TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

KABLOSUZ AĞLARIN İŞLETİMİ REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Mart 2019

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Mart 2019	İlk sürüm	TÜBİTAK BİLGEM YTE

TELİF HAKKI KORUMALI BELGE

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

YÖNETİCİ ÖZETİ

Dijital Devlet (d-Devlet) alanında ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan, kurumsal dijital kabiliyetlerini bütüncül bir yapı üzerinden değerlendirmeyi sağlayan **Dijital Olgunluk Değerlendirme Modeli**'nin geliştirilmesi ve bu **Model** ile uyumlu **Rehberlerin** hazırlanması ile dijital kurumsal kapasitenin artırılmasına ihtiyaç bulunmaktadır. Bu ihtiyaç doğrultusunda TÜBİTAK-BİLGEM-YTE tarafından iç destekli olarak **Dijital Olgunluk Modeli ve Rehberlik** (DİJİTAL-OMR) Projesi 2016 yılında başlatılmıştır. Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanacaktır.

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2500 soru belirlenmiştir.

Model'in 7 kamu kurum ve kuruluşuna uygulaması yapılarak Dijital Olgunluk Seviyeleri belirlenmiş ve dijital kabiliyetler bazında tespit değerlendirmeleri gerekçelendirilerek Dijital Olgunluk Seviyesini geliştirmeye yönelik kısa, orta ve uzun vadede çözüm önerileri sunulmuştur.

Dijital Olgunluk Değerlendirme Modeli kapsamında yer alan yetkinlikler ve söz konusu yetkinlikler kapsamında yer alan dijital kabiliyetler dikkate alınarak yol gösterici olarak kullanılmak üzere **Rehberler** hazırlanmaktadır. Kurumsal kaynakların büyük bir kısmının işletim ve bakım proje ve faaliyetlerine ayrılmış olduğu tespitinden hareketle, ilk olarak **İşletim ve Bakım Rehberi** hazırlanmış ve 2017 yılında yayımlanmıştır. **Rehber**'de, işletim

ve bakım yetkinliği altında toplanan kabiliyetler bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna yönelik referans, rol, işleyiş, iş akışı ve çıktılar ile ilgili bilgiler sunulmaktadır. Aynı yıl **Model** ile belirlenen tüm dijital kabiliyetler için, yatırım planlanırken dikkate alınması gereken unsurlar ve alternatifleri ile ilgili bilgi ve yönlendirmeleri içeren 32 adet **Dijital Kabiliyet Rehberi** hazırlanmıştır. Söz konusu rehberlerin yetkinlikler altında ve tüm yaşam döngüsü dikkate alınarak genişletilmesine yönelik rehber hazırlama çalışmaları devam etmekte olup bu kapsamda 2018 yılında **BT Hizmetleri** yetkinliği altında yer alan **Veri Merkezi Rehberi**, 2019 yılında aynı yetkinlik altında **Kablosuz Ağların Kullanımı Rehberi** yayımlanmıştır. **Kablosuz Ağların İşletimi Rehberi** hazırlıkları devam etmektedir. 2019 yılı içerisinde bunlara ek olarak **Aktif Dizin Rehberi, Sunucu Rehberi** ve **İstemci Rehberi**'nin hazırlanması planlanmaktadır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitaldonusum.gov.tr** platformu ile açık erişimi sağlanmakta ve **Rehberlerin** kullanımının yaygınlaşması amacıyla eğitim programları, toplantılar ve çalıştaylar düzenlenmesi ile **Rehberlik Mekanizmaları** hayata geçirilmektedir. Bu sayede d-Devlet ekosisteminde görev alan bilişim uzmanlarının yetkinliklerinin artırılması hedeflenmektedir. Yanı sıra **Dijital Olgunluk Değerlendirme Modeli** ile uyumlu olarak 2017 yılında Türkiye'ye özgü **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiş ve **Model** ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönlerinin belirlenmesi ve eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmıştır. 28 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 41 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 5 kurumda yaklaşık 1000 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

2019 Yılı Yıllık Programı'nda belirlenen kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilmesinin ihtiyacının karşılanmasında Dijital Devlet ekosistemine katkı sağlayacağını öngördüğümüz Türkiye'ye özgü geliştirilen ilk **Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri** ile **Dijital Kabiliyet Rehberleri'nin** içeriği ile ilgili **epid.yte@tubitak.gov.tr** ve **www.dijitaldonusum.gov.tr** adresleri aracılığıyla ileteceğiniz değerlendirmelerinizle ilgili çalışmaların tüm ekosistemin bilgi ve tecrübesiyle iyileştirilmesini temenni ederiz.

1 GİRİŞ

Kablosuz Ağların İşletimi Rehberi 5 bölümden oluşmaktadır:

1. Bölüm'de, dokümanın kapsamı, kullanılan terimler ve yararlanılan kaynaklar,
2. Bölüm'de, Proje'nin amacı ve kapsamı,
3. Bölüm'de Dijital Olgunluk ve Yetkinlik Değerlendirme Modelleri ile ilgili bilgiler,
4. Bölüm'de, Kablosuz Ağların İşletimi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Kablosuz Ağların İşletimi Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
ARP	[Address Resolution Protocol] Adres Çözümleme Protokolü
ARP Zehirlenmesi	[ARP Poisoning] Cihazlardaki ARP tablosuna yönelik yapılan bir saldırı çeşididir.
Beamforming	Kablosuz sinyallerin dağılımını bağlanan cihazların konumuna göre değiştiren teknoloji
Bellenim	[Firmware] – Donanımın işlevini ne şekilde gerçekleştireceğini bildiren yazılım
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi Güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
Bilgi Güvenliği İhlal Olayı	Yüksek bir olasılıkla iş fonksiyonlarını kesintiye uğratabilecek bilgi güvenliğini tehdit eden, istenmeyen ya da beklenmeyen bilgi güvenliği olayıdır.
Bluetooth	Kısa mesafe kablosuz veri transfer teknolojisi
Broadcast	Yayımlama – Verinin ağ üzerindeki tüm istemcilere iletilmesi

Terim / Kısaltma	Tanım
BT	Bilgi Teknolojileri
Bulut	Yazılımın, altyapının ve platformun hizmet olarak sunulması ve bu bilişim kaynaklarına çoğunlukla internet üzerinden erişim sağlanmasıdır.
d-Devlet	Dijital Devlet
DHCP	Dinamik Bilgisayar Konfigürasyon Protokolü – Cihazlara IP adresi dağıtan protokol
DHCP Snooping	Sadece belirli portlar üzerinden DHCP yayınına izin verilen savunma mekanizmasıdır.
DMZ	[DeMilitarized Zone] İnternet üzerinden erişilebilir sunucuların konumlandırıldığı, iç ağdan ayrıştırılmış bölge
Dynamic ARP Inspection	Geçersiz ve kötü amaçlı ARP isteklerini reddeden savunma mekanizmasıdır.
Dolaşım	[Roaming] İstemcinin hareket etmesi nedeni ile mevcut erişim noktasından daha iyi sinyal aldığı başka bir erişim noktasına otomatik olarak geçiş yapmasıdır.
EAP	[Extensible Authentication Protocol] Ağ üzerinde kullanılan bir kimlik doğrulama protokolü
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
Failback	Ana bileşende oluşan sorunun düzelmesi sonucu, yedek bileşenden ana bileşene dönüş yapılmasıdır.
Failover	Hizmetin erişilebilirliğini sağlamak için ana bileşende oluşan sorun nedeni ile yedek bileşene geçiş yapılmasıdır.

Terim / Kısaltma	Tanım
Girişim	[Interference] Kablosuz sinyallerin çakışarak birbirini yok etmesi durumudur.
Hizmet	Kullanıcının ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (Örnek: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
Hizmet Bileşeni	Bir hizmetin tam olarak sunulabilmesi için bir araya getirilen hizmet birimleridir. Donanım, yazılım, araç, uygulama, doküman, bilgi, süreç ve destek hizmetler örnek olarak verilebilir. Bir hizmet bileşeni bir ya da birden fazla konfigürasyon öğesi içerebilir.
Hizmet Gereksinimi	Hizmet edinen ve hizmet kullanıcılarının ihtiyaçlarıdır.
Hizmet Kataloğu	Hizmet kataloğu, tüm canlı ve canlıya alınması planlanan BT hizmetlerine ilişkin bilgileri içeren bir doküman / veritabanı / listedir.
Hizmet Sürekliliği	Bir hizmet ya da hizmetlerin üzerinde mutabık kalınmış hizmet seviyelerinde sürekli olarak verilmesine yönelik ciddi etkileri olan olay ve risklerin yönetilmesidir.
Hotspot	Halka açık alanda internete erişim olanağı sağlayan kablosuz erişim noktalarıdır.
IPSec	[Internet Protocol Security] IP Paketlerini kimlik doğrulaması ve şifrelemeye tabi tutarak iletişimi güvenli hale getiren protokol
İkizlenmiş port	[Mirror Port] Anahtar cihazında bir porttan geçen trafiği izlemek için trafiğin bir kopyasının gönderildiği port
İzinsiz Giriş Saldırısı	[Intruder Attack] İzinsiz olarak sisteme giriş yapmaya yönelik saldırı

Terim / Kısaltma	Tanım
Kaba Kuvvet Saldırısı	[Brute Force Attack] Deneme yanılma yöntemiyle parolayı tahmin etmeye yönelik bir izinsiz giriş saldırısı
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanma durumudur.
Kablosuz Erişim Noktası	[Access Point] Kablosuz yerel ağ oluşturan cihaz
Kapasite Planı	Gelecek dönem ihtiyaçları doğrultusunda, alternatif iş senaryolarının göz önünde bulundurularak, gerekli kaynak gereksinimlerinin tespit edildiği ve bu gereksinimlerin karşılanması için gerçekleştirilecek faaliyetlerin yer aldığı plandır.
Köprüleme	[Bridging] Birden fazla ağ bağlantısının birbiri ile iletişime geçerek aralarında veri alışverişi yapacak şekilde yapılandırılmasıdır.
Kriptografi	Protokol ve algoritmaların iletişim güvenliğini sağlamak için kullanılan bir yöntemdir.
Kriptografik Anahtar	Kriptografide, mesaj şifreleme ve mesaj çözme amaçlı kullanılan anahtardır.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
LAN	[Local Area Network] Yerel Ağ
MAC Adresi	[Media Access Control] Ağ adaptörüne atanmış tanımlayıcı adres
Multicast	Verinin ağ üzerindeki birkaç istemciye tek kopya olarak iletilmesidir.

Terim / Kısaltma	Tanım
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
Olgunluk Değerlendirme Modeli	Başlangıç durumundan, önceden tanımlanmış yetkinlik alanlarındaki olgunluk durumuna kadar, öngörülen, arzu edilen ya da tercih edilen yol doğrultusunda, sıralı düzeyler ya da aşamalar içeren modeldir. İlgili alanda referans modele göre mevcut durumun değerlendirilmesi ve referans modele göre iyileştirme alanlarının belirlenmesi için kullanılır.
Ön Paylaşımlı Anahtar	[Pre-Shared Key] Güvenli kanal oluşturmak üzere kullanılan, önceden paylaşılan kriptografik anahtar
Önleyici Faaliyet	Olası bir uygunsuzluk ya da istenmeyen durumdan kaçınmak ya da oluşma ihtimalini azaltmak için duruma sebep verdiği belirlenen kök nedenlerin ortadan kaldırılmasına yönelik faaliyetlerdir.
PoC	[Proof Of Concept] Kavram Kanıtlama Çalışması
Problem	Bir veya birden fazla arızaya/kesintiye ilişkin kök neden olarak tanımlanan durumdur.
QoS	[Quality of Service] Hizmet kalitesini belirli bir seviyede tutmak için kullanılan trafik önceliklendirme ve kaynak rezerve etme mekanizmasıdır.
RADIUS	Kimlik doğrulama, yetkilendirme ve aktivite izleme protokolü
Risk	Bir faaliyetin içerdiği belirsizlik ve zarar olasılığıdır.
SSID	[Service Set IDentifier] Kablosuz ağ kimliği
STK	Sivil Toplum Kuruluşu
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme

Terim / Kısaltma	Tanım
Tedarikçi	Hizmet sağlayan organizasyonun dışında hizmet sağlayan ile bir sözleşme ile muhatap olan hizmet tasarım, sunum ve iyileştirme faaliyetlerinde katkıda bulunan organizasyondur. Tedarikçilerin alt yüklenicileri tedarikçi olarak ele alınmaz.
Tekrarlayıcı	[Repeater] Kablosuz ağ sinyallerini tekrar yayınlayarak kapsama alanını artıran cihaz
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Tünelleme	[Tunneling] Ağları, aradaki ağ altyapısından bağımsız olarak birleştirme yöntemi
Uygunsuzluk	Bir gereksinimin karşılanamaması durumudur.
VLAN	[Virtual Local Area Network] Sanal Yerel Ağ
Voice over WLAN	Kablosuz ağların ses trafiği için kullanımıdır.
VPN	[Virtual Private Network] İletişimi, kimlik doğrulaması ve şifrelemeye tabi tutarak güvenli hale getiren tünelleme yöntemi
WEP/WPA/WPA2	Kablosuz ağların güvenliğini sağlamak amacıyla kullanılan güvenlik protokolleridir.
Wi-Fi	IEEE 802.11 standartlarını temel alan, kablosuz cihazların birlikte çalışabilirliğini sağlayan teknoloji
WLAN	[Wireless Local Area Network] Kablosuz Yerel Ağ
WLAN Bileşenleri	WLAN altyapısında yer alan cihazlar
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1.2 REFERANSLAR

Ref 1. NSA (2018), Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), Amerika Birleşik Devletleri

Ref 2. IT Grundschutz 1.Yayım (2018): Bilgi Teknolojileri Güvenliği Enstitüsü (BSI), Almanya.

Ref 3. ISO (2013). ISO/IEC 27001 - Information security management.

Ref 4. ISO (2013). ISO/IEC 27002 - Information technology - Security techniques - Code of practice for information security controls

2 DİJİTAL OLGUNLUK MODELİ VE REHBERLİĞİ PROJESİ

Dijital Olgunluk Modeli ve Rehberlik (DİJİTAL-OMR) Projesi, 2016 yılında TÜBİTAK-BİLGEM-YTE tarafından yürütülen iç destekli bir projedir. Projenin amacı, Dijital Devlet (d-Devlet) alanında gelinen düzeyde ülkemiz koşulları ile kamu kurumlarının ihtiyaçlarını göz önünde bulunduran ve uluslararası çalışmaları dikkate alan kurumsal **Dijital Olgunluk Değerlendirme Modeli'nin** geliştirilmesi ve bu yönde kurumsal kapasitenin artırılması için **Model** ile **Rehberlerin** hazırlanmasıdır.

Bu proje ile 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de katkı sağlanacaktır:

- "*E1.1.4-e-Devlet Ekosistemi Rehberlerinin Hazırlanması ve Güncellenmesi*" eylemi, e-Devlet ekosisteminin etkin bir şekilde çalışabilmesi ve sürdürülebilirliği için birlikte çalışabilirlik, kamu kurum / kuruluşlarının internet siteleri ve mobil uygulamaları ile kamu kurum / kuruluşlarının resmi sosyal medya hesaplarının kullanımı ve yönetimine dair rehberler başta olmak üzere mevcut rehberlerin güncellenmesi ve ihtiyaç duyulan yeni rehberlerin hazırlanmasına yönelik bir eylemdir.
- *"E1.1.6-Ulusal e-Devlet Olgunluk Seviyesi Ölçümleme Mekanizmasının Oluşturulması"* eylemi, yaşamsal olaylar bütünlüğünde kamu hizmetlerinin e-Devlet olgunluk düzeyi, Kurum seviyesinde e-Devlet olgunluk düzeyi ve Ulusal e-Devlet olgunluk düzeyi kapsamında e-Devlet olgunluk ve olgunluk ölçümleme modellerinin tanımlanması, tanımlanan bu modeller kullanılarak ulusal düzeyde e-Devlet olgunluk düzeyi ölçümleme çalışmaları ile birlikte, seçilen e-Devlet hizmetleri ve kamu kurumları için e-Devlet olgunluk düzeyi ölçümleme çalışmalarının yürütülmesine yönelik bir eylemdir.

Proje kapsamında yapılacak faaliyetler, kurumsal düzeydeki dijital dönüşümü ve 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'ndaki eylemler ile hayata geçirilmesi öngörülen ulusal düzeydeki olgunluk değerlendirme modelini destekleyecektir. Bir başka ifadeyle, Proje kapsamında üretilecek **Model** ve **Rehber** ile kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek adına kurumsal düzeyden başlayan ve ulusal düzeye çıkan ölçümleme çalışmalarına katkı sağlanacaktır. Dolayısıyla mikro seviyede kurum düzeyindeki kurumsal etkinliği artırma odağı ile şekillendirilen proje çıktıları, makro seviyede ulusal olgunluk düzeyine çekilebilecek bir alt yapı oluşturacaktır. Bu alt yapı sayesinde 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda yer alan eylemlerin uygulanabilirliği artırılacaktır.

Dijital Olgunluk Değerlendirme Modeli ile;

- Kamu kurumlarının bilişim proje ve faaliyetlerine sistemli ve bütüncül bakış açısının geliştirilmesi desteklenecektir.
- Kamu kurumları ve sundukları hizmetlerin dijital olgunlukları hakkında bir değerlendirme yapabilmek ve seviye tespit edebilmek mümkün olacaktır.
- Kurumların içinde bulunduğu dijitalleşme sürecinde değişimlere ve yeniliklere uyumu desteklenecektir.

Model kapsamında hazırlanacak **Rehberler** ve **Rehberlik** mekanizması ile;

- Bilişim projeleri ve faaliyetlerinin daha verimli, etkin ve güvenli planlanması, yürütülmesi ve tamamlanması sağlanarak başarı oranının artırılmasına katkı sağlanacaktır.
- Bilişim proje ve faaliyetlerinin verimliliği artırılarak ilgili hizmetlerin kalite ve performansı iyileştirilecektir.
- Bilişim uzmanlarının dijital kabiliyetleri artırılacaktır.
- TÜBİTAK tarafından yürütülen Kamu BT projeleri ile edinilen bilgi ve tecrübenin, özel sektör ve STK ile açık paylaşımı sağlanacak ve ilgili paydaşlar ile karşılıklı bilgi ve tecrübe alışverişi gerçekleştirilecektir.

3 DİJİTAL OLGUNLUK VE YETKİNLİK DEĞERLENDİRME MODELLERİ

Dijital Olgunluk Değerlendirme Modeli, bir organizasyonun önceden tanımlanmış yetkinlik alanlarındaki yetkinlik durumundan hedeflenen ya da gerekli görülen seviyeye kadar, dijital dönüşüm ve/veya dijital hizmet kabiliyetlerindeki seviyelerin değerlendirilmesini ve iyileştirilmesini sağlayan kademeli referans modeldir.

Dijital teknolojilerin yenilikçi fırsatlarıyla iş süreçlerine uyarlanması ve dijital teknolojiler doğrultusunda yeni katma değerli hizmet ve süreçler oluşturulması kurumsal düzeyde dijital dönüşümün en öncelikli amacı olmaktadır. Dünyada özellikle son 10 yıldır dijitalleşmenin ve ülkelerin farklılaşan koşullarına göre geliştirilen birçok dijital olgunluk değerlendirme modeli olmasına karşın, Türkiye'de kamu kurumlarında "e-Kurum" "e-Devlet" ve "dijital" gibi kavramların hiçbirine yönelik olgunluk referans modelinin olmadığı görülmüştür.

Günümüz koşulları değerlendirildiğinde "dijital" kavramı doğrultusunda hazırlanacak ve kurumların dijital dönüşümlerini analiz edip referanslar doğrultusunda yönlendirecek bir modelin ve model uygulama yaşam döngüsünün olması önemli bir ihtiyaçtır. Ancak bilişim ya da bilgi güvenliği standart ve rehberlerine benzer şekilde uluslararası kabul gören bir kurumsal dönüşüm standardı mevcut değildir.

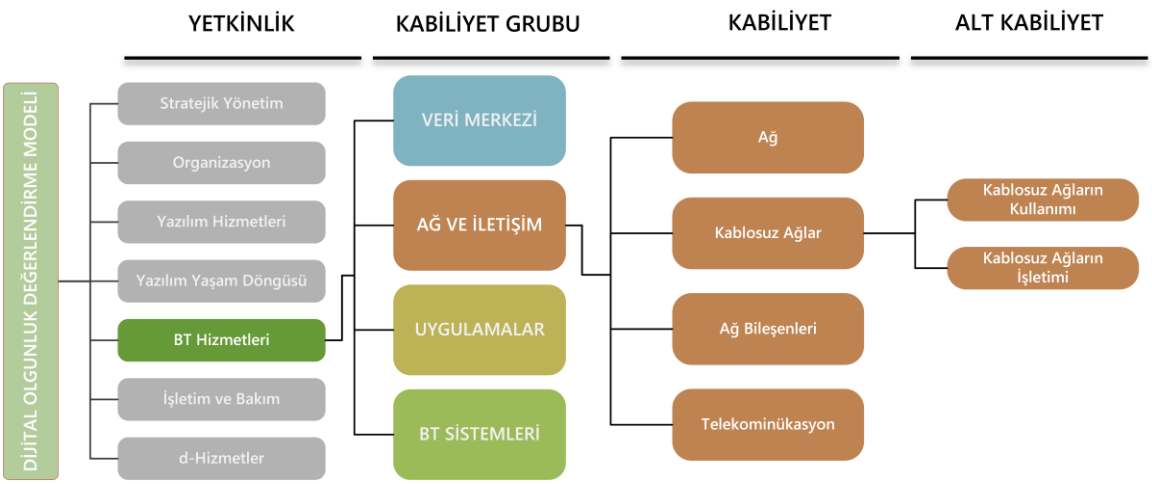
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. Ancak ortak alanlar olmakla birlikte kamu kurumlarının ihtiyaçları özel sektör ihtiyaçlarından ayrışmaktadır. Üstelik kamu yönetim anlayışı ve birikimi göz önüne alındığında, ülkemiz diğer ülkeler ile de ayrışmaktadır. Teknoloji odaklı dönüşüm çabası içerisinde olan tüm organizasyonlar için ortak gereksinimler söz konusu iken mevcut koşulları doğrultusunda her organizasyon tipinin kendi içerisinde özelleşmiş ihtiyaçları da olabilmektedir. Bu doğrultuda, kamu kurumlarında dijital dönüşüme yön verilmesi ve uygulamanın başarı ile hayata geçirilebilmesi için öncelikli olarak, kamu kurumlarına yönelik **Dijital Olgunluk Değerlendirme Modeli** oluşturulmuş ve **Modelin** ülke koşullarına uygun yapıya sahip olması sağlanmıştır. Oluşturulan **Model**, aynı zamanda ülkenin mevcut dijital dönüşüm politikalarıyla uyumludur ve uluslararası tecrübeleri dikkate almaktadır.

Model ile bir organizasyonun dijital kabiliyetlerini değerlendirerek, tespit edilen mevcut kabiliyet seviyelerinin iyileşmesi için yol haritası sağlanmaktadır. Böylece, kurumların dijital

dönüşümlerinin yapısal, standart, tutarlı, etkin ve verimli bir şekilde yapılmasına katkı sağlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli gereksinim ağacı 3 basamak olarak oluşturulmuştur:

- Yetkinlik
- Kabiliyet Grubu
- Kabiliyet
    - Alt Kabiliyet



Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 38 kabiliyet grubu ve bu kabiliyet grupları altında gruplandırılmış çeşitli kabiliyetlerden oluşmaktadır:

- **Yetkinlik**, kendi aralarında ilişki söz konusu olan kabiliyet gruplarından oluşmaktadır. Her bir yetkinlik kendi içerisinde bir bütündür ve organizasyonlarda dijital dönüşüm için müstakil olarak ele alınabilir. Belirlenecek tespitler ve değerlendirmeler doğrultusunda organizasyonun her bir yetkinlik için yetkinlik seviyesi ortaya konmaktadır.
- Birbirlerine yakın olan kabiliyetler **kabiliyet grupları** altında toplanmıştır. Her bir yetkinlik altında tanımlanmış kabiliyet grupları arasında ilişki mevcuttur. Bu ilişki genel olarak bir döngü ya da pratikler üzerinden tarif edilmektedir.
- **Kabiliyetler**, organizasyonun iş ve işlemlerini gerçekleştirebilmek için gerek duyduğu/duyacağı en küçük bileşenlerdir. Kabiliyetler uluslararası normlara ve ulusal gereksinimlere uygun olarak belirlenmiştir.

- **Alt Kabiliyetler,** kabiliyetlerin; amaç, hedef kitle ve operasyonel sorumluluk alanlarına göre özelleşmiş alt bileşenleridir.
- **Seviye**, kurumun varlıklarının, uygulamalarının ve süreçlerinin gerekli çıktıları güvenilir ve sürdürülebilir bir şekilde üreterek olgun bir yapıya ulaşması amacıyla yapılandırılmış düzeylerdir.

Dijital dönüşümü hedefleyen kurumların ihtiyaç duyacağı yetkinlik alanları **Dijital Olgunluk Değerlendirme Modeli** kapsamında aşağıdaki gibi tanımlanmıştır:

Şekil 2. Dijital Olgunluk Değerlendirme Modeli - Genel Görünüm

1. Yetkinlik: STRATEJİK YÖNETİM

Dijital dönüşüm ve dijital hizmet yönetimi kapsamında orta ve uzun vadeli amaçları, temel ilke ve politikaları, hedef ve öncelikleri ve bunlara ulaşmak için izlenecek yol ve yöntemleri içeren strateji belgelerinin; kapsamına ilişkin faaliyetleri amaç, yöntem ve içerik olarak düzenleyen ve gerçekleştirme esaslarının bütününü içeren politika belgelerinin hazırlanmasını, izlenmesini ve güncellenmesini kapsar. Bu strateji ve politikalar doğrultusunda, kurumsal mimari yapısının kurulması, ihtiyaçların tanımlanması, çözümlerin planlanması ve bütçenin yönetilmesi amaçlanmaktadır. Bu yetkinlik, dijital strateji yönetimi, politika, kurumsal mimari, ihtiyaç tanımlama ve çözüm planlama ve bütçe kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON

Dijital dönüşüm çalışmalarının (portföy, program vb.) yönetişim mekanizmasından sorumlusu ekip / kişilerin mevcudiyeti, yönetişim mekanizmasının işlerliği, rol, yetenek ve yetkinliklerinin yönetilmesini kapsar. Bu yetkinlik, organizasyon, dijital kültür ve yetkinlik kabiliyet gruplarını içermektedir.

3. Yetkinlik: YAZILIM HİZMETLERİ

Kurum ihtiyaçlarına göre bir yazılımın yaşam döngüsü için yapılan yazılım fizibilitesi, geliştirilmesi, bakımı ve modernizasyonu, hazır paket yazılımların tedariki ile veri üretimi ve sayısallaştırma hizmetlerini kapsar. Bu yetkinlik, yazılım fizibilite, yazılım geliştirme, yazılım modernizasyonu, yazılım tedarik, yazılım bakımı, veri üretimi ve sayısallaştırma kabiliyet gruplarını içermektedir.

4. Yetkinlik: YAZILIM YAŞAM DÖNGÜSÜ

Yazılım projesinin planlamasından başlayarak teslimatına kadar geçirmiş olduğu bütün aşamaları ve bu aşamalardan oluşan döngüyü kapsar. Bu yetkinlik, proje yönetimi, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, teknoloji sahipliği, donanım/BT altyapı fizibilitesi, donanım/BT altyapı tedariği, yapım işi, hizmet alımı ve BT Altyapısı Bakımı / Modernizasyonu kabiliyet gruplarını içermektedir.

6. Yetkinlik: İŞLETİM VE BAKIM

Kurumsal BT hizmetlerinin planlanması ve yönetişimi, yeni planlanan / değişen BT hizmetlerinin devreye alınması ve kontrolü, BT hizmetlerinin yönetimi, sunulması ve desteği ile BT Hizmet kalitesinin sürekli iyileştirilmesi için gerekli kabiliyetleri kapsar. Bu yetkinlik, planlama ve yönetişim, geçiş ve kontrol, sunum ile izleme ve değerlendirme kabiliyet gruplarını içerir.

7. Yetkinlik: D-HİZMETLER

Kurumun sahip olduğu idari uygulamaların yönetimini, kurum dijital tanıtım kanalları (internet sitesi, sosyal medya hesapları vb.) ve dijital olarak sunulan kamu hizmetlerinin

tasarımını ve iyileştirilmesini içeren tüm adımları kapsar. Bu yetkinlik, kurumsal uygulamaların kullanımı, kurumsal bilgi yönetimi, d-hizmet yönetişimi, d-hizmet tasarımı, d-hizmet sunumu, d-hizmet iyileştirme, d-hizmet inovasyonu kabiliyet gruplarını içerir.

Kabiliyet grubu altındaki hangi kabiliyetlerin organizasyon için gerekli olduğu ve mevcut durumu dijital olgunluk değerlendirmesi kapsamında belirlenebilmektedir. Bu sayede, bazı kabiliyetler ya da kabiliyet grupları değerlendirme dışında bırakılabilmektedir. Benzer şekilde, kurumsal faaliyetlerin çeşitliliğine göre bazı kabiliyet ya da kabiliyet grupları diğerlerinden daha öncelikli olabilmektedir. Nihai kurumsal dijital olgunluk değerlendirmesi, kurumun faaliyet alanı, iş ve işlemlerini dikkate alarak kuruma uygun olarak özelleştirilebilmektedir. Bu sayede, dijital dönüşüm çalışmaları özelleşmiş ihtiyaçlara göre yönlendirilebilmektedir.

Kurumsal Dijital Olgunluk Seviyesi 4 ana gruba ayrılmıştır:

- Seviye 0 (Eksik): kabiliyet yoktur.
- Seviye 1 (Uygulanan): kabiliyetin temel pratikleri uygulanmaktadır.
- Seviye 2 (Kurumsallaşmış): kabiliyetler tanımlı, olup pratikleri, standart ve tutarlı bir şekilde uygulanmaktadır.
- Seviye 3 (Optimize Edilen): kabiliyet seviyeleri ölçülmekte olup, gerçek ve potansiyel problemlerin kaynağı analiz edilerek sürekli iyileşen kabiliyetler vardır.

Her kabiliyet seviyesinin altında tanımlanan sorular, doküman inceleme, ilgili personelle görüşmeler, yerinde gözlemleme, katılımcı gözlemi, fiziksel bulgular gibi çeşitli veri toplama yöntemleri kullanılarak yanıtlanmaktadır. Elde edilen yanıtların konu uzmanlarının değerlendirmeleri ile kabiliyetin seviyesi tespit edilmektedir.

Dijital Olgunluk değerlendirmesi kapsamında kurumun büyüklüğüne göre değişen ortalama 16 haftalık bir süreçte, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarıyla **Dijital Olgunluk Öz Değerlendirme Anketi** yolu ile bilgi toplanmakta, kurum uzmanları ile 3-4 tam gün değerlendirme mülakatları yapılmakta, bilgi, belge ve dokümanlar incelenmekte ve değerlendirme sonrası kurumun mevcut **Dijital Olgunluk Seviyesi** belirlenmektedir. Dijital Olgunluk Seviyesinin bir üst seviyeye çıkması amacı ile değerlendirme sonucu elde edilen tespitler gerçekleşme etkisi ve gerçekleşme süresi üzerinden sınıflandırılarak kısa, orta ve uzun vadeli öneriler ilgili uzman görüşleri dijital kabiliyet rehberleri ile desteklenecek şekilde raporlanmaktadır.

Dijital Olgunluk Değerlendirme Modeli ile;

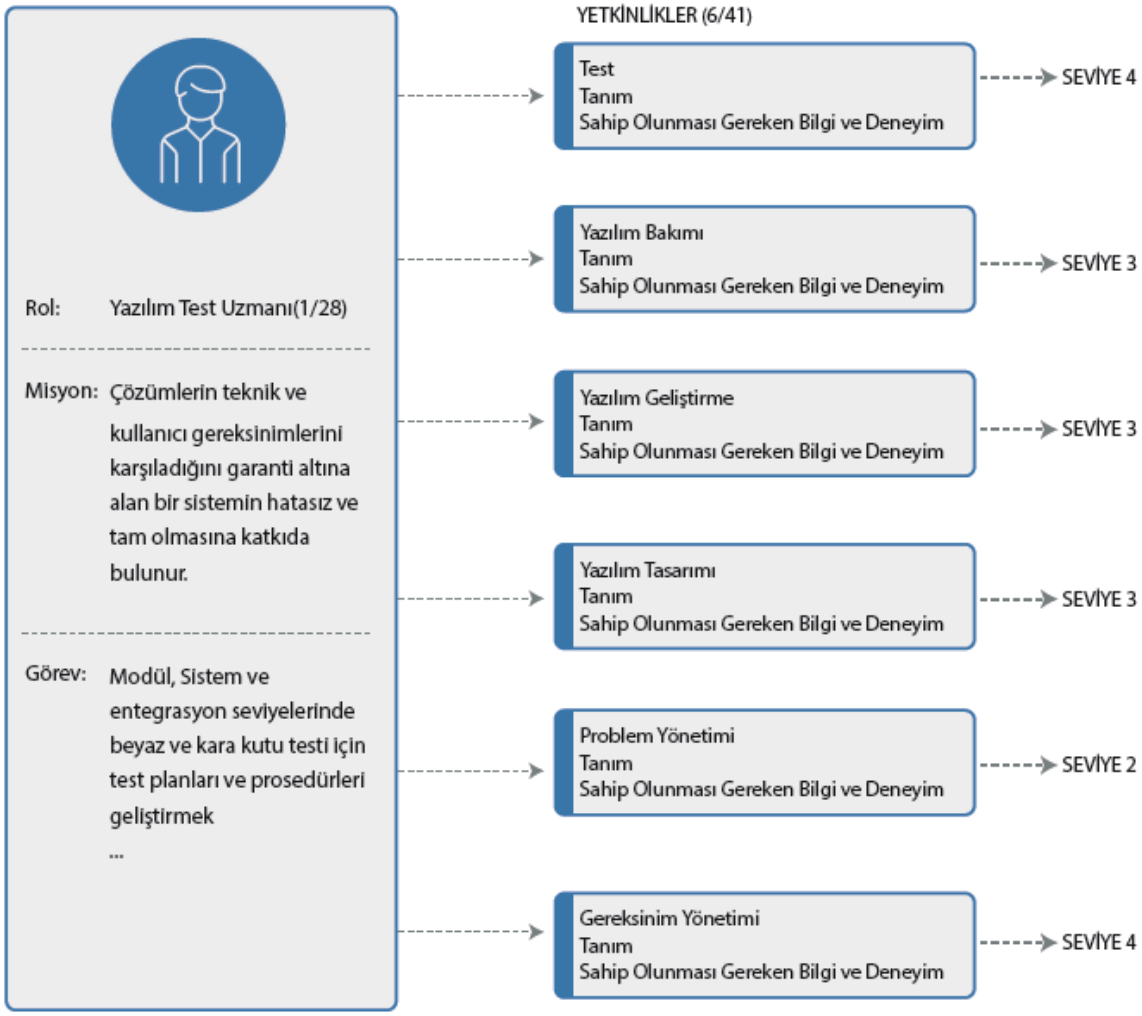
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının belirlenmesi,
- Dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi, çalışan ve vatandaş memnuniyetinin arttırılması

sağlanmaktadır.

Kurum dijital olgunluğunun yetkin insan kaynağı ile iyileştirilmesine yönelik **Dijital Olgunluk Değerlendirme Modeli'nde** yer alan kabiliyetler baz alınarak TÜBİTAK-BİLGEM-YTE tarafından **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Model ile kamu kurumlarında çalışan bilişim uzmanlarının yetkinlik değerlendirmesi yapılarak güçlü ve zayıf yönleri belirlenmekte, eğitim ve mesleki gelişim açısından iyileştirmeye açık alanların tanımlanması amaçlanmaktadır. "SFIA - Skills Framework for the Information Age" ve "European e-Competence Framework" modelleri analiz edilerek Türkiye'ye özgü ihtiyaçlar dikkate alınarak **Dijital Yetkinlik Değerlendirme Modeli** geliştirilmiştir. Dijital Yetkinlik Değerlendirme Modeli'nde;

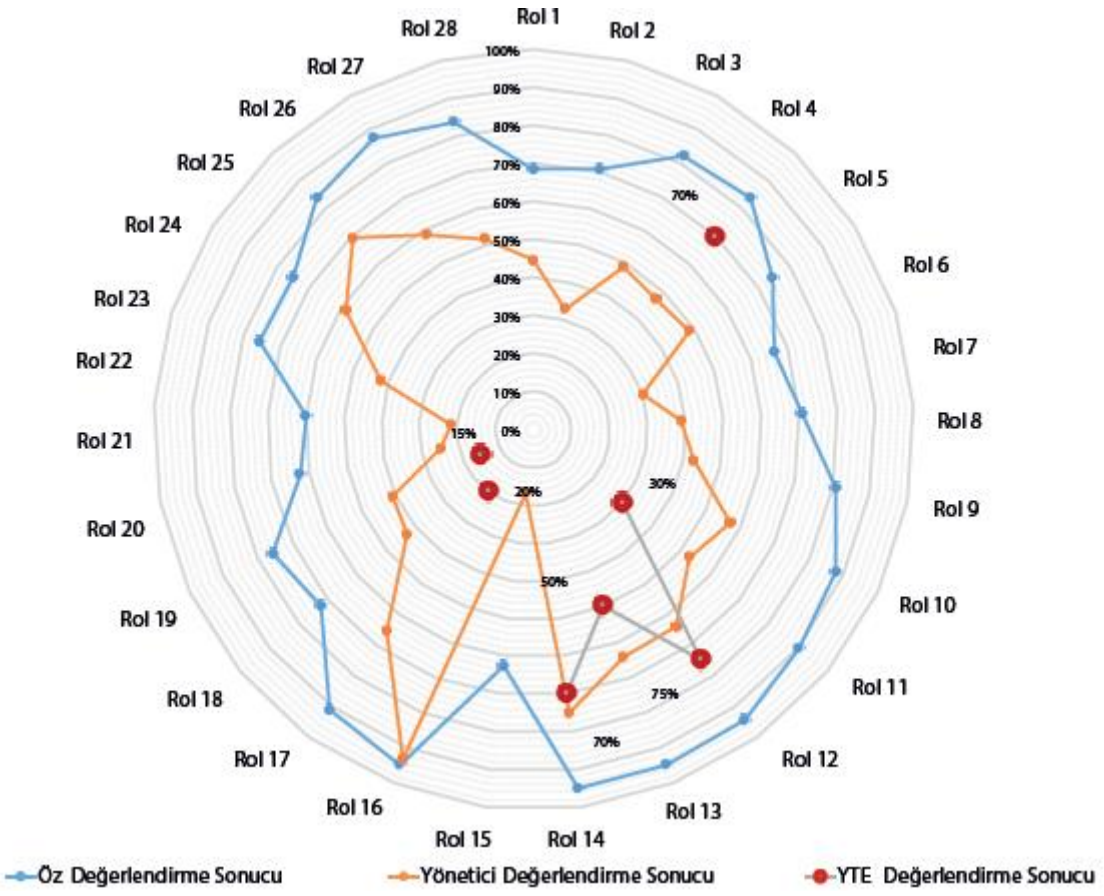
- Bilişim Üst Yönetimi,
- Proje Yönetimi,
- Ağ ve Sistem Yönetimi,
- Bilgi Güvenliği Yönetimi,
- Yazılım Teknolojileri Yönetimi,
- Bütçe ve Tedarik Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 28 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 41 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



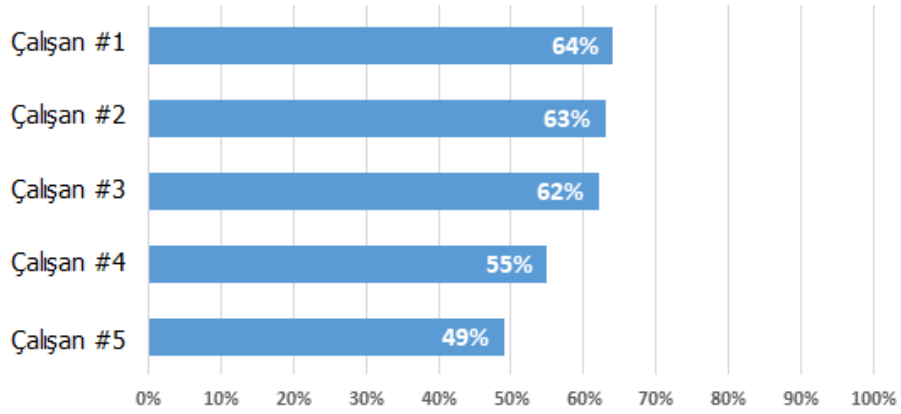
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

Dijital yetkinlik değerlendirmesi kapsamında kurumdaki bilişim uzmanı sayısına bağlı olarak değişen bir sürede, ilgili alan uzmanlarından oluşan 10-15 kişilik **Değerlendirme Ekibi** tarafından değerlendirme yapılmaktadır. Kurum çalışanlarının **Dijital Yetkinlik Öz Değerlendirme Anketi** yolu ile kendilerini değerlendirmesinin yanında, çalışanın bağlı olduğu bir üst yöneticisi tarafından **Yönetici Çalışan Değerlendirme Anketi** yoluyla yöneticisinin çalışanı değerlendirmesi sağlanmaktadır. Çalışan sayısına bağlı olarak değişen sürede çalışanlar ile değerlendirme mülakatları gerçekleştirilmektedir. Çalışan öz değerlendirme ve yönetici değerlendirmesi ile YTE değerlendirme sonucu üzerinden 28 rol bazında uygunluğu raporlanmaktadır:



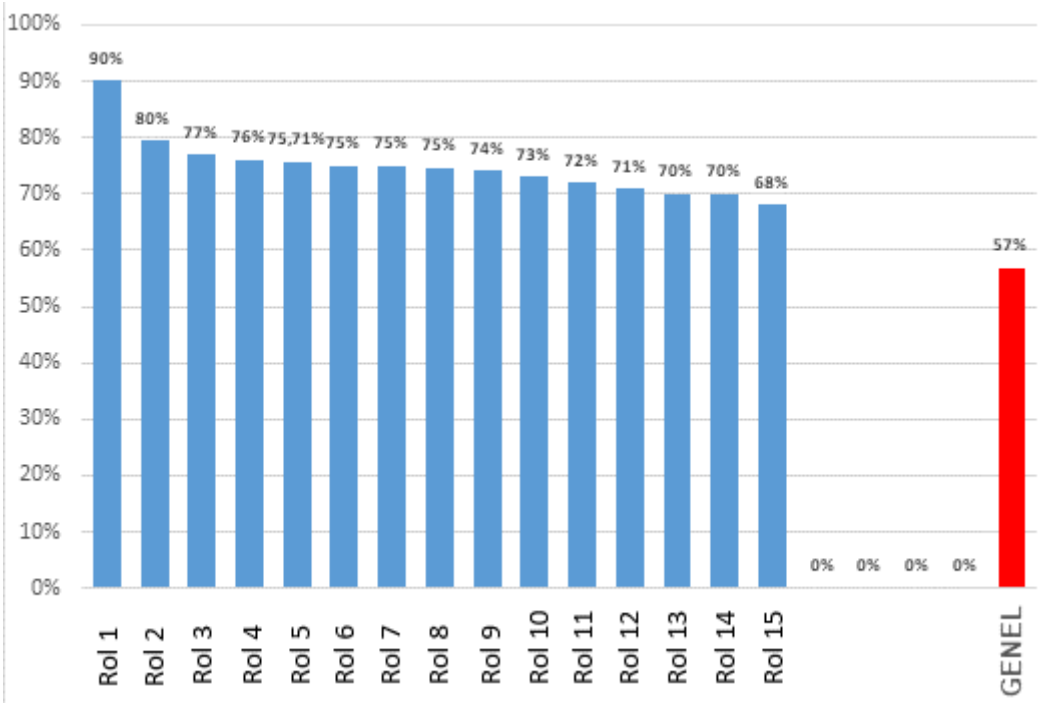
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

Rol bazlı çalışan karşılaştırması yapılarak insan kaynağı kapasitesi değerlendirilmektedir:



Şekil 5. Rol Bazında Dijital Yetkinlik Değerlendirmesi

Bunun yanı sıra kurumdaki roller bazında değerlendirme raporlanmaktadır ve **Kurum Dijital Yetkinlik Haritası** çıkarılmaktadır:



Şekil 6. Kurum Dijital Yetkinlik Haritası

Kurumun büyüklüğü ve bağlı olduğu sektöre göre benzer kategoriye giren dünyadaki en iyi örnekler ile bilişim istihdam dağılımının karşılaştırması yapılarak kurumun istihdam planına rehberlik sağlanmaktadır.

Dijital Yetkinlik Değerlendirme Modeli ile;

- Yetkin bilişim insan kaynağı kapasitesinin arttırılması,
- Bilişim insan kaynağı yetkinliğinin ve kapasitesinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Bilişim uzmanlarının kariyer planı için gerekli yetkinlikleri ve gereken yetkinlik seviyelerini içeren yol haritasının belirlenmesi,
- Bilişim insan kaynağının etkin bir şekilde yönetilmesi

sağlanmaktadır.

4 BT HİZMETLERİ YETKİNLİĞİ

BT Hizmetleri Rehberleri, BT sistemleri için standartlaştırılmış koruma gereksinimlerini ve bu gereksinimleri karşılamak için gerekli uygulama faaliyetlerini açıklar. Bu rehberlerin amacı, kamu kurumlarına BT hizmetleri alanında yol göstermek; "Ağ ve İletişim", "Veri Merkezi", "BT Sistemleri" ve "Uygulamalar" kabiliyetleri bazında tespit edilen seviyelendirilmiş sorular ile kurumların mevcut olgunluğuna ve bu olgunluğu geliştirmeye yönelik bilgiler sunmaktır. Böylece, bu kabiliyet için öncelikli yapılması veya kontrol edilmesi gereken noktalar ve bundan sonra uygulanması gereken faaliyetler sıralı bir şekilde verilmektedir. Bu sayede, bir yol haritası da sunulmaktadır. Bu anlamda bu rehber, kurumun olgunluk seviyesini artırmaya yönelik sürekli kullanılabilecek bir rehber olma özelliği taşımaktadır.

Her konu, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

Bu rehberler, korunma gereksinimlerini basit ve ekonomik bir şekilde oluşturmayı mümkün kılmaktadır. Geleneksel risk analizi yöntemi ilk olarak tehditleri tanımlar ve bunların meydana gelme olasılıkları ile değerlendirir, ardından uygun güvenlik önlemlerini seçer ve sonra kalan riski değerlendirir. Bu adımlar, BT hizmetlerinin her temel bileşen rehberi içerisinde zaten yapılmıştır. Rehberler içerisindeki standartlaştırılmış güvenlik gereksinimleri, BT çalışanları tarafından kendi kurumsal koşullarına uyan koruma önlemlerine kolay bir şekilde dönüştürülebilir. Rehberlerde uygulanan analiz yöntemi, temel bileşenlerde önerilen güvenlik gereksinimleri ile mevcut durumun karşılaştırılmasını mümkün kılmaktadır.

BT hizmetleri rehberlerinde belirtilen gereksinimleri, yeterli düzeyde korunma amaçlı uygulanmalıdır. Bu gereksinimler; 1. seviye koruma, 2. seviye koruma ve 3. seviye koruma olarak ayrılmıştır. 1. seviye gereksinimler, sistemlerin korunması için gerekli asgari/temel ihtiyaçları içerir. Başlangıç olarak kullanıcılar, en önemli gereksinimleri öncelikli karşılamak için kendilerini 1. seviye gereksinimlere göre sınırlandırabilirler. Ancak, yeterli korunma yalnız 2. seviye gereksinimlerin uygulanmasıyla sağlanacaktır. 3. seviye koruma gereksinimleri için örnek olarak, uygulamada kendini kanıtlamış ve kurumun daha fazla korunma gereksinimi durumunda, kendini nasıl emniyet altına alabildiğini göstermektedir.

Yüksek gereksinimler, ele alınması gereken 3. seviye güvenlik eksikliklerini gösterir. Yüksek gereksinim hedefleri, bir taraftan sistemlerin en iyi şekilde korunması sağlar diğer tarafta uygulamada ve bakımda önemli ölçüde maliyetleri artıracaktır. Bundan dolayı yüksek koruma gereksinimleri hedefleniyorsa, maliyet ve etkililik yönleri dikkate alınarak bireysel bir risk analizi yapılmalıdır. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin

uygulanması ve bu yöndeki ihtiyaçların giderilmesi, kurumun veya organizasyonun hedefleri doğrultusunda yeterlidir.

Temel bileşen rehberlerine ek olarak oluşturulan uygulama rehberleri, hedeflenen gereksinimlerin en iyi şekilde nasıl uygulanabileceğine dair ek bilgiler içerir. Bu rehberlerde yer alan 1. ve 2. seviye gereksinimlerin yerine getirilmesi, ISO 27001 sertifikasının alınması sürecine katkı sağlayacaktır.

4.1 YÖNTEM

BT Hizmetleri yetkinliğinde hazırlanan **Kablosuz Ağların İşletimi Rehberi** çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar ve çerçevelerden faydalanılmıştır.

Faydalanılan kaynaklar şunlardır:

- Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) [Ref 1], Amerika Birleşik Devletleri.
- Bilgi Teknolojileri Güvenliği Enstitüsü (BSI) [Ref 2], Almanya.
- ISO 27001 [Ref 3]: Bilgi Güvenliği Yönetimi Sistemi gereksinimlerini tanımlayan uluslararası denetlenebilir standarttır.
- ISO 27002 [Ref 4]: Bilgi Güvenliği Yönetim Sistemine ait iyi uygulama örneklerini içeren dokümandır.

Özellikle **Rehberde** detaylandırılacak alt kabiliyetlerin belirlenmesi için IT-Grundschutz BSI, ISO 27001 ve ISO 27002 temel alınmıştır. Türkiye'nin yapısına uygun uluslararası model ve standartlar örnek alınarak ilgili temel başlıklar oluşturulmuş ve kabiliyetler üzerinden **Rehberin** yapısı belirlenmiştir.

4.2 REHBER YAPISI

Her kabiliyet, temel bileşen (açıklamalar, riskler ve gereksinimler) ve buna ek olarak uygulama rehberlerinden (gereksinimlerin nasıl karşılanacağına dair talimatlar) oluşur.

TEMEL BİLEŞEN YAPISI

Temel bileşenler, ilgili konunun prosedürlerini ve açıklamalarını içermekte, risklere ve bileşenin korunmasını sağlamaya yönelik özel gereksinimlere kısa bir genel bakış sunmaktadır. Ayrıca BT bileşenleri, aynı fihrist/dizin yapısında düzenlenmiştir. Temel bileşen yapısı aşağıdaki gibi oluşturulmuştur:

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım**: Bileşenin kısa tanımıdır.

- **1.2 Hedef**: Bu bileşenin uygulanmasıyla ne tür güvenlik kazanımlarının sağlanacağı hedefler verilmektedir.
- **1.3 Kapsam Dışı**: Bileşende ele alınmayan kapsamın yanı sıra hangi bileşenin konusu olduğu gibi bilgiler yer alır.

- **Bölüm 2 – Risk Kaynakları**
  - Temel bileşene ait özet riskler anlatılmaktadır. Bunlar, sistemlerin kullanımında önlem alınmadığı takdirde ortaya çıkabilecek güvenlik sorunlarının bir resmini çizer. Olası risklerin açıklanması, kullanıcının konu hakkındaki bilinç düzeyini artırır.
- **Bölüm 3 – Gereksinimler**
  - **3.1 1. Seviye Gereksinimler:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir .
  - **3.2 2. Seviye Gereksinimler:** İhtiyaçlar doğrultusunda bu standart gereksinimlerin yerine getirilmesi tavsiye edilir.
  - **3.3 3. Seviye Gereksinimler:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 4 – Detaylı Bilgi için Kaynaklar**
  - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

BT Hizmetleri rehberleri içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi numaralandırılmıştır. Örneğin, BT Hizmetleri rehberlerinde yer alan AGY.2.1.G1 kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

Ağ ve İletişim rehberleri için kullanılan kısaltma (Üst başlık)	Kablosuz Ağlar için atanan numara (1. Alt Başlık)	Kablosuz Ağların İşletimi için atanan numara (2. Alt Başlık)	1. Gereksinim maddesi
AGY	2	1	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberlerinde ise yalnız “G” harfi yerine “U” harfi kullanılmıştır. Örneğin, AGY.2.1.G1 gereksinim maddesinin karşılığı AGY.2.1.U1 olarak geçmektedir.

Ayrıca madde başlıklarında, köşeli parantez içinde madde konusundan ana sorumlu/önerilen kişiler verilmektedir. Bu şekilde, kurum içerisinde hangi role sahip

kişilerin ilgili maddenin uygulamasından sorumlu olduğu açıklanır. Kurumdaki konuyla ilgili uygun kişiler, bu roller yardımıyla tespit edilebilir.

UYGULAMA REHBER YAPISI

BT hizmetlerinin temel bileşenleri için ayrıntılı uygulama talimatları (öneriler ve tecrübe edilmiş pratikler) bu rehberlerde detaylandırılmıştır. Bunlar, gereksinimlerin nasıl uygulanabileceğini ve uygun korunma önlemlerini ayrıntılı olarak açıklar. Korunma konseptleri için bu tür önlemler bir temel olarak kullanılabilir, ancak ilgili kurumun hedef ve koşullarına uyarlanmalıdır.

- **Bölüm 1 – Açıklama:** Bileşenin konusu açıklanmaktadır.
    - **1.1 Tanım:** Bileşenin detaylı tanımıdır.
    - **1.2 Yaşam Döngüsü:** Uygulama rehberleri “Planlama ve Tasarım”, “Tedarik”, “Uygulama”, “Operasyon”, “Elden Çıkarma” ve “Acil Durum Hazırlık” gibi aşamalardan oluşan yaşam döngüsüne yönelik önlemlerin genel resmini içerir.
- **Bölüm 2 – Uygulamalar:**
    - **2.1 1.Seviye Uygulamalar:** Kurumlar öncelikli olarak bu başlık altında yer alan maddeleri zorunlu olarak değerlendirmelidir.
    - **2.2 2.Seviye Uygulamalar:** İhtiyaçlar doğrultusunda bu standart gereksinimleri yerine getirilmesi tavsiye edilir.
    - **2.3 3.Seviye Uygulamalar:** Yüksek gereksinim maddeleri bu alt başlıkta sunulmaktadır.
- **Bölüm 3 – Detaylı Bilgi için Kaynaklar**
    - Rehberlerde kullanılan ve referans alınan kaynakları içermektedir.

Uygulama rehberlerinde yer alan gereksinimlere ait hazırlanan kontrol soruları **EK-A**’da verilmektedir.

4.3 KABİLİYET GRUPLARI

BT Hizmetleri yetkinliğinde ele alınan kabiliyet gruplarının açıklaması ve altlarındaki kabiliyetler şu şekildedir:

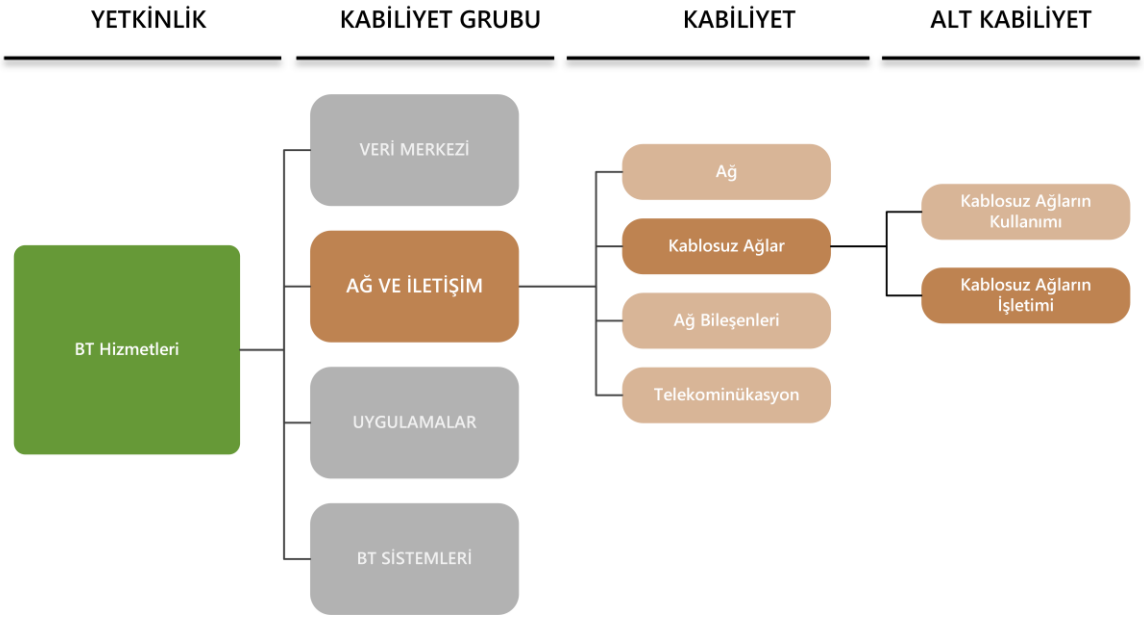
Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

- **Veri Merkezi;** Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Genel Bina
        - Veri merkezi içerisinde bulunan binalar için, genel bina önlemleri en az bir kere uygulanmalıdır.
    - Veri Merkezi ve/veya Sistem Odası
        - Veri merkezi ve/veya sistem odası modülü, kurumun kritik odaları için uygulanmalıdır.
        - Kurum/organizasyon erişilebilirlik hedeflerine veya organizasyon boyutuna göre bu tür alanlar, rehber içeriğinde kritiklik düzeyine göre özelleştirilerek verilmiştir.
    - Elektrik Kablolama
        - Veri merkezini ve kritik bileşenleri besleyen güç kaynaklarının hedeflenen erişilebilirlik prensipleri doğrultusunda en az bir kere uygulanması gereklidir.
    - BT Kablolama
        - Kural olarak bu modül veri merkezinin içerisinde yer alan bina veya yerleşke için en az bir kere uygulanmalıdır. Ayrıca veri merkezi için de kullanılabilir.
- **Ağ ve İletişim;** Ağ ve iletişim hizmetlerinin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
    - Ağ
        - Ağ Mimarisi ve Tasarımı ile Ağ İşletimi konularındaki kabiliyetleri içermektedir.

- Kablosuz Ağlar
  - Kablosuz Ağların Kullanımı ve İşletimi konularındaki kabiliyetleri içermektedir.
- Ağ Bileşenleri
  - Yönlendirici ve Ağ Anahtarlama Cihazı, Güvenlik Duvarı, VPN ve IDS/IPS konularındaki kabiliyetleri içermektedir.
- Telekomünikasyon
  - PBX, VOIP, Fax ve Video Konferans konularındaki kabiliyetleri içermektedir.

- **Uygulamalar;** BT hizmetlerinde kullanılan çeşitli uygulamaların planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler; ofis ve web tarayıcısı uygulamaları gibi kullanıcı uygulamaları, Active Directory hizmeti, Web uygulamaları, dosya sunucusu, DNS, ilişkisel veri tabanı sistemleri, e-posta ve anlık mesajlaşma sistemleridir.
- **BT Sistemleri;** BT hizmetlerinde kullanılan sistemlerin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler; sunucu, sanallaştırma, istemci, mobil cihazlar ve çevresel cihazlardır.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

AGY: AĞ VE İLETİŞİM

AGY.2.1.G KABLOSUZ AĞLARIN İŞLETİMİ

TEMEL BİLEŞEN REHBERİ

AGY.2.1.G KABLOSUZ AĞLARIN İŞLETİMİ TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

Kablosuz yerel ağlar (WLAN), mevcut kablolu ağları genişletmek veya cihazları ağa kablosuz olarak dâhil etmek için kullanılabilir. WLAN bileşenlerinin büyük çoğunluğu IEEE 802.11 standardı temel alınarak üretilmektedir. “Wi-Fi”, bir üretici konsorsiyumu olan “Wi-Fi Alliance” tarafından, IEEE 802.11 standardı temel alınarak oluşturulmuş bir endüstri standardıdır. Bu alanda özel bir role sahip olan “Wi-Fi Alliance”, cihazların belirli birlikte çalışabilirlik ve uygunluk testlerini geçtiğini Wi-Fi onay mührü (Wi-Fi CERTIFIED™) ile onaylar.

WLAN’lar kolay kurulabilir olmaları nedeniyle (ör. fuarlar ve benzeri etkinlikler) geçici ağ ihtiyaçları için de tercih edilir. Ayrıca, havaalanları veya tren istasyonları gibi kamusal alanlarda, ağ erişimi hizmeti sunmak için hotspot’lar kullanılabilir. Bu durum, mobil cihaz kullanıcılarının internete veya kurum iç ağına bağlanmasına olanak sağlar .

1.2 HEDEF

Bu rehber, WLAN'ların bir kurumda nasıl güvenli bir şekilde kurulabileceğini ve işletilebileceğini anlatmayı amaçlamaktadır.

1.3 KAPSAM DIŞI

Bu rehber, WLAN'ları kurarken ve işletirken gözetilmesi ve yerine getirilmesi gereken temel gereksinimleri içerir. WLAN'ların güvenli kullanımı için gereksinimler ise “AGY.2.2 Kablosuz Ağların Kullanımı Rehberi”nde ele alınmıştır.

WLAN'lar, mevcut donanım ve kurumun ihtiyaçlarına göre, Ad-Hoc ve altyapı olmak üzere iki farklı modda çalıştırılabilir. WLAN’lar çoğunlukla altyapı modunda işletilirler. Bu modda istemciler ağa bir erişim noktası üzerinden bağlantı kurarlar. Ad-Hoc modunda ise, kablosuz ağ kartı bulunan iki veya daha fazla mobil cihaz doğrudan birbirleriyle iletişim kurar. Bu modda WLAN'lar herhangi bir sabit altyapı olmaksızın yapılandırıldığından, güvenlik gereksinimi ön planda olan ortamlarda Ad-Hoc modunun kullanımı uygun değildir. Bu sebeple Ad-Hoc modu bu rehberin kapsamına dâhil edilmemiştir.

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler “AGY.2.1 Kablosuz Ağların İşletimi” açısından özellikle önemlidir.

2.1 KABLOSUZ AĞIN İŞLEVİNİN BOZULMASI VEYA TAMAMEN DEVRE DIŞI KALMASI

Kablosuz ağlarda bilgi, elektromanyetik radyo dalgaları aracılığıyla iletilir. Aynı frekans aralığında çalışan diğer elektromanyetik kaynaklar (ör. Bluetooth aygıtları, mikrodalga fırınlar, diğer kablosuz ağlar, radyo sistemleri, vb.) girişime (interference) neden olabilir. Bu durum, WLAN'ın çalışmasını engelleyebilir veya performans düşüklüğüne yol açabilir.

Kablosuz ağlar servis reddi (DoS) saldırılarına maruz kalabilir. Örneğin, kontrol ve yönetim sinyallerinin tekrar tekrar gönderilmesi nedeniyle, kablosuz ağlar kullanılamaz hale gelebilir.

2.2 WLAN KURULUMUNUN EKSİK VEYA YETERSİZ PLANLANMASI

Planlama hataları sıklıkla, güvenlik açıkları oluşturabilecek durumlara sebep olur. WLAN kurulumu, yetersiz şekilde planlanmışsa veya hiç planlanmamışsa, aşağıdaki gibi çeşitli sorunlar ortaya çıkabilir:

- Güncel olmayan WLAN standartları kullanımı durumunda (ör. şifreleme için WEP), kurumun gizli verileri üçüncü şahıslar tarafından ele geçirilebilir.
- İletim kapasitesinin yetersiz olması durumda, fazla bant genişliğine ihtiyaç duyan uygulamalar için gerekli servis kalitesi (QoS) sağlanamaz.

2.3 WLAN İŞLETİMİNDEKİ EKSİK VEYA YETERSİZ DÜZENLEMELER

Merkezi olarak yönetilmeyen bir WLAN altyapısında, varsayılan ayarda bırakılan kablosuz erişim noktaları genellikle güvenlik gereksinimleri açısından yetersiz kalır. Bu cihazlarda hiçbir güvenlik mekanizması dahi bulunmayabilir. Örneğin, güvenlik politikalarının yetersizliği nedeniyle, kurum içi ağa onay sürecinden geçmemiş ya da yeterli güvenlik önlemleri alınmamış bir kablosuz erişim noktası eklenirse, kurum ağında alınan tüm güvenlik önlemleri zayıflatılmış olur.

2.4 UYGUN OLMAYAN KİMLİK DOĞRULAMA METOTLARININ SEÇİMİ

Uygulanan kimlik doğrulama yöntemleri ve güvenlik mekanizmalarının eksik veya yetersiz olması durumunda güvenlik açıkları ortaya çıkabilir. IEEE 802.1X (Port Tabanlı Ağ Erişim Kontrolü) standardı, EAP'yi (Extensible Authentication Protocol) tanımlamaktadır. Tanımlanan EAP yöntemlerinden bazıları, güvenlik açıkları içerir. Örneğin EAP-MD5, *ortadaki adam* veya *sözlük* saldırılarına karşı

savunmasızdır. EAP-MD5 kullanılan altyapılarda, şifreler tahmin edilebilir ve iletişim dinlenebilir.

2.5 WLAN ALTYAPISININ YANLIŞ YAPILANDIRILMASI

Kablosuz erişim noktaları ve WLAN bileşenleri (ör. WLAN kontrolörleri) özellikle güvenlik işlevleriyle ilgili birçok yapılandırma ayarı içerir. Yanlış veya eksik yapılandırılan ayarlar, iletişimin hiç sağlanamamasına ya da iletişimin yeterli seviyede koruma ile gerçekleştirilmemesine neden olabilir.

2.6 YETERSİZ VEYA EKSİK WLAN GÜVENLİK YAPILANDIRMALARI

WLAN bileşenleri çoğu zaman üzerlerinde bulunan güvenlik ayarları etkinleştirilmeden ya da yetersiz şekilde yapılandırılarak teslim edilirler. Ayrıca bazı güvenlik yöntemleri, güncel güvenlik ihtiyaçları açısından yeterli koruma sağlayamamaktadır. Özellikleri itibari ile sadece bu yetersiz güvenlik mekanizmalarını (ör. WEP) barındıran çeşitli WLAN bileşenleri halen kullanılmaktadır. WLAN bileşenlerini güncelleyerek daha güçlü güvenlik mekanizmalarına sahip olmalarını sağlamak her zaman mümkün değildir. Bu tür cihazların kullanılması durumunda, bir saldırgan tüm iletişimi kolayca dinleyebilir ve gizli bilgilere erişebilir.

2.7 WLAN İLETİŞİMİNİ DİNLEME

Kablosuz iletişim birçok kullanıcının paylaştığı bir ortamda sağlandığından, WLAN'lar aracılığıyla gönderilen veriler kolayca dinlenebilmekte ve kaydedilebilmektedir. Veriler hiç şifrelenmeden ya da yeterli güvenlik seviyesinde şifrelenmeden iletiliyorsa, aktarılan veriler kolaylıkla ele geçirilebilir. Buna ek olarak kablosuz sinyaller, kurumun fiziksel sınırlarının dışına taşabilir. Bu sebeple, veriler kontrol edilemeyen ve güvenilmeyen alanlara da yayılabilir.

2.8 GEÇERLİ BİR KABLOSUZ ERİŞİM NOKTASINI TAKLİT ETME

Bir saldırgan, kendi kablosuz erişim noktasını uygun şekilde seçilmiş bir SSID ile yapılandırabilir ve kendini WLAN altyapısının bir parçası olarak gösterebilir. Bu şekilde oluşturulan sahte kablosuz erişim noktasına "rogue access point" denir. Bu sahte erişim noktası, WLAN istemcisine gerçek erişim noktasından daha güçlü bir sinyal sağlıyorsa ve WLAN altyapısında çift taraflı kimlik doğrulaması mecbur kılınmıyorsa, istemci tarafından bu sahte erişim noktası kullanılabilir. Ek olarak, saldırgan tarafından gerçekleştirilecek bir servis reddi (DoS) saldırısı ile gerçek kablosuz erişim noktası devre dışı bırakılabilir. Kullanıcılar bu durumda, hedef ağ olduğunu iddia eden sahte bir ağa giriş yaparlar. Bu tür zehirlenme (poisoning) veya sahtekârlık (spoofing) yöntemleri aynı zamanda bir saldırganın sahte bir kimliği taklit etmesine veya ağ trafiğini kendi sistemlerine

yönlendirmesine izin verir. Saldırgan böylece iletişimi dinleyebilir ve kontrol edebilir. Özellikle halka açık kablosuz ağlarda (ör. hotspot'lar) sahte erişim noktası yöntemi, popüler bir saldırı aracıdır.

2.9 KABLOSUZ ERİŞİM NOKTASI ÜZERİNDEN YETKİSİZ YEREL AĞ ERİŞİMİ

Kablosuz erişim noktaları fiziksel koruma olmadan, dışarıdan kolaylıkla görünür ve erişilir bir şekilde monte edilirse, bir saldırgan erişim noktası ile kablolu ağ altyapısı arasındaki bağlantıyı sağlayan kablodan yararlanarak kablolu ağ altyapısına erişebilir.

2.10 DONANIM HASARI

Donanım hasarı, kablosuz ağ trafiğinin aksamasına ve hatta WLAN'ın hizmet verememesine neden olabilir. Bu durum özellikle, fiziksel olarak korunmayan alanlardaki WLAN cihazları için geçerlidir (ör. açık alanları kapsamak için kurulanlar). Bu tarz alanlarda hizmet veren cihazlara saldırganlar tarafından kasıtlı olarak zarar verilebilir. Ayrıca cihazlar, kötü hava şartlarına (ör. yıldırım) maruz kalabilir.

2.11 BİR KABLOSUZ ERİŞİM NOKTASININ ÇALINMASI

WLAN erişim noktaları, halka açık alanlardaki kolay erişilebilir bölgelere herhangi bir fiziksel koruma olmaksızın monte edilirlerse çalınabilirler. Bu durumda, yapılandırma bilgileri, kayıtlı veriler ve kullanılan parolalar kötü niyetli kişiler tarafından ele geçirilebilir. Daha sonra bu bilgiler, WLAN'a yetkisiz erişim amacı ile kullanılabilir.

3 GEREKSİNİMLER

"AGY.2.1 Kablosuz Ağların İşletimi" rehberinin özel gereksinimleri aşağıda listelenmiştir. Temel olarak, BT Operasyon Ekibi bu gereksinimlerin karşılanmasından sorumludur. Buna ek olarak, Bilgi Güvenliği Birimi her zaman stratejik kararlarda yer almalıdır. Bilgi Güvenliği Birimi tüm ihtiyaçların belirlenen güvenlik politikasına uygun olarak karşılanmasını ve doğrulanmasını sağlamaktan sorumludur. Ayrıca, gereksinimlerin uygulanmasında ilave sorumlulukları olan başka roller de olabilir. Bunlar daha sonra ilgili gereksinimlerin başlığında köşeli parantez içinde açıkça listelenecektir.

Rehber içerisinde gereksinimler, üç ana başlık altında toplanmıştır. Kurumların öncelikli olarak "1. Seviye Gereksinimler" başlığı altında yer alan maddeleri zorunlu olarak değerlendirmeleri, daha sonra ihtiyaçları doğrultusunda "2. Seviye Gereksinimler" ve "3. Seviye Gereksinimler" başlıklarını ele almaları önerilmektedir.

Tablo 2. Kablosuz Ağların İşletimi Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Operasyon Ekibi
Diğer Sorumlular	Bina Hizmetleri, BT Yöneticisi, BT Mimari

3.1 1.SEVİYE GEREKSİNİMLER

Kablosuz ağların işletimi için aşağıda listelenen gereksinimler öncelikli olarak uygulanmalıdır.

AGY.2.1.G1 WLAN kullanımı stratejisinin belirlenmesi [BT Yönetimi]

WLAN'ların bir kurumda kullanılmasından önce, kurumun WLAN kullanımı ile ilgili hangi genel stratejiyi benimseyeceği mutlaka belirlenmelidir. Strateji kapsamında; hangi organizasyonel birimlerde, hangi uygulamalar için, ne amaçla WLAN kullanılacağı ve bu yolla ne tür bilgilerin iletilebileceği açıkça belirtilmelidir. Ayrıca, WLAN bileşenlerinin hangi noktalara kurulacağı da mutlaka planlanmalıdır.

Planlama aşamasında, farklı WLAN bileşenlerinin yönetiminden kimin sorumlu olduğunun, operasyonda yer alan kişiler arasında ne tür bir bilgi alışverişi yapılacağının tanımlanması gereklidir.

AGY.2.1.G2 Uygun WLAN standardının seçimi [BT Mimari]

Mevcut WLAN standartlarının güvenlik yaklaşımları birbirleriyle karşılaştırılmalıdır. Şifreleme ve kimlik doğrulama için güvenilir yöntemlerin kullanıldığından kesinlikle emin olunmalıdır. Standartlar ayrıntılı olarak değerlendirildikten sonra, kuruma özgü bir WLAN

standardı oluşturulmalıdır. Kararın gerekçeleri mutlaka dokümante edilmelidir. Güvenlik gereksinimlerini karşılamayan cihazlar, kesinlikle planlamaya dâhil edilmemelidir.

AGY.2.1.G3 WLAN için uygun şifreleme yöntemlerinin seçimi [BT Mimari]

Kablosuz yerel ağların güvenli şekilde işletimi için, kablosuz arayüz üzerinden iletişim kriptografik olarak korunmalıdır. Güvenlik gereksinimleri açısından WPA2'den daha düşük seviyede olan şifreleme yöntemlerinin kullanılmaması önerilmektedir.

WPA2'nin ön paylaşımlı anahtarla (WPA2-PSK) kullanıldığı durumda, yeterince uzun ve karmaşık bir anahtar tercih edilmelidir. Ayrıca bu anahtar, mutlaka düzenli aralıklarla değiştirilmelidir.

AGY.2.1.G4 Kablosuz erişim noktalarının kurulumu [Bina Hizmetleri]

Kablosuz erişim noktaları, fiziksel güvenliği sağlanacak şekilde monte edilmelidir. Ayrıca, WLAN altyapısının planlanmadığı mekânlarda kablosuz sinyaller mümkün olduğunca azaltılmalıdır. Bina dışına kurulan kablosuz erişim noktaları hava koşullarına ve elektrostatik boşalmalara karşı yeterli düzeyde korunmalıdır.

AGY.2.1.G5 Erişim noktalarının güvenli yapılandırılması

Kablosuz erişim noktaları kesinlikle fabrika ayarlarında kullanılmamalıdır. Kablosuz ağ güvenliğini tehlikeye atmamak için cihazlardaki ön tanımlı SSID'ler, yönetici parolaları ve kriptografik anahtarlar değiştirilmelidir. Ayrıca, güvenli olmayan yönetim amaçlı erişim yöntemleri (ör. Telnet veya HTTP) devre dışı bırakılmalıdır. Kablosuz erişim noktaları mutlaka şifreli bağlantı üzerinden yönetilmelidir.

AGY.2.1.G6 WLAN istemcilerinin güvenli yapılandırılması

Güvenli WLAN işletimi için, WLAN'lara bağlanan tüm istemcilerin de güvenli bir şekilde yapılandırılması önemlidir. İstemcilerin güvenli yapılandırılması için detaylı gereksinimlere "BSY 2.1 Genel İstemci" ve "AGY.2.2 Kablosuz Ağların Kullanımı" rehberlerinden ulaşılabilir. Ayrıca, aşağıdaki WLAN gereksinimlerine uyulmalıdır:

- WLAN arayüzü, uzun bir süre kullanılmadığında mutlaka devre dışı bırakılmalıdır.
- Farklı güvenlik gereksinimlerine sahip ağların WLAN'lar aracılığı ile birbirine bağlanmaması, böylece güvenlik önlemlerinin atlatılamaması sağlanmalıdır.

AGY.2.1.G7 Dağıtım sisteminin kurulumu [BT Mimari]

Bir dağıtım sistemi oluşturulurken, kablolu ve kablosuz tasarımlar analiz edilmeli, bu tasarımların avantaj ve dezavantajları göz önünde bulundurularak karar verilmelidir. Özellikle kablosuz tasarımlar uygulanacak ise güvenlik konuları daha detaylı değerlendirilmelidir.

AGY.2.1.G8 WLAN güvenlik ihlal olayları için davranış kuralları

Bir güvenlik ihlal olayı durumunda, BT Operasyon Ekibi aşağıdaki önlemleri uygulayabilir:

- Kablosuz ağ bağlantısı ile yerel ağ bağlantısı arasındaki aktarım noktasına bir saldırı olması durumunda; iletişimin öncelikle bir veya bir kaç kablosuz erişim noktasında mı, SSID düzeyinde mi yoksa WLAN altyapısının tamamında mı engellenmesinin gerekliliği değerlendirilmelidir.
- Kablosuz erişim noktalarının çalınması durumunda, erişim noktasının kötü amaçlı olarak kullanımını önlemek için güvenlik önlemleri mutlaka uygulanmalıdır.
- WLAN istemcilerinin çalınması durumunda, sertifika tabanlı kimlik doğrulaması kullanılıyorsa istemci sertifikaları engellenmelidir.

Güvenlik ihlal olaylarının kök nedenleri ve olası etkileri mutlaka araştırılarak dokümante edilmelidir.

3.2 2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, kablosuz ağların işletimini daha iyi bir seviyeye getirmeyi düşünen kurum veya organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

AGY.2.1.G9 WLAN'ların LAN'a güvenli şekilde bağlanması [BT Mimari]

WLAN ile LAN arasında bağlantı bulunuyorsa, bu bağlantı üzerinden gerçekleştirilen iletişim, güvenlik yöntemleri (ör. paket filtreleme) ile korunmalıdır. Kablosuz erişim noktalarının, “AGY.2.1.G7 Dağıtım sisteminin kurulumu” gereksinimi dikkate alınarak altyapıya dâhil edilmeleri önerilir.

AGY.2.1.G10 WLAN işletimi için güvenlik politikası oluşturulması

Kurumlarda, WLAN bileşenlerinin kullanımına dair, kurumun genel güvenlik politikasına uygun bir güvenlik politikası oluşturulması önerilmektedir. Bu politika, WLAN'ların kurulumu ve işletilmesi ile ilgili olan herkes tarafından bilinmeli ve ilgili çalışmalar bu politika temel alınarak gerçekleştirilmelidir. Politikanın uygulanıp uygulanmadığının düzenli olarak gözden geçirilmesi ve sonuçların raporlanması tavsiye edilir.

AGY.2.1.G11 Uygun WLAN bileşenlerinin seçimi

Bir WLAN altyapısı oluşturmaya karar verilmişse, yapılan planlama dikkate alınarak bir gereksinim listesi oluşturulmalıdır. Satın alınacak ürünlerin bu liste kullanılarak seçilmesi tavsiye edilmektedir. Ayrıca WLAN bileşenlerinin tedarik sürecinde, bu bileşenlerin mevcut ağın özellikleri ile (güvenlik, kimlik doğrulama, izleme, günlüğe kaydetme vb.) uyumluluğu kontrol edilmelidir.

AGY.2.1.G12 Uygun WLAN yönetim aracının seçimi

WLAN bileşenlerinin güvenlik açısından en uygun şekilde yapılandırılmasını sağlamak için merkezi bir yönetim aracının kullanılması tavsiye edilir. Kullanılan aracın, WLAN stratejisinin gereksinimleriyle uyumlu olması gerekir.

AGY.2.1.G13 WLAN altyapısında rutin güvenlik kontrolleri

Güvenlik açıklarının tespit edilebilmesi için WLAN'ların rutin olarak güvenlik kontrollerinden geçirilmesi önerilir. Buna ek olarak, WLAN'larda kontrol dışı kurulmuş kablosuz erişim noktalarının var olup olmadığı düzenli olarak kontrol edilmeli, ayrıca performans ölçümleri de yapılmalıdır. Rutin güvenlik kontrol sonuçlarının raporlanması, hedef durumla karşılaştırılması ve hedef durumdan sapma sebeplerinin araştırılması tavsiye edilir.

AGY.2.1.G14 WLAN bileşenlerinin rutin güvenlik denetimleri

WLAN altyapısının tüm bileşenleri için (kablosuz erişim noktaları, dağıtım sistemi, WLAN yönetim aracı vb.) tanımlanmış güvenlik önlemlerinin uygulandığı ve doğru bir şekilde yapılandırıldığı düzenli olarak denetlenmelidir. Halka açık alanlara kurulan kablosuz erişim noktaları, fiziksel zorlama girişimlerine karşın rastgele seçilerek düzenli şekilde kontrol edilmelidir. Denetim sonuçlarının izlenebilir olarak raporlanması, hedef durumla karşılaştırılması ve hedef durumdan sapma sebeplerinin araştırılması tavsiye edilir.

3.3 3.SEVİYE GEREKSİNİMLER

1. ve 2.seviye gereksinimler sonrasında, kablosuz ağların işletimi için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip, parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

AGY.2.1.G15 Kablosuz yerel ağların korunması için VPN kullanımı (GB)

Yüksek koruma gereksinimlerinin olması durumunda, WLAN altyapısı üzerinden kurumsal ağa bağlantı sağlanırken VPN kullanılması tavsiye edilir.

AGY.2.1.G16 WLAN'ların LAN'a bağlanması için ilave güvenlik önlemleri (GBE)

WLAN altyapısının LAN'a bağlandığı durumlarda; WLAN'lar ile LAN arasındaki geçişin, daha yüksek koruma gereksinimine uygun olarak güvence altına alınması önerilir.

AGY.2.1.G17 Kablosuz erişim noktaları arasındaki iletişimi koruma (G)

Kablosuz erişim noktaları arasındaki kablosuz arayüz ve LAN üzerinden sağlanan iletişim, iletilen bilgilerin (ör. kullanıcıların erişim verileri) gizliliğini sağlamak amacıyla şifrelenmelidir.

AGY.2.1.G18 Kablosuz saldırı tespit / önleme sistemlerinin kullanımı (GBE)

Güvenlik ihlal olaylarının ve güvenlik zafiyetlerinin zamanında tespit edilmesi ve gerekli önlemlerin alınması için kablosuz saldırı tespit sistemlerinin ve/veya kablosuz saldırı önleme sistemlerinin kullanılması önerilir.

AGY: AĞ VE İLETİŞİM

AGY.2.1.U KABLOSUZ AĞLARIN İŞLETİMİ

UYGULAMA REHBERİ

AGY.2.1.U KABLOSUZ AĞLARIN İŞLETİMİ UYGULAMA

1 AÇIKLAMA

1.1 TANIM

WLAN'lar, mevcut donanım ekipmanına ve kurumun ihtiyaçlarına göre iki farklı modda (Ad-Hoc ve altyapı) çalıştırılabilir. Ad-hoc modunda, kablosuz ağ kartı bulunan iki veya daha fazla mobil cihaz doğrudan birbirleriyle iletişim kurar. Bu modda WLAN'lar bağımsız olarak, yani sabit altyapı bileşenleri olmaksızın yapılandırıldığından, güvenlik gereksinimi ön planda olan ortamlarda Ad-Hoc modunun kullanımı uygun değildir. Bu sebeple Ad-Hoc modu bu rehberde ele alınmamaktadır. Mevcut uygulama rehberi, tüm kablosuz erişim noktalarının merkezi olarak yönetildiğini ve Ad-Hoc modunun kullanılmadığını varsaymaktadır.

Rehberdeki uygulama maddelerini örneklendirmek üzere, farklı güvenlik gereksinimlerine sahip üç adet senaryo tanımlanmıştır. Tanımlanan senaryolar aşağıdaki gibidir:

1. Senaryo

- Bilgiler “GİZLİ” olarak sınıflandırılmamıştır.
- Kablosuz erişim noktaları bir bulut altyapısı aracılığıyla yönetilebilir.
- Kullanıcılar, telefon hizmeti için WLAN altyapısını kullanır.

2. Senaryo

- Bilgiler kısmen “GİZLİ” olarak sınıflandırılmıştır.
- Kablosuz erişim noktaları bir bulut altyapısı üzerinden kesinlikle yönetilemez.
- Kullanıcılar, telefon hizmeti için WLAN altyapısını kullanır.
- Kullanıcılar, WLAN altyapısı üzerinden doküman yönetim sistemlerine erişebilirler.

3. Senaryo

- Bilgiler kısmen “ÇOK GİZLİ” olarak sınıflandırılmıştır.
- Kablosuz erişim noktaları bir bulut altyapısı üzerinden kesinlikle yönetilemez.
- Kullanıcılar, telefon hizmeti için WLAN altyapısını kullanır.
- Kullanıcılar, WLAN altyapısı üzerinden kurumun doküman yönetim sistemlerine, finansal verilere ve/veya kritik sistemlerine erişebilirler.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

WLAN altyapı planlama ve tasarım çalışmalarına; tüm kullanım senaryoları, istenilen özellikler ve yasal gereksinimler dâhil edilmelidir. Bu konuda detaylı bilgiye, “AGY.2.1.U1 WLAN kullanımı stratejisinin belirlenmesi” maddesinden ulaşılabilir. Mevcut süreçler, gelecekteki WLAN altyapı ihtiyaçlarını karşılayıp karşılayamadığı açısından analiz edilmeli ve gerekirse güncellenmelidir. Ayrıca, WLAN altyapısının gerektirdiği işlevselliklerin güvenlik, veri koruma ve iş yönetmeliklerine uygun olup olmadığı incelenmelidir.

Stratejiye ek olarak, doğru WLAN standardının ve ilişkili şifreleme yönteminin seçimi (bkz. “AGY.2.1.U2 Uygun WLAN standardının seçimi ” ve “AGY.2.1.U3 WLAN için uygun şifreleme yöntemlerinin seçimi”), planlama aşamasında ele alınmalıdır.

Güvenlik ayarları, seçilen WLAN standartları ve WLAN yönetimi ile ilgili alınan tüm kararlar, WLAN güvenlik politikasında belirtilmelidir (bkz. “AGY.2.1.U10 WLAN işletimi için güvenlik politikası oluşturulması”).

Uygulama

WLAN bileşenleri seçilirken, “AGY.2.1.U11 Uygun WLAN bileşenlerinin seçimi” maddesi dikkate alınmalıdır. WLAN’larda kullanılan standartlar, protokoller ve entegre güvenlik mekanizmaları sürekli ve hızlı bir şekilde gelişmektedir. Bu durum, WLAN altyapısının ve bileşenlerinin sıklıkla değişime uğramasını gerektirmektedir. WLAN bileşenlerinin ve WLAN altyapısının yenilenmesi için gerekli adımlar dikkatli bir şekilde planlanmalı ve üretim ortamına geçiş öncesinde bir PoC (Proof of Concept) çalışması yapılmalıdır.

İşletim

WLAN işletimi sırasında, yapılan tüm güvenlik ayarlarının daima güncel ve etkin olduğu düzenli denetimler ile kontrol edilmelidir (bkz. “AGY.2.1.U14 WLAN bileşenlerinin rutin güvenlik denetimleri”). WLAN üzerinde güvenli iletişimi sağlamak için kullanılan kriptografik anahtarların yönetimi kritik öneme sahiptir. Bir WLAN yönetimi aracı kullanılıyor ise (bkz. “AGY.2.1.U12 Uygun WLAN yönetim aracının seçimi”) anahtarlar, ayarlar ve WLAN bileşenleri merkezi olarak yönetilebilir.

Kullanım Dışı Bırakma

WLAN bileşenleri kullanım dışı bırakılacaksa, yapılandırma ayarları kaldırılmalı ve fabrika ayarlarına döndürülmelidir.

Acil Durum Hazırlık Planı

WLAN'lara yönelik bir saldırı tespit edildiğinde, acil durum planının ne şekilde uygulanacağı sorumlular tarafından bilinmelidir (bkz. “AGY.2.1.U8 WLAN güvenlik ihlal olayları için davranış kuralları”). Bununla ilişkili olarak acil durum planında, bir güvenlik ihlal olayı meydana geldiğinde hangi adımların atılacağı ve kimlerin bilgilendirileceği yer almalıdır.

2 UYGULAMALAR

Aşağıda yer alan maddeler, "Kablosuz Ağların İşletimi Rehberi"ne özel önlem maddeleridir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

AGY.2.1.U1 WLAN kullanımı stratejisinin belirlenmesi [BT Yönetimi]

Temel WLAN strateji ilkelerini oluşturmak için aşağıdaki sorulardan yararlanılabilir.

- WLAN altyapısı hangi alanlarda kullanılmalıdır?
- WLAN altyapısının kullanımı ne tür faydalar sağlayabilir?
    - Kablosuz yerel ağlar, kuruma ne tür hareket kabiliyetleri kazandırır?
    - WLAN kullanımı ile hangi işlevler veya uygulamalar desteklenmektedir? (ör. Voice over WLAN, Ses/Video Yayını, Video Konferans, Hotspot, Mobil Cihazların Entegrasyonu)
    - WLAN kullanımı ile hangi iş süreçleri optimize edilebilir?
- WLAN altyapısının kullanılması ile ne tür güvenlik riskleri (veri kaybı vb.) ortaya çıkmaktadır?
- Hangi yasal düzenlemelere uyulmalıdır?
- Hangi sınıflandırılmış bilgiler ilave kriptografik koruma mekanizmaları olmadan iletilmemelidir?
- WLAN altyapısının işletilmesinden kim sorumlu olmalıdır?
    - WLAN altyapısı harici olarak yönetilmeli midir?
    - WLAN altyapısı bulut tabanlı olarak yönetilmeli midir?
- WLAN altyapısının kullanılabilirliği için gereksinimler nelerdir?

AGY.2.1.U2 Uygun WLAN standardının seçimi [BT Mimari]

Kurulması planlanan erişim noktaları yakınında yer alan bozucu etki oluşturabilecek unsurlar, WLAN tasarım sürecinde belirlenmeli ve değerlendirilmelidir. Örneğin mikrodalga cihazlar erişim noktalarının veya diğer BT sistemlerinin yakınında çalışıyorsa ağda girişim oluşabilir. Ayrıca Bluetooth vericileri, güç hatları, kablosuz telefonlar (DECT), LCD monitörler ve bina yapı malzemeleri de girişim yaratabilir.

WLAN bileşenleri tedarik edilirken "IEEE 802.11i-2004 (WPA2)" veya daha güncel bir kimlik doğrulama standardının desteklendiğine dikkat edilmelidir.

Wi-Fi parolalarına yönelik kaba kuvvet saldırılarını önlemek için, WLAN altyapısı IEEE 802.11s standardını desteklemelidir. Bu standart, "Simultaneous Authentication of Equals

(SAE)" yöntemini kullanarak gerçek şifrenin radyo kanalı üzerinden iletilmemesinin gerekliliğini açıklar. Böylelikle, saldırganın bağlantıları kaydedip akabinde kaba kuvvet saldırısı aracılığı ile WLAN parolalarını elde etmesi engellenir. IEEE 802.11ac standardı, saldırganlar tarafından gönderilen sahte bağlantı koparma paketlerine karşı gerekli önlemleri içerir. Bu standardın etkin olarak kullanılabilmesi için WLAN istemcileri de IEEE 802.11ac standardını desteklemelidir.

Aşağıdaki tablo, üç kurgusal senaryo için uygulanabilecek kimlik doğrulama seçeneklerini göstermektedir:

Tablo 3. WLAN kimlik doğrulama yöntemleri

Kimlik doğrulama seçeneği	1.Senaryo	2.Senaryo	3.Senaryo
Kimlik Doğrulaması Yok	Hayır	Hayır	Hayır
Wired Equivalent Privacy (WEP)	Hayır	Hayır	Hayır
Message Authentication Code (MAC)	Hayır	Hayır	Hayır
Ön paylaşımlı anahtar (PSK)	Evet	Hayır	Hayır
Standart IEEE 802.1X / Extensible Authentication Protocol (EAP)	Evet	Evet	Evet
Captive Portal (misafir ağları için önerilen yöntem)	Evet	Evet	Evet

Aşağıdaki tablo istemci işletim sistemleri bazında desteklenen IEEE 802.1X EAP çözümlerini listelemektedir. Listede, tüm işletim sistemleri sürümleri gösterilmemiştir. EAP-PEAP, EAP-TTLS veya EAP-SIM yerine EAP-TLS veya EAP-AKA kullanılmalıdır. Ancak, EAP-PEAP ve EAP-TTLS hala yaygın kullanımda olduğundan tabloda yer almaktadır.

Tablo 4. İşletim sistemlerine bağlı olarak WLAN EAP kimlik doğrulama türleri

İşletim Sistemi	EAP-PEAP	EAP-TTLS	EAP-TLS
Windows 10	Evet	Evet	Evet
Windows 8.1	Evet	Evet	Evet
Windows 7	Evet	Evet	Evet

İşletim Sistemi	EAP-PEAP	EAP-TTLS	EAP-TLS
Mac OS X	Evet	Evet	Evet
Linux	Evet	Evet	Evet
iOS	Evet	Evet	Evet
Android	Evet	Evet	Evet
BlackBerry 10	Evet	Evet	Evet
Windows Phone 10	Evet	Evet	Evet
Windows Phone 8.1	Evet	Evet	Evet

EAP-TTLS kullanılıyorsa, kriptografik olarak güvenli kimlik doğrulama yöntemleri kullanılmalıdır. Ayrıca akıllı telefonların ve tabletlerin kimlik doğrulaması için IEEE 802.1X tabanlı EAP-SIM ve EAP-AKA protokolleri de mevcuttur.

AGY.2.1.U3 WLAN için uygun şifreleme yöntemlerinin seçimi [BT Mimari]

Kablosuz yerel ağların güvenli şekilde işletimi için, iletişimin en az WPA2 kullanılarak kriptografik olarak güvence altına alınması gerekmektedir. Kolayca kırılabilen şifreleme yöntemleri kullanılmamalıdır. WEP veya WPA hala kullanımdaysa, WPA2'ye geçiş planlanmalıdır.

WPA2'nin ön paylaşımlı anahtarla (WPA2-PSK) kullanıldığı durumlarda, yeterince uzun ve karmaşık bir anahtar tercih edilmelidir. Anahtarın düzenli olarak değiştirilmesi gerektiğinden, bu yöntem yalnızca az sayıda bileşen içeren WLAN kurulumları için verimli olarak uygulanabilir. Ayrıca, WPA2-PSK ile anahtar oluştururken, Türkçe karakterler ve özel kontrol karakterlerinin kullanılmamasına dikkat edilmelidir.

AGY.2.1.U4 Kablosuz erişim noktalarının kurulumu [Bina Hizmetleri]

Kablosuz erişim noktalarına fiziksel olarak müdahale edilmesini önlemek için cihazlar, binanın iç kısımlarında yer alan duvarlara monte edilebilen sağlam kutular içerisinde muhafaza edilmelidir. Buna ek olarak, kablosuz erişim noktası kutuya sabitlenerek emniyete alınmalıdır. Wi-Fi erişilebilirliğini etkileyebileceğinden, harici antenler kullanılmadıkça kablosuz erişim noktalarının asma tavanlara yerleştirilmesi tavsiye edilmemektedir. Özellikle 802.11ac standardında tanımlanan "beamforming" tekniğinin etkin olduğu durumlarda, erişim noktalarını korumak için kullanılan metal kafesler de iletim kalitesini etkileyebilir.

Erişim noktalarının yerleştirilebilecekleri en uygun konumlar, WLAN kapsama alanı ölçümleri ile belirlenmelidir.

Açık alanlardaki kablosuz ağ bileşenleri (antenler, erişim noktaları vb.), kötü hava koşullarına, elektrostatik boşalmalara, yüksek gerilimlere ve yetkisiz erişime karşı yeterli düzeyde korunmalıdır. Kablosuz erişim noktalarının mümkünse, binaların dış cephelerine kurulmaması tavsiye edilmektedir.

AGY.2.1.U5 Erişim noktalarının güvenli yapılandırılması

Kablosuz ağ güvenliğini tehlikeye atmamak için cihazlardaki ön tanımlı SSID'ler, yönetici parolaları ve kriptografik anahtarlar değiştirilmelidir. Tedarik edilen cihazların işletime doğrudan dâhil edilmesine izin verilmemelidir. Örneğin, cihazın varsayılan ayarları ile tanımlanmış olan SSID içerisinde donanım, kurum, hizmet alınan servis sağlayıcı veya cihazların kullanım amacı hakkında bilgi bulunabilir. Cihazlar bu bilgileri içermeyecek şekilde yeniden yapılandırılmalıdır.

Teknik sorumlularca, WLAN altyapı bileşenlerine ait tüm güvenlik güncellemelerinin ve yamalarının uygulanıp uygulanmadığı düzenli olarak kontrol edilmelidir. Alıcı ve verici arasındaki iletişimin uyumlu ve güvenli bir şekilde gerçekleşebilmesi için, WLAN istemcilerinde de ilgili güncelleme ve yamaların yüklenmesine dikkat edilmelidir. Yeni bir yazılım sürümü veya yaması, ancak gerekli testler yapıldıktan sonra yüklenmelidir. Değişiklik yönetimi prosedürlerinde, bu değişikliklerle ilgili kimin, ne şekilde bilgilendireceği yer almalıdır. Aynı şekilde, WLAN altyapı dokümantasyonu da bu bilgiler doğrultusunda güncellenmelidir.

Aşağıda önerilen ayarlar ile gereksiz portlar ve servisler kapatılarak WLAN altyapısı daha da güvenli hale getirilebilir:

Gereksiz portların kapatılması

WLAN bileşenlerinde çoğunlukla açık bulunan portlar ve bunlar ile ilgili bilgiler aşağıdaki tabloda verilmiştir.

Tablo 5. WLAN bileşenlerinde bulunan portlar

Port Numarası	Tanım	Notlar
21 / TCP	FTP - Çoğunlukla kablosuz erişim noktasına ilişkin işletim sisteminin ve yapılandırma bilgilerinin transferi için kullanılır	İleri seviye güvenlik gereksinimlerinin karşılanması gerekiyorsa (senaryo 3), işletim sistemi ve yapılandırma bilgilerinin transferi kriptografik olarak güvence altına alınarak (şifreli bir biçimde) gerçekleştirilmelidir.
23 / TCP	Telnet	Telnet ile erişime kesinlikle izin verilmemelidir.
67 / UDP	DHCP sunucusu	DHCP servisi kullanılmıyorsa, DHCP sunucusu özellikleri devre dışı bırakılmalıdır.
80 / TCP	HTTP	HTTP servisleri kullanılmıyorsa, bu hizmet devre dışı bırakılmalıdır.
123 / UDP	NTP - erişim noktaları için zaman servisi	İleri seviye güvenlik gereksinimlerinin (senaryo 3) karşılanması gerekiyorsa, zaman senkronizasyonu kriptografik olarak güvenli hale getirilmelidir.
161 / UDP	SNMP yönetim erişimi	SNMP ile erişim, versiyon 3 temel alınarak gerçekleştirilmelidir.
514 / UDP	Syslog - Kablosuz erişim noktalarından mesajların alınması	İleri seviye güvenlik gereksinimlerinin (Senaryo 3) yerine getirilmesi gerekiyorsa, kablosuz erişim noktalarından gelen mesajlar sadece kriptografik olarak güvenli şekilde alınmalıdır.

Gereksiz servislerin engellenmesi

Her üç senaryo için de, WPA2-TKIP yerine WPA2-AES-CCM (128 bit) şifreleme yönteminin kullanılması önerilir.

Aşağıdaki tablo, hangi senaryolarda hangi TLS versiyonları ile bilginin güvence altına alınabileceğini göstermektedir:

Tablo 6. Senaryo bazında önerilen TLS versiyonları

Versiyon	1. Senaryo	2. Senaryo	3. Senaryo
TLS v1.0	Evet	Hayır	Hayır
TLS v1.1	Evet	Evet	Hayır
TLS v1.2	Evet	Evet	Evet

Gereksiz yönetim erişimlerinin engellenmesi

Saldırı yüzeyini azaltmak için WLAN bileşenleri, güvenli bir protokol (ör. SSH, HTTPS veya SNMP) kullanılarak özel bir yönetim ağı üzerinden yönetilmelidir. WLAN altyapısı, WLAN'a bağlı bir istemci aracılığı ile yönetilmemelidir.

İzinsiz giriş saldırılarını (intruder attack) önlemek için, kişiselleştirilmiş kullanıcı hesaplarına dayalı merkezi bir kimlik doğrulaması oluşturulmalıdır. Yönetici hesabına verilen yetkiler, asgari düzeyde tutulmalıdır.

Acil durumlar için yerel bir acil durum kullanıcı hesabının oluşturulması tavsiye edilir. Acil durum kullanıcı hesabının şifresi, kurumun mevcut şifre politikasına uygun olmalıdır. Her kullanımından sonra acil durum kullanıcı hesabının şifresi değiştirilmelidir. Hesabın kullanım nedeni ve hesapla yapılan işlemler, anlaşılabilir bir şekilde dokümante edilmelidir.

Yetkisiz kullanıcı erişiminin tespit edilmesi ve engellenmesi

IP adresleri DHCP sunucusu üzerinden atanıyorsa, ARP zehirlenmesi saldırıları tespit edilebilmeli ve engellenmelidir. Bu amaçla DHCP Snooping ve Dynamic ARP Inspection yöntemleri kullanılabilir.

AGY.2.1.U6 WLAN istemcilerinin güvenli yapılandırılması

Güvenli WLAN işletimi için, WLAN'lara bağlanan tüm istemcilerin de güvenli bir şekilde yapılandırılması önemlidir. İstemcilerin güvenli yapılandırılması için detaylı gereksinimlere "BSY.2.1 Genel İstemci" ve "AGY.2.2 Kablosuz Ağların Kullanımı" rehberlerinden ulaşılabilir. Ayrıca, aşağıdaki WLAN gereksinimlerine uyulmalıdır:

- WLAN arayüzü uzun bir süre kullanılmadığında, mutlaka devre dışı bırakılmalıdır.
- Farklı güvenlik gereksinimlerine sahip ağların WLAN'lar aracılığı ile birbirine bağlanmaması, böylece güvenlik önlemlerinin atlatılamaması sağlanmalıdır.
- WLAN istemcilerinde (ör. akıllı telefonlar) hotspot özellikleri kullanılacak ise, cihazlar ile birlikte gelen ön tanımlı SSID'ler, şifreleme anahtarları ve parolalar

değiştirilmelidir. Şifreler (WPA2 anahtarı), tahmin edilmesi zor olacak şekilde seçilmelidir.

AGY.2.1.U7 Dağıtım sisteminin kurulumu [BT Mimari]

Bir dağıtım sistemi, birden fazla kablosuz erişim noktasının birbirine bağlantısını sağlar. İki tip dağıtım sistemi vardır:

- Kablolu dağıtım sistemleri
- Kablosuz dağıtım sistemleri

İleri seviye erişilebilirlik hedefleniyorsa, kablosuz dağıtım sistemi kurulmamalıdır. Kablosuz dağıtım sisteminde sinyal tekrarlayıcılar hem kablosuz istemcilerle hem de kablosuz erişim noktası ile iletişim kurduğu için iletim hızı yarıya iner. Aktarım hızındaki bu ciddi düşüş ancak tekrarlayıcıların istemcilerle iletişim kurmak için kullandıkları frekansın, tekrarlayıcıların erişim noktalarıyla/kablosuz yönlendiricilerle iletişim kurmak için kullandıkları frekanstan farklı seçilmesiyle önlenebilir.

Kablolu bir dağıtım sistemi kurarken; altyapının fiziksel olarak (fiziksel/sanallaştırılmış ağ anahtarı kullanılarak) mı yoksa mantıksal olarak (VLAN'lar kullanılarak) mı bölümlendirileceğine karar verilmelidir. Kurulum sürecinde güvenlik gereksinimleri de dikkate alınmalıdır.

AGY.2.1.U8 WLAN güvenlik ihlal olayları için davranış kuralları

WLAN kullanımındaki beklenmeyen durumlar (ör. uzun bir süre boyunca WLAN bağlantısı sağlanmaması, kablosuz ağda sürekli olarak kesintiler yaşanması vb.) bir güvenlik ihlal olayından kaynaklanıyor olabilir. Bu durumda BT Operasyon Ekibi, aşağıdaki önlemleri uygulamalıdır:

- Kullanıcılar, uygun iletişim kanallarını kullanarak BT Operasyon Ekibine ulaşabilmelidir.
- Kablosuz ağ bağlantısı ile yerel ağ bağlantısı arasındaki aktarım noktasına bir saldırı olması durumunda; iletişimin öncelikle bir veya bir kaç kablosuz erişim noktasında mı, SSID düzeyinde mi yoksa WLAN altyapısının tamamında mı engellenmesinin gerekliliği değerlendirilmelidir.

Bir güvenlik ihlal olayı gerçekleştiğinde, BT Operasyon Ekibi uygun güvenlik önlemlerini almalıdır. Bu tarz durumlarda izlenecek adımlar, mevcut prosedürlere uygun olarak gerçekleştirilmelidir. Uygulanabilecek olası eylemler aşağıda listelenmiştir:

- Kablosuz erişim noktalarının kapatılması,
- Sunucuların kapatılması,

- Kablosuz erişim noktalarının yapılandırmalarının kontrol edilmesi,
- Sorunun nedenini ortaya koyabilecek tüm dosyaların, özellikle de ilgili kayıt dosyalarının yedeklenmesi (ör. gerçekten bir saldırının gerçekleşip gerçekleşmediği ve saldırganın nasıl başarılı olduğu gibi),
- Gerekiyorsa, orijinal yapılandırma verilerinin geri yüklenmesi,
- Kullanıcıların, herhangi bir anormalliğe karşın, çalışma alanlarını kontrol etmeleri için bilgilendirilmesi.

Kablosuz erişim noktaları çalınmışsa, aşağıdaki güvenlik önlemleri alınmalıdır:

- Kullanılan tüm kriptografik anahtarların değiştirilmesi (WPA2-PSK kullanılması durumunda PSK'lar vb.),
- Çalınan kablosuz erişim noktasını engellemek için RADIUS sunucularında gerekli yapılandırma değişikliklerinin (IP, isim, RADIUS istemcisi, IPSec) uygulanması.

WLAN istemcileri çalınmışsa aşağıdaki güvenlik önlemleri alınmalıdır:

- Sertifika tabanlı bir kimlik doğrulama kullanılıyorsa, istemci sertifikalarının engellenmesi,
- Çalınan cihazların kurum ağına erişiminin engellenmesi için gerekli önlemlerin alınması.

Güvenlik ihlal olaylarının kök nedenleri ve olası etkileri mutlaka araştırılarak dokümante edilmelidir.

2.2 2. SEVİYE UYGULAMALAR

1.seviye uygulamalar sonrasında, kablosuz yerel ağ işletimini daha iyi bir seviyeye getirmeyi düşünen kurum ve organizasyonlar aşağıdaki uygulamaları dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

AGY.2.1.U9 WLAN'ların LAN'a güvenli şekilde bağlanması [BT Mimari]

WLAN ile LAN arasında bağlantı bulunuyorsa, bu bağlantı üzerinden gerçekleştirilen iletişim, güvenlik yöntemleri (ör. paket filtreleme) ile korunmalıdır. Gereksiz broadcast ve multicast trafiğinden kaçınmak için, her SSID'ye karşılık bir VLAN kurulması tavsiye edilir.

WLAN'lar yerel ağ bağlantılarına güvenli bir şekilde bağlanacaksa, kontrolör tabanlı veya bağımsız olarak yönetilen kablosuz erişim noktalarının arasında bir tercih yapılabilir. Bu konuya dair oluşabilecek risklerden korunma önlemleri aşağıda listelenmiştir.

Erişim noktalarının kontrolör tabanlı yönetimi

Aşağıdaki tabloda, senaryo bazında erişim noktası tabanlı güvenlik önlemleri sıralanmıştır:

Tablo 7. Senaryo bazında önerilen erişim noktası özellikleri

Erişim noktası özellikleri	1. Senaryo	2. Senaryo	3. Senaryo
Kullanıcıların merkezi kimlik doğrulaması	Evet	Evet	Evet
Trafiğin WLAN kontrol cihazı üzerinde anahtarlanması (Central Switching)	Hayır	Hayır	Evet
Kablosuz erişim noktasının bağlı olduğu ağ anahtarında trafiğin yerel olarak anahtarlanması (Local Switching)	Evet	Evet	Hayır
Dolaşım (roaming) yetenekleri	Hayır	Evet	Evet
Misafir / hotspot erişimi	Evet	Evet	Hayır

WLAN'a yetkili erişimin IEEE 802.1X ve EAP-TLS protokolleri ile kontrol edilmesi ve erişim noktaları ile istemcilerin IEEE 802.11ac standardını tam olarak desteklemesi koşuluyla, trafiğin yerel olarak anahtarlanması Senaryo 3'te kısmen uygulanabilir. Ayrıca kablosuz erişim noktaları ve WLAN kontrolörü arasındaki iletişim de mutlaka kriptografik olarak korunmalıdır. Kablosuz olarak iletilen verinin gizliliğinin ve bütünlüğünün korunmasına yönelik potansiyel riskleri bertaraf etmek için güçlü şifreleme yöntemlerinin kullanılması önerilir.

Senaryo 1 ve Senaryo 2 için, kablosuz erişim noktasından dâhili ağlara doğru kullanıcı iletişimi, ağ anahtarı aracılığıyla gerçekleşebilir. Ağa sadece, kurumun onay süreçlerinden geçmiş kablosuz erişim noktaları bağlanabilmelidir. Bu kontrolün, IEEE 802.1X standardı aracılığıyla sağlanması tavsiye edilir.

Kablosuz erişim noktaları, işletim sistemlerini doğrudan, bağlı oldukları WLAN kontrolörlerinden alır. Kablosuz erişim noktalarının işletim sistemleri, kriptografik olarak güvenli bir kanal aracılığıyla güncellenmelidir. İşletim sistemlerinin şifrelenmemiş bir kanal aracılığıyla güncellenmesi gerekiyor ise, yazılımın bütünlüğünün dijital imzalar kullanılarak doğrulanması tavsiye edilir.

Misafir erişimi için sağlanan WLAN, DMZ içerisinde sonlandırılmalıdır. Misafir WLAN'ından yapılan erişim, internet üzerinden yapılan bir erişim gibi ele alınmalı ve bu trafik, güvenlik ağ geçidi üzerinden geçirilmelidir.

Erişim noktalarının bağımsız olarak yönetilmesi

Erişim noktaları kontrolör kullanılmadan yönetilirken, kullanıcı trafiği kablosuz erişim noktasından dâhili ağlara doğrudan ağ anahtarı ile geçiş yapmaktadır. Bu yönetim şekli, kontrolör tabanlı yönetime kıyasla yeterince esneklik sağlayamamaktadır.

Dolaşım (roaming) hizmeti için, erişim noktalarında genellikle varsayılan VLAN kullanılır. Kablosuz erişim noktalarının işletim gereksinimlerinin güvenlik gereksinimleriyle uyumlu olup olmadığı, aşağıdaki sorular ile kontrol edilebilir:

- Erişim noktaları arasındaki iletişim, kriptografik olarak yeterince güvence altına alındı mı?
- Ağ anahtarındaki trafiğin izlenmesi için ikizlenmiş portlara erişimi olan kullanıcı grupları biliniyor mu ve sınırlandırılmış mı?
- Kullanılmayan ağ anahtar portları varsayılan VLAN'dan çıkarıldı mı?
- Ağ anahtar portunda donanım kimlik doğrulaması yapılandırıldı mı?
- Dolaşım (roaming) işlevleri köprüleme (bridging) ve tünelleme (tunneling) yöntemleri kullanılarak gerçekleştirildi mi?
- Misafir kullanıcı erişimi, DMZ'de kriptografik tünel aracılığıyla mı sonlandırılıyor?

Kontrolör kullanılmadan gerçekleştirilen yönetimlerde de kurumun onay sürecinden geçmemiş kablosuz erişim noktaları, kurum ağına bağlanamamalıdır. Bu kontrolün, IEEE 802.1X standardı aracılığıyla sağlanması tavsiye edilir. İstemcilerin WLAN'a yetkili erişiminde de IEEE 802.1X ve EAP-TLS kullanılması tavsiye edilir.

Tüm kablosuz erişim noktaları, işletim sistemlerini doğrudan, bağlı oldukları WLAN yönetim siteminden alır. Kablosuz erişim noktalarının işletim sistemleri, kriptografik olarak güvenli bir kanal aracılığıyla güncellenmelidir. İşletim sistemlerinin şifrelenmemiş bir kanal aracılığıyla güncellenmesi gerekiyor ise, yazılımın bütünlüğünün imzalar aracılığıyla doğrulanması tavsiye edilir.

Kullanılan erişim noktaları ve WLAN istemcileri, IEEE 802.11ac standardını tamamen desteklemelidir. İki erişim noktası arası iletişim, IPsec veya TLS kullanılarak şifreli bir biçimde sağlanmalıdır.

AGY.2.1.U10 WLAN işletimi için güvenlik politikası oluşturulması

Kurumlarda, WLAN bileşenlerinin kullanımıyla ilgili, kurumun genel güvenlik politikasına uygun bir güvenlik politikasının oluşturulması önerilmektedir. Politikanın güncelliği düzenli olarak kontrol edilmeli ve gerekli güncellemeler yapılmalıdır.

Kablosuz ağ güvenlik politikası içerisinde:

- Kurumda WLAN bileşenlerini kimlerin kurabileceği, yapılandırabileceği ve kullanabileceği açıklanmalıdır.
- Tüm WLAN bileşenleri için güvenlik önlemleri ve varsayılan yapılandırmaları belirtilmelidir.
- Güvenlik ihlal olaylarından şüphelenilmesi durumunda, bilgi güvenlik ekibinin ne şekilde bilgilendirileceği belirtilmelidir.

BT Operasyon Ekibi, WLAN bileşenlerinin maruz kaldığı tehlikeler ve alınması gereken güvenlik önlemler hakkında bilgilendirilmelidir.

WLAN güvenlik politikasında açıklanan güvenlik önlemlerinin doğru şekilde uygulanıp uygulanmadığının düzenli olarak gözden geçirilmesi ve raporlanması tavsiye edilir.

AGY.2.1.U11 Uygun WLAN bileşenlerinin seçimi

WLAN bileşenlerinin seçiminde güvenlik, gizlilik ve uyumluluk kriterleri önemlidir. Çok sayıda farklı WLAN bileşeninin olduğu durumlarda, bileşenlerin birbirleri ile uyumluluğuna özellikle dikkat edilmelidir. Uyumluluk sorunlarını önlemek için tüm bileşenlerin, Wi-Fi sertifikalı olması ve IEEE 802.11 standartlarını desteklemesi gerekir. WLAN bileşenleri, sadece düzenleyici kurumlar tarafından onaylanan frekans aralıklarını kullanabilir. WLAN bileşenlerine dair bu bilgilere, ürün kullanım kılavuzlarından ulaşılabilir.

Kablosuz erişim noktalarının ve ilgili yönetim sistemlerinin satın alımı kapsamında, aşağıdaki noktaların kontrol edilmesi önerilir:

- Kaç WLAN kanalı yönetilebilir?
- SSID'nin değiştirilebilmesi destekleniyor mu?
- Hangi kriptografik yöntemler uygulanabilir?
- Kimlik doğrulama için hedeflenen ayarlar uygulanabilir mi?
- Hangi EAP yöntemleri destekleniyor?
- Cihazların yönetiminin sadece kriptografik olarak güvenli iletişim kanalları ile yapılması sağlanabilir mi?
- Bilgi akışı kontrolü için Netflow sürüm 9 (RFC 3954) kullanılabilir mi?
- Erişim kontrol mekanizmaları mevcut mu?

- Uygulama tabanlı QoS destekleniyor mu?

Bazı WLAN bileşenleri, kablosuz arayüz üzerinden yapılandırılabilme özelliğine sahiptir. Riski en aza indirmek için bu özelliğin devre dışı bırakılması önerilir. Kurumdaki rol ve yetkilendirme politikası kapsamında, WLAN bileşenlerinin yönetim amaçlı erişiminin sadece yetkili kişiler tarafından gerçekleştirilmesi sağlanmalıdır.

Tedarik edilecek WLAN bileşenlerinin mevcut altyapıda hizmet veren ağ, güvenlik, kimlik doğrulama, izleme ve günlüğe kaydetme bileşenleri ile uyumluluğu kontrol edilmelidir. Örneğin:

- WLAN'da kullanılan kimlik doğrulama yöntemleri; istemcilerin işletim sistemleri ve donanımı, erişim noktaları, ağ yönetim sistemleri ve kimlik doğrulama sunucuları tarafından desteklenmelidir.
- WLAN kimlik doğrulaması IEEE 802.1X gereğince gerçekleştirilirse, kablosuz erişim noktaları EAP kimlik doğrulama yöntemlerini desteklemeli ve iletilen bilgiler doğru şekilde işlenmelidir.
- Ek olarak, kimlik doğrulama isteklerinin merkezi kullanıcı veri tabanına güvenli yöntemler ile iletilip iletilmediği kontrol edilmelidir.

Geniş kapsamlı WLAN altyapı kurulumlarında, belirlenen gereksinimlerin yerine getirilip getirilmediği satın alımı öncesinde test edilerek kontrol edilmelidir.

AGY.2.1.U12 Uygun WLAN yönetim aracının seçimi

WLAN bileşenlerinin güvenlik açısından en uygun şekilde yapılandırılmasını sağlamak için merkezi bir yönetim aracının kullanılması tavsiye edilir. Kullanılan WLAN yönetim aracı aşağıdaki hususları içermelidir:

- Erişim noktalarının ve WLAN istemcilerinin bellenim (firmware) sürümlerinin belgelenmesi,
- Yapılandırma belgeleri,
- Yapılandırma değişikliklerinin geçmişe yönelik olarak izlenebilmesi,
- Alarmların üretilebilmesi ve değerlendirilebilmesi,
- Sorun giderme istatistiklerinin değerlendirilebilmesi,
- Güvenlik ihlal olayı durumunda önlemlerin tetiklenebilmesi,
- WLAN kullanımı değişikliğinde, alarm üreten eşik değerlerin uyarlanabilmesi,
- Günlük kayıt tutma ve geriye dönük analiz için tutulan kayıtların merkezi bir kayıt sistemine gönderilebilmesi.

WLAN yapılandırma yönetiminin güvenliği açısından, güvenli yönetim kanallarının oluşturulması ve güvenlik ayarlarının merkezi olarak yönetilmesi önemlidir. Ayrıca, WLAN

yönetim sistemlerinde, kablosuz arayüzün izlenmesine ve elde edilen ölçüm sonuçlarının yorumlanmasına yardım edecek özelliklerin (ör. sahte erişim cihazlarının tespiti, kablosuz saldırı tespit/önleme) bulunması beklenir. Aşağıdaki iki tablo, saldırıların ve olası tahribatın algılanması için gerekli asgari parametreleri, senaryo bazında sunmaktadır:

Tablo 8. Altyapıdaki saldırıların kablosuz saldırı tespit sistemleri ile algılanması

	1. Senaryo	2. Senaryo	3. Senaryo
Geçersiz MAC OUI'ye sahip istemcilerin tespiti	–	–	✓
Sahte oturum sonlandırma isteklerinin tespiti	✓	✓	✓
Sahte ağdan koparma isteklerinin tespiti	✓	✓	✓
Ad-Hoc ağlarda geçerli SSID'lerin kötüye kullanımının tespiti	–	✓	✓
Malformed Frame (Large Duration) saldırılarının tespiti	–	✓	✓
Malformed Frame (HT-IE) saldırılarının tespiti	–	–	✓
Malformed Frame (Association Request) saldırılarının tespiti	–	–	✓
Malformed Frame (Authentication) saldırılarının tespiti	–	–	✓
Kablosuz erişim noktası kimliğini taklit etme saldırılarının tespiti	–	–	✓
Geçerli SSID'lerin kötüye kullanımının tespiti	–	–	✓
Kablosuz köprü cihazlarının tespiti	–	–	✓
802.11 40MHz intolerans ayarlarının tespiti	–	–	✓
Aktif 802.11n Greenfield modunun tespiti	–	–	✓

	1. Senaryo	2. Senaryo	3. Senaryo
Erişim noktası flood saldırılarının tespiti	–	–	✓
İstemci flood saldırılarının tespiti	–	–	✓
CTS Rate Anomaly tespiti	–	–	✓
RTS Rate Anomaly tespiti	–	–	✓
Geçersiz adres kombinasyonlarının tespiti	–	–	✓
Overflow IE tespiti	–	–	✓
Overflow EAPOL Key tespiti	–	–	✓
Beacon Frame saldırılarının tespiti	–	–	✓

Tablo 9. İstemcideki saldırıların kablosuz saldırı tespit sistemleri ile algılanması

	1. Senaryo	2. Senaryo	3. Senaryo
WLAN istemcilerinde yanlış bağlantıların tespiti	✓	✓	✓
Ağdan koparma saldırılarının tespiti	–	✓	✓
Omerta saldırılarının tespiti	–	✓	✓
FATA-Jack saldırılarının tespiti	–	✓	✓
Block ACK DoS saldırılarının tespiti	–	✓	✓
Hotspot saldırılarının tespiti	–	✓	✓
Power-Save-DOS saldırılarının tespiti	–	✓	✓
Şifrelenmemiş olarak trafik ileten istemcilerin tespiti	–	✓	✓
Anormal EAP paketlerinin tespiti	–	–	✓
Anormal paket trafiğinin tespiti	–	–	✓

	1. Senaryo	2. Senaryo	3. Senaryo
TKIP Replay saldırılarının tespiti	–	–	✓
ASLEAP saldırılarının tespiti	–	–	✓
Air Jack saldırılarının tespiti	–	–	✓

Kontrolör tabanlı bir çözüm kullanıldığı durumda WLAN bileşenleri merkezi olarak yönetilebilir ve trafik WLAN kontrolöründe sonlandırılabilir. Bu sayede örneğin, misafir ağı trafiği DMZ veya güvenlik duvarına iletilebilir. Kontrolör kullanılmayan durumlarda ise, erişim noktaları ile güvenlik cihazları arasında VPN bağlantısı oluşturulmalıdır.

Kontrolör tabanlı çözümün bir başka özelliği de, failover/failback durumlarının kolayca koordine edilebilmesidir. Kontrolör tabanlı bir modelde, kontrolör tüm kablosuz erişim noktaları için tek bir koordinasyon noktası görevi görür. Kablosuz erişim noktalarından biri devre dışı kalırsa, kontrolör cihazı gecikme sürelerini mümkün olduğunca kısa tutmak için önlem alır. Bu durum, WLAN kullanıcısının merkezi olarak depolanmış oturum bilgisinin bir başka erişim noktasına iletilmesiyle sağlanır. Kontrolör bulunmayan altyapılarda ise bu özellik, yerel ağdaki yönlendirme protokolüne benzer mekanizmalar aracılığı ile sağlanmalıdır.

AGY.2.1.U13 WLAN altyapısında rutin güvenlik kontrolleri

WLAN altyapılarının güvenli bir şekilde işletilmesi, güvenlik gereksinimlerinin uygulanmasına ve erişilebilirliğin düzenli olarak kontrol edilmesine bağlıdır. Performans ölçümleri, mevcut izleme ve kayıt altyapısına entegre edilmelidir. WLAN analizi, en basit durumda, uygun yazılım yüklenmiş bir WLAN istemcisi üzerinden gerçekleştirilebilir. Bu tür bir izleme sadece Senaryo 1 için önerilir. Gerekli izleme fonksiyonları kablosuz erişim noktaları ile entegre ise, WLAN altyapısı daha iyi ve daha tutarlı bir şekilde kontrol edilebilir. Erişim noktalarındaki entegre izleme fonksiyonları yardımıyla, aşağıdaki faaliyetler otomatik olarak gerçekleştirilebilir:

- Üçüncü taraf cihazların (özellikle yabancı erişim noktaları) tespit edilmesi,
- Kapsama alanı, veri hızları, iletim kapasitesi, uygulama bit hızı, kullanıcı başına bit hızı, hizmet kalitesi (QoS), vb. bilgileri elde etmek amacıyla kablosuz saha keşiflerinin gerçekleştirilmesi,
- WLAN ağ bileşenlerinin yapılandırmalarının izlenmesi.

BT Operasyon Ekibinin, alarm ve hataların analizi için aşağıdaki adımları planlaması ve gerçekleştirmesi tavsiye edilir:

- Alarmlar tespit edilmeli ve değerlendirilmelidir.
- İstatistikler, sorun giderme için değerlendirilmelidir.
- Güvenlik ihlali olayları durumunda, güvenlik önlemleri tetiklenmelidir.
- WLAN kullanımı değişikliğinde, alarm üreten eşik değerler uyarlanmalıdır.

Güvenlik kontrolünün bir parçası olan sızma testleri yapılarak WLAN'lardaki zayıf noktalar tespit edilmelidir. Alınan tüm güvenlik önlemlerinin, karşılamaları gereken saldırılar için yeterli olup olmadıkları dikkatle kontrol edilmelidir. Aşağıdaki tablo, içeriden ve dışarıdan yapılan sızma testlerinin asgari uygulanma periyodlarına yönelik tavsiyeleri içermektedir:

Tablo 10. Sızma testleri için önerilen zaman aralıkları

	1. Senaryo	2. Senaryo	3. Senaryo
İçeriden yapılan sızma testleri	Yılda bir	Altı ayda bir	Üç ayda bir
Dışarıdan yapılan sızma testleri	–	Her iki yılda bir	Yılda bir

AGY.2.1.U14 WLAN bileşenlerinin rutin güvenlik denetimleri

WLAN altyapısının tüm bileşenleri (kablosuz erişim noktaları, kablosuz dağıtım sistemi, WLAN yönetim aracı, vb.) için tanımlanmış güvenlik önlemlerinin uygulanmış olduğu ve doğru bir şekilde yapılandırıldığı düzenli olarak denetlenmelidir. Halka açık alanlara kurulan kablosuz erişim noktaları, fiziksel zorlama veya manipülasyon girişimlerine karşı rastgele seçilerek düzenli olarak kontrol edilmelidir. Herhangi bir anormallik veya zayıflık tespit edilirse, bu durum dokümante edilmeli ve hedef durumdan sapma sebepleri incelenmelidir.

WLAN yönetim aracının, mevcut yapılandırmalar ile beraber önceki yapılandırmaları da yönetebilmesi rutin güvenlik denetimleri açısından kolaylık sağlayacaktır.

2.3 3. SEVİYE UYGULAMALAR

1. ve 2. seviye gereksinimler sonrasında, kablosuz ağların işletimi için artan koruma koşullarında dikkate alınması gereken gereksinimler aşağıda yer almaktadır. Kurumların kendi ihtiyaçları doğrultusunda ve risk analizi çerçevesinde uygun gereksinimleri belirlemeleri önerilmektedir. Gereksinim tarafından öncelikli koruma sağlanan prensip, parantez içinde bulunan harfler ile belirtilmektedir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

AGY.2.1.U15 Kablosuz yerel ağların korunması için VPN kullanımı (GB)

Yüksek koruma gereksinimlerinin olması durumunda, WLAN altyapısı üzerinden kurumsal ağa bağlantı sağlanırken VPN kullanılması tavsiye edilir.

AGY.2.1.U16 WLAN'ların LAN'a bağlanması için ilave güvenlik önlemleri (GBE)

WLAN altyapısının LAN'a bağlandığı durumlarda; WLAN'lar ile LAN arasındaki geçişin, daha yüksek koruma gereksinimine uygun olarak güvence altına alınması (ör. saldırı tespit/önleme sistemleri kullanımı) önerilir.

AGY.2.1.U17 Kablosuz erişim noktaları arasındaki iletişimi koruma (G)

Kablosuz erişim noktaları arasındaki kablosuz arayüz ve LAN üzerinden sağlanan iletişim, iletilen bilgilerin (ör. kullanıcıların erişim verileri) gizliliğini sağlamak amacıyla şifrelenmelidir.

Kablosuz arayüz üzerinden iletişim

Kablosuz arayüz üzerinden haberleşmeyi sağlamak için, “AGY.2.1.U3 WLAN için uygun şifreleme yöntemlerinin seçimi” ve “AGY.2.1.U5 Erişim noktalarının güvenli yapılandırılması” uygulama maddeleri kullanılmalıdır.

Kablosuz erişim noktası ve WLAN yönetim aracı arasındaki iletişim

Artan koruma gereksinimleri nedeniyle, kablosuz erişim noktaları ile WLAN yönetim aracı arasındaki iletişimin bulut tabanlı olmaması beklenmektedir. Aşağıdaki tabloda iletişimi sağlamak için kullanılabilecek protokollere uygun kimlik doğrulama yöntemleri listelenmektedir.

Tablo 11. Kablosuz erişim noktası ve WLAN yönetim aracı arasındaki iletişim

	CAPWAP + DTLS	IPSec	TLS v1.2
Kimlik doğrulama	Sertifika veya parola (en az 16 karakter)	Sertifika veya parola (en az 16 karakter)	Sertifikalar (ideal olarak TPM'de)

Kablosuz erişim noktalarının kendi aralarındaki iletişimi

Kontrolör tabanlı WLAN altyapısında iletişim, her zaman merkezi WLAN kontrolör üzerinden gerçekleştiğinden, bir kablosuz erişim noktasından başka bir kablosuz erişim noktasına doğrudan iletişim mümkün değildir. Olası protokoller ve ilgili kimlik doğrulama yöntemleri Tablo 9'da listelenmiştir. Aşağıdaki tabloda, kontrolör kullanılmadan bağımsız olarak yönetilen WLAN altyapısı için protokoller ve ilişkili kimlik doğrulama yöntemleri listelenmektedir.

Tablo 12. Kablosuz erişim noktalarının kendi aralarındaki iletişimi

	GRE (varsayılan VLAN'da)	GRE IPSec	TLS v1.2
Kimlik doğrulama	Yok	Sertifika	Sertifikalar

GRE protokolü IPSec kullanılmadığı durumda, şifreleme sağlamamaktadır. Bu nedenle, dolaşım ve WLAN yönetim bilgilerinin gizliliği ile bütünlüğü yeterince korunmadığı için kullanılması önerilmemektedir.

AGY.2.1.U18 Kablosuz saldırı tespit / önleme sistemlerinin kullanımı (GBE)

Güvenlik ihlal olaylarının ve güvenlik zafiyetlerinin zamanında tespit edilmesi ve gerekli önlemlerin alınması için kablosuz saldırı tespit sistemlerinin ve/veya kablosuz saldırı önleme sistemlerinin kullanılması önerilir.

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U1	WLAN kullanımı stratejisinin belirlenmesi	Kablosuz ağların, hangi organizasyonel birimlerde, hangi uygulamalar için ne amaçla kullanılacağı ve bu yolla ne tür bilgilerin iletilebileceği dökümante edilmiş midir?
AGY.2.1.U2	Uygun WLAN standardının seçimi	Kullanılacak WLAN standardı kurum güvenlik politikası içinde tanımlanmış mıdır?
		Kablosuz bağlantı kalitesini etkileyebilecek ve girişime sebep olabilecek kaynaklara (kablosuz telefon, Bluetooth, mikrodalga fırınlar vb.) karşı önlem alınıyor mu?
		802.1x kullanıyorsa şifre değişimi sadece güvenli protokollerle mi sağlanmaktadır? (PEAP/EAP-TLS)
AGY.2.1.U3	WLAN için uygun şifreleme yöntemlerinin seçimi	Kablosuz ağ bağlantıları yeterince güvenli bir şifreleme standardı kullanılarak korunuyor mu?
		Ön paylaşımlı anahtarlar kullanılıyorsa yeterince uzun ve karmaşık bir anahtar belirlendi mi?
		Kablosuz ağlara bağlantı için kullanılan şifreler / anahtarlar düzenli olarak değiştiriliyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U4	Kablosuz erişim noktalarının kurulumu	Kablosuz erişim noktalarının kapsama alanı sınırları, ölçüm yapılarak belirlendi mi?
		Kablosuz erişim noktaları yetkisiz fiziksel erişime karşı korunuyor mu?
		Açık alanlardaki kablosuz ağ bileşenleri, kötü hava koşullarına, elektrostatik boşalmalara, yüksek gerilimlere karşı yeterince korunuyor mu?
AGY.2.1.U5	Erişim noktalarının güvenli yapılandırılması	Erişim noktasının SSID'si; donanım, kurum, hizmet alınan servis sağlayıcı veya cihazların kullanım amacı hakkında bilgi vermeyecek şekilde yapılandırıldı mı?
		WLAN cihazlarının yönetimi için merkezi bir kimlik doğrulama servisi kullanılıyor mu?
		WLAN bileşenlerinin yönetici parolaları düzenli aralıklarla değiştiriliyor mu?
AGY.2.1.U6	WLAN istemcilerinin güvenli yapılandırılması	İstemcilerde güvenlik ayarlarının değiştirilmediği düzenli olarak kontrol ediliyor mu?
		İstemcilerde WLAN arayüzü uzun bir süre kullanılmadığında devre dışı bırakılıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U7	Dağıtım sisteminin kurulumu	Dağıtım sisteminin, kurum ağından fiziksel veya mantıksal ayrımı için alınan karar ve koruma önlemleri dokümante edildi mi?
AGY.2.1.U8	WLAN güvenlik ihlal olayları için davranış kuralları	Güvenlik ihlal olayları sırasında izlenecek adımlar rol bazında tanımlanmış mıdır?
		Güvenlik ihlal olaylarını bildirmek için kullanılacak iletişim kanalları belirlendi mi?
		Güvenlik ihlal olayı sırasında kablosuz ağ bağlantısı ile yerel ağ bağlantısı arasındaki iletişiminin engellenebilmekte midir?
AGY.2.1.U9	WLAN'ların LAN'a güvenli şekilde bağlanması	WLAN ile LAN arasındaki bağlantı güvenlik yöntemleri (paket filtreleme vb.) ile güvence altına alınmış mıdır?
AGY.2.1.U10	WLAN işletimi için güvenlik politikası oluşturulması	WLAN güvenlik politikası düzenli olarak güncelleniyor mu?
		WLAN bileşenlerinin yönetiminden kimin sorumlu olduğu belirlendi mi?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U11	Uygun WLAN bileşenlerinin seçimi	WLAN bileşenlerinin tedariği için bir gereksinim listesi oluşturuldu mu?
		WLAN cihazları, kurumun WLAN güvenlik stratejisine ve mevcut donanım ve yazılım bileşenlerine uyumlu olarak seçildi mi?
		WLAN bileşenlerinin kablosuz arayüz üzerinden yönetilme özelliği devre dışı bırakılıyor mu?
		WLAN bileşenlerinin yönetiminin sadece yetkili kişiler tarafından yapılması sağlanıyor mu?
		WLAN bileşenlerinin satın alınmasından önce, gereksinimlerin karşılandığına dair testler gerçekleştiriliyor mu?
AGY.2.1.U12	Uygun WLAN yönetim aracının seçimi	Merkezi bir WLAN yönetim aracı kullanılıyor mu?
		Kablosuz ağ bileşenlerinin kayıtları merkezi bir kayıt sistemine aktarılıyor mu?
		WLAN yönetim aracı, kullanılan WLAN bileşenlerinin bellenimlerini (firmware) takip ediyor mu?
		WLAN yönetim aracı yapılandırma verilerini yedekleyerek değişikliklerin geçmişe yönelik olarak izlenebilmesini sağlıyor mu?
		WLAN yönetim aracı tanımlanan alarmları üretebiliyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U13	WLAN altyapısında rutin güvenlik kontrolleri	WLAN'lar için güvenlik gereksinimlerinin uygulandığı düzenli olarak kontrol ediliyor mu?
		Kablosuz ağların erişilebilirliği düzenli olarak kontrol ediliyor mu?
		Güvenlik ihlal olaylarının zamanında tespit edilmesi için kayıtlar düzenli aralıklarla inceleniyor mu?
		WLAN istemcilerinin yazılım durumları ve adaptör yapılandırmaları düzenli olarak kontrol ediliyor mu?
		Onay sürecinden geçmemiş WLAN bileşenlerinin veya saldırı amaçlı kurulan sahte erişim noktalarının tespiti için düzenli kontroller yapılıyor mu?
AGY.2.1.U14	WLAN bileşenlerinin rutin güvenlik denetimleri	Halka açık alanlarda kurulu olan WLAN bileşenleri görsel olarak denetleniyor mu?
		Güvenlik denetim sonuçları, anlaşılır şekilde dokümante ediliyor ve hedef durumdan sapma sebepleri inceleniyor mu?
		Güvenlik denetimlerinde uyumsuzluk ve zafiyetlerin bulunması durumunda, düzeltici faaliyetlerin gerçekleştirilmesi için kurallar tanımlanmış mıdır?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.1.U15	Kablosuz yerel ağların korunması için VPN kullanımı	Kablosuz ağlarda ilave koruma gerekiyorsa, kurum iç ağına bağlantının sadece VPN üzerinden yapılması sağlanıyor mu?
AGY.2.1.U16	WLAN'ların LAN'a bağlanması için ilave güvenlik önlemleri	WLAN'lar ile LAN arasında ilave koruma gerekiyorsa, geçiş noktasında gereksinimlere uygun güvenlik sistemleri (ör. Saldırı tespit/önleme sistemleri, güvenlik duvarı, antivirus) kullanılıyor mu?
AGY.2.1.U17	Kablosuz erişim noktaları arasındaki iletişimi koruma	Erişim noktaları arasındaki iletişim şifrelenmekte midir?
AGY.2.1.U18	Kablosuz saldırı tespit / önleme sistemlerinin kullanımı	Kablosuz ağlardaki saldırıların tespiti ve gerekli önlemlerin alınması için herhangi bir saldırı tespit/önleme sistemi (IDS/IPS) kullanılıyor mu?

TÜBİTAK BİLGEM
Yazılım Teknolojileri Araştırma Enstitüsü

Çukurambar Mah. Malcolm X Cad. No: 22 06100 Çankaya - ANKARA
T 0312 284 92 22 **F** 0312 286 52 22
E epid.yte@tubitak.gov.tr

www.yte.bilgem.tubitak.gov.tr
www.dijitaldonusum.gov.tr