VoIP/UC Güvenliğinin Bütünsel Bilgi Güvenliği Planlamasına Dâhil Edilmesi
Integrating VoIP/UC Security into the Holistic Information Security Planning

İ.Melih TAŞ
Siber Güvenlik Ar-Ge Departmanı, Netaş
Bilgisayar Mühendisliği Bölümü
Bahçeşehir Üniversitesi, İstanbul, Türkiye
meliht@netas.com.tr

Bahar UĞURDOĞAN
Uygulamalı Matematik Bölümü
Bahçeşehir Üniversitesi
İstanbul, Türkiye
bahar.ugurdogan@stu.bahcesehir.edu.tr

Hüseyin TAŞ
Bilgisayar Programcılığı Bölümü
İstanbul Gelişim Üniversitesi
İstanbul, Türkiye
htas@gelisim.edu.tr

***Özetçe* —VoIP (IP üzerinden ses iletimi - Voice over Internet Telephony), modern şirket iletişimlerinin önemli bir bileşeni haline gelmeye başlamıştır ve birçok kurum ses ve multimedya iletişimi için tamamen VoIP'e bağımlıdır. Her yeni teknoloji gibi VoIP ile beraber hem güvenlik fırsatları, hem de riskler söz konusudur ve bu teknoloji ile ilgili henüz adreslenmemiş güvenlik sorunlarını da beraberinde getirmektedir. Finans kuruluşlarında ve müşteri bilgi güvenliğini sağlamak adına uyumluluk denetimlerinin sıkı olduğu diğer endüstrilerde, VoIP/UC (tümleşik haberleşme - Unified Communication) güvenliği konusundaki önem eksikliği, sonuç olarak organizasyonları yasal ve ticari risklere açık konumda bırakmaktadır.**

Bu çalışmada VoIP/UC haberleşmesi ile ilişkili kurumsal haberleşme altyapısındaki güvenlik tehditleri ile birlikte iş dünyası riskleri ve etkileri bahsedilip, VoIP/UC'nin bütünsel şirket bilgi güvenliği planlamasına dâhil edilmesi için En İyi Uygulama Kontrolleri derlenmiştir.

Anahtar Kelimeler—VoIP, UC, Güvenlik, Güvenlik Planlaması, VoIP Güvenliği En İyi Uygulama, VoIP Güvenliği Kontrol Listesi, VoIP/UC

***Abstract*—VoIP has become an important component of modern corporate communications, and many enterprises depend entirely on it for voice and multimedia. As with most new technologies, there are both security opportunities and risks with VoIP and many of the security concerns associated with this technology are not being addressed. In financial institutions and other industries where there are strict regulatory controls to ensure the privacy of customer information, a continued lack of emphasis on VoIP security will eventually leave organizations open to legal risks.**

This study deals with the VoIP/UC security threats associated with enterprise communication along with business risks and impacts and provides VoIP/UC Security Best Practices Checklist in order to help integrating VoIP/UC into the holistic corporate information security planning.

Keywords—VoIP, UC, Security, Security Planning, VoIP Security Best Practices, VoIP Security Checklist, VoIP/UC

978-1-4799-4874-1/14/$31.00

I. GİRİŞ

IP üzerinden ses iletimi (Voice-over IP, VoIP), IP ağları üzerinden iki-yönlü ses ve multimedya iletişimini sağlamak için kullanılan iletişim protokolleri ve iletim tekniklerinin dâhil olduğu teknoloji ailesinin genel terimidir. IP verisi gibi, VoIP de paket-tabanlıdır; telefon çağrısından çıkan analog ses sinyalleri ikilik tabanda birler ve sıfırlar haline dönüştürülerek sayısallaşır, sonra kodlanır ve paket-anahtarlamalı ağlar üzerinden IP paketleri gibi iletilirler. İletilen tarafta, IP paketlerini tekrar ses ve videoya dönüştürmek için benzer adımlar tersi sıra ile gerçekleşir.[1]

VoIP/UC, kendini geleneksel telefonculuğun yerini alan veliaht teknoloji olarak konumlandırmıştır. VoIP, modern şirket iletişimlerinin önemli bir bileşeni haline gelmeye başlamıştır ve birçok kurum ses ve multimedya iletişimi için tamamen VoIP'e bağımlıdır. VoIP/UC'ye geçişi motive eden ana etkenler; maliyet avantajı sağlaması, esneklik ve verimlilik sağlayan özellikleri sağlamasıdır. VoIP/UC; toplam sahip olma bedelini düşürmekte, tümleşik haberleşme ve mesajlaşma uygulamaları ile IP dünyası ve haberleşme dünyasının yakınsanmasını sağlamaktadır.[2,3]

VoIP kullanımı, kurumsal elektronik iletişimin birincil bileşeni haline gelmeye başlamıştır. Aslında, ses, kısa mesaj (SMS), metin ve video dâhil olmak üzere tüm multimedya elektronik iletişimi için bir kanaldır. Tutarlı servis kalitesi (QoS) gereksinimlerini sağlamadaki beceriksizlik (düşen çağrılar, belirsiz ya da bozulmuş video iletimi, vb.), ofislerden çalışanlara ve üst yönetime kadar kurumlardaki günlük operasyonlar üzerinde belirgin bir şekilde olumsuz etki yaratmaktadır.[2,3]

VoIP, IP protokolünü kullandığı için, hacker'lar, zararlı yazılımlar, vs. tarafından gelebilecek potansiyel saldırılara zafiyetlidir. Ek olarak, ses ve veri iletim yolları arasındaki yeterli ayrımın uygulanmasındaki başarısızlık, her iki tarafın da ihlal edilmesi anlamına gelebilmektedir ve kurumun kritik fonksiyonlarının kısmen ya da tamamen kaybına maruz kalabilmektedir.[4,5,6]

Ayrılmış bant genişliğinin (genellikle 64 Kbit/saniye)

%100'ünü kullanan PSTN'den farklı olarak, VoIP bağlantıları, o andaki mümkün olan en iyi IP ağı üzerinden yönlendirilecektir ve bir ses işaretinin iletilebilmesi için genellikle 16 Kbit/saniye'lik iletişim kapasitesi yeterli olacaktır. VoIP bağlantılarında, ağ tıkanıklığı yaşanabileceğinden dolayı daha düşük QoS deneyimlenir. Böylece, çağrının kalitesi temeldeki ağın kalitesine bağımlı olacaktır. Örneğin; VoIP çağrıları, tüketici seviyesi düşük bant-genişliği üzerine gerçekleşmektedir. Tüketici seviyesindeki "En İyi Girişim (Best Effort)" internet bağlantısı, kurumların yüksek-hızlı (örneğin T1 sınıfı ya da daha üzeri) yerel alan ağı (LAN) ya da geniş ağ (WAN) üzerinden yapılandan daha düşük kalitede olacaktır. IP ağların gerçek zamanlı ses, video ve veri iletişimini bütünleştirerek iletmesi ve merkezi ağ yönetimini kolaylaştırması da önemli bir avantajdır.[1,5]

VoIP/UC'ye geçiş yaparken bazı organizasyonlar, ses ve multimedya çağrılarındaki IP-tabanlı iletim ile birlikte gelen güvenlik tehditlerini gözden kaçırmaktadırlar. İşin ticari riskinin yanında bunun sonucu olarak özel yönetmelikler ile uyumlu olmakta sıkıntılar yaşamaktadırlar.[2,4]

Finans sektöründe bu konu, özel olarak dikkat edilmesi gereken bir konudur ve ilgili teknoloji gelişimi ile dolaylı olarak büyüyen bir endişe söz konusudur. Finans kurumları yönetmeliklere ve kanunlara uymak zorundadırlar. Müşteri bilgilerine karşı gizlilik ve güvenilirliği riske atabilecek güvenlik ihlallerine karşı tam koruma sağlandığından emin olmak zorundadırlar. Ülkemizde de bir takım yönetmelikler ve kanunlar ile kısmen adreslenebilmiş konular bulunmaktadır, ancak henüz bu konulara özel bir uyumluluk ve/veya kanunlar olmadığı için bu konuda bir gereksinim söz konusudur.[7]

VoIP/UC; her gün kullandığımız internetin güvenliğindeki benzer risklere sahiptir ve bunlara karşı çok yüksek duyarlılığa sahiptir. VoIP/UC cihazlarında ve temelindeki işletim sistemlerindeki yapılandırma zayıflıkları; DoS, telekulak, hijacking (gasp) ve toll fraud (servis hırsızlığı) saldırılarına sebep olabilmektedir ve tüm bu tehditler de gizlilik ihlali ve bütünlük kaybı ile sonuçlanabilmektedir. Geleneksel haberleşme yapısından miras kalan tehditlerin yanı sıra, veri ağı ile birlikte gelen tehditler ve yeni nesil haberleşme teknolojilerine özgü zafiyetlerin (SIP/RTP protokol zafiyetleri gibi) kombinasyonundan oluşabilecek tehditler ile VoIP/UC altyapısı daha karmaşık bir güvenlik mimarisine ihtiyaç duymaktadır. Nitekim piyasadaki mevcut IPS, IDS ve firewall çözümleri, henüz VoIP/UC protokollerine yönelik sağlıklı sonuçlar verememektedir ve SPIT (IP telefonculuk üzerinden spam - Spam over IP Telephony) gibi sorunlara yönelik çözüm sağlayan ürünler verimli çalışamamaktadır. Dolayısı ile veri güvenliğini sağlayan mevcut cihazlar ile VoIP/UC güvenliğini sağlamak çok mümkün olamamaktadır.[2,3,4,8]

Bilgi teknolojileri ve haberleşme sistemleri çalışanlarının büyük çoğunluğu henüz bu konular hakkında yeterli bilgiye sahip değildirler. Kurumsal şirketlerin hepsinde, içinde network ve güvenlik işleri ile ilgilenen bir takım bulunan Bilişim Teknolojileri (BT) bölümleri ve bu gruplardan ayrı olarak çalışan haberleşme grupları vardır. BT grubu çalışanları haberleşme teknolojileri, haberleşme grubu çalışanları da IP ağları ve güvenlik hakkında yeterli bilgi sahibi değildirler. Sorun şu ki; bu iki takım birbiriyle ortak çalışıp VoIP/UC güvenliği için politika ve prosedürleri belirlemek üzere bir çalışma yapmamaktadırlar ya da hali hazırdaki ağ güvenlik planlamasına doğru bir şekilde VoIP/UC sistemlerini dâhil edememektedirler. Bu noktada bu iki gruptaki çalışanlarının VoIP/UC güvenliği eğitim programları ile eğitilmesine ihtiyaç duyulmaktadır. Buna paralel olarak VoIP/UC politika ve prosedürlerinin belirlenmesi, uyumluluk/düzenleme, denetim gereksinimleri ile ağ sızma testlerine dâhil edilmesi için kullanılabilecek çatı tasarımlarına ihtiyaçları bulunmaktadır.[3,6]

Bu çalışma ile VoIP/UC haberleşmesi ile ilişkili kurumsal haberleşme altyapısındaki güvenlik riskleri ve etkileri bahsedilip, bütünsel bilgi güvenliği planına ve iş sürekliliği prosedürlerine VoIP/UC'nin dahil edilmesi için En İyi Uygulama Kontrolleri derlenmiştir.

II. İŞ DÜNYASINDAKI RISKLER VE ETKILER

VoIP iletişimlerindeki bağımlılık aşağıdaki konularda direkt ya da dolaylı etkiler içermektedir:[9,10]

- Hem kurumsal ve hem de dış dünya ile iletişim
- Mevcut devam eden iş operasyonları
- Müşteri ilişkileri
- Yardım masası ve teknik destek
- Sözleşmeli konular
- Yasal yükümlülükler ve uyumluluk konuları (örneğin; hassas kişisel teşhis edilebilir bilgilerin (PII-Personal Identifiable Information) VoIP SMS mesajları ya da sohbet oturumları üzerinden iletimi, PCI (Payment Card Industry) gereksinimlerinin ihlal edilmesi)

Ses ve multimedya iletişimleri tipik olarak, iş-kritik bilgileri ya da bu bilgiler ile ilgili başka bilgileri içermektedir. Bu bilgiler aşağıdakileri içerir ancak sadece bunlar ile sınırlı değildir:[9,10]

- Fikri haklar (örneğin; patentler, telif hakları materyalleri)
- Finansal veriler, pazarlama ve strateji planlaması, hassas kişisel bilgiler, satış ve pazarlama ve günlük iş operasyonlarını içeren hassas şirket materyalleri
- Müşteriler, devlet otoriteleri, harici yasal hukuk danışmanları, ortaklıklar, hissedarlar, borsa acentaları ve harici denetçiler gibi üçüncü partiler ile iletişim
- Denetim evrak çalışmaları
- Olay izleme
- Dâhili kontrol dokümantasyonları ve testler

Etkili VoIP kontrollerinin tasarlanması ve yönetilmesindeki başarısızlık aşağıdaki durumlar ile sonuçlanabilir:[9,10]

- Korumasız VoIP ağlarından gelen sızmadan dolayı kurumsal verinin tahrip edilmesi ya da kaybı
- Halka açık ağlar üzerinden şifresiz olarak gönderilen hassas bilgilerin açığa çıkarılması
- Paydaşlar, iş ortakları, yatırımcılar ve müşteriler tarafından güven kaybına ve itibar zedelenmesine sebep olabilecek kötü tanıtım ya da hassas bilgilerin açığa çıkarılması

- Ticari sırların ve dijital varlıkların çalınması ya da kaybedilmesi
- Bilgisayar varlıklarının çalınması
- E-mail, ses iletişimi ve anlık mesajlaşma gibi kritik elektronik varlıkların kullanılamaz olmasından dolayı oluşabilecek verimlilik kaybı
- Taciz, istenmeyen içerik ve şirket casusluğu gibi istenmeyen aktiviteler için şirket VoIP ağlarının kullanımı ya da uygunsuzluğundan dolayı cezalar ve yaptırımlar
- Anlık mesajlaşma ile taşınan zararlı yazılımlardan dolayı oluşabilecek güvenlik açıklıkları
- Müşterilerin satış personeline ulaşmak için yetersizliklerden dolayı oluşabilecek satış kayıpları
- Marka zedelenmesi ve rekabet avantajı kaybı
- Eğer hacker'lar diğer sitelere saldırmak için ihlal edilmiş VoIP sunucuları kullanmada başarılı olursa mağdur üçüncü partiler tarafından açılan davalar
- Yasal keşif talepleri ile uyumluluktaki yetersizlikler
- Makul zaman aralığı içerisindeki ses ya da multimedya iletişiminin geri getirilmesindeki yetersizlik
- Resmi yükümlülükler

III. VoIP/UC Güvenliği En İyİ Uygulama Kontrolleri

Bazı kurumlar, VoIP/UC sistemlerinin sadece yerel alan ağı içinde sınırlandırılmış oldukları düşüncesi ile VoIP/UC sistemlerinin saldırılara duyarlı olmadığına inanmaktadırlar. Bu düşünce, tabiri caizse bir şehir efsanesi olarak değerlendirilebilir. VoIP/UC ağları nadiren veri ağından tamamen ayrı tutulmuşlardır ve sonuç olarak veri ağında oluşacak bir saldırıya zafiyetlidirler.[10,11]

Bankalar ve finans kurumlarının benimsemeleri gereken önlemler için; güvenlik tehditlerini adreslemek, müşteri bilgilerinin güvenliğini sağlamak ve endüstrideki özel yönetmeliklere uyum sağlamak için izleyecekleri adımlara ve VoIP/UC'yi bütünsel güvenlik yaklaşımının bir parçası haline getirmek için organizasyonlara rehber olabilecek En İyi Uygulama Kontrollerine gereksinimleri vardır.[11,12]

Kamu kuruluşları ve finans kurumlar gibi yönetmeliklere tabi kurumlar güvenlik planlaması hazırlarken; TSE, BDDK, BTK, TİB gibi organizasyonlar bilgi güvenliği ile ilgili yönetmelikleri/düzenlemeleri geliştirilirken; VoIP/UC'nin de dâhil olduğu bütünsel güvenlik yaklaşımı için VoIP/UC Güvenliği En İyi Uygulama Kontrol Listesinin dikkate alınması gerekmektedir. Bu listenin organizasyonlardaki mevcut en iyi güvenlik uygulama dokümanlarına eklenmesi tavsiye edilmektedir. Burada yer alan kontroller tam güvenli bir tümleşik haberleşme ağını garanti etmeyecektir ancak tümleşik haberleşme için güvenliğin seviyesinin arttırılmasına yardımcı olacaktır. VoIP/UC Güvenliği En İyi Uygulama Kontrol Listesi sunucu/uygulama-tabanlı kontroller, ağ-tabanlı kontroller ve sürekli yapılması gereken kontroller olarak üç ana grupta derlenmiştir:[9,10,11,12]

Sunucu/Uygulama-Tabanlı Kontroller:

1) Hem sinyalleşme hem medya iletişimi için şifrelemenin aktif edilmesi
2) Sesli-mesaj etkileşimi için şifreleme kullanılması
3) Konfigürasyon yedeklemesi için şifreleme kullanılması
4) Yönetim trafiğinin güvenli tutulması (HTTPS ve SNMPv3'ün aktif edilmesi)
5) Güvensiz servislerin hizmet dışı bırakılması ve güvenli servislerin aktif edilmesi
6) VoIP/UC telefonların güvenlik ayarlarının sağlamlaştırılması (802.1x doğrulamanın aktif edilmesi)
7) Açık bölgelerdeki telefonların fonksiyonelliğinin sınırlandırılması
8) Sistem ve ağ yönetici doğrulaması için mevcut kimlik yönetimi veritabanı (RADIUS, LDAP, AD) ile ilişkilendirilmesi
9) Sistemlerdeki çeşitli yöneticiler için rollerin oluşturulması
10) Uygulanabilir yerlerde saldırı tespit için sunucuların derin sistem izleme uygulamaları ile izlenmesi
11) Sistemdeki kayıt seviyesinin arttırılması ve kayıtların gözden geçirme için kayıt sunucusuna gönderilmesi
12) Sistem ve ağ yöneticileri için karmaşık şifrelerin kullanılması
13) Tüm varsayılan şifrelerin değiştirildiğinden emin olunması
14) Her bir dâhili telefon için istasyon güvenlik kodu uygulanması
15) Servis hırsızlığını azaltmak için uzak mesafe erişiminin ve çağrı sürelerinin sınırlandırılması
16) Ağ problemlerini ve DoS/DDoS saldırılarını tespit etmek için RTCP izleme yetkinliğine sahip izleme araçlarının kullanılması

Ağ-Tabanlı Kontroller:

1) VoIP ağları için veri ağının ses ağından ayrılması
2) VoIP/UC bilişenlerine gelen/giden portları açan durum kontrolsüz güvenlik duvarı konuşlandırılması
3) Sinyalleşme trafiğini kontrol eden durum kontrollü VoIP/UC güvenlik duvarı konuşlandırılması
4) SIP Trunking varsa DoS/DOS koruması, SIP paket kontrolü, topoloji gizleme vs. için SBC (Session Border Controller) konuşlandırılması
5) Gereksiz port ve protokollerin kapatılması
6) Gereksiz iletişimin sınırlandırılması (sadece bilinen yetkili sunucuların birbiriyle iletişimine izin verilmesi)
7) Ağdaki tüm modemlerin devre dışı bırakılması
8) Eğer ağ yönetimi üretici ya da iş ortağı kontrolünde ise, güvenli uzaktan izleme çözümlerinin kullanılması

Sürekli Yapılması Gereken Kontroller:

1) Sızma testi, zafiyet analizi ve risk değerlendirmesinin uygulanması ve düzenli olarak VoIP/UC sistemlerin güvenliğinin test edilmesi
2) VoIP/UC ortamına karşı şirketinin maksimum şekilde hafifletebileceği risk boyutunu tespit etmek için uyumluluk ve tehdit değerlendirmelerinin yapılması

3) Gerektiği durumda, değerlendirme ve testlerde tespit edilen sorunların adreslenmesi için özel plan geliştirilmesi.
4) İmzaların sürekli olarak güncellendiğinden emin olmak için VoIP/UC IPS sisteminin monitör edilmesi
5) Çok sayıda evden ve mobil çalışanları olan organizasyonlar için VoIP/UC NAC (Network Access Control) sisteminin konuşlandırılması
6) Değerlendirme ve test fazlarında eğer SPIT bir risk olarak tanımlanmış ise, anti-SPIT araçlarının kullanılması
7) VoIP/UC güvenlik altyapısının mevcut güvenlik izleme ve yönetim platformları ile bütünleşik olduğunun onaylanması
8) BT Güvenliği, Ağ ve Haberleşme gruplarının VoIP/UC Güvenlik Planlamasına dâhil edilmesi
9) Pharming ve phishing gibi sosyal mühendislik tipi saldırılarının adreslenmesi için çalışan eğitim programı tasarlanması
10) VoIP/UC altyapısını korumak için fiziksel kontrollerin konuşlandırılması
11) İşin ehli danışmanlar ile gizlilik, kayıt (log) tutma ve kayıt yönetimi için kanuni gereksinimlerin dikkatli bir şekilde gözden geçirilmesi
12) Tekrar eden doğrulama girişimleri gibi şüpheli davranışlar için kayıt dosyalarının gözden geçirilmesi
13) Son yamaların yüklü olunduğundan emin olunması
14) Üreticilerin varsa Güvenlik Tavsiye Bildirimlerine abone olunması

IV. SONUÇ

Finansal kurumlar ve daha yaygın olarak organizasyonlar, VoIP/UC teknolojilerinin hızla yayıldığı için güvenlik ihlallerinin de hızla çoğalması ile uçtan uca ağ güvenlik programlarının bir parçası olarak VoIP/UC'yi dikkate almaları ve VoIP/UC'ye özgü güvenlik konuları hakkında tedbir almaları gerekmektedir.

Çoğu durumda, VoIP/UC dünyasına geçişler organizasyonların operasyonel yapısına bazı düzenlemeler gerektirmektedir. Bütünsel güvenlik strateji kapsamındaki dâhil edilen bilişim teknolojileri, geleneksel haberleşme, uyumluluk ve güvenlik planlama ve karar verme fonksiyonlarının ile birlikte bu kapsama dâhil edilmek üzere ayrı bir alan olarak VoIP/UC güvenliğinin de dikkate alınması söz konusu olmaktadır.

Haberleşme ağlarının güvenli olduğundan ve zorunlu standartlar ve yönetmeliklere uyumlu olduğundan emin olabilmek için, organizasyonlar uçtan uca güvenlik planlaması yaparken daha bütünsel bir yaklaşımı benimsemeye ihtiyaç duymaktadırlar ve VoIP/UC güvenlik seviyesinin arttırılmasına yardımcı olmak için bu çalışma ile sağladığımız En İyi Uygulama Kontrol Listesini uygulamaları ve mevcut en iyi güvenlik uygulama prosedürlerine dâhil etmeleri önerilmektedir.

V. BILGILENDIRME

Bu çalışma TEYDEB 3130514 numaralı proje ile desteklenmiştir.

KAYNAKÇA

[1] RFC3261, "SIP: Session Initiation Protocol", June 2002

[2] York D., "*Seven Deadlist Unified Communications Attacks*", Elsevier Inc., 2010

[3] Taş İ. M., "*Tümleşik Haberleşme Güvenlik Riskleri ve Savunma Stratejileri*", NopCon Uluslararası Hacker Konferansı, Bilgi Üniversitesi, Istanbul, Türkiye, Mayıs 21 2012

[4] Endler D., Collier M., "*Hacking Exposed Unified Communications & VoIP Security Secrets & Solutions*", McGRAW-Hill/Osborne, 2013

[5] Thermos P., Takanen A., "*Securing VoIP Networks*", Pearson Education, Inc Massachusetts, USA, 2008

[6] Taş İ. M., "*SIP Kayıt Silme Saldırısının Anatomisi ve Savunma Stratejileri*", 22. SIU Konferansı, KTU, Trabzon, Türkiye, Nisan, 2014

[7] Taş İ. M., "*VoIP/Hacking*", Siber Güvenlik Konferansı, ODTU, Ankara, Türkiye, Aralık, 2011

[8] Özbirecikli O., VoIP, "*SIP Sinyalleşmeye Yönelik Saldırı Uygulamaları, Zafiyet Analizleri ve Güvenlik Önlemleri*", Kocaeli Üniversitesi Lisans Tezi, Mühendislik Fakültesi, Kocaeli 2013

[9] ISACA, "*VoIP Audit/Assurance Program*", 2012

[10] Kuhn, D. Richard, Thomas J. Walsh, Steffen Fries, "*SP 800-58: Security Considerations for Voice Over IP Systems*, National Institute of Standards (NIST)", USA, 2005

[11] AVAYA, "*Security Best Practices Checklist*", USA, 2010

[12] VoIP Security Alliance (VoIPSA), www.voipsa.org