ELEKTRİKLİ ARAÇ ŞARJ CİHAZI (EVC) & SİBER GÜVENLİK

Elektrikli Araç Şarj Cihazı ve Siber Güvenlik: Enerji Dönüşümünün Görünmeyen Yüzü

Elektrikli araçların hızla yaygınlaşması, yalnızca otomotiv sektöründe değil enerji altyapılarında da köklü bir dönüşümü beraberinde getirmektedir. Ancak bu dönüşüm, enerji güvenliği ile siber güvenliğin kesişim noktasında yeni risk alanları yaratmaktadır. Şarj üniteleri, dijital ağlar üzerinden kimlik doğrulama, ödeme sistemleri ve uzaktan güncellemelerle çalışırken, aynı zamanda enerji şebekesinin kritik parçalarıdır. Bu yazı, elektrikli araç şarj altyapısının karşılaştığı siber tehditleri, Avrupa'daki güvenlik standartlarını, enerji savaşları bağlamındaki jeopolitik riskleri ve kullanıcı farkındalığının gelecekteki önemini tartışmayı amaçlamaktadır.

E-Mobility ve Siber Güvenlik Paradigması

Son yıllarda küresel ölçekte yaşanan enerji dönüşümü, otomotiv sektörünü yeniden tanımlamaktadır. 2030'a kadar dünya genelinde 150 milyonun üzerinde elektrikli araç yollarda olacak. Türkiye'de de hızla büyüyen pazar, altyapıya olan talebi artırırken, güvenlik konusunu daha kritik hale getirmektedir.

Elektrikli araç şarj üniteleri artık yalnızca enerji aktarım noktası değil; internete bağlı akıllı cihazlar konumundadır. Bu durum onları yalnızca teknik bakım gerektiren bir donanım olmaktan çıkarıp, siber saldırıların hedefi haline getirmektedir.

Altyapıda Görülen Siber Tehditler

EVC'ler farklı tipte saldırılarla karşı karşıya kalabilir:

- Kimlik doğrulama zafiyetleri (yetkisiz erişim),
- Man-in-the-Middle saldırıları (iletişimin manipüle edilmesi),
- İletişim güvenliğinde yetersiz şifreleme,
- Hizmet dışı bırakma (DoS/DDoS) saldırıları,
- Zararlı yazılım yüklü güncellemeler.

Bu tehditler, yalnızca bireysel kullanıcıların değil, ulusal enerji şebekelerinin de güvenliğini tehlikeye atabilecek boyuttadır.

Avrupa ve İngiltere'den Güvenlik Yaklaşımları

Avrupa'da elektrikli araç şarj altyapısının güvenliği yalnızca gönüllü standartlarla değil, bağlayıcı yasal düzenlemelerle de desteklenmektedir. Avrupa Birliği'nin yeni düzenlemeleri, cihazların kablosuz iletişim güvenliği, kullanıcı verilerinin korunması ve ürünün tüm yaşam döngüsü boyunca yazılım güncellemeleri ile desteklenmesini zorunlu hale getirmiştir. AB'nin Radyo Ekipmanları Direktifi (RED) kapsamındaki güvenlik hükümleri, bu alanda gizlilik ve siber güvenlik şartlarını tanımlarken, Siber Dayanıklılık Yasası (Cyber Resilience Act – CRA) üreticilere uzun vadeli güncelleme yükümlülüğü getirmektedir.

Buna paralel olarak İngiltere'de yürürlüğe giren UK Smart Charging Regulations, doğrudan elektrikli araç şarj cihazlarına odaklanmaktadır. Bu düzenleme ile varsayılan şifre kullanımı yasaklanmış, her cihaz için benzersiz güvenlik kimliği şart koşulmuş ve üreticilere yazılım desteğini uzun vadeli sürdürme sorumluluğu yüklenmiştir.

