

Penetrasyon (Sızma) testleri:

- Araçlar hizmete hazır hale getirildikten sonra detaylı sızma testine tabi tutulmalıdır.
- Yapılacak testler yalnızca yazılımı değil donanım ve gömülü sistemleri de kapsmalıdır.

Haberleşme Protokolleri ve Ağ Sistemleri

- Araç içinde kullanılacak haberleşme protokolleri güvenlik açısından kendini ispatlamış ve yüksek güvenilirlik standartlarına sahip olmalıdır.
- Haberleşme sistemlerinde ileri düzey kriptografiye sahip şifreleme mekanizmaları kullanılmalıdır.
- Aracın tamamında haberleşme ve bilgi depolamada şifreleme esas olmalı ve gelişmiş şifreleme teknolojileri kullanılmalıdır.

Kimlik doğrulama ve yetkilendirme

- Araç erişiminde kimlik doğrulama ve yetkilendirme sistemleri kullanılmalıdır.
- İki faktörlü kimlik doğrulama (Two factor authentication) teknolojisi ile kimlik ve erişim yetkilendirme sistemi kullanılmalıdır.

Çözüm ortakları ile çalışma güvenliği

- Yazılım ya da donanım ürünleri araç üreten firmaya üçüncü bir firma üzerinden sağlanıyorsa bu güvenilir firma olması ve siber güvenlik konusunda gerekli sertifika süreçlerini tamamlamış olmalıdır.
- Çözüm ortağı, denetlenebilir ve hesap verebilirlik konusunda açık olmalıdır.

Araç sahiplerinin alması gereken önlemler

- Kullanıcılar araç içinde ya da dış haberleşmede olabilecek şüphe oluşturan aktiviteleri üretici firmaya bildirmelidirler.
- Şarj istasyonlarında şüpheli bir durumun tespit edilmesi durumunda ilgili kişi ya da kuruluşlara bilgi vermelidirler.
- Kullanıcılar siber güvenlik tehditler konusunda farkındalık eğitimi almalı ve bunlardan korunma yollarını öğrenmelidirler.
- Güçlü şifreleme ve iki faktörlü doğrulama gibi teknolojilerde bilgi sahibi olmalıdırlar.
- Yazılımların sürekli olarak güncel olmasını takip etmeli gerekmesi durumunda üretici firma ile irtibatta olmalıdırlar.
- Kimlik avı saldırılarına karşı dikkatli olunması ve yalnızca güvenilir kaynaklardan uygulama veya yazılım indirilmesi ve e-mail/mesaj alınması gerekir.

Gelecekte Elektrikli Araçlarda Siber Güvenliği Geliştirme ve Güçlendirme Yolları nelerdir?

Elektrikli araçlarda ilerleyen zamanda daha da karmaşık hale gelecek olan yazılım kontrol sistemleri, elektronik bileşenler vb. sistemler berberinde daha farklı siber güvenlik açıklarını oluşturacakları bir gerçektir. Bu konuda alınabilecek bazı önemli tedbirleri şunlardır;

1. İleri düzey Tehdit ve Tespit önleme sistemleri

- Yapay Zekâ (AI) ve Makine Öğrenim (ML) Teknolojilerinin kullanımı: İnsan kaynaklı hataların önüne geçebilmek için doğru eğitilmiş ve güvenilirliği ispatlanmış Yapay Zekâ modelleri elektrikli araçlarda kullanılmalıdır. Bu şekilde şüpheli ya da normal olmayan tehditlerin engellenmesi sağlanacaktır. Proaktif olarak siber güvenlik tedbirlerinin alınması sağlanacaktır.
- Elektrikli araç üreticileri arasında kurulacak ortak bir siber güvenlik veri tabanı aracılığı ile yeni çıkmış olan tehditlerden haberdar olma sağlanacak ve bunlar için önceden tedbir alınabilecektir.

2. Elektrikli Araç Tasarımları

- Elektrikli araçlarda siber güvenlik konusu esas tasarımın ortasında yer almalı ve geliştirilecek aracın bütün mimarisi(yazılım ve donanım) bu çerçeveye uygun olarak tasarlanmalıdır. Siber güvenliğe uygun bulunmayan ya da sorun çıkartabilecek her türlü üretimden vaz geçilmez.
- Üretim ekipmanları ve yazılımlar siber saldırılara karşı dayanıklı olarak üretilmelidir.
- Araç için hayati öneme sahip bileşenlerin erişimleri izole edilmeli yetkisiz erişimler engellenmeli ve ileri düzey güvenliğe sahip metotlarla bu sistemlere giriş kontrol sağlanmalıdır.
- Araç içinde kullanılmakta olan haberleşme protokollerinde siber güvenlik açığı barından iletişim metotları terk edilmeli yerine daha güvenilir ve sürdürülebilir protokollere geçilmelidir.

3. Veri Şifreleme ve Yedekleme

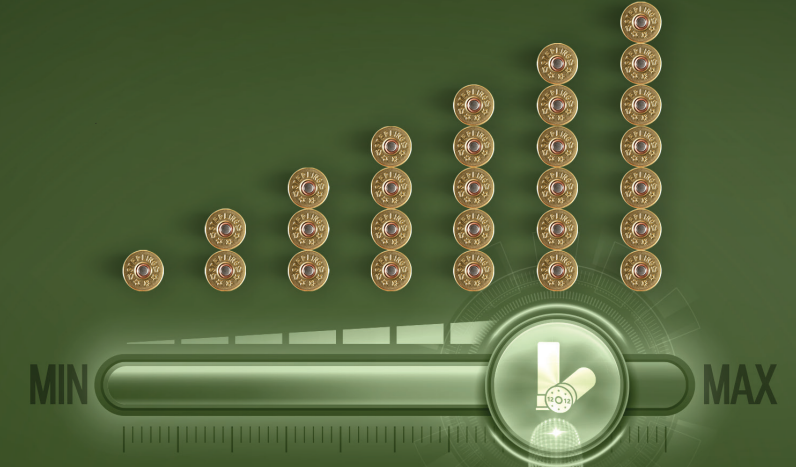
- Araç içinde depolanan ve dışarı aktarılan verilerin korunmasında güçlü şifreleme algoritmaları kullanılmalı gereken yerlerde veri anonimleştirilmelidir.
- Ransomware vb. saldırılara karşı düzenli olarak veri yedekleme mekanizması olmalıdır.

4.Yasal Düzenlemeler:

- Mevcutta geliştirilmiş olan siber güvenlik standartlarına uymak zorunlu hale getirilmeli, yaptırımı ve denetleme mekanizması siber saldırılara göre sürekli güncellenmelidir.

MIN SIZE, MAX CAPACITY

Redefining Firepower!



A first from Turaç in Türkiye!

- Mini Slug 12 Cal., produced with a 50 mm case, is 15 mm shorter than a regular shell
- 50% more shell capacity
- Uninterrupted firing performance
- 28 grams



sterling.com.tr



sterlingammunition



Sterling High Quality Ammunition



Sterling_Ammo



SterlingAmmunition

STERLING
HIGH QUALITY AMMUNITION

