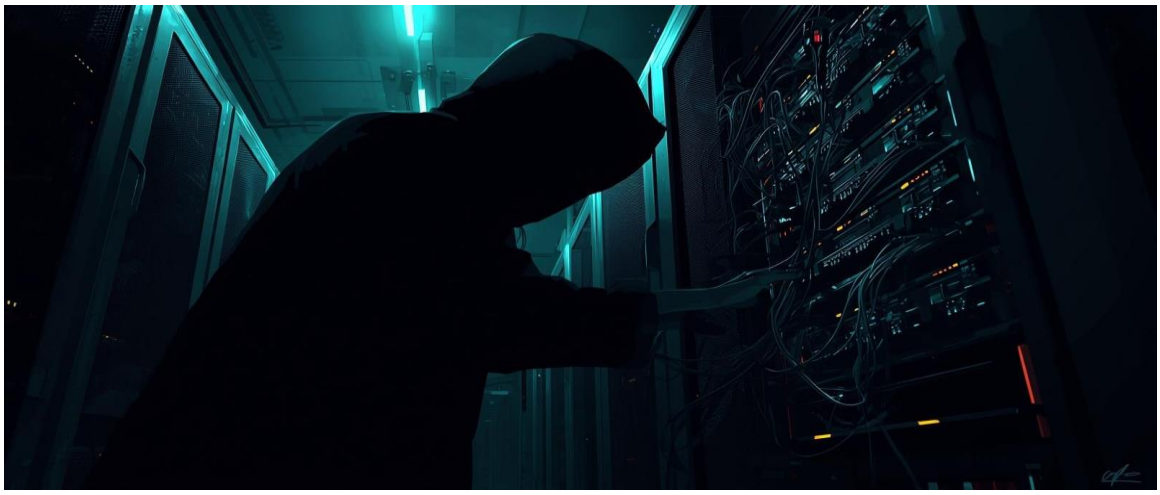
Elektrikli Araç Şarj İstasyonlarının Fiziksel Güvenlik Risk Analizi Raporu

Giriş

Elektrikli araç şarj istasyonları, enerji iletimi, kullanıcı kimlik doğrulaması, veri iletişimi ve ödeme işlemleri gibi kritik fonksiyonları bir arada barındırır. Bu karmaşık yapı, yalnızca yazılım güvenliğini değil, **fiziksel güvenliği** de aynı derecede önemli hale getirir.
Fiziksel zafiyetler, sistemin doğrudan manipülasyonuna, kullanıcı güvenliğinin tehlikeye girmesine ve enerji altyapısına zarar verilmesine yol açabilir.

1.Yetkisiz Erişim



Olası Sorunlar:

- Yetkisiz kişilerin **bakım panellerine** veya **kontrol kutularına** erişim sağlaması
- Güvenliksiz veya standart dışı kilit mekanizmalarının kolayca kırılması
- Personel erişim anahtarlarının kopyalanması

Nasıl Oluşur:

- Bakım kapaklarının zayıf fiziksel korumaya sahip olması (örneğin basit tornavida ile açılabilir paneller)
- RFID veya manyetik kilitlerin mekanik olarak devre dışı bırakılması
- Personel kimlik kartlarının veya anahtarlarının sosyal mühendislik yoluyla ele geçirilmesi

Olası Sonuçlar:

- Şarj kontrol modülüne erişilerek **veri manipülasyonu** veya **yetkisiz şarj başlatma**
- Güç hattı kesilmesi veya kısa devre oluşturularak **cihazın çalışmaz hale gelmesi**
- İstasyonun iç bileşenlerinden veri çalınması (ör. işlem geçmişi, kullanıcı logları)

Çözüm Nedir?

Amaç: Kasa, bakım paneli ve kritik bağlantılara izinsiz fiziksel erişimi engellemek; erişim gerçekleştikten sonra zarar verme veya veri çalma ihtimalini azaltmak.