Bu yaklaşım, teknik uyumun ötesinde, kullanıcı güvenini artırmayı ve pazarda sürdürülebilir bir güvenlik kültürü oluşturmayı hedeflemektedir.

Jeopolitik Bağlam: Siber Savaşlar ve Enerji Güvenliği

Enerji altyapısı, artık yalnızca teknik bir mesele değil, aynı zamanda jeopolitik bir güvenlik alanıdır.

• Ukrayna – Rusya savaşında enerji altyapısına yönelik saldırılar, milyonlarca kişiyi etkilemiştir.

• İran – İsrail arasındaki siber çatışmalar, enerji şebekelerinin IoT tabanlı saldırılara açık olduğunu göstermektedir.

• Mira Botnet gibi örnekler, sıradan cihazların bile küresel ölçekte hizmet dışı bırakma saldırılarında kullanılabileceğini kanıtlamıştır.

Bu tablo, elektrikli araç şarj istasyonlarının da benzer şekilde stratejik riskler taşıdığını ortaya koymaktadır.

Kullanıcı Farkındalığı ve Güvenlik Kültürü

Teknik çözümler tek başına yeterli değildir. Siber güvenliğin en zayıf halkası çoğu zaman kullanıcı davranışıdır. Bu nedenle güvenlik kültürü geliştirmek kritik önem taşımaktadır.

Kullanıcılara Öneriler

• Güçlü ve özgün parolalar kullanın. Tekrar eden ya da kolay tahmin edilebilir parolalardan kaçının.

• RFID kartınızı fiziksel olarak koruyun; kaybolması veya çalınması halinde vakit kaybetmeden operatörünüze bildirin.

• Sadece güvenli ve izole ağlarda bağlantı kurun. Ortak Wi-Fi ağlarından uzak durun; mümkünse güvenli Wi-Fi ya da mobil operatörlerin sunduğu özel/izole APN SIM çözümlerini tercih edin.

• Cihaz ve yazılımlarınızı güncel tutun; düzenli güncellemeler bilinen güvenlik açıklarına karşı en güçlü korumadır.

Dijital Güvenlikle Güçlenen Enerji Dönüşümü

E-mobilite, enerji dönüşümünün merkezinde yer alırken, siber güvenlik bu dönüşümün görünmeyen cephesidir. Avrupa'da geliştirilen standartlar, üreticiler ve operatörler için önemli bir yol haritası sunarken, kullanıcı farkındalığı da bu zincirin tamamlayıcı halkasıdır.

Siber tehditlere karşı dirençli bir şarj altyapısı oluşturmak, yalnızca teknik bir gereklilik değil; aynı zamanda sürdürülebilir ulaşım ve enerji güvenliği için stratejik bir zorunluluktur. Türkiye'nin de bu alandaki uluslararası deneyimlerden faydalanarak kendi güvenlik modelini geliştirmesi, geleceğin enerji ekosisteminde kritik bir adım olacaktır.

Hazırlayan: Kaan KAHRAMAN

Tasarım Doğrulama ve Test Mühendisi

KAYNAKÇA:

European Commission, Cyber Resilience Act (CRA), 2023.

ETSI EN 303 645, Cyber Security for Consumer IoT, European Telecommunications Standards Institute, 2020.

ISO 15118, Road Vehicles – Vehicle to Grid Communication Interface, International Organization for Standardization, 2018.

ENISA, Threat Landscape for Smart Infrastructure, European Union Agency for Cybersecurity, 2022.

ENCS & ElaadNL, EV Charging Security Requirements, European Network for Cyber Security, 2021.

Symantec, The Mirai Botnet Explained: IoT under Siege, 2017.

BBC News, Ukraine power grid cyberattack: Security concerns, 2016.

The Times of Israel, Iran-Israel cyber clashes highlight vulnerabilities in critical infrastructure, 2021.

IEA, Global EV Outlook 2024, International Energy Agency, 2024.

OWASP, IoT Top 10 Security Issues, OWASP Foundation, 2022.