

ATATÜRK ÜNİVERSİTESİ

MÜHENDSİLİK FAKÜLTESİ

BİLGİSAYAR MÜHENDİSLİĞİ

**İşletme Genelinde Ana Bilgisayar Tabanlı Güvenlik Duvarlarını Dağıtma:**

**Bir Durum Çalışması Anında Mesaj Güvenliği**

**Mayıs 2019**

**ABDULSAMET HAŞILOĞLU**

**İÇİNDEKİLER**

[Özet ............................................ ...................................................... ....................... 2](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#3)

[I. Anlık Mesajlaşma nedir?](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#4).................................................. ..................................... 5

IM'de İşletme Kullanım Eğilimleri ......................................... ................................ 10

[II.](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#6) [Potansiyel tehditler .............................................................................................. 15](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#6)

[III.](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#8) [Kurumsal IM Çözümü Seçerken Dikkat Edilmesi Gerekenler …...................... 17](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#8)

[IV.](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#9)En İyi Uygulamalar .......................................... .................................................. 21

[Kurumsal Kullanıcılar için İpuçları ................................... ...................................... 28](https://translate.googleusercontent.com/translate_c?depth=1&hl=tr&prev=search&rurl=translate.google.com&sl=en&sp=nmt4&u=https://www.infosec.gov.hk/english/technical/files/instant.pdf&xid=25657,15700022,15700186,15700190,15700256,15700259&usg=ALkJrhhtDoeUj3SvI1HE-QPg3VldX004Nw#9)

8Son Kullanıcılar İçin İpuçları ......................................... ....................................... 30

**ÖZET**

Anlık mesajlaşma (IM), her ikisiyle de popüler olan hızlı büyüyen bir iletişim aracıdır.

ev ve kurumsal kullanıcılar. IM etkili ve kolay bir ağ aracı olsa da-

tabanlı iletişim, uygun güvenlik durumunda bir dizi güvenlik riski doğurur

önlemler uygulanmadı. Bu yazıda, kullanım ile ilgili güvenlik riskleri tartışılmaktadır

Bu popüler iletişim kanalı ve olabilecek en iyi uygulamaları sunar.

teknolojiyi bir iş ortamında uygularken uygulanır.

**I. ANINDA MESAJ NEDİR?**

Anlık Mesajlaşma (IM), geçici

Neredeyse anında mesaj gönderip alarak 'canlı' işbirliği

bir ağ bağlantısında

1. ICQ gibi mesajlaşma araçlarının tanıtımıyla

2.MSN Messenger

3. giderek daha fazla insan rahatlık ve kolaylıktan keyif alıyor

gerçek zamanlı mesajlaşma sistemleri tarafından günlük yaşamlarında sağlanır. IM ayrıca bir

Müşterilerle ve ortaklarla iletişim kurmak gibi hizmetler için işyerinde yer almak,

müşteri desteği sunmak, gerçek zamanlı uyarılar almak, yönetim ve

proje koordinasyonu. IM araçları, hızlı yanıt veren ve hızlı olan tüm işlemleri destekler

problem çözme gerekli ve e-postalardan daha hızlı iletişim olduğunda veya

telefonlar faydalıdır.

Genel olarak, kullanıcının bir IM istemcisini müşterisine indirmesi ve yüklemesi gerekir.

cihaz (bir masaüstü bilgisayar, akıllı telefon veya PDA olabilir) ve bir kullanıcı

iletişim kurabilmesi için önce hesap. Bir IM sunucusu bir veritabanı olarak görev yapar.

temas noktaları bulunur. ICQ ve MSN Messenger gibi halka açık IM hizmetleri için,

sunucular internette barındırılıyor. Kurumsal IM sistemlerinde, IM sunucuları

kuruluşun iç ağında barındırıldı

**İŞLETMELERDE IM'NİN KULLANIMI**

2007 yılında yapılan anlık mesajlaşma trend anketine göre

4

, IM sadece değil

ev kullanıcıları arasında popüler olmakla birlikte, işyerinde de giderek yaygınlaşmaktadır. Daha

Ankete katılanların yüzde 27'den fazlası işte anlık mesajlaşma kullandıklarını belirtti.

Sohbet kullanıcılarının yaklaşık yüzde 19’u, mesajından çok daha fazla anlık mesaj gönderdiklerini

İş arkadaşlarına ve iş arkadaşlarına e-posta gönderirken, gençlerin yüzde 55'i yardım alıyor

IM aracılığıyla ev ödevleriyle. Ayrıca, işyerindeki IM kullanıcılarının yarısı

IM'nin onları işte daha üretken kıldığına inanıyordu. Ancak, yaklaşık yüzde 79

ofiste IM kullanan işçiler, kişisel konular için IM kullandıklarını belirtti

**II.** **POTANSİYEL TEHDİTLER**

Kamu IM hizmetleri hızla yayılması için alternatif bir kanal haline geliyor

virüsler ve kötü amaçlı kod. Genel kamuya açık IM hizmetleri genellikle yerel değildir

iletilmekte olan bilgileri korumak için şifreleme ve

kurumsal içerik denetim filtreleri. Ayrıca, kapsamlı bir denetimin olmaması

iz, belirli güvenlik veya yasal uyumluluk gerekliliklerini karşılamayabilir.

IM servislerini kullanırken olası tehditler şunlardır:

1. Kötü Amaçlı Kodun Yayılması İçin Bir Araç

IM'in kurumsal kullanımı hem hacim hem de önem bakımından artmaktadır. IM kullanıcıları

daha hızlı bir karar alma sürecinden yararlanabileceklerini bildirir, daha yüksek

verimlilik ve daha düşük telekomünikasyon maliyetleri. Aynı zamanda, IM tehditleri

(tipik olarak virüsler), saldırganlar değişmeye başladıkça hızla dikkat çekiyorlar

odakları daha iyi korunan e-posta sistemlerinden IM ağlarına kadar. İstenmeyen e

mesajlar IM yoluyla da yayılabilir. Bir kullanıcının bir üzerinden aldığı spam

Anlık Mesajlaşma Servislerine “spim” denir

2. IM yazılımı Güvenlik Açıkları

Diğer herhangi bir yazılım uygulamasında olduğu gibi, popüler IM istemcilerinin bir geçmişi var.

ortak güvenlik açıkları. Bir IM istemcisinin kurulması yeni

bilgisayar sistemine açıkları.

3. Hassas Bilgilerin Sızıntısı

İçin bir kamuya açık IM servisini kullanırken gizlilik önemli bir husustur.

iletişim. Genel IM şebekelerinde, kullanıcılar arasında mesaj alışverişi

genellikle servis sağlayıcılar tarafından kontrol edilen IM sunucusu çiftlikleri üzerinden yönlendirilir

kendilerini. İstemci IM yazılımı eşler arası bir yeteneğe sahipse, kullanıcılar

Sohbet sunucularından geçmeden birbirleriyle iletişim kurun. Önemli değil

Hangi mod kullanılıyorsa, IM trafiği gizlice dinlenmeye karşı savunmasızdır, çünkü

çoğu kamuya açık IM istemcisi herhangi bir şifreleme özelliğine sahip değildir. Bu nedenle

yetkisiz bilgilerin yetkisiz kişilerce okunabileceği veya koklayabileceği mümkündür.

kullanıcılar. Halka açık IM servisleri kullanıldığında durum daha da kötü olabilir

kuruluş dışındaki kişilerle iletişim kurar.

Genel IM servisleri tarafından kullanılan protokoller genellikle sahte

protokoller, çünkü standart güvenlikten kaçınmak için özel olarak tasarlanmıştır

kontrolleri. IM istemcileri yalnızca SOCKS üzerinden bağlanacak şekilde yapılandırılamaz

veya web proxy sunucuları, ancak protokol de kendi yolunu bulma yeteneğine sahiptir.

Güvenlik duvarı üzerinden, TCP bağlantı noktası gibi açık bir bağlantı noktası arayarak

80 veya HTTP istekleri içindeki trafiğini tünelleyerek,

standart web trafiğinden tanınmayan. Komut dosyası ve dosya aktarımı

IM sistemlerinin yetenekleri ayrıca bir kuruluşu sızıntılara maruz bırakabilir

hassas bilgi. Bu nedenle, kuruluşlar uygun

IM kullanımı ile ilgili politika ve kontroller.

4.İzleme ve Tutma Baş Ağrıları

Sohbet mesajlarını izlemek ve mesajları iş kayıtları için saklamak

kolay görev. Hangi anlık mesajların kaydedilmesi ve kaydedilmesi gerektiğine karar vermek,

IM ortamında büyük olasılıkla daha zor

belirli bir mesaj için anlamlı bir bağlam sağlamak için mesajlara ihtiyaç duyulur.

5. Sorumluluk

Bir kamuya açık IM şebekesinde, IM gönderenlerin ve alıcıların kimlikleri olamaz.

doğrulanmadı. Herkese açık IM hesapları, kaçırılma veya sahtekarlığa karşı savunmasızdır;

meşru kullanıcılar ile bir konuşma taklit etmek için davetsiz misafir

**III.** **İŞLETME SEÇENEĞİNDEKİ ÖNEMLER**

**IM ÇÖZÜM**

Şu anda piyasada mevcut bir dizi IM servis sağlayıcısı bulunmaktadır.

kendi dahili IM hizmetlerini oluşturma ve yönetme becerisini düzenler.

Kurumsal IM seçerken aşağıdaki güvenlik özellikleri göz önünde bulundurulmalıdır

(EIM) çözümü

1. Kimlik Doğrulama Kontrolleri: Herhangi bir kurumsal IM çözümü entegre edilmelidir

gibi şirketin mevcut kimlik doğrulama mekanizmaları ile

Microsoft Active Directory ile arayüz oluşturma.

2. Gizlilik Kontrolleri: Bütçe veya

satış hacmi verileri kurumsal IM sisteminde iletilebilir,

EIM ürünleri tüm mesajları korumak için güçlü şifreleme sağlamalıdır

şirket ağları içerisinde seyahat etmek.

3. Anti-Virüs Kontrolleri: Bir EIM ürünü,

tüm dosyaların EIM üzerinden aktarılmasını sağlamak için bir virüsten koruma çözümü

kanallar virüssüzdür.

4. Günlük Kaydı / Denetleme Kontrolleri: Kuruluş içindeki tüm iletişim

Çalışanların hizmeti kötüye kullanmadıklarından emin olmak için oturum açmanız gerekebilir,

veya belirli düzenleyici gereklilikleri yerine getirmek için. Seçilen EIM ürünü

Ayrıca kuruluşun kayıt gereksinimlerini de karşılamalıdır.

Ayrıca, kuruluşun kabul edilebilir bir IM kullanımı ve gizliliği tanımlaması gerekir.

politikası kullanın ve tüm çalışanlara IM'i işinde kullanmanın risklerini iletin. Eğer ben

iletişim şirket tarafından kaydedilmeli ve izlenmelidir;

ayrıca çalışanlara açıkça dağıtılmalıdır

**IV.** **EN İYİ UYGULAMALAR**

**İŞLETİCİ KULLANICI İÇİN İPUÇLARI**

Bir IM sisteminin dağıtımında bir dizi potansiyel güvenlik riski bulunduğundan,

anlık mesajlaşma kullanımı yalnızca ticari amaçlarla sınırlı

Herhangi bir sistem (kamu veya özel) kurulmadan önce onay alınmalıdır. Eğer bir

kuruluş bir IM sistemi kullanmaya karar verirse, aşağıdaki güvenlik kontrolleri

uygulanan:

1. Tüm Güvenlik Prosedürlerine uyun

Genel kural olarak, tüm ilgili güvenlik gereksinimleri **[dahil olmak üzere**

**Güvenlik Kuralları, Temel BT Güvenliği Politikası ve BT güvenliği**

**Yönergeler (örtülü metin yalnızca ITGInfoStation sürümü içindir)**

IM kullanırken dikkat edilmesi gerekenler.

2. Bir Sohbet Kullanım Politikası Geliştirin ve Tüm Sohbet Kullanıcılarına Açıkça Yayın

Bir IM kullanım politikası, IM kullanımının kabul edilebilir olup olmadığını açıkça belirtmelidir.

kuruluş içinde ve eğer öyleyse, kısıtlamaların ne olduğunu. IM kullanımı

Politika teknoloji ve ürün tarafsız olmalıdır. IM ile oluşturulan mesajlar

Olup olmamalarına bakılmaksızın, işletme kayıtları olarak görülmelidir

kamuya açık bir sistemde veya dahili bir kurumsal sistemde üretilir. Eğer kullanımı

IM ticari amaçlar için, bir iç tutma politikası veya dış

düzenlemelere uyulmalıdır

3. IM Hijyen Çözümlerini Uygulayın

IM hijyen çözümleri, kuruluşların

kullanımı izleyerek, IM trafiğini yöneterek ve

istenmeyen mesajları, bilgisayar virüslerini ve rahatsız edici şeyleri engellemek için içerik filtreleme

materyallerin yanı sıra tüm IM mesajlarını denetim amacıyla kaydetme.

4. Kullanıcıları En İyi IM Kullanımı konusunda Eğitin ve Masaüstü Korumasını Güçlendirin

IM tarafından şirket ağında ortaya çıkan en büyük tehditlerden biri IM tabanlı

zararlı kod saldırıları. IM virüsleri genellikle ya olduğu gibi bulaşır.

çalıştırılabilir dosya ekleri veya IM metninde köprüler olarak mağdurları yönlendirmek

zararlı web sunucuları. Çoğu durumda, bu virüsler otomatik olarak değil

idam. Aksine, kurbanları ikna etmek için sosyal mühendislik taktiklerini kullanıyorlar

bilinmeyen dosyaları açmak veya şüpheli bağlantılara tıklamak için.

Özel IM hijyen ürünleri korumak ve yönetmek için bir çözümdür

IM kullanımı. Tüm dosya eklerinin yanı sıra etkin köprüleri de filtreleyerek

ürünler kullanılan saldırı vektörlerinin büyük bir bölümünü etkili bir şekilde ortadan kaldırabilir

IM virüsleri ile. Masaüstü anti-virüs ürünleri de bunların çoğunu tespit etmeye yardımcı olabilir

tehditleri.

Son kullanıcıları gelen anlık mesajlaşma konusunda daha şüpheci olmaları için eğitmek,

kendi arkadaş listelerinden olanlar bile, genel bir parçası olmalı

stratejisi. Hızlı bir şekilde yama ekleyen yazılım açıkları hakkında genel önlemler,

Anti-virüs yazılımı ve kişisel güvenlik duvarlarını çalıştırmak IM'ye karşı etkilidir

tehditleri.

Yukarıdakilerin ışığında, kullanıcı eğitimi ve masaüstü koruması alınmalıdır

IM'nin şirkete dağıtımını planlarken hesaba katın.

5. Genel IM kullanmak yerine Kurumsal IM (EIM) Çözümü uygulayın

Müşteriler

IM hizmetleri iş amacıyla gerekliyse, kuruluşlar

kendi Enterprise IM mimarisini kullanma olasılığını keşfedin

ağ ortamında. Bu, kapsamlı izlemeye izin verecektir

ve verilerin depolanması ve dahili kullanıcı ile ilgili güvencelerin sağlanmasına yardımcı olunması

kimlikler. Buna ek olarak, kapalı bir sistem hala anahtar için kullanılabilir hale getirilebilir

müşterileri ve satıcıları dışardan alır, ancak tüm harici IM'lerin geçmesi gerekir

izlenebileceği ve yönetilebileceği bir ağ geçidi. Kurumsal IM çözümleri

kuruluşlara, kendi müşterileri ve yerleşik sunucuları olan sunucular sağlamak

engelleme, günlüğe kaydetme, denetleme, izleme dahil kurumsal güvenlik özellikleri,

yönlendirme ve şifreleme

6. IM Müşteri Koruması

Kullanıcılar IM servisi tarafından sağlanan tüm şebeke servislerini devre dışı bırakmalı,

Gelen mesajlar / çağrılar / dosyalar alındığında tüm bildirimler devre dışı

kaynakların paylaşımı ve mikrofonların ve videoların uzaktan etkinleştirilmesini devre dışı bırakma kameralar.

**SON KULLANICILAR İÇİN İPUÇLARI**

Aşağıdaki ipuçları, IM'yi düzenli iletişim olarak kullanan son kullanıcılar için tasarlanmıştır.

Araç

1. IM istemcinizi dosya aktarımlarını otomatik olarak kabul edecek şekilde ayarlamayın. Yaparsan, sen

virüs bulaşmış dosyaları otomatik olarak kabul etme riskine girdiğinizden emin olun

bilmeden.

2. IM ile alınan herhangi bir dosyayı açmadan önce, göndereni doğrulamanız gerekir.

o dosyayı gerçekten size gönderdiğini söyledi. Ayrıca, dosyanın olduğundan emin olun.

açmadan önce anti-virüs yazılımı tarafından tarandı.

3. Güvenilmeyen / bilinmeyen durumdan gönderilen bir IM içindeki URL bağlantılarını asla tıklamayın

kişileri. Tıklanan kullanıcılar tarafından yayılan virüs raporları var.

IM URL’sind

4. Asla kişisel bilgileri veya hassas bilgileri IM ile göndermeyin. Olsa bile

Bunu yapmak için zorunlu nedenler, hassas bilgilerin şifrelenmiş olmasını sağlayın.

5. IM yazılımınızı (ve diğer sistem bileşenlerini) aşağıdaki

En yeni yamalar, kişisel güvenlik duvarı korumasını etkinleştir ve virüsten koruma yazılımı yükle

en yeni virüs imzalarına sahip yazılım ve kötü amaçlı kod tanımları gibi

algılama ve tamir motorlarının yanı sıra

**Anlık Mesajlaşma İçin Genel Güvenlik Endişeleri**

**Gizlilik:** Anlık Mesajlaşma aracılığıyla iletilen bilgiler, mesaj alıcısına ulaşmadan önce birkaç açıklama noktasından geçer. Bu, mesajların güvenli olan veya olmayan sunuculardan ve ağlardan geçtiği anlamına gelir, bu nedenle gönderdiğiniz bilgilerin güvenli olmalarının garantisi yoktur. Sorunları karmaşıklaştırmak için, Anında Mesajlaşma servisleri genellikle oturumu sonlandırdıktan sonra sunucuda gizli bilgiler bırakabilen dosya paylaşım programları içerir.