Kısa Vadeli

- Bakım panellerini **tek yönlü cıvata/özel vidalar** ile sabitle (tamper-proof vidalar).
- Kasa etrafına **tamper-evident mühür** (bozulduğunda belli olur) uygula.
- Bakım/servis etiketleri ve gözetim logları bulundur (kimin, ne zaman eriştiği not edilir).

Orta Vadeli

- Bakım kapağına **manyetik/lojik tamper switch** tak — kapağın açılması sistem loglarına düşsün ve alarm tetiklesin.
- Kritik servis portları (USB, UART, Ethernet) için **kilitlenebilir kapak** veya fiziksel port-kilitleri uygula.
- Yetkili erişim için **iki faktörlü fiziksel erişim** (ör. fiziksel anahtar + bakım PIN'i) uygulaması getir.

Uzun Vadeli

- Kasa içeriğini sadece yetkili personel görebilsin: **akıllı erişim kontrolü** (kayıtlı RFID + merkezi doğrulama).
- Bakım anahtarlarının dağıtımını sınırlandır; yedek anahtarlar için kayıtlı prosedür belirle.

2.Elektriksel Tehlikeler

Olası Sorunlar:

- Topraklama eksikliği veya gevşek bağlantılar sonucu **elektrik çarpması riski**
- Kablo izolasyonlarının kesilmesi veya aşınmasıyla **ark oluşumu ve yangın riski**
- Şarj portunun su veya nem temasıyla **kısa devre** oluşturması

Nasıl Oluşur:

- Kabloların dış ortamda uygun koruma olmadan bırakılması
- Kullanıcıların kabloları zorlaması veya yanlış tak-çıkar işlemleri
- Aşırı ısınma sonucu iç bileşenlerin izolasyonunun zayıflaması

Olası Sonuçlar:

- Kullanıcı veya bakım personelinde **elektrik çarpması yaralanmaları**
- Donanım arızası ve **enerji iletim kesintileri**
- Şarj istasyonunun tamamen devre dışı kalması

Çözüm Nedir?

Amaç: Topraklama, kaçak akım ve aşırı gerilim kaynaklı yaralanma/yangın riskini asgariye indirmek.

Kısa Vadeli

- Topraklama bağlantılarının görünür şekilde etiketlenmesi ve gevşek bağlantıların tespiti; acil düzeltme.
- Kaçak akım koruma rölesi (RCD/RCCB) ve MCB etiketlerinin kontrolü; çalışıp çalışmadığını üretici önerisi ile doğrula.
- IP ve kablo kılıfı kontrolü: yıpranmış izolasyon tespit edilirse koruyucu spiral/kanal koy.

Orta Vadeli

- Harici SPD (Surge Protection Device) montajı; özellikle dış ortamdaki istasyonlarda.
- Kabloların metal koruyucu conduit veya zırhlı boru içine alınması.
- Kasa içinde termal sensör/ısı izleme ile aşırı ısınma erken tespiti.

Uzun Vadeli

- Elektriksel tesisat için periyodik (yıllık/2 yıllık) **toprak direnci ölçümü**, izolasyon direnç testi ve termal görüntüleme.
- Kullanıcı alanında akım kaçaklarını azaltmak için **AC/DC izolasyon önlemleri** ve üretici destekli güvenlik devreleri.

3. Kart ve Ödeme Sistemleri Manipülasyonu

Olası Sorunlar:

- **Kredi kartı veya RFID kimlik sistemlerinin klonlanması**
- **Kart okuyucuların içine yerleştirilen skimmer cihazları**
- Ödeme modülünün devre dışı bırakılarak sistemin “ücretsiz şarj”a zorlanması

Nasıl Oluşur:

- Kart okuyucu bölgesine fiziksel olarak sahte modül takılması
- USB/seri port bağlantılarına doğrudan erişim sağlanması
- Okuyucu modülün yazılım güncelleme portunun fiziksel olarak manipüle edilmesi

Olası Sonuçlar:

- Kullanıcıların **finansal bilgilerinin sızdırılması**
- Yetkisiz kişilerin **ücretsiz enerji kullanımı**
- Şarj istasyonunun **ödeme sistemi devre dışı kalmasıyla gelir kaybı**

Çözüm Nedir?

