Biznet Bilişim

Endüstriyel Kontrol Sistemleri için Purdue Katmanlı Güvenlik Mimarisi

08.01.2019

Yazar: Murat Aydemir

Endüstriyel Kontrol Sistemleri için Purdue Katmanlı Güvenlik Mimarisi

Endüstriyel Kontrol Sistemleri (EKS), teknolojinin gelişmesi ve bu teknolojilerin endüstriyel ortamlarda kullanılmasıyla beraber her geçen gün daha yetenekli sistemler haline gelmektedir. Bu gelişimin önemli sebeplerinden birisinin geleneksel IT teknoloji/metotlarının endüstriyel kontrol sistemlerine uyarlanması olduğunu söylemek yanlış olmayacaktır. Bu durum IT ve OT teknolojilerinin yakınsamasının bir sonucu olarak ortaya çıkmaktadır. Şüphesiz Endüstri 4.0 devrimi, IoT ve IIoT teknolojilerinin yaygınlaşması ve işletmelerin artan verimlilik, kolay erişilebilirlik gibi taleplerinin bir sonucu olarak IT ve OT ortamlarının birbirine yakınsaması kaçınılmaz oldu. Ancak IT-OT yakınsamasının kontrolsüz şekilde artması kritik altyapılar için yeni saldırı yüzeyleri oluştururken, IoT ve IIoT teknolojilerinin OT ortamlarında aktif olarak kullanılmaya başlanması EKS' ler için atak vektörü sayısını arttıran diğer bir nokta olmaktadır.

Endüstriyel altyapılarda genellikle birbirleriyle ilişkili ve birbirlerini besleyen çok sayıda farklı süreçten oluşmaktadır; bu sebeple yapıları gereği flat(düz) ağ mimarisinden ziyade çok katmanlı mimarilere sahip topolojilerdir. Her katman, kendisiyle ilişkili başka katmanlarla iletişim halinde olmakla beraber, her katman için uygulanması gereken güvenlik kriterlerinin farklı olması sebebiyle, her katman güvenlik mekanizmaları açısından farklılık gösterebilmektedir. Bu nedenle EKS gibi çok katmanlı topolojiler için derinlemesine güvenlik(defense-in-depth) anlayışı uygulanmalıdır. Bu anlayış, siber saldırılara karşı alınan tüm önlemlerin bir şekilde atlatılacağı fikrini baz alarak geliştirilmiştir. Derinlemesine güvenlik anlayışı; her katman için, ilgili katmanın gerekliliklerine, özelliklerine ve bulundurduğu varlıklara göre önlem alınıp, saldırganın başarı oranını düşürmeyi hedef almaktadır.

Endüstriyel altyapılarda güncel teknolojilerin kullanılması, bu sistemleri daha becerikli hale getirirken, sistemlerin olası atak yüzeylerini arttırarak siber tehditleri de arttırdığından bahsetmiştik. Bu bağlamda gerek atak yüzeylerinin minimum seviyede tutulması, gerekse - her katman için- kontrol sistemlerin yönetimini daha güvenli hale getirmek için Purdue Üniversitesi (Indiana) tarafından "Purdue Model" katmanlı ağ mimarisi geliştirilmiş ve International Society of Automation ISA tarafından EKS' lere uyarlanmıştır. ISA; mühendislik, teknoloji gibi alanlarda iyileştirmeler yapan, aynı zamanda endüstriyel otomasyon ve kontrol sistemleri için standartları oluşturan bir kurum olup ISA-99 standardıyla beraber EKS' ler için siber güvenlik standardını oluşturmuştur.

Farklı EKS/SCADA sistemleri için işletmelere özel ağ güvenlik mimarileri bulunmakla beraber, bu spesifik mimarilerin Purdue modelin modifiye edilmiş versiyonları olduğu görülmektedir. Purdue Model, referans alınan kaynağa ve notasyona göre değişmekle beraber 5 ya da 6 katmanlı olarak tanımlanmaktadır. (Örn: SANS ve ISA dökümanlarında 6 katmanlı bir mimari anlatılırken, bazı üreticilerin referans modellerinde 5 katmanlı bir mimari görebilirsiniz.) Bu yazıda Purdue model;

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

katmanları olmak üzere toplamda 6 katmanlı olduğu düşünülerek yazılmıştır. Yukarıda bahsedilen her katman için sahada problem olarak karşılaşılan aşağıdaki dört ana başlık üzerine yoğunlaşılmıştır:

- Erişim kontrolü (Access Control)
- Log yönetimi (Log Management)
- Ağ güvenliği (Network Security)

- Uzak Erişim (Remote Access)

Purdue model katmanlı mimarisi, IT ve OT ağlarını, her katmanın gereksinimleri dikkate alarak alt ağlara(subnets ya da VLAN) ayırma prensibine dayanmaktadır. Buradaki amaç; alt ağlara kontrollü erişim(INTER-VLAN routing, Access Control List(ACL) ya da diğer teknolojiler kullanılarak izole ağlar oluşturma) sağlamak ve tehdit oluşturabilecek olası gereksiz erişimleri kısıtlamaktır.

