TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

ALAN ADI (DOMAIN) SİSTEM YÖNETİMİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Temmuz 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Temmuz 2020	İlk sürüm	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.

Model 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 2834 soru belirlenmiştir.

Model'in 8 kurumda 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 İşletimi Rehberi**, **Kablosuz Ağların Yönetimi Rehberi**, **Aktif Dizin Yönetimi Rehberi**, **Sunucu Yönetimi Rehberi ve İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılı içerisinde bunlara ek olarak **Uzaktan Çalışma Rehberi**, **VOIP Rehberi ve Alan Adı Sistem Yönetimi Rehberi** yayınlanmıştır.

Dijital Devlet ekosistemi paydaşlarının değerlendirmesine yönelik tüm **Rehberlerin** **www.dijitalakademi.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. 38 bilişim profesyonel rolü ile bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller, yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. 6 kurumda yaklaşık 550 uzman için yetkinlik değerlendirmeleri yapılmış ve kurumların dijital kapasitelerinin geliştirilmesi için öneriler geliştirilmiştir.

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

1 GİRİŞ

Alan Adı Sistem Yönetimi 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, Alan Adı Sistem Yönetimi Rehberi'nin gerekçesi, yapısı, kapsamı ve ilgili çalışmalar,
5. Bölüm'de, Alan Adı Sistem Yönetimi kapsamında tanımlanan kabiliyetlere ilişkin yönlendirici bilgiler

sunulmaktadır.

TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Ana bilgisayar adı	[Hostname] Network üzerinde bulunan ana bilgisayarların DNS isim karşılığına denir.
Arındırılmış bölge	[DMZ: demilitarized zone] İnternet üzerinden erişilebilir sunucuların konumlandırıldığı, iç ağdan ayrıştırılmış bölge
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
BT	Bilgi Teknolojileri
Caching only DNS-sunucusu	[Caching-Only DNS-Server] DNS sunucular, üzerlerinde herhangi bir alan adına ait kayıt tutmaksızın, istemcilerden gelen sorguların cevaplarını ilgili isim sunucularından alarak istemciye sunmasıdır.
d-Devlet	Dijital Devlet
DNS	[Domain Name System] TCP/IP ağlarda kullanılan isim çözümleme protokolüdür.
DNS bölge transferi	[DNS Zone Transfer], DNS sunucusunda bulunan zone kayıtlarının, başka bir DNS sunucusuna aktarılması işlemidir.

Terim / Kısaltma	Tanım
Domain	Etki Alanı. Aynı dizin veritabanını paylaşan objeler bütünüdür.
DOS saldırısı	[Denial of Servise] İnternete bağlı bir host'un hizmetlerini geçici veya süresiz olarak aksatarak, bir makinenin veya ağ kaynaklarının asıl kullanıcılar tarafından ulaşılamamasını hedefleyen bir siber saldırıdır.
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
FQDN	[Fully Qualified Domain Name] Alan Adı sisteminde bir alan adının tamamıdır.
Hash	Herhangi bir metnin şifrelenerek, okunamaz veya önceden tahmin edilemez hale getirilmesi algoritması ve işlemidir.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (örn.Örnek: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)
IP sahteciliği	[IP Spoofing] Alan Adı Sistemi verisini bozarak, DNS çözümleme önbelleğine bozuk verinin yerleştirildiği bir tür siber saldırıdır.
Yönlendirici	[Forwarder] DNS sunucular, üzerlerinde herhangi bir alan adına ait kayıt tutmaksızın, istemcilerden gelen sorguların cevaplarını ilgili isim sunucularından alarak istemciye sunmasıdır.
İsim çözümlemesi	[Name Resolution] Ana bilgisayar adlarına, hesap kullanıcı adlarına, grup adlarına ve diğer varlıklara karşılık gelen sayısal değerlerin çözümlenmesidir
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanma durumudur.
Kısa süreli anahtar	[ZSK: Zone Signing Key] Zone'da barındırılan bağımsız kayıtları imzalamak için kullanılır.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu

Terim / Kısaltma	Tanım
	hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.
NS	[Name Server] Alan adının sorgulanmasında kullanılan ad sunucularıdır.
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
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.
Özet tabanlı mesaj doğrulama kodu	[Keyed-Hash Message Authentication Code] Kriptografide, özet tabanlı mesaj doğrulama kodu, kriptografik özet fonksiyonu ve gizli bir kriptografik anahtar içeren bir mesaj doğrulama kodu türüdür. Diğer MAC türleri gibi, HMAC de hem veri bütünlüğünü kontrol etmek hem de mesaj içeriğini onaylamakta kullanılabilir
Özyinelemeli sorgu	[Recursive Query] İstemcinin, ağ üzerinde herhangi bir kaynağa ya da internet sitesine bağlanmak için ip adresini DNS sunucusuna sorarken yaptığı sorgudur.
Problem	Bir veya birden fazla arızaya/kesintiye ilişkin kök neden olarak tanımlanan durumdur.
Risk	Bir faaliyetin içerdiği belirsizlik ve zarar olasılığıdır.
STK	Sivil Toplum Kuruluşu
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme
Tekrarlamalı sorgu	[Iterative Query] DNS sunucuların kendi aralarında yaptıkları sorgulara tekrarlamalı sorgu denir.
TSIG	[Transaction Signatures] Alan transferi sırasında iki sunucunun birbirleriyle konuştuklarının sağlanması ve simetrik şifreleme yöntemiyle imkan tanınmasıdır.

Terim / Kısaltma	Tanım
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Uzun süreli anahtar	[KSK: Key Signing Key] Zone root'da tüm DNSKEY kayıtlarının imzalanması için kullanılır.
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

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 Değerlendirme 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, On Birinci Kalkınma Planı'nda "Kamu Hizmetlerinde e-Devlet Uygulamaları" başlığı altında yer alan aşağıdaki politika ve tedbirler ile desteklenmektedir:

- "811.2. Kamu kurumlarının bilişim projeleri hazırlama ve yönetme kapasitelerinin artırılmasına yönelik eğitimler verilecek ve rehberler hazırlanacaktır."
- "814.2. Kamu kurumlarında bilgi güvenliği yönetim sistemi kurulması ve denetlenmesine yönelik usul ve esaslar belirlenecek, hazırlanacak rehberlerle bu konuda kamu kurumlarına yol gösterilecektir."
- "811.3. Kurumsal olgunluk ve insan kaynağı yetkinlik modelleri geliştirilerek kamu kurumlarında yaygınlaştırılacaktır."

2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı'nda doğrudan rehberlik mekanizmalarına yönelik tanımlanan aşağıdaki eylemlere de bu proje ile 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 **Rehberler** 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.

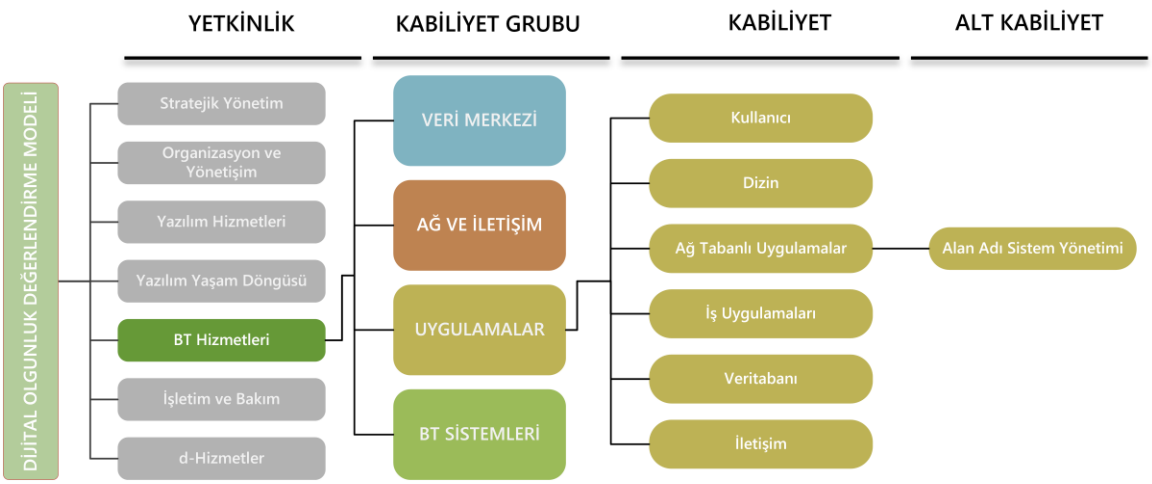
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır.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



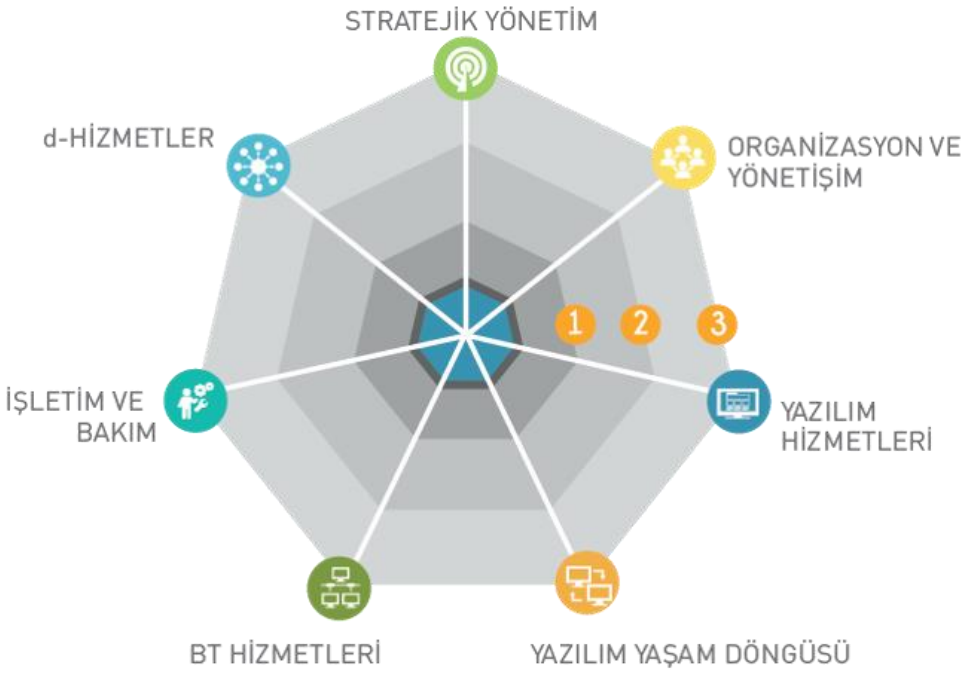
Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

Dijital Olgunluk Değerlendirme Modeli 7 yetkinlik altında tanımlanmış 35 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 yönetimi, kurumsal mimari yönetimi, dijital dönüşüm yönetimi ve bütçe yönetimi kabiliyet gruplarını içermektedir.

2. Yetkinlik: ORGANİZASYON VE YÖNETİŞİM

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, dijital kapasite geliştirme ve dijital yönetişim 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, gereksinim mühendisliği, teknik çözüm, doğrulama ve geçerleme, konfigürasyon yönetimi ve kalite güvence kabiliyet gruplarını içermektedir.

5. Yetkinlik: BT HİZMETLERİ

Kurumun sahip olduğu teknolojiler ile mevcut donanım ve altyapıların yönetilmesini kapsar. Bu yetkinlik, ağ ve iletişim, veri merkezi, uygulamalar ve BT sistemleri 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, 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;