**Şebeke Sorunları:** Anlık Mesajlaşma uygulamasıyla servis reddi saldırılarının riski çok daha fazladır. Hizmet reddi saldırıları meşru kullanıcıların kaynakları tüketmek, yapılandırmaları yok etmek ve ağ bileşenlerini değiştirmek için ağı aşırı kullanarak ağa erişmelerini önler. Davetsiz misafir mesajları arayabilir, birbirleriyle yasa dışı olarak iletişim kurmak için aygıtlar kurabilir ve işletim sisteminizin düzgün çalışması için ihtiyaç duyduğu diğer kaynakları kullanabilir.

**Kötü Amaçlı Yazılım:** Reklam yazılımı, casus yazılım, solucanlar, Truva atları ve diğer virüsler gibi **kötü** amaçlı yazılımlar, Anlık Mesajlaşma programınız aracılığıyla kolayca iletilebilir. Bu ayrıca, kendilerini meşru olarak gizleyen ve daha sonra kişisel bilgilerinizi açığa vurmanız için kandıran kimlik avı programlarını da içerir.

**Uygulama Exploits:** Tıpkı PC işletim sistemi güvenlik açıkları gibi, Anında Mesajlaşma uygulamalarının da bilgisayar korsanlarının yararlanabileceği kendi güvenlik açıkları olabilir. Meseleleri karmaşıklaştırmak için, Anında Mesajlaşma uygulamalarını destekleyen yazılım, üzerinde çalışması için Anlık Mesajlaşma uygulaması tarafından devralınabilecek yeni bir güvenlik açığı kümesi içerebilir.

**Mobil IM:** Kablosuz mobil cihazların kullanımının artması, PC'nizi Anlık Mesajlaşma için kullanmayla ilişkili olanların ötesinde yeni güvenlik açıkları ve güvenlik kaygıları yaratır. Mobil cihazlar ve kablosuz bağlantı sayesinde, bilgisayar korsanlarının bu uygulamalarla ilişkili güvenlik açıklarını tanıyarak e-posta iletilerinden ve kişi listenizdeki üyelerden yararlanmaları çok daha kolaydır.

Anlık Mesajlaşma, [**güvenliği**](http://www.spamlaws.com/network-security.html) ihlal etmek söz konusu olduğunda bilgisayar korsanları için yepyeni bir yol getiriyor çünkü daha fazla insan bu uygulamayı dosya aktarma dahil birçok farklı kullanım için kullanıyor. Bilgisayar korsanlarının PC'nize veya mobil cihazınıza uzaktan kolayca erişebilmelerini sağlayan yeni ve gelecek olan güvenlik açıkları keşfedildi.

Anlık Mesajlaşmayı kullanmanın birçok yararı olsa da, bu uygulamayı kullanırken hiçbir güvenlik garantisi olmadığını unutmayın. Avantajlardan yararlandığınızdan ve bu uygulamayı dikkatli kullandığınızdan emin olun.

**Anlık Mesajlaşma Güvenlik Endişeleri**

Anlık Mesajlaşma, hem kişisel kullanım hem de iş kullanımı için çok popüler bir iletişim şekli haline geliyor. Anlık Mesajlaşma uygulamalarının popülaritesi ve rahatlığı nedeniyle, bu tür uygulamaları kullanmak için pek çok platform PC'ler ve mobil cihazlar için uygun hale gelmiştir. Bu, IM kullanıcıları için uygun olsa da, kötü niyetli saldırılar ve [**güvenlik**](http://www.spamlaws.com/network-security.html) ihlalleri olasılığını da arttırır .

Anlık mesajlaşma  Güvenlik sorunları

William Hugh Murray, CISSP

  Belirli bir uygulama ve çevre bağlamı dışında bir mekanizmanın güvenliği hakkında faydalı bir şey söylenemez.

- Robert H. Courtney, Jr.

Gizlilik, hükümete sürveyansın maliyeti ile orantılı olarak değişir.

  - Lawrence Lessig  
  
Anlık mesajlaşma (IM), bir oyuncaktan bir kurumsal uygulamaya, evden odaya taşındı. Sosyal altyapımızın bir parçası oldu ve ekonomik altyapımızın bir parçası olacak. Çoğu teknoloji gibi, birçok kullanım alanı vardır - bazıları iyi, bazıları kötü. Hem temel hem de uygulamaya bağlı sorunları vardır. Bu bölüm IM'yi açıklar ve uygulanmasına örnekler verir. İşlemi açıklar ve bazı örnek kullanımlarını inceler. Tipik tehditleri ve açıkları tespit eder ve IM'nin ortaya çıkardığı güvenlik sorunlarını inceler. Tipik güvenlik gereksinimlerini ve bunları karşılamak için mevcut kontrolleri tanımlar. Son olarak, kullanıcılar, operatörler, işletmeler ve ebeveynler için güvenlik önerileri yapar.

Giriş ve Arkaplan

Anlık mesajlaşma veya sohbet, yaklaşık 15 senedir devam ediyor. Bununla birlikte, yaşamının çoğu için kullanımı seyrek olmuştur ve uygulamaları önemsizdir. America Online’ın hizmetine girmesiyle kullanımı hızla genişledi. Birçok çocuk için İnternetin ilk uygulaması ve oyundan sonra bilgisayarın ikinci uygulamasıydı. Her ne kadar birçok işletme hala dirense de, artık kültürün bir parçası. Tüketici pazarında ortaya çıkması ve işletme pazarına taşınması ilginç bir teknolojidir. Web'de gezinmeden önce olduğu gibi, IM kuruluştan aşağıdan yukarıya - kullanıcıdan kuruma - giriyor. Birçok kullanıcı birden tutamaklıdırlar ve birden hizmetlerine abone çünkü Orada 100 milyondan fazla gibi IM kullanıcıları olabilir ama, herhangi bir kon fi Insidans ile bilmek dif fi kült olduğunu. K. Petersen

 Seattle Times

  Birçok kullanıcının çoğu zaman iki veya daha fazla IM istemcisi açtığını bildirir. IM, yaşamı boyunca oldukça iyi huylu bir ortamda işletiliyordu. Yani, İnternet oldukça iyi huylu olduğu günlerde İnternet'te işletiliyordu. İnternetin genelinde olduğu gibi, iş ve hükümet partiye geç kaldı. 11 Eylül’de, ulus ve özellikle de New York’taki iletişim, çoğunlukla beklenmeyen bir yük nedeniyle ciddi bir şekilde bozuldu. Biri şehir dışına telefon açabilir ancak şehir içine çağrı yapamaz. WWW’deki çoğu haber sitesi pek çok talebe cevap vermedi; Cevaplar bir ya da iki satırla sınırlıydı. Şehirdeki yayın TV, birincil antenlerinin kaybolmasıyla bozuldu; sadece bir kaçının yedeği vardı. Kablolu TV ve şehir dışında yayın yapan televizyonlar, kısmen oldukları için yüke duyarlı değildir. Cep telefonları birkaç dakika boyunca iyi çalıştı ancak yakında yüklemek için düştü. Yük altında en iyi sonuç veren iletişim, anlık mesajlaşma idi. “İlk yanıtlayanlar” kendilerini çağrı cihazlarını (tek yön), cep telefonlarında SMS, AOL Anında Mesajlaşma, BlackBerrys ve diğer anlık mesajlaşma yöntemlerini kullanarak buldu.

Klişe kullanma riski altında olan IM yeni bir paradigmadır. Dünyayı görme şeklimizi değiştiriyor ve sonunda dünyayı değiştirecek. IM, işyerini e-postadan önceki gibi değiştiriyor. (Evet, e-posta işyerini değiştirdi. Hepimiz farkedecek kadar uzun süre bulunmamasına rağmen, her zaman olduğu gibi olmadı.) Dün meslektaşım Roger ile “sohbet ediyordum”. PDA'larımıza kurduğumuz yeni bir IM istemcisinden bahsediyorduk. (İkimiz de Handspring Treo iletişimcilerini, Palm OS PDA ile entegre cep telefonlarını kullanıyoruz.) “IM, PDA'ların katil uygulamasıdır” dedi. Şaşırdım. Ona bu bölümde çalıştığımı söyledim ve detaylandırmasını istedim. Şimdi esas olarak evden ve yoldan çalışanlar için (hem bizleri hem de meslektaşlarımızın çoğunu içeren) IM'nin şimdi sanal su soğutucumuz olduğunu söylemeye devam etti. O işi yaptığımız yer, salonlarda yürürken ya da kafeteryada buluşarak yapardık. Aynı zamanda, konuşmanın uygun bir zaman olup olmadığını görmek için kapı eşiğimiz. Telefonda bir meslektaşı aramayı planlasa bile, ilk önce bir anlık mesaj gönderir. IM, bir PDA ile yaptığımız diğer spontan şeyleri tamamlar. Aşağıdaki tartışmada IM'in bir donanım ağı üzerine kurulu bir insan ağı olduğunu göreceksiniz. Sunucular ve protokoller yerine getirildiğinde, yetenekleri ve diğer iletişim yöntemleriyle entegrasyonu yalnızca yazılım istemcilerinin karmaşıklığı ile sınırlıdır. IM, kendiliğinden bir işbirliği aracıdır.

Açıklama   Bu bölüm anlık mesajlaşmayı (IM) açıklarken, sonraki bölümlerde açıklayıcı sistemler ve tipik işlemler tartışılarak ayrıntılı bilgi verilmektedir. En soyut haliyle IM, kullanıcıların kısa sürede gerçek zamanlı olarak iletişim kurduğu bir istemci / sunucu uygulamasıdır. İstemci giriş ve çıkış gerçekleştirir, İnternet ulaşım ve bağlantı sağlarken, sunucular mesaj adresleme ve isteğe bağlı olarak mesaj yönlendirme sağlar. IM’in en popüler örneklemesi AOL Anında Mesajlaşma (AIM). AOL istemcisine yerleşik bir AIM istemcisi var. Diğer uygulamalara ve uygulama paketlerine yerleşik AIM istemcileri de vardır. Sohbet kullanıcıları, masaüstünde veya istemci uygulamasında adlandırılmış pencereler olarak temsil edilir. Bir pencereyle temsil edilen kullanıcıya mesaj göndermek için, bir kişi imleci pencereye yerleştirir (aktif pencere yapar) ve mesaja yazar. Bu mesaj daha sonra, eşzamanlı olarak, eşzamanlı olarak, bağlantının diğer ucunu temsil eden başka birinin sistemindeki pencerede görünür. En basit haliyle trafic  bire bir.   Ancak, bir var  grup modu   A, bir topluluk grubunun üyelerine katılmak için bir davetiye gönderdi.  Bire birçok   veya   çoktan çoğa modu.  “Sohbet odası” nın kurulduğu ikinci bir çoktan fazla modu var. Sanal oda bir gruba, bir konuya veya bir tartışmaya tahsis edilebilir. Katılımcılar  oda   - yani, tartışma - irade. Odaya katılanlar isim etiketleri veya simgeler ile temsil edilebilir. Teoride, IM eşzamanlıdır: yani, A'dan B'ye bir mesaj, ardından B'den A'ya bir cevap gelir. Uygulamada, daha "eşzamanlıya yakındır" dır; iki veya daha fazla eşzamanlı ipliğin düzensiz olması. IM nispeten açık bir uygulamadır. Ağlar, sunucular, odalar veya gruplar, adlandırılmış ve belirlenmiş katılımcılar dışındaki herkese kapalı olabilirken, çoğu tüm katılımcılara açıktır. Altyapı (yani, müşteriler, sunucular ve bağlantılar) herkese açıktır. IM ayrıca nispeten birlikte çalışabilir. Çoğu ağ ve sunucu birincil olarak eşleriyle birlikte çalışsa da, birçok farklı istemci başkalarıyla birlikte çalışabilir ve çoğu müşteri birden çok ağ ve sunucu ile çalışacaktır. Cerulean Studios'un Trillian Professional istemcisi, AOL, MS, Yahoo, ICQ ve çoklu IRC ağları üzerinden eşzamanlı bağlantıları destekleyecektir. Hem AIM hem de ICQ işletmecisi olan Time Warner, ikisinin birlikte çalışmasına izin vermeyi planladığını açıkladı. IM sistemleri yalnızca birbirleriyle değil, e-posta ve sesli postayla da çalışır.Sistemler bu bölüm daha önemli IM sistemlerinden bazılarını tanımlamaktadır.

AOL IM

 En popüler tüketici IM sistemi uzak ve uzak AOL IM'dir (AIM). Kayıtlı kullanıcı veya trafik sayısı ile ölçülür, başka bir sistem yaklaşmaz. AOL, bir IM sisteminin değerinin düzenli kullanıcı sayısı ile geometrik olarak arttığının farkındadır. IM, AOL istemcisine eklenmiş ve başlangıçta AOL’nin arama yapan müşterileri için tasarlanmasına rağmen, İnternet’i tüm gelenlere açık olduğu yerlerde kullanır. AOL müşterisi olan veya olmayan herkes, AIM sunucusuna bir ad kaydedebilir. AOL’un yazılım iştiraki Netscape’den bir tanesi de dahil olmak üzere bir dizi bağımsız müşteri kullanılabilir. AOL, ISS'leri (İnternet servis sağlayıcıları) ve diğer servisleri bir AOL istemcisini tekliflerine dahil etmeye teşvik eder.

ICQ

 Time Warner aynı zamanda İnternet CQ (ICQ) operatörüdür. Amatör radyo operatörleri modeli tanıyacaktır. AOL IM telefon gibi olsa da, ICQ daha çok bir jambon kanalı gibi. Konferans görüşmesi yapmak mümkün olsa da, telefon öncelikle bire birdir. Bir bire bir modda bir jambon radyo kullanmak mümkün olsa da, esasen çoktan çoğa bir ortamdır.

IRC

 Bazı İnternet tarihçileri, 1996 yılında ICQ'dan IM ile çıkarken, çoğu, 1988'de ortaya çıkan Internet Relay Chat'i (IRC), tüm anlık mesajlaşmaların büyükbabası olarak tanıyor. IRC (UNIX’den UNIX’e) için bir alternatif ve detaylandırma olarak inşa edildi

 konuşma

 Komut. IRC sunucuları genellikle UNIX sistemlerinde çalışırken, istemciler Wintel sistemleri, IBM VM, EMACS, Macintosh, NeXTStep, VMS ve diğerleri için kullanılabilir. Erken IRC istemcileri komut satırı ile yönlendirildi ve yönlendirildi. Birçok temizlikçi hala bu modda kullanmayı tercih ediyor. Ancak, modern istemciler grafiksel bir kullanıcı arayüzü kullanır. Örneğin, BitchX, UNIX / X-Windows sistemleri için bir GUI istemcisidir. ICQ gibi, IRC de temelde çoktan çoğadır. Bir kullanıcı başka bir kullanıcıya kullanıcı adıyla değil, bir kanal adına referansla bir kanala bağlanır. Gerçekten de, IRC kullanıcıları kendi adlarına bile sahip değiller. Bir kullanıcının bir kanal içindeki girişi, yalnızca kullanıcı kanala bağlı kaldığı sürece iyi olan isteğe bağlı bir takma adla tanımlanır. Bir kullanıcının bir takma adı yoktur. Takma ad geçerli kullanımda olmadığı sürece, herkes kullanabilir. Böylece, IRC çoğu IM sisteminden bile daha adsızdır. (IRC takma adlarının bir kaydı vardı, nickserv, ancak kullanımı isteğe bağlıydı. Bir kullanıcının takma adını kaydetmesine gerek yoktu; kanallar kayıt defterini kontrol etmedi. Böyle bir gönüllü kayıt defteri, nickserv'in ilkbahardan bu yana çok az bir değeri vardı. 1994 ve hiç kimse bir ikame kurmak istemedi.) IRC için Web tabanlı istemciler de var. Web posta sunucuları gibi, bunlar iki katmanlı istemciyi / sunucuları üç katmanlı hale getiren sunuculardır. Gerçek IRC istemcisi bir sunucu üzerinde çalışır ve daha sonra bir WWW istemcisi (yani bir tarayıcı) tarafından erişilir. Bu, bir kullanıcının ICQ istemcisine kendi sisteminde sahip olması gerekmediği, ancak IRC'ye daha fazla yerden erişebileceği ve “ağda” açıkça görüneceği anlamına gelir.

Lotus Sametime Bağlantısı  Lotus Sametime Connect sistemi kurumsal IM için sunulur ve mevcut bir kurumsal dizinin (Notes sunucusu) kullanılması ve anahtar yönetimi ile uçtan uca şifreleme (Lotus Notes genel anahtar altyapısına dayanan) gibi özellikler sunar. Metne ek olarak, Sametime sesi ve görüntüyü destekler.   NetMeeting  NetMeeting (NM), tam fonksiyonlu bir işbirliği istemcisidir. NM, adresleri çözmek için dizinleri kullanırken, genellikle tek bir ağ adres alanında (veya bir proxy üzerinden adres alanlarında) eşler arası çalışır. Sohbete ek olarak, NM sesli sohbeti, hareketli görüntüyü, beyaz tahtayı (grafiksel sohbeti düşün), dosya aktarımını, uygulama paylaşımını ve hatta masaüstü paylaşımını destekler.   AU1997\_Frame\_Ch050 Sayfa 603 17 Kasım 2003 Pazartesi 13:20 © 2004, CRC Press LLC tarafından   604   Bilgi Güvenliği Yönetimi El Kitabı   Yahoo!  Yahoo! Mesajlaşma web tabanlı, tüketici odaklı ve halka açıktır. Hem kullanıcıdan kullanıcıya mesajlar hem de sohbet odalarını destekler. Bir kullanıcı kaydı var ancak ortak kullanıcı rehberi yok; ve büyük bir sohbet odası rehberi var.   MS Windows Messenger  Windows Messenger, IM'nin MS Windows işletim sistemine entegre edilmesidir. Kullanıcıları e-posta adresleri altında kaydetmek için .Net Passport sunucusunu veya kullanıcı adlarını kaydetmek için yerel bir dizini kullanır. NetMeeting'in özelliklerinin çoğu (örneğin, gönderme ve alma, ses, video, beyaz tahta, uygulama paylaşımı ve masaüstü paylaşımı) Messenger istemci işlevine eklenmiştir.   Diğerleri  Ek IM sistemleri, Jabber (kurumsal IM), businessim, Akonix (kamuya açık IM'in kurumsal kullanımı için bir ağ geçidi), 12 gezegen (kurumsal sohbet sunucusu), e / pop (kurumsal) ve GTV'yi (genel ağ geçidi ile kurumsal IM) içerir.

Operasyon

Bu bölümde tipik IM işlemleri açıklanmaktadır.

