Elektrikli Sarj Istasyonlarinin Guvenligi Uzerine SWOT Analizi

1. Guclu Yonler (Strengths)

Gelismis Sifreleme ve Iletisim Protokolleri:
Yeni nesil sarj istasyonlari, OCPP 2.0.1 ve ISO 15118 standartlarinda yer alan TLS 1.3 sifreleme teknolojilerini kullanarak veri iletisimini guvence altina almaktadir. Bu durum, ortadaki adam (MITM) saldirilarina karsi yuksek koruma saglar.

Donanim Tabanli Guvenlik Modulleri (HSM):
Gomulu Donanim Guvenlik Modulleri sayesinde anahtar yonetimi donanim duzeyinde yapilmakta, yetkisiz erisim riski en aza indirilmektedir.

Gercek Zamanli Izleme ve Guncelleme:
Merkezi yonetim sistemleri (CSMS) araciligiyla log kayitlari analiz edilmekte, uzaktan yazilim guncellemeleri (OTA) guvenli bicimde uygulanmaktadir.

Uluslararasi Standartlarla Uyum:
IEC 61851, IEC 63119 ve ISO/IEC 27001 standartlarina uyum, sistem guvenilirligini artirarak yatirimci guvenini saglamaktadir.

2. Zayif Yonler (Weaknesses)

Fail-Open Davranisi:
Kimlik dogrulama servisinin cokmesi halinde bazi sistemler, hizmet devamliligini korumak amaciyla fail-open moduna gecerek yetkisiz enerji kullanimina yol acmaktadir.

Guncelleme ve Tedarik Zinciri Aciklari:
Firmware guncellemelerinde yeterli dogrulama yapilmamasi, kotu niyetli yazilimlarin sisteme yuklenmesine neden olabilir.

Ag Segmentasyonu Eksikligi:
Sarj istasyonlarinin dogrudan internete baglanmasi, ag guvenligini zayiflatmakta ve siber saldiri riskini artirmaktadir.

Insan Faktoru ve Bilinc Eksikligi:
Kurulum ekiplerinin varsayilan parolalari degistirmemesi, yetkisiz erisim riskini artirmaktadir.

Enerji Yonetimi ile Guvenlik Arasindaki Kopukluk:
Enerji muhendisligi ile siber guvenlik ekipleri arasinda koordinasyon eksikligi, sistem butunlugunu olumsuz etkilemektedir.

3. Firsatlar (Opportunities)

Yapay Zeka Destekli Guvenlik Sistemleri:
Makine ogrenmesi tabanli algoritmalarla anomali tespiti yapilarak saldirilar erken asamada belirlenebilir.

Blok Zinciri (Blockchain) Tabanli Kimlik Dogrulama:
Kullanici kimlikleri ve sarj islemleri blok zincirinde saklanarak degistirilemez guvenlik kayitlari olusturulabilir.

Mikro Sebeke (Microgrid) Guvenligi:
Zero-trust prensipleri mikro sebeke altyapilarinda uygulanarak sistem dayanikliligi artirilabilir.

Regulasyon ve Yasal Tesvikler:
EPDK, AB NIS2 ve ISO/IEC 27019 standartlari guvenli sistem gelistirmeyi tesvik etmektedir.

Hibrit Guvenlik Yaklasimlari:

Fiziksel sensorler ile yazilim tabanli guvenlik katmanlarinin entegrasyonu, cok katmanli savunma saglar.

4. Tehditler (Threats)

Siber Saldirilar ve Devlet Destekli Tehditler:
Kritik altyapilar hedef alinara enerji surekliligi tehlikeye atilabilir.
Zincirleme Ariza (Cascade Failure):
Tek bir CSMS sisteminin cokmesi, binlerce istasyonun hizmet disi kalmasina neden olabilir.
Enerji Manipulasyonu:
Kasitli voltaj veya akim degisiklikleri fiziksel cihaz arizalarina yol acabilir.
Sosyal Muhendislik ve Sahte Bakim Vakalari:
Saldirganlar bakim personeli kiligina girerek fiziksel erisim saglayabilir.
Veri Gizliligi ve Yasal Riskler:
Kullanici verilerinin sizmasi, KVKK ve GDPR ihlallerine yol acabilir.

5. Stratejik Degerlendirme (Meta Katman)

Elektrikli sarj istasyonlari, yalnizca enerji noktasi degil ayni zamanda siber-fiziksel sistemlerdir. Bu sistemler hem IoT cihazi, hem odeme terminali hem de enerji yonlendiricisidir. Dolayisiyla geleneksel bilisim guvenligi yerine Endustriyel Kontrol Sistemleri (ICS) prensipleri benimsenmelidir.

6. Onerilen Stratejik Yaklasimlar

• Sifir Guven Mimarisi (Zero Trust): Her bilesen yalnizca dogrulama sonrasinda erisim saglamalidir.
• Yapay Zeka Tabanli Anomali Tespiti: Enerji akis ve kullanici davranislari analiz edilerek anomali tespiti yapilmalidir.
• Fail-Closed Politikasi: Sistem cokmesi durumunda guvenlik oncelikli sekilde kapanmalidir.
• Surekli Guvenlik Testleri: Penetrasyon testleriyle zafiyetler duzenli olarak analiz edilmelidir.
• Siber-Fiziksel Entegrasyon: Enerji guvenligi ve siber guvenlik disiplinleri esgudumlu calismalidir.

7. SWOT Sonuc Tablosu

Kategori	Teknik Odak	Operasyonel Odak	Gelecek Odakli Etki
Guclu Yonler	TLS, HSM, OCPP 2.0.1	Merkezi CSMS kontrolu	Standart uyumlulugu ve guven artisi
Zayif Yonler	Fail-open, firmware riskleri	Zayif fiziksel guvenlik	Guvenlik butunlugu eksikligi
Firsatlar	Yapay zeka, blok zinciri	Regulasyon ve Ar-Ge tesvikleri	Akilli sebekelerde liderlik
Tehditler	APT, enerji manipulasyonu	Sosyal muhendislik	Ulusal altyapi guvenligi riski