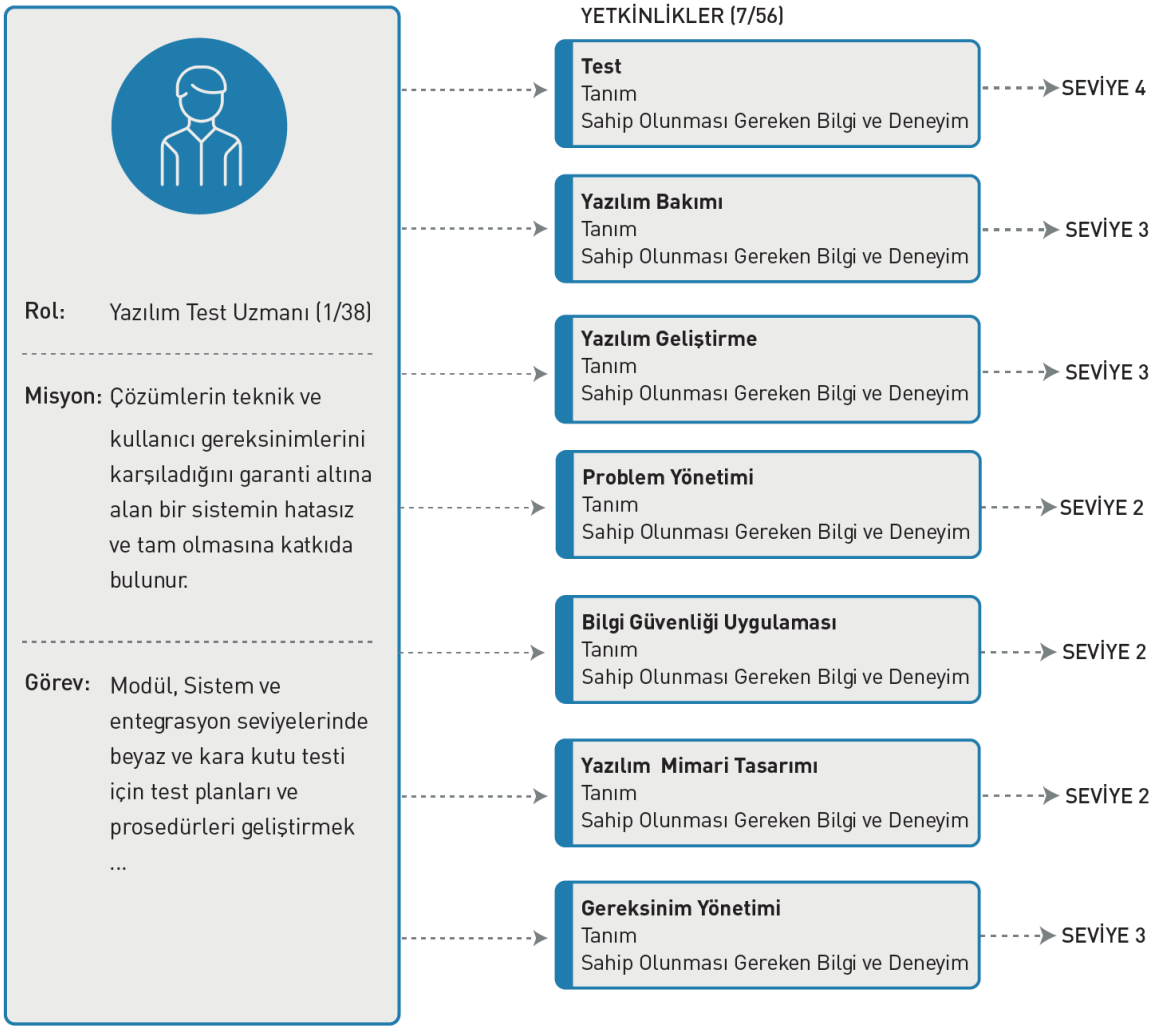
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının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

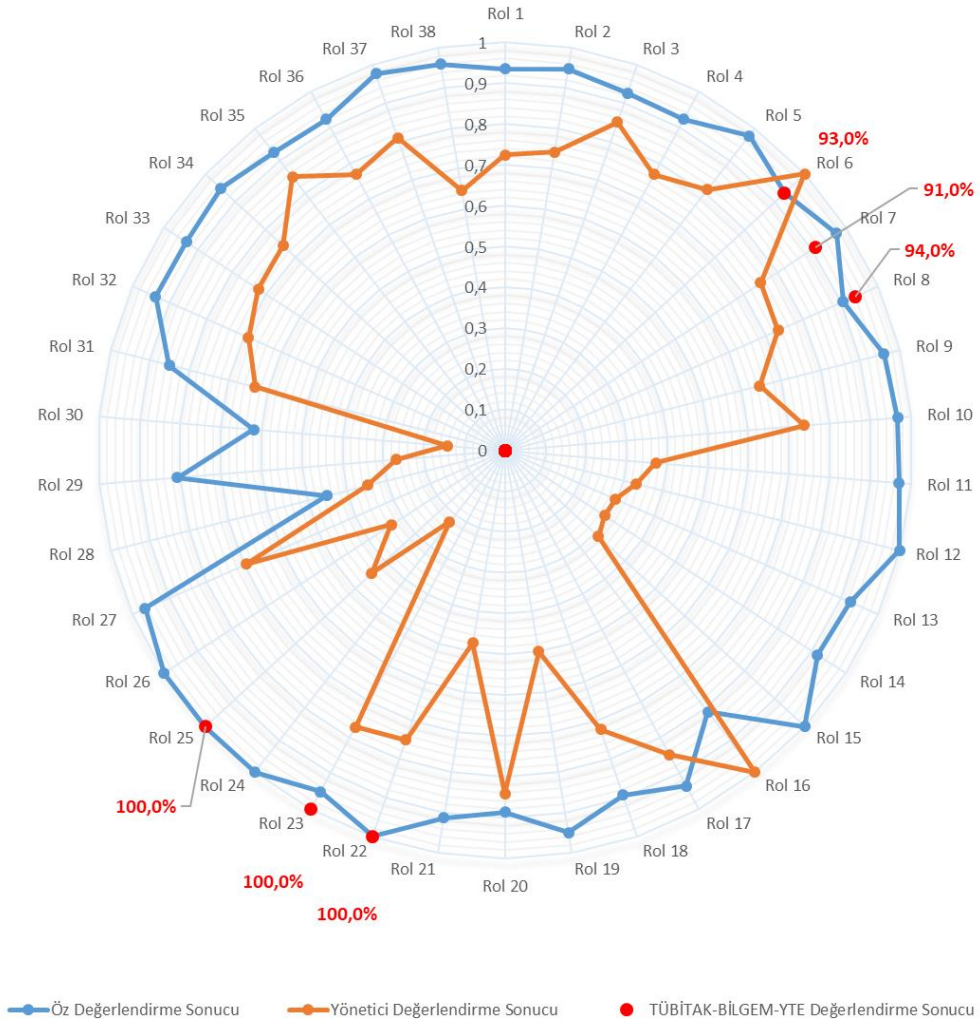
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

alanlarında Türkiye'deki organizasyon yapılarına özgü 38 bilişim profesyonel rolü tanımlanmıştır: Ayrıca, bu rollerdeki çalışanların sahip olması hedeflenen 56 yetkinlik ve yetkinlik için 5 kademeli seviye tanımlanmış olup, roller; yetkinlik alanları ve yetkinlik seviyeleri arasındaki ilişkiler belirlenmiştir. Bunun için bir örnek aşağıdaki gibidir:



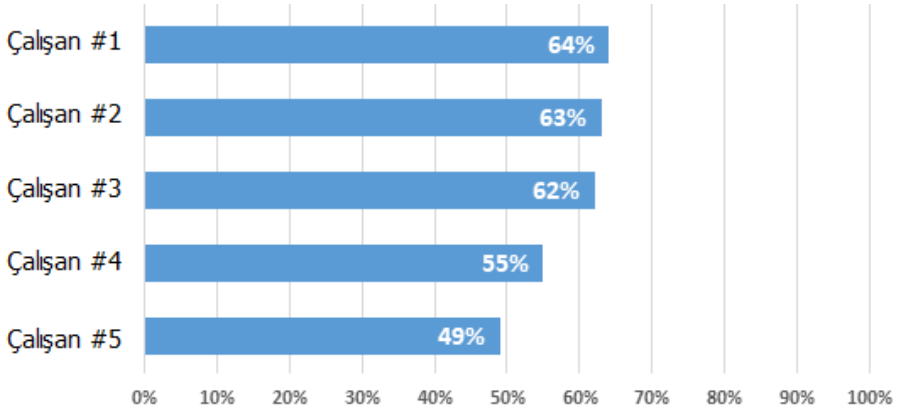
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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 38 rol bazında uygunluğu raporlanmaktadır:



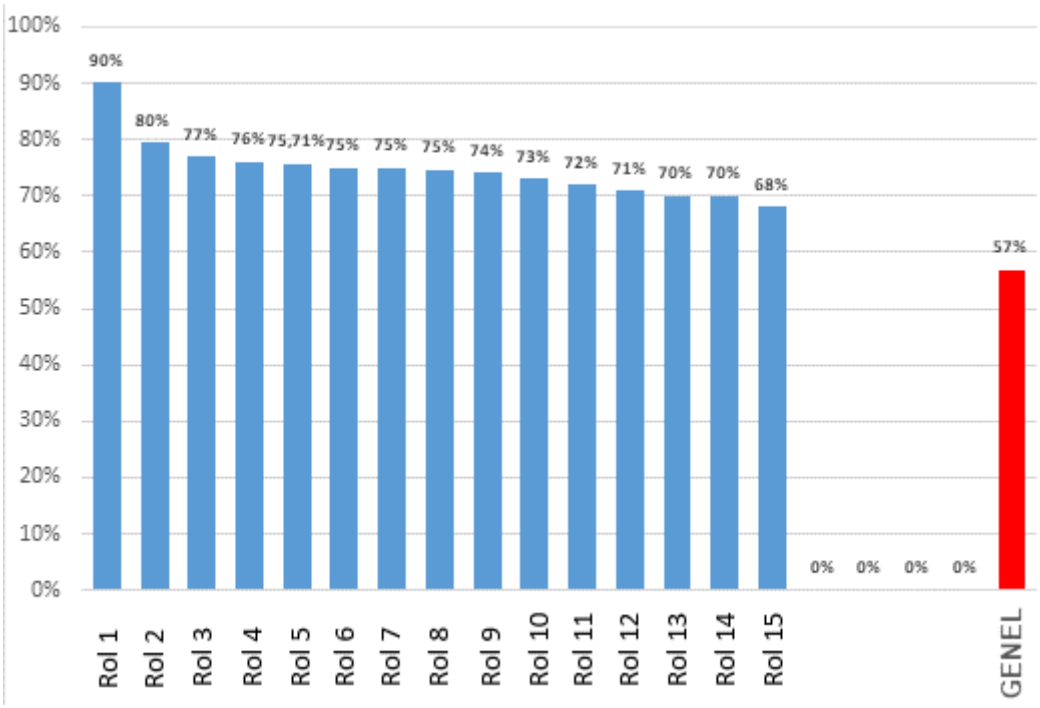
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 **Alan Adı Sistem Yönetimi 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 **Rehber'de** 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 **Rehber'in** 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 UYG.3.6.G1 DNS dağıtım planı'nın kod tanımı aşağıdaki şekildedir:

Tablo 1 Örnek Kod Tanımı

"Uygulamalar" kabiliyet grubu için kullanılan kısaltma	"Ağ Tabanlı Uygulamalar" kabiliyeti için atanan numara	"Alan Adı Sistemi" alt kabiliyeti için atanan numara	1. Gereksinim maddesi
UYG	3	6	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberlerinde ise yalnız "G" harfi yerine "U" harfi kullanılmıştır. Örneğin, UYG.3.6.G1 DNS dağıtım planı gereksinim maddesinin karşılığı UYG.3.6.U1 DNS dağıtım planı 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.

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

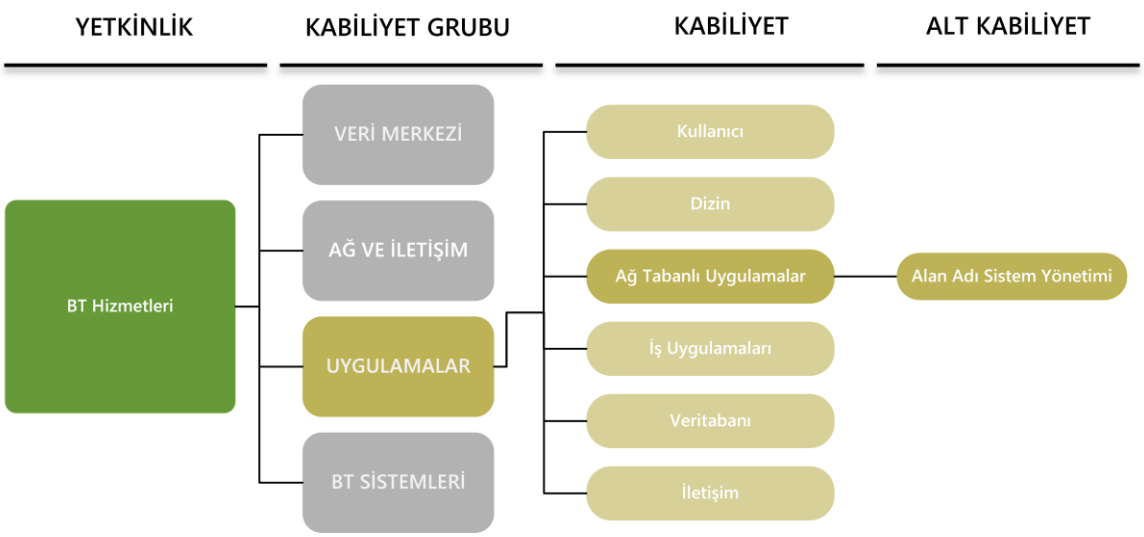
içermektedir.

- 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:
  - Kullanıcı
    - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan ofis uygulamalarını, web tarayıcılarını ve/veya mobil uygulamalarını içerir.
  - Dizin
    - Kurum veya organizasyonda kullanılan dizin hizmetine (Active Directory, OpenLDAP vs.) özel kabiliyetleri kapsar.
  - Ağ Tabanlı Uygulamalar
    - BT sistemlerinde kullanılan web hizmetleri (ör. İntranet veya internet), web sunucusu, dosya paylaşımı, DNS hizmetleri gibi kabiliyetleri kapsar.
  - İş Uygulamaları
    - Kurum veya organizasyon genelinde, kurumsal kaynakların yönetimi için iş birimleri tarafından kullanılan uygulamalara özel kabiliyetleri içerir.
  - Veritabanı
    - Belli bir amaca yönelik düzenli, büyük miktarda veriyi depolayabilen, bu verilerin hızlı bir şekilde yönetilip değiştirilebilmesine ve raporlanmasına imkan sağlayan ilişkisel veya ilişkisel olmayan veritabanı uygulamalarına dair kabiliyetleri içerir.
  - İletişim Uygulamaları
    - Organizasyon genelinde, çalışanların iletişim amaçlı kullandıkları uygulamalara dair kabiliyetleri kapsar.

