Rapor: Elektrikli Araç (EV) Şarj İstasyonları Güvenliği ve Türkiye Pazar Analizi

Tarih: 2 Kasım 2025
Konu: Küresel ve ulusal ölçekte elektrikli araç şarj altyapılarına yönelik siber güvenlik risklerinin, Türkiye pazarındaki regülasyonların ve operatörlerin güvenlik yeterliliklerinin incelenmesi.

1. Tespit Edilen Riskler ve Küresel Örnek Olaylar

Elektrikli araç şarj istasyonları (EVSE), izole güç üniteleri değil, internete bağlı, ödeme sistemleri entegre edilmiş ve enerji şebekesiyle (grid) doğrudan iletişim kuran karmaşık siber-fiziksel sistemlerdir. Bu durum, onları ciddi siber güvenlik tehditlerine açık hale getirmektedir.

Tespit edilen başlıca riskler, sadece bireysel araçların veya kullanıcı verilerinin tehlikeye atılmasıyla sınırlı değildir; aynı zamanda enerji şebekesinin istikrarını bozmaya yönelik (Grid-level) saldırı potansiyeli de taşımaktadır.

Başlıca Küresel Olaylar ve Zafiyetler:

- **İstasyon Manipülasyonu:** 2022'de Rusya ve İngiltere'de, şarj istasyonlarının kontrolünün ele geçirildiği, ekranlarında propaganda amaçlı veya uygunsuz içeriklerin yayınlandığı olaylar raporlanmıştır.
- **Veri Sızıntıları:** Kullanıcı verilerini (ödeme bilgileri, konum kayıtları) hedef alan saldırılar gerçekleşmiş, bir vakada ~116.000 kullanıcının kaydı sızdırılmıştır.
- **Uzaktan Komut Çalıştırma (CVE):** 2024'te "eCharge" marka istasyonlarda, saldırganların kimlik doğrulaması olmadan istasyon üzerinde uzaktan komut çalıştırmasına olanak tanıyan kritik güvenlik açıkları (CVE) keşfedilmiştir.
- **Ağ Zafiyetleri:** Birçok istasyonun zayıf varsayılan yapılandırmalar (örn. açık SSH/HTTP portları, şifresiz iletişim) kullandığı tespit edilmiştir.
- **Fiziksel Saldırılar:** 2025 tarihli akademik çalışmalar, şarj portuna takılan fiziksel bir cihaz aracılığıyla "sinyal enjeksiyonu" (Signal Injection) yapılarak şarj sürecinin manipüle edilebileceğini göstermiştir.

2. Türkiye Pazarındaki Gelişmeler ve Operatörler

Türkiye EV şarj pazarı, hızlı bir büyüme ve aynı zamanda ciddi bir regülasyon sürecinden geçmektedir.

2.1. Düzenleyici Çerçeve: EPDK ve Lisans İptalleri

Pazar, Enerji Piyasası Düzenleme Kurulu (EPDK) tarafından sıkı bir şekilde

düzenlenmektedir. 2024 ve 2025 yıllarında, pazara giren ancak mevzuatta belirtilen yükümlülükleri (belirlenen sürede yeterli sayıda şarj ağı kurma vb.) yerine getirmeyen veya finansal yeterlilik gösteremeyen çok sayıda firmanın (örn. Altunkaya Enerji, Tunalar Otomotiv, Yiğit Akü) şarj ağı işletmeci lisansı EPDK tarafından iptal edilmiştir.

Bu durum, pazarın "gerçek yatırım yapan" ve operasyonel yeterliliğe sahip oyuncular lehine konsolide olduğunu göstermektedir.

2.2. Aktif Pazar Oyuncuları ve Pazar Payları (Ekim 2025 İtibarıyla)

2025 son çeyreği itibarıyla Türkiye'deki toplam şarj soketi sayısı 33.500 ila 35.000 bandına ulaşmıştır. Pazar, üç büyük oyuncu tarafından domine edilmektedir:

1. **ZES (Zorlu Enerji):** Toplam soket sayısında pazar lideridir. Özellikle şehir içi lokasyonlarda ve AC (normal hız) şarj noktalarındaki yaygınlığı ile öne çıkmaktadır.
2. **Trugo (Togg):** Pazarın en hızlı büyüyen oyuncularından biridir. Stratejisi belirgin şekilde DC (hızlı şarj) odaklıdır ve özellikle otoyol koridorlarında güçlü bir ağa sahiptir.
3. **Eşarj (Enerjisa):** DC (hızlı şarj) soket sayısında Trugo ile başa baş bir konumdadır ve yine otoyol ile kurumsal lokasyonlarda güçlüdür.

