TÜBİTAK BİLGEM YTE

DİJİTAL KABİLİYET REHBERLERİ

VOIP REHBERİ

BİLGİ TEKNOLOJİLERİ HİZMETLERİ

Haziran 2020

DEĞİŞİKLİK TARİHÇESİ

Rev. No	Yayın Tarihi	Yayın Nedeni	Hazırlayan(lar)
Sürüm 1	Haziran 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 Değerlendirme Modeli ve Rehberlik** (DİJİTAL-OMR) Projesi 2016 yılında başlatılmıştır. Proje kapsamında d-Devlet çalışmalarında sistemli ve bütüncül bakış açısı getirilerek kamu kurumlarının dijital yetkinliklerinin geliştirilmesi ve yürüttükleri proje ve faaliyetlerinin etkililik, etkinlik ve bilgi güvenliği niteliklerinin artırılması ile dijital kamu hizmetlerinin kalite ve performansının iyileştirilmesi sağlanacaktır.

Modeli ve **Rehberlerin** hazırlanmasına yönelik ulusal politika hedefleri, ülkemizde geliştirilen ve uygulamaya alınan Bilgi Teknolojileri (BT) rehber ve olgunluk modelleri ile 5 uluslararası kuruluş, 12 danışmanlık firması, 6 ülke tarafından geliştirilen standart, rehber ve çerçeve modelleri, uygulama örnekleri ve ilgili akademik çalışma örnekleri incelenmiştir. Farklı dijital kabiliyet alanlarında 34 bilişim uzmanından tecrübe aktarımı sağlanmıştır. Merkezi Yönetim ile yapılan anket üzerinden ilgili kapsama giren konular özelinde anket sonuçları analiz edilmiştir. Elde edilen tespitler doğrultusunda, **Dijital Olgunluk Değerlendirme Modeli**'nin taslağı oluşturulmuş ve seçilen kamu kurumlarında pilot uygulama yapılmıştır. Pilot uygulama sırasında alınan geri bildirimler doğrultusunda **Model** nihai hale getirilmiştir. **Model** ile Stratejik Yönetim, Organizasyon, Yazılım Hizmetleri, Yazılım Yaşam Döngüsü, BT Hizmetleri, İşletim ve Bakım, d-Hizmetler başlıklarında yedi yetkinlik belirlenmiştir. Bu yetkinlikler altında gruplandırılmış dijital kabiliyetler bazında seviyelendirilmiş 2764 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 Ağlar Rehberi, Aktif Dizin Rehberi, Sunucu Yönetimi Rehberi** ve **İstemci Yönetimi Rehberi** yayımlanmıştır. 2020 yılının Mayıs ayında bunlara ek olarak **İşletim ve Bakım** yetkinliğinin altında yer alan **Uzaktan Çalışma Rehberi** ve aynı yılın Haziran ayında da BT Hizmetleri yetkinliğinin altında **VoIP Rehberi** yayımlanmıştır.

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

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

sunulmaktadır.

1.1 TERİMLER VE KISALTMALAR

Terim / Kısaltma	Tanım
Ağ Geçidi	[Gateway] Farklı ağlar ve protokoller arası geçişi sağlayan ağ bileşenleridir.
Ağ Geçidi Denetçisi	[Gatekeeper] VoIP ağına bağlı cihazları yöneten, kimlik doğrulama işlevlerini gerçekleştiren, telefon numaralarını veya kullanıcı adlarını IP adreslerine dönüştüren ağ bileşenleridir.
Ara Katman	[Middleware] VoIP mimarisinde anahtarlamanın yapıldığı bileşenlerdir.
Bellenim	[Firmware] Donanımın işlevini ne şekilde gerçekleştireceğini bildiren yazılımdır.
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
Bilgi Güvenliği	Bilginin gizlilik, bütünlük ve erişilebilirlik niteliklerinin korunmasıdır.
BT	Bilişim Teknolojileri

Terim / Kısaltma	Tanım
Çoklu Ortam	[Multimedia] Ses, video ve metin gibi farklı içeriklerin bir arada bulunduğu dijital ortamlardır.
Dalga Bozulumu	[Jitter] İletilen dijital sinyallerin fazında meydana gelen bozulmadır.
d-Devlet	Dijital Devlet
Devre Anahtarlama	[Circuit Switch] İhtiyaç duyulduğunda hattın tahsis edilmesini sağlayan iletişim yöntemidir.
Devre Anahtarlamalı Telefon Şebekesi (PSTN)	[Public Switched Telephone Network] Devre anahtarlama yöntemini kullanan analog telefon şebekesinin genel adıdır.
Dinleme	[Sniffing] Dinleme araçları kullanarak ağdan geçen tüm veri paketlerini yakalayıp izleme sürecidir.
DMZ	[Demilitarized Zone] İnternet üzerinden erişilebilir sunucuların konumlandırıldığı, iç ağdan ayrıştırılmış bölgedir.
Erişilebilirlik	Hizmetin veya hizmeti oluşturan bileşenin ihtiyaç duyulduğunda istenilen fonksiyonu gerçekleştirebilme durumudur.
Evrensel Tak Çalıştır	[UPnP - Universal Plug & Play] İlave ayar gerektirmeden, cihazların birbirine bağlandığı anda kullanıma hazır hale geldiği bağlantı türüdür.

Terim / Kısaltma	Tanım
Fiziksel Telefon	[Hardphone] VoIP aracılığıyla telefon görüşmesi yapılmasını sağlayan uç cihazlardır.
Gerçek Zamanlı Akış Protokolü (RTSP)	[Real Time Streaming Protocol] Gerçek zamanlı veri akşının kontrolü için uygulama katmanında kullanılan bir protokoldür.
Gerçek Zamanlı İletim Kontrol Protokolü (RTCP)	[Real-time Transport Control Protocol] RTP kullanılırken, veri iletiminin kontrolünden ve izlenmesinden sorumlu olan protokoldür.
Gerçek Zamanlı İletim Protokolü (RTP)	[Real-time Transport Protocol] Gönderilen gerçek zamanlı ses ve görüntü gibi verilerin bir veya daha fazla alıcıya iletimini sağlayan bir internet protokolüdür.
Güvenli Gerçek Zamanlı İletim Kontrol Protokolü (SRTCP)	[Secure Real-time Transport Control Protocol] SRTP'nin RTP için sağladığı güvenlik özelliklerini RTCP için sağlayan bir versiyondur.
Güvenli Gerçek Zamanlı İletim Protokolü (SRTP)	[Secure Real-time Transport Protocol] RTP'nin şifreleme ve kimlik doğrulama sağlanarak oluşturulan güvenli versiyonudur.
Güvenli Giriş Katmanı (SSL)	[Secure Sockets Layer] Sunucu ile istemci iletişimi esnasında verilerin şifrelenmesine ortam sağlayan bir teknolojidir.
Hizmet	Kullanıcını ihtiyaçlarını karşılayarak bir fayda yaratma biçimidir. (Ör: Kullanıcıların iletişim ihtiyaçları için sunulan e-posta hizmeti, kurum içi yazışmaların oluşturulması ve yönetilmesi için sunulan doküman yönetim hizmeti, vb.)

Terim / Kısaltma	Tanım
IETF	[Internet Engineering Task Force - İnternet Mühendisliği Görev Gücü] SIP gibi bazı internet protokollerini geliştiren ve standartlaşmasını sağlayan organizasyondur.
IPSec	[Internet Protocol Security – İnternet Protokolü Güvenliği] IP Paketlerini kimlik doğrulaması ve şifrelemeye tabi tutarak iletişimi güvenli hale getiren protokoldür.
Kabiliyet	Bir işin kalite, bilgi güvenliği, performans vb. gereksinimlerinin karşılanma durumudur.
Kalıcı Bellek	[Non-volatile Memory] Güç bağlantısı kesildikten sonra da içindeki verinin kalıcı olarak depolanmasını sağlayan cihazlardır (ör. CD-ROM, SSD, USB Bellek).
Kayıt Sunucusu	[Registrar] SIP protokolü kullanılırken istemcilerden gelen kayıt isteklerini tutan sunucudur.
Kodek	[Codec] Sinyalin sıkıştırılarak kodlanmasını ya da kodlanmış sinyalin çözülmesini sağlayan yazılım ya da donanımdır.
Köprüleme Modu	[Bridged Mode] Birden fazla ağ bağlantısının birbiri ile iletişime geçerek aralarında veri alışverişi yapacak şekilde yapılandırılmasıdır. Bu yapılandırma seçilirse NAT, DHCP gibi fonksiyonlar kullanılmaz.
Kullanıcı	Hizmeti kullanan kişilerdir. Kurum içi BT hizmeti kullanıcıları olabileceği gibi, kurumun elektronik ortamda sunduğu kamu hizmetlerinin son kullanıcıları (vatandaş, özel sektör, diğer kurumlar vb.) da olabilir.

Terim / Kısaltma	Tanım
Kullanıcı Aracısı	[User Agent] SIP protokolü kullanılırken SIP mesajlarını alıp gönderebilen uç noktalardır.
Kullanıcı Aracısı İstemcisi	[User Agent Client] Çağrıyı başlatan kullanıcı aracısıdır.
Kullanıcı Aracısı Sunucusu	[User Agent Server] Kendisine doğru çağrı yapılan kullanıcı aracısıdır.
Kullanıcı Datagram Protokolü (UDP)	[User Datagram Protocol] Verilerin hızlı aktarımı için kullanılan ancak karşı tarafa ulaşıp ulaşmadığını kontrol etmeyen bir iletişim protokolüdür.
MIKEY	[Multimedia Internet KEYing - Multimedya İnternet Anahtarlama] Gerçek zamanlı uygulamalarla kullanılmak için özel olarak tasarlanmış bir anahtar yönetim protokolüdür.
NAT	[Network Address Translation - Ağ Adres Çevrimi] Yerel ağda bulunan bir bilgisayarın IP adresinin ve port numarasının internete çıkarken bir yönlendirici cihaz tarafından değiştirilmesidir.
Olgunluk	Önceden tanımlanmış bir durumu sağlama halidir.
Olgunluk Değerlendirme Modeli	Başlangıç durumundan, önceden tanımlanmış yetkinlik alanlarındaki olgunluk durumuna kadar, öngörülen, arzu edilen ya da tercih edilen yol doğrultusunda, sıralı düzeyler ya da aşamalar içeren modeldir. İlgili alanda referans modele göre mevcut durumun değerlendirilmesi ve referans modele göre iyileştirme alanlarının belirlenmesi için kullanılır.

Terim / Kısaltma	Tanım
Ortak Kriterler	[Common Criteria] Ortak Kriterler, bilgi teknolojileri ürün ve/veya sistemlerinin güvenlik seviyelerinin tespit edilmesi ve bağımsız laboratuvarlarda test edilebilmesi için geliştirilmiş olan ISO 15408 güvenlik standardıdır.
Oturum Başlangıç Protokolü (SIP)	[Session Initiation Protocol] İnternet üzerinden telefon hizmeti sağlanabilmesi için geliştirilen yeni nesil bir protokoldür.
Oturum Tanımlama Protokolü (SDP)	[Session Description Protocol] İki uç nokta arasındaki medya alışverişi parametrelerini tanımlayan protokoldür.
Port	Ağ üzerinde iletişimin sağlandığı bağlantı noktasıdır.
Problem	Bir veya birden fazla arızaya/kesintiye neden olan ve çözülmesi istenen sorundur.
Risk	Hedeflenen kazanç veya çıktıya, gelecekte olumlu veya olumsuz etkisi olabilecek belirsizliklerdir.
Sağlama Toplamı	[Checksum] Şifrelenmiş hash fonksiyonu algoritması çalıştırıldıktan sonra elde edilen veridir.
Sahtecilik	[Spoofing] Bir kaynağı güvenli gibi gösterip, yine bu kaynaktan güvenli gibi gösterilen bir paketi göndererek alıcının kandırılmasıdır.
Sesli Posta	[Voice Mail] Kullanıcılara ulaşılamadığı durumlarda bırakılan sesli mesajların, kullanıcılara gönderildiği e-postadır.
STK	Sivil Toplum Kuruluşu

Terim / Kısaltma	Tanım
Şifreleme	Bir veriyi matematiksel işlemler kullanarak şifreli duruma getirme işlemidir.
Taşıma Katmanı Güvenliği (TLS)	[Transport Layer Security] İki bilgisayar arasındaki iletişimin güvenli olarak gerçekleşmesini sağlayan bir protokolüdür.
Tek Yöne Yayım	[Unicast] Verinin ağ üzerindeki yalnızca bir istemciye iletilmesidir.
Tekrarlama Listesi	[Replay List] Alınan ve kimliği doğrulanan SRTP paketlerinin bir listesidir.
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
Uç Cihaz	[Terminal] VoIP ortamında kullanıcıların birbirleriyle etkileşime ve iletişime geçebilmesi için kullandıkları aygıtlardır.
Vekil Sunucu	[Proxy] Ağa bağlanılan cihazın trafiğinin başka bir sunucu üzerinden iletilmesini sağlayan teknolojidir.
Yayımlama	[Broadcast] Verinin ağ üzerindeki tüm istemcilere iletilmesidir.
Yazılım Tabanlı Telefon	[Softphone] Bir kullanıcının bilgisayar gibi uç cihazlardan yazılım aracılığıyla telefon görüşmesi yapmasına izin veren teknolojidir.
Yetkinlik	Kabiliyet ya da kabiliyet gruplarının bir yaşam döngüsü ve amaç bazında gruplanmış şeklidir.
Yoğunlaştırıcı	[Concentrator] Az sayıda bağlantı ile daha çok verinin iletilmesini sağlayan sistemdir.

Terim / Kısaltma	Tanım
Yönlendirme Modu	[Routed Mode] Farklı ağların birbirine bağlanmasını ve NAT, DHCP gibi fonksiyonların kullanılmasını sağlayan yapılandırma türüdür.
YTE	Yazılım Teknolojileri Araştırma Enstitüsü

1.2 REFERANSLAR

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

Ref 2. IT Grundschutz 1.Yayım (2019): 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

Ref 5. RFC3261, İnternet Mühendisliği Görev Gücü (IETF), Amerika Birleşik Devletleri

2 DİJİTAL OLGUNLUK DEĞERLENDİRME 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.

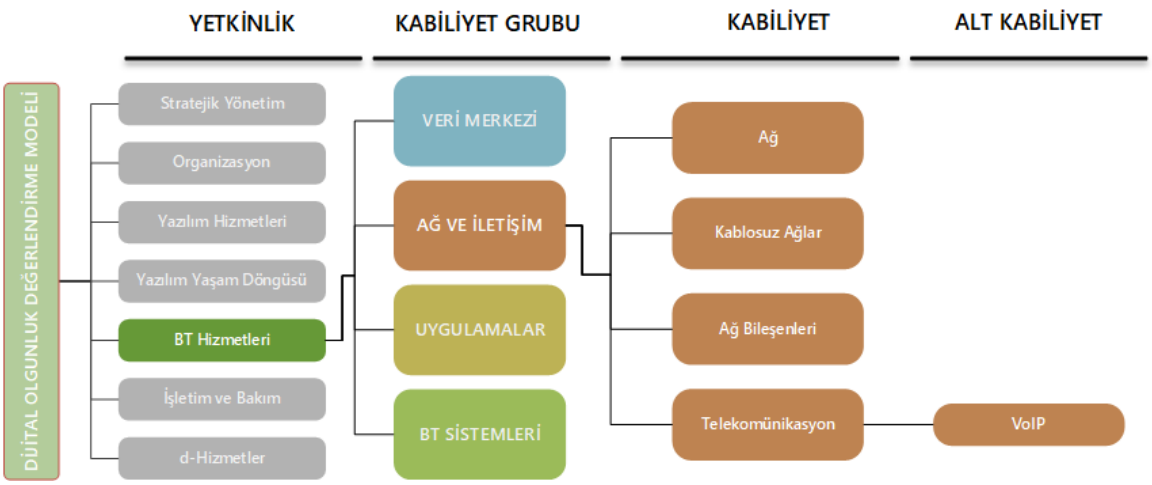
Bununla birlikte, kurumların teknoloji odaklı güncel dönüşüm ihtiyaçlarına cevap verebilmek üzere danışmanlık firmaları ve teknoloji firmaları tarafından oluşturulmuş birçok ticari dijital dönüşüm modeli söz konudur. Bu modellerin çoğunluğu özel sektöre yönelik olarak özel sektör bakış açısıyla hazırlanmaktadır.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



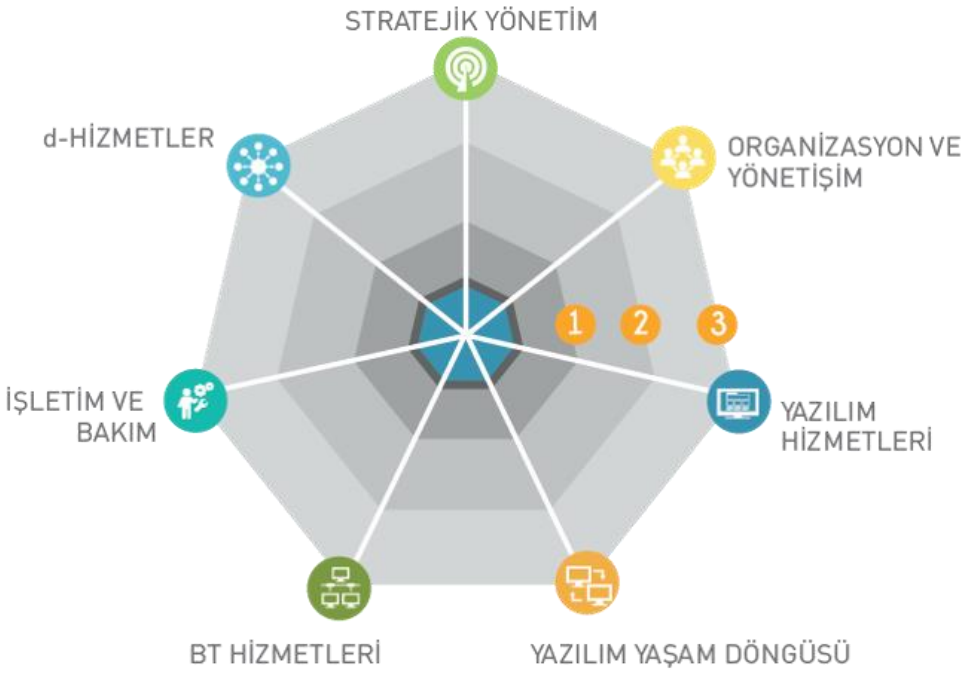
Şekil 1. Dijital Olgunluk Değerlendirme Modeli Gereksinim Seviyeleri

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;

