**GÜVENLİK DUVARI NEDİR? VE TÜRLERİ:**

**Güvenlik duvarı** veya **ateş duvarı**, ([İngilizce](https://tr.wikipedia.org/wiki/%C4%B0ngilizce): *Firewall*), güvenlik duvarı yazılımı, bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Birçok farklı filtreleme özelliği ile [bilgisayar](https://tr.wikipedia.org/wiki/Bilgisayar) ve ağın gelen ve giden paketler olmak üzere [İnternet](https://tr.wikipedia.org/wiki/%C4%B0nternet) trafiğini kontrol altında tutar. [İP filtreleme](https://tr.wikipedia.org/w/index.php?title=%C4%B0P_filtreleme&action=edit&redlink=1), [port filtreleme](https://tr.wikipedia.org/w/index.php?title=Port_filtreleme&action=edit&redlink=1), [Web](https://tr.wikipedia.org/wiki/Web) filtreleme, içerik filtreleme bunlardan birkaçıdır. [[*kaynak belirtilmeli*](https://tr.wikipedia.org/wiki/Vikipedi:Kaynak_g%C3%B6sterme)]

Birçok kişisel bilgisayar işletim sistemleri, Internet'ten gelen tehditlerine karşı korumak için yazılım tabanlı güvenlik duvarları içerir.Ağlar arasında veri aktaran birçok yönlendirici firewall bileşenleri içerir ve, birçok firewall temel yönlendirme işlevlerini gerçekleştirebilir.

İnternet küresel kullanım ve bağlantı açısından oldukça yeni bir teknoloji iken Firewall teknolojisi 1980'lerin sonunda ortaya çıkmıştır.

**Paket filtrelemeli güvenlik duvarı**

Paket filtreleri, Internet üzerindeki bilgisayarlar arasında transfer edilen paket başlıklarını inceleyerek hareket eder.Bir paket güvenlik duvarından geçtiği sırada eğer başlık bilgisi, güvenlik duvarı üzerinde daha önceden tanımlanmış olan, "güvenlik duvarı paket filtresi" ile eşleşirse, ya paket atılır ya da reddedilerek kaynağa hata mesajları gönderilir.

Bu tür paket filtreleme, paketin mevcut ağ akışının bir parçası olup olmadığına bakmaz.

Paket filtrelemeli güvenlik duvarı [OSI Modeli](https://tr.wikipedia.org/wiki/OSI_modeli)'nin ilk 3 katmanında çalışır. Paket başlığındaki bilgilerin hepsini baz alarak filtreleme işlemi gerçekleştirilebilir.

**Durumlu denetim güvenlik duvarı**

[Veriyi](https://tr.wikipedia.org/wiki/Veri) kaynağından hedefine kadar takip eder. Uygulama tabakası güvenlik duvarı ise yalnızca gelen ve giden verinin başlık kısımlarını kontrol eder ve uygulama katmanındaki protokolleri kısıtlayarak güvenliği sağlar. Örneğin [HTTP](https://tr.wikipedia.org/wiki/HTTP) protokolü üzerinden bir Web sitesinin erişiminin engellenmesi buna örnek olarak verilebilir. Daha gelişmiş olanı durumlu denetim özellikte olanlar olup daha çok büyük [ağların](https://tr.wikipedia.org/wiki/Bilgisayar_a%C4%9F%C4%B1) [İnternet](https://tr.wikipedia.org/wiki/%C4%B0nternet) ve iç ağdaki trafiklerini kontrol eder.

**Uygulama katmanı güvenlik duvarı**

[OSI Modelinde](https://tr.wikipedia.org/wiki/OSI_Modeli) uygulama katmanı düzeyinde çalışır. En sık kullanılan güvenlik duvarı tekniğidir. Uygulama katmanındaki güvenlik duvarı, gelen paketin veri kısmına kadar olan tüm paket başlıklarını açıp kontrol edebilir ve filtreliyebilir.

Uygulama katmanında filtreleme yapmanın en önemli avantajı bazı uygulamalar ve protokollerin anlaşılır olmasıdır (FTP, DNS, HTTP gibi).

Günümüzdeki güvenlik duvarları da sadece port kapamak amaçlı kullanılmıyor. Yeni nesil güvenlik duvarları da U.T.M. (Unified Threat Management) (güvenlik duvarı, [antivirüs](https://tr.wikipedia.org/wiki/Antivir%C3%BCs" \o "Antivirüs), anti[spam](https://tr.wikipedia.org/wiki/Y%C4%B1%C4%9F%C4%B1n_mesaj), IDS/IPS, VPN, [yönlendirici](https://tr.wikipedia.org/wiki/Y%C3%B6nlendirici) (router) gibi özellikleri olan) tümleşik cihazlardır. Her ne kadar bir dönem bilinen ateş duvarı markaları U.T.M. cihazlarının hantal ve başarız olduğunu iddia etse de günümüzde tüm ateş duvarı üreticileri U.T.M. cihazlarını üretmektedir.