Bu üç operatör dışında **Voltrun (Zebra)** kurumsal ve lojistik odaklı, **Tesla Supercharger** ise kendi kapalı ekosistemine yönelik hizmet vermektedir.

3. Türkiye Operatörleri İçin Siber Güvenlik Analizi ve Sonuç

Pazardaki rekabet artarken, operatörlerin siber güvenlik yeterlilikleri kritik bir ayrıştırıcı haline gelmektedir. Bir operatörün güvenlik olgunluğunu belirleyen iki temel uluslararası standart öne çıkmaktadır:

1. **ISO/IEC 27001 (BGYS):** Bilgi Güvenliği Yönetim Sistemi. Operatörün veri güvenliği, risk yönetimi ve operasyonel süreçlerini uluslararası bir standarda göre yürüttüğünü belgeler.
2. **OCPP (Open Charge Point Protocol) 2.0.1 - Güvenlik Profili 3:** Bu, güncel en yüksek güvenlik standardıdır. İstasyon ile merkez arasındaki iletişimin karşılıklı kimlik doğrulama (mTLS) ile şifrelenmesini ve güvenli firmware güncellemelerini zorunlu kılar.

3.1. Operatörlerin Güvenlik Karnesi (Kamusal Beyanlar)

Operatörlerin kamuya açık belgeleri (web siteleri, kurumsal raporlar) incelendiğinde, güvenlik sertifikasyonlarına ilişkin şu tablo ortaya çıkmaktadır:

- **ZES (Zorlu Enerji):** Grup (Zorlu Enerji) düzeyinde ISO/IEC 27001 politikası ve sertifikasyon beyanı bulunmaktadır.
- **Eşarj (Enerjisa):** Ana grup (Enerjisa) bünyesinde ISO/IEC 27001'e referans veren bir Bilgi Güvenliği Yönetim Sistemi yaklaşımı mevcuttur.
- **Trugo (Togg):** ISO 9001, 14001 gibi kalite ve çevre yönetimi sertifikaları kamuya açıktır. Ancak, **ISO 27001 (Bilgi Güvenliği) için kamuya açık bir beyan veya**

sertifika tespit edilmemiştir.

- **Voltrun (Zebra):** Operasyonel yeterlilikleri belirtilmekle birlikte, **ISO 27001 için kamuya açık bir beyan tespit edilmemiştir.**

3.2. Rapor Sonucu ve Nihai Değerlendirme

EV şarj altyapısı güvenliği, hem küresel hem de ulusal düzeyde kanıtlanmış bir risktir. Türkiye pazarında, EPDK'nın düzenleyici hamleleri pazarı konsolide ederken, operatörlerin güvenlik konusundaki olgunlukları farklılık göstermektedir.

ZES ve Eşarj, ana grupları aracılığıyla ISO 27001 standartlarına uyum konusunda kamusal beyanlara sahipken, pazarın en önemli oyuncularından olan Trugo ve Voltrun için bu konuda kamuya açık bir bilgi bulunmamaktadır (Bu, ilgili standarda sahip olmadıkları anlamına gelmez, yalnızca kamusal olarak beyan edilmediği anlamına gelir).

Eyleme Geçirilebilir Sonuç: Bireysel kullanıcıların güvenilir operatörleri tercih etmesi; kurumsal müşterilerin veya filo yöneticilerinin ise anlaşma yapacakları operatörden **ISO/IEC 27001 sertifikasyonunun kapsamını** ve **OCPP 2.0.1 Güvenlik Profili 3 (mTLS ile)** kullandıklarını yazılı olarak teyit etmeleri, siber güvenlik risklerini en aza indirmek için kritik bir öneme sahiptir.