Kapsamlı Saldırı Senaryosu: "Operasyonel Felç" (Yaygın Hizmet Reddi - DoS)

Bu belge, "Anormal Protokol Etkileşimleri" dokümanındaki prensiplere (özellikle Bölüm 2.1) dayanan "Yaygın Hizmet Reddi" senaryosunu detaylandırmak için hazırlanmıştır.

1. Senaryo Özeti

"Operasyonel Felç", bir saldırganın bir Şarj Noktası Operatörü'ne (CPO) ait çok sayıda şarj istasyonunu (EVSE) eş zamanlı olarak hedef alarak, meşru kullanıcıların hizmet almasını engellediği, kasti bir Hizmet Reddi (Denial of Service - DoS) saldırısıdır. Saldırı, OCPP protokolünün operasyonel komutlarını (örn. `RemoteStopTransaction`) kötüye kullanarak, aktif şarjları toplu halde durdurmayı veya CSMS'i sahte mesajlarla boğarak tüm ağı kilitletmeyi amaçlar. Sonuç, anlık bir operasyonel kaos, gelir kaybı ve ciddi bir itibar zedelenmesidir.

2. Senaryonun Amacı

- **Birincil Amaç:** Bir CPO'nun tüm şarj ağını veya belirli bir bölgedeki istasyonlarını toplu olarak devre dışı bırakmak, sistemi meşru kullanıcılar için erişilemez hale getirmek ve operasyonel kaosa yol açmak.
- **İkincil Amaç:** Aktif şarj işlemlerini zorla ve aniden sonlandırarak kullanıcı memnuniyetini sabote etmek, CPO'ya doğrudan anlık gelir kaybı yaşatmak ve marka itibarına kalıcı hasar vermek.

3. Hedef Varlıklar ve Temel Zafiyetler

- **Hedef Varlık:** EVSE ağı, Merkezi Yönetim Sistemi (CSMS) ve aradaki OCPP iletişim kanalı.
- **Zafiyet 1 (Ağ Katmanı):** Zayıf Kimlik Doğrulama (OCPP Güvenlik Profili 1 veya 2). Karşılıklı sertifika (mTLS) kullanılmaması, saldırganın kendini meşru bir CSMS olarak tanıtmasına (Spoofing) olanak tanır. (PDF Ref: Bölüm 2.1)
- **Zafiyet 2 (Ağ Katmanı):** Güvensiz veya şifrelenmemiş ağ iletişimi. Saldırganın bir "Ortadaki Adam" (MitM) saldırısıyla araya girip komutları yakalamasına veya enjekte etmesine izin verir.
- **Zafiyet 3 (Uygulama Katmanı):** CSMS tarafında Hız Sınırlaması (Rate Limiting) veya davranışsal analiz eksikliği. Bu durum, bir saldırganın kısa sürede binlerce anormal komut göndermesine karşı sistemi savunmasız bırakır.

4. Saldırı Yöntemleri ve Adım Adım Yürütme

Saldırı, iki ana vektör üzerinden gerçekleştirilebilir:

Vektör A: Toplu Oturum Sonlandırma (Aktif Kullanıcılara Yönelik)

1. **Hazırlık ve Erişim:** Saldırgan, bir grup istasyonun ağ trafiğini (MitM - Zafiyet 2) izleyebileceği bir konuma gelir veya zayıf kimlik doğrulamayı (Zafiyet 1) kullanarak sahte bir CSMS gibi davranır.

2. **Keşif:** Saldırgan, ağdaki `StatusNotification` (Durum Bildirimi) mesajlarını izleyerek veya tahmin yürüterek 'Charging' (Şarj Oluyor) durumundaki istasyonları tespit eder.
3. **Toplu Saldırı:** Saldırgan, hedef aldığı tüm aktif istasyonlara *eş zamanlı olarak* veya çok hızlı bir döngü içinde `RemoteStopTransaction` (Uzaktan İşlemi Durdur) komutları gönderir.
4. **Fiziksel Sonuç:** Ülkenin/bölgenin farklı yerlerindeki yüzlerce (veya binlerce) elektrikli aracın şarjı aniden kesilir. İstasyonlardaki röleler açılır ve oturumlar sonlanır. Kullanıcılar, araçlarının başında ne olduğunu anlayamaz ve CPO'nun müşteri hizmetleri kilitlenir.

Vektör B: CSMS Sel Baskını (Sistemi Kilitleme)

1. **Hazırlık:** Saldırgan, ele geçirdiği birkaç EVSE'yi (veya bir botnet ağını) veya yine sahte bir CSMS kimliğini (Zafiyet 1) kullanır.
2. **Sistemik Saldırı:** Saldırgan, hedef CPO'nun CSMS sunucusuna yönelik binlerce sahte mesaj gönderir.
3. **Sahte Önyükleme (BootNotification Flood):** Saldırgan, CSMS'e saniyede binlerce sahte `BootNotification` (Önyükleme Bildirimi) mesajı yağdırır. (PDF Ref: Bölüm 2.1). CSMS, bu sahte "merhaba, ben yeni açıldım" mesajlarını işlemekten kaynakları (CPU, RAM, veritabanı bağlantıları) tükenir ve kilitlenir.
4. **Siber Sonuç:** CSMS kilitlendiği için, meşru istasyonlardan gelen `MeterValues` (Sayaç Değerleri) gibi kritik verileri işleyemez, yeni şarj taleplerini (`Authorize`) onaylayamaz. Tüm ağ fiilen durmuş olur.