Bilinen U.T.M. cihaz markaları Cisco ASA, Fortinet, Labris, Juniper, NetSafe-Unity, Netscreen ve Symantec serisidir. Bu cihazlar üzerinde port protokol bazısında kısıtlama yapabilir. Web filtrelemesi (terör, şiddet, silah gibi kategorilerine göre yasaklama) yapabilir. Dosya indirme gibi işlemleri durdurabilir. İyi kurulmuş bir güvenlik duvarı, bilgisayarı bir [daktiloya](https://tr.wikipedia.org/wiki/Daktilo) çevirebilir

**Comparing Firewall Technologies**

(Güvenlik Duvarı Teknolojilerini Karşılaştırma)

ocak 2001’nin başında yeni bir Web sayfası açıldı. Netscan olarak adlandırıldı, 1 ve yaratıcılar Web sitelerini yayınlamadan önce biraz çalışma yaptılar. Aslında, çalışma oldukça basit ama zaman alıcıydı. Yönlendirilen IPv4 adres alanının tamamına ping attılar; ya da daha kesin olmak gerekirse, bunlar .0 veya .255 ile biten her IP adresi ping. Gönderilen her PING için karşılığında bir PING REPLY bekleniyor. Ve her ağ içinBirden fazla paketle cevap verdiler, cevap sayısını saydılar ve veriyi bir veritabanına koydular. HerşeyGönderilen her paket için birden fazla paketle cevap veren ağların bir yükseltici olduğu kabul edildi.ağ. İnternetin tamamına ping yaptıktan sonra (az çok), Web sitelerinde 1024'ün bir listesini yayınladılarIP adresinden sorumlu olan kişinin e-posta adresi ve onunla ilişkili en kötü ağlarağ. En kötü ağlar, onlara tek bir cevap için en çok cevap veren ağlardır.PING veya en iyi amplifikasyon efekti.

Buradaki güvenlik sorunu, bir sahtekarlığı kullanarak bir ağa PING isteği göndermenin oldukça kolay olmasıdır. Kaynak IP Adresi. Ve alıcı ağ cevap verdiğinde, tüm bu cevaplar ilk PING’de verilen şekilde kaynak adrese gönderilecektir. Exhibit 42,1 gösterildiği gibi, saldırganın sürekli bu işlemi tekrarlayarak nihai alıcının İnternet bağlantısını da boyayabilirsiniz.

Aslında, saldırgan bir T3 (45-Mbit) bağlantısını kesmek için yeterli trafik oluşturmak için bir ISDN bağlantısı kullanabilir,

saldırının başlatılması için birkaç SMURF amplifikatör ağının kullanılması. Ve izin veren ağlar olduğu sürece

Bu tür bir büyütme işlemi, bir şebeke, kendisinin büyütme sorunu olmasa bile, bir saldırının hedefi olabilir ve saldırıyı önlemek için güvenlik duvarları gibi yapılabilecek çok fazla güvenlik sistemi yoktur.

Bu tür bir saldırı, İnternet'teki en büyük sitelerin bazılarına saldırmak için tekrar tekrar kullanıldı.

Şubat 2000’de Yahoo, CNN, Ebay ve Amazon’a yapılan saldırılar da dahil. Bugünlerde, SMURF amplifikatör ağlarını arayan ve sonuçlarını yayınlayan birçok Web sitesi var.

alenen. Mart 2001'de verilen bir sunumda bu yazar gerçeği olduğuna dikkat çeken ağların sayısı

Böyle amplifikatörler Ocak 2001 yılından bu yana 1000'den fazla yüzde artmıştı olarak kullanılmasına karşı korunmasını değil.

Bu saldırıların ilginç bulgularından biri de yönlendiricilerin sorunlardan sorumlu tutulmasıydı.

güvenlik duvarları. Ve haklıydılar; kötü yapılandırılmış İnternet yönlendiricileri, bu sorunların önemli bir parçasıydı.

vakalar. Daha da kötüsü, bu spesifik PING tabanlı saldırının engellenmesi için tek gereksinimin ortaya konmasıydı

ağları İnternete bağlayan tüm yönlendiricilerdeki bir parametre. Bu şimdi, “Yönlendiricilerdeki Yönlendirilmiş Yayın için Varsayılanın Değiştirilmesi” adlı RFC 2644 / BCP 34'te önerilen varsayılan haline gelmiştir. IP Kaynak Adresini Sahtecilik, ”, sahtekarlık saldırılarını daha iyi anlamak için.