Amaç: Kart/kullanıcı verilerinin fiziksel müdahale ile çalınmasını önlemek; ödeme modülünün manipülasyonunu engellemek.

Kısa Vadeli

- Kart okuyucu çevresine **anti-skimming çerçevesi/conta** ekle (fiziksel boşlukları azaltır).
- POS/okuyucu montaj noktalarını sağlamlaştır; yüzeydeki çizik/ek parçaları düzenli denetle.
- Ödeme kablolarını iç kasadan geçir ve dışarıdan erişimi kes.

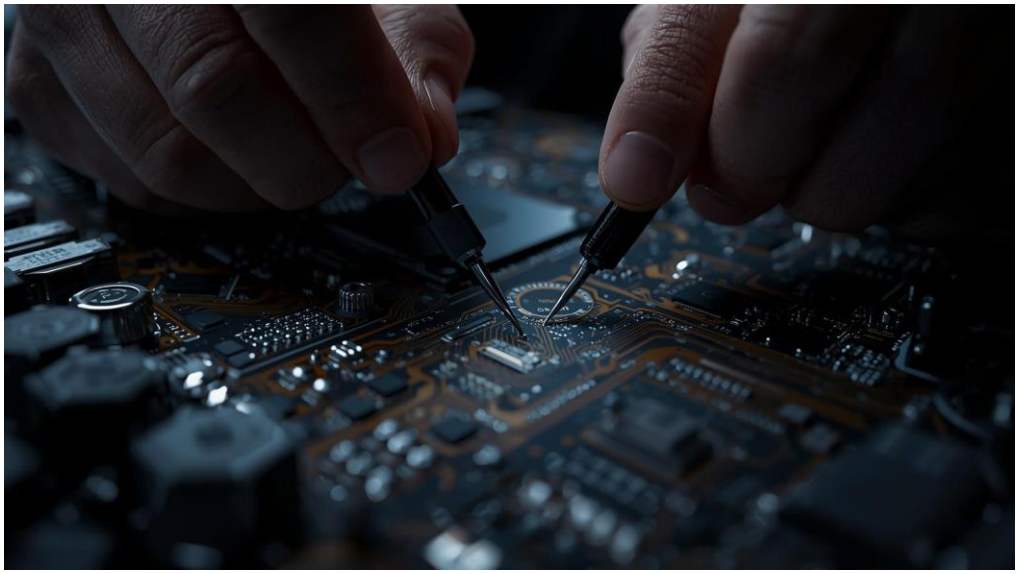
Orta Vadeli

- Kart okuyucu ve POS için **tamper-evident tasarım**; okuyucuda fiziksel değişim algılanırsa cihaz işlevini durdursun.
- Ödeme modülü ile merkezi sunucu arasında sonlandırılmış, şifreli iletişim sağlayarak fiziksel veri hattına erişilse dahi verinin okunmasını engelle.

Uzun Vadeli

- Okuyucu güvenlik standardına uygun (PCI-DSS uyumlu veya üretici sertifikalı) donanım tercih et.
- Düzenli POS/ödemeye yönelik güvenlik denetimleri ve üçüncü parti skimming testleri uygula.

4.Donanım Manipülasyonu ve Sabotaj



Olası Sorunlar:

- Şarj ünitesinin iç devrelerine müdahale edilmesi
- Güç kartlarının sökülmesi, modüllerin yerinden çıkarılması
- Güvenlik sensörlerinin veya termal korumanın devre dışı bırakılması

Nasıl Oluşur:

- Saldırganın kapağı açarak donanım bileşenlerine fiziksel müdahale etmesi
- Firmware veya diagnostic portları üzerinden donanım yeniden programlanması
- Küçük cihazlar (ör. Raspberry Pi, microcontroller) yerleştirilerek veri toplanması

Olası Sonuçlar:

- **Veri sızıntısı** (ör. kimlik doğrulama logları, şarj süreleri)
- **Aşırı ısınma ve yangın riski**
- **Uzaktan saldırıların** fiziksel arka kapı üzerinden yapılabilmesi

Çözüm Nedir?