İstemciyi Kurmak

 Çoğu kullanıcı için bu gerekli bir adımdır ve genellikle bir simgeye tıklamak ve bir veya iki istemde yanıt vermek kadar basittir. Çoğu IM istemcisi, kullanıcının zaten sahip olduğu başka bir işletim sistemine veya uygulamaya dahil edilir. Ancak, İnternet'te tercih edilen müşteriyi bulmak ve bir kopyasını indirmek zorunda kalabilir. Biri AOL veya MSN kullanıcısıysa, IM bu istemcilerde istemcilere dahil edilir. (Bazen sorun bunlardan birinden kurtulmaktır.) Kullanıcıdan yükleme sırasında bir veya iki genel seçenek belirlemesi istenebilir.

İstemciyi Başlatma

 İstemciyi başlatmak genellikle bir simgeye tıklamak kadar basittir. IM istemcileri genellikle başlangıç ​​listesindedir ve çoğu, kurulum sırasında kendilerini oraya koymayı dener.

Kaydol

 Birçok sistemde, yeni kullanıcılar, kullanıcı kimliklerini, "ekran adlarını", tanıtıcıları veya diğer adlarını kaydetmelidir. Tüketici sistemlerinde, bu, istemci programından bir iki isteme yanıt vermek kadar basit olabilir. Kurumsal sistemlerde, zaten çalışan veya kullanıcı dizininde bulunanlar için otomatik olabilir, ancak form doldurup imzalamayı ve olmayanlar için yönetim onayı almayı içerebilir.

Kişi Listelerini Doldurma

 Bazen gerekli ve daima yararlı bir adım, bir kişinin kişisini veya arkadaş listesini doldurmaktır. Bu genellikle kişinin kullanıcı adını girmek kadar basittir. İsteğe bağlı olarak, kullanıcılar gruplar halinde düzenlenebilir. Çoğu müşteri, kullanıcı adlarını kayıt defterine göre kontrol eder ve kayıt defterinin tanımadığı adları bildirir.

Bağ

 İstemciyi servise bağlamak genellikle yazılımı başlatmak kadar kolaydır. Sistem başlangıcında otomatik bile olabilir. İstemci ve sunucu birbirine IP adresi ve port numarası gibi bakıyor. Çoğu tüketici ve kurumsal sistem için, bu bilgi istemci yazılımına yerleştirilmiştir ve kullanıcı tarafından görülemez veya anlamsız değildir. IRC ağları veya çoklu ağ istemcileri için bir IP adresi tanımlamayı ve girmeyi içerebilir.

Log-on

 Sohbet servisleri, kullanıcının tanıtıcısıyla oturum açmasını gerektirebilir. İstemci uygulamaları genellikle bu değeri hatırlar; böylece açılır listeden seçilebilir veya varsayılan olarak girilebilir. Çoğu IM servisi de bir şifre bekler. Yine, müşteriler genellikle parolaları hatırlama ve bunları otomatik olarak girme özelliğini içerir. Güvenlik uygulaması açık olmalıdır. Sohbet servislerinde oturum açmak olağandışı bir şekilde kalıcıdır; çoğu sistemde zaman aşımı olmaz. weemanjr (a.k.a. Tigerbait, Gatorbait veya Bitesize) yakın zamanda beni ziyaret etti. AOL IM'de oturum açmak için dizüstü bilgisayarımı ve istemci yazılımımı kullandı. Aslında, o sık sık yaptı ki, varsayılan ekran adını weemanjr olarak ayarladı, şifresini sakladı ve müşteriyi otomatik olarak oturum açması için ayarladı. Onun parolasını göremesem de, bundan çok faydalanıyorum. Weemanjr'ın daha düşman bir yerden bağlanmış olabileceğini unutmayın.

İletişim Listeleri

 Çoğu istemci uygulaması, rastgele sayıda kişi veya muhabirin adını saklama ve bunları klasörler halinde düzenleme yeteneğine sahiptir. Bir kullanıcının muhabirlerinin isimlerine, bir kişi listesi veya “arkadaş listesi” adı verilir. Bir kurumsal IM sistemi, Lotus Sametime Connect, iki ayrı kişi listesi sağlar: biri Lotus Notes dizin sunucusuna dayalı, biri de dışarıdakiler için. AOL IM sunucusunda kayıtlı. Oturum açma zamanında, kişi listesi istemci uygulamasına geri yüklenir. İstemci tarafında veya sunucu tarafında saklanmış olabilir. Diğer şeyler eşittir, müşteri tarafı açıklamaya karşı daha dirençlidir ancak sunucu tarafında depolandığı kadar çok yerden temin edilemez. Kişi listesi geri yüklendikten sonra, sunucuya ve istemci uygulaması kişi listesi penceresinde görüntülenen her bir kişinin durumuna karşı çalıştırılabilir. Ayrıca Weemanjr’ın arkadaş listesini de kullandım. İki klasörü var: “arkadaşlar” ve “kızlar”. Arkadaşların kolları onların erkek kaykay arkadaşları veya oyun arkadaşı olduğu anlamına gelir. Kızların kulpları, kendilerini tanımlayan (kendi kimlikleriyle) belirlenmiş, kendilerini değiştiren ve dedikodu yapan, weemanjr'ın kızlarının temel etkinlikleri olduklarını öne sürüyorlar. Gençler, genellikle ortak ve tanımlayıcı isimleri nitelemek için doğum tarihlerini kullanırlar. Bu nedenle, bu arkadaş listesi sadece partinin cinsiyeti hakkında değil aynı zamanda yaşı hakkında da bilgi sızdırıyor. Bu bilgi, Weemanjr'ın kodu bilmeyen veya onu ilgilendirmek için çok yaşlı olan muhabirleri olabileceğini göstermektedir.

Mesaj gönderme

 Bir kişi bir kişinin adını veya simgesini tıkladığında, istemci uygulaması kişiyle bağlantı kurmayı dener; Girişim başarılı olursa, göndericiyle ilişkili bir uygulama penceresi alıcının sisteminde açılır. İstemci uygulaması, tanımlayıcı ve durum bilgisini pencereye koyacaktır. Bu bilgiler, alıcının adını, çevrimiçi / ine, son etkinlikten bu yana geçen zamanı ve isteğe bağlı olarak müşterisinin yeteneklerini (örneğin ses, görüntü, simge gösterme, gönderme / alma) içerebilir. Biri () penceresinin alt yarısına bir mesaj yazabilir; Yeni hat / dönüş tuşlandığında, mesaj gönderilir. Tüm mesajlar gönderenin adı ile belirlenen pencerenin üst yarısında görüntülenir.

Gruplar

 Biri birden fazla alıcıyı davet etmeye davet edebilir

 geçici

 grubudur. Katılan tüm istemci uygulamalarında bir pencere açılacaktır. Gruptaki tüm katılımcılar arasındaki trafik, tüm pencerelerde ilgili pencerede görünecektir. Her mesaj gönderenin adı ile etiketlenecektir. Son kullanıcı bıraktığında grup kaybolur.

Kanallar ve Odalar

 Kanallar ve odalar, genellikle bir konuyla veya konuyla ilişkilendirilen kalıcı tartışmalardır. Kullanıcılar bir kanala veya bir odaya istedikleri zaman katılabilir, tüm trafiği görebilir, mesaj gönderebilir ve istek üzerine bırakabilir. Traf the c gönderenin adı ile etiketlenebilir. Uygulamaya bağlı olarak, pencere kanala veya odaya bağlı olanların tutamaçlarını gösterebilir veya göstermeyebilir; farkedilmemiş “lurkerler” olabilir. Kanallar, odalar ve bunların trafiği, son kullanıcı bağlantısının kesilmesinden sonra bile devam edebilir.

Dosya Gönderme ve Alma

 İstemci uygulamasında yer alan işlevselliğe bağlı olarak, bağlantılar, e-posta adresleri, “ifadeler” (örneğin gülen yüz) veya diğer (isteğe bağlı) nesneler bir bağlantı penceresine "sürüklenip bırakılabilir". Eğer ve bunların nasıl alıcının sistemde görünen alıcının uygulamanın bir fonksiyonudur. Gönderici, bir nesnenin etiketini veya simgesini (örneğin, program veya veri dosyası) başka bir kullanıcıya bir IM bağlantısını temsil eden pencereye sürükler. Alıcının sisteminde, kartı almak isteyip istemediğini soran bir pencere açılacaktır. Eğer öyleyse, kendisine depolanacağı yer (örneğin, klasör veya dizin) ve kendisine atanacak isim sorulur. IMemanın kendisine gönderilen bir dosyayı kabul ederek Weemanjr'ın sistemimi kolayca bir virüsle kirletmiş olabileceğini düşünün.

Uygulamalar

IM'in en genel uygulaması bir

 konuşma

  iki veya daha fazla insan arasında. Çocuklar için bu konuşma şeklidir.

 sosyalleşme

 ; Yetişkinler için olabilir. Konular güncel olayları, sporları, sorguları, dedikoduları vb. İçerir. Müşteriye verilen desteğe bağlı olarak, diğer birçok uygulama IM'de “geridönüşlü” olabilir (içinde kapsüllenebilir). Örneğin, birçok müşteri dosya aktarımını destekler. Benzer şekilde, müşteri seslerin, seslerin, görüntülerin, hareketli görüntülerin, diğer keyfi nesnelerin, uygulamaların ve hatta tüm sistemin kontrolünün geçişini destekleyebilir. En gelişmiş IM istemcisi MS NetMeeting, bunların hepsini aynı anda destekliyor. (NetMeeting kendi başına bir sınıfa girmiştir. Diğer IM istemcilerinden çok daha karmaşıktır; genellikle sınıfın bir üyesi olarak tanınmaz.) Sunucunun rolü ileti iletme ve adresleme olduğundan, işlevsellikte değişiklik olmamalıdır. Sunucunun bu karmaşıklık seviyesine ulaşması gerekebilir. Benim için

 müşteri ve kullanıcı desteği

  birçok iş stratejisinin önemli bir parçası haline gelmiştir. Telefon desteği personeli, müşterileri veya aboneleri ile konuşurken yardım almak için onu “geri kanal” olarak da kullanır. Danışmanlık, tasarım ve programlama ekipleri IM kullanıyor işbirliği,

  hepsi aynı masada otururken bile. Üretkenliğe o kadar çok şey katıyor ki, çoğumuz onsuz çalışmayı reddediyor. Şirkette, IM genel adresi, ilan tahtalarını ve e-postaları tamamlar.

 duyurular.

 Özellikle virüs uyarıları veya zamanında olmanın zorunlu olduğu hava durumu gibi bildirimler için kullanışlıdır. Son olarak, IM “

 dedikodu,

 “Çoğu kurumun direndiği ancak yine de etkinlikleri için gerekli olabilecek alternatif iletişim kanalı.

Yetenekleri

 Bazı sunucular ve istemciler basit adresleme ve iletme dışındaki işlemleri yürütme özelliğini destekler. Bu özellik, uygulamanın kolay işlevsel uzantısını desteklemek, yani yeni yazılımı tanıtmayı kolaylaştırmak için mevcuttur. Bir IRC istemcisi (Bitchx), daha önceki bir istemciye karmaşık bir komut dosyası aracılığıyla eklenen işlevlerin birleştirilmesinden kaynaklandı. Bu eklenen programlar tamamen keyfi olabilir. Yeterli ayrıcalığı veya özel bilgileri olan herkes tarafından yazılabilir ve örneklendirilebilir. Bu özelliğe sahip sunucular, internete bağlı genel amaçlı bilgi işlem motorları olarak görülebilir. Çoğu, saldırı motorları olarak kirlenmelerini veya kullanılmalarını önlemek için güvenlik kontrollerine (örneğin kilit kelimeler veya parolalar) sahiptir. Ancak, bu sömürülebilecek birçok şey bırakıyor. Bir veya daha fazla botun, aksi takdirde daha güvenli botların kontrollerine karşı kapsamlı saldırılar yapmak için kullanıldığı “bot savaşları” gördük. Hileli bilgisayar korsanları, saldırıların kaynağını gizlemek için IM sunucularını kullanır. Bir senaryoda, tehlike altındaki sistemler bir sohbet odasına bağlanır ve bir mesaj bekler. Bu haydut hacker daha sonra o odaya bağlanır ve onu kapsamlı ve hizmet reddi saldırısının zamanını ve hedefini içeren bir mesaj göndermek için kullanır. Başka bir yolla, kanal veya oda tüm dinleme ve saldırma sistemlerini koordine etmek için kullanılır.

Simgeler

 Birçok istemci uygulaması, bir kullanıcının başka bir kullanıcıya, gönderen kullanıcının penceresindeki alıcı penceresini tanımlamak için bir simge göndermesini sağlar. Bu görüntüler rahatsız edici olabileceğinden, bu uygulamaların çoğu, çirkin bir sürprizden kaçınmak için bir seferde birkaç bit gösterme bile olsa, simgenin dahil edilmesini kontrol etme özelliğini de içerir.

IM'in güvenlik açıklarının kimseyi şaşırtması muhtemel değildir. Bunlar, İnternet’in diğer bölümlerinde gördüğümüz güvenlik açıkları. Bununla birlikte, gerekli olmadığında bunları numaralandırmak faydalıdır. Aynı temel sınıflara giriyorlar.

Temel Güvenlik Açıkları

 Temel güvenlik açıkları, çevreye veya uygulamaya özgü olanlardır. Herhangi bir eylem veya eylemsizlikten kaynaklanmazlar; onlar sadece. Bunun için tazmin edilebilirler ancak ortadan kaldırılamazlar. IM'in en büyük temel güvenlik açığı açık olmasıdır. Hizmetlere açıktır; herkes bir tane koyabilir. Ağlar sunuculara açıktır; Varsayılan olarak, herkes bir tane ekleyebilir. IM kullanıcılara açıktır; Yine, varsayılan olarak, herkes bir servise kaydolabilir. Bu, ağın girişime veya kirlenmeye karşı savunmasız olmasını ve trafiğin sızıntıya karşı savunmasız olmasını sağlar. Kapalı IM popülasyonları veya ağları oluşturmak mümkün olsa da, bu kapalı popülasyonlar ve ağlar açık olanlardan önemli ölçüde daha az faydalıdır. Ayrıca, birçok istemci uygulaması, kullanıcıların ve istemcilerin, aksi takdirde ayrık olmayan iki ağ arasında bağlantılar oluşturmasını kolaylaştırır. Kullanıcı anonimliği, ikinci bir temel güvenlik açığıdır. Tanıtıcılarda veya diğer adların kullanılması IM'de standarttır. Bu takma adlar ile benzersiz bir kimlik arasındaki bağın gücü, sahte olandan hatalı olanı lokalize etmek için yeteri kadar ama kötüyü etkili bir şekilde gizlemek için yeterince gevşektir. Bu, kullanıcının sorumluluğunu önemli ölçüde azaltır ve bazı durumlarda sorumlu tarafların kimliğini başarıyla gizlemek için kullanılabilir. Kötülüğü davet ediyor gibi görünüyor. Herhangi bir veri gizleme, gönderici ile alıcı arasında önceden ayarlamalar içerdiğinden, IM'deki çoğu trafik net bir şekilde hareket eder. Bu ağda sızıntı olabileceği anlamına gelir. Bu, trafiğin çoğunun önemsiz olduğu gerçeğiyle dengelense de, genel olarak IM'nin kurumsal uygulamalar için uygun olmayabileceği anlamına gelir. Dahası, IM kullanımı o kadar rahat ve kendiliğinden ki, kullanıcılar önemsiz trafik ile hassas trafik arasındaki çizgiyi bile fark etmeden geçiyorlar.

Uygulamaya Bağlı Güvenlik Açıkları

 Uygulamaya bağlı güvenlik açıklarının mevcut olması gerekmez. Bunlar eylemciler, ihmaller veya uygulayıcıların seçimleriyle ortaya çıkar. Çoğu hata veya gözetim sonucu ortaya çıkar. IM'deki uygulama kaynaklı güvenlik açıklarının çoğu kendisine özgü değildir. İnternetin geri kalanıyla paylaşılıyorlar. Bunlar, genellikle kanıtları ile belirlenmeyen düşük kaliteli yazılımları içerir. İnternetteki çoğu yazılım gibi, bu yazılım

 girişini kontrol etmez veya kontrol etmez

  ve bu girdiden kaynaklanan kirlenmelere karşı savunmasızdır (aşırı akma korkunç tampon). İnternetteki çoğu yazılım gibi,

 kaçış mekanizmaları

  Bilginin uygulamadan ve kontrollerinden kaçmasını sağlayan. Birçok sunucuya karşı savunmasız

 diğer uygulamalardan gelen girişim

  Aynı donanım veya yazılım ortamında çalışan. Bu yazılımın çoğu kullanır

 bant içi kontroller.

 Bazı servislerde, kullanıcı verileri (örneğin, arkadaş listeleri ve dizin girişleri) sunucularda depolanır. Bu meşru bir tasarım seçimidir; Uygulamayı daha taşınabilir hale getirir. Örneğin, birinin arkadaş listesini bir kişinin (kablosuz) PDA'sından veya bir havaalanı ya da kahve dükkanı kulübesinden kullanabilirsiniz. Ancak, milyonlarca küçük hedefi iki veya üç büyük hedefle değiştiriyor. Bu sunuculara yapılan başarılı bir saldırının sonuçlarını ortaya koyuyor. Böyle başarılı bir saldırı, büyük miktarda veri gizliliğinin tehlikeye girmesine neden olur. Bu verilerden bazıları açıklamaya duyarlı olabilir. Örneğin, irtibat listeleri kişisel dernekler hakkında bilgi içerir; Rehber kayıtları, kişisel çıkarlar hakkında, zorunlu olarak söylenmeyecek bilgileri içerebilir. Bir dereceye kadar, kullanıcılar bu bilgilerin hassasiyetini düşünmemişlerdir. Bir dereceye kadar bu bağlamda paylaşmaya isteklidirler. Çoğu durumda hiçbir şey umursamıyor. Ancak, bazıları internette yayınlanmak istemez.

Operatörün Neden Olduğu Güvenlik Açıkları

 Herhangi bir şey için IM'ye güvendiğimiz ölçüde, sunucuların operatörlerine güveniriz. Bazı durumlarda, belki de çoğu durumda, operatörlerle anlaşmamız var. Bu anlaşmalar, hizmet için hizmet şartlarını içerir; Bu TOS çoğunlukla kullanıcıyı bağlar. Genel olarak, operatörler “en iyi çabaları” vaat ediyorlar, ancak herhangi bir şey için onlara güvenebileceğimiz ölçüde, TOS'un vaatlerine güvenebiliriz. Bununla birlikte, bazı hizmetler (örneğin, IRC) doğada işbirliği içindedir. Bakabileceğimiz tek bir sağlayıcı yok. Ağ, içindeki en zayıf sunucudan daha güçlü olmayabilir.