5. İlgili Tehditler (STRIDE Modeli)

- **D - Denial of Service (Hizmet Reddi):** Saldırının ana kategorisi ve amacıdır. Sistemin meşru işlevini yerine getirmesi engellenir.
- **S - Spoofing (Kimlik Sahtekarlığı):** Saldırganın, Vektör A veya B'yi gerçekleştirebilmek için meşru bir CSMS sunucusunu veya meşru bir EVSE'yi taklit etmesi gerekebilir.

6. Anomali Göstergeleri ve Tespit Yöntemleri

- **Ana Gösterge:** CSMS loglarında, normal operasyonel kalıpların dışında, anormal derecede yüksek sayıda ve sıklıkta `RemoteStopTransaction` komutunun gözlemlenmesi.
- **Korelasyon Eksikliği:** Çok sayıda şarj oturumunun, kullanıcı talebi (`StopTransaction`), tam şarj (`EVFull`) veya şebeke kesintisi gibi meşru bir neden olmaksızın, *aynı anda* sonlanması.
- **Ağ Davranışı:** Tek bir IP adresinden veya IP bloğundan, normal bir istasyonun gönderebileceğinden çok daha fazla `BootNotification` veya `Heartbeat` (Kalp Atışı) mesajı gelmesi.
- **Operasyonel Geri Bildirim:** Müşteri hizmetlerine, farklı lokasyonlardan "şarjım aniden durdu" veya "istasyon çalışmıyor" şikayetlerinin aniden yığılması.

7. Önlemler ve Azaltma Stratejileri

1. **Ağ Güvenliğini Sağlama (Zafiyet 1 ve 2'ye karşı):**

    - **Zorunlu OCPP Güvenlik Profili 3 Kullanımı:** Karşılıklı TLS (mTLS) sertifika doğrulamasını zorunlu kılmak. Bu, sahte CSMS (Spoofing) saldırılarını ve MitM komut enjeksiyonunu büyük ölçüde engeller. (PDF Ref: Bölüm 4.1)
2. **Uygulama Güvenliğini Artırma (Zafiyet 3'e karşı):**
    - **Akıllı Hız Sınırlaması (Rate Limiting):** CSMS tarafında, kritik komutlar (`RemoteStopTransaction`, `BootNotification` vb.) için istasyon başına veya IP başına akıllı hız sınırları uygulamak. (Örn: Bir istasyon 1 dakika içinde 3'ten fazla `BootNotification` gönderemez).
    - **Davranışsal Analiz:** Bir anomali tespit sisteminin (IDS) "Normal operasyonda bir CPO, 1 saniye içinde 500 farklı istasyona 'durdur' komutu göndermez" kuralını bilmesi ve bu tür anormal toplu komutları bloke etmesi veya bir operatör onayına sunması.
3. **Dayanıklılık ve Hızlı Müdahale:**
    - **CSMS Yedekliliği:** DoS saldırılarına karşı yük dengeleyiciler (load balancers) ve coğrafi olarak yedekli CSMS sunucuları kullanmak.
    - **Acil Durum Prosedürü:** Toplu bir DoS saldırısı tespit edildiğinde, etkilenen istasyonların güvenli iletişim kanallarını (örn. VPN tünelleri) otomatik olarak sıfırlayıp yeniden kuracak veya şüpheli komutları geçici olarak yoksayacak bir "kilitlenme" (lockdown) modu tanımlamak.

SWOT Analizi :

1. Yönetici Özeti ve SWOT Matrisi

Bu rapor, elektrikli araç (EV) şarj altyapılarını hedef alan ve "Operasyonel Felç" olarak adlandırılan sofistike siber saldırı senaryosunu analiz eden teknik dokümanın [1] derinlemesine bir SWOT (Güçlü Yönler, Zayıf Yönler, Fırsatlar, Tehditler) analizini sunmaktadır. Analiz edilen doküman, bir Şarj Noktası Operatörü'nün (CPO) ağını, OCPP (Open Charge Point Protocol) protokolünün operasyonel komutlarını kötüye kullanarak toplu bir Hizmet Reddi (Denial of Service - DoS) saldırısı yoluyla nasıl devre dışı bırakılabileceğini ayrıntılı bir şekilde ortaya koymaktadır. Saldırının temel amacı, operasyonel kaosa yol açmak, doğrudan gelir kaybına neden olmak ve marka itibarını ciddi şekilde zedelemektir.[1]

Bu değerlendirme, söz konusu tehdit modelinin stratejik değerini ortaya koymaktadır. Dokümanın güçlü yönleri arasında; saldırgan niyetini ve iş etkisini net bir şekilde tanımlaması, zafiyetler ile saldırı vektörleri arasında doğrudan nedensel bağlar kurması ve katmanlı bir "derinlemesine savunma" (defense-in-depth) yaklaşımı önermesi bulunmaktadır. Ancak analiz, dokümanın harici saldırganlara örtük bir şekilde odaklanarak iç tehditleri göz ardı etmesi, önerilen azaltma stratejilerinin operasyonel karmaşıklığını ve maliyetini yeterince vurgulamaması ve nicel bir risk modellemesi sunmaması gibi önemli zayıflıkları da tespit etmiştir.