Amaç: Fiziksel erişimle cihaza arka kapı konulmasını, firmware yükleme veya diagnostic portlarla sistem ele geçirilmesini engellemek.

Kısa Vadeli

- Kullanılmayan servis/diagnostic portlarını **fiziksel olarak kapat** (koruyucu kapak + mühür).
- Port üzerindeki etiketleri ve vidaları kontrol et; izinsiz müdahale izlerini kaydet.

Orta Vadeli

- Cihazda **secure boot** ve imzalı firmware mekanizması talep et/etkinleştir.
- Kritik portlara erişim sadece yetkili uygulama ile mümkün olsun; port erişimi için fiziksel anahtar veya kod gereksinimi getir.

Uzun Vadeli

- Donanım üzerinde TPM veya güvenlik çipi ile kimlik doğrulama; firmware güncellemeleri sadece dijital imzalı paketlerle yapılabilsin.
- Cihaz üzerindeki değişiklikleri merkezi olarak raporlayacak telemetri ve HSM tabanlı doğrulama altyapısı kur.

5.Vandalizm ve Çevresel Sabotaj

Olası Sorunlar:

- Kırılmış ekranlar, kesilmiş kablolar, sprey boya veya yapıştırıcı ile zarar verme
- Metal parçalar veya sıvı maddelerle donanımın kısa devreye sokulması
- Harici darbe veya bükülme sonucu şarj portlarının devre dışı kalması

Nasıl Oluşur:

- Kamuya açık istasyonlarda gözetimsizlik
- Kamera veya aydınlatma eksikliği
- Koruyucu kabin veya bariyer bulunmaması

Olası Sonuçlar:

- İstasyonun **tamamen devre dışı kalması**
- **Onarım ve bakım maliyetlerinde artış**
- Kullanıcı güveninde azalma ve **altyapı itibarı kaybı**

Çözüm Nedir?

Amaç: İstasyona yönelik kasıtlı zarar eylemlerinin tespitini, müdahalesini ve etkisini en aza indirmek.

Kısa Vadeli

- İstasyona yakın alanı **aydınlatma** ile güçlendir.
- Görünür şekilde "güvenlik ile izleniyor" levhaları as — caydırıcı etki yapar.
- Kablolar için açıkta kalan bölümlere koruyucu kanal koy.

Orta Vadeli

- Kamera ve hareket sensörü tabanlı gözetim (CCTV) kur; kayıtlar merkezi bir sunucuya gönderilsin.
- Fiziksel bariyer veya montaj braketlerini güçlendir (şiddetli darbelere dayanıklı montaj).
- Ekran ve kullanıcı arayüzlerini darbelere karşı güçlendirilmiş cam/kapak ile koru.

Uzun Vadeli

- Bölge için saha güvenlik protokolleri: rutin devriye, uzaktan izleme, sigorta & SLA anlaşmaları.
- İstasyona yönelik saldırı sonrası hızlı müdahale ekibi ve yedek parça stoğu oluştur.

Sonuç ve Değerlendirme

Fiziksel güvenlik, şarj istasyonlarının bütünsel güvenlik mimarisinin temel bileşenidir. Yetkisiz erişim, donanım manipülasyonu, ödeme sistemleri saldırıları veya vandalizm olayları; hem **kullanıcı güvenliği**, hem de **enerji altyapısının sürekliliği** açısından ciddi riskler taşır.
Bu nedenle fiziksel koruma önlemleri (kilit mekanizmaları, sensör tabanlı izleme, kamera sistemleri, erişim loglama, kabin mühürleme vb.) yazılımsal güvenlikle birlikte düşünülmelidir.