1. Amaç

Bu prosedürün amacı, Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası çerçevesinde; kurum bünyesinde kullanılan IoT cihazlarının bilgi güvenliği risklerini azaltmak, yetkisiz erişimleri önlemek, veri gizliliğini korumak ve sistem sürekliliğini (kurulum, yapılandırma, güncelleme ve kurtarma süreçleri dahil) güvenli bir şekilde sağlamaktır,. Bu doğrultuda, cihazların operasyonel ve yönetsel faaliyetleri sırasında bilgi güvenliği ihlallerini önlemek ve kurumu ilgili siber tehditlere karşı korumak hedeflenmektedir.

2. Kapsam

Bu prosedür, Nesnelerin İnterneti (IoT) Cihazlarının Güvenliği Politikası çerçevesinde; kurum ağına bağlı veya dolaylı olarak erişimi olan veya kurum ağına bağlı olmasa da kurumun fiziksel sınırları içinde olan tüm IoT cihazlarını, bu cihazlardan sorumlu kişileri ve bu cihazların bağlı olduğu altyapıları kapsar.

3. Tanımlar

IoT Cihazı: İnternet veya kurumsal ağ üzerinden veri alışverişi gerçekleştiren fiziksel donanım.

Firmware: Cihazın çalışmasını sağlayan gömülü sistem yazılımı.

Zero Trust: Hiçbir kullanıcıya/cihaza varsayılan olarak güvenilmemesi ve her erişimin doğrulanması modelidir.

4. Roller ve Sorumluluklar

Bilgi Güvenliği Ekibi: Bilgi Güvenliği Ekibi, IoT güvenlik politikalarını oluşturmak, risk değerlendirmelerini gerçekleştirmek ve güvenlik kontrollerinin uygulanmasını denetlemekten sorumludur.

Sistem ve Ağ Yöneticileri: Sistem ve Ağ Yöneticileri, IoT cihazlarının güvenli ağ yapılandırmasını sağlamak, güncellemeleri uygulamak ve sistem loglarının sürekli olarak izlenmesini gerçekleştirmekle yükümlüdür.

Cihaz Sahipleri: Cihaz sahipleri, sorumluları veya kullanıcıları, kendilerine tahsis edilen IoT cihazlarının güvenli kullanımını sağlamak ve fiziksel güvenliğini korumaktan sorumludur.

5. IoT Güvenlik Prensipleri

IoT cihazlarının yönetiminde minimum yetki prensibi uygulanmalı, hiçbir cihaz varsayılan olarak güvenilir kabul edilmemeli ve tüm sistemler güvenli varsayılan yapılandırmalar ile devreye alınmalıdır.

Güvenlik kontrolleri sürekli izleme ve düzenli güncelleme yaklaşımı ile sürdürülebilir hale getirilmelidir.

6. Cihaz Envanter Yönetimi

Kurum ağına bağlanan tüm IoT cihazları resmi envanter sistemine kaydedilmelidir. Her cihaz için cihaz adı, IP adresi, MAC adresi, firmware versiyonu, fiziksel lokasyon ve sorumlu kişi bilgileri tutulmalıdır. Envantere kayıtlı olmayan cihazların kurumsal ağa bağlanmasına izin verilmemelidir.

7. Kimlik Doğrulama ve Erişim Kontrolü

IoT cihazlarında bulunan varsayılan kullanıcı adı ve parolalar devreye alma aşamasında değiştirilmelidir. Güçlü parola politikası uygulanmalı, mümkün olan durumlarda çok faktörlü kimlik doğrulama kullanılmalıdır. Kullanıcı erişimleri rol tabanlı olarak tanımlanmalı ve cihaz üzerinde gereksiz servisler kapatılmalıdır. Cihaz üzerinde kullanılmayan Telnet (23), FTP (21), HTTP (80) gibi güvensiz portlar kapatılacaktır. Yönetim sadece HTTPS (443) ve SSH (22) üzerinden yapılacaktır.

8. Ağ Güvenliği

IoT cihazları kurumsal ağdan mantıksal olarak ayrılmış ağ segmentlerinde veya VLAN yapısında çalıştırılmalıdır. Ağ erişimleri güvenlik duvarı kuralları ile sınırlandırılmalı ve yalnızca gerekli portların açık kalmasına izin verilmelidir. Uzaktan erişim işlemleri yalnızca güvenli VPN bağlantısı üzerinden gerçekleştirilmelidir.

9. Yazılım ve Firmware Güncellemeleri

IoT cihazlarının firmware ve yazılım güncellemeleri düzenli aralıklarla takip edilmeli ve üretici tarafından yayımlanan güvenlik yamaları gecikmeden uygulanmalıdır. Güncellemeler mümkün olduğunca test ortamında doğrulandıktan sonra canlı ortama aktarılmalıdır. Üretici desteği sona ermiş cihazlar güvenlik riski oluşturduğundan kullanım dışı bırakılmalıdır.

Yazılım ve Firmware Güncelleme Operasyonlarında aşağıdaki hususlara dikkat edilmelidir:

- **Dosya Doğrulama:** Güncelleme dosyaları sadece üreticinin resmi HTTPS portalından indirilecek ve **SHA-256 Hash** kontrolü yapılacaktır.
- **Bilgisayarı Güvenliği:** Güncelleme yapılacak bilgisayar ortak kullanımda olmayacak, antivirüs taraması yapılacak ve USB otomatik çalıştır özelliği kapalı tutulacaktır.
- **Yedekleme:** Güncelleme öncesi mevcut konfigürasyon yedeği alınacak, 15 dakikalık bir "Rollback" (Geri Dönüş) planı hazır bulundurulacaktır.

10. Veri Güvenliği

IoT cihazları tarafından üretilen veya iletilen veriler güvenli iletişim protokolleri kullanılarak şifrelenmelidir. Hassas verilerin cihaz üzerinde kalıcı olarak saklanması engellenmeli ve veri minimizasyonu prensibi uygulanmalıdır .

Kriptografik Protokoller ve Sertifika Yönetimi

- **TLS Yapılandırması:** Özellikle yönetim arayüzlerinde SSL 2.0/3.0 ve TLS 1.0/1.1 tamamen devre dışı bırakılacaktır. Sadece TLS 1.2 ve TLS 1.3 kullanılacaktır.
- **Zafiyetli Algoritmaların Kapatılması:** RC4, DES, 3DES ve MD5 tabanlı şifreleme setleri (cipher suites) kapatılacak; yerine AES-GCM-256 ve SHA-384 tabanlı modern setler aktif edilecektir.
- **Sertifika:** "Self-signed" sertifikalar yerine kurum içi CA tarafından imzalanmış dijital sertifikalar kullanılacaktır.

11. İzleme ve Loglama

IoT cihazlarından elde edilen sistem kayıtları ve tüm başarılı/başarısız işlemler kendi üzerinde ve merkezi log yönetim veya SIEM sistemlerine anlık olarak aktarılmalıdır. Ağ trafiği sürekli olarak izlenmeli ve anormal davranışlar tespit edildiğinde gerekli güvenlik aksiyonları alınmalıdır. Log kayıtları kurum politikalarına uygun süre boyunca saklanmalıdır.

12. Fiziksel Güvenlik

IoT cihazları yetkisiz kişilerin erişemeyeceği güvenli alanlarda konumlandırılmalıdır. Cihazların fiziksel portları, bakım ihtiyacı bulunmadığı durumlarda devre dışı bırakılmalı ve cihazlara yapılan fiziksel müdahaleler kayıt altına alınmalıdır. Cihazların bütünlüğünü ve ağ bağlantı sürekliliğini korumak adına; IoT uç birimlerinin montaj alanlarından izinsiz demontajını imkansız kılacak koruyucu muhafazalar veya kilit sistemleri uygulanmalıdır.
Tamper Switch (Kapak Alarmı): Turnike gibi sistemlerde gövde kapağı açıldığı anda sistem merkezi yazılıma anlık alarm üretmeli ve bu durum güvenlik merkezine bildirilmelidir.

13. Güvenlik Testleri

IoT altyapısı düzenli aralıklarla zafiyet taramasına tabi tutulmalı ve gerekli durumlarda penetrasyon testleri gerçekleştirilmelidir. Firmware ve cihaz yapılandırmaları güvenlik açıkları açısından periyodik olarak analiz edilmelidir.

14. Olay Yönetimi

IoT cihazları ile ilgili güvenlik olayları tespit edildiğinde olay derhal SOME Ekibine bildirilmelidir. Riskli olduğu değerlendirilen cihazlar ağdan izole edilmeli, olay inceleme süreci başlatılmalı ve olay sonrası kök neden analizi yapılarak düzeltici faaliyetler uygulanmalıdır.

15. Tedarikçi ve Üçüncü Taraf Güvenliği

IoT cihaz tedarikçileri seçilirken üreticinin güvenlik güncelleme politikası, destek süresi ve güvenlik sertifikasyonları değerlendirilmelidir. Üçüncü taraf servisler üzerinden erişilen cihazlar için ek güvenlik kontrolleri uygulanmalıdır.

16. Eğitim ve Farkındalık

Kurumda hizmet içi eğitim kapsamında yürütülen bilgi güvenliği farkındalık eğitimlerine IoT (Nesnelerin İnterneti) güvenliği dahil edilmelidir. Bu kapsamda, kullanıcıların IoT cihazlarına ilişkin güvenlik riskleri, güvenli kullanım esasları ve sorumlulukları konusunda düzenli olarak bilgilendirilmesi sağlanır.

17. Denetim ve Uyum

Bu prosedür kapsamında belirlenen kontroller düzenli aralıklarla denetlenmeli ve ulusal veya uluslararası bilgi güvenliği standartları ile uyumluluk sağlanmalıdır. Tespit edilen uygunsuzluklar için düzeltici ve önleyici aksiyon planları oluşturulmalıdır.

18. Yaptırım

Bu prosedür adımlarına uyulmaması durumunda, Konya Teknik Üniversitesi Bilgi Güvenliği Politikası'ndaki yaptırım hükümleri uygulanır.

19. Yürürlük

Bu prosedür, BGYS komisyonu tarafından onaylandıktan sonra Konya Teknik Üniversitesi Bilgi İşlem Daire Başkanlığının web sayfasında yayımlanarak duyurusu yapıldığı tarihte yürürlüğe girer.

20. Yürütme

Bu prosedür, Bilgi İşlem Daire Başkanlığı tarafından yürütülür.