- **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

UYG: UYGULAMALAR

UYG.3.6.G ALAN ADI SİSTEM YÖNETİMİ

TEMEL BİLEŞEN REHBERİ

UYG.3.6.G ALAN ADI SİSTEM YÖNETİMİ
TEMEL BİLEŞEN

1 AÇIKLAMA

TANIM

DNS adlandırma sistemi, internet veya özel bir ağa bağlı herhangi bir kaynak adının IP adreslerini çözmek için (örn. web tarayıcının adres çubuğuna yazılan adresinin sayısal IP adreslerine dönüştürülmesi) kullanılan ağ hizmetini ifade eder. Ana bilgisayar (Host) alan adına karşılık gelen IP adresi, DNS üzerinden aranır. IP adresi bilinen ve ana bilgisayar adı aranan durumlarda ise ters DNS sorgulama veya ters DNS çözümleme tespiti yapılır. Kısa adıyla DNS, telefon rehberine benzetilebilir. Alan adlarının hangi IP adreslerine ait olduğu ad alanından (domain name space) yönetilir. Bu alanlar, hiyerarşik olarak yapılandırılmış ve DNS sunucuları tarafından kullanıma hazır sunulmuştur.

DNS sunucuları, internet üzerindeki ad alanını yönetmekle sorumludur. Fakat aynı zamanda bir kurumun iç ağında da kullanılır. Kurumun iç ağında bulunan BT sistem kullanıcılarına standart olarak çözümleyiciler (Resolver) yüklenir. Bunlar üzerinden DNS sunucuya sorgular yapılır ve alan adı üzerinden istenilen sorgu yanıtları bu şekilde dönülmüş olur.

DNS sunucu terimi, aslında kullanılan yazılımı ifade eder ve genellikle yazılımın üzerinde çalıştığı BT sistemi ile eşanlamlı olarak da kullanılır.

DNS sunucuları, görevlerine göre temelde Advertising DNS sunucusu ve Resolving DNS sunucusu olarak ikiye ayrılırlar. Advertising DNS sunucuları genellikle internetten gelen taleplerin karşılanmasından sorumludur. Buna karşın, Resolving DNS sunucuları iç ağdan gelen istekleri işler.

DNS sunucularının arızalanması, DNS tabanlı hizmetlerin kısıtlanmasına yol açacağından BT hizmetlerinin düzgün bir şekilde verilebilmesini ciddi şekilde etkileyebilir. Bu sorun ile örneğin, web ve e-posta sunucularına erişilemez. DNS hizmeti, birçok ağ uygulaması tarafından kullanıldığı için RFC 1034 standardına göre, en az iki yetkili ad sunucusundan oluşan bir mimaride kullanılması önerilmektedir.

HEDEF

Bu rehber, DNS sunucusunun bir kurumda nasıl güvenli bir şekilde kurulabileceğini ve işletilebileceğini anlatmayı amaçlamaktadır.

KAPSAM DIŞI

Bu bileşen rehberi, BT sistemlerinde kullanılan her DNS sunucusunda veya her DNS sunucusu grubunda uygulanabilir.

DNS sunucuları kullanan kurum ve organizasyonların uyması ve yerine getirmesi gereken temel gereksinimler, bu hizmet rehberinde sunulmaktadır. Ayrıca rehberin odak noktası, DNS sunucularının erişilebilirliği, iletilen bilgilerin bütünlüğü ve DNS sunucularının işletiminde ortaya çıkabilecek sorunlardır. Sunucu işletim sistemine ve/veya yazılımına özgü yönler, bu modülün konuları içerinde yer almamaktadır. Bunlar, BTS.1.1 Genel Sunucu rehberinde ve BT sistemleri kabiliyet grubunda bulunan ilgili işletim sistemine özgü rehberlerde ele alınır.

2 RİSK KAYNAKLARI

Aşağıdaki riskler ve eksiklikler “UYG.3.6 Alan Adı Sistem Yönetimi” açısından özellikle önemlidir.

2. 1 DNS SUNUCUSUNUN ARIZALANMASI

DNS sunucularının arızalanması, DNS tabanlı hizmetlerin kısıtlanmasına ve BT hizmetlerinin düzgün bir şekilde verilememesine yol açar. DNS sunucusunun aksaması durumlarında; istemciler ve diğer sunucular ana bilgisayar adlarına dayalı olarak iç ve dış adresleri çözümleyemediğinden, veri bağlantıları artık kurulamaz. Ayrıca dış BT sistemleri (örn. uzaktan çalışanlar, dış müşteriler ve iş ortakları), kurumun sunucusuna erişemez ve önemli iş süreçleri aksamaya başlar.

2.2 YETERSİZ HAT KAPASİTELERİ

Bir DNS sunucusunun hat kapasitesi yetersizse, iç ve dış hizmetlere erişim süreleri artabilir. Bu, sınırlı kullanıma veya hiç ulaşılamama durumlarına sebebiyet verebilir. Ek olarak saldırganlar, hizmet reddi (DOS) saldırısıyla DNS sunucusunun aşırı yüklenmesine sebebiyet verebilir.

2.3 DNS KULLANIMININ YETERSİZ VEYA EKSİK PLANLANMASI

Planlama hataları, sistemde planlanmayan veya düşünülmeyen çalışmalar sonucunda güvenlik boşluklarına sebebiyet verebilir. DNS kurulumu ve dağıtımı yetersiz bir şekilde projelendirilmişse, bu durum işletim sırasında sorunlara ve güvenlik açıklarına yol açabilir. Örneğin, DNS trafiğini denetleyen güvenlik duvarı kuralları çok serbest bir şekilde tanımlanırsa, bu saldırılara neden olabilir. Ancak kurallar çok kısıtlı olarak formüle edilirse, meşru istemciler DNS sunucularına herhangi bir istekte bulunamazlar.

2.4 HATALI ALAN ADI BİLGİLERİ

DNS kullanımı dikkatli bir şekilde planlanmış ve güvenlikle ilgili tüm noktalar dikkate alınmış olsa bile, anlamsal ve sözdizimsel olarak yanlış etki alanı bilgilerinin dikkate alınmadığı durumlar sistem arızalarına sebebiyet verebilir. Örneğin, bir ana bilgisayar adına yanlış bir IP adresi atanması, verilerin eksik kalmasına, geçersiz karakterler kullanılmasına veya geri çözünme tutarsızlıklarının meydana gelmesine neden olur. Son olarak hatalı etki alanı bilgileri, bu bilgileri kullanan hizmetlerin yanlış bilgiler nedeniyle sınırlı ölçüde çalışmasına sebebiyet verir.

2.5 DNS SUNUCUSUNUN YANLIŞ YAPILANDIRILMASI

DNS sunucusunun manuel yapılandırılan ayarları veya yanlış yapılandırmalar, DNS sunucusunda hatalara sebebiyet verebilir. Örneğin, Resolving DNS sunucusu, kısıtlama olmaksızın özyinelemeli istekleri kabul edecek şekilde yapılandırılırsa (hem iç veri ağından hem de Internet'ten), sunucunun erişilebilirliği artan yük nedeniyle ciddi şekilde sekteye uğrayabilir. Ayrıca, DNS yansıma saldırılarına (DNS reflection attacks) karşı açık hale gelinebilir.

Benzer şekilde, yanlış yapılandırılmış DNS sunucularında, Zone transferlerin yetkili DNS sunucular ile sınırlandırılamama riski oluşabilir. Bu durum, DNS sunucularına istekte bulunma seçeneğine sahip her ana bilgisayarın, bu sunuculardaki tüm etki alanı bilgilerini okuyabileceği anlamına gelir. Bu şekilde elde edilen veriler saldırıları kolaylaştırabilir.

2.6 DNS ÖNBELLİK ZEHİRLENMESİ

DNS önbellek zehirlenmesi (DNS spoofing); Alan Adı Sistemi verisini bozarak, DNS çözümleme önbelleğine bozuk verinin yerleştirildiği bir bilgisayar güvenliği saldırısıdır. Bu yolla isim sunucusunun yanlış sonuç dönmesi sağlanabilir (örn. IP adresi). Böylece saldırgan, trafiği kendi bilgisayarına (ya da başka bir bilgisayara) yönlendirebilir.

Normalde ağa bağlı bir bilgisayar, İnternet servis sağlayıcısını (ISS) veya kullanıcının bilgisayarı tarafından sağlanan bir DNS sunucusunu kullanır. Bir kuruluşun ağında kullanılan DNS sunucuları, daha önce elde edilen sorgu sonuçlarını önbelleğe alarak çözünürlük yanıt performansını artırır. Tek bir DNS sunucusuna yapılan zehirlenme saldırıları ile kullanıcılar, tehlikeye girmiş sunucu ile direkt etkileşimle veya tehlikeye girmiş sunucunun alt sunucuları ile dolaylı olarak etkilenebilir.

Önbellek zehirlenmesi saldırısı gerçekleştirmek için saldırgan, DNS yazılımındaki eksiklerden ve açıklardan yararlanır. Sunucu, yetkili bir kaynaktan gelindiğinden emin olunması için DNS yanıtlarını doğrulamalıdır (örn. DNSSEC kullanarak); aksi halde, sunucu yanlış girdileri önbelleğe alabilir ve aynı isteği yapan diğer kullanıcılara sunabilir.

Bu saldırı ile kullanıcılar bir web sitesinden, saldırganın seçtiği başka bir web sitesine yönlendirilebilir. Örneğin saldırgan, DNS sunucusundaki hedef web sitesinin IP adresini, kontrolü altındaki bir sunucunun IP adresi ile değiştirir. Bu kişiler daha sonra kendi sunucusundaki dosyaları, hedef sunucudakilerle eşleşecek şekilde oluşturur. Bu dosyalar genellikle bilgisayar solucanları veya bilgisayar virüsleri gibi zararlı yazılımları içerir. Böylece, bilgisayarı hacklenmiş DNS sunucusuna bağlanan bir kullanıcı, orijinal olmayan bir sunucudan gelen içeriği kabul edebilir ve kötü niyetli içeriği bilmeden indirebilir.

2.7 DNS KORSANLIĞI

DNS korsanlığı (DNS hijacking) veya DNS yönlendirmesi, alan adı sunucu sorgu sonuçlarını değiştirme pratiğidir. Bu işlem, Malware adı verilen kötü amaçlı yazılımlar kullanılarak bir sunucunun TCP/IP ayarları değiştirilip korsanlığı yapan kişinin kontrolü altındaki sahte bir DNS sunucusuna yönlendirilerek veya güvenilir bir DNS sunucunun davranışları internet standartlarına uygun olmayacak şekilde değiştirilerek yapılır.

Bu değişiklikler phishing adı verilen e-dolandırıcılık gibi kötü amaçlar için yapılabileceği gibi İnternet Servis Sağlayıcılar (ISP) tarafından kullanıcıları kendi reklam sayfalarına yönlendirme, istatistik toplama ve belirli alan adlarına engel koyup o alan adını sansürleme gibi amaçlar için de yapılabilir.

2.8 DNS DDoS

Bir DNS sunucusuna DDoS saldırısı, DNS sunucusuna veya DNS sunucu ağ bağlantısına aşırı yüklenilmesi için çok fazla istek gönderir. Teknik olarak, gerekli veri hızına ulaşmak için sorgular bot Net'ler aracılığıyla iletilir. Bu şekilde aşırı yüklenmiş bir DNS sunucusu, artık kurumun normal isteklerini bile yanıtlayamaz hale gelir.

2.9 DNS REFLECTION SALDIRILARI

DNS Amplification saldırısı; çok fazla sayıdaki DNS sorgusu cevabını hedef sisteme yönlendirerek, hedef sistemi işlemez hale getirmeyi, hedefleyen bir servis dışı bırakma (DDoS - Denial of Service) saldırısıdır. Gerçekleştirmesi oldukça kolay bir saldırı olduğundan dolayı sistemler için ciddi bir tehlike arz etmektedir.

DNS sunucusuna gönderilen küçük boyutlu bir sorguya DNS sunucusundan oldukça büyük boyutlu bir cevap alınabilir. ANY DNS sorgusu buna bir örnek olarak verilebilir. ANY DNS sorgusunda, DNS sunucusuna 64 baytlık bir istek gönderilirken, bu isteğe DNS sunucusundan gelen cevap 3000 bayt civarındadır. Yani yapılan isteğin yaklaşık 50 katı kadar büyük bir cevap DNS sunucusundan istemciye dönmektedir. Teorik olarak internet bağlantı hızı 100Mbps olan bir istemci, DNS sunucusundan 5Gbps boyutunda bir DNS cevabı alabilecektir.

Bu saldırı bir den fazla bilgisayardan, botnet ağları üzerinden yapıldığı takdirde hedef sisteme yönlendirilebilecek DNS cevap trafiğinin boyutu da astronomik olarak artacaktır.

