KONU: Güvenlik Senaryosu SWOT Analizi: BMS Manipülasyonu Riski

Tarih: 11 Kasım 2025
Aşağıdaki SWOT analizi, "Maksimum Güçte Anormal Şarj (BMS Manipülasyonu)" güvenlik senaryosu özelinde, şarj ağı operatörünün veya istasyon üreticisinin mevcut durumunu ve pozisyonunu analiz etmektedir.

GÜÇLÜ YÖNLER (Strengths)

(Kuruluşun bu tehdide karşı sahip olduğu mevcut avantajlar)

- **Detaylı Risk Analizi:** Tehdidin, ilgili sistemlerin (DC Hızlı Şarj, BMS, CSMS), vektörlerin (BMS Spoofing), zafiyetlerin ve potansiyel etkilerin derinlemesine analiz edilmiş ve belgelenmiş olması.
- **Varlık Tanımlaması:** Korunması gereken birincil fiziksel varlıkların (güç modülleri, kablolar, konnektörler) ve soyut varlıkların (marka itibarı) net bir şekilde tanımlanmış olması.
- **Teknik Bilgi Birikimi:** Normal operasyonel beklentilerin (örn: "tapering" veya güç azaltma eğrisi) ve protokol detaylarının (ISO 15118) kuruluş içinde biliniyor olması.

ZAYIF YÖNLER (Weaknesses)

(Bu tehdidi artıran mevcut içsel eksiklikler ve zafiyetler)

- **Körü Körüne Güven (Z-1):** Şarj istasyonunun (EVSE), aracın BMS'inden gelen güç talebi komutlarına, bu taleplerin süresi mantıksız olsa bile "körü körüne güvenmesi".
- **Yetersiz Sunucu Denetimi (Z-2):** Merkezi Yönetim Sistemi (CSMS) tarafında, bir şarj işleminin süresi ve ortalama gücü hakkında mantıksal kontrollerin (sanity checks) bulunmaması veya zayıf olması.
- **Protokol Zayıflığı (Z-3):** Özellikle eski DC protokollerinin, aracın kimliğini (ve BMS'inin meşruluğunu) güçlü bir şekilde doğrulamadan (örn: kriptografik imza olmadan) iletişime izin vermesi.
- **Tasarım Sınırlaması:** İstasyon bileşenlerinin (güç modülleri, kablolar), "tapering" olmadan %100 yükte sürekli çalışmaya uygun tasarlanmamış olması.

FIRSATLAR (Opportunities)

(Tehdidi azaltmak veya ortadan kaldırmak için kullanılabilecek dışsal faktörler ve iyileştirme alanları)

- **CSMS/EVSE İş Mantığını Güçlendirme:** Zaman (örn: > 60 Dakika) ve ortalama güce (örn: > MaksGücün %90'ı) dayalı katı kurallar ve alarmlar tanımlayarak anomaliyi durdurma fırsatı.
- **Donanımsal Korumaları İyileştirme:** BMS iletişiminden bağımsız çalışan fiziksel sıcaklık sensörlerinin (kablolar, konnektörler) gücü otomatik olarak kesmesi (derating) için eşik

değerlerin optimize edilmesi.
- **Modern Protokollere Geçiş:** "Plug & Charge" (PnC) ve ISO 15118-20 gibi, aracın kimliğini kriptografik sertifikalarla doğrulayan gelişmiş protokolleri benimseyerek sahte cihazları engelleme imkanı.
- **Akıllı Analiz (Makine Öğrenimi):** Şarj eğrilerini (örn: 2 saat %100 güç) makine öğrenimi ile analiz ederek normal olmayan seansları otomatik tespit eden ve alarm üreten sistemler geliştirme.

TEHDİTLER (Threats)

(Kuruluşun kontrolü dışındaki olumsuz faktörler ve riskin sonuçları)

- **Tehdit Aktörleri:** Birincil amacı şarj ağı altyapısına fiziksel zarar vermek (yangın çıkarmak, ekipmanı eritmek) olan Vandallar ve Sabotajcılar ile sistemin sınırlarını tehlikeli bir şekilde test eden kötü niyetli güvenlik araştırmacıları.
- **Saldırı Vektörleri:** "Man-in-the-Middle" (MitM) görevi gören özel donanımlar (BMS Spoofing Cihazı) veya yazılımı değiştirilmiş (root'lanmış) araçlar kullanılarak saldırının gerçekleştirilmesi.
- **Kritik Güvenlik Riski:** Ekipmanın erimesi ve alev alması sonucu ortaya çıkan yangın tehlikesi, can güvenliğini ve çevredeki diğer mülkleri tehlikeye atar.
- **Finansal ve İtibari Yıkım:** On binlerce dolarlık ekipman değişim maliyeti ve "şarj istasyonu alev aldı" haberlerinin neden olacağı, müşteri güvenini yok edecek geri dönülemez marka itibarı hasarı.