Kullanıcının Neden Olduğu Güvenlik Açıkları

 Benzer şekilde, kullanıcıların güvenlik açıkları sağlamak için yaptıkları şeyleri bilmeniz gerekir.

 Zayıf Şifreler

 IM şifreleri botlarda saldırıya (sunucularda) rağmen, çoğu istemci uygulaması güçlü şifre kuralları uygulamamaktadır. Varsayılan olarak, çoğu IM uygulaması kullanıcının kullanıcının şifresini saklamasına ve otomatik olarak göndermesine izin verir. Ve çoğu müşteri otomatik olarak uzun parolalar girecek olsa da, kullanıcılar hala kısa olanları tercih ediyor.

 Varsayılan Ayarların Kullanımı

 Kullanıcılar varsayılan ayarları tercih eder; Kurulumu kolaylaştırır ve bir ürünün kullanımıyla ilgili özel bilgileri içerir. Mesaj alma gibi olaylar için, istemci uygulamaları varsayılan olarak "sormak" gibi görünmektedir. Örneğin, kullanıcı bir mesaj alıp almayacağını belirtmezse, Trillian istemcisi soracaktır. Ancak, diğer seçimler için sormayabilir. Varsayılan ayar, Enter tuşuna basıldığında mesajı göndermektir. Bu, mesajın incelenmeden önce yanlışlıkla gönderilmesine neden olabilir. Bir daha güvenli bir seçenek olduğunu bile anlamadım.

 Yem Nesnelerini Kabul Etmek

 Kullanıcılar, yem nesnelerini kabul ederek sistemlerini ve kurumsal ağlarını her zaman tehlikeye atabilirler. Saldırganın bakış açısından, her şey başarısız olduğunda, kullanıcı davranışlarından yararlanıldığı söylenir. Görüldüğü gibi, IM isteğe bağlı nesneleri içerecek şekilde salt metin olmaktan büyüdü. Bir kullanıcıyı tehlikeye atmak için gereken tek şey, direnmediği bir yem bulmak. Bireyler için yem kendi çıkarları bilgisinden yararlanabilir. Sohbet odalarında balık tutmak, yeterince büyük bir partide, bazı insanların ıslak patates cipsi yiyeceği gerçeğinden yararlanmaktadır. Her sherman bilir ki ısırmazsa yemi değiştirir. Hala ısırmazlarsa, yeni bir noktaya geçin. IM, çok fazla with sh olan büyük bir alandır.

 Diğer

 Tüm güvenlik açıkları listesinin “diğer” ile bitmesi gerekir. Geniş güvenlik açıkları kategorilerini belirleme konusunda iyi olduğumuza rağmen, hiçbir insan grubunun kullanıcıların tüm aptalca şeylerini tanımlaması olası değildir

Sorunlar

Bu bölümde, IM'yi çevreleyen güvenlikle ilgili bazı konular tartışılmaktadır.

Politika ve Farkındalık

 IM kullanımından kaynaklanan çoğu hasar aksi takdirde iyi niyetli kullanıcılar tarafından yanlışlıkla yapılacaktır. Çoğu teknolojide olduğu gibi, problemler gerçekten insanların problemleridir. Yönetimin kullanıcı davranışına dayanması gerekiyorsa, bu davranışı kullanıcılara açıklaması esastır. Yönetim, sevdiği neredeyse tüm politikaları belirleyebilir ancak sessiz olmayabilir. Yararlı bir kural, güvenlik politikasının tüm iletişim ortamlarına tutarlı davranması gerektiğidir. Kullanıcılar bir mesaj için en etkili ortamı seçebilmelidir. Basit bir şekilde, keyfi kuralları, güvenliği veya başka bir şeyi yerine getirmek için yetersiz bir ortam seçmeye zorlanmamalıdırlar.

Anlık Mesajlaşma Güvenliği Sorunları ve Çözümleri

Ef eksiklik

 Yönetim, IM'in gerçekten verimsizliği ve kullanıcıları işten uzaklaştırma potansiyelini telafi etmek için verimliliği artırıp artırmadığını sorguluyor. Yönetimin artık telefonun en müdahaleci teknolojisi hakkında aynı soruyu sormaması artık öğreticidir. Her durumda, yönetimin çok fazla seçeneği varmış gibi değil. IM kullanımı için büyüme paterni iyi bir şekilde oluşturulmuştur ve tersine çevrilmesi veya hatta dengelenmesi beklenmemektedir. Yönetim en iyisine alışmıştı; işçiler olacak. İşçiler, telefon, bilgisayar ve e-postaları olduğu için IM'yi çalışma stillerine entegre edeceklerdir. Dikkat dağıtıcı olarak görülmeyecek, çalışma alanının bir parçası olarak görülecektir. 1950’lerin başlarında işe girdiğimde masalar varsayılan olarak bir telefonla gelmedi. Dizinde sadece birinin adı olmalı. “Açık” diyorum, çünkü genellikle bir ya da iki sayfa uzunluğundaydı. Doğrudan içeri arama yapılmamıştı (DID); gelen tüm çağrılar operatörden geçti. Bazı iş telefonlarında arama bile yoktu; operatör giden aramaları tamamladı. Ücretli telefon hizmeti dünyasında, artık müşterilerimden iş aramalarının maliyetini geri almaya çalışmıyorum

Kişisel kullanım

 Tüm iletişimler için önemli bir politika konusu kişisel kullanım konusudur. İşletmenin kaynaklarını korumak için yönetimin temel bir sorumluluğu vardır. Kullanıcılara, kurumsal kaynakların nasıl tüketilebileceği konusunda talimat vermelidir. Kişisel kullanım ile ilgili olarak, IM telefon veya posta odası ile aynı şekilde ele alınmalıdır. Yönetim, telefonun kişisel kullanımına izin veriyorsa, benzer kurallar altında IM'in kişisel kullanımına izin vermelidir. 20 yıl kadar önce, işverenim bana atanan telefondan yapılan tüm aramaların ayrıntılı bir muhasebesini gönderdi. “Kişisel” olanları tanımlamam ve bu çağrıları karşılamak için kasiyere bir çek yazmam bekleniyordu. Hatırlamak için çok genç olanlarınız “Ne kadar ilginç” diyeceklerdir. O zaman bile, “kişisel” çağrıların maliyeti, harcadığım zamanın değeri ile karşılaştırıldığında önemsizdi. Bu 20 yılda, telefon görüşmelerinin maliyeti düştüğü için, kişisel kullanım için toplam muhasebe maliyeti, elde edilebilecek harcamalardaki azalmayı aşmaya başladı ve bunu durdurduk. Artık işçiler cep telefonlarını işe koyuyor ve üzerlerinde kişisel görüşmeler yapıyor ve alıyorlar.

Anonimlik

 Daha önce belirttiğimiz gibi, takma adların ve "tutamaçların" kullanımı IM'de varsayılandır. Bu tutamaçların adı, rolü veya (e-posta) adresiyle ilgili olabilir, ancak genellikle kullanıcının yansıtmak istediği bir kişiyle ilgilidir. Bazı kullanıcılar çok var. Dizin girişleri de bu görüntüyü bilgilendirmek için yansıtmak için kullanılır. Hizmete veya ortama bağlı olarak, tanıtıcı kullanıcının kimliğine bağlı olabilir veya olmayabilir. Örneğin, AOL IM kullanıcılarının mesaj hedefleri olarak bir isim belirtmeleri gerekir. Bununla birlikte, AIM, kullanıcının birden fazla isteğe bağlı ad belirtmesini sağlar. Ancak, bir kez kaydolduktan sonra bir isim kullanıcıya aittir. Onu terk edebilir; ama bunu yapana kadar ve o olmadıkça, onun. IRC, yalnızca bir bağlantının ömrü boyunca takma ad ayırır.

Görünürlük

 Anonimliğin diğer tarafı görünürlük - yani, IM sisteminin birisini diğer kullanıcılar tarafından nasıl tanıttığıdır. Sizi tamamen gizleyen bir sistem hiç faydalı olmayabilir. Ancak, birini çok görünür kılan, konunun düşündüğünden daha fazla bilgi sızdırması olabilir. Eğer A B'ye bir mesaj gönderirse, A B'nin çevrimiçi / çevrimiçi olmadığını belirten bir mesaj alabilir. Eğer A ve B birbirlerinin irtibat listesinde ise, her birinin diğerinin durumu (çevrimiçi / ine, aktif / pasif, ev / uzakta) hakkında bilgi bulunabilir. Birçok sunucu, kullanıcı sunucuya kaydolduğunda, kullanıcının kişi listesindeki herkes hakkında bilgi verecektir. Weemanjr AIM'ye bağlanıp oturum açtığında, müşterimde adının yanındaki simge yanar. İmlecimi simgesinin üzerine geçirirsem, bağlantısının durumu hakkında, örneğin çevrimiçi olup olmadığı, ne kadar süredir çevrimiçi olduğu veya en son ne zaman görüldüğü; AOL çevirmeli ağ istemcisi veya İnternet üzerinden bağlı olup olmadığı ve müşterisinin yetenekleri

Bilgi Güvenliği Yönetimi El Kitabı

vardır. Tabii ki kimliğini bilmeliyim, Weemanjr. IM adının e-posta adresiyle veya AOL ekran adıyla aynı olduğunu varsayabilirim, ancak hatalı olurdum. Ancak, biri benim hakkımda bu varsayımı yaptıysa, biri doğru olacaktır.

İhlal

 En iyi durumda ve zaman zaman anlık iletiler izinsiz girer. Spam kadar müdahaleci olmasalar ve telefondan kesinlikle daha az müdahaleci olmalarına rağmen, yine de müdahalecidirler. Çoğu istemci uygulaması, kullanıcının belirli kullanıcılardan gelen trafiği reddetmesine izin vermek için kontroller sağlar; izin verici politika. Gerçekten, belirli kullanıcılar dışındaki tüm trafiğin reddedilmesine izin veriyorlar: kısıtlayıcı politika. Her iki durumda da, kullanıcının politikayı seçmesi ve yönetmesi için bir miktar işlem yapılması gerekir.

Kaçak

 Girişimcinin IM'nin güvenliği konusunda endişelendiği ölçüde, genellikle gizli bilgilerin sızması ile ilgilidir. IM birçok yönden bilgi sızdırabilir. Kullanıcı, yanlışlıkla ya da öfke ya da spite gibi motiflerden bilgi sızdırabilir. Bilgi aktarımda sızıntı olabilir. Ayrıcalıklı sunucu kullanıcılarına veya tehlike altındaki sunuculardan sızıntı yapabilir. Dizinler veya kayıt defterleri aracılığıyla sızıntı yapabilir. Kişi listelerinin yerel olarak veya sunucuda saklanabileceğini unutmayın. Sunucuların bir dereceye kadar güvenilmesine ihtiyaç duyulmasına rağmen, orada saklanan bilgiler sızıntıya açıktır. Bir sunucuda bu bilgilerin toplanması, müşteri tarafında depolanan ayrı kayıtlardan daha çekici bir hedeftir. Kurumsal IM sistemleri, bazı trafiğe günlükleri kaydeder. Bu günlükler hedef haline gelir ve bilgi sızıntısı olabilir.

Kablosuz

 Giderek, IM kablosuz içerir. İnternet özellikli cep telefonlarının çoğu, genellikle AOL IM veya Yahoo! AOL ve Yahoo! Palm OS ve Windows Pocket PC cihazları için istemciler. Bu cihazlara trafik aktarma mekanizması tarafından kısmen gizlenmiş olsa da, bu cihazlar henüz uçtan uca şifrelemeyi desteklememektedir. IM ayrıca dizüstü bilgisayarlara kablosuz LAN teknolojisi (802.11) üzerinden kullanılır. Bu cihazlar hem bağlantı şifrelemeyi (örneğin, SSL) hem de uçtan uca şifrelemeyi destekleyebilir. Kablosuz LAN şifrelemesi, standart (WEP) veya tescilli, birinin kablosuz bağlantıların farkında olduğu yerlerde faydalı veya belirtilmiş olabilir. Ancak asıl mesele, ucuz kablosuz ağın taşıma katmanını güvenilmez hale getirmesidir. Bu, uçtan uca şifreleme kullanılarak telafi edilmelidir.

Dolaysızlık

 IM “gönder” tuşuna basıldığında, olabilecek herhangi bir hasar çoktan yapıldı. Ne kullanıcı ne de yönetim ikinci bir şans alır. Gönderme tuşu, dönüş veya yeni hat tuşuyla aynıysa, erken veya yanlışlıkla yapılan göndermelerle sonuçlanabilir. Bazı anlık mesajlaşma uygulamaları birisinin müşteri tercihlerini belirleyebilmesine izin verir, böylece bir mesaj göndermenin güçlü bir niyet gerektirmesi gerekir.

Geç bağlama  Görüldüğü gibi IM geç programlanabilirlik için ayrı bir tercih ortaya koyuyor; yani, istemci uygulama programının işlevini değiştirmek kolay olabilir. Ne de olsa, IM'nin çoğu “programcılar için programcılar tarafından oluşturuldu”. Bunun bir anlamı, bu tekliflerin tutarlı davranışına güvenmenin zor olduğudur.   dolandırıcılık  Anonimlik veya hatta onsuz, IM her türlü aldatmaca ve sahtekarlığı gerçekleştirmek için kullanılır. Kullanıcılar, özellikle güvenilir kaynaklardan geliyor gibi görünüyorsa, ekranlarında açılan mesajlara inanma eğilimindedir. Örneğin, bir mesaj, alıcının bir parola girmesini, bir komut girmesini veya bir simgeyi veya bağlantıyı tıklatmasını önerebilir. Bu, alıcının kimliği ve imtiyazları ile bu işlemi başlatmanın bir yoludur.   AU1997\_Frame\_Ch050 Sayfa 610 17 Kasım 2003 Pazartesi 13:20 © 2004, CRC Press LLC tarafından   Anlık Mesajlaşma Güvenliği Sorunları   611   Güven  Genel bir kural olarak, IM kullanıcıları, birbirlerini içerik olarak tanıma yeteneklerine güvenirler; çevreye güvenmiyorlar ve güven de bir sorun değil. Ancak, gelecekte, nüfuslar daha büyük olacak ve güvenilir dizinler ve kayıtlar için gereklilik de daha yüksek olacaktır.

Gözetim

 Yönetim, sürveyansı genel olarak iletişim kullanımını ve özellikle de IM kullanımını kontrol etmek için bir kontrol olarak kullanabilir. Bazı durumlarda öyle yapmalı. Bununla birlikte, herhangi bir iletişim ortamının sürveyansı yaygın veya hatta rutin hale gelirse, kullanımı devam eder ve değerini azaltır. Yönetimin iletişim içeriğine olan ilgisi, çalışanın makul mahremiyet hakkına karşı dengelenmelidir. IM, spontanlık açısından ve bıraktığı kaydın değeri ve kalıcılığı açısından telefon ve e-posta arasında bir yerdir. Benzer şekilde, IM'nin otomatik denetlemesinin maliyeti ve faydası, telefonun ve e-postanın da arasındadır. Sesli telefonun otomatik olarak izlenmesini sağlayanlar kesinlikle IM'in izlenmesini de otomatikleştirmek isteyeceklerdir. Bununla birlikte, e-posta denetlemesini otomatik olarak almayanlar kesinlikle IM'nin denetlenmesini otomatikleştirmek istemeyeceklerdir. Herhangi bir iletişim gözetimi kaydı, açıklamaya, orijinal iletişimin kendisinden daha hassastır. Bir saldırı hedefi ve “süren keşif gezileri” haline geldi. İyi uygulama, böyle bir kaydın erken kullanılmasını ve sonra imha edilmesini önerir.

Saldırgan İçerik

 En azından kenarlarda, İnternet de dahil olmak üzere toplum çirkinlik içeriyor. IM buna bir istisna değildir. Bu, kısmen IM'nin çocukların sevdiği bir uygulama olması ve çocuklar için en sevdiği uygulamanın sosyalleşmesi nedeniyle sıkıntılı bir durumdur. Çocuklar aynı zamanda diğer yerlerde tatmin etmekten çekindikleri (cinsel) merakı tatmin etmek için IM'yi kullanırlar. Yüksek sesle ve yüz yüze söylemekten alıkoydukları şeyleri söyleme pratiğini yapmak için kullanırlar. Rutin gizlenme veya kullanıcı kimliğinin yanlış beyanı (örneğin, yaş, cinsiyet, görünüm, sınıf, rol) ile birleştiğinde, sonuç çocukların çirkinliğe ve hatta baştan çıkarmaya maruz kalabileceğidir. İnternetin baştan çıkarma konusunda evden, okuldan, kiliseden, alışveriş merkezinden veya oyun alanından daha güvenli olabileceği ancak bu durum özellikle mümkün olduğunda küçük bir rahatlık olabileceği anlamına gelebilir. İşletmelerdeki benzer davranışlar veya içerikler, işletmelerin daha uyumlu bir çalışma ortamı sağlama sorumluluğunu tehlikeye atabilir. Bir başka şekilde, işletme, çalışanlarını çirkinlikten korumaktan sorumlu olsalar bile, sorumlu tutulabilir.

Disiplin

 IM alanı çok hoşgörülüdür ancak kibar davranış standartlarına sahiptir. Diğer sosyal popülasyonlarda olduğu gibi, bu standartları ihlal etmek için yaptırımlar var. Herhangi bir kaba davranışta olduğu gibi, ilk yaptırım toplum tarafından da ön plana çıkmaktadır. Kaba bir şekilde davrananlar kendilerini dışa vurdular, yani dışlanmışlardı. Servis sağlayıcı daha sert yaptırımlar uygulayabilir. Örneğin, AOL hizmet şartlarını şiddetle uygulamaktadır. Littleone “ICQ sohbet odasındaydı”. AOL hizmet şartlarını ihlal eden bir dil kullandı. Bu, littleone'nin IM tarafından sağlanan anonimlik pelerini olmadan kullanmamış olması muhtemel bir dildi. Littleone, annesinin ondan veya başka birinden duymasını istemediği bir dildi. Hesap sahibi olan annesi, AOL destek temsilcilerinden bir çağrı aldıktan sonra ona dili hatırlattı. Destek temsilcileri, onun hareketlerini biraz çözemezse hesabını iptal edeceğini söyledi. Biri IRC'den tamamen yasaklanamazken, kanal sahipleri IP adreslerine göre kaba kullanıcıları engelleyebilir ve engelleyebilir. Davranış standartlarını zorlamak için tüm alanları dışlamaları ya da aralıkları ele almaları bilinmektedir. Girişim yönetimi çok fazla güç ve disiplin kullanıyor. IM işyerinin bir parçasıdır ve orada olanlardan yönetim sorumlu ve sorumludur. Bazı kullanıcı IM davranışlarından yönetim sorumlu tutulabildiğinden, bazı kontroller uygulamalıdır. En azından, yönetim işçilere söylemelidir

Bilgi Güvenliği Yönetimi El Kitabı

Hangi kullanım uygun, hangisi uygun değil. Diğer güvenlik ihlallerinde olduğu gibi, yönetim disiplin cezalarını da kullanabilir - kınamadan sona erdirmeye kadar.