Bu zayıflıklara rağmen, doküman bir kuruluşun siber güvenlik duruşunu güçlendirmek için önemli fırsatlar sunmaktadır. Proaktif tehdit avcılığı ve gerçekçi kırmızı takım (red team) tatbikatları için bir plan görevi görebilir, yüksek doğruluklu SIEM/SOAR otomasyon oyun kitaplarının (playbook) geliştirilmesine temel oluşturabilir ve sektör genelinde daha güvenli

standartların benimsenmesi için bir savunuculuk aracı olarak kullanılabilir. Son olarak, bu analiz, önerilen savunma mekanizmalarının dahi yapay zeka destekli adaptif saldırılar, protokol seviyesindeki sıfırıncı gün (zero-day) zafiyetleri ve insan faktöründen kaynaklanan riskler gibi gelişen tehditler karşısında yetersiz kalabileceğini vurgulamaktadır.

1.1. "Operasyonel Felç" Tehdidine Giriş

"Operasyonel Felç" senaryosu, bir CPO'ya ait çok sayıda şarj istasyonunu (EVSE) eş zamanlı olarak hedef alarak meşru kullanıcıların hizmet almasını engelleyen, kasıtlı ve koordineli bir DoS saldırısı olarak tanımlanmaktadır. Saldırı, OCPP protokolünün `RemoteStopTransaction` gibi operasyonel komutlarının kötüye kullanılmasıyla aktif şarj oturumlarını toplu halde durdurmayı veya Merkezi Yönetim Sistemi'ni (CSMS) sahte `BootNotification` mesajlarıyla kilitlemeyi amaçlar. Sonuç, anlık bir operasyonel kaos, gelir kaybı ve ciddi bir itibar zedelenmesidir.[1]

1.2. Stratejik Sentez

Sonuç olarak, "Operasyonel Felç" dokümanı, taktiksel bir siber güvenlik aracı olarak son derece değerlidir. Ancak, gerçek değeri, bir kuruluşun güvenlik stratejisini reaktif savunmadan proaktif bir duruşa dönüştürmesi için bir katalizör olarak kullanıldığında ortaya çıkmaktadır. Bu analiz, dokümanın bulgularının sadece teknik zafiyetleri gidermek için değil, aynı zamanda proaktif tehdit avcılığı programları oluşturmak, otomatik savunma yetenekleri geliştirmek ve sektör genelinde güvenlik standartlarını yükseltmek gibi daha geniş stratejik girişimleri yönlendirmek için kullanılması gerektiğini ortaya koymaktadır.

Tablo 1: SWOT Analizi Özet Matrisi

Güçlü Yönler (Strengths)	**Zayıf Yönler (Weaknesses)**
• Zafiyetler ve saldırılar arasında net nedensel bağ kurma	• Harici saldırganlara örtük odaklanma (iç tehdit kör noktası)
• Teknik tehditleri doğrudan iş etkisine (gelir, itibar) bağlama	• Azaltma stratejilerinin karmaşıklığını ve maliyetini hafife alma
• Katmanlı ve uygulanabilir "derinlemesine savunma" önerileri	• Nicel risk ve etki modellemesinin eksikliği
Fırsatlar (Opportunities)	**Tehditler (Threats)**
• Gerçekçi kırmızı takım (red team) tatbikatları için bir plan	• Statik kuralları aşan yapay zeka destekli ve adaptif saldırılar

Güçlü Yönler (Strengths)	Zayıf Yönler (Weaknesses)
• SIEM/SOAR otomasyon oyun kitapları (playbook) için temel	• Protokol seviyesinde sıfırıncı gün (zero-day) zafiyetleri riski
• Tasarımdan güvenlik (secure-by-design) ve sektör standartlarını yönlendirme aracı	• İnsan faktörü: Sosyal mühendislik ve operasyonel hatalar

---

2. Tehdit Modeli Dokümanının Güçlü Yönleri

Analiz edilen "Operasyonel Felç" dokümanı, EV şarj altyapılarına yönelik siber tehditlerin anlaşılması ve bunlara karşı savunma stratejileri geliştirilmesi açısından birçok temel güce sahiptir. Bu güçlü yönler, dokümanı sadece teorik bir çalışma olmaktan çıkarıp, siber güvenlik profesyonelleri için eyleme geçirilebilir bir kaynak haline getirmektedir.