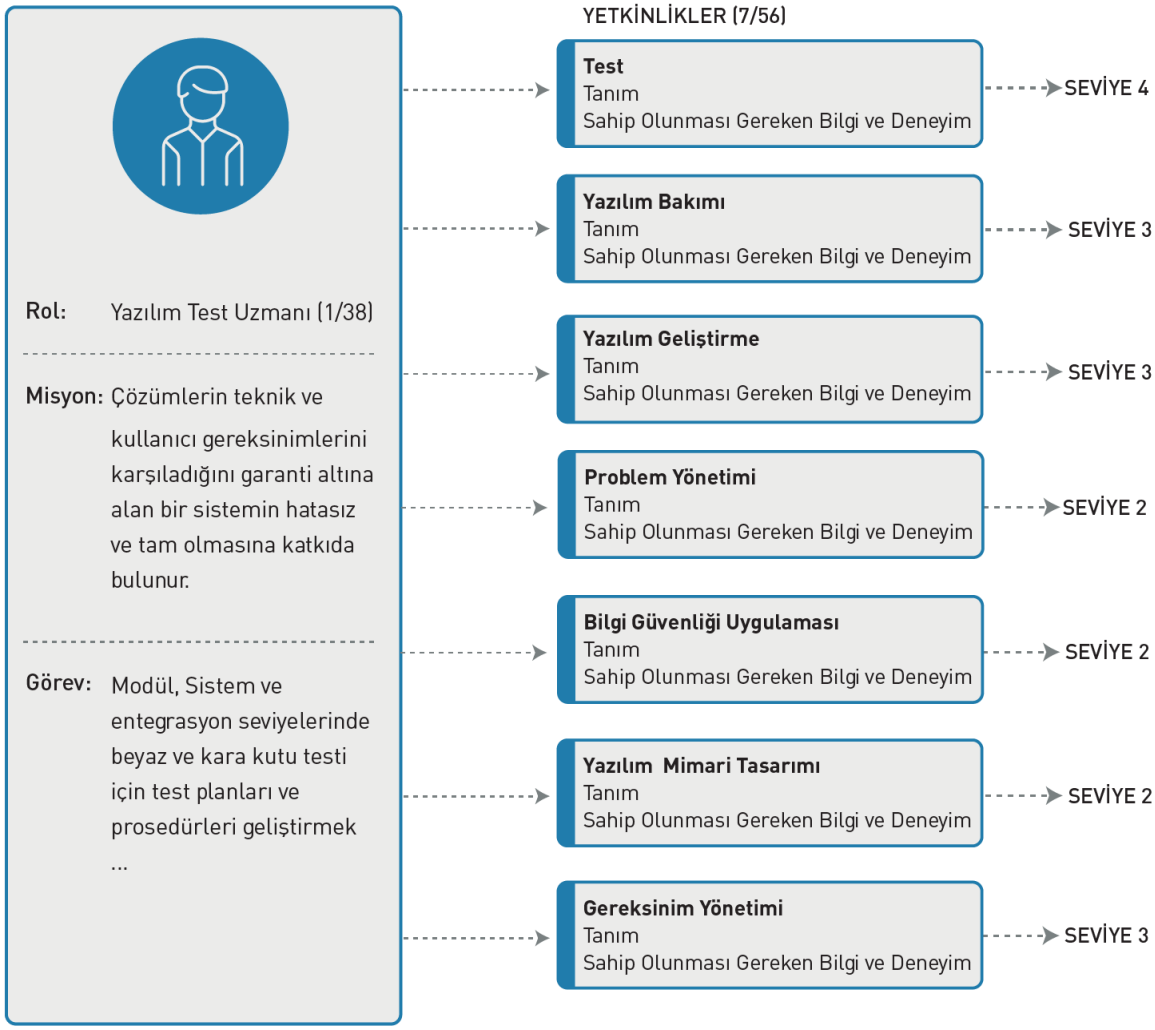
- Dijital Devlet çalışmalarında sistemli ve bütüncül bakış açısının geliştirilmesi,
- Kamu kurumların dijital kapasitelerinin yapısal, standart ve tutarlı bir şekilde değerlendirilmesi,
- Kamu kurumların dijital kapasitelerinin etkin ve verimli bir şekilde arttırılması için rehberlik edecek yol haritasının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

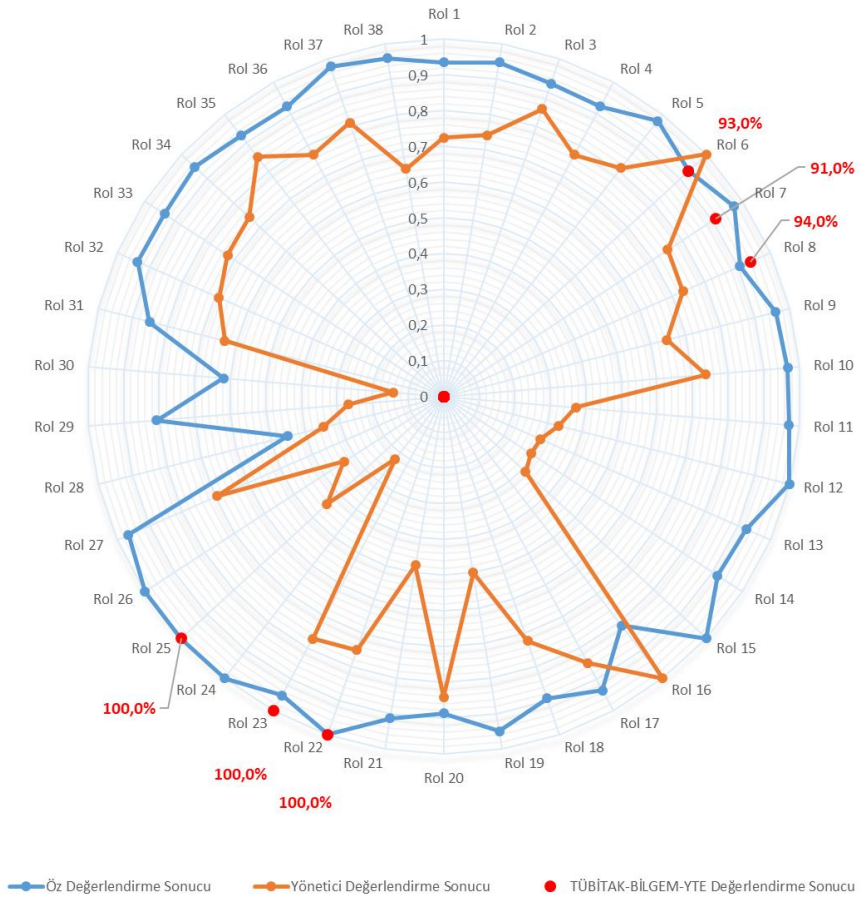
- BT Yönetimi,
- İhtiyaç Tanımlama ve Çözüm Planlama,
- Bilişim Sistemleri Yönetimi,
- Yazılım Teknolojileri Yönetimi

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:



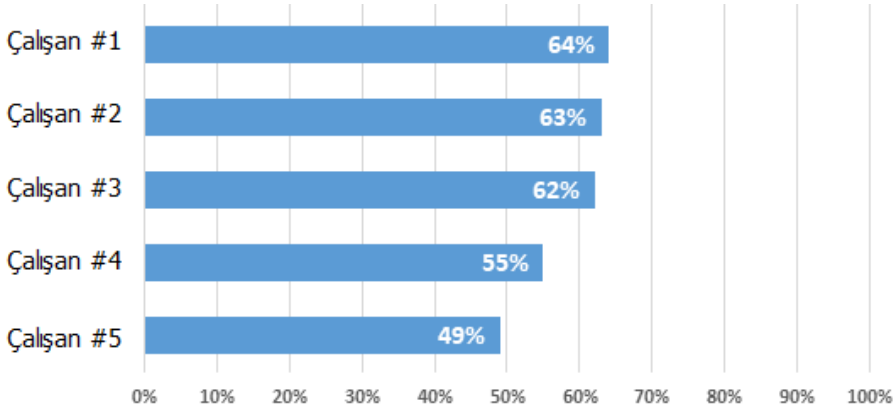
Şekil 3. Örnek Rol-Yetkinlik-Yetkinlik Seviyesi Eşlemesi

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:



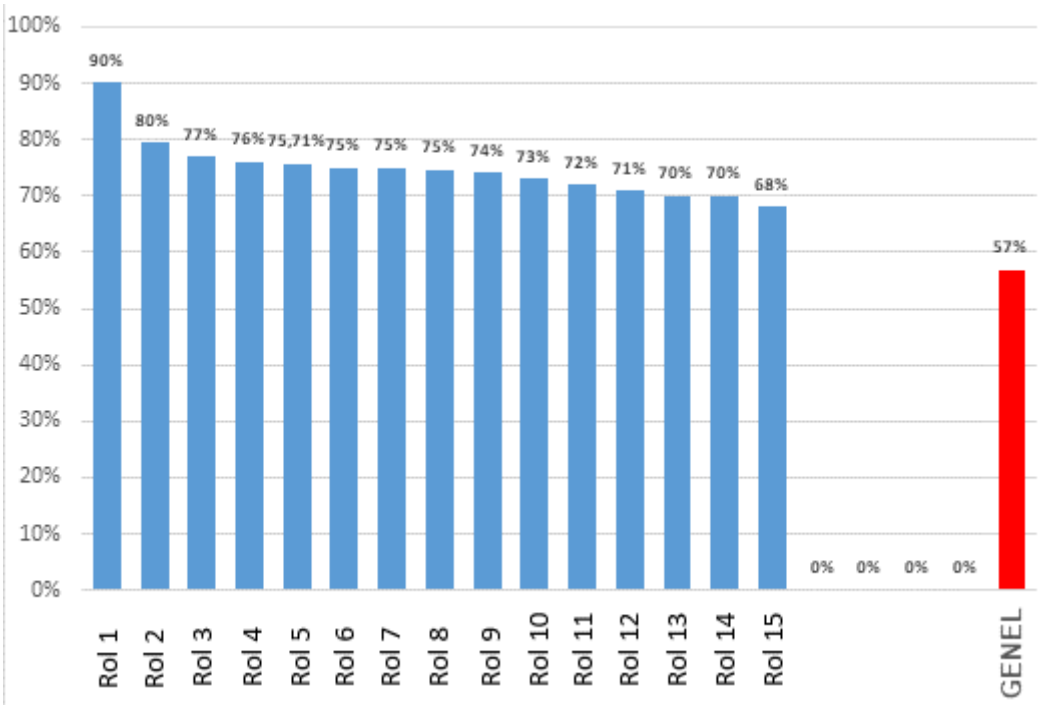
Şekil 4. Çalışan Dijital Yetkinlik Değerlendirmesi

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 **VoIP Rehberi** çalışmaları sırasında, uluslararası boyutta hazırlanmış ve bu alanda kabul görmüş çeşitli standartlar, çerçeveler ve makalelerden 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 rehberinden (gereksinimlerin nasıl karşılanacağına dair talimatlardan) 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. 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.

Rehberler içerdikleri konular itibari ile birbirleri arasındaki ilişkinin kurulması için bir referanslama metodu kullanılmıştır. Bu amaçla her gereksinim maddesi numaralandırılmıştır. Örneğin, VoIP rehberlerinde yer alan **AGY.4.2.G1** kod tanımı aşağıdaki şekildedir:

Tablo 1. Örnek Kod Tanımı

"Ağ ve İletişim" kabiliyet grubu için kullanılan kısaltma	**"Telekomünikasyon" kabiliyeti için atanan numara**	**"VoIP" alt kabiliyeti için atanan numara**	**1. Gereksinim maddesi**
AGY	4	2	G1

Gereksinim maddelerinin detaylı açıklamalarının yer aldığı uygulama rehberinde ise yalnız "**G**" harfi yerine "**U**" harfi kullanılmıştır. Örneğin, AGY.4.2.G1 gereksinim maddesinin karşılığı AGY.4.2.U1 olarak geçmektedir.

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 rehberi "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 rehberinde yer alan gereksinimlere ait hazırlanan kontrol soruları **EK-A**'da verilmektedir.

4.3 KABİLİYET GRUPLARI

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

Şekil 7. BT Hizmetleri Yetkinliği Kabiliyet Grupları

- **Veri Merkezi;** Veri merkezi kapsamında, kritik BT bileşenlerini içeren kurumun yapısal-teknik koşullarının yanında, altyapı güvenliği ile ilgili yönlerini de irdeler.

Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:

- Genel Bina
  - Veri merkezi içerisinde bulunan binalar için, genel bina önlemleri en az bir kere uygulanmalıdır.
- Veri Merkezi ve/veya Sistem Odası
  - Veri merkezi ve/veya sistem odası modülü, kurumun kritik odaları için uygulanmalıdır.
  - Kurum/organizasyon erişilebilirlik hedeflerine veya organizasyon boyutuna göre bu tür alanlar, rehber içeriğinde kritiklik düzeyine göre özelleştirilerek verilmiştir.
- Elektrik Kablolama
  - Veri merkezini ve kritik bileşenleri besleyen güç kaynaklarının hedeflenen erişilebilirlik prensipleri doğrultusunda en az bir kere uygulanması gereklidir.
- BT Kablolama
  - Kural olarak bu modül veri merkezinin içerisinde yer alan bina veya yerleşke için en az bir kere uygulanmalıdır. Ayrıca veri merkezi için de kullanılabilir.

- **Ağ ve İletişim;** Ağ ve iletişim hizmetlerinin planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan kabiliyetler şunlardır:
  - Ağ
    - Ağ Mimarisi ve Tasarımı ile Ağ İşletimi konularındaki kabiliyetleri içermektedir.
  - Kablosuz Ağlar
    - Kablosuz Ağların Kullanımı ve İşletimi konularındaki kabiliyetleri içermektedir.
  - Ağ Bileşenleri
    - Yönlendirici ve Ağ Anahtarlama Cihazı, Güvenlik Duvarı, VPN ve IDS/IPS konularındaki kabiliyetleri içermektedir.
  - Telekomünikasyon
    - PBX, VOIP, Fax ve Video Konferans konularındaki kabiliyetleri içermektedir.

- **Uygulamalar;** BT hizmetlerinde kullanılan çeşitli uygulamaların planlanması ve güvenli bir şekilde yönetilmesi için gerekli kabiliyetleri kapsar. Bu kabiliyet grubunda ele alınan temel kabiliyetler:

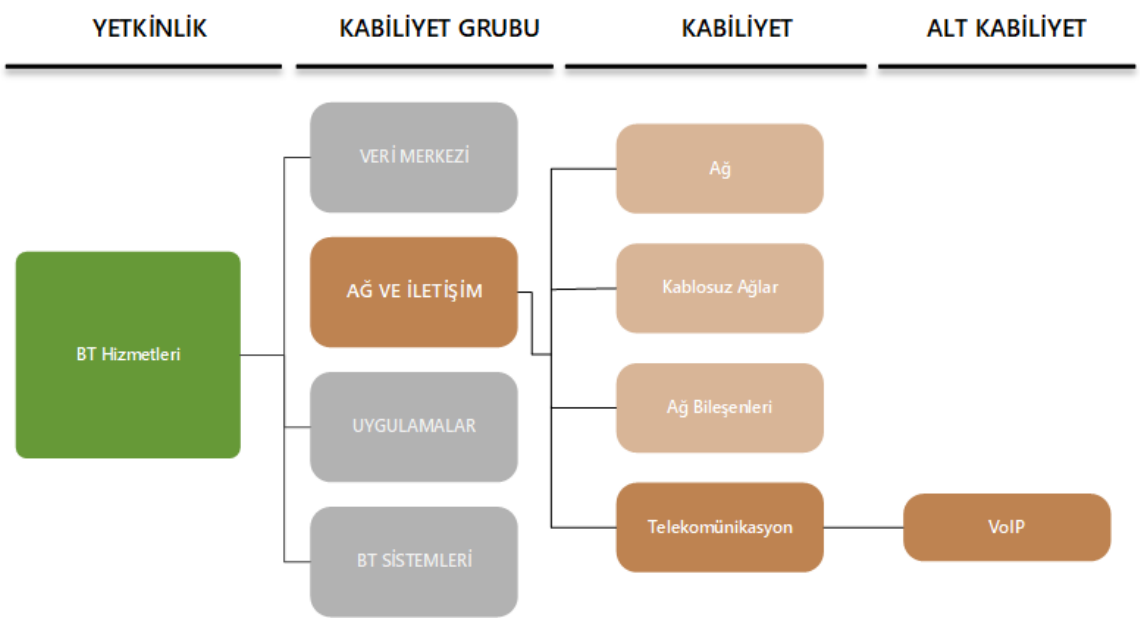
- Kullanıcı
  - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan ofis uygulamalarını, web tarayıcılarını ve/veya mobil uygulamalarını içerir.
- Dizin
  - Kurum veya organizasyonda kullanılan dizin hizmetine (Active Directory, OpenLDAP vs.) özel kabiliyetleri kapsar.
- Ağ Tabanlı Uygulamalar
  - 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.
- Veri tabanı
  - Belli bir amaca yönelik düzenli, büyük miktarda veriyi depolayabilen, bu verilerin hızlı bir şekilde yönetilip değiştirilebilmesine ve raporlanmasına imkan sağlayan ilişkisel veya ilişkisel olmayan veri tabanı 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, istemci sanallaştırma ve depolama ünitesi yönetimlerini kapsar.
  - Sunucu Yönetimi
    - Bu kabiliyet, tüm kurum veya organizasyonda kullanılan sunucuların yaşam döngüsü boyunca güvenli bir şekilde yönetimi için kabiliyetleri kapsar.
  - İstemci Yönetimi
    - Kurumda kullanılan istemcilerin yaşam döngüsü boyunca güvenli yönetimi ve kullanımı için kabiliyetleri kapsar.
  - Sanallaştırma

- BT sistemlerinde kullanılan sanal altyapıların güvenli yönetimi için kabiliyetleri kapsar.

- Depolama Ünitesi Yönetimi
  - Kurum BT altyapısında bulunan depolama ünitelerinin yaşam döngüsü boyunca güvenli bir şekilde yönetimi için kabiliyetleri kapsar.

5 KABİLİYETLER



Şekil 8. Kabiliyetler

AGY: AĞ YÖNETİMİ

AGY.4.2.G VOIP TEMEL BİLEŞEN REHBERİ

AGY.4.2.G VOIP
TEMEL BİLEŞEN

1 AÇIKLAMA

1.1 TANIM

Voice over IP (VoIP) veri ağları üzerinden özellikle de İnternet üzerinden yapılan telefon görüşmelerini ifade eder. Sinyalleşme bilgisinin iletilmesi için her aramaya özel sinyalleşme protokolleri kullanılır. Kullanıcı verisi (ses ya da video) ise bir medya aktarım protokolü ile iletilir. Her iki protokol de bir çoklu-ortam (multimedya) bağlantısının oluşturulması ve sürdürülmesi için gereklidir. Bazı yöntemlerde hem sinyalleşme hem de ortam verisi taşımak için tek bir protokol yeterli olmaktadır.

1.2 HEDEF

Bu rehber, uç cihazların ve anahtarlama birimlerinin (ör. ara katman) güvenlik hususlarını içermektedir.

1.3 KAPSAM DIŞI

VoIP üzerinden ses aktarımı ve VoIP bileşenlerinin güvenlik hususları bu rehberde ele alınmıştır. Devre anahtarlamalı PBX'lerin bir veri ağı üzerinden birbirleriyle iletişiminin nasıl olacağı da ayrıca bu rehber içeriğinde bulunabilir. VoIP yazılımları için genellikle özel donanım ihtiyacı bulunmaz ve bu yazılımlar standart BT sistemleri üzerinde çalıştırılabilir. Eğer istemcilere yazılım tabanlı telefonlar kuruluysa, BTS.2 İstemci Yönetimi rehberi ve istemcinin işletim sistemine özgü gereksinimler dikkate alınmalıdır. VoIP yazılımı eğer sunucularda çalıştırılıyorsa, sunucunun işletim sistemine özgü gereksinimler ve BTS.1 Sunucu Yönetimi rehberi dikkate alınmalıdır.

2 RİSK KAYNAKLARI

Aşağıdaki tehdit unsurları ve güvenlik açıkları AGY.4.2 VoIP rehberi kapsamında öncelikle dikkate alınmalıdır.

2.1 VOIP ara katmanının yanlış yapılandırılması

IP tabanlı telefon sistemleri, devre anahtarlamalı telefon sistemlerine benzer şekilde yapılandırılmaya çalışılırsa bazı olumsuzluklar ortaya çıkabilir. Örneğin, kullanıcılara yanlış telefon numaraları atanabilir veya bütün telefon altyapısı kullanılamaz hale gelebilir. Bununla beraber, telefon rehberine kullanıcı isminin yanlış yazılması gibi kritik olmayan hatalar da ayrıca dikkate alınmalıdır.

VoIP üzerinden iletişim kurarken genellikle birkaç BT sistemine ihtiyaç vardır. Eğer iletişim için Oturum Başlangıç Protokolü(SIP) kullanılacaksa, genellikle kayıt sunucuları, SIP vekil sunucular ve konum sunucuları gibi sistemler de gerekir. VoIP altyapısı değişirse, tüm BT sistemlerinin de bu değişikliğe göre uyarlanması gerekir ki bu durum yapılandırma hatalarına neden olabilir. Tüm hizmetler tek bir sunucuda olsa bile, bu hizmetlerin çoğu zaman ayrı ayrı yapılandırılması gereklidir. Yalnızca bir sistemin bile doğru şekilde yapılandırılmaması, tüm telefon altyapısının kullanılamaz hale gelmesine sebep olabilir.

2.2 VOIP bileşenlerinin yanlış yapılandırılması

Yapılandırma, VoIP bileşenlerinin donanım veya yazılım tabanlı sistemler olup olmadığına bakılmaksızın, sistemin doğru çalışması için çok önemlidir. Yapılan sinyalleşme ayarlarına ek olarak, medya akışlarının hangi yöntem ile sağlanacağı da önemlidir. Örneğin, ses bilgisi içeren veri paketlerinin boyutu, seçilen bir sıkıştırma yöntemi ile azaltılabilir. Bu işlem için en doğru yöntemin kullanılması da çok önemlidir. Konuşma bilgileri çok fazla sıkıştırılırsa genellikle konuşma kalitesi bozulur. Öte yandan, yeterince sıkıştırmayan bir yöntem seçilirse de, mesaj akışı yeterince azaltılamaz ve veri ağına aşırı yük binebilir.

2.3 Telefon görüşmelerinin dinlenmesi

Telefon görüşmeleri veya aktarılan veriler şifrelenmemişse, bu bilgiler saldırganlar tarafından dinlenebilir ve izlenebilir. Örneğin, saldırganlar telefon kablolarına doğrudan müdahale ederek veya anahtarlamanın yapıldığı telekomünikasyon sistemi üzerinden dinleyebilir. Geleneksel telekomünikasyon sistemlerinde olduğu gibi VoIP'te de, telefon görüşmeleri ve veri aktarımları dinlenebilir. VOIP ortamı saldırganlara, sahtecilik (spoofing) ve dinleme (sniffing) gibi yöntemlerle veri ağlarında her türlü saldırı imkânı sağlar. Birçok PBX sisteminde arayanlar, arama sırasında telefonla ulaşılamazsa alıcılara mesaj bırakabilir. Özellikle VoIP sistemlerinde bazı telesekreterler, bu bilgileri bir ses dosyası

olarak e-posta yoluyla gönderir. Bu postanın içeriği doğrudan bir saldırgan tarafından ele geçirilerek dinlenebilir.

2.4 Serbestçe erişilebilen telefonların kötüye kullanılması

Bazı telefonlar herhangi bir kullanıcıya kişisel olarak atanmamış olarak çalışabilir. Bir yanda yalnızca sınırlı bir grup insanın erişebileceği telefonlar varken diğer yanda ziyaretçi alanları gibi yerlerde bulunan herkesin erişebileceği telefonlar da vardır. Bu telefonlarda dahili telefon numaralarının saklandığı elektronik telefon rehberi de ele geçirilebilir. VoIP telefonlar yazılım içeriğine sahiptir ve genellikle diğer BT uygulamaları için de kullanılan veri ağlarında çalıştırılır. Bu nedenle bir saldırgan, VoIP bileşenine doğrudan erişerek veya kötü amaçlı yazılım yükleyerek güvenlik açıklarından yararlanmaya çalışabilir. Ayrıca saldırgan bir BT sistemini VoIP'in dahil olduğu veri ağına bağlayabilir ve dahili ağa erişebilir. Bu erişimi gizlilik, bütünlük ve erişilebilirliğe yönelik saldırılar için kullanabilir.

3 GEREKSİNİMLER

AGY.4.2 VoIP rehberinin özel gereksinimleri aşağıda listelenmiştir. Temel olarak BT operasyon ekibi, VoIP'in gereksinimlerini karşılamaktan sorumludur. Buna ek olarak, Bilgi Güvenliği Birimi her zaman stratejik kararlarda yer almalıdır. Bilgi Güvenliği Birimi tüm ihtiyaçların belirlenen güvenlik politikasına uygun olarak karşılanmasını ve doğrulanmasını sağlamaktan sorumludur. Ayrıca, gereksinimlerin uygulanmasında ilave sorumlulukları olan başka roller de olabilir. Bunlar daha sonra ilgili gereksinimlerin başlığında köşeli parantez içinde açıkça listelenecektir.

Tablo 2. Rol Listesi

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

3.1 1.SEVİYE GEREKSİNİMLER

AGY.4.2 VoIP için aşağıdaki gereksinimler öncelikli olarak dikkate alınmalıdır.

AGY.4.2.G1 VoIP dağıtımının planlanması [BT Yöneticisi]

VoIP'in hangi koşullarda kullanılacağı belirlenmelidir. VoIP'e tamamen mi yoksa kısmen mi geçileceğine karar verilmelidir. VoIP'in erişilebilirliği, telefon görüşmelerinin ve sinyalleşme bilgilerinin gizliliği ile bütünlüğü konusunda herhangi özel bir gereksinim olup olmadığı önceden belirlenmelidir. Kullanmaya başlanmadan önce uygun sinyalleşme ve medya aktarım protokolleri seçilmelidir. VoIP altyapısının genel telefon şebekesine bağlanıp bağlanmayacağına karar verilmelidir. Mevcut veri ağlarının kapasiteleri ve tasarımı planlama sırasında dikkate alınmalıdır.

AGY.4.2.G2 VoIP ara katmanının güvenli yönetimi [BT Yöneticisi]

Farklı yetki seviyelerine sahip rolleri içeren bir yönetim prosedürü oluşturulmalıdır. Kullanılan yazılım bileşenlerinin güncellenmesi, sadece güvenilir kaynaklardan sağlanmalıdır. VoIP bileşenleri farklı sunucularda farklı servisler çalışacak şekilde tasarlanmalıdır. Kullanılan işletim sistemi tüm gereksiz bileşenlerden arındırılmış minimal bir işletim sistemi olarak tasarlanmalı ve ara katmanda çalışan uygulamalar mümkün olduğunca az sayıda tutulmalıdır.

AGY.4.2.G3 VoIP uç cihazlarının kurulumu ve güvenli yönetimi

Gerekli olmayan uç cihazlar devreden çıkarılmalıdır. Yapılandırma ayarları, sadece yetkilendirilen çalışan tarafından gerçekleştirilmelidir. Uç cihazların tüm güvenlik işlevleri kullanımdan önce test edilmelidir. Kullanılan uç cihaz yazılımları, güvenilir kaynaklardan

gelen güncellemelerle düzenli olarak güncellenmelidir. Kullanılan güvenlik fonksiyonları ve parametreler dokümante edilmelidir.

AGY.4.2.G4 VoIP'te erişilebilirliği sınırlandırma [BT Yöneticisi]

Harici bir çağrının VoIP mimarisi aracılığıyla nasıl bağlanacağına karar verilmelidir. Güvensiz ağlardan gelen BT sistemlerinin, kurumun VoIP bileşenlerine doğrudan bağlantı kurabilmeleri önlenmelidir. Gelen ve giden tüm çağrılar merkezi bir BT sistemi ile yoğunlaştırılacaksa, genel telefon şebekesi ve dahili ağ arasındaki tüm sinyalleşme ve ses bilgilerinin sadece bu yetkili yoğunlaştırıcı ile yönlendirilmesi sağlanmalıdır.

AGY.4.2.G5 VoIP ara katmanının güvenli kurulumu

VoIP bileşenleri, güvenlik gereksinimlerini yeterince karşılayacak şekilde yapılandırılmalıdır. VoIP ara katmanı da devreye alınmadan önce yapılandırılmalıdır. Tüm kurulum ve yapılandırma adımları, daha sonra kullanılabilecek şekilde dokümante edilmelidir. VoIP ara katmanının gerekli olmayan tüm hizmetleri devre dışı bırakılmalıdır.

AGY.4.2.G6 VoIP'te Loglama

Verilerin, hangilerinin loglanacağına, ne kadar süreyle saklanması gerektiğine, kimlerin hangi koşullarda bu logları görüntüleyebileceğine karar verilmelidir. Tüm loglar yetkisiz erişime karşı korunmalıdır. Genel olarak, güvenlikle ilgili tüm sistem olayları loglanmalı ve değerlendirilmelidir.

3.2 2.SEVİYE GEREKSİNİMLER

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

AGY.4.2.G7 VoIP için güvenlik politikasının oluşturulması

VoIP için güvenlik gereksinimleri ve seviyesi, kurum güvenlik politikasına dahil edilmeli ve güvenlikle ilgili tüm genel özellikler burada belirtilmelidir. Ayrıca, güvenlik politikasında VoIP bileşenlerinin çalışması ve kullanımı için gereksinimler de düzenlemelidir. VoIP güvenlik politikaları ilgili tüm personel tarafından bilinmeli ve erişilebilir olmalıdır.

AGY.4.2.G8 VoIP'in şifrelenmesi

Hangi ses ve sinyalleşme bilgilerinin şifreleneceğine karar verilmelidir. Genel olarak, güvenli yerel ağdan ayrılan tüm VoIP veri paketleri uygun güvenlik mekanizmaları ile korunmalıdır. Şifreli haberleşme mümkün değil ise kullanıcılar bu konuda bilgilendirilmeli ve hassas olmaları sağlanmalıdır.

AGY.4.2.G9 Uygun VoIP bileşenlerinin seçimi

VoIP bileşenlerinin tedarikinden önce, piyasadaki mevcut ürünlere dayalı bir gereksinim listesi oluşturulmalıdır. Satın alma kararı verilmeden önce, alınacak ürünün işletim gereksinimlerini sağlayıp sağlamadığına dair bir değerlendirme yapılmalıdır. Aynı zamanda bu liste, istenen güvenlik düzeyini elde etmek için gereken tüm özellikleri içermelidir.

AGY.4.2.G10 Sistem yöneticileri için VoIP eğitimi

Sistem yöneticileri için bir eğitim tasarlanmalı ve gerçekleştirilmelidir. Bu eğitim, VoIP için uygulama alanlarını ve hata yönetimini kapsamalıdır.

AGY.4.2.G11 VoIP uç cihazlarının güvenli kullanımı [Kullanıcı]

Kullanıcılar, VOIP kullanırken karşılaşacakları temel tehditler ve bunlara karşı alacakları güvenlik önlemleriyle ilgili bilgilendirilmelidir. Yetkisi olmayan kişilerin kullanımını engellemek için, kullanıcılar kısa bir süre için bile uzaklaşsalar telefonu kilitlemelidir.

AGY.4.2.G12 VoIP bileşenlerinin güvenli şekilde kullanım dışı bırakılması

VoIP bileşenleri kullanım dışı bırakıldığında veya değiştirildiğinde, cihazların güvenlikle ilgili tüm bilgileri silinmelidir. Verileri sildikten sonra, işlemin başarılı olup olmadığının kontrolü sağlanmalıdır. Hassas bilgiler yedekleme ortamından da silinmelidir. Özellikle uç cihazlardaki tüm etiketler cihazlar atılmadan önce çıkarılmalıdır. Güvenlikle ilgili bilgilerin silinmesi; üreticiler, bayiler veya tedarikçilerle yapılan sözleşme ve garanti koşullarında göz önünde bulundurulmalı ve tanımlanmalıdır.

AGY.4.2.G13 VoIP kullanımı için güvenlik duvarı gereksinimleri

VoIP kullanımını planlarken, mevcut güvenlik duvarının VoIP kullanımına uyarlanıp uyarlanamayacağı kontrol edilmelidir. Aksi takdirde, ek bir güvenlik duvarı temin edilmeli ve kurulmalıdır.

3.3 3.SEVİYE GEREKSİNİMLER

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

AGY.4.2.G14 Sinyalleşmenin şifrelenmesi (GB)

Sinyalleşme bilgilerinin bütünlüğü ve gizliliği uygun şifreleme yöntemleri ile sağlanmalıdır. VoIP ağ geçidine erişim, IP adresleri ve H.323 kimliklerine dayanarak mümkün olduğunca kısıtlanmalıdır. Ayrıca, medya aktarımı ve sinyalleşme için uçtan uca güvenlik mekanizmaları kullanılmalı ve bu durum dokümante edilmelidir.

AGY.4.2.G15 SRTP kullanarak güvenli medya aktarımı sağlama (GB)

IP telefon sisteminde medya verilerini iletmek için Gerçek Zamanlı İletim Protokolü (RTP), bu verileri kontrol etmek için de Gerçek Zamanlı Akış Protokolü (RTSP) kullanılır. Kullanıcı verileri Güvenli Gerçek Zamanlı İletim Protokolü (SRTP) / Güvenli Gerçek Zamanlı İletim Kontrol Protokolü (SRTCP) kullanılarak korunmalıdır. Güvenlik ile ilgili bu uygulamalar dokümante edilmelidir.

AGY.4.2.G16 Veri ve VoIP ağının ayrılması (GBE)

VoIP ağı ile veri ağı birbirinden ayrılmalı ve bu ayrımın nasıl yapılması gerektiğine karar verilmelidir. VoIP ve veri ağına erişmesi gereken cihazların nasıl yönetileceğine de karar verilmelidir. VoIP ağındaki cihazlar diğer BT sistemlerine yalnızca VoIP amaçlı bağlantılar kurabilmelidir.

AGY: AĞ YÖNETİMİ

AGY:4.2.U VOIP UYGULAMA REHBERİ

AGY.4.2.U VOIP UYGULAMA

1 AÇIKLAMA

1.1 TANIM

Voice over IP (VoIP) veri ağları üzerinden özellikle de internet üzerinden yapılan sesli iletişim görüşmelerini ifade eder. Sinyalleşme bilgisinin iletilmesi için her aramaya özel sinyalleşme protokolleri kullanılır. Kullanıcı verisi (ses ya da video) ise bir medya aktarım protokolü ile iletilir. Her iki protokol de bir çoklu-ortam (multimedya) bağlantısının oluşturulması ve sürdürülmesi için gereklidir. Bazı yöntemlerde hem sinyalleşme hem de ortam verisi taşımak için tek bir protokol yeterli olmaktadır.

1.2 YAŞAM DÖNGÜSÜ

Planlama ve Tasarım

VoIP kullanımı “AGY.4.2.U1 VoIP dağıtımının planlanması” maddesi dikkate alınarak planlanmalıdır. Farklı cihaz üreticileri genellikle sadece bir VoIP protokolünü desteklediğinden, sinyalleşme protokolünün seçimi planlama aşamasında önem kazanmaktadır. Sinyalleşme protokolleri kendi arasında uyumsuz olduğundan, verilen karar VoIP bileşenlerinin seçimini de etkileyecektir.

IP iletişiminde yaşanan problemlerle, VoIP üzerinden konuşulurken de karşılaşılabilir. IP veri ağlarında, gizlilik ve bütünlüğe yönelik bilinen saldırıların çoğu doğrudan VoIP için gerçekleştirilebilir. Bunlardan korunmak için alınan tedbirlerin yanında sinyalleşme ve medya aktarım bilgilerinin şifrelenmesi de gerekir. Hangi ağlarda hangi içeriğin korunması gerektiği “AGY.4.2.U8 VoIP’in şifrelenmesi” maddesinde belirtilmiştir. Bununla birlikte, genel güvenlik politikası detaylı bir VoIP kullanım politikası ile desteklenmelidir. (bkz. AGY.4.2.U7 VoIP için güvenlik politikasının oluşturulması). “AGY.4.2.U14 Sinyalleşmenin şifrelenmesi” ve “AGY.4.2.U15 SRTP kullanarak güvenli medya aktarımı sağlama” başlıklarında da şifreleme ve medya aktarım güvenliği ayrıca detaylandırılmaktadır.

Tedarik

Sonraki adımda, uç cihazların ve VoIP ara katmanının nasıl tedarik edilmesi gerektiği açıklanmıştır. Bu amaçla yazılım ya da donanım kullanılabilir. Senaryolara göre ihtiyaçlar belirlenerek uygun ürünler seçilmelidir. “AGY.4.2. U9 Uygun VoIP Bileşenlerinin Seçimi” başlığında konuyla ilgili öneriler yer almaktadır.

Uygulama

Bir VoIP altyapısı oluşturmak veya mevcut altyapıdan VoIP'e geçiş yapmak için sistem yöneticilerine gerekli eğitimler verilmelidir (bkz. AGY.4.2.U10 Sistem yöneticileri için VoIP eğitimi). VoIP'e özel değişiklikler için mevcut veri ağında gerekli ayarlar yapılmalıdır. Bazı durumlarda iki paralel ağ oluşturulması fayda sağlayabilir. Fakat VoIP ses ağının geri kalan veri ağından ayrılması her zaman kolay olmayabilir. Bu ayrım "AGY.4.2.U16 Veri ve VoIP ağının ayrılması" başlığında anlatıldığı gibi mantıksal ya da fiziksel olarak yapılabilir. VoIP bileşenlerine erişim de ayrıca kısıtlanmalıdır. (bkz. AGY.4.2.U4 VoIP'te erişilebilirliği sınırlandırma)

Özellikle, genel bir ağdan erişim için bazı önlemler alınmalıdır. Bu önlemler genel ve özel ağ arasındaki geçişin ayarlanması ile ilgilidir. Özel IP adreslerinin Ağ Adresi Çevirisi (NAT) aracılığıyla genel IP adreslerine çevrilmesi bu ayarlara bir örnek olabilir. Bununla birlikte "AGY.4.2.U13 VoIP kullanımı için güvenlik duvarı gereksinimleri" başlığında açıklanan gereksinimler de güvenlik duvarlarına uygulanmalıdır.

İşletim

Kurulum ve test aşamasından sonra işletim süreci başlatılır (bkz. AGY.4.2.U2 VoIP ara katman güvenli yönetimi ve AGY.4.2.U3 VoIP uç cihazlarının kurulumu ve güvenli yönetimi). Önemli problemlerin çözümü için log tutulmalı ve gerektiğinde bu loglar değerlendirilmelidir. Konuyla ilgili daha detaylı bilgi "AGY.4.2.U6 VoIP'te loglama" uygulama maddesinde açıklanmaktadır.

Günümüzde ofis tipi uç cihazların bazıları oldukça karmaşık olmalarına rağmen, telefon kullanımı konusunda kullanıcı eğitimi verilmesi genellikle tercih edilmez. Ancak, kullanıcılar temel riskler hakkında bilgilendirilmelidir.

Kullanım Dışı Bırakma

Genellikle VoIP bileşenlerinin hafızalarında hassas bilgiler bulunur. Bu nedenle bileşenler kullanım dışı bırakılırken "AGY.4.2.U12 VoIP bileşenlerinin güvenli şekilde kullanım dışı bırakılması" maddesi dikkate alınmalıdır.

Acil Durum Hazırlık Planı

Arızalarda, donanım hasarlarında, kasıtlı veya kasıtsız veri silinmelerinde; depolanan tüm verilerin tekrar kullanılabilir olmasını sağlamak için düzenli ve kapsamlı veri yedeklemesi yapılmalıdır.

2 UYGULAMALAR

Aşağıda yer alan maddeler, VOIP kullanımına özel uygulama maddeleridir. VOIP kullanan kurum, kuruluşlar ve çalışanlar için dikkat edilmesi gereken hususlar, alınması gereken önlemler ve en iyi uygulama örnekleri aşağıda belirtilmiştir.

2.1 1. SEVİYE UYGULAMALAR

Öncelikli olarak aşağıdaki önlemler uygulanmalıdır.

AGY.4.2.U1 VoIP dağıtımının planlanması [BT Yöneticisi]

Kapsamlı dağıtım planlamasının oluşturulması, VoIP'in güvenli kullanımı için temel ön koşuldur. VoIP kullanımı genelden özele giden tasarım metoduna göre birkaç adımda planlanabilir. Tüm sistem için temel bir kavramdan başlayarak, belirli alt kavramlar için adım adım planlamalar yapılır. Planlama, yalnızca güvenlik ile bağlantılı olan kavramlarla değil, aynı zamanda normal işletimsel kavramlarla da ilgilidir.

Örneğin, ana hatlar aşağıdaki tipik sorular ile ele alınabilir:

- Tamamen mi yoksa kısmen mi VoIP'e geçilmek istenmektedir? VoIP, sadece mevcut devre anahtarlamalı PBX'ler arasındaki iletişim için mi kullanılacaktır?
- VoIP'in erişilebilirliği, telefon görüşmelerinin ve sinyalleşme bilgilerinin gizliliği ile bütünlüğü konusunda herhangi özel bir gereksinim var mıdır?
- Hangi sinyalleşme ve medya aktarım protokolleri kullanılacaktır?
- VoIP üzerinden kaç kullanıcı iletişim için etkin olacaktır?
- Genel telefon şebekesine bağlantı nasıl yapılacaktır? VoIP tabanlı iletişim ağına, genel telefon şebekesinden doğrudan bağlantı izni verilecek midir?
- Mevcut Yerel Ağların (LAN) güvenliği VoIP'ten etkilenmekte midir? VoIP kullanımı için mevcut Yerel Ağın kapasitesi yeterli midir? Ağ mimarisinde değişiklik yapılması gerekecek midir?

VoIP dağıtımını planlarken aşağıdaki alt kavramlar dikkate alınmalıdır:

- Şifrelemenin kapsamı: Hangi verilerin şifreleneceği belirlenmelidir. Örneğin, yerel ağ üzerindeki tüm iletişimin şifrelenmemesine karar verilebilir, ancak tüm harici çağrıların, üçüncü bir tarafça erişim ve manipülasyonuna karşı korunması gerekir (bkz. AGY.4.2.U8 VoIP'in şifrelenmesi). Ayrıca, çoklu ortam verilerinin ve sinyalleşmenin şifrelenip şifrelenmeyeceğine de karar verilmesi gerekir.
- Şifreleme yapısı: Bağlantıların uçtan uca şifrelenmesi kararlaştırılmışsa, korumanın nasıl uygulanacağına karar verilmelidir. Şifreleme hem H.235 veya SRTP gibi uygulama katmanında, (bkz. AGY.4.2.U14 Sinyalleşmenin şifrelenmesi

ve AGY.4.2.U15 SRTP kullanarak güvenli medya aktarımı sağlama) hem de Güvenli Giriş Katmanı (SSL) / Taşıma Katmanı Güvenliği (TLS), IPSec veya VPN'ler gibi alt katmanlarda gerçekleştirilebilir.

- Bileşen seçimi: Alınan kararların uygulanması için, kullanılan cihazların da bunu desteklemesi gerekir. Tüm gereksinimleri karşılayan bir cihaz temin edilemiyorsa mevcut planlama düzeltilmelidir. Bundan kaynaklanan değişiklikler güvenlik açısından değerlendirilmeli ve dokümante edilmelidir.
- Acil durum hazırlığı: Telefon altyapısına erişilebilirlik, sadece iş süreçleri açısından önemli bir gereklilik değildir. Arıza durumunda acil yardım numaraları (112, 155 vb.) da aranamaz. Bu nedenle uygun önlemlerin alınması gerekmektedir.
- Ağların ayrılması: Bazı durumlarda, VoIP ağının veri ağından mantıksal veya fiziksel olarak ayrılması yararlı olabilir (bkz. AGY.4.2.U16 Veri ve VoIP ağının ayrılması). Planlama aşamasında, bu ayrımın gerekli olup olmadığına karar verilmesi gerekmektedir.
- Özellikler: VoIP bileşenleri, temel özelliklerin yanı sıra bazı ek özellikler de sunabilir. Bu özellikler, ek bir ara katman bileşeninin çalışmasını gerektirebilir ve güvenlikle ilgili bazı dezavantajlara sahip olabilir. Mevcut bir çağrıya izinsiz müdahale, görüşme odasının izlenmesi ve interkom gibi özellikler güvenlik açısından kritiktir. Bu nedenle, planlama sırasında hangi özelliklerin kullanılacağına karar verilmelidir.
- Yönetim ve yapılandırma: Yönetim ve yapılandırma yetkisine kimin sahip olacağına önceden karar verilmelidir. VoIP'ten sorumlu bir sistem yöneticisi bunun için görevlendirilebilir. Ayrıca yönetimin nasıl yapılması gerektiğine karar verilmelidir (bkz. AGY.4.2.U2 VoIP ara katmanının güvenli yönetimi ve AGY.4.2.U3 VoIP uç cihazlarının güvenli yönetimi).
- Loglama: Tek tek VoIP bileşenlerinden gelen iletilerin loglanması, hataların teşhisi ve giderilmesinde veya saldırıların tespiti ve araştırılmasında önemli bir rol oynar. Planlama aşamasında hangi bilgilerin loglanması ve log verilerinin ne kadar süreyle saklanması gerektiğine karar verilmelidir. Logların sistemde yerel olarak mı yoksa ağdaki merkezi bir log sunucusunda mı saklanacağı da belirlenmelidir.

Planlama aşamasında alınan tüm kararlar, daha sonraki bir zamanda da yararlanılabilecek şekilde dokümante edilmelidir. Bu bilgilerin, dokümanı hazırlayanların dışındaki kişiler tarafından da değerlendirilebileceği dikkate alınmalıdır. Bu nedenle belgeler uygun şekilde yapılandırılmalıdır.

AGY.4.2.U2 VoIP ara katmanının güvenli yönetimi [BT Yöneticisi]

VoIP ara katmanının da diğer sunucu sistemleri gibi bir takım güvenlik önlemleriyle korunması gerekmektedir. Ayrıca, VoIP sistemlerine yönelik özel tehditlere karşı ilave güvenlik önlemleri de uygulanmalıdır.

VoIP bileşenleri devreye alınmadan önce güvenli bir şekilde yapılandırılmalıdır. İlk kurulum prosedürü oluşturulmalıdır. Aşağıda, güvenli bir yapılandırma ve yönetim için dikkate alınması gereken bazı noktalar sunulmaktadır.

Özellikler

VoIP sistemleri, geleneksel telekomünikasyon sistemleri gibi çeşitli özellikler sunar. Bir VoIP sistemini devreye almadan önce, hangi özelliklerin gerekli ve hangilerinin kullanılabilir olduğu açıklığa kavuşturulmalıdır. Gerekli olmayan ve güvenlik tehdidi oluşturan özellikler devre dışı bırakılmalıdır.

Yönetim ve Erişim

Ara katmanın yönetimi ve yapılandırması her zaman konsol ya da güvenli bağlantılarla gerçekleştirilmelidir. Yönetim, güvenli kabuk (SSH) veya VPN gibi güvenli bir bağlantı üzerinden gerçekleştirilebilir.

Birçok VoIP sistemi, web arayüzü üzerinden yapılandırmayı destekler. Yapılandırma için kullanılan web sunucusu ilave bir güvenlik riski oluşturabilir. Bu nedenle, yapılandırma arayüzü için kullanılacak web sunucusunun ağ geçidi (gateway) ve ağ geçidi denetçisi (gatekeeper) gibi kritik ara katmanlarda çalıştırılmaması önerilir. Ayrıca, web tabanlı yapılandırma kullanılacaksa, SSL veya TLS ile güvenli hale getirilmelidir.

Farklı yetki seviyelerine sahip rolleri içeren bir yönetim konsepti olmalıdır ve her bir role en az iki kişi atanmalıdır.

Yazılım tabanlı telefonları veya ara katman uygulamalarını, yaygın olarak kullanılan işletim sistemlerine sahip bilgisayarlara kurulmasında genellikle bir sakınca görülmemektedir. Bu şekilde kullanımlarda mümkünse, işletim sistemlerinin yönetimi VoIP uygulamalarının yönetiminden ayrılmalıdır.

Yapılandırmada yapılan değişiklikler, manipülasyonların izlenebilmesi için sistem tarafından loglanmalıdır. Loglar, sistem yöneticilerinin dahi müdahale edemeyeceği şekilde korunmalıdır. Loglar, WORM (Write Once Read Many) özelliğine sahip bir ortamda saklanmalı veya loglara erişim sınırlandırılmalıdır.

Yedekleme

Kapsamlı bir veri yedekleme stratejisi, olası bir problemde hızlı bir şekilde geri dönüşü sağlamak ve aynı zamanda bütünlüğü kontrol edebilmek için önemli bir gereksinimdir. Kişisel verilerin güvenliğini sağlarken, izinsiz erişime karşı korunacak şekilde depolanma sağlanmalıdır.

Yazılım Güvenliği

Kullanılan yazılımın (ör. İşletim sistemi) daima güncel tutulması ve güvenlikle ilgili yamaların gerçekleştirilmesi sağlanmalıdır.

Yalnızca orijinal güncellemelerin ve yamaların uygulandığı teyit edilmelidir. Örneğin, bir üreticinin İnternet sayfasından yapılan satın alımlarda ve VoIP bileşenlerine aktarımlarda bu madde geçerlidir. Aşağıdaki önlemler aktarım sırasında manipülasyonu daha zor hale getirebilir veya tespit edebilir:

- Sağlama toplamlarının (Checksum) karşılaştırılması,
- Güvenli haberleşme kanallarının kullanımı,
- Sertifikaların kullanımı.

Yazılımın düzgün uygulanması, sistemin güvenirliği için çok önemlidir. Özellikle, çağrı aktarımı gibi telefon sisteminin önemli fonksiyonları özel bir değerlendirme sürecine tabi tutulmalıdır.

İşletim Sistemi Güvenliği

VoIP bileşenleri farklı sunucularda farklı servisler çalışacak şekilde tasarlanmalıdır. Fakat özellikle tek bir donanım bileşeni olan kompakt ve bağımsız sistemlerde, servislerin tamamen ayrılması her zaman mümkün olmayabilir.

Kullanılan işletim sistemi tüm gereksiz bileşenlerden arındırılmış minimal bir işletim sistemi olarak tasarlanmalı ve ara katmanda çalışan uygulamalar mümkün olduğunca az sayıda tutulmalıdır. Her ilave uygulama, saldırı yüzeyini genişletebilir. Bu yüzden tam olarak hangi uygulamaların gerekli olduğuna karar verilmeli ve gereksiz uygulamalar kaldırılmalıdır. Derleyici gibi sadece kurulum için gerekli olan yazılımlar uç cihazlardan kaldırılmalıdır. Gerekli olmayan ağ servisleri devre dışı bırakılmalı ve diğer ağ servislerine erişim de paket filtreleyiciler tarafından sınırlandırılmalıdır.

AGY4.2 U3 VoIP uç cihazlarının kurulumu ve güvenli yönetimi

VoIP ara katmanı ve uç cihazları çok sayıda güvenlik gereksinimini karşılamalıdır. Ancak, ara katman ve VoIP uç cihazlarının güvenli olarak yapılandırılmaları için birbirinden farklı güvenlik önlemleri alınmalıdır.

Güvenilir Bellenim (Firmware) Güncellemeleri

Birçok VoIP uç cihazı, bellenimi otomatik güncelleme imkânı sunar. Yeni bellenimin, kod bütünlüğü ve güvenilirliği doğrulandıktan sonra kurulduğundan emin olunmalıdır. Eğer üretici güncellemeler için doğrulama imkânı veriyorsa veya güncelleme paketlerini dijital olarak imzalıyorsa, sağlama toplamları ve dijital imzalar kurulumdan önce doğrulanmalıdır. Eğer bu imkânlar üretici tarafından sağlanmıyorsa güncellemelerin güvenilir kaynaklardan alındığından emin olunmalıdır.

Güvenilir Yapılandırma ve Dijital Sertifikalar

Birçok VoIP uç cihazı, çeşitli yapılandırma seçenekleri sunar. Bunlara örnek olarak; uç cihazda yerel yapılandırma, uç cihaza entegre bir web sunucusuna erişerek yapılandırma ve http(s) veya TFTP sunucusundan çekerek otomatik yapılandırma gösterilebilir.

Genellikle yerel yapılandırma çok nadir kullanılır. Eğer bu yapılandırma tercih ediliyorsa bir şifreyle korunmalı, ayrıca kullanılmadığı durumlarda devre dışı bırakılmalıdır. Web tabanlı yapılandırma erişimi sadece şifreyle sağlanmalı ve SSL veya TLS gibi güvenilir bağlantılar kullanılmalıdır. İstemcileri doğrulamak için istemci sertifikası kullanarak ek koruma sağlanabilir.

TFTP sunucusu aracılığıyla yapılan otomatik yapılandırma yeterli seviyede güvenli olmadığından dolayı tercih edilmemeli ve devre dışı bırakılmalıdır. Özellikle, DHCP önyükleme işlemi sırasında bir TFTP sunucusunun otomatik seçimi birçok saldırı olasılığını doğurmaktadır.

Otomatik yapılandırma her zaman https sunucusu aracılığıyla yapılmalıdır. Https sunucusu, yapılandırma yüklenmeden önce, kendisini uç cihaz tarafından kontrol edilebilecek bir sertifikayla doğrulamalıdır. Sunucu sertifikası, genellikle ilk devreye almadan önce uç cihaza manuel olarak kurulur.

Güvenlik İşlevselliği

Birçok VoIP telefonu parola tabanlı tek veya çok seviyeli erişim kontrol seçeneği sunar. Kullanıcıların, telefonu sadece oturum açarak mı kullanacağına karar verilmelidir. Eğer parola koruması aktif ve oturum açılmadıysa, sadece acil durum çağrıları kullanılabilir olmalıdır. Yetkisiz erişimin önüne geçilmesi amaçlı, kullanıcılar kısa bir süre için bile uzaklaşsalar kullandıkları telefonu kilitlemelidir.

Giriş parolası gibi güvenlik fonksiyonları, hayata geçirilmeden önce doğru uygulandığından emin olmak adına ayrıntılı bir şekilde test edilmelidir. Test sürecinde bu güvenlik fonksiyonları kullanıcılar tarafından da kullanılmalıdır. Bununla birlikte kullanıcılar, güvenlik açıkları konusunda bilgilendirilmelidir.

Yazılım tabanlı telefonlar genellikle diğer işlemleri de yapan bir bilgisayarda çalışır. Bu durum aynı zamanda uygun bir seviyede güvenlik sağlayacak şekilde yönetilmelidir. Örneğin, bilgisayar üzerindeki mikrofonun üçüncü şahıslar tarafından aktifleştirilmesi önlenmelidir. Eğer bu önlem alınmadıysa, mikrofon bu şahıslar tarafından gizli dinleme amacıyla kötüye kullanılabilir.

Birçok fonksiyon barındıran iş istasyonlarının beraberinde getirdiği geniş saldırı alanı sebebiyle, yüksek koruma gerekli ise yazılım tabanlı telefonlar kullanılmamalıdır.

VoIP bileşenlerinin dokümanları, genellikle hangi güvenlik fonksiyonlarının desteklendiğiyle ilgili bilgi içerir. Hangi güvenlik fonksiyonlarının devreye alındığı dokümante edilmelidir.

AGY.4.2.U4 VoIP'te erişilebilirliği sınırlandırma [BT Yöneticisi]

Çoğu durumda, VoIP bileşenlerine internet üzerinden doğrudan erişim tavsiye edilmez. Örneğin, dahili bir IP adresine bağlantı kurma şeklindeki doğrudan erişimler, çok sayıda saldırı fırsatı doğurur. Bu nedenle, harici bir çağrının VoIP mimarisi aracılığıyla nasıl bağlanacağına karar verilmelidir.

İlk olarak, VoIP bileşenlerinin doğrudan harici bir bağlantıyı destekleyip desteklemediği kontrol edilmelidir. Genel olarak, devre anahtarlamalı telefon şebekesi (PSTN) kullanılarak kurulan bağlantı yeterlidir. Bu durumda, hiçbir dahili VoIP bileşeni genel telefon şebekesinden erişilebilir durumda olmaz. Genel devre anahtarlamalı telefon şebekesi (PSTN) ile yerel VoIP ağı arasında çalışan ağ geçidi de genel telefon şebekesinden erişilebilir olmamalıdır. Fakat VoIP aracılığıyla dışarıdan erişimin sınırlanması, harici çağrılar açısından dezavantaja sebep olur. Eğer genel telefon şebekesine bağlantı kurulacaksa, bu bağlantı yine de genel devre anahtarlamalı telefon şebekesi aracılığıyla gerçekleştirilmelidir. Bunun için yapılan maliyetler, genellikle SIP URL'si gibi bir VoIP adresine doğrudan bağlantı maliyetlerine oranla daha yüksektir. Bununla birlikte, özellikle güvenlik açısından kritik uygulamalarda birçok avantajı da olduğundan, VoIP üzerinden dışarıdan erişilebilirlik önemli bir özellik olarak görülmektedir.

Eğer genel telefon şebekesine doğru giden veya bu şebekeden gelen bağlantılara her koşulda izin verilmesi kararlaştırılırsa, alınan bu kararlar riskleri de içerecek şekilde dokümante edilmelidir. Ayrıca uygun güvenlik önlemleri alınmalıdır. Örneğin, tüm veri trafiği, vekil sunucu (Proxy server) gibi bağlantı isteklerini kabul eden ve bunları bir sonraki sunucuya veya doğrudan uç cihaza yönlendiren bir yoğunlaştırıcı (Concentrator) tarafından iletilmesi tercih edilebilir. Yoğunlaştırıcı kullanımı ayrıca, NAT (Network Address Translation) tanımları yapılırken ortaya çıkan problemleri de önleyebilir.

Bir yoğunlaştırıcı kullanırken aşağıdaki noktalara dikkat edilmelidir:

- Genel ve özel veri ağları arasındaki sinyalleşme ve ses verileri yoğunlaştırıcı aracılığıyla yönlendirilmelidir. Bu tip yapılarda bireysel bağlantıların kurulması önlenmelidir. Bu amaçla; paket filtreleri ve güvenlik duvarları, harici çağrılar yalnızca bir yoğunlaştırıcı aracılığıyla gerçekleştirilecek şekilde yapılandırılmalıdır. Örneğin, yoğunlaştırıcı güvenlik duvarının DMZ'inde çalıştırılabilir. Bu yöntemle yerel ağdan genel ağa veya genel ağdan yerel ağa doğrudan bağlantı önlenebilir.
- Bütünsel yaklaşan bir sinyalleşme standartlarının bulunmaması nedeni ile mümkün olduğunca çok sinyalleşme protokolünün desteklenmesi tavsiye edilir. Bu sebeple yoğunlaştırıcı, yerel veri ağlarının kullandıkları protokoller ile harici kullanılan protokoller arasında ağ geçidi olarak çalışabilmelidir.
- Dahili ağdan harici veri ağına doğru olan çağrılara, kötüye kullanımı önlemek için yoğunlaştırıcıda doğrulama işlemi yapıldıktan sonra izin verilmelidir.
- Yerel veri ağı içindeki bağlantılara yoğunlaştırıcı dahil edilmemelidir.
- Sesli iletişime ek olarak hangi fonksiyonların harici abonelere sağlanacağı tanımlanmalıdır.
- Yoğunlaştırıcı, çok büyük veri paketleri gibi protokole uymayan tüm sinyalleşme ve ses paketlerini tespit edip engellemelidir.
- Yoğunlaştırıcıya genel veri ağından doğrudan erişilebilmesi nedeniyle yapılandırma kritik güvenlik seviyesine uygun olmalıdır.
- Genel telefon şebekesinden arayanlar, bağlantı kurabilmek için yoğunlaştırıcının IP adresini bilmelidir. Bu yüzden, bir DNS sunucusunda yoğunlaştırıcının IP adresini yayınlanması önerilir.
- Ses ve sinyalleşme bilgisinin alınması, işlenmesi ve iletilmesi yüksek kaynaklar gerektirebilir. Bu yüzden, ağ bağlantısı ve sistem kaynakları en verimli olacak şekilde yapılandırılmalıdır.
- Eğer erişilebilirlik konusunda çok talep varsa, yoğunlaştırıcı yedekli olarak tasarlanmalıdır. Yedekli bir tasarım ile yapılan yük dağıtımında, kalan sistemler olası bir hatayı telafi etmek için yeterli kaynak sağlamalıdır.

Birçok üretici bu amaç için lisanslı sistemler sunmakla beraber, açık kaynaklı yazılımlar ile de bu gereksinimlerin çoğu karşılanabilir.

AGY.4.2.U5 VoIP ara katmanının güvenli kurulumu

VoIP ara katmanının işlevselliği ve güvenliği, büyük ölçüde yapılandırma parametreleri tarafından belirlenir. VoIP kullanımı için ağ geçidi ve ağ geçidi denetçisi gibi farklı bileşenler

de gerekebileceğinden; bir bileşen üzerinde, diğer bileşenlerle koordine olmadan yapılan parametre değişimi, iletişimde problemlere yol açabilir.

VoIP hizmeti verilmeye başlandıktan sonra da sistem yöneticileri tarafından birçok değişiklik yapılması gerekebilir. Örneğin, çalışanların işten ayrılması veya yeni çalışanların işe başlaması durumunda bazı değişikliklerin yapılması gerekecektir. Aynı zamanda, çalışanlar başka bir ağ segmentine geçtikleri durumda (ör. başka bir binaya taşındıklarında) da ayarlamalar yapılabilmelidir. Bu sebepten dolayı sistem yöneticisinin bu ayarlamaları verimli bir şekilde yapmasını sağlayacak bir kurulum arayüzünün olması önemlidir.

Genellikle, VoIP kullanımı için her kullanıcıya birer kullanıcı adı ve parola tanımlanır. Kullanıcılar, çok kısa ve tahmin edilmesi kolay olan parolaları seçmemelidir. Sadece güçlü parolalara izin veren ayarlar etkinleştirilmelidir. Statik IP adresine sahip sabit cihazları olan kullanıcıların, yalnızca bu IP adresinin atandığı cihazla oturum açmasına izin verilmelidir.

Kullanıcı adı ve telefon numaraları atanırken, mevcut iç gereksinimlere uyulmalıdır. Herhangi bir kullanıcıya atanmamış (kullanıcıyla eşleştirilmemiş) olan telefon numaralarına da ayrıca dikkat edilmelidir. Örneğin, konferans odalarındaki telefonlara ziyaretçiler tarafından da serbestçe erişilebilir. Prensip olarak, bu telefonlara mümkün olduğunca az izin verilmesi gerektiğinden, sadece dahili kullanıcıların aranabilmesi yeterli ve uygun olacaktır.

Genel olarak, hangi kullanıcının hangi sinyalleşme protokolünü kullanacağını tanımlamak mümkündür. Yönetim karmaşasını engellemek için, eğer mümkün ise, tüm kullanıcıların sadece tek bir protokolü kullanmasına izin verilmelidir. Eğer uç aygıtlar şifrelenmiş sinyalleşmeyi destekliyorsa, şifrelenmemiş kayıtların mümkün olmadığından emin olunmalıdır.

Telekomünikasyon sistemlerinin kullanıcılarına belirli haklar atanabilir veya geri çekilebilir. Örneğin, yurt dışı aramalar veya özel servis numaralarına doğru yapılan aramalar sınırlandırılabilir. Yapılandırma sırasında, her kullanıcının yalnızca kendisiyle ilgili haklara sahip olduğundan emin olunmalıdır.

Sistem yöneticileri, yapılandırmayı kolaylaştırmak için koşullara uyarlanmış kendi makrolarını geliştirebilirler. Makroları kullanmadan önce, detaylı kalite güvence testlerine tabii tutulduklarından emin olunmalıdır. Aksi takdirde, tespit edilmesi zor olan yapılandırma hatalarına veya istenmeyen sonuçlara sebep olabilirler. Bu makrolar detaylı olarak dokümante edilmelidir.

Yapılandırma sırasında, kesinlikle gerekli olmayan ilave servisler devre dışı bırakılmalıdır. Aksi takdirde, bu servislerin saldırılar için kullanılma riski doğar.

VoIP ara katmanında, olayları takip etmek amacıyla loglama yapılabilir. Örneğin, sinyalleşme bilgisi hangi kullanıcının, kiminle, ne kadar süre telefonda kaldığını değerlendirmek için kullanılabilir. Eğer, ortam bilgileri doğrudan uç aygıtlar arasında değil, ara katman yazılımı aracılığıyla iletiliyorsa, temel olarak konuşma içeriğinin merkezi olarak değerlendirmesi yapılabilir. Loglama fonksiyonları VoIP operasyonlarının izlenebilirliğini arttırırken diğer taraftan, bu fonksiyonların bilgi güvenliği ihlalleri konusunda kötüye kullanılması da engellenmelidir.

Hangi bilginin loglanacağı ve log verisinin nasıl değerlendirileceği belirlenmeli ve belirlendiği şekliyle düzenli olarak uygulanmalıdır. İlgili bütün birimler değerlendirme sürecine dahil edilerek detaylı incelemeler yapılmalıdır. Bütün ayarlar düzenli olarak denetlenmelidir.

AGY.4.2.U6 VoIP'te loglama

VoIP üzerinden iletişim kurarken birçok bilgi loglanabilir. Çoğu zaman, sorunsuz bir işletim için VoIP ara katmanın belirli durum bilgilerinin loglanması gerekir. Bu logların değerlendirilmesiyle, aygıtların doğru çalışıp çalışmadığı tespit edilebilir. Ayrıca çoğu zaman, loglar kullanılarak saldırı denemelerinin izi sürülebilir ve yapılandırma buna göre değiştirilebilir.

Yalnızca doğru bir filtreleme ile çok sayıda verinin içerisinden anlamlı bir bilgiye ulaşılabileceğinden, loglama işlevinin dikkatli yapılandırılması çok önemlidir.

Logların önem seviyesine göre hızlı bir şekilde müdahale edilmesi gerekebileceğinden, tutulan loglar düzenli olarak değerlendirilmelidir.

Loglama fonksiyonları VoIP operasyonlarının izlenebilirliğini arttırırken, diğer taraftan bu fonksiyonların bilgi güvenliği ihlalleri konusunda kötüye kullanılması da engellenmelidir. Hangi bilginin loglanacağı ve log verisinin nasıl değerlendirileceği belirlenmeli ve belirlendiği şekliyle düzenli olarak uygulanmalıdır. İlgili bütün birimler değerlendirme sürecine dahil edilerek detaylı incelemeler yapılmalıdır. Logların kapsamı ve değerlendirme kriterleri kurum içerisinde belirlenip kayıt altına alınmalıdır.

Sinyalleşmenin Loglanması

Sinyalleşmenin analiz edilmesiyle çok miktarda bilgi elde edilebilir. Bir SIP vekil sunucuda, ağ geçidinde veya ağ geçidi denetçisinde aşağıdaki veriler loglanmalıdır:

- Kim, kimi aradı?

- Görüşme ne kadar sürdü?
- Aranan kişi çağrıya cevap verdi mi?
- Çağrı hangi ağdan ve hangi IP adresinden yapıldı?
- Hangi ortam aktarım protokolleri ve hangi kodek kullanıldı?

Bu bilgiler, masraf hesaplama veya VoIP alt yapısının optimizasyonu gibi süreçlerde kullanılabilir.

Ortam Aktarımının Loglanması

Ağda uygun bir noktada, belirli şartlarda çağrı içerikleri loglanabilir. Çağrıların, vekil sunucu gibi bir noktada ağdan ayrılması durumunda, loglama doğrudan burada yapılabilir.

Dahili çağrılar için çoğu zaman bir vekil sunucuya ihtiyaç duyulmayabilir. Bu durumda ise, çağrı içeriklerinin ilgili uç cihazlarda veya yönlendiricilerde loglanması mümkün olabilir.

Şifrelenmiş medya aktarımında; kriptografik anahtarlar görüşmeye katılan taraflarca karşılıklı olarak doğrudan paylaşılırsa, merkezi bir yerde daha az bilgi toplanmış olur.

Sistem Durum Bilgisinin Loglanması

Eğer mümkün ise, aşağıda bahsedilen bilgiler de VoIP ara katmanında loglanmalıdır:

- Ara katman yazılımı veya donanımı üzerinde açılan bütün oturumlar,
- Ara katman yapılandırma değişiklikleri,
- VoIP hizmetindeki hatalı oturum açma bilgileri,
- Sistem hataları,
- İş yükü,
- Kullanıcı yönetimindeki değişiklikler (kullanıcı ekleme veya çıkarma, kullanıcı ve telefon numarası arasındaki eşleştirmedeki değişiklikler gibi),
- VoIP uygulamasının çalıştığı BT sisteminde hataya sebep olabilecek donanım arızaları gibi kritik olaylar.

Log Verisinin Merkezi Yönetimi

Log verisinin, bir ağ üzerinden ayrı bir syslog sunucusuna aktarılması önerilir. VoIP donanımlar genellikle bunun için yeterli kaynağa sahip olmadığından, log verilerinin merkezi olarak toplanması, arşivlenmesi ve değerlendirilmesi için bu yöntem kullanılır. Merkezi log sunucusunun tercih edilmesi durumunda; eğer bir VoIP donanımı saldırıya uğrarsa, log verisi zaten sunucuya iletilmiş olduğundan, saldırgan tarafından da manipüle edilemez.

Eğer log verisinin syslog sunucusuna iletimi sırasında şifreleme uygulanmıyorsa, iletim yolunu dinlemek mümkündür. Bu nedenle, loglar yalnızca sunucunun kendisine

kaydedilmelidir. Bu yapılamıyorsa aktarım şifrelenmeli veya yönetim ağı gibi ayrı bir ağ üzerinden yapılmalıdır.

Zaman Senkronizasyonu

Mümkünse tüm log verilerinin zaman bilgisi doğru olmalıdır. Bu şekilde, saldırı denemelerinin ve tamamlanan saldırıların analizinde, verinin etkili bir şekilde değerlendirilmesi sağlanabilir. Bu nedenle, uygun bir sunucu NTP gibi bir protokolle dahili ağdaki bütün sistemlere doğru zamanı sağlamalıdır

2.2 2. SEVİYE UYGULAMALAR

1.seviye uygulamalar sonrasında, VoIP işletimini daha iyi bir seviyeye getirmeyi düşünen kurumlar aşağıdaki uygulamaları dikkate alarak, iyileştirme/geliştirme faaliyetlerini gerçekleştirebilirler.

AGY.4.2.U7 VoIP için güvenlik politikasının oluşturulması

Telefon hizmeti verilirken, erişilebilirlik konusu daha ön planda tutulmasına yanı sıra gizlilik konusuna da aynı derecede önem verilmelidir. Gizlilik ve erişilebilirlik konusundaki beklentileri karşılamak için mevcut güvenlik politikalarının kapsamı, telekomünikasyon donanımının güvenli ve düzgün çalışmasını da sağlayacak nitelikte olmalıdır.

VoIP için belirlenen güvenlik gereksinimleri ve güvenlik seviyesi, kurum güvenlik politikasına uygun olmalıdır. Genel güvenlik politikasının yanında, VoIP'e özel detaylı bir güvenlik politikası da oluşturulmalıdır. Buna ek olarak, BT, parola ve internet kullanımına ilişkin yönergeler gibi diğer yönergeler de dikkate alınmalıdır.

VoIP bileşenlerinin planlaması, tedariki ve işletiminden sorumlu olan bütün personel VoIP güvenlik politikasını bilmeli ve çalışmalarını buna uygun yapmalıdır. Bu politikanın içeriği ve uygulanıp uygulanmadığı düzenli olarak kontrol edilmelidir.

Güvenlik politikası, öncelikle güvenlik seviyesini belirlemeli ve VoIP'in işletimi için gerekli temel gereksinimleri içermelidir. Dikkate alınması gereken bazı hususlar aşağıdaki şekilde listelenmiştir.

VoIP kullanımına ilişkin genel düzenlemeler

Tüm VoIP kullanıcıları, VoIP kullanımının sağladığı faydaların yanı sıra, alınan güvenlik önlemlerinin sınırları olduğunun ve bunun da potansiyel risk oluşturduğunun farkında olmalıdır.

VoIP bileşenleriyle ilgili sürekli yeni güvenlik açıkları ortaya çıktığı için güncel riskler takip edilmeli ve çalışanlar bu riskler hakkında bilgilendirilmelidir.

Güvenlik politikasında aşağıdaki hususlar açıkça belirtilmelidir:

- VoIP bileşenlerinin nerede kullanılıp nerede kullanılmayacağı,
- VoIP'in hangi teknik çalışma koşullarında kullanılacağı,
- Hangi bilgilerin VoIP aracılığıyla görüşülemeyeceği,
- Hangi özelliklerin ve fonksiyonların destekleneceği.

Farklı güvenlik düzenlemeleri gerekebileceğinden dolayı tüm kullanıcılar, VoIP'i hangi durumlarda kurumlarının dışından kullanabilecekleri konusunda bilgilendirilmelidir.

VoIP Ara katmanı

VoIP ara katmanının işletimi için güvenlik politikasında aşağıdaki maddelere yer verilmelidir:

- VoIP bileşenlerinin temin edilmesinden önce bir gereksinim listesi oluşturulmalıdır (AGY.4.2.U9 Uygun VoIP bileşenlerinin seçimi).
- Sorumluluklar tanımlanmalı ve düzenlenmelidir.
- Sistem yöneticisinin çalışmaları için bazı sorular cevaplandırılarak güvenlik politikasında düzenlemeler yapılmalıdır. Örnek olarak;
    - Sistem yöneticisinin hangi yollardan sisteme erişim izni olacak (konsol veya yönetim ağı gibi ayrı bir ağ üzerinden vb.)?
    - Hangi yönetimsel işlemler dokümante edilecek?
    - BT sistem yöneticisi ile VoIP yöneticisinin sorumluluk alanları ayrılabilir mi?
- Montaj ve yapılandırma için aşağıdaki gibi süreçler tanımlanmalı ve dokümante edilmelidir:
    - İlk kurulum için prosedürün oluşturulması,
    - Güvenlik riskleri kapsamında varsayılan ayarların kontrol edilmesi,
    - Yapılandırma işleminin gerçekleştirilmesi.
- Kullanıcılar için yetkilendirme ve görev tanımları yapılmalıdır:
    - Kimlik doğrulama ve yetkilendirme yöntemleri, güncellemeler, yapılandırma değişiklikleri gibi tanımlamaların yapılması.
    - Kullanıcılar oluşturulup telefon numaralarının atanması,
    - Kullanıcılara ücretli hizmet numaralarını arayabilmeleri gibi belirli öncelikler verilmesi.
- Güvenli işletim için aşağıdaki düzenlemeler gereklidir:
    - Dokümantasyonun oluşturulması, kapsamı (işletim talimatları, çalışma kitapçığı vb.) ve güncellenmesi,
    - İzin verilecek hizmetlerin ve protokollerin belirlenmesi,

  - Halka açık ağlarda dahili VoIP sistemlerine doğrudan bağlantı izni verilmemesi,
  - Yazılım güncellemelerinin uygulanması,
- VoIP ara katmanının çalıştığı BT sistemlerinin güvenlik politikalarının oluşturulması,
  - Ara katmanın çalıştığı işletim sisteminde hangi güvenlik önlemlerinin uygulanacağının belirlenmesi,
  - Şifreli sinyalleşme ve ortam aktarım protokollerinin kullanılması,
  - İşletim ve bakım için hangi araçların kullanılacağının belirlenmesi,
- Loglamayla ilgili aşağıdaki hususlar belirlenmelidir:
  - Hangi olayların loglanacağı,
  - Log verilerinin nerede depolanacağı,
  - Log verilerinin nasıl değerlendirileceği.
- VoIP bileşenlerindeki verilerin yedeklenmesi ve kurtarılması için kurum genelinde bir yedekleme politikası oluşturulmalıdır.
- İşletimden kaynaklı kesilmelere, güvenlik ihlal olaylarına ve teknik aksaklıklara müdahale etmek için gerekli düzenlemeler yapılmalıdır (ör. yerinde müdahale, uzaktan destek vb.).

VoIP Uç Cihazları

VoIP uç cihazlarının işletimi için güvenlik politikasında olması gereken maddeler aşağıda yer almaktadır:

- VoIP uç cihazlarının temin edilmesinden önce bir gereksinim listesi oluşturulmalıdır.
- Sistem yöneticilerinin görev ve sorumluluklarıyla ilgili düzenlemeler yapılmalıdır. Kullanılacak yazılım tabanlı telefon yönetiminin BT sistem yönetiminden ayrılması buna bir örnek olarak verilebilir.
- Güvenlik politikasına, kurulum ve yapılandırma gereksinimleri dahil edilmelidir. Bunun için aşağıdaki sorular cevaplanmalıdır:
  - Fiziksel telefonlar için varsayılan yapılandırma yeterli mi yoksa farklı bir yapılandırma mı gereklidir?
  - Uç cihaz sayısının fazla olması durumunda, yapılandırma değişiklikleri merkezi mi yoksa tek tek mi yapılmalıdır?
  - Sistem yöneticileri hangi erişim yöntemleriyle uç cihazlara ulaşabilir?
  - Kullanıcıların, arama yönlendirme gibi hangi tür yapılandırma değişikliklerini yapmasına izin verilecektir?

- Güvenli işletim için aşağıdaki düzenlemeler gereklidir:
  - Yönetimin güvenli hale getirilmesi (ör. sadece güvenli bağlantılarla erişim),
  - Şifreli sinyalleşme ve ortam aktarım protokollerinin kullanılması,
  - İşletim ve bakım için kullanılacak araçların var olan ağ yönetimine entegrasyonu,
  - Yazılım güncellemeleri ve yapılandırma değişiklikleri için gerekli prosedürlerin oluşturulması ve yetkilendirmelerin yapılması,
  - Kullanıcı, telefonun yanında değilken yapılacak işlemlerin tanımlanması (arama yönlendirme veya telefonun kilitlenmesi vb.),
  - Yazılım tabanlı telefonun çalıştığı işletim sisteminde hangi güvenlik önlemlerinin uygulanacağının belirlenmesi,
  - Acil durum hazırlığı için alternatif iletişim kanallarının belirlenmesi.

VoIP güvenlik politikasının uygulanmasına ilişkin sorumluluk BT'ye aittir. Bu politikadaki değişiklikler ve sapmalar ise yalnızca Bilgi Güvenliği ekibi ile mutabık kalınarak yapılabilir.

AGY.4.2.U8 VoIP'in şifrelenmesi

Bir saldırgan dahili ağa erişmeyi başardıysa, Yerel Ağ üzerindeki bütün haberleşmeyi görüntüleyebilir. Eğer VoIP verisi şifrelenmemiş ise saldırgan bütün içeriği okuyabilir. Örneğin, sinyalleşme bilgisini değerlendirerek kimin, kiminle, ne kadar süre görüştüğü bilgisine ulaşabilir. Bununla birlikte, bir saldırgan medya aktarım protokolü aracılığıyla alınıp verilen mesajları değerlendirerek, telefon konuşmalarını dinleyebilir ve gizli bilgilere erişebilir. Bu nedenle, VoIP kullanıcı verilerinin şifrelenmesi özellikle göz önünde bulundurulması gereken bir konudur. Ancak, şifrelemenin bütün telekomünikasyon sistemleri tarafından desteklendiği teyit edilmelidir.

Bir yerel ağ içerisindeki VoIP telefon çağrıları için şifrelemenin gerekli olmadığı düşünülebilir. Fakat yerel ağa dışarıdan bir saldırgan tarafından güvenli olmayan bir ağ aracılığıyla erişilemeyeceğinden emin olunmalıdır. Bununla birlikte, dahili çağrıların yerel ağdan yapılacak saldırılardan da korunması gerekeceğinden burada uygulanacak şifreleme faydalı olabilir. Bu amaçla, VoIP cihazlarının VPN uç noktaları olarak çalışması veya SRTP gibi şifreli bir medya aktarım protokolü kullanılması düşünülebilir.

Kullanılan tüm VoIP cihazları şifreli sinyalleşme protokollerini destekliyorsa, bu protokollerin kullanılması önerilir. Bunların dışında, saldırganın başkasına ait parolalara erişip, bunları kullanarak oturum açması da şifrelemeyle önlenebilir.

Eğer VoIP paketleri güvenli yerel ağın dışına çıkıyorsa uygun prosedürlerle korunmalıdır. VoIP haberleşmesini korumak için aşağıda verilen prosedürlerden biri veya daha fazlası kullanılmalıdır:

- SRTP (Secure Realtime Transport Protocol) gibi şifreli ortam aktarım protokollerinin kullanımı,
- Sinyalleşme protokollerini TLS (Transport Layer Security) vb. yöntemlerle şifrelenmesi,
- **VPN (Virtual Private Networks) kullanımı**

Farklı lokasyonlardaki Yerel Ağlar arasında VPN ağ geçitleri kullanılarak bilgi şifreli olarak iletilebilir. Bireysel cihazlar VPN uç noktası olarak çalışabilirler. Bu durum içerden bir saldırganın da bilgiye erişmesini engeller. VPN kullanarak sinyalleşme ve ortam aktarım protokollerinin doğrudan şifrelenmesi yerine, protokolden bağımsız bir şifreleme yapılmış olur. Örneğin, farklı binalarda bulunan VoIP ara katmanları arasındaki bağlantı, herhangi bir şifreleme mekanizması ile korunmuyorsa, bütün çağrılar bir saldırgan tarafından dinlenebilir. Bu durumu önlemek için kurum binaları arası bağlantı, VPN kullanılarak korunabilir. Eğer VoIP ara katman yazılımı bir BT sistemi üzerinde çalışıyorsa, bir VoIP protokolünden bağımsız olarak VPN desteği kolaylıkla sağlanabilir.

- **Kablosuz ağın şifrelenmesi**

Bir kurum içerisindeki güvenli olmayan kablosuz ağlara, aynı zamanda kurum dışından da erişilebilir. Eğer VoIP kullanıcıları bir kablosuz ağ aracılığıyla bağlanıyorsa, bu kablosuz ağlar WPA2 gibi bir şifreleme yöntemiyle korunmalıdır (bkz. AGY.2.1 Kablosuz Ağlar Rehberi). Ancak, bu şifreleme kablosuz ağ ile sınırlı olduğundan, yerel ağın geri kalanında bilginin korumasız olarak iletildiğinin de ayrıca bilinmesi gereklidir.

Eğer kullanıcıya genel telefon şebekesi aracılığıyla bir telefon çağrısı yapılacaksa, VoIP uç cihazı ile IP - PSTN geçişini sağlayan ağ geçidi arasındaki bağlantı; şifreli sinyalleşme protokolleri, VPN veya şifreli ortam aktarım protokolleriyle korunabilir. Az sayıda telefon, devre anahtarlamalı ağlar için koruma mekanizması sağladığından ve bu korumaların aktivasyonu ilgili alıcıya bağlı olduğundan, VoIP ağ geçidi ile bu telefonlar arasındaki şifreleme çoğu zaman etkin değildir.

Şifreli haberleşme mümkün değil ise kullanıcılar bu konuda bilgilendirilmeli ve hassas olmaları sağlanmalıdır. Eğer şifreleme mevcut değil ise gizli görüşmeler telefon üzerinden yapılmamalıdır.

VoIP bileşenleri tedarik edilirken, şifreli sinyalleşme ve ortam aktarım protokollerini (ör. SRTP) veya TLS gibi şifreleme yöntemlerini desteklediklerinden emin olunmalıdır.

AGY.4.2.U9 Uygun VoIP bileşenlerinin seçimi

Çeşitli telekomünikasyon firmaları, telefon hizmeti için sayısız çözümler sunmaktadır. Sadece VoIP teknolojisini destekleyen cihazlar ya da hem analog hem de dijital mimariyi destekleyen cihazlar tedarik edilebilir. VoIP mimarisi ile bir devre anahtarlamalı telefon şebekesi arasında geçiş yapılabilen ağ geçitleri buna örnek olarak gösterilebilir. Seçim yapılırken, gerekli sinyalleşme ve medya aktarım protokollerinin desteklenmesi gibi temel özelliklere ek olarak, güvenlikle ilgili hususlar da dikkate alınmalıdır.

VoIP bileşenlerinin tedarikinden önce, piyasadaki mevcut ürünlere dayalı bir gereksinim listesi oluşturulmalıdır. Satın alma kararı verilmeden önce, alınacak ürünün işletim gereksinimlerini sağlayıp sağlamadığına dair bir değerlendirme yapılmalıdır.

Genel Gereksinimler

VoIP donanımı ve yazılımı satın alınırken dikkat edilmesi gereken gereksinimler aşağıda listelenmektedir:

1. Genel Kriterler

- Bir VoIP donanımı mı yoksa standart bir PC üzerinde çalışabilecek bir yazılım mı tedarik edilecek? Her iki durumda da işletim sistemi, yalnızca gereken işlevleri etkinleştirilecek, erişim hakları kısıtlı olarak atanacak ve zayıf noktaları ortadan kaldırılacak şekilde yapılandırılmalıdır.
- Ürün, gerekli tüm protokolleri destekliyor mu?
- Ürünle ilgili tedarikçi ya da üretici tarafından gerekli eğitimler veriliyor mu?
- VoIP bileşenleri, performans gereksinimlerini karşılayabilir mi?
- Ürün değerlendirmesi, Ortak Kriterler (Common Criteria) gibi resmi bir yönteme dayanıyor mu?
- VoIP bileşeni, mevcut ürünlerle uyumlu çalışabilir mi?
- VoIP bileşeni, güvenli oturum açma ve kullanıcı yönetimini destekliyor mu?
- Ürün dokümanı, tüm teknik ve yönetimsel detayları ayrıntılı şekilde içeriyor mu?
- VoIP bileşeni için sunulan bir bakım sözleşmesi var mı? Bakım sözleşmesinde müdahale ve çözüm süreleri tanımlanmış mı? Teknik sorunlar için hızlı dönüş alınabilecek bir teknik destek hattı var mı?
- Ürün kolayca kurulabilir, yapılandırılabilir ve yönetilebilir mi?

2. Loglama

Loglama için önerilen çözümler, en azından güvenlik politikasında belirtilen koşulları karşılamalıdır. Aşağıdaki hususlara özellikle dikkat edilmelidir:

- Log seviyesi yapılandırılabiliyor mu?
- Loglama yapılarak ilgili tüm veriler kayıt edilebiliyor mu?
- Loglara erişimin güvenliği sağlanıyor mu?
- Sistem, merkezi loglamayı destekliyor mu?
- Yapılacak loglama yasal mevzuat hükümlerini yerine getiriyor mu?

3. Güncelleme

- Ürün için düzenli olarak güncellemeler ve yamalar sunuluyor mu? Bir güvenlik açığı bulunduktan sonra bununla ilgili güvenlik yamaları kısa sürede sunuluyor mu?
- Güvenlik açıklarının giderildiği ve ek güvenlik mekanizmalarının sağlandığı yazılım güncellemeleriyle, sinyalleşme ve medya aktarım protokollerinin de yeni sürümleri sağlanıyor mu?
- İşletim sistemi güncellemeleri gibi VoIP bileşeni ile doğrudan ilgili olmayan diğer güncellemelerin yapılması düşünülüyor mu?
- Cihazın işletim sistemindeki veya yazılımın kurulduğu bilgi teknolojileri sistemindeki mevcut güvenlik açıkları da güncelleniyor mu?
- Güncellemeler ve yamaların, aktarım sırasında manipüle edilmiş sürümlerle değiştirilmesinden korunması için bir mekanizma sağlanıyor mu?

4. Yönetim

- VoIP bileşenleri, güvenli yönetim protokollerini destekliyor mu?
- VoIP bileşenleri, istenilen güvenlik kriterlerini sağlayacak şekilde yapılandırılabilir mi?
- Kritik yapılandırma parametrelerinin kullanıcılar tarafından değiştirilmesine karşı koruma sağlanıyor mu?

VoIP bileşenleri, merkezi bir yönetim arayüzü ile yönetilebilir mi? Yazılım arayüzü, hatalı veya tutarsız yapılandırmayı önleyecek şekilde tasarlanmış mı?

5. Şifreleme

VoIP üzerinden şifrelenmiş iletişim kurmak için ilgili cihazların bu özelliği desteklemesi gerekmektedir. Koruma ihtiyacına bağlı olarak, planlama sırasında dahili VoIP iletişiminin şifrelenmemesine karar verilebilir. Bununla birlikte yine de, şifreleme yeteneğine sahip olan ya da sonradan bu özellik eklenebilen VoIP bileşenleri tercih edilmelidir.

Aşağıdaki hususlar dikkate alınmalıdır:

- VoIP bileşenleri, medya aktarım ve sinyalleşme bilgilerinin şifrelenmesini destekliyor mu veya bu özellik daha sonra eklenebilir mi?

- VoIP bileşenleri, VPN uç noktaları olarak çalışabilir mi?

Anahtarlama Sistemlerinin Seçimi (Ara Katman)

Telefon, genellikle iş süreçlerinin önemli bir parçasıdır. Bu nedenle, erişilebilirlik konusunda yüksek talepler oluşabilir. Dolayısıyla tedarik yapılırken aşağıdaki kriterler dikkate alınmalıdır:

- VoIP ara katmanı yedeklenebilir mi?
- Üretici yüksek erişilebilirlik çözümleri sunuyor mu?
- Tüm VoIP işlevini, merkezi cihazlar mı sağlamalı yoksa birbirine bağlı birkaç cihaz mı sağlamalı? Birbirine bağlı cihazlara örnek olarak kayıt sunucuları, vekil sunucuları ve konum sunucuları gösterilebilir. Tüm VoIP işlevlerini sağlayan bir merkezi çözümün yapılandırılması genellikle daha kolay olabilir. Birden fazla cihazın yönetimi genellikle daha karmaşık olduğundan, yanlış yapılandırmalar daha olasıdır.

Aktif Ağ Bileşenlerinin Seçimi

VoIP'e geçiş için, ağ anahtarı gibi yeni ağ bileşenleri tedarik edilecekse, bu bileşenlerin VoIP'e özel gereksinimleri de karşılaması gerekir. VoIP, mevcut bir veri ağı üzerinden kullanılacaksa, ağ cihazları VoIP paketlerini tanımalı ve bunları iletebilmelidir. İki farklı yerel ağ arasında, internet gibi güvenli olmayan bir ortam üzerinden arama yapabilmek için ek gereksinimlere ihtiyaç duyulacaktır. Örneğin, herhangi bir şifreleme önlemi alınmamışsa, güvenli olmayan ağa bağlı ağ geçitleri, VPN uç noktaları olarak kullanılabilmelidir.

AGY.4.2.U10 Sistem yöneticileri için VoIP eğitimi

Telefon hizmeti, dayandığı teknolojiden bağımsız olarak, bir kurumdaki iletişimin temelidir. Bu nedenle, sistemi yönetecek personelin gerekli işlevleri ve güvenlik özelliklerini en iyi şekilde kullanabilmeleri için yeterli eğitimi almış olmaları gerekmektedir.

Eğitim, VoIP bileşenlerinin kurulumu ve işletimi için gerekli prosedürler, araçlar ve teknikler hakkında yeterli bilgiyi sağlamalıdır. Ayrıca bu eğitim, VoIP bileşenlerinin farklı üreticilere özgü özelliklerini de kapsamalıdır. VoIP'in verimli kullanımı için ayrıntılı bir ağ bilgisi gerektiğinden, bu bilgilere de eğitimde mutlaka yer verilmelidir.

Eğitim, genel olarak aşağıdaki konuları içermelidir:

- Ses ve görüşmenin VoIP bileşenleri üzerinden sıkıştırılması ve iletim sırasında oluşabilecek dalga bozulumu (jitter), yankı, gecikme gibi etkiler hakkında temel bilgiler,
- Uygulama katmanında kullanılan protokoller hakkında temel bilgiler (ör. RTP, SIP ve H.323).
- Sistem Yönetimi:
  - Her VoIP bileşeni için kurulum, işletim, bakım, sorun giderme ve güvenlikle ilgili temel bilgiler,
  - VoIP bileşenlerinin çalıştırılacağı BT sistemlerinin yönetimi,
  - VoIP işletimindeki yasal mevzuat hükümleri,
  - Kullanılacak bileşen ve araçların yönetimi,
  - Loglama,
  - Yapılandırma verilerini koruma ve yönetme,
  - Saldırı senaryoları (ör. ARP kimlik sahtekârlığı, IP kimlik sahtekârlığı, DNS sahtekârlığı, virüsler ve diğer kötü amaçlı yazılımlar),
  - VPN'in temelleri,
  - Şifreleme ve şifrelenmiş verilerle ilgili temel kavramlar (ör. SRTP veya IPSec ile şifreleme).
- Ağ Teknolojisi:
  - Ağ altyapısı ve hizmet kalitesi ile ilgili temel bilgiler,
  - IP ile ilgili temel bilgiler ve buna dayalı protokoller (ör. IP adresleme, ICMP, TCP, Kullanıcı Datagram Protokolü (UDP))
  - Sanal yerel alan ağı (VLAN) ile ilgili bilgiler.
- Sorun Giderme:
  - Hata kaynakları ve nedenleri,
  - Ölçüm ve analiz araçları,
  - Sorun giderme için test stratejileri.

Sistem yöneticileri arasında görev dağılımı yapılmış olsa bile, bu görevlilerin genel olarak tüm sistemler hakkında temel bilgilere sahip olması önemlidir. Buna dayanarak, bireysel uzmanlık alanları da genişletilebilir.

Üreticiler ve tedarikçiler, genellikle sağladığı ürünlerle ilgili detaylı eğitimler de sunmaktadır. Dolayısıyla, belirli bir üreticiye karar verirken mevcut eğitimlerin niteliği de göz önünde bulundurulmalıdır.

BT bileşenlerinin tedarikinde, eğitim için de yeterli bir bütçe planlanmalı ve tüm sistem yöneticileri için bir eğitim planı hazırlanmalıdır.

AGY.4.2.U11 VoIP uç cihazlarının güvenli kullanımı [Kullanıcılar]

Kullanıcılar, VOIP kullanırken karşılaşacakları temel tehditler ve bunlara karşı alacakları güvenlik önlemleriyle ilgili bilgilendirilmelidir. Bu bilgilendirmeler, talimatların veya broşürlerin yardımıyla yapılabilir. Kullanıcılar, normalin dışında bir davranışla karşılaştıklarında, bu durumu ilgili sistem yöneticilerine rapor etmeleri konusunda uyarılmalıdır.

Birçok VoIP telefonu, parola tabanlı erişim kontrol seçeneği sunar. Eğer, oturum açılması için parola koruması aktif hale gelmiş ise, sadece acil yardım numaraları kullanılabilir olmalıdır. Yetkisi olmayan kişiler tarafından kullanımı engellemek için kullanıcılar, kısa bir süre için bile uzaklaşsalar telefonu kilitlemelidir.

Kullanıcılar, çok kısa ve tahmin edilmesi kolay olan parolaları seçmemelidir. Sadece güçlü parolalara izin veren ayarlar etkinleştirilmelidir. Statik IP adresine sahip sabit cihazları olan kullanıcıların, yalnızca bu IP adresinin atandığı cihazla oturum açmasına izin verilmelidir.

AGY.4.2.U12 VoIP bileşenlerinin güvenli şekilde kullanım dışı bırakılması

Uç cihazlar veya ara katman gibi VoIP bileşenlerinin yenileriyle değiştirilmesi veya tamamen kullanım dışı bırakılması gerekiyorsa, güvenlikle ilgili tüm bilgilerin cihazlardan silinmesi gerekir. Örneğin, cihazların hurdaya çıkarılması, taşınması, diğer kullanıcılara aktarılması ve üretici, tedarikçi veya atık imha şirketlerine verilmesi durumunda güvenlikle ilgili bilgiler cihazlardan silinmelidir. Ayrıca, yapılan bu güvenlik uygulaması onarım, bakım ve garanti değişimi için de geçerlidir.

Güvenlikle ilgili bilgilerin silinmesi; üreticiler, bayiler veya tedarikçilerle yapılan sözleşme ve garanti koşullarında göz önünde bulundurulmalı ve tanımlanmalıdır.

Bileşenlerin kullanım amacına bağlı olarak, aşağıdaki bilgiler cihazlarda saklanabilir:

- Kimin kimi aradığının listesi,
- Aramaların zamanı ve konuşma süresi,
- VoIP altyapısında oturum açmak için gerekli olan kullanıcı adı ve parolalar,
- Kullanıcıların yetkileri,
- Telesekreter bilgileri,
- Bırakılan sesli mesajlar,
- Sesli posta için kullanıcıların e-posta adresleri,
- IP adresleri ve ağ yapısını gösteren diğer bilgiler,

- Log dosyaları,
- Sertifikalar ve anahtarlar,
- Yapılandırma dosyaları,
- Kişisel telefon rehberi,
- Kurum telefon rehberi,
- Randevu hatırlatıcı gibi ek servislerin üzerinde tutulan kayıtlar,
- İstisnai durumlarda, görüşme içeriklerinin kayıtları.

Arızalı veya güncel olmayan cihazlar, kullanımdan kaldırılmadan veya değiştirilmeden önce bu verilerin silinmesine veya okunamaz hale getirilmesine dikkat edilmelidir. Verileri sildikten sonra, işlemin başarılı olup olmadığının kontrolü yapılmalıdır.

VoIP bileşenleri olarak kullanılan BT sistemlerinin diskleri, uygun bir araçla silinerek dosyalar geri yüklenemez hale getirilmelidir. Örneğin, BT sistemlerini harici bir önyükleme ortamından başlatıp, disklerin üzerine rastgele veriler tekrar tekrar yazılarak, silinen dosyaların kurtarılması engellenebilir.

VoIP cihazlarında ise bir sabit sürücünün takılı olup olmadığına veya verilerin kalıcı bir bellekte (non-volatile memory) depolanıp depolanmadığına bağlı olarak farklı prosedürler uygulanabilir. Cihazlar genellikle, tüm yapılandırma ayarlarının varsayılan değerlere döndürüldüğü bir "Fabrika Sıfırlaması" seçeneği sunar. Fabrika sıfırlaması yaptıktan sonra, verilerin gerçekten silindiği veya belirli veri dosyalarının hala kullanılabilir olmadığı kontrol edilmelidir.

Cihazlarda depolanan bilgilere ek olarak, hassas bilgilerin yedekleme ortamında da bulunup bulunmadığı kontrol edilmelidir. Yedekleme ortamının arşivleme ya da yasal düzenlemeler gibi sebeplerden dolayı saklanması gerekli değilse, cihaz kullanım dışı bırakıldıktan sonra ortam silinmelidir.

Bileşenler üzerindeki etiketler genellikle, hızlı arama tuşları, IP adresleri ve telefon numaraları gibi teknik bilgiler içerebilir. Bu nedenle, bileşenler atılmadan önce etiketler de çıkarılmalıdır.

AGY.4.2.U13 VoIP kullanımı için güvenlik duvarı gereksinimleri

VoIP için bir IP veri ağı kullanılıyorsa, özellikle bu ağın güvenliğini sağlama amaçlı ilave gereksinimler olabilir. Ses ve veri ağlarını kesin bir şekilde birbirinden ayırmak mümkün değildir. Örneğin, yazılım tabanlı telefonlar, ses ağındaki VoIP sunucusuna veri ağı üzerinden erişim sağlar. Buna ek olarak, farklı lokasyonlara sahip olan bir kurumda, lokasyonlar arasındaki bağlantı, hem kurum genelindeki iletişim için hem de veri alışverişi için kullanılabilmektedir.

Güvenlik duvarı; dahili ve güvenli bir sistemi, güvenli olmayan bir ağdan yetkisiz erişime karşı korumak ve sınırlandırılmış alanlara yetkili erişime izin vermek için tasarlanmıştır. Bir ağın güvenli olup olmadığı, hangi kaynakların korunması gerektiği ve bunların nasıl korunacağı, kurumun güvenlik politikalarında belirtilmelidir.

VoIP kullanımını planlarken, mevcut güvenlik duvarının VoIP kullanımına uyarlanıp uyarlanamayacağı kontrol edilmelidir. Aksi takdirde, ek bir güvenlik duvarı temin edilmeli ve kurulmalıdır.

Güvenlik Duvarının Seçimi ve Gereksinimleri

VoIP kullanırken, güvenlik duvarının performansı sadece güvenliği değil, aynı zamanda iletilen sesin kalitesini de etkiler. VoIP'te birçok küçük veri paketinin işlenmesi, güvenlik duvarına ilave yük getirerek iletilen ses sinyallerinin dalga bozulumuna ve gecikmesine sebep olabilir.

VoIP trafiği güvenlik duvarının üzerinden geçiyorsa, kullanılan sinyalleşme protokollerini analiz edebilen ve ilgili durumları kaydedebilen VoIP özellikli bir güvenlik duvarı kullanılmalıdır. Bu şekilde protokol verilerine dayanarak, gerekli portlar iletişim süresi boyunca açılır (ör. RTP ile iletilen ses verileri için kullanılacak UDP portları).

Doğru sistemin seçimi aşağıdaki faktörlere bağlıdır:

- Ağ ne kadar büyüktür?
- Mevcut yönlendiriciler ve anahtarlar, güvenlik duvarlarının işlevlerini desteklemekte midir?
- Veri ağı için bir güvenlik duvarı mevcut mudur?
- IP telefonun yalnızca yerel ağda mı kullanılması planlanmaktadır?
- İlgili BT personelinin VoIP konusunda yetkinliği nelerdir?
- Güvenlik hedeflerini uygulamak için ne kadarlık bir bütçe planlanmaktadır?

Güvenlik Duvarı Kavramı

VoIP için mevcut veya yeni bir güvenlik duvarının kullanılıp kullanılmayacağına bakılmaksızın, güvenlik duvarı aşağıdaki kavramları içermelidir:

- **Durum Denetimsiz Paket Filtreleme (Stateless Packet Filter)**

  Veri ve ses ağlarını ayırmak için yönlendiricilerde, 3. katman ağ anahtarlarında veya güvenlik duvarlarında basit paket filtreleme yapılabilir. Filtreleme işlevi bu şekilde kullanıldığında, durum denetimli paket filtrelemeye veya uygulama katmanı ağ geçitlerine kıyasla önemli ölçüde sınırlıdır.

- **Durum Denetimli Paket Filtreleme (Stateful Packet Inspection)**

  Durum denetimli paket filtreleri, bir iletişim için gereken dönüş paketlerini dinamik olarak geçirerek ağ için daha yüksek bir güvenlik düzeyi sağlayabilir. Bir bağlantının durum bilgisini saklayarak, mevcut bağlantıya ait dönüş paketlerine açık erişim listelerini (ACL) yapılandırmak zorunda kalmadan izin verebilirler.

- **Uygulama Katmanı Ağ Geçidi**

  Bir uygulama katmanı ağ geçidi, yukarıda belirtilen sistemlerin aksine, sadece IP adreslerine ve bağlantı noktalarına göre değil, aynı zamanda uygulama katmanına göre de filtreleme yapabilir. Uygulama katmanı ağ geçidinin avantajı, özellikle RTP paketleri iletilirken ortaya çıkar. RTP iletimi için kullanılacak UDP portları, sinyalleşmenin bir parçası olarak uç noktalar arasında Oturum Tanımlama Protokolü(SDP) aracılığıyla değiştirilir. Kullanılacak UDP portları genellikle her yeni aramada değiştiğinden, bu portlara güvenlik duvarında da izin verilmelidir. Uygulama katmanı ağ geçidi, IP adresleri ile kullanılacak UDP bağlantı noktalarının üzerinde anlaşıldığı protokol mesajlarının değişimini izlediğinden, ilgili RTP akışının geçmesine izin veren filtreleri dinamik olarak ayarlayabilir.

Durum denetimsiz paket filtrelerini, durum denetimli paket filtrelerini ve uygulama katmanı ağ geçitlerini karşılaştırmak gerekirse, avantajları nedeniyle uygulama katmanı ağ geçidinin kullanılması önerilir. Gelen RTP trafiğinin etkinleştirilmesi ve ses verisine sahip RTP paketlerine izin verilmesi için, durum denetimli ve durum denetimsiz güvenlik duvarlarında geniş port aralıklarının kalıcı olarak açılması gerekir. Böyle bir yapılandırma önemli bir güvenlik riski oluşturabilir.

Uygulama katmanı ağ geçitleri, iletişim süresi boyunca sadece gerekli olan portları açar ve bu nedenle daha az potansiyel saldırı yüzeyi sunar.

IAX (Inter-Asterisk eXchange) gibi protokollerin kullanılması güvenlik duvarının tasarımını kolaylaştırır. Hem sinyalleşme hem de ortam aktarım bilgisi mesaj akışı yoluyla iletildiğinden, sadece bir port tanımlanması yeterlidir. Port müzakeresi yapılmadığından dinamik port filtrelemesine gerek yoktur.

Güvenlik Duvarı Konfigürasyonu

VoIP'te kullanılan güvenlik duvarları klasik güvenlik duvarlarından pek farklı değildir. VoIP'e özgü ayarların nasıl uygulanacağı, kullanılan ürünün dokümanında bulunabilir.

2.3 3. SEVİYE UYGULAMALAR

Aşağıda, koruma ihtiyacının artması durumunda dikkate alınması gereken önlemler listelenmiştir. Parantez içinde verilen harfler, hangi temel değerlerin öncelikle korunduğunu gösterir (G = gizlilik, B = bütünlük, E = Erişilebilirlik).

AGY.4.2.U14 Sinyalleşmenin Şifrelenmesi (GB)

VoIP kullanırken sinyalleşme bilgilerinin bütünlüğünü ve gizliliğini sağlamak, medya akışlarını korumaktan çok daha önemlidir. Bunu yapmanın bir yolu, sinyalleşme bilgisini şifreli VPN kanalları üzerinden taşımaktır. Başka bir yolu da kendi koruma mekanizmalarını sağlayan sinyalleşme protokollerini kullanmaktır. VoIP sinyalleşmesi için en önemli protokoller, SIP ve H.323 çerçevesindeki H.225 ile H.245'tir. Bu sinyalleşme protokollerinin güvenlik mekanizmaları aşağıda açıklanmaktadır.

Bu protokollere ek olarak, kendi güvenlik mekanizmalarına sahip olmayan IAX2 gibi diğer sinyalleşme protokolleri de vardır. Ayrıca, kendi güvenlik mekanizmalarını sunmayan, medya ağ geçitlerini kontrol etmek için kullanılan MGCP gibi özel sinyalleşme protokolleri de vardır. Bu nedenle, bu protokoller genellikle ağ katmanındaki uygun güvenlik önlemleri kullanılarak güvence altına alınmalıdır.

H.235

H.323 çerçevesi üzerinden gerçekleşen sinyalleşme, taşıma veya ağ katmanındaki güvenlik mekanizmaları (ör. SSL, TLS veya IPSec) ile korunabilir. Sinyalleşme protokolünden bağımsız olan bu mekanizmalar, ilave güvenlik gereksinimleri olan ortamlar için kullanılabilir. Ek olarak, standart bir koruma ihtiyacı olduğunda, sinyalleşmenin tek koruması olarak bütünlüğü ve gizliliği korumak için de H.235 protokolü kullanılabilir. Sinyalleşmenin H.323 ile korunup korunmayacağına veya nasıl korunacağına karar verilmeli ve bu karar dokümante edilmelidir.

H.235, H.323 tabanlı telefon hizmetini korumak için kapsamlı güvenlik mekanizmaları tanımlar. Belirtilen bu mekanizmalar özellikle çağrı sinyalleşmesinin (H.225 / Q.931) ve kontrol kanalının (H.245) korunmasının yanı sıra medya akışının güvenliğini de içerir.

H.235, şifrelenmiş bir H.245 kontrol kanalının veya şifrelenmiş bir mantıksal kanalın uç noktaları olan bileşenlerini, kimlik doğrulaması gereken güvenilir bileşenler olarak kabul eder. Güvenilir ve kimlik doğrulaması yapan sistem bileşenlerine örnek olarak ağ geçitleri verilebilir.

Aşağıdaki kimlik doğrulama türlerinden biri seçilmelidir:

- **Simetrik şifreleme ve paylaşılan, önceden belirlenmiş gizli bir bilgi (ör. parola) kullanılarak kimlik doğrulama:** Simetrik şifreleme veya kriptografik hash fonksiyonuyla şifreleme yöntemleri kullanılabilir. Paylaşılan, önceden belirlenmiş gizli bilgi her durumda simetrik bir şifreleme anahtarı olarak kullanılabilir.
- **Onaylı ortak (Public) anahtarlara ve imzalı mesajlara dayalı kimlik doğrulama:** Bu yöntemlerin her biri, zaman damgaları kullanan iki mesajla veya meydan okuma-karşılık verme protokolü (challenge-response authentication) kullanarak rastgele üç meydan okuma mesajıyla uygulanabilir.
- **Diffie-Hellman anahtar değişim protokolü:** Her iki iletişim tarafı da sertifikalı ortak anahtarlara dayanan bir Diffie-Hellman protokolü çalıştırır. Bu şekilde üretilen ortak simetrik anahtar isteğe bağlı ikinci kimlik doğrulama aşamasında kullanılır.

H.235 ayrıca, RTP paketinin alıcı bilgisini, orijinal olup olmadığını ve yetkili bir gönderenden gelip gelmediğini kontrol edebilir. Bunun için, RTP paketlerinin seçilen alanlarında kısa bir MAC (Mesaj Kimlik Doğrulama Kodu) hesaplanır ve alıcı, RTP Paketlerinin işlenmesine başlamadan önce bunu kontrol eder. MAC bir şifreleme algoritmasıyla ya da bir hash fonksiyonuyla hesaplanabilir.

Bu mekanizma, bilinen RTP portlarında RTP flood ve SPIT (Spam over IP Telephony) olarak yapılan DoS saldırılarını önlemeye yöneliktir ve mümkünse etkinleştirilmelidir.

VoIP ağ geçitleri, H.235 üzerinden iletişimi desteklemiyorsa, IP adreslerine ve H.323 kimliklerine dayanarak ağ geçidine erişimin mümkün olduğunca kısıtlanması önerilir. Bu nedenle bir ağ geçidi denetleyicisi kullanılması ve VoIP ağ geçidine erişimin yalnızca "Yönlendirme Modu"nda kısıtlanması önerilir. Ağ geçidi denetleyicisinin yalnızca kimlik doğrulama ve kayıt işlemine dahil olduğu "Köprüleme Modu"nun aksine, "Yönlendirme Modu"nda tüm sinyalleşmeler ağ geçidi denetleyicisi aracılığıyla gerçekleşir.

SIP

SIP gibi sinyalleşme protokollerini güvence altına almanın temel zorluğu, sinyalleşmenin genellikle birkaç farklı bileşeni (uç cihazlar, sunucular vb.) içermesi ve bu bileşenlerin her bir sinyalleşme mesajını okumak veya değiştirmek zorunda olmasıdır. Bu nedenle, uçtan uca güvenlik mekanizmalarının basit bir şekilde uygulanması mümkün değildir, uygulamaya özel ayarlamalar yapılmalıdır.

SIP standardı, uygulama katmanının altındaki katmanlarda güvenlik mekanizmalarının kullanımını destekler. SIP bileşenleri (UA, vekil sunucu, yönlendirme ve konum sunucusu)

arasındaki iletişimin güvenliği genellikle "hop-by-hop" mekanizması ile sağlanır. Artan güvenlik gereksinimleri sebebiyle, medya aktarımını korumak için ilave uçtan uca güvenlik mekanizmalarının da (ör. SRTP için anahtar değişimi) gerekli olup olmadığına dikkat edilmelidir.

Özellikle artan güvenlik gereksinimleri ile SIP sinyalleşmesi SSL veya TLS (Taşıma Katmanı Güvenliği) ile korunmalıdır. SIP protokolünü anlatan RFC 3261 dokümanında, tüm uyumlu SIP sunucularının karşılıklı kimlik doğrulama ve tek yönlü kimlik doğrulama ile TLS protokolünü desteklemesi gerektiği belirtilir. Uç cihazlar, vekil sunucu, yönlendirme ve kayıt sunucularıyla iletişimini korumak için TLS kullanmalıdır.

AGY.4.2.U15 SRTP kullanarak güvenli medya aktarımı sağlama (GB)

IP telefon sisteminde medya verilerini iletmek için Gerçek Zamanlı İletim Protokolü (RTP), bu verileri kontrol etmek için de Gerçek Zamanlı Akış Protokolü (RTSP) kullanılır. Her iki protokol de IP çağrılarının dinlenmesi ve değiştirilmesine karşı kendi koruma mekanizmalarını sağlayamamaktadır. Bundan dolayı, RTP ve Gerçek Zamanlı İletim Kontrol Protokolü (RTCP) için koruma mekanizmaları sağlayan protokoller SRTP ve SRTCP kullanılabilir. VoIP'te, SRTP ve SRTCP kullanılarak kullanıcı verilerinin korunmasına dikkat edilmeli ve bu karar dokümante edilmelidir.

Genel Bakış

VoIP kullanırken, RTP'ye dayalı medya iletiminde, tekrarlama saldırılarına karşı gizlilik ve koruma elde etmek için SRTP kullanılabilir. Bu şekilde, güvenilir tek yöne yayım ve yayımlama sağlanır. İletim için kullanılan RTP ve RTCP paketleri, SRTP ve SRTCP paketlerinde gömülüdür.

Anahtar Yönetimi

SRTP protokolü, şifreleme ve kimlik doğrulama için bir ana anahtar ve bir oturum anahtarı tanımlar. SRTP, en az 128 bit'lik bir ana anahtara ihtiyaç duyar. Ancak bunun oluşturulması ve yönetimi için bir mekanizma içermez. Bu durum, Multimedya İnternet Anahtarlama (MIKEY) gibi diğer standartlarla sağlanabilir.

SRTP kullanımında, ana anahtarın ve oturum anahtarının hangi aralıklarla değiştirildiği tanımlanmalıdır.

Şifreleme

VoIP'te SRTP kullanırken, simetrik şifreleme yöntemi AES-CTR (Gelişmiş Şifreleme Standardı - Sayaç Modu) etkinleştirilmelidir. Bu, hem uçtan uca hem de bölüm bölüm ("hop-by-hop") şifreleme için uygundur.

Özgünlük ve Bütünlük

RTP mesajlarının özgünlüğü ve bütünlüğü, HMAC-SHA1 işlevine karşılık gelen bir oturum anahtarıyla birlikte kullanılarak SRTP'de güvence altına alınabilir. İletilen sağlama toplamının önerilen uzunluğu 80 bittir. Buna göre, HMAC-SHA1'in 160 bitlik sağlama toplamı 80 bite indirilmelidir. Bu durum, SRTP paketlerinin iletim boyutunu azaltmasına rağmen, iletilerin bütünlüğünün korunmasını zayıflatır. Bu nedenle, bu ayar yalnızca istisnai durumlarda etkinleştirilmelidir. Alternatif olarak, diğer bilinen hash algoritmalarına dayanan fonksiyonlar da kullanılabilir. Seçim yapılırken, bazı yaygın hash algoritmalarının şifreleme zayıflıklarının bulunduğuna dikkat edilmelidir. Bundan dolayı, Hash fonksiyonunun seçimi gerekçelendirilmeli ve dokümante edilmelidir. Aynı güvenlik mekanizması SRTCP için de sağlanabilir.

SRTP, zayıf olan ya da hiç olmayan kimlik doğrulamaya izin verir. Bu durum saldırganların şifreli mesajı manipüle ederek sonraki şifreleri çözmek için anlamlı mesajlar elde etmesine yol açabilir. Mümkünse, RTP paketleri için zayıf kimlik doğrulaması kullanılmamalıdır. RTCP için artan güvenlik gereksinimlerinde, HMAC-SHA1 sağlama toplamı etkinleştirilmelidir.

Tekrarlama Saldırılarına Karşı Koruma

SRTP; bir saldırganın, yakalanan RTP veya RTCP paketlerini depoladığı ve daha sonra DoS saldırıları gerçekleştirmek için bunları yeniden gönderdiği tekrarlama saldırılarına karşı koruma sağlar. Tekrar mesajlarını önlemek için bütünlük koruması ve mesaj kimlik doğrulaması mevcut olmalıdır. SRTP paketlerinin alıcısı, daha önce doğrulanan paketlerin bilgisini içeren bir tekrarlama listesi (Replay list) tutar.

Tekrarlama listesine kaydedilebilecek maksimum sayı önceden belirlenmelidir. Yeni bir paket alındığında, bu liste eşleşmeler için kontrol edilir ve tekrarlanan paketler atılır. Belleği daha düşük olan IP telefonlar için tekrarlama listesinin uzunluğu, artan güvenlik gereksinimleri durumunda dikkate alınması gereken bir güvenlik parametresidir. Tekrarlama listesinin kapsamı mümkün olduğunca büyük seçilmeli ve karar dokümante edilmelidir.

MIKEY ile anahtar yönetimi

MIKEY (Multimedya İnternet Anahtarlama), gerçek zamanlı multimedya iletişimi için anahtar yönetimini tanımlar. Ayrıca, bu protokol katılımcılar arasında anahtar ve diğer güvenlik parametrelerinin değiştirilmesini sağlar. VoIP'te MIKEY, uç cihazlar arasında güvenli SRTP iletimini sağlamak için ana anahtar ve diğer güvenlik parametrelerini değiştirmek için kullanılabilir.

MIKEY, H.323 veya SIP gibi temel sinyalleşme protokollerinden bağımsızdır. MIKEY ayrıca farklı iletişim oturumları ve iletişim protokolleri için anahtar ve güvenlik parametrelerinin paralel olarak değiştirilmesini destekler. Buna göre, RTP ve RTCP bağlantılarını ayrı ayrı güvenli hale getirmek mümkündür. MIKEY, birkaç paralel oturum için ortak bir ana anahtar kullanılmasına izin verir. Böylece, VoIP konferansları daha verimli bir şekilde güvence altına alınır.

VoIP kullanımı şifreleme mekanizmaları kullanılarak güvence altına alınacaksa, VoIP sistemleri tarafından desteklenen anahtar değişim prosedürleri belirlenmeli ve dokümante edilmelidir.

AGY.4.2.U16 Veri ve VoIP ağının ayrılması (GBE)

Ağların VLAN'lar ile ayrılması

Yerel ağlar, etkin ağ bileşenleri tarafından fiziksel olarak veya uygun bir VLAN yapılandırmasıyla mantıksal olarak bölümlere ayrılabilir. VLAN özellikli anahtarlarla 2.katmanda mantıksal bir ayrım yapılabilir. Ancak, yalnızca VLAN'lara ayırmak fiziksel olarak bir VLAN'a bağlanan BT sistemlerini (ör. PC, dizüstü bilgisayar veya sunucu) saldırılara karşı korumaz. Telefonun kullandığı ağ soketi herkes tarafından erişilebilir olduğundan, bir saldırgan bu sokete doğrudan bağlanarak VLAN'daki telefonlara saldırabilir (ör. VLAN'a telefon yerine PC bağlayarak). Bu nedenle, bu tür saldırılara karşı, mantıksal ağ ayrımının ötesinde başka önlemler de alınmalıdır.

Ağların fiziksel olarak ayrılması

Artan güvenlik gereksinimleri nedeniyle, ses ağının veri ağından fiziksel olarak tamamen ayrılması yararlı bir uygulama olabilir. Veri ve ses ağlarının fiziksel olarak ayrılması saldırı olasılığını önemli ölçüde azaltır. Ayrılan ses ve veri ağlarının birbirlerinin kullanımı üzerinde hiçbir etkisi yoktur. Ayrıca, kablo ya da herhangi bir ağ bileşeninin arızası sebebiyle bir ağda oluşacak kesinti durumunda, iletişime kalan ağ üzerinden de devam edilebilir.

Ağları ayırmada karşılaşılabilecek problemler

VoIP ağının IP veri ağından ayrılması bazı noktalarda ek performans gereksinimleri ortaya çıkarabilir:

- VoIP bileşenleri, tipik olarak veri ağında bulunan LDAP dizinleri gibi kullanıcı veri tabanlarına erişim gerektirir, ancak aralarındaki bağlantı kesilirse sorunun kaynağını tespit edebilmek için her iki tarafın da kontrol edilmesi gerekebilir.
- VoIP ağının yönetimi sırasında, DNS üzerinden isim çözümleme gibi ihtiyaçlar için genellikle veri ağına erişim gerekir.

- Ağlar ayrılırsa VoIP bileşenlerinin yönetimi daha karmaşık olabilir. Örneğin, VoIP bileşenlerinin yazılım güncellemeleri ağlar ayrıldıktan sonra veri ağı üzerinden (ör. SFTP yoluyla) yapılamayacağından, bu işlemlerin direkt yerinde yapılması gerekir. Ayrıca, VoIP bileşenlerinin uzaktan yapılandırılması (ör. SSH veya HTTPS yoluyla) için de, bir veri ağına ya da ayrı bir BT sistemine bağlantısı gerekir.

Ancak, bu sorunlar, veri ve ses ağı arasındaki uygun ağ geçitleri ile çözülebilir. Birçok hizmet için, ses ağında bir vekil sunucu çalıştırılabilir ve ses ağından veri ağına doğru yapılan talepler veri ağına iletilir.

- E-posta istemcisine sahip VoIP telefonlar veya yaygın yazılım tabanlı telefonlar gibi çok işlevli aygıtların kullanılması, ağ ayırımında daha fazla sorun yaratır. Bu aygıtların hem ses hem de veri ağına erişmesi gerekir. Bu noktada fiziksel bir ayrım yapılması mümkün değildir. Bu sorunu çözmenin bir yolu, cihazları kendileri için oluşturulan mantıksal bir ağda çalıştırmaktır.
- Kablolama eforunu azaltmak için birçok telefonun entegre bir mini ağ anahtarı vardır. Telefondaki ağ anahtarının bir portu doğrudan duvardaki ağ soketine bağlanır ve bilgisayar gibi başka bir BT sistemi de telefondaki ağ anahtarının diğer portuna bağlanır. Bu düzenlemeyle, ses ve veri ağı fiziksel olarak ayrılamaz. Mantıksal bir ayırma için erişim anahtarı, tek portuna bağlı iki cihazı birbirinden ayırt edebilmelidir. Örneğin MAC adresi veya IEEE 802.1X protokolü yoluyla bu işlemi gerçekleştirmek mümkündür.

Portların güvenliği

Fiziksel telefonlar veya diğer VoIP uç cihazlar yalnızca arama yapmak için kullanılacaksa, bu cihazların bağlı olduğu ağ bağlantılarından yalnızca VoIP için gerekli olan bağlantılar kurulabilmelidir. Aksi takdirde, bir saldırgan bir BT sistemini ağ soketine bağlayarak, yetkisinin olmadığı bilgi ve hizmetlere erişebilir. Örneğin, sürekli denetlenmeyen bir ortamda bulunan bir telefonun bağlı olduğu ağ soketi böyle bir saldırı amacıyla kullanılabilir. Aktif ağ bileşenlerindeki uygun filtre kuralları ile bu durumdan korunmak mümkündür.

Koruma gereksinimine bağlı olarak, daha güvenli çalışmayı sağlamak için IEEE 802.1X'e göre kimlik doğrulama gibi ek önlemler kullanılabilir. MAC adresleri kolayca taklit edilebileceğinden dolayı, bu adreslerin bir anahtar portuna veya VLAN erişim listesine, dinamik veya statik olarak tahsis edilmesinin yeterli koruma sağlamadığı unutulmamalıdır.

3 DETAYLI BİLGİ

3.1 Yararlı Bilgiler

VoIP'te IP ağları üzerinden ses iletimi için farklı uygulamalar vardır. Bu nedenle, potansiyel tehditler ve güvenlik gereksinimleri de farklıdır. Genel uygulamalar aşağıda gösterilmiştir:

Kurum içi Sesli iletişim için VoIP kullanımı

İlk uygulama senaryosu, VoIP'in kurum içi sesli iletişim için kullanılmasıdır. IP telefonlar, içinde katma değerli fonksiyonları barındıran LAN tabanlı bir telekomünikasyon sisteminin yanı sıra dış dünyaya bağlantıyı da sağlar. Dijital telefon şebekesine bağlantı, yerel ağ geçitleri veya bir VoIP sağlayıcısı aracılığıyla yapılabilir. Hibrid sistemlerde IP telefonların kullanılabilmesi için genellikle geleneksel telekomünikasyon sistemlerine VoIP modülleri entegre edilmektedir.

Bu entegrasyon, hatların kullanımı ve ağ bileşenlerinin yönetimi, işletimi ve bakımı açısından potansiyel tasarruflar sağlarken, aynı zamanda veri bağlantısına kolaylıkla müdahale edilmesi gibi dikkate alınması gereken ek tehditler ortaya çıkarabilir. Mevcut bir veri ağını VoIP kullanımı için uyarlarken, alınması gereken güvenlik önlemlerin uygulanması ek maliyetler oluştururken, bu önlemler teknolojinin güvenli kullanımı için mutlak bir ön koşul teşkil eder.

PBX'leri bağlamak için VoIP kullanımı

Geleneksel olarak, PBX'ler çoğunlukla çevirmeli veya kiralık hatlarla birbirine bağlanır. VoIP'in giderek artan bir diğer uygulaması da, yerel telekomünikasyon sistemlerinin IP bağlantıları yoluyla birleştirilmesidir. Farklı konumlardaki geleneksel PBX'ler, bir WAN veri ağı kullanılarak birleştirilir. Telefon ve veri ağlarının bu şekilde birleştirilmesi, önemli ölçüde esneklik, daha verimli bant genişliği ve dolayısıyla potansiyel tasarruflar sağlar.

İnternet telefonu için VoIP kullanımı

Bir diğer senaryo, ses iletimi için genel IP ağlarının, özellikle de İnternet'in kullanılmasıdır.

Günümüzde, giderek artan bant genişlikleriyle, ses kalitesi kabul edilebilir bir seviyeye gelmiştir. Bu durum, İnternet telefonuna yönelimi hızlandırmıştır.

Mesajlaşma servislerine benzer şekilde, yazılım tabanlı telefonlar kullanılabilir. Kompakt ve ucuz VoIP ağ geçitleri giderek daha popüler hale gelmektedir. Bu durum da, İnternet telefon servislerinin geleneksel telefonlarla (analog veya ISDN) birlikte kullanılmasını mümkün kılmaktadır. Ayrıca, üreticiler tarafından özel kullanım için ucuz fiziksel telefonlar sunulmaktadır.

VoIP kullanırken, kontrol bilgileri ve gerçek ses verileri genellikle farklı iletim protokolleri kullanılarak birbirinden ayrı olarak taşınır. "Meşgul" olma durumu gibi kontrol bilgileri, H.323 veya SIP gibi sinyalleşme protokolleri yoluyla iletilir. Ses verilerinin iletiminden de genellikle RTP (Gerçek Zamanlı Taşıma) protokolü sorumludur. Kontrol ve medya bilgilerinin ayrılması, sadece IAX gibi az sayıda protokolde söz konusu değildir.

Birçok farklı sinyalleşme protokolü bulunmaktadır. Bu protokoller birbiriyle uyumlu olmadığından, protokol seçimi bir VoIP ağı kurulmasında önemli bir rol oynar. Ortak bir protokolü desteklemeyen VoIP bileşenleri, ağ geçidi olmadan birbirleriyle iletişim kuramazlar. Bir protokolün bileşenlerini bir diğer protokole çeviren ağ geçidinin kullanımı çok karmaşıktır. Bu nedenle, mümkünse yalnızca bir sinyalleşme protokolünün kullanılması sağlanmalıdır.

Birçok VoIP bileşeni yalnızca belirli bir sinyal protokolünü desteklediğinden, kullanılan VoIP bileşenlerinin seçimi, sinyalleşme protokolünün seçimini de etkiler. Güvenlik açısından değerlendirildiğinde, protokoller arasında sadece küçük farklar bulunmaktadır.

H.323

H.323 kapsamındaki protokol grubu, paket tabanlı ağlarda gerçek zamanlı bilgilerin (video, ses, veri) iletimini tanımlar. H.225.0, H.245 ve H.450 ve H.235 protokolleri de bu protokol grubunda tanımlanmıştır. H.323 sinyalleşme protokollerinin çerçevesini, H.225.0 gerçek sinyalleşmeyi, H.245 ses bilgisinin iletimini ve kontrolünü, H.450 ise gerçek telefon işlevini kapsar. H.235 opsiyonel özelliği ile sinyalleşmenin bütünlüğünü ve gizliliğini korur. Ayrıca konu ile ilgili daha fazla bilgi, bu protokollerin oluşturulduğu Uluslararası Telekomünikasyon Birliği'nde (ITU) bulunabilir.

H.323 aşağıdaki bileşenleri içerebilir:

- Uç cihazlar, son kullanıcı için H.323 iletişiminin uç noktalarını temsil eder. Bu uç cihazların genellikle bir hoparlörü ve bir mikrofonu vardır ve kullanıcıya başka bir katılımcıyla bağlantı kurma fırsatı sunar. Uç cihazlar arasında doğrudan bağlantı ancak IP adresleri biliniyorsa mümkündür.
- Ağ geçidi denetleyicileri, yönetim için kullanılır ve H.323 kullanılan ağlarda bir merkezi kontrol bileşeni olarak görev yapar.
- Çok Noktalı Kontrol Ünitesi (MCU) konferanslara, yani ikiden fazla kullanıcı arasındaki görüşmelere olanak sağlar. MCU'da, katılımcılar tarafından gelen tüm medya akışları birleştirilir.
- Ağ geçitleri, kullanıcı verilerini ve sinyalleşme bilgilerini uyarlayarak, diğer ağlara geçişleri sağlar. Örneğin, ağ geçitleri IP ile analog telefon ağları arasında aracılık eder.

H.323'ün en büyük dezavantajı protokolün karmaşık yapıda olmasıdır. Bu karmaşıklık sorun gidermeyi zorlaştırabilir ve ek maliyetlere yol açabilir.

Oturum Başlatma Protokolü (SIP)

SIP, multimedya servisleri arasındaki bağlantının kurulumunu ve sonlandırılmasını kontrol etmek için kullanılan, metin tabanlı bir sinyalleşme protokolüdür. Video konferans, anlık mesajlaşma gibi ek işlevler için SIP'e ait ek uzantılar gereklidir. Multimedya mesaj akışı da, bir telefon görüşmesi sırasındaki ses verileri gibi RTP ile oluşturulur. Sinyalleşme genellikle SSL, TLS veya IPSec ile korunur.

Aşağıdaki VoIP bileşenleri SIP üzerinden iletişime dahil olabilir:

- Uç cihazlar (ör. telefon, yazılım tabanlı telefon, ağ geçidi) kullanıcı aracıları (UA) olarak adlandırılır. Bir kullanıcı aracısı, bir istemcinin veya sunucunun rolünü üstlenebilir. Bir çağrıyı başlatan Kullanıcı Aracısı İstemcisi (UAC) diğer taraftan Kullanıcı Aracısı Sunucusu (UAS) olarak da çalışabilir. Bir SIP uç cihazı her zaman her iki işlevi de içerir.
- Konum sunucusu, bir istek yapıldığında aranmak istenen kullanıcının IP adresini verir. Bu istek, kullanıcı adıyla yapılabilir.
- Kayıt sunucusu (Registrar) kullanıcıların kaydolmasını ve oturum açmasını sağlar. Bunu yapmak için, uç cihaz kayıt defterine bir tanımlayıcı (kullanıcı adı, parola) ve SIP adresi ile oturum açar. Kayıt sunucusu, uç cihazın IP adresini konum sunucusu tarafından bilinir hale getirir. Daha sonra bu kayda göre uç cihaza erişilebilir.
- SIP vekil sunucu, sinyalleşme mesajlarını işleyen veya ileten bir aracı rolü üstlenir. Kullanıcı aracısı vekil sunucuya bir istek gönderir. Vekil sunucu isteği yorumlar ve işledikten sonra kullanıcı aracısına geri gönderir. Gerekirse, mesaj vekil sunucu tarafından değiştirilir.

SIP, standart hale getirilmiş olmasına rağmen, cihaz üreticileri tarafından genellikle farklı şekilde yorumlanmaktadır. VoIP ağındaki farklı üreticilerin bileşenlerinden kaynaklanan bu farklılıklar, VoIP işlevlerinin bir kısmının kullanılamamasına yol açar. Bu durum genellikle, sistemler arasındaki kimlik doğrulamasını, şifrelemeyi ve katma değerli hizmetlerin sağlanmasını etkiler. Bu nedenle, VoIP bileşenleri tedarik edilirken, mevcut bileşenlerle birlikte çalışabilirlikleri kontrol edilmelidir.

VoIP için Ağ Adresi Dönüştürme (NAT) Kullanımı

NAT özel/dahili IP adreslerinin genel/harici IP adreslerine dönüştürülmesini sağlar. Bu adres dönüştürme ile NAT ağ geçidi, özel kaynak IP adreslerini ve özel kaynak portlarını, genel kaynak portlarına ve genel kaynak IP adreslerine dönüştürür. NAT ağ geçidi, genel

IP adresine dışarıdan gelen paketleri veya cevap paketlerini iç ana bilgisayara (host) iletmesini sağlamak için, genel IP adresleri / portları ile özel IP adreslerine / portlarına karşılık gelen bir eşleme tablosu tutar.

NAT, medya akışının UDP veya TCP başlığındaki kaynak IP adresini ve kaynak port numarasını değiştirir. Bununla birlikte, sinyalleşme mesajının kaynak IP adresi ve kaynak bağlantı noktası bilgileri değişmeden kalır. Sonuç olarak, medya akışları bir NAT ağ geçidinin arkasındaki VoIP telefona gönderilemez. Özel IP adresi İnternete yönlendirilmediğinden, İnternet ortamında bulunan VoIP cihazları, NAT ağ geçidinin arkasında bulunan VoIP telefonuna medya akışı gönderemez.

Aşağıdaki bölümlerde NAT kullanılan ortamlarda VoIP'in işletim seçenekleri gösterilmektedir.

Oturum Sınır Kontrolörü

Oturum sınır kontrolörleri; genellikle hizmet seviyesi anlaşmalarının (SLA) izlenmesi, çağrı kabul kontrolü (Call Admission Control) ve faturalandırma gibi ek işlevler sunmaktadır. Bu sistem, donanım ya da yazılım olarak sağlanmaktadır.

Evrensel Tak Çalıştır (UPnP)

UPnP, özellikle ev kullanımlarında giderek daha popüler hale gelen bir endüstri standartıdır. UPnP mimarisi, PC'lerin ve son kullanıcı cihazlarının (ör. yazıcılar, tarayıcılar, WLAN erişim noktaları) ağ altyapısını basitleştirmeyi amaçlamaktadır. UPnP ile uygulamalar NAT ağ geçidinin genel IP adresini öğrenebilir, kullanılacak NAT atamalarını belirleyebilir ve oturum sona erdikten sonra bunları kaldırabilir. NAT'ın geçerlilik süresini tanımlayan bir zaman dilimi de belirtilebilir. Birden fazla NAT ağ geçidi seri olarak bağlanırsa, UPnP ile NAT geçişi gerçekleştirilemez.

STUN

NAT ağ geçidinin arkasında bulunan istemciler STUN (NAT ile UDP Üzerinden Basit Geçiş) yardımıyla, genel IP adreslerini belirleyebilir ve ağ geçidinin NAT atamasını öğrenebilir. Ancak, STUN Simetrik NAT'ı desteklemez. VoIP'te NAT atamaları sinyalleşme protokolüyle iletilir, böylece gelen RTP akışları NAT ağ geçidinin arkasındaki VoIP telefonuna ulaşmak için adreslenecek uygun NAT eşleşmesine yönlendirilir. STUN teknolojisi mevcutta çoğu VoIP sağlayıcısı tarafından sunulmakta ve birçok VoIP telefonu tarafından desteklenmektedir.

TURN

TURN (Traversal Using Relay NAT) bir NAT ağ geçidinin veya güvenlik duvarının arkasındaki istemcilerin gelen TCP ve UDP bağlantılarını almalarını sağlar. Aynı zamanda, her IP adresi ve port eşleşmesi için yalnızca bir oturum izni verilerek bu seçeneğin web sunucuları veya e-posta sunucuları gibi genel olarak erişilebilir sunucularda kullanılması engellenir. STUN'un aksine, simetrik NAT ağ geçitlerinin arkasındaki sistemler TURN ile gelen bağlantıları da alabilir. TURN, kimlik doğrulamanın parolalara dayandığı basit bir istemci / sunucu protokolüdür.

ICE

ICE (Etkileşimli Bağlantı Kurulumu), SIP için STUN ve TURN gibi protokolleri kullanarak SDP aracılığıyla NAT geçişini etkinleştirmek için kullanılan bir yöntemdir. Bir istemcinin, medya akışlarını alabileceği çeşitli adresleri (ör. STUN veya TURN'den öğrenilen adresler) olduğu varsayılır. İstemciler hangi adresin çalışıp çalışmayacağını bilmediğinden, bunları öncelik sırasına göre sırayla kontrol ve test eder. Öncelikler en düşük maliyetler ve maksimum QoS (Hizmet Kalitesi) temel alınarak belirlenir ve SDP içinde birbiri ardına listelenir. ICE, SIP için tasarlanmıştır ancak, RTSP ve H.323 ile birlikte de çalışır ve bir uç cihazın NAT ortamından bağımsız olarak çalıştırılmasını sağlar.

LAN, İnternet'e bir NAT ağ geçidi üzerinden bağlıysa, sunulan bu mekanizmalardan biri seçilebilir. Bu seçim de dokümante edilmelidir.

EKLER

EK-A: KONTROL SORULARI

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.4.2.U1	VoIP dağıtımının planlanması	Kullanıma başlamadan önce VoIP mimarisinin ana hatları planlandı mı?
AGY.4.2.U1	VoIP dağıtımının planlanması	VoIP kullanımı için mevcut yerel ağın kullanılmasına karar verildiyse, bu ağın kapasitesinin yeterli olup olmadığı değerlendirildi mi?
AGY.4.2.U1	VoIP dağıtımının planlanması	Telefon altyapısında yaşanacak bir problem sırasında uygulanacak acil durum senaryoları ile ilgili önlemler alındı mı?
AGY.4.2.U2	VoIP ara katmanının güvenli yönetimi	VoIP kullanılırken hangi özelliklerin kullanılmayacağı belirlenip, gerekli olmayan ve güvenlik tehdidi oluşturan özellikler devre dışı bırakıldı mı?
AGY.4.2.U2	VoIP ara katmanının güvenli yönetimi	Kullanılan yazılımların güncel olduğu teyit edildi mi?
AGY.4.2.U3	VoIP uç cihazlarının kurulumu ve güvenli yönetimi	Uç cihazların yapılandırmaları, sadece şifreli bağlantı yöntemleri ile sağlanacak şekilde ayarlandı mı?
AGY.4.2.U4	VoIP'te erişilebilirliği sınırlandırma	Harici çağrıların VoIP mimarisine nasıl bağlanacağına karar verildi mi?
AGY.4.2.U5	VoIP ara katmanının güvenli kurulumu	Herhangi bir kullanıcıya atanmadan ortak kullanıma sunulan telefonların yetkilendirilmesi uygun şekilde gerçekleştirildi mi?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.4.2.U5	VoIP ara katmanının güvenli kurulumu	Ara katmanın yapılandırılması sırasında, kullanıcıların hangi haklara sahip olduğundan ve bu kullanıcılara sadece ilgili yetkilerin verildiğinden emin olundu mu?
AGY.4.2.U6	VoIP'te loglama	Logların hangi periyotlarda değerlendirileceğine karar verildi mi?
AGY.4.2.U6	VoIP'te loglama	VoIP'te sinyalleşme sırasında hangi bilgilerin loglanacağına karar verildi mi?
AGY.4.2.U7	VoIP için güvenlik politikasının oluşturulması	VoIP için oluşturulan güvenlik politikaları ile genel güvenlik politikaları arasındaki uyum kontrol edildi mi?
AGY.4.2.U8	VoIP'in şifrelenmesi	Yerel Ağ içerisindeki VoIP iletişiminin şifrelenip şifrelenmeyeceği değerlendirildi mi?
AGY.4.2.U8	VoIP'in şifrelenmesi	VoIP haberleşmesinin korunması için hangi prosedürlerin uygulanması gerektiği belirlendi mi?
AGY.4.2.U9	Uygun VoIP bileşenlerinin seçimi	Tedarik edilecek VoIP bileşenlerinin mevcut altyapı ile uyumlu olup olmadığı kontrol edildi mi?
AGY.4.2.U9	Uygun VoIP bileşenlerinin seçimi	Tedarik edilecek VoIP bileşenlerinin istenilen güvenlik gereksinimlerini karşılayacağı teyit edildi mi?
AGY.4.2.U9	Uygun VoIP bileşenlerinin seçimi	Tedarik edilecek VoIP bileşenlerindeki loglama özelliğinin yasal mevzuatlara uygun olup olmadığı kontrol edildi mi?
AGY.4.2.U10	Sistem yöneticileri için VoIP eğitimi	VoIP sistem yöneticilerinin günlük operasyonları gerçekleştirebilmesi için gerekli eğitimler planlandı mı?

Uygulama Kodu	Uygulama Adı	Kontrol Soruları
AGY.4.2.U11	VoIP uç cihazlarının güvenli kullanımı	Kullanıcılar, VoIP kullanımı sırasında karşılaşabilecekleri tehditler hakkında bilgilendirildi mi?
AGY.4.2.U12	VoIP bileşenlerinin güvenli şekilde kullanım dışı bırakılması	Kullanım dışı bırakılacak VoIP bileşenlerinde kayıtlı olan kritik bilgilerin yedekleriyle beraber kurtarılamayacak şekilde tamamen silindiği kontrol edildi mi?
AGY.4.2.U13	VoIP kullanımı için güvenlik duvarı gereksinimleri	VoIP altyapısında kullanılmak üzere bir güvenlik duvarı tedarik edildiğinde, bu güvenlik duvarının sinyalleşme protokollerini desteklediği ve analiz edebildiği teyit edildi mi?
AGY.4.2.U14	Sinyalleşmenin şifrelenmesi	Sinyalleşme bilgilerinin bütünlüğünü korumak için şifreli VPN kanallarının mı kullanılacağı, yoksa kendi koruma mekanizmalarını sağlayan sinyalleşme protokollerinin mi kullanılacağı kararlaştırıldı mı?
AGY.4.2.U15	SRTP kullanarak güvenli medya aktarımı sağlama	SRTP kullanılırken uçtan uca mı yoksa bölüm bölüm mü şifreleneceğine karar verildi mi?
AGY.4.2.U15	SRTP kullanarak güvenli medya aktarımı sağlama	Kullanılan IP telefonların bellek kapasiteleri, belirlenen tekrarlama listelerini tutabilecek büyüklükte mi?
AGY.4.2.U16	Veri ve VoIP ağının ayrılması	VoIP ve veri ağının ayrılması durumunda, ağlar arası geçişin nasıl kısıtlanacağı belirlendi mi?

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