3 GEREKSİNİMLER

"UYG.3.6 Alan Adı Sistem Yönetimi" 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. Alan Adı Sistem Yönetimi Rehberi Rol Listesi

Temel Bileşen Sorumlusu/Sahibi	BT Operasyon Ekibi
Diğer Sorumlular	BT Yöneticisi, Üst Yönetici

1.SEVİYE GEREKSİNİMLER

DNS, alan adı sistem yönetimi için aşağıda listelenen gereksinimler öncelikli olarak uygulanmalıdır.

UYG.3.6.G1 DNS dağıtım planı

DNS sunucularının dağıtımı dikkatle planlanmalıdır. DNS sunucularının güvenli şekilde işletilebilmesi, önceden oluşturulmuş bir planlama ile ancak sağlanabilir. Her şeyden önce, DNS'nin nasıl kurulması gerektiğini ve hangi alan bilgisinin korunmaya değer olduğunu açıklayan bir prosedür oluşturulmalıdır. Sorumlu kişiler tarafınca DNS sisteminin BT ağına nasıl entegre edileceği de ayrıca belirtilmelidir. Son olarak, güvenlik ile ilgili unsurların yanında güvenlik gereksinimlerine yol açabilecek hususlarda planlanmaya eklenmelidir. Bu çalışmalar belgelendirilmelidir.

UYG.3.6.G2 Yedekli DNS sunucularının dağıtımı

Advertising DNS sunucuları yedekli mimaride tasarlanmalıdır. Ayrıca fiziksel sunucu kullanımında, sunucuların kabin yedekliliğinin sağlanması ile de esnek ve güvenli mimari arttırılmış olur.

UYG.3.6.G3 İç ve dış sorgular için ayrı DNS sunucularının kullanılması

Advertising ve Resolving DNS sunucuları farklı görevleri üstenir. Bundan dolayı aralarındaki bağlantı kesinlikle kesilmeli ve bağımsız olarak yönetilmelidir. Dahili BT sistem çözümleyicileri (Resolver) yalnızca iç Resolving DNS sunucularını kullanmalıdır.

UYG.3.6.G4 DNS sunucusunun güvenli yapılandırılması

Resolving DNS sunucusu, yalnıza iç ağdan gelen sorguları kabul edecek şekilde yapılandırılmalıdır. Sorgu gönderimlerinde, rasgele kaynak portları kullanılmalıdır. Ayrıca, DNS sunucularının yanlış alan adı bilgilerini sorgular ile gönderdiği durumlar, Resolving DNS sunucusu tarafından engellenmelidir. Advertising DNS sunucusu ise her zaman Internet'ten gelen ve yinelenen istekleri işleyecek şekilde yapılandırılmalıdır.

Zone transferin yalnız birincil ve ikincil DNS sunucuları arasında gerçekleşecek şekilde yapılandırılması garanti altına alınmalıdır. Zone transferler belirli IP adresleriyle sınırlandırılmalıdır. Kullanılan DNS sunucusu ürününün sürümü gizli tutulmalıdır.

UYG.3.6.G5 Güvenlikle ilgili yama ve güncellemelerin zamanında yüklenmesi

DNS'ten sorumlu BT çalışanı, kullanılan yazılımdaki mevcut güvenlik açıklıkları hakkında en güncel bilgiye sahip olmalıdır. Yazılım firmasının bildirdiği açıklar ve güncellemeler dışında, alternatif bilgi kaynakları da incelenmeli ve tehditlere karşı hazır hale gelinmelidir.

UYG.3.6.G6 Güvenli dinamik DNS güncellemeleri

Dinamik güncellemeler kullanılarak alan adı bilgilerinin güvenli şekilde değiştirilmesi, yalnızca kurumun uygun gördüğü BT çalışanlarına bağlıdır. Ayrıca, sorumlu BT çalışanlarının hangi alan bilgilerini değiştirebileceği de belirlenmelidir.

UYG.3.6.G7 DNS sunucularının izlenmesi

DNS sunucuları sürekli olarak izlenmeli ve sunucunun donanım güç kapasitesini ayarlamak için kapasite kullanım oranları düzenli olarak takip edilmelidir. DNS sunucusunun bir yazılım yardımıyla günlük kayıtlardan izlenilmesi önemlidir.

UYG.3.6.G8 Alan adlarının yönetimi [BT Yöneticisi]

Kurum veya organizasyon tarafından kullanılan internet alan adlarına yönelik kayıtların düzenli ve zamanında yenilenmesi sağlanmalıdır. Bu amaçla, alan adları yönetimini koordine eden bir birim tanımlanmalı veya kişi atanmalıdır.

UYG.3.6.G9 DNS sunucuları için iş sürekliliği planı oluşturma

DNS sunucuları için iş sürekliliği planı hazırlanmalıdır. Bu planlama, mevcut iş sürekliliği planına dâhil edilmelidir. Ayrıca, Zone dosyaları için bir veri koruma prosedürü

oluşturulmalı ve bu prosedür, mevcut veri koruma prosedürüne dahil edilmelidir. DNS sistem yapılandırılması dokümante edilmelidir. Acil durumlarda, BT personeli tarafından tüm sistem tekrar ayağa kaldırılabilecek şekilde tanımlanmalıdır.

2.SEVİYE GEREKSİNİMLER

1.seviye gereksinimler sonrasında, alan adı sistemini daha güvenli bir seviyeye getirmeyi hedefleyen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

UYG.3.6.G10 DNS sunucu yazılımının seçilmesi

DNS sunucusunun yazılım ürünleri tedarikinde, kurumun tüm güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilmelidir. DNS sunucu yazılımının kendini kanıtlamış olmasına ve RFC standartlarını karşıladığına dikkat edilmelidir. Ayrıca Master dosyalarının el ile yapılan değişikliklerinde, Zone verilerinin sözdizimsel (syntactic) olarak doğru yapılandırıldığı yazılım tarafından kontrol edilebilmelidir.

UYG.3.6.G11 DNS sunucu kapasitesi

DNS sunucu altyapısı tüm BT sisteminin performansını etkilediğinden yeterli kapasitede hizmet vermelidir. Bundan dolayı, DNS sunucuları için ayrı donanım altyapıları oluşturulmalıdır. DNS sunucularının ağ bağlantılarının da yeterli olup olmadığı ayrıca kontrol edilmelidir.

UYG.3.6.G12 Sorumlu personel eğitimi [Üst Yönetim, BT Yöneticisi]

Eğitimler ile sorumluların, DNS sunucusunun yapılandırma seçeneklerine ve güvenlikle ilgili yönergelere hakim olması sağlanmalıdır. Kurum, eğitimler için yeterli bir bütçe planlamalıdır.

UYG.3.6.G13 Alan adı görünürlüğünün sınırlandırılması

Kurum içerisinde kullanılan bilgisayarların ve ağ bileşenlerinin alan adı bilgileri kurum içerisinde tutulmalıdır. Kurum'un bilişim ağı, dışarıya açık ve kurum içi alanlar olarak ikiye bölünmelidir. Dışarıya açık alan bilgileri, dış hizmetlerin sorunsuz bir şekilde erişilebilir olması için yalnızca alan adı bilgilerini içermelidir.

DNS kullanımının planlanmasında, hangi alan adı bilgisinin dışarıya açık ve hangilerinin kapalı olması gerektiği dikkate alınmalıdır.

UYG.3.6.G14 İsim sunucularını konumlandırma

Birincil ve ikincil DNS sunucuları, farklı IP alt ağlarına konumlandırılmalıdır.

UYG.3.6.G15 Günlük verilerinin değerlendirilmesi

DNS sunucusunun ve işletim sisteminin günlük dosyaları düzenli olarak kontrol edilmeli ve değerlendirilmelidir.

UYG.3.6.G16 DNS sunucusunun "P-A-P" yapısına entegrasyonu

DNS sunucusu bir P-A-P (Packet filter - application level gateway) yapısına entegre edilmelidir. Dışarıya açık bilgileri içeren Advertising DNS sunucusu DMZ üzerine yapılandırılmalı, güvenli ağın birincil DNS sunucusu olarak kurulmalı ve yalnızca temel bilgileri içermelidir. Tehdit oluşturmayan kurum personeli için Resolving DNS sunucusunun (iç paket filtresinin bir DMZ'de çalışması yerine) iç ağda kullanılması tercih edilebilir.

UYG.3.6.G17 DNSSEC kullanımı

DNS protokolünün uzantısı DNSSEC, hem Resolving DNS sunucularında hem de Advertising DNS sunucularında etkinleştirilmelidir. ZSK (Zone Signing Key) ve KSK (Key Signing Key) anahtarları dikkatlice yönetilmeli ve düzenli olarak değiştirilmelidir.

UYG.3.6.G18 İleri seviye Zone Transfer ayarları

Zone Transfer'in korunma seviyesini artırmak amaçlanıyorsa, bu bölgeler Transaction Signatures (TSIG) üzerinden güvence altına alınmalıdır.

UYG.3.6.G19 DNS Sunucusunun elden çıkarılması

Bir DNS sunucusunu çalıştırmama veya ayırma kararı alındıysa, tekrar kullanım öncesi, etkilenen tüm bilgisayarların depolama ortamı güvenli bir şekilde silinmelidir. Ayrıca ağ ve işletim sistemi seviyesindeki tüm referanslar yok edilmelidir. Son olarak uzak DNS sunucusu ile mevcut DNS sunucuları arasında yapılandırılan Zone aktarımları da silinmelidir.

3.SEVİYE GEREKSİNİMLER

Aşağıdaki öneriler, standart koruma seviyesinin ötesine geçen ve arttırılmış koruma ihtiyaçları için göz önünde bulundurulması gereken önlemlerdir. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını gösterir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

UYG.3.6.G20 İş sürekliliği planının test edilmesi (E)

DNS sunucuları için oluşturulan iş sürekliliği planının işlerliği düzenli aralıklarla test edilmelidir.

UYG.3.6.G21 Gizli master (GBE)

Birincil Advertising DNS sunucusunun dışarıdan erişilememesi ve DNS Zone verilerinde görünmemesini sağlamak amaçlı gizli master yapılandırmaları kullanılmalıdır.

UYG.3.6.G22 DNS sunucularının farklı sağlayıcılar üzerinden erişilmesi

Harici olarak erişilebilen DNS sunucularının farklı sağlayıcılar aracılığıyla bağlandığı bir mimari oluşturulmalıdır.

UYG: UYGULAMALAR

UYG.3.6.U ALAN ADI SİSTEM YÖNETİMİ

UYGULAMA REHBERİ

UYG.3.6.U ALAN ADI SİSTEM YÖNETİMİ UYGULAMA REHBERİ

1 AÇIKLAMA

TANIM

Alan adı sistem yönetimi rehberi, bu sistemin temel güvenlik özelliklerini ve bunun için gerekli sunucuların görevlerini kapsar. DNS adlandırma sistemi, internet veya özel bir ağa bağlı herhangi bir kaynak adının IP adreslerini çözmek için kullanılan ağ hizmetini ifade eder. İnternet veya özel bir ağdan oluşan bu sistem, DNS sunucularından ve çözümleyicilerinden oluşur. Diğer taraftan DNS sunucuları olarak düzenlenen bilgisayarlar, host isimlerine karşılık gelen IP adresi bilgilerini tutarlar. Buna karşın çözümleyiciler ise DNS istemcileridir. DNS istemcilerinde, DNS sunucusu ya da sunucuların adresleri bulunur. DNS istemcileri, bilgisayarın ismine karşılık gelen IP adresini bulmak istediği zaman DNS sunucusuna başvurur. Başvurulan adres, DNS sunucusunun kendi veri tabanında mevcutsa ve depolandıysa, bu isme karşılık gelen IP adresi istemciye gönderilir.

DNS sunucuları, görevlerine göre temelde Advertising DNS sunucusu ve Resolving DNS sunucusu olarak ikiye ayrılırlar. Advertising DNS sunucuları genellikle internetten gelen taleplerin karşılanmasından sorumludur. Buna karşın, Resolving DNS sunucuları iç ağdan gelen istekleri işler.

DNS sunucularının arızalanması, DNS tabanlı hizmetlerin kısıtlanmasına yol açacağından bu durum BT hizmetlerinin düzgün şekilde verilebilmesini önemli ölçüde etkileyebilir. Bu sorun ile örneğin, web ve e-posta sunucularına erişilemez. DNS hizmeti, birçok ağ uygulaması tarafından kullanıldığı için RFC 1034 standardına göre, en az iki yetkili ad sunucusundan oluşan bir mimaride kullanılması önerilmektedir.

Alan adı sistemleri birçok uygulama için mecburi ve ön koşul oluştururlar. Bundan dolayı DNS sunucuları dikkatlice planlanmalı, uygun şekilde kurulmalı ve işletilmelidir. Bu rehberin odak noktası; DNS sunucularının erişilebilirliğinin, iletilen bilgilerin gizliliğinin ve bütünlüğünün yanı sıra DNS sunucusunun işletilmesi sırasında ortaya çıkabilecek sorunlarına ilişkindir.

YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

DNS sunucusu seçilmeden ve altyapısı planlanmadan önce, istenen alan adının hala kuruma ait olup olmadığının kontrol edilmesi gerekir (bkz. UYG.3.6.U8 Alan adlarının yönetimi). DNS Güvenlik Uzantıları (DNSSEC) kullanılacaksa, “UYG.3.6.U17 DNSSEC

kullanımı" önlem maddesi uygulanmalıdır. DNS sunucularının kurum ağına nasıl entegre edileceği planlama aşamasında belirlenmelidir (bkz. UYG.3.6.U1 DNS dağıtım planı). Ayrıca bir DNS sunucusunun performans ve kapasitesinin nasıl olması gerektiğine de karar verilmelidir (bkz. UYG.3.6.U11 DNS sunucu kapasitesi).

Tedarik

Alan adı sistemlerinin kullanım amaçlarına yönelik sektörde birçok farklı yazılım ürünleri bulunmaktadır. Uygun bir seçim yapmak için, potansiyel ürünlerin gerekli tüm işlevlere sahip olup olmadığı ve tüm güvenlik gereksinimlerinin karşılanıp karşılanmadığı kontrol edilmelidir (bkz. UYG.3.6.U10 DNS sunucu yazılımının seçilmesi).

Uygulama

Kurulum sonrası, DNS sunucusu güvenli şekilde yapılandırılmalıdır (bkz. UYG.3.6.U4 DNS sunucusunun güvenli yapılandırılması), (bkz. UYG.3.6.U6 Güvenli Dinamik DNS güncellemeleri) ve (bkz. UYG.3.6.U13 Alan adı görünürlüğünün sınırlandırılması). Ek olarak DNS yönetiminden sorumlu personel, ilgili güvenlik önlemleri konularında yeterli düzeyde eğitilmelidir (bkz. UYG.3.6.U12 Sorumlu Personel Eğitimi).

Operasyon

DNS sistemlerinin işletiminde, kullanılan yazılımın güncellenmesi ve diğer güvenlik önlemlerinin uygulanması ile en son güvenlik açıklıklarına karşı güncel kalınması önemlidir (bkz. UYG.3.6.U5 Güvenlikle ilgili yama ve güncellemelerin zamanında yüklenmesi). Paket filtre kuralları kullanılarak, DNS sunucusu ile diğer DNS sunucuları ve istemcileri arasındaki iletişim en aza indirilmelidir (bkz. UYG.3.6.U16 DNS sunucusunun "P-A-P" yapısına entegrasyonu). Sistemin düzgün çalışmasının sağlanması ve olası arıza veya anormalliklerin tespit edilmesi için DNS sunucusunun sürekli izlenmesi ve günlük verilerinin düzenli olarak analiz edilmesi gerekir (bkz. UYG.3.6.U7 DNS sunucularının izlenmesi ve UYG.3.6.U15 Günlük verilerinin değerlendirilmesi).

DNS sunucusunun yapılandırılmasında veya DNS bilgilerinin elle değiştirilmesi öncesinde, DNS sunucusunun yedeği alınmalıdır. Bu sayede olası bir hata durumunda, geri yükleme yaparak hızlı bir şekilde sorun çözülebilir.

Elden Çıkarma

DNS sunucuları kullanım dışı bırakılacaksa, düzenli bir şekilde elden çıkarılmalıdır (bkz. UYG.3.6.U19 DNS Sunucusunun elden çıkarılması).

İş Sürekliliği Planı

Alan adı sisteminin barındırdığı olası güvenlik açıkları için iş sürekliliği planları hazırlanmalıdır (bkz. UYG.3.6.U9 DNS sunucuları için iş sürekliliği planı oluşturma). Ek olarak, Advertising DNS sunucuları yedekli şekilde yapılandırılmalıdır (bkz. UYG.3.6.U2 Yedekli DNS sunucularının dağıtımı).

2 Uygulamalar

Aşağıda yer alan maddeler, alan adı sistem yönetimine özel uygulama maddeleridir.

1. SEVİYE UYGULAMALAR

Aşağıdaki uygulamaların öncelikli olarak ele alınması önerilmektedir.

UYG.3.6.U1 DNS dağıtım planı

DNS sunucularının güvenli şekilde işletilebilmesi, yalnızca önceden oluşturulmuş bir planlama ile sağlanabilir. Her şeyden önce, DNS'nin nasıl kurulması gerektiğini ve hangi alan bilgisinin korunmaya değer olduğunu açıklayan bir prosedür oluşturulmalıdır. Sorumlu kişiler tarafınca DNS sisteminin BT ağına nasıl entegre edileceği de belirlenmelidir. Son olarak, güvenlik ile ilgili unsurların yanında güvenlik açıklarına yol açabilecek hususlarda planlanmaya eklenmelidir.

UYG.3.6.U2 Yedekli DNS sunucularının dağıtımı

Yüksek erişilebilirlik amaçlanıyorsa, yeterli donanım yedekliliği garanti edilmelidir. Bu yedeklik, en az iki bağımsız alan adı sunucusu mimari ile çözümlenebilir. Ayrıca, eğer sunucular fiziksel ise, sunucuların kabin yedekliğinin sağlanması ile de esnek ve güvenli mimari arttırılmış olur.

UYG.3.6.U3 İç ve dış sorgular için ayrı DNS sunucularının kullanılması

Advertising ve Resolving DNS sunucuları farklı görevleri üstenir. Bundan dolayı aralarındaki bağlantı kesinlikle kesilmeli ve bağımsız olarak yönetilmelidir. Bu amaçla, farklı türdeki DNS sunucuları için farklı sunucu altyapıları uygulanmalıdır. Advertising DNS sunucusu, harici olarak kullanılan alan bilgisini yönetir ve yalnızca yinelemeli sorguları destekler. Resolving DNS sunucusu ise dahili (içte) kullanılan bilgileri yönetir ve hem tekrarlayan (iterative requests) hem de özyinelemeli sorguları (recursive requests) destekler.

İstemci uygulamaları, DNS kullanmak için bir çözücüye (Resolver) ihtiyaç duyar. Bu ihtiyaç, yaygın işletim sistemlerine standart olarak entegre edilmiştir. Ancak, dahili BT sistemlerinin çözümleyicileri, domain çözümlemesi için iç Resolving DNS sunucularını kullanmalıdır. Hiçbir koşulda, harici DNS sunucularına sorgu atılmamalıdır. Ayrıca,

çözücüler tarafından kullanılan DNS suffix de belirtilmelidir (örn. yte.tubitak.gov.tr). Bu hostx'i adlandırırken, alan adının kalan kısmını otomatik olarak “Tam Nitelikli Alan Adı (FQDN) hostx. yte.tubitak.gov.tr” dosyasına ekler.

UYG.3.6.U4 DNS sunucusunun güvenli yapılandırılması

Sunucular saldırganlar için öncelikli hedeflerdir. Sunuculara yetkisiz kişiler tarafından erişilirse (örn. web sunucuları, e-posta sunucuları veya uzaktan yönetim uygulamaları gibi), DNS kullanan tüm hizmetler kötü amaçlı olarak kullanılabilir ve kuruma ciddi şekilde zarar verilebilir. Bu nedenle, DNS sunucularının eksiksiz yapılandırılması esastır.

DNS Sunucu Yazılımının Sürümü

Kullanılan DNS sunucu yazılımının sürümü, bir saldırgana saldırı için kullanabileceği değerli bilgiler sağlayabilir. Bu nedenle, sürüm numarası gizlenmelidir. Bu önlem, DNS sunucusunun güvenlik düzeyini doğrudan artırmasa da, bir saldırganın bilgi edinmesini zorlaştırır.

DNS Sorgu Türleri

DNS sunucularına gelen sorgular kısıtlanmaz ise bu durum “Cache poisoning attacks” riskini artırır. Bu nedenle, hangi sorguların kabul edileceğinin sınırlandırılması önemlidir.

Resolving DNS sunucuları, kurum ağından çözümleyici talep etmekten sorumludur ve genellikle özyinelemeli istekleri ele alır. Harici ağlardan gelen sorguların karşılanma görevi ise Advertising DNS sunucuları sorumluluğundadır.

İnternetten gelen talepler her zaman yinelemeli bir şekilde ele alınmalıdır. Böylece, Advertising DNS sunucusu yalnızca yönetilen Zone’lar hakkında bilgi sağlar ve sahte yanıtlar gönderemez.

Resolving DNS-Server’in güvenlik düzeyini artırmak için bu tür sunucular ancak kurum içi BT sistemlerinden özyinelemeli talepleri kabul edecek şekilde yapılandırılmalıdır. Saldırganlar, DNS’e yapılan bir sorguya sahte bir sonuç döndürebilir. Bundan dolayı, sorgu cevaplarına atanan özellikler aşağıdaki şekilde yapılandırılmalıdır:

- IP adresi,
- Sorgunun kimliği (rastgele sayılar),
- Sorgunun kaynak portu.

IP adresi ve kimliği yeterli seviyede koruma sağlamadığından, sorgu gönderilirken ek önlem olarak farklı kaynak portları kullanılmalı; ayrıca, Resolving DNS-Server için birkaç IP adresi yapılandırılmalı ve rastgele atanmalıdır.

Zone Transfer

Zone Transfer'in amacı, birincil DNS sunucularını ikincil DNS sunucuları ile eşlemektir. Birincil DNS sunucusu, Zone Transfer dosyalarından etki alanı bilgilerini okur ve Zone transfer üzerinden ikincil DNS sunucularına ulaşır. Bu şekilde etki alanı bilgileri senkronize tutulur. Birincil ve İkincil DNS sunucusu arasındaki Zone aktarımının gerçekleştiği test edilmeli ve işlevselliği garanti altına alınmalıdır.

Zone Transferinin yetkisiz kişilerce başlatmasının ve böylece Zone alan bilgisinin elde edilmesinin önüne geçilmesi, Zone transferin yalnız birincil ve ikincil DNS sunucuları arasında gerçekleşecek şekilde yapılandırılması ile sağlanabilir (örn. DNS sunucusunun IP adreslerine kısıtlama getirilmesi). Daha güvenilir alternatif olarak "Transaction Signatures" kullanılabilir (UYG.3.6.U18 İleri seviye Zone Transfer ayarları).

IP adreslerindeki kısıtlamalar kapsamında birincil DNS sunucusu, ilişkili ikincil DNS sunucusu olan her Zone için yapılandırılmalıdır. Bir Zone için, birincil DNS sunucusu sorumlu olacak şekilde bir veya daha fazla ikincil DNS sunucusu ayarlanabilir.

Zone Transfer ayarlarında yapılan her değişiklikten sonra sistemin çalıştığı kontrol edilmelidir. Değişiklik sonrası hatalar veya eksiklikler günlük verilerinden tespit edilebilir. Küçük sistemlerin bölgesel ayarları için birincil DNS sunucusu tarafından yönetilen alan adı bilgisini, ikincil DNS sunucusu ile manuel olarak karşılaştırmak mümkündür.

Belirli DNS sunucularının hariç tutulması

Kurumun ve/veya organizasyonun DNS sunucularının yanlış etki alanı bilgisi sağlayan Resolving DNS sunucuları biliniyor ise, bu sunucuların alan adı sunucularına sorgu göndermesi engellenmelidir. Kurumda 10/8, 172.16 / 12 ve 192.168 / 16 gibi özel IP ağları kullanılmıyorsa, güvenlik nedeniyle bu ağlardan gelen sorgular dikkate alınmamalıdır.

UYG.3.6.U5 Güvenlikle ilgili yama ve güncellemelerin zamanında yüklenmesi

DNS'ten sorumlu BT personeli, kullanılan yazılımdaki mevcut güvenlik açıkları hakkında en güncel bilgiye sahip olmalıdır. Yazılım firmasının bildirdiği açıklar ve güncellemeler dışında, diğer bilgi kaynakları da incelenerek tehditlere karşı hazır hale gelinmelidir.

Üretici firmanın güncel güvenlik açıklarını gideren yamaları destekledikleri ve sorumlu oldukları kontrol edilmelidir.

Herhangi bir güncelleme veya değişiklik paketi kurulmadan önce; sistemin yedeklenmesi, değişiklik sonrası olası sorunlar karşısında geri dönüşün garanti altına alınması gerekmektedir. Ayrıca, güvenlik güncellemelerinin uyumlu olup olmadığı ve herhangi bir hataya yol açıp açmadığı test ekibi tarafından mutlaka kontrol edilmelidir.

Yama ve güncellemelerin ne zaman, kim tarafından ve hangi nedenle uygulandığı belgelenmelidir. Sistemin mevcut yama seviye bilgisi hızlıca belirlenebilmelidir. Bu şekilde, sorumlu kişiler tarafından yeni bir güvenlik açığının sistemleri de tehlikeye atıp atmadığı ortaya çıkarılabilir.

UYG.3.6.U6 Güvenli Dinamik DNS güncellemeleri

Dinamik güncellemeler kullanılarak alan adı bilgilerinin güvenli şekilde değiştirilmesi, yalnızca kurumun uygun gördüğü BT çalışanlarınca uygulanmasına bağlıdır. Ayrıca, BT çalışanlarının hangi alan bilgilerini değiştirebileceği de belirlenmelidir. Yetkisiz BT personeli tarafından, etki alanı bilgilerinin dinamik güncellemeler kullanılarak manipüle edilmediğinden emin olunması için aşağıdaki bilgiler dikkate alınmalıdır:

- Yetkili ana bilgisayarların IP adresi kullanarak sınırlandırılması,
- Yetkili ana bilgisayarların TSIG kullanarak sınırlandırılması (bkz. UYG.3.6.U18 İleri seviye Zone Transfer ayarları).

IP adresi kullanarak sınırlandırmada, dinamik güncellemenin kaynağı IP adresi üzerinden teşhis edilir. TSIG'de ise dinamik güncellemenin kaynağını tanımlamak için simetrik şifreleme kullanır.

IP adreslerinin kullanımında, IP-Spoofing'e karşı güvenlik açıklarının haricinde farklı türlü güvenlik sorunları da ortaya çıkabilir. Bundan dolayı ikincil alan adı sunucuları, dinamik güncelleme yönlendirici (Forwarder) olarak ayarlanmalı ve birincil DNS sunucusu yalnızca ikincil DNS sunucularından gelen güncellemeleri kabul edecek şekilde yapılandırılmalıdır.

Kaynağı tanımlamanın yanı sıra, değiştirilebilecek etki alanı bilgilerinin de belirlenmesi gerekmektedir. Örneğin, DHCP sunucusu, alan adlarının ve IP adreslerinin eşlemesini değiştirmek için izin alması gerekir. Buna karşın bir DHCP sunucusuna, Zone'dan sorumlu DNS sunucusunu değiştirme izni verilmemelidir.

UYG.3.6.U7 DNS sunucularının izlenmesi

DNS sunucusunun güvenli şekilde işletimi için oluşturulan planlama ve ilk yapılandırmalar yeterli olmayabilir. Potansiyel problemleri ve güvenlik açısından kritik açıkları belirlemek için bir takım önlemler alınmalıdır.

Ayrıca, kapasite gereksinimleri önceden planlamada belirtilmelidir. Kapasite gereksinimlerinin;

- Zone büyüklüğüne,
- Sorgu sayısına,
- Özyinelemeli sorgu sayısına,

- Zone transfer sayısına,
- Dinamik güncelleme sayısına

bağlı olması nedeniyle gerekli kapasiteyi planlamak zordur. Bu nedenle örneğin, DNS sunucusunun donanım güç kapasitesini ayarlamak için kapasite kullanım oranları düzenli olarak izlenmelidir. Ayrıca, artan bir yük olası mevcut bir saldırının göstergesi olabilir. DNS sunucusunun bir yazılım veya günlük kayıtlarından izlenilmesi önemlidir.

UYG.3.6.U8 Alan adlarının yönetimi [BT Yöneticisi]

İnternet alan adları, alan adı kayıt şirketlerince tescil edilmelidir. Tescil firmaları "Top-Level domain" üst seviye ve eksiz alan adlarını belirli bir süre için kayıt edebilirler. Bu alan adları genellikle .com, .org ve .net benzeri uzantılara sahiptir. Belirli bir süre sonunda, bu alan adı kullanımı ücret karşılığında yenilenmeli, aksi takdirde bu eksiklik istenmeyen sonuçlar doğurabilir. Bu nedenle, bir kurum tarafından kullanılan tüm alan adlarına yönelik kayıtların düzenli ve zamanında yenilenmesi sağlanmalıdır. Bu amaçla, her kurumun alan adları yönetimini koordine eden bir sorumlu tanımlanmalıdır.

Alan adı gaspı (domain grabbing) önleme

Domain Grabbing, domain tescilinde bulunan kişinin; başkasına ait marka, isim, ticaret unvanı, işletme adı ve vb. ilerde gerçek hak sahibine çok yüklü bir meblağ karşılığında satmak amacıyla, internet alan adı olarak kendi adına tescilini yaptırmasıdır.

Hizmet sağlayıcının, alan adlarının yönetimindeki hataları ve ihmalleri önleme amaçlı düzenlemeler uygulanmalıdır.

Eğer DNS sunucuları kurumda bulunmuyorsa ve bir servis sağlayıcı tarafından barındırılıyorsa özellikle alan adı sunucularının erişilebilirliği ve kurumun DNS'sindeki değişikliklerin işlem süreleri için servis seviyesi anlaşmalarının (SLA) şartları tanımlanmalıdır.

UYG.3.6.U9 DNS sunucuları için iş sürekliliği planı oluşturma

DNS sunucusuna erişilemediği durumlar, BT altyapısının çalışmasını ciddi şekilde etkiler. Asıl sorun, DNS tabanlı hizmetlere erişilememesidir. Bu koşullar altında web sunucularına, alan adı kullanılarak erişilemez ve yine alan adı kullanılarak uzaktan masaüstü bağlantısı sağlanamaz.

DNS sunucusunun arıza verdiği durumlarda, kurum içerisinde ki ve / veya dışarısında ki alan adı çözümlemeleri gerçekleşmeyebilir. Örneğin, dışarıdan gelen isim çözümlemesinin çalışmadığı normal veya uzun süreli kesintiler, kurumun müşterilerine karşı imaj kaybına neden olabilir.

Bu tür kesintilerin önüne geçmek için aşağıdaki hususlar dikkate alınmalıdır:

- DNS sunucularının iş sürekliliği planlaması mevcut iş sürekliliği planına dahil edilmelidir,
- Sistem arızaları veri kaybına neden olabilir. Bu nedenle, Zone dosyaları için bir veri koruma prosedürü oluşturulmalı ve bu prosedür, mevcut veri koruma prosedürüne dahil edilmelidir,
- DNS sunucusunun iş sürekliliği planına ek olarak, DNS'nin üzerinde çalıştığı işletim sistemi için de bir iş sürekliliği planı bulunmalıdır,
- DNS sistem yapılandırılması dokümante edilmelidir. Acil durumlarda, BT personeli tarafından tüm sistem tekrar ayağa kaldırılabilecek şekilde tanımlanmalıdır.
- Saldırı durumlarında, güvenlik açığı düzeltilmeli ve belgelendirilmelidir.
- BT sistemlerinin yeniden başlatılabilmesi için bir kurtarma planı oluşturulmalıdır.

2. SEVİYE UYGULAMALAR

1.seviye gereksinimler sonrasında, alan adı yönetim sistemini daha güvenli bir seviyeye getirmeyi hedefleyen kurum ve organizasyonlar aşağıdaki gereksinimleri dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

UYG.3.6.U10 DNS sunucu yazılımının seçilmesi

DNS sunucusunun yazılım ürünleri, performans ve kullanım kolaylığı bakımından farklılık gösterir. Bu tür bir ürün tedarik edilirken, aşağıdaki hususlar göz önünde bulundurulmalıdır:

- DNS sunucu yazılımının kendini kanıtlamış olması,
- DNS hizmeti gereksinimlerini karşılaması ve personel tarafından aşina olunması,
- Seçilen DNS sunucu yazılımının, uygulama standartlarını karşılamadığı durumlarda (RFC 1034, 1035 vb.) yalnızca uygunluk kontrolleri sonrası kullanılması,
- DNSSEC'nin kullanılması durumunda, bunun DNS sunucu yazılımı tarafından desteklendiğinden emin olunması,
- Master dosyalara el ile yapılan değişikliklerde, Zone verilerinin sözdizimsel (syntactic) olarak doğru yapılandırıldığının yazılım destekli olarak kontrol edilmesi.

UYG.3.6.U11 DNS sunucu kapasitesi

DNS sunucusunun çalıştırılacağı donanım, alan adı sisteminin genel performansını kesin olarak etkiler. Ayrıca, DNS sunucusunun ortalama kaç sorguya cevap vereceği, özyinelemeli istekleri kabul eden Resolving DNS sunucusu olup olmadığı veya yalnızca

Advertising DNS sunucusunun yinelemeli sorguları karşılayıp karşılamadığı ve de DNSSEC'nin kullanılıp kullanılmadığı gibi durumlar dikkate alınmalıdır.

DNS sunucuları için, sunucunun bellek içeriğini hızlı şekilde sabit diske aktarabilen ve böylece yanıt sürelerini artıran yeterli ana bellek alanları önemlidir. DNSSEC'nin kriptografik işlemlerinde yeterli verim alınabilmesi için işlemci performansının uygun şekilde artırılmasının sağlanması gerekmektedir. Ana bellek ve işlemci performansı için seçilen kapasitelerin sistemin normal işletimi esnasında kontrol edilmesiyle, sistemin gerekli kapasiteleri ortaya çıkarılabilir.

DNS sunucusunu diğer sistemlerin etkilememesi için, kullanılan donanımda yalnızca DNS sunucusu çalıştırılmalıdır. "Distributed denial-of-service (DDoS)" ataklarının engellenmesi, DNS sunucularının geniş bant'a ve güçlü ağ bağlantılarına sahip olmalarına bağlıdır.

UYG.3.6.U12 Sorumlu personel eğitimi [Üst Yönetim, BT Yöneticisi]

DNS sunucusunun doğru ve güvenli bir şekilde yönetilmesi, sorumlu personel yetkinliğinin arttırılması ile doğrudan ilgilidir. Küçük yapılandırma hataları bile kritik güvenlik açıklarına neden olabilir. DNS sunucularının kaynak kullanımının planlanması ve sistemi kullanacak personelin belirlenmesi veya yetki kısıtlamaları ciddi uzmanlık gerektirmektedir.

Güvenli ve etkin DNS yönetimi için genel işletim sistemi güvenliği unsurlarına ek olarak, aşağıdaki konular da önemlidir:

- DNS sunucu kurulumu,
- DNS sunucusunun işletim sistemine önyükleme (boot) seçenekleri,
- Olası tehlikelere karşı alınacak önlemlerin eğitimi,
- Hem yönetici yapılandırma hakları, hem de DNS sunucusu yetkilendirmesi için prosedürlerin oluşturulması,
- Resolving DNS sunucusu ile Advertising DNS sunucusu arasındaki fark,
- DNS sunucu yapılandırması,
- Güvenli sorgu mekanizmaları,
- Güvenli Zone Transfer sistemleri,
- Güvenli dinamik güncelleme sistemleri,
- DNSSEC'nin amacı ve yapılandırması,
- DNS sunucularının erişilebilirliğini sağlama amaçlı yedekli sistemler,
- Zone bilgisini koruma amaçlı sistemler

Kurum, eğitimler için yeterli bir bütçe planlamalıdır.

UYG.3.6.U13 Alan adı görünürlüğünün sınırlandırılması

DNS'nin ana işlevi, isimleri ve IP adreslerini eşleştirmektir. Bu gereksinimleri karşılamak için DNS sunucuları, tüm bilgisayarların ve ağ bileşenlerinin adlarını ve IP adreslerini atar. Bu bilgilerin bir kısmının yayınlanması mecburidir (örn. DNS sunucusu, web sunucusu, posta sunucusu, dosya sunucusu, VPN bağlantı noktaları gibi). Alan ad bilgileri dışarıya açık olmasaydı, internet üzerinden bu sunuculara alan adı ile bağlantı kurmak mümkün olmazdı.

Buna karşılık, kurum içerisinde kullanılan bilgisayarların ve ağ bileşenlerinin alan adı bilgileri genellikle dışarıya açık değildir ve kurum içerisinde tutulmalıdır. Alan adı bilgileri, genellikle söz konusu BT bileşeninin rolü veya konumu hakkında bilgileri içerir (örn. DNS Leak Tehlikesi). Bu bilgilerin dışarıya açılması, bilgi ağına doğrudan bir zarar vermez fakat buna karşın elde edilen alan bilgisi, bilgi ağına bir saldırı hazırlamak için kullanılabilir. Saldırgan ağa, güvenlikle ilgili bileşenlere ve değerli hedeflere genel bir bakış sağlayabilir.

Kurum'un genel ağı, dışarıya açık ve kurum içi alanlar olarak ikiye bölünmelidir. Dışarıya açık alan bilgileri, dış hizmetlerin sorunsuz bir şekilde erişilebilir olması için yalnızca alan adı bilgilerini (genellikle IP adresi ve ana bilgisayar adı (host name)) içermelidir.

Kurum içinde, bilgilerin görünürlüğü genellikle sınırlı olmak zorunda değildir. DNS kullanımının planlanmasında, hangi alan adı bilgisinin dışarıya açık ve hangilerinin kapalı olması dikkate alınmalıdır.

UYG.3.6.U14 İsim sunucularını konumlandırma

Ağ iletişiminde yüksek erişilebilirliğinin sağlanması için, harici DNS sunucuları yedekli mimaride tasarlanmalı ve farklı ağ katmanlarına bağlanmalıdır. Bu şekilde, isim çözümlemelerinde IP alt ağı (subnet) veya bir ağ öğesi kesintisinden etkilenilmez.

Sonuç olarak bir DNS sunucusunun fiziki olarak nereye konumlandırıldığı, kurumun ağ altyapısına bağlıdır. Bunun için uyulması gereken bazı temel kurallar aşağıda listelenmiştir:

- Birincil ve ikincil DNS sunucuları, farklı IP alt ağlarına yerleştirilmelidir. Ayrıca, aynı network kartlarına bağlanmamalıdırlar. Bu mimari, IP alt ağının veya ağ anahtarının kesinti durumlarında bile isim çözümlemesinin düzgün çalışmasını garanti altına alır.
- Advertising DNS sunucuları arındırılmış bölgelere (DMZ: demilitarized zone) konumlandırılmalı,
- Resolving DNS sunucuları, kurum içi BT sistemlerinden gelen sorgulardan sorumludur. Bu nedenle, uzun yanıt süreleri ve gereksiz ağ yükünden kaçınmak için kurumun

güvenli ağı içindeki ilişkili BT sistemlerine mümkün olduğunca yakın yerleştirilmelidirler.

- Resolving DNS sunucularına, dış BT sistemlerden erişilememeli,
- Bilginin görünürlüğü sınırlı ise dışa açık alan adı bilgileri DMZ'deki Advertising DNS sunucusu tarafından yönetilmeli,
- Dış alan ad sunucusu, internet alan adını çözmek için bir yönlendirici (Forwarder) kullanıyorsa, bu sunucular dış ağa yerleştirilmemeli,
- Kurumun iç ağında Caching-only DNS sunucusu kullanılıyorsa, istemcilerdeki çözümleyiciler (Resolver), alan adı bilgilerini önbelleğe yüklememelidir. Önbellek, Caching Only DNS-Server tarafından gerçekleştirilmelidir. Buna ek olarak, merkezi bellek yolu ile de sorgu sayısı en aza indirilebilir. Ayrıca, Cache poisoning atakları esnasında (yalnızca önbellekleme yapan DNS sunucusunun merkezi önbelleği) taklit edilen veriler kolayca silinebilir.
- Güvenlik duvarında DNS ağ trafiği için kurallar oluşturulmalıdır. Planlama sırasında, mümkün olduğu kadar az route ve port açılmasına da ayrıca dikkat edilmelidir.

UYG.3.6.U15 Günlük verilerinin değerlendirilmesi

DNS sunucusunun ve işletim sisteminin günlük dosyaları düzenli olarak kontrol edilmeli ve değerlendirilmelidir. Günlük dosyasındaki olası sorunlar ve düzensizlikler aşağıdaki gibi ortaya çıkabilir:

- Belirli kaynaklardan sıkça yapılan sorgular,
- Sıkça yapılan (başarısız) Zone Transferleri,
- Belirli alan adları için sık yapılan sorgular,
- Var olmayan alan adları için sıkça yapılan sorgular,
- Yetkisiz özyinelemeli sorgular.

Düzensizlikler, sunucunun tehlike altında olduğunu direkt olarak göstermediği gibi genellikle yanlış ayarlardan dolayı da ortaya çıkabilirler.

UYG.3.6.U16 DNS sunucusunun "P-A-P" yapısına entegrasyonu

DNS sunucu yazılımı güvenlik açısından birçok risk barındırabilir. Alan adı bilgilerinin önemi ve DNS yazılımının saldırılara maruz kalması nedeniyle, etki alanı bilgilerinin güvenli bir şekilde kullanılması için doğru kurulum mimarisi önem arz etmektedir.

Paket filtreleri ile iletişimin en aza indirilmesi

DNS sunucuları aşağıdaki iletişim kanallarına ihtiyaç duymaktadır:

- Advertising DNS sunucusunun 53 numaralı port noktasında Resolving DNS sunucusuna izin verilmeli (UDP),
- Resolving DNS sunucusunun bütün portlarında Advertising DNS sunucusuna izin verilmeli (UDP),
- İleticinin 53 numaralı bağlantı noktasında Resolving DNS sunucusuna izin verilmeli (UDP),
- Resolving DNS sunucusunun tüm bağlantı noktalarında yönlendiriciye (Forwarder) izin verilmeli (UDP),
- Advertising DNS sunucusunun 53 numaralı portunda dış ağa izin verilmeli (UDP),
- Advertising DNS sunucusuna dış DNS sunucusunun tüm port noktalarında izin verilmeli (UDP/TCP),
- Resolving DNS sunucusunun 53 numaralı port noktasında dış ağa izin verilmeli (UDP),
- Resolving DNS sunucusunun iç ağın tüm portlarına izin verilmeli (UDP),
- Birincil DNS sunucusuna, ikincil DNS sunucusunun 53 numaralı port noktasında izin verilmeli (UDP/TCP),
- İkincil DNS sunucusuna, Birincil DNS sunucusunun 53 numaralı port noktasında izin verilmelidir (UDP/TCP).

Bu kuralların uygulanması, kurumun kullandığı servislere internetten iletişimi sınırlandırır. Kurumun iletişim politikası ne kadar sıkılaştırılabilirse, dışarıdan gelecek tehlikelere ve saldırılara karşı internet sunucuları o oranda korunur ve ulaşılamaz hale gelir.

Yukarıdaki kurallar; ICMP'nin geçmesine izin vermediğinden, DNS sunucusuna erişilememe durumu ortaya çıkabilir. Bu nedenle, internet sunucusuna dış ağlardan gelen sorgularda, icmp subtype'i "icmp unreachable" bırakılması önerilir.

"P-A-P" yapısındaki DNS sunucusu

Dışarıya açık bilgileri içeren Advertising DNS sunucusu DMZ üzerine yapılandırılır, güvenli ağın birincil DNS sunucusu olarak kurulur ve yalnızca temel bilgileri içerir. Örneğin:

- Dış e-posta sunucusunun ismi ve IP adresi (MX kaydı),
- Sunucuların isim ve adres bilgileri dış dünyaya bilgi sağlar. Bu nedenle, Application Level Gateway'in (ALG) önünde ve arkasında bulunan sunucular arasında ayrım yapılmalıdır.

Resolving DNS sunucusu, DMZ'in üzerindeki filtrelerde yapılandırılır. Bu sunucular, iç ağ bilgisayarları hakkında bilgi içerirler. İç ağda bulunan bilgisayarlar için Resolving DNS sunucusu, DNS sunucusu olarak girilir (örn. Unix bilgisayarlarda "/etc/resolv.conf" yapılandırma dosyasına bilgilerin girilmesi). Güvenilir ağdaki bir istemci güvenilmeyen

ağdan alan adı bilgisi isterse, sorgu Resolving DNS sunucusuna gönderilmelidir. İleticiler, sunucu harici sorgular için genel bir DNS sunucusu kullanır. Güvenilmeyen ağdan Resolving DNS sunucusuna doğrudan erişim, paket filtre kuralları tarafından engellenmeli, böylece güvenilen ağın etki alanı bilgileri yalnızca güvenilen ağda görünmesi sağlanır.

Kullanılan paket filtresi, DNS sunucuları arasında yalnızca DNS hizmetine izin verilecek şekilde yapılandırılmalıdır (örn. kaynak / hedef portu 53 olarak). Ayrıca, Advertising DNS sunucusundan iç ağ bağlantılarına izin verilmemelidir. Sunucu yalnızca güvenli bağlantılarla yönetilmelidir.

Tablo 1, erişim kuralları için olası yapılandırma politikasının maddelerini içerir. Listede değinilen yapılandırmalar için, sunucuların iç ağdan SSH bağlantısı ile yönetildiği ve DNS için UDP'nin protokol olarak kullanıldığı varsayılmaktadır. Ayrıca günlük verileri, syslog aracılığıyla günlük sunucusuna iletilir.

Tablo 3. Yapılandırma Erişim Kuralları

Kaynak	Hedef	İzin/Ret	Açıklama
Dışa açık DNS sunucusunun internet ile iletişimi			
Dış Ağ	Advertising DNS-Sunucusu Port 53	İzin verilir	Dış ağdan DNS sorguları ve yanıtları
Dış Ağ	Advertising DNS sunucusunun diğer bağlantı noktaları	İzin verilmez	
Advertising DNS-Server	İnternete açık DNS sunucusu, tüm portlar ve UDP	İzin verilir	Dışarıdaki adların DNS sunucusu tarafından çözümlenmesi
Dış DNS sunucusunun iç ağ ile iletişimi			
Advertising DNS-Sunucusu	İç Ağa tüm bağlantılar	İzin verilmez	
İç ağ (yönetim ağında kısıtlama olabilir)	Advertising DNS-Sunucu portu 22 (SSH)	İzin verilir	Yönetim ve veri aktarımı SSH ve SCP yoluyla gerçekleştirilir

İç Ağ	Advertising DNS sunucusuna tüm bağlantılar	İzin verilmez	İç ağdan DNS talepleri iç ağdaki sunucular üzerinden yapılır
DNS sunucularının birbiriyle haberleşmesi			
Resolving DNS sunucusu	Advertising DNS sunucusu UDP bağlantı portu 53	İzin verilir	Resolving DNS sunucusu istekleri Advertising sunucusuna iletir (gerekirse ayrı bir Forwarder ayarlanabilir)
Advertising DNS Sunucusu	Resolving DNS sunucusu, tüm UDP bağlantı portları	İzin verilir	
Dış DNS sunucusunun dış ağ ile iletişimi			
İç Ağ	Resolving DNS sunucusu UDP bağlantı portu 53	İzin verilir	Dış ağdan gelen DNS istekleri, Resolving DNS sunucusu ile yapılır
Resolving DNS sunucusu UDP bağlantı portu 53	İç Ağ	İzin verilir	İç ağa gelen DNS cevapları
Resolving DNS sunucusu, Diğer kaynak portları	İç Ağ	İzin verilmez	
İç ağ (yönetim ağında kısıtlama olabilir)	Resolving DNS-Sunucu portu 22 (SSH)	İzin verilir	Yönetim ve veri aktarımı SSH ve SCP yoluyla gerçekleştirilir
Günlük alma			
Resolving ve Advertising DNS sunucuları	Loghost UDP portu 514	İzin verilir	Log verilerinin loghost'a aktarılması

Dış servis sağlayıcısına alan adı kaydı

Bu alternatifte, etki alanı bilgileri dış servis sağlayıcıda saklanır ve fakat bu DNS sunucusu tarafından barındırılmaz. Dış ağdan gelen ve iç ağdaki etki alanı bilgileri için kullanılan Advertising DNS istekleri, kurumun DNS sunucusuna değil de dış hizmet sağlayıcısının DNS sunucusuna gönderilir ve yanıtlanır. DNS sunucusu, dış DNS adlarını veya IP adreslerini sorgularken, dış ağdaki bir DNS sunucusuna doğrudan güvenlik duvarı üzerinden erişir.

Bu şekilde kurulan ve uygulanan mimarilerde, gerekli alan bilgileri üçüncü kişiler ile paylaşılabilmekte, fakat bunun dışında kalan alan bilgileri kesinlikle bu kişilere aktarılmamalıdır (örn. posta sunucusunun adı ve IP adresi). Tehdit oluşturmayan kurum personeli için Resolving DNS sunucusunun (iç paket filtresinin bir DMZ'de çalışması yerine) iç ağda kullanılması tercih edilebilir. Bu yöntem paket filtrelerinin uygulanmasını kolaylaştırır.

Bu mimarinin avantajları ise yatırım maliyetlerinin düşürülmesi ve bir P-A-P yapısına entegrasyonun kolaylaştırılması olarak ortaya çıkmasıdır.

UYG.3.6.U17 DNSSEC kullanımı

DNSSEC, DNS önbellek zehirlenmesi saldırıları da dahil olmak üzere DNS'i saldırılara karşı korumak için tasarlanmış bir internet mühendisliği görev grubu (IETF) dokümanıdır. Bu metot, asimetrik şifreleme ile gerçekleştirilir. DNSSEC'de, tüm bölge bilgileri özel bir anahtarla imzalanır. Bu imzalar, ilişkili ortak anahtar kullanılarak doğrulanabilir. Bu ortak şifreleme çiftine, kısa süreli anahtar (ZSK: Zone Signing Key) denir. DNSSEC destekli bir çözümleyici, DNSSEC'in yapılandırılmış olduğu bir DNS sunucusuna istekte bulunursa, sunucu imzaları içeren etki alanı bilgisini döndürerek yanıt verecektir. Çözümleyici, etki alanı bilgilerinin doğruluğunu tespit etmek için imzayı ve genel anahtarı kullanır.

Kısa süreli anahtarın doğruluğu, uzun süreli anahtar (Key Signing Key) ile sağlanır. KSK'in dışa açık hash değeri, ana etki alanına (domain) iletilir. Ana etki alanı anahtarları yardımıyla hash değeri imzalanır ve hash değerinin doğruluğu onaylanır. Bu şekilde güven zinciri oluşturulmuş olur. Ana etki alanı DNSSEC kullanmıyorsa, KSK'yi doğrulamak için bir imza oluşturulamaz. Buna karşın, etki alanı altındaki DNS sunucuları kendi anahtarları ile güven ortamını sağlar ve böylece güven adaları (Island-of-Trust) oluşturulmaya çalışılır. DNSSEC'in yaygın kullanımında, bu güvenli adalar daha da büyür ve sistemin güvenlik seviyesini artırır. DNSSEC aşağıdaki güvenlik yöntemlerini kullanır:

- DNS bilgilerinin kaynağını doğrulama,

- Etki alanı bilgilerinin bütünlüğünün sağlanması sonucunda bu bilgiler manipüle edilemez, imza bu manipülasyonu görünür hale getirir. Kullanıcılar örneğin, doğru web sunucusuyla veya posta sunucusuyla iletişim kurduğundan bu şekilde emin olabilirler.
- Bir etki alanı adı bulunmuyorsa, kimliği doğrulama hata mesajı sistem tarafından oluşturulur.

ZSK ve KSK anahtarları dikkatlice yönetilmeli ve düzenli olarak değiştirilmelidir. ZSK ile fazla veri imzalandığından, daha sık değiştirilmelidir. İmzalanan bölgelerin büyüklüğüne bağlı olarak, bir ila üç aylık zaman diliminde ki değişiklik uygun bir güvenlik seviyesi oluşturur. Ayrıca değiştirme süreci, azami bir yılı geçmemelidir. KSK ve ZSK bir şekilde dışarıya açık hale gelirse, anahtarların hemen değiştirilmesi önerilir.

DNSSEC ve şifreleme işlemleri, DNS sunucularında performans sıkıntıları oluşturabileceğinden, sunucu kapasitelerinin artırılması gerekebilir. Sistemin en yoğun zamanlarında bile cevap sürelerinin kabul edilebilir seviyelerde tutulması sağlanmalıdır.

UYG.3.6.U18 İleri seviye Zone Transfer ayarları

Zone Transfer'in korunma seviyesini artırmak amaçlanıyorsa, bu bölgeler Transaction Signatures (TSIG) üzerinden güvence altına alınmalıdır. TSIG, birincil DNS ve ikincil DNS sunucularında simetrik anahtarları tanımlar. Zone Transfer başlatıldığında TSIG, simetrik anahtar ve bir hash metodunu kullanarak isteğin ikili verilerinden bir Hash Message Authentication Code (HMAC) üretir ve HMAC sorguya eklenir. Anahtarı tanıyan ikincil DNS sunucusu ise HMAC'yi bağımsız olarak hesaplar. Alınan ve hesaplanan HMAC eşleşirse, Zone Transfer gerçekleştirilir. Aksi takdirde sorgu reddedilir. Bu yöntem aynı zamanda IP adres tabanlı korumanın aksine IP sahtekârlığına (IP Spoofing) karşı koruma sağlar. TSIG'nin, her DNS sunucu ürününde bulunamayacağı konusuna da dikkat edilmelidir. Ayrıca, uygulamada üreticiye özgü ayarların yapılandırmaları planlamalara dahil edilmelidir.

UYG.3.6.U19 DNS sunucusunun elden çıkarılması

Bir DNS sunucusunu çalıştırmama ve/veya ayırma kararı verildiyse (örn. etki alanı hizmeti kaldırıldığı için), hizmetten alındığında dikkat edilmesi gereken hususlar bulunmaktadır (örn. ayırma planında, etki alanında eski DNS sunucusuna ait referanslar bırakılmamalı).

Depolama ortamlarının silinmesi veya yok edilmesi

Etkilenen tüm bilgisayarların depolama ortamı yeniden kullanılmadan önce güvenli bir şekilde silinmelidir. Ayrıca, donanımın elden çıkarılması da güvenli yoldan yapılmalıdır.

DNS sunucusunun etki alanından silinmesi

DNS sunucusu ana etki alanına kayıtlı değilse, herhangi bir çalışmaya gerek yoktur. Bununla birlikte, DNS sunucusu etki alanına kayıtlıysa, bu ayrımın etki alanındaki tüm DNS sunucularının Zone girişlerinde silinmeleri için etki alanı yöneticilerine bildirilmesi gerekir.

Sistemin ağdan silinmesi

Ağ ve işletim sistemi seviyesindeki tüm referanslar silinmelidir. Ayrılmış sunucu, kurumun iç sistemlerinde varsayılan DNS sunucusu olarak girilmişse, bu girişlerin silinmesi de gerekir. Uzak DNS sunucusu ile mevcut DNS sunucuları arasında yapılandırılan Zone aktarımları da ayrıca güvenli şekilde silinmelidir.

3. SEVİYE UYGULAMALAR

Aşağıdaki öneriler, standart koruma seviyesinin ötesine geçen ve arttırılmış koruma ihtiyaçları için göz önünde bulundurulması gereken önlemlerdir. Parantez içindeki harfler, önlem özelinde hangi temel değerler için öncelikli koruma sağlandığını gösterir (G = gizlilik, B = bütünlük, E = erişilebilirlik).

UYG.3.6.U20 İş sürekliliği planının test edilmesi (E)

DNS sunucuları için oluşturulan iş sürekliliği planının uygulanabilirliği düzenli aralıklarla test edilmelidir. Acil durum planında açıklanan önlemlerin gerçekten uygulanabilir olduğundan yalnız bu şekilde emin olunabilir. Aynı zamanda testlerin amacı çalışanların iş sürekliliği süreçlerini tanıması ve çalışanların bilinçlenmesi olarak sıralanabilir. Ayrıca test adımları ve gerçekleştirmeleri, sistemlerin ne kadar zamanda tekrar ayağa kaldırılabileceği hakkında da bilgi verebilir.

UYG.3.6.U21 Gizli master (GBE)

Gizli master yapılandırması, birincil Advertising DNS sunucusunun dışarıdan erişilememesini ve DNS Zone verilerinde görünmemesini sağlar. Sorgular yalnızca, en az iki ikincil DNS sunucusu tarafından yanıtlanır ve bu sorgu verileri gizli birincil Advertising DNS sunucusunun güvenli hattından alınır.

UYG.3.6.U22 DNS sunucularının farklı sağlayıcılar üzerinden erişilmesi

Alan adı kayıt ve/veya tescil işlemlerinde, bilgisayar adlarının IP adreslerine atanmasından sorumlu en az iki DNS sunucusu (Birincil ve İkincil DNS sunucusu) belirlenmelidir. Bir DNS sunucusu genellikle internet erişim sağlayıcısı tarafından yürütülebilir, fakat kurumun kendisi de işletebilir. DoS/DDoS saldırılarını önlemek için, birincil ve ikincil DNS sunucuları farklı ağlarda bulunmalı ve farklı sağlayıcılar üzerinden ağa bağlanmalıdır.

3 DETAYLI BİLGİ İÇİN KAYNAKLAR

Alan Adı Sistem Yönetimi rehberi ile ilgili detaylı konulara, aşağıdaki referans ve kaynaklardan ulaşılabilir:

- DNS hizmetlerinin güvenli dağıtımı [Çevrimiçi] Erişim: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_055.pdf [Erişim tarihi: 24.06.2020]
- DNSSEC'nin Uygulanması [Çevrimiçi] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Umsetzung_von_DNSSEC.html [Erişim tarihi: 24.06.2020]
- Secure Domain Name System (DNS) - Deployment Guide [Çevrimiçi] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf [Erişim tarihi: 24.06.2020]
- IT Grundschutz Kompendium DNS Server [Çevrimiçi] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/APP/Umsetzungshinweise_zum_Baustein_APP_3_6_DNS-Server.html [Erişim tarihi: 24.06.2020]
- Active Directory Antivirüs taramasına dair öneriler [Çevrimiçi] https://support.microsoft.com/en-us/help/822158/virus-scanning-recommendations-for-enterprise-computers-that-are-running [Erişim tarihi: 24.06.2020]

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
UYG.3.6.U1	DNS dağıtım planı	DNS sunucularının BT sistemlerine entegrasyonu planlı şekilde uygulanıyor mu?
UYG.3.6.U2	Yedekli DNS sunucularının dağıtımı	Yüksek erişilebilirlik kapsamında, yeterli donanım yedekliliği garanti ediliyor mu?
		Fiziksel sunucu kullanımında kabin yedekliği sağlanıyor mı?
UYG.3.6.U3	İç ve dış sorgular için ayrı DNS sunucularının kullanılması	Dahili ve harici ağlardan gelen sorgular için farklı DNS sunucuları oluşturuluyor mu?
UYG.3.6.U4	DNS sunucusunun güvenli yapılandırılması	DNS sunucularının yönetim hakları gerekli seviyelerde sınırlandırılıyor mu?
		Özyinelemeli DNS isteklerinin yalnızca yetkili ana bilgisayarlar tarafından iletildiği kontrol ediliyor mu?
UYG.3.6.U5	Güvenlikle ilgili yama ve güncellemelerin zamanında yüklenmesi	Yama yönetimi için kurallar/prosedürler tanımlanıyor mu?
		Yamalar, yalnızca güvenilir kaynaklardan sağlandığına dikkat ediliyor mu?
		Yamalar kullanıma sunulmadan önce test ediliyor mu?
		Başarısız güncelleme durumlarında güncelleme öncesine geri dönülebiliyor mu?
		Karşılaşılan yama güncelleme sorunları belgeleniyor mu?
UYG.3.6.U6	Güvenli dinamik DNS güncellemeleri	Dinamik DNS güncellemeleri yetkili ana bilgisayarlarla sınırlandırılıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
UYG.3.6.U7	DNS sunucularının izlenmesi	DNS sunucularındaki yük düzenli olarak kontrol ediliyor mu?
		DNS sunucusundaki yapılandırma değişiklikleri belgeleniyor mu?
		DNS sunucusunun erişim hakları düzenli olarak kontrol ediliyor mu?
UYG.3.6.U8	Alan adlarının yönetimi	İnternet alan adlarının yönetimi için sorumlu bir kişi atandı mı?
		Kullanılan tüm alan adlarının kaydı tutulup düzenli şekilde yenileniyor mu?
		Web alan adlarının farklı uzantıları alınarak site ziyaretçilerinin kandırılması engelleniyor mu?
UYG.3.6.U9	DNS sunucuları için iş sürekliliği planı oluşturma	DNS sunucuları için iş sürekliliği planları oluşturuluyor mu?
		DNS sunucuları için oluşturulan iş sürekliliği planı mevcut iş sürekliliği planlarına entegre ediliyor mu?
UYG.3.6.U10	DNS sunucu yazılımının seçilmesi	Yazılım güncellemelerinin yalnızca güvenilir kaynaklardan indirildiği kontrol ediliyor mu?
		Karşılaşılan yazılım güncelleme sorunları belgeleniyor mu?
		Yöneticiler, DNS sunucusu yazılımı ile ilgili mevcut güvenlik açıkları hakkında bilgilendiriliyor mu?
UYG.3.6.U11	DNS sunucu kapasitesi	DNS sunucularının geniş bant'a ve güçlü ağ bağlantılarına sahip oldukları gibi kapasite durumları kontrol ediliyor mu?
UYG.3.6.U12	Sorumlu personel eğitimi	Güvenli ve etkin DNS yönetimi için sorumlu personel eğitimleri planlanıyor mu?
UYG.3.6.U13		Alan adı bilgilerinin görünürlüğü kısıtlanıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
	Alan adı görünürlüğünün sınırlandırılması	DNS kullanımının planlanmasında, hangi alan adı bilgisinin dışarıya açık ve hangilerinin kapalı olması dikkate alınıyor mu?
UYG.3.6.U14	İsim sunucularını konumlandırma	Ağ iletişiminde yüksek erişilebilirliğinin sağlanması amaçlı harici DNS sunucularının farklı ağ katmanlarına bağlandığı dikkate alınıyor mu?
UYG.3.6.U15	Günlük verilerinin değerlendirilmesi	DNS sunucusunun günlük dosyaları, yetkisiz özyinelemeli ve belirli alan adları için sık yapılan sorgular gibi durumlar için düzenli olarak takip ediliyor mu?
UYG.3.6.U16	DNS sunucusunun "P-A-P" yapısına entegrasyonu	Dışarıya açık bilgileri içeren Advertising DNS sunucusu DMZ üzerinde mi yapılandırılıyor?
		Resolving DNS sunucusu, DMZ'in üzerindeki filtrelerde mi yönetiliyor?
		Kullanılan paket filtresi, DNS sunucuları arasında yalnızca DNS hizmetine izin verilecek şekilde mi yapılandırılıyor?
		Günlük veriler, syslog aracılığı ile günlük sunucusuna iletiliyor mu?
		Kurum içi kullanılan alan adı bilgileri üçüncü kişiler ile paylaşılıyor mu?
UYG.3.6.U17	DNSSEC kullanımı	DNSSEC'in tüm bölge bilgileri özel bir anahtar ile (ZSK) şifreleniyor mu?
		ZSK ve KSK anahtarları ne sıklıkla güncelleniyor?
		DNS sunucularının performans kapasitesi DNSSEC bulunmayan DNS sunucularına kıyasla arttırılıyor mu?
UYG.3.6.U18	İleri seviye Zone Transfer ayarları	Zone Transfer'in korunma seviyesini artırmak amaçlanıyorsa, bu bölgeler Transaction Signatures (TSIG) üzerinden güvence altına alınıyor mu?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
		Zone transferlerinin yalnızca birincil ve ikincil DNS sunucuları arasında gerçekleşmesi sağlanıyor mu?
UYG.3.6.U19	DNS sunucusunun elden çıkarılması	DNS sunucusunun sabit sürücüleri güvenli bir şekilde elden çıkarılıyor mu?
		DNS sunucusu donanımı uygun şekilde elden çıkarılıyor mu?
		Ağ ve işletim sistemi seviyesindeki tüm referanslar siliniyor mu?
UYG.3.6.U20	İş sürekliliği planının test edilmesi	DNS sunucuları için oluşturulan acil durum planının uygulanabilirliği düzenli aralıklarla test ediliyor mu?
UYG.3.6.U21	Gizli master	Birincil Advertising DNS sunucusunun dışarıdan erişilememesini ve DNS Zone verilerinde görünmemesini sağlayan bir gizli master uygulaması kullanılıyor mu?
UYG.3.6.U22	DNS sunucularının farklı sağlayıcılar üzerinden erişilmesi	Alan adı kayıt ve/veya tescil işlemlerinde, en az iki DNS sunuculu (birincil ve ikincil DNS sunucuları) mimari üzerinden erişiliyor 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.dijitalakademi.gov.tr