Kontroller

Beklediğiniz gibi IM, kullanıcılarını ve trafiğini korumak için kullanılabilecek kontroller ile birlikte gelir. Kullanıcı, ebeveynler ve veliler veya yöneticiler bu özellikleri riski yönetmek için kullanabilir. Bununla birlikte, IM'in doğal olarak yüksek riskli olduğunu ve bu kontrollerin ihtiyatlı bir şekilde uygulanmasında bile genellikle böyle kalacağını unutmayın.

Kayıt

 Birçok IM sistemi, kullanıcının benzersiz bir kamu kimliğini kaydetmesini gerektirir. Diğer kullanıcılar bu tanımlayıcıyı kendisine mesaj göndermek için kullanacaktır. Servis bu mesajı mesajların gönderileceği ağ adresini bulmak için kullanacaktır. Aynı zamanda, kullanıcının servisle sır değiştirmesi gerekebilir. Bu parola, hizmetin yalnızca gönderen tarafından amaçlanan tarafa mesaj göndermesini sağlamak için kullanıcının kimliğini doğrulamak için kullanılacaktır. Bazı sistemler, halihazırda kullanıcısı olanlardan sadece bir tane kayıt kabul edecek olsa da, çoğu kişi hemen hemen herkesin keyfi bir numarasına izin verecektir.

Dizinler

 Servisler bir kullanıcı dizini ve adreslerini tutabilir. Kullanıcılar bu dizini, mesaj göndermek istediklerinin kimliğini bulmak için kullanabilir. Birçok kamu sisteminde, dizindeki bilgiler kullanıcı tarafından sağlanır ve güvenilir değildir. Bazı servis sağlayıcılar, bir kullanıcı kimliği ile örneğin gerçek bir isim ve adres arasındaki ilişkiyi geliştirmek için hesap ve fatura bilgilerini kullanabilir. Örneğin, AOL kullanıcılarının bir dizini tutar. Bu dizine erişim, AOL aboneleri tarafından kullanılabilir. AOL, abonelerin kendi dizin girişlerine erişimi sınırlamalarına izin verir. Özel sistemlerde, yönetim dizinin sahibine sahip olabilir ve tüm kullanıcıların yetkilendirilmiş, doğru adlandırılmış ve dizindeki tüm tanımlayıcı bilgilerin (örneğin bölüm, işlev veya rol) güvenilir olmasını sağlayabilir.

Kimlik ve Kimlik Doğrulama  Çoğu IM uygulaması, gönderenleri ve alıcıları tanımlamak ve doğrulamak için kullanılabilecek kontroller sağlar. Çoğu, hem tanımlayıcı hem de parolanın kimliğin hem açık hem de taklit edilmesinin zorlaştırılmasında yeterli uzunlukta olmasına izin verir. Bununla birlikte, çoğu güvenlik üzerinden bağlantı için bir tercih uygulamaktadır; yani, başlarlar, bağlanırlar ve hatta otomatik olarak oturum açarlar. Bu, değerin bağlantıların sayısı ve sürekliliği ile arttığını kabul eder. Parolanın veya parolanın yerel olarak depolanmasını gerektirir. Bağlanabilirliğin değeri çok yüksek olduğundan, bağlantı zaman aşımına uğramaz. Böylece, makine uygun şekilde başlatıldığında, bağlantılar ve kimlik, makineye erişimi olan herkes tarafından kullanılabilir. Parolayı öğrenmek yeterli olmayabilir, ancak bir süre kullanmak yeterli olabilir. Elbette, sistemi çalışan bir durumda fiziksel erişimi olan bir kişiden korumak çok zordur, bu yüzden bu bir I&A sistemi kadar fiziksel bir güvenlik sorunudur. Bu nedenle, şifreler, masaüstünün denetlenmesini veya bağlantıyı sürdürürken ekran ve klavyenin zaman aşımına uğramasını gerektirmek pahasına sunucuya saldırmaya karşı direnç gösterir (Windows NT veya 2000'de olduğu gibi). Öte yandan, şifrelerin saklanması ve otomatik olarak girilmesi, hataların ve yeniden deneme işlemlerinin uzunluğa (hızla) yükselmediği anlamına gelir. Uzun isimler, kimliği daha patentli kılar ve adresleme hatalarını azaltır. Uzun parolalar ayrıntılı ve tahmin edici saldırılara karşı koyar. Parolalar IM programları tarafından desteklenen tek kimlik doğrulayıcılar olsa da, bunlar istemci makinede kullanılan güçlü kimlik doğrulama yöntemleriyle tamamlanabilir. Örneğin, eğer BIOS ve OS şifreleri kullanılıyorsa, bunlar saklanan IM şifresini korurlar.   Tercihler  İstemci uygulamaları, kullanıcının tercihleri ​​belirtmesini sağlar. Bunların çoğu güvenlikle ilgilidir. Kullanıcı, sistem başlangıcında, müşteri başlangıcında, bağlandığında ve bir mesaj alındığında ne olacağını belirleyebilir. İçin   AU1997\_Frame\_Ch050 Sayfa 612 17 Kasım 2003 Pazartesi 13:20 © 2004, CRC Press LLC tarafından   Anlık Mesajlaşma Güvenliği Sorunları   613   Örneğin, kullanıcı sistem başlangıcında istemciyi başlatabilir, uygulama başında bağlanıp oturum açabilir, kişi listesini ve uygulama başlangıcında kişi durumunu yükleyebilir ve ardından “uzakta” ​​durumunu ve varsayılan uzak mesajı ayarlayabilir. Kullanıcı alarm olaylarını, sesleri ve eylemleri ayarlayabilir. Günlüğe kaydedilecek olayları ve mesajları, günlüğün nereye kaydedileceğini ve onu görüntülemek için hangi programı kullanacağını belirtebilir (ör. Notepad, Excel). Kullanıcı alınan dosyaları saklamak için varsayılan dizini belirleyebilir. Simgeleri otomatik olarak kabul edip etmeyeceğini, hiçbir zaman kabul etmeyeceğini veya kullanıcıya sorabileceğini belirtebilir.

Bloke etme

 Sohbet uygulamaları, varsayılan olarak ve belirli kullanıcılardan gelen tüm kullanıcılardan gelen mesajları engelleme olanağı sağlar. Engelleme, izinsiz giriş, taciz veya rahatsız edici içerik riskini azaltır. İstemcide engelleme gönderenin adına dayanır. Alıcıyı izinsiz giriş, çirkinlik ve istenmeyen postalardan korumak için kullanılır. Varsayılan olarak, alıcının irtibat listesinde olmayan bir göndericiden gelen bir mesaj engellenebilir; kullanıcıdan mesajı alıp göndereni irtibat listesine eklemek isteyip istemediği sorulacaktır. Engelleme, işletme çevresinde veya sunucuda da yapılabilir. Burada gönderen adına veya alıcı adına bağlı olabilir. Gönderenin adı engelleme yukarıdaki gibi çalışır. Alıcı adına engelleme, alıcıyı gönderenin adının randomize edildiği hizmet reddi saldırısından korumak için giriş kontrolü olarak kullanılabilir. Bir ağ veya bir kullanıcı popülasyonu üzerinden merkezi blokaj yönetimi için ürünler mevcuttur.

Doğrudan bağlantı

 Bazı istemci uygulamaları, kullanıcıların doğrudan birbirine bağlanmasını sağlar; böylece trafik sunucudan geçmez ve o sunucunun ayrıcalıklı kullanıcıları tarafından görülemez.

Şifreleme

 Benzer şekilde, bazı kurumsal IM istemci uygulamaları kullanıcıların iletişimlerini şifrelemelerini sağlar. Birçok IM uygulaması (tek yönlü) SSL kullanıcıdan sunucuya ve sunucudan kullanıcıya kullanarak şifreler. Bu uygulama, mesajın A’nın anahtarından şifresini çözmesini ve B’nin altında sunucuda tekrar şifrelenmesini gerektirir. Bu, mesaj içeriğini sızdırmamak için sunucunun güvenilir olması gerektiği anlamına gelir. IM sunucusu her durumda bir dereceye kadar güvenilirdir; İşletme içerisinde oldukça güvenilir olabilir. Bu sistemin avantajı, emsalsiz istemciler arasında bilgilerin çoğundan çoğa şifrelenebilmesidir. Tek şart, tüm istemcilerin SSL'yi desteklemesidir. Birkaç ürün trafiğin uçtan uca şifrelenmesini ancak sadece akran sistemlerine izin vermektedir. Örneğin, Trillian Professional müşterileri doğrudan iletişim kurabilir ve oturumlarını baştan sona şifreleyebilir. Bu, kullanıcıların kısmında fazladan bir seçim ve biraz daha fazla kurulum süresi gerektirse de, sistemler arasında sızıntı riskini azaltır. Lotus Sametime Connect, kurum içindeki AIM sunucusunda kayıtlı diğer kullanıcılara şifrelenmemiş oturumlara izin verirken, kurum içindeki iki veya daha fazla kullanıcı arasında otomatik olarak uçtan uca IM oturumları oluşturmak için Lotus Notes PKI'sini kullanır.

Günlüğü

 Enterprise IM istemcileri ve hizmetleri, sunucuda yapılan ve kullanıcının kontrolünde olmayan günlükleri içeren günlük oluşturma yetenekleri sunar. Bu, trafiğin bilgi sızıntısı, dolandırıcılık, taciz veya diğer yasaklanmış faaliyetler için kanıtlanmasına izin verir (örneğin, borsacılar tarafından talep edilmesi, sağlık hizmetlerinin yasaklanması amacıyla sipariş verilmesi). Telefon trafiğini benzer şekilde kaydetmek mümkün olsa da, bu kayıtları denetlemenin maliyeti yasak olacaktır. İşletmeler bunu anladıkça, IM sadece bu tür bir iletişim için izin verilen bir araç değil, aynı zamanda tercih edilen bir araç haline gelir. İşletme yönetimi, log değerinin zamanla hızlı bir şekilde azaldığını ancak sıkıntı değerlerinin arttığını unutmamalıdır. Doğru şeyi yapmayı sağlamadaki değerleri, doğru şeyi yapmadığınızı gösterme potansiyeli arttıkça azalır. Günlükler hassas bilgiler içerebilir ve hedef olabilir. Kullanımları üzerinde erişim kontrolleri faydalı olmalarını sağlamak için gereklidir ancak bilgi sızdırmaz.

Raporlama

 Kurumsal IM ürünleri, hem IM kullanımını hem de mesaj trafiği içeriğini bildirir. Doğru şekilde ayrıcalıklı kullanıcılar ve yöneticiler yalnızca trafiğin içeriğini görmekle kalmaz, aynı zamanda dizinde ve kayıt sunucularında gönderen ve alıcıyla ilgili açıklayıcı bilgilere geri dönebilir. Bazı ürünler bu bilgilerin zayıf bir istemci (Web tarayıcısı) ile görüntülenmesine izin verir.

Denetleme

 Denetim, amaçlanan ve beklenenlere olanların uzlaşması olarak görülebilir. Ayrıca, içeriğini anlamak için kayıtların gözden geçirilmesi olarak da görülebilir. Yöneticinin veya denetçinin, politika içeriğini ve problemin düzeltilmesini yönlendirmek için günlük içeriğini bilgiye dönüştürmesine yardımcı olmak için kullanabileceği veri azaltma, analiz ve görselleştirme ürünleri vardır. Bu ürünler, türler, elektronik tablolar, veritabanları ve veri madenciliği araçları gibi genel amaçlı araçları içerir. Ayrıca, ne arayacakları, nasıl bulabilecekleri ve ne yapacaklarıyla ilgili özel bilgileri içeren özel araçlar da vardır.

Süzme

 Hassas veya uygunsuz içerik veya virüs imzaları öneren anahtar kelimeler için mesajlar ve diğer veri nesneleri için ürünler kullanılabilir. Bilgi sızıntısına, sistem ve ağ kirliliğine karşı koymak için kullanılabilirler. Etkin kullanım için, bu ürünler hem politikaya (hangi trafiğin yüklenmemesi gerektiğini belirtmek gerekir) hem de yönetim (bu politikayı, kullanıcının kullanabileceği kurallara dönüştürmek için) gerektirir. Mesajına gecikme eklerler ve meşru trafiği engelleyebilecek yanlış pozitifler üretirler. Kural koymada rehberlik etmek için yalnızca politika değil aynı zamanda düzenlemelerin mevcut olduğu sağlık ve finansal hizmetler gibi düzenlenmiş işletmelerde de uygulanabilirler. IM kullanımı arttıkça ve bilgisayarlar daha verimli hale geldikçe, uygulamaların daha etkili ve verimli olmaları beklenebilir.

Alarmlar ve Mesajlaşma  IM trafiğini virüs ve hassas içerik bakımından trafiğe sokan ürünler alarm üretecektir. Bu alarmlar, gerekli düzeltici eylemi başlatacak konumda olanlara iletilmelidir. Alarmlara sürekli cevap vermemek, suistimali davet edecek veya teşvik edecektir.

Öneriler

Karayolu güvenliği veya telefondaki güvenlik gibi, IM'deki güvenlik, kullanıcıların ve kurumların çabalarının bir sonucu olacaktır. Bir kişi veya kurum tek başına hareket ederek güvenliği sağlayamadığından, aşağıdaki tavsiyeler rolle düzenlenmiştir. • Genel: —P, bağlantı ve sipariş arasındaki makul bir denge için AOL IM kayıt defterine bakın. —P, eksiksiz işlevsellik ve uçtan uca trafik gizleme için MS NetMeeting'e bakın. —P güvenilirlik ve özgünlük için işletme dizinlerine bakın. • İşletmeler için: — Uygun politikaları yayınlayın ve uygulayın. Kişisel kullanım, yazılım ve içeriği göz önünde bulundurun (tehdit edici, cinsel içerikli veya çirkin olanlar dahil). Özel bilgilerin sızıntısını göz önünde bulundurun. —P kurumsal IM istemcisi ve sunucu uygulaması ürünlerini gösterir. —Yalnızca yönetim tarafından seçilen ve güvenilir uygulamalardan, güvenilir kaynaklardan ve kurcalanmayacak ambalajdan yararlanın.

P, güvenlik için kapalı ağlara ve şirket tarafından yönetilen sunuculara bakın. - Çevre veya ağ geçitlerinde kontrol trafiğini kontrol edin; uygun duvarlar ve proxy'ler kullanın. —Şirket dizinlerini kullanın. - Uzun parolalar isteyin. - Kurumsal veriler için doğrudan müşteriden-müşteriye bağlantılar ve uçtan uca şifreleme gerektirir veya tercih edin. - Trafik ve denetim trafiği ﬁ c; Düzenlemeyle cesareti kırılmadığı sürece, denetim tamamlandıktan sonra kütüğü imha edin. - Poliçe veya yönetmelik ile belirtilen yerlerde trafiği filtreleyin. • Ağ ve sunucu operatörleri için: —Uygun servis koşullarını yayınlayın ve uygulayın. —Bilgisayarları tek uygulama sistemleri olarak yapılandırın. —Sistemdeki geç değişikliklere izin vermeyin; script veya komut işlemcileri çalıştırmayın (“bot” yok). —P (bant dışı) sunucu kontrolleri için güvenli kanalı yönlendirir. - Kayıt veritabanı için ayrı bir cihaz düşünün. • Kullanıcılar için: İhtiyaçlarınızı karşılayan, işlevsel olarak en sınırlı müşteriyi kullanın. —P, AOL, MS Messenger ve Yahoo! Gibi popüler tüketici sistemlerini ifade eder. - Kullanım amacınıza uygun en sınırlı ayarları kullanın. - Yalnızca sizin zaten bildiklerinizden gelen mesajları ve diğer veri nesnelerini (örneğin, dosyalar, simgeler, görüntüler) kabul edin; varsayılan olarak diğer tüm trafiği engelle. - Gizliliğinizi kişileriniz için kullanım kolaylığına karşı dengelemek için kullanıcı adlarınızı seçin. Kapsamlı saldırılara karşı koymak için uzun parolalar kullanın. Sadece gerekli verileri halka açık rehberlere yerleştirin. —Bir cevap modelini belirleyene kadar çoğu tercih için “bana sor” ayarını kullanın. - Beklenmeyen nesneleri kabul etmeyin; Beklenmeyen istemlere veya mesajlara cevap vermeyin. - Başkaları tarafından önerilen nesneleri veya metin dizelerini istemcinize girmeyin. • Ebeveynler ve veliler için: —Çocuklarınızın bağlantılarını bilin. —Küçük çocukların temaslarını tanıdıklarınızla sınırlamak için engelleme kontrolleri kullanın. • Çocuklar olgunlaştıkça mahremiyete karşı korumayı dengeleyin.

**Güvenlik Vaka Çalışması: Cisco IT, Cisco Internet Access Konumlarını Korumak İçin Güvenlik Duvarlarını Nasıl Kullanır?**

Cisco PIX Security Appliance, daha küçük İnternet ağ geçitlerinde durumsal güvenlik duvarı koruması sağlar.

Cisco Systems®, verilerini ve ağını şirket içinde ve dışında yetkisiz kullanıcılardan korumaya büyük öncelik vermektedir. Uzun yıllardır kabul edilen çözüm, dünya çapında çok kanallı İnternet ağ geçitlerinin her birinde bir güvenlik duvarı kullanmaktı. Donanım veya yazılım tabanlı olabilen bir güvenlik duvarı ağ trafiğini inceler ve paketleri erişim kontrol listelerine (ACL'ler) ve inceleme kurallarına göre hedeflerine iletip iletmeyeceğine karar verir.

