**Protecting Against Dial-In Hazards: Voice Systems**

**(Çevirme Tehlikelerine Karşı Koruma: Ses Sistemleri)**

**SES POSTA GÜVENLİĞİ SINIRLARI ÖRNEKLERİ**

Akıllı bir bilgisayar korsanı, bir şirketin sesli postasındaki otomatik sesi, şirketin kullandığı sistemin türünden dinlemesini anlatabilir. Bu felaket olabilir, çünkü bilgisayar korsanları genellikle fabrika varsayılanını da bilir

kodlar sisteme girer ve bu sayede işletim sistemine geçmelerini sağlar.

sistemi. Bu, uluslararası arama yapabilmeleri anlamına gelebilir. O

Aşağıdaki örnekte belirtildiği gibi, diğer bazı ilginç durumlar için de geçerlidir.

Bir seminerde tanıştığım bir kullanıcı, sesli posta sisteminin için kullanıldığını söyledi.

Bir kaç kız çocuğu ameliyatı yapmak için birkaç ay. Hackerlar başardı

özel sesli posta kutularını açıp kurma (yetkili kullanıcıları kullanarak

kutular) saat sonra. Çalışanlar saat 8: 00'de gelmeden önce tüm bu mesajları silmek için her zaman dikkatli oldular.

Kız operasyonu ya basıldı, taşındı ya da sese olan ilgisini kaybetti

posta sistemi “Müşterilere” verilen tüm iletiler

vardiya pazartesi sabahı geldi! Bu mesajların içeriği

telekom yöneticisi tarafından ayrıntılandırılmamış, ancak sabahın hala şirket içinde efsanevi olduğu tespit edilen şaşırtıcı mesajların çoğuna söylenmişti. Bu komik, özellikle de gerçek bir maliyet olmadığı için

Büroyu yükseltmek dışında bir şirket dedikodu bir ya da iki dedikodu.

Bununla birlikte, katılan herkes için rahatsız edici olan şey, gitmiş olmasıydı.

çok uzun süredir algılanmadı. Şirketiniz bu kodları sık sık değiştiriyor mu? Başarısız girişimleri izler mi? Eğer bilseydi

Şu anda saldırıya uğradılar mı?

İkinci bir şirket o kadar şanslı değildi. Bu şirketin, sesli postadan dış hatlara yapılan tüm operatör transferlerini engelleme konusunda resmi bir politikası vardı.

911'e kadar. Operatörler yeni prosedür üzerine eğitildi ve imzalarını verdiler.

© 2002 CRC Press LLC

© 2004, CRC Press LLC tarafından

dure. Operatörler kapalıyken Şükran Günü hafta sonu ve

Telefonlar güvenlik görevlisine devredildi (eğitilmemiş), arkadaş canlısı bir arayan kendini “AT&T’deki Bill” olarak tanımladı ve test etmek için dış transfer istedi

telefonlar. “Bill” Şükran Günü'nü ve önümüzdeki üç gününü geçirdi,

şirketi hacklemek. Her defasında gardiyan “Assissted AT&T” günlüğüne bir giriş yaptı. Pazartesi sabahı bir güvenlik amiri düzinelerce gördüm

girişleri şüphelendi ve telekom yöneticisi olarak nitelendirdi. Sonuç? bir

Pakistan'a beş haneli telefon faturası! Bunun şu an organizasyonunuzda olup olmadığını biliyor musunuz? Herkes eğitildi mi?

**SES POSTA İÇİN ÖNLEYİCİ ÖNLEMLER**

Bir kullanıcı bu sistemlerdeki kötüye kullanıma karşı korunmak için ne yapabilir? Aşağıdaki aktiviteler önleme kontrol listesi sağlar:

1. Her durumda dış hatlara transfer yapılmasını yasaklayan politika uygulamak,

911 acil durum transferi olası istisnası hariç.

2. DISA bağlantısını kesin (doğrudan içeriye sistem erişimi). Hackerlar buna atıfta bulunur

Çevirmeli / Uzak Çalın. Göçebe ya da evden çalışan işçiler tarafından kullanılır.

uzak bir konumdan PBX çevir sesine erişme. Arayan kişi arar

geri çevir sesi duyulur, bir erişim kodu girilir, ardından telefondaki aramayı tamamlar.

şirket anahtarı. Bu sistemler kelimenin tam anlamıyla dünyaya haykırıyor, “Lütfen

beni hack! ”Bu sistem gerekliyse, uzun, karmaşık erişim kullanın

kodları girin ve sistemin bir arama değil sessizlikle cevap vermesini sağlayın.

Arayana kodu girene kadar

3. Şüpheli faaliyetler için sistemleri izleyin. 300 başarısız girişimde bulunursa

dün gece DISA veya dial-in modem portlarında yapıldı.

şirket bunu biliyor mu?

4. Çoklayıcılara, yönlendiricilere ve PBX’e giriş bağlantı noktaları izleniyor mu?

şüpheli aktivite? Orijinal fabrika kodları değiştirildi mi? dışında

satıcılar, şu anda kim arıyor olabilir?

5. Dumpster dalgıçlarını izleyin. Birçok insan şirketten geçer

kredi kartı makbuzları ve uzun mesafe giriş kodları arayan çöp!

6. Gümrüklü bakım işçilerini kiralayın. Temizlik biliyor musun

Crews? Kullanıcılara hassas erişim kodlarını açık bırakmamaları talimatı veriliyor mu?

mürettebatın onları bulabileceği masalar? Bir müşterim aslında bir

üst düzey faks makinesi, 17. kattaki bir ofisten çalındı! Bulurdu

Birkaç gün sonra yakındaki bir rehin dükkanında.