5. Kurumsal DMZ – DMZ' ler genel olarak güvenli ve güvensiz/az güvenilir ağlar arasına konumlandırılarak -bir tarafı güvenilir ağa bakarken diğer tarafı daha az güvenilir ağa bakacak şekilde- iki network arasında gelişecek trafiğin güvenli/kontrollü bir şekilde gerçekleştirilmesini sağlayan yapılardır. Purdue model için IT networkleri güvensiz olarak kabul edilip OT ağı güvenli ağ olarak belirlenir.

Kurumsal DMZ katmanı, Purdue modelin en üst katmanında adreslenir ve internete(dış dünyaya) en yakın katmandır. Bu katmanda VPN bileşenleri, DMZ web sunucuları, gibi internet üzerinden erişilebilir IT varlıkları bulunmaktadır. Bu katmandaki sunuculara internetten erişilebileceği için internet ile bu katman arasındaki trafik bir güvenlik cihazı/çözümü(Örn: Güvenlik Duvarı) üzerinden gerçekleştirilip, firewall üzerinden tanımlanmış kurallar ile denetlenir. Bununla beraber IPS/IDS gibi teknolojilerle internet katmanı üzerinden oluşabilecek ihlallerin denetimi ve tespiti yapılabilmektedir.

4. Yerel Kurumsal Ağ – Bu katmanda bulunan temel varlıklar genellikle yerel ağ üzerinden kurum bünyesine hizmet eden bileşenlerin yer aldığı ağdır. Bu katmanda yerel DNS, DHCP, AD gibi IT servisleri bulunmaktadır.

Bu katmanda bulunan servis ve varlıkların hareketlerinin loglanması ve aynı zamanda kurumun hesap verilebilirliğini(accountable) arttırmak için, Kurumsal Ağ katmanı içerisinde İzleme Katmanı olarak adlandırılan bir alt katman daha bulunmaktadır. İzleme Katmanında bulunan varlıklar (genelde Log collector ve SIEM sunucusu) Yerel Kurumsal Ağ katmanının içerisinde olmasına rağmen Yerel Kurumsal Ağ ile arasındaki trafik bir firewall üzerinden gerçekleştirilmelidir.

3. Kontrol DMZ – DMZ' lerin genel çalışma prensiplerinden yukarıda bahsetmiştik. Kontrol DMZ ile Kurumsal DMZ' i birbirinden ayıran en önemli kısım ise güvenli ve güvensiz/daha az güvenilir olarak kabul edilen bacaklarının farklı olmasıdır. Şekil 1' den örnek vermek gerekirse Kontrol DMZ için Yerel Kurumsal Ağ ve Kurumsal DMZ katmanları güvensiz/daha az güvenilir olarak tanımlanırken Supervisory, Lojik ve Saha&Enstürmanlar katmanları güvenilir ağ olarak tanımlanmaktadır.

Her iki taraftan (IT&OT) Kontrol DMZ' e gelen trafik güvenlik duvarı ya da routing yapabilme özelliğine sahip bileşenler üzerinden (en az layer 3 seviyede çalışmalı) geçerek denetlenmelidir.

EKS için IT ağından OT ağına –ya da tam tersi bir senaryo düşünülebilir- kesinlikle doğrudan bir erişim olmamalıdır. Kontrol DMZ bu işte bu noktada doğru yapılandırılıp, IT ve OT ağları arasında oluşan trafiğin istenilen bir şekilde gerçekleşmesi sağlanmalıdır. Kontrol DMZ' in endüstriyel ortamlardaki kullanım senaryosu Şekil 2' de anlatılmaktadır.

DMZ' da hem IT hem OT ağındaki kullanıcı/bilgisayarların erişmesi gereken;

- İşletmenin IT Ağı ile alakalı kritik verilerin saklandığı Merkezi Historian sunucu
- Dosya sunucuları
- Yama/Patch sunucuları
- Uzak erişim(Jump server) gibi bileşenler bu katmanda bulunmalıdır.

Her ne kadar güvenilir olduğu varsayılsa da OT ağından IT ağına erişmek istenildiğinde OT ağından çıkarken OT firewall üzerinden gelen trafik buradaki kurallara göre bir üst katman olan Kontrol DMZ katmanına aktarılmalıdır.

