesi, kullanılan Modbus protokolünün çeşidine göre değişiklik gösterir. Temel Modbus mesajlaşması olan seri haberleşme mesaj formatı Şekil 2.3.'te verilmiştir.

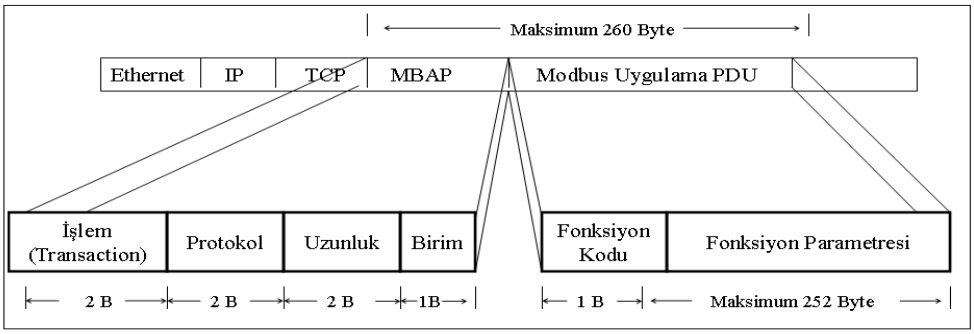


Şekil 2.3. Modbus seri haberleşme mesaj formatı [20]

Şekil 2.3.'ten anlaşılacağı üzere Modbus seri haberleşme formatı, *Adres Birimi, Protokol Veri Birimi(PDU) ve Hata Kontrol Birimi* olarak üç farklı bileşenden oluşur. PDU ise şu iki bileşenden meydana gelir [20]:

(i) Mesajın amacını tanımlayan fonksiyon kodu,
(ii) Fonksiyonun yürütülmesine (talep için) veya sonuçlarına bağlı fonksiyon parametreler.

Modbus TCP, Modbus Seri ile aynı protokol veri birimine sahiptir. İki Modbus çeşidinin mesajları arasındaki fark, PDU haricindeki çerçevelerdeki farklardır. Şekil 2.4. 'te Modbus TCP mesaj yapısı gösterilmiştir [20].



Şekil 2.4. Modbus TCP mesajı [20]

Modbus TCP, diğer OSI alt katman başlıkları haricinde, Modbus Seri'den farklı olarak Modbus Uygulama Protokolü (MBAP) başlığını içerir [21].

Modbus sunucu birimi, TCP 502'inci porttan kendisine gelecek istekleri dinler. Modbus istemci birimi ise sunucunun 502'inci portuna bağlantı isteğinde bulunarak TCP iletişim kanalını açar. Açılan tek bir TCP kanal üzerinden istemci-sunucu birimler arasında birden çok işlem yürütülebilir [20].

Veri alanı, fonksiyon kodları ile tanımlı işlemlerin tamamlanması için gerekli ilave bilgiyi sunucu birime sağlar. Modbus uygulama protokolündeki veri birimde yer alan fonksiyon kodlarının her biri bir işlemi tanımlar. Temelde, Modbus üç tür fonksiyon koduna sahiptir. Bunlar [9,21]:

- *Genel:* Tanımlanmış ve belgelendirilmiş fonksiyonların kullandığı kodlardır. Her türlü topluluk ve üretici tarafından kabul edilen ve kullanılan Modbus fonksiyonlarıdır.
- *Kullanıcı Tanımlı:* 65-72 ve 100-110 arasında tanımlı, özel tasarlanan Modbus fonksiyonları için kullanılan kodlardır. Üreticiden üreticiye değişir ve farklı ürün ve sürümlerde bu kodlar için uyumluluk garantisi yoktur.
- *Ayrılmış:* Üreticilerin daha önceki ürünlerinde kullanmış olduğu ve genel kullanıma kapalı olan kodlardır.

Çizelge 2.2.'de tüm ürün ve üreticilerde ortak kullanılan Modbus genel fonksiyon kodları verilmiştir.

Çizelge 2.2. Modbus genel fonksiyon kodları [9]

			Fonksiyon Kodları	
	Fiziksel Birim	**Yürütülen Fonksiyon**	**Ondalık Taban**	**Onaltılık Taban**
Veri Erişimi	Fiziksel Ayrık Giriş Dahili Bitler Fiziksel Sarmal	Ayrık Girişleri OKU	02	02
		Sarmal OKU	01	01
		Tek Sarmal YAZ	05	05
		Çok Sarmal YAZ	15	0F
	Fiziksel Giriş Kayıtçısı	Giriş Kayıtçısını OKU	04	04
		Tutucu Kayıtçısı OKU	03	03
		Tek Kayıtçıya YAZ	06	06
	Dahili Kayıtçı veya Fiziksel Çıkış Kayıtçısı	Çoklu Kayıtçıya YAZ	16	10
		Çoklu Kayıtçıya OKU/YAZ	23	17
		Kayıtçıya YAZ	22	16
		FIFO Kuyruğunu OKU	24	18
	Dosya Kayıt Erişimi	Dosya Kayıtçısını OKU	20	14
		Dosya Kayıtçısını YAZ	21	15
		İstisna durumlarını OKU	07	07
	Tanılar	Tanı	08	08

Çizelge 2.2. (Devam) Modbus genel fonksiyon kodları [9]

		Port Durum Sayacını AL	11	0B
		Port Durum Günlüğünü AL	12	0C
		Bağımlı (Slave) ID Raporla	17	11
		Aygıt Tanımlayıcısını OKU	43	2B

Modbus protokolü de dahil olmak üzere, Çizelge 2.1'de yer alan DDS protokolleri başlangıçta tasarlanırken, DDS sistemlerin siber saldırılara karşı güvenlik gereksinimleri yeterince dikkate alınmamıştır [22-23]. Bu nedenle, bu protokollerin taşıdıkları veriyi gizleme, bütünlük kontrolünü gerçekleştirme gibi bugünkü şartlarda hayatiyet kazanmış güvenlik fonksiyonlarını sağlamamaktadır. Dolaysıyla iletişim kanallarına sızılması durumunda, DDS iletişim protokollerinin taşıdıkları veri ve komutların elde edilmesi ve değiştirilmesi mümkün olabilmektedir.

3. SİBER GÜVENLİK RİSK DEĞERLENDİRME YAKLAŞIMLARI

Bir sürecin, organizasyonun, tesis veya sistemin ne derece güvende olduğu ve nasıl daha güvenli hale getirilebileceğini saptamak, iyileştirme ve güvenli bir model önerisinde bulunabilmek için güvenlik risk saptama ve değerlendirmesinin yapılması bir gereklilik olarak ortaya çıkmaktadır.

Kritik işlev görev DDS sistemlerin siber saldırılardan kaynaklı güvenlik risklerin belirlenebilmesi için siber saldırıların oluşabilme ihtimalinin ve saldırılar sonrası ortaya çıkabilecek olumsuz etkilerinin şiddetinin öngörülmesine ihtiyaç vardır. Bir siber saldırının olma olasılığı ise mevcut tehdit kaynaklarının ve açıklıkların belirlenebilmesi ile mümkün olacaktır.

3.1. Güvenlik Risk Değerlendirmesi ve İlgili Kavramların Tanımlanması

İstenmeyen bir olayın olma ihtimali ve belirli bir varlık için olay sonrası etkileri şeklinde de tanımlanabilir [24]. ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), SP 800-30 isimli Bilgi Teknolojileri Sistemleri için Risk Yönetimi Rehberinde riski, bir sistem veya organizasyonu olumsuz etkileyecek bir olayın, sistemdeki potansiyel bir güvenlik açıklığının kullanılmasıyla ortaya çıkaran tehdittin gerçekleşmesi ihtimalinin fonksiyonu olarak tanımlanmaktadır [25]. Bu tanımdan hareketle, aynı güvenlik açıklığının farklı sistemler ve organizasyonlar için farklı bir risk değeri üreteceği yorumu yapılabilir. Bu nedenle, bir organizasyondaki güvenlik risklerinden bahsederken, risklerin değerlendirilmesi ve yönetilmesi süreci de dahil olmak üzere ilgili tüm tanımları yapmak gerekecektir.

Aşağıda, öncelikli olarak risk değerlendirmesi yapılırken kullanılacak olan kavramlara ilişkin tanımlar yer almaktadır.

Varlık (Asset): Korunması gereken fiziki varlıklar ve/veya bilgi varlıkları ile iş sürekliliği, saygınlık, can ve mal güvenliği gibi kıymetleri kapsar [25,26].

Açıklık (Vulnerability): Bir varlığı tehditlere karşı korumasız hale getiren her türlü unsur (sistem bileşenlerinden; güvenlik politika ve prosedürlerinin yokluğundan, yetersizliğinden veya uygulanmayışından; eksik veya hatalı sistem tasarım ve uygulamalarından; organizasyon yapısı, yönetici ve çalışanların bilgi birikimi ve tutumundan kaynaklı nedenler) olarak tanımlanır. Açıklıklar, dış veya iç bir kaynak tarafından kazara veya kasıtlı olarak bir güvenlik olaylarının ortaya çıkmasına sebebiyet verebilirler [25,26].

Tehdit Kaynakları (Threat Source): Bir süreç, organizasyon, sistem veya tesisin var olan bir veya birkaç açıklığını kullanarak ona kısmen veya tamamen zarar verecek unsurlardır. NIST SP 800-30 [25] rehberi tehdidi, bir tehdit kaynağının, kazara veya kasıtlı olarak belirli bir açıklığı harekete geçirme potansiyeli olarak tanımlamaktadır. Bu çalışmada tehdit kaynakları ağırlıklı olarak, farklı motivasyonlara sahip kişi, grup veya organizasyonlar olarak ele alınmıştır.

*İstenmeyen Olay (Unwanted Incident):*Bir varlığa veya onun değerine zarar veren olay ve/veya durumdur [26].

3.2. Risk Değerlendirmesi ve Yönetimi Kavramları

Riskleri yönetmek mümkün olmakla birlikte, çoğu durum için riskleri tamamen ortadan kaldırmak mümkün değildir. Risk Yönetimi (RY) ilgili güvenlik programı yöneticilerine, riskin giderilmesinden beklenen fayda ile operasyonel ve ekonomik giderler arasında bir denge kurmasına imkân verebilmektedir [25-28].

Risk Değerlendirmesi (RD), çoğu zaman riskintespiti ve bazı zamanlarda risk yönetimiyle birlikte anılan ve bunlardan biri veya her ikisi yerine kullanılan genel bir tanım olarak karşımıza çıkmaktadır. Bu bağlamda, farklı RD yaklaşımlar için değişmekle birlikte birçok RD sürecinin aşağıdakine benzer aşamaları içerdiği söylenebilir [29].

- Risklerin Tanımlanması,

- Risklerin Ölçülmesi,
- Risklerin Analiz Edilmesi,
- Riskin Yönetilmesi.

RD süreçleri için farklı araştırmacılar ve metotlar, izlenen süreçlerde takip edilen sıralamaları değiştirebilmekte, farklı kademeler ilave etmekte veya aynı süreç parçalarını farklı şekilde isimlendirebilmektedir. Örneğin, yukarıdaki aşamalarla kıyaslandığında Ralston ve ark. [30] tarafından tanımlanan RD, risk tanımlama, risk analizi, risk çözümü ve sıralaması, yönetim ve iyileştirme olarak benzerlikler ve farklılıklar gösterdiği kolayca görülebilecektir.

3.3. Risk Değerlendirme Yöntemleri

Temel olarak iki tür risk değerlendirme metodundan bahsetmek mümkündür. Bunlar:

- Nicel Risk Değerlendirme Yöntemleri,
- Nitel Risk Değerlendirme Yöntemleri.

Her iki kategorideki risk değerlendirme yöntemleri de riskleri araştırma, inceleme ve değerlendirme için genel bir çerçevenin oluşturulmasında kullanılır.

Nicel risk değerlendirme yöntemlerinin en önemli avantajları, oluşacak etkilere ilişkin ölçülebilir değerleri sağlamasıdır. Öte yandan, nümerik aralıklara olan bağlılık nedeniyle sonuçları doğrudan anlaşılamayabilir ve nitel şekliyle de ayrıca yorumlanması gerekebilir [31].

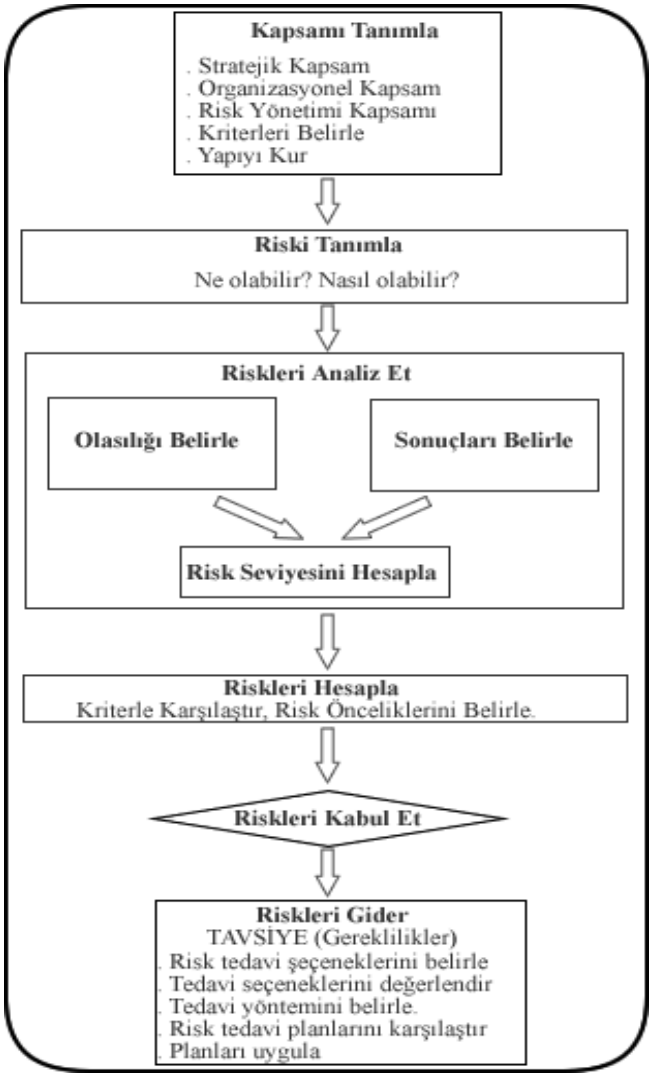
Literatürde farklı alanlar için geliştirilmiş çok sayıda risk değerlendirme ve hesaplama yöntemlerine rastlamak mümkündür. Ancak burada sadece bilgi ve iletişim teknolojilerine dayalı sistemlere ilişkin güvenlik RD yöntemlerinden birkaçı üzerinde durulacaktır.

NIST Özel Yayın (Special Publication: SP) 800-30 Bilgi Teknolojileri Sistemleri Risk Yönetimi Rehberi isimli belgesinde, değerlendirme metodu 9 adımdan oluşmaktadır. Bunlar [25,32] :

I. Sistem tanımlama,
II. Tehdit tespiti,
III. Açıklık tespiti,
IV. Kontrol analizi,
V. Olasılık belirleme,
VI. Etki analizi,
VII. Risk saptama,
VIII. Kontrol Önerileri,
IX. Sonuç Dokümanı.

Uluslararası Standartlar Organizasyonunun (ISO) risk yönetimi için özel ve kamu sektörlerin uygulanabilecek prensipleri, çerçeveleri ve genel kılavuzu sağlayan standart ailesi, ISO 31000:2009'dur [33]. Bu standart, esasen Avustralya-Yeni Zelanda standardı olan AS/NZS 4360'ın ISO tarafından benimsenmiş şeklidir.

RD ve RY süreçlerinin temeline AS/NZS 4360 standardını koyan ve Avrupa Birliği fonuyla desteklenen CORAS projesinde (Proje Kodu: IST-2000-25031) güvenlik-kritik sistemlerin risk değerlendirmesi ve güvenlik analizi için kullanılan bir yöntem ve açık kaynaklı araç olarak geliştirilmektedir [34]. CORAS projesi, AS/ NZS 4360 temelli risk yönetimi sürecini temel almaktadır [35].Şekil 3.1'de görüldüğü gibi, CORAS'ın temel aldığı AS/ NZS 4360 risk yönetimi kapsam tanımlama, risk tanımlama, riskleri analiz etme, riskleri hesaplama ve riskleri giderme olmak üzere beş alt süreçten meydana gelmektedir.



Şekil 3.1. AS/ NZS 4360 risk yönetimi süreci [35]

3.4. Güvenlik Riski Hesaplanma Yöntemleri

Risk Değerlendirme çalışmalarında, riskin hesaplanmasında nicel ve nitel yöntemler kullanılabilmektedir. Nicel yöntemlerde risk, rakamsal bir değer olarak hesaplansa da, hesaplanan miktarın gerçekteki karşılığı nitel olarak değerlendirilmesi gerekir. Örneğin risk, 1-10 aralığında 8 olarak hesaplanmışsa, buna ‘kritik’ veya ‘hayati’ gibi nitel bir karşılık atandığında anlamlı ve anlaşılır bir hale gelecektir.

NIST SP 800-30 Risk Yönetimi Rehberinde [25], Bölüm 3.3’de gösterildiği üzere risk değerlendirme süreci dokuz adımdan oluşmakla birlikte, riski hesaplama işlemi

5, 6 ve 7. adımlar içinde yer almaktadır. Bu adımlardan, belirli bir tehdidin oluşma ihtimalin belirlenmesi (5. adım) ve etkinin analizi (6. adım) riskin nitel veya nicel olarak tanımlanabilmesine imkân veren adımlardır. Beşinci ve altıncı adımlardan sonra risk ve etki hesaplanırken "Eş.3.1" kullanılmaktadır [36].

*Risk= Etki*Olasılık*
Etki=Max(kayıp, hasar, zarar) (3.1)

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation), bilgi güvenliği ihtiyacını anlamak isteyen organizasyonlar için üretilmiş olan, bilgi güvenliği değerlendirmesi ve planlaması için araçlar, teknikler ve yöntemler takımı olup, Carnegie Mellon Üniversitesi tarafından geliştirilmiştir [37]. Toplamda üç yöntem bulunur ve nispeten küçük organizasyonlar için tanımlanmış metot, OCTAVE-S olarak adlandırılmıştır.

OCTAVE-S metodunda ise risk "Eş.3.2" ile tanımlamaktadır [36].

Risk= Etki= İstenmeyen olay Sıklık* (3.2)

OCTAVE-S etkiyi, unvan/müşteri güveni, finansal kayıp, üretim, güvenlik/sağlık, yasal cezalar ve diğer kriterler olmak üzere w_r, w_f , w_p , w_s , w_i , w_o gibi farklı ağırlık değerleri atanan 6 parametre ile ifade etmektedir [36].

$$ETKİ= w_r*Unvan + w_f*FinansalKayıp + w_p*ÜretimKabı + w_s*ÇevreEmniyetiSağlık + w_{l*}YasalCezalar + w_o*Diğerleri \quad (3.3)$$

Benzer bir yaklaşım ile I3P Risk Belirleme Raporunda risk, "Eş.3.4" ile karakterize edilmektedir [38].

*Risk=Tehdit Kaynağı*Açıklıklar*Etki* (3.4)

Risk hesaplamalarında, istenmeyen bir olayın ortaya çıkması sonucu oluşan olumsuz bir etkinin boyutu veya bir tehdidin saldırıya dönüşme ihtimali bir aralık dahilinde tanımlanmaktadır. Örneğin Çizelge 3.1. ve Çizelge 3.2.'de verildiği üzere etki derecesi ve olasılık aralıkları beş adımda tanımlanabileceği gibi daha dar veya daha geniş bir aralıklarda da tanımlanabilir.

Çizelge 3.1. Etkinin derecesinin rakamsal karşılıkları

Çok Kısıtlı	%0-10	0-1
Kısıtlı	%10-30	0-3
Orta	%30-60	3-5
Ciddi	%60-80	6-8
Hayati	%80-100	8-10

Çizelge 3.2. Güvenlik tehdidinin ortaya çıkma olasılığına rakamsal karşılık atama

Mümkün ama Muhtemel Değil	%0-10	0-1
Seyrek	%10-30	0-3
Muhtemel	%30-60	3-5
Oldukça Muhtemel	%60-80	6-8
Yüksek	%80-100	8-10

Bir güvenlik olayı (örneğin siber saldırı) sonucunda ortaya çıkacak olumsuz bir etkinin (istenmeyen bir olayın) boyutları, işletmenin türüne, altyapısına ve faaliyet alanına bağlı olarak daraltılabilir veya genişletilebilir. Benzer biçimde bir tehdidin saldırıya dönüşme olasılıkları için de eldeki verilerin yoğunluğu ve elverişliliğine göre daha geniş veya dar bir ölçeklendirmeye gidilebilir.

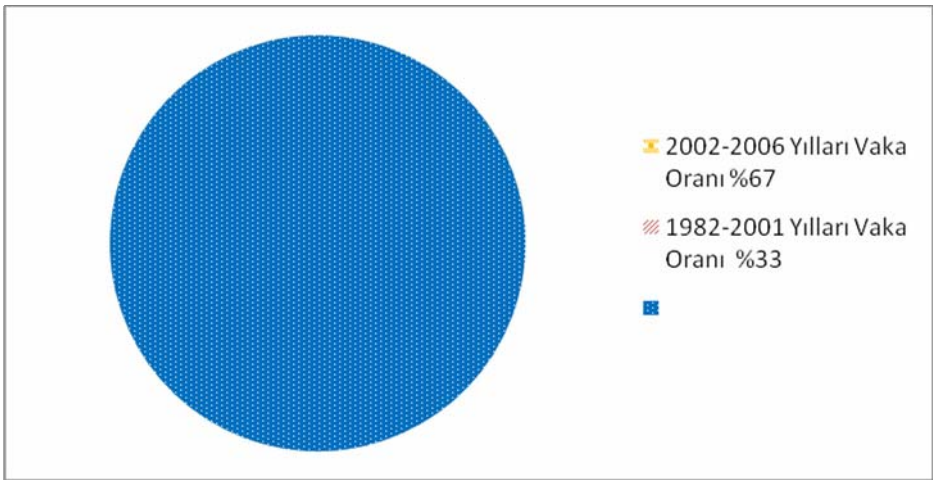
4. DENETİM SİSTEMLERİN AÇIKLIKLARINA VE GÜVENLİĞİNE İLİŞKİN MEVCUT ÇALIŞMALARIN İNCELENMESİ

Bu bölümde literatürdeyer alan önemli güvenlik olaylarına, tek olması nedeniyle çokça referans alınan ISID veritabanı(Endüstriyel Güvenlik Olayları Veritabanı) çalışmasına, AB ve ABD örneğinde kritik altyapıların siber saldırıla karşı korunması hususunda yürütülen çalışmalara ve ABD'de yürütülmüş iki önemli çalışma sonrasında yayımlanan raporlarda açıklanan bulgulara yer verilmiştir.

4.1. Güvenlik Olayları ve Bir Veritabanı Oluşturma Çalışmasının İncelenmesi

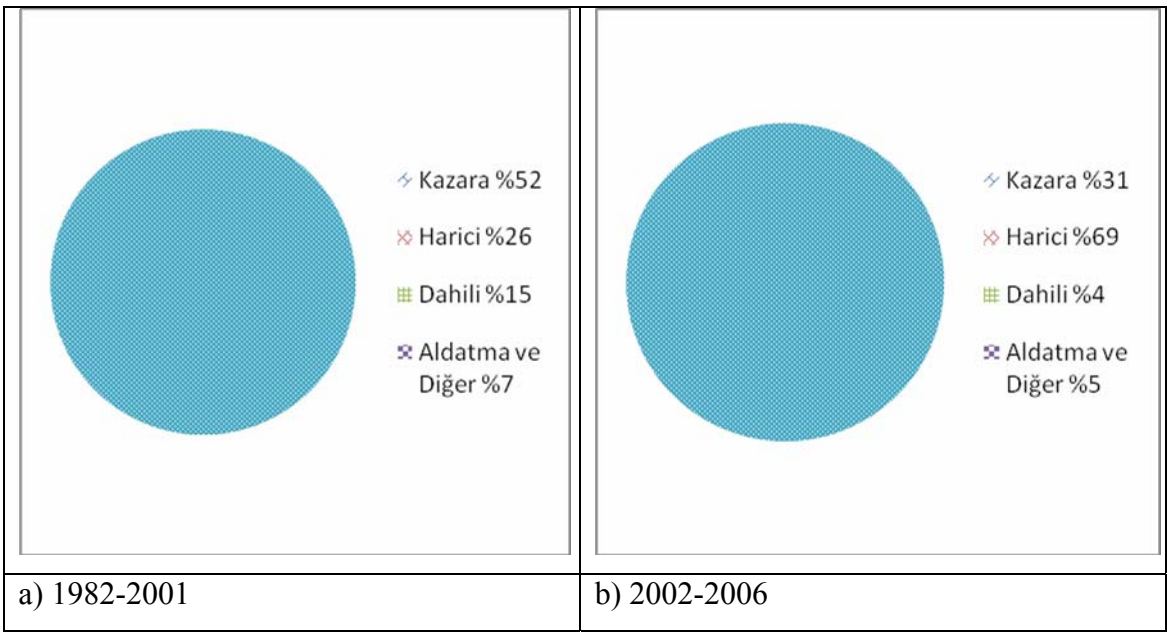
British Columbia Teknoloji Enstitüsünden (BCIT: British Columbia Institute of Technology) Eric Byres ve ark. [39], 2001-2006 yıllarını kapsayanISIDçalışmaları, 2002 yılı ve sonrasında SCADA/DSS sistemlerinde yaşanan güvenlik olaylarında ciddi bir artış olduğunu göstermektedir. 1982'den 2006 yılı ortasına kadar hakkında bilgi topladıkları ve ISID veritabanına kaydettikleri 116 olay ile ilgili olarak Eric Byres ve ark.yürüttükleri çalışma [39], literatürde gerçek güvenlik olaylarını içeren en önemli kaynak olarak dikkatleri çekmektedir.

ISID veritabanını üzerindeki analizlere göre[39], 2002 yılı ve sonrasında SCADA/DSS sistemlerinde yaşanan güvenlik olaylarında ciddi artış olduğunu ve 1982'den bu yana bilgi sahibi olunan toplam 116 olayın 78'inin 2002-2006 yılları arasında gerçekleştiği görülmektedir.



Şekil 4.1. Endüstriyel Güvenlik Olaylarının 1982-2001 ve 2002-2006 dönemine göregerçekleşme oranları [39]

Şekil 4.2.'de görüldüğü üzere, 1982-2001 yılları arasındaki 23 olayın sadece % 26'sı dış kaynaklı iken 2002-2006 döneminde olayların %60'ının dış kaynaklı olduğuna tespit raporda yer almaktadır.



a) 1982-2001 b) 2002-2006

Şekil 4.2. Bazı yıllara göre güvenlik olaylarının ve tiplerinin sıklığı [39]

ISID veritabanı üzerinde yapılan incelemelerde oldukça dikkat çekici bir husus da, 2002-2006 yılları arasındaki güvenlik olaylarının %78'inin virüs, truva atı ve solucanlardan kaynakladığının tespitidir [39].

Dünya ölçeğinde SCADA/DDS altyapılarına yönelik güvenlik olaylarını bir veritabanında toplayan ve yayımlayan bu kapsamda başkaca bir çalışma olmadığından, 2006 sonrasında meydana gelen önemli bazı olaylar (stuxnet gibi) ancak farklı yayınlarda teker teker veya basına yansıdığı kadarıyla öğrenilebilmektedir.

Aşağıda çeşitli gazete, dergi ve raporlara konu olan örnek güvenlik olaylarındanbazıları yer almaktadır [40-44].

- 1998 yılında bilgisayar korsanları tarafından GasProm boru hattının denetim sistemine girmiştir [40].
- 2001 Kasım ayında kullanılan SCADA yazılımının Hollanda'daki gaz çevrim santralında neden olduğu hata, 26000 eve üç gün boyunca doğalgaz verilememesine neden olmuştur [40].
- 2000 yılında Avustralya'da işinden atılan işçi, eski şirketinin 150 kanalizasyon pompasını yöneten birimine bir dizüstü bilgisayar ve radyo vericisi kullanarak sızmış ve üç ay boyunca 1 milyon litre kanalizasyon atığını dilediği gibi yönetebilmiştir [41].
- 2000 yılında bilgisayar korsanları Rus doğal gaz dağıtım şirketi GasProm'un kontrollünü ele geçirmeleri vakası yaşanmıştır [42].
- 2003 Ocak ayında bir SQL solucan ismi belirtilmeyen bir elektrik enerji sisteminin bir güç santralıyla olan erişimin kesilmesine neden olmuş ve bundan SCADA yönetim biriminin telemetri sistemlerini de etkilemiştir. Yine aynı solucan Davis-Besse nükleer santralının güvenlik izleme istasyonuna saldırmıştır [40].
- The Washington Post gazetesinin 5 Temmuz 2008'de yayımladığı habere göre, ABD'nin Georgia Eyaleti bağlı Baxley yakınlarındaki nükleer santralın izleme

sisteminde kullanılan bilgisayarın güncellenmesi, denetim birimindeki başka bir sistemin kapatmasına neden olmuştur. Bunun sonucunda ise, santralın otomatik koruma sistemi devre dışı kalmış ve iki sistem beş saatten fazla kararsız duruma geçmiştir [43].

- The Wall Street Journal gazetesinin 5 Nisan 2009'da yayımladığı haberinde, Çin, Rus ve diğer ülkelerden gelen siber ajanların ABD elektrik şebekesi denetim sistemlerine ABD'li uzmanların sızdığı ve sistemin işleyişini bozucu programlar bıraktığı iddia edilmektedir [44].
- 2010 yılında doğrudan SCADA sistemlere yönelik siber saldırı düzenlemek için geliştirilen ve spesifik bir sisteme saldırmak için tasarlandığı anlaşılan 'Stuxnet' virüsü tespit edilmiştir. Stuxnet, endüstriyel denetleyicileri yeniden programlamak ve yaptığı değişiklikleri gizlemek için özellikle hazırlanmış bir program olması bakımından ayrıca önem taşımaktadır [42]. Stuxnet'in duyulmasıyla birlikte literatürde çok fazla tartışılma yer almış ve birçok kaynakta bir olgu haline dönüştürülerek yeni dönem siber savaşı başlatıcısı olarak gösterilmiştir.

4.2. Kritik Altyapılara İlişkin Dünyada Mevzuat Çalışmaları

Kritik altyapılara yönelik siber saldırılara karşın ilk yasal düzenleme ve çalışmaların ABD'de yürütülmeye başlandığı görülmektedir. Bu bağlamda ilk olarak, 1998 yılında 63. ABD Başkanlık Karar Direktifi (PDD-63: Presidential Decision Directive No 63) ile Amerikan hükümeti ve ekonomisi için önem arz eden her türlü altyapının korunması ve işlevinin devamlılığının sağlanması için ilgili kurum ve birimlerden gerekli tedbirlerin alınması istenmiştir [5,45]. 2000'li yıların başında ise, elektrik, gaz, su, petrol üretim, iletim ve dağıtım şebekeleri ile nükleer santrallarda, kimyasal tesislerde ve diğer endüstriyel üretim altyapılarında kullanılan DDS sistemlerin güvenliğine dikkat çeken en önemli olayların başında Amerika Birleşik Devletlerinde meydana gelen 11 Eylül 2001 saldırısı gelmektedir. Bu saldırı sonrasında yasalaşan USA PATRIOT ACT 2001 (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) ile "hasar görmesi veya etkisizleştirilmesi halinde ulusal halk

sağlığını, güvenliği, ekonomik güvenliği veya tümünü olumsuz etkileyecek fiziki veya sanal tüm varlık ve sistemler" kritik altyapı sistemler olarak tanımlanmış; tehditler arasında siber saldırı ve açıklıklara da yer verilmiştir. Aynı yasa ile bu altyapıların korunmasına yönelik ABD'de ciddi tedbirler getirilmiştir [1,4].

2003 yılında ABD'de yayınlanan 7 numaralı Ülke Güvenliği Başkanlık Direktifi (HSPD-7:Homeland Security Presidential Directive No 7) ile her türlü kritik altyapının korunmasını temin için, ilgili idare ve kuruluşlardan gerekli her türlü yöntem ve teknolojiyi geliştirmesi istenmiştir [4,46].

ABD'nin ardından Avrupa'da ise, Avrupa Konseyinin talebi üzerine ilgili komisyonca hazırlanan ve Avrupa Birliği (AB) Meclisine sunulan "Terörist Saldırılara Karşı Kritik Altyapıların Korunması" başlıklı 2004 yılı tebliğinde Kritik Altyapılar, "kesilmesi veya hasar görmesi halinde vatandaşların güvenliği, sağlığı ve ekonomik refahı üzerinde veya üye hükümetlerin etkin ve verimli işleyişi üzerinde ciddi olumsuz etkiler oluşturacak fiziki ve bilgi teknolojileri tesisleri, hizmetleri ve varlıkları " olarak tanımlanmış ve aynı yıl içinde "Kritik Altyapılar İçin Avrupa Programı (EPCIP: European Programme for Critical Infrastructure Protection)" ve "Kritik Altyapı Erken Bilgi Ağı (CIWIN: Critical Infrastructure Warning Information Network)" yasalaştırılmıştır [2-3].

İsviçre Federal Teknoloji Enstitüsü Güvenlik Çalışmaları Merkezinden Brunner ve Suter'inhazırladığı Kritik Bilgi Altyapısı Sistemleri El Kitabı 2008/2009'da (Critical Information Infrastructure Systems Handbook 2008/2009) 25 ülke ve 7 uluslararası organizasyonca, kritik sektörler ve bu sektörlerde kullanılan bilgi altyapısıyla ilgili düzenlemelerini kapsamlı olarak anlatmaktadır [47].

4.3. Bir Test Yatağı Çalışması ve Açıklanan Bulgular: NSTB

ABD Enerji Bakanlığı Elektrik Dağıtımı ve Enerji Güvenliği Ofisince, ulusal enerji dağıtım sisteminin güvenlik ve güvenilirliğini iyileştirmek amacıyla 2003 yılında Ulusal SCADA Test Ortamı (NSTB) programı başlatılmıştır [48]. NSTB programı,

SCADA / DDS sistemlerine ait açıklıkların tanımlanması ve çözümüne; mevcut ve yeni ekipmanların testlerinin yapılması ve güvenli mimari tasarımlarının geliştirmesine yardımcı olmak üzere başlatılan bir programdır. Ayrıca, Argonne, Idaho, Oak Ridge, Pacific Northwest ve Sandia National laboratuarlarının konuyla ilgili birikim, deneyim ve imkânlarını birleştirmek de NSTB programı kapsamında yer almaktadır [48].

NSTB programı kapsamında, Idaho Ulusal Laboratuarınca (INL) Amerika Birleşik Devletleri Enerji Bakanlığı Elektrik Dağıtımı ve Enerji Güvenliği Ofisine sunulmak üzere 2008 yılında hazırlanan Denetim Sistemleri Değerlendirmelerinde Gözlenen Genel Güvenlik Açıklıkları (INL-NSTB 2008) [49] raporunda, enerji sistemlerinde kullanılan SCADA/DDS sistemlere ait genel güvenlik kusurları çeşitli alt başlıklarda sınıflandırılmış ve güvenlik kusurlarını azaltıcı önlemlere yer verilmiştir.

INL-NSTB çalışması kapsamında hem laboratuvar ortamında birçok üreticinin ürünleri test edilmiş hem de gerçek saha ortamında cihazların işletimi ve yapılandırılmasıyla ilgili incelemelerde bulunulmuştur. Ancak INL ile SCADA/DDS üreticileri ve işletmeler arasında yapılan gizlilik sözleşmeleri nedeniyle raporda tespit edilen açıklıklara ilişkin tam ayrıntı ve sayı verilmemiştir.

INL-NSTB 2008 raporunda [49] sistem güvenlik boyutunu, güvenlikten sorumlu grubun sahip olduğu bilgi, saldırgan grubun sahip olabileceği bilgi, erişimin güvenliği, açıklıklar, potansiyel hasar, tespit ve kurtarma olmak üzere yedi başlıkta toplamış ancak bunlardan sadece ilk dördü için detaylı inceleme verilmiştir. Raporda, sistemin güvenliğinden sorumlu grup, güvenlik grubu; muhtemel saldırganlar ise saldırgan grup olarak nitelendirilmiştir. Güvenlik grubunun sahip olmadığı bilgi ve imkân ile saldırgan grubun sahip olduğu bilgi ve imkânın sistem güvenliği üzerindeki etkileri alt başlıklar altında raporda değerlendirilmiştir.

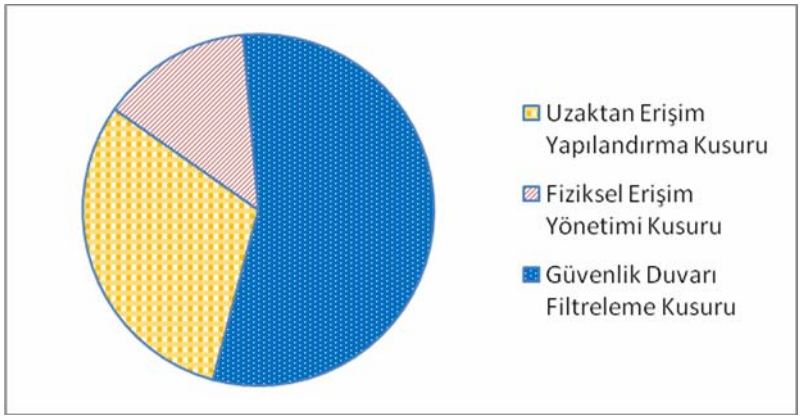
Çizelge 4.1.'de INL-NSTB 2008 raporunda ABD'de yer alan ve aynı çalışmada değerlendirmeye tabi tutulan işletmelere ilişkin güvenlik gurubu kusuru taşıyan işletmelerin kaç adetinin hangi kusur bileşenini taşıdığı bilgisi verilmiştir.

Çizelge 4.1. INL-NSTB 2008 raporu güvenlik grubu kusuru taşıyan işletme adeti [49].

Kusur Bileşeni	**Kusuru Tespit Edilen İşletme Sayısı**
Sistemdeki Değişimin Yönetilememesi	4
Dokümantasyon Eksikliği	3

Aynı raporda, saldırgan grubun hedef sisteme ait bilgiye ulaşımını sağlayan kusurlar özetle, kullanılan kriptosuz servisler ve protokoller, kullanıcı izinlerinin korunma zayıflığı, sistem bileşenleri ve kullanılan ürünler hakkında yayınlanmış bilgiler olarak yer almaktadır.

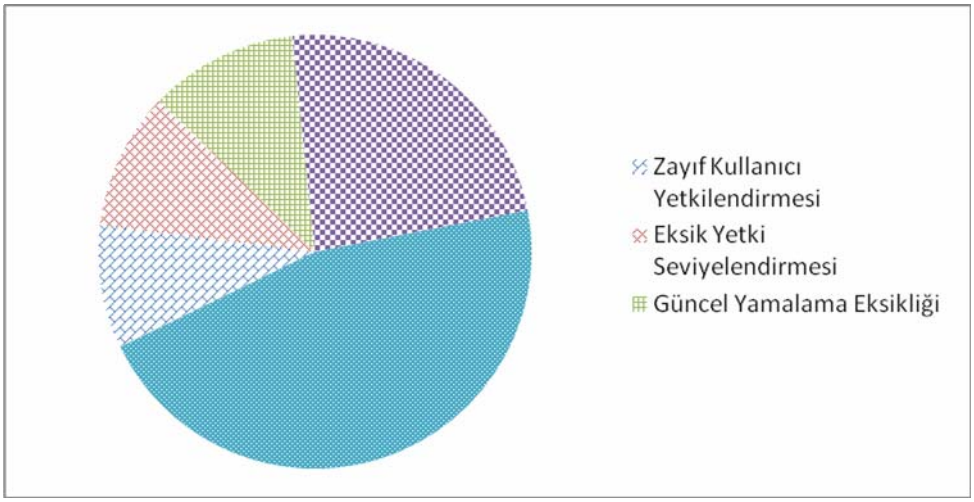
Erişim güvenliği boyutu; fiziksel erişim, güvenlik duvarı filtreleri, uzaktan erişim yapılandırmasına ilişkin kusurlar olarak üç ana başlıkta sınıflandırılmıştır. Değerlendirmeye tabi tutulan işletmelerin bu başlıklara göre tespit edilen kusurları, gizlilik nedeniyle tam rakamların yer almadığı Şekil 4.3.'de kabaca görülmektedir.



Şekil 4.3. INL- NSTB 2008 raporu erişim güvenliği kusur bileşenlerinin kabaca dağılımı[49]

INL-NSTB 2008 raporunda, güvenlik açıklıkları boyutu beş ayrı başlıkta incelenmiş ve her bir başlık alt başlıklarla da detaylandırılmıştır. Bu kusurlar, bellek taşmalarına ve SQL enjeksiyonuna sebebiyet veren giriş geçerleme eksikliği; bütünlük sınamasını ve içerik şifrelemeyi yapmayan veya zayıf yapan iletişim protokolleri açıklıkları; zayıf şifre kullanımı veya şifre kullanmamadan kaynaklı kullanıcı yetkilendirmesi kusurları; yetki seviyelendirmesi eksikliği olarak tanımlanmıştır. Raporda değerlendirmeye tabi tutulan işletmelerin, bu başlıklara göre tespit edilen

kusurlarının toplamdaki payları gizlilik nedeniyle Şekil 4.4.'teki gibi kabaca gösterilmiştir.



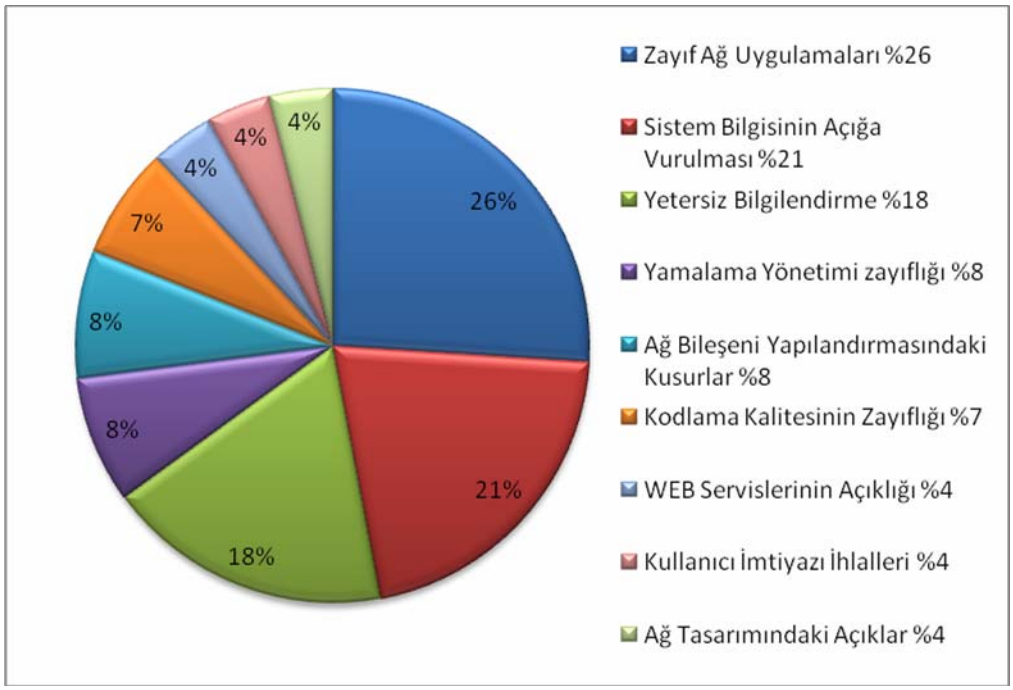
Şekil 4.4. INL-NSTB 2008 raporu güvenlik açıklıkları kusur bileşenlerinin kabaca dağılımı [49]

4.4. Denetim Sistemleri Güvenlik Programı (CSSP)

NSTB çalışmayla benzer amaçlar taşıyan ancak sonuçları itibariyle farklı açılardan da SCADA/DDS sistemlerinin açıklıklarını ve güvenliğini değerlendirme imkânı veren 2009 yıllıda yayımlanan bir rapor, toplam dört yıllık saha ve laboratuar çalışmasının ürünü olarak ABD Savunma Bakanlığı Ulusal Siber Güvenlik Bölümü'nün Denetim Sistemleri Güvenlik Programı (CSSP) kapsamında hazırlanmıştır [50].

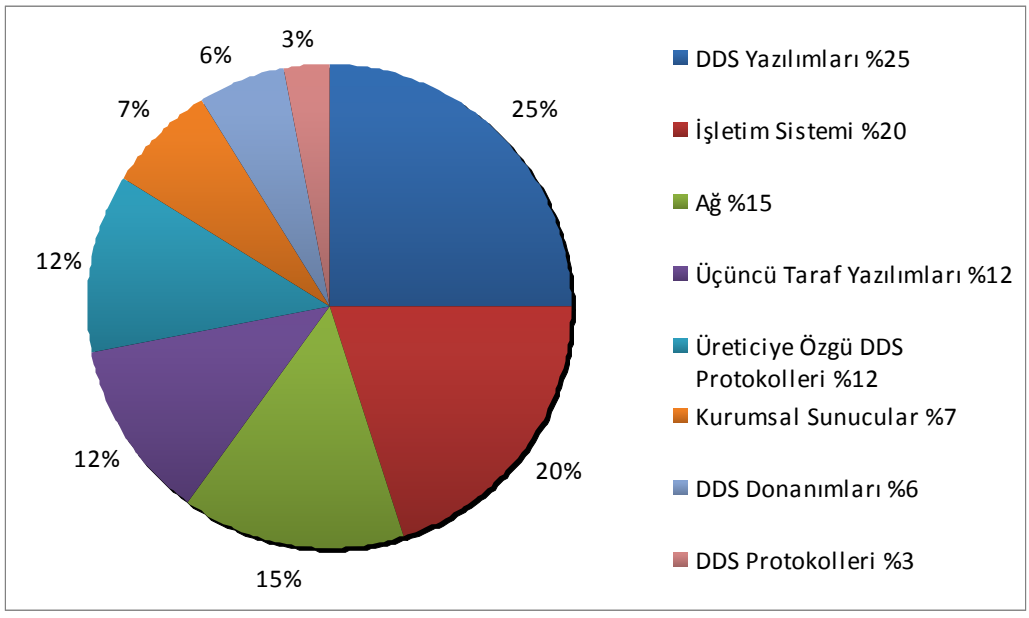
Farklı SCADA/DDS sistem üreticine ve işleticisine ait değerlendirmeleri içeren CSSP 2009 raporunda, ürün, uygulama, servis ve işletme gibi çeşitli başlıklarda oldukça yararlı bulgu ve değerlendirmelerde yer almaktadır.

Şekil 4.5.'te CSSP'nin 9 ayrı güvenlik problemi kategorisi için yaptığı inceleme ve değerlendirmelerin sonucu gösterilmiştir.



Şekil 4.5. CSSP 2009 Raporu güvenlik açıklıkları oranları [50]

Aynı raporda, bu defa DDS sistemlerin içerdikleri bileşenlere göre yapılan açıklık inceleme ve değerlendirmesinde elde edilen bulgular da Şekil 4.6.'da verilmiştir.



Şekil 4.6.DDS sistem bileşenlerine göre güvenlik açıklıklarının oranları [50]

CSSP 2009 raporunda [50] birçok alt başlıkta yapılan farklı değerlendirmelere ilişkin sonuçlar da yer almaktadır. Toplamda 2004-2008 yılları arasında yapılan 15 ayrı değerlendirmede kritik sistemleri siber saldırılara maruz bırakacak toplam 245 açıklığın bulunduğu ifade edilmektedir. İşletmelerle ve üreticilerle yapılan gizlilik sözleşmeleri gereği açıklıkların hangi altyapılarda ve hangi ürünlerde olduğu belirtilmemiştir.

Oldukça önemli ve kapsamlı çalışmalar olan 2008 yıllı INL-NSTP Raporu ve CSSP Raporları kritik altyapılarda kullanılan DDS sistemlerin ciddi güvenlik riskleri taşıdıklarını ayrıntılarıyla göstermektedir.

Yapılan literatür taramasında, DDS sistemlerin güvenliğinin 2000 yıllarda ortaya çıkmaya başlayan güvenlik olaylarının sayısının artmasıyla birlikte gerek batılı ülkelerin hükümetlerince gerek akademik çevrelerce oldukça ilgi görmeye başladığı ancak bu konuda yeterli akademik çalışma eksikliğinin devam ettiği gözlenmiştir.

Türkiye'de ise bilinen benzer laboratuar ve saha çalışmaların yapılmadığı gözlenmektedir. Bu nedenle araştırmacıların doğrudan veya bir gizlilik sözleşmesi karşılığı ulaşabileceği veri bankası ülkemizde bulunmamaktadır. Bu durumu birkaç açıdan gerekçelendirmek mümkün olabilecektir. Birincisi, Türkiye'debaşta ilgili kurum ve kuruluşlar olmak üzere yönetici ve karar alıcılar düzeyinde yeterli farkındalık oluşmamıştır. İkincisi, Türkiye'de araştırmacılar için, DDS sistemlerde kullanılan farklı ürün ve uygulamaları test etmekte kullanılabilecek test yatakları ve laboratuarları bulunmamaktadır.

Özellikle Stuxnet ve Flame kötücül yazılımlarının tanımlanması ve neler yapabildiklerinin anlaşılmasından sonra birçok ülkenin konuyu ciddiyetle takip ettikleri ve açıklamasalar da çeşitli çalışmalar yürüttükleri ancak konunun hassasiyeti nedeniyle çalışmalarına ilişkin güncel rapor veya detay yayımlamadıkları değerlendirilmektedir.

5. DENETİM SİSTEMLERİNİN KORUNMASINA YÖNELİK ÇALIŞMA VE STANDARTLAR

Bir organizasyonu veya sistemi güvenli hale getirmek ve güvenli halinin devamlılığını sağlamak için çeşitli güvenlik standartları oluşturulmuştur. Bu bölümde, odak noktası dağıtık denetim sistemleri kullanan kritik altyapılar olmak üzere, çeşitli bilgi ve bilgi sistemleri güvenliği standartları, rapor ve rehber niteliğindeki dokümanlar incelenecektir.

5.1. BT ve DDS Sistemlerinin Karşılaştırılması

Bilgi ve bilgi sistemleri güvenliğinin yönetimini konu alan çalışmalar, çoğunlukla Bilişim Sistemlerine ve bu sistemler üzerinde işlenen, taşınan, saklanan veri ve bilgilere yönelik çalışmalar olmakla birlikte, özel olarak DDS'leri de kapsayan Endüstriyel Denetim Sistemlerine yönelik çeşitli standart, rehber ve rapor çalışmaları bulunmaktadır.

Bu bölümde, öncelikle Dağıtık Denetim Sistemleri/Endüstriyel Denetim Sistemleri ileBilişim Sistemlerinin farkının ortaya konulması, yapılacak inceleme ve karşılaştırmaların daha sağlıklı olması açısından önemli olacaktır. Her ne kadar Endüstriyel Denetim Sistemleri, veri işleme ve iletme için BT altyapısında kullanılan sistem ve sistem bileşenlerini kullansa da, hem yönettiği süreçler ve altyapısından kaynaklanan hem de sonuçlarından kaynaklanan bazı farklılıklara sahiptir. Çizelge 5.1.'de BT ve DDS sistemlerinin 9 başlıkta karşılaştırması yer almaktadır. Karşılaştırma için ağırlıklı olarak NIST'den Stouffer ve ark. [51] hazırladıkları "SCADA ve Endüstriyel Denetim Sistemleri Güvenliği Rehberi" çalışması referans alınmakla birlikte, bu çalışma kapsamında yürütülen saha çalışmalarında gözlenen gerçek ve ihtiyaçlara göre bazı ilave ve değişiklikler yapılmıştır.

Çizelge 5.1. BT ve DDS sistemleri arasındaki farkların sınıflandırılması [51]

Kategori	**Bilişim Sistemleri**	**Endüstriyel Denetim Sistemleri Dağıtık Denetim Sistemleri**
Performans Gereksinimi	Çoğunlukla gerçek zamanlı değildir Yüksek gecikme ve jitter kabul edilebilir Yüksek bant genişliği gereksinimi var	Çoğunlukla gerçek zamanlıdır Yüksek gecikme ve jitter ciddi sorunlar oluşturabilir Düşük ve orta bant genişliği kabul edilebilir
Süreklilik Gereksinimi	Yeniden başlatma gibi durumlar kabul edilebilir Sistemin operasyonel gereksinimlerine bağlı olarak kesintiler kabul edilebilir	Yeniden başlatma gibi durumlar gerekli tüm şartlar sağlanırsa kabul edilebilir Kesintiler günler veya haftalar önce planlanmalıdır
Risk Yönetimi Gereksinimi	En önemli konu verinin gizliliği ve bütünlüğüdür Hata toleransı kısmen önemlidir, anlık kesintiler majör risk oluşturmaz Majör risk etkisi genellikle iş kaybıdır	En önemli konu can ve mal güvenliğidir Hata toleransı gereklidir, anlık kesinti dahi kabul edilemez Majör risk etkisi, yaşam, ekipman veya üretim kaybı olabilir
Mimari Güvenlik Odağı	Birincil odak bilginin ve BT varlıklarının korunmasıdır En çok koruma merkezi sunucular için gereklidir	Birincil odak süreçlerin korunmasıdır Merkezi sunucuların korunması önemlidir. İletişim Birimlerinin ve Uç Birim Cihazların korunması önemlidir
İşletim Sistemi	Genel amaçlı işletim sistemleri kullanılır Güncellemeler otomatik araçlar marifetiyle yürütülür	Genel veya özel amaçlı işletim sistemleri kullanılır Sahada çoğunlukla güvenlik fonksiyonları hiç veya yeterli olmayan cihazlar kullanılır Güncellemeler dikkat gerektirir ve genellikle üreticilerin yapması gerekir
Kaynak Kısıtları	Sistemler üzerine ilave güvenlik uygulamaları (antivirüs, sanal özel ağ vb.) gibi üçüncü taraf uygulamalarını destekleyecek kaynağa sahiptirler	Sistemler önceden belirli süreçleri destekleyecek donanım kaynaklarına göre üretilmiştir Mevcut yazılım ve donanım kaynakları üzerine ilave edilecek güvenlik uygulamaları için kısıtlı kaynağa sahiptirler
Haberleşme	Standart haberleşme protokolleri kullanılır Çoğunlukla kablolu ve yer yer kablosuz sistemler kullanılır Uzak alan haberleşmesi için genellikle ticari telekomünikasyon servisleri kullanılır	Standart ve üreticiye özgü haberleşme protokolleri kullanılır Farklı tip kiralık kablolu ve kablosuz hatlar kullanılır Uzak alan haberleşmesi için ticari veya işletmelere özel haberleşme altyapıları kullanılır
Yazılım Değişim Yönetimi	Genelde otomatize edilmiş süreçlerle	Kesintileri de öngörerek, sistemin bütünlüğü garantiye alınarak
Malzeme Yaşam Süresi	3-5 yıl arası	15-20 yıl

5.2. Güvenlik Standartları

Bilgi ve bilgi sistemleri güvenliğinin iyileştirilmesi ve yönetimine ilişkin çalışmaların, tüm sistemlere yönelik olarak hazırlandığı gibi belirli sektör veya sistem türlerine özgü olarak da hazırlandığı görülmektedir. Örneğin, ISO 27000 standartları tüm bilgi sistemlerini kapsarken, ISA SP 99 teknik raporları üretim ve denetim sistemlerine özgü olarak hazırlanmıştır.

Çizelge 5.2.'de, bu bölüm içinde çoğunluğu incelenecek standart ve çalışmaların, odak konusu ve sektörüne göre tasnifi görülmektedir.

Çizelge 5.2. Güvenlik standartlarının odak konu ve sektörlere göre sınıflandırılmaları [52]

Organizasyon	Standart Kodu	Standardın Adı	Odak Konu	Odak sektör	Türü
ISO	ISO 17799	Information Technology – Security Techniques – Code Of Practice For Information Security Management	Bilgi Teknolojileri	Sektörler arası	Standart
ISO	ISO 27001	Information Technology – Security Techniques – Information Security Management Systems	Bilgi Teknolojileri	Sektörler arası	Standart
ISA	ISA TR99-01	Security Technologies For Manufacturing And Control Systems	Denetim Sistemleri Siber Güvenliği	Endüstriyel üretim ve denetim sistemleri kullanan tüm sektörler	Teknik Rapor
ISA	ISA TR99-02	Integrating Electronic Security Into The Manufacturing And Control Systems Environment	Denetim Sistemleri Siber Güvenliği	Endüstriyel üretim ve denetim sistemlerini kullanan tüm sektörler	Teknik Rapor
NIST	SPP-ICS	System Protection Profile – Industrial Control Systems	Denetim Sistemleri	Endüstriyel üretim ve denetim sistemlerini kullanan tüm sektörler	Koruma Profili
NIST	SP800-53	Recommended Security Controls For Federal Information Systems	Bilgi Teknolojileri	Sektörler arası	Rehber
NIST	SP800-82	Guide For Scada And ICS Security	Denetim Sistemleri	Endüstriyel Üretim ve Denetim Sistemlerini Kullanan Tüm Sektörler	Rehber
NERC	NERC CIP	NERC Critical Infrastructure Protection	Denetim Sistemleri	Enerji-Elektrik	Standart
IEC	IEC 62351	Data and Communications Security	İletişim		Standart
API	API 1164	Pipeline Scada Security	Denetim Sistemleri	Enerji-Petrol ve Gaz	Standart
IEEE	IEEE 1402	IEEE Guide For Electric Power Substation Physical And Electronic Security	Denetim Sistemleri	Enerji-Elektrik	Standart
AGA	AGA 12	Cryptographic Protection of Scada Communications	Denetim Sistemleri Şifreli İletişim	Enerji-Gaz	Rapor

5.2.1. ISO 27000 serisi

ISO 27001, bilgi güvenliği yönetimi için uluslararası standartlar serisi olan ve Uluslararası Standartlar Organizasyonu (ISO) ile Uluslararası Elektroteknik Komisyonunun (IEC) ortak komitesi tarafından geliştirilen ISO / IEC 2700 ailesinin bir parçasıdır. 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 ve revize edilmiş 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 27002standardı ISO/IEC 17799:2005 olarak adlandırılmıştır [53-55].

ISO/IEC 27001, BGYS için şart olan gereksinimleri tanımlar. ISO/IEC 27002 ise, bir sertifikalandırma standardından ziyade BGYS için uygulama esaslarını sunar. Ancak organizasyonlar diğer bilgi güvenliği denetim takımlarını da seçmekte özgürdürler [53-55].

ISO/IEC 27002, giriş bölümleri dışında 12 ana bölümden oluşmaktadır. Bunlar [54-56];

- Risk Yönetimi: Risk değerlendirme, risk analizi, riski azaltma
- Güvenlik Politikası: Prensipler ve aksiyomlar, politikalar, standartlar, rehberler ve prosedürler
- Bilgi Güvenliğinin Organizasyonu: Yapı, raporlama, irtibat
- Varlık yönetimi: Envanter, sınıflandırma, sahiplik
- İnsan Kaynakları Güvenliği: Sistem erişimi yönetimi; güvenlik farkındalığı, eğitim ve öğretim
- Fiziki Güvenlik ve Çevre Güvenliği: Fiziki erişim; havalandırma; yangın / su baskını; enerji / güç kaynakları
- İletişim ve Operasyon Yönetimi: Arşivleme, yedekleme, loglama, yamalama, izleme, yapılandırma

- Erişim Denetimi: Fiziki erişim, ağ erişimi, sistem erişimi, uygulama erişimi, fonksiyon çalıştırma
- Bilgi Sistemleri Edinimi, Geliştirme ve Bakımı: Gereksinim, tasarım; geliştirme/edinim, test, uygulama, bakım ve destek
- Bilgi Güvenliği Olay Yönetimi: Hazırlık, tanımlama, reaksiyon, yönetim ve içerik, çözüm, öğrenme
- İş Sürekliliği: Dirençlilik, afet yedekleme/kurtarma
- Uyumluluk: Denetim, yasa ve düzenlemeler, güvenlik politikaları-standartları ve teknik uyumluluk

5.2.2. ISA SP99: TR1 ve TR2

Enstrümantasyon, Sistem ve Otomasyon (ISA) topluluğu bünyesinde bulunan ve dünya genelindeki endüstriyel siber güvenlik uzmanlarından oluşturulmuş ISA99 / ISA SP99 komitesi, endüstriyel otomasyon ve denetim sistemleri üzerine ISA standartları geliştirmektirler. Bu komite, faaliyet çerçevesini, endüstriyel otomasyon ve denetim sistemlerindeki aşağıdaki olaylara sebebiyet verecek konuları incelemek olarak tanımlamaktadır [57].

- Halkın veya çalışanların güvenliğinin tehlikeye düşmesi,
- Kamu güveninin sarsılması,
- Düzenleyici gereksinimleri ihlali,
- Tescilli veya gizli bilgilerin kaybı,
- Ekonomik kayıplar,
- Ulusal güvenliğe olumsuz tesirler.

ISA 99 faaliyet çerçevesindeki üretim ve denetim sistemleri elektronik güvenliği kavramının, tüm endüstrilerdeki saha, tesis ve sistemleri kapsadığı; kullanılan her türlü sensor, uç birim cihaz, SCADA izleme ve yönetme donanım-yazılımlarını içerdiğini ancak bunlarla sınırlı kalmadığını ifade etmektedir.

ISA SP99 faaliyet çerçevesinden de anlaşılacağı üzere, üretim ve denetim sistemlerinde kullanılan bileşenlerin gizlilik, bütünlük ve kullanılırlığını daha iyi bir duruma getirmek amacıyla güvenlik denetim sistemi uygulama ve temini için kriter oluşturma çalışmalarını yürütmektedir [58].

ISA SP99, BS 7799 Bilgi Güvenliği Yönetimi standardını referans aldıkları, ISA-TR99.00.01-2004 veya kısa şekliyle TR1 kodlu "Üretim ve Denetim Sistemleri için Güvenlik Teknolojileri" başlıklı teknik raporunu ve bu raporun tamamlayıcısı niteliğindeki ISA- ISA-TR99.00.02-2004 veya kısa şekliyle TR2 kodlu "Üretim ve Denetim Sistemleri Çevresinde Tümleşik Elektronik Güvenlik" başlıklı teknik raporu yayımlamıştır [59].

TR1 kodlu ISA raporunda, üretim ve denetim sistemlerine uygulanabilecek 28 elektronik güvenlik teknolojisi, altı kategoride ayrılmıştır. Bunlar [59];

1. Kimlik doğrulama ve yetkilendirme teknolojileri: Bu teknolojiler, rol tabanlı yetkilendirme cihazları, zorluk-tepki yetkilendirme metotları, akıllı kartlar, biyometrik sistemler ve şifre yönetimi araçlarını kapsamaktadır.
2. Filtreleme, engelleme ve erişim denetimi teknolojileri: Bu teknolojiler güvenlik duvarlarını ve sanal yerel alan ağlarını kapsamaktadır.
3. Şifreleme ve veri geçerlilik sınaması: Bu metotlar, simetrik ve açık anahtar şifreleme, anahtar yönetimi, sayısal imza ve sanal özel ağları kapsamaktadır.
4. Denetim, ölçüm, izleme ve tarama araçları: Bu araçlar içerisinde, denetim logları, virüs tespit ve saldırı tespit sistemleri, açıklık tarama ve otomatik yazılım yönetimi yer almaktadır.
5. Bilgisayar yazılımları: İşletim sistemleri ve web tabanlı uygulamalar içerir.
6. Fiziksel güvenlik denetimi: Fiziksel koruma ve fiziksel güvenlik mekanizmalarını kapsar.

ISA-TR99.00.02-2004 veya kısa adıyla TR2 bilgi güvenliği metodolojileri ve teknolojiler hakkında TR1'den daha fazla ve ayrıntılı tartışmalar sağlamaktadır. Zira TR1 özetle, üretim ve denetim sistemlerinin elektronik güvenliği için genel bir bakış

sunarken, TR2 elektronik güvenlik programı geliştirecek bir çerçeve ve güvenlik planı-organizasyonu için tavsiyeler içermektedir [60]. TR2 belgesi ayrıca, denetleme fonksiyonları ve sigortalama değerlendirmelerine de yer vermekte olup, farklıdağıtık denetim sistemleri, SCADA sistemleri, toplu ve ayrık süreç denetim sistemleri için uygulanabilir kriterler bulundurmaktadır [59].

TR1 ve TR2 teknik raporları, üretim ve denetim sistemlerine yönelik güvenlik problemleri tanımlamak için faydalı olmakla birlikte, sistem ve bileşenlerini test etme ve sertifikalandırma için gerekli gereksinimleri ayrıntılı tanımlayan standartlar değildirler [58].

5.2.3. NIST SPP-ICS

SPP-ICS çalışması, NIST'in sponsor olduğu Süreç Denetimi Güvenlik Gereksinimleri Forumunun (PCSRF) parçası olarak geliştirilmiştir. Başlangıçta, 'Ortak Kriterler' temelinde endüstriyel denetim sistemleri için güvenlik gereksinimleri belirlemeyi hedeflemiştir [61].

SPP-ICS çalışmasında, Sistem Hedef Değerlendirme (STOE) başlığı altında, veri gizliliği-bütünlüğü ve sistem kullanılırlığını korumaya yönelik tanımlamalar yapılmış; açıklık, atak, tehdit ve varlık sınıflandırması için oldukça kullanışlı bir notasyon kullanımı yoluna gidilmiştir. SPP'nin kullandığı notasyonun elverişli bir sınıflandırma imkânı vermesi nedeniyle Bölüm 7'deki çalışmalarda açıklık, varlık ve saldırıların etiketlenmesi için aynı notasyonun kullanımı tercih edilecektir.

SPP çalışmasındaki Sistem Hedef Değerlendirmesinin teknik ve teknik olmayan bileşenleri Çizelge 5.3'deki gibi tanımlanmıştır.

Çizelge 5.3. SPP Sistem hedef değerlendirmesi bileşenleri [61]

SPP STOE Bileşenleri	**Örnek Donanım ve Yazılım Bileşeni**
Fiziki Sınır Koruması	Denetim merkezinin güvenliği, sistemlerin erişim denetimi
Mantıksal Sınır Koruma	Güvenlik duvarı, ağ geçidi, güvenlik cihazları (Örn: Saldırı tespit sistemleri)
Veri Yetkilendirme	Denetim sistemlerindeki bileşenlerin veri yetkilendirme servisleri
Veri Gizliliği	Kriptolama servisleri, farklı birimler arasındaki hattı şifreleyen cihazlar
Kullanıcı Yetkilendirme	Fiziksel erişim birimlerine entegre kullanıcı yetkilendirme servisleri
Operasyonun Sürekliliği	Sistem yedekleme ve kurtarma
İşletim Prosedürü	Sitem politikaları ve prosedürleri (Örn: Yedekleme sıklığı, şifre gereksinimi)
Eğitim	Güvenlik ve güvenlik farkındalığı eğitimi ve kursları
Yönetim Prosedürleri	Çalışanların seçimi, disiplin önlemleri ve diğer personel politikaları

Ayrıca SPP Sistem Hedef Değerlendirmesi Güvenlik Özellikleri şu başlıklarda tanımlanmıştır: Yetkilendirme, gizlilik, bütünlük, kullanılırlık, sınır koruma, erişim denetimi, yedekleme/kurtarma, denetleme/teftiş, sistem izleme, güvenlik fonksiyonlarının çalışır sisteme etki etmemesi, acil durum gücü/enerjisi, kendini doğrulama, güvenlik planları-politikaları ve prosedürleri.

5.2.4. NIST 800-82

ABD Ulusal Standartlar ve Teknoloji Enstitüsünün 800-82 kodlu ve 'Endüstriyel Denetim Sistemleri Güvenliği Rehberi' başlıklı çalışması, genel olarak, SCADA/DDS sistemlerinin daha güvenli hale getirilebilmesi için muhtemel tehdit ve açıklıkların tanımlanmasını ve böylece farklı güvenlik metot ve tekniklerini birlikte sunmayı hedeflemektedir [62].

NIST 800-82, doğrudan bir güvenlik kontrol listesi sunmamakla birlikte, risk değerlendirmesi çalışmaları için yararlanılacak güvenlik gereksinimleri ve çözümleri sunmaktır. DDS altyapısında kullanılan donanımsal veya yazılımsal bileşenlerini

incelemekte ve daha güvenli ağ-uygulama servisleri için öneride bulunmakta ve örnekler sunmaktadır. Bu nedenle, pratik inceleme ve düzeltmeler için başvurulabilecek kaynaklar arasında yer almaktadır.

NIST 800-82 rehberinde, endüstriyel denetim sistemlerinde ortaya çıkabilecek muhtemel istenmeyen olaylar aşağıdaki şekilde özetlenmiştir [62].

- Ağda taşınan bilginin bloklanması 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 etkilerin oluşması,
- Güvenli sistemlere müdahale ile insanların hayatının tehlikeye düşürülmesi.

5.2.5. IEEE 1402-2000 (R2008)

IEEE (The Institute of Electrical and Electronics Engineers) tarafından 2000 yılından oluşturulan ve 2008 yılında yeniden gözden geçirilen IEEE 1402-2000 (R2008) standardında çoğunlukla elektik güç üretim ve dağıtım istasyonların fiziksel seviyede güvenliği konu edilmekle birlikte, elektronik ortamdan sızmalara da yer vermektedir[63].

5.2.6. IEC 62351

Uluslararası Elektroteknik Komisyonunun, TCP/IP protokolü de dahil güç sistemleri denetiminde kullanılan iletişim sistemlerine ait veri aktarım güvenliğini sağlamaya yönelik bir standart çalışmasıdır [52]. Bu standartta ait dokümanlarda açıklıkların giderilmesine yönelik sunulan yöntemlerin teknik ayrıntıları bulunmaktadır.

5.2.7. NERC kritik altyapı koruma

Kuzey Amerika Elektrik Emniyeti Kuruluşu (NERC), ilk olarak 2003 yılında Acil Aksiyon Standardı olan "1200 Siber Güvenlik" belgesini yayınlamış ve bunu takiben NERC 1300 çalışmasını başlatılmıştır. Bu çalışmaların ardından 2006 ve sonrasında NERC, daha kapsamlı olan ve alt başlıklardan oluşan Kritik Altyapı Koruma CIP:002-1 ile CIP 009-2arasındaki çalışmalarını yayınlamıştır. NERC 1200, iletim ve dağıtım birimlerini kapsayan bir çalışmayken, CIP 002-1 ile CIP 009-2 serisindeki çalışmalar üretim tesislerini de içerecek şekilde genişletilmiştir [64]. ABD Federal Enerji Düzenleme Komisyonu (FERC) tarafından 2006 yılında NERC CIP standartlarını onaylamasının ardından, CIP standartlarına uyumluluk enerji sektörü için yükümlülük haline gelmiştir [65].

5.2.8. AGA 12

Amerikan Gaz Birliği (AGA) tarafından SCADA sistemlerinin iletişim güvenliği için dört başlık altında AGA 12 geliştirilmiştir. AGA 12, elektrik, gaz ve su tesislerini de kapsayacak şekilde SCADA otomasyon sistemi için kripto mekanizmalarını içermektedir. Ayrıca, nispeten düşük veri işleme ve iletme kapasitesine sahip (genellikle seri) olan endüstriyel iletişim sistemleri için şifreleme yöntemlerini ele almaktadır [52].

5.2.9. API 1164 SCADA güvenliği:

İlk olarak 2004 yılında yayımlanan API 1164, petrol ve doğalgaz boru hattı işletmecilerinin SCADA sistem güvenliğini sağlamaya yönelik bir standarttır. Bu standartta fiziksel güvenliğe yer verilmekle birlikte ağırlıklı olarak iletişimin güvenliği, erişimin kontrolünü, felaketten kurtulma ve iş sürekliliği planı konu edilmektedir [52].

5.3. Güvenlik Standartlarının Karşılaştırılması

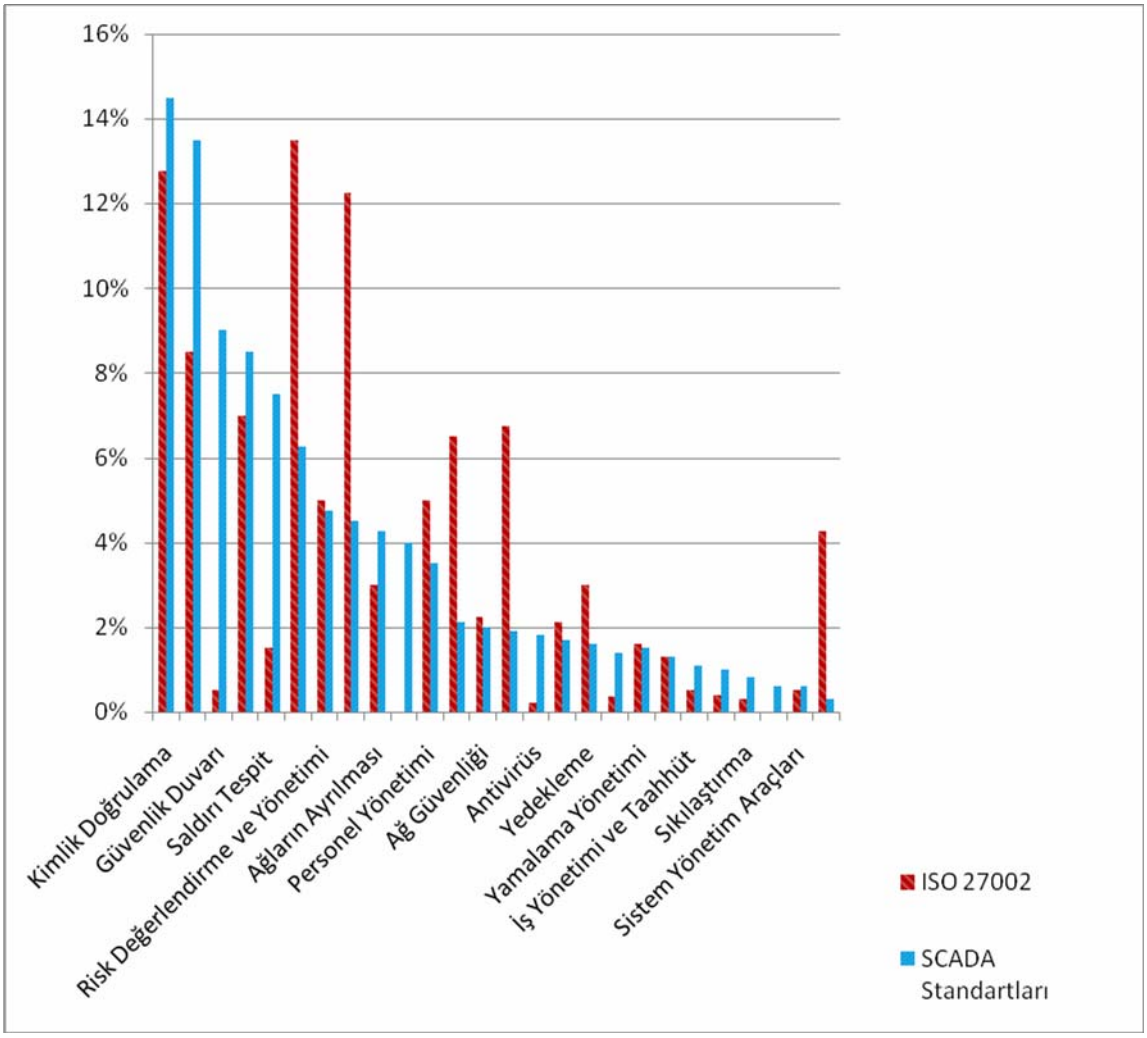
Kritik altyapı ve DDS sistemlerin korunmasına yönelik çalışma ve standartlar arasında yaklaşım, içerik ve kapsam yönüyle farklılıklar bulunmaktadır. Çizelge 5.4.'te güvenlik politikaları, açıklık ve risk değerlendirmesi, organizasyon güvenliği, varlık sınıflandırma ve denetim, personel güvenliği ana başlıklarında ve ilgili alt başlıklarda yukarıda yer alan çalışma ve standartların karşılaştırılması yer almaktadır.

Çizelge 5.4. Kritik altyapı ve DDS sistemlerin korunmasına yönelik çalışma ve standartların kapsam yönüyle sınıflandırılması [52]

	API 1164	IEEE 1402	AGA 12	NERC CIP	ISA TR99-01	ISA TR99-02	PCSRF	IEC 6210	IEC 62351
GÜVENLİK POLİTİKALARI									
Bilgi Güvenliği Politikaları	√	√	√	√	√	√	√	√	√
AÇIKLIK VE RİSK DEĞERLENDİRMESİ									
			√	√	√	√	√		
ORGANİZASYON GÜVENLİĞİ									
Bilgi Güvenliği Altyapısı		√	√	√			√	√	
Üçüncü Şahıs Erişim Güvenliği	√		√	√		√	√	√	
Dış Kaynak Kullanımı				√				√	
VARLIK SINIFLANDIRMA VE DENETİM									
Varlıkların Sorumluluğu				√	√	√	√	√	
Bilginin Sınıflandırılması	√				√	√		√	
PERSONEL GÜVENLİĞİ									
İş Tanımı ve Kaynak Güvenliği	√	√	√	√	√	√	√		
Kullanıcı Eğitimi	√	√	√	√	√	√	√		
Güvenlik Olaylarını ve Sorunları Karşılama	√	√	√	√	√		√		
Personel Niteliği		√							

Sommestad ve ark.[66] bu bölümde yer alan NERC CIP, ISA TR99-01, NIST 800-82, NIST SPP-ICS standart ve çalışmalara ilaveten ABD Ulusal Altyapı Koruma Merkezince hazırlanan "Süreç Denetim ve SCADA Güvenliği İyi Uygulama

Örneği", ABD Savunma Bakanlığınca hazırlanan "Denetim Sistemleri için Siber Güvenlik Tedarik Dili", ABD Enerji Bakanlığınca hazırlanan "SCADA Ağının Siber Güvenliğinin İyileştirmek için 21 Adım" gibi standart ve rehberleri de içeren çalışmalarında incelenen tüm belgelerde önerilen önemleri sayarak normalize ettiklerinde ve benzer sayma ve normalizasyon ile daha genel bir standart olan ISO/IEC 17799 (yeni ISO/IEC 27002) ile kıyasladıklarında Şekil 5.1.'i elde etmişlerdir.



Şekil 5.1. SCADA güvenlik standart ve rehberlerinde geçen güvenlik grubu başlıklarının normalize edilmesi ve ISO/IEC 27002 ile kullanım sıklıklarının karşılaştırılması [66]

Şekil 5.1.'de net olarak görülebileceği gibi daha genel bir bilgi güvenliği standardı olup odak olarak BT ihtiyaç ve özelliklerini aldığı söylenebilecek ISO/IEC 27002 ile

diğer SCADA/DDS standart ve rehberlerle karşılaştırıldığında, alınması gereken önlemlerin önceliklerine ilişkin anlamlı farklılıklar içerdiği söylenebilecektir.

6. ÖRNEK DURUM İNCELEMELERİ: AÇIKLIKLARIN ARAŞTIRILMASI, GÜVENLİK TARAMALARI VE ALTYAPI BİLEŞENLERİNİN KRİTİKLİĞİ

Bu çalışma kapsamında, aşağıda sıralı nedenlerden ötürü saha çalışmalarının yapılmasına karar verilmiş ve Türkiye'de faaliyet gösterip altyapısında SCADA/DDS sistemlerini iş süreçlerini izlemek ve yönetmek için kullanan iki farklı işletmeci ile ortak çalışmalar yürütülmüştür. Yürütülen saha çalışmalarından (Örnek Durum İncelemelerinden) beklenen ve hedeflenenler özetle aşağıda sunulmuştur.

- SCADA/DDS altyapı ve bileşenlerini yerinde görmek, yürütülen kritik iş süreçlerini gözlemek,
- İncelenen altyapı ve süreçlerinin siber güvenlik gereksinimlerini ve önceliklerini belirlemek, güvenlik açıklıklarını tespit etmek ve literatürde yer alan gereksinim ve açıklıklarla karşılaştırmak,
- Çalışmanın devamında yürütülecek olan 'güvenlik iyileştirme önerisi' aşamalarının çalışan işletmelerdeki önceliklerle, gerçeklerle ve ihtiyaçlarla uyumlu olmasını sağlamak,
- Saha çalışmaları sayesinde, endüstri/sanayi ile ortak yürütülen çalışmalardan karşılıklı fayda edinilmesini sağlamak.

Örnek Durum İncelemeleri iki farklı işletmenin altyapısı ve iş süreçleri üzerinde gerçekleştirilmiştir. İşletmeler seçilirken aşağıdaki kriterler esas alınmıştır:

- İşletmecilerin SCADA/DDS altyapısına sahip olması,
- Bölge veya ülke ölçeğinde hizmet vermesi ve verdiği hizmetin devamlılığının kamu ihtiyaçları ve sağlığı, bölge/ülke ekonomisi ve refahı için önemli olması,
- İşletmecilerin birbirinden farklı hizmet dallarında yer alması,
- İşletmecilerin farklı altyapı ürünleri (marka, model, ağ mimarisi ve erişim teknolojisi) kullanması.

Ortak çalışma yürütülen iki işletmeden birincisi bölge ölçeğinde, ikincisi ise ülke genelinde hizmet vermektedir. Verdikleri hizmete ilişkin üretim, dağıtım ve iletim gibi iş süreçlerinin tümünün izlenmesi ve yönetilmesi için dağıtık denetim sistemleri kullanmaktadırlar. Örnek Durum çalışmalarından da elde edilen kritik bilgiler (somut açıklık bulguları, altyapı bileşenleri gibi) ve işletmeci isimleri,ortak çalışma yürütülen işletmecilerin güvenliğini zarar vermemek için burada verilmemiştir.

6.1. Açıklık İnceleme ve Penetrasyon Testleri

Siber güvenlik durum değerlendirme çalışmaları genel olarak açıklık inceleme ve penetrasyon testleri olarak iki başlık altında sınıflandırılmaktadırlar. Açıklık inceleme ile penetrasyon testleri arasından hem uygulanış hem de uygulandığı sistem üzerinde bıraktıkları etkiler açısından ciddi farklılıklar bulunmaktadır. Açıklık inceleme ve değerlendirmeleri, araştırmacıların sistem hakkında bilgi toplayacağı kaynaklara ulaşmalarını içerir. Penetrasyon testleri ise, bir açıklığın kullanılarak sisteme verilecek zararın ve saldırı tekniklerinin uygulanabilirliğinin ölçülmesi kapsar. Bu nedenle, test ortamı olmadıkça fiziki süreçleri yöneten DDS sistemlere yönelik penetrasyon testlerinin uygulanması da önerilmemektedir [67-69]. Bu sebeple, Örnek Durum İncelemelerinin kapsamı sadece açıklık incelemeleri ile sınırlı tutulmuş ve sistem üzerinde etki oluşturacak hiçbir araç kullanılmamış, kullanılan açıklık tarama araçlarının güvenli tarama kiplerinin bulunmasına dikkat edilmiştir.

6.2. Açıklık İnceleme Yöntemi

Açıklık incelemelerinde, sistemin sadece yazılımsal araçlarla taranması sağlıklı ve yeterli bilgiyi vermeyecektir. Bu tür tarama testlerinin yanı sıra, altyapı bileşenlerinin, bağlantılarının, bulundukları fiziki şartların gezilerek görülmesi ve haklarında notlar alınması; ayrıca sistem işleticilerine yönetilmek üzere sorular hazırlanması ve varsa yazılı belge haline getirilmiş mevcut güvenlik politika, prosedür ve talimatlarının incelenmesi resmin tümünün ortaya konulması açısından önem taşımaktadır. Bu sebeple incelenen sistemleri tehdit kaynaklarının saldırılarına maruz bırakabilecek ‘Açıklıklarını’ araştırılmaya başlanmadan önce, açıklıklarının

nerelerde aranacağının tarif edilmesine ve inceleme yöntemlerinin tanımlanmasına ihtiyaç vardır.

Güvenlik açıklıklarının tespiti için uygulanma safhası ise aşağıdaki gibi planlanmıştır (İlk dört adım NIST SP 800-30 [25] belgesinde açıklık tespiti için önerilen bilgi toplama teknikleri arasındadır).

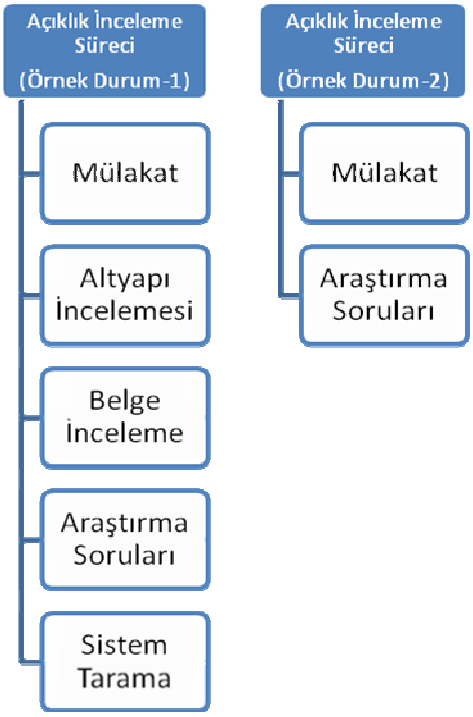
I. Mülakat ve saha gezileri: Teknik ve idari personelle yüz yüze görüşmelerdedestek, tedarik, altyapı güncelleme, sorumlulukların tayini gibi konularda soruların yöneltilmesi,teknik personel eşliğinde altyapının farklı birimlerinin gezilmesi ve notlar alınmasını içerençalışmalar
II. Araştırma soru formu (Anket): Literatür araştırmalarından elde edilen bilgi ve birikime dayanarak altyapı, sistem bileşen ve teknolojileri, personel, mevcut güvenlik uygulamaları, takip edilen güvenlik süreçleri hakkında sorular hazırlamak ve ilgililerinin cevaplarını almak (Hazırlanan ve işletmelere sorulan sorular Ek-1'de yer almaktadır)
III. Mevcut belgelerin incelenmesi: Var olan politika, prosedür ve denetleme raporlarının incelenmesi
IV. Ağ ve sistem taraması: Ağ ve sistem bileşenlerinin saptanması ve güvenlik açıklıklarının tespiti için kullanılabilecek araçların kullanımı
V. Sosyal Mühendislik: A işletmecinin kullandığı ürünlere (marka, model ve versiyon) ilişkin bilinen güvenlik açıklıklarının var olup olmadığının, B işletmecinin kullandığı altyapı ve bileşenlerine ait hangi bilgilerin internet ortamında var olduğunun araştırılması

Birinci Örnek Durum İncelmesi için yukarıda tanımlı olan 'açıklık tespiti uygulama planındaki' aşamalarının tümü gerçekleştirilmiştir. Üstelik işletmecinin sunduğu imkankarşısında, 'Sistem İncelemeleri' adı altında bir aşama daha plana eklenmiş ve bu aşamada NIST SP 800-115 'Bilgi Güvenliği Test ve Değerlendirmesi' [70] belgesinde yer alan ve aşağıda yazılı olan gözden geçirme tekniklerinden ilk üçü kullanılabilmiştir.

1. Logların gözden geçirmesi-Kullanıldı
2. Erişim ve engelleme kural setlerinin gözden geçirme-Kullanıldı
3. Sistem konfigürasyonlarının gözden geçirme-Kullanıldı
4. Ağ tarama ve paket yakalama- Ağ ve sistem taraması adımı içinde kullanıldı
5. Dosya bütünlük kontrolü—Kullanılmadı

İkinci Örnek Durum İncelemesi için ise planlanan uygulama aşamalarından sadece, 1. Adımdaki teknik personelle mülakat kısmı ile 2. Adımının tamamı gerçekleştirilebilmiştir.

Şekil 6.1.'de Örnek Durum İncelemesi 1 ve 2 için gerçekleşen uygulama aşamaları yer almaktadır.



Şekil 6.1.Örnek Durum İncelemesi-1 ve 2 için açıklık incelmesinde takip edilen aşamalar

6.3. Araştırma Soruların Hazırlanması ve Cevaplanması

İlgili çalışanlarca cevaplanmak üzere, EK-1'de yer alan 'Dağıtık Denetim Sistemi Kullanan Kritik Altyapılar için Güvenlik Araştırma Soruları' adlı form, ortak çalışma yürütülen her iki işletmeciye sunulmuş ve cevaplandırılması istenmiştir.
Bu soru formu, Genel (2 soru), Organizasyon ve Personel (7 soru), Fiziki Güvenlik (8 soru), Erişim Kontrolü ve Hesap Yönetimi (17 soru), İletişim ve İletişim Güvenliği (7 soru), Sistem Güncelleme ve Yedeklilik (10 soru), Denetim (9 soru), Dış Kaynak Kullanımı (4 soru) olmak üzere 64 sorudan oluşmaktadır.

Sorular hazırlanırken, Bölüm 4 ve 5'de atıfta bulunulan kaynaklarda ele alınan konu başlıklarından da yararlanılmıştır. Sorulara verilen cevapların, Bölüm 8'deki güvenlik iyileştirmeleri çalışmalarına, diğer açıklık inceleme aşamalarıyla birlikte zemin oluşturması hedeflenmiştir.

Araştırma soruları formunda, bazı konular yapılan mülakatlarda da geçmiş veya saha incelemelerinde gözlenebilmiş olsa da yazılı soru olarak yeniden yönetilmiştir. Burada, yazılı 'Araştırma Formunun' sözlü mülakat ve göz yordamıyla yapılan incelemelerle desteklenmesi; diğer yandan, sözlü mülakat ve göz yordamıyla yapılan incelemelerindeki bazı hususlarında teyit edilmesi amaçlanmıştır.

6.4. Güvenlik Açıklıklarının Taranması

Bir sistemin güvenlik açıklıkları belirlenirken, Bölüm 6.2'de sunulan bilgi toplama tekniklerinden mümkünse tümünün kullanılması gerekir. Bu tekniklerden dördüncü adımdaki ağ ve sistem taraması haricindekiler, çoğunlukla açıklık kaynaklarının tespitine yönelikken, ağ ve sistem bileşenlerinin taranması mevcut olan teknik açıklıkların doğrudan tespitine imkân verecektir. Açıklık taramaları bu yönüyle farklı olduğu gibi, inceleme yapılan sistemde olumsuzluk oluşturabilme riski nedeniyle de diğer tekniklerden ayrılmaktadır.

Yukarıda değinildiği gibi Örnek-Durum İncelemelerinden sadece biri için açıklık taraması gerçekleştirilebilmiştir.

Kademelendirilmemiş ve toptan yürütülen açıklık taramalarının, 7/24 esasına göre hizmet veren altyapının güvenliğini tehlikeye sokacağı hesaba katıldığından, tarama ve incelemeler merkez, iletişim ağı ve tek bir saha (uç) birimi için ayrı ayrı yapılmıştır.

Taramanın ilk olarak yapıldığı Merkez Birimdeki doğrudan varlıklar aşağıdaki gibidir.

- Sunucu donanımları
- İş istasyonu donanımları
- İşletim sistemleri
- Uygulama yazılımları (SCADA uygulama yazılımı)
- Veri tabanı
- Yerel alan ağı anahtarı (Ethernet Switch)

İletişim birimindeki doğrudan varlıklar ise;

- Kablolu kablosuz erişim ortamları,
- Modemler,
- Ağ anahtarları,
- Ortam geçit ve dönüştürücüleri (Gateway),
- Yönlendiricilerdir.

Uç birimlerindeki incelemeye dâhil edilen doğrudan varlıklar ise sadece RTU/PLC denetleyici cihazlarıdır.

Ağ ve sistem güvenlik taraması ile elde edilmek istenen bilgiler aşağıda tanımlanmıştır. Bunlardan ilk beşinin tarama araçlarıyla sonuncusunun ise el ve göz yordamıyla kontrollerinin yapılması planlanmıştır.

1. Ağdaki varlıkların saptanması
2. Ağ tabanlı kullanılan servislerin saptanması
3. Kullanılan servislerinin açıklıklarının tespiti
4. Ağ trafiğinden numune alınması
5. Ağda kullanılan protokollerin saptanması
6. Kullanılan işletim sistemlerinin eksik yama, yanlış yapılandırma durumlarının ve sıkılık düzeylerinin araştırılması

Yukarıda yer alan tespit ve saptamaların ilk beşi için kullanılabilecek ulaşılabilir araçlar araştırıldığında, bu tür incelemeler için mevcut olan yüzlerce yazılımsal araç içerisinden Nmap, Nessus ve Wireshark adlı programların kullanılmasına karar verilmiştir.

NMAP (Network Mapper*)*, hem RTU/PLC hem de SCADA uygulamasının yer aldığı işletim sistemlerindeki kullanılan veya açık olan TCP/UDP servislerini, işletim sistemi adı ve versiyonu tespiti için kullanılmıştır. Bu sayede yukarıda yer alan 6 tespit ve saptama hedefinin ilk ikisi NMAP sayesinde gerçekleştirilmiştir.

Nessus, sistemde yamalanmamış uygulamaların, ön tanımlı şifre kullanımının, yanlış yapılandırılmış servislerin varlığı gibi nedenlerden kaynaklı açıklıkların tespitinde kullanılan oldukça güçlü bir yazılımdır [71].

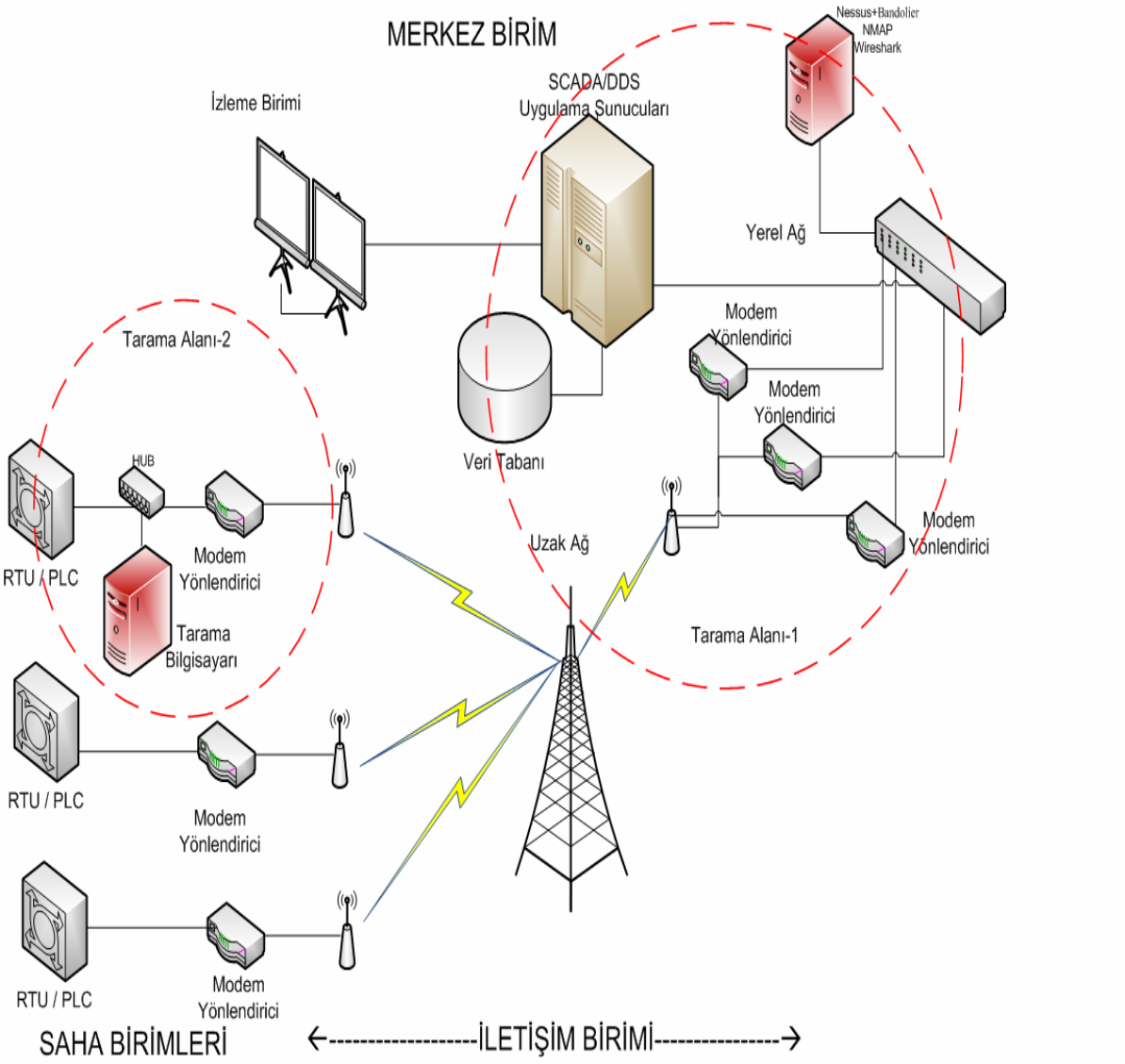
En önemlilerinden biri Nessus olmakla birlikte, tipik BT sistemleri için geliştirilmiş çok sayıda ağ ve host tabanlı güvenlik tarama aracı bulunurken, SCADA/DDS sistemlerine yönelik olarak geliştirilmiş özel bir açıklık tarama aracı bulunmamaktadır. Buna karşılık, ABD Enerji Bakanlığının desteğiyle DigitalBond tarafından geliştirilen ve TenableNessus 4inceleme ve tarama aracı üzerinde çalışan Bandolier eklentisi geliştirilmiştir. Nessus Bandolier eklentisi, çalışan sistem

üzerinde herhangi bir etki oluşturmadan SCADA konfigürasyonlarının değerlendirilmesi ve bulunan açıklıkların listelenmesi işlevini görmektedir [67, 72]. Bu yönüyle Bandolier eklentisi ile birlikte kullanıldığında Nessus, tipik BT açıklık tarayıcılarından çok daha fazla ve incelenen SCADA/DDS sistemine özgü açıklıkları gösterebilmektedir.

İnceleme sırasında, çalışan sisteme zarar vermemek için Bandolier eklenti etkin olan Nessus, “Safe checks" seçili ve "Thorough tests" etkisiz olarak yapılandırılmıştır. Nessus ile 6 tespit ve saptama hedefinin üçüncüsü gerçekleştirilmiştir.

Ağda akan trafiği izleme, analiz etme ve kaydetme maksadıyla, bir endüstri standardı haline gelmiş olan Wireshark yazılım aracı kullanılmıştır. Bu yazılım aracının bu inceleme için en önemli getirisi ise Fieldbus, Modbus, OPC, DNP3, IEC 60870-5-104 ve IEEE C37.118 gibi SCADA protokollerini çözümleyebiliyor olmasıdır [67]. Wireshark trafik analizörü ile birbiriyle iletişim kuran birimlerin hangi protokolle ve nasıl haberleştiklerini (açık metin olarak mı yoksa şifreli ve yetkilendirilmiş biçimde mi) tespite çalışılmıştır. Wireshark ile 6 tespit ve saptama hedefinin dört ve beşincisi gerçekleştirilmiştir.

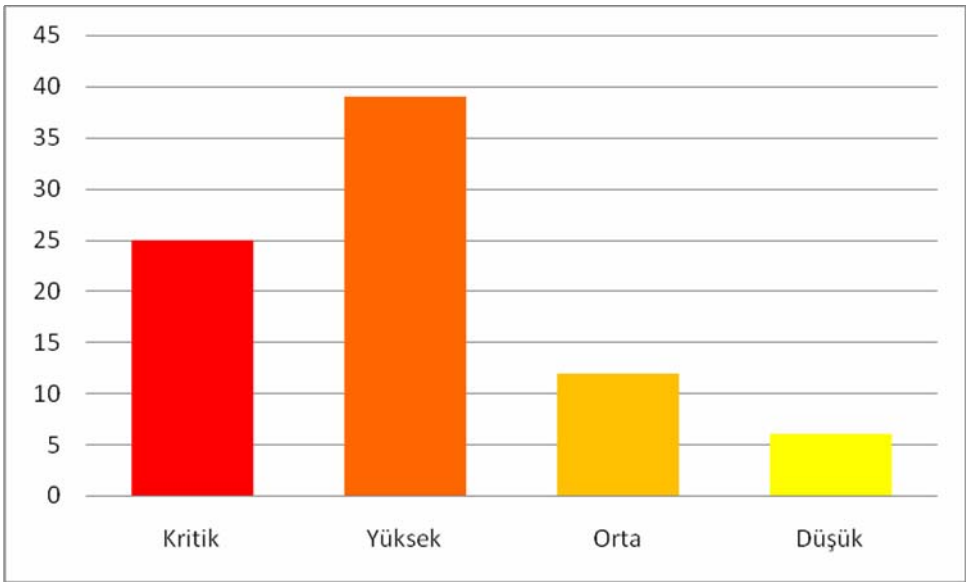
Şekil 6.2.’de yukarıda belirtilen tarama araçları kullanılarak Örnek Durum İncelemesi-1 için altyapıdaki tarama alanları gösterilmiştir.



Şekil 6.2. Örnek Durum İncelemesi-1 için altyapıdaki tarama alanları Son tespit hedefi ise sistemler üzerinde el ve göz yordamıyla yapılan incelemeler ile tamamlanmıştır.

6.5. İncelemelerde Elde Edilen Açıklık Bulguları

Ağ ve sistem taramalarının gerçekleştirildiği Örnek Durum I incelemesinde, altyapıdaki tüm varlıklar üzerinde Şekil 6.3.'te gösterildiği üzere 25 kritik, 39 yüksek, 12 orta, 6 düşük olmak üzere toplam 82 güvenlik açıklığı tespit edilmiştir. Bu açıklıklardan önemli bir bölümü kullanılan işletim sistemleri ve üzerlerindeki servis ve uygulamalara ilişkin güvenlik açıklıklardır. İkinci sırada,kullanılan iletişim ağı ve iletişim protokollerinden kaynaklı açıklıklar yer almaktadır.



Şekil 6.3. Örnek Durum I incelemesi için ağ ve sistem taramalarından elde edilen açıklık bulgularının sayıları

Elde edilen somut açıklık bulguları ortak çalışma yürütülen işletmeciye özel olarak hazırlananraporda ayrıntılı olarak sunulmuştur. Anket, mülakat ve diğer saha incelemeleri birlikte ele alındığında,tespit edilen önemli açıklık bulgularının aşağıdaki sıralı nedenlerden kaynaklandığı anlaşılmıştır.

I. Kullanılmayan servislerin açık durumda bulunması,
II. Kullanılmayan ağ protokollerinin açık durumda bulunması,
III. Sıkılaştırılmamış ve yamalanmamış işletim sistemlerinin kullanımı,
IV. Kullanılan endüstriyel iletişim protokollerinin ve erişim tekniklerinin güncel ve yeterli gizlilik, bütünlük ve kimlik doğrulama mekanizmalarını desteklememesi,
V. Erişim denetimi ve hesap yönetimden kaynaklı açıklıklar,
VI. Değişiklik yönetimi ve yedekleme eksikliklerin kaynaklı açıklıklar,
VII. İnternet gibi çeşitli ortamlardan işletmeye ait bazı hassas bilgilere ulaşılabilmesi,
VIII. Çalışanların yeterli güvenlik eğitimi almaması, sorumluluk ve yükümlülüklerin net olarak tarif edilmemesi.

Tespit edilen açıklık bulguların önemli bir bölümünün mevcut kaynaklar içinde uygun kural ve politikalar oluşturularak sürdürülebilir bir çözüme kavuşturulabileceği görülmüştür. Ancak bazı açıklıkların giderilmesinin ise altyapıdaki bileşenlerin değiştirilmesi, altyapı tasarımının baştan ele alınmasıyla sağlanabileceği anlaşılmıştır.

İkinci Örnek Durum incelemesi için, ağ ve sistem taramaları gerçekleştirilemediği için ilk üç açıklık kaynaklarının varlığından söz etmek mümkün olmasa son beş açıklık kaynağına ilişkinbulguların varlığına rastlanmıştır

6.6. Altyapı Bileşenleri İçin Operasyonel Kritiklik ve Güvenlik Riski Sıralaması

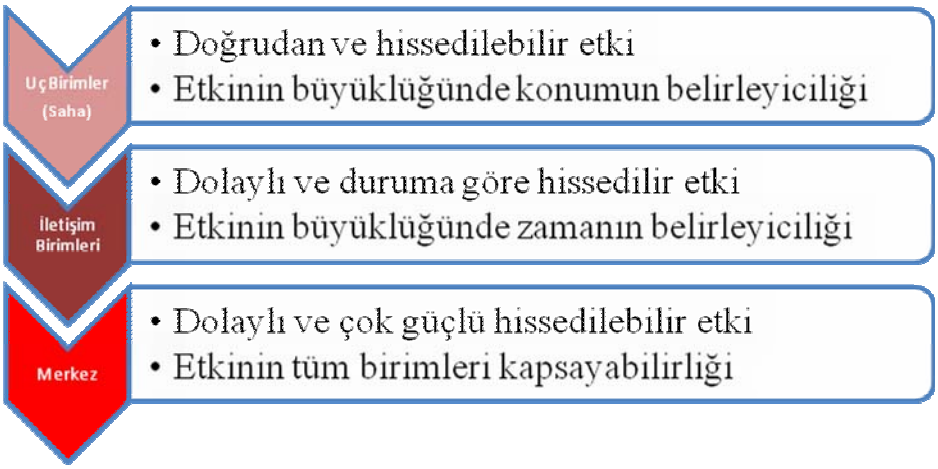
İşletmeci teknik personelleriyle yapılan mülakatlarda, altyapı bileşenleri için sınıflandırma ve her bileşenin gördüğü fonksiyonlar itibariyle kritiklik sıralamaları yapılmıştır.

Sınıflandırmalarda donanım, yazılım ve fiziki bileşen ayrımı yapılmadan, altyapının topolojik olarak farklı katmanları, merkez, iletişim ve uç olmak üzere üç ana bileşen şeklinde değerlendirilmiş ve güvenlik kritikliği sıralaması bu üç bileşen üzerinden yapılmıştır. Böyle bir sıralama ve sınıflandırma ayrıca, Bölüm 6.4'de yer alan ağ ve sistem açıklık taraması öncesinde taramadan kaynaklı risklerin önceden bilinmesi açısından da önem arz etmektedir. Bu bağlamda, inceleme yapılacak işletmenin teknik personelleriyle yapılan değerlendirme ve görüş alış verişi ile hangi ana bileşende oluşabilecek sorunların (kısmı veya tamamen çalışmama, yanlış fonksiyonlar icra etme), hangi istenmeyen olayları (etkileri) meydana getirebileceği, istemeyen etkilerin olumsuzluk şiddetinin ve alanının neler olabileceği tartışılmıştır. Böylece sistemde oluşabilecek istenmeyen olayların neler olabileceği, bunların hangi bileşen veya ana bileşenlere yönelik yetkisiz müdahalelerin neticesinde çıkabileceği anlaşılmaya çalışılmıştır.

Yapılan güvenlik kritikliği sıralamasına göre, süreçleri izleme ve yönetme görevini icra eden SCADA uygulama yazılımı ve onun koşturulduğu sistem (işletim sistemi

ve donanımlar) ile yer aldığı ağ etki alanı açısından en kritik bileşen olarak değerlendirilmiştir. Aynı değerlendirmenin devamında, ikinci sırada uç birimlerle iletişimi sağlayan iletişim birimleri ve en son olarak da uç birimlerdeki RTU/PLC türü denetleyiciler yer bulmuştur.

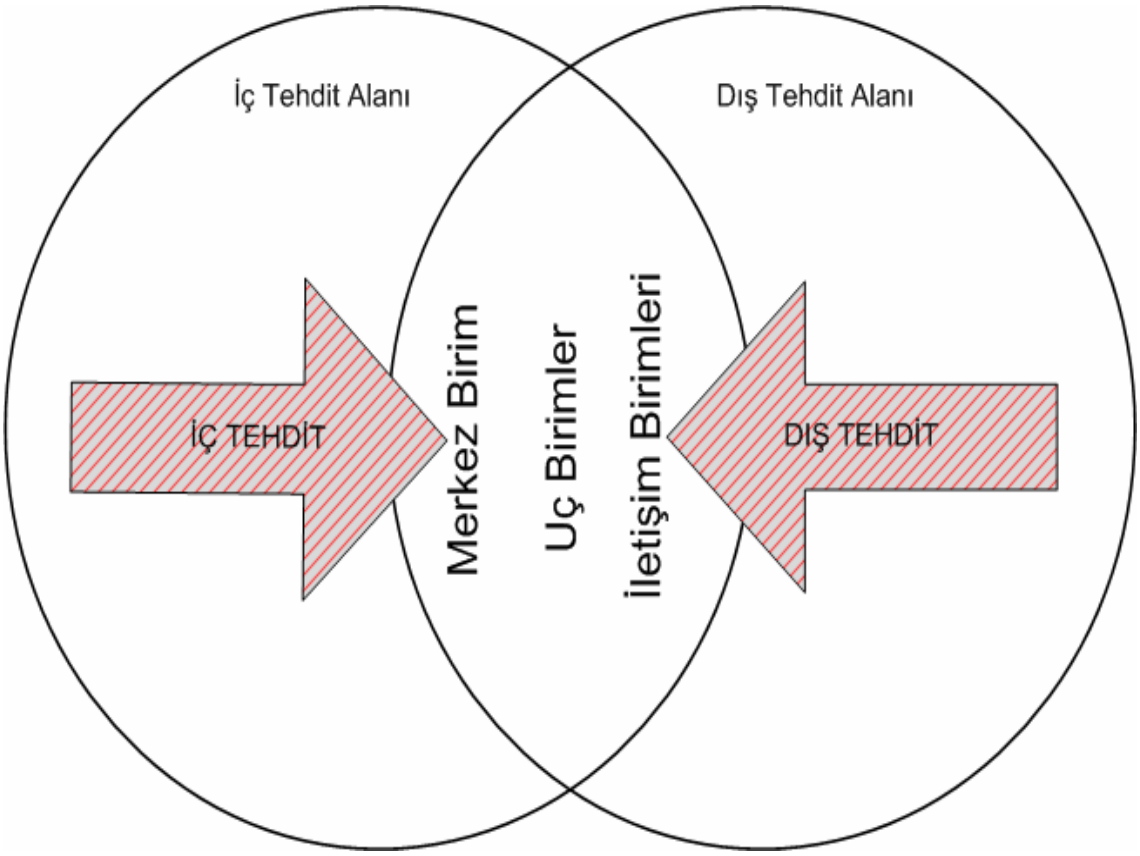
Şekil 6.4.'te sistem bileşenlerinin etki alanı açısından operasyonel kritikliğe göre sıralaması görülmektedir. Ancak bu sıralamanın, bir problemin oluşturacağı etkinin kapsamına göre yapıldığını yenilemek yerinde olacaktır. Zira oluşan etki kadar etkinin konumu, zamanlaması, süresi ve zamanlamaya bağlı olarak tetikleyeceği diğer problemlerin de önemli olduğunu; konum, zamanlama ve süreye göre Şekil 6.4.'te verilen operasyonel kritikliğin sıralaması değişebileceği göz önünde bulundurmak gerekecektir.



Şekil 6.4. Altyapı bileşenlerinin etki kapsamına göre operasyonel kritikliğin sıralaması

Altyapının barındığı bir açıklığın bir tehdit kaynağı tarafından saldırıya dönüştürülmesi ihtimali bakımından, altyapı bileşenlerinin güvenlik kritikliği ele alındığında iç ve dış tehdit kaynaklarına göre iki farklı sıralamanın çıkabileceği anlaşılmıştır.

Uygunsuz bir müdahalenin kasıtlı veya kasıtsız olarak gerçekleştirilebilme ihtimalini tehdit kaynaklarının altyapı bileşenlerine erişebilirlik durumları belirlemektedir. Bu anlamda, iç tehdit kaynakları için erişim alanı Merkez ve Uç birimlerinden başlamaktadır. İletişim Birimi, bu iki sistem bileşenine doğrudan erişim imkânının olmadığında durumlarda kullanılması düşünülebilecek bir birim olarak değerlendirilebilecektir. Kasıtlı veya kasıtsız bir müdahalenin yol açacağı problemleri oluşturacak dış siber tehditler sınıflandırılmasında, tehdidi ortaya çıkarabilecekler için sistem bileşenlerine erişilebilirlik sınıflandırması İletişim Birimlerinden başlamaktadır. Bu değerlendirmelere uygun olarak Şekil 6.5.'te iç tehdit ve dış tehdit kaynakları yaklaşımına göre DDS altyapı bileşenleri için güvenlik riski sıralamaları gösterilmiştir.



Şekil 6.5. İç ve dış siber tehdit yaklaşımına göre altyapı bileşenleri için güvenlik riskleri

Bu bağlamda güvenlik iyileştirme önerileri çalışmalarında öncelikle 'İletişim' ve sonrasında 'Merkez' birimi odak alan bir yaklaşım takip edilecektir. Çünkü 'Uç'

birimlere yönelik tehditlerin çoğunlukla, 'İletişim' ve sonrasında 'Merkez' birimlerdeki açıklıkların kullanımı sonucu olarak saldırıya dönüşebileceği değerlendirilmektedir. SCADA/DDS altyapılarına yönelik olası tehdit kaynaklarının hedefi nihayetinde uç birimlerdeki bileşenlerinin kontrolünü almak veya işlevsiz bırakmak olarak ele alınsa dahi, siber saldırılar açısından iletişim veya merkez birimlere müdahale etmeden bu hedefin gerçekleşmesi mümkün görülmemektedir.

6.7. Örnek Durum İncelemelerinin Değerlendirilmesi ve Çalışmaya Katkısı

Her iki Örnek Durum İncelemesinden birincisi planlandığı gibi tamamlanabilmiş, ikincisinin ise ilk iki aşaması gerçekleştirilebilmiştir. İncelemelerin tamamlanmasıyla yürütülen saha çalışmalarından (Örnek Durum İncelemelerinden) beklenen ve hedeflenenlerönemli gerçekleştirilebilmiştir.

Örnek Durum İncelemeleri, neticesinde elde edilenler aşağıda özetle sıralanmıştır.

- Çalışan DDS altyapılar için güvenlik açığı inceleme yaklaşımının nasıl yürütülebileceğinin anlaşılması,
- DDS altyapıları için olası açıklıklarının listelenebilmesi ve literatürde tanımlı olanlarla karşılaştırılması,
- Gerçekleştirilecek saldırıların hangi etkileri (istenmeyen olayları) doğurabileceğinin anlaşılması,
- Örnek durum incelemeleri için somut açıklık bulguları ile olası açıklıkların giderilmesine yönelik 'mevcut tedbir' ve 'eksik tedbirlerin' tespit edilmesi (yayımlanmadı),
- Güvenlik açıklıklarını oluşturan açıklık kaynaklarının anlaşılması,
- Saha tespit ve gözlemlerine dayalı olarak ihtiyaç duyulan güvenlik iyileştirmelerinin saptanması.

Bu bağlamda elde edilen veri, bulgu ve deneyimler, Bölüm 7 ve Bölüm 8'deki çalışma ve tartışmalar için zemin teşkil etmiştir.

Çalışmalarda elde edilebilen açıklık ve açıklık kaynaklarına ilişkin somut tespitler, olası açıklıkların giderilmesine yönelik mevcut ve eksik tedbirler, ortak çalışma yürütülen işletmecilerin güvenliğini tehlikeye düşürmemek ve başlangıçta yapılan karşılıklı taahhütlere uygun davranmak için burada verilmemiştir. Bu sebeple, Bölüm 7.'deki risk belirleme ve değerlendirme çalışmalarında DDS sistemler için tanımlanabilen tüm açıklıklar dikkate alınmış ve Örnek Durum İncelemelerine dayalı olarak 'İstenmeyen Olay-Saldırı-Kullanılabilecek Açıklıklar' eleştirme ve ilişkilendirmeleri kullanılmıştır. Benzer şekilde Bölüm 8.'de sadece Örnek Durum İncelemelerinde tespit edilen somut açıklıklar değil olası tüm açıklıkların giderilmesine yönelik iyileştirme önerilerinde bulunulmuştur.

7. KRİTİK ALTYAPILARDA KULLANILAN DENETİM SİSTEMLERİNE YÖNELİK SİBER RİSKLERİN DEĞERLENDİRİLMESİ: OLASI GÜVENLİK AÇIKLIKLARIN KRİTİKLİĞİNİ BELİRLEYEN BİR YAKLIŞIM ÖNERİSİ

Bu bölümde, DDS sistemleri kullanan ve hasar görmesi halinde kamu sağlığı, emniyeti ve bölge/ülke ekonomisini doğrudan etkileyebilecek altyapılara özgü olarak güvenlik açıklıkların kritikliğini ve böylece öncelikli iyileştirmeleri bulmaya yönelik güvenlik riski saptama yaklaşımı önerilmiştir.

Güvenlik risklerinin belirlenebilmesi için öncelikle;

I. Varlıkların belirlenmesi
II. Açıklıkların tanımlanması ve tespiti
III. Tehdit kaynaklarının tanımlanması
IV. Muhtemel saldırı hedeflerinin ve biçimlerinin belirlenmesi

sıralaması takip edilecektir. Sonrasında ise risklerin belirlenmesi için tehdit kaynaklarının gücüne değer biçilmesi ve istenmeyen olayların güvenlik açıklıklarının fonksiyonu biçiminde tanımlanması süreçleri takip edilecektir.Önerilen risk yaklaşımı, başta tanımlı istenmeyen olayların doğrudan açıklıklara bağlı bir fonksiyon olarak tanımlanması ve açıklıkların önem/kritiklik derecelerine göre sıralamasına dayanmaktadır. Böylece açıklıkların kritiklik değerlerine göre her işletmece için iyileştirme önceliklerinin belirlenmesi mümkün hale gelebilecektir.

7.1. Varlık,Açıklık,TehditKaynaklarıveSaldırılarınTanımlanması,Etiketlenmesi, Sınıflandırılması ve Eşleştirilmesi

İncelenen bir sistemin siber güvenlik risk değerlendirmesinin yapılabilmesi için öncelikle sistemin açıklıklarının tanımlanması ve ortaya çıkarılmasına, hangi açıklığın hangi saldırılar için kullanılabileceğinin ve devamındaki olumsuz etkilerinin neler olabileceğinin belirlenmesine, doğrudan ve dolaylı varlık envanterinin çıkarılmasına ihtiyaç vardır.

Bu çalışma kapsamındakisiber güvenlik risk değerlendirme çalışmalarına kolaylık sağlaması için, öncelikle olası tüm güvenlik açıklıklarının, varlıkların, tehdit kaynaklarının ve saldırılarının tanımlanması ve etiketlenmesi yoluna gidilmiştir. Etiketleme için, ABD Ulusal Standartlar ve Teknoloji Enstitüsünün Endüstriyel Denetim Sistemleri için Sistem Koruma Profili (SPP-ICS) [61] çalışmasında kullanılan ve Örnek Durum İncelemeleri için yürütülen risk değerlendirme süreçleri için de elverişli olacağı değerlendirilen 'V.' , 'ATTACK.', 'ASSET.' notasyonu tercih edilmiştir. Ayrıca tanım ve sınıflandırmalardan da büyük ölçüde yararlanılmış, literatürdeki diğer kaynaklardaki tanımlamalarda kullanılarak, Örnek Durum İncelemeleri için uygun olan tanımlamalar belirlenerek kullanılmıştır.

7.1.1. Varlıkların tanımlanması ve sınıflandırması

Güvenlik risk analizi ve değerlendirmesi çalışmalarında korunması gereken somut ve soyut mal ve değerler "varlık" adı altında tanımlanmaktadır. Somut varlıklara, elektrikli motor, bilgisayar gibi fiziki nesneler örnek verilebileceği gibi bilgi sistemlerinde yer alan veritabanı gibi bilgi varlıkları da örnek verilebilir. Diğer yandan, iş sürekliliği, işletmeci itibarı gibi soyut varlıklar da korunması ve risk değerlendirmesinde yer alması gereken varlıklardandır.

SPP-ICS [61] çalışmasında tanımlı 'Endüstriyel Denetim Sistemleri' varlıkları Çizelge 7.1.'de verilmiştir. Burada tanımlı varlıklar, otomasyon sistem ve süreçlerine ilişkin varlıklar olarak nitelendirilebilir. Çizelge 7.1.'de tanımlı varlıklar, otomasyon sistemlerinin veya süreçlerinin bir parçası olduğu için *Doğrudan Varlıklar* olarak da adlandırılabilecektir.

Çizelge 7.1. Doğrudan varlıkların türü ve etiketlendirilmesi [61]

	Otomasyon Süreçlerine Ait Varlıklar / Doğrudan Varlıklar		
	Varlık Etiketi	**Varlık Türü**	**Açıklama ve Örnekler**
1	ASSET.MECHANIC	Mekanik Varlıklar	Pompa, elektrik motorları, depo gibi sahada kullanılan tüm malzemeler
2	ASSET.SENSOR	Sensorlar	Açma,kapamai kesme, ölçme vb. işleri icra eden her türlü birimler
3	ASSET.CONTROLLER	Denetleyiciler	Komutları alan, gönderen ve ölçüm verilerini merkeze ileten PLC, RTU türü bilgisayar tabanlı birimler
4	ASSET.HMI	HMI	Yönetim, izleme işlerinin merkezi olarak icra edilmesini sağlayan bilgisayar donanımı ve uygulama yazılımları
5	ASSET.COMMUNICATION	İletişim Birimleri	Merkez ile uç birim arasındaki iletişimi sağlayan kablolu kablosuz ortam ve cihazlar
6	ASSET.CTRLPROCESS	Denetlenen Süreçler	Denetlenmesi ve yönetilmesi gereken asli otomasyon süreçleri
7	ASSET.CTRLINFO	Denetlenen Süreçlere Ait Bilgiler	Denetlenen ve yönetilen süreçlere ilişkin değerlendirilmek üzere toplanan, işlenen ve/veya saklanan süreç bilgileri
8	ASSET.BUSINFO	Süreçlere İlişkin Ticari Bilgiler	Ticari karşılığı olan girdi ve çıktılara ait veriler

Doğrudan varlıkların kendi içindeki önem sıralamaları ekonomik değerlerinden çok işlevsel değerlerine dayandırılabilir.

Risk değerlendirme ve güvenlik analizi çalışmalarının amaca uygun şekilde icra edilebilmesi için sistemde istenmeyen olayların meydana gelmesi durumunda etkilenecek tüm varlıklarının tanımlanması ve değerlendirme süreçlerine dâhil edilmesine gerekir. Ancak Çizelge 7.1.'de yer alan varlık sınıflandırması, otomasyon sistem ve süreçlerini kapsamakla birlikte, sistemden beklenen ve istenen tüm çıktıları ve bu çıktıların sonuçlarını kapsamamaktadır. Bu sebeple, Çizelge 7.2.'deki soyut ve somut varlıkların da tanımlanması ve değerlendirme süreçlerine dâhil edilmesine ihtiyaç vardır.

Çizelge 7.1.'den farklı olarak, Çizelge 7.2.'de tanımlı varlıklar;

1. Sağlık ve can güvenliği (kamu/hizmet alıcı ve işletme personeli için),
2. Mal güvenliği (kamu ve işletme için)

3. Ekonomik kayıplar (kamu ve işletme için)

kriterlerini esas alan önem sıralamasına göre listelenmiştir.

Çizelge 7.2. Dolaylı varlıkların türü, önem sıralaması ve etiketlendirilmesi

	Dolaylı Varlıklar		
	Varlık Etiketi	Varlık Türü	Açıklama ve Örnekler
1	ASSET.PUBLIC_SAFETY	Kamunun Güvenliği	Hizmetten doğrudan veya dolaylı olarak faydalanan vatandaşların sağlığı ve can güvenliği
2	ASSET.PERSONEL_SAFETY	Personelin Güvenliği	İşletme çalışanlarının sağlığı ve can güvenliği
3	ASSET.PUPLIC_GOODS	Kamuya Ait Mallar	Hizmetten faydalanan veya faydalanmayan vatandaşların malları ve genel kamu malları
4	ASSET.BUSINESS_GOODS	İşletmenin Malları	İşletmenin "Otomasyon Süreçlerine Ait Varlıkları" da dahil olmak üzere olmak üzere her türlü mal
5	ASSET. SERVICE_CONTINUITY	İşletmenin Hizmet Devamlılığı	İşletmenin sunduğu hizmetin sürekliliği
6	ASSET.BUSINESS_REPUTATION	İşletmenin İtibarı	İşletmenin genel anlamda kamuoyu önündeki itibarı ve müşterilerinin hizmete duyduğu güven, müşteri bağlılığı

Hem doğrudan varlıkların hem de dolaylı varlıkların kendi aralarında ilişki içerisinde olmaları olağan bir durumdur. Örneğin, iletişim birimlerindeki (ASSET.COMMUNICATION) problem, denetim süreçleri (ASSET.CTRLPROCESS) ve bilgilerini (ASSET.CTRLINFO) doğrudan etkileyecektir.

7.1.2. Açıklık sınıflandırması

Güvenlik açıklıklarını tanımlarken, kelime dizileri ve cümleler kullanmak yerine kodlanabilir bir etiket kullanmak, sınıflandırma, karşılaştırma, kümeleme ve hatta matematiksel ifadeler içinde kullanma gibi pratik faydalar getireceği değerlendirilmiştir. Etiketleme için SPP-ICS belgesinde

kullanılannotasyonseçilmiştir [61]. Çizelge 7.3.'te SPP-ICS çalışmasında yer alan açıklık sınıflandırması olduğu haliyle yer almaktadır.

Çizelge 7.3. SPP-ICS çalışması açıklık sınıflandırması [61]

Açıklık Etiketi	**Açıklık**	**Açıklama ve Örnekler**
V.PLAINTEXT	Açık-Metin Protokol Kullanma	Uçlar arası iletişim de kriptolu veri aktarımı yerine verinin gizlenmeden taşınması
V.SERVICES	Gereksiz, Kullanılmayan Servisler	İhtiyaç duyulmayan ve kullanılmayan servislerin açık olarak bulundurulması
V.REMOTE	Uzaktan Erişim	Sistemlere doğrudan veya dolaylı olarak internetten, diğer dahili iş ağlarından erişime imkanı tanınması; sistem yöneticilerinin ve ürün tedarikçiler kullandıkları kontrolsüz çevirmeli modem erişimleri; zayıf yapılandırılmış Sanal Özel Ağlar (VPN); yetersiz kimlik doğrulama ve yetkilendirme teknikleri.
V. ARCHITECTURE	Zayıf Sistem Mimarisi	İş veya operasyonel gereksinimlerin güvenlik tedbirlerinin planlanması ve uygulanmasına etkisi
V.DEVELOPMENT	Zayıf Sistem Geliştirme Uygulamaları	Sistem konfigürasyon yönetimi ve kalite testi gibi süreçlerdeki eksikliği nedeniyle sistem uyarlamaları ve üçüncü parti ürünlerde hata oluşumu
V.NOPOLICIES	Yetersiz Sistem Güvenlik Politika, Plan ve Prosedürü	Yedekleme prosedürü, olaya müdahale planı, şifre ve konfigürasyonyönetimi gibi prosedür, plan ve politikaların eksik olması veya olmaması
V.NOTRAINING	Kullanıcı Eğitimi Yetersizliği	Sistem güvenliği hakkında kullanıcılara yeterli eğitimin verilmemesi ve sistem kullanıcılarında güvenlik farkındalığının zayıflığı
V.3RDPARTY	Üçüncü Parti Yazılım, Donanım, Servis Kullanımı	
V.NORISK	Risk Değerlendirmesi Eksikliği	Risk değerlendirme aktivitelerinin yetersizliği nedeniyle bilinmeyen veya farkında olunmayan güvenlik risklerine tedbir alma imkânının olmaması

Örnek durum incelemelerinde araştırılan ve tespit edilen açıklıkların, Çizelge 7.3.'teki sınıflandırmaya genel olarak uygunluk gösterdiği görülmüştür. Ancak hem tanımlama pratiği hem de kapsamın daha anlaşılır belirlenmesi açısından Çizelge 7.4.'teki gibi, Çizelge 7.3.'ü referans alan yeniden sınıflandırmanın daha uygun olacağı değerlendirilmiş ve çalışmalarda Çizelge 7.4.kullanılmıştır. Örneğin, literatürde sıkça geçen zayıf kimlik doğrulama ve yetkilendirme, erişimin denetiminin ve hesap yönetiminin yetersizliği gibi açıklık tanımları Çizelge 7.3.'teki gösterim şekillerine uygun olarak Çizelge 7.4.'e ayrı birer başlık olarak dahil edilmiştir.

Çizelge 7.4.'te yer alan son dört tanımlama (V.NOTRAINING, V.NOPOLICIES, V.PRODUCT, V.NORISK), ilk onundan farklı olarak doğrudan somut güvenlik

açıklıklarına değil ilk on açıklığa sebebiyet verecek açıklık kaynaklarına karşılık gelmektedir.

Çizelge 7.4. Güvenlik açıklıklarının yeniden sınıflandırılması [61,73]

Açıklık Etiketi	**Açıklık**	**Açıklama ve Örnekler**
V.PLAINTEXT	Açık-Metin Protokol Kullanma	Uçlar arası iletişim de kriptolu veri aktarımı yerine verinin gizlenmeden taşınması
V.UNUSEDSERVICES	Kullanılmayan Servisler	İhtiyaç duyulmayan ve kullanılmayan servislerin açık olarak bulundurulması
V.REMOTE_ACCESS	Uzaktan Erişim	Sistemlere doğrudan veya dolaylı olarak internetten, diğer dâhili iş ağlarından erişime imkânı tanınması; sistem yöneticilerinin ve ürün tedarikçiler kullandıkları kontrolsüz çevirmeli modem erişimleri; zayıf yapılandırılmış Sanal Özel Ağlar (VPN); yetersiz kimlik doğrulama ve yetkilendirme teknikleri.
V.NOAUTHENTICATION	Kimlik Doğrulamama veya zayıf yetkilendirme	Birimler arasında kurulan iletişimde host ve/veya oturum tabanlı yetkilendirme (kimlik doğrulama) metotlarının kullanılmaması
V.NOACCESS_CONTROL	Erişimin Denetlenmemesi	Birimler arasında kurulan iletişimde host, port ve /veya oturum tabanlı erişim denetiminin uygulanmaması (Güvenlik duvarı, erişim listesi vb. kullanmama)
V.ADDRESSRESOLUTION	Adres Çözümlemeleri	Aldatma (spoofing) ve atlatma (bypassing) için kolaylıkla kullanılabilecek DNS, ARP gibi adres çözümleme protokollerinin kullanılması
V.UNPATCHEDCOMPONENTS	Yamalanmamış Bileşenler	Güvenlik açıkları tespit edilen veya güncelliğini yitirmiş yazılımların, iyileştirilmiş üst versiyonlarının kullanılması ve/ veya yamalarının yapılmaması
V.NOACCOUNTMANAGEMENT	Hesap Yönetiminin Yokluğu veya Zayıflığı	Seviyelendirilmiş ve kullanıcı ihtiyaçlarına özgü hesap oluşturmama; Kullanılan sistem bileşenlerinin buna imkân vermemesi, şifre seçimi ve kullanımının kurala bağlanmaması
V.PHYSICAL_ACCESS	Fiziki Erişim	Merkez denetim birimi ile uç/istasyon birimlerindeki BT ve DDS sistemlerine yetkisizce fiziksel erişimin engellenmemesi veya yetkisiz erişimi engelleyen yeterli tedbirlerin alınmayışı
V.INFORMATION_LEAKAGE	Bilgi Sızmaları	Sistemin işleyişi, altyapısını ve altyapı bileşenlerini ve bu sayede güvenlik imkân, kabiliyetler ve zafiyetlerinin neler olduğunu anlamakta kullanılabilecek bilgilerinin internet ortamından veya diğer sosyal mühendislik vasıtalarıyla elde edilmesi
V.NOTRAINING	Kullanıcı Eğitimi Yetersizliği	Sistem güvenliği hakkında kullanıcılara yeterli eğitimin verilmemesi ve sistem kullanıcılarında güvenlik farkındalığının zayıflığı
V.NOPOLICIES	Yetersiz Sistem Güvenlik Politika, Plan ve Prosedürü	Yedekleme prosedürü, olaya müdahale planı, şifre ve konfigürasyon yönetimi gibi prosedür, plan ve politikaların eksik olması veya olmaması
V.PRODUCT	Sistem Ürün Tedarik ve Entegrasyonu Sorunları	Kullanılan her bir sistem bileşeninin gelecekte nasıl tedarik edileceği meselesindeki belirsizlikler; yazılımların bugün ve gelecekte güncellenmesi ve destek ömürleri; bir tedarikçiden alınan bir bileşenin endüstri standardı başka bir ürünle ortak veya yerine çalışırlığı önündeki sorunlar
V.NORISK	Risk Değerlendirmesi Eksikliği	Risk değerlendirme aktivitelerinin yetersizliği nedeniyle bilinmeyen veya farkında olunmayan güvenlik risklerine tedbir alma imkânının olmaması

7.1.3. Tehdit kaynakları

Bir sistem veya altyapıya yönelik siber saldırıların tamamına yakını esasında kazara veya kasıtlı olarak ortaya çıkan insan kaynaklı tehditlerdir. Örneğin kötücül bir

yazılımın üretilmesi ve yayılması, bu tür yazılımların kazara veya kasıtlı olarak bir sisteme yüklenmesi nihayetinde bir insan unsuru gerektiren fiillerdir.

Bu çalışma kapsamında siber tehdit olarak, iş süreçlerinin denetim ve yönetimi için DDS sistemleri kullanan ve kritik işleve sahip olan altyapılara, kişi ya da grupların;

- Sahadaki denetleyiciler de dâhil olmak üzere komut alma-gönderme, veri işleme-saklama, süreç izleme ve yönetme fonksiyonlarına sahip her türlü donanım ve yazılımlara,
- Merkez ve uç birimler arasındaki iletişimi sağlayan yerel ve geniş alan ağlarına ve ağ üzerinden sunulan servislere

yönelik olarak hasar verme, kesinti oluşturma, veri ve bilgileri silme, işlevsiz bırakma, yanlış veya uygun olmayan bir işlevi icra ederek denetim ve izleme süreçlerini sabote etme gibi fiillerin oluşma potansiyelleri kast edilmektedir.

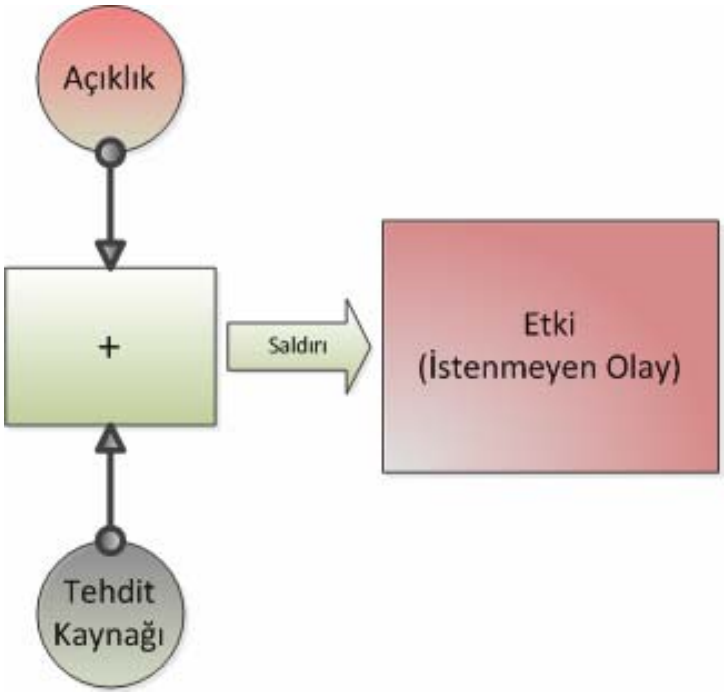
Yukarıda tarif edilen siber tehditleri saldırıya dönüştürecek muhtemel tehdit kaynakları ise aşağıda tanımlanmıştır [74].

I. *Yabancı Devletler:* Tıpkı fiziki saldırı ve savaşlarda olabileceği üzere, bir ülke diğer bir ülkeyi zayıflatmak, önemli ve kritik varlıklarına zarar vermek veya onları imha edebilmek için çeşitli siber saldırı yöntemlerini kullanabilir. Devletler tarafından icra edilecek saldırılar zarar vermek dışında, espiyonaj veya psikolojik propaganda için de yürütülebilir. Siber saldırıların bir devlet veya devletin sponsor olduğu grup veya gruplarca gerçekleştirilmesi durumunda ortaya çıkarabilecek fiziki ve psikolojik etkiler, diğer saldırganların icra edeceklerinden nispeten yüksek olabilecektir. Örneğin, resmi kaynaklarca doğrulanmasa da İran Nükleer programını durdurmak için üretildiği iddia edilen Stuxnet'in İsrail ve ABD tarafından hazırlandığı New York Times [75] gibi ciddi kaynaklarca yazılmıştır.

II. *Terörist Gruplar:* Bugün için terörist gruplar daha çok fiziki saldırıları kullansalar da ilerleyen yıllarda bir yöntem olarak siber saldırıları daha sık kullanabilecekleri öngörülmektedir.
III. *Endüstriyel Siber Casuslar ve Organize Siber Suçlular:* Daha çok çıkar amaçlı yapılar tarafından endüstriyel espiyonaj, şantaj ve para aktarma/çalma gibi amaçlarla gerçekleştirilen saldırılardır. Bu gruplar, bilgisayar korsanlarını çalıştırmak ve kiralamak suretiyle faaliyetlerini devam ettirirler.
IV. *Siber Eylemciler (Hacktivist):* Kritik tesis ve altyapılara zarar vermekten çok, psikolojik etki oluşturmak ve böylece kamuoyunun dikkatini çekmek gibi amaçları bulunmaktadır. Ulusal veya uluslararası örgütlenmeyle çevrecilik, ifade özgürlüğü gibi farklı değer öncelikleri etrafında veya görüntüsünde politik propaganda yapmak için siber saldırıları kullanan gruplardır. Politik propaganda yapan meşhur siber eylemci gruplardan biri olan 'Anonymous' farklı eylemleri [76] nedeniyle son yıllarda sıkça tartışılmıştır.
V. *Bilgisayar Korsanları (Hackers):* Bu tanımlama, kendi içinde amaç ve kabiliyet düzeyine göre aşağıdaki gibi farklı alt başlıklar barındırır.
    a. Çaylaklar (Script Kiddie): Yeni açıklıkları keşfetmek ve bunları istismar edici araçlar yazmak yerine, internet ortamından indirdikleri hazır araçları kullanmak suretiyle saldırılarını gerçekleştirirler.
    b. Solucan ve virüs yazarları: Yazdıkları solucan ve virüslerin internet ağı veya taşınır diskler üzerinden bilgisayarlara yayarlar.
    c. Güvenlik araştırmacıları ve beyaz şapkalı korsanlar: Bunlar güvenlik açıklıklarını bulmak ve güvenlik iyileştirmeleri yapmak suretiyle bu işten para kazanan kişilerdir.
    d. Profesyonel korsanlar- siyah şapkalılar: Bir ağa giriş yapmak veya bir sistemi istismar edici kod yazmak için para alan kişilerdir.

Siber tehdit kaynakları olarak, yukarıdaki tanımlara benzer adlandırma ve sınıflandırma ile farklı kaynaklarda farklı tanımlamalara da rastlamak mümkündür. Genel olarak yukarıda tarif edilen tehditleri, kasıtlı dış tehdit kaynakları (outsider) olarak adlandırmak mümkün olmakla birlikte, örgütlü tehdit kaynaklarının iç destekçilerinin (insider) olma ihtimalini göz önünde bulundurmak gerekir.

Bir tehdidin saldırıya dönüşebilmesi için, tehdit kaynağının yanı sıra tehdidin yöneldiği sistemde bir açıklığın varlığına ihtiyaç vardır. Stoneburner tarafından tanımlanan Birleşik Güvenlik Çerçevesinin, istenmeyen olaya kadar olan bölümü Açıklık-Tehdit Kaynağı-Etki (İstenmeyen Olay) ilişkisini güzel biçimlemesi bakımından aşağıda sunulmuştur [77-78].



Şekil 7.1. Açıklık-tehdit kaynağı ve etki ilişkisi [77-78]

Kasıtlı olarak gerçekleştirilecek bir saldırı için tehdit kaynağının bir motivasyonunun ve tehdidi gerçekleştirecek kabiliyetinin olması gerekir [25]. Başka bir ifadeyle, bir tehdidin saldırıya dönüşmesi için tehdit kaynağını teşvik edici bir niyetin ve kaynağın yetkinliğin bulunması gerekir.

Tehdit kaynaklarının motivasyonlarını üç ana başlık altında sınıflandırmak mümkündür. Bunlar;

- Politik motivasyon,
- Ticari motivasyon,
- Kişisel motivasyon.

Devletlerarası gerçekleşen bir siber savaş veya terörist bir gurubun siber saldırıları politik bir motivasyonun ürünü olan saldırılardır. Bu tür saldırılar, tıpkı fiziki saldırılarda olduğu gibi karşısındakine doğrudan zarar verme veya onu bir imkânından mahrum bırakarak ekonomik veya sosyal açıdan ona zarar verme ve böylece karşısındakini bir şeye zorlamak gibi bir nedenden ötürü yapılabilecektir [11,79].

İşveren-yüklenici arasındaki ciddi bir anlaşmazlıktan, rakip şirketler arasındaki göz karartıcı bir rekabetten veya endüstriyel espiyonaj gibi nedenlerden kaynaklı siber saldırılar ticari bir motivasyonun ürünü olacaktır. Kişisel hırs, merak, kendini ispat, işten kovulduğu için intikam alma gibi nedenlerle yapılan saldırılarsa kişisel motivasyonlara dayanmaktadır.

Yukarıda yapılan 'tehdit kaynakları için motivasyon tanımlamaları' bağlamında, hangi motivasyona sahip grupların hangi seviyede tehdidi icra kabiliyetine sahip olduğunu kestirmek zor olmayacaktır. Çizelge 7.5.'te farklı motivasyona sahip bilinmeyen tehdit kaynakları için beklenen kabiliyet seviyeleri tanımlanmıştır. Ancak bilinen tehdit kaynakları için, mevcut durumuna (kaynağın siber teknoloji ve araçlara yatkınlığı ve yetkinliği gibi) özgü teknik kabiliyet değeri belirlenmesi daha gerçekçi bir yaklaşım olacaktır.

Çizelge 7.5. Bilinmeyen tehdit kaynakları için motivasyona göre teknik kabiliyet beklentisi

Motivasyon Türü	**Beklenen Teknik Kabiliyet**
Politik	Yüksek
Ekonomik	Orta
Kişisel (Şirket İçinden)	Yüksek
Kişisel (Şirket Dışından)	Düşük

Yukarıdaki tehdit kaynaklarına ilişkin tanımlamalardan yararlanarak tehdit kaynakları için Sandia 'Jenerik Tehdit Profilleri' raporundakine [79] benzer biçimde Çizelge 7.6.'da olduğu gibi profiller oluşturmak mümkün olabilecektir.

Çizelge 7.6. Tehdit kaynakları profilleri

Profil	**Tehdit Türü**	**Niyet**	**Yapı**	**Motivasyon**
Profil-1	Dış Tehdit	Kasıtlı	Organize	Politik
Profil-2	Dış Tehdit	Kasıtlı	Organize	Ekonomik
Profil-3	Dış Tehdit	Kasıtlı	Kişisel	Kişisel
Profil-4	İç Tehdit	Kasıtsız	Kişisel	-
Profil-5	İç Tehdit	Kasıtlı	Kişisel	Kişisel
Profil-6	İç Tehdit	Kasıtlı	Organize	Ekonomik

Bir tehdidin gerçekleştirilerek başarılı bir saldırıya dönüşmesi, tehdit kaynağının saldırı için sahip olduğu veya ayırdığı ekonomik kaynağa, amacının kuvvetine, siber alandaki bilgi ve yeteneğe, organizasyonun büyüklüğüne, gizliliğe ve zamanlamaya bağlıdır [38,79]. Bu unsurlardan saldırıyı gerçekleştirme amaç ve isteğinin kuvveti *Motivasyon* başlığı altında, diğer imkân, durum ve uzmanlıklar ise *Kabiliyet* başlığı altında toplanabilir [25].

Bir tehdit kaynağının gücü, motivasyonun derecesi 'M' ve teknik kabiliyetiyle 'C' ile ifade edilirse ve öngörülebilinen dört farklı tehdit kaynağı için;

M_1= Politik motivasyon

C_1= Politik motivasyonlu saldırgan için teknik kabiliyet

M_2= Ekonomik motivasyon

C_2= Ekonomik motivasyonlu saldırgan için teknik kabiliyet

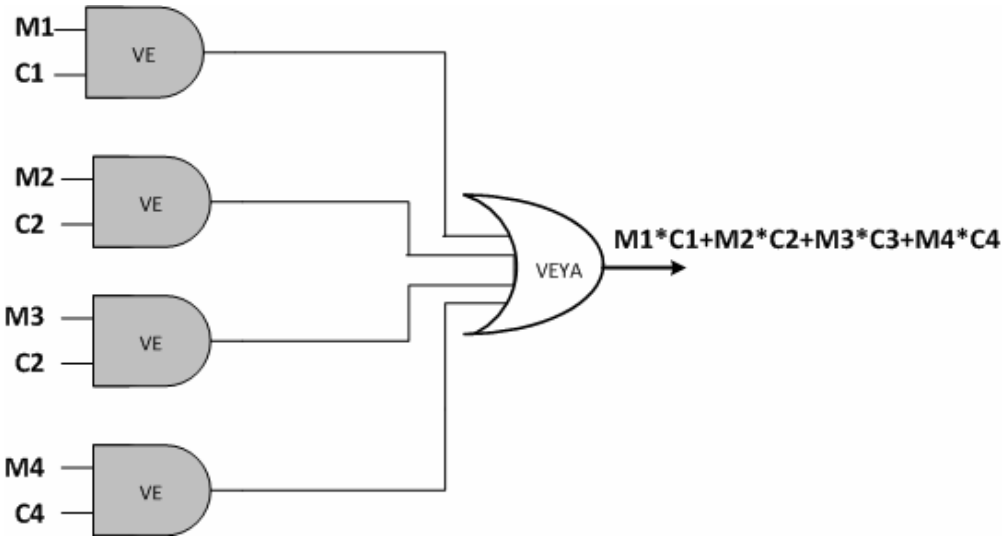
M_3= Kişisel motivasyon-şirket içi

C_3= Kişisel motivasyonlu saldırgan için teknik kabiliyet

M_4= Kişisel motivasyon-şirket dışı

C_4= Kişisel motivasyonlu-şirket dışı saldırgan için teknik kabiliyet

olarak tanımlanırsa, tüm tehdit kaynaklarının gücü Şekil 7.2'deki gibi gösterilebilir.



Şekil 7.2. Dört farklı tehdit kaynağı için toplam tehdit gücü

Aynı örneğe devam edildiğinde, yukarıdaki tehdit kaynağı tanımlarından da yararlanarak bu dört tehdit kaynağının beklenen motivasyon ve kabiliyet değerleri için Çizelge 7.7.'de olduğu gibi 0-1 aralığında değerler atanırsa, yine Çizelge 7.7.'de yer alan 'Tehdit Gücü' değerleri hesaplanabilir.

Çizelge 7.7. Dört farklı tehdit kaynağı için toplam tehdit gücü belirleme

Motivasyon Türü	**Motivasyon Değeri**	**Beklenen Teknik Kabiliyet**	**Beklenen Kabiliyet Değeri**	**Tehdit Gücü**
Politik	0.5	Yüksek	0.7	0.35/0.35=1 , Yüksek
Ekonomik	0.3	Orta	0.4	0.12/0.35=0.34 , Orta
Kişisel (İşletme İçinden)	0.2	Yüksek	0.8	0.16/0.35=0.46 ,Orta
Kişisel (İşletme Dışından)	0.1	Düşük	0.2	0.02/0.35=0.06 , Düşük

M ve C için beklenen değerleri atamak mümkün olmakla birlikte, durum, koşul ve taraflara göre her iki değerinde değişeceğini hatırda tutmak gerekecektir. Örneğin M_1 değeri, politik gerginliğin olduğu zamanlarda; M_2 acımasız rekabet ortamlarında ve son olarak M_3 değeri işten çıkarmaların yoğun olduğu zamanlarda yüksek olacaktır. Diğer yandan işten çıkarılan bir BT/SCADA sistem yöneticisi veya yardımcısı için

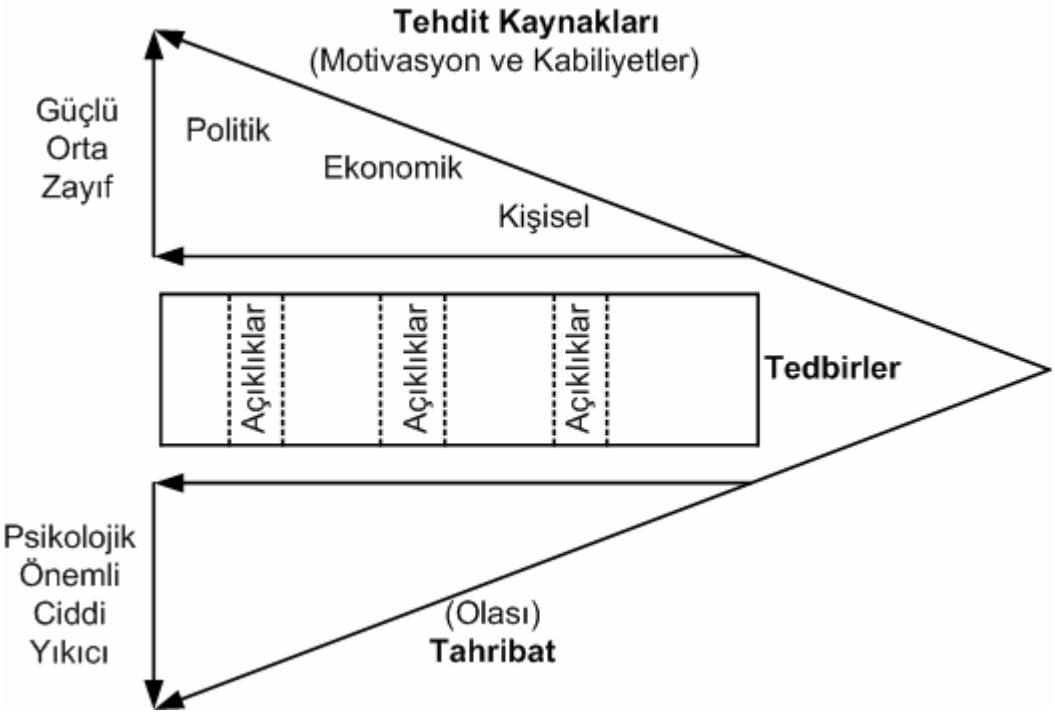
C_3 çok yüksek olacaktır. Dolayısıyla bulunulan duruma ve şartlara bağlı olarak tehdit gücünün yeniden hesaplanması gerekecektir.

Eğer tehdit kaynakları bilme imkânı varsa (Örneğin, kritik bir işletmeye yönelik 2 farklı politik, 3 farklı ekonomik bilinen tehdit kaynağı gibi), yukarıdaki tehdit gücü hesaplaması için "Eş.7.1." gibi genelleştirilebilir.

Tehdit Kaynağının Gücü (7.1.)

Kasıtsız olarak ortaya çıkan istenmeyen sonuç ve etkiler için siber saldırı yerine 'siber kaza' demek daha uygun olacaktır. Siber kazalara yol açan en önemli etmenler arasında çalışanların uzmanlık eksikliği, yetkilendirme alanlarının genişliği ve çalışanların iş yükü sayılabilir.

Genel beklenti ve kabul olarak, tehdit kaynakların kabiliyet ve motivasyonları dikkate alındığında hedef alacakları sistemler üzerinde bırakacakları tahribatın büyüklüğünün sırasıyla politik, ekonomik ve kişisel olarak sıralanması mümkündür. Yukarıdaki tehdit kaynakları tanımlarından da yararlanarak, Şekil 7.3.'te gösterildiği üzere, politik tehditlerin alınan olası tedbirleri aşarak açıklıklardan yararlanma ve hedef aldıkları sistem üzerinde tahribat bırakmak olasılıkları her zaman büyük olacağını öngörülebilir.



Şekil 7.3. Tehdit, Tedbir, Tahribat (T^3) üçgeni yaklaşımı

7.1.4. Siber saldırıların tanımlanması ve sınıflandırılması

Siber saldırılar, temel olarak aktif ve pasif saldırılar olarak iki ana başlık altında toplanabilirler. Pasif saldırılar, sistemlerinin çalışmasına zarar vermeyen ancak sistemeait veri veya bilgilerin kopyasının çalınmasına imkân veren saldırılardır. İletişimi kesmemesi ve açıktan bir zarar vermemesi nedeniyle pasif saldırıları tespit etmek çoğu durumda güçtür. Aktif saldırılar ise, bir veri veya komutu değiştirmek suretiyle sistemi bozmaya, işlevini doğru olarak icra edemez hale getirmeye yönelik saldırılardır. Aktif saldırılar ayrıca, iç ve dış saldırılar olarak da ikiye ayrılırlar. Genelde dış saldırılar belirli ve dar alanda zarar verirken, iç saldırılar daha yıkıcı olabilmektedir. Genel güvenlik yaklaşımları, dış kaynaklı saldırılara karşı tedbir almak yönündedir. Ancak bir dış saldırı neticesinde başka sistem bileşenlerine erişebilen bir iç bileşenin ele geçirilmesi, dış kaynaklı başlayan saldırının iç kaynaklı olarak devam etmesine ve böylece tahribatını arttırmasına neden olabilecektir [80].

Başarılı olmuş bir aktif saldırının sistem üzerinde doğrudan veya dolaylı olumsuz etkilerinin (istenmeyen olayların) olması kaçınılmazdır. Örneğin Çizelge 7.8.'de

kritik bir sisteme yönelik üç başarılı aktif saldırının ardından doğrudan veya dolaylı oluşabilecek olumsuz etkileri tanımlanmıştır.

Çizelge 7.8. Tanımlanan üç aktif saldırı için doğrudan ve dolaylı etkiler

Aktif Saldırılar	**Etkiler**	
	Etki-1: Kesinti, Patlama	Etki-2: Sistem Bileşenlerine Erişememe, Kararsız ve Yönetilemez Hale Gelme
Ağda Uygunsuz Komut Çalıştırma (Yeniden Oynatma, Yerine Geçme)	*Doğrudan*	*Doğrudan*
Ağ ve Ağ Servislerini Kesme	*Dolaylı*	*Doğrudan*
Veri ve Bilgileri Silme	*Dolaylı*	*Dolaylı*

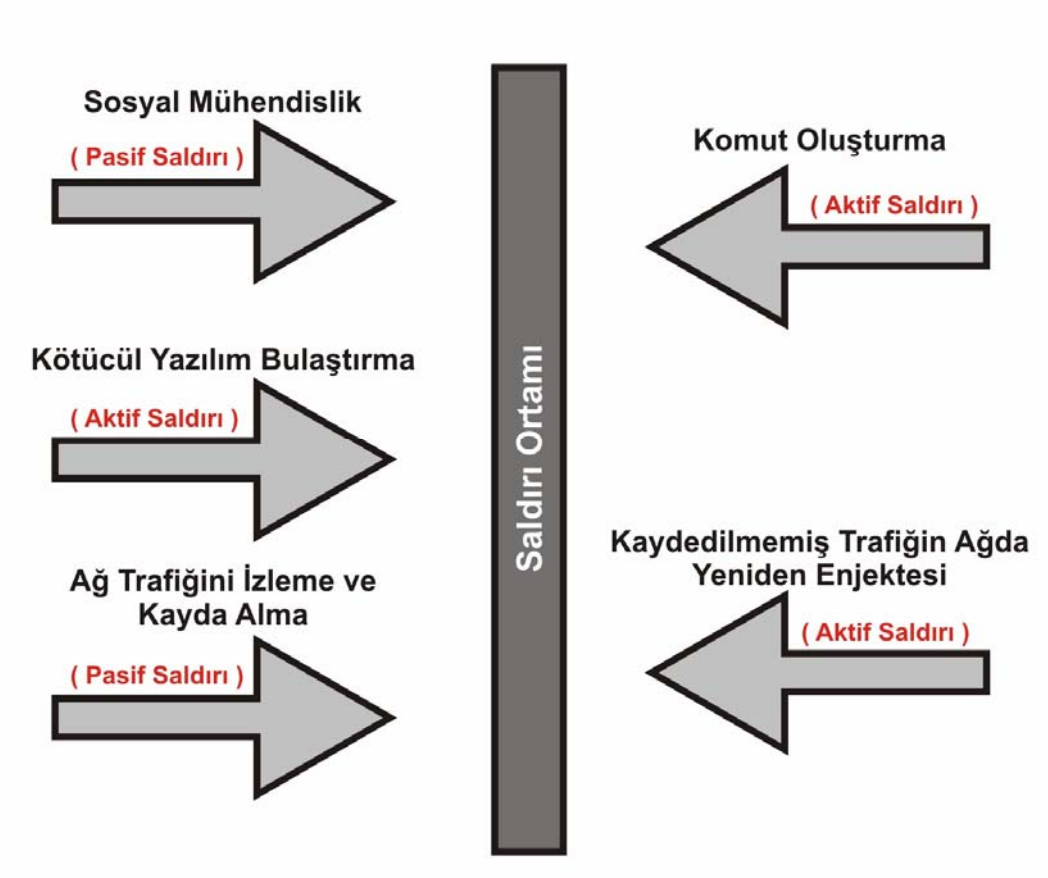
Pasif saldırılar, sisteme sızma, veri ve bilgi toplama, kayıt alma türünden saldırılardır [80]. Bu bağlamda, daha çok aktif saldırın yapılmasına kolaylık ve hazırlık sağlayan saldırılardır diye nitelendirilebilir.

Siber saldırı türleri için önerilebilecek diğer bir sınıflandırma ise aşağıda verilmiştir.

- Hazırlayıcı Saldırılar
- Tamamlayıcı Saldırılar

Bu tanımlamaların aktif ve pasif saldırılarla ilişkisi aşağıda olduğu gibi kurulabilir.

Pasif saldırılar hazırlayıcı saldırılar olmakla birlikte, hazırlayıcı tüm saldırılar pasif değildir. Örneğin bir kötücül yazılımını sisteme bulaştırma aktif bir saldırıdır. Ancak bir sisteme kötücül bir yazılımın sadece bulaştırılmış olması doğrudan saldırının misyonu olmadığından 'hazırlayıcı' saldırı' olarak kalmıştır. Diğer yandan, bulaştırma eylemi sonrasında, uygun zaman ve koşullarda kötücül yazılımın aktive edilerek sisteme zarar verecek bir işlevi gerçekleştirmesi 'tamamlayıcı' bir saldırıdır. Bu bağlamda, Şekil 7.4.'te örnek birkaç saldırı gösterilmiştir.



Şekil 7.4. Hazırlayıcı ve tamamlayıcı saldırılar

Literatürde, SCADA/DDS sistemlerine yönelik siber saldırı tanımlama ve sınıflandırmalarının, ortak öğe ve tanımlamalar barındırmakla birlikte farklılıklar da içerdiği gözlenmektedir. Örneğin, Avrupa Komisyonu Birleşik Araştırma Merkezi (European Commission Joint Research Centre), Vatandaşların Güvenliği ve Korunması Enstitüsü'nce (IPSC), SCADA sistemlerine yönelik olarak yapılabilecek saldırılar şu başlıklarda sınıflandırılmıştır [81]:

- Yeniden oynatma saldırıları (Replay attack)
- Araya girme saldırısı (Man-in-the-middle attacks)
- SCADA servis durdurma saldırıları (Denial of service attacks)
- Kötücül servis komutları saldırıları (Malicious service commands attacks)

SPP-ICS [61] dokümanındayukarıdaki tanımlarından farklı olarak tanımlanan siber saldırılar;

- Ağ trafiğini izleme ve kayda alma,
- Başkası gibi davranma ve yerine geçme,
- Operatör hatası,
- Sosyal mühendislik,
- Virüs bulaştırma,
- İş, denetim ve konfigürasyon bilgilerini silme,
- İş, denetim ve konfigürasyon bilgilerini değiştirme,
- Güvenlik Fonksiyon ve mekanizmalarını atlatma

olarak yer almaktadır.

Patel ve ark. [82] ise, SCADA/DDS sisteminin güvenliğine doğrudan etki edecek olan ve sistem haberleşmesine yönelik olan saldırıları;

- Yeniden oynatma saldırıları
- Başkası gibi davranma ve yerine geçme,
- Servis durdurma saldırıları,
- Master Terminal Birime (MTU) yazma,
- Uzak Terminal Birim (RTU) cevabını değiştirme,
- Uzak Terminal Birime (RTU) yazma

olarak tanımlamışlardır.

Patel ve ark. [82] çalışmasındaki benzer ancak biraz daha ayrıntılı bir sınıflandırmanın Byres ve ark. [83] çalışmalarında görülmektedir. Her ne kadar Modbus protokolünü esas alan bir çalışma olsa da, diğer SCADA/DDS iletişim protokollerini kullanan sistemler için de benzer bir tasnif kullanılabilecektir. Byres ve ark. [83], aşağıdaki 15 farklı saldırıyı saldırgan hedefi olarak tanımlamış, bunlardan ilk 11'ini doğrudan Modbus kullanan sistemler için, diğerleri ise tüm BT sistemlerini kapsayacak şekilde tanımlamışlardır.

(Modbus kullanan SCADA/DDS için)

1. SCADA sistemine erişim
2. MODBUS cihazları saptama
3. Master-Bağımlı (master-slave) iletişimini bozma
4. Bağımlı birimi etkisiz kılma
5. Bağımlıdan veri okuma
6. Bağımlıya veri yazma
7. Bağımlıyı programlama
8. Bağımlının ihlali
9. Master birimi etkisiz kılma
10. Master birimine veri yazma
11. Yönetenin ihlali

(Diğer BT sistemleri de kapsayan)

12. Ağ servislerini durdurma
13. Araya girerek ağdaki verileri alma ve değiştirme

Literatürdeki farklı kaynaklar incelendiğinde, aslında saldırı hedefi ile saldırının kendisinin birbirinden tam olarak ayrılmadığı ve bu nedenle birbirleriyle karıştığı da görülebilmektedir. Bu anlamda, NIST (SPP-ICS) [61], IPSC [81], Patel ve ark. [82] ile Byres ve ark. [83] saldırı tanım ve sınıflandırmaları yeniden ele alınarak Çizelge 7.9.'daki 'Hedeflenen Saldırı' ve 'Saldırı (Saldırı Biçim ve Aşamaları)' ayrımına gidilmiştir.

Öncelikli olarak SCADA/DDS sistemlere yönelik saldırı hedeflerinin, başka bir ifadeyle saldırı sonucunda varılmak istenen durumun neler olabileceği sıralamak gerekir. Başarılı bir saldırı sonucunda bu tür altyapılarda ortaya çıkabilecek olumsuz durumlar sırasıyla, sistemin kontrol dışı bırakılması veya saldırganlarca sistem yönetiminin ele geçirilmesi, altyapının sunmuş olduğu hizmetlerin kesintiye uğratılması, hassas bilgi ve verilerin çalınması veya imha edilmesi olabilecektir. Şimdi bu tanımlarını ayırt edici biçimde sınıflandırsak, Çizelge 7.9.'da tanımlı dört

hedeflenen saldırı veya saldırı hedefi elde edilecektir. Ayrıca Çizelge 7.9.'da her bir saldırı hedefi için kullanılabilecek aynı veya farklı saldırı biçim veya aşamaları ile eşleştirme yoluna gidilmiştir.

Çizelge 7.9. SCADA/DDS yönelik hedeflenebilecek siber saldırı ve kullanılabilecek saldırı biçimlerinin sınıflandırma ve ilişkilendirmesi

Hedeflenen Saldırı	**Saldırı (Saldırı Biçim ve Aşamaları)**
1- Ağda uygunsuz komut çalıştırma	Sosyal mühendislik- Hazırlayıcı Kötücül yazılım bulaştırma - Hazırlayıcı (İletişim Ağına) Yetkisiz erişim - Hazırlayıcı Ağı dinleme ve kayda alma - Hazırlayıcı Yerine geçme/ Araya Girme -Tamamlayıcı Yeniden oynatma-Tamamlayıcı (Sistem birim, bileşen veya servislerine) Yetkisiz Erişim- Tamamlayıcı
2- Saklı veri ve bilgileri silme veya değiştirme	Sosyal mühendislik- Hazırlayıcı Kötücül yazılım bulaştırma - Hazırlayıcı (Sistem birim, bileşen veya servislerine) Yetkisiz Erişim- Tamamlayıcı
3- Sistemi işlevsiz bırakma/ Kararsız hale getirme	Sosyal mühendislik- Hazırlayıcı Kötücül yazılım bulaştırma – Hazırlayıcı Yerine geçme- Tamamlayıcı (Sistem birim, bileşen veya servislerine) Yetkisiz Erişim- Tamamlayıcı
4- Ağ veya ağ servislerini kesme	Sosyal mühendislik- Hazırlayıcı (İletişim Ağına) Yetkisiz erişim- Hazırlayıcı Kötücül yazılım bulaştırma – Hazırlayıcı Yerine geçme- Tamamlayıcı Servisi Engelleme –Tamamlayıcı

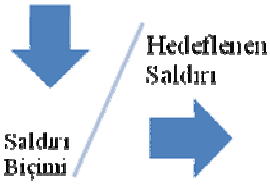
Çizelge 7.9.'da tanımlanan saldırı biçim ve aşamaları, SPP-ICS [61] gösterimiyle etiketlendiğinde Çizelge 7.10. elde edilmiştir.

Çizelge 7.10. Saldırı biçim ve aşamalarının etiketlenmesi

Saldırı Etiketi	**Saldırı Biçimi**
ATTACK.UNAUTHORIZEDACCESS	Yetkisiz Erişim
ATTACK.SNIFF	Ağı Dinleme
ATTACK.REPLAY	Yeniden Oynatma
ATTACK.SPOOF	Yerine Geçme/ Araya Girme
ATTACK.DOS	Servis Engelleme
ATTACK.MALICIOUS	Zararlı Kod Bulaştırma
ATTACK.SOCIAL	Sosyal Mühendislik

Kullanılan ortak veya farklı saldırı biçim ve aşamaları bakımından hedeflenen saldırılar arasında daha rahat karşılaştırma yapılabilmesi için Çizelge 7.9.'dan yararlanarak Çizelge 7.11. türetilmiştir.

Çizelge 7.11. Hedeflenen saldırı- saldırı biçimi matrisi

	Ağda uygunsuz komut çalıştırma	Saklı veri ve bilgileri silme veya değiştirme	Sistemi işlevsiz bırakma/ Kararsız hale getirme	Ağ veya ağ servislerini kesme
ATTACK.UNAUTHORIZED ACCESS	Evet	Evet	Evet	Evet
ATTACK.SNIFF	Evet	Hayır	Hayır	Hayır
ATTACK.REPLAY	Evet	Hayır	Hayır	Hayır
ATTACK.SPOOF	Evet	Hayır	Bazen	Bazen
ATTACK.DOS	Hayır	Hayır	Hayır	Evet
ATTACK.MALICIOUS	Bazen	Evet	Evet	Bazen
ATTACK.SOCIAL	Bazen	Bazen	Bazen	Bazen

7.1.5. Siber saldırıları biçim ve aşamaları

Bir siber saldırının hedefine ulaşılabilmesi için saldırganların hedefe yönelik bir veya birden fazla saldırı biçimini kullanmasına ihtiyaç vardır. Çizelge 7.10.'da tanımlanan 7 farklı siber saldırı biçim ve aşamaları aşağıda sırayla açıklanmıştır.

A. *Yetkisiz Erişim:* İki farklı durum için tanımlamak mümkündür. Birincisi, birbirleriyle haberleşen sistem birim ve bileşenlerinin yer aldığı iletişim ağına yetkisiz erişim veya ağa sızma olarak tanımlanabilir. Bir ağdan veri veya bilgi toplayabilmek, ona trafik enjekte edebilmek, ağdaki bir cihaz veya servisin yerine geçebilmek için saldırganların öncelikle o ağa erişebilmelerine, başka bir ifadeyle ağa sızabilmelerine ihtiyaç vardır. Bu, ağ temelli saldırıların tümü için saldırının ilk aşamasıdır. Yetkisiz erişimin diğer bir türü ki bu çalışmada daha çok bu anlamıyla kullanılmıştır, doğrudan veya bir ağ üzerinden bir sisteme veya bileşenine yetkisi olmadığı hale

bağlanmaktır. Bu erişim, sistemin tüm fonksiyonlarına (root, admin konsol gibi) ulaşmayı ifade edebileceği gibi belirli servis veya fonksiyonlarına (FTP, SNMP gibi) ulaşmakla da sınırlı kalabilir. Sistemlere fiziksel erişimin olmadığı durumlarda, sistem bileşenlerine veya servislerine yetkisiz erişmek isteyen saldırganların öncelikle o sistemin doğrudan veya dolaylı olarak bağlı olduğu ağ veya ağlara sızmaları gerekir.

B. *Ağı Dinleme ve Kayda Alma:*İyi niyetli olarak yapıldığında, ağ iletişimden kaynaklı bir problemi tespit etmek için kullanılır. Ağ dinleyiciler veya başka bir ifadeyle paket koklayıcılar (sniffers), kablolu veya kablosuz bir iletişim ortamı üzerinden bağlandıkları ağda geçen trafiği izler ve kaydederler. Ağ dinleme iki şekilde saldırı haline dönüşebilir. Birincisi, yetkisiz birinin veya saldırganın ağ hakkında bilgi toplamasıdır. İkincisi, dinlenen trafiğin kaydedilmesi suretiyle ağda yeniden oynatılmak üzere hazır edilmesidir. Böylece kayıt edilen trafik, 'yeniden oynatma' saldırısında kullanılabilir.

C. *Yeniden Oynatma:* Daha önceden dinlenerek kayda alınmış ağ trafiğine ait paketlerin başka bir zamanda başka biri tarafından sanki gerçek göndereni tarafından o an göndermiş gibi ağa enjekte edilmesi saldırısıdır. Paketler olduğu gibi gönderilebileceği gibi içeriğinde değişiklik yapılarak da gönderilebilir. Her iki durumda da yapılan saldırının tam etkisi önceden bilinemeyebilir. Yeniden oynatma saldırısı, sekans numarasının takip edilmesi durumunda IPSec tüneli ile kriptolanmış hatlara bile uygulanabilir [84]. Daha önceden gönderilmiş bir komutun sanki o an gönderiliyormuş gibi işleme konulması durumunda, denetlenen sürece bağlı olarak ciddi olumsuzlukların meydana gelmesinin olası olduğu saldırılardan biridir. Örneğin, merkezi birim üzerinden uç birime bir vanayı açması komutunun gönderildiği varsayılırsa, bu komutunun kablolu veya kablosuz bir iletim ortamı üzerinden gönderilmesi esnasında üçüncü bir taraf bu iletişimin kopyasını kolaylıkla alıp kaydedebilir. Böylece, kaydedilen paketlerin aynı kablolu veya kablosuz iletim ortamına yeniden enjekte edilmesi durumunda, istenmediği halde vanayı açma işlemi saldırgan tarafından gerçekleştirilebilir. Yeniden oynatma saldırısı, haberleşen iki taraf arasındaki iletişim

protokolünün paket sayısı ve sırasını tutma ve izleme gibi özellikleri mevcut ise gerçekleştirilemez [85].

D. *Yerine Geçme/Araya Girme:* Saldırgan, ağ ortamına sızdıktan sonra, sanki o ağdaki haberleşen taraflardan biriymiş gibi davranır. Örneğin, ağda var olan bir bilgisayarın IP veya MAC adresiyle kendini anons ederek karşı bilgisayardan gelecek cevabı bekler. Şayet iletişim kuran iki tarafın arasına üçüncü bir taraf girerek, kendisini sanki diğer tarafmış gibi gösterir ve iletişim trafiğini üzerine alırsa, bu 'araya girme' saldırısı olarak adlandırılır. Bir defa araya girildikten veya başka bir ağ varlığının yerine geçildikten sonra, karşı tarafın bilgilerini alma veya ona yanıltıcı bilgi, komut gönderme mümkün olabilecektir. Bazı kaynaklarda [86], yeniden oynatma saldırıları da yerine geçme (spoofing) saldırılarına dâhil edilmektedir.

E. *Servisi Engelleme:*Bu saldırı türü doğrudan hizmeti kesmeye veya engellemeye yöneliktir. Özellikle, TCP/IP haberleşmesi için kolaylıkla uygulanabilmektedir. Kablosuz ağlara yönelik olarak da doğrudan sinyal bozucu ve karıştırıcılar (jammer) kullanılarak, ağ erişiminin ve ağ üzerinden verilen servislerin kesilmesi sağlanmaktadır. Literatürde [87], servis durdurma (DOS: Denial of Service) denilince daha çok TCP/ IP tabanlı iletişime yönelik PING seli, SYN seli gibi ağ kaynaklarını tüketmeye veya ağ servislerini cevap veremez hale getirmeye yönelik saldırılara işaret edilmektedir.

F. *Zararlı Kod Çalıştırma:* Ağ ve bilgisayarlara bir şekilde sızdıktan sonra, bulaştığı sistem birimlerini tamamen veya kısmen çalışmaz ya da kararsız çalışır hale getiren kötücül yazılımların kullanıldığı saldırılardır. Zararlı kod ve yazılımların bulaşması, doğrudan internet üzerinden yayılabileceği gibi, kapalı ağ ve sistemlere taşınır diskler üzerinden de geçebilmektedir. Virüs, truva atı, solucan gibi yazılımlar kullanılarak belirli veya rastgele sistemlere verilen zararlar, 'Zararlı Kod Saldırıları' sınıfına dâhil edilebilir. SCADA/DDS sistemlere yönelik kayda geçmiş en önemli zararlı kod saldırısı, 2010 Haziran'ında ilk kez VirusBlokAda tarafından varlığı tespit edilen ve güvenlik uzmanları tarafından siber savaş dönemini başlatan olay olarak ilan edilen Stuxnet kurtçuğudur [88].

G. *Sosyal Mühendislik:* Teknik olmayan yöntemlerle şifre, topoloji, kullanılan ürün adı modeli gibi önemli bilgilere ulaşarak, teknik saldırıların yapılabilmesine imkân ve kolaylık sağlayan bir yöntem ve aşamadır. Bilgi güvenliği bağlamında sosyal mühendislik, insanlar arasındaki iletişimdeki ve insan davranışındaki modelleri açıklıklarolarak tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahaleler olarak tanımlanır [89]. Çoğunlukla hassas bilgilere erişim veya yetkisiz erişim için güvenlik zincirinin en zayıf halkası olarak tarif edilen insan faktörünü kullanır. Sosyal mühendislik denildiğinde akla ilk olarak telefonda başka biriymiş gibi davranılarak önemli bilgilerin elde edilmesi gelmektedir.Ancak günümüzde internet, kurum, kuruluşlar hatta kişiler hakkında bilgi toplamak için oldukça yaygın olarak kullanılan ve çoğu durumda ulaşılmak istenen bilgiyi sağlamasa dahi, o bilgiye giden yolu gösteren bir ortamdır [90]. Örneğin hakkında bilgi toplanan kurumun web sayfasını ziyaret etmek, arama motorlarında ilgili kelimelerle birlikte sorgulamak, sosyal medya ortamında çalışanların profilini ziyaret etmek beklenenin çok üstünde bilgi sunabilmektedir.

7.2. Saldırı-Açıklık Eşleştirmesi

Girişiminde başarılı olmak isteyen her saldırgan, hedef aldığı sistemin açıklıklarını kullanarak saldırısını gerçekleştirir. Bu bağlamda, bir altyapıya yönelik güvenlik riskleri sorgulanırken sorulması gereken birinci soru aşağıdaki gibi olmalıdır.

Birinci Soru:

Uygulanabilecek her bir saldırı biçimi için yararlanabilecek açıklıklar neler olabilir?

(Saldırı Biçimi- Açıklıklar Eşleştirmesi)

NIST SPP-ICS [61] belgesindeki Saldırı-Açıklık eşleştirmesinin bir benzeri, Çizelge 7.10.'da tanımlı saldırı biçimleri ve Çizelge 7.4.'te tanımlı güvenlik açıklıkları kullanılarak eşleştirildiğinde Çizelge 7.12. elde edilmiştir.

Çizelge 7.4.'te tanımlı güvenlik açıklıklarından, V.NOPOLICIES, V.NOTRAINING, V.PRODUCT ve V.NORISK aslında tüm saldırı biçimlerine karşılık gelen açıklıklar arasındadır. Zira bu beş açıklığının temsil ettiği eksiklik giderilmeden, siber saldırılara karşı etkili bir modelden bahsetmek mümkün olmayacaktır.

Çizelge 7.12. Saldırı biçimi-açıklıklar eşleştirmesi

Saldırı Etiketi (Saldırı Biçimleri)	**Açıklıklar**
ATTACK.UNAUTHORIZEDACCESS	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION
ATTACK.SNIFF	V.PLAINTEXT V.NOACCESS_CONTROL V.PHYSICAL_PROTECTION
ATTACK.REPLAY	V.PLAINTEXT V.NOACCESS_CONTROL V.NOAUTHENTICATION V.PHYSICAL_PROTECTION
ATTACK.SPOOF	V.NOACCESS_CONTROL V.NOAUTHENTICATION V.PHYSICAL_PROTECTION V.ADDRESSRESOLUTION
ATTACK.DOS	V.NOACCESS_CONTROL V.REMOTE_ACCESS
ATTACK.MALICIOUS	V.UNUSEDSERVICES V.UNPATCHEDCOMPONENTS V.NOACCOUNTMANAGEMENT
ATTACK.SOCIAL	V.INFORMATION_LEAKAGE V.NOTRAINING

Hedeflenen Saldırı-Saldırı Biçimi Matrisi (Çizelge 7.11.) göz önünde bulundurulduğunda, Saldırı Hedefleri-Açıklıklar Eşleştirmesi Çizelge 7.13.'deki gibi türetilebilecektir.

Çizelge 7.13. Hedeflenen saldırı-açıklıklar eşleştirmesi

Hedeflenen Saldırı	**Açıklıklar**
1- Ağda uygunsuz komut çalıştırma	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PLAINTEXT V.ADDRESSRESOLUTION V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING
2- Saklı veri ve bilgileri silme veya değiştirme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING
3- Sistemi işlevsiz bırakma/ Kararsız hale getirme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.ADDRESSRESOLUTION V.INFORMATION_LEAKAGE V.NOTRAINING
4- Ağ veya ağ servislerini kesme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.ADDRESSRESOLUTION V.INFORMATION_LEAKAGE

7.3. Saldırı-Etki Eşleştirmesi

İster siber isterse fiziki olsun her saldırı hedefi üzerinde bir etki bırakmaya yönelik olarak düzenlenir. Bu etki saldırganın amacına yönelik olarak psikolojik olabileceği gibi zarar verici hatta yıkıcı da olabilir.

Güvenlik risklerine daha gerçekçi yaklaşabilmek için cevabı aranması gereken ikinci soru aşağıdaki gibi olmalıdır.
İkinci Soru:

Hedeflenebilecek her bir saldırıların muhtemel etkileri neler olabilir?
(Hedeflenen Saldırı- Etki Eşleştirmesi)

Hedeflenen Saldırı-Etki Eşleştirmesi, güvenlik incelemesi yapılan her altyapı için farklılıklar gösterecektir. Örneğin, aynı saldırı biçim ve aşamaları kullanılsa da elektrik dağıtım şebekesi denetim sistemlerine yönelik siber saldırının etkisi ile su dağıtım şebekesine yönelik saldırının ortaya çıkaracağı olumsuz etkiler birbirinden farklı olacaktır. Dolayısıyla yakınlıklar gösterse de, 'Saldırı - Etki' eşleştirmesi altyapı ve hizmet türü (elektrik, gaz, su, üretim tesisi gibi) ile ölçeğine (kampus, bölge, ülke geneli altyapı) göre önemli farklılıklar gösterecektir.

Hedeflenen Saldırı - Etki Eşleştirmesi yapılmadan önce, kullanılacak etki (impact) kavramının iki farklı şekilde tanımlaması ihtiyacı ortaya çıkmıştır. Bunlar:

- Operasyonel Etki (OI:Operational Impact): Siber bir saldırı sonrasında kurban seçilen altyapıda ortaya çıkan ve doğrudan iş süreçlerini etkileyen olay ve durumlar.
- Gerçek Etki veya İstenmeyen Olay (UI:Unwanted Incident): Bir saldırı sonrası ortaya çıkan operasyonel etki sonrasında ortaya çıkan kesinti, veri kaybı, yangın, su baskını, patlama gibi olumsuzluklar.

Çizelge 7.9.'da tanımlı dört farklı siber saldırı hedefinin her biri için, gerçekleşmeleri durumunda saldırıya maruz kalacak altyapı işletmecileri üzerindeki operasyonel etkileri (OI) Çizelge 7.14.'te eşleştirilmiştir.

Çizelge 7.14. Hedeflenen saldırı- operasyonel etkiler

Hedeflenen Saldırı	**Altyapı İşletmecisi Üzerindeki Operasyonel Etkisi**	
Ağda uygunsuz komut çalıştırma	OI-1	Süreç durum verilerini değiştirme
	OI-2	Süreç denetimini durdurma
	OI-3	Kritik iş süreçlerine ait denetim komutlarının değiştirilmesi
Saklı veri ve bilgileri silme veya değiştirme	OI-4	Denetim sisteminin veri ve bilgilerini silme
	OI-5	Denetim sisteminin veri ve bilgilerini değiştirme
	OI-6	Yazılım ve servis konfigürasyon bilgilerini silme veya değiştirme
	OI-7	Ticari bilgileri çalma, silme, değiştirme
Sistemi işlevsiz bırakma/ Kararsız hale getirme	OI-8	Süreç denetimine ilişkin servisleri kapatma
	OI-9	Süreç denetimine ilişkin servislerin çalışma kipini değiştirme
	OI-10	Süreçlere ilişkin alarm, eşik değer bilgilerini değiştirme
	OI-11	Uç birim denetleyici ekipmanlarını kapatma
Ağ veya ağ servislerini kesme	OI-12	Trafik yükleyerek iletişim hat kapasiteleri doldurma (Örneğin ping paketi gönderme gibi)
	OI-13	Ağ servislerine yönelik gerçek olmayan talep oluşturma (Örneğin SYN paketleri gönderme gibi)
	OI-14	İletişimi kesme (sinyal bozma ve karıştırma)

Çizelge 7.14.'te tanımlanan operasyonel etkiler, SCADA/DDS kullanan her türlü altyapı için ortak olabilecek etkilerdir. Bu etkiler doğrudan altyapıdan hizmet alanlara yönelik değil işletmenin kendi iş süreçlerinin doğru icrasının engellenmesine yöneliktir. Diğer yandan, 'Gerçek Etki' veya 'İstenmeyen Olaylar', saldırlar sonucu ortaya çıkan operasyonel etkilere bağlı olan ve devamında ortaya çıkan durum ve olaylardır. Gerçek etki, operasyonel etkilerin aksine elektrik, su, gaz, petrol iletim ve dağıtım hatları gibi farklı altyapılar için farklı şekil ve şiddetlerde ortaya çıkabilir.

Örneğin, su arıtma ve dağıtım tesisleri ele alınırsa, denetim sistemine yapılacak saldırılar neticesinde ortaya çıkabilecek etkiler aşağıdaki gibi tanımlanabilir [91]:

Operasyonel Etki:

a) Alarm bilgilerinin okunamaması veya yanlış okunması (OI-1: Süreç durum verilerini değiştirme, OI10: Süreçlere ilişkin alarm, eşik değer bilgilerini değiştirme)
b) Kritik iş süreçlerine ait denetim komutlarının değiştirilmesi (OI-3)

Gerçek Etki, İstenmeyen Olay:

c) Su arıtma süreçlerinde yanlış ve yanıltıcı veriler nedeniyle kimyasal dozajın uygun ölçüler dışında yapılması,
d) Uç birimlerdeki RTU, PLC gibi denetleyicilere yetkisiz erişerek temiz su dağıtım ve kirli su tahliye sisteminin ele geçirilmesi neticesinde basınç değiştirme (servis kesintisi veya patlaklara yol açabilir), kirli ve temiz suların birbirine karıştırılması.

Yukarıdaki ilk iki etki (a ve b), başarılı siber saldırılar neticesinde her türlü DDS sistemi için mümkün olabilecek operasyonel etkilerdir. Diğer yandan son iki etki (c ve d), sadece su arıtma ve dağıtım altyapı işletmecileri için tanımlanabilir.

Sistemlere yönelik operasyonel etkiler Çizelge 7.14'de yer aldığı üzere somut olarak ifade edilebilirken, devamında ortaya çıkacak gerçek etkilerin tümümün önceden tanımlanabilmesi ve belirlenebilmesi iki nedenden ötürü mümkün olmayacaktır. Birincisi aynı denetim ve izleme sistemini kullansa da farklı altyapı ve hizmet türleri ile farklı şebeke ölçeğine göre gerçek etkiler de farklılaşabilecektir. İkincisi, aynı etkilerin o anki şartlara bağlı olarak farklı etkileri de tetikleyebilmesi ihtimalidir. Örneğin, basınç değişikliği o anki şartlara bağlı olarak altyapıda patlaklara, patlaklar ise su baskınlarına neden olabilir. Nitekim sadece altyapı işletmecileri değil saldırganlar bile hedefledikleri saldırı sonrasındaki tüm etkileri öngöremeyebilirler.

7.4. Açıklık Kritikliği Belirleme Yöntemi Önerisi

Bir organizasyon, sistem veya tesisin güvenlik açıklıklarının tespit etmek kadar, tespit edilen veya olası tüm açıklıklarının kendi içindeki öncelik sıralamasının yapılabilmesi de büyük önem taşır. Çünkü bilinen veya tespit edilen açıklıkların

tümünün biranda giderilmesi altyapıda çok ciddi değişiklikler gerektirecek ve kısa sürede bu çapta bir değişiklik ise ekonomik, yönetsel veya operasyonel nedenlerle çoğu işletmeci için mümkün olmayacaktır. Bu sebepten ötürü, açıklıkların kritiklik düzeylerine göre önceliklendirilmesi ve iyileştirme süreçlerinde açıklık önceliğinin takip edilmesi uygun bir yaklaşım olacağı değerlendirilmektedir.

'Saldırı–Etki' eşleştirmesinde yukarıda tarif edilen farklılaşma ve belirsizliklere karşılık, öngörülebilecek gerçek etkilerin birkaç başlıkta toplanabileceği ve altyapıdaki açıklıklarla aşağıda önerildiği şekilde eşleştirilebileceği değerlendirilmektedir. 'Gerçek Etki (İstenmeyen Olay)- Açıklık' eşleştirmesi, açıklıklar arasında kritiklik sıralaması yapma imkânı sunacaktır.

Aşağıda olası tüm açıklıkların (hiçbir tedbirin alınmadığı duruma göre) başta tanımlanan istenmeyen olaylar ve her bir istenmeyen olay için atanan olumsuzluk derecesine bağlı olarak kritiklik sıralamasını bulmak için takip edilmesi gereken adımlar yer almaktadır.

ADIM 1: İstenmeyen olayların tanımlanması

İncelenen Örnek Durum için, doğrudan ve dolaylı varlıklara yönelik oluşabilecek istenmeyen olayların (UI) tanımlanması ve listelenmesiadımıdır. Takip eden satırlarda her iki örnek durum incelemesi için dörder istenmeyen olay tanımlanmıştır.

Örnek Durum İnceleme I için;
Aşağıda tanımlanan 4 istenmeyen olay örnek olarak ele alınırsa,

UI1: Yanlış Kimyasal Dozaj (Uygun Ölçü Değişikliği),
UI2: Patlama (Ani ve Anormal Basınç Değişikliği),
UI3: Hizmetin Sunulamaması,
UI4: Geçmiş İşlem Kayıtlarının Silinmesi.

Örnek Durum II incelemesi için;
Aşağıda tanımlanan 4 istenmeyen olay örnek olarak ele alınırsa,

UI1:Ani Aşırı Yükleme/ Boşaltma (Uygunsuz anahtarlama),
UI2:Koruma Ayarlarını Değiştirme veya İşlevsiz Bırakma,
UI3:Arıza Yeri Tespit Engellenmesi (Alarm engelleme veya değiştirme, düzeltici komutları engelleme),
UI4: Geçmiş Yük Yönetim Verilerinin Silinmesi.

ADIM 2: İstenmeyen olaylar için olumsuzluk değerini belirlenme

Birinci adımda listelenen istenmeyen olaylara olumsuzluk derecesi atanırken (Çizelge 7.2.'de tanımlı dolaylı varlıkların türünden, önem sıralamasından ve gerekiyorsa Çizelge 7.1.'deki doğrudan varlıklardan yararlanılarak) aşağıdaki kriterler göz önünde bulundurulur:

- Hizmetin sunumuna etkisi
- Operasyonun etkin yapılmasına etkisi
- İşletmenin itibar kaybı
- İşletmenin mal kaybı (Ekonomik etki)
- Hizmet alanın /kullanıcının mal kaybı (Ekonomik etki)
- İşletme çalışanında yaralanma, can kaybı
- Hizmet alanda (kullanıcının) yaralanma, can kaybı.

Örnek Durum I incelemesive Örnek Durum II incelemesi-için I. Adımda tanımlı dörder istenmeyen olayın olumsuzluk derecelerine göre sınıflandırılması Çizelge 7.15.'te gerçekleştirilmiştir. Tanımlı her istenmeyen olay için II. Adım'da Çizelge 7.15.'deki gibi bir 'olumsuzluk derecesi' atanmıştır.

Çizelge 7.15. Örnek Durum I ve Örnek Durum II için istenmeyen olayların olumsuzluk derece ve tanımlamaları

Örnek Durum I İncelemesi		
İstenmeyen Olay / Gerçek Etki	**Atanan Olumsuzluk Derecesi**	**Gerekçesi**
UI1:Yanlış Kimyasal Dozaj (Uygun Ölçü Değişikliği)	HAYATİ:4	Hizmetten doğrudan veya dolaylı olarak faydalanan tüketicilerin sağlığı ve can güvenliği (ASSET.PUBLIC_SAFETY)
UI2: Patlama Ani ve Anormal Basınç Değişikliği	YIKICI:3	Hizmetten faydalanan veya faydalanmayan vatandaşların malları ve genel kamu malları (ASSET.PUPLIC_GOODS)İşletme altyapısındaki teçhizat ve malları (ASSET.BUSINESS_GOODS)
UI3:Hizmet Verememe	CİDDİ:3 ŞİDDETLİ:2	İşletmenin sunduğu hizmetin sürekliliği (ASSET. SERVICE_CONTINUITY)İşletmenin genel anlamda kamuoyu önündeki itibarı ve müşterilerinin hizmete duyduğu güven, müşteri bağlılığı (ASSET.BUSINESS_REPUTATION)
UI4:Geçmiş İşlem Kayıtlarının Silinmesi	KISITLI:1	Denetlenen ve yönetilen süreçlere ilişkin değerlendirilmek üzere toplanan, işlenen ve/veya saklanan süreç bilgileri (ASSET.CTRLINFO)
Örnek Durum II İncelemesi		
İstenmeyen Olay / Gerçek Etki	**Atanan Olumsuzluk Derecesi**	**Gerekçesi**
UI1:Ani Aşırı Yükleme/ Boşaltma (Uygunsuz anahtarlama) UI2:Koruma Ayarlarını Değiştirme veya İşlevsiz Bırakma	HAYATİ:4	Hizmetten doğrudan veya dolaylı olarak faydalanan tüketicilerin sağlığı ve can güvenliği (ASSET.PUBLIC_SAFETY) Hizmetten faydalanan veya faydalanmayan vatandaşların malları ve genel kamu malları (ASSET.PUPLIC_GOODS)İşletme altyapısındaki teçhizat ve malları (ASSET.BUSINESS_GOODS)İşletmenin sunduğu hizmetin sürekliliği (ASSET. ERVICE_CONTINUITY) İşletmenin genel anlamda kamuoyu önündeki itibarı ve müşterilerinin hizmete duyduğu güven, müşteri bağlılığı (ASSET.BUSINESS_REPUTATION)
UI3: Arıza Yeri Tespit Engellenmesi (Alarm engelleme veya değiştirme, düzeltici komutları engelleme) UI4: Geçmiş Yük Yönetim Verilerinin Silinmesi	CİDDİ:2	İşletmenin sunduğu hizmetin sürekliliği (ASSET. SERVICE_CONTINUITY) İşletmenin genel anlamda kamuoyu önündeki itibarı ve müşterilerinin hizmete duyduğu güven, müşteri bağlılığı (ASSET.BUSINESS_REPUTATION) Denetlenmesi ve yönetilmesi gereken asli otomasyon süreçleri (ASSET.CTRLPROCESS) Denetlenen ve yönetilen süreçlere ilişkin değerlendirilmek üzere toplanan, işlenen ve/veya saklanan süreç bilgileri (ASSET.CTRLINFO)

ADIM 3: Hedeflenen saldırı- istenmeyen durum eşleştirmesi

Birinci adımda tanımlanan ve ikinci adımda sınıflandırılan istenmeyen olayların, hedeflenen saldırılarla ilişkilendirilmesi (Çizelge 7.14.'te tanımlı operasyonel etkiler dikkate alınarak) ertesinde Çizelge 7.16.'da Örnek Durum I için, Çizelge 7.17.'de

Örnek Durum II için Hedeflenen Saldırı-İstenmeyen Olay (gerçek etki) eşleştirme yapılmıştır.

Çizelge 7.16. Örnek Durum I için hedeflenen saldırı- istenmeyen olay eşleştirmesi

Hedeflenen Saldırı	İstenmeyen Olay	Olumsuzluk Derecesi	Operasyonel Etki
• Ağda uygunsuz komut çalıştırma	UI1	HAYATİ:4	OI-1, OI-2, OI-3
• Ağda uygunsuz komut çalıştırma • Sistemi işlevsiz bırakma/ Kararsız hale getirme	UI2	YIKICI:3	OI-1, OI-2, OI-3 OI-8, OI-9, OI-10, OI-11
• Ağda uygunsuz komut çalıştırma • Sistemi işlevsiz bırakma/ Kararsız hale getirme	UI3	CİDDİ:3	OI-1, OI-2, OI-3 OI-8, OI-9, OI-10, OI-11
• Saklı veri ve bilgileri silme veya değiştirme	UI4	KISITLI:1	OI-4, OI-5, OI-6

Çizelge 7.17. Örnek Durum II için hedeflenen saldırı- istenmeyen durum eşleştirmesi

Hedeflenen Saldırı	İstenmeyen Olay	Olumsuzluk Derecesi	Operasyonel Etki
• Ağda uygunsuz komut çalıştırma • Sistemi işlevsiz bırakma/ Kararsız hale getirme	UI1 UI2	HAYATİ:4	OI-1, OI-2, OI-3 OI-8, OI-9, OI-10,OI-11
• Saklı veri ve bilgileri silme veya değiştirme • Ağ veya ağ servislerini kesme	UI3 UI4	CİDDİ:3	OI-4, OI-5, OI-6 OI-12, OI-13, OI-14

ADIM 4: İstenmeyen olay-açıklık eşleştirmesi

Üçüncü adımda elde edilen ‘Hedeflenen Saldırı- İstenmeyen Durum’ eşleştirme çizelgeleri, ‘Hedeflenen Saldırı -Açıklıklar’ eşleştirmesi (Çizelge 7.13.) ile birlikte kullanılarak hangi açıklığın hangi istenmeyen olaylara sebebiyet vereceğini karşılaştırma imkânı ortaya çıkacaktır. Bu durumda Örnek Durum I incelemesi için ‘İstenmeyen Olay-Açıklıklar’ eşleştirmesi Çizelge 7.18.’deki gibi olacaktır.

Çizelge 7.18. Örnek Durum I incelemesiiçin istenmeyen olay-açıklıklar eşleştirmesi

İstenmeyen Durum	Olumsuzluk Derecesi	Hedeflenen Saldırı	Açıklıklar
UI1	HAYATİ:4	Ağda uygunsuz komut çalıştırma	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.ADDRESSRESOLUTION V.PLAINTEXT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING
UI2	YIKICI:3	Ağda uygunsuz komut çalıştırma	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.ADDRESSRESOLUTION V.PLAINTEXT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING
		Sistemi işlevsiz bırakma/ Kararsız hale getirme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.ADDRESSRESOLUTION V.INFORMATION_LEAKAGE V.NOTRAINING
UI3	CİDDİ:2	Ağda uygunsuz komut çalıştırma	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.ADDRESSRESOLUTION V.PLAINTEXT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING
		Sistemi işlevsiz bırakma/ Kararsız hale getirme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.ADDRESSRESOLUTION V.INFORMATION_LEAKAGE *V.NOTRAINING*
UI4	KISITLI:1	Saklı veri ve bilgileri silme veya değiştirme	V.UNUSEDSERVICES V.REMOTE_ACCESS V.NOAUTHENTICATION V.NOACCESS_CONTROL V.NOACCOUNTMANAGEMENT V.PHYSICAL_PROTECTION V.UNPATCHEDCOMPONENTS V.INFORMATION_LEAKAGE V.NOTRAINING

Çizelge 7.18.'deki her bir istenmeyen olay için tekrar eden açıklıklar önce kendi aralarında toplandığında ve istenmeyen olayın olumsuzluk derecesiyle çarpıldığında

(HAYATİ için 4,YIKICI için 3, CİDDİ için 2, KISITLI için 1), açıklığın incelenen sistem için kritiklik değerlerine nicel bir karşılık atanabilecektir. Her bir istenmeyen durum için hesaplanan açıklık kritiklik değeri her bir açıklık için kendi aralarında toplandığında ise hangi açıklığın incelenen sistem için daha kritik olduğu görülebilecektir.

ADIM 5: Açıklıkların kritikliğinin belirlenmesi

İlk dört adımda atanan ve elde edilen değer ve eşleştirmeler kullanılarak, her bir Örnek Durum İncelemesine ait açıklık kritikliği belirlenmesini, başka bir ifadeyle tanımlı açıklıkların tanımlı istenmeyen olaylar için kritikliğinin belirlenmesinde aşağıdaki adım takip edilmiştir.

Çizelge 7.13.'te yer alan 'Hedeflenen Saldırı-Açıklıklar' eşleştirmesi için *fv(Saldırı)* fonksiyonu aşağıdaki gibi tanımlanabilir.

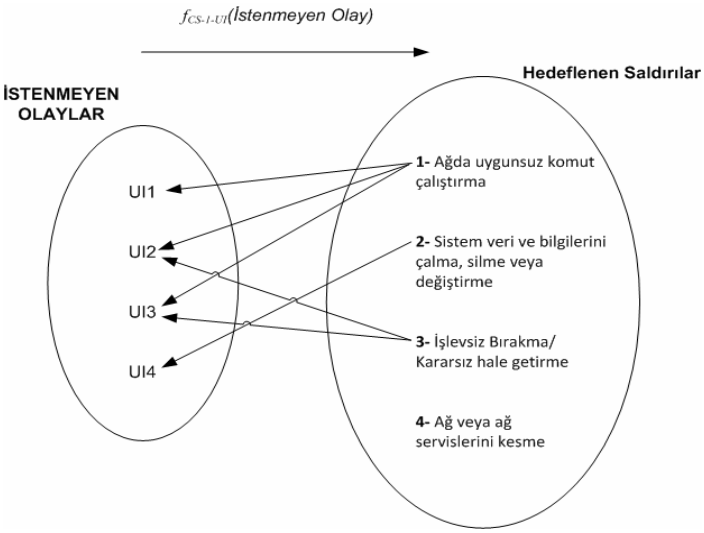
f_V(Saldırı1= Ağda uygunsuz komut çalıştırma) =
{V.*UNUSEDSERVICES*, V.REMOTE_ACCESS, V.NOAUTHENTICATION,
V.NOACCESS_CONTROL, V.NOACCOUNTMANAGEMENT,
V.PLAINTEXT, V.NOACCESS_CONTROL, V.ADDRESSRESOLUTION,
V.PHYSICAL_PROTECTION, (1/2)*V.UNPATCHEDCOMPONENTS,
(1/2)*V.INFORMATION_LEAKAGE,(1/2)*V.NOTRAINING }

f_V (Saldırı2= Saklı veri ve bilgileri silme veya değiştirme)=
{V.UNUSEDSERVICES, V.REMOTE_ACCESS,
V.NOAUTHENTICATION,V.NOACCESS_CONTROL,
V.NOACCOUNTMANAGEMENT, V.PHYSICAL_PROTECTION,
V.UNPATCHEDCOMPONENTS, (1/2)*V.INFORMATION_LEAKAGE,
(1/2)*V.NOTRAINING}

f_I (Saldırı3= Sistemi işlevsiz bırakma-Kararsız hale getirme)=
{V.UNUSEDSERVICES, V.REMOTE_ACCESS,

V.NOAUTHENTICATION,V.NOACCESS_CONTROL,
V.NOACCOUNTMANAGEMENT, V.PHYSICAL_PROTECTION,
V.UNPATCHEDCOMPONENTS, (1/2)*V.ADDRESSRESOLUTION,
(1/2)*V.INFORMATION_LEAKAGE, (1/2)*V.NOTRAINING}

f_V (Saldırı4= Ağ veya ağ servislerini kesme)=
{V.UNUSEDSERVICES, V.REMOTE_ACCESS,
V.NOAUTHENTICATION, V.NOACCESS_CONTROL,
V.NOACCOUNTMANAGEMENT, V.PHYSICAL_PROTECTION,
(1/2)*V.ADDRESSRESOLUTION, (1/2)*V.UNPATCHEDCOMPONENTS,
(1/2)*V.INFORMATION_LEAKAGE }



Şekil 7.5. İstenmeyen olaylar-hedeflenen saldırı küme eşleştirmesi

Örnek Durum I (CS-1: Case Study-1) için, Çizelge 7.16. ve Şekil 7.5.'te yer alan 'İstenmeyen Olaylar-Hedeflenen Saldırı' eşleştirmesi kullanıldığında $f_{CS\text{-}1\text{-}UI}$*(İstenmeyen Olay)* aşağıdaki gibi tanımlanabilir.

$f_{CS\text{-}1\text{-}UI}$(UI1)= {Ağda uygunsuz komut çalıştırma}

$f_{CS\text{-}1\text{-}UI}$ (UI2)= {Ağda uygunsuz komut çalıştırma, Sistemi işlevsiz bırakma-Kararsız hale getirme}

$f_{CS\text{-}1\text{-}UI}$ (UI3)= {Ağda uygunsuz komut çalıştırma, Sistemi işlevsiz bırakma-Kararsız hale getirme}
$f_{CS\text{-}1\text{-}UI}$ (UI4)= {Saklı veri ve bilgileri silme veya değiştirme}

Yukarıda tanımlı f_V(Saldırı) ve $f_{CS\text{-}1\text{-}UI}$(UI) kullanılarak, Örnek Durum I için tanımlı her bir istenmeyen olay açıklık kümesi, takip eden alt satırlarda tanımlı f_{CS1V}(UI) fonksiyonu kullanılarak elde edilebilecektir.

$f_{CS\text{-}1\text{-}V}$(UI)= f_V ($f_{CS\text{-}1\text{-}UI}$(UI))
$f_{CS\text{-}1\text{-}V}$(UI1)= f_V (Ağda uygunsuz komut çalıştırma)
$f_{CS\text{-}1\text{-}V}$(UI2)= f_V(Ağda uygunsuz komut çalıştırma) + f_V(Sistemi işlevsiz bırakma Kararsız hale getirme)
$f_{CS\text{-}1\text{-}V}$(UI3)= f_V(Ağda uygunsuz komut çalıştırma) + f_V(Sistemi işlevsiz bırakma Kararsız hale getirme)
$f_{CS\text{-}1\text{-}V}$(UI4)= f_V{ Saklı veri ve bilgileri silme veya değiştirme}

Örnek Durum I için, Çizelge 7.16. (II. Adım'da) yer alan 'Olumsuzluk Dereceleri', her bir istenmeyen olaya çarpan olarak atanırsa,her bir açıklığının tanımlı dört istenmeyen olay için toplam kritikliği 'Eş.7.2.' ile ifade edilebilir.

$$f_{ToplamKritiklik\text{-}CS\text{-}1} = 4*f_{CS\text{-}1\text{-}v}(UI1) + 3*f_{CS\text{-}1\text{-}v}(UI2) + 2*f_{CS\text{-}1\text{-}v}(UI3) + 1*f_{CS\text{-}1\text{-}v}(UI4) \quad (7.2.)$$

Bu durumdaf $_{ToplamKritiklik\text{-}CS\text{-}1}$ aşağıdaki gibi olacaktır.

$f_{ToplamKritiklik\text{-}CS\text{-}1}$= { 15*V.UNUSEDSERVICES,
15*V.REMOTE_ACCESS,
15*V.NOAUTHENTICATION,
15*NOACCESS_CONTROL,
15*V.NOACCOUNTMANAGEMENT,
15*V.PHYSICAL_PROTECTION,
11.5* V.ADDRESSRESOLUTION
9*V.PLAINTEXT,
6*V.UNPATCHEDCOMPONENTS,
7.5*V.INFORMATION_LEAKAGE,
7.5*V.NOTRAINING }

Çizelge 7.19.'da Örnek Durum I incelemesi için V. adımdaki hesaplamaların tümü gösterilmiştir.

Çizelge 7.19. Örnek Durum I incelemesiiçin V. Adım hesaplama cetveli

İstenmeyen Durum	Olumsuzluk Derecesi	Açıklıklar Toplamı	Açıklığın Kritikliği=(İstenmeyen Durum Olumsuzluk Derecesi)*Açıklıklar Toplamı
UI1	HAYATİ:4	1*V.UNUSEDSERVICES 1*V.REMOTE_ACCESS 1*V.NOAUTHENTICATION 1*V.NOACCESS_CONTROL 1*V.NOACCOUNTMANAGEMENT 1*V.ADDRESSRESOLUTION 1*V.PLAINTEXT 1*V.NOACCESS_CONTROL 1*V.PHYSICAL_PROTECTION ½*V.UNPATCHEDCOMPONENTS ½*V.INFORMATION_LEAKAGE ½*V.NOTRAINING	4*1*V.UNUSEDSERVICES 4*1*V.REMOTE_ACCESS 4*1*V.NOAUTHENTICATION 4*1*V.NOACCESS_CONTROL 4*1*V.NOACCOUNTMANAGEMENT 4*1*V.ADDRESSRESOLUTION 4*1*V.PLAINTEXT 4*1*V.PHYSICAL_PROTECTION 4*½*V.UNPATCHEDCOMPONENTS 4*½*V.INFORMATION_LEAKAGE 4*½*V.NOTRAINING
UI2	YIKICI:3	2*V.UNUSEDSERVICES 2*V.REMOTE_ACCESS 2*V.NOAUTHENTICATION 2*V.NOACCESS_CONTROL 2*V.NOACCOUNTMANAGEMENT 1*V.PLAINTEXT 2*V.PHYSICAL_PROTECTION (1+1/2)*V.ADDRESSRESOLUTION (1+1/2)*V.UNPATCHEDCOMPONENTS (1/2+1/2)*V.INFORMATION_LEAKAGE (1/2+1/2)*V.NOTRAINING	3*2*V.UNUSEDSERVICES 3*2*V.REMOTE_ACCESS 3*2*V.NOAUTHENTICATION 3*2*V.NOACCESS_CONTROL 3*2*V.NOACCOUNTMANAGEMENT 3*1*V.PLAINTEXT 3*2*V.PHYSICAL_PROTECTION 3*(1+1/2)*V.ADDRESSRESOLUTION 3* (1+1/2)*V.UNPATCHEDCOMPONENTS 3* (1/2+1/2)*V.INFORMATION_LEAKAGE 3* (1/2+1/2)*V.NOTRAINING
UI3	CİDDİ:2	2*V.UNUSEDSERVICES 2*V.REMOTE_ACCESS 2*V.NOAUTHENTICATION 2*V.NOACCESS_CONTROL 2*V.NOACCOUNTMANAGEMENT 1*V.PLAINTEXT 2*V.PHYSICAL_PROTECTION (1+1/2)*V.ADDRESSRESOLUTION (1+1/2)*V.UNPATCHEDCOMPONENTS (1/2+1/2)V.INFORMATION_LEAKAGE (1/2+1/2)V.NOTRAINING	2*2*V.UNUSEDSERVICES 2*2*V.REMOTE_ACCESS 2*2*V.NOAUTHENTICATION 2*2*V.NOACCESS_CONTROL 2*2*V.NOACCOUNTMANAGEMENT 2*1*V.PLAINTEXT 2*2*V.PHYSICAL_PROTECTION 2*(1+1/2)*V.ADDRESSRESOLUTION 2*(1+1/2)*V.UNPATCHEDCOMPONENTS 2*(1/2+1/2)V.INFORMATION_LEAKAGE 2* (1/2+1/2)V.NOTRAINING
UI4	KISITLI:1	1*V.UNUSEDSERVICES 1*V.REMOTE_ACCESS 1*V.NOAUTHENTICATION 1*V.NOACCESS_CONTROL 1*V.NOACCOUNTMANAGEMENT *V.PHYSICAL_PROTECTION 1*V.UNPATCHEDCOMPONENTS (1/2)*V.INFORMATION_LEAKAGE (1/2)*V.NOTRAINING	1*1*V.UNUSEDSERVICES 1*1*V.REMOTE_ACCESS 1*1*V.NOAUTHENTICATION 1*1*V.NOACCESS_CONTROL 1*1*V.NOACCOUNTMANAGEMENT 1*1*V.PHYSICAL_PROTECTION 1*1*V.UNPATCHEDCOMPONENTS 1*(1/2)*V.INFORMATION_LEAKAGE 1* (1/2)*V.NOTRAINING
Olası Her bir Açıklığının Tanımlı Dört İstenmeyen Olay için Toplam Kritikliği ($f_{ToplamKritiklik-CS-1}$)=			15*V.UNUSEDSERVICES 15*V.REMOTE_ACCESS 15*V.NOAUTHENTICATION 15*NOACCESS_CONTROL 15*V.NOACCOUNTMANAGEMENT 15*V.PHYSICAL_PROTECTION 11.5* V.ADDRESSRESOLUTION 9*V.PLAINTEXT 7,5*V.INFORMATION_LEAKAGE 7,5*V.NOTRAINING 6*V.UNPATCHEDCOMPONENTS

V. Adım'da önerilen tanımlı istenmeyen olaylara bağlı olarak olası tüm açıklıklar için kritiklik hesaplama yaklaşımı, Örnek Durum II için de kullanılırsa, açıklıkların toplam kritikliği için "Eş 7.3" ile tanımlanır.

$$F_{ToplamKritiklik\text{-}CS\text{-}2} = 4*(f_{CS\text{-}1\text{-}v}(UI1) + f_{CS\text{-}1\text{-}v}(UI2)) + 3*(f_{CS\text{-}1\text{-}v}(UI3) + f_{CS\text{-}1\text{-}v}(UI4)) \quad (7.3.)$$

$f_{ToplamKritiklik\text{-}CS\text{-}2}$= {14*V.UNUSEDSERVICES,
14*V.REMOTE_ACCESS,
14*V.NOAUTHENTICATION,
14*NOACCESS_CONTROL,
14*V.NOACCOUNTMANAGEMENT,
14* V.PHYSICAL_PROTECTION,
10.5 V.UNPATCHEDCOMPONENTS,
7.5*V.ADDRESSRESOLUTION
7* V.INFORMATION_LEAKAGE,
5.5*V.NOTRAINING,
4*V.PLAINTEXT}

Çizelge 7.20.'de Örnek Durum II incelemesi için V. adımdaki hesaplamaların tümü gösterilmiştir.

Çizelge 7.20. Örnek Durum II incelemesiiçin V. Adım hesaplama cetveli

İstenmeyen Olay	Olumsuzluk Derecesi	Hedeflenen Saldırı	Açıklığın Kritikliği=(İstenmeyen Durum Olumsuzluk Derecesi)*Açıklıklar Toplamı
UI1 UI2	HAYATİ:4	Ağda uygunsuz komut çalıştırma Sistemi işlevsiz bırakma / Kararsız hale getirme	2*V.UNUSEDSERVICES 2*V.REMOTE_ACCESS 2*V.NOAUTHENTICATION 2*V.NOACCESS_CONTROL 2*V.NOACCOUNTMANAGEMENT 2*V.PHYSICAL_PROTECTION (1+1/2)* V.ADDRESSRESOLUTION 1*V.PLAINTEXT (1+1/2)*V.UNPATCHEDCOMPONENTS (1/2+1/2)*V.INFORMATION_LEAKAGE (1/2+1/2)*V.NOTRAINING

Çizelge 7.20. (Devam) Örnek Durum II incelemesi için V. Adım hesaplama cetveli

İstenmeyen Olay	Olumsuzluk Derecesi	Hedeflenen Saldırı	Açıklığın Kritikliği=(İstenmeyen Durum Olumsuzluk Derecesi)*Açıklıklar Toplamı
UI3 UI4	CİDDİ:3	Saklı veri ve bilgileri silme veya değiştirme Ağ veya ağ servislerini kesme	2*V.UNUSEDSERVICES 2*V.REMOTE_ACCESS 2*V.NOAUTHENTICATION 2*V.NOACCESS_CONTROL 2*V.NOACCOUNTMANAGEMENT 2*V.PHYSICAL_PROTECTION (1+½)*V.UNPATCHEDCOMPONENTS (½)* V.ADDRESSRESOLUTION (½+½)*V.INFORMATION_LEAKAGE (1/2)*V.NOTRAINING
Olası Her bir Açıklığının Tanımlı Dört İstenmeyen Olay için Toplam Kritikliği **(**$f_{ToplamKritiklik\text{-}CS\text{-}2}$**)=**			14*V.UNUSEDSERVICES 14*V.REMOTE_ACCESS 14*V.NOAUTHENTICATION 14*NOACCESS_CONTROL 14*V.NOACCOUNTMANAGEMENT 14* V.PHYSICAL_PROTECTION 10,5 V.UNPATCHEDCOMPONENTS 7.5*V.ADDRESSRESOLUTION 7* V.INFORMATION_LEAKAGE 5.5*V.NOTRAINING 4*V.PLAINTEXT

ADIM 6: Sonuçların değerlendirilmesi ve yorumlanması

$f_{ToplamKritiklik\text{-}CS\text{-}1}$ vef $_{ToplamKritiklik\text{-}CS\text{-}2}$, SCADA/DDS sistemi kullanan iki farklı işletme içinÇizelge 7.4.'te tanımlı güvenlik açıklıklarından hangilerinin, her bir işletmeci için tanımlanan dört farklı 'İstenmeyen Olayın' meydana gelmesinde ne ölçüde katkı sağlayabileceği göstermektedir.

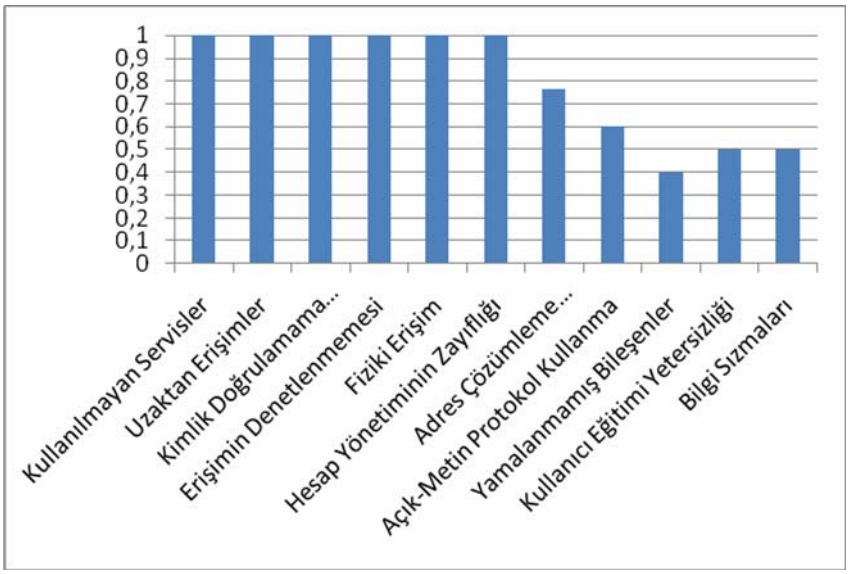
Her bir durum için elde edilen açıklık kritiklik sıralaması, tanımlanan istenmeyen olaylara (I. Adım'da) ve her bir olay için atanan olumsuzluk derecesine (II. Adımda atanan) doğrudan bağlıdır.

$f_{ToplamKritiklik\text{-}CS\text{-}1}$ vef $_{ToplamKritiklik\text{-}CS\text{-}2}$ ile açıklık kritiklik öncelikleri belirlenirken, her bir Örnek Durum için oluşturulan 'Hedeflenen Saldırı-İstenmeyen Durum'

eşleştirmesi (III. Adımda yapılan) ile daha önceden belirlenen ve her örnek durum için kullanılabilecek 'Hedeflenen Saldırı-Açıklıklar' eşleştirmelerinden yararlanılmıştır.

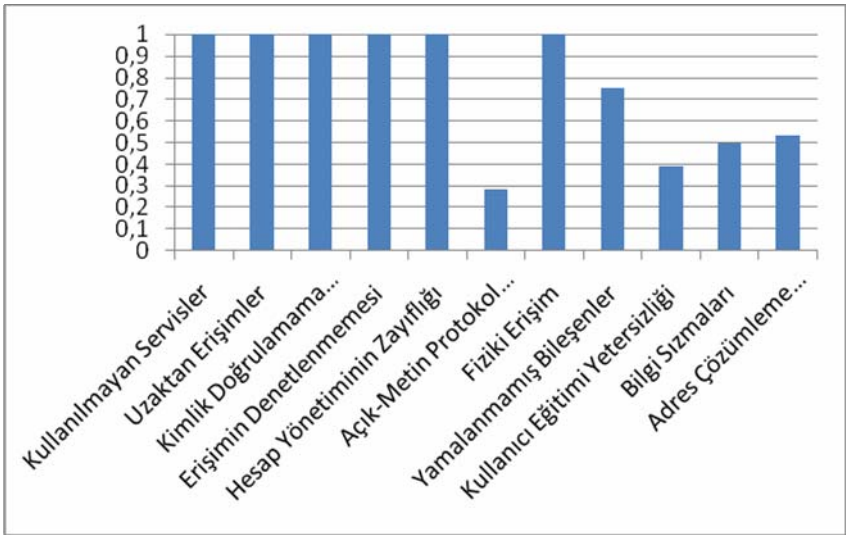
Çizelge 7.4.'te tanımlı güvenlik açıklıklarından, V.NOPOLICIES, V.PRODUCT ve V.NORISK diğer tüm açıklıkların oluşma veya giderilmeme nedeni, başka bir ifadeyle açıklıkların kaynağı olduğundan diğer açıklıklarla (kritikliği önceliklendirilen açıklıklarla) birlikte önem sıralamasına tutulmasının doğru olmayacağı değerlendirilmiştir. V.NOTRAINING ise, sadece sistemi sosyal mühendisliğe açık hale getirmesi yönüyle değerlendirilmiştir. En genel ifadeyle, önerilen açıklık kritikliği belirleme yöntemine sadece V.UNUSEDSERVICES, V.REMOTE_ACCESS gibi somut açıklıkların dâhil edilmesi yöntemin başarısını arttıracaktır.

$f_{ToplamKritiklik\text{-}CS\text{-}1}$ ve $f_{ToplamKritiklik\text{-}CS\text{-}2}$ 'deki açıklıkların önlerindeki katsayılar (15, 14 gibi açıklığın kritiklik katsayısı), o açıklığının incelenen her bir durum içindeki önem sırasını belirleme açısından önemlidir. Diğer türlü, Örnek Durum I'de elde edilen '15*V.UNUSEDSERVICES' ile Örnek Durum II'de elde edilen '14*V.UNUSEDSERVICES' arasında doğrudan karşılaştırma yapmak doğru bir yaklaşım olmayacaktır. Bu nedenle, her bir Örnek Durum için $f_{ToplamKritiklik\text{-}CS}$'lerde tanımlı en büyük açıklık kritiklik katsayısını kullanarak açıklık kritikliklerinin normalize edilmesi, farklı örnek durum incelemelerinin kıyaslanması için daha elverişli bir yol olabilecektir. Bu durumda, $f_{ToplamKritiklik\text{-}CS\text{-}1\text{-}Normalize}$ Şekil 7.6.'daverildiği gibi yeniden hesaplanabilecektir.



Şekil 7.6. Örnek Durum I normalize edilmiş açıklık kritiklik değerleri

Benzer şekilde Çizelge 7.20.'de hesaplanan $f_{ToplamKritiklik\text{-}CS\text{-}2}$ normalize edildiğinde Şekil 7.7. elde edilecektir .



Şekil 7.7. Örnek Durum II normalize edilmiş açıklık kritiklik değerleri

$f_{ToplamKritiklik\text{-}CS\text{-}1}$ ve $f_{ToplamKritiklik\text{-}CS\text{-}2}$ 'de yer almayan açıklıkları var olmayan açıklıklar olarak kabul etmek yanlış olacaktır. Zira $f_{ToplamKritiklik\text{-}CS\text{-}1}$ ve $f_{ToplamKritiklik\text{-}CS\text{-}2}$'deki açıklıkların varlığı ve kritiklik katsayısı I. Adım'da tanımlı istenmeyen

olaylarla doğrudan bağlıdır. Farklı veya ilave istenmeyen olaylar tanımlandığında, güvenlik açığı kritiklik sıralaması değişebilecektir.

Yukarıdaki yöntem, tanımlı olası açıklıklardan hangisinin, belirli bir işletmecisi için tanımlı istenmeyen olayların gerçekleşmesine ne ölçüde neden olabileceğini kestirmekte kullanılabilir. Ancak yukarıdaki hesaplamalarda, işletmeci bazında açıklıkları giderici iyileştirmelerin etkisine yer verilmemiştir. Örnek Durum İncelemelerinde, hangi açıklığının giderilip giderilmediği dikkate alınarak elde edilen $f_{ToplamKritiklik\text{-}CS}$ açıklık kümeleri üzerinden giderilmiş açıklıkların eksiltmesi yapılabilecektir.

7.5. Siber Güvenlik Risk Hesaplama Yöntem Önerisi

Üçüncü Bölümde “Eş.3.1.”, “Eş.3.2.”, “Eş.3.3.”, “Eş.3.4.” ile üç farklı kaynağın [36-37] birbirini destekleyen ve bazı yönleriyle benzeyen risk hesaplama şekilleri verilmiştir. Ancak her üç yöntemde de etkinin ortaya çıkma veya tehdidin gerçekleşme olasılığının nasıl hesaplanacağıyla ilgili açık bir yol sunulmamaktadır. Bu çalışmada, istenmeyen etkilerin,başka bir ifadeyle istenmeyen olayların ortaya çıkma ihtimali olası açıklıkların kritikliğine dayandırılmış ve açıklık kritikliğinin belirlenmesi için bir yöntem önerisinde bulunulmuştur. Ancak bunun için öncelikle istenmeyen olayların tanımlanması ve onlar için bir olumsuzluk değeri atanması şartı getirilmiştir. Aksi halde, önceden tanımlanmayan ve ne kadar olumsuz olduğu belirlenmeyen olayların (etkilerin) oluşmasına dair bir risk değerlendirmesi yapmak mümkün olmayacaktır. Bununla birlikte tehdit kaynağının gücünün belirlenmesi bu çalışma için de bir sorun olarak ortaya çıkmıştır. Her ne kadar, “Eş.7.1.” ile tanımlandığı üzere siber tehdit kaynağının gücünün hesaplanması için bir denklem sunulsa da, denklemde yer alan M (motivasyon derecesi) ve C’nin (teknik kabiliyet derecesi) belirlenmesi, durum, koşul ve taraflara (saldıran ve savunan) göre ciddi değişiklikler içerecektir. Bu nedenle, belirli bir tehdit kaynağından bahsedilmiyorsa, politik, ekonomik ve kişisel tehdit kaynakları için Çizelge 7.7.’de olduğu gibi tanımlarından yola çıkarak ön kabulle ‘değer atama’ yoluna gidilebilecektir.

Risk değeri “Eş 7.4.” hesaplanmadan önce kat edilmesi gereken aşamalar aşağıda özetlenmiştir.

- Bölüm 7.4.’te yer alan altı adım takip edilerekişletme, tesis veya organizasyona ilişkin tanımlı istenmeyen olaylara kaynaklık yapabilecek olası tüm açıklıklara ilişkin kritiklik değeri saptanır.
- Bölüm 6.’da yer alan açıklık inceleme ve tarama yaklaşımları kullanılarak incelenen sistem üzerindeki eksik ve mevcut tedbirler tespit edilir. Mevcut tedbirlerle giderildiği tespit edilen açıklıklar listeden çıkarıldıktan sonra“$f_{ToplamKritiklik-CS}$” son haline getirilir.
- Çizelge 7.7.’deki gibi motivasyon türüne göre farklısiber tehdit kaynakları için değerler atanır.

Risk= Açıklık Kritikliği*Tehdit Kaynağının Gücü (7.4.)

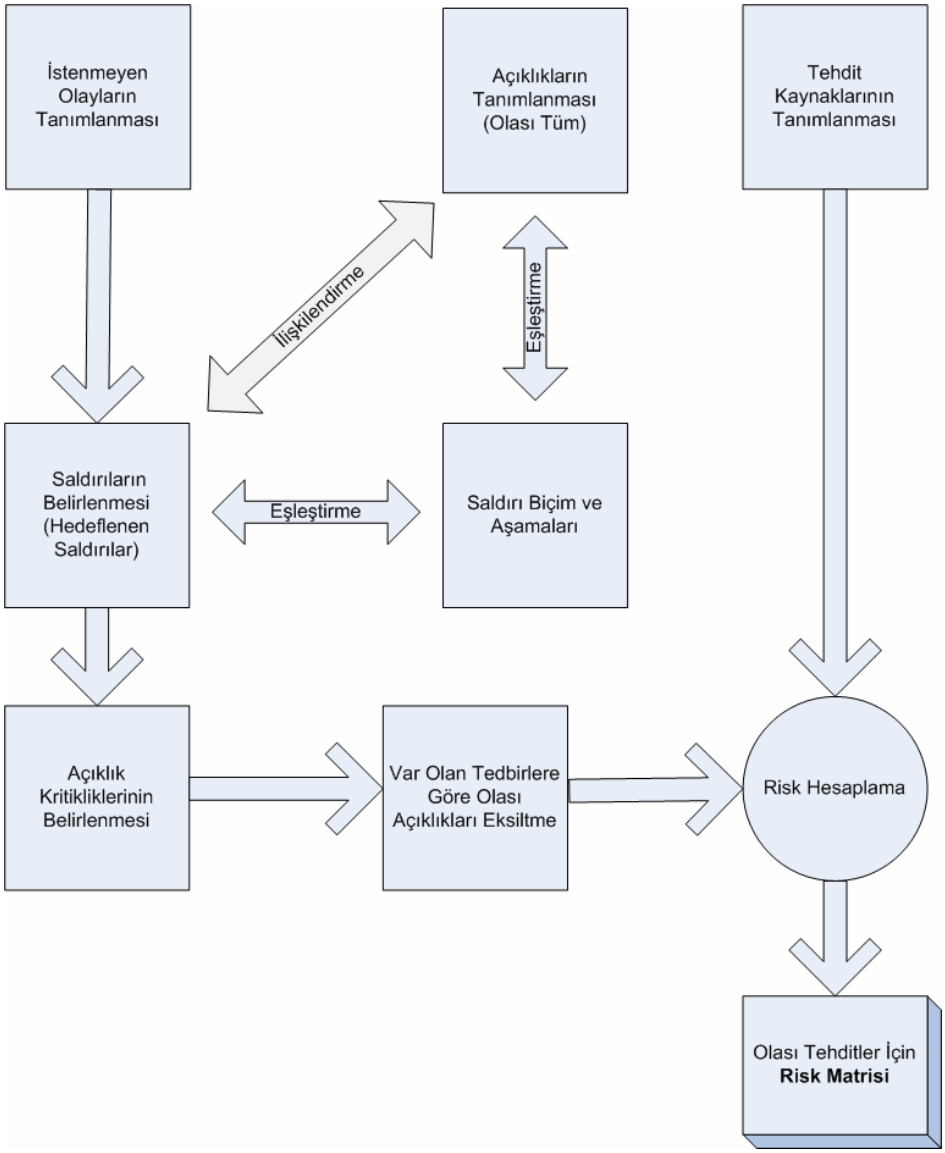
$$\text{Risk} = f_{ToplamKritiklik-CS} * \sum_{i=1}^{n=BelirlenenToplamTehditKaynağı} (Mi * Ci)$$

“Eş.7.4.” kullanılarak ‘Açıklık Kritikliği-Tehdit Gücü’ matrisi oluşturulursa, riskin hangi tehdit kaynakları ve açıklıklar için daha yüksek olduğu daha rahat görülebilecektir. Çizelge 7.21.’de Örnek Durum İncelemesi I için tanımlı dört istenmeyen olaya ilişkin olası tüm açıklıklar ve dört farklı tehdit kaynağı için risk matrisi görülmektedir. $f_{ToplamKritiklik-CS-2-Normalize}$ ve Çizelge 7.7. kullanılarak Örnek Durum İncelemesi-2 için de risk matrisini oluşturmak mümkündür.

Çizelge 7.21. Örnek Durum I incelemesiolası tüm açıklıklar ve tehdit kaynakları için risk matrisi

Açıklıklar / Tehdit Kaynakları	Politik	Ekonomik	Kişisel İşletme İçinden	Kişisel İşletme Dışından
V.UNUSEDSERVICES	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.REMOTE_ACCESS	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.NOAUTHENTICATION	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.NOACCESS_CONTROL	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.NOACCOUNTMANAGEMENT	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.ADDRESSRESOLUTION	0.77*1=0.77	0.77*0.34=0.26	0.77*0.46=0.35	0.77*0.06=0.046
V.PLAINTEXT	0.6*1=0.6	0.6*0.34=0.2	0.6*0.46=0.276	0.6*0.06=0.036
V.PHYSICAL_PROTECTION	1*1=1	1*0.34=0.34	1*0.46=0.46	1*0.06=0.06
V.UNPATCHEDCOMPONENTS	0.4*1=0.4	0.4*0.34=0.136	0.4*0.46=0.184	0.4*0.06=0.024
V.INFORMATION_LEAKAGE	0.5*1=0.6	0.5*0.34=0.17	0.5*0.46=0.23	0.5*0.06=0.03
V.NOTRAINING	0.5*1=0.6	0.5*0.34=0.17	0.5*0.46=0.23	0.5*0.06=0.03

Önerilen risk belirleme yaklaşımı, açıklıklardan başlayarak istenmeyen olayların olma olasılığının belirlenmesi yerine, istenmeyen olayları tanımlayıp onlara olumsuzluk değeri atayarak buradan açıklıklara doğru gitmektedir. Bu yönüyle, izlenen yöntem için tümden parçalara gelindiğini söylemek mümkün olacaktır. Şekil 7.8.'de önerilen açıklık kritikliği belirleme ve güvenlik riski hesaplama yönteminin kısa akış ve ilişki diyagramı yer almaktadır.



Şekil 7.8. Önerilen siber güvenlik risk belirleme yaklaşımı için akış ve ilişki şeması

Elektrik, su, gaz, petrol üretim, dağıtımı ve iletimi gibi sadece işletmecinin kendisi için değil toplumun ve ülkenin bir bölümü veya tamamı için önemli olan altyapılarının denetim ve yönetiminde kullanılan sistem ve sistem bileşenleri için doğrudan varlıklara dayalı veya sadece ekonomik değerlere odaklı risk değerlendirme çalışmaları yanıltıcı ve eksik olacaktır. Çünkü bu tür altyapılar bölge veya ülke ölçeğinde birçok üretim ve hizmet biriminin çalışması için temel girdi sağladıkları gibi hizmet alanı içerisindeki can ve mal emniyetini de yakından ilgilendirebilirler. Örneğin bir bölgeye elektrik hizmeti veren bir işletmecinin 12 saatlik hizmet kesintisinin ekonomik kaybı o işletmeci özelinde hesaplanabilse de, girdi sağladığı alanlardaki toplam ekonomik kayıp çok daha büyük olacak ve bu kaybı hesaplayabilmek de çoğu durumda mümkün olmayacaktır. Bu sebeple, kritik işlev gören denetim sistemlerine ilişkin olarak ekonomik kayıpların değil, operasyonel kayıpların ve beraberindeki istenmeyen etkilerin olma olasılığını hesaplamak mümkün olacaktır. Örneğin Patel ve ark. [82] hasar analizinin ekonomik kayıplara dayandırılması ancak dışarı sürekli hizmet veya kaynak sunmayan, hasar durumunda çevreye, çalışanlara ve tedarik zincirindeki önde ve arkada kalan endüstrilere zarar vermeyen yapılar için söz konusu olabilecektir.

7.6. Riski Giderme ve İyileştirme Önceliği

Bir saldırı biçiminin kullanılabilirliği, saldırılacak altyapıda ilgili güvenlik açığının var olup olmamasına bağlıdır. Önerilecek güvenlik iyileştirmeleri, ilgili açıklığının giderilerek kullanılacak saldırı biçim veya aşamalarının kullanışsız ve işlevsiz bırakılması yönünde olmalıdır.

Açıklık kritikliği belirleme yöntemi ile bir işletmeye özgü olarak tanımlı istenmeyen olaylar için açıklıkların önem sırasına göre sıralanması mümkün hale gelebilecektir. En önemliden önemsize doğru sıralanan olası açıklıklar için tek tek var olan veya olmayan açıklık giderme/iyileştirme yol ve tekniklerinin çıkarılması ile hangi iyileştirme kullanılırsa hangi açıklığının ne ölçüde giderilebileceği veya iyileştirilebileceği görülecektir. Örneğin, Çizelge 7.22.'de örnek olarak sunulan iki açıklık için gerekli iyileştirme önerilerinden bazıları gösterilmiştir. Bu iyileştirme

uygulamalarından birinin kullanımı aynı anda birden fazla açıklığının giderilmesine veya azaltılmasına katkı sağlamaktadır. Örneğin Çizelge 7.22.'deki iyileştirmelerden 'Adres (Örn: IP) Denetimi / Filtrelenmesi', çizelgede tanımlı her iki açıklığının iyileştirilmesinde kullanılacağından öncelikli iyileştirme olarak ele alınması gerekecektir.

Çizelge 7.22. Örnek açıklık-mevcut tedbir-eksik tedbir eşleştirmesi

Açıklık	Mevcut Tedbir	Gerekli İyileştirme (Bazıları) Eksik Tedbir
Uzaktan Erişim (V.REMOTE_ACCESS)	VPN Kullanımı	Adres Denetimi / Filtrelenmesi Erişim Loglama Uzak Yetki Kısıtlama
Erişim Denetimi (V.NOACCESS_CONTROL)	YOK	Ağ Segmentasyonu (VLAN) Adres Denetimi / Filtrelenmesi Oturum Denetimi

Çizelge 7.22. benzeri bir çizelgenin, tüm açıklıklar için incelenecek sistemlerde kullanımı, hangi iyileştirmelerin öncelikli kaç açıklığının giderilmesi için kullanılabileceğini göstermesi bakımından önemlidir. Bu sayede, hangi iyileştirmelerin kaç önemli açıklığın giderilmesine katkı sağladığını görmek ve hangi iyileştirmenin öncelikli olduğu kestirmek mümkün olabilecektir.

Açıklıkların giderilmesi için yapılacak iyileştirmelerin (alınacak tedbirlerin) işletmecilere ekonomik, idari ve operasyonel maliyetler getirmesi beklenen bir durumdur. Çok fazla eksik tedbirinin olduğu altyapı ve işletmeciler için, ekonomik, yönetsel ve operasyonel gerekçelerle eksik tedbir önceliklendirmesi yoluna gidilmesi gerekebilir. Bu durumlarda, 'Açıklık- Eksik Tedbir' eşleştirmesinde, tedbirin eşleştiği açıklığın kritikliği ve eksik tedbirinin kaç açıklık için gerektiği önceliklendirme değerleri olarak kabul edilebilir. Bir işletmeye özel güvenlik iyileştirmeleri yapılmadan önce, 'Açıklık-Mevcut Tedbir- Eksik Tedbir' eşleştirmesinin yapılması, maliyet-etkin ve öncelik sırasına uyulmuş bir iyileştirme sürecinin yürütülmesine imkân verecektir.

Bu çalışma kapsamında yürütülen Örnek Durum İncelemeleri için risk belirleme ve giderme aşamaları aşağıda Çizelge 7.23.'te tam liste halinde sunulmuştur.

Çizelge 7.23. Risk belirleme ve giderme süreçleri

Risk Belirleme Adımları	• Oluşabilecek istenmeyen olayların tanımlanması • İstenmeyen olayların etkilerinin tanımlanması ve olumsuzluk değeri atanması • 'İstenmeyen Olay-Hedeflenen Saldırı-Saldırı Biçimi-Açıklık' eşleştirmeleri kullanılarak 'İstenmeyen Olay-Açıklık' eşleştirmesinin elde edilmesi • Açıklıkların kritikliğini belirleme • (Bilinen veya varsayılan) Tehdit kaynakları için güç değeri belirleme • Açıklıklara karşı alınan mevcut tedbirleri (iyileştirmeleri) tespit (Mülakat, soru-cevap ile giderildiği anlaşılan veya ve sistem tarama yöntemleri ile varlığına rastlanmayan açıklıklar) • Açıklıkların kritikliği yeniden ele alma ($f_{ToplamKritiklik-CS}$ için eksiltme ve çıkarmalar) • Riskmatrisi oluşturma
Risk Giderme Adımları	• 'Olası Açıklıklar - Mevcut Tedbir - Eksik Tedbir' eşleştirmesi • Eksik tedbirleri önceliklendirilmesi

Bu bölümde, kritik altyapılarda kullanılan dağıtık denetim sistemlerine yönelik siber risklerin tanımlanması ve değerlendirilmesi için öncelikle literatürdeki tanımlamalardan faydalanarak açıklıkların ve varlıkların tanımlanması, motivasyon kategorisine göre tehdit kaynaklarının tanımlanması, saldırı hedef ve biçimlerinin tanımlanması gerçekleştirilmiştir. Özellikle açıklık tanımlamaları yapılırken saha çalışmalarında elde edilen bilgi, bulgu ve gözlemelere dayalı bir açıklık tasnifin

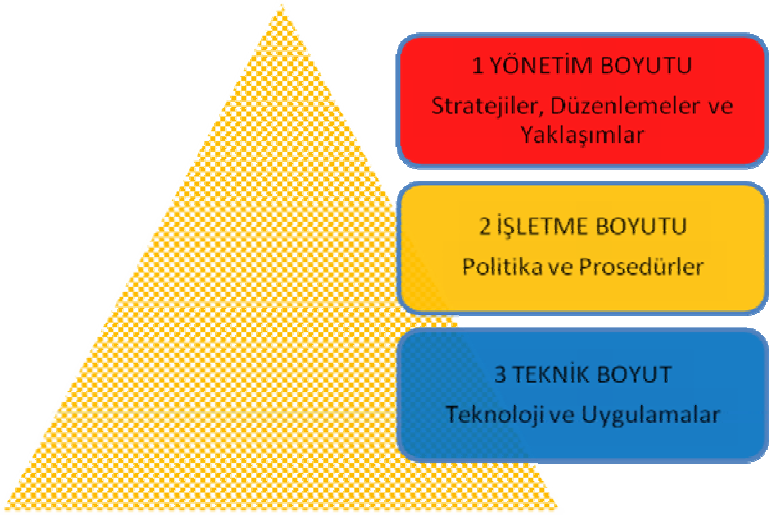
yapılmasına özen gösterilmiştir. İstenmeyen olayların tanımlanması ve olumsuzluk derecelerinin belirlenmesi her bir işletmeci için ayrı ayrı yapılmıştır. Sonrasında tüm bu tanımlamalara dayalı olarak siber güvenlik risk giderme aşaması öncesi olası açıklıklar arasında kritiklik sıralaması veya sınıflandırılmasının yapılmasıhedeflenmiştir. Böylece incelenen kritik altyapı türleri için güvenlik önceliklerinin ve gerekliliklerinin neler olması gerektiği belirlenebilecektir.

8. GÜVENLİK İYİLEŞTİRMELERİ

Yönetim ve işletme boyutundaki eksiklik ve kusurlar ile bunların devamı sayılacak güvenlik iyileştirmeleri için elverişli olmayan altyapı mimari ve bileşenleri, beraberinde birçok güvenlik açığının oluşmasına sebebiyet verecektir. Bu anlamda, Örnek Durum İncelemeleri ve literatür araştırmaları da göstermiştir, bir işletmeye ait güvenlik kusurlarını sadece teknik boyutta aramak eksik bir güvenlik bakış açısı olup, bir çok teknik güvenlik açıklığın kaynağı olan yönetim ve işletme boyutlarını güvenlik süreçlerinin en başında bulundurmak gerekmektedir.

NIST SP 800-30 Risk Yönetimi Rehberinde [25] güvenlik iyileştirmeleriyönetim, işletme ve teknik olmak üç başlıktatanımlanmış ancak anılan çalışmada bu bağlamda yeterli öneri, ilişkilendirme ve tartışma sunulmamıştır. Öte yandan, literatürdeki birçok farklı kaynakta dagüvenlik iyileştirme yaklaşım ve tartışmalarınıngenel olarak teknik, işletme veya yönetim boyutlarından biri etrafından şekillendiği ve her üç boyutun birlikte yeterince tartışılmadığı gözlenmektedir. Bu çalışmada ise sürdürülebilir bir güvenlik yaklaşımının geliştirilebilmesi için konu her üç başlıkta birlikte tartışılmıştır. Yönetim, işletme ve teknik iyileştirmelerin her biri ayrı bir boyut olarak ele alınmış ve bu şekilde de adlandırılmıştır.Her güvenlik boyutu için sunulacak öneri ve tartışmalar, saha çalışmalarında gözlenen öncelik ve ihtiyaçlara göre ele alınmıştır. Önerilerin işletmelerin ve endüstrinin gerçekleriyle uyumlu ve uygulanabilir olması temel kriter olarak belirlenmiştir. Yönetim boyutunda ise Türkiye özelindeki gözlenen eksikliklerin giderilerek, tüm paydaşları kapsayacak biçimde yapılması gerekenler belirlenerek ve önerilerde bulunulmuştur.

Şekil 8.1.'de ele alınacak bu üç güvenlik boyutu için önem sıralaması görülmektedir.

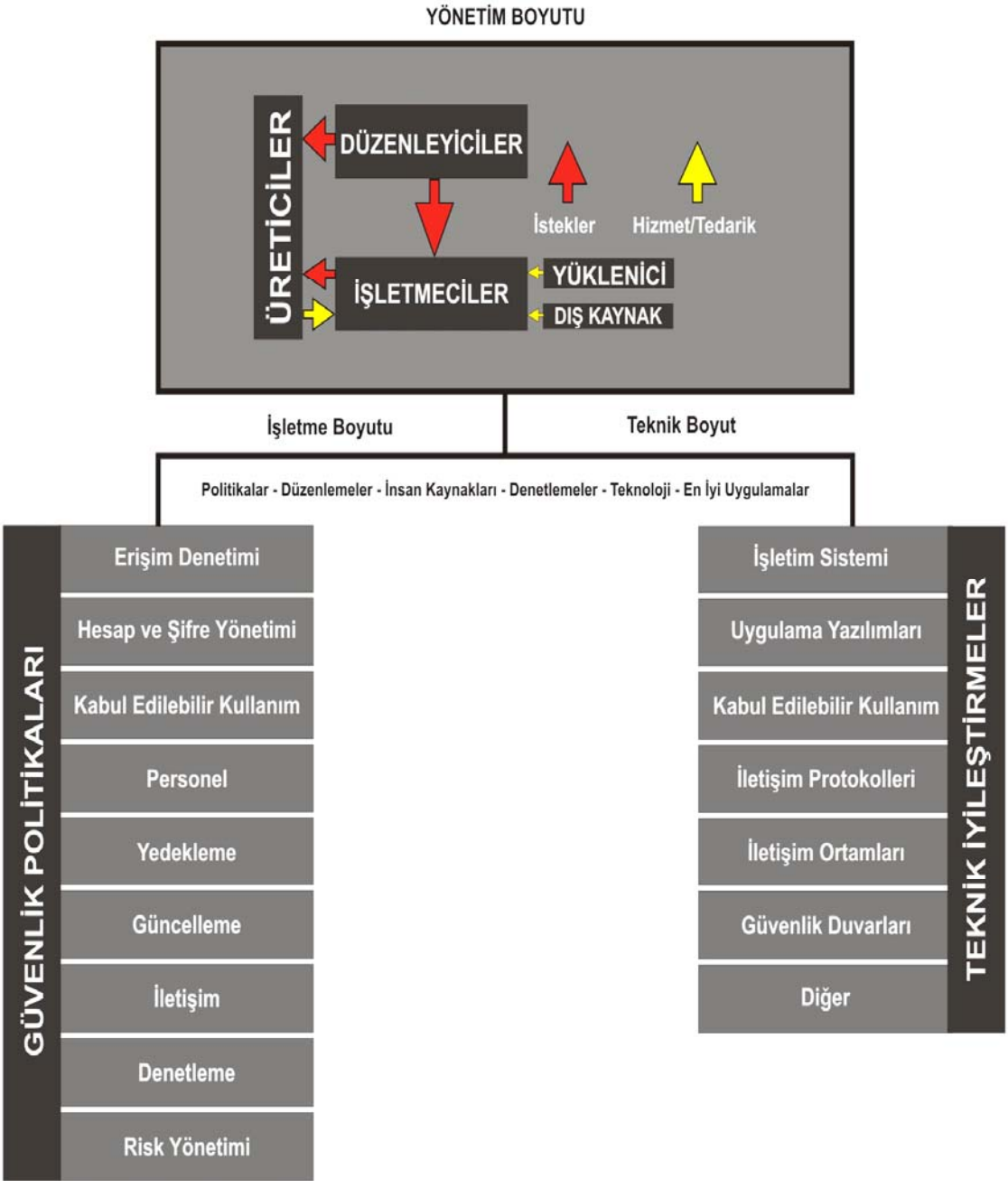


Şekil 8.1. Güvenlik boyutları önem sıralaması

Üç boyutlu güvenlik yaklaşımında, tartışılacak olan her boyutun ayrıca kendi aralarında farklı ya da aynı başlıklarda bir ilişki içerisinde olduğundan bahsetmek mümkündür. Bu başlıklar en genel haliyle Politikalar (Yazılı Kurallar), Çalışanlar (İnsan Kaynakları - Personel), Teknoloji,Düzenlemeler ve Denetleme olarak sınıflandırılabilir. Üç boyutlu güvenlik yaklaşımının her bir boyutu arasındaki ilişkiŞekil 8.2.'deki gibi ifade edilmiştir.

Şekil 8.2. Güvenlik boyutları arasındaki ilişki diyagramı

Aşağıda, her üç güvenlik boyutu Şekil 8.3.'te gösterilen üç boyutlu güvenlik yaklaşımı çerçevesinde gösterilen bağ ve sıralamaya uygun olarak tartışılacaktır.



Şekil 8.3. Üç boyutlu güvenlik iyileştirme yaklaşımı çerçevesi

8.1. Yönetim Boyutu

Yönetim boyutunda ele alınması gereken başlıca paydaşlardan birincisi düzenleyici kurumlar veya ilgili devlet kurumlarıdır. Birinci paydaş grubuna sektör birlikleri gibi tüzel kuruluşlarda ilave edilebilir. Farklı ad veya organizasyonlara karşılık, çalışmanın bundan sonraki kısmında yönetim boyutunun birinci gruptaki paydaşlarına genel olarak 'Düzenleyici' veya 'Kamu Düzenleyicisi' adı verilecektir.

Yönetim boyutunda ele alınacak ikinci paydaş ise, her bir DDS altyapı işletmecisinin kendi yönetimi, diğer bir ifadeyle karar alıcılarıdır.

İşletmeci yöneticileri karar, tutum ve öncelikleriyle işletmenin nasıl işletileceğini belirlerler. Kullanılacak ürün ve teknolojilerin seçimi, yatırım yapma ve satın alma, dış destek ve altyüklenici kullanımı gibi konularda nihai kararları işletmeci yöneticileri almaktadır. Şayet işletme, düzenleyici bir kuruma karşı sorumlu ise yöneticilerin aldıkları kararların düzenleyici kurumun gerekliliklerileyle uyumlu olması gerekecektir.

Yönetim boyutunda diğer paydaşlar ise, teknoloji üreticileri/tedarikçileri, yükleniciler ve dış kaynak destekler olarak tanımlanabilir.

Şekil 8.3.'te yönetim boyutundaki tüm paydaşlar, aralarındaki ilişkilerle birlikte gösterilmiştir. Aşağıdaki alt başlıklarda yöntemi boyutundaki paydaşların işletmelerdeki güvenlik kural ve yaklaşımlarının gelişmesinde nasıl bir rol ve etkinliğe sahip oldukları da tartışılacaktır.

8.1.1. Düzenleme ve bir ülke yaklaşım örneği

Belirli bir sektörü düzenlenme yaklaşımı ilk olarak ABD'de ortaya çıkmış, Avrupa ise özelleştirmelerin hız kazandığı 1980 sonrasında düzenleyici kuruluşlarını oluşturmaya başlamıştır. Türkiye, Avrupa ile birlikte belirli sektörler için kendi düzenleyici kuruluşlarını oluşturmaya 1980'li yıllarda başlamıştır. İngiltere özelinde

Proser'in düzenleme yaklaşımları incelendiğinde, kamu özerk düzenleyicilerine alternatif olarak düzenleme yapmama, devletleştirme, düzenlemeyi piyasalara bırakma veya özdüzenlemeyi tesis etme şeklinde sıralanabilir [92].

Türkiye'de kamu düzenleyici kurumlarına örnek olarak EPDK (Enerji Piyasası Düzenleme Kurulu), BDDK (Bankacılık Düzenleme ve Denetleme Kurumu), BTK (Bilgi Teknolojileri ve İletişim Kurumu) gibi kurumlar örnek olarak verilebilir.

Ülkelerin enerji, telekomünikasyon gibi farklı sektörlerde düzenleyici kuruluşlar oluşturma nedenleri arasında teknolojinin katkısıyla hızla gelişen bu alanların aynı zamanda uzmanlaşmayı da gerektirmesi sayılabilir[93].

Düzenleyicilerin kendi alanları için izin verme, kural koyma, izleme, yaptırım uygulama, kamuoyunu bilgilendirme, bilgi isteme, araştırma ve geliştirme faaliyetlerinde bulunma, anlaşmazlıkları çözme hususlarında görev ve yetkileri bulunmaktadır [93].

Doğrudan bir kamu düzenleyicisi kuruluşun olmadığı alanlardaki düzenleme, sektörün ilgili olduğu bakanlık veya ona bağlı kuruluşlar üzerinden yapılabileceği gibi doğrudan sektörün kendi içinde oluşturduğu organizasyonlar eliyle de yürütülebilir.

Özelikle ABD'de düzenleyici kuruluşlar kadar özdüzenleyici kuruluşlarında sektör üzerinde ciddi etki ve yaptırımları olduğu görülmektedir. Aşağıda özdüzenleyici bir kuruluş olarak NERC örneği ve siber güvenlik alanında kendi sektörünü ne şekilde düzenlediği konusu ele alınmıştır.

Amerika Birleşik Devletlerinde enerji sektörünü düzenlemekle yetkili olan FERC adlı kuruluştur. FERC ilk olarak ilk 2002 yılında yayımlanan SSEMP (Security Standart for Electric Market Participants) ile elektrik dağıtım piyasasında kullanılacak elektronik ekipmanların yazılım, donanım ve iletim bileşenlerinin sağlaması gereken minimum güvenlik standartları ortaya koyan bağlayıcı bir

düzenleme oluşturmuştur [52,94]. Ancak NERC'nin daha kapsamlı CIP (Kritik Altyapı Koruma) çalışmalarıyla SSEMP oldukça dar kalmıştır. Peki, NERC aslında kimdir ve bunu nasıl yapmaktadır? ABD Federal Enerji Regülasyon Komisyonu ve Kanada Hükümet otoritelerinin gözetimine bağlı olmakla birlikte, NERC Kuzey Amerika'daki elektrik enerjisi sektörünün özdenetimini yapmak üzere 1968'de kurulan bir kuruluş olup kamu düzenleyicisi olan FERC tarafından akredite edilmiş bir organizasyondur. NERC bünyesinde geliştirilenstandartları aynı zamanda sektöre uygulatmaktadır. Bununla birlikte sektördeki personellerin eğitilmesi ve sertifikalandırılması, elektrik enerjisi üretimiyle ilgili tahminlerin yapılması işlerini de üstlenmektedir [95-96]. NERC tarafından Kuzey Amerika Elektrik Üretim ve Dağıtım Enterkonnekte sisteminin fiziki ve siber güvenliğini iyileştirmek için Kritik Altyapı Koruma Programını başlatmış ve bu program kapsamında, standartların geliştirilmesi ve sektörün standartlara uymasının zorlanması, kritik güvenlik bilgilerinin sektöre duyurulması ve bilgi bankası kurulması, güvenlik farkındalığının arttırılması gibi hedefler konmuştur [97]. Güç sistemlerindeki açıklıkların tespiti için NERC ABD Enerji ve Savunma Bakanlıklarıyla birlikte çalışmalar yürütmektedir [98]. NERC, ilk olarak 2003 yılında hazırladığı 'Acil Eylem Standart 1200' siber güvenlik standardını 2004'de genişleterek CIP002'den CIP009'a kodlarla farklı başlık ve alt başlıklarda genişleterek, elektrik sektörünün 2006 yılında bu standartlara uygunluk sağlamasını istemiştir [99-100]. Ardından geçilen hızlı uyumluluk süreci ile işletim maliyetleri artsa da, bu düzenleme birbirine bağlı Kuzey Amerika elektrik şebekesinin güvenliğini arttırması bakımından önemli görülmüştür [101]. Doğrudan kamu otoritesi olmadığı halde düzenleme görevini üstlenen bir organizasyon olarak NERC, Kuzey Amerika elektrik sektöründe kullanılan kritik altyapının korunması konusunda diğer sektörlere ve ülkelere öncülük etmektedir.

Kamu düzenleyicisi olmayıp sadece sektör birliği olan AGA ise, SCADA/DDS altyapısının iletişim sistemlerinin güvenliğinin sağlanması konusunda önemli bir inisiyatif alarak, sektörün kullanımına uygun güvenli iletişim standardı tasarlamış ve bunu kendine bağlı kuruluşlarında altyapı değişikliğine gidilmeden kullanıma hazır bir ürün haline getirmiştir [100,102].

Bu açıdan ülkemiz göz önünde bulundurulduğunda, her ne kadar çeşitli federasyonlar, meslek oda ve birlikleri olsa da, NERC gibi kendi standartlarını kapsamlı şekilde hazırlayan ve bunları etkili şekilde uygulatabilen bir özdüzenleyici kuruluş kültürünün bulunduğunu ve bunların yeterli seviyede olduğunu söylemek gerçekçi olmayacaktır. Bu nedenle Türkiye özelinde en uygun çözümün, kamu düzenleyicileri eliyle kritik altyapılara ilişkin siber güvenlik standartlarının belirlenmesi, denetimlerinin yapılması veya yaptırılması, uygunsuzluklarında yasal mevzuatta karşılığı olan yaptırımlara bağlanması olduğu değerlendirilmektedir. Belki de bu noktada tartışılması gereken önemli hususlardan biri de ülkemizdeki kamu düzenleyici kuruluşlarının bu alanda bir görevleri olup olmadığı, eğer varsa bu görev ve sorumluluklarını yerine getirip getirmedikleri meselesidir.

Kamu düzenleyici kurum ve kuruluşları, kuruluş yasalarında yer alan görev ve yetkilere bağlı olarak düzenledikleri sektörün ve o sektörden hizmet alan kesimlerinin faydasına yönelik düzenlemelerde bulunurlar. Bu bağlamda, belirli bir bölgeye veya ülkenin tamamına hizmet veren kritik altyapı işletmecilerinin siber saldırılara karşı güvenliklerinin sağlanması da kamu mal ve can güvenliği, bölge ve ülke ekonomisinin sağlıklı işleyişi açısından ilgili düzenleyici ve denetleyicilerin ilgi alanı içinde olması gerektiği değerlendirilmektedir.

8.1.2. Türkiye'deki mevcut durum ve iyileştirme önerileri

Türkiye'de, sadece dağıtık denetim sistemi bulunan kritik altyapılara yönelik değil, genel olarak siber güvenlik alanında ciddi yasal mevzuat boşluğu bulunmaktadır. Günümüz ihtiyaçları ve teknolojinin kullanımı dikkate alındığında, siber güvenlik konusundaki yasal mevzuat anlamında yeterli bir yapının bulunmaması istenmeyen sonuçlar doğurabilecektir.Her ne kadar telekomünikasyon sektörüne ilişkin olarak 20.07.2008 tarih ve 26942 sayılı Resmi Gazetede yayımlanan "Elektronik Haberleşme Güvenliği Yönetmeliği", Bankacılık sektörüne ilişkin olarak 14.09.2007 tarih ve 26643 sayılı Resmi Gazetede yayımlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" yayınlanmış, "Kişisel Verilerin Korunması Kanun Tasarısı" yasalaşmak için Türkiye Büyük Millet Meclisi'nde

2008'den bu yana bekliyor olsa da, bugün için, ülke kritik altyapılarının siber güvenlik ihtiyacı karşısında kapsamlı ve yeterli düzenlemelere gidilmemiş olması yönetim boyutundaki eksikliklerin temel nedenlerindendir. Bu sebeple, Türkiye'de acilen başta enerji (elektrik, gaz, petrol) ve su üretim, iletim ve dağıtım altyapısı olmak üzere çeşitli sektörlerde kullanılan denetim sistemlerinin güvenliğini de içeren yasal mevzuat oluşturulmalı, güvenlik kriterleri açık olarak tarif edilmeli ve ilgililerince uygulatılmalı ve denetlenmelidir.

Türkiye özelinde önemli eksikliklerden biri de, birçok batılı ülkede oluşturulmuş ve uygulama safhasına geçmiş olmasına rağmen Türkiye'de hala bir resmiyet ve işlerlik kazanmış bir siber güvenlik stratejisinin olmamasıdır. Her ne kadar, yeni bir adım olarak, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı ile Bilgi Güvenliği Derneği bünyesinde böyle bir çalışma başlatılmış ve 19 Haziran 2012 tarihinde ilgili kamu kurumlarının da katılımıyla bir çalıştay ortamında tartışmaya açılmışsa olsa da, bugün için tartışılan bir taslak dışında herhangi resmi bir belgeden bahsetmek mümkün değildir.

Siber güvenlik strateji belgeleri, ülkeler özelinde öncelikleri belirleyen ve atılması gereken adımları özetle tarif eden belgelerdir. Dünya örnekleri incelendiğinde bu belgelerin çoğunluğunun [103-105] ülke kritik altyapılarını, sıralamada ve tanımlamadaki bazı ufak farklılıklar olsa da, birbirine benzer şekilde tarif ettikleri görülmektedir.

Bilgi Güvenliği Derneği taslağında [106], kritik altyapılar dünya örneklerine benzer olarak;

- Bilgi ve iletişim
- Enerji
- Finans
- Sağlık
- Gıda

- Su
- Ulaşım
- Savunma
- Kamu güvenliği
- Nükleer, biyolojik, kimyasal ve radyoaktif maddeler

şeklinde tarif edilmiştir. Bu taslakta [106], 'Türkiye'de devletin öncülüğünde gerekli adımların atılarak, siber saldırılara karşı kritik altyapıların dayanıklılığının ve sürekliliğinin temin edilmesi hedefler arasına konulmuştur. Ancak taslaktaki birçok önerinin aksine, 'Kritik altyapıları işleten kamu veya özel kurum ve kuruluşları, BT altyapılarını 2013 yılı sonuna kadar TS ISO IEC 27001 Bilgi Güvenliği Yönetim Sistemine uyumlu hale getireceklerdir' önerisi, kritik altyapılar için sadece 'TS ISO IEC 27001 Bilgi Güvenliği Yönetim Sisteminin' yer alması bakımından eksik kalmıştır. Fiziki iş süreçlerini yönetmekte DDS kullanan kritik altyapılar için önerilmesi ve dayandırılması gereken güvenlik yönetim sistemini tek başına TS ISO IEC 27001 olarak tarif etmek önemli bir eksiklik olacaktır. Nitekim Bölüm 5.'te tartışıldığı üzere, BT sistemlerinin aksine DDS sistemlerin kendi iş süreçleri ve risk sınıfına uygun olarak geliştirilen farklı güvenlik standartları bulunmaktadır. Dolayısıyla tüm kritik altyapılar için, başlangıç için olsa da, sadece TS ISO IEC 27001 standardını önermek, altyapı işletmeci ve düzenleyicilerde güvenlik yönetimi için yeterli şartın büyük ölçüde tamamlandığı algısını oluşturabilecektir. Bu sebeple, kritik altyapıları kendi içinde tasnif etmeden ortak bir standart ve/veya güvenlik kılavuzunun önerilmesi, yönetici boyutunda eksik tutum oluşması ve hatalı karar alınmasına yol açabilecektir.

Yukarıda da belirtildiği üzere ve batılı ülkelerde olduğu gibi, Türkiye'nin de kendi ulusal siber güvenlik stratejisini belirleyerek siber güvenliğin yönetim boyutundaki en önemli eksikliğini gidermesi gerekmektedir. Belirlenecek stratejide, kritik altyapılar tanımlanmalı ve bu altyapıları denetleyecek ve düzenleyecek kurum, kuruluş ve organizasyonlar belirlenmelidir. Strateji belgesinde, tek veya birkaç güvenlik standardına değinilmemeli, mevcut standartlar ve en iyi uygulamalar göz

önünde bulundurularak her sektörün kendi ihtiyaçları ve önceliklerine uygun standartların belirlenmesi veya oluşturulması önerilmelidir.

Bu çalışmanın önemli çıktılarından biri olarak, Türkiye özelinde saha uygulamaları ve gözlemlerinden yararlanarak ve diğer ülke uygulamalarını da dikkate alarak EK-3'te "Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi" sunulmuştur.

8.1.3. Altyapı yöneticileri

İşletme yöneticilerinin aldıkları kararlar kadar tutumları da işletme önceliklerinin belirlenmesinde, işletme politika, talimat ve prosedürlerinin oluşturulması ve uygulanmasında tayin edici öneme sahiptir.

İşletme yöneticileri için karar ve tutumları üzerindeki en önemli etmen şüphesiz ki piyasa şartları ve gereklilikleri ile sahip olunan imkânların sınırlarıdır. Siber güvenliğin bir işletme için ihtiyaç veya gereklilik haline gelmesi ve altyapısını bu ihtiyaca göre tasarlaması, işletmeyi güç durumda bırakan bir siber olayın meydana gelmesi gibi tetikleyici veya düzenleyici bir otoritenin şart koşması gibi zorlayıcı bir durum karşısında gelişecektir. Üçüncü bir ihtimal ise, hiçbir olumsuzluk veya zorlayıcılık olmadığı halde, yöneticilerin kendi bakış açıları gereği siber güvenliği öncelikleri arasına almasıdır. Ancak bir sektörün geneli için işletme yönetimlerini yatırıma ve sürekli denetlemeye zorlayacak etmen düzenleyici otoritelerin gerekliliklerdir. Benzer şekilde işletme yönetiminin tutumu ve kararları ise çalışanlar eliyle işletme ve teknik boyuttaki güvenlik gerekliliklerinin yerine getirilebilmesinin en önemli nedeni olacaktır. Bu bağlamda, teknik ve işletme boyutunda gerekli güvenlik şartlarının oluşturulabilmesi için yöneticilerin yapmasıönerilenler EK-4'te yer alan "Denetim Sistemi Kullanan Kritik Altyapılar İçin Kurumsal Siber Güvenlik Eylem Planı Önerisi" belgesinin ikinci başlığı olan "İşletme Yöneticileri İçin Öneriler" başlığı altıda topluca sunulmuştur.

8.1.4. Diğer paydaşlar

Yönetim boyutunda ele alınması gereken diğer paydaşlar ise altyapı ve teknoloji üreticileri, yükleniciler ve dış kaynak destek sağlayıcılardır.

Altyapı ve teknoloji üreticileri, ürünlerini sattıkları işletmecilerin isteklerine ve dolaylı olarak da düzenleyicilerin gerekliliklerine uygun ürün ve teknoloji tasarlamak durumundadırlar. Altyapı işletmecileri düzenleyici otoritenin isteklerini karşılayamayan ürünleri alamayacağından, üreticiler de düzenleyici gerekliliklerine uygun ürünleri tasarlamak zorunda kalacaklardır.

Otomasyon ürünlerini geliştiren ve üretenler hem güvenlik konusunda uzman üreticiler olmadıklarından hem de rekabet edebilmek için ucuz çözümler sunmaya çalışacaklarından, farklı kaynaklardan toplanmış hazır ürünleri ve güvenlik mekanizmalarını kullanmak isteyeceklerdir. Benzer şekilde, sistem entegratörleri de kendilerinden beklenen güvenlik gereklilikleri sağlamak için farklı üreticilerin ürettikleri ve mevcut BT pazarı için hazırlanmış farklı üreticilere ait ürünleri kullanma yoluna gidebileceklerdir [99]. Bugünkü piyasa şartları otomasyon üreticilerini BT tabanlı hazır ürünleri ve beraberinde hazır güvenlik çözümlerini kullanmaya zorlasa da, hem SCADA/DDS sistemlerinin gerçek zamanlılık ve hatasız-sürekli çalışırlık kriterine hem de bu bölüm içindeki teknik güvenlik boyutu başlığı altında tartışılan gerekliliklere uygun ürünlerin üretilmesine ve entegrasyonuna ihtiyaç vardır.

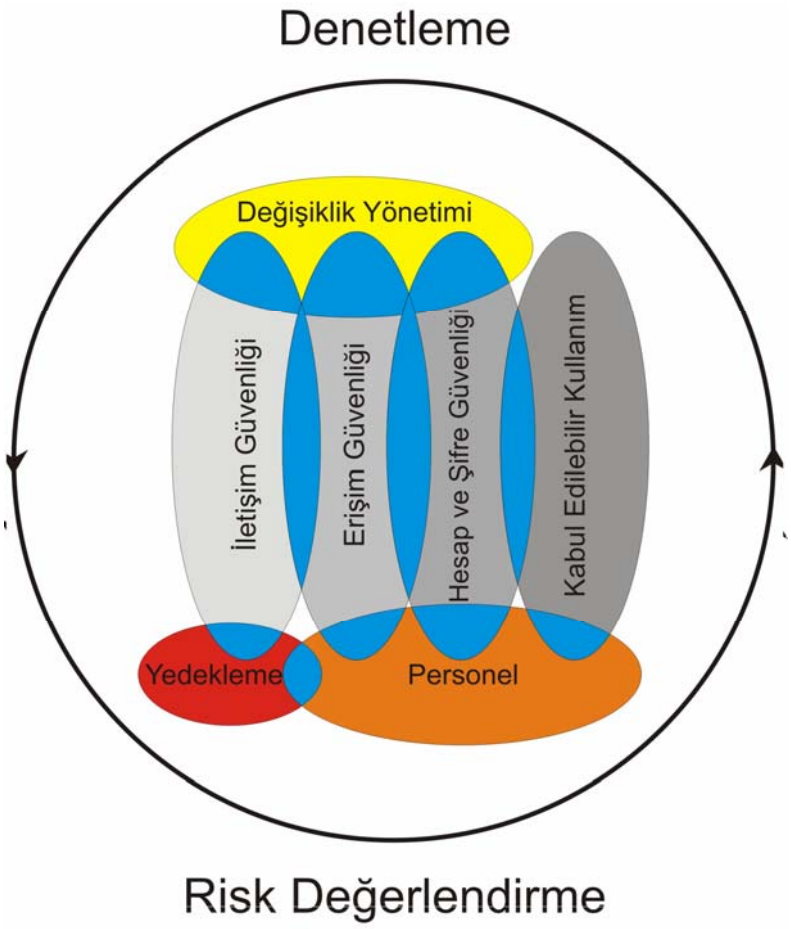
Son olarak yükleniciler ve dış destek sağlayıcılar, altyapı işletmecisiyle yaptığı anlaşmalara uygun şekilde hizmet vermek ve onların hizmet alımına şart koyduğu hususları yerine getirmeye zorunda olan taraflardır. Bu sebeple, işletmecinin şart koşması halinde siber güvenlik kriterlerine ve yazılı güvenlik belgelerine uygun davranmak zorunda kalacaklardır.

8.2. İşletme Boyutu

İşletme boyutunda, yönetim boyutundaki karar, öncelik, tutum ve yaklaşımlara uygun olarak oluşturulacak ve uyulacak yazılı güvenlik kuralları (politikaları) yer alır. Oluşturulan kurallara ise uygun teknolojiler kullanılarak ilgili çalışanlarca uygulanır ve diğer çalışanlar ise bu kurallara uygun olarak işlerini yaparlar. Şayet yönetim boyunda siber güvenlik ele alınmamışsa, işletmenin kendi güvenlik politikaları oluşturması ve onlara uygun olarak iş süreçlerini devam ettirmesi çoğu durumda mümkün olmayacaktır.

İşletmelerin güvenlik ihtiyacının karşılanması için en önemli unsur, sistem işletimi için kuralların, çalışanların görev, yetki tanım ve kısıtlamalarının önceden belirlenmiş kaidelere göre yapılmış olmasıdır. Bazı işletmelerde, işletme kural ve kaideleri herkesçe bilinmesine rağmen yazılı bir metne dayanmamaktır. Zira ortada işletme ve güvenlik konularında hazırlanmış yazılı metinlerin olmaması bir işletmeninin hiçbir güvenlik kural ve kaidesine sahip olmadığı anlamına gelmemekle birlikte, bu şartlarda sürdürülebilir bir güvenlik yapısının oluşturulabilmesiniimkânsızhale gelmektedir. Başka bir bakış açısıyla, işletim ve güvenlik politika ve prosedürleri yazılı metne dayanmayan işletmelerin, iş süreçlerini daha hızlı ilerletebilme ve daha hızlı karar alma gibi avantajlara sahip olabildikleri ileri sürülebilecektir. Ancak özelikle kritik altyapı işleticilerinin bilgi ve denetim sistemlerine erişim, kullanım ve değiştirme gibi eylemleri ve planları yazılı bir metne dayandırmaları ve sürekli başvurulan kontrol listeleri oluşturmaları bir zorunluluk olarak ortaya çıkmaktadır.

BT ve DDS sistemlerine sahip işletmecilerin, oluşturulmaları ve uyulmaları gereken en önemli politikalar ve bu politikaların birbirleriyle ilişkileri Şekil 8.4.'te gösterilmiştir.



Şekil 8.4. Güvenlik politikaları ve birbirleriyle ilişkileri

Şekil 8.4.'te gösterilen ve aşağıda tartışılan güvenlik politikalara uygun ve ilave olarak işletme boyutunda hazırlanması gerekenler 'İş Sürekliliği ve Felaket Kurtarma', 'Siber Olaylara Müdahale' ve son olarak 'Eğitim' planlarıdır.

Güvenlik politikalarının etkin olarak hayata geçirilmeleri, var olan veya oluşturulacak altyapı ve bileşenlerinin bu politikalarda tanımlanan kuralların gerçekleştirilebilmesi için elverişli olmalarına bağlıdır. Bunun için güvenlik politikaları geliştirilirken var olan altyapının sağlayabildiği fonksiyonlara uygun olmalı; altyapı tasarımı veya güncellemelerin de uygulanması öngörülen politikalar için gerekli imkânları sağlayıp sağlamadığı mutlaka kontrol edilmelidir. Örneğin tek tip kullanıcı hesabı sağlayan bir bileşende, farklı kullanıcı gruplarına göre tasarlanmış hesaplar oluşturma imkânı olmayacaktır.

8.2.1. Erişim denetimi politikası

Erişim denetimi, belli bir varlığa sadece yetkili kişi veya grupların tanımlanan haklar dahilinde erişebilmesini sağlamak amacıyla uygulanır. Bu erişim fiziksel olabileceği gibi bir bilgi varlığına bilgisayar aracılığıyla yapılan mantıksal bir erişim de olabilir [107].

Erişim denetimi, ISO/IEC 27002 [55] belgesinde yer alan aşağıdaki alanlar için uygulanabilir.

I. *Fiziki erişimi:* Doğrudan ağ veya sistem bileşenlerinin olduğu fiziki ortama erişim
II. *Ağa erişimi:* Ağ cihazlarına veya kablolu/kablosuz iletişim ortamlarına erişim
III. *Sisteme erişim:* Sunucu, istemci veya RTU/PLC türü cihazlarının işletim sistemlerine erişim
IV. *Uygulama erişimi:* Bir işletim sistemi üzerindeki uygulamaya erişim
V. *Fonksiyon çalıştırma:* Bir uygulamanın sağladığı fonksiyona erişim

İşletmede kullanıcıların üstlendikleri rol ve sorumluluğa bağlı olarak erişim haklarının nasıl belirleneceği bu politika içinde yer alır. Bu itibarla erişim denetimi kullanıcılarının sahip oldukları hesap bilgileriyle de doğrudan ilişki içindedir. Sadece kullanıcıların değil, cihaz, servis ve uygulamaların birbirine erişimini de tanımlanması ve denetlenmesi gerekenler arasındadır.

Erişimin etkin denetlenebilmesi için aşağıdaki temel işlevlerin gerçekleştiriliyor olması gerekir [107].

- Kimlik doğrulama ile sisteme hangi kullanıcıların giriş yapabileceğinin belirlenmesi,
- Yetkilendirme ile kullanıcıların hangi işlemleri yapmaya veya hangi varlıklara erişmeye yetkili olduğunun belirlenmesi,
- İzlenebilirlik ile kullanıcıların sistemde hangi işlemleri yaptıklarının veya hangi bileşene erişebildiklerinin bilinmesi ve gözlenebilmesi.

Erişim denetimi politikası, kullanılan sistemlere uygun olmalıdır. Zira kullanılan cihaz, yazılım ve sistemler erişimi denetleme, kimlik doğrulama ve takip fonksiyonlarını, politikada tanımlandığı şekliyle gerçekleştiremiyorsa, tanımlanan politikanın uygulanamaması veya başka bir ifadeyle ihlali durumu ortaya çıkacaktır.

8.2.2. Hesap ve şifre yönetimi politikası:

Kullanıcı hesaplarının nasıl oluşturulacağı ve şifre kullanımı hakkında kurallar içerir. Bu nedenle öncelikle kullanıcı türlerinin ve her kullanıcı türünün sahip olacağı haklarının hazırlanacak politikada yer alması gerekir.

Hesap yönetimi, kullanıcıların sistemde hangi uygulama ve fonksiyonlara erişebileceklerine ve kullanabileceklerine bağlı olarak yürütülür. Her bir kullanıcıya kendisine açılan hesaplara erişmek için şifre kullandırılmalıdır. Şifrelerin nasıl seçileceğine ilişkin kriterlerin ve şifre ömürlerinin hazırlanacak politika ile belirlenmesi gerekir.

Hesap ve şifre yönetimi politikasında, kullanıcı hesaplarını kimlerin açması veya kapatması gerektiğinin tanımlanması gerekir. Ayrıca hesap verebilirlik adına kullanıcı hesaplarının kişiye özel olarak açılması, zaman aşımı, bağlantı limiti gibi güvenlik gereklilikleri de bu politika içinde tanımlanmasına ihtiyaç vardır [108].

8.2.3. Kabul edilebilir kullanım politikası

Çalışanların kullanımına sunulan, internet ve intranet ağlarını, bilgisayarlar ve üzerindeki her türlü uygulamayı, veri saklama ünitelerini, giriş/çıkış kartı, e-posta, sistem ve uygulamalara erişim sağlayan her türlü hesaplarını nasıl kullanmaları gerektiği tanımlayan politikadır [109].

Kapsamlı bir kabul edilebilir kullanım politikası oluşturabilmek için farklı kullanıcı türlere sağlanan her türlü imkâna ilişkin kullanım şeklinin tarif edilmesi gerekir. Ayrıca, misafirlerin, alt yüklenici veya dış kaynak destek personelinin hangi araç ve

uygulamaları ne şekilde ve gerekiyorsa kimlerin refakatinde kullanması gerektiği politikaya dahil edilmelidir.

DDS altyapısında bulunan varlık ve kullanıcılar için kabul edilebilir kullanım politikası ayrıca veya ek olarak hazırlanmalıdır. Politika hazırlanırken aşağıdaki hususlarında yer alması sağlanmalıdır.

Kritik işlev gören veya bilgi barındıran BT ve DDS yazılım, donanım ve ağlarına bir şekilde erişim sağlanmış olsa dahi yetkisiz personelce müdahale edilmesi kesinlikle yasaklanmadır.

Taşınabilir her türlü diskin ve modemlerin (GSM, GPRS, 3G modem) DDS yazılım, donanım ve ağlarında kullanımı yasaklanmalıdır. Şayet yetkili personelce güncelleme, yamalama, yedekleme gibi maksatlarda geçici olarak kullanım zorunluluğu oluşuyorsa, hangi hallerde kimler tarafından ne şekilde kullanılabilecekleri ilgili politikalar içinde yer almalıdır.

Yetkili kişilerce dahi DDS ağı içinde mümkünse taşınır bilgisayarlar kullanılmamalıdır. Bakım, arıza tespit ve giderim gibi nedenlerle kullanılan taşınır bilgisayarların diğer zamanlarda internete bağlanması kesinlikle yasaklanmalı ve bu bilgisayarlar üzerinde gerekli bakım ve güncelleme programları haricinde uygulama bulundurmaması sağlanmalıdır. Bu bilgisayarlara dış ortamlardan kötücül yazılımların bulaşabileceği ihtimali sürekli dikkate alınmalıdır.

Son olarak, kabul edilebilir kullanım politikasının etkin uygulanabilmesi, sistemin yanlış kullanımları engelleyecek biçimde tasarlanmasına bağlıdır. Aşağıda buna örnek bir uygulama önerisi yer almaktadır.

İzleme ve kumanda salonlarında SCADA/DDS uygulamalarına bağlanmak için monitör ve klavyeden olaşan terminaller kullanılmalı, sunuculara bağlantı için kullanılan bilgisayar ayrıca kapalı bir odada, izleme ve kumanda operatörlerin erişimi dışında olmalıdır. Böylece doğrudan DDS uygulama ve ağına bağlanan

bilgisayarların harici modemler ile internete bağlanabilmesi veya onlara taşınabilir disklerin takılması önlenmiş olacaktır.

Kabul edilebilir kullanım politikasının açık ve anlaşılır şekilde hazırlanmasının, kullanıcılara imza karşılığında elden dağıtılmasının, denetlenmesinin ve ilgili kullanıcı grubuna özgü olarak belirli aralıklarla bilgilendirme toplantıları yapılmasının, hazırlanacak politikanın etkin hale gelmesi ve ihlallerin engellenmesi açısından önemli olduğu değerlendirilmektedir.

8.2.4. Personel politikası

Personel politikası, personelin seçimi ve işe alımı, yetki ve sorumluluklarının belirlenmesi, diğer politikalara uygun davranıp davranmadığının denetlenmesi ve eğitimi olmak üzere farklı başlıkta oluşturulabilir.

Personel politikasına, şayet varsa kritik iş süreçlerinde yer alan alt yüklenici ve dış kaynak destek personelleri de dahil edilmelidir. Hazırlanacak politikada, hangi iş tanımları için hangi nitelik ve yetkinlikte personelin seçileceği, görev ve sorumluluklarının neler olacağı belirlenmelidir. Ayrıca personel alımlarında, çalıştırılacak personelin kendi rol ve sorumluklarını anlayabilecek ve görevlerini yerine getirebilecek düzeyde olması aranmalıdır. Kritik işler için çalıştırılacak kişilerin güvenlik soruşturmasının yapılması ve çalışan personelin iş akdinin fes edilmesi sonrasında tanımlı tüm erişim yetkilerinin ve hesap bilgilerin sonlandırılması hususları politika da yer almalıdır [110].

Önemli iş süreçlerinde yer alan veya kritik sistemlerin işletilmesi ve yönetilmesinden sorumlu olan personelin yedeklenmesi veya yokluğunda işlerini devam ettirebilecek başka personellerin yetiştirmesi, önemli personellere ilişkin öncelikler arasında yer almalıdır. İşletme için hassas bilgilere erişimde teknik imkânlardahilinde giriş yetkileri ikili veya üçlü (iki veya üç kişinin birlikte) onaylama mekanizmalarına dayandırılmalıdır.

Personelin, kabul edilebilir kullanım politikası başta olmak üzere diğer tüm politikalara uygun davranıp davranmadığı gözlenmeli veya denetlenmeli, politikalara uymama durumu müeyyidelere bağlanmalıdır.

Son olarak, hangi personelin ne tür eğitim ve sertifikasyon süreçlerine dahil edileceği, yıllık eğitim planlarının nasıl hazırlanacağı ve sosyal mühendisliğe karşı farkındalık ve bilinçlendirme faaliyetlerinin nasıl yürütüleceği personel politikasında tanımlanmalıdır.

8.2.5. Yedekleme politikası

İşletilen sistemlerin maruz kalacağı doğal bir afet, uğrayacakları saldırılar veya oluşabilecek kazalar karşısında etkisiz hale gelen işlevlerini yerine getirecek alternatiflerin hazır bulundurulması, iş sürekliliğini garanti altına alacak ve bu sayede güvenlik risklerini indirgeyecektir. Her türlü yedeklilik kuşkusuz ki işletmeler için ilave maliyet de oluşturacaktır.

Yedekleme politikası, hangi varlıkların nerede, ne şekilde yedekleneceğine ilişkin hususların yer alacağı güvenlik politikasıdır. BT sistemleri için yedekleme denildiğinde öncelik verilerin yedeklenmesi ise de DDS sistemler için yedeklilik önceliği çoğunlukla iş süreçlerini yerine getiren altyapı bileşenlerine göre şekillenecektir.

Aşağıda yedekleme politikasında bulunması gereken başlıklar yer almaktadır.

- Kritik uygulamaların çalıştırıldığı sunucuların yedeklenmesi,
- Sistemleri besleyen enerji birimlerinin yedeklenmesi,
- Yük, kullanım gibi değerin kestirimi ve denetleme için kullanılacak geçmiş durum ve kullanım bilgileri, alarm ve log kayıtlarının yedeklenmesi,
- Sahada kullanılan uç birim cihazlar (PLC/RTU) için yedek parça ve cihaz bulundurulması,

- İletişim birimleri için parça, kart ve cihaz bulundurulması,
- Ana bölgeler için kablolu veya kablosuz iletişim hatlarının yedeklenmesi (İletişim Güvenliği Politikasına uyumlu olarak),
- Uygulama yazılımı, geçmiş ve bugünkü konfigürasyon dosyaları ve kural setlerinin yedekliliği (Güncelleme ve Değişiklik Yönetimi politikasına uyumlu olarak),
- Kritik personelin yedeklenmesi (Personel güvenliği politikasına uyumlu olarak).

Yukarıda sıralı maddelerden de anlaşılacağı üzere (son üç madde), yedekleme politikasının diğer güvenlik politikaları ve planlarıyla (iş sürekliliği ve felaket kurtarma gibi) uyumlu olması gerekir. Özellikle felaket kurtarma için yedeklemelerin nerede yapıldığı ve yedeğin nasıl kullanılacağı konusu ayrıca önem taşımaktadır.

Yedek bulundurma kapasitesinin ne kadar olacağı doğal olarak işletmelerin ayırabileceği bütçe ile doğrudan ilişkilidir. Bu nedenle, yedekleme politikasında yer alacak yedekleme kapasiteleri (kaça kaç yedekleneceği) işletmelerin yatırım imkânlarına göre değişiklik gösterebilecektir.

8.2.6. Güncelleme ve değişiklik yönetimi politikası

Güncelleme ve değişiklik yönetimi, özellikle kritik BT ve DDS sistemleri için çok aşamalı bir süreçtir. Bu aşamalar arasında, değişiklik talebi ya da gerekliliğinin tanımlanması, değerlendirilmesi, onaylanması, planlanması, uygulanması ve test edilmesi gibi süreç parçaları yer almaktadır [111]. Yapılacak herhangi bir değişiklik, ağ ve sistemde yeni bir açıklığa da neden olabileceğinden uygulanmadan önce iyi değerlendirilmesi ve kontrol edilmesi gerekir [108,112].

Güncelleme ve değişiklik politikası hazırlanırken aşağıda tanımlanan tüm değişikliklere ilişkin hususları kapsamalıdır.

- Güvenlik duvarı ve saldırı tespit sistemleri de dâhil her türlü ağ ve sistem bileşenlerinde kullanılan kural setlerinin değiştirilmesi,
- Sistem yapılandırma bilgilerinin değiştirilmesi,
- Kullanılan uygulamaların veya sürümlerinin güncellemeleri,
- Önemli uygulamaların çalıştığı işletim sistemlerinin güncellenmesi ve yamalanması,
- RTU/PLC gibi birimlerin gömülü işletim sistemlerinin güncellenmesi,
- Kullanılan donanımların değiştirilmesi, üzerine kart/port ilaveleri yapılması,
- Kullanılan her türlü donanımın BIOS güncellemelerinin yapılması,
- Kullanılan iletişim ortamının (kablolu, kablosuz), tekniklerinin (xDSL, FR, Metroethernet, GPRS, EDGE, 3G) değiştirilmesi veya topolojisinin değiştirilmesi.

Kullanılan donanım, yazılım veya servisler üzerinde yapılacak her türlü değişiklik ve güncellemelerin beklenmedik problem ve açıklıklara sebebiyet vermesi her zaman olası bir durum olarak göz önünde bulundurulmalıdır. Merkezi bir onay sürecinden geçmeyen her türlü değişiklik diğer güvenlik politikalarının (erişim denetimi, iletişim güvenliği gibi) ihlal edilmesine de sebep olabilecektir.

Güncelleme ve Değişiklik Yönetimi politikası, değişiklik sonrası beklenmeyen durumlar karşısında geriye dönüşü mümkün kılacak biçimde hazırlanmalıdır.

8.2.7. İletişim güvenliği politikası

İşletmelerin dışarıdan gelecek siber saldırılara karşı korunması bağlamında en önemli politikalardan biri ‘İletişim Güvenliği’ politikasıdır. İletişim güvenliği politikası, altyapı üzerinden gönderilecek ve alınacak veri ve komutların hangi iletişim ortamlarından ve birimlerinden nasıl geçeceğini, hangi güvenlik mekanizmalarının kullanılacağını, ağın ne şekilde bölümleneceği ve hangi güvenlik alanlarının oluşturulacağını konularını içerir [108**].**

Aşağıda iletişim güvenliği politikasında, güvenlik bölgelerine göre ayrı ayrı tanımlanması gerekebilecek başlıca hususlar maddeler halinde sunulmuştur.

- Kullanılacak iletişim ortamı ve tekniklerinin tanımlanması,
- Topolojinin çıkarılması ve varsa ağlar arası geçişlerin işaretlenmesi,
- Kullanılmasına izin verilecek iletişim protokollerin (Modbus, DNP3, HTTP SFTP gibi) önceden belirlenmesi,
- Ağ trafiğinin ve ağda geçen protokollerin izlenmesi, ani artış ve düşüşlerin raporlanması, ilgililerine haber verilmesi (saldırı tespit sistemi kullanımı),
- Şifreli veri akışı için kullanılacak şifreleme tekniklerinin ve güvenlik mekanizmalarının belirlenmesi ve uygulanması,
- Ağa bağlanabilirlik için asgari şartların belirlenmesi (MAC, IP temelli kontrolleri gibi)
- Adres ve protokol temelli güvenlik filtrelerinin kullanımı (Güvenlik duvarı kullanımı)
- Ağda kullanımına izin verilecek çözümleme protokollerinin (DNS, ARP, BOOTP, NetBIOS gibi) tanımlanması,
- Ağ cihazlarındaki kullanılmayan portların durumu,
- Kesinti durumda yedeklerin ve alternatif güzergâhların nasıl kullanılacağının belirlenmesi,
- (Şayet kaçınılmaz ise) Dış erişimlerin hangi durumlarda, kimlere, nereden ve hangi kontroller sağlanarak açılacağı.

Kritik altyapılarda kullanılan SCADA/DDS denetim ağının hiçbir suretle internete fiziki bağının olmaması ve dış erişimlere tamamen kapalı olması gerekir. Ağ varlıklarının birbirlerine erişimi önceden tanımlanmış kurallara göre yapılmalı ve mutlaka izlenmelidir. Ayrıca, güvenlik duvarları seçiminde endüstriyel iletim protokollerini tanıması ve bu sayede sadece adres ve port temelli değil fonksiyon (komut) bazlı filtrelemelerde uygulanabilmelidir.

8.2.8. Denetim politikası

Buraya kadar incelenen güvenlik politikalarına uyulup uyulmadığının denetlenmesine ilişkin hususları içeren politikadır.

Denetim politikasında, işletmenin kimler tarafından hangi aralıklarla denetleneceği, denetleme kapsamında nerelerin inceleneceği ve değerlendirileceği, denetim raporlarının kimlere sunulacağı bilgileri de yer almalıdır. Şayet işletmede, tanımlı güvenlik politikalarının ihlali söz konusuysa bunların denetim raporlarında sunulması gerekir. Etkili bir denetim için sadece yazılı belgelerin değil, farklı sistemlere ilişkin log kayıtları da dâhil yerinde teknik incelemelerin yapılması gerekmektedir.

8.2.9. Risk değerlendirme

Hangi güvenlik iyileştirmelerinin öncelikli olduğu, yapılacak risk değerlendirme çalışmaları neticesinde belirlenecektir. Bölüm 3.'teyer aldığı ve Bölüm 7.'de önerildiği üzere farklı güvenlik riski değerlendirme yöntem ve yaklaşımları mevcuttur. Risk Değerlendirme politikası, hangi yöntemle ve sıklıkla risk değerlendirme çalışmalarının yürütüleceği belirleyen politikadır.

8.3. Teknik Boyut

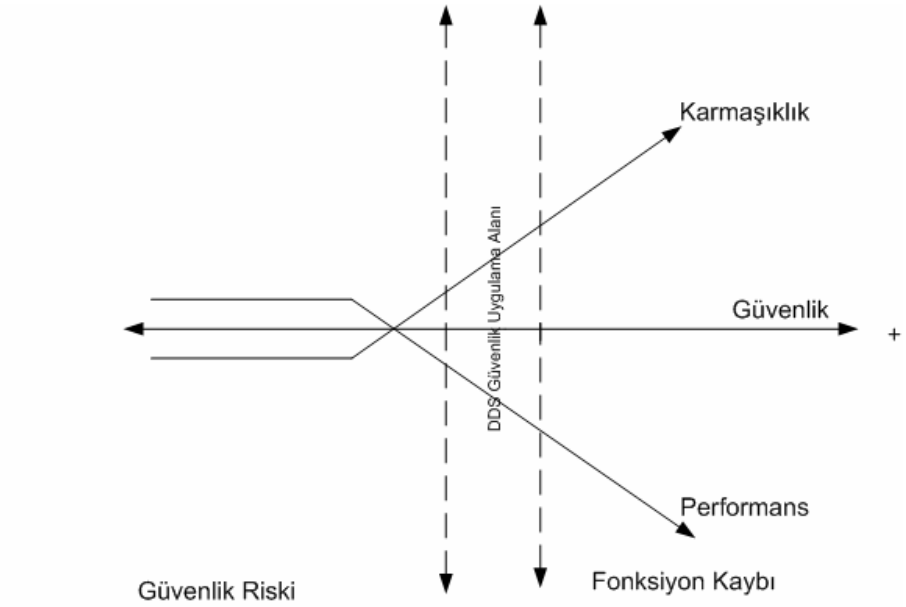
Gelişen ve ucuzlayan bilişim ve iletişim teknolojileri sayesinde, DDS merkez ve uç birim bileşenlerde, standart bilgisayar donanımları ve yazılımları kullanılmaya başlanmış ve bu durum SCADA/DDS sistemler için daha önce geçerli olmayan yeni siber tehditlerin ortaya çıkmasına neden olmuştur. Ayrıca, internetin ve mobil erişim tekniklerinin yaygın kullanımı ile SCADA/DDS mimarileri bu erişim kolaylığı ve çeşitliliğinden daha fazla etkilenmeye başlamıştır [6,7,10].

Teknik boyutta işletmecilerce benimsenmesi ve takip edilmesi gereken güvenlik yaklaşımlarına ve kullanılacak iyileştirme adımlarına ilişkin temel prensipler şu şekilde olmalıdır:

I. Karmaşıklığı Engelleme: İyileştirme adımları, uygulanamaz, uygulansa da sürdürülemez ölçüde zorluk ve karmaşıklığa sahip olmamalıdır.

II. Performansı Koruma: Uygulanan güvenlik iyileştirmeleri sistem performansını (gerçek zamanlılık ve sürekli kullanılırlık) kabul edilebilir değerlerin altına düşürmemelidir.

DDS yapıların teknik boyutta güvenlik iyileştirmelerinin, yukarıda ifade olunan iki prensibi dayanarak Şekil 8.5.'te gösterildiği gibi kabul edilemez karmaşıklığa ve performans kayıplarına neden olmayacak ölçüde mevcut yapılar için de *uyumlu* ve *uygulanabilir*, saha gerçekleri ve ihtiyaçlarıyla da *uygun* olacak biçimde belirlenmesi ve tasarlanmasına ihtiyaç vardır.



Şekil 8.5. DDS güvenlik uygulama alanı tanımı

Aşağıda, yukarıda ifade edilen prensiplere uygun olarak,DDS altyapı ve bileşenlerinin karşı karşıya olduğu bugünkü tehditlere karşılık teknik boyutta alınabilecek tedbirler ve iyileştirme önerileri araştırmacı, üretici ve işletmeci bakış açılarıyla tartışılmıştır.

8.3.1. İşletim sistemi güvenliği

Her ne kadar son dönemde değişmeye başlasa da DDS uç birimlerinde kullanılan geleneksel RTU türü cihazlarda çoğunlukla gerçek zamanlı denetim fonksiyonlarına barındıran gömülü işletim sistemine sahiptirler [113]. Bu cihazlar, genel amaçlı işletim sistemlerine kıyasla daha az güvenlik fonksiyonlarına sahip olmalarına karşın mikro çekirdek mimariye sahip olduklarından daha az güvenlik açığı barınmaları beklenen bir durumdur.

DDS merkez biriminde ise çoğunlukla üzerinde Unix veya Microsoft Windows gibi genel amaçlı işletim sistemi bulunan sunucu bilgisayarlar bulunmaktadır. Geçmişte, SCADA/DDS uygulamalarının çalıştığı merkez birim sunucularında çoklu görev yeteneğine sahip UNIX işletim sistemleri kullanılırken, günümüzde daha çok Microsoft Windows işletim sistemlerinin olduğu görülmektedir. Ayrıca, maliyet avantajı sağlayan ve Unix tipi özelliklere sahip olan Linux işletim sistemleri de ciddi bir alternatif olarak kullanılmaya başlamıştır [6].

Unix ve esasen Unix türevi olan Linux, çok işlemli ve çok kullanıcılı bir işletim sistemleridir. Ancak yürüttükleri her bir süreç için sistem kaynaklarını zamana göre paylaştırdıklarından ötürü gerçek zamanlı işletim sistemi sınıfına girmemektedirler. Bu sebeple Unix ve Linux türü işletim sistemlerinin zaman paylaşımlı süreç yönetimi, DDS sistem uygulamaları için engel olarak görülmektedir [114]. Ancak günümüzdeki farklı Unix türleri ve Linux dağıtımları için gerçek zamanlı süreç yönetimi fonksiyonları eklenmektedir.

Bilgisayar donanım maliyetlerinin düşmesiyle birlikte, günümüz DDS uç birim bileşenleri için de geçmişe oranla yüksek işlem kapasitesine sahip hazır donanımlar

üzerinde Microsoft Windows veya Linux gibi genel amaçlı işletim sistemleri kullanılmaya başlanmıştır. Gömülü işletim sistemlerine göre çok daha fazla çekirdek kodu ve servis içeren bu işletim sistemleri, DDS sistemler için ciddi tehdit oluşturmaktadır [78].

Genel amaçlı işletim sistemleri ve onların açıkları hakkında internet ortamında birçok bilgi ve belge bulunmak mümkündür. Ayrıca bu tür işletim sistemlerine yönelik olarak hazırlanan virüs, solucan, truva atı ve diğer zararlı kodların fazla ve yaygın oluşu nedeniyle DSS altyapısında genel amaçlı işletim sistemi kullanımı güvenlik riskini oldukça arttırmaktadır.

Saha gerçekleri göstermektedir ki çoğunlukla ekonomik nedenlerle endüstrideki SCADA/DDS uygulama ve sistem geliştiricileri özellikle merkezde çalışacak uygulamalarını genel amaçlı işletim sistemlerine göre tasarlamakta ve derlemektedir.

Endüstrideki çoğu mikro kontroller veya mikro çekirdek tabanlı cihazlar genel amaçlı işletim sistemlerine oranla çok kısıtlı fonksiyonlar sunmakta olup adapte olma ve yeniden yapılandırılma kapasiteleri de oldukça sınırlıdır [115]. Bu nedenle bu tür cihazlar da günümüzde gerekliliğine dönüşmüş olan iletişim protokollerini ve güvenlik fonksiyonlarını destekleyemez durumdadırlar. Diğer taraftan merkezde kullanılmak durumunda kalan genel amaçlı işletim sistemleri de mikro çekirdek mimarisindeki işletim sistemleriyle kıyaslanamayacak ölçüde güvenlik açıklıkları barındırmakta ve bu açıklıkların neler olduğuna internet ortamından kolaylıkla erişilebilmektedir. Bu durumda, iki taraflı problemin çözümü için iki öneri getirilebilir. Bunlar:

1. Öneri: Merkezdeki genel amaçlı işletim sistemlerinin sıkılaştırılması ve korunması
2. Öneri: Sahadaki uç birim cihazlarının yeterli güvenlik fonksiyonlarını sağlayan ek geçit cihazlarla birlikte kullanımı.

Birinci iyileştirme önerisi, genel amaçlı işletim sistemi kullanımından kaynaklı tüm problemleri gidermemekle birlikte, mevcut durumun iyileştirilmesi bakımından

oldukça önemlidir. İkinci önerinin uygulanabilmesi ise ek maliyet ve uyumluluk testlerinin mecbur hale getirmektedir.

DDS uygulamasının bulunduğu ticari veya açık kaynak kodlu işletim sistemleri üzerindeki kullanılmayan her türlü ağ servisi kapatılmalıdır [112]. Dışarıdan yapılacak taramalara karşılık TCP/IP parmak izleri kaldırılmalı veya tarayanları aldatacak şekilde değiştirilmelidir [116-117].

Kullanılmayacak servis ve uygulamalara ilişkin ön tanımlı olarak yüklenen çekirdek modülleri, sürücüler kaldırılmalı, her türlü izinler baştan düzenlenmeli ve sadece çalışacak uygulamanın kullanacağı modül ve servisler açık bırakılmalıdır. NSA başta olmak üzere çeşitli kaynaklarda farklı işletim sistemlerine ilişkin çok ayrıntılı sıkılaştırma yöntem ve rutinleri yer almaktadır [118].Ancak sıkılaştırma öncesi doğrudan ve bağımlı servis, modül, sürücü gerekliliklerin titizlikle tespit edilmesi, mümkünse uygulama üreticisiyle birlikte ve yedek sistemler üzerinden başlayarak sıkılaştırmalar gerçekleştirilmelidir.

DDS uygulamalarının koştuğu işletim sistemlerinde, çalışan sistemin performansına etki edebileceği düşüncesiyle, kullanılan işletim sistemlerinin yamalanması, anti-virüs/casus yazılımlarının yüklenmesi göz ardı edilmektedir. Radikal yamalama ve güncellemeler, anti-virüs kullanımları üreticiye sorularak ve yük altında olmayan yedek sistemlerden başlanarak yapılmalıdır. Aksi halde kötücül yazılımlardan korunmak için test edilmeden kullanılan güvenlik yazılımları denetim sistemlerinin performansı üzerinde olumsuz etkiler oluşturabilecektir [119].

İkinci öneri ‘İletişim Güvenliği’ başlığı içerisinde ayrıca tartışılacaktır.

8.3.2. DDS uygulama yazılımlarının seçimi

Sanz ve Arzen’e göre, DDS sistemlerde kullanılacak süreç yönetimine ilişkin denetim uygulamalarının sahip olması gereken özellikleri aşağıdaki gibi tanımlamıştır[6].

- *Zaman Kritik Süreç Yönetimi:* Yazılımlar yüksek performanslı olmalı ve gerçek zamanlı süreçlere göre tasarlanmalıdır.
- *Gömülülük:* Yazılımlar, kısıtlı işlem kaynağına sahip platformlar üzerinde çalıştırılabilmeli ve harici çevre birimleriyle etkileşime geçebilmelidir.
- *Hata Toleransı:* Yazılımlar, sistemde bir hatanın meydana gelmesi durumunda da belirli bir performansta çalışmaya devam edebilmelidir.
- *Dağıtıklık:* Yazılım bileşenleri dağıtık olmalı ve farklı bileşenler farklı bilgisayarlar üzerinde ortak bir işlemi yürütme özelliği olmalıdır.
- *Açıklık:* Yazılımlar, kapalı olmamalı ve farklı uygulamalarla birlikte kullanılabilmelidir.
- *Heterojenlik:* Yazılımlar, farklı işletim ortamlarında çalıştırılabilmelidir.

DDS uygulama yazılımlarında ayrıca;

- Uçtan uca şifreli veri taşıyan ve bütünlük kontrolleri gerçekleştiren iletişim protokollerin yer alması,
- Farklı kullanıcı rollerine uygun olarak servis ve fonksiyonlara erişimimkânını sağlamaları,
- Girişlerin doğruluğunu ve bütünlüğünü denetlemeleri,
- Farklı işletim sistemleri üzerinde kullanılabilir dağıtımlarının bulunması

gibi şartlar aranmalıdır.

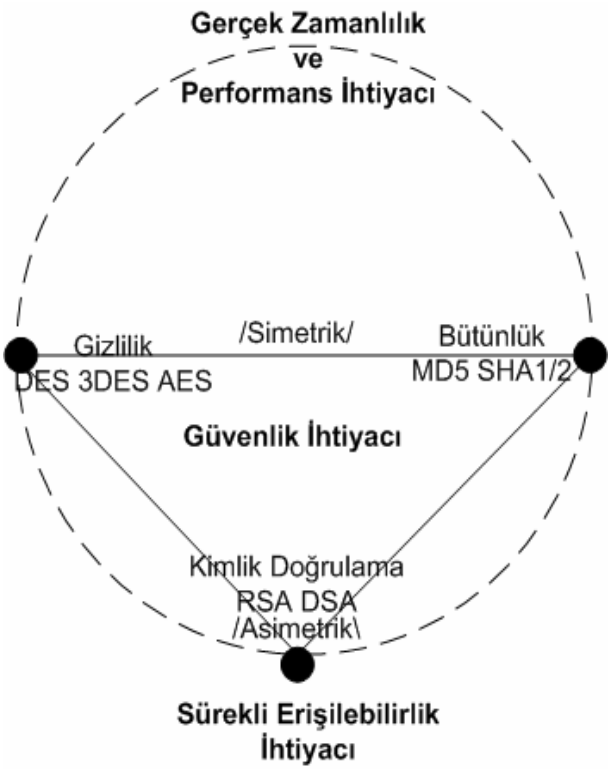
Yukarıda verilen özelliklere sahip uygulama yazılımlarının kullanımı daha güvenli DDS altyapı tasarımı ve uygulamaları açısından önemlidir. Ancak işletmeci perspektifinden, yukarıdaki sayılan tasarım özellikler ancak alım aşamasında gözetilecek kriterler olarak değerlendirilebilir.

8.3.3. İletişim protokolü güvenliği

İki uç birim arasındaki veri haberleşmesinde güvenliğin sağlanabilmesi için, öncelikli olarak kimlik doğrulama ile karşılıklı tarafların birbirini doğrulaması, sonrasında uçlar arası iletilen verinin gizliliğinin ve bütünlüğünün sağlanması

gerekmektedir. Ancak gerçek zamanlı olarak sürekli haberleşme ihtiyacı duyan sistemler için güvenlik ihtiyacının gerçek zamanlılık ve sürekli erişilebilirlik ihtiyaçlarını da ihlal etmemesi gerekir.

Şekil 8.6.'da kritik altyapılarda kullanılan DDS sistemlerinin bu üç ihtiyacı birlikte gösterilmiştir.



Şekil 8.6. Denetim sistemlerinin güvenlik, gerçek zamanlılık ve sürekli erişilebilirlik ihtiyacı

DDS ağlarının fiziksel olarak diğer ağlardan izole olduğu; internetin ve internet ile gelen tehditlerin henüz mevcut olmadığı zamanlarda tasarlanan DNP, Profibus ve Modbus gibi endüstriyel iletişim protokollerinde yetkilendirme, bütünlük ve gizlilik gibi güvenlik özelliklerine yer verilmemiştir [120].

BT sistemlerde olduğu gibi yeni nesil DDS iletişim sistemlerinde de internet erişiminde kullanılan ethernet arayüzü ve TCP/IP protokolü kullanılmaktadır. Bu nedenle BT iletişim altyapılarına yönelik siber tehditler DDS sistemler için de aynen

geçerli hale gelmiştir. IP protokolünün yaygın kullanımından önce DDS sistemler için geliştirilmiş endüstriyel iletişim protokollerinin sonradan ilave güvenlik fonksiyonları eklenmeden doğrudan IP iletişim ortamına uyarlanması,bu protokollerin hem geçmiş açıklıklarını hem de IP protokolünden kaynaklı açıklıkları barındırmalarına sebebiyet verecektir.

Bugün gizlilik, bütünlük denetimi gibi fonksiyonlar içermeyen IP temelli iletişim protokollerinin, kolaylıkla analizi, alınan/gönderilen paketlerin değiştirilebilmesi ve yeniden oynatma gibi saldırılarda kullanılması mümkündür. Bu nedenle, geçmişteki güvensiz haliyle IP ortamına adapte edilmiş protokollere yönelik saldırıların uygulanabilirliği daha da kolaylaşmıştır. Örneğin, Carcano ve ark. [121] oluşturdukları test ortamında, yetkilendirme ve bütünlük denetimi özelliklerinden yoksun Modbus protokolünü kullanarak, merkezdeki bir kaç bilgisayara bulaştırılan Modbus DOS kötücül yazılımı ile sahadaki uç birim cihaz ve erişim düzenekleri üzerinde ne tür bozucu etkiler oluştuğunu gösteren çalışmaları oldukça dikkat çekicidir.

DDS altyapısında merkez ve uç birimler arasında kurulan iletişimin güvenliği ile ilgili tartışmalar iki ayrı merkezde devam etmektedir. Bu tartışmalardan birincisi, güvenlik fonksiyonlarının doğrudan iletişim protokollerine eklenmesi, ikincisi ise güvenlik fonksiyonlarının mevcut teknikler kullanılarak iletişim ortamına kazandırılması üzerindedir [122-123]. Birinci yöntem, iletişim güvenliğini uygulama seviyesine çıkarması bakımından önemlidir. Ancak endüstride çok sayıda iletişim protokolü kullanılmaktadır ve bu yöntem her bir iletişim protokolü için ayrı ayrı geliştirme gerektirmektedir. İkinci yöntem ise, doğrudan bir çözüm olmaktan öte güçlü bir güvenlik uyumlaştırma şekli olarak ele alınabilir ve en iyi tarafı farklı iletişim protokolleri için uygulanabilir yapıda olmasıdır.

Birinci yönteme ilişkin olarak, çeşitli araştırmacılar, standart kuruluşları ve üreticilerce bazı endüstriyel protokollerine güvenlik özellik ve fonksiyonlarının kazandırılması için çeşitli çalışmaların son yıllarda yürütüldüğü görülmektedir.

Modbus protokolüne ilişkin bu tür önemli çalışmalardan birine örnek olması bakımından aşağıda yer verilmiştir.

Modbus protokolü sonradan herhangi bir güvenlik fonksiyonu kazandırılmadığı takdirde, aşağıda sıralanan güvenlik kusurlarına sahiptir [120].

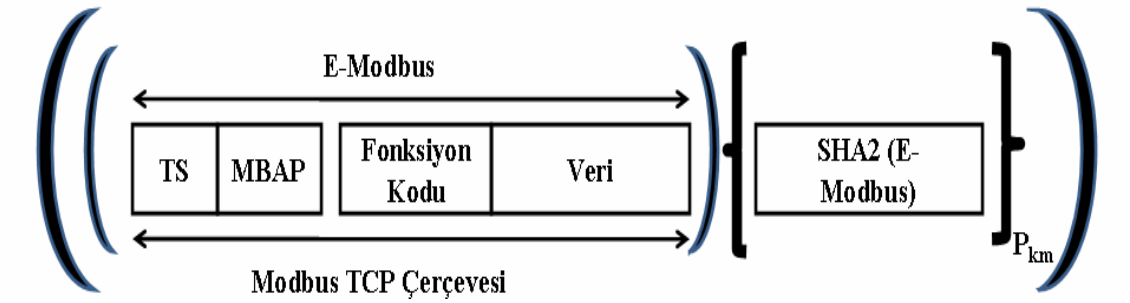
- Mesaj içeriğinin dışarıdan görünmesini engelleyen herhangi bir yetkilendirme mekanizması yoktur.
- Mesaj içeriğinin dışarıdan alınıp değiştirilmesini engelleyebilecek herhangi bir yetkilendirme mekanizması yoktur.
- Kaydedilen bir mesajlaşma trafiğinin daha sonra yeniden oynatılmasını (yeniden oynatma saldırısını) engelleyecek bir mekanizma yoktur.

Bu kusurları gidermek için Fovino ve ark. [120] güvenli Modbus tasarımına ilişkin önerilerde bulunmuşlardır. Oldukça etkili olabilecek bu çözüm aşağıda başlıklar halinde verilmiştir.

- *Bütünlük:* Modbus paketinin bütünlüğünün korunabilmesi için, mesaj içeriğinin sağlaması (hashing), SHA2 fonksiyonu ile yapılabilir. Böylece uçtan uca gönderilen paketinin içeriğinin değiştirilmediği garanti edilebilir. Paketin bütünlüğünün sağlanması, onu gönderen kaynağın bu paketi göndermeye yetkili olup olmadığı konusunda bilgi vermez. Zira yetkisiz bir birim de içinde zararlı mesaj veya kod içeren bir paketi sağlama bilgisiyle birlikte gönderebilir.
- *Yetkilendirme:* RSA temelli imzalama, göndericinin yetkilendirilmesinde kullanılabilir. Örneğin, SHA2 *sağlama özeti* göndericinin RSA *özel anahtarıyla* şifrelenir ve paket imzalı sağlama özetiyle birlikte alıcıya gönderilir. Alıcı, göndericinin açık anahtarı ile gelen paketin sağlama özetini doğrularsa paketin içeriğini kabul eder. Şayet doğrulayamazsa, bu paketin yetkisiz bir birimce gönderildiği kararını verir ve imha eder.
- *İnkâr Edememe:* RSA özel anahtarı aynı zamanda inkar edememe mekanizmasını sağlar.

- *Yeniden Oynatma saldırısının engellenmesi:* SHA2 ve RSA tek başlarına böyle bir saldırıyı/aldatmacayı tespit edemezler. Ancak pakette zaman damgası kullanmak ve özet bilgisini zaman damgasını da içerecek biçimde düzenlemek suretiyle yeni ve eski paketler ayırt edilebilir.

Şekil 8.7.'de yukarıda sayılan güvenlik işlevlerini sağlamak üzere kullanılabilecek Güvenli Modbus Uygulama Veri Biriminin yapısı görülmektedir.



Şekil 8.7. Güvenli Modbus uygulama veri birimi [120]

SCADA/DDS haberleşmesinde kullanılacak iletişim protokolünün yukarıdaki örnekte yer aldığı gibi güvenli hale getirilmesi veri paketlerin içeriğinin okuması ve yakalanan verilerin yeniden oynatılması saldırılarını bertaraf edecektir.

Benzer bir çalışma da DNP3 endüstriyel iletişim protokolü için, Majdalawieh ve ark. [124-125] yaptıkları güvenlik çerçevesi ve benzetim çalışmalarıdır. Bu çalışmalarda DNP3 protokolüne güvenlik özellikleri kazandırılması ve bu özelliklerinin protokolün performansına etkileri yer almaktadır.

IP özelliği kazandırılmamış ve doğrudan seri linkler üzerinden kullanılan endüstriyel iletişim protokollerinin aktif ve pasif siber saldırılara karşı korunmasına ilişkin Amerikan Gaz Birliğinin hazırladığı AGA 12 SCADA İletişiminin Kriptografik Korunması isimli raporu pratik bir tasarım modeli içermektedir [124-125]. Bu rapor ve önerdiği tasarım, mevcut endüstriyel iletişim protokollerinin iyileştirilmesine yönelik ilk çalışmalardan biri olması bakımından da ayrıca önemlidir. Bu çalışmaya

ilişkin diğer önemli bir husus da önerilen tasarımın uygulanabilir ve iletişim performansı üzerinde düşüşe neden olmayan ürünlere dönüşebilmiş olmasıdır [102].

Bugün için, geçmişte kullanılan endüstriyel iletişim protokollerine güvenlik fonksiyonu kazandırılmış yeni tasarımların endüstride yaygın kullanılmadığı gözlen mektedir. Bu durumun sebepleri arasında, bu tür çalışmaların yeterli olgunluğa erişmemesi ve henüz standartlarının oluşmaması, bugün için endüstride yaygın olarak kullanılan uygulama ve ürünlerle birlikte kullanımlarının mümkün olamaması sayılabilir. Ancak en önemli sebeplerden birinin, birinci yöntemin yani protokol tasarımlarının değiştirilmesinin saha da kullanılan uç birim cihazların da değiştirilmesini zorunlu kılmasıdır.

Yukarıda sayılan nedenlerden ötürü, uzun dönem için mutlak bir ihtiyaç olan gizlilik ve bütünlük özellikleri kazandırılmış güvenli endüstriyel iletişim protokollerinin tasarımı, mevcut altyapılar için bir çözüm sunmamaktadır.

Tamamlayıcı veya alternatif olarak kullanılabilecek iletişim ortamının güvenli hale getirilmesi için endüstri standardı haline gelmiş IPSec ve SSL kullanımı yöntemleri Bölüm8.3.4.'te ayrıca tartışılmıştır.

8.3.4. Güvenli iletişim ortamı: Endüstri güvenlik standardı IPSec ve SSL çözümlerinin değerlendirilmesi

Bir iletişim kanalını veya ağını güvenli hale getirmek, ağda birbiriyle iletişime geçen uç birimler arasında dolaşan verilerin üçüncü bir tarafça ele geçirilmek suretiyle okunmasını, aynen veya değiştirilerek ağa yeniden enjekte edilmesini engellemek için gerekli doğrulama, yetkilendirme ve gizleme gibi güvenlik fonksiyonlarını sağlayan ağ protokollerini kullanmakla mümkün olabilecektir.

OSI (Açık Sistem Mimarisi) iki uç arasındaki veri iletişimini 7 katmanda tanımlar. Bir kullanıcı başka bir kullanıcıya ağ üzerinden veri aktardığında, parçalara ayrılan veri, fiziksel sinyal olarak iletim ortamına verilene kadar her katmanda tanımlayıcı

ilave bilgiler alır. Başlık olarak anılan bu bilginin boyutu büyüdükçe iletişimin verimliliği de düşecektir. Ancak iletişimin başarılı ve önceden belirlenmiş kurallara uygun olması için bu başlıklar olmak zorundadır.

TCP/IP protokol takımının her katmanı için farklı güvenlik mekanizmaları uygulanabilir. Her katman için uygulanan güvenlik mekanizmasının farklı zorluk, avantaj ve dezavantajları bulunmaktadır.

Uygulama seviyesindeki güvenlik mekanizmalarının yüksek seviyede kontrol edilebilme ve ayarlanabilme özeliğine karşın her bir uygulama için ayrı ayrı gerçekleştirilmesi gerekir. Bu durum da birçok uygulamada açıklıkların oluşmasına neden olabilecektir [126].

Aktarım katmanında, iki uç arasındaki her bir oturum için ayrı ayrı güvenlik mekanizması uygulanabilir. Bu katmanda, güvenlik mekanizmalarının uygulanması için uygulamanın fonksiyonların ve karakteristiğinin anlaşılmasına ihtiyaç yoktur. Örneğin SSL/TLS aktarım katmanında güvenli iletişimi sağlamak için endüstride yaygınca kullanılan bir güvenlik protokolüdür [126].

Ağ katmanı güvenlik protokolleri, sadece belirli bir uygulama veya oturum için değil, iki host veya ağ arasındaki tüm iletişimi koruma altına almak üzere tasarlanırlar. İletişimde kullanılan adres bilgisi (IP adresi gibi) dahi bu katmanda koruma altına alınabilir.

IPSec (IP Security), ağ katmanında güvenliği sağlamak için en çok kullanılan protokoldür. Uygulama ve aktarım katmanın güvenlik protokollerine göre daha az kontrol edilebilme ve ayarlanabilme özeliğine sahiptir [126].

Bağlantı katmanında tanımlı güvenlik mekanizmaları daha çok uzak erişim servislerini genişletebilmek için tasarlanmışlardır. PPTP ve L2TP bağlantı seviyesinde çalışan protokollerdendir [127].

Farklı katmanlarda tanımlanan güvenlik mekanizmaları, birçok kaynakça VPN olarak da adlandırılmaktadır. Bazı kaynaklar da sadece ağ seviyesi (OSI 3. katman) ve altındaki güvenlik mekanizmaları için VPN terimini kullanmaktadır. Bu çalışmada, uygulama katmanının altındaki oturum, ağ veya bağlantı katmanında tanımlı her türlü güvenlik protokolü aynı zamanda VPN olarak da adlandırılacaktır.

Doğrudan fiziksel katmanda veya tahsisli fiziksel hatlar seviyesinde güvenliği sağlamak için üst seviye protokollerden bağımsız olarak donanımsal şifreleme kullanılması gerekir. Bu tür ağlar, tahsisli fiziksel hatlar üzerinden kurulduğundan sanal değil, gerçek özel ağlar sınıfında yer alırlar.

Yaygınlık, uyumluluk ve kolay kullanılabilirlik kriterleri göz önüne alındığında, günümüzde TCP/IP iletişiminde en çok kullanılan güvenlik mekanizmaları, aktarım katmanı için SSL/TLS, ağ katmanı için IPSec güvenlik protokolleridir. Aşağıda her iki protokole ait detay ve karşılaştırmalar yer almaktadır.

SSL/TLS bağlantı kurulurken, iki uç arasında (istemci sunucu) desteklenen şifreleme takımı üzerinde görüşmeye başlanır. Şifreleme takımı, uçlar arasında gizli anahtar değişimi metotları (RSA veya Diffie-Hellman) ile veriyi doğrulamak ve şifrelemek için kullanılacak algoritmaları (doğrulama için HMAC-MD5, HMAC-SHA-1 şifrelemek için AES, DES, RC2, RC4 gibi) içerir. SSL, anahtar değişimi ve yetkilendirme için iki genel protokolü kullanır. Bunlardan birincisi, Ephemeral Diffie-Hellman (EDH) anahtar değişim algoritması ile birlikte yetkilendirme için Sayısal İmza Standardı(DSS); ikincisi ise yine Ephemeral Diffie-Hellman (EDH) anahtar değişim algoritması ile birlikte yetkilendirme için RSA algoritmasıdır. Üçüncü bir seçenek ise, hem anahtar değişimi hem de yetkilendirme için sadece RSA algoritmasının kullanımıdır. Pratikte, SSL oturumlarında anahtar değişimi için en çok kullanılan RSA yöntemidir. Açık anahtarlı şifreleme veya asimetrik şifreleme algoritması olan RSA için günümüzde 512 bit anahtar uzunluğu artık güvensiz olarak düşünülmektedir. Açık anahtarlı şifrelemede 1024 bit anahtar uzunluğu, simetrik şifrelemedeki 80 bitlik bir şifreleme gücüne sahip olup, RSA laboratuvarı 2010-2030 yılları için simetrikte 112 bite karşılık gelen 2048 bitlik açık anahtar boyutunu

önermektedir [128]. SSL oturumu kurulurken, açık anahtar şifreleme ile simetrik şifrelemede kullanılacak anahtar üzerinde her iki tarafta da uzlaştırsa, artık uç birimler arasındaki verinin simetrik şifreleme teknikleriyle korunaklı olarak gönderilmesi mümkün hale gelmiş olur. Bu aşamadan sonra iletişim güvenliğinin gücü kullanılan simetrik şifreleme algoritmasının ve seçilen anahtar uzunluğunun gücüne denk demektir.

IPSec,haberleşen iki farklı birimin güvenli iletişimi için bir çerçeve düzenler. IETF'ce standartlaştırılan IPSec, ağ katmanında yetkilendirme ve gizlilik servisleri sağlayan bir protokol setidir. IPSec, birçok RFC dokümanında tanımlanmakla birlikte temel dokuman IETF RFC 2401'dir. IPv6 için bir zorunluluk olan IPSec uygulaması, IPv4 için opsiyonel bir güvenlik mekanizmasıdır. IPSec, AH (Authentication Header / Yetkilendirme Başlığı) ve ESP (Encapsulating Security Payload /Güvenlik Veri Yükünü Kapsülleme) olmak üzere iki farklı tip yetkilendirme ve bütünlük mekanizmasına sahiptir. IP paketine eklenen AP başlığı, verinin karşı uçta doğrulanması için gerekli bilgiyi içerirken, ESP şifrelenen verinin hem doğrulanması hem de şifrelenmesi için gerekli bilgileri içerir [129]. Hem AH hem de ESP için tünel ve aktarım olarak nitelendirilen iki farklı çalışma modu bulunur. Tünel modu, iki ağ veya geçit arasında IP adresleri de dahil olmak üzere tüm paketleri şifreli olarak gönderir ve alır [130]. Aktarım modu ise, daha çok doğrudan iletişim kuran iki bilgisayar için daha uygun olan ve IP paketlerinin mevcut başlıklarına karışmadan sadece veri kısmını koruyan çalışma şeklidir. Son olarak, IPSec bağlantısı iki aşamada kurulur. Birinci aşamada (ISAKMP SA: Internet Security Association and Key Management Protocol Security Associations), karşılıklı doğrulama ve bir sonraki bağlantı aşaması için şifreleme anahtarının üretimi yer alır. İkinci aşamada (IPSec SA) ise, daha sonraki akacak olan trafiği korumak için kullanılacak simetrik şifreleme (DES, 3DES, AES) ve doğrulama algoritmaları üzerinde iki uç arasında anlaşma sağlanır [131].

Uygulama, kabiliyet ve özellikler açısından IPSec ile SSL arasındaki temel farklar aşağıda sıralanmıştır [132-133].

- IPSec tüm IP paketlerini korumaya yönelikken, SSL sadece ilgili oturumu korumaya yöneliktir.
- IPSec, iki uç (aktarım modu) veya ağ arasındaki (tünel modu) tüm trafiği güvence altına almak için; SSL bir sunucu istemci çiftinin trafiğinin (bir TCP oturumu gibi) güvene almak için daha uygundur.
- IPSec sadece ortak doğrulama metodunu desteklerken, SSL, istemci doğrulama, sunucu doğrulama ve anonim olmak üzere üç farklı doğrulama metodunu destekler.
- IPSec istemcisi daha önceden tanımlı belirli bir porta bağlanır. SSL istemcisi ise kullanılacak uygulamaya ve yapılandırmaya bağlı olarak farklı portlara bağlanabilir.
- IPSec önce veriyi şifreler ve sonrasında şifrelenmiş veri için bütünlük özeti alırken; SSL önce verinin özetini alır ve sonrasında veriyi şifreler. Verinin değiştiği veya değiştirildiği durumlarda, SSL sistem kaynakları boş yere daha fazla tüketir.
- Farklı üreticilere ait IPSec ürünlerinde birbirleriyle tam bir uyumda çalışması beklenemezken, SSL için böyle bir problem yoktur.

DDS ağları açısından, iletişim kanallarının güvenli hale getirilmesi için hem IPSec tabanlı VPN çözümleri hem de SSL tabanlı VPN çözümleri değerlendirilebilir. Ancak her iki güvenlik çözümünün kullanılacağı ağdaki performansını değerlenirken başlık yükü, bant genişliği tüketimi ve gecikme gibi değerlerinin ölçülmesi gerekir [133]. Bu sayede kullanılacak ağ ve uygulamaya bağlı olarak hangi güvenlik çözümünün daha elverişli olduğunu söylemek mümkün olabilecektir.

Çizelge 8.1.'de görüldüğü üzere kullanılabilecek iki güvenlik protokolünden IPSec'in daha fazla başlık yükü getirdiği görülmektedir.

Çizelge 8.1 IPSec ve SSL ilave başlık yükleri [132]

Protokol	**Mod**	**İlave Bayt**
IPSec Tunel	ESP	32
	ESP ve AH	44
IPSec Aktarım	ESP	36
	ESP ve AH	48
SSL	HMAC-MD5	21
	HMAC-SHA-1	25

Çizelge 8.1.'deki başlık yüklerine ilaveten, IPSec tunel mod için her IP paketine yeni adres bilgisi yüklendiğinden 20 bayt daha ilave başlık yükü daha getirdiğini de belirtmek gerekir.

Kanal bant genişliklerinin ne kadar verimli kullanıldığı ayrıca, hem IPSec hem de SSL'de blok şifreleme için kullanılan dolgu verisinin (padding) miktarlarına bağlıdır. Genel olarak VPN uygulamaları ele alındığında çoğunda yüksek başlık yükü bulunmakta ve bu yükün yaklaşık %75'ini farklı katmanlardan genel başlıklar teşkil etmektedir. Bu yükün yaklaşık %25 kadarı ise kriptografik algoritmalardan kaynaklanmakta olupkripto algoritmalarından kaynaklı başlık yükünün indirgenmesi de mümkün değildir [134].

Başlık yükü daha çok iletişim kanal kapasitelerinin dar olduğu ve uygulamaların yüksek trafik değişimine ihtiyaç duyduğu durumlarda önem kazanır. DDS altyapılar için konu ele alındığında özellikle uzak mesafe kanaların dar band genişliklerine sahip olduğu ancak uygulamaların trafik değişimi ihtiyacının da küçük olduğu görülmektedir.

Hangi VPN çözümünün, çoğu durumda gerçek zamanlı iletişim ihtiyacına sahip olan DDS altyapıları için daha uygun olacağı belirlenirken, kriptografik işlemeler ve başlık yüklerinden kaynaklanabilecek iletişimdeki gecikmeye olan katkı değerleri belirleyecektir. Açık DDS altyapıları açısından asıl problem, özellikle uç birim bileşenlerin düşük işlem gücü kapasitelerinin olması ve bu sebeple IPSec ve SSL gibi protokollerin kriptografik işlemelerinden kaynaklı olarak ortaya çıkacak gecikme ve

bu gecikmelerin SCADA/DDS uygulamaların duyabileceği gerçek zaman iletişim ihtiyaçlarını ihlal etme olasılığıdır.

Bow Networks Inc ve California ISO gibi bazı SCADA/DDS uygulamalarında, güvenli iletişim sağlamak maksadıyla SSL/TLS çözümünü başarıyla kullanılmaktadır [122].

Önerilen teknik iyileştirme yöntemlerinden bazılarını test edebilmek, bu çalışma kapsamında kurulan test ortamında yapılan çalışmalardan biri olan Modbus protokolü için SSL VPN kullanımına ilişkin test ortamı oluşturulmuştur. Yapılan laboratuar testlerinde 50 uç birimden oluşturulmuş ağ ortamı için yeniden üretilen gerçek Modbus trafiğinin, blok şifrelemeden kaynaklı doğrulama ve SSL başlık yükleri dahil %80 civarı artış gösterdiği buna karşılık merkez ile saha arasında 2048 Kbps'lik bağlantı kullanılması halinde, 1 saatlik toplam zaman için ağ kaynaklı gecikmenin 2,451 saniye ile sınırlı kaldığı görülmüştür. Ancak bu değere uç bileşenlerin (bilgisayarların) işlem gücünden kaynaklı gecikmenin dahil edilmediği hatırlamak yerinde olacaktır.

Zaman içerisinde SCADA/DDS ağlarını ve iletişimini daha güvenli hale getirmek için hem SSL/TLS hem de IPSec güvenlik mekanizmasının daha da yaygınlaşacağı öngörülmektedir. DDS ağlarındaki nispeten düşük ağ trafik değerleri dar kapasiteli kanallar için dahi her iki yöntemin rahatlıkla kullanılabilmesine imkan verecekken, uç birim bileşenlerinin düşük işlem güçlerin ve bu nedenle kriptografik işlemelerinden kaynaklı olarak ortaya çıkacak gecikmenin dikkate alınması gerekir. Ayrıca, mevcut açık metin protokollere göre çok fazla güvenlik fonksiyonu sağlıyor olsada, IPSec ve SSL/TLS protokollerinin de açıklıkları sahip oldukları [122,135] hatırda tutulmalıdır. Mevcut yapı ve protokoller için büyük bir adım olmakla birlikte mutlak güvenlik sağladıklarını söylemek doğru olmayacaktır.

Sahada kullanılan ve çoğunlukla IPSec ve SSL gibi güvenlik protokollerini işletim sistemi ve/veya donamım kaynağı kısıtlarıyla çalıştıramayacak RTU gibi uç birim

bileşenlerin önünde IPSec veya SSL VPN donanımlarının haricen kullanılması aşağıdaki iki nedenden ötürü avantaj sağlayacaktır. Bunlar;

- Her türlü uç birim bileşen için kullanılabilir olması ve karşılıklı kullanımla uyumsuzluk problemlerini gidermesi,
- Doğrudan uç birim bileşenler üzerinde çalıştırılmadığından ve donanımsal kaynaklarını kullanmadığından mevcut kaynakların performansları üzerine de olumsuz etkisinin olmamasıdır.

IPSec VPN çözümlerinin daha uzun yıllardır var olduğu ve BT sistemlerde yaygın olarak kullanıldığı gözlenmektedir. Diğer taraftan haricen SSL/TLS VPN çözümlerinin ise bugün için yaygın üretim ve kullanımının olmadığı gözlenmektedir.

8.3.5. Ağ güvenliği

Güvenli ağ tasarımı için en önemli konu ağdaki erişimin denetlenmesi ve trafiğinin izlenmesidir.

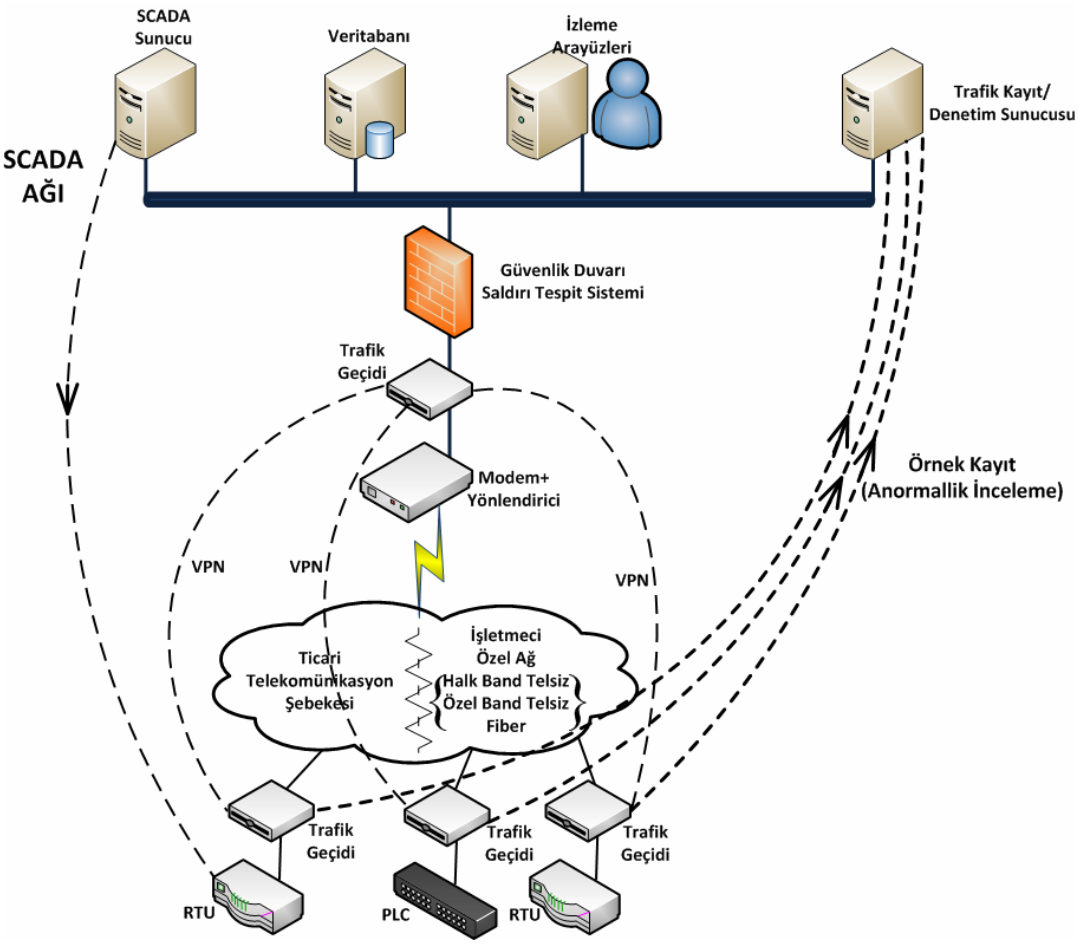
Ağ erişiminin denetlenmesi için öncelikli olarak ağda hizmet sunan bileşenlerinin fonksiyonlarına ve birbirleriyle iletişim kurma ihtiyaçlarına bağlı olarak güvenlik alanlarının oluşturulması gerekir. Bu alanlar, ağ anahtarları vasıtasıyla sanal özel ağlar (VLAN) ve birden fazla ağ arayüzüne sahip güvenlik duvarları ile farklı ağ bölümleri oluşturularak elde edilebilir.

Günümüz güvenlik duvarları, adres, port ve oturum temelli inceleme ve filtreleme özelliklerine sahipken denetim sistemlerinde kullanılan endüstriyel protokolleri tanıyan ve fonksiyon bazında filtreme yapan güvenlik duvarlarını kısıtlı sayıda bulunmakta olup çoğunluğu deneme ve geliştirme aşmasındadır. Bu tür çalışmalarında daha çok Modbus protokolü özelinde yoğunlaştığı gözlenmektedir [9,136]

Güvenli ağ tasarımının diğer önemli unsuru ise ağdaki trafiğin izlenerek anlık veya en kötü durumda geçmişe dönük anormalliklerin tespit edilmesidir. Ağ trafiğini izleme, raporlama ve gerektiğinde müdahale etme gibi işlemler ağda yer alan trafik geçiş noktası veya noktalarında konuşlandırılan saldırı tespit ve engelleme sistemleri vasıtasıyla gerçekleştirilmektedir.

Gerek güvenlik duvarı gerekse saldırı tespit sistemleri, güvenli bir ağ tasarımının önemli ve çoğu durumda vazgeçilmez bileşenleri olmasına rağmen gerçek zamanlı iletişim ihtiyacı duyan kritik sistemler üzerinde olumsuz etkiler oluşturabilmeleri riskleri de ihtimal dahilindedir. Bu bileşenlerin ağda geçen ve yoğun olarak kullanılan protokolleri tanıyor olmaları bu tür olumsuzlukların indirgenmesi ve kendilerinden beklenen güvenlik fonksiyonlarını icra edebilmeleri bakımından oldukça önemlidir.

Çoğu tasarımda güvenlik duvarı ve saldırı tespit sistemlerin yeri, BT ve DDS ağlarını birbirinden ayırmak üzere konuşlandırılmaktadır. Ancak DDS ağının kendi iç trafiğini denetlemek, Merkez ve Uç birimler arasındaki iletişim ortamlarından doğrudan gelebilecek saldırıları engelleyebilmek açısından büyük önem taşımaktadır. Şekil 8.8.'de DDS ağının kendi için de konuşlandırılmış güvenlik duvarı ve saldırı tespit sistemi gösterilmiştir. Ayrıca aynı şekilde uçlar arası iletişimi IPSec /SSL VPN gibi çözümlerle şifreleyen ve akan trafiğin bir örneği merkezi bir kayıt ve inceleme sunucuya ileten harici bir iletişim birimi (trafik geçidi) daha ilave edilmiştir.



Şekil 8.8. DDS Ağı için güvenlik duvarı konumu ve trafik geçitleri

Şekil 8.8.'de olduğu gibi DDS ağ ortamında kullanılması önerilen ve trafik geçidi olarak adlandırılan bileşenler, şifreleme, bütünlük kontrolü, erişimi denetleme, oturumu takip etme gibi işlemleri kendi kaynakları üzerinden icra edebileceklerinden uç birimlerdeki programlanabilir denetleyiciler üzerinde de performans düşürücü bir etkileri olmayacaktır. Ancak mevcut yapılardan farklı olarak nispeten yüksek iletişim kanal kapasitelerine ihtiyaç duyacaktır.

9. SONUÇ VE DEĞERLENDİRMELER

Bu çalışmada, elektrik, su, gaz üretim, dağıtım ve iletim sistemleri başta olmak üzere kritik altyapı ve endüstriyel tesislerdeki fiziki iş süreçlerini otomatize ederek, süreçlerin bir veya belirli merkezlerden izlenmesi ve yönetilmesine imkân sağlayan Dağıtık Denetim Sistemlerinin güvenlik açıklıklarının ve risklerinin belirlenmesi için literatür incelemeleri ile anket, mülakat, gezi-gözlem ve güvenlik taramalarından oluşan saha çalışmaları yapılmıştır. Belirlenen güvenlik açıklıklarının giderilebilmesi için literatürdeki mevcut çözüm önerilerinden de yararlanılarak, saha ve ülke gerçeklerine uygun ve uygulanabilir çözüm önerileri ve güvenlik yaklaşımları, stratejileri ve eylem planları geliştirilmiştir.

Mevcut çalışmalar incelendiğinde;

- Ülkemizde benzer bir çalışmanın daha önce yapılmadığı, benzer konulardaki çalışmaların ağırlıklı olarak ABD ve bazı AB ülkelerinde yürütüldüğü,
- Özellikle ABD ve AB ülkelerinin kritik altyapıların güvenliğinin sağlanmasına yönelik olarak düzenlemeler yaptığı, strateji dokümanlarını yayımladığı, hazırlamış oldukları eylem planlarının kısmen veya tamamen uygulamaya geçtikleri,
- Farklı kritik sektör ve altyapılarda kullanılan DDS'lerin güvenliğine ilişkin paydaşların ve rollerinin yeterince tartışılmadığı, özellikle yönetici boyutunda yapılabileceklere hiç ya da çok az değinildiği,
- Çözüm önerilerinde uygulanabilirlik, geriye ve ileriye dönük uyumluluk kriterlerinin yeterince dikkate alınmadığı ve tartışılmadığı,
- Mevcut çalışmaların çoğunlukla BT sistemlerine yönelik olup, DDS altyapılar için nispeten kısıtlı sayıda ve devlet destekli güvenlik çalışmaları yürütüldüğü,
- Yürütülen saha ve laboratuvar çalışmalarından elde edilen somut bulgu ve verilerin çoğunlukla yayınlarda paylaşılmadığı veya kısmen paylaşıldığı,

görülmüştür.

Bu çalışmada ise, ülkemizde bu alandaki eksiklerin giderilmesine yönelik çıktıların hazırlanması, önerilen çözüm yaklaşımlarının ve tespitlerin dikkate alınarak, hem

ülkemizin bu konuda eksiği olan strateji belgesinin oluşturulmasına katkılar sağlaması hem deliteratüre katkıların sağlanması amaçlanmıştır. Bu çalışma ile kritik altyapılarda kullanılan denetim sistemlerinin güvenliği konusunda, ülke ve ilgili kurum ve işletmeciler için strateji, politika ve en iyi uygulama yaklaşımları belirlemeye yönelik dokümanlar oluşturulmuştur.

Hem güvenlik risklerinin değerlendirilmesi hem de tespit edilen risklerin giderilmesine yönelik çözüm önerilerinin üretilmesinde literatürdeki yaklaşımlar kadar saha gerçekleri ve önceliklerinin de dikkate alınması büyük öneme sahiptir. Önerilen güvenlik strateji, politika ve uygulamalarının kapsamlı, gerçekçi ve uygulanabilir olması için bu çalışma kapsamında biri bölge diğeri ülke ölçeğinde hizmet sunan iki önemli işletmeciyle birlikte ortak çalışmalar yürütülmüştür.

Saha çalışmalarında karşılaşılan en önemli güçlük, böyle bir çalışmaya işletmecileri ikna etme sürecinde yaşanmıştır. İncelenmekistenilen birçok işletmeci çeşitli kaygılarla, altyapıları üzerinde güvenlik inceleme çalışmalarının yapılmasını istememişlerdir. İşletme yöneticilerinin genel yaklaşımı, yıllardır çalışan altyapılarının güvenli olduğu, çalışanların kusurlarından kaynaklı birkaç olay dışında siber güvenlik olayları ile karşılaşmadıkları şeklindedir. Bu bağlamda, birçok işletmeci açısından siber güvenliğin bir ihtiyaç olarak hissedilmediği, mevcut iş süreçleri ve alışkanlıklarını devam ettirme yönünde eğilime sahip oldukları gözlenmiştir. Bu dirence rağmen, biri kısmen gerçekleştirilebilmiş olsa da iki farklı işletmeci ile ortak çalışma yürütülmüş ve bu iki örnek durum çalışmasından elde edilen veri, bilgi, gözlem ve deneyimler ile önerilen güvenlik çözümlerinin gerçekçi ve uygulanabilir olması sağlanmıştır. Saha çalışmalarındaki diğer önemli bir güçlük de elde edilen somut açıklık bulgularına ilişkin verilerin yayınlanmasının ortaya çıkaracağı güvenlik zafiyeti olup, somut bulgular sadece ilgilisi olan işletme ile paylaşılabilmiştir.

Saha çalışmalarıyla, SCADA/DDS altyapı ve bileşenlerini yerinde görme, yürütülen kritik iş süreçlerini gözleme, incelenen altyapı ve süreçlerinin siber güvenlik gereksinimlerini ve önceliklerini belirleme, güvenlik açıklıklarını tespit etme gibi

hedefler belirlenmiştir. Yürütülen, “mülakat ve saha gezileri”, “araştırma soru formu hazırlama ve cevaplarını değerlendirme”, “mevcut belgelerin incelenmesi”, “ağ ve sistem taraması” çalışmalarıyla da başta konulan hedeflere ulaşma imkânına sahip olunmuştur. Böylece saha çalışmaları beraberinde ve sonrasında yürütülen ‘güvenlik risk değerlendirmesi’ ve ‘güvenlik iyileştirme önerileri’ çalışmaları için gerçek ihtiyaçlara uygun ve uyumlu yaklaşımların geliştirilmesi ve önerilerin sunulması mümkün hale gelmiştir.

Güvenlik riski değerlendirme yöntemleri, çeşitli tehdit kaynaklarının belirli bir sistemde var olan zayıflık ve açıklıklardan yararlanılarak o sisteme ne ölçüde ve hangi olasılıkla zarar verebileceğini belirlemekte kullanılmaktadır. Bu kapsamda, literatürde farklı risk değerlendirme yöntem ve yaklaşımları yer almaktadır. Ancak yapılan araştırmalarda, güvenlik riski değerlendirme yöntemlerinin ağırlıklı olarak BT sistemlerine yönelik olarak geliştirildiği görülmektedir. Buna karşın Bölüm 7’da tartışıldığı üzere, SCADA/DDS altyapılarına yönelik kısıtlı sayıda risk belirleme ve değerlendirme çalışmalarından biri olmakla birlikte, Patel ve ark. [82] konuya yönelik önerdikleri yöntem de ekonomik kayıpları temel almaktadır. Oysaki kritik altyapı ve tesislerde kullanılan DDS sistemlere yönelik yetkisiz müdahale ve saldırıların sonuçlarını sadece ekonomik ölçütlerle ifade etmenin eksik ve bazı durumlar için hatalı bir yaklaşım olacağı değerlendirildiğinden, bu çalışmada güvenlik risklerini belirleme yaklaşımı doğrudan bir zararı ölçmeye yönelik değer hesabı olarak değil, iyileştirme çalışmalarındaki giderilmesi gereken açıklıkların önceliklerinin belirlenmesi için bir araç olarak kullanılmıştır. Bu sayede, her bir örnek durum ve istenmeyen olay/etki tanımlamasına bağlı olarak farklı SCADA/DDS altyapıları için giderilmesi gereken açıklıkların listelenmesi ve her bir açıklık için nicel kritiklik değerlerinin hesaplanması mümkün hale gelmiştir. Açıklıklar için kritiklik değerinin belirlenmesi ile birlikte ise hangi güvenlik iyileştirmesi veya iyileştirmelerinin öncelikli olduğu belirlenebilmektedir.

Yedinci Bölümde önerilen ve altı adımdan oluşan açıklık kritikliği sıralama yaklaşımı, tanımlı istenmeyen olaylara göre hangi açıklıkların bir işletme için daha kritik olabileceğini tespit etmek üzere kullanılabilecektir. Böylece aynı altyapıyı

kullanan farklı alanlardaki işletmeciler için olası tüm güvenlik açıklıkları arasında öncelik sıralamalarının yeniden yapılması mümkün olabilecektir. Bu yönüyle, literatürde yer alan ve çalışma içinde de tartışılan risk değerlendirme yaklaşımlarından farklı olarak önerilen risk değerlendirme yaklaşımı;

- Bir güvenlik olayı sonrası ortaya çıkan zararı hesaplamaya dönük olmayıp, giderilmesi öncelikli açıklıkları bulmaya yönelik çözümler sunabilmektedir.
- Aynı DDS sistemini kullansa da üzerindeki farklı üretim ve hizmet türlerine özgü olarak farklı kritiklik seviyelerine sahip altyapılara özgü sonuçlar verebilecek yapıdadır.
- Güvenlik açıklıkları için nicel kritiklik değeri atanması mümkün olabilmektedir.
- Açıklık kritiklik değerleri sayesinde öncelikli güvenlik iyileştirmelerinin bulunmasına imkân sağlamaktadır.
- BT sistemleri için de kullanılabilecek bir yapıda ve esnekliktedir.

DDS sistemlere özgü güvenlik açıklıklarının tanımlanmasını ve duruma özgü kritikliklerinin belirlenmesi sonrası, güvenlik açıklıkları ve açıklık kaynaklarının giderilmesine ilişkin öneriler sunulmuştur. Bu bağlamda, saha gerçekleri ve önceliklerine de uygun olarak üç boyutlu güvenlik iyileştirme önerileri, birbirini destekleyici ve tamamlayıcı unsurlarıyla birlikte verilmiştir.

Bir işletmeye ait güvenlik kusurlarını sadece teknik boyutta aramak eksik bir güvenlik bakış açısı olup, birçok teknik güvenlik açıklığının kaynağı olan yönetim ve işletme boyutlarını güvenlik süreçlerinin en başında bulundurmak gerekmektedir. Bölüm 8.'de, çoğunluğu belirli ve önemli sektörlerdeki fiziki süreçleri izlemek ve yönetmek için kullanılan denetim altyapılarına yönelik tehditleri giderici çözüm önerileri yer almaktadır. Çözüm önerileri sunulmadan önce, "düzenleyici", "altyapı üretici" ve "işletmeci" başta olmak üzere tüm paydaşlar ve aralarındaki ilişki tanımlanmış ve her bir paydaşa ait sorumluluklara yer verilmiştir. Böylece önerilen çözümlerin gerçekleştirilmesinde kimlerin nasıl bir role sahip olması gerektiği de güvenlik modelinin içine dâhil edilmiştir.

Saha çalışmaları da bir kez daha göstermiştir ki yönetim ve işletme boyutundaki eksiklik ve kusurlar, teknik güvenlik açıklıklarının en önemli nedenleridir. Türkiye özelinde, enerji ve su gibi kritik kaynakların üretim, iletim ve dağıtımında kullanılan DDS altyapılarını olası siber saldırılara karşı koruyacak tedbirlere ilişkin düzenlemelerin olmadığı görülmektedir. En üst seviyedeki bu boşluk, doğal olarak işletme boyutundaki tutum ve teknik boyuttaki uygulamalara yansımaktadır.İşletmelerden,her ne kadar çok önemli altyapıları işletiyor olsalar da, iş öncelikleri ve uzmanlıkları itibariyle siber saldırılara karşı kendilerini koruma alanında üstün uzmanlık ve birikim beklemek doğru bir yaklaşım olmayacaktır. Bu konuda yönlendirici ve destekleyici olması gerekenlerin ilgili düzenleyici kuurmlar ile ülke stratejiler ve kurumsal güvenlik politikları olacağı değerlendirilmektedir.

Bölüm 8.'de yer alan 'İşletme Boyutu' güvenlik politikaları, Bölüm 5.'te tartışılan mevcut güvenlik standartlarında var olan politikalardır.Fakat burada,mevcutlardan farklı olarak, politikalardan bazılarının DDS altyapılarına ve kapsamına göre yeniden tasnifi ve aralarındaki ilişkinin tarifi yoluna gidilmiştir. İşletme boyutunda yapılması gerekenler, literatürde yer alan ve bir kısmı çeşitli başlıklarda standartlaştırılan çözüm önerilerinden çok farklı değildir. Türkiye özelinde, ISO 27000 serisi güvenlik standartları bilinmekle ve yer yer uygulama imkânı bulmakla birlikte, DDS altyapılara özgü diğer güvenlik standartlarının ve güvenlik belgelerinin neredeyse hiç bilinmediği ve hiç yararlanılmadığı gözlenmiştir. Bu önemli eksiklik, Türkiye'deki kritik altyapı işletmecilerin altyapılarını, olası siber saldırılardan korumalarının önündeki en önemli problemler arasındadır.

Bölüm 8.'deki 'Teknik İyileştirme' önerilerinde, geçmişten farklı olarak günümüz DDS altyapı bileşenlerinin BT sistemler için üretilmiş hazır ürün, uygulama, arayüz ve protokolleri yoğun bir biçimde kullandığı gerçeğinden hareket edilmiştir. Özellikle TCP/IP protokolünün ve genel amaçlı işletim sistemlerinin artık sadece merkez birimlerde değil giderek uç birimlerde de kullanılmaya başlanması durumu, çözüm önerisinde göz önünde bulundurulan en önemli hususlardan olmuştur. Teknik boyutta sahada güvenlik iyileştirmelerinin önündeki en önemli problemler ise kapalı ve üretici bağımlı uygulama ve protokollerin kullanımı, mevcut yazılımsal ve

donanımsal kaynakların önerilebilecek birçok çözümü uygulamayı imkânsız kılmasıdır. Bu sebeple, teknik iyileştirmelerin, saha gözlemelerine ve endüstri gerçeklerine dayalı olarak farklı yapılar için de uygulanabilir, mevcut ve gelecek uygulamalarla uyumlu olması gerekmektedir. Önerilen çözümlerde bu kriterler dikkate alınmıştır.

Bu tez çalışması kapsamında kritik altyapılarda kullanılan denetim sistemlerinin güvenliğine ilişkin tespit edilen en önemli eksiklikler, bu konuda bir ülke stratejisinin, kurumsal politika ve eylem planlarının olmayışıdır. Bu iki önemli eksikliğin giderilmesi durumunda altyapılarda bulunan güvenlik açıklıklarının giderilmesi ve güvenliklerinin sürdürülebilir hale getirilebilmesi mümkün olabilecektir. Bu hususlar dikkate alınarak; bu çalışmada, "Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi" ve "Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı" belgeleri üretilmiştir (Bakınız Ek-3 ve Ek-4). Ayrıca ortak çalışma yürütülen işletmecilerden birine, tespit edilen tüm güvenlik açıklıklarını ve giderilmesi için iyileştirme ve çözüm önerilerini içeren kapsamlı bir rapor hazırlanmış ve sunulmuştur (Bu dokümanın tamamı, yapılan protokol gereği burada verilmemiştir. Özeti için Ek-2'e bakınız). Benzer belgelerin ABD ve bazı AB ülkelerince hazırlandığı ve bazı kritik sektörler için uygulamaya geçildiği yapılan araştırmalarda görülmüştür.

Ülkemizde, denetim sistemine dayalı üretim, iletim ve dağıtım yapan kritik altyapıların siber güvenliğine yönelik bu kapsamdaki ilk çalışmalardan olan bu tez çalışmasında, üretilen ve ekte sunulan çıktılar kullanılarak mevcut altyapılardaki güvenlik açıklıklarının ve açıklık kaynaklarının önemli ölçüde giderileceği bir yapının oluşturulabileceği değerlendirilmektedir. Ayrıca üretilen belgelerin ve tez içindeki tartışmaların araştırmacılar, üreticiler ve karar vericilerin çalışmalarına katkı sağlayacağı değerlendirilmektedir.

Sonuç olarak, bu tez kapsamında, ülkemizde farkındalığı yeni yeni artan bir alan için somut çözümler ve öneriler sunulmuştur. Bu çözümlerin ve önerilerin ülkemiz kritik altyapı ve siber güvenlik stratejilerine katkılar sağlayacağı değerlendirmektedir.

Ülkemizde bundan sonraki süreçte, bu tez kapsamında yapılan önerilerin hayata geçirilmesi, farklı işletmelerin daha detaylı incelenmesi, üniversitelerle daha çok işbirliği yapılarak karşılaşılabilecek sorunlara ortak çözümler bulunması, kritik altyapı farkındalığının arttırılmasına yönelik eğitim programlarının yapılması, DDS altyapılarının güvenlik, gerçek zamanlılık ve performans ihtiyaçlarını karşılayacak endüstriyel iletişim protokollerinin tasarlanması ve geliştirilmesi, oluşturulması önerilen test yataklarında farklı ürün, uygulama ve protokollerin penetrasyon testlerinin yapılmasına ihtiyaç vardır.

KAYNAKLAR

1. İnternet: Electronic Privacy Information Center "Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001", http://epic.org/privacy/ terrorism/hr3162.pdf (2009).

2. İnternet:Official Journal of the European Union "Critical InfrastructureProtection inTheFightAgainstTerrorism",http://eur-lex.europa.eu/LexUriServ/ LexUriServ.do?uri=COM:2004:0702:FIN:EN:PDF (2009).

3. İnternet:Official Journal of the European Union"CommunicationFromThe Commission on a EuropeanProgrammefor Critical Infrastructure Protection786Final",http://eur-lex.europa.eu/LexUriServ/ site/en/com/2006/com2006_0786en01.pdf (2009).

4. İnternet: Bilgi Teknolojileri Kurumu "Kritik Altyapıların Korunması" http://www.cybersecurity.gov.tr/publications/CIP_Rapor.pdf(2010).

5. İnternet:Türkiye Cumhuriyeti Ulusal Bilgi Güvenliği Portalı "İki Kritik Kavram: Kritik Altyapılar ve Kritik Bilgi Altyapıları" http://www.bilgiguvenligi . gov.tr/siber-savunma/iki-kritik-kavram-kritik-altyapilar-ve-kritik-bilgi-altyapilari.html(2010).

6. Sanz, R.,Arzen, K., "Trends in Software and Control", ***Control Systems Magazine***, 23(3):12–15 (2003).

7. Chandia, R., Gonzalez, J., Kilpatrick, T., Papa M. &Shenoi S. (2007). "Security Strategies for SCADA Networks", Critical Infrastructure Protection, ***Springer***, New York, 117-131 (2007).

8. İnternet: ABB Group of Companies "SCADA over IP-basedLAN-WAN connections" http://www05.abb.com/global/scot/scot221. nsf/ veritydisplay /51912692be234e5ec1256d11002c73e9/$File/802.pdf(2012).

9. Bayındır, R., Sağıroğlu, Ş., Çolak, İ., Özbilen, A., "İzlenebilir Elektrik Enerjisi Dağıtım Sisteminin Bilgi Güvenliği Açısından Endüstriyel Risklerinin Araştırılması ve Çözüm Önerileri", ***Gazi Üniversitesi Mühendislik-Mimarlik Fakültesi Dergisi***, 24(4), 715-723 (2009).

10. Sağıroğlu, Ş., Çolak, İ., Bayındır, R., Özbilen, A., "Dağıtık Denetim Sistemlerine Yönelik Elektronik Tehditler", ***TUBAV Bilim Dergisi***, 1(2):82-88 (2008).

11. Ozbilen, A.,Sagiroglu, S., Çolak, İ., "Siber Savaş ve Türkiye için Öneriler**",** ***Siber Güvenlik Çalıştayı*****,** Ankara (2011)

12. Özbilen A., Çolak, İ., Sağıroğlu Ş., "A Survey on SCADA / Distributed Control SystemCurrent Security Development andStudies", ***IST-091 Symposium on Information AssuranceandCyberDefence,*** Tallinn 14: 1-12 (2010).

13. Kara, M.,Çelikkol,S., "Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği", ***4. Ağ ve Bilgi Güvenliği Sempozyumu***, Ankara 19-24(2011).

14. McDonald, J.D., "DevelopingandDefining Basic SCADA SystemConcepts", ***37th AnnualRuralElectricPower Conference***, Kansas City, Missouri, 3: 1-5 (1993).

15. Thomas, M.S., "Remote Control, ThePowerAutomationLabs at Jamia MilliaIslamia", ***PowerandEnergy Magazine***, 8(4):53-60 (2010).

16. İnternet : Motorola Company "ScadaSystems"http://www.motorola.com /web/Business/Products/SCADA%20Products/_Documents/Static%20Files /SCADA_Sys_Wht_Ppr-2a_New.pdf (2012).

17. Ghosh, S.K., "Changing Role of SCADA in ManufacturingPlant", ***Thirty-First IAS Annual Meeting***, San Diego, CA, 1565–1566 (1996).

18. Igure, V.M.,Laughter, S.A., Williams, R.D, "Security issues in SCADA Networks", ***Computers& Security***, Elsevier 25(7):498–506, (2006).

19. İnternet: Shenzhen Youkong Electromechanical CO. Ltd. "Modbus Protocole" http://www.automation-drive.com/modbus-protocole , (2012).

20. Gonzalez., J., Papa, M., "PassiveScanning in Modbus Networks", ***Critical InfrastructureProtection***, 253:175-187 (2007).

21. İnternet: Modbus Organization "Modbus Application Protocol Specification, Version1.1" http://www.modbus.org/docs/Modbus_Application_Protocol_V1_ 1b.pdf (2008)

22. Haji, F.,Lindsay, L., Song., S., "Practical Security Strategyfor SCADA AutomationSystemsand Networks",***Proceedings of the Canadian Conferenceon Electrical and Computer Engineering,Saskatoon*** 172 – 178 (2005).

23. Kropp, T., "SystemThreatsandVulnerabilities: an EMS and SCADA Security SystemOverview", ***IEEE Power&Energy Magazine***, 46-50 (2006).

24. İnternet:International Academy, Research and Industry Association "Analysing Risk in PracticeThe CORAS Approachto Model-Driven Risk Analysis" http://www.iaria.org/conferences2011/filesSECURWARE11/part1_securware_ CORAS.pdf (2011)

25. İnternet: NationalInstitute of Standardsand Technology “Guide for Conducting Risk Assessments" http://csrc.nist.gov/publications/drafts/800-30-rev1/SP800-30-Rev1-ipd.pdf (2011).

26. Lund, M.S,Solhaug, B., Stølen, K, "Model-Driven Risk Analysis: The CORAS Approach 1st Ed”, ***Springer***, 47-58 (2010)

27. İnternet:NationalInstitute of Standards andTechnology"Information Security Handbook: A Guide forManagers” http://csrc.nist.gov/publications /nistpubs/800-100/SP800-100-Mar07-2007.pdf (2011).

28. İnternet: TBD Kamu-BİB Kamu Bilişim Platformu VIII “Bilişim Teknolojilerin deRiskYönetimi" http://www.tkgm.gov.tr/turkce/dosyalar /diger%5Cicerikdetaydh273.doc (2011).

29. İnternet: Lasa Information Systems Team “ICT Risk Assessment” http://ictknowledgebase.org.uk/riskassessment (2011).

30. Ralston, P.A.S.,Grahamb, J.H., Hiebb, J.L., “Cyber Security Risk Assessment for SCADA and DCS Networks”, ***ISA Transactions***,46:583–594(2007).

31. Hall J.A., "Information System Auditing andAssurance", Accounting Information Systems 4th, ***South-Western CollegePub***.,17:1-8 (2004).*

32. İnternet: SANS Institute "An Introductionto Information System Risk Management", http://www.sans.org/reading_room/whitepapers /auditing/introduction-information-system-risk-management_1204(2011).

33. İnternet: InternationalOrganizationforStandardization"ISO 31000–Risk Management" http://www.iso.org/iso/iso_catalogue/management and_leadership_standards/risk_management.html (2011).

34. İnternet: InstituteforEnergyTechnology, http://www.ife.no/departments/ RID/project/coras (2011).

35. Stolen, K.,Braber, F., Fredriken, R., Gran, B. A., Houmb, S.H., Lund M.S., Stamatio, Y.C., Aagedal, J.O., “Model-based Risk Assessment The Coras Approach”,***NorskInformatik Konferanse***, Kongsberg, Norway,239-249(2002)

36. Buyens, K., Win, B.D., Joosen, W, "Empiricaland Statistical Analysis of Risk Analysis-Driven Techniquesfor Threat Management”, ***The Second International Conference on Availability, Reliabilityand Security***, IEEE ComputerSociety, Vienna, Austria,1034-1041 (2007).

37. İnternet: Carnegia Mellon University Software Engineering Institute “OCTAVE”http://www.cert.org/octave(2011).

38. İnternet: The Institute for Information InfrastructureProtection (I3P)"I3P Risk Characterization Report 2007" http://www.thei3p.org/docs/ publications/researchreport9.pdf (2012)

39. E. Byres, D. Leversage, N. Kube, "Security Incidentand Trends in SCADA and Process Industries: A Statistical Review of the Industrial Security Incident Database (ISID)", ***White Paper:Symantec Corporation***, Cupertino, California, 1-28 (2007).

40. Christiansson, H.,Luiijf, E., "Creating a European SCADA Security Testbed", ***Critical InfrastructureProtection***, 253**:**237-247 (2007).

41. Slay, J., Miller, M., "LessonsLearnedFromtheMaroochyWaterBreach", ***Critical Infrastructure Protectio****n*,253**:**73-82 (2007).

42. Daniela, T., " Communication Security in SCADA PipelineMonitoring Systems"*,****Roedunet International Conference (RoEduNet) 10th***, 1–5 (2011).

43. İnternet:The Washingtonpost "Cyber Incident Blamed for Nuclear Power Plant Shutdown"http://www.washingtonpost.com/wp- dyn/content/article/ 2008/06/05/AR2008060501958.html (2009).

44. İnternet: "Electricity Grid in U.S. Penetrated by Spies", http://online.wsj.com /article/SB123914805204099085.html (2009).

45. İnternet:The Federation of American Scientists "PresidentialDecision Directive/Nsc-63" http://www.fas.org/irp/offdocs/pdd/pdd-63.htm (2009).

46. İnternet : The Department of Homeland Security http://www.dhs.gov/homeland-security-presidential-directive-7#1 (2010).

47. İnternet:The International Relations and Security Network "An Inventory of 25 National and 7 International Critical Information InfrastructureProtectıonPolicies" , http://www.crn.ethz.ch/publications/crn_team/detail.cfm?id=90663 (2009).

48. İnternet: U.S. Secretary of Energy "SCADA National Test Bed Fiscal Year 2009 Work Plan"http://energy.gov/sites/prod/files/oeprod/DocumentsandMedia /FY09_Work_Plan_External.pdf (2009).

49. İnternet: Roadmap to Achieve Energy Delivery Systems Cybersecurity "CommonCyber Security VulnerabilitiesObserved in Control System Assessments by the INL NSTBProgram"http://www.controlsystemsroadmap .net/pdfs/ INL_Common_Vulnerabilties.pdf (2009).

50. İnternet: United States Computer Emergency Readiness Team "CommonCyber Security Vulnerabilities Observed in DHS Industrial Control Systems Assessments", http://www.us-cert.gov/control_systems/pdf/DHS_Common VulnerabilitiesR1_08-14750_Final_7-1-09.pdf (2009).

51. İnternet: NationalInstitute of StandardsandTechnology"Guide toSupervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security"http://www.securitymanagement.com/archive/library/nist_scada 0107.pdf (2010).

52. Robert, P. E.,"Process Control System Cyber Security Standards–an Overview", ***52nd International Instrumentation Symposium***, Cleveland (2006).

53. Önel, D.,Dinçkan, A., "Bilgi Güvenliği Yönetim Sistemi Kurulumu", ***TUBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü***, Kocaeli (2007).

54. Calder, A., Watkins, S.,"*IT Governanee*:A Manager's Guide to Data Security and ISO 27001 / ISO 27002: A Manager's Guide to Data Security and BS 7799/ IS0 17799", ***Kogan Page US***, 372 (2005).

55. İnternet: IsecT Ltd. "ISO/IEC 27002:2005 Information Technology-Security Techniques-Code of Practice for Information Security Management" http://www.iso27001security.com/html/27002.html (2011).

56. İnternet: Infracritical, Inc., "SCADA Information Security Management Guide" http://www.infracritical.com/papers/scada-security-mgmt-guide.pdf (2011).

57. İnternet: The International Society of Automomation "ISA99, Industrial Automation and Control Systems Security", http://www.isa.org/MST emplate.cfm?MicrositeID=988&CommitteeID=6821(2011).

58. İnternet: Idaho National Laboratory "A Comparison of Cross-Sector Cyber Security Standards", http://www.inl.gov/scada/publications/d/a comparison_of_cross-sector_cyber_security_standards.pdf(2011).

59. Ronald L. Krutz,"Securing SCADA SystemBook",***Wiley***, 11 (2005).

60. Creery, A., Byres, E.J, "Industrial Cybersecurity for Power System and SCADA Networks", Industry Applications Society 52nd Annual***,Petroleum and Chemical Industry Conference***, 303-309 (2005).

61. İnternet: National Institute of Standards and Technology "System Protection Profile-Industrial Control Systems", National Institute of Standards&Technology http://www.isd.mel.nist.gov/documents/stouffer/NISTIR_7176.pdf (2011).

62. İnternet: National Institute of Standards & Technolog, Special Publication:800-820 "Guide to Industrial Control Systems (ICS) Security" http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (2011).

63. Bio, M. J. ve diğerleri, "IEEE Standard 1402-2000: IEEE Guide for Electric Power Substation Physical and Electronic Security", ***IEEE Power Engineering Society***, New York,1(2000).

64. İnternet:The North AmericanElectricReliability Corporation *"ReliabilityStandards "*http://www.nerc.com/page.php?cid=2%7C20(2009).

65.:İnternet:Federal EnergyRegulatoryCommissionhttp://www.ferc.gov/news/news-releases/2008/2008-1/01-17-08-E-2.asp (2009).

66. Sommestad, T., Ericsson, G.N., Nordlander, J, "SCADA System Cyber Security–A Comparison of Standards", ***Power and Energy Society General Meeting***, 1–8 (2010)

67. Hahn, A., "An Evaluation of Cybersecurity Assessment Tools on a SCADA Environment", ***Power and Energy Society General Meeting***,Detroit, Michigan, 1–6 (2011)

68. Duggan, D. P., "SAND2005-2846P: Penetration Testing of Industrial Control Systems", Technical Report, ***Sandia National Laboratories***, 1-7 (2005).

69. Christiansson, H., Luiijf, E., "Creatıng A European Scada Security Testbed", Critical Infrastructure Protection, ***IFIP International Federation for Information Processing***, 253:237-247 (2007)

70. İnternet: National Institute of Standards and Technology "Technical Guide to Information Security Testing and Assessment" http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf (2011).

71. İnternet:Control SCADA Web Portal"Nessus SCADA for Automation Control Device Assessment"http://www.controlscada.com/download-free-nessus-scada-automation-control-device-assessment (2011).

72. İnternet:Digital Bond, Inc. http://www.digitalbond.com/tools/the-rack/nessus/ (2011).

73. İnternet: Idaho National Laboraty "Lessons Learned from Cyber Security Assessments" http://www.inl.gov/scada/publications/d/nstb lessons_learned_from_cyber_security_assessments.pdf (2011).

74. İnternet: United States Computer Emergency Readiness Team "Control Systems SecurityProgram(CSSP)"http://www.us- cert.gov/control_systems/csthreats.html(2011).

75. İnternet: The Wewyork Times “Cyber Attacks on Iran — Stuxnet and Flame”, http://topics.nytimes.com/top/reference/timestopics/subjects/c/computer_malware/stuxnet/index.html(2012).

76. İnternet: The Guardian “"Anonymous Hacktivists Expose TheIntelligenceGap”, http://www.guardian.co.uk/commentisfree/2012/jan/09/anonymous-hacktivist-expose-intelligence-gap (2012).

77. Stoneburner,G., "Toward a Unified Security-Safety Model**," *IEEE Computer***, 39(8): 96-97 (2006)

78. Hentea, M., “Improving Security for SCADA Control Systems”, ***Interdisciplinary Journal of Information, Knowledge, and Management*** , 3:73-86 (2008)

79. İnternet: Sandia National Laboratories “Generic Threat Profiles SANDIA REPORT”,http://prod.sandia.gov/techlib/access-control.cgi/2005/055411.pdf (2012).

80. Lu, R., Li, X., Liang, X,Shen, X, Lin, X., "GRS: The Green, Reliability, and Security Of Emerging Machine to Machine Communications", ***Communications Magazine IEEE***, 49(4):28-35 (2011)

81. İnternet: Europen Commision Joint Research Centre Institute for The Protection and Security of the Citizen Security Technology Assessment Unit “Intrusion Detection in SCADA Systems for Critical Infrastructures”, http://sta.jrc.ec.europa.eu/index.php/scada-security/156-intrusion-detection-in-scada-systems-for-critical-infrastructures (2011).

82. Patel, S.C.,Grahamb, J.H., Ralstonb, P.A.S.,"Quantitatively Assessing the Vulnerability of Critical Information Systems: A New Method for Evaluating Security Enhancements",***International Journal of Information Management*** , 28(6):483-491, (2008).

83. Byres, E.J., Franz, M., Miller, D; "The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems", ***International Infrastructure Survivability Workshop (IISW'04),*** Lisbon (2004).

84. İnternet:The SANS Institute, http://www.sans.org/security-resources/security_plus/replay_attack_sp08.php(2011)

85. İnternet: Microsoft Corporation “Internet Protocol Security and Packet Filtering”, http://technet.microsoft.com/en-us/library/bb727017.aspx (2011).

86. Mallouhi, M.,Al-Nashif, Y.; Cox, D., Chadaga, T.; Hariri, S., "A Testbed for Analyzing Security of SCADA Control Systems (TASSCS)", ***Innovative Smart Grid Technologies (ISGT)***, 1-7 (2011).

87. Queiroz, C., Mahmood, A. Hu, J., Tari, Z., Yu, Z., "Building a SCADA Security Testbed", ***Third International Conference on Network and System Security***, Gold Coast, Australia, 357-364(2009).

88. Chen, T.M., "Stuxnet, The Real Start of Cyber Warfare?", ***IEEE Network***, 24(6):2-3 (2010)

89. İnternet: Tübitak Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi "Sosyal Mühendislik Saldırıları" http://www.uekae.tubitak.gov.tr/uekae_content_files/EtkinlikWeb/SosyalMuhendislikSaldirilari.pdf (2011).

90.İnternet:Symantec "SocialEngineering Fundamentals, Part I: Hacker Tactics" http://www.symantec.com/connect/articles/social-engineering-fundamentals-part-i-hacker-tactics (2012)

91. İnternet: Automation.com Web Portal "Protecting Water Industry Control and SCADA Systems fromCyberAttacks", http://www.automation.com/pdf articles/WaterIndustryCyberSecurity_final.pdf (2012).

92. Sarısoy, S., "Düzenleyici Devlet ve Regülasyon Uygulamalarının Etkinliği Üzerine Tartışmalar", ***Maliye Dergisi,*** 159:278-298 (2010).

93. Karakaş, M., "Devletin Düzenleyici Rolü ve Türkiye'de Bağımsız İdari Otoriteler", ***Maliye Dergisi*****,** 154:99-120 (2008).

94. İnternet:North American Electric Reliability Corporation "Security Standards for Electric Market Participants" http://www.nerc.com/docs/cip /SecurityStandardsforElectricMarketParticipants.pdf (2009).

95. Sulzberger, V., Gallagher, T., "Reliability and Security the NERC New Standards Development Process", ***IEEE Power & Energy Magazine***, 56-61 (2004).

96. İnternet: U.S. Federal Energy Regulatory Commission "Cyber & Grid Security "http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp (2011).

97. İnternet: North American Electric Reliability Corporation "Programs: Critical Infrastructure Protection" http://www.nerc.com/page.php?cid=6|69 (2012).

98. Tate, J.E., Okhravi, H., Grier, C., Overbye, T.J., Nicol, D., "SCADA Cyber Security Testbed Development", ***Power Symposium NAPS***, 483-488 (2006).

99. Naedele, M., "Standardizing Industrial IT Security-A First Look at the IEC Approach", ***Emerging Technologies and Factory Automation*****,** 2:857-863 (2005).

100. Hurd, S., "Tutorial: Security in Electric Utility Control Systems", ***61st Annual Conference for Protective Relay Engineers***, 304-309 (2008).

101. Robert, M., "New Considerations for Security Compliance, Reliability And Business Continuity", ***Rural ElectricPower Conference***, Charleston, B1:1-7 (2008).

102. İnternet: IGS Energy "AGA 12 Recommends How to Protect SCADA Communications From Cyber Attack"http://igs.nigc.ir/igs/OTHER/AGA-12-SCADA.PDF (2012).

103. İnternet: U.S. The White House "TheComprehensiveNationalCyber SecurityInitiativehttp://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative (2012).

104. İnternet: European Network and information Security Agency "Cyber Security Strategy for Germany", http://www.enisa.europa.eu/media/ news-items/german-cyber-security-strategy-2011-1 (2011).

105. İnternet: French Network and Information Security Agency "Information systems defence and securityFrance's Strategy" http://www.ssi., gouv.fr/IMG/pdf/2011-02-15_Information_system_defence_and_security_-_ France_s_strategy.pdf(2012).

106. İnternet: Ulaştırma Bakanlığı-Bilgi Güvenliği Derneği "Ulusal Siber Güvenlik Strateji Belgesi Taslağı" http://www.bilgiguvenligi.org.tr/ files/Ulusal_Siber_Guvenlik_Stratejisi (2012)

107. İnternet: Türkiye Cumhuriyeti Ulusal Bilgi Güvenliği Portalı "Erişim Kontrol Politikası Oluşturma Kılavuzu" ,http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0006-erisim-kontrol-politikasi-olusturma-kilavuzu/download.html(2012).

108. İnternet: Sandia National Laboratories "Sustainable Security forInfrastructure SCADA",http://energy.sandia.gov/wp/wp- content/gallery/uploads/ SustainableSecurity.pdf(2012).

109. İnternet: The SANS Institute "InfosecAcceptableUse Policy"http://www. sans.org/security-resources/policies/Acceptable_Use_Policy.pdf(2012).

110. Susanto H, Almunawar, M.N., Tuan, Y.C.,"Information Security Management System Standards: A Comparative Study of the Big Five", ***International Journal of Electrical & Computer Sciences***, 11(5):23-29 (2011).

111. İnternet: Processdox Team Web Portal "Configuration Change and Release Management Policies andProcedures Guide"http://www.processdox. com/ConfigChangeReleaseMgmt.pdf(2011).

112. İnternet: The Office of Electricity Delivery andEnergyReliability“21 Stepsto Improve Cyber Security of Scada Networks” http://www.oe.netl.doe. gov/docs/prepare/21stepsbooklet.pdf(2012).

113. Igure, V., Laughter, S., Williams, R., “Security Issues in SCADA Networks”, ***Computers & Security***, 498 – 506 (2006)

114. Qizhi, C., Qinquan, Q., “The Research of UNIX platform for SCADA”, ***Power Engineering Society Winter Meeting,*** 3:2041 - 2045 (2000).

115. Albertos,P., Crespo,A., Vallés, M.,"Embedded Control Systems: Some Issues and Solutions",***16th IFAC World Congress***, Prague (2005)

116. İnternet: Nmap Security Scannerhttp://nmap.org/misc/defeat-nmap-osdetect.html (2012)

117. İnternet: The USENIX Association “Defeating TCP/IP StackFingerprinting”, http://static.usenix.org/publications/library/proceedings/sec2000/full_papers /smart/smart_html/index.html(2012).

118. İnternet: National Security Agency “Operating Systems” http://www.nsa .gov/ia/mitigation_guidance/security_configuration_guides/operating_ systems.shtml(2012).

119. İnternet: İnternet: National Institute of Standards and Technology http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (2011)

120. Fovino, I.N., Carcano, A., Masera, M. ve Trombetta, A., "Design and Implementation of a Secure Modbus Protocol",***Critical Infrastructure Protection III Chapter 6,*** Springer, 311:83-96 (2009).

121. Carcano, A., Fovino, I.N., Masera, M. ve Trombetta, A., "Scada Malware, a Proof of Concept", Critical Information Infrastructure Security***, Springer***, 5508: 211-222, (2009).

122. Graham, J.H, Patel, S.C., "Security Considerations in SCADA Communication Protocols", Technical Report TR-ISRL-04-01, ***Intelligent System Research Laboratory,***Louisville, Kentucky, 8-15 (2004).

123. Patel, S.C., Bhatt, G.D, Graham, J.H, "Improving the Cyber Security of SCADA Communication Networks", ***Communications of the ACM Archive,*** 52(7): 139-142, (2009).

124. Majdalawieh, M., Parisi-Presicce, F, Duminda, W., "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework", ***Advances in Computer, Information, and Systems Sciences and Engineering***, 227-234 (2007).

125. West, A.,"Securing DNP3 and Modbus with AGA12-2J", ***Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century***, Sydney (2008)

126. İnternet: National Institute of Standards and Technology "Guide to IPsecVPNs", http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf(2010).

127. Diab, W.B., Tohme, S., Bassil, C., "VPN Analysis and New Perspective for Securing Voice over VPN Networks", ***Fourth International Conference on Networking and Services***,73-78 (2008).

128. Lee, H.K., Malkin, T.,Nahum, E., "Cryptographic Strength of SSL/TLS Servers: Current and Recent Practices", ***Proceedings of the 7th ACM SIGCOMM Conference On Internet MeasurementTable Of Contents***, San Diego, 83 - 92 (2007).

129. Elkeelany, O., Matalgah, M.M., Sheikh, K.P., Thaker, M., Chaudhry, G.; Medhi, D., Qaddour, J., "Performance analysis of IPSec protocol: encryption and authentication", ***ICC 2002 IEEE International Conference***,New York, 2: 1164-1168 (2002).

130. Paterson, K.G., Yau, A.K.L., "Cryptography in Theory and Practice: The Case of Encryption in IPsec", Advances in Cryptology - EUROCRYPT 2006,***Lecture Notes in Computer Science***, 4004:12-29(2006).

131 .Zhou., J., "Further Analysis of the Internet Key Exchange Protocol", **C*omputer Communications***, 23(17):1606-1612, (2000).

132. Alshamsi, A., Saito, T., "A Technical Comparison of IPSec and SSL", ***19th International Conference on Advanced Information Networking and Applications,***Taipei,2: 395-398 (2005).

133. İnternet: Drachma Technology, Inc "A Comparative Analysis of IPSecand SSL",https://drachma.colorado.edu/dspace/bitstream/123456789/21/1/A+ comparative+analysis+of+IPSec+and+SSL.pdf (2010).

134. Khanvilkar, S., Khokhar, A., "Virtual Private Networks: An Overview with Performance Evaluation", ***Communications Magazine*****,** 42(10): 146 – 154, (2004).

135. Vaudenay, S., "Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS", ***Proceedings of In Advances in Cryptology*****-EUROCRYPT'02**, Amsterdam, Netherlands, 534 - 545, (2002).

136. İnternet: The International Society of Automomation “Creating a SCADA-AwareDistributedFirewall”,http://www.isa.org/Content/Microsites988/SP99,_Manufacturing_and_Control_Systems_Security1/Home964/ISA-SP99 Presentations/ISA-Users-Spk1-SCADA-Aware-Firewalls-EByres-etal.pdf (2012)

EKLER

EK-1. Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

Genel

1. İşletmeniz altyapısında üretilen ve/veya iletilen ürün hangi ölçekte hizmet vermektedir
   - Sınırlı bir yerleşke içinde
   - Bir şehir içinde
   - Birkaç şehri kapsayan bir bölgede
   - Ülke genelinde
   - Uluslararası ölçekte
2. İşletmenize ait istasyonlar için aşağıdaki durumlardan hangisi geçerlidir?
   - Otomasyon sistemimiz sadece merkez birimdeki birkaç alanda yer alır, istasyonlarda bulunmaz.
   - İstasyonlarımızdaki ekipmanların çoğu manüel işletilir, çok az programlanabilir cihazlar (RTU, PLC) bulunmaktadır ve merkez birim ile haberleşmesi yoktur.
   - İstasyonlarda eskiden kalma bazı elektromekanik cihazlar var olsa da, seri haberleşme arayüzüne sahip programlanabilir cihazlar (RTU, PLC) da istasyona entegre edilmiştir. Ancak merkezle haberleşmeyi sağlayan bir ağ altyapısı (LAN ve WAN) yoktur.
   - İstasyonlarda eskiden kalma bazı elektromekanik cihazlar var olsa da, seri haberleşme arayüzüne sahip programlanabilir cihazlar (RTU, PLC) da istasyona entegre edilmiş olup merkezle haberleşmeyi sağlayan bir ağ altyapısı (LAN ve WAN) bulunmaktadır.
   - Programlanabilir cihazlar (RTU, PLC) istasyona entegre edilmiş olup merkezle haberleşmeyi sağlayan bir ağ altyapısı (LAN ve WAN) bulunmaktadır.

Organizasyon ve Personel

1. İşletmenizde daha önceden güvenlik ve risk değerlendirmesi çalışmaları gerçekleştirildi mi?
   - Evet
   - Hayır
2. İşletmenizin iş süreçlerine ilişkin sahip olduğu güvenlik sertifikasyonu (ISO 27001 gibi) var mıdır?
   - Evet. Adı/Adları:.....
   - Hayır
3. İşletmeniz faaliyetlerinden ötürü düzenleyici resmi bir kurula (EPDK, Bakanlık vb.) bağlı mıdır?
   A. Evet. Adı:.....
   B. Hayır

(Bir önceki sorunun cevabı A ise cevaplanacak)

4. İşletmenizin tabi olduğu düzenleyicinin, iş süreçlerinize ilişkin getirmiş olduğu güvenlik şartları / kriterleri bulunmakta mıdır?
   - Evet. Bunlar:.....
   - Hayır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

5. İşletmeniz merkezinde ve istasyonlarında çalışan ilgili personel, otomasyon sistemlerinin işletimi de dahil olmak üzere genel iş süreçleri güvenliği üzerine eğitimler aldılar mı?
   - o Kısıtlı sayıda personel adı. Eğitimin adı: .....
   - o İlgili tüm personel. Eğitimin adı: .....
   - o Hiçbiri almadı.
6. İşletmenizde iş süreçlerinizi otomatize etmek için kullanılan denetim ve izleme sistemleri sistemlerinin güvenliğiyle ilgili yetkili personel ve/veya çalışma gurubu bulunmakta mıdır?
   - o Evet
   - o Hayır
7. İşletmeniz ilgili personelinin otomasyon sistemlerinin işletimine yönelik uymaları gereken güvenlik politika ve prosedürü var mıdır?
   - o Evet, dar kapsamlı da olsa bulunmakta
   - o Evet, geniş kapsamlı olarak bulunmakta
   - o Hayır

Fiziki Güvenlik

1. Merkez denetim ve izleme biriminizdeki aktiviteler kamera ile kayıt altına alınmakta mıdır?
   - o Evet
   - o Hayır
2. Merkez denetim ve izleme birimine girebilecek personel daha önceden tanımlı kişiler midir?
   - o Evet
   - o Hayır
3. Merkez denetim ve izleme birimine girebilecek personel kapı giriş çıkışlarında hangi metodu kullanır? (Çoklu seçim olacak)
   - o Güvenlik görevlisi nezaretinde
   - o Anahtar ile
   - o Kartlı okuma sistemi ile
   - o Parmak okuma sistemi ile
   - o Ses tanıma sistemi ile
   - o Göz tanıma sistemi ile
4. İstasyonlarınızda aktiviteler kamera ile kayıt altına alınmakta mıdır?
   - o Evet
   - o Hayır
5. İstasyonlarınız girebilecek personel kapı giriş çıkışlarında hangi metodu kullanır? (Çoklu seçim olacak)
   - o Güvenlik görevlisi nezaretinde
   - o Anahtar ile

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

- Kartlı okuma sistemi ile
- Parmak okuma sistemi ile
- Ses tanıma sistemi ile
- Göz tanıma sistemi ile

6. Merkezdeki ve istasyonlardaki otomasyon ve ağ cihazlarının portlarına (seri, ethernet vb.) erişimi kısıtlayıcı kilitli dolap, kutu, kapı gibi tedbirler mevcut mudur?
   - Sadece merkezde
   - Sadece istasyonlarda
   - Tümünde
   - Hiçbirinde
7. Sahada çalışan personeller istasyonlardaki otomasyon ve ağ cihazlarına fiziki olarak erişebilmekte midir?
   - Tümü erişebilmektedir
   - Sadece yetkili personel
   - Hiçbiri
8. Merkez denetim ve izleme biriminin güvenliğine yönelik aşağıdaki fiziki unsurlardan hangileri bulunmaktadır?
   (Çoklu seçim yapılabilir)
   - Kapalı-kilitli ortam
   - Kapı giriş kontrolü
   - Kamera kaydı
   - Girişte 7x24 güvenlik görevlisi

Erişim Kontrolü ve Hesap Yönetimi

1. Merkezi ve uç birim otomasyon cihaz ve yazılımlarına konsoldan (cihaz başında) ve/veya uzaktan erişim için (telnet, ssh vb.) kullanım politikası mevcut mudur?
   - Evet
   - Hayır
2. İstasyonlarınızdaki uç birim otomasyon cihazlarında (RTU, PLC) bağlantı şifresi (login password) kullanılmakta mıdır?
   A. Kullanılmamaktadır ve gerek yoktur
   B. Kısmen kullanılmaktadır
   C. Tamamında kullanılmaktadır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

(Bir önceki sorunun cevabı B veya C ise cevaplanacak)

3. İstasyonlarınızdaki uç birim otomasyon cihazların bağlantı şifreleri ne sıklıkla değiştirilmektedir?
   - o Henüz üzerlerinde fabrika çıkışı öntanımlı şifreler bulunmaktadır
   - o Yılda birden daha uzun
   - o Yılda birkaç defa
4. Merkez denetim ve izleme biriminizde güvenlik duvarı (firewall) kullanılmakta mıdır?
   - A. Evet
   - B. Hayır

(Bir önceki sorunun cevabı A ise cevaplanacak)

5. Güvenlik Duvarı tanımlamaları ve kural değişiklikleri için işletilecek prosedürler belirlenmiştir midir?
   - A. Evet
   - B. Hayır

(Bir önceki sorunun cevabı A ise cevaplanacak)

6. Güvenlik Duvarı tanımlamalarında değişiklik yapıldığında diğer kurallar ve genel politikalar ile uyumluluğu incelenmekte midir?
   - o Evet
   - o Hayır
7. İşletmenizdeki merkezi ve istasyon (uç birim) otomasyon cihaz ve sistemleri uzaktan erişim servislerine (telnet, ssh vb.) sahip midir?
   - o Evet
   - o Hayır
   - o Bazıları
8. Merkez denetim ve izleme biriminizde kullanılan ağ cihazları (router, switch gibi) aşağıdaki erişim denetimlerinden hangileri kullanılmaktadır?
   (Çoklu seçim yapılabilir)
   - o VLAN
   - o MAC filtreleme
   - o IP filtreleme
   - o Yönlendirme kısıtlama
   - o Farklı ağlar için farklı cihaz kullanımı (fiziki izolasyon)
   - o Hiçbiri
9. İşletmedeki farklı birimlerin (muhasebe, pazarlama vb.) kullandığı ağlardan merkezdeki ve istasyonlardaki otomasyon cihaz ve yazılımlarına erişebilmekte midir?
   - o Evet
   - o Hayır, tamamen izole yapıdadır
   - o Bazılarına

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

10. SCADA/DDS sistemini sadece izlemekle mesul operatörlerin, uygulama sunucularına bağlanma, program açma kapama; CD/DVD-ROM ve USB disk bağlama; ethernet kablolarını değiştirebilme gibi imkanları bulunmakta mıdır?

    - o Evet
    - o Hayır

11. Şirket dışı ağlardan (internet üzerinden veya çevirmeli modemle) bakım, kontrol gibi nedenlerle merkezdeki ve istasyonlardaki otomasyon cihaz ve sistemlerine uzaktan erişebilme izin verilmiş midir?

    A. Evet, verilmiştir ve hiçbir erişim kısıtlama yoktur
    B. Belirli IP ve modem numaralarına erişim hakkı verilmiştir
    C. Hiçbir suretle işletme dışından sistemlere erişim hakkı verilmemiştir.

(önceki sorunun cevabı B veya C ise)

12. Üretici/Tedarikçi firmalar arıza gibi acil durumlarda sahadaki programlanabilir cihazlara veya merkezdeki sunuculara ne şekilde bağlanmaktadır?
    - o İnternet bağlantısı ile doğrudan sunucu ve sahadaki cihazlara
    - o Önce internet üzerinden İşletme merkezine VPN ile ve oradan sunucu ve sahadaki cihazlara
    - o Önce çevirmeli modemle İşletme merkezine VPN ile ve oradan sunucu ve sahadaki cihazlara
    - o Çevirmeli modemlerle doğrudan sahadaki cihazlara
    - o GSM/GPRS modemle doğrudan sunucu ve sahadaki cihazlara
    - o İşletme merkezine mutlaka gelir ve bakım/müdahale yerinde yapılır
13. İşletmenizdeki merkez ve istasyon otomasyon cihaz ve uygulama yazılımları farklı erişim rolleri tanımlama imkânı vermekte midir? (İzleme Kipi, Temel bakım kipi ve tüm fonksiyonları çalıştıran Yönetici Kipi gibi)
    - o Hiçbiri vermemektedir
    - o Sadece belirli cihaz ve yazılımlar
    - o Tümü

(önceki sorunun cevabı b veya c ise)

14. Farklı yetki ve sorumluluktaki personelleriniz için işletmenizdeki merkezi ve istasyon otomasyon cihaz ve uygulama yazılımlarına bağlanırken farklı erişim rolleri tanımlanmış mıdır?
    - o Evet
    - o Hayır
    - o Kısmen

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

15. İşletmenizde, Merkez ve istasyon otomasyon cihaz ve yazılımları için kullanıcı rolü tanımlayan güvenlik politikası mevcut mudur?
    - o Evet
    - o Hayır
16. Merkezi ve istasyon otomasyon cihaz ve yazılımlarına uzaktan erişimi kayıt altına alan (kullanıcı adı, IP vb.) kayıt (log) sunucusu bulunmakta mıdır?
    - o Evet, sadece merkez birimlerdeki erişimler kayda alınmaktadır
    - o Evet, sadece istasyonlardaki erişimler kayda alınmaktadır
    - o Evet, tüm erişimler kayda alınmaktadır
    - o Hayır, hiçbir erişim kayıt altına alınmamaktadır

17. Merkez Denetim ve İzleme Biriminizde saldırı tespit sistemi kullanılmakta mıdır?
    - o Evet
    - o Hayır

İletişim ve İletişim Güvenliği

1. İstasyonlardaki cihazlarla merkezi birim arasındaki iletişimi sağlamada hangi iletişim hatları kullanılmaktadır

(Çoklu seçenek)

- o Fiber optik hatlar (Metro ethernet, SDH)
- o Kiralık E1 hatları
- o Frame-Relay
- o G.SHDSL
- o Çevirmeli modem (Dial-up)
- o Özel tahsisli Radyo Frekansları
- o Ortak kullanımlı Radyo Frekansları
- o 802.11 WiFi
- o 802.16 WiMAX
- o Uydu
- o Enerji Nakil Hatları (Power Line Carrier)
- o GSM Modem
- o GPRS
- o 3G/UMTS
- o İnternet bağlantısı (ADSL vb.)
- o Diğer

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

2. İşletmeniz istasyon-merkez birim haberleşmesinde kullandığı erişim hatları kendisine mi aittir?

   (Çoklu seçenek)

   - o Evet, kendi çektiği fiber-optik hatları bulunmaktadır
   - o Evet, kendi çektiği bakır hatları bulunmaktadır
   - o Evet, kendi yönetiminde telsiz/kablosuz hatları bulunmaktadır
   - o Sabit telekomünikasyon operatörlerinden kablolu hat/devre kiralamaktadır
   - o Mobil telekomünikasyon (GSM, 3G) operatörlerden kablosuz hat/devre kiralamaktadır

3. Farklı istasyonlardaki programlanabilir cihazlar veya modemler arasında doğrudan haberleşme gerçekleşmekte midir?

   - o Evet
   - o Hayır

4. İstasyonların kendi içinde ve merkezle iletişiminde hangi endüstriyel iletişim protokolleri kullanılmaktadır?

(Çok Seçenekli)

   - o DNP 3.0 (Seri)
   - o DNP 3.0 (TCP)
   - o Modbus (Seri)
   - o Modbus (TCP)
   - o Modbus Plus
   - o Ethernet /IP
   - o ControlNet
   - o Profibus
   - o Fieldbus
   - o Üretici Firmaya Özel (Belirtiniz: .....)
   - o Diğer (Belirtiniz:.....)

5. İstasyonlarınızdaki uç birim otomasyon cihazların kendi aralarında veya merkezle yaptıkları haberleşmede veri şifreleme teknikleri (kriptolama) kullanılmakta mıdır?

   A. Kullanılmamaktadır ve çünkü buna ihtiyaç hissedilmemiştir
   B. Kullanılmamaktadır çünkü cihazlar desteklememektedir
   C. Kullanılmamaktadır çünkü şifreli iletişimin gerçek zamanlı otomasyon süreçlerini etkileyebileceği düşünülmektedir.
   D. Mevcut şifresiz çalışan sisteme müdahale etmek istenmediğinden kullanılmamaktadır.
   E. Kullanılmamaktadır ancak kullanımı planlama aşamasındadır
   F. Kısmen kullanılmaktadır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

G. Tamamında kullanılmaktadır

(Bir önceki sorunun cevabı E, F veya G ise cevaplanacak)

6. İstasyonlarınızdaki uç birim otomasyon cihazları hangi kriptolama servislerini desteklemektedirler ?

(İlk 6 seçenek için çoklu seçim yapılabilir)

- o AES (Simetrik)
- o 3DES (Simetrik)
- o RSA (Asimetrik)
- o DSA (Asimetrik)
- o MD5 (Hash)
- o SHA1/2 (Hash)
- o Cihaza özgü (Property/ Müseccel)
- o Bilinmiyor
- o Diğer. Adı:.....

7. İstasyonlarınız içindeki, kontrol edilen saha ekipmanlarıyla saha denetleyicileri (IED, PLC, RTU) arasında ne tür bağlantılar bulunmaktadır?

(Çoklu seçenek)

- o Seri kablo
- o Cat5 / Cat 6 bakır kablo
- o Koaksiyel kablo
- o Radyo Frekansları (UHF-VHF Telsiz ağı)
- o 802.11 WiFi
- o IWLAN (Industrial Wireless LAN)
- o IEEE 802.15
- o Ultra-wideband (UWB)
- o Zigbee
- o Bluetooth
- o Enerji Nakil Hatları Üzerinden Haberleşme (Power Line Communication)
- o Diğer

Sistem Güncelleme ve Yedeklilik

1. İşletmenizde, 'değişiklik yönetimi' politika veya prosedürleri bulunmakta mıdır?

- o Evet
- o Hayır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

2. İşletmeniz otomasyon altyapısında kullanılan sunuculardaki işletim sistemlerinin güncellemeleri ve yamalamaları yapılmakta mıdır?
- o Evet, düzenli olarak
- o Evet, ama uzun aralıklarla
- o Hayır, çünkü gerek duyulmuyor
- o Hayır, çünkü çalışan sistemi etkileyebilir

3. İşletmenizde kullanılan sunucu ve PLC, RTU gibi istasyon cihazların yazılım (firmware) güncellemeleri yapılmakta mıdır?
- o Evet, düzenli olarak
- o Evet, ama uzun aralıklarla
- o Hayır, çünkü gerek duyulmuyor
- o Hayır, çünkü çalışan sistemi etkileyebilir

4. Bir hata durumunda geriye dönebilmek için (rollback) sistem yazılım (firmware, OS) ve yapılandırma dosyalarının (konfigürasyon) saklandığı merkezi depolama birimi var mıdır?
- o Evet sadece merkez birimlerdeki cihaz ve yazılımlar için
- o Evet sadece istasyonlardaki cihaz ve yazılımlar için
- o Evet tüm cihaz ve yazılımlar için
- o Hayır

5. İşletmeniz de üretici desteği kalkmış donanım, işletim sistemi, uygulama yazılımı kullanılmakta mıdır?
- o Evet
- o Hayır

6. Üzerinde kritik uygulamalar çalışan merkezi sunuculardan bir veya birkaçının arızalanması durumunda yerine geçmeye hazır başka bir sunucu bulunmakta mıdır?
- o Evet, yedek derhal devreye girer
- o Evet, ancak bazı ayar ve değişiklikler ile yedek devreye girer
- o Hayır

7. Sistem merkezinde önemli bir hasar durumunda (yangın, su baskını vb.) sistemin yönetimine devam edilecek başka bir yer var mıdır?
- o Evet, sistem coğrafi yedeklidir, yedek derhal devreye girer
- o Evet, ancak bazı ayar ve değişiklikler ile yedek devreye girer
- o Hayır

8. İstasyonlardaki cihazlar ile merkez arasındaki hatların yedeği bulunmakta mıdır?
- o Evet. Nasıl bir yedekleme?.....
- o Hayır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

9. Sistem merkezinde kullanılan sunucu ve cihazlar için kesintisiz güç kaynağı ve jeneratör kullanılmakta mıdır?
- o Evet
- o Hayır

10. İstasyonlarda kullanılan IED/ PLC/ RTU cihazları için kesintisiz güç kaynağı ve jeneratör kullanılmakta mıdır?
- o Evet
- o Hayır

Denetim

1. Sistem salonlarına girişi çıkışlara ait (kartlı giriş/çıkış-kamera vb.) kayıtlar saklanmakta mıdır?
- o Evet
- o Hayır

2. Sistem sunucu ve cihazlarına kullanıcı (users) ve yöneticilerin (administrators) bağlantı işletmeleri (login) ve sistem üzerindeki aktivitelerine ait log bilgileri tutulmakta mıdır?
- o Evet
- o Hayır
- o Bazı sunucu ve cihazlar için
- o Bazı kullanıcılar için

3. Sistem sunucu ve cihazlarına bağlanan kullanıcı ve operatörler aynı kullanıcı adı ve şifreyi kullanırlar mı?
- o Evet
- o Hayır

4. Sistem sunucu ve cihazlarına bağlanan kullanıcı ve operatörlerin şifre seçimi (karakter sayısı ve türleri gibi) ve aynı şifreyi kullanım süresi ile ilgili belirlenmiş ve takip edilen kurallar bulunmakta mıdır?
- o Evet
- o Hayır

5. Sistem sunucu ve cihazlarında, işletim sistemi ve uygulama yazılımlarda oluşan hatalara (system error vb.) ilişkin log bilgileri tutulmakta mıdır?
- o Evet
- o Hayır
- o Bazılarında

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

6. Sistem haberleşme altyapısında trafik akışı (hangi cihazdan hangisine doğru veri akışı olduğu) ve türü (HTTP, DNP vb gibi) izlenmekte midir?

- o Evet, tüm şebekenin trafiği izlenmektedir.
- o Sadece merkezdeki sistemlerin trafiği izlenmektedir
- o Hayır böyle bir takip yapılmamaktadır.

7. Sitemde bilgi sızmaları ve var olan açıklıklara karşı tarama ve inceleme testleri gerçekleştirildi mi?

A. Evet, kapsamlı bir test gerçekleştirildi
B. Evet, kısmı testler gerçekleştirildi
C. Hayır, çünkü bu testlerin sistemi kararsız hale getirebileceği kuşkusu taşınmakta
D. Hayır, çünkü böyle bir ihtiyaç hissedilmedi

(Bir önceki sorunun cevabı A veya B ise)

8. Sitemde bilgi sızmaları ve var olan açıklıklara karşı tarama ve inceleme testleri ne sıklıkta yapılır?

- o Sadece sistem kabul sırasında yapıldı
- o Kabul sonrası bir kez yapıldı
- o Birkaç kez yapıldı
- o Düzenli olarak yapılmaktadır

9. İşletmenizde, sosyal mühendislikle (telefon, internet veya kişisel münasebetlerle altyapı topolojisi, şifre vb. önemli bilgilerin ifşası) bilgi sızmalarına karşı personeli bilgilendirme/ farkındalık faaliyetleri düzenleme gibi tedbirler alınmakta mıdır?

- o Hayır
- o Evet

Dış Kaynak Kullanımı

1. İşletmenizde kullanılan sunucu, cihaz ve uygulama yazılımlarının bakımı için dış kaynak (tedarikçi firma veya destek firması) kullanımı mevcut mudur?

a. Evet
b. Hayır
c. Sadece problem durumunda

(Bir önceki sorunun cevabı A veya C ise)

2. Tedarikçi ve/veya destek firmalarıyla gizlilik ve uygun kullanım sözleşmesi yapılmış mıdır?

- o Evet
- o Hayır

EK-1. (Devam) Kritik Altyapılarda Kullanılan Denetim Sistemleri Açıklık İncelemesi Anket Soruları

3. Tedarikçi ve/veya destek firmalarının tek başına sistem merkezlerine girebilmelerine ve cihazlarına bağlanmalarına izin verilmekte midir?

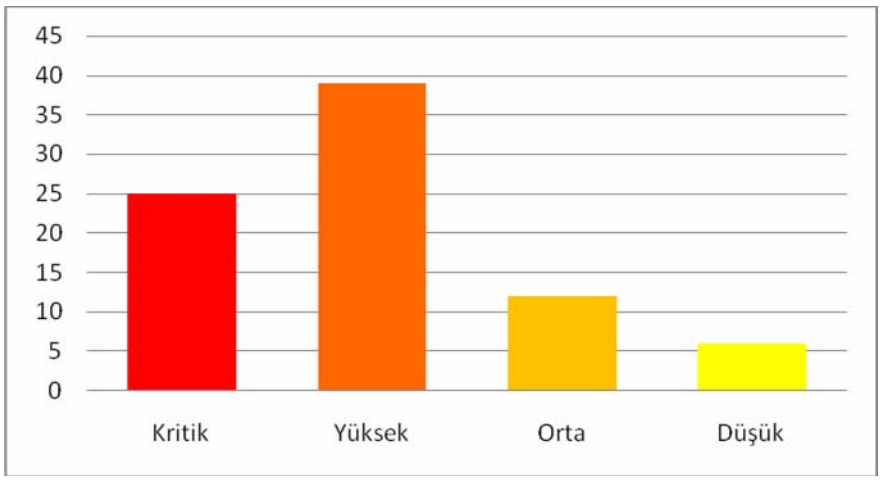
- o Evet
- o Hayır

4. İşletmenize alınan otomasyon ve bilgi sistemleri altyapı donanım ve yazılımlarında 'önceden belirli güvenlik şartları' aranmakta mıdır?

- o Evet. Kendi oluşturduğumuz güvenlik kriterleri/şartları aranmaktadır.
- o Evet.....standardındaki güvenlik kriterleri/şartları aranmaktadır.
- o Hayır

EK-2. İncelemelerde Elde Edilen Açıklık Bulguları ve Çözüm Raporu Hakkında

Ağ ve sistem taramalarının gerçekleştirildiği birinci örnek durum incelemesinde, altyapıdaki tüm varlıklar üzerinde, 25 kritik, 39 yüksek, 12 orta, 6 düşük olmak üzere toplam 82 güvenlik açıklığı tespit edilmiştir.



Örnek Durum I incelemesi için ağ ve sistem taramalarından elde edilen açıklık bulgularının sayıları

Taramalardan elde edilen açıklık bulguları sırasıyla;

I. İşletim sistemleri ve üzerlerindeki servis ve uygulamalardan,
II. İletişim ağı ve iletişim protokollerinden,
III. Kullanılan veritabanlarından

kaynaklanmaktadır. Ağ ve sistem taramalarına ilaveten yürütülen anket, mülakat ve diğer saha incelemeleri birlikte ele alındığında, tespit edilen önemli açıklık bulgularının;

IX. Kullanılmayan servisler
X. Kullanılmayan ağ protokolleri
XI. Sıkılaştırılmamış ve yamalanmamış işletim sistemleri,
XII. Kullanılan endüstriyel iletişim protokolleri
XIII. Erişim denetimi ve hesap yönetimi kusurları
XIV. Değişiklik yönetimi ve yedekleme eksikliği
XV. Sosyal mühendislik,
XVI. İnsan kaynakları ve eğitim eksikliği

gibi nedenlerinden kaynaklandığı tespit edilmiştir. Somut güvenlik açıklıkları, açıklık kaynakları ve giderilmesine yönelik çözüm önerileri ortak çalışma yürüten işletmeciye 136 sayfalık rapor halinde ayrıca sunulmuştur.

EK-3. Denetim Sistemi Kullanan Kritik Altyapılar içinSiber Güvenlik Strateji Belgesi Önerisi

1. Giriş

BT ve DDS sistemlerin toplum hayatında kapladığını yerin her geçen gün artması ve maruz kalabilecekleri saldırıların ortaya çıkarabileceği yıkıcı ve katlanılmaz sonuçlar bu konuda stratejik bir yaklaşımın geliştirilmesini zorunlu kılmıştır. Bugüne kadar güvenlik stratejileri ağırlıklı olarak fiziki güvenliğe dayandırılsa da birçok hizmet ve üretimin BT/DSS altyapılarına dayandığı günümüzde bu yaklaşımın daha fazla geçerliliği kalmamıştır.

Elektrik, doğalgaz, petrol, su altyapıları ile birçok modern endüstriyel üretim tesisleri ülkeler için ekonominin işlemesi, modern toplum ihtiyaçlarının ve düzeninin sağlanması için vazgeçilmez tesisler olup, birçok ülke tarafından kritik altyapılar sınıfına dahil edilmektedir. Bu altyapıları diğer BT altyapılarından farklı kılan ortak özellikleri, sahadaki fiziki süreç ve unsurlarını "denetim sistemleri" üzerinden izlemeleri ve yönetmeleridir. BT altyapılarına yönelik saldırılar çoğu durumda kurum ve işletmelerin bilgi varlıkların çalınması, değiştirilmesi, tahrif veya imha edilmesi gibi sonuçlar doğururken, çoğunluğu kamunun fiziki ihtiyaçlarını karşılayan üretim, iletim, dağıtım tesis ve altyapılarının denetim sistemlerine (SCADA/DDS) yönelik saldırılar çalışanların ve hizmet alanların can ve mal emniyetinin tehlikeye düşmesi dahil çok daha yıkıcı sonuçların doğmasına sebebiyet verebilirler. Dolayısıyla kritik altyapılarda kullanılan denetim sistemlerinin siber güvenliği, toplumun refahını, can ve mal güvenliği ile doğrudan ilgilidir. Bu nedenle, birçok ortak unsur barındırsa da BT ve DDS altyapıların siber güvenlik ihtiyaçlarındaki farklılıklarını da dikkate alan bir güvenlik yaklaşımının geliştirilmesine ihtiyaç bulunmaktadır. Önerilecek iyileştirmeler adımları da DDS sistemler için yeniden veya ayrıca tanımlanan güvenlik ihtiyaçlarına uygun olarak belirlenmelidir.

Geçmişte diğer ağ ve BT yapılarından izole olan ve kendine özgü ürünleri kullanan DDS'ler artık bilgi ve iletişim dünyasında yaşanan yakınsama ve gelişmelerden etkilenerek, kendi 'ayrı' durumunu koruyamamıştır. Bu sebeple DDS kullanan kritik altyapılar için ön kabule dayalı 'güvenlidir' yaklaşımı ve aşağıda sayılı nedenlerden ötürü geçmişteki güvenlik paradigması artık değişmiştir. Bu değişimi mecbur kılan şartlar özetle;

- Mobil ve sabit erişilebilirliğin yaygınlaşması,
- IP temelli protokolünün veri iletişiminde standart hale gelmesi ve bu durumunun bilgisayar temelli tüm cihazları doğrudan veya dolaylı erişilebilir hale getirmesi,
- Kapalı ağların kolay izlenebilirlik, uzaktan yönetim, işletmelerin diğer ağlarına farklı nedenlerle veri aktarma ihtiyaçları nedeniyle uzak erişimlere veya internete açılması,
- BT altyapılarının maruz kalabileceği saldırıların DDS altyapıları için de geçerli olmaya başlaması,

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

- Doğrudan endüstriyel denetim sistemlerine yönelik devlet destekli kötücül yazılımların ve saldırıların varlığı (Stuxnet gibi)
- Son yıllarda gerçekleşen ve birçok kaynakça siber savaş olarak adlandırılan olaylar

DDS sistemlerinin güvenliği tek başına bu altyapıları kullanan işletmecilerin çabalarıyla sağlanamayacak kadar çok boyutludur. ABD ve bazı AB ülkelerinde SCADA/DDS kullanan hizmet ve üretim altyapılarının güvenliğine yönelik yasal düzenleme ve kamu fonlarına dayalı araştırma-iyileştirme çalışmalarının yapıldığı bilinmektedir. Bu nedenlerle, Türkiye için de başta yasa koyucu, uygulayıcı, uygulatıcı ve denetleyicileri olmak üzere tüm paydaşlara düşen görev ve sorumlulukların belirlenmesi ve bunların yerine getirilmesi gerekmektedir.

Bu belgede, temel kavramlar, stratejik hedefler, stratejinin hayata geçilmesinde rol sahibi olacak tüm paydaşların görev ve sorumluluklarının tanımlanması ayrı birer bölüm olarak ele düzenlenmiştir. Bu bağlamda, Türkiye'nin bugünkü durumu ve şartları dikkate alınarak orta ve uzun vade de yapılması ve dikkate alınması gereken hususlar sunulmuştur.

2. Temel Kavramlar

Siber Saldırılar:

Hedef seçilen işletmelerin BT ve DDS altyapılarına bir yolla erişilerek, veri ve bilgilerinin çalınması ve/veya değiştirilmesi, sunduğu hizmetlerin kısmen veya tamamen engellenmesi, uygunsuz komutlar icra edilerek iş süreçlerinin amacı dışına çıkarılması suretiyle zarar verilmesidir.

Siber saldırılar amaçlarına göre aşağıdaki gibi ikiyi ayrılabilirler:

- *Psikolojik Siber Saldırılar:* Saldırganların, hedef seçtikleri işletmenin altyapısına zarar vermekten ziyade psikolojik etki oluşturmak ve böylece işletme idaresinin veya tüm kamuoyunun dikkatini çekmeye yönelik propaganda yapmak amacıyla yürüttükleri saldırı türüdür. Kurumsal web sayfalarının indeksinin değiştirilmesi, internet bant genişliklerinin tüketilmesi gibi saldırılar kalıcı tahribat oluşturmayan psikolojik saldırılara örnek olarak verilebilir.
- *Gerçek Siber Saldırılar:* Güçlü bir motivasyonun ürünü olarak bir devlet, çıkar grubu veya örgütçe başka bir devlete, kuruma veya işletmeye, tıpkı fiziki saldırılarda olduğu gibi, doğrudan zarar vererek veya sahip olduğu imkânlarından mahrum bırakarak bir şeye zorlamak amacıyla yapılan saldırılardır.

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

Siber Saldırılar kullanılan yöntem ve sonuçlarına ikiye ayrılabilirler:

- *Pasif Saldırılar:* Sistemlerinin çalışmasına doğrudan zarar vermeyen ancak sisteme ait veri veya bilgilerin ele geçirilmesinde kullanılan saldırılardır. Açıktan bir zarar vermemesi nedeniyle tespit etmek çoğu durumda güçtür. Pasif saldırılar bazı durumlarda aktif saldırılar için ön bilgi toplamaya yönelik hazırlayıcı saldırılardır.
- *Aktif Saldırılar:* Bir veri veya komutu değiştirmek suretiyle sistemi bozmaya, işlevini doğru olarak icra edemez hale getirmeye yönelik saldırılardır.

Siber Güvenlik:

Siber saldırılara karşı oluşturulmuş strateji, politika, prosedür ve uygulamaların tümünü içeren ve değişen şartlara uygun olarak değiştirilen ve geliştirilen süreçler bütünüdür. Her bir varlığının taşıdığı değerle orantılı olarak korunmasına yönelik tedbir imkânlarının oluşturulmasına dayanır. Teknik uygulama ve sistem bileşenleri (güvenlik duvarı, saldırı tespit sistemi, antivirüs gibi) gerektirir ancak başta yazılı güvenlik belgelerinin ve rehberlerinin oluşturulması, uygulamaların denetlenmesi, kullanıcıların eğitimi, hesap verebilirliğin etkin hale getirilebilmesiyle mümkün hale getirilebilir.

3. Stratejik Hedefler

Stratejinin başarılı olması için hangi unsurlarla hayata geçirileceğin ve oluşturulacak her yapıdan nelerin hedeflendiğinin net olarak tanımlanması gerekir.

Hedef 1: Mevzuatın hazırlanması

Kritik altyapıların güvenliğine ihtiyaç her türü yapının oluşturulabilmesi için öncelikle yasal altyapılarının oluşturulması gerekir. Oluşturulacak mevzuat aşağıdaki hususların gerçekleştirilmesine imkan sağlamalıdır.

- Kurumsal yapıların oluşturulması,
- İlgili kamu kurumları, sivil toplum kuruluşları, üreticiler ve ticari işletmeler dâhil tüm paydaşların rol ve sorumluluklarının belirlenmesi,
- Siber güvenlik teşvik, desteklerine öncelik sağlanması

Hedef 2: Kurumsal yapıların oluşturulması

Stratejide ortaya konulan hedeflere uygun ilerlenebilmesi, karar alma, uygulama ve uygulatma mekanizmalarının oluşması kurumsal yapılara ihtiyaç vardır. Bu bağlamda oluşturulması gereken kurumsal yapılar:

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

- Stratejik hedeflere uygunluğu izleyen, mevzuatta tanımlı olmayan hususlarda düzenleme hakkına sahip karar alıcı bir düzenleme kurulu,
- BT ve DDS altyapılarına dayanan kritik sektör birliklerinin siber güvenlik alanında özdenetim kapasitelerinin oluşturulması, aralarındaki ilişki ve paylaşımlarım organize edilmesi ile uzmanlık, danışmanlık, eğiticilik ve denetçilik için gerekli kriter ve yetkilendirmelerin yapılmasından sorumlu icra, yetkilendirme ve koordinasyon kurumu,
- Kritik altyapı işletmecilerin çalışmalarına karşılıksız danışmanlık hizmeti veren ve uzmanlardan oluşan bir destek kuruluşları,
- İşletmelere getirilecek yükümlülüklere uygulanıp uygulanmadığını denetleyecek kuruluşlar,
- Gerekli insan unsurunu yetiştirecek eğitim kurumları.

Hedef 3: Ülke kritik altyapıları için sürdürülebilir siber güvenlik unsurlarının oluşturulması

Kritik altyapılarda siber güvenliğin sürdürülebilir olması, oluşturulacak mevzuatın ve kurumsal yapıların işlerlik kazanması için aşağıdaki güvenlik unsurların hayata geçirilmesine ihtiyaç bulunmaktadır.

- Uzman insan kaynağının yetiştirilmesi, mevcut kaynakların geliştirilmesi
- Kullanıcı, yönetici ve karar vericilerin eğitimi,
- Güvenlik standartlarının oluşturulması, uygulanması ve denetlenmesi,
- BT/ DDS yazılım ve donanımlarının yerli üretiminin teşvik edilmesi,
- Sektörel düzeyde siber güvenlik ihtiyaçlarının belirlenmesin
- Test yataklarının oluşturulması ve laboratuarlarının kurulması,
- Siber olayları izleme ve müdahale ekiplerinin oluşturulması

4. Paydaşların Tanımlanması, Görev ve Sorumlulukları

Düzenleyiciler:

Kritik altyapılarda siber güvenlik gereksinimlerinin belirlenmesi, uygulatılması ve denetlenmesi düzenleyici kuruluşlar eliyle yürütülebilir. Düzenleme doğrudan bir kamu kurumu eliyle yapılabileceği gibi ilgili sektör birlikleri üzerinden özdüzenlemeyle de gerçekleştirilebilir.

Düzenleyicilerin şart koşacağı gereklilikler sadece ilgili altyapı işletmecilerini değil BT/DDS bileşenlerini üreten ve entegrasyonunu sağlayan şirketleri de yakından ilgilendirecektir.

Türkiye'de belirli sektörler için doğrudan düzenleyici kuruluşlar (örneğin enerji için EPDK gibi) oluşturulmuş olsa da bazı kritik sektörler için (örneğin su dağıtım gibi) doğrudan ilişkilendirilecek

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

düzenleyici kuruluşlar bulunmamaktadır. Bu nedenle, ilgili her sektör için siber güvenlik gereksinimlerini belirleyecek ve denetleyecek düzenleyici bir yapı oluşturulmalıdır.

Üretim ve hizmetlerinde BT ve DDS altyapısının yoğun olarak kullanan sektörlerin ilgili birliklerinin siber güvenlik için özdüzenleme kapasiteleri arttırılmalıdır.

İşletmeciler:

İşletme yöneticileri, kendi önceliklerine uygun olarak aldıkları kararlarla işletmelerinin nasıl işletileceğini belirlerler. Yöneticilerin kararları üzerindeki en önemli etmen çoğunlukla piyasa şartları ile sahip olunan imkânlarının sınırlarıdır. Siber güvenlik ise, tecrübe edinilen ciddi bir olay veya karşılığında maliyetinin üzerinde yaptırım olan bir düzenleyici gereksinimi yoksa işletmeler için bir gereklilik haline gelmeyecektir. Diğer bir problem de siber güvenliğin birçok sektör için odak iş ve hizmet dışında bir uzmanlık gerektirmesidir. Tüm bu sebeplerden ötürü, kritik altyapı işletmecileri için düzenleyiciler tarafından hem güvenlik gereklilikleri belirlemeli hem de işletmelerin ihtiyaç duyacakları uzmanlığa ve danışmanlığa ulaşabilmelerini sağlamalıdır.

Teknoloji Üreticileri:

BT/DDS yazılım ve donanım üreticileri müşterileri olan işletmelerin ihtiyaçlarına uygun çözümler üretirler. İşletmecilerin ürün tercihlerini belirleyen şartlar arasında çoğunlukla fonksiyonellik ve ucuzluk yer alır. Ancak düzenleyicilerin işletmecilerde aradığı güvenlik gereklilikleri işletmecilerde ürün tedarikçilerinden arayacaktır. Bu nedenle düzenleyici gereklilikleri üreticiler üzerinde de önemli etki oluşturacaktır. Düzenleyicilerin şart koşacağı her husus üreticilere de yön verecek biçimde hazırlanmalıdır.

Özellikle kritik altyapılarda kullanılacak BT/DDS yazılım ve donanımların yerli üretimi ve işletmeciler tarafından kullanımı teşvik edilmeli, yerli ARGE projelerine destek sağlanmalıdır. Ürün geliştirmede açık kaynak kodlu mevcut yazılımlardan da gerekli kontroller yapılarak faydalanılmalı, veri ve trafiğinin gizliliği ve bütünlüğü için mevcut yöntemlerde dışa kapalı özelleştirmeye gidilmelidir.

Yerli üreticilerin ve ithalatçıların ürünlerinin, düzenleyici gerekliliği olarak ortaya konulan siber güvenlik fonksiyonlarını sağlayıp salamadıkları oluşturulacak inceleme laboratuarlarınca test edilmelidir.

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

5. Somut Adımlar

İş süreçlerinde BT ve DDS sistemlerini etkin olarak kullanan kritik sektör ve işletmeciler için, Türkiye'deki ilgili kurum ve kuruluşlar eliyle yapılması gerekenler özetle aşağıda önerilmiştir.

- Mevcut güvenlik standartları (ISO 27001, ISA TR99-01/02, NIST SP800-82, NERC CIP, IEC 62351, API 1164 gibi) ile EK-4'de yer alan "Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi" belgesindeki güvenlik yaklaşım ve iyileştirmelerinden yararlanılarak, dağıtık denetim sistemi kullanan kritik altyapı işletmecileri için siber güvenlik gereklilik ve en iyi uygulama örneklerinin tanımlanması, 'TR-DDS Güvenlik Standardı' başlığında yayımlanması ve düzenleyiciler eliyle tanımlanan standardın ilgili sektörlerin kullanımına sunması,
- Üretici, işletmeci ve araştırmacılar için milli SCADA/DDS test yatağının oluşturulması, geliştirilecek veya uygulanacak teknik güvenlik mekanizmaların bu test ortamlarında (ağ ve uygulama penetrasyon testleri dahil) sınanması,
- Yerli olarak geliştirilecek olan veya ithal edilen ürünlerin düzenleyici gereksinimlerine uygunluğunun kurulması önerilen milli test yataklarında incelenmesi, uyumluluk ve penetrasyon testlerinin yapılması ve sertifikalandırılması,
- DDS kullanan kritik altyapı işletmecilerinin altyapı alım şartnamelerinde, belirlenecek standartlara uygun, milli test ortamlarında incelenmiş ve sertifikalandırılmış ürünlerin yer almasının sağlanması,
- İş süreçlerini DDS ile otomatize eden kritik altyapı işletmecilerinin ilgili personeli için eğitim müfredatı hazırlanması, güvenlik eğitimlerinin ilgili düzenleyiciler veya özdüzenleyiciler tarafından yetkilendirilmiş eğitim kuruluşlarınca verilmesi, eğitim alanlarının yapılacak sınav karşılığı sertifikalandırılması,
- Kritik altyapı işletmelerinde DDS sistemlerinin izleme, işletim ve yönetiminden sorumlu olarak çalışanlar için ilgili düzenleyici veya özdüzenleyici kuruluşlar tarafından sınavlarda başarılı olma karşılığı verilmiş sertifika şartlarının aranması,
- Hazırlanacak Milli DDS Güvenlik Standardına uygunluğu denetleyecek akredite edilmiş denetleme kuruluşlarının oluşturulması; işletmecilerden denetleme raporlarının, kullanılan ürün ve çalıştırılan personele ilişkin sertifikaların belirli aralıklarla ilgili düzenleyiciler tarafından istenmesi,
- Her sektör için kendi içinde ve tüm sektörler için merkezi bir veritabanında 'siber olay' günlüklerin oluşturulması, raporlanan olayların, merkezi ve yetkili bir birimce ("Siber Olaylara Müdahale Ekibi" gibi) değerlendirilmesi; ulusal güvenlik açıklıkları veritabanı

EK-3. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Siber Güvenlik Strateji Belgesi Önerisi

oluşturulması ve yeni keşfedilen açıklıklar hakkında tüm işletmecilere çözümleriyle birlikte acil bilgi ulaştırılması (erken uyarı ve bilgilendirme kanallarının oluşturulması),

- Siber saldırı ve olaylara karşı farkındalık ve bilincin yüksek tutulması için, ilgili düzenleyicilerin kendi sektörü için en fazla 6 ayda bir, tüm düzenleyiciler için kendi aralarında en fazla yılda bir kez toplanmasının sağlanması ve katılımcılardan yürütülen çalışmalarla ilgili raporlar istenerek aktif katılımlarının sağlanması,
- Yerli araştırmacı ve geliştiricilerin;
    - SCADA/DDS merkez ve uç birim uygulamalarını geliştirmeleri,
    - Açık kaynaklı işletim sistemi ve protokollerden de yararlanarak, sıkılaştırılmış, görev odaklı olacak şekilde minimize edilmiş ve güvenlik fonksiyonları ilave edilmiş işletim ve iletişim platformlarının oluşturulmasının sağlanması,
    - Geliştirilen iletişim protokollerini tanıyan ve fonksiyon bazında filtreleme ve inceleme yapan güvenlik duvarları, saldırı tespit sistemleri vb. güvenlik bileşenlerini geliştirilmesi,

  sağlanmalı ve bu çalışmalar öncelikli ARGE teşvikleri sınıfına dâhil edilmelidir.
- Yerli geliştirilen ürün ve uygulamalarının güçlü destek ağlarının kurulması ve Türkiye'deki kritik altyapılarda kullanılan denetim sistemlerinde yerli uygulamalarının kullanımına öncelik verilmesi sağlanmalıdır.

EK-4. Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

1. Tanımlar

Denetleme:

Önceden belirlenmiş güvenlik ihtiyaçlarına bağlı olarak oluşturulmuş güvenlik politikalarına uygun davranılıp davranılmadığını inceleyen, varsa ihlalleri raporlayan faaliyetleri tanımlar.

Risk Değerlendirme:

Güvenlik risklerini belirleme ve gidermeyedönük olarak açıklıkları tanımlama, bulma ve gidermeye yönelik araştırma faaliyetlerdir. Risk değerlendirme, denetleme faaliyetlerinden farklı olarak, başta veya değişen yapılar ve şartlar göz önünde bulundurularak nispeten daha uzun aralıklarla yapılması gereken güvenlik faaliyetleridir. Çoğu durumda uzmanlık kadar farklı ve dışarıdan bakabilen gözlemler gerektirir.

Açıklıkların Tespiti:

Kusurlu yapı veya eksik tedbirler nedeniyle altyapıdan veya işleyişten kaynaklı açıklıkların belirlenmesi faaliyetleridir. Açıkların tespiti çalışmaları, risk değerlendirme faaliyetlerinin parçası olarak yürütülebileceği gibi ayrıca veya periyodik olarak da gerçekleştirilebilir. Açıklık tespit çalışmaları temel olarak ikiye ayrılır.

- Pasif İncelememe: Çoğunlukla dış uzmanlarca yürütülen, 'Mülakat', 'Saha İncelemeleri', 'Anket (Araştırma Soruları)' ve 'Mevcut Belgelerini İncelenmesi' aşamalarını kapsar. Uzun aralıklarla veya şirketin el değiştirmesi, çalışan istihdamındaki yoğun sirkülasyon, kullanılan altyapıdaki önemli değişiklikler gibi şartlardaki önemli değişikliklerin oluşması durumlarında yeniden yapılması gerekir.
- Aktif İnceleme: Kapsamlıları aralıklı olarak gerçekleştirilse de, sürdürülebilir güvenlik için süreklilik gerektiren faaliyetler arasındadır. Logların, , erişim ve engelleme kural setlerinin, ağ ve sistem yapılandırma dosyalarının gözden geçirilmesi; tarama araçlarıyla ağın ve sistem bileşenlerindeki açıklıkların kontrol edilmesi; ağ trafiğinin dinlenilerek anormallikler olup olmadığının tespiti gibi süreçlerden oluşur.
- Penetrasyon Testleri: Canlı sistemler üzerinde uygulanması beklenmedik önemli problemlere neden olabilir.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

Güvenlik Politikaları:

Kurum ve işletmelerin güvenlik gereksinimlerine uygun olarak belirlenen, *erişim denetimi, hesap ve şifre yönetimi, kabul edilebilir kullanım, personel, yedekleme, güncelleme ve değişiklik yönetimi, iletişim güvenliği, denetleme* gibi farklı başlıklarda adlandırılan ve sınıflandırılan kurallar bütünüdür.

Şartlardaki Önemli Değişiklikler:

Başlangıç sayılabilecek bir tarihi referans alınarak, risk değerlendirme faaliyetlerinin yürütülmesi ve bunun bir parçası olarak güvenlik açıklık taramalarının yapılması, gerekli teknik yatırımların yapılması ve güvenlik uygulamalarının gerçekleştirilmesi siber güvenliğinin bundan sonraki tüm zamanlarda sağlanacağı anlamına gelmemektedir. Zira siber güvenlik süreklilik gereken bir olgu olup, gerekli faaliyetlerin belirlenmiş takvimler içinde yapılması gerekir.

Bir risk değerlendirme çalışması ertesindeki oluşturulmuş yapı ve kurallar aşağıdaki üç sebepten ötürü değişiklik gösterebilecektir. Aşağıda sıralanan bu durumlar "Şartlardaki Önemli Değişiklikler" olarak adlandırılabilir.

- İşletme altyapısında önemli değişiklikler olması (Örneğin, yeni bir hizmetin ilaveten sunumu veya mevcut kapasitenin artırımı şeklindeki anlamlı büyümeler),
- İşletme çalışanlarında önemli değişiklikler (Örneğin kritik personellerin istihdamına ilişkin olarak önemli sayıda yer değişiklikleri, altyapıdan sorumlu önemli bir veya birkaç çalışanın rakip bir şirkete geçmesi durumları),
- Siber güvenlik politikalarının belirlenmesi ve teknik uygulamalarının gerçekleşmesi üzerinden 5 yıl gibi bir süre geçmesi (Zaman karşında kullanılan ürünlere bağlı olarak güvenlik uygulamalarındaki teknik yetersizleşme, geçmişte var olmayan güvenlik açıklıklarının varlığı, güvenlik tedbirlerinin bugünün ihtiyaçlarının karşılayamaz duruma gelmesi)

Şartlardaki Önemli Değişiklikler, risk değerlendirme çalışmalarının tekrarlanması, mevcut güvenlik politikalarının gözden geçirilerek revize edilmesi, altyapıdaki yeni gerekliliklerin gözden geçirilerek ihtiyaç duyulan değişikliklerin yapılmasını gerektiren durumlardır.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

2. İşletme Yöneticileri İçin Öneriler

Teknik ve işletme boyutunda gerekli güvenlik şartlarının oluşturulabilmesi için yöneticilerin yapması gerekenler aşağıda önerilmiştir.

- Yatırım kararı alma süreçlerine (varsa) düzenleyici gerekliliklerini ve güncel siber güvenlik ihtiyaçlarını dâhil etmek,
- İşletme güvenlik kriterlerini belirlemek ve bu kriterlerin (varsa) düzenleyici gerekliliklerıyle uyumlu olmasını sağlamak,
- Siber güvenliği asli iş süreçlerinin parçası olarak kabul etmek,
- Belirlenen güvenlik kriterlerine uygun politika, prosedür ve talimatları hazırlatmak,
- Hazırlanan yazılı güvenlik belgelerine uygunluğu belirli aralıklarla, (varsa) akredite ve onaylı denetim kuruluşlarına denetlettirmek,
- Çalışanların sorumluluk alanlarını ve sorumluluklarını net olarak tarif etmek ve bu sayede hesap verebilirliği mümkün kılmak,
- İşletmede siber güvenlik kriterlerine ve yazılı belgelere uygun çalışmayı performans kriterlerine dâhil etmek, uymamayı ve ihlalleri ise cezai müeyyidelere bağlamak,
- Dış kaynak destek ve alt yüklenici kullanımlarında gizlilik, güvenlik ve uygun kullanım şartlarını yazılı hale getirtmek.

İşletmeler kendi iş öncelikleri ve farklı alanlardaki uzmanlıkları nedeniyle, kendi siber risk değerlendirmelerini yapmakta zorluk çekebilirler. Bu nedenle, kritik altyapı işletmecilerinin kendi siber takımlarını ayrıca oluşturmalı, işleri sadece var olan işleyiş ve uygulamaları güvenlik perspektifinden incelemek, raporlamak ve iyileştirme önerileri sunmak olan siber güvenlik müfettişleri istihdam edilmelidir. Bunun mümkün olmadığı durumlarda bağımsız ve güvenilir siber güvenlik uzmanlarınca denetleme, risk belirleme ve giderme faaliyetleri uygun periyotlarda yürütülmelidir. Bu bağlamda, yukarıdaki önerilerin devamında işletme yöneticileri için öneriler aşağıda yer almaktadır.

- Siber güvenlik konusunda uzman personel istihdam edilmelidir.
- İşletmede görevi sadece siber güvenlik çalışmalarını yürütmek olan bir ekip oluşturmalı, ekipten açıklık taramalarını yapmaları, ağ trafiği ve olası tüm sistem kayıtlarını sürekli gözlemeleri ve düzenli raporlamalar yapmaları istenmelidir.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

- Kurulan siber güvenlik ekibi veya bağımsız ve güvenilir denetçilerce yılda en az bir denetleme faaliyetlerinin gerçekleştirilmesi sağlanmalı ve böylece mevcut güvenlik politikalarının ihlali anlamına gelecek durumların oluşup oluşmadığının araştırılması sağlanmalıdır.
- Şartlardaki Önemli Değişiklikler nedeniyle Güvenlik Risk Değerlendirmesi çalışmaları yenilenerek,
    - İşletmenin doğrudan ve dolaylı varlıklarında, tehdit kaynaklarında değişiklik olup olmadığı,
    - Değişen şartlardan veya zaman karşısındaki teknik yetersizleşmeden kaynaklı olarak önceden var olmayan güvenlik açıklıkların oluşup oluşmadığı,
    - Daha önceden kritiklik düzeyi düşük ve giderim maliyeti yüksek olduğu için giderilmemiş olan güvenlik açıklıklarının kritiklik düzeyinde veya giderim maliyetinde bir değişiklik olup olmadığı,
    - Mevcut tedbirlerin (hem teknik uygulama hem de güvenlik politikalarını olarak) yeterlilik şartlarını sağlayıp sağlamadığı

  gözden geçirtilmelidir.
- Konusu güvenlik olmasa da hem BT hem de DDS altyapısında görevli diğer personellerinin ilgili güvenlik ve farkındalık eğitimleri almasını sağlanmalıdır.

3. Somut Uygulama Önerileri

- Hangi kullanıcının hangi sisteme erişebileceğinin, eriştiği sistemde hangi servis ve fonksiyonlara müdahale edebileceği tanımlanmalı, tüm erişimler kayıt altına alınarak saklanmalıdır.
- Tüm sistemler ve servislerin öntanımlı şifreleri mutlaka değiştirilmelidir.
- Her kullanıcı için ayrı şifre tanımlanmalı, yönetici şifreleri belirli ve sorumlu birkaç kişide bulunmalıdır. Üretici veya dış destek personeli, kurum/işletme yetkililerinin onanıyla ve gözetiminde sistemlere bağlanmalıdır. Şifre üretiminde güncel minimum gereksinimler belirlenmeli, şifre ömürleri altı aydan fazla olmamalıdır.
- Sistemler için makul sürelerde bağlantı zaman aşımı tanımlanmalı, kritik sistemler için anlık bağlantı sayısı sınırlandırılabilmelidir. Kullanılan sistemlerin provizyon kilitleri (aynı anda tek bir kişinin değişiklik yapabilmesi) olmalı ve anlık birden fazla yapılandırma değişikliklerin önüne geçilmelidir.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

- Taşınabilir diskin ve modemlerin DDS yazılım, donanım ve ağlarında kullanımı yasaklanmalıdır. Yetkili personelce güncelleme, yamalama, yedekleme için kullanılacak diskler başka amaçlarla kullanılmamalı, sisteme bağlanmadan güvenlik taramaları yapılmalıdır.
- Bakım, arıza tespit ve giderim gibi nedenlerle kullanılan taşınır bilgisayarların diğer zamanlarda internete ve koruma altında olmayan taşınır disklere bağlanması kesinlikle yasaklanmalıdır. Bu tür bakım bilgisayarlarına, ilgili bakım araç ve dosyaları hariç herhangi bir yazılım, servis, veri yüklenmemelidir.
- İzleme ve kumanda salonlarında sadece klavye ve monitörlerden oluşan terminaller olmalıdır. İzleme ve kumanda operatörleri, sunuculara ve sunuculara erişmekte kullanılan bilgisayarlara fiziki olarak erişememelidir.
- Personellerin yaptıkları iş, görev ve sorumluluklarına uygun olarak güvenlik eğitimleri almaları sağlanmalıdır. Kritik sistemlere ve verilere erişebilen personel için işe alımlarda güvenlik soruşturması yapılmalı, iş ahdine tüm personele uygulanacak kabul edilebilir kullanım sözleşmesine ilaveten hazırlanmış özel güvenlik sözleşmeleri eklenmelidir.
- Uygulama ve işletim sistemleri versiyon değişiklikleri, her türlü konfigürasyon ve kural seti değişiklikleri, değişikliğin yapıldığı tarih ve saat bilgileri de kullanılarak kayda alınmalıdır. Tüm yazılım ve dosyaların değişiklik öncesi ve sonrası versiyonları ayrıca kopyalanmalı ve ihtiyaç duyulduğunda geriye dönmeye hazır halde bekletilmelidir.
- Her türlü sistem, uygulama ve servise ilişkin yapılandırma dosya ve seçenekleri gözden geçirilmelidir. İlgili yapılandırmalara ilişkin belgeler incelenerek daha güvenli yapılandırma seçenekleri araştırılmalı ve uygulanmalıdır.
- Merkez ve kenar birim cihazlarda kullanılmayan servis ve uygulamalar kapatılmalıdır. İlgili üretici desteği de alınarak, öncelikle kullanımına ihtiyaç duyulan servis uygulamalar tek tek belirlenmelidir. Bunların dışındaki servis ve uygulamalara ilişkin öntanımlı olarak yüklenen çekirdek modülleri ve (varsa) sürücüleri de kaldırılmalı, her türlü izinler baştan düzenlenmelidir. Kullanılan işletim sistemlerine ilişkin sıkılaştırma dokümanları mümkünse üreticisinden, değilse internetteki güvenilir açık kaynaklardan temin edilmelidir.
- DDS altyapısında kullanılan işletim sistemi ve uygulamaların yamalama ve güncellemeleri, anti-virüs kullanımları tedarikçinin onayı alınarak ve yedek sistemlerden başlanarak yapılmalıdır.
- Merkez, Uç Birim ve varsa diğer güvenlik alanları içeren ve ayıran ağ segmentasyonuna gidilmeli geçişler güvenlik duvarlarının farklı ağ arayüzleri üzerinden sağlanmalıdır.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

- Merkez ağ üzerinde, farklı güvenlik ve iletişim ihtiyaçlarına uygun olarak sanal yer ağlar oluşturulmalıdır.
- Erişimin yedeklenmesi ihtiyaçları dışında uç birimlerin birbirine erişmesi engellenmelidir.
- Kullanılan endüstriyel iletişim protokolü tasarımından kaynaklık teknik bir zorunluluk yoksa ağda yayın (broadcast) trafiğine izin verilmemelidir.
- Ağ topolojisi çıkarılmalı, (varsa) ağlar arası geçişlerin işaretlenmelidir. Ağda, adres, protokol ve fonksiyon temelli filtreleme yapan, oturumları takip eden güvenlik duvarları kullanılmalıdır. Sadece IP/Port bazında değil kullanılan endüstriyel iletişim protokollerinin fonksiyonlarına göre de filtreleme yapılmalıdır.
- Mümkünse ağda adres çözümleme protokolleri kullanılmamalı, ağa bağlanabilirlik için IP, MAC ve port temelli kısıtlamalar uygulanmalı, kullanılmayan sunucu, anahtar, yönlendirici portları kapalı tutulmalıdır.
- Ağ trafiği izlenmeli, nominal trafik değerlerine ilişkin hafta, gün ve saatlik istatistik değerleri oluşturulmalı, beklenen istatistik değerlerine aykırı trafik düşüş ve artışları alarm eşikleri olarak tanımlanmalıdır.
- Altyapıdaki hiçbir bileşen ve alan internete kesinlikle bağlanmamalıdır. Ağda toplanan veriler ayrıca faturalandırma gibi farklı sebeplerle kullanılacak ve bu bilgiler internet ortamından müşterilere sunulacaksa, aynı ağda bulunmayan başka bir sunucu üzerinden eriştirilmelidir.
- Güvenlik duvarları ve diğer ağ cihazlarında kullanılan erişim kural setlerinde yapılacak değişiklikler için gerekçelendirme ve onay süreçleri tanımlanmalıdır.
- Trafiği şifreleme yeteneği olmayan kablolu ve özellikle kablosuz erişim teknolojiler kullanılmamalıdır. Erişim için ticari telekomünikasyon servisleri tercih ediliyorsa, şebekeye erişimi denetleyen ve donanımsal bir anahtar kaynağıyla yetkilendiren, taşıdığı trafiği şifreleyen hatlar tercih edilmelidir.
- Lokal bağlantılar haricinde, ağda akan trafiğinin gizliliği ve bütünlüğünü sağlayıcı güvenlik protokol ve mekanizmaları kullanılmalı, açık metin trafik taşıyan protokoller kesinlikle kullanılmamalıdır.
- İnternet başta olmak üzere DDS ağındaki hiçbir bileşene dışarıdan uzaktan bağlantıya izin verilmemelidir. Uzaktan bir müdahale mecbur ve kaçınılmaz hale gelmiş ise, çevirmeli modem veya VPN bağlantıları, acil duruma müdahale için lokaldeki görevlice fiziksel olarak bağlanmalı ve çalışma biter bitmez çekilmelidir.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

- Altyapıda kullanılan ürünler, ağ topolojileri, her türlü adres bilgileri internet ortamında kesinlikle yayımlanmamalıdır. Ürünleri ve çalışmalarını referans olarak gösteren tedarikçi, yüklenici ve üreticilerinde bu bilgileri yayımlamaması sağlanmalı, hizmet ve ürün alımlarında tedarikçi firmalardan kurum/işletme adlarını hiçbir suretle yayımlamamaları, kurulum ve yapılandırmalara ilişkin bilgi ve ayrıntıları gizli tutmaları yazılı sözleşmelere bağlanmalıdır.
- Tüm personel soysal mühendislik ve bilgi sızmalarına karşı eğitimden geçirilmeli ve böylece güvenlik farkındalık düzeyleri arttırılmalıdır.
- Kurum ve işletmelere DDS altyapı bileşen alımlarına ilişkin şartnamelerini yayımlamamalı. İlgili tedarikçi ve entegratörlere gizlilik sözleşmesi karşılığında vermelidir.

4. Altyapı Eskimeleri ve Tedarik Kriterlerine İlişkin Öneriler

Bu belgede tanımlı güvenlik kavramlarından biri de Şartlardaki Önemli Değişiklikler olup, teknik eskime ve bu suretle güncel güvenlik ihtiyaçlarının karşılanamaması altyapıları yeniden gözden geçirmeyi gerekli kılan önemli değişikliklerin başında gelmektedir. Bu nedenle, kullanılan her türlü bileşenin erişim denetimi, yetkilendirme, kimlik denetimi fonksiyonları ile gizlilik ve bütünlük şartlarını güncel kriptografik gerekliliklerine uygun olarak sağlayıp sağlamadığı belirli aralıklarla gözden geçirilmeli ve ortaya çıkan duruma göre yapısal değişiklik ve yenilemelere gidilmelidir. Bu aralık, tedarik edilen ürünlerdeki işletim sistemi ve uygulamalarının desteğinin devam edip etmediği, bir önceki değerlendirmenin üzerinden kullanılan ürünler ve sahip oldukları bileşenlere ilişkin anons edilen çok kritik açıklıkların varlığına bağlı olarak en fazla 5 yıl olmalıdır.

Sahadaki çok sayıdaki uç birim nedeniyle DDS altyapı bileşenleri için öngörülen teknik ve ekonomik ömür 15 ila 20 yıl iken BT altyapıları için bu ömür genel olarak 5 yıl civarındadır. Birçok sunucu, işletim sistemi, veritabanı, uygulama yazılımı gibi DDS altyapısında da kullanılan birçok BT yazılım ve donanım bileşeni 10 yılı bulmayan bir süre içerisinde ömürlerini tamamlamakta, üreticileri tarafından artık destekleri (yedek parça, güncelleme gibi) verilmemektedir. Bu durum ise eskimesine rağmen DDS işletmecilerinin operasyonel ihtiyaçlarını karşılayan ürünlerin güncel güvenlik ihtiyaçlarını karşılayamaz hale gelmesine sebebiyet vermektedir. Bu çok önemli problemin çözümüne yönelik olarak aşağıdaki öneriler imkânlar ölçüsünde değerlendirilmelidir.

EK-4. (Devam) Denetim Sistemi Kullanan Kritik Altyapılar için Kurumsal Siber Güvenlik Eylem Planı Önerisi

- İşletim sistemi bağımsız ve diğer işletim platformlarına da taşınır yazılım uygulamaları tercih edilmeli ve istenmelidir.
- Tedarikçilerden SCADA/DDS uygulama yazılımlarını en az 15 yıl boyunca yeni işletim sistemleri için güncelleme garantisi (uygulama yazılımlarının yeni işletim sistemleri için derlenmiş halinin istenmesi) istenmeli veya uygulamalar ileride derlenebilmek için kaynak kodlarıyla birlikte teslim alınmalıdır.
- (Yukarıdaki önerilerin uygulama imkânının kalmadığı veya olmadığı durumlar için) Mevcut uygulama yazılımını eski işletim sistemi ile birlikte sanallaştırılmış bir işletim platformuna taşınmalıdır. Eskimiş bir işletim sisteminin güncel bir işletim sistemi üzerinde bulundurulması sayesinde, güncel işletim sisteminin sağladığı fonksiyonlar sayesinden birçok erişim denetimi ve kısıtlamaları kullanılabileceği gibi eskimiş işletimim sisteminin izlenebilmesi de mümkün hale gelebilecektir. Ayrıca desteği kalmamış sunucu donanımlarının kullanımları da bu sayede terk edilebilecektir. Taşıma işlemi, bir deneme ortamında, sanallaştırma çözümünün ve taşıyıcı (host) işletim sisteminin sağladığı güvenlik fonksiyonlarının tümü, ihtiyaç duyulan performans kriterleri de dikkate alınarak yapılmalıdır.
- Tek bir üreticiye özgü endüstriyel iletişim protokolüne ve ağ arayüzlerine sahip DDS bileşenleri tercih edilmemelidir. Bunun yerine OSI ve TCP/IP katman yapısına uygun olarak tasarlanmış, geçişlere ve farklı katmanlar için ilave güvenlik fonksiyonlarının uygulanmasına izin veren bir iletişim mimarisi alınacak bileşenlerde aranmalıdır.
- Bileşenler, gizlilik, bütünlük ve kimlik doğrulama gibi güvenlik fonksiyonlarını güncel kriptografik gereksinimlere uygun olarak OSI 7. Katmanda tanımlı uygulama seviyesinde de sağlayabilmelidir.
- Geçmişte edinilmiş ve gizlilik, bütünlük, kimlik doğrulama gibi iletişim güvenliği özelliklerini sağlamayan bileşenler için IPSec veya SSL VPN gibi iletişim kanalına haricen de uygulanabilir çözümler ilave edilmelidir. Bu tür çözümler için öncelikle deneme ortamlarında mevcut iletişim kanal kapasiteleri de dikkate alınarak test edilmeli, ihtiyaç duyulan performans değerleri (paket gecikme, jitter vb.) üzerinde kabul edilmeyecek etki oluşturup oluşturmadığı görülmelidir.
- Canlı DDS bileşenleri üzerinde penetrasyon testleri uygulanamayacağından, tedarikçilerinden bağımsız laboratuarca hazırlanan penetrasyon test raporlarını istemelidirler.

EK-5. 42 Kritik İyileştirme Adımı (Kontrol Listesi)

(EK-4. Kurumsal Siber Güvenlik Eylem Planına göre bu kontrol listesi üretilmiştir.)

I. YÖNETİM BOYUTU	Evet/Hayır
Yatırım	
1. Altyapı yatırım süreçlerine güncel siber güvenlik ihtiyaçlarını dâhil edilmelidir.	
Personel ve Eğitim	
2. Çalışanların sorumluluklarını tarif edilerek, hesap verebilirlik sağlanmalıdır.	
3. İlgili tüm personele siber güvenlik eğitimileri aldırılmalıdır.	
4. İş tanımı sadece siber güvenlik olan personel istihdam edilmeli ve tüm altyapıyı izleyecek ve denetleyecek siber güvenlik takımları oluşturulmalıdır.	
Kurallar ve Denetleme	
5. İşletmenin güvenlik ihtiyacını ve taşıdığı siber güvenlik risklerini belirlemek için profesyonellere risk değerlendirme çalışmaları yaptırılmalıdır.	
6. İşletme için güvenlik kriterleri belirlenmeli, bu kriterlere ile ilgili güvenlik standartları ve rehberlerine (ISO 2700, ISA TR99-01 ve 02, NERC CIP gibi) uygun politika, prosedür ve talimatlar hazırlatılmalıdır	
7. Kurallara uygunluğu izlemek veya ihlalleri görmek için denetlemeler yaptırılmalıdır.	
II. İŞLETME BOYUTU	Evet/Hayır
Şifre ve Hesap Yönetimi	
8. Tüm sistem ve ağ bileşenlerinin ön tanımlı şifreleri mutlaka kaldırılmalıdır.	
9. Tüm şifreler için ömür ve minimum gereklilikler tanımlanmalıdır.	
10. Sistem işletmede görevli her çalışanın rol ve sorumluğuna uygun kullanıcı hesabları tanımlanmalıdır.	
11. Sistem ve ağ bileşenleri üzerindeki işlemlerin ve bağlantıların kayıtları tutulmalı ve saklanmalıdır.	
Yedekleme	
12. Tüm uygulamaların, yapılandırma bilgilerinin, erişim kural setlerinin düzenli yedekleri alınmalıdır.	
13. Mekez denetim biriminin hayati fonksiyonlarını yürütecek bir yedek yönetim birimi oluştulmalıdır.	
Değişiklik Yönetimi	
14. Kural seti, konfigürasyon, uygulama sürümü değişiklikleri ve yamalamalar için merkezi bir onay süreci oluşturulmaldır. Sistem ve ağ bileşenleri üzerindeki her değişiklik onaya bağlanmalıdır.	

EK-5. (Devam) 42 Kritik İyileştirme Adımı (Kontrol Listesi)

Fiziki Erişimler	
15. Merkez ve uç birim sistem odalarına giriş çıkışlar kart ve/veya biyometrik yöntemlerle sağlanmalı, kamera ile kayıt altına alınmalıdır.	
Sosyal Mühendislik	
16. İnternet ortamında altyapıya ilişkin hiç bir bilgi yayınlamalı, tedarikçi ve yüklenicilerde bu konuda uyarılmalıdır.	
17. Tüm personele bilgi güvenliği farkındalığı kazandıracak faaliyetler düzenlenmelidir.	
III. TEKNİK BOYUT	Evet/Hayır
Sistem Bileşenleri ve Uygulamalar	
18. Kullanılamayan servisler belirlenmeli ve kapatılmalıdır.	
19. İşletim sistemlerinin kullanılmayan çekirdek modüllerini ve sürücüleri belirlenmeli ve kaldırılmalıdır.	
20. Uygulama ve işletim sistemlerinin güvenlik yamaları önce test/yedek sistemler üzerinde denenmeli ve gözlenmelidir. Aktif sistemler üzerinde testlerden sonra uygulanmalıdır.	
21. Tüm uygulama ve işletim sistemlerinin uzaktan tanıma imkanı veren parmak izlerini kapalı tutulmalıdır.	
22. Uygulamaların öntanımlı yapılandırma dosyaları gözden geçirilmeli, uzak bğlantılar için tipik olmayan parametreler tercih edilmelidir.	
23. Kullanılan uygulamalarda giriş doğrulama özelliklerinin test edilip edilmediği üreticisinden sorulmalıdır.	
24. Kullanılan uygulamaların platform bağımsız olmaları veya farklı işletim sistemleri için de sürümlerinin mevcut olması şartı aranmalıdır.	
25. Sistem bileşenlerinde dış ortamlarda kullanılan harici disklerin kullanımı yasaklanmalıdır. Güncelleme ve yamalama gibi özel durumlar için gerekli kullanımlar kurala bağlanmalıdır.	
26. Sistem bileşenlerine harici modemlerle, internet ortamında da kullanılan taşınır bilgisayarla bağlanmak yasaklanmalıdır.	
Ağ Servisleri ve Ağ Bileşenleri	
27. Ağda kullanılmasına izin verilecek protokoler belirlenmeli, kullanılmayan ağ protokolleri kaldırılmalı ve ağda dolaşmasına izin verilmemelidir.	
28. Kullanımlması gerekli olanlar haricindeki TCP/UDP portlarına erişim engellenmelidir.	

EK-5. (Devam) 42 Kritik İyileştirme Adımı (Kontrol Listesi)

29. (İhtiyaç duyulmuyorsa) Adres çözümleme protokolleri kullanılmamalıdır.	
30. Ağda yayın (broadcast) trafiğine izin verilmelidir.	
31. Dış dünyaya kapalı ağlarda, gerçek IP adresi kullanılmalı, tipik olmayan özel IP bloklarını seçilmelidir.	
32. Dış dünyaya kapalı ağlarda, sistem ve ağ birimlerinde varsayılan yönlendirme tanımları kaldırılmalıdır. Oluşturulacak erişim şemalarına göre yönlendirme kuralları tek tek belirlenmelidir.	
33. Dış dünyaya kapalı ağlarda, sistem ve ağ birimlerinde varsayılan yönlendirme tanımları kaldırılmalıdır. Oluşturulacak erişim şemalarına göre yönlendirme kuralları tek tek belirlenmelidir.	
Ağda Erişim ve Ağ Trafiği	
34. Ağda güvenlik bölgeleri oluşturulmalı, birbirine erişim ihtiyacı duyan tüm bileşenler belirlenmelidir.	
35. Ağ bileşenleri arasında tanımlı iletişim ihtiyacına uygun olarak adres (IP/MAC gibi), servis (TCP/UDP) ve fonksiyon bazlı filtrelemeler uygulanmalıdır.	
36. Ağ bileşenleri arasındaki normal iletişim trafik değerleri gün ve saatlere uygun olarak çıkarılmalı, beklenen değerlerin altı ve üstü için alarm seviyeleri oluşturulmalı ve ağ trafiği sürekli izlenmelidir.	
37. İşletme dışı ağlardan tüm uzaktan erişimler iptal edilmelidir.	
38. Uç birim cihazlara (PLC, RTU) sadece şirket içi denetim ağındaki önceden belirlenmiş bilgisayarlardan erişilebilmelidir.	
39. Yerel ağ dahil tüm ağ trafiğinin şifreli olarak dolaşımı sağlanmalıdır.	
40. Coğrafi olarak farklı yerlerden olan birimler arasında VPN teknikleri kullanılmalıdır.	
41. Üretici özel ve harici güvenlik uygulamalarına geçiş vermeyen endüstriyel iletişim protokollerini kullanılmamalıdır.	
42. Ticari erişim sağlayıcılarından olası DDOS saldırılar için alternatif band/hat kullanımı, trafik filtreleme vb. içeren çözüm ve uygulama planlarının hazır edilmesi istenmelidir.	

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ÖZBİLEN, Alper

Uyruğu : T.C.

Doğum tarihi ve yeri : 08.01.1980 ANTAKYA

Medeni hali : Evli

Telefon :+90 (505) 256 26 80

e-mail: alper@ozbilen.net.

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Y.Lisans	Gazi Ünv./ Fen Bilimleri Enstitüsü (Elektrik-Elektronik Müh.Ana Bilim Dalı)	2006
Lisans	Gazi Ünv. / Elek.-Elektronik Müh.	2003
Lise	Kırıkhan Lisesi	1996

İş Deneyimi

Yıl	Yer	Görev
2002-2003	Emre Bil. A.Ş	Ağ Mühendisi
2003-2006	Türk Telekom	Telekom Uzm. Yrd.
2006-Devam	BTK	İletişim Uzmanı

Yabancı Dil

İngilizce

Yayınlar

Bildiriler:

Özbilen A., Çolak, İ., Sağıroğlu Ş., "Siber Güvenlik Perspektifinden Makineler Arası İletişim Uygulamalarının İncelenmesi" ***International Information Security and Cryptology Conference***, Ankara (2012)

Ozbilen, A.,Sagiroglu, S., Çolak, İ., "Siber Savaş ve Türkiye için Öneriler**",** ***Siber Güvenlik Çalıştayı*****,** Ankara (2011)

Özbilen A., Çolak, İ., Sağıroğlu Ş., "A Survey on SCADA / Distributed Control SystemCurrent Security Development and Studies", ***IST-091 Symposium on Information Assuranceand Cyber Defence,*** Tallinn (2010).

Makaleler:

Bayındır, R., Sağıroğlu, Ş., Çolak, İ., Özbilen, A., "İzlenebilir Elektrik Enerjisi Dağıtım Sisteminin Bilgi Güvenliği Açısından Endüstriyel Risklerinin Araştırılması ve Çözüm Önerileri", ***Gazi Üniversitesi Mühendislik-Mimarlik Fakültesi Dergisi***, 24(4), 715-723 (2009).

Sağıroğlu, Ş., Çolak, İ., Bayındır, R., Özbilen, A., "Dağıtık Denetim Sistemlerine Yönelik Elektronik Tehditler", ***TUBAV Bilim Dergisi***, 1(2):82-88 (2008).

Hobiler:

Sinema, Yüzme, Bilgisayar Teknolojileri, Gezi