Son zamanlarda Cisco® IT, uzaktan erişim VPN bağlantısını daha iyi desteklemek için veri merkezlerinde İnternet ağ geçitlerini dağıtmaya başladı. Uzaktan çalışan çalışanların, Internet üzerinden dolambaçlı yollardan paket göndermek yerine doğrudan en yakın Cisco VPN ağ geçidine bağlamak için şirket intranetine daha iyi erişimi gerekir. 2001'den 2004'e kadar Cisco IT, İnternet erişim noktalarının sayısını 5'ten 11'e yükseltti. Cisco IT, bu küçük ağ geçidi sitelerinde erişim güvenliği sağlamak için Cisco PIX® 535 Firewall'u seçti. Cisco PIX 525 Güvenlik Uygulaması kullanıma sunulduğunda, Cisco IT bunu tüm yeni İnternet ağ geçitlerinde dağıtmayı seçti, çünkü 525 tüm Cisco IT ihtiyaçlarını daha küçük bir formda destekledi. Cisco PIX güvenlik cihazında bulunan önemli bir avantaj, durumsal incelemedir. Durum denetimi yapan bir güvenlik duvarı, bir yönde geçen bir ağ bağlantısının durumunu hatırlar, böylece akış diğer yönde döndüğünde, güvenlik duvarı onu tanır ve hedefine iletir. Hasan Talukdar şöyle açıklıyor: “Ana bilgisayar A ile ana bilgisayar B arasında bir TCP bağlantımız olduğunu varsayalım. İlk paket akışının bir kaynak IP adresi ve bir hedef bağlantı noktası ve kimliği olacak. Trafik geri geldiğinde, kararsız güvenlik duvarı onu hatırlamaz ve bu nedenle izin verilip verilmediğini görmek için kurallara bakmak gerekir. Durum bilgisi olan bir bağlantı güvenlik duvarı, bunun tersine, geri dönüş trafiğini görmeyi ve kuralları kontrol etmeden, performansı iyileştirmeden ve ikinci bir ACL dizisi sağlama ihtiyacını ortadan kaldırmadan iletmeyi bekler. " güvenlik duvarı onu tanır ve hedefine iletir. Hasan Talukdar şöyle açıklıyor: “Ana bilgisayar A ile ana bilgisayar B arasında bir TCP bağlantımız olduğunu varsayalım. İlk paket akışının bir kaynak IP adresi ve bir hedef bağlantı noktası ve kimliği olacak. Trafik geri geldiğinde, kararsız güvenlik duvarı onu hatırlamaz ve bu nedenle izin verilip verilmediğini görmek için kurallara bakmak gerekir. Durum bilgisi olan bir bağlantı güvenlik duvarı, bunun tersine, geri dönüş trafiğini görmeyi ve kuralları kontrol etmeden, performansı iyileştirmeden ve ikinci bir ACL dizisi sağlama ihtiyacını ortadan kaldırmadan iletmeyi bekler. " güvenlik duvarı onu tanır ve hedefine iletir. Hasan Talukdar şöyle açıklıyor: “Ana bilgisayar A ile ana bilgisayar B arasında bir TCP bağlantımız olduğunu varsayalım. İlk paket akışının bir kaynak IP adresi ve bir hedef bağlantı noktası ve kimliği olacak. Trafik geri geldiğinde, kararsız güvenlik duvarı onu hatırlamaz ve bu nedenle izin verilip verilmediğini görmek için kurallara bakmak gerekir. Durum bilgisi olan bir bağlantı güvenlik duvarı, bunun tersine, geri dönüş trafiğini görmeyi ve kuralları kontrol etmeden, performansı iyileştirmeden ve ikinci bir ACL dizisi sağlama ihtiyacını ortadan kaldırmadan iletmeyi bekler. " Trafik geri geldiğinde, kararsız güvenlik duvarı onu hatırlamaz ve bu nedenle izin verilip verilmediğini görmek için kurallara bakmak gerekir. Durum bilgisi olan bir bağlantı güvenlik duvarı, bunun tersine, geri dönüş trafiğini görmeyi ve kuralları kontrol etmeden, performansı iyileştirmeden ve ikinci bir ACL dizisi sağlama ihtiyacını ortadan kaldırmadan iletmeyi bekler. " Trafik geri geldiğinde, kararsız güvenlik duvarı onu hatırlamaz ve bu nedenle izin verilip verilmediğini görmek için kurallara bakmak gerekir. Durum bilgisi olan bir bağlantı güvenlik duvarı, bunun tersine, geri dönüş trafiğini görmeyi ve kuralları kontrol etmeden, performansı iyileştirmeden ve ikinci bir ACL dizisi sağlama ihtiyacını ortadan kaldırmadan iletmeyi bekler. "

Cisco'nun Cisco PIX güvenlik cihazını konuşlandırması için bir başka teşvik, durumsal denetleme güvenlik duvarları ile ilgili ancak bunlardan farklı bir durum olan durumsal yük devretme tarafından mümkün kılan gelişmiş uygulama kullanılabilirliği idi. Varlığın her noktasında (POP), Cisco'nun iki yedek Cisco yönlendiricisi vardı. Birincil yönlendirici başarısız olursa, ikincil otomatik olarak kontrol altına aldı; ancak, başarısız olduğunda birincil yönlendiriciden geçen paketler atılır. Bu gerçekleştiğinde, H.323 ve Oturum Başlatma Protokolü (SIP) gibi gecikmeye bağlı uygulamaları kullanan Cisco çalışanları, uygulamada gecikmeler yaşadı. “Cisco yönlendiricileri çok güvenilir ve çevremizde çok nadiren başarısız olmak zorunda kaldı”. Talukdar, “Cisco BT'nin iş sürekliliğini sağlamaya yardımcı olmak için yapabileceği her şeyi yapıyoruz.

**ÇÖZÜM**

Cisco IT, dünya çapındaki altı küçük POP'da durumsal bağlantı içeren bir güvenlik duvarı çözümü dağıtmaya karar verdi. Bu bölgelerdeki nispeten küçük kullanıcı popülasyonları için en büyük POP, 1600 çalışana hizmet verdi - Cisco, Cisco PIX 535 Güvenlik Uygulamasını seçti. Bu güvenlik cihazı, derin paket incelemesi gerçekleştirirken ve tüm ağ iletişimlerinin durumunu takip ederken yönetici tarafından tanımlanmış erişim kontrolü politikalarını uygulayarak güçlü ağ ve uygulama güvenliği sağlar. Talukdar, “Cisco PIX 535 Güvenlik Cihazı, yüksek hacimli Cisco ortamında önemli olan 280.000 eşzamanlı oturumu yönetme yeteneği ile 360 ​​Mbps'den fazla güvenlik duvarı verimi sağlıyor” diyor. Entegre donanım VPN hızlandırma özellikleri, güvenlik duvarı işlemcisinden hesaplama yoğun şifrelemeyi boşaltarak en yoğun trafik zamanlarında bile yüksek performans sağlar. Güvenlik duvarı çözümü, 70 Mbps'ye kadar Üçlü Veri Şifreleme Standardı (3DES) VPN ve 2000 IP Güvenliği (IPSec) tüneli desteği sağlayarak, on binlerce Cisco çalışanı, mobil çalışanı ve telefona bağlanan ortaklar için gereken ölçeklenebilirliği sağlar. VPN tarafından Cisco intraneti. Cisco PIX güvenlik cihazları, Cisco'nun Ağ Tabanlı Uygulama Tanıma (NBAR) gibi Cisco için uzmanlaşmış denetim motorlarını kullanarak, 4. ve 7. katlardaki paket akışlarını inceleyen akıllı, uygulamaya duyarlı güvenlik hizmetleri biçiminde ek bir güvenlik katmanı sağlar. popüler uygulamalarında solucanlar ve virüslerin yayılmasını engellemek için kullanır.

Yeni durum denetlemesi güvenlik duvarı ile Cisco IT, yalnızca benzersiz gelen ve giden akışlar için bir ACL'yi yapılandırmaya ihtiyaç duyar. Cisco PIX işletim sisteminin bir parçası olan Uyarlamalı Güvenlik Algoritması (ASA), kaynak ve hedef adreslerine, rastgele TCP sıra numaralarına, port numaralarına ve ek TCP bayraklarına dayalı bir oturum akışı için bağlantı tablosu girişi oluşturur. Talukdar, “Bir akış bir yönde geldiğinde, güvenlik duvarı hatırlar ve geri gelmesini bekler” diyor Talukdar, Cisco PIX Security Appliance, tüm gelen ve giden trafiği bu güvenlik tablosu girişlerini bu bağlantı tablosu girişlerine uygulayarak kontrol ediyor.

**Geçiş Süreci**

Cisco'yu Cisco IOS® Yazılımındaki kararsız güvenlik duvarından Cisco PIX Güvenlik Cihazına geçirmek için, Cisco IT aşağıdaki adımları izler:

* Mimariyi San Jose merkezindeki laboratuarda, geçiş yapılacak siteyle aynı yönlendirici, çekirdek ve omurgayı kullanarak inşa edin.
* Cisco PIX güvenlik cihazlarını ACL ve kurallarla yapılandırın. Aşağıdakiler bir Cisco sitesi konfigürasyonundan alıntılardır. Kural setinin tamamı 1000 ila 2000 satır içerir. (Örnek IP adreslerinin burada kullanıldığını unutmayın.)
* Yapılandırmayı test edin. Talukdar, “Bu aşamada yapılandırma konularını keşfediyoruz” diyor. Yapılandırma sorunları Cisco Technical Assistance Center mühendislerinin yardımıyla çözüldü.
* Uygulamayı test edin. Cisco IT, konfigürasyonu sitenin halen kullandığı çözüme paralel olarak test eder - tipik olarak bir Cisco 7200 Serisi Router. Test cihazları, iki Cisco PIX güvenlik duvarını bağlamak ve uygun bağlantı ve yerine çalışmalarını onaylamak için çekirdek anahtarındaki boş bağlantı noktasını kullanır.
* Mevcut altyapıya paralel olarak Cisco PIX güvenlik duvarlarını üretime yerleştirin. Bu aşama genellikle yaklaşık iki hafta sürer veya Cisco IT uygulamasının dağıtımın istikrarlı olduğunu doğrulayana kadar.
* Zamanlanmış bir bakım penceresi sırasında Cisco PIX Güvenlik Cihazı sistemine geçiş yapın.
* Doğru çalışmayı onaylamak için altyapıyı bir hafta boyunca izleyin. Talukdar, “Güvenlik duvarlarının çok sayıda kuralı olduğu için bir veya ikisini özlemek kolaydır” diyor.
* Cisco IT’nin göç ettiği ilk siteler için, konsept kanıtı (1. ve 4. adımlar) 2 hafta sürdü, farklı ülkelerdeki nakliye ekipmanlarıyla ilgili sorunlar nedeniyle ekipman teslimatı 2 hafta sürdü ve gerçek geçiş toplam 6 hafta boyunca 2 hafta sürdü. haftalar.

**Yapılandırma**

Cisco PIX Güvenlik Cihazı, çeşitli yöntemler kullanılarak yapılandırılabilir: Cisco PIX Aygıt Yöneticisi olarak adlandırılan entegre, Web tabanlı bir yönetim arayüzü; merkezi, politika temelli yönetim araçları; ve Telnet, Secure Shell (SSH) Protokolü veya bant dışı bir konsol portu kullanılarak erişilen bir komut satırı arayüzü (CLI). Kes ve yapıştır işlemi sırasında istemeden 10.000 satırlık bir yapılandırma dosyasından bir veya iki satırını bırakmaktan kaçınmak için Cisco, tüm kuralları bir dosyaya girer, kaydeder ve yapılandırmayı yükler. “Kuralları sadece bir kez yarattık; O zamandan beri, konfigürasyonu yeni bir site için güvenlik duvarlarına yüklemek sadece birkaç saniye sürüyor ”diyor.

Cisco PIX Güvenlik Cihazı, Yönlendirme Bilgi Protokolü'nü (RIP) anlar ve şirketler bu protokolü kullanıyorsa rotaları dinamik olarak öğrenir. Ancak Cisco, Geliştirilmiş İç Ağ Geçidi Yönlendirme Protokolü'nü (EIGRP) kullanır. Bu nedenle, Cisco PIX 535 üzerinden trafiği yönlendirmek için Cisco, 5 ila 10 statik yol yapılandırdı. Cisco BT ağ mühendisi Jawahar Sivasankaran, “Statik yollar tasarımı basit tutar ve EIGRP yönlendirme alanına yeniden dağıtılmasını önler” diyor.

**SONUÇLAR**

**Yapılandırma süresi yarıya indirildi**

Cisco IT, durumsal denetimli bir güvenlik duvarına geçiş için birincil bir teşvik olan güvenlik duvarı yapılandırmalarını oluşturma ve değiştirme süresini azaltma hedeflerine ulaşmıştır. Talukdar “Cisco PIX Security Appliance, denetimli inceleme özelliğiyle, gelen ve giden trafik için ACL'deki giriş sayısını azaltarak BT yükünü en aza indiriyor” diyor Talukdar “Cisco PIX güvenliği nedeniyle önceki yükü yarı yarıya düşürdük. Cihazlar hem gelen hem de giden ACL'ler ve kurallar için dönüş trafiğine otomatik olarak izin verir. "

Cisco PIX Güvenlik Cihazı ayrıca, Cisco güvenlik duvarları olarak gereksiz Cisco 7500 Series yönlendiricileri kullandığında, ikincil yönlendiriciyi ayrı olarak yapılandırma gereksinimini de ortadan kaldırır. Yedeklemeli iki Cisco PIX güvenlik duvarından yalnızca birinin yapılandırılması gerekir: Birincil güvenlik duvarı yapılandırması, yük devretme kablosu üzerinden otomatik olarak ikincil olarak kaydedilir. Talukdar, “Yapılandırmanın otomatik olarak kopyalanması, hata olasılığını azaltır ve idari ek masraflardan tasarruf sağlar” diyor.

**Yükseltilmiş güvenlik**

Cisco PIX Güvenlik Cihazı, Cisco ağının güvenliğini çeşitli şekillerde arttırır. TCP, UDP veya Internet İleti Kontrol Protokolü (ICMP) akışının durumunu hatırladığından, ağdan gelen bir davetsiz misafirin başka bir akış eklemesini önler. Srinivasan, “Sağlam Adaptif Güvenlik Algoritmasının yanı sıra, TCP Intercept, TCP SYN çerezleri, DNS Guard, Flood Defender gibi yerleşik izinsiz giriş koruma özelliklerini kullanarak hizmet reddi ve hatalı paket saldırılarına karşı savunmaya yardımcı oluyor. Taşkın Koruma, Posta Koruma ve Tek Noktaya Yayın Ters Yol İletme. Ayrıca 59 farklı saldırı imzası arar. Bu saldırıları engelleyebilir ve yöneticilere gerçek zamanlı olarak onlar hakkında bilgi verebiliriz. "

**Yüksek kullanılabilirlik**

Birincil Cisco PIX Güvenlik Cihazı herhangi bir nedenle başarısız olursa, ikincil cihaz hiçbir paketin kaybolmaması için kontrolü ele alır. Cisco kullanıcıları uygulama hatalarını görmezler ve çalışmaları kesintisiz kalır.

Cisco PIX Security Appliance'ın kullanılabilirliği sağlamasının bir başka yolu Port Adres Çevirisi (PAT) işlevini özel bir ağ geçidinden daha verimli bir şekilde gerçekleştirmektir. Talukdar, “PAT için Cisco PIX Güvenlik Cihazını kullanmaya başladığımızdan beri, bellek veya kaynak sorunlarıyla ilgili tek bir kesinti yaşamadık” diyor.

**Azaltılmış Raf Alanı Gereksinimleri**

Cisco, daha yeni uygulamalarda Cisco 7200 Serisi yönlendiricileri daha küçük Cisco PIX 525 Güvenlik Cihazı ile değiştirerek veri merkezi raf alanı gereksinimlerini azaltmıştır. “Cisco PIX 525 Güvenlik Cihazı, önceki yönlendirici için üç raf ünitesine kıyasla iki raf ünitesidir” diyor Talukdar. “Raf alanının birinci sınıf olduğu veri merkezimizde bu önemli.” Diyor.

**DERSLER ÖĞRENİLDİ**

Tel Aviv’deki dağıtım sırasında Cisco ekibi şunları kaydetti:

Message Digest Algorithm 5 (MD5) kimlik doğrulamasını kullanarak Cisco PIX güvenlik cihazı aracılığıyla iki yönlendirici arasında Sınır Ağ Geçidi Protokolü (BGP) komşularının yapılandırılması gerekiyorsa, güvenlik duvarı MD5 kimlik doğrulama paketleri için sıra numaralarını rasgele olarak belirler. Bu nedenle, komşuların şifreleri uyuşmuyor.

Talukdar, “Kaynak IP adresi için statik Ağ Adresi Çevirisi (NAT) etkinleştirerek ve Cisco PIX güvenlik duvarı için statik NAT komutunda norandomseq anahtar sözcüğünü kullanarak bir geçici çözüm oluşturduk,” diyor Talukdar. global NAT içinde komut içinde değiştiriliyor. " Cisco PIX Security Appliance, iç ağda 172.16.0.0 IP adresine sahip, yönlendirici A ile güvenlik duvarı dışında bir IP adresine sahip olan yönlendirici B arasında dağıtılmışsa, şu çözüm uygulanır:

nat (inside) 0 erişim listesi olmayan

statik (içeride, dışarıda) 172.16.0.0 172.16.0.0 ağ maskesi 255.255.255.255 0 0 norandomseq

erişim-list nonat inkar ip ana 172.16.0.0 herhangi

erişim-list nonat herhangi bir ip izin

**SONRAKİ ADIMLAR**

Uzun vadeli planlar arasında Cisco PIX güvenlik cihazlarının diğer Cisco lokasyonlarındaki benzerlerine teslim edilmemesine izin veriliyor. “İnternet bağlantısı kesilirse, Cisco PIX güvenlik duvarı hala farkında değil” diyor Talukdar. “Bu nedenle, İnternet için tasarlanan paketler İnternet ağ geçidine kadar uzanıyor, yalnızca bırakılmak üzere. Bir konum yalnızca bir ISS bağlantısına sahipse, şu anda alternatif yok. " KOK'lar arasında fazladan bir rota sağlamak için Cisco IT, ISP ağ geçitlerinin şartlı rotaların reklamını yapmak için kullanabileceği farklı gelişmiş BGP özelliklerine bakıyor.

Talukdar, “Cisco PIX Güvenlik Uygulaması, küçük POP ortamında iş sürekliliği ve basitleştirilmiş yönetim hedeflerimizi gerçekleştirmemize yardımcı oldu” diyor. “FWSM [firewall services module] ile aynı avantajları en büyük sitelerimize de genişleteceğiz. "

**Deploying Host-Based Firewalls across the Enterprise: A Case Study**

**İşletme Genelinde Ana Bilgisayar Tabanlı Güvenlik Duvarlarını Dağıtma: Bir Durum Çalışması**

Toplantı sahipleri çeşitli tehditlere maruz kaldıklarından, kuruluşların kuruluş genelinde ana bilgisayar tabanlı güvenlik duvarları dağıtma gereksinimi artmaktadır. Bu bölüm, bir ana bilgisayar tabanlı güvenlik duvarının ideal özelliklerini - tipik olarak gerekmeyen veya tamamen bulunmayan özellikler - içermektedir.  kişiye özel   owned Özel bir PC'de duvar yazılımı uygulaması. Buna ek olarak, yazar bir kuruluş genelinde acenta tabanlı, ana bilgisayar tabanlı duvarları dağıtma konusundaki deneyimlerini ve bunlardan edinilen dersleri açıklar. Yazar, sunucu tabanlı güvenlik duvarlarının değerli bir ek güvenlik katmanı sağladığı sonucuna varmıştır.

**SEMANTİK BİR GİRİŞ**

 Kişisel duvarlar genellikle “her zaman açık” genişbant İnternet bağlantılarına bağlı ev bilgisayarları ile ilişkilendirilir (ve bunun için tasarlandı). Gerçekten, terim  kişisel güvenlik duvarı   kendisi, ürünün tarihinin bir parçası: aslında  kuruluş   fi rewalls,  kişiye özel  ﬁ duvarlar başlangıçta ev bilgisayarlarını korumanın bir yolu olarak görülüyordu.

1. Zamanla, kişisel duvarların başka kullanımları olduğu da kabul edildi. Güvenlik topluluğu, İnternet üzerinden kurumsal LAN'a bağlanan dizüstü bilgisayarları korumak ve kişisel olarak kurumsal LAN'da bulunan dizüstü bilgisayarları korumak için kişisel duvarları kullanmaktan bahsetmeye başladı.

Bu eğilim ile tutarlı olarak - ve derinlemesine savunma ilkesine uygun olarak - kişisel duvarların potansiyel kullanımının bir kez daha genişletilmesi için zaman geldiği söylenebilir. Kişisel duvarlar gerçekten şu şekilde görülmeli

 host tabanlı  fi rewalls. Ana bilgisayar tabanlı ve ağ tabanlı ağ duvarları arasında ayrım yapıldığında, ana bilgisayar tabanlı ağ duvarının ek kullanımı belirginleşir. Tıpkı kuruluşların ana bilgisayar tabanlı konuşlandırması gibi  Saldırı Tespit Sistemleri (IDS) kritik sunucular için ek bir algılama özelliği sağlamak için, kuruluşların ana bilgisayar tabanlı konuşlandırmayı düşünmeleri gerekir. fi rewalls  kritik sunucular için ek bir erişim kontrolü katmanı sağlamak (örneğin, değişim sunucuları, etki alanı denetleyicileri, baskı sunucuları vb.). Nitekim, çoğu ana bilgisayar tabanlı ağ topluluğunun yerleşik bir IDS özelliğine sahip olması nedeniyle, en azından bazı küçük kuruluşlar için ana bilgisayar tabanlı ağ duvarlarının bile değiştirmek  uzman ana bilgisayar tabanlı IDS yazılımı.

Bir duvarın diğerinin arkasına yerleştirilmesi fikri yeni değildir. Yıllar boyunca, güvenlik uzmanları özellikle hassas arka sistemleri korumak için iç duvarlar denilen hakkında konuşmuşlardır.

 2)Ancak, genel olarak ağ tabanlı güvenlik duvarları gibi dahili güvenlik duvarları hala özel aygıtlardır. (Bu, hem Cisco’nun PIX gibi güvenlik duvarı cihazları ve hem de Symantec’in Raptor'u gibi yazılım tabanlı “geri dönüş duvarları” için geçerlidir.) Buna karşılık, ana bilgisayar tabanlı “geri dönüşler” fazladan ekipman gerektirmez. Ana bilgisayar tabanlı bir güvenlik duvarı, önceden var olan bir sunucuda veya istemci makinede çalışan bir güvenlik duvarı yazılımıdır. Bir ana bilgisayar tabanlı güvenlik duvarının bir sunucuda veya istemci makinede çalıştığı göz önüne alındığında (vE Sadece bu makine), ana bilgisayar tabanlı duvarlar, tek bir makineyi korumaya adanmış iç duvarlar dahil olmak üzere, ağ tabanlı duvarlardan daha fazla işlevsellik sunar. Hem ağ hem de ana bilgisayar tabanlı ﬁ geri dönüş duvarları, gelen ve giden ağ bağlantılarını ability ltre etme yeteneğine sahipken, yalnızca ana bilgisayar tabanlı ﬁ geri alma duvarları ek  belirli programlara bağlı ağ bağlantılarını engelleme ve posta eklerinin yürütülmesini önleme yetenekleri.

Bunu doğru bir perspektife sokmak için, Microsoft’un dahili ağına yapılan Kasım 2000 saldırısında kullanılan istismar olduğundan şüphelenilen ağ kurdu ve Truva atı programı QAZ’yı düşünün. QAZ, NOTEPAD.EXE programını kaçırarak çalışır. Son kullanıcının bakış açısından, Notepad hala normal çalışıyor gibi görünüyor; ancak Notepad başlatıldığında, QAZ, Çin'deki bir adrese (virüslü makinenin IP adresini içeren) bir e-posta iletisi gönderir.

3)  Bu arada, arka planda, Truva atı, davetsiz misafirin herhangi bir uygulamayı yükleyip yürütebileceği, 7597 numaralı TCP bağlantı noktasında bir bağlantı için sabırla bekler.

4 ) QAZ'ın bunun yerine TCP bağlantı noktası 80 üzerinden çalışacak şekilde değiştirildiğini varsayalım.

5) Tüm duvarlar TCP bağlantı noktası 80'deki giden bağlantıları engelleyebilse de, böyle bir yapılandırmanın uygulanması meşru trafiğe müdahale edecektir. Yalnızca ana bilgisayar tabanlı bir güvenlik duvarı, NOTEPAD.EXE ile ilişkili TCP bağlantı noktası 80 üzerindeki bir bağlantıyı engelleyebilir ve olayı kullanıcıya bildirir. Steve Riley'in dediği gibi, “Kişisel ödevler       giden bağlantıları izlemenin bir uyarı vereceğini; 'Not Defteri, İnternet’e bağlanmaya çalışıyor' bildirimini içeren bir iletişim kutusu görerek, kimsenin şüphelerini uyandırmalıdır. ”

6)STAND-ALONE VERSUS FİRMASINA AİT YANGIN DUVARLARI

 Ana bilgisayar tabanlı geri duvarlar iki kategoriye ayrılabilir: tek başına ve aracı tabanlı.

 7)Tek başına ﬁ duvarlar, konfigürasyonlarının yönetildiği (ve günlükleri) makinenin kendisinde saklandığı için diğer ağ cihazlarından bağımsızdır. Tek başına ew geri dönüş duvarlarına örnek olarak ZoneAlarm, Sygate Personal Firewall Pro, Network Associates’in PGP Masaüstü Güvenliği, McAfee Personal Firewall,

  8)Norton Internet Security 2000 ve Symantec Desktop Firewall. Buna karşılık, ajan bazlı duvarlar yerel olarak yapılandırılmamakta veya izlenmemektedir. Temsilci tabanlı güvenlik duvarları, merkezi bir işletme sunucusundan yapılandırılır (ve kayıtları kopyalanır). Temsilci tabanlı ew geri dönüş duvarlarına örnek olarak ISS RealSecure Desktop Protector (daha önce Network ICE’nin Black ICE Defender'ı) ve InfoExpress’in CyberArmor Kişisel Güvenlik Duvarı verilebilir. Ana bilgisayarlarımıza ajan tabanlı güvenlik duvarı yazılımı uygulamayı seçtik. Tek başına geri duvarlar genellikle bir kurumsal çözüm olarak dağıtılırken, aracı tabanlı yeteneklerin kurum genelinde tutarlı bir erişim kontrol listesi (ACL) merkezi olarak yönetmesini ve uygulanmasını istedik. Ve en iyi uygulama, ağ tabanlı güvenlik duvarlarının günlüklerinin düzenli olarak gözden geçirilmesini gerektirdiğinden, kurum genelinde ana bilgisayar güvenlik duvarlarından gelen günlükleri düzenli inceleme ve analiz için tek bir kaynaktan toplayabilmeyi istedik.

**ÜRÜN SEÇİM KRİTERLERİMİZ**

 Bir ajan tabanlı güvenlik duvarı modelini benimsediğimizde, bir sonraki adım bir ürün seçmek oldu. Yine, bu bölümün yazıldığı tarih itibariyle seçeneklerimiz RealSecure Desktop Protector veya CyberArmor idi. Bir ürün seçmek için aşağıdaki kriterleri kullandık:

9) Atakları engellemede etkinlik.

  Ana bilgisayar tabanlı güvenlik duvarı, kötü amaçlı gelen trafiği engellemelidir. Ayrıca, en azından giden bağlantıları etkin bir şekilde filtreleme yeteneğine de sahip olmalıdır. Steve Gibson'ın dediği gibi, “İnternet bağlantılarımız sadece engellemekle kalmaz

 dış saldırı,ayrıca, güvenli bir şekilde yönetilmelerini sağlamalıdırla iç ekstrüzyon”

10)Dahili ekstrüzyon yoluyla, Gibson, Truva atları, virüsler ve casus yazılımlar tarafından başlatılan giden bağlantılardan bahsediyor. Giden bağlantıları etkin bir şekilde filtrelemek için, ana bilgisayar tabanlı güvenlik duvarının şifreleme toplamlarını kullanması gerekir. Ana bilgisayar tabanlı güvenlik duvarı ilk önce her yetkili uygulama için şifreleme toplamları oluşturmalı ve daha sonra herhangi bir programdan önce (adın ne olursa olsun) erişime izin verilsin, bu toplamı veritabanında depolanan ile yeniden oluşturmalı ve karşılaştırmalıdır. Eğer uygulama  tüm yetkili uygulamalar için şifreleme toplamları veritabanını tutmaz (ve bunun yerine sadece adları veya dosya yollarını kontrol eder), ana bilgisayar tabanlı güvenlik duvarı bir kuruluşa yanlış bir güvenlik hissi verebilir.

**Merkezi konfigürasyon.**

  Sadece ana bilgisayar tabanlı güvenlik duvarının yapılandırmasını merkezi olarak belirleme yeteneğine değil, aynı zamanda

 zorlamak

  bu yapılandırma. Başka bir deyişle, son kullanıcıların hangi uygulamalara veya trafiğe izin verileceği konusunda güvenlik kararları almalarını önleme seçeneğindeyiz.

Son kullanıcılara şeffaflık.

  Son kullanıcılar herhangi bir yapılandırma kararı vermeyeceğinden, ürünün kendilerine mümkün olduğunca şeffaf olmasını istedik. Örneğin, kullanıcıların doğru politikayı uygulamak için dizüstü bilgisayarlarının nasıl bağlandığını (örneğin, kurumsal LAN, ev İnternet bağlantısı, VPN, extranet vb.) “Duvarına” söylemelerini istemedik. Bir saldırı olmadığında, duvarın arka planda sessizce performansı düşürmeden sessizce çalışmasını istedik. (Elbette, bir saldırı durumunda, kullanıcının bir uyarı almasını isteriz.)

Çoklu platform desteği.

  Sadece kişisel duvarlarla ilgileniyor olsaydık, bu endişe olmazdı. (Linux dizüstü bilgisayarlar kişisel güvenlik duvarı korumasına ihtiyaç duyabilir olsa da, ortamımızda bu tür makinelere sahip değiliz.) Ancak, sunucularımızda olduğu gibi istemci bilgisayarlarımızda da sunucu tabanlı ana duvarları uygulamakla ilgilendiğimiz için birden fazla işletim sistemi desteği bir gereksinim.

Uygulama desteği.

  Güvenlik duvarı tüm yetkili uygulamalarla ve bu uygulamalar tarafından kullanılan protokollerle uyumlu olmalıdır.

VPN desteği.

 Ana bilgisayar tabanlı güvenlik duvarı VPN uygulamamızı ve istemci yazılımımızı desteklemelidir. Ayrıca, VPN bağlantılarını algılayabilmeli ve şeffaf bir şekilde adapte edebilmelidir.

Güvenlik duvarı mimarisi.

  Paket filtreleme, uygulama düzeyinde proxy ve durum denetimi dahil olmak üzere, ana bilgisayar tabanlı geri dönüş duvarları için birçok seçenek vardır.

IDS teknolojisi.

  Aynı şekilde, her biri kendi güçlü ve zayıf yönleri olan IDS teknolojisine birkaç farklı yaklaşım vardır. Ana bilgisayar tabanlı bir güvenlik duvarı tarafından tespit edilebilecek saldırıların sayısı burada açıkça geçerli olacaktır.

Kullanım ve montaj kolaylığı.

  Girişimci bir çözüm olarak, ürün uzaktan dağıtım ve kurulumu desteklemelidir. Ek olarak, merkezi yönetim sunucusunun (göreceli) kullanımı ve yapılandırılması kolay olmalıdır.

Teknik Destek.

  Kalite ve bulunabilirlik bizim için önemli olanlardır.

Ölçeklenebilirlik.

  Küçük bir şirket olsak da, büyümeyi bekliyoruz. Çok sayıda ajanı destekleyebilecek sağlam bir ürüne ihtiyacımız var.

Disk alanı.

  Son kullanıcı makinelerinde gereken disk alanı miktarının yanı sıra merkezi politika ve günlük sunucusu konusunda endişeliydik. Örneğin, ﬁ rewall kaç kez sayıyor?

Her saldırı için tek bir olayı günlüğe kaydetmek yerine bir saldırı mı gerçekleşiyor?

Birden fazla politika grubu.

 Her biri farklı ihtiyaçlara sahip farklı son kullanıcı gruplarımız olduğundan, farklı gruplar üzerinde farklı politikalar uygulama esnekliğini istedik. Örneğin, çalışanlarımızın geri kalanı için böyle bir trafiği reddederken, SQLNet trafiğini geliştirme masaüstlerimizden izin vermek isteyebiliriz.

Raporlama.

  Benzer kurumsal çözümlerde olduğu gibi, ideal bir raporlama özelliği de, belirli bir süre zarfında en fazla davetsiz misafirlere yönelik dahili raporları, hedefleri ve saldırı yöntemlerini (örneğin, aylık, haftalık vb.) İçerecektir.

Maliyet.

  Göreceli olarak küçük bir kuruluş olarak, özellikle yüksek kaliteli bir işletme çözümü seçmenin maliyeti konusunda endişeliydik.

TEST METODOLOJİMİZ

 Sonunda, küçük ve temsili bir kullanıcı örneği ile her üründe pilot bir çalışma yaparak hem CyberArmor hem de RealSecure Desktop Protector'ı kurmayı ve değerlendirmeyi planlıyoruz. (Bu bölüm yazıldığı sırada, CyberArmor'un değerlendirmesine ve ISS Real Secure'ın pilot çalışmasına başlamak üzereyiz.) Her iki ürünü de ölçütlerimizin çoğuna göre değerlendirme yöntemi açıkken, bir kriteri test etmek detaylı bir açıklamayı hak ediyor: saldırıların engellenmesinde etkinlik. Her ürünün yetkisiz bağlantıları engellemedeki etkinliğini birkaç yolla test ettik:

 HackYourself.com'dan Uzaktan Hızlı Tarama.

 Bir çevirmeli bağlantıdan, basit ve uzak bir TCP ve UDP bağlantı noktası taramasını tek bir IP adresine karşı yürütmek için HackYourself.com’un Hızlı Taramasını kullandık. •

 Nmap taraması.

 İki farklı tarama yapmak için nmap kullandık. Öncelikle, güvenlik duvarının durum denetlemesi veya basit bir paket filtresi yapıp yapmadığını belirlemek için bir ACK taraması yaptık. İkinci olarak, ana bilgisayar tabanlı güvenlik duvarının hedef makinelere baskı yapma girişimlerini etkili bir şekilde engelleyip engellemediğini belirlemek için nmap işletim sistemi “ngerprinting” özelliğini kullandık.

Güvenlik duvarı, güvenilen uygulamanın, kötü amaçlı DLL'nin etkisine bağlı olarak uzaktaki bir makineye küçük bir metin mesajı göndermesini sağlar. Mesaj şu anda oturum açmış olan kullanıcının adını, bilgisayarın adını ve güvenlik duvarı ve mesajın gönderildiği saatte zafer kazandığını iddia eden bir mesaj içeriyor.

YAPILANDIRMA

 Ana bilgisayar tabanlı güvenlik duvarlarını dağıtma nedenlerimizden biri, Truva atlarına, casus yazılımlara ve giden ağ bağlantılarını başlatan diğer programlara karşı ek bir koruma katmanı sağlamaktı. Ana bilgisayar tabanlı ağ duvarları ağ bağlantısı göndermeyen veya almayan Truva atlarına müdahale etmek için tasarlanmamış olsa da, doğru şekilde yapılandırıldığında, yetkisiz uygulamalardan ağ trafiğini engellemede oldukça etkili olabilirler. Aslında, bir anlamda, ana bilgisayar tabanlı güvenlik duvarları virüsten koruma yazılımlarına göre bir avantaja sahiptir. Anti-virüs yazılımı yalnızca bilinen bir eşleşerek eşleşen Truva atlarını tespit edebilir.

 imza

 , ana bilgisayar tabanlı ﬁ ödüllendirmeler ağlarına bağlı olarak Truva atlarını tespit edebilir

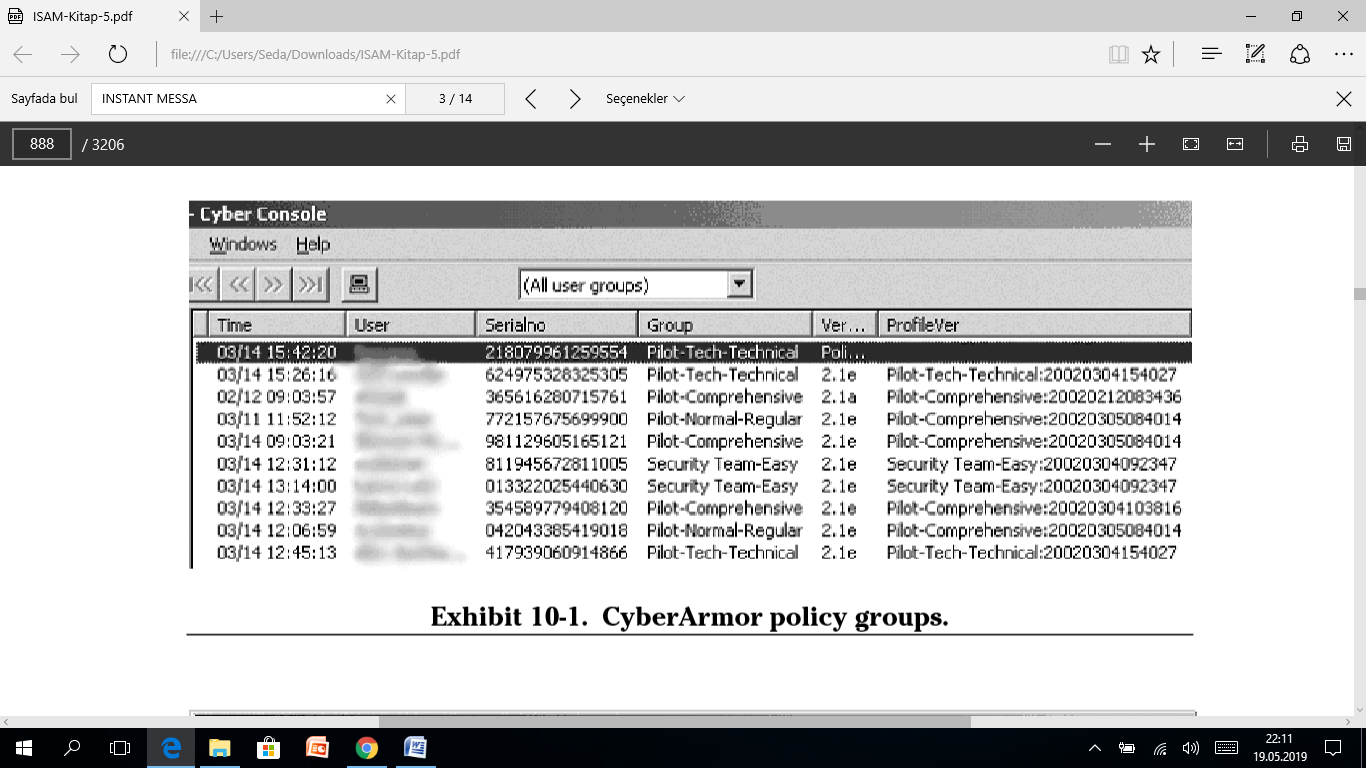
 davranış

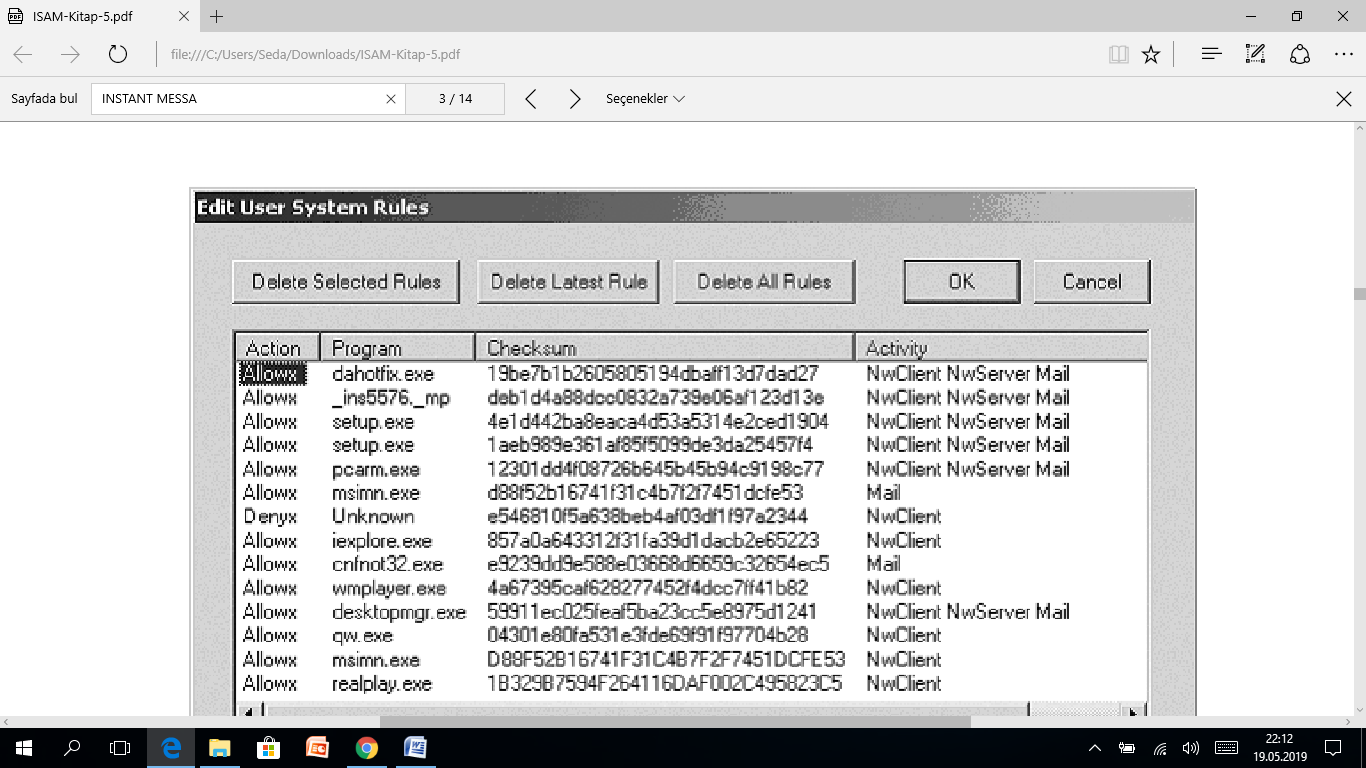
 . Ana bilgisayar tabanlı geri duvarlar, bağlantıyı TCP 80 gibi iyi bilinen bir bağlantı noktasında olsa bile veya bağlantıya neden olan uygulama meşru görünse bile (NOTEPAD), giden bağlantı başlatmaya çalışan herhangi bir yetkisiz uygulamayı tespit edebilir, engelleyebilir ve hatta sonlandırabilir. EXE). Bununla birlikte, Truva atlarını engellemek için ana bilgisayar tabanlı bir duvarı yapılandırmak için iyi bilinen iki uyarı vardır. Öncelikle, güvenlik duvarı yeni uygulamalar tarafından başlatılan tüm bağlantıları engellemelidir.

 varsayılan olarak

 . İkincisi, güvenlik duvarı, yeni bir uygulamanın giden trafiği başlatmasına izin verip vermemesi gerektiğinden, herhangi bir nedenle, güvenlik duvarı tarafından istendiğinde “evet” e tıklayan son kullanıcılar tarafından engellenmemelidir. Birlikte ele alındığında, bu iki uyarı, ana bilgisayar tabanlı duvar duvarlarının sahip olma maliyetinin hızla artmasına neden olabilir. Aslında, her iki uyarıyı da zaten uygulamış olan diğer şirketler, belirli bir başvuruyu yetkili kılmak isteyen kullanıcılardan çok sayıda yardım masası çağrısı yaptığını bildirmiştir.

 Standart bir masaüstü imajımız olmadığı ve çok küçük bir yardım masası personelimiz olduğu göz önüne alındığında, pilot kullanıcılarımızı iki farklı politika grubuna ayırmaya karar verdik: pilot teknik teknolojisi ve teknik normal pilot normal (Bkz. Ek 10 1). İlk yapılandırma, kullanıcıların bir uygulamanın giden bağlantı başlatmasına izin verip vermemesine karar vermelerini sağladı. Bu yapılandırma yalnızca BT personelimizin masaüstünde gerçekleştirildi. Kullanıcı, bağlantıda istenen ağ bağlantısına izin verilip verilmeyeceğini seçmelidir. Kullanıcı bu seçimi yaptığında, ana bilgisayar tabanlı güvenlik duvarı bir sağlama toplamı oluşturur ve kullanıcının kararını yansıtan bir kural oluşturur. (CyberArmor'da ayarlanmış bir örnek kural için bkz. Ek 10-2.)



Sergi 10-1. Siber Zırh politika grupları.

Sergi 10-2. Siber Zırh'ta örnek kullanıcı tanımlı kurallar

DERSLER ÖĞRENİLDİ

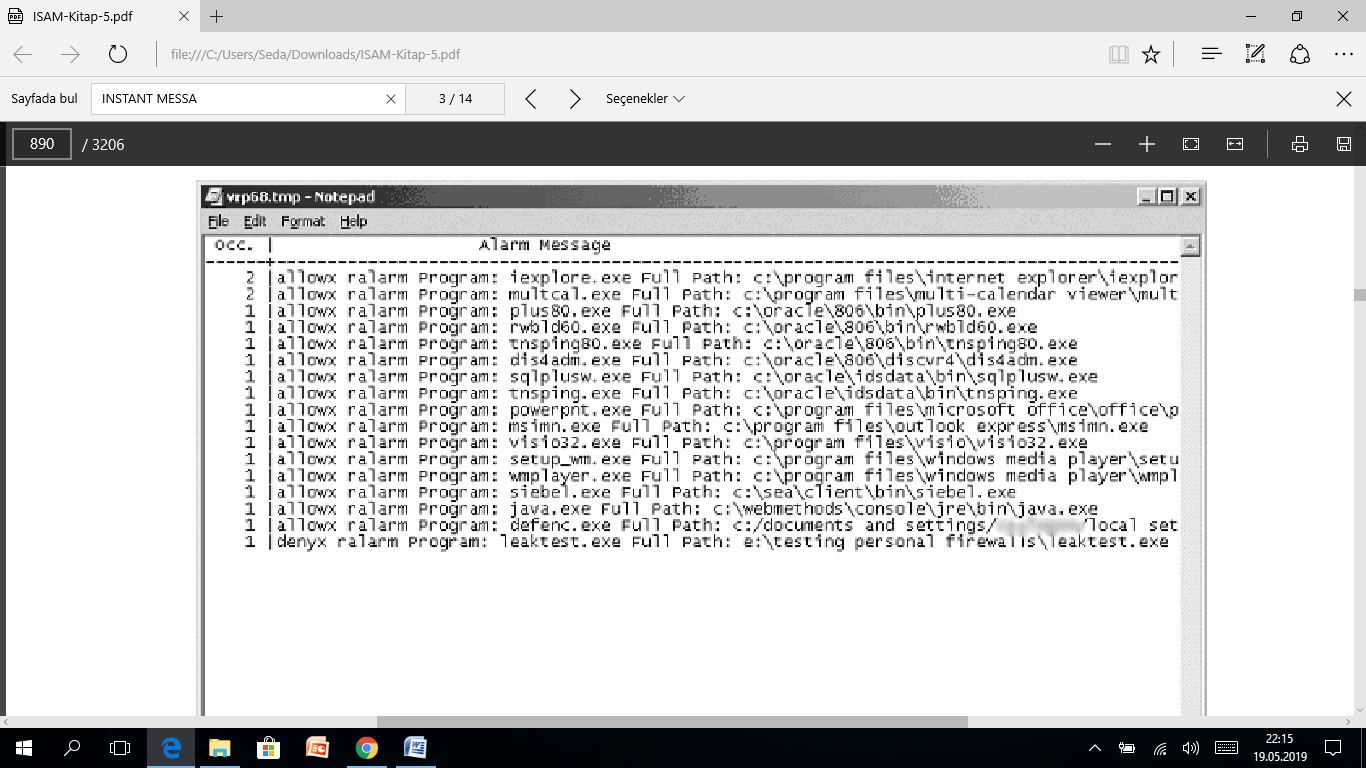
 Her ne kadar bu bölüm bittiyse de, her iki ana bilgisayar tabanlı güvenlik duvarı ürünüyle ilgili pilot çalışmalarımızı henüz tamamlamamış olsak da, zaten

Sergi 10-1. CyberArmor politika grupları.

Sergi 10-2. CyberArmor'da örnek kullanıcı tanımlı kurallar.

Ajan tabanlı, ev sahibi tabanlı şirket duvarları dağıtımı hakkında çeşitli dersler öğrendim. Bu dersler aşağıdaki gibi özetlenebilir. 1. Pilot çalışmamız, standart dışı ve gerçekten de yetkisiz bir ağ yapılandırmasına sahip bir dizüstü bilgisayarı belirledi. Standart bir masaüstü görüntüsünü zorlamayan küçük kuruluşlar için bu sürpriz olmamalıdır. 2. Farklı makinelere farklı politikalar uygulama yeteneği her şeyden önemlidir. Bu, giden ağ bağlantılarını kısıtlamak için ana bilgisayar tabanlı güvenlik duvarı deneyimimizden açıkça görüldü. Kullanıcılarımızı iki gruba ayırabiliriz, yapılandırma kararları almamıza izin verdiklerimiz ve vermeyeceğimiz kararlarla hem esneklik hem de güvenlik elde edebildik. 3. Ağ tabanlı izinsiz giriş tespit sistemlerinde olduğu gibi, deneyimimiz iyi hazırlanmış kural kümelerine duyulan ihtiyacı doğruladı. Yapılandırmamız, gelen NetBIOS trafiğini engelleyen bir kural içermektedir. Hem iç ağımızda hem de dış ağlarda bulunan NetBIOS trafiği miktarı göz önüne alındığında, önemli miktarda uyarı oluşturdu. Bu da, yalnızca uyarlanmış uyarı kurallarına duyulan ihtiyacın altını çizdi.

4. Yazar ağ tabanlı güvenlik duvarları uygularken bulduğu gibi, ana bilgisayar tabanlı güvenlik duvarı kural kümesi oluşturma ve sonra ayarlama süreci zaman alıcıdır. Bu, özellikle giden trafikte kısıtlamalar uygulamaya karar verirse (ve kullanıcıların veya kullanıcıların bir kısmının kendilerine ait karar kararları almalarına izin vermezse), bu durum geçerlidir; bir giden bağlantı başlatmak için. Bu hiçbir şekilde aşılmaz bir sorun olsa da, bu yapılandırmaya ulaşmak için sınırlı bir zaman yatırımı vardı. 5. Güvenlik duvarı yazılımının neden olduğu son kullanıcı makinelerde herhangi bir önemli performans düşüşü gözlemlemedik. Bununla birlikte, bu bölüm yazıldığı sırada, ana bilgisayar tabanlı güvenlik duvarı yazılımını kritik sunucularda dağıtmayı henüz test etmedik. 6. Altıncı gözlemimiz ürün özellikleridir. CyberArmor tarafından sağlanan yerleşik raporlama aracının ilkel olduğunu keşfettik. Grafiksel raporlar için yerleşik bir destek yoktur ve metin raporlamayı kullanarak bilgi bulmak zordur. Örneğin, yerleşik metin raporlama özelliğini kullanarak, bir "alarm" raporu alınabilir. Elektronik tablo biçiminde sunulan bu rapor yalnızca alarm mesajlarını ve olay sayısını listeler. Kaynak IP adresleri, tarih ve saat bilgileri rapora dahil edilmemiştir. Dahası, alarm mesajları biraz şifrelidir. (Örnek CyberArmor Alarm Raporu için bkz. Ek 10-3). CyberArmor, Crystal Reports ile uyumluyken, faydalı raporlar üretmek için Crystal Reports kullanmak, fazladan yazılım ve zaman gerektirir.



Sergi 10-3. Örnek Siber Zırh alarm raporu.

UNIX İÇİN Ana bilgisayar güvenlik duvarları?  Ana bilgisayar tabanlı güvenlik duvarları, kişisel güvenlik duvarı yazılımının tarihçesi ve evrimi göz önüne alındığında, genellikle Windows platformlarıyla ilişkilendirilir. Ancak, teoride ana bilgisayar tabanlı systems duvarların UNIX sistemlerinde de uygulanamamalarının (ya da kullanılmamasının) bir nedeni yoktur. Emin olmak için, bazı UNIX paket filtreleri ipchains, iptables ve ipfw dahil olmak üzere zaten var.  16   UNIX platformlarının ticari ana bilgisayar tabanlı güvenlik duvarı ürünlerine yaygın bir şekilde entegre edilmediği göz önüne alındığında, bu yardımcı programlar girişimci bir ana bilgisayar tabanlı güvenlik duvarı dağıtımında çok yararlı olabilir. Ancak, bu tür araçlar genellikle kayda değer iki sınırlamalar vardır. İlk olarak, kişisel fi rewalls aksine, bu yardımcı programları paket fi lters vardır. Dolayısıyla, giden bir ağ bağlantısını, bağlantıyı oluşturan uygulamaya göre değerlendirme kabiliyetine sahip değillerdir. İkinci olarak, yardımcı madde, esas değildir. Böylece, bir kurumsal çözüm olarak, bu araçlar kolaylıkla ölçeklenebilir olmayabilir. Bu tür araçlarda ajan tabanlı bir mimarinin olmayışı, UNIX sistemlerinde tespit edilen olaylar hakkında merkezi raporlama yapılmasını zorlaştırabilir.

SONUÇLAR

 Ana bilgisayar tabanlı güvenlik duvarları geleneksel olarak kurumsal dizüstü bilgisayarları ve özel mülkiyete sahip bilgisayarları korumanın bir yolu olarak düşünülse de, ana bilgisayar tabanlı güvenlik duvarları ayrıca sunucular için değerli bir ek koruma katmanı sağlayabilir. Benzer şekilde, ana bilgisayar tabanlı ağ duvarları tipik olarak Windows platformlarıyla ilişkilendirilir.

KAYNAKLAR: (REFERENCES)

1. Garip, M. ve Kılıç, B., (2007). İstanbul için sürdürülebilir şehir aydınlatma politikası, IV. Ulusal Aydınlatma Sempozyumu ve Sergisi Bildirileri, 1-6.

2. İşler, T., (2009). Enerji kalitesi ve sürekliliği için OG dağıtım sistemlerinin yönetimi-1, EMO Dergisi, Nisan, 32-34.

3. Bayındır, R., Demirbaş, Ş., Bektaş, A. ve Çolak, I., (2008). Bir endüstriyel işletmede elektrik enerjisinin izlenmesi, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 24(1-2), 154-164.

4. Çalışkan, N.O., (2007). Elektrik dağıtım sisteminin bilgisayarla programlanması ve otomasyon, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi.