TÜBİTAK SİBER GÜVENLİK TEST VE İSTERLERİ

1. Kontrol Maddesi:

Cihaz ve sistemlerde varsayılan parola kullanılmamalıdır. İlk giriş sonrası kullanıcıya parola değiştirme zorunluluğu getirilmelidir. Parolalar en az 8 karakter uzunluğunda olmalı. Parola deneme sayısı sınırlandırılmalı ve başarısız denemelerde kullanıcı girişi için süre kilidi uygulanmalıdır.

Kaynak: ETSI EN 303 645 - Madde 5.1, ETSI TS 103 701 - Madde 5.1

- Tüm cihazlar benzersiz, güçlü ve varsayılan olmayan parolalarla gelmelidir.
  (ETSI EN 303 645 - Madde 5.1.1, ETSI TS 103 701 - Madde 5.1.1.1)

- Kullanıcıların güvenli parolalar oluşturması teşvik edilmelidir.
  (ETSI EN 303 645 - Madde 5.1.2, ETSI TS 103 701 - Madde 5.1.1.2)

Uygulanacak Testler:

Cihazlarda ve sistemlerde varsayılan parolanın kullanılmadığı, ilk girişten sonra kullanıcıya parola değiştirme zorunluluğu getirildiği, parolaların en az 8 karakter uzunluğunda olacak şekilde oluşturulduğu, parola deneme sayısının sınırlandırıldığı ve başarısız denemeler sonucunda belirli bir süre için hesap kilitleme mekanizmasının devreye girdiği kontrol edilecektir.

2. Kontrol Maddesi:

Yazılımlar güncel tutulmalıdır.

Kaynak: ETSI EN 303 645 - Madde 5.3, ETSI TS 103 701 - Madde 5.3

- Cihazların yazılım güncellemeleri düzenli olarak sağlanmalı ve eski sürümler için destek belirli bir süre devam etmelidir.
  (ETSI EN 303 645 - Madde 5.3.1, ETSI TS 103 701 - Madde 5.3.1.1)

Uygulanacak Testler:

Cihazların güncel (bilinen zafiyet içermeyen) yazılım sürümleriyle desteklenip desteklenmediği kontrol edilecektir.

3. Kontrol Maddesi:

Hassas güvenlik parametreleri güvenli şekilde saklanmalıdır.

Kaynak: ETSI EN 303 645 - Madde 5.4, ETSI TS 103 701 - Madde 5.4

- Parolalar ve kimlik doğrulama bilgileri gibi hassas veriler şifrelenmiş olarak saklanmalıdır.
  (ETSI EN 303 645 - Madde 5.4.1, ETSI TS 103 701 - Madde 5.4.1.1)

Uygulanacak Testler:

Kimlik doğrulama bilgileri ve diğer kritik güvenlik parametrelerinin güvenli şekilde saklanıp saklanmadığı kontrol edilecektir.

4. Kontrol Maddesi:

Veri iletimin güvenli iletişim kanalları üzerinden sağlanmalıdır. Ağ trafiği güncel ve güçlü kriptografik iletişim protokolleri kullanılarak korunmalı; şifrelenmemiş, zayıf veya güvenli kabul edilmeyen protokoller ile veri iletimi yapılmamalıdır.

Kaynak: (ETSI EN 303 645 - Madde 5.5, ETSI TS 103 701 - Madde 5.5)

- Tüm ağ bağlantıları TLS (Transport Layer Security) veya benzeri güvenlik protokolleri kullanılarak şifrelenmelidir.
  (ETSI EN 303 645 - Madde 5.5.1, ETSI TS 103 701 - Madde 5.5.1.1)

- Hassas verilerin açık metin halinde iletilmemesi sağlanmalıdır.
  (ETSI EN 303 645 - Madde 5.5.2, ETSI TS 103 701 - Madde 5.5.2.1)

Uygulanacak Testler:

Tüm veri iletişiminde güçlü şifreleme yöntemlerinin kullanılıp kullanılmadığı ve hassas bilgilerin açık metin halinde iletilip iletilmediği kontrol edilecektir.

5. Kontrol Maddesi:

Sistemler kesintilere dayanıklı hale getirilmelidir.

Kaynak: ETSI EN 303 645 - Madde 5.9, ETSI TS 103 701 - Madde 5.9

- Cihazlar, ani elektrik kesintilerine ve bağlantı kayıplarına karşı dayanıklı olmalıdır.
  (ETSI EN 303 645 - Madde 5.9.1, ETSI TS 103 701 - Madde 5.9.1.1)

Uygulanacak Testler:

Cihazların kesintiler karşısında hizmet sürekliliğini ve veri bütünlüğünü koruyup korumadığı kontrol edilecektir.

6. Kontrol Maddesi

Dış yüzeyden erişilebilecek fiziksel seri arayüzler (UART/JTAG/SWD, RS-232/RS-485, I²C, SPI vb.) gereksiz ise varsayılan olarak devre dışı bırakılmalı; gerekli durumlarda ise yetkisiz erişime karşı korunmalıdır.
Seri arayüzler üzerinden iletilen loglarda IP, kimlik ve benzeri hassas verilerin maskelenmesi/filtrelenmesi sağlanmalıdır. Cihaza yönelik fiziksel müdahalelere karşı kurcalama kanıtı çözümleri kullanılmalıdır.

Kaynak: ETSI EN 303 645 - Madde 5.6 - EN 303 645 — Madde 5.6-4A

- Cihaz donanımı, fiziksel arayüzleri gereksiz yere saldırıya maruz bırakmamalıdır. *(ETSI EN 303 645 – Madde 5.6.-3)*
- Hata ayıklama arayüzleri devre dışı bırakılmalı veya iyi uygulamalara uygun kimlik doğrulama/erişim kontrolü mekanizmasıyla korunmalıdır. *(ETSI EN 303 645 – Madde 5.6.-4A)*

Uygulanacak Testler:
Cihaz kasası açılmadan fiziksel seri arayüzlere erişilemediği, erişim sağlansa dahi yönetim yetkisine veya hassas verilere ulaşılamadığı ve açık bırakılması gereken operasyonel saha portlarının kurcalama kanıtı çözümleri ile korunarak konumlandırıldığı kontrol edilecektir. Bu kapsamda; Mühür ve Etiket Bütünlüğü İnceleme Testleri kapsamında etiketlerin yırtılma, bozulma ve sökülme davranışının gözlemlenmesi; UART/JTAG/SWD Port Tespit ve Sınıflandırma Testleri kapsamında seri portların varlığının ve işlevsel olup olmadığının belirlenmesi; Shell/Bootloader Erişim Açıklığı İnceleme Testleri kapsamında port üzerinden doğrudan yönetim erişimi olup olmadığının doğrulanması; Kasa Üzerinden Erişilebilen Portların İnceleme Testleri kapsamında dış yüzeyden fiziksel temas sağlanabilen bağlantı noktalarının tespiti; Isı, Soğutma ve Solvent ile Mühür Atlatma Dayanım Testleri kapsamında mühür ve etiketlerin çevresel müdahaleler ile sökülme davranışının test edilmesi; Servis Modu Kimlik Doğrulama Doğrulama Testleri kapsamında ise servis erişiminin parola, token veya benzeri yöntemlerle kontrol altına alınmış olup olmadığının doğrulanması gerçekleştirilecektir.