2.1. Senaryo Tanımı ve Saldırgan Niyetindeki Keskinlik

Dokümanın en belirgin güçlü yönlerinden biri, saldırı senaryosunu ve saldırganın niyetini son derece net bir şekilde tanımlamasıdır. Tehdit, sadece teknik bir eylem olarak değil, aynı zamanda stratejik bir iş hedefi olarak çerçevelenmiştir. Doküman, saldırının *Birincil Amacı* ("Bir CPO'nun tüm şarj ağını... devre dışı bırakmak") ile *İkincil Amacı* ("kullanıcı memnuniyetini sabote etmek, CPO'ya doğrudan anlık gelir kaybı yaşatmak ve marka itibarına kalıcı hasar vermek") arasında bilinçli bir ayrım yapmaktadır.[1]

Bu ayrım, dokümanı basit bir teknik DoS açıklamasından, kapsamlı bir iş riski değerlendirmesine yükseltmektedir. "Gelir kaybı" ve "itibar hasarı" gibi kavramları açıkça isimlendirerek, güvenlik ekiplerinin tehdidin ciddiyetini teknik olmayan iş liderlerine ve yöneticilere etkili bir şekilde iletebilmesi için gerekli dili sağlar. Bu, siber güvenlik yatırımları için bütçe onayı ve stratejik destek alınmasını kolaylaştıran kritik bir özelliktir. Bu yaklaşım, bir siber olayın etkisini ölçmek için dolaylı bir çerçeve de oluşturur. "İkincil Amaçlar" olarak belirtilen unsurlar, müşteri kayıp oranı (churn rate), destek merkezi çağrı hacmi ve günlük gelir rakamları gibi temel performans göstergelerine (KPI) doğrudan eşleştirilebilir. Bu sayede, olası bir saldırı sonrası yapılacak etki analizi daha somut ve ölçülebilir hale gelir. Bu bağlantı, genellikle tamamen teknik odaklı tehdit modellerinde eksik kalan bir köprü görevi görür.

2.2. Zafiyetler ve Saldırı Vektörleri Arasındaki Nedensel Bağlantı

Dokümanın temel gücü, belirli zafiyetler ile bu zafiyetlerin nasıl istismar edildiği arasında kurduğu kusursuz nedensel bağlantıdır. Doküman, zafiyetleri ve saldırıları iki ayrı liste olarak sunmak yerine, mantıksal bir anlatı inşa eder: "*Bu zayıflık* nedeniyle, bir saldırgan *bu spesifik eylemi* gerçekleştirebilir ve bu da *bu sonuca* yol açar."

Örneğin, `Zafiyet 1` (Zayıf Kimlik Doğrulama) doğrudan bir saldırganın "kendini meşru bir CSMS olarak tanıtmasına (Spoofing)" olanak tanıyan temel neden olarak belirtilmiştir. Bu

sahtekarlık eylemi, hem `Vektör A` (Toplu Oturum Sonlandırma) hem de `Vektör B` (CSMS Sel Baskını) için bir ön koşuldur.[1] Benzer şekilde, `Zafiyet 3` (CSMS tarafında Hız Sınırlaması eksikliği), `Vektör B`'deki bir `BootNotification Flood` saldırısının neden başarılı olacağını açıkça ortaya koymaktadır.[1] Bu nedensel zincir, iyileştirme çabalarının önceliklendirilmesi için paha biçilmez bir rehberdir. `Zafiyet 1`'i karşılıklı TLS (mTLS) uygulayarak düzeltmenin sadece bir uyumluluk gereksinimi olmadığını, CSMS sahtekarlığı için saldırı zincirini doğrudan kıran kritik bir karşı önlem olduğunu net bir şekilde gösterir.

2.3. Uygulanabilir ve Katmanlı Azaltma Stratejileri

Dokümanda önerilen karşı önlemler, olgun bir "derinlemesine savunma" (defense-in-depth) yaklaşımını yansıtan üç farklı katmanda organize edilmiştir: Ağ Güvenliği (`OCPP Güvenlik Profili 3 Kullanımı`), Uygulama Güvenliği (`Akıllı Hız Sınırlaması`, `Davranışsal Analiz`) ve Dayanıklılık (`CSMS Yedekliliği`, `Acil Durum Prosedürü`).[1]

Bu yapı, tek bir "sihirli değnek" çözüm önerme tuzağından kaçınır ve sağlam güvenliğin katmanlı olması gerektiğini anladığını gösterir. Örneğin, ağ katmanındaki mTLS savunması (`Zafiyet 1`'e karşı) bir şekilde aşılsa bile, uygulama katmanındaki hız sınırlaması (`Zafiyet 3`'e karşı) bir CSMS sel baskını saldırısının etkisini köreltmek için ikinci bir savunma hattı olarak hizmet edecektir. Bu katmanlı strateji, yüksek kaliteli güvenlik mimarisinin bir alametifarikasıdır. Azaltma planının bu üç parçalı yapısı, aynı zamanda çok yıllı bir güvenlik programı için bir yol haritası sunar. Bir kuruluş bu girişimleri sıralı veya paralel olarak ele alabilir; "Ağ Güvenliği"ni temel bir proje, "Uygulama Güvenliği"ni yazılım geliştirme yaşam döngüsü (SDLC) için bir iyileştirme ve "Dayanıklılık"ı operasyonel mükemmellik hedefi olarak belirleyebilir. Bu kategoriler, bir teknoloji organizasyonundaki farklı ekiplere (Ağ Mühendisliği, Yazılım Geliştirme, Saha Güvenilirliği Mühendisliği) doğal olarak karşılık gelir. Bu da, her bir azaltma akışı için sorumlulukların atanmasını ve proje planlarının oluşturulmasını kolaylaştırır.

---

3. Zayıf Yönler ve Analitik Boşluklar

"Operasyonel Felç" dokümanı, tehdidi tanımlama ve temel savunma stratejileri sunma konusunda güçlü olsa da, analitik derinlikte bazı boşluklar ve örtük varsayımlar içermektedir. Bu zayıflıkların eleştirilmesi, daha kapsamlı ve dayanıklı bir güvenlik duruşu geliştirmek için kritik öneme sahiptir.

3.1. Harici Saldırgan Profiline Dair Örtük Varsayım (İç Tehdit Kör Noktası)

Dokümanda açıklanan saldırı vektörleri, özellikle Ortadaki Adam (`MitM`) ve CSMS Sahtekarlığı (Spoofing) gibi yöntemler, saldırganın güvenilir ağ sınırlarının dışından faaliyet gösterdiği varsayımına dayanmaktadır.[1] Doküman, tehdidin içeriden kaynaklandığı bir senaryoyu hiç ele almamaktadır. Bu, önemli bir analitik boşluktur.

Örneğin, CSMS yönetici kimlik bilgilerine sahip hoşnutsuz bir çalışan (kötü niyetli iç tehdit) veya tedarik zincirinde güvenliği ihlal edilmiş bir bileşen (örneğin, arka kapı içeren bir EVSE yazılımı), `RemoteStopTransaction` veya `BootNotification` sel baskını saldırılarını çok daha kolay ve gizli bir şekilde gerçekleştirebilir. Böyle bir saldırgan, mTLS gibi önerilen tüm ağ seviyesi savunma mekanizmalarını tamamen atlayabilir. Dokümanın savunma stratejisi,

büyük ölçüde bağlantının kimliğini doğrulamaya odaklanmıştır; ancak zaten doğrulanmış bir oturum *içindeki* komutun niyetini veya kaynağını sorgulamamaktadır. Bu durum, mTLS uygulandıktan sonra yanlış bir güvenlik hissine yol açabilir. Bir kuruluş, problemi "çözdüğünü" düşünebilirken, meşru ve doğrulanmış bir kaynaktan aynı OCPP komutlarını kötüye kullanabilen bir iç tehdide karşı tamamen savunmasız kalabilir. Asıl risk, saldırganın konumundan bağımsız olarak, protokolün işlevselliğinin kötüye kullanılmasıdır.

3.2. Azaltma Stratejilerinin Karmaşıklığı ve Maliyetinin Hafife Alınması

Doküman, "Zorunlu OCPP Güvenlik Profili 3 Kullanımı"nı basit ve doğrudan bir çözüm olarak sunmaktadır.1 Ancak bu öneri, arkasında yatan muazzam operasyonel ve finansal zorlukları gizlemektedir. Coğrafi olarak dağıtılmış binlerce EVSE'den oluşan bir filoyu yeni bir güvenlik profiline geçirmek son derece karmaşık bir süreçtir ve aşağıdaki adımları içerir:

a) Tüm donanım ve aygıt yazılımlarının (firmware) yeni profili desteklediğinden emin olmak.

b) Sertifika yaşam döngüsü yönetimi için sağlam bir Açık Anahtar Altyapısı (PKI) geliştirmek ve yönetmek.

c) Cihazların kullanılamaz hale gelme (bricking) riski yüksek olan büyük ölçekli bir uzaktan aygıt yazılımı güncelleme kampanyası düzenlemek.

d) Sürekli birlikte çalışabilirliği sağlamak için kapsamlı testler yapmak.

Doküman, "ne" yapılması gerektiğini söylerken, bu sürecin inanılmaz derecede karmaşık ve maliyetli olan "nasıl" yapılacağına değinmemektedir. Bu eksiklik, dokümanın pratik bir planlama aracı olarak kullanılabilirliğini sınırlar.

3.3. Nicel Risk ve Etki Modellemesinin Yokluğu

Doküman, saldırının sonuçlarını "operasyonel kaos," "gelir kaybı," ve "itibar zedelenmesi" gibi nitel terimlerle tanımlamaktadır.[1] Bu tanımlar doğru olmakla birlikte, iş önceliklendirmesi açısından eyleme geçirilebilir değildir. Doküman, nicel bir çerçeveden yoksundur. Örneğin:

- Ulusal çapta bir ağ kesintisinin saatlik tahmini finansal kaybı nedir?
- Mevcut altyapıya karşı bu saldırının başarılı olma olasılığı (örneğin, 1-5 arası bir ölçekte) nedir?

Bu nicel bağlam olmadan, bir üst düzey yöneticinin OCPP Güvenlik Profili 3'ü uygulamanın (çok gerçek) maliyetini, "operasyonel kaos" gibi (soyut) bir riske karşı tartması zordur. Bu boşluk, güvenlik yatırımlarını gerekçelendirmeyi ve önceliklendirmeyi zorlaştırır.

---

4. Kurumsal Gelişim İçin Stratejik Fırsatlar

"Operasyonel Felç" dokümanı, sadece reaktif savunma mekanizmaları kurmak için değil, aynı zamanda bir kuruluşun genel güvenlik duruşunu proaktif olarak geliştirmek için de bir dizi

stratejik fırsat sunmaktadır. Bu doküman, pasif bir uyarı belgesinin ötesine geçerek, kurumsal siber dayanıklılığı artırmak için bir kaldıraç olarak kullanılabilir.

4.1. Proaktif Tehdit Avcılığı ve Red Team Tatbikatları İçin Bir Temel

Doküman, hem `Vektör A` (Toplu Oturum Sonlandırma) hem de `Vektör B` (CSMS Sel Baskını) için son derece ayrıntılı, adım adım saldırı zincirleri sunmaktadır.[1] Bu detaylı vektörler sadece birer uyarı değil, aynı zamanda birer senaryodur. Bir kuruluş, bu senaryoları gerçekçi kırmızı takım (red team) tatbikatları oluşturmak için bir plan olarak kullanabilir ve kullanmalıdır.

Bir güvenlik ekibi, saldırgan rolünü üstlenerek bu adımları bir test ortamında (staging environment) veya hatta üretim ağının dikkatlice izole edilmiş bir bölümünde uygulamaya çalışabilir. Bu, kuruluşu pasif, savunmacı bir duruştan aktif, saldırgan bir duruşa geçirir. Bu sayede, gerçek bir saldırı gerçekleşmeden önce tespit ve müdahale yeteneklerini test etme imkanı bulurlar. Bu tatbikatların sonuçları, güvenlik yatırımları için güçlü bir geri bildirim döngüsü yaratabilir. Örneğin, kırmızı takım "Vektör B"yi başarıyla uygular ve test ortamındaki CSMS'i çökertirse, güvenlik ekibi artık zafiyetin varlığına dair inkar edilemez bir kanıta ve dokümanda belirtilen "CSMS Yedekliliği" ve "Akıllı Hız Sınırlaması" projelerini finanse etmek için ikna edici bir iş gerekçesine sahip olur. Hipotetik bir saldırıyı gerçeğe dönüştüren bir simülasyon, "30 saniyede 10.000 sahte `BootNotification` mesajından sonra CSMS çöktü" gibi somut veriler üretir. Bu somut veriler, bütçe onayı için soyut bir tehdit modelinden çok daha ikna edicidir. Dolayısıyla doküman, güvenlik girişimleri için siyasi ve finansal sermaye yaratma aracına dönüşür.

4.2. Yüksek Doğruluklu Otomatik Güvenlik Oyun Kitaplarının (Playbook) Geliştirilmesi

Dokümanın "Anomali Göstergeleri" bölümü, "anormal derecede yüksek sayıda ve sıklıkta `RemoteStopTransaction` komutunun gözlemlenmesi" ve "Tek bir IP adresinden... çok daha fazla `BootNotification`... mesajı gelmesi" gibi spesifik ve ölçülebilir göstergeler listelemektedir.[1]

Bu göstergeler, bir Güvenlik Bilgi ve Olay Yönetimi (SIEM) sistemine entegre edilmek için mükemmel adaylardır. Doğrudan yüksek doğruluklu tespit kurallarına dönüştürülebilirler. Dahası, bir SOAR (Güvenlik Orkestrasyonu, Otomasyonu ve Müdahalesi) platformu aracılığıyla otomatik müdahale eylemlerini tetikleyebilirler. Örneğin, şöyle bir kural oluşturulabilir: "Eğer tek bir CPO yönetim kaynağından 60 saniyeden kısa bir sürede 100'den fazla farklı şarj noktasına `RemoteStopTransaction` komutu gönderilirse, bu komut setini otomatik olarak manuel insan incelemesi için bir kuyruğa al ve güvenlik operasyon merkezine (SOC) kritik bir uyarı gönder." Bu yaklaşım, reaktif bir tespit sürecini proaktif, otomatik bir savunmaya dönüştürür.

4.3. Tasarımdan Güvenlik (Secure-by-Design) Prensiplerini ve Sektör Standartlarını Şekillendirme

Dokümanın tamamı, özellikle eski OCPP güvenlik profillerinin zayıflıklarına odaklanmasıyla [1], güvenliğin sonradan eklenen bir özellik olamayacağının bir kanıtı niteliğindedir. Bu bulgular, kuruluşun iç Güvenli Yazılım Geliştirme Yaşam Döngüsü'ne (SDLC) entegre

edilmelidir. Tüm yeni CSMS özellikleri ve EVSE aygıt yazılımları, en başından itibaren bu "Operasyonel Felç" senaryolarına karşı tasarlanmalı ve test edilmelidir.

Dahili kullanımın ötesinde, bir CPO bu analizi sektör genelinde daha güçlü temel güvenlik gereksinimlerini savunmak için kullanabilir. Yeni şarj donanımları için Teklif Talebi (RFP) belgelerine daha katı güvenlik maddeleri eklemeyi gerekçelendirmek ve Açık Şarj İttifakı (Open Charge Alliance) gibi organlara katılarak güvensiz eski profillerin kullanımdan kaldırılması için baskı yapmak amacıyla bu dokümandan faydalanabilirler.

---

5. Önerilen Savunma Duruşuna Yönelik Dış Tehditler

"Operasyonel Felç" dokümanında önerilen savunma stratejileri mevcut bilinen tehditlere karşı sağlam bir temel oluştursa da, gelişen siber tehdit ortamı bu savunmaları aşabilecek veya etkisiz kılabilecek yeni riskler barındırmaktadır. Bu dış tehditlerin anlaşılması, statik bir savunma duruşu yerine sürekli adapte olan bir güvenlik stratejisi geliştirmek için zorunludur.

5.1. Gelişen Tehdit Ortamı: Yapay Zeka Destekli ve Adaptif Saldırılar

Doküman, "Akıllı Hız Sınırlaması" (Rate Limiting) için statik bir örnek önermektedir: "Bir istasyon 1 dakika içinde 3'ten fazla `BootNotification` gönderemez".[1] Bu tür bir savunma, modern ve dağıtık bir saldırı karşısında savunmasızdır. Sofistike bir saldırgan, saldırıyı tek bir kaynaktan başlatmaz. Bunun yerine, yüzlerce veya binlerce ele geçirilmiş EVSE'den oluşan bir botnet kullanır. Bu botnet'teki her bir cihaz, mesajları statik eşik değerinin *hemen altında* bir hızda göndererek bireysel olarak görünmez kalır. Ancak, bu "düşük ve yavaş" (low-and-slow) saldırının kolektif hacmi, CSMS'i alt etmek için yine de yeterli olacaktır.

Yapay zeka destekli saldırılar bu tehdidi daha da ileri taşıyabilir. Bu tür saldırılar, bir ağın normal davranışını ve savunma mekanizmalarının eşiklerini öğrenebilir ve tespit edilmemek için davranışlarını gerçek zamanlı olarak adapte edebilir. Özetle, önerilen savunmalar "aptal" ve kaba kuvvet saldırılarını durdurmak için tasarlanmışken, modern saldırganlar giderek daha "akıllı," dağıtık ve adaptif hale gelmektedir.

5.2. Sıfırıncı Gün (Zero-Day) Zafiyetleri ve Protokol Seviyesi Kusurlar

Dokümandaki ağ savunmasının temel taşı, mTLS'e dayanan "OCPP Güvenlik Profili 3"tür.[1] Bu savunma, temel kriptografik kütüphanelerin (örneğin, OpenSSL) ve OCPP protokol mantığının kendisinin kritik zafiyetlerden arınmış olduğu varsayımına dayanır. Ancak, EVSE'ler tarafından kullanılan TLS uygulamasında gelecekte keşfedilecek bir "sıfırıncı gün" (zero-day) zafiyeti, bir saldırganın kimlik doğrulamasını tamamen atlamasına olanak tanıyarak mTLS'i etkisiz hale getirebilir.

Benzer şekilde, OCPP durum makinesindeki (state machine) mantıksal bir kusur, belirli bir amaç için geçerli ve doğrulanmış bir oturuma sahip bir saldırganın yetkilerini yükseltmesine veya yetkisiz eylemler gerçekleştirmesine izin verebilir. Buradaki tehdit, "bilinmeyen bilinmeyenler"dir; yani önerilen güvenlik modelinin temelini oluşturan teknolojilerdeki henüz keşfedilmemiş bir kusurdur.

5.3. İnsan Faktörü: Sosyal Mühendislik ve Operasyonel Hatalar

Dokümanın analizi tamamen teknik zafiyetlere ve kontrollere odaklanmıştır; sistemin insan operatörlerinden hiç bahsetmemektedir. Bu, kritik bir eksikliktir. Mükemmel teknik güvenlik önlemleri alınsa bile, sistem insan hatasına karşı savunmasızdır.

Bir saldırgan, sofistike bir oltalama (phishing) e-postası veya telefon görüşmesi kullanarak bir CPO destek operatörünü kandırabilir. Operatör, meşru kimlik bilgilerini kullanarak, gerekli bir sistem güncellemesi yaptığını zannederek toplu bir `RemoteStopTransaction` komutu yayınlayabilir. Bir saha teknisyeni, yeni bir EVSE'yi yanlış yapılandırarak zayıf veya varsayılan kimlik bilgileriyle ağa bağlanmasına neden olabilir. Buradaki tehdit, en sağlam teknik savunmaları bile atlamak için bir yol sağlayan insan unsurunun genellikle en zayıf halka olmasıdır. Bu durum, dokümanın teknik tavsiyelerini teknik olmayan kontrollerle tamamlayan bütünsel bir güvenlik programının gerekliliğini vurgulamaktadır. Bu program, tüm operatörler için zorunlu güvenlik farkındalığı eğitimlerini, herhangi bir toplu komutun yürütülmesi için katı "dört göz" onay süreçlerini ve operasyonel prosedürlerin düzenli denetimlerini içermelidir. Dokümanın teknik çözümleri gereklidir, ancak insan risk vektörünü ele almadan yeterli değildir.

---

6. Sentez ve Stratejik Tavsiyeler

Bu SWOT analizi, "Operasyonel Felç" tehdit modelinin EV şarj altyapısı güvenliği için değerli ancak eksik bir çerçeve sunduğunu ortaya koymaktadır. Doküman, belirli saldırı vektörlerini ve temel savunma mekanizmalarını tanımlamada mükemmeldir, ancak iç tehditler, uygulama karmaşıklığı ve gelişen saldırı teknikleri gibi kritik alanlarda yetersiz kalmaktadır. Bu sentezden yola çıkarak, bir kuruluşun siber dayanıklılığını artırmak için acil taktiksel düzeltmelerden uzun vadeli stratejik geliştirmelere kadar uzanan öncelikli bir eylem planı aşağıda sunulmuştur.

6.1. Acil Eylemler (Taktiksel)

Bu adımlar, dokümandaki en belirgin ve hızlıca uygulanabilecek bulgulara odaklanarak anında risk azaltımı sağlamayı amaçlamaktadır.

- **Anomali Tespiti için Temel Kurallar Geliştirme:** Dokümanda belirtilen "Anomali Göstergeleri"ni [1] temel alarak SIEM sistemi için derhal tespit kuralları oluşturulmalıdır. Özellikle, anormal sayıda `RemoteStopTransaction` ve `BootNotification` olaylarını izleyen kurallar önceliklendirilmelidir.
- **Mevcut Hız Sınırlaması Yapılandırmalarını Gözden Geçirme:** CSMS üzerindeki mevcut hız sınırlaması (rate limiting) politikaları, dokümanda belirtilen sel baskını saldırılarına karşı ne kadar etkili olduklarını değerlendirmek için acilen gözden geçirilmelidir.
- **Acil Durum Müdahale Prosedürlerini Gözden Geçirme:** Toplu bir hizmet kesintisi durumunda mevcut müdahale planlarının yeterliliğini değerlendirin. İletişim planları, teknik izolasyon prosedürleri ve müşteri hizmetleri protokolleri bu senaryo ışığında test edilmelidir.

6.2. Orta Vadeli Girişimler (Stratejik)

Bu girişimler, daha fazla planlama ve yatırım gerektiren ancak kuruluşun güvenlik duruşunda temel bir iyileşme sağlayacak projelere odaklanır.

- **OCPP Güvenlik Profili 3'e Geçiş için İş Gerekçesi ve Proje Planı:** OCPP Güvenlik Profili 3'e geçiş için maliyetleri, zaman çizelgesini, riskleri ve operasyonel karmaşıklıkları açıkça kabul eden resmi bir iş gerekçesi ve aşamalı bir proje planı geliştirilmelidir.
- **Kırmızı Takım (Red Team) Tatbikatı:** Dokümanın saldırı vektörlerini [1] bir senaryo olarak kullanarak mevcut savunma yeteneklerini test etmek üzere bir kırmızı takım tatbikatı düzenlenmelidir. Bu tatbikatın sonuçları, gelecekteki güvenlik yatırımlarını yönlendirmek için somut veriler sağlayacaktır.
- **İç Tehdit Programı Başlatma:** Yalnızca dış tehditlere odaklanmak yerine, meşru kimlik bilgilerinin kötüye kullanımını izlemeye ve tespit etmeye yönelik bir iç tehdit programı oluşturulmalıdır. Bu, özellikle toplu komutların kullanımını denetlemeyi içermelidir.

6.3. Uzun Vadeli Program Geliştirmeleri (Dönüşümsel)

Bu hedefler, güvenliği tek seferlik bir proje olmaktan çıkarıp, kurum kültürünün ve operasyonlarının ayrılmaz bir parçası haline getirmeyi amaçlayan dönüşümsel değişikliklerdir.

- **Tehdit Modelini SDLC'ye Entegre Etme:** "Operasyonel Felç" gibi tehdit modelleri, yeni yazılım ve donanım geliştirme süreçlerinin bir parçası haline getirilmelidir. Güvenlik, tasarım aşamasından itibaren düşünülmelidir.
- **Otomatik Müdahale (SOAR) Yetenekleri Geliştirme:** Tespit edilen anormalliklere insan müdahalesi olmadan yanıt verebilecek otomatik SOAR oyun kitapları (playbook) oluşturulmalıdır. Örneğin, şüpheli bir toplu durdurma komutunu otomatik olarak karantinaya almak gibi.
- **Sektör Standartlarına Liderlik Etme:** Bu analizin bulguları, sektördeki diğer paydaşlarla paylaşılmalı ve daha güvenli protokollerin ve standartların benimsenmesi için aktif bir rol alınmalıdır. Bu, tüm ekosistemin güvenliğini artıracak ve uzun vadede kurumu koruyacaktır.