7. Şirketin telekomünikasyon gizlilik politikası var mı? Bu

E-posta, sesli posta ve diğer ortamları kapsayacak şekilde uygulanmalı ve yeterince geniş olmalıdır.

Örneğin:

“ABC Şirketi, iletişimin mutlak gizliliğine kendini adamıştır,

ve her çalışanın iletişim iznine sahip olmama hakkı vardır.

© 2002 CRC Press LLC

© 2004, CRC Press LLC tarafından

itored. Bununla birlikte, normal bakım faaliyeti sırasında istemeden yasadışı faaliyeti keşfedersek, bunu bildirme hakkımızı saklı tutarız.

sorumlu makamlara faaliyet. ”

Bir durumun izlenmesi gerekliyse, bu durum bir miktar iyileşme sağlayacaktır.

Bir imalat şirketinin çalışanları üç T1’yi bulmak için bir tatilden sonra pazartesi sabahı geldiler (bilgisayar korsanları uzun hafta sonları sever)

ABD Sprint’ine girmeye değer, hepsi İspanyolca konuşan insanlarla dolu:

Uzaktaki bir ülkeye yabancı bir dil konuşan 72 kanal insan

şirketin nikeli. Şirketin İspanyolca konuşan herhangi bir yoktu

müşteriler, çalışanlar veya denizaşırı şubeler. Üzerindeki insanların çoğu

Aramalar muhtemelen yasadışı olduğunu bilmiyordu. Aldatmaca sanatçılar sürekli çalışmak

Göçmen toplulukları ve ankesörlü telefonlardaki yeni göçmen hatları

itibarsız hırsızlardan “indirim çağrıları” bekleniyor ortak bir manzara

birçok şehirde.

**TESİS GÜVENLİĞİ**

Peki ya faks makinesi gibi diğer dahili güvenlik ödünleri? Çünkü bilgi güvenliği iş dünyasında çok önemlidir ve

Bilgilerin yetkisiz erişimi daha yaygın hale geliyor, faks iletimleri ihmal edilmemelidir. Faks makinesi yaygın olarak kabul görmekte ve yoğun şekilde kullanılmaktadır, ancak bu cihazlar için güvenlik önlemleri sıklıkla

içermiyor.

Faks güvenliği yalnızca faks makinelerini değil aynı zamanda iş istasyonlarındaki faks kartlarını da ilgilendirir. Bir şirket ne kadar özel bilgi bilmeli

kuruluşunuzu bu 79 $ 'lık faks panosundan hemen terk ediyor olabilir.

Bunun LAN (yerel alan ağı) standartları üzerinde doğrudan bir etkisi vardır.

her şirketin sahip olması gerekir. Aldığı takdirde şirketin sorumluluğu nedir?

Bir çalışan veya çalışanlar fakstan öğrenilen bilgileri kişisel kazanç için kullanıyorsa, başka bir şirkete yönelik veya hatta daha fazla kasıtlı olarak mı? Önemli olabilir.

Bununla birlikte, daha da rahatsız edici olan şey, kasıtlı olarak bir şirketten özel bilgi almaya çalışan insanlar. Örneğin,

faks makinesinin yanındaki çöp kovası rutin olarak parçalanmış veya bunlar

materyaller basitçe atılır mı? Makine görünür bir alanda mı? bu mu

Gizli yazışmaların uzun süre açık görünümde olmasını önlemek için gelen mesajlar için sık sık kontrol edildi mi? Mı

faks makinesi herhangi bir zamanda gerçekten özel veriler için kullanılıyor mu? Eğer öyleyse, ek

önlemler gerekli. Sıklıkla, faks durdurmanın (veya herhangi bir gizli bilginin herhangi bir türünün) başlıca nedeni dahilidir.

kaynaklar. Şirketler, meraklı veya hoşnutsuz çalışanların tehdidini genellikle görmezden gelir. Bu çalışanlar faks trafiğini okuyabilir. Yetkisiz erişimin bordro, güç azaltma veya finansal durumlara olumsuz etkisi

güvenli olmayan faks makineleri aracılığıyla edinilen bilgiler açıktır.

**FAKS GÜVENLİĞİ ÖNLEYİCİ ÖNLEMLERİ**

Faks makinelerine istenmeyen erişimi önlemek için bir şirket birkaç proaktif adım atabilir. İsme özgü marka ve modeller yerine

(hızlı bir şekilde eskimeyen) ekipman, faks makinesinin güvenliği için istenen özellikler, çalışma ortamı

makine veya her ikisi de aşağıdaki bölümlerde açıklanmıştır.

**Üstün Bir Faks Makinesi Kullanın**

Bu makineler faks iletimlerini belleğe alır ve saklar

Gizli posta kutusundaki bir sabit sürücüde. Adresleme şeması

Faksı, telefona depolamak için gönderen tarafından genişletilmiş aramanın kullanılmasını gerektirir.

gizli posta kutusu. Uygun güvenlik koduna sahip bir kullanıcı

faks makinesini telefondan almak için bu kodu makineye girin.

sürücü. Faks sonra yazdırılır ve dosya aynı anda silinir

**Düşük Uçlu Masaüstü Makine Kullanın**

Sürekli olarak gizli veya hassas bilgiler gönderen veya alan kullanıcılar için, düşük kaliteli bir masa üstü makinenin kullanılması tavsiye edilebilir. Bu olabilir

ihtiyaç duyulan alanda kontrol edilebilir. İhtiyaç duyulan bir makine olarak, bu

Gizli bilgileri göndermek için belirli bir bölüm tarafından kullanılabilir. Rutin idari trafik için normal merkezileştirilmiş faks makinesi kullanılabilir. Bu, trafiği ayırır ve ilave bir kullanım sağlar.

güvenlik seviyesi Ayrıca bu masaüstünün maliyeti de ucuz

Makineler, gerekli özelliklere ve telefon hattı maliyetlerine bağlı olarak genellikle 400 doların altındadır.

**Yerel Ağlarda Depolama ve İletme Faks ve Faks Sunucuları**

Burada bir bilgisayar bellekten gönderir ve belleğe geçer.

mesaj göndermek ve almak için gizli uzun süreli prosedürlerin kullanılması,

yüksek kaliteli faks makinelerine benzer. Yerel alan ağları şimdi ağlarda faks sunucusu kullanıyor. Bunlar aslında kullanıcılardan faks alan ve aktarım gerçekleşene kadar saklayan bilgisayarlardır.

Orijinal belgeler, bir seviye ekleyen sisteme taranmalıdır

karmaşıklık Ayrıca, gelen trafik yönlendirilebilmeli

Üstün tek başına faks makinelerine benzer, gizli bir posta kutusuna.

Bu uygulanmazsa, bir sistem yöneticisinin faksı okumak zorunda kalacağı ve ardından onu ağ üzerinde veya kağıt biçiminde istenen kişiye yönlendirmesi gerektiği için güvenlik ihlal edilir.

**Sesli Posta Sistemiyle Ön Uç**

Yeni tarif edilen bazı programlara benzer şekilde, bir sesli posta sistemi

Bilgi saklama için şifre ve şifre koruması sağlayacak şekilde

© 2002 CRC Press LLC

© 2004, CRC Press LLC tarafından

faks gönderme Sistem bir mesajla cevap vermek için programlanmış

örneğin: “İki mesajınız ve bir faksınız var.” Kullanıcı daha sonra sesli mesajları herhangi bir telefondan alır ancak aramak zorunda kalır.

faksı almak için bir faks makinesinden Bir faksa geçmenin alternatifi

Cihaz bir kod girip, telesekreter sisteminin bir

ortak faks makinesi; Ancak, bu daha riskli olarak kabul edilir. Bir çalışan kodunu girip hemen başka bir gelen posta alabilir.

arayın ya da dikkatini başka bir yere vermeyin. Bu arada,

faks korumasız bir katılımsız makineye giriyor. Yerleşik korumalar

Çalışanları makinede olmaya zorlayan prosedürleri

Bu nedenle faks tercih edilir.

Çünkü hemen hemen her türlü müdahale ve izleme mümkün

Telefon hattında, özellikle hassas faks makinelerine hizmet veren hatlar

Bir şifreleme cihazının kullanılmasıyla güvenli hale getirildi. Bu cihazlar,

pahalı olabilir, gönderilmeden önce verileri karıştırın. Biraz iş

hem faks makineleri hem de konuşmalar için. Bu, her ikisinin de bittiği anlamına gelir

Bilginin şifrelenmesi / şifresinin çözülmesi için karşılaştırılabilir donanıma sahip olması. Aksi takdirde, faks trafiği güvenli olmayan bir modda gönderilmelidir.

**Kullanıcıları Eğitmek**

Dizüstü bilgisayarların veya faks kartlarının kişisel bilgisayarlarda olduğu kullanıcılar

iletim ve alım ile ilgili riskler hakkında eğitilmiş

bu sistemlerdeki faksların sayısı. Uygun denetim ve güvenlik kontrolleri

Gizli dosyaların ve bilgilerin fakslanmasını önlemeye yardımcı olur

Şirketin bir PC'den kağıda kaydedilmeden doğrudan.

**Otel Faksları**

En iyi yaklaşım, gizli bilgilerin gönderilmemesi veya

otel faks makinesi aracılığıyla. Otel görevlileri genellikle faksın kopyasını alır

Trafik durumu ile ilgili bir soruşturma olması durumunda. Ayrıca otel personelinin yanlış tarafa faks göndermesi de nadirdir.

**HÜCRESEL TELEFON GÜVENLİĞİ**

Yol savaşçısının sıkça suistimal ettiği bir başka silahlanma hücreseldir.

telefon. Çok milyarlık bir üretim şirketi finansman ayarlıyordu

şirket için. CEO her gün cep telefonunda işlemin en ayrıntılı ayrıntılarını tartışacak. Sadece anlaşma yaklaştığı gibi

Birisi onun konuşmalarını izleyip izleyemeyeceğini sordu.

Neyse ki, işler sorunsuz gitti. Bununla birlikte, CEO için şok oldu

200 $ 'lık ayı tarayıcısına sahip olan herkesin tüm sohbeti kolaylıkla izleyebileceğini öğrenin.

**Cep Telefonlarına Yönelik Önlemler**

1. Hiçbir zaman cep telefonu üzerinden kredi kartı veya telefon kredi kartı numarası vermeyin.

2. Asla herhangi bir kablosuz telefon üzerinden söylemeyeceğiniz bir şey söylemeyin

tüm dünyayı bilmeyi umursama.

3. Mümkün olduğunca yoldayken, 800 numarayı aramayı deneyin.

kredi kartıyla arama yapmaktan daha çok. Zeki bir bilgisayar korsanı yakalayabilir

otomatik bir kredi kartı araması yaptığınızda, hatta

Numara bir operatöre okunmuyorsa.

4. Hücresel faturanızı yakından izleyin ve olağandışı arama aktivitelerini (numaranızın klonlandığını gösteren) hücrenize bildirin.

hemen sağlayıcı.

**Tavsiye Edilen Telefon Dolandırıcılığı Önlemleri**

Kuruluşlar bu türden önlemeleri önlemek için çeşitli önlemler almalıdır.

. Bunlar şunları içerir:

• Mümkünse, DISA hatlarını ayırma. Bu garantili tek çözümdür. Bağlantı kesilmesi mümkün değilse, kalan önerileri dikkate alın.

• Daha uzun erişim kodları kullanmak. Üç basamaklı bir erişim kodu kullanmayın; bunun yerine 7, 8 veya 9 basamaklı bir kod kullanın. Oran katlanarak artmaktadır.

koda eklediğiniz her numara. Sisteminiz çok zorsa

çatlak, hacker daha kolay bir işarete geçmesi muhtemeldir.

• Sessizce cevap vermek için bir DISA opsiyonu. En çok duyan çevir sesi

Yanıtlama bir ölü vermek ve açık olmak olduğunda ortaya çıkan DISA hatları

bilgisayar korsanlarına ve meraklılara davet. Hattı sessizce yanıtlayarak, bilgisayar korsanı tarafından kullanılan otomatik ekipman hattı görecek

bir sesli arama olarak ve onu kullanışlı olarak işaretlemeyecektir.

• Trafiği izlemek. Yaklaşan felaketin çeşitli uyarı işaretleri şunlardır:

1. 1-800 satırında artan trafik hacmi

2. Giden gövdelerde artan trafik hacmi

3. 950'ye daha fazla erişim

Bu trafiği izleyerek, sahtekarlığı çok geç olmadan tespit etmek mümkün olabilir. Benzer şekilde, taşıyıcılar bu arayışta yardımcı olabilir. Çoğu şimdi

olağandışı durumlar veya trafik yüklerinin trafik takibi ve raporlanmasını sağlayan aylık ücret karşılığında dolandırıcılık sigortası sunmak.

**SONUÇ**

Bir şirketin hangi finansal para cezasını ödeyebileceği

dikkat eksikliği sadece bir makalede ele alınamayacak kadar çoktur. O

Bunu sağlamak için en sıradan sistemlere bile dikkat etmeyi öder

Ofisin bu küçük kolaylıkları üzerinde büyük bir baskı haline gelmez

başka önemli bir sistem - kardiyovasküler sistem. Madde 5-04-42

madalyonun diğer tarafını, yani veri taşıyıcıyı güvence altına alacak

yetkisiz davetsiz misafirlerden.

**Voice Security(Ses Güvenliği)**

Chris Hare, CISSP, CISA

Günümüz işletmelerindeki çoğu güvenlik uzmanı, zamanlarının çoğunu şirkete güvenli bir şekilde erişebilmek için çalışır.

elektronik bilgi Ancak, ses ve telekomünikasyon dolandırıcılığı hala kurumsal iş dünyasında her yıl milyonlarca dolar tutuyor. Telekomünikasyon arenasında kayıpların çoğu paralı dolandırıcılıktan kaynaklanmaktadır;

birçok farklı yöntemle uygulanmaktadır.

Milyonlarca insan günlük olarak ses ve veri ihtiyaçları için telekomünikasyon altyapısına güveniyor

temeli. Bu bağımlılık telekomünikasyon sisteminin kritik bir altyapı olarak sınıflandırılmasına neden oldu

bileşen. Telefon olmadan, günlük faaliyetlerimizin çoğu, neredeyse olmasa da, daha zor olacaktır.

imkansız.

Birçok güvenlik uzmanı ses güvenliğini düşündüğünde, otomatik olarak şifreli telefonları düşünür,

faks makineleri ve benzerleri. Ancak, ses güvenliği çok daha basit olabilir ve doğrudan cihazdan başlayabilir.

telefonunuz bağlı. Bu bölüm telefon sisteminin nasıl çalıştığını, ücretli dolandırıcılık, sesli iletişim güvenliği kaygılarını ve telekomünikasyonlarını korumak için herhangi bir kuruluş için uygulanabilir teknikleri ele alıyor.

altyapısı. Yaygın olarak kullanılan telefon terimlerinin açıklamaları bölüm boyunca bulunur.

POTS: Eski Düz Telefon Servisi

Çoğu insan “telefon” olarak adlandırır. Alıcıyı alır, çevir sesini duyar ve aramalarını yapar. Onlar

ailelerini aramak, iş yapmak, mal satın almak ve yardım ya da acil yardım almak için kullanın. Ve onlar

her zaman çalışmasını beklerim.

Günlük olarak evlerimizde kullandığımız telefon hizmeti, telefon endüstrisinde POTS olarak bilinir,

veya eski telefon servisi. POTS aboneye çeşitli bileşenlerle ulaştırılmaktadır (bkz.

Sergi 51.1):

• Telefon ahizesi

• Kablolama

• Bir hat kartı

• Bir anahtarlama cihazı

Telefon ahizesi veya istasyonu, halkın en aşina olduğu bileşendir. Ne zaman

müşteri ahizeyi alır, devre kapatılır ve anahtara kurulur. Hat kartı

telefonun kapalı olduğu ve telefondan kapalı olduğu bir çevir sesi duyulur.

Anahtar, abonenin darbeli telefon kullanıp kullanmadığını ya da abone tarafından aranan rakamları toplar.

Dokunmatik Tone®. Bir darbeli telefon telefon hattındaki voltajı değiştirir, anahtardaki bir röleyi açar ve kapatır.

Bu, hatta duyulan tıklamaların veya darbelerin nedenidir. Dokunmatik Tonlu arama ile

anahtarı aramayı yapmak için zil sesleri oluşturur.

Anahtardaki işlemci rakamları kabul eder ve aramayı alıcıya yönlendirmenin en iyi yolunu belirler.

abone. Alıcı telefon seti aynı anahtara veya diğer yarıya bağlı olabilir

dünyada Ne olursa olsun, çok karmaşık bir şebeke nedeniyle aramanın yönlendirilmesi kalp atışıyla gerçekleşiyor

anahtarları, sinyal ve yönlendirme.

**Bir Arada Bağlamak**

Teknolojinin çoğu alanındaki sorun terminoloji ile ilgilidir. Telefon endüstrisi farklı değil. mayo

ve her ikisi de aynı şeyi ifade eder - sinyali aboneye iletmek için kullanılan devre ve kablolama.

Aralarındaki temel fark, kullanıldığı yer.

Hem sandıklar hem de çizgiler dijital veya analog olabilir. Hat, öncelikle kablolama ile ilgili

telefon aboneye geçer (bkz. Ek 51.2). Bu konut veya iş abonesi olabilir,

doğrudan telefon şirketinin anahtarına veya bir PBX’e Temel olarak, çizgi genellikle ilişkilidir

tek bir abonenin iletişimini anahtara taşıyarak.

Öte yandan, ana hat, genellikle PBX’ten telefon operatörünün anahtarına bağlantı

veya bir anahtardan diğerine. Bir ana hat, hat ile aynı işlevi görür. Tek fark

ikisinin taşıyabileceği arama veya trafik miktarı. Ana hat, anahtarları birbirine bağlamak için kullanıldığından, ana hat

hattan çok daha fazla trafik ve arama taşıyabilir. Devre terimi genellikle bağlantıyı tanımlamak için kullanılır.

Bir cihazdan diğerine, bağlantı türüne, analog veya dijital veya

Her iki uç (istasyon veya cihaz).

**Analog ve Dijital**

Hem gövde hem de hat analog veya dijital sinyalleri taşıyabilir. Yani sadece bir tane taşıyabilirler.

bir seferde yazın. Kavramsal olarak, başlangıç noktasından varış noktasına olan bağlantıya devre adı verilir ve iki

ana devre tipleri.

Analog devreler, sese dönüştürüldükten sonra ses trafiğini ve dijital sinyalleri taşımak için kullanılır. Analog iken

geleneksel olarak ses devreleriyle ilişkilendirilir, birçok sesli çağrı dijital ekipman aracılığıyla yapılır ve işlenir.

Ancak, analog / dijital dönüşüm süreci yoğun bir teknik tartışmadır ve burada açıklanmamıştır.

Bir analog devre bilgi iletmek için genlik (hacim) ve frekanstaki değişiklikleri kullanır

bir arayandan diğerine. Devrenin mevcut bant genişliği 64 K'dır, ancak 8K kullanılabilir

bant genişliği ahize ve anahtar arasında sinyal vermek için kullanılır, gerçek ses veya veri için 56K bırakılır

sinyaller.

Bir bilgisayar modemi telefon hattına bağlamayı düşünün. Modemin maksimum kullanılabilir hızı

de çalışabilir 56K. 56K modem için gerekçe şimdi açık olmalıdır. Ancak çoğu insan biliyor

Devre kalitesi, hat gürültüsü ve mesafe arasındaki uzaklık nedeniyle modem bağlantısı nadiren 56K’da yapılır.

telefon taşıyıcısının anahtarına abone. Modemler daha sonra tekrar bölümde tartışılmaktadır.

Analog çizgiler görüşme için gerçek ses sinyallerini taşıdığı için kolayca ele geçirilebilirler. Kimse

evinde birden fazla telefon olması, gizli dinleme ile ilgili bir problem yaşamıştır. Kim

telefon devresine erişebilir konuşmayı dinleyebilirsiniz. Bir telefon musluğu gerçekten gerekli değildir - sadece bilgi

eklenecek teller ve telefon ahizesi.

Bununla birlikte, gizli dinlemeyle ilgili soruna rağmen, birçok insan da kendileriyle ilgilenmez

Birisi telefon görüşmelerini dinliyor olabilir.

Analogın alternatifi dijitaldir. Analog hat bilgi iletmek için ses kullanırken, dijital

devre verileri temsil etmek için dijital sinyaller kullanır. Sonuç olarak, dijital devre teknolojileri taşıma kapasitesine sahiptir.

bant genişliği devre üzerinde arttıkça hızları önemli ölçüde artar.

Dijital devreler birçok avantaj sunar. Daha fazla miktarda veri trafiği ve daha fazlasını taşıyabilirler

Analog bir devreden daha fazla eşzamanlı telefon görüşmesi. İzinsiz dinlemelere karşı daha iyi koruma sağlarlar ve

tasarımları nedeniyle telefon dinleme. Ancak, dijital sinyale rağmen, aynı paylaşan herhangi bir telefon istasyonu

devre hala konuşmadan konuşmayı zorlanmadan gizleyebilir.

Devreler, güvenlik sorunlarının başlıca nedeni değildir. Aksine, çoğu işletme için endişe ve

bireyler bu devrelerin yetkisiz ve uygunsuz kullanımından kaynaklanmaktadır.

Hatlar ve gövdeler, istenen seviyeyi sağlamak için birçok farklı şekilde ve yapılandırmada kullanılabilir.

hizmet. Tipik olarak, bir istasyona bağlı hat hem gelen hem de giden aramaları sunar. Ancak, bu yapar

her durumda böyle olması gerekmez.

**Doğrudan içeri arama (DID)**

Dışarıdaki bir arayan kişi, işletmedeki partisine ulaşmadan önce bir operatöre bağlanmalıdır.

genellikle anahtar şalter PBX olarak adlandırılır. Bununla birlikte, birçok PBX sistemi, her birinin olduğu yerde doğrudan içe doğru arama veya DID sunar

telefon istasyonuna harici arayanı doğrudan alıcıya bağlayan bir telefon numarası atanır.

Doğrudan içeriye doğru arama, herhangi bir operatör dahil olmadığından amaçlanan alıcıya ulaşmayı kolaylaştırır. Ancak,

DID'nin dezavantajları da vardır. DID servislerine bağlı modemlere yetkili ve yetkisiz kişilerce ulaşılabilir.

benzer insanlar. Ayrıca, bireylerin işgücünden bilgi almadan bilgi almalarını ve talep etmelerini kolaylaştırır.

merkezi bir operatör veya görevli tarafından taranması.

**Doğrudan Dış Arama (DOD)**

Doğrudan dışa doğru arama tam olarak DID'nin tam tersidir. Bazı PBX kurulumlarında kullanıcının serbest bir hat seçmesi gerekir.

Telefonunda veya bir dış arama yapmak için bir operatöre erişin. DOD ile, arayan kişi telefonu açar, arar

9 rakamı gibi bir erişim kodu ve ardından harici telefon numarası. Çağrı telefona yönlendirilir

Taşıyıcı ve alıcı kişiye bağlı.

Telefon operatörü, abonelerine hizmet vermek için burada açıklanan bileşenleri birleştirir.

telefon operatörleri daha sonra kamusal anahtarlamalı telefonu sağlamak için sistemlerini ağ geçitleri üzerinden birbirine bağlar.

**Özel Alan Şubesi Değişimi (PABX)**

Özel alan şube değişimi veya PABX, genel olarak PBX olarak da adlandırılır. Sonuç olarak, olacak

birbirinin yerine kullanılan terimleri görün. PBX, bir işletme için etkili bir telefon anahtarıdır; ve, gibi

kurumsal, farklı boyutlarda geliyor. PBX, hat kartı, çağrı işlemcisi ve bazı temel yönlendirmeler sağlar.

Temel fark, PBX’in telefon operatörünün şebekesine nasıl bağlandığıdır. PBX'i karşılaştırırsak

İnternete bağlanan bir veri ağındaki bir yönlendiriciye, her iki cihaz da bilgi göndermek için yalnızca bir yol bilir,

veya şebekenin dışındaki noktalara yapılan telefon görüşmeleri (bkz. Ek 51.3).

PBX'in telefon taşıyıcısı düğmesi gibi kendisine bağlı birçok telefon istasyonu vardır. PBX biliyor

çağrıları doğrudan aynı PBX’e bağlı olan istasyonlara yönlendirmek için. Harici telefon numarası araması

Taşıyıcının anahtarına yönlendirilir; bu durumda aramayı işler ve alıcı istasyona yönlendirir.

Telefon taşıyıcısının belirli endişeleri olmasına rağmen, her iki cihazın da benzer güvenlik sorunları vardır:

iletişim ağı kritik bir altyapı unsuru olarak kabul edilmektedir ve

hizmet verememek. İşletme nadiren bu sorunlarla baş etmek zorunda kalır; ancak, başarısız olan girişim

PBX'in zarar görmesini önlemek için yeterli kontrolün sağlanması, ayrıca belirli yükümlülüklerle de karşı karşıya kalabilir.

**Sesli mesaj**

Telesekreter bugün iletişim ile her yerde. Bununla birlikte, sesli posta genellikle

telefon sistemi ve saldırgan için ücretsiz telefon görüşmeleri - ve sistem sahibi için ücretsiz dolandırıcılık.

Telesekreter, telefonlarına cevap veremeyen kullanıcıların telefon mesajlarını kaydetmek için kullanılır.

Kullanıcılar mesajlara, genellikle telefon dahili numaraları olan bir tanımlayıcı girerek

parola.

Sesli posta sorunları genellikle şifre yönetimi etrafında döner. Çünkü sesli mesajla çalışmak zorunda

Şifre, şifre yalnızca basamak içerebilir. Bu, şifreye saldırmanın, şifreden oldukça önemsiz olduğu anlamına gelir.

saldırganın bakış açısı. Sonuç olarak, geleneksel şifre ve hesap yönetimi sorunları burada olduğu gibi bulunmaktadır.

diğer sistemler:

• Hesap adıyla aynı şifreleri

• Parola karmaşıklığı kuralları yok

• Parola yaşlanma veya son kullanma tarihi yoktur

• Hesap kilitlemesi yok

• Diğer sesli posta yapılandırma sorunları

Yaygın bir yapılandırma sorunu çevirmedir. Çevirmeli bağlantı ile, sistem telefonu kabul eder

numarayı ve aramayı yapar. Bu özellik yalnızca dahili veya yerel numaralara izin vermek veya devre dışı bırakmak üzere kısıtlanabilir

o. Çevirmeye izin veriliyorsa ve uygun şekilde yapılandırılmamışsa, işletme şimdi uzun süreli veya diğer ücretli aramalar için faturaları öder.

Saldırganlar erişim kazanmak için eski posta kutularını (bir süre sonra erişilmemiş) kullanırlar.

posta kutusuna. Posta kutusu şifresi alınırsa ve sesli posta sistemi, yeniden aramaya izin verecek şekilde yapılandırılmışsa, saldırganlar şimdi ücretsiz aramalar yapıyor. Saldırgan önce posta kutusundaki selamlamayı bir

basit “evet”. Şimdi, “evet” kelimesini bekleyen otomatik bir sistem aracılığıyla yapılan herhangi bir arama çağrısı

otomatik olarak kabul edildi. İşletme, aramanın ücretini öder.

Saldırgan, hesap tanımlayıcısına, tipik olarak posta kutusunun telefon uzantısına ve şifreye girer.

Telesekreter tarafından kimliği doğrulandıktan sonra, saldırgan uygun kodu ve telefon numarasını girer.

harici arama için. Kullanılabilir basamaklarda herhangi bir kısıtlama yoksa, saldırgan herhangi bir telefonu arayabilir.

dünyanın herhangi bir yerinde sayı.

Burada gösterilen senaryo çoğu sisteme uygulanabilir basit teknikler kullanılarak önlenebilir:

• Yönetici ve görevli şifreleri değiştirin.

• Dahili numarayı ilk şifre olarak kullanmayın.

• Doğrudan aramayı devre dışı bırak.

• Telesekreteri, şifre için en az altı hane kullanacak şekilde yapılandırın.

• Varsa, şifre geçmişi seçeneklerini etkinleştirin.

• Varsa şifre son kullanım tarihini etkinleştirin.

• Eski posta kutularını kaldırın.

Düzgün yapılandırılmış sesli posta, veri ağı ve ses gibi kurum için güçlü bir araçtır

konferans.

**Sesli Konferans**

Birçok işletme düzenli olarak iş yapmak için konferans görüşmeleri kullanır. Mevcut ekonomik ortamda, birçok

İşletmeler, konferans görüşmelerini farklı konumlardaki toplantılar için seyahat etmenin uygun maliyetli alternatifi olarak kullanıyor.

Konferans görüşmesi, aramaları kabul eden ve arayanın hangi konferansı olduğunu belirleyen bir “köprü” kullanır.

telefon numarası ve konferans araması şifresine göre yönlendirilir.

Konferans görüşmesi köprüsünde bulunan güvenlik seçenekleri teknolojiye bağlıdır. Ne olursa olsun, konferans görüşmesine katılanlara, kurumsal duyarlı bilgileri tartışmamaları gerektiği hatırlatılmalıdır.

Konferans görüşme bilgisini edinen veya tahmin eden kişi aramaya katılabilir. Sonuç olarak, konferans araması

Katılımcı bilgileri, katılımı sınırlandırmak için korunmalıdır.

Konferans köprüleri, çeşitli teknolojileri kullanarak tek seferlik, tekrarlayan ve geçici aramalar için kullanılır. Bazı

konferans araması satıcıları, kuruluştaki herkesin isteğe bağlı konferans yapmasına izin veren hizmetler sağlar

köprü. Bu konferans köprüleri, konferans görüşmesini başlatmak için hazır olması gereken bir “ev sahibi” veya başkan kullanır.

Başkanın, çağrıyı başlatmak için kullanılan ikinci bir şifresi vardır. Ev sahibi veya başkanı öğrenen herhangi bir kullanıcı

kodu köprüyü istediğiniz zaman kullanabilirsiniz.

Konferans köprüleri ile ilgili güvenlik sorunları:

• Başkan kodunun kaybı

• Köprünün izinsiz kullanımı

• Köprüye uygunsuz erişim

• Köprüdeki hassas bilgilerin kaybı

Bu sorunların tümü, doğru kullanıcı bilinci ile ele alınmaktadır - ki bu çok az sayıda işletme için şanslı

Aslında, kendi konferans köprülerini işletmek yerine, telefonun

konfigürasyonları.

**Mümkünse, konferans köprüsü aşağıdaki ayarlar ve yeteneklerle yapılandırılmalıdır:**

• Konferans görüşmesi, başkan hazır olana kadar başlayamaz.

• Başkan köprüden ayrıldığında tüm katılımcıların bağlantısı kesilmelidir.

• Başkan, köprüye girmek için ikinci bir güvenlik erişim kodu belirleme seçeneğine sahip olmalıdır.

• Başkan, köprüyü değiştirmek için,

Arayanı susturma, susturma veya susturma, köprüleri kilitleme ve konferansa erişme

Şebeke.

Başkanın komutları konferans aramasının güvenliği için önemlidir. Tüm katılımcılar bir kez

Katılan, başkan herkesin orada olduğunu doğrulamalı ve köprüyü kilitlemelidir. Bu kimseyi önler

Konferans görüşmesine katılmak için.

**Güvenlik sorunları**

Bölüm boyunca, teknolojiler ve güvenlik konularını tartıştık. Ancak, özel ne olursa olsun

İşletmenizin kullandığı telefon sisteminin yapılandırması, yapmanız gereken bazı güvenlik endişeleri var.

bilgili olmak.

Geçiş Ücreti Dolandırıcılığı

Geçiş ücreti sahtekarlığı, işletmeler, bireyler ve telefon operatörleri için büyük bir endişe kaynağıdır. Geçiş ücreti sahtekarlığı gerçekleştiğinde

ücretli veya ücretli telefon görüşmeleri sahtekarlıkla yapılır. Dahil olmak üzere çeşitli dolandırıcılık yöntemleri vardır

yetkili kullanıcılar tarafından uygunsuz kullanım, hizmetlerin çalınması, telefon kartları ve kurumun iletişim sistemine doğrudan dahili arama.

1998 Tüketici Haberleri raporuna göre, yılda yaklaşık 4 milyar dolarlık bir dolandırıcılıktan mahrum olmak için kaybedilmektedir. Rapor

URL adresinde çevrimiçi olarak erişilebilir: http://www.fcc. gov / Büroları / Common\_Carrier / Bültenlerimizde / ttf & you.pdf.

Dolandırıcılık maliyeti sonuçta daha yüksek iletişim maliyetleri ile işletmelere ve tüketicilere aktarılır. Bazı durumlarda, telefon operatörü aboneyi masraflardan sorumlu tutar.

yıkıcı ol. Sonuç olarak, işletmeler telefon operatörlerine ödeme yapan yolsuzluk sigortası için ödeme yapabilirler.

Ses Güvenliği işletme indirildikten sonra öder. Ücretli dolandırıcılık sigortası cazip gelse de, pahalı ve

indirimler genellikle çok yüksektir.

Kuruluşunuzdaki geçiş yolsuzluğunu tespit etmek imkansız değildir. Küçük bir şirketiniz varsa,

basitçe çeşitli insanlar için telefon kullanımının izlenmesi, çağrı modellerini tanımlamaya yeterli olmalıdır.

Daha büyük kuruluşlar için, analiz için PBX'ten bilgi almak gerekebilir. İçin

Örneğin, her telefon görüşmesinden arama kayıtlarını kaydedebiliyorsanız, bir ücretlendirme yapmak mümkündür.

**Yetkili Erişimin Uygunsuz Kullanımı**

Bir işletmedeki her çalışanın genellikle masada bir telefonu vardır veya şirket tarafından sağlanan bir telefona erişimi vardır.

Çoğu çalışan, masalarından uzun mesafeli gişe aramaları yapma olanağına sahiptir. Çalışanların çoğu yapmak

işlerinin bir parçası olarak günlük olarak yapılan uzun mesafeli aramalar, çoğu kişinin uzun vadeli aramalar yapmasını pahasına yapmak için iki kez düşünmez.

Bu tür bir kullanımın izlenmesi ve önlenmesi işletme için zordur. Sık sık çağrı kalıpları

numara analizi denir ve çalışanlara aylık telekomünikasyon maliyetlerini bildirmenin birkaç yolu vardır.

bu problemle mücadele. Ayrıca, kurumsal telefon hizmetlerinin kullanımına ilişkin kurumsal politikalar ve

İşletmenizde zaten yoksa, uygunsuz kullanım için cezalar verilmelidir. En sonunda,

Birçok kuruluş, uzun mesafeli telefon görüşmeleri yapmak için faturalandırma veya yetkilendirme kodları kullanır.

kullanımı ve masrafları belirli departmanlara veya müşterilere faturalandırmak.

Ancak, kuruluşunuz bir özellik olarak koşullu ücretli reddetme (CTD) özellikli bir PBX'e sahipse,

bunu, şehirlerarası veya ücretli aramalara izin verilmeyen telefon istasyonlarında etkinleştirmeyi düşünerek. Örneğin,

Kullanıcılar belirli telefon numaralarını veya alan kodlarını arayamamalı. Alternatif olarak, bir telefon istasyonu

tamamen ücretli arama ayrıcalıklarını reddetti.

Ancak, Avrupa'da, CTD uygulamak daha zordur, çünkü pek çok kişiyi aramak nadir değildir.

bir günde farklı ülkeler. Sonuç olarak, CTD parametrelerinin yönetimi çok zorlaşır.

CTD, daha önce bölümde tartışıldığı gibi bir NCOS tanımında özel bir seçenek olarak yapılandırılabilir.

Arama kartları

Çağrı kartları en yaygın yolsuzluk dolandırıcılık şeklidir. Arama kartı numaraları günlük olarak çalınır ve satılır

dünya çapında temeli. Çağrı kartı hırsızlığı, genellikle bir kişi aboneyi gözlemlediğinde gerçekleşir.

numarayı kamuya açık bir telefona girme. Kart numarası daha sonra hırsız tarafından kaydedilir ve satışa sunulur.

diğer aramalar

Çağrı kartı hırsızlığı, takip için genellikle dolandırıcılık birimleri olan telefon operatörleri için büyük bir problemdir.

hırsızlık ve arama yazılımı, arama düzenlerini izler ve dolandırıcılık araştırmacılarını olağandışı uyarır

çağıran desenler.

Bazı durumlarda, oteller arama kart numarasını, konuklarına verilen faturalara yazdırabilir,

çeşitli insanlara uygun rakamlar. Ek olarak, PBX doğru yapılandırılmamışsa, arama kartı bilgileri telefon ekranında gösterilir; böylece yakındaki herkesin rakamları görmesini kolaylaştırır ve

**Numarayı kullan.**

Diğer PBX tabanlı problemler, son numarayı tekrar arama işlemini içerir. PBX son numarayı tekrar aramayı destekliyorsa, herhangi bir çalışan

Aranan son numarayı hatırlayabilir ve erişim ve arama kartı numaralarını alabilirsiniz.

Çalışanlar, çağrı kartlarının yasal olmayan kullanımıyla ilgili sorunların ve maliyetlerin farkında olmalıdır.

Arama kartı kullanırken uygun koruma şunları içerir:

• Numarayı girerken elinizle koruma

• Numarayı ezberlemek, aramayı yaparken görünür bir kartın olmaması için

• Şirketinizin PBX'in rakamlarını kaydetmediğinden emin olun.