5. İzmir Rüzgâr Sempozyumu ve Sergisi

Rüzgar Santrallerinde Alınması Gereken Siber Güvenlik Önlemleri

Çağrı POLAT | 05.10.2019 |12:00

Çağrı POLAT

Siber Güvenlik Uzmanı / Eğitmeni
ISO 27001 Baş Denetçi & Danışman
Endüstri 4.0 Güvenlik Uzmanı

Facebook.com/cagripolatmsc
Twitter.com/cagripolatmsc
Instagram.com/cagripolatmsc
Linkedin.com/in/cagripolat

Firma:
Maxion İnci Jant Grubu - Türkiye IT Operasyonları Md.

Eğitim:
Yüksek Lisans: Bilgisayar Mühendisliği (DEU)
Lisans: Elektrik-Elektronik Mühendisliği (Anadolu Üni.)
Lisans: İşletme Fakültesi (Anadolu Üni.)

Sertifikalar:
MCSE+S & CEH (Eğitmen)
ISO 27001 Baş Denetçi
Bilirkişi

Çalışma Alanları:
#Siber Güvenlik, #Endüstri 4.0, #Kritik Altyapı Güvenliği
#ISO27001, #Sızma Testi, #KVKK Güvenlik, #Blockchain

Mail / Telefon:
cagripolat@gmail.com , 0 553 337 48 11

Web Sitesi:
https://www.cagripolat.com

0 İçerik

- **Kritik Altyapı/Rüzgar Santrallerinde Güvenlik**
- **ISA 99 (Industrial Automation and Control Systems Security)**
- **ISA/IEC 62443**
- **Purdue Modeli/Şeması**
- **Alınması Gereken Önlemler**
- **Sorular**

1Kritik Altyapı/Rüzgar Santrallerinde Güvenlik

- “Kritik altyapı” terimi ilk defa Ekim 1997 tarihli “Amerika Birleşik Devletleri Başkanlık Komisyonu’nun Kritik Altyapıların Korunması Hakkında Raporunda kullanılmıştır.

- Siber Güvenlik Kurulu 2013-2014 Eylem planının 5 numaralı maddesinde ülkemizin kritik altyapıları bilgi güvenliği kapsamında ilk etapta "Ulaşım, Enerji, Elektronik Haberleşme, Finans, Su Yönetimi" Kritik Kamu Hizmetleri olarak belirlenmiştir. [1]

- Rüzgar santrallerinde var olan altyapı bileşenleri:
  - Endüstriyel Kontrol Sistemleri(***EKS***) bileşenleri: Scada, PLC, HMI, controller, DCS bileşenleri
  - Kurumsal Bilişim Sistemleri(***KBS***) bileşenleri: Masaüstü/Kişisel bilgisayarlar, Dosya, uygulama, veri tabanı, e-posta sunucuları vb.
  - Fiziksel Bileşenler: Çit, bariyer, sistem odası, donanım güvenliği vb.

- Rüzgar çiftliği için tipik bağlantı modeli bir halka topolojisi olarak bilinen ve bir kontrol merkezi ve buna bağlı olan her bir türbinün kendi IP adresine sahip olduğu bir yapıdır.

Mevcut yenilebilir enerji alanında yapılan yatırımlarda yaklaşık **%90** oranında siber güvenlik sistemine yatırım yapılmadığı raporlanmıştır. [2]

2 ISA 99 (Industrial Automation and Control Systems Security)

- ISA 99(Industry Standards on Automation) Endüstriyel Otomasyon ve Kontrol Sistemleri Güvenlik Standardıdır. Ağ üzerinde *etkin ve güvenli üretim uygulamalarının* tasarlanması için politikaları ve yapıları tanımlar. [3]

- ISA99 standartları geliştirme komitesi, endüstriyel otomasyon ve kontrol sistemleri güvenliği konusunda ISA standartlarını geliştirmek için dünya genelindeki endüstriyel siber güvenlik uzmanlarını bir araya getirir.

- Üretim ve kontrol sistemleri elektronik güvenliği kavramı, *tüm endüstrilerdeki her tür tesisi ve sistemi kapsayan* mümkün olan en geniş anlamda uygulanır. Üretim ve kontrol sistemleri şunları içerir, ancak bunlarla sınırlı değildir: [4]

    - DCS, PLC, SCADA, ağ bağlantılı elektronik algılama, izleme ve tanılama sistemleri gibi donanım ve yazılım sistemleri

    - Sürekli, toplu, ayrık ve diğer işlemlerde kontrol, güvenlik ve üretim işlemlerinin işlevselliğini sağlamak için kullanılan insan, ağ veya makine ara yüzleri

3 ISA/IEC 62443

- ISA99 komitesi tarafından geliştirilmiş standartlar serisidir. [5]
  (IEC: International Electrotechnical Commission)

- Bu standart ile ***şirketlerin kritik altyapı ve kontrol sistemlerindeki olası açıkları*** incelenmesi ve etkin koruma önlemleri geliştirilmesi için temel oluşturulması hedeflenmektedir.

- Endüstriyel otomasyon ve kontrol sistemlerine yönelik IT güvenliği, bu standardın odak noktasıdır. [6]

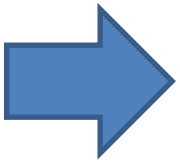
- IEC 62443 standardı, dört temel üzerinde şekillendirilmiştir.
  1. Standart fonksiyonları içerir.
  2. Zorunlu şartları karşılayan endüstriyel otomasyon ve kontrol sistemleri için IT güvenlik yönetimi sisteminin çerçevesini belirlemektedir.
  3. Endüstriyel otomasyon ve kontrol sistemleri (IACS) için tasarı kılavuzu olarak kullanılabilecek teknik özelliklerdir.
  4. Kontrol sistemi bileşenlerine ilişkin tasarım ve geliştirme şartlarından oluşmaktadır.

4 Purdue Modeli

- ISA 99 komitesi, Purdue Enterprise Reference Architecture (PERA) modeli ve ICS ağ bölümlemesi için bu modeli kullanmıştır. [7]

- Purdue model katmanlı mimarisi, **her katmanın gereksinimlerini dikkate alarak BT ve kritik ağları alt ağlara (alt ağlar veya VLAN) ayırma ilkesine dayanır.**

- Purdue modeli 6 katmandan oluşur:
  - Seviye 5: Kurumsal ağ
  - Seviye 4: Yerel ağ
  - Seviye 3: Saha işlemleri
  - Seviye 2: Saha kontrolü
  - Seviye 1: Mantık kontrol
  - Seviye 0: Sensör, sürücü vb.

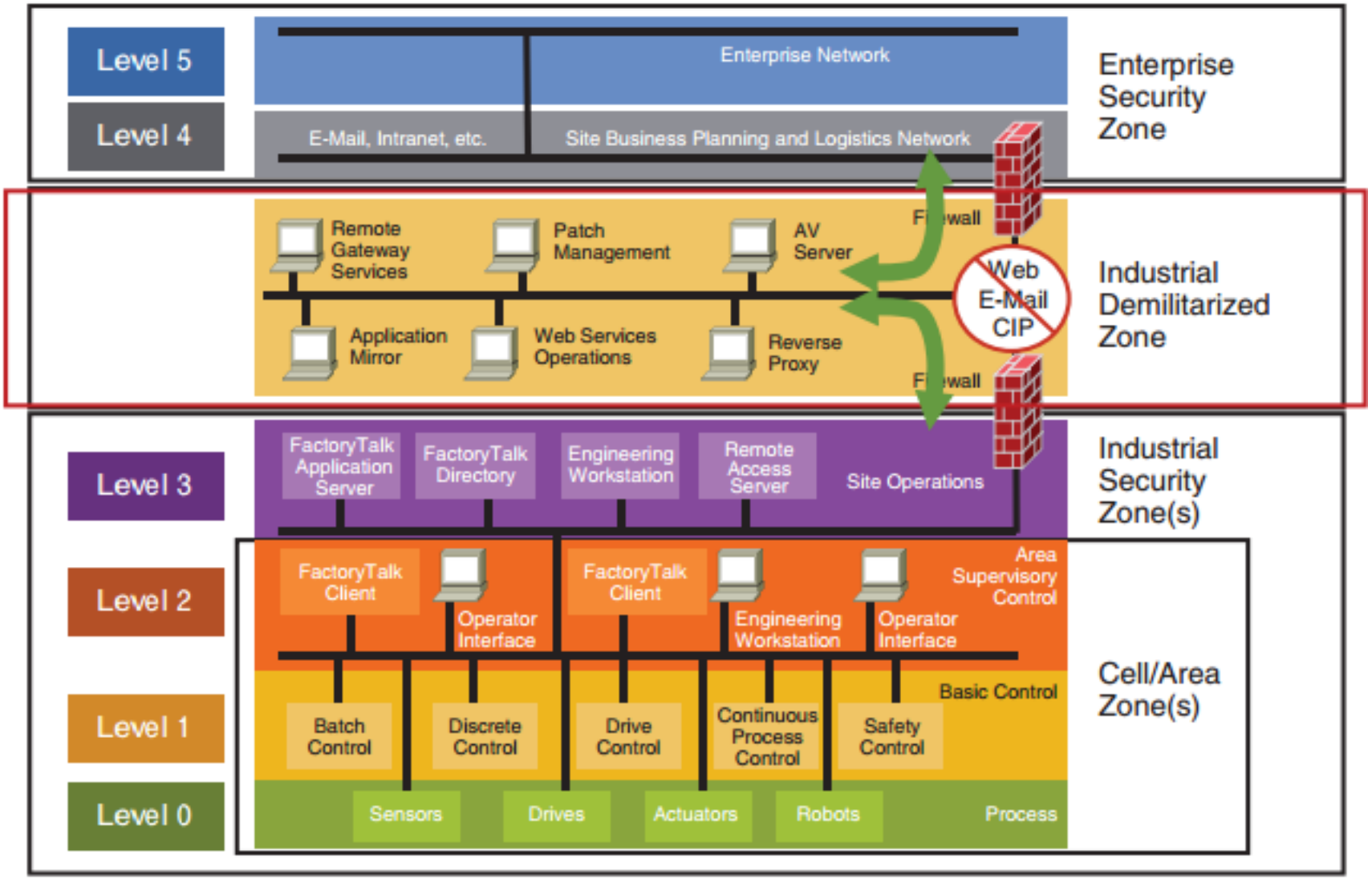


Yanda belirtilen 6 katmanın her biri için, aşağıdaki dört ana odak alanı tartışılmalıdır:

1.Giriş kontrolü
2.Log Yönetimi
3.Ağ güvenliği
4.Uzaktan erişim

Çok katmanlı Güvenlik Mimarisi!

Purdue Şeması



https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems

5 Alınması Gereken Önlemler

- Endüstriyel kontrol sistemleri direkt internete bağlanamaz!
- Sisteme giriş yapmak için kimlik doğrulamayı ve çok faktörlü korumayı(2FA, MFA) zorunlu yapılmalı.
- Hesap kilitleme özelliğini aktif hale getirilmeli.
- Ağdan dışarı ve içeri yetkisiz uzaktan bağlanma programları kullanılmamalı.
- Türbinlere ve merkezi veri toplama sistemlerine yapılacak uzak bağlantı altyapısı için güvenli VPN yapısı kurulmalı ve bu oturumlar kayıt edilmeli.
- Varsayılan sistem hesaplarını kaldırın, devre dışı bırakın veya yeniden adlandırılmalı.
- Tüm hesaplar için güçlü karmaşıklığı olan şifreler seçilmeli ve 3/6 ayda bir bunlar değiştirilmeli.

TR & 502 TCP : 805

Teamviewer?

Admin:admin !

Alınması Gereken Önlemler

- Yönetici hesaplar sürekli incelenmeli. ✗
- Loglar sürekli kontrol edilmeli ve korelasyon kuralları yazılmalı. ✗
- Saha düzeyinde(OT) zafiyet ve tehlikelerden haberdar olunmalı! IPS,IDS? ✗
- Donanımlar ve yazılımlar olabildiğince güncel olmalı. Güvenli yama mekanizması! ✗
- Çalışan farkındalığı ve eğitim sürekli yapılmalıdır. İnsan! ✗
- Kritik bir durumda ne yapılması gerektiği bilinmeli ve belirli aralıkla tatbikatlar yapılmalıdır. ✗
- Risk analizleri, politikalar, dökümantize edilmiş süreçler ve kontrol listeleri hayat kurtarabilir! ISO27001 zorunlu alınıyor ama bizi bu sertifika saldırılara karşı korumaz!
- Network seviyesinde önlemler (üretim FW, VLAN ayrılması, ACL, anti-virüs, USB bloklama vb.) alınmalı.
- Sızma testleri belirli aralıklar ile yapılmalı ve çıktıları üzerinde durulmalı!

Kaynaklar

[1] https://www.slideshare.net/ZhreAydn/kritik-enerji-altyapilarinin-korunmasi-ve-siber-gvenlik
[2] http://ozdenercin.com/2018/07/31/gunes-ve-ruzgar-ciftliklerinin-siber-guvenligi/
[3] https://otomasyonadair.com/2014/11/07/bilinmesi-gereken-4-it-standardi/
[4] https://www.isa.org/isa99/
[5] https://www.isa.org/intech/201810standards/
[6] https://www.tuv-sud.com.tr/tr-tr/merkez/kaynak-merkezi/yayimlar/e-ssentials-haber-buelteni/demiryolu-hizmetleri-ile-ilgili-e-ssentials/e-ssentials-3-2015/certification-according-to-iec-62443-boosting-security-against-cyber-attacks
[7]https://subscription.packtpub.com/book/networking_and_servers/9781788395151/1/ch01lvl1sec10/the-purdue-model-for-industrial-control-systems


SORULAR
TEŞEKKÜRLER