2. Supervisory Katmanı - Bu katmanda, sahadan aldığı dataları görselleştirerek, bir operatör tarafında güncel olarak takip edilen bir sistem olan Human Machine Interface' ler (HMI), SCADA sistemleri ve -varsa DCS' lere- hizmet veren SCADA/DCS sunucuları ve çeşitli kontrol odaları bulunmaktadır. HMI' ler aracılığıyla interaktif şekilde sahadaki proseslere müdahale edilebildiği için (örn: tanklarda bulunan kimyasalların aktarılması için valf veya vanaların açılıp/kapatılması) bu katmandaki olası bir yetkisiz erişim sahadaki sürece doğrudan müdahale etmek anlamına gelmektedir.

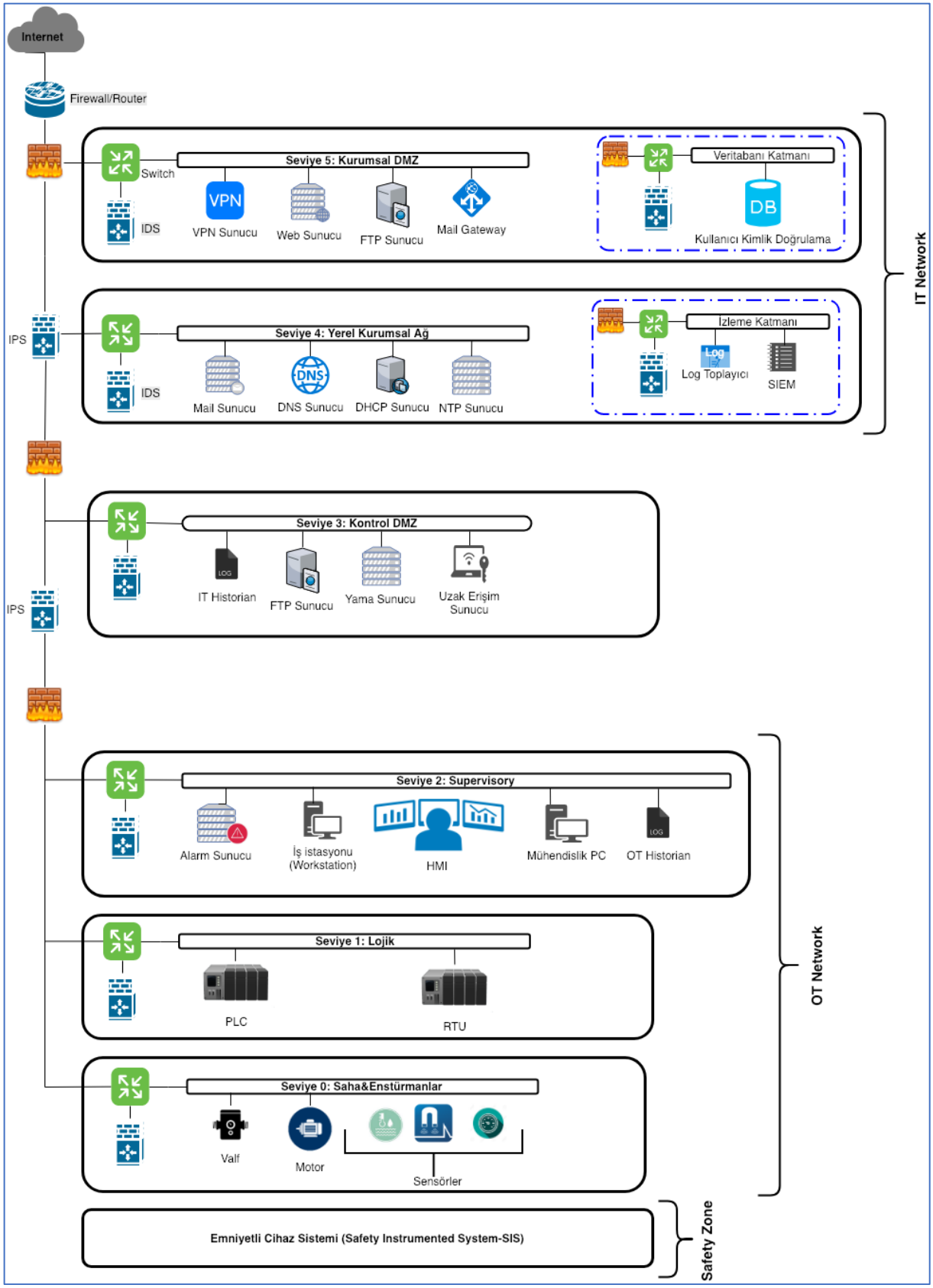
Her katmanda olduğu gibi bu katmanda da monitoring/IDS konumlandırılıp, olası ihlaller belirlenmelidir. Aynı zamanda alarm sunucuları da bu katmanda bulunmaktadır. OT ağındaki herhangi bir proses temelli anomali durumunda alarm üretip, bu alarmlara göre aksiyon alınmasını sağlar.

IT ortamlarıyla OT ağlarının gereksinim ve önceliklerinin birbirlerinden farklı olduğu her fırsatta dile getiriliyor. Bu durum loglama işlemleri ve geriye dönük veri toplama işlemleri için de geçerlidir. İşletme prosesleriyle alakalı verilerin loglanıp anlamlandırılması için OT Historian sunucuları da bu katmanda bulunmaktadır.

1. Lojik(Kontrol) Katmanı – Bu katmanda, I/O, sensör gibi ekipmanlardan aldığı datayı Supervisory Katmanına ileten (genellikle özelleştirilmiş bir protokol aracılığıyla) ve aynı zamanda bu ekipmanların lojik kontrolünü sağlayan Programmable Logical Controller(PLC), Remote Terminal Unit (RTU) gibi endüstriyel bileşenlerden oluşmaktadır. Bu cihazlar üzerinde üreticiye özel bir işletim sistemi/framework çalışmakla beraber, Mühendislik PC' leri kullanılarak programlanır.

0. Saha&Enstürmanlar - Bu katmanda sahadan gerek analog gerek sayısal veri toplayan sensörler(ısı, sıcaklık, basınç, seviye vb.) ve ilgili ekipmanlar bulunmaktadır. Bu ekipmanlar lojik kontrol katmanındaki PLC/RTU gibi ekipmanlar tarafından kontrol edilmektedir.

ESD/SIS Katmanı – ESD/SIS sistemleri özellikle endüstriyel işletmelerde kullanılan, özel olarak tasarlanmış bir dizi yazılım ve donanım kontrollerinden oluşmaktadır. Bu sistemlerin görevi, Endüstriyel Kontrol Sistemleri' nde bulunan kritik süreçlerde oluşabilecek olası acil durumlarda devreye girip hem işletme sahasını hem de endüstriyel prosesleri güvenli bir şekilde durdurmak ve oluşabilecek olası hasarları engellemektedir. Bu sistemler çoğunlukla sinyal seviyesinde çalışıp, doğrudan sahadaki enstrümanlarla iletişim halindedir. Kimi sistemlerde ise Supervisory katmana doğrudan entegre çalışmaktadır.


Internet
Firewall/Router
Switch
IDS
Seviye 5: Kurumsal DMZ
VPN
VPN Sunucu
Web Sunucu
FTP Sunucu
Mail Gateway
Veritabanı Katmanı
DB
Kullanıcı Kimlik Doğrulama
IT Network
IPS
IDS
Seviye 4: Yerel Kurumsal Ağ
Mail Sunucu
DNS
DNS Sunucu
DHCP Sunucu
NTP Sunucu
İzleme Katmanı
Log
Log Toplayıcı
SIEM
IPS
Seviye 3: Kontrol DMZ
IT Historian
FTP Sunucu
Yama Sunucu
Uzak Erişim Sunucu
Seviye 2: Supervisory
Alarm Sunucu
İş istasyonu (Workstation)
HMI
Mühendislik PC
OT Historian
Seviye 1: Lojik
PLC
RTU
Seviye 0: Saha&Enstürmanlar
Valf
Motor
Sensörler
OT Network
Emniyetli Cihaz Sistemi (Safety Instrumented System-SIS)
Safety Zone

Şekil 1

Ne öneriliyor?

EKS altyapılarını daha güvenli hale getirmek için Purdue katmanlı güvenlik mimarisinde alınacak önlemlerin birkaçı aşağıdaki gibidir;

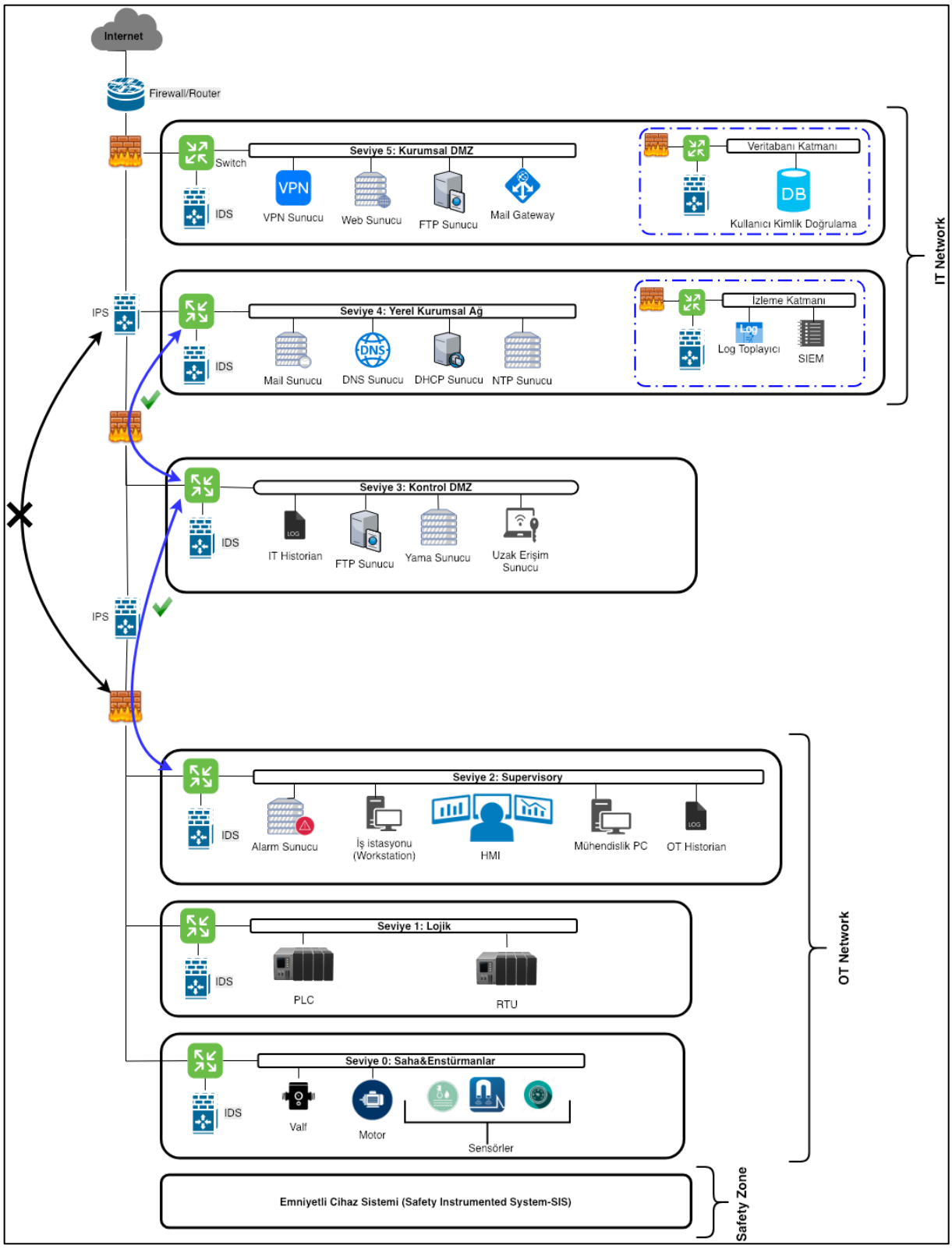
- IT ve OT networklerinin her ne kadar izole olması önerilse de birbirlerine erişimlerinin gerektiği durumlarda, OT ağına giriş noktalarının minimum seviyede tutulması önerilir. Bu sayede atak yüzeyi minimize edilmiş olacaktır.
- Yukarıda açıklandığı üzere Kontrol DMZ' in üst kısmında bulunan ve genel olarak IT Ağı olarak isimlendirebileceğimiz alan iki farklı alt katmana bölünmüştür. Bunun sebebi Kurumsal DMZ katmanında bulunan web ve dosya sunucuların, VPN, e-mail gibi servislerin internete erişiminin olmasıdır. Kurumsal DMZ' de bulunan VPN gatewayi sadece OT ağında tanımlı bir uzak masasüstü kullanıcısı tarafından erişebilecek şekilde konfigüre edilerek atak yüzeyi minimize edilebilir.
- OT verilerini içeren kritik sistemlere erişim (Historian sunucular gibi) kesinlikle Kontrol DMZ' den geçerek gerçekleştirilmelidir. Firewallardaki kurallar öncelikle "deny all" olarak tanımlanmalı, sonrasında ise sadece yetkilendirilmiş kullanıcıya özel izinler verecek şekilde yapılandırılmalıdır.
- DMZ' larda ikili firewall yapısı (pair of firewall concept) önerilmektedir. Kontrol DMZ için örnek vermek gerekirse; güvenli tarafa bakan firewall OT ağından IT ağına giden trafiğin yönetilmesini sağlarken ikinci firewall IT ağından OT ağına giden trafiği kontrol edecek şekilde konumlandırılmalıdır. Böylece görev paylaşımı yapılarak tüm yük tek bir ekip ya da kişiye yüklenmemiş olacaktır. (separation of duties)
- Kritik sistemler için Yerel Kurumsal Ağ katmanı içerisine monitoring ve database katmanları eklemek güvenlik açısından fayda sağlamaktadır. Bu katmanlar, bulundukları katmanın firewallundan izole bir şekilde, ayrı bir firewallun arkasında bulunmalıdır. İşletmenin üretimi ile ilgili kritik bilgiler izleme(monitoring) katmanda tutulurken, çalışanların kullanıcı-parola bilgileri, kişisel kimlik bilgileri, işletme kontrol ve hiyerarşisi gibi bilgiler ilgili katman içerisinde, bağımsız bir firewallun arkasında ve izole bir şekilde veri tabanı katmanında saklanmalıdır.

Erişim kontrolü (Access Control) nasıl olmalıdır?

OT ağlarına yetkisiz erişimin engellenmesi için ilgili kullanıcılar, erişim sağlamadan önce kimlik doğrulama ve yetkilendirme işlemlerine tabii tutulmalıdır. Kullanıcılara yetki verilirken ki yaklaşım "mümkün olan en az yetkilendirme ile ilgili erişimin sağlanabilmesi" şeklinde olmalıdır. Bu noktada kullanıcıyı doğrudan bir sunucu ya da alt ağa erişim için yetkilendirmek yerine, sadece ilgili servis/feature üzerinde yetkilendirme yapılmalıdır. İlgili ağlar için yetkilendirme yapılırken önce layer 3(OSI Model-Network Layer) kısıtlama işlemleri uygulanmalı, sonrasında servis ve uygulama tabanlı kısıtlamalar yapılmalıdır.

Erişim için kullanılan kullanıcı parolaları geleneksel IT ağlarında olduğu gibi bir parola politikasına bağlı kalınarak oluşturulmalı ve bu politikaya göre değiştirilip, güncel tutularak parola saldırılarına karşı önlem alınmalıdır.

Burada özellikle OT ağlarında atak yüzeyini minimize etmek için çoklu kimlik doğrulama(örn:2FA) kullanılması güvenlik açısından daha verimli olmaktadır. Gelişen örüntü tanıma teknolojileriyle birlikte üçüncü faktör de kullanılabilir. Üçüncü faktör için iris örüntüsü tanıma(pattern recognition), face ID, parmak izi gibi biometrik özellikler olarak seçildiği görülmektedir.


Internet
Firewall/Router
Switch
IDS
Seviye 5: Kurumsal DMZ
VPN
VPN Sunucu
Web Sunucu
FTP Sunucu
Mail Gateway
Veritabanı Katmanı
DB
Kullanıcı Kimlik Doğrulama
IT Network
IPS
Seviye 4: Yerel Kurumsal Ag
Mail Sunucu
DNS
DNS Sunucu
DHCP Sunucu
NTP Sunucu
İzleme Katmanı
Log
Log Toplayıcı
SIEM
Seviye 3: Kontrol DMZ
IT Historian
FTP Sunucu
Yama Sunucu
Uzak Erişim Sunucu
Seviye 2: Supervisory
Alarm Sunucu
İş istasyonu (Workstation)
HMI
Mühendislik PC
OT Historian
Seviye 1: Lojik
PLC
RTU
Seviye 0: Saha&Enstürmanlar
Valf
Motor
Sensörler
OT Network
Emniyetli Cihaz Sistemi (Safety Instrumented System-SIS)
Safety Zone

Şekil 2

Log yönetimi (Log Management) nasıl olmalıdır?

EKS' ler -log politikalarına bağlı olmakla beraber- büyük boyutlarda event log üretmektedir. Genelde, üretilen bu loglar merkezileştirilmek amacıyla bir log sunucusunda toplanmaktadır. Bu log sunucuları kritik verilere erişimde hatalı ve başarılı katılım bilgileri, sistemlerin yeniden başlatılma bilgileri, yetkisiz bir kullanıcının bir servis/sistem üzerinde hak yükseltme işlemleri gibi bilgiler tutmaktadır. Log yönetimi sırasında;

- Log sunucusunun fiziksel kapasite olarak uygunluğu sürekli olarak denetlenmelidir.
- Loglar mümkün olduğu kadar detay içermelidir(source/destination IP, port, protocol, kullanıcı, tarih, zaman vb.).
- Birbiriyle ilişkili kritik sistem ve uygulama loglarının düzenli bir şekilde tutulması için Network Time Protocol (NTP) stabil bir şekilde çalışmalıdır.
- IT ve OT ağları için ayrı log sunucuları kullanılmalıdır. Bu log sunucuları IT Ağı için Yerel Kurumsal Ağ Katmanının altında, OT Ağı için doğrudan Kontrol DMZ Katmanında ya da Kontrol DMZ Katmanının altında bir İzleme Katmanı içerisine konumlandırılmalıdır. İki log sunucusu da firewalllar ile izole edilmelidir.
- Burada kritik nokta, endüstriyel ortamdaki bileşenlerin uçtan uca proses bilgisi dikkate alınarak loglar alınmalı ve IT katmanında loglar ile ilişkilendirilmelidir.

Ağ Güvenliği

EKS' ler için ağ güvenliği dört başlık altında incelenebilir:

1. Ağ segmentasyonu
2. Firewall yapılandırması
3. IDS' lerin doğru kullanılması
4. Ağa giriş kontrolü

Ağ segmentasyonu : Sistemler, kendi özellik ve kritiklik seviyelerine göre –doğru konfigüre edilmek koşuluyla- subnetwork/vlan' lara ayrılmalıdır. Oluşturulan vlanlar birbirlerinden izole edilip, erişim güvenliğini sağlayıcı metotlarla (firewall, ACL, inter-vlan routing vb.) desteklenmelidir.

Firewall yapılandırılması : Purdue Model' de, gelen(inbound) ve giden(outbound) trafiği denetleme, katmanlar ve katmanlararası yetkisiz erişimlerin tespiti vb. gibi çeşitli amaçlar için firewalllar kullanılmaktadır. Bu ürünler amaca yönelik bir şekilde yapılandırılmalı ve periyodik bir şekilde kontrol edilmelidir.

IDS : Her katmana IDS ürünleriyle ek koruma sağlanmalıdır. IDS' ler, katmanlararası ihlal/atak denemelerini ve gerçekleşmiş olan ihlal/atakları tespit ederek alarm üretmekte kullanılır.

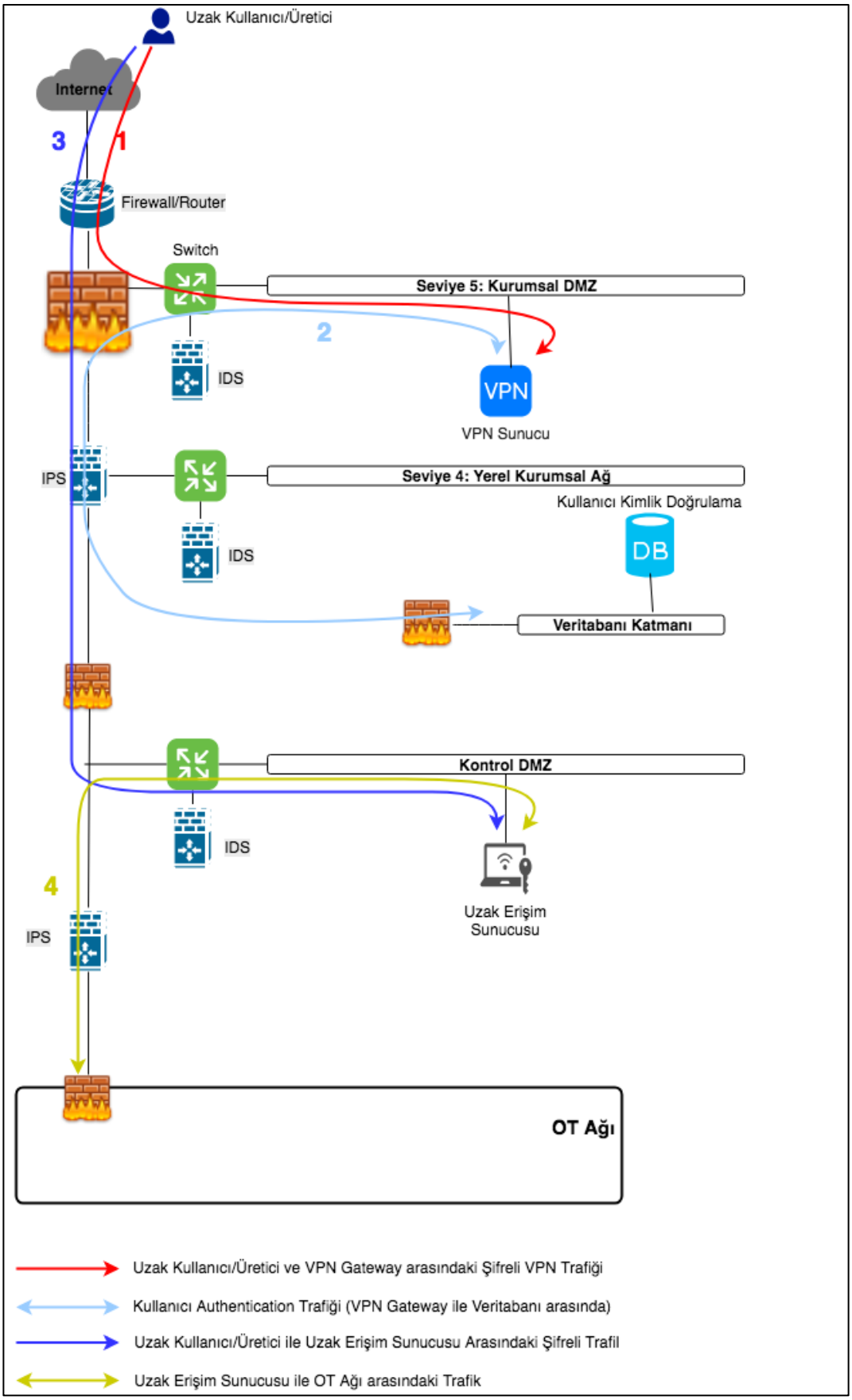
IDS' ler için en büyük problem üretilen false positive alarmlardır. IDS' ler yapılandırılırken ilgili ağdaki olağan/normal trafik olası bir atak ya da ihlal gibi tanımlandığı durumlarda, false positive alarm sayısı artacaktır. Bunun sonucu olarak olası bir ihlal/atak durumunda analistlerin işlerini zorlaştıracaktır. Bu sebeple IDS' ler kullanılırken doğru bir biçimde yapılandırmak ağ güvenliği açısından kritik bir öneme sahiptir.

Ağa giriş kontrolleri endüstriyel altyapıların ihtiyaçları dikkate alınarak tüm uç noktaları kapsayacak şekilde devreye alınmalı ve izlenmelidir. Burada kritik başarı faktörü rahat sınıflandırılamayan uç nokta bileşenlerinin sınıflandırılmasıdır.

Uzak Erişim(Remote Access) nasıl olmalıdır?

Purdue model, OT networküne erişim için iki aşamalı doğrulama (two factor authentication -2FA) kullanılmasını önermektedir. Şekil 3' de gösterilen yapıya göre, bir uzak masaüstü bağlantısı için aşağıdaki adımlar izlenmelidir:

1. Kullanıcı ile Kurumsal DMZ' de bulunan VPN sunucu arasında şifreli(encrypted) bir kanal oluşturulur.
2. VPN sunucu, gelen kullanıcıyı doğrulamak için Kullanıcı Kimlik Doğrulama(user authentication database) ile konuşur. Bu doğrulama işlemi iki aşamadan oluşmaktadır. İlk aşamada kullanıcı adı ve parola doğrulanır, ikinci aşama içinse genellikle OTP kullanılmaktadır.
3. Kullanıcı 2FA geçtikten sonra DMZ' da bulunan OT ağına erişim için kullanılacak uzak erişim sunucu/sunucularına erişir.
4. İlgili kullanıcının bu aşamadan sonra Uzak Erişim Sunucusu üzerinden OT ağına erişimi mümkün olmaktadır.


Uzak Kullanıcı/Üretici
Internet
3
1
Firewall/Router
Switch
Seviye 5: Kurumsal DMZ
2
IDS
VPN
VPN Sunucu
IPS
Seviye 4: Yerel Kurumsal Ağ
Kullanıcı Kimlik Doğrulama
IDS
DB
Veritabanı Katmanı
Kontrol DMZ
IDS
4
IPS
Uzak Erişim Sunucusu
OT Ağı
Uzak Kullanıcı/Üretici ve VPN Gateway arasındaki Şifreli VPN Trafiği
Kullanıcı Authentication Trafiği (VPN Gateway ile Veritabanı arasında)
Uzak Kullanıcı/Üretici ile Uzak Erişim Sunucusu Arasındaki Şifreli Trafil
Uzak Erişim Sunucusu ile OT Ağı arasındaki Trafik

Şekil 3

Referanslar

1. https://www.sans.org/reading-room/whitepapers/ICS/secure-architecture-industrial-control-systems-36327
2. https://na-production.s3.amazonaws.com/documents/industrial-control-system-cyber-kill-chain-36297.pdf
3. https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg-22-eng.pdf
4. https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf