TÜBİTAK
BİLGEM
YTE

DİJİTAL KABİLİYET
REHBERLERİ

KABLOSUZ AĞLARIN KULLANIMI REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Mart 2019

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Şubat 2019	İlk sürüm	TÜBİTAK BİLGEM YTE
Sürüm 2	Mart 2019	Revizyon	TÜBİTAK BİLGEM YTE

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 Kullanımı 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 Modeli ile ilgili bilgiler,
4. Bölüm'de, Kablosuz Ağların Kullanımı Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Kablosuz Ağların Kullanımı Rehberi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
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.
BT	Bilgi Teknolojileri
d-Devlet	Dijital Devlet
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme 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.

Terim / Kısaltma	Tanım
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.
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.
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
Mobilite	İstemcilerin mekândan bağımsız olarak ağa dâhil olmasını sağlayan hareket kabiliyetidir.
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.

Terim / Kısaltma	Tanım
Olgunluk 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.
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.
Problem	Bir veya birden fazla arızaya/kesintiye ilişkin kök neden olarak tanımlanan durumdur.
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
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.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Tünelleme	[Tunneling] Ağları, aradaki ağ altyapısından bağımsız olarak birleştirme yöntemi
Uygunsuzluk	Bir gereksinimin karşılanamaması durumudur.
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.

Terim / Kısaltma	Tanım
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.

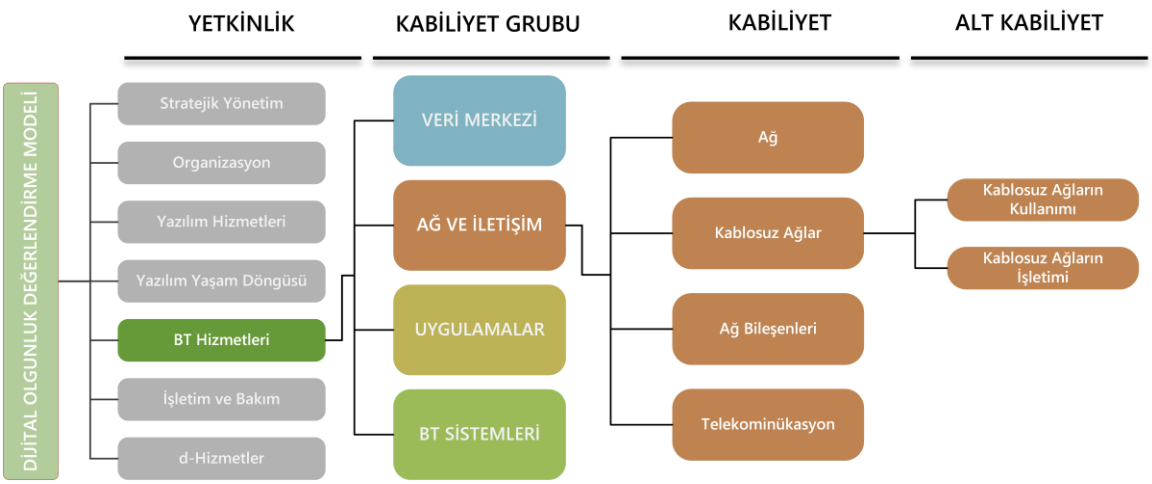
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır. 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;

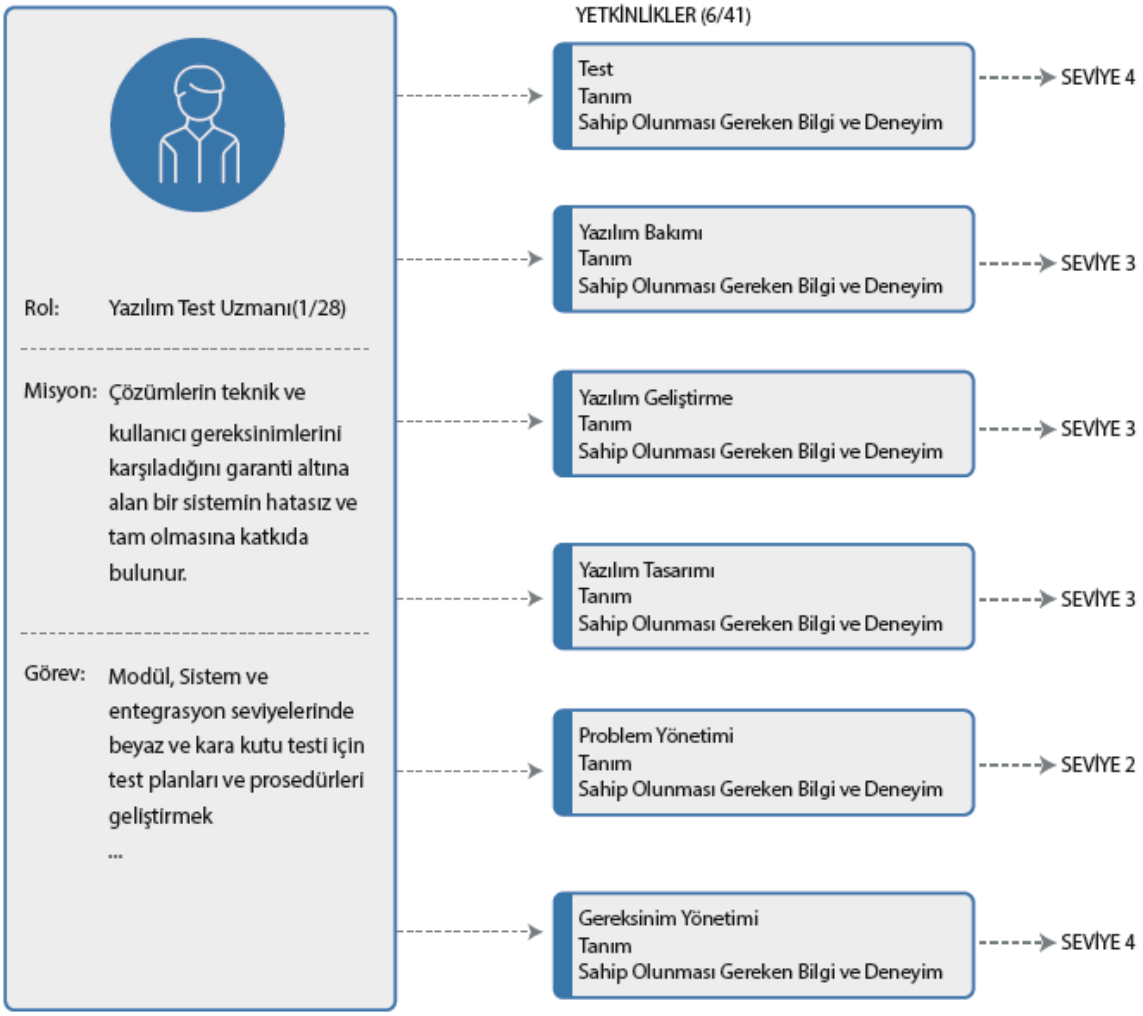
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının 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;

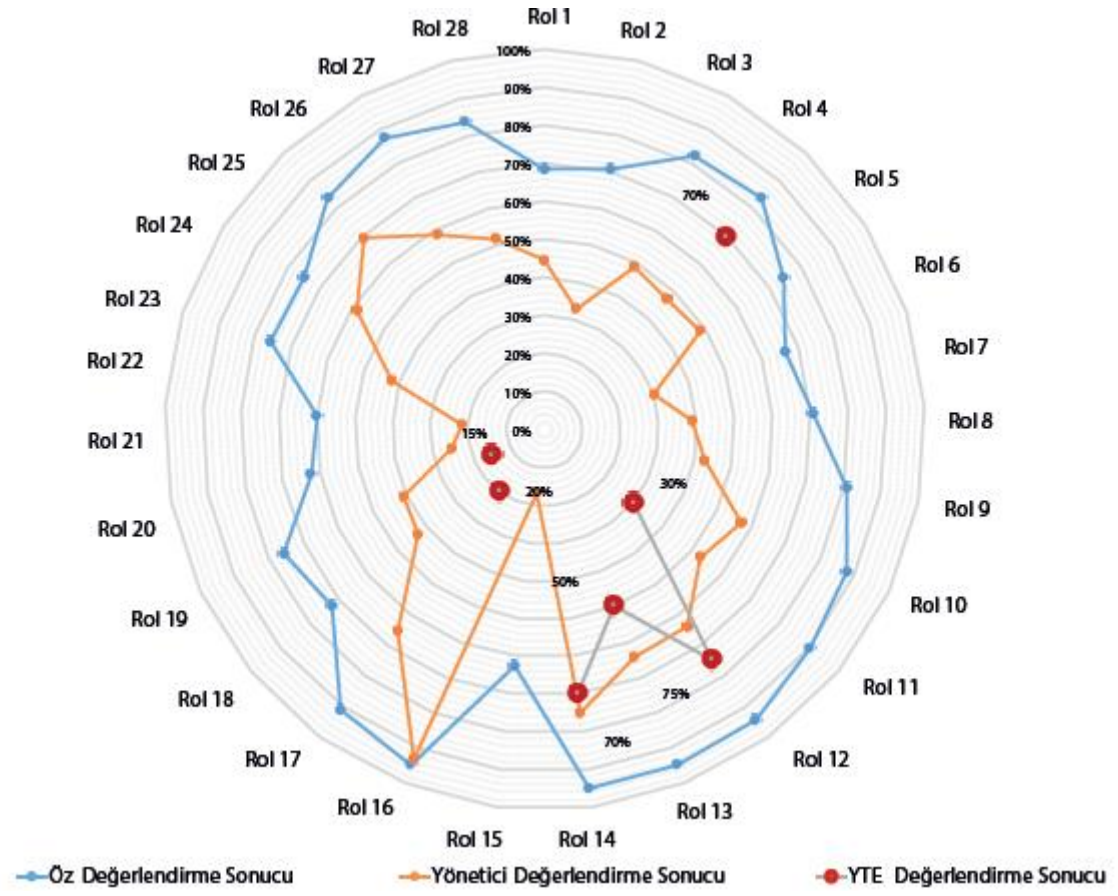
- Bilişim Üst Yönetimi,
- Proje Yönetimi,
- Ağ ve Sistem Yönetimi,
- Bilgi Güvenliği Yönetimi,
- Yazılım Teknolojileri Yönetimi,
- Bütçe ve Tedarik Yönetimi

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:



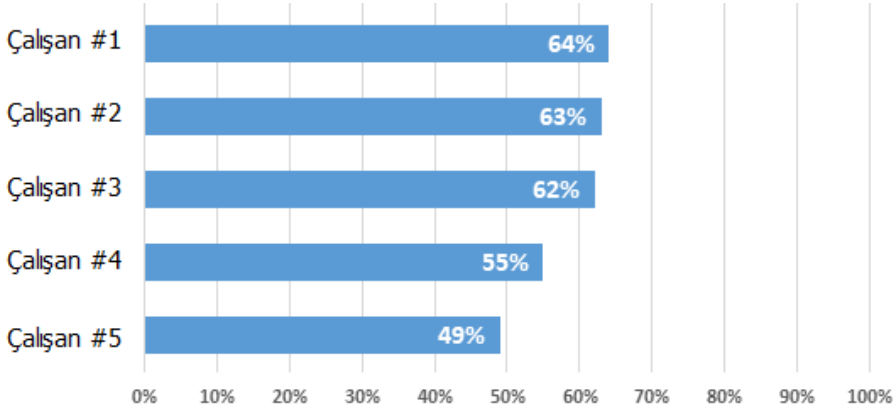
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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:



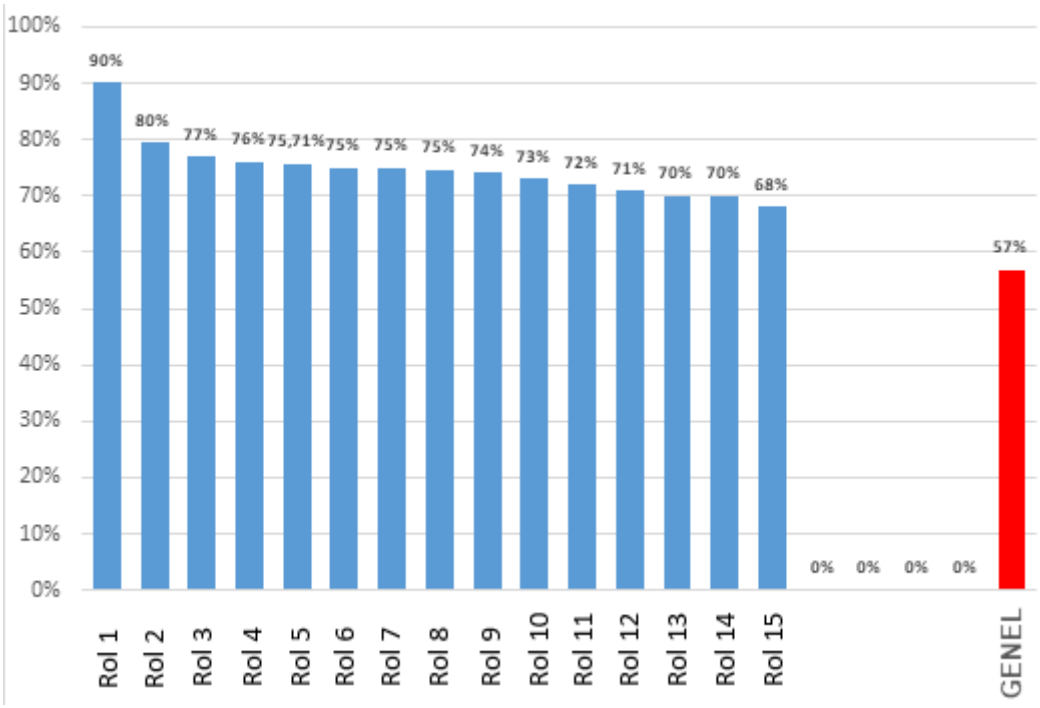
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 Kullanımı 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 Kullanımı için atanan numara (2. Alt Başlık)	1. Gereksinim maddesi
AGY	2	2	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:

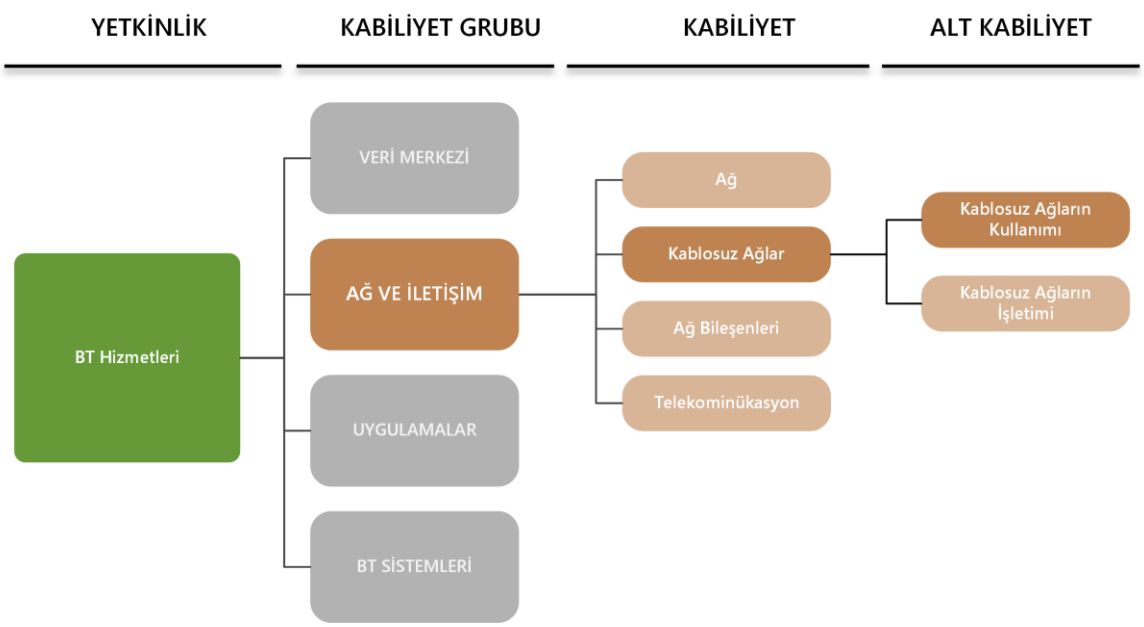
Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

- **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.2.2.G KABLOSUZ AĞLARIN KULLANIMI

TEMEL BİLEŞEN REHBERİ

AGY.2.2.G KABLOSUZ AĞLARIN KULLANIMI 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.

Kurum yöneticileri de dâhil olmak üzere tüm kullanıcılar, WLAN temelleri hakkında bilgilendirilmeli ve WLAN’ların uygun olmayan şekilde kullanıldığında ortaya çıkabilecek olası tehlikelere karşı duyarlı olmaları sağlanmalıdır. Kullanıcılar, güvenlik önlemlerinin tam olarak uygulanabilmesi için gerekli bilgiye sahip olmalıdır. Özellikle WLAN’ların kullanımı sırasında yaşanabilecek bir bilgi güvenliği ihlal olayı durumunda, kullanıcılar kendilerinden ne beklendiğinin ve ilgili duruma nasıl tepki vermeleri gerektiğinin farkında olmalıdırlar.

1.2 HEDEF

Bu rehber, WLAN’ların bir kurumda nasıl güvenli bir şekilde kullanılabileceğini anlatmayı amaçlamaktadır.

1.3 KAPSAM DIŞI

Bu rehber, belirli tehlikelere karşı koyabilmek için, WLAN’lar kullanılırken gözetilmesi ve yerine getirilmesi gereken temel gereksinimleri içerir. Bununla birlikte WLAN'ların güvenli işletim gereksinimleri AGY.2.1 rehberinde açıklanmıştır. İstemcilerin gereksinimleri "BSY.2.1 Genel İstemci" rehberinde ele alınmıştır.

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler “AGY.2.2 Kablosuz Ağların Kullanımı” açısından özellikle önemlidir.

2.1 YETERSİZ MEVZUAT BİLGİSİ

Kullanıcılar, WLAN’ların doğru kullanımıyla ilgili kurallar hakkında yeterli bilgiye sahip değilse, bunlara uymayabilirler ve bu durum risk oluşturur. Örneğin, WLAN istemcileri (dizüstü bilgisayarlar, akıllı telefonlar, tabletler vb.) yabancı ağlara bilinçsiz bir şekilde bağlanmışlarsa, bu ağ aracılığıyla iletilen bilgiler (oturum çerezleri, parolalar vb.) ele geçirilebilir.

2.2 GÜVENLİK ÖNLEMLERİNE UYULMAMASI

Kontrol eksikliği ve ihmalden dolayı kullanıcılar, güvenlik önlemlerini tam olarak dikkate almayabilirler. Örneğin, kullanıcı politikasına aykırı olmasına rağmen, bir WLAN istemcisi “Ad-Hoc” modunda kullanılıyorsa, başka bir istemci doğrudan WLAN istemcisiyle iletişim kurabilir ve istemcide saklanan belgelere yetkisiz erişim sağlayabilir.

2.3 WLAN İLETİŞİMİNİ DİNLEME

Kablosuz iletişim birçok kullanıcının paylaştığı bir ortamda sağlandığından, WLAN’lar aracılığıyla gönderilen veriler kolayca dinlenilebilmekte 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.

2.4 KABLOSUZ İLETİŞİMDE BAĞLANTI VERİLERİNİN DEĞERLENDİRİLMESİ

Kablosuz ağlarda, veri aktarımı sırasında ağ kartının MAC adresi de iletilir. Bu adres şifrelenmemiş olarak iletildiğinden, ilgili verilerin değerlendirilmesiyle kullanım profilleri oluşturulabilir. Örneğin, halka açık hotspot’lara hangi zaman diliminde bağlantı yapıldığı tespit edilebilir.

2.5 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.

3 GEREKSİNİMLER

"AGY.2.2 Kablosuz Ağların Kullanımı" 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.

Tablo 2. Kablosuz Ağların Kullanımı Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	Kullanıcı
Diğer Sorumlular	BT Operasyon Ekibi, BT Yöneticisi, Yöneticiler

3.1 1. SEVİYE GEREKSİNİMLER

Kablosuz Ağların kullanımı için aşağıda listelenen gereksinimler öncelikli olarak uygulanmalıdır.

AGY.2.2.G1 WLAN kullanıcı politikası oluşturma [BT Yöneticisi]

Güvenli WLAN kullanımı için gerekli hususlar, kurumun genel güvenlik politikası temel alınarak, WLAN kullanıcı politikasında belirtilmelidir. Bu politika, WLAN kullanım kurallarını açıklamalıdır (ör. hotspot'lar hangi şartlarda kullanılabilir).

Politikada, WLAN üzerinden hangi verilerin iletilebileceği ve hangilerinin iletilemeyeceği (özellikle gizli/hizmete özel vb. olarak sınıflandırılmış veriler) belirtilmelidir.

İstemci tarafındaki güvenlik çözümlerinin nasıl kullanılacağı anlatılmalıdır. Kullanıcı politikası, yetkisiz erişim noktalarının kurum ağına bağlanması konusunda açık bir yasaklama maddesi içermelidir. Uzun bir süre kullanılmadığı durumda WLAN arayüzünün devre dışı bırakılması gerektiği de politikada belirtilmelidir.

Politikanın doğru bir şekilde uygulanıp uygulanmadığı düzenli olarak kontrol edilmeli ve sonuçları raporlanmalıdır.

AGY.2.2.G2 WLAN kullanıcı farkındalığı ve eğitimi [Yöneticiler, BT Yöneticisi]

WLAN kullanıcıları, WLAN kullanıcı politikasında belirtilen önlemler hususunda bilinçlendirilmeli ve eğitilmelidirler. Kullanıcıların, WLAN'a özgü güvenlik ayarlarının ne

anlama geldiği ve neden önemli oldukları ve bu güvenlik ayarlarını atlatmanın veya devre dışı bırakmanın getireceği tehlikeler konusunda bilgi sahibi olmaları sağlanmalıdır.

Farkındalık eğitimi, pratikte karşılaşılması muhtemel senaryoları içermelidir. Bununla birlikte kullanıcılara, kurumun kablosuz güvenlik politikası hakkında da bilgi verilmelidir. Ayrıca kullanıcılar, yabancı WLAN'ları kullanmanın tehlikelerinden de haberdar edilmelidirler.

AGY.2.2.G3 Güvensiz ortamlarda WLAN kullanımının güvenliğini sağlama [BT Operasyon Ekibi]

Harici hotspot'ların kullanımı durumunda, aşağıdaki önlemler alınmalıdır:

- Hotspot'un her kullanıcısı, güvenlik gereksinimlerini bilmeli ve hotspot'u kullanıp kullanmayacağına ve kullanacaksa hangi koşullarda kullanacağına karar vermelidir.
- Geçici olarak kullanılmış olan WLAN'lar cihazın ayarlarından kaldırılmalıdır. Böylece cihazın istem dışı olarak WLAN'a girişi engellenebilir.
- Mümkünse, hotspot'ların kullanımı için güvenli temel yapılandırma ve kısıtlayıcı haklara sahip özel kullanıcı hesapları oluşturulmalıdır. Hiçbir koşul altında, yönetici haklarına sahip bir kullanıcı ile harici WLAN'lara giriş yapılmamalıdır.
- Hassas veriler, sadece uygun güvenlik önlemleri uygulandığında ve uygun güvenli protokoller kullanılıyorsa iletilmelidir.
- Yabancı WLAN'lar kullanılırken (ör. üçüncü taraf kurumlar veya halka açık hotspot'lar üzerinden internet erişiminin sağlandığı durumlarda), kullanıcıların kurumun iç kaynaklarına yalnızca VPN aracılığıyla erişmelerine izin verilmelidir.

3.2 2. SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, WLAN kullanımını daha iyi bir seviyeye getirmeyi düşünen kurumlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

AGY.2.2.G4 WLAN güvenlik ihlal olayları için davranış kuralları

Bir güvenlik ihlal olayı gerçekleştiğinde WLAN kullanıcıları, aşağıdakileri eylemleri gerçekleştirmelidir:

- İş amaçlı kullanılan uygulamaların verileri yedeklenmeli, WLAN erişimi durdurulmalı ve istemcinin WLAN erişim arayüzü devre dışı bırakmalıdır.

- Alınan hata mesajlarına göre istemcinin normal dışı davranışları belgelenmelidir. Ayrıca, kullanıcının güvenlik ihlal olayından önce veya güvenlik ihlal olayı sırasında ne yaptığı da dokümante edilmelidir. BT operasyon ekibi, bu bilgilerle olayın nedenini ve etkisini daha hızlı saptayabilir ve hedefe yönelik çözüm üretebilir.
- Kullanıcılar, BT operasyon ekibini uygun bir kritiklik seviyesi kullanarak bilgilendirmelidir.

3.3 3. SEVİYE GEREKSİNİMLER

Kablosuz Ağların Kullanımı Temel Bileşen içeriğinde 3. Seviye gereksinim bulunmamaktadır.

AGY: AĞ VE İLETİŞİM

AGY.2.2.U KABLOSUZ AĞLARIN KULLANIMI

UYGULAMA REHBERİ

AGY.2.2.U KABLOSUZ AĞLARIN KULLANIMI UYGULAMA

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.

Kurum yöneticileri de dâhil olmak üzere tüm kullanıcılar, WLAN temelleri hakkında bilgilendirilmeli ve WLAN’ların uygun olmayan şekilde kullanıldığında ortaya çıkabilecek olası tehlikelere karşı duyarlı olmaları sağlanmalıdır. Kullanıcılar, güvenlik önlemlerinin tam olarak uygulanabilmesi için gerekli bilgiye sahip olmalıdır. Özellikle WLAN’ların kullanımı sırasında yaşanabilecek bir bilgi güvenliği ihlal olayı durumunda, kullanıcılar kendilerinden ne beklendiğinin ve ilgili duruma nasıl tepki vermeleri gerektiğinin farkında olmalıdırlar.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

Kablosuz ağların işletimi ve kullanımı öncesinde detaylı bir planlama yapılması gereklidir. Son kullanıcıya WLAN kullanımı ile ilgili olmayan detayların verilmemesi için, WLAN politikasına ek olarak kullanıcılara özel bir WLAN politikası oluşturulmalıdır (bkz. “AGY.2.2.U1 WLAN kullanıcı politikası oluşturulması”).

Uygulama

WLAN’ların kullanımında kurumun güvenlik gereksinimlerinin karşılanabilmesi için, kullanıcıların sürece dâhil edilmesi gerekir. Kullanıcılar, tek başına teknik araçlar ile uygulanamayan ve kendilerinin katılımını gerektiren güvenlik önlemleri hakkında bilgilendirilmelidir. WLAN’ların uygun olmayan bir şekilde kullanılması durumunda ortaya çıkabilecek olası tehlikelere dikkat çekmek ve güvenlik ihlal olaylarını en aza indirmek için eğitimler düzenlenmeli ve kullanıcıların farkındalığı artırılmalıdır (bkz. “AGY.2.2.U2 WLAN kullanıcı farkındalığı ve eğitimi”).

İşletim

Harici hotspot'lar kullanılacaksa, kullanıcılar hotspot'ların kullanımı ve uygun önlemlerin alınması konusunda özel olarak eğitilmelidir (bkz. "AGY.2.2.U3 Güvensiz ortamlarda WLAN kullanımının güvenliğini sağlama").

Acil Durum Hazırlık Planı

Kullanıcıların WLAN'a yönelik içeriden veya dışarıdan bir saldırı durumunda, nasıl davranacakları hakkında bilgi sahibi olmaları gerekmektedir (bkz. "AGY.2.2.U4 WLAN güvenlik ihlal olayları için davranış kuralları").

2 UYGULAMALAR

Aşağıda yer alan maddeler, “Kablosuz Ağların Kullanımı” rehberine özel uygulama maddeleridir.

2.1 1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

AGY.2.2.U1 WLAN kullanıcı politikası oluşturulması [BT Yönetimi]

WLAN altyapısının işletim ve güvenlik detaylarıyla ilgili kullanıcılara gereksiz bilgi vermemek için, kullanıcılara özel bir WLAN politikası oluşturulmalıdır. Kullanıcı politikası, kurumun genel güvenlik politikasını temel almalı ve WLAN’ın güvenli olduğundan emin olunması için gerekli tüm hususları içermelidir. Bu şekilde oluşturulmuş bir kullanıcı politikasında, WLAN kullanımına dair aşağıdaki hususlara yer verilmelidir:

- WLAN istemcilerinin hangi dâhili ve harici ağlara bağlanabileceği,
- Dâhili ve harici WLAN’lara hangi şartlarda giriş yapılmasına izin verildiği,
- Hotspot’ların kullanılıp kullanılamayacağı ve hangi şartlarda kullanılabileceği,
- Diğer istemcilerin WLAN istemcilerine doğrudan erişimini engellemek için Ad-Hoc modunun kapatılması gerektiği,
- WLAN istemcilerinde güvenlik ihlali olayı veya ihlal şüphesi olduğunda, öncelikli olarak kimin haberdar edileceği,

Kullanıcı politikasında, istemci tarafı ile ilgili güvenlik yapılandırmalarına dair hususların da açıkça belirtilmesi önemlidir. Örneğin;

- Güvenlikle ilgili yapılandırmalar değiştirilmemelidir,
- Mevcut güvenlik duvarı kapatılmamalıdır,
- Tüm dizin veya hizmet paylaşımları devre dışı bırakılmalı veya en azından güçlü parolalarla korunmalıdır,
- Harici WLAN’ların kullanımında, mümkünse kısıtlayıcı haklara sahip olan özel kullanıcı hesapları kullanılmalıdır.

Kullanıcı politikası, yetkisiz erişim noktalarının kurum ağına bağlanmaması için açık bir yasaklama maddesi içermelidir. Ayrıca, uzun bir süre kullanılmadığı durumda WLAN arayüzünün devre dışı bırakılması gerektiği de politikada belirtilmelidir. WLAN üzerinden hangi verilerin iletilebileceği ve hangilerinin iletilemeyeceği (özellikle gizli/hizmete özel vb. olarak sınıflandırılmış veriler) politika içerisinde açıkça tanımlanmalıdır. Kullanıcılar, WLAN tehditlerinin yanı sıra WLAN politikasının içeriği ve etkileri konusunda da bilgilendirilmelidir.

Politikanın doğru bir şekilde uygulanıp uygulanmadığı düzenli olarak kontrol edilmeli ve sonuçları raporlanmalıdır.

AGY.2.2.U2 WLAN kullanıcı farkındalığı ve eğitimi [Denetçiler, BT Yönetimi]

Günümüzde neredeyse her bir kurum çalışanı bir mobil cihaza sahiptir ve mobil cihazı aracılığı ile halka açık veya kurum içi bir WLAN'a bağlanabilir. Mobil cihazlar (ör. akıllı telefonlar) başkaları için hotspot'lar oluşturmak veya Ad-Hoc WLAN'lar kurmak için de kullanılabilir. Bu şekildeki kullanımlar, cihazlar yanlış yapılandırıldığında güvenlik sorunlarına yol açabilir. Bu nedenle, tüm çalışanların, özellikle de gizli bilgilere erişen kullanıcıların, mobil cihazlar aracılığı ile WLAN kullanımı konusundaki farkındalıkları artırılmalıdır. Örneğin, WLAN'ların kullanımındaki olası tehlikeler hakkında bilgi veren bir broşür vasıtasıyla bu gerçekleştirilebilir. Broşür, bu tür tehlikelere karşı koymak için ilgili önlemleri ve davranışları içermelidir. Bu broşür, cihazlarla birlikte teslim edilerek kullanıcıların mobil cihazları bilinçli bir şekilde kullanmasına yardımcı olmalıdır. Kullanıcıların, cihazlarını bir hotspot olarak kullanmalarına izin veriliyor ise, ilgili tehlikeler ve önlemler de broşür içeriğine eklenmelidir. Örneğin, WLAN iletişiminin karmaşık bir parola kullanılarak korunabileceği belirtilebilir.

Halka açık kablosuz ağların (hotspot'ların) kullanımında öncelikli amaç kullanıcıların kolay erişim sağlaması olduğu için, hotspot'larda ya hiçbir güvenlik mekanizması yapılandırılmamakta ya da zayıf güvenlik mekanizmaları kullanılmaktadır. Bu nedenle, iletilen bilgiler kötü niyetli kişiler tarafından kolayca ele geçirilebilmektedir. Hotspot'lar, kuruma bağlantı yapılması için kullanılacaksa veya bu bağlantı ile gizli bilgiler iletilecekse, kullanıcılar hotspot'ların kullanımı konusunda özel olarak eğitilmeli ve kullanıcıların uygun önlemleri almaları sağlanmalıdır. Örneğin, kullanıcılar tüm bağlantıların düzgün bir şekilde şifrelenmiş olduğundan emin olmalıdır. Kurumun bir parçası olmayan BT sistemlerine yönlendirilme şüphesi veya alınan herhangi şüpheli bir uyarı mesajı, bir güvenlik ihlali olarak değerlendirilmelidir.

Her kullanıcı, WLAN kullanımının kullanıcıya mobilite esnekliği sağladığını bilmeli ancak saldırganlar görüş alanının dışında da olabilecekleri için, bu durumun riskler de içerdiğinin farkında olmalıdır.

AGY.2.2.U3 Güvensiz ortamlarda WLAN kullanımının güvenliğini sağlama [BT Operasyon Ekibi]

Hotspot'lar sınırlı bir alanı kapsarlar. Çoğu hotspot, yabancı katılımcıların kullanımı için özel olarak oluşturulmuştur. Ana amaçları internete kablosuz erişimi sağlamaktır. Genellikle oteller, havaalanları, sergi salonları, tren istasyonları ve kongre merkezleri gibi kamusal alanlarda bu tür hotspot'lar bulunmaktadır.

Mevcut güvenlik seviyelerinin bilinmemesinden ve paylaşılan bir ağ olmalarından dolayı hotspot'lar her zaman güvenli olmayan ağlar olarak görülmelidir. Hotspot'lar kullanılırken, genellikle her bir istemciden ağdaki diğer bir istemciye erişmek mümkündür. Bir hotspot kullanımından kaynaklanan risk tahmin edilemezse, WLAN güvenlik yönergesiyle hotspot kullanımı tamamen yasaklanabilir.

Hotspot'lar üzerinde alınan güvenlik önlemleri kullanıcıların işbirliği olmadan tek başına yeterli değildir. Hotspot'ların kullanımı durumunda aşağıdaki önlemler alınmalıdır:

- Hotspot'un her kullanıcısı, güvenlik gereksinimlerini bilmeli ve hotspot'u kullanıp kullanmayacağına ve kullanacaksa hangi koşullarda kullanacağına karar vermelidir.
- Hotspot'ta kayıt işlemi, genellikle bir web portali üzerinden veya bir web uygulaması aracılığı ile yapılır. Kayıt için kullanılan yöntem kullanıcı bilgilerini korumalıdır. Kimlik doğrulama bilgileri her zaman şifreli kanaldan iletilmelidir.
- Geçici olarak kullanılmış olan WLAN'lar cihazın ayarlarından kaldırılmalıdır. Böylece cihazın istem dışı olarak WLAN'a girişi engellenebilir.
- Mümkünse, hotspot'ların kullanımı için güvenli temel yapılandırma ve kısıtlayıcı haklara sahip özel kullanıcı hesapları oluşturulmalıdır. Hiçbir koşul altında, yönetici haklarına sahip bir kullanıcı ile harici WLAN'lara giriş yapılmamalıdır.
- Kredi kartı numaraları, PIN'ler, şifreler veya e-postalar gibi mali, kişisel veya diğer hassas verilerin iletilmesi gerektiğinde, cihazlar üzerinde, özellikle şifreleme hususunda gerekli olan tüm güvenlik önlemlerinin etkinleştirilmesi sağlanmalıdır. Örneğin, e-posta hizmetine bir HTTPS web arayüzü üzerinden güvenli bir şekilde erişilmelidir. Gizli bilgiler yabancı ağlar üzerinden asla şifrelenmemiş olarak iletilmemelidir.
- Yabancı WLAN'lar kullanılırken (ör. üçüncü taraf kurumlar veya halka açık hotspot'lar üzerinden internet erişiminin sağlandığı durumlarda), kullanıcıların kurumun iç kaynaklarına yalnızca VPN aracılığıyla erişmelerine izin verilmelidir. Bu şekilde, kişinin kendi kurumu ile bağlantısı, kullanılan WLAN altyapısının koruma mekanizmalarından bağımsız olarak güvence altına alınabilir.

2.2 2. SEVİYE UYGULAMALAR

1.seviye gereksinimler sonrasında, WLAN kullanımını daha iyi bir seviyeye getirmeyi düşünen kurumlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

AGY.2.2.U4 WLAN güvenlik ihlal olayları için davranış kuralları

WLAN kullanımındaki beklenilmeyen durumlar (ör. uzun bir süre boyunca WLAN bağlantısı sağlanamıyorsa, ağ sürekli olarak kesiliyorsa) bir güvenlik ihlal olayından kaynaklanmış olabilir.

Bir güvenlik ihlal olayı gerçekleştiğinde WLAN kullanıcıları, aşağıdakileri eylemleri gerçekleştirmelidir:

- İş amaçlı kullanılan uygulamaların verileri yedeklenmeli, WLAN erişimi durdurulmalı ve istemcinin WLAN erişim arayüzü devre dışı bırakmalıdır.
- Alınan hata mesajlarına göre istemcinin normal dışı davranışları belgelenmelidir. Ayrıca, kullanıcının güvenlik ihlal olayından önce veya güvenlik ihlal olayı sırasında ne yaptığı da dokümante edilmelidir. BT Operasyon Ekibi, bu bilgilerle olayın nedenini ve etkisini daha hızlı saptayabilir ve hedefe yönelik çözüm üretebilir.
- Kullanıcılar, BT Operasyon Ekibini uygun bir kritiklik seviyesi kullanarak bilgilendirmelidir.

2.3 3. SEVİYE UYGULAMALAR

Kablosuz Ağların Kullanımı Uygulama içeriğinde 3. Seviye uygulama bulunmamaktadır.

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.2.2.U1	WLAN kullanıcı politikası oluşturulması	WLAN kullanımı için ayrı bir güvenlik politikası oluşturuldu mu?
		WLAN kullanım koşulları kullanıcıya onaylatılıyor mu?
		WLAN kullanıcı politikasında, kurum dışı kablosuz ağlara bağlanma kurallarına yer veriliyor mu?
		WLAN kullanıcı politikasında, hotspotlara bağlanma kurallarına yer veriliyor mu?
		WLAN kullanıcı politikasında, istemcilerde Ad-Hoc modunun devre dışı bırakılmasına yer veriliyor mu?
AGY.2.2.U2	WLAN kullanıcı farkındalığı ve eğitimi	Kullanıcılara WLAN'da oluşabilecek güvenlik risklerini ve alınması gereken güvenlik önlemlerini içeren farkındalık eğitimi veriliyor mu?
		Eğitimde, hotspot kullanımında oluşabilecek güvenlik riskleri ve alınması gereken güvenlik önlemleri özellikle vurgulanıyor mu?
AGY.2.2.U3	Güvensiz ortamlarda WLAN kullanımının güvenliğini sağlama	Yönetici yetkisine sahip kullanıcı hesapları ile hotspotlara bağlantı yapılması engelleniyor mu?
AGY.2.2.U4	WLAN güvenlik ihlal olayları için davranış kuralları	WLAN kullanıcıları için güvenlik ihlal olayları sırasındaki davranış kuralları ve önlemler belirlenmiş midir?

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