Bu saldırıların ardından ilginç bir gözlem, Başkan Clinton’un Ulusal bir ilan etmesiydi.

Bilgi Sistemleri Koruma Planını, Türkiye'deki en iyi güvenlik uzmanlarından bazılarının değerli yardımıyla

Amerika Birleşik Devletleri. Bu yazarın görüşüne göre, bu, kimin başında olması gerekenlerin mükemmel bir örneğidir.

güvenlikten sorumlu - yönetim kurulu ve bir şirketin CEO'su.

Son olarak, CNN, Yahoo ve Amazon gibi Web sitelerinin hepsinde güvenlik duvarları mevcuttu, ancak bunların önüne geçmedi saldırılar. Bu nedenle, güvenlik duvarı teknolojilerinin ve gerçekte ne tür bir güvenlik sağlayabileceklerinin tartışılması sipariş.



Güvenlik Duvarı Teknolojileri Açıklaması

İnternet Güvenlik Duvarları SSS 2

İki temel güvenlik duvarı türünü tanımlar: ağ katmanı güvenlik duvarları ve uygulama katmanı güvenlik duvarları (ayrıca uygulama proxy güvenlik duvarları veya yalnızca proxy'ler olarak da bilinir). Bu bölümde, durumsal inceleme güvenlik duvarları, aralarındaki benzerlik ve farklılıkları daha kolay anlamayı kolaylaştırmak için ilk iki güvenlik duvarı türünün bir karışımı olarak tanımlanmaktadır.

Okuyucu, ağ katmanının katman 3 olan OSI katman modelini zaten biliyor olabilir.

uygulama katmanı, Ek 42.2'de gösterildiği gibi katman 7'dedir. Bir güvenlik duvarı, üzerine bir tür güvenlik filtresi uygulanmış olarak, iki veya daha fazla ağ arasında paketleri ileri geri ileten bir yönlendirici olarak gösterilebilir.

Ağ Düzeyinde Güvenlik Duvarları: Paket Filtreler Paket filtre güvenlik duvarları genellikle erişim listelerine sahip bir yönlendiricidir. En temel haliyle, paket filtre güvenlik duvarı Her IP paketinin kaynak ve hedef IP adresini ve hedef portu temel alarak trafiği kontrol eder. Birçok paket filtre güvenlik duvarı ayrıca gelen arayüze dayanarak paketleri kontrol etmeyi sağlar ( İnternet veya dahili ağ?). Ayrıca, kaynak portu baz alınarak IP paketinin kontrolüne izin verebilirler, ürüne bağlı olarak gün ve saat, protokol türü (TCP, UDP veya ICMP) ve diğer IP seçenekleri de vardır. Paket filtre güvenlik duvarları hakkında hatırlanması gereken ilk şey, her IP paketini tek başına denetlemeleridir; onlar IP paketlerini bir oturumun parçası olarak görmeyin. Paket filtre güvenlik duvarları hakkında hatırlanması gereken ikinci şey, birçoğunun, varsayılan olarak, açık bir yapılandırmaya sahip olmalarıdır; Ve son olarak, paket filtreleri sadece bir paketin başlığını kontrol eder, paketin DATA kısmını kontrol etmez. Bu, bir servisi başka bir servis içinde tünelleme gibi tekniklerin kolayca bir paket filtresini atlayacağı anlamına gelir (örneğin, Telnet'i 80 numaralı port üzerinde standart Telnet portu 23'ün engellendiği bir güvenlik duvarı üzerinden çalıştırmak, ancak HTTP portu 80 açıktır. kaynak / hedef ve port numarasını görür, geçmesine izin verir).



Paket Filtre Güvenlik Duvarlarını Neden Kullanmalı? Bazı güvenlik yöneticileri bunun farkında olmayabilir, ancak büyük olasılıkla zaten içinde çok sayıda cihaz var. paket filtreleme yapabilen bir ağ. En iyi örnekler çeşitli yönlendiricilerdir. Günümüzde çoğu (tümü değilse) yönlendiriciler, yönlendiriciden akan IP trafiğini çeşitli güvenlik dereceleriyle denetleyen erişim listeleriyle donatılabilir. Birçok ağda, sadece paket filtre güvenlik duvarı görevi görmek için onları doğru bir şekilde yapılandırma meselesi olacaktır. Aslında, yazar genellikle tüm yönlendiricilerin en az bir yönlendiricinin kendisinin ve çevresinin güvenliğini en düşük seviyede tutmak için erişim listelerini kullanın. kullanma paket filtreleme genellikle, diğer teknolojilere göre başka bir artı olan verim üzerinde çok az etki eder veya hiç bir etkiye sahip değildir. Son olarak, paket filtre güvenlik duvarları çoğu (tümü değilse) TCP / IP tabanlı hizmetleri destekler.

Neden Paket Filtre Güvenlik Duvarlarını Kullanmıyorsunuz?

Eh, onlar sadece OSI katman 3'te veya ağ katmanında genellikle denildiği gibi çalışırlar. Paket filtre güvenlik duvarları sadece tek IP paketlerini kontrol eder; Paketin bir oturumun parçası olup olmaması umrunda değil. Ayrıca, onlar yok

Temel başlık bilgisi tamamlandığı sürece, paketin gerçek içeriğini kontrol edin.

kaynak ve hedef IP adresi). Paket filtre güvenlik duvarları için kurallar oluşturmak sinir bozucu ve zor olabilir,

ve birçok farklı paket filtre güvenlik duvarı arasında tutarlı kuralları korumak genellikle çok zor olarak kabul edilir. Daha önce belirtildiği gibi, tipik açık-açık varsayılanlar çoğu durumda tehlikeli olarak düşünülmelidir.

Durumsal Denetim Güvenlik Duvarları

Temel olarak, durumsal inceleme güvenlik duvarları, paket filtre güvenlik duvarları ile aynı şeydir, ancak paket filtreleme yeteneklerine ek olarak bağlantıların durumunu takip edebilme özelliğine sahiptir. Bir oturumun başlatılıp başlatılmadığını, şu anda veri iletildiğini (her iki yönde) veya kapatıldığını dinamik olarak takip ederek güvenlik duvarı, veri aktarımına daha güçlü güvenlik uygulayabilir. Ayrıca, durum bilgisi olan denetleme güvenlik duvarlarının HTTP, FTP ve SMTP gibi popüler hizmetleri kullanmanın çeşitli yolları vardır. Bu son seçenekler (bunlardan pek çok çeşidi olan)

üründen ürüne) güvenlik duvarının gerçekten de TCP trafiğine gidiyorsa HTTP trafiği olup olmadığını kontrol etmesini sağlar 80

trafiği “analiz ederek” bir ağdaki bir ana bilgisayarda. Bir paket filtresi yalnızca bunun HTTP trafiği olduğunu varsayar, çünkü

bir ana sistemde 80 numaralı TCP bağlantı noktasına gidiyor; paketin VERİ bölümünü kontrol etmenin hiçbir yolu yoktur, ancak durumsal inceleme bunu kısmen yapabilir.

Durum bilgisi olan bir inceleme güvenlik duvarı;

oturumları. Durum bilgisi olan denetleme güvenlik duvarları genellikle başarısız bir varsayılan konfigürasyona sahiptir, yani bir paketin nasıl işleneceğini bilmiyorlarsa bir paketin geçmesine izin vermeyecekleri anlamına gelir. Buna ek olarak, onlar da sağlayabilir

paket filtreleriyle karşılaştırıldığında paketler ve oturumlar içindeki gerçek içerikleri (verilerin kendisini) “anlayarak” ilave bir güvenlik seviyesi. Bu son bölüm yalnızca üründen ürüne farklı olabilecek belirli hizmetler için geçerlidir.

Neden Durumlu Denetim Güvenlik Duvarları Kullanmalı?

Durumlu inceleme güvenlik duvarları, paket filtrelemeden daha yüksek performans sağlar ve daha fazla güvenlik özelliği sunar. Bu özellikler ortak ve popüler servislerin ekstra kontrolünü sağlayabilir. Durumsal denetleme güvenlik duvarları, çoğu (tümü değilse de) hizmetlerin çoğunu, örneğin paket filtreleri gibi, saydam bir şekilde destekler ve istemci yapılandırmalarını değiştirmeye ya da çalışması için herhangi bir ek yazılım eklemeye gerek yoktur.

Neden Durumlu Denetim Güvenlik Duvarları Kullanmıyorsunuz?

Durum bilgisi olan inceleme güvenlik duvarları, uygulama düzeyi güvenlik duvarlarıyla aynı güvenlik seviyesini sağlayamayabilir. Onlar izin verir

Sunucu ve müşteri, paket filtreler gibi birbirleriyle “doğrudan” konuşurlar. Bu bir güvenlik riski olabilir.

güvenlik duvarı, güvenlik duvarından geçen paketlerin DATA içeriğinin nasıl yorumlanacağını bilmiyor. Üstelik

daha rahatsız edici, birçok insanın durumsal denetim güvenlik duvarlarını yapılandırmanın daha kolay olduğunu düşünmesi

Yanlış, uygulama düzeyinde güvenlik duvarlarına kıyasla. Bunun nedeni paket filtrelerinin ve durum kontrolünün yapılmasıdır.

güvenlik duvarları çoğu hizmeti şeffaf bir şekilde desteklemese bile, uygulama düzeyinde güvenlik duvarları genellikle çok sınırlı sayıda hizmeti destekler ve desteklenmeyen servislerle çalışmak için istemci yazılımında değişiklik yapılmasını gerektirir.

Network Associates adlı bir bildiri kitabında, 3

Bilgisayar Güvenlik Enstitüsü (CSI), “Güvenlik duvarı üzerinden tehlikeli hizmetlere izin vermek için durumsal denetim güvenlik duvarlarını yapılandırmak oldukça önemsiz, aslında önemsiz…” demiştir. Uygulama proxy güvenlik duvarları, tasarım gereği, yapılandırma sırasında hata yapmayı çok daha zorlaştırır. ”

Network Associates'ten bir bildiri kitabında, 3, Bilgisayar Güvenliği Enstitüsü (CSI), “Tehlikeli hizmetlere izin vermek için durumsal denetim güvenlik duvarlarını yapılandırmak, aslında önemsiz bir şeydir.

Güvenlik duvarı…. Uygulama proxy güvenlik duvarları, tasarım sırasında, hatalar sırasında hata yapmayı çok daha zor hale getirir

yapılandırması.”

Tabii ki, eğer doğru bir şekilde yapılandırılmadıysa, hiçbir sistemin güvenli olmadığını söylemek gereksizdir. İnsan hataları ve hataları, güvenlik sorunlarının bir, iki ve üç nedenidir, değil mi?

Uygulama Seviyesi Güvenlik Duvarları

Uygulama düzeyinde güvenlik duvarları (veya yalnızca proxy'ler), müşteriden proxy'den istemci adına bir görev gerçekleştirmesini istediği “ortadaki adam” olarak çalışır. Bu, Web sayfalarını almak, posta göndermek, FTP kullanarak dosyaları almak, vb. Gibi görevleri içerebilir. Proxy'ler uygulamaya özeldir, yani kullanılacak belirli bir uygulamayı (veya daha tam olarak uygulama düzeyinde protokolü) desteklemeleri gerekir. . İçin standartlar da var

En popüler SOCKS olmak üzere, genel proxy işlevi. SOCKS, aslen David tarafından yazıldı.

Koblas ve NEC tarafından daha da geliştirilmiştir. SOCKS'i destekleyen uygulamalar iletişim kurabilecektir

SOCKS standardını da destekleyen güvenlik duvarları.4 Durumlu bir inceleme güvenlik duvarına benzer şekilde, uygulama düzeyinde bir güvenlik duvarının normal varsayılanı başarısız olur, bu da nasıl kullanılacağını anlamadığı paketleri / oturumları engelleyeceği anlamına gelir.

Neden Uygulama Seviyesi Güvenlik Duvarları Kullanmalı?

Her şeyden önce, temelde yalnızca destekledikleri basit gerçeğe dayanarak yüksek düzeyde güvenlik sağlarlar.

çok sınırlı sayıda hizmet; bununla birlikte günlük olarak ihtiyaç duyulan olağan hizmetlerin çoğunu olmasa da destekler. Uygulama katmanındaki protokolleri anlarlar ve böylece bir protokolün bölümlerini engelleyebilirler (FTP kullanarak dosya alınmasına izin verir, ancak örnek olarak FTP kullanarak dosya göndermeyi reddederler). Güvenlik duvarı satıcısına ve sürümüne bağlı olarak güvenlik açıklarını da tespit edip engelleyebilirler.

Ayrıca, müşteri ile sunucu arasında doğrudan temas yoktur; güvenlik duvarı idare edecek

müşteri ve sunucu için tüm istek ve cevaplar. Bir proxy sunucusu ile kullanıcı gerçekleştirmek de kolaydır

Kimlik doğrulama ve pek çok güvenlik uygulayıcısı, mevcut kapsamlı günlük kaydı düzeyini takdir edecektir.

uygulama düzeyinde güvenlik duvarları.

Performans nedenleriyle birçok uygulama düzeyinde güvenlik duvarı, verileri daha hızlı yanıt vererek önbelleğe alabilir

Örneğin, sık erişilen Web sayfalarına erişim için süreleri ve daha yüksek verimi Yazar genellikle bir güvenlik duvarının bunu yapmasını önermez, çünkü bir güvenlik duvarının trafik denetimini ele alması ve yüksek düzeyde güvenlik sağlaması gerekir. Bunun yerine, güvenlik uzmanları tek başına bir önbellekleme kullanmayı düşünmelidir.

Ortak Web sitelerine erişirken performansı artırmak için proxy sunucusu. Böyle bir tek başına önbellekleme proxy sunucusu elbette ek içerik güvenliği ile de donatılabilir ve böylece içeriğe ve diğer sorunlara bağlı olarak Web sitelerine erişimi kontrol edebilir.

Neden Uygulama Seviyesi Güvenlik Duvarlarını Kullanmıyorsunuz?

Tasarım gereği, uygulama düzeyinde güvenlik duvarları yalnızca sınırlı sayıda hizmeti destekler. Diğer uygulama hizmetleri / protokolleri için destek isteniyorsa, uygulama düzeyinde bir güvenlik duvarı üzerinden çalışmak için uygulamaların değiştirilmesi gerekebilir. Bu tür bir güvenlik duvarının sağlayabileceği yüksek güvenlik seviyesi göz önüne alındığında (konfigürasyonuna bağlı olarak elbette), paket filtrelemeye ve durumsal inceleme güvenlik duvarlarına kıyasla performans üzerinde çok olumsuz bir etkisi olabilir.

Pazarın Gerçekte Neye İhtiyacı Var? Günümüzde pek çok güvenlik duvarı, bu teknolojileri birlikte basit ve kullanımı kolay bir ürüne karıştırıyor gibi görünmektedir. Güvenlik duvarları “anahtar teslimi” veya “hepsi bir arada” çözümü olmaya çalışır. Güvenlik duvarında, az ya da çok tarafından yapılandırılabilen güvenlik takıp açmak, bu yazarın çok az inancının olduğu bir şeydir. Ve hepsi bir arada çözüm VPN, virüsten koruma, içerik güvenliği / filtreleme, trafik şekillendirme ve benzeri işlevleri entegre eden Bu yazarın çok az güvendiği bir şey. Aslında, güvenlik duvarları giderek daha karmaşık hale geliyor gibi görünüyor Son kullanıcılar için yapılandırma, kullanma ve anlamalarını kolaylaştırır. Bu biraz yanlış görünüyor; artırarak Bir üründeki kod miktarı, üründeki güvenlik açıklarının artması ve çoğu muhtemelen üstel olarak. Yazarın görüşüne göre, bir güvenlik duvarı, çoğu kullanıcının görmeyeceği veya Not. Kullanıcılar orada olduğunu bile bilmemeli. Piyasa ne istediğine karar verir ve satıcılar tam olarak bunu sağlar. Ancak piyasa her zaman biliyor mu bunun için iyi olan nedir? Bu, güvenlik profesyonellerinin her zaman - öğretmeye öncelik vermesi gereken bir problemdir güvenlik anlayışı ve güvenlik bilinci.

Firewall Technologies: Hızlı Özet

Genel bir kural olarak, paket filtreleri en düşük güvenlik seviyesini sağlar, ancak en yüksek verimi sağlar. Onlar sahip

Sınırlı güvenlik seçenekleri ve özellikleri ve özellikle çok sayıda varsa, yönetimi zor olabilir

bunların bir ağda. Durum bilgisi olan denetleme güvenlik duvarları daha yüksek bir güvenlik düzeyi sağlar, ancak paket filtrelerle aynı verimi vermeyebilir. Bugün piyasadaki önde gelen güvenlik duvarları, çoğu ortam için en iyi güvenlik, yönetilebilirlik, verimlilik ve şeffaf entegrasyon karışımı olarak kabul edilen durumsal denetim güvenlik duvarlarıdır.

Uygulama düzeyinde güvenlik duvarları, en yüksek düzeyde güvenlik sağlamak için birçok kişi tarafından kabul edilir, ancak diğer iki güvenlik duvarı teknolojisine kıyasla daha az verim verir.

Her durumda, güvenlik uzmanları iyi güvenlik sağlamak için hiçbir zaman güvenlik duvarına asla güvenmemelidir. Ve hayır

Bir şirketin hangi güvenlik duvarını kullandığı önemli değil, doğru yapılandırılmadığı takdirde fazla güvenlik sağlamaz. Ve bu genellikle oldukça fazla iş gerektirir.

Çevre Savunması ve Güvenlik Duvarları Nasıl Uyuyor?

Pek çok insan, kötü niyetli bilgisayar korsanlarının İnternet’te “dışarıda” olduğuna inanıyor gibi gözüküyor

bir firmadaki meslektaşlar, içten veya dıştan yasadışı bir şey yapmayı düşünürlerdi. Ne yazık ki, ancak, dahili çalışanların bilgisayarla ilgili tüm suçların belki de yüzde 50'sini gerçekleştirdiğini gösteren istatistikler var. Bu nedenle güvenlik duvarı ve çevresindeki ortamdaki güvenliğin iki şekilde çalıştığını açıklamak gerekir. İnternetteki bilgisayar korsanlarının dahili ağa erişmesine izin verilmez ve dahili ağdaki kişilerin (veya virüsler ve Truva atları gibi düşmanca kodlar) dışlara hassas veriler göndermesi engellenmelidir

ağ. İlki yapılandırmak ikinciden daha kolaydır. Bunun pratik bir örneği olarak, işte bu

Yazar tarafından bir süre önce gerçekleştirilen bir İnternet penetrasyon testi sırasında oldu.

Saldırı Tespit Sistemleri ve Güvenlik Duvarları Son zamanlarda, gittikçe daha fazla şirket, ağlarına izinsiz giriş tespit sistemleri (IDS) kullanıyor. İşte hata yapmanın kolay olduğu başka bir alan. Her şeyden önce, bir IDS bir şirketin bilgisayar korsanlarına karşı güvenliğini arttırmasına gerçekten yardımcı olmuyor. Bir IDS bir şirketin bir saldırıyı daha iyi tespit etmesine ve belgelemesine yardımcı olur, ancak çoğu durumda saldırıyı durduramaz. Bir IDS'nin, şu sıralar uzun zamandır var olan kapsamlı günlük ve otomatik / manuel analizler için yeni bir terim olduğunu söylemek caziptir. Bir süre önce, birisi otomatik olarak engelleyebilecek bir IDS oluşturma fikriyle geldi çeşitli saldırılar veya saldırıları engellemek için güvenlik duvarları gibi diğer sistemleri yeniden yapılandırın. Bir sahtekarlık saldırısı yaparak (bugünlerde çok kolay), bilgisayar korsanları güvenilir bir kaynaktan (üçüncü taraf) kaynaklanan sahte bir saldırı oluşturarak IDS'nin şirket ile güvenilir kaynak arasındaki tüm iletişimi engellemesini sağlayabilir. Birdenbire herkes bu tür otomatik sistemler fikrinin muhtemelen kötü bir fikir olduğunu anladı.

Genel Öneriler ve Sonuçlar

Hareket ettiği çeşitli ağlara ve sistemlere ek olarak, bir güvenlik duvarı da kendini korumak için yapılandırılmalıdır.

ve dan veri. Aslında, bir güvenlik duvarı da İnterneti “korumalıdır”;

“Hacker'lar”, nerede ve kim olursa olsun, İnternet’e bağlı diğer partilere saldırmaktan. çevreleyen

Yönelticiler, anahtarlar ve sunucular gibi ağ donanımları da güvenlik duvarını koruyacak şekilde yapılandırılmalıdır.

sistemin kendisine ek olarak çevre. Güvenlik uzmanları, İnternete erişime izin vermeden önce kullanıcı kimlik doğrulamasını kullanmayı düşünmelidir. Bu, çoğu durumda, virüslerin ve Truva atlarının örneğin HTTP, FTP ve Telnet gibi protokolleri kullanarak Internet'teki ana makinelerle temas kurmasını engeller.

Söylemeye gerek olmayabilir, ancak İnternet’in bir şirket ağından kişisel olarak kullanılması,

yasak olmak. Tabii ki, buradaki kontrol seviyesi tartışılabilir, ancak konu kullanıcıları engellemektir

tehlikeli içerik indirme (virüs, Truva atları) ve dahili ağdan dosya gönderme

POP3, SMTP, FTP, HTTP gibi protokoller ve ASCII veya ikili dosyalarda dosya gönderilmesine izin veren diğer protokoller

biçimleri. Son olarak, güvenliği, şirketin güvenlik politikasında istenen (veya aranan) seviyeyle gerçekten eşleşen seviyeye getirmek için de başka araçlar kullanılmalıdır. Yazarın deneyiminde, muhtemelen tüm güvenlik duvarı kurulumlarının yüzde 50'sinden azı kapsamlı bir günlük kaydı yapıyor ve güvenlik duvarı sahiplerinin yüzde 5'inden azı aslında

faydalı log analizi, raporlama ve istatistiklere bile benzeyen bir şey yapmak. Bazılarına göre

Tutum “güvenlik duvarımız var, bu yüzden güvendeyiz.” Böyle bir tutum hem aptal hem de yanlıştır.

**Güvenlik Sanal Özel Ağlar**

*James S. Tiller, CISA, CISSP*

Sanal özel ağların (VPN) pek çok farklı işletme disiplini içinde olağanüstü bir şekilde popüler hale gelmesi şaşırtıcı değildir. Dikey pazar veya ticaretten bağımsız olarak, VPN'ler iletişim gerekliliklerinde önemli bir rol oynayabilir, bu durum uygulandığında esneklik ve yatırım geri dönüşü sağlar.

düzgün şekilde kullanıldı. VPN'lerin kabulü geniş ve hızlı olmuştur; ve teknoloji ilerledikçe, bu eğilim

sadece artış. VPN’lerin popülaritesinin bir kısmı, uygulamanın algılanan nispi kolaylığından kaynaklanmaktadır.

teknolojisi. Bu algılanan basitlik ve ucuz, sınırsız erişim vaadi için çılgın bir acele yarattı

bu yeni haberleşme iletişim türünden yararlanın. Maalesef, VPN’lerin bu baskın özellikleri, gizli kaldığı ve satış sözlüklerinden ve ürün sunumlarından gizlenmiş gibi görünen temel güvenlik kusurlarını gölgede bıraktı. Bu bölüm VPN'lerle ilgili güvenlik risklerine ışık tutmaya adanmıştır.

ve VPN’lerin güvenlik ile eşanlamlı olduklarını yanlış anlama.

Okuyucunun burada açıklanan güvenlik sınırlamalarının VPN teknolojisinin kendisiyle hiçbir ilgisi olmadığını anlaması çok önemlidir. Kullanılabilecek birkaç VPN teknolojisi türü vardır - örneğin, IPSec, SSL

ve PPTP, birkaçı belirtmeksizin - ve her birinin gereksinimlere ve uygulamaya bağlı olarak avantaj ve dezavantajları vardır. Ek olarak, her biri bir koşul karışımını barındırmak için yükseltilebilecek çeşitli güvenlik seviyelerine sahiptir. VPN'lerin orta ve süreç olarak güvensizlikleri, teknik yönleri veya standartları değil, tartışılmaktadır.

Ele alınan, VPN’lerin satışlardan gelen genel tüketici tarafından değerlendirilmesidir.

gereçler piyasayı ve sektörün tüketicilerin ihtiyaçlarını karşıladığını iddia eden ürünleri sular altında bırakıyor. Ne yazık ki,

talep çok büyük ve artmaya entegre olabilecek yeterli kontrollerin geliştirilmesi

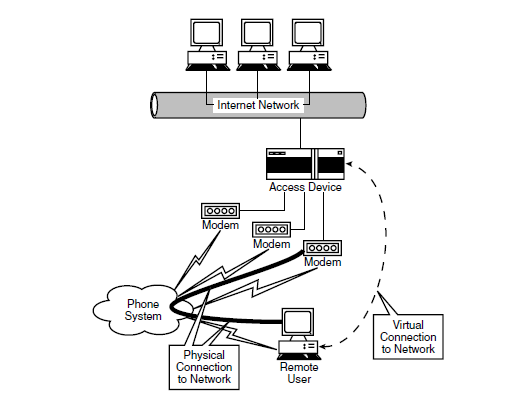
Güvenlik şu anda yaşanmakta olanın gerisinde kalıyor. “Güvenlik” sözcüğü sık sık göründüğünde

Genelde VPN'i tanımlarken geçerli olan VPN'ler tartışılmaktadır - içindeki verilerin korunması

transit. Ne yazık ki, iletişimin güvenliği, güvenliğin en önemli olduğu nokta olan VPN'in sonlandırma noktasında durmaktadır.

**Dolaşan Kullanıcılar**

Dolaşım, esir nüfusa hizmet sağlayan ve aynı hizmetlere normal sınırların dışından erişilebilmesini sağlayan erken ağların doğal ilerlemesi ile karakterize edilir. ağ. Görünüşe göre bir gecede, kullanıcılara uzaktan erişim sağlanması çok önemliydi ve bunu sağlamak için muazzam kaynaklar tahsis edildi. İlk olarak, Ek 43.1’de gösterildiği gibi, modemler toplandı ve ortak bir cihaza bağlandı. dahili ağa erişim sağlanmış ve tabii ki modemler telefon hatlarına bağlanmış sonuçta erişim sağladı. Uygulama gereksinimleri katlanarak arttıkça, modemlerin iletim hızı ılımlı bir şekilde artmış ve değişim ufukta gerçekleşmiştir. İlk değişim dalgası şeklinde geldi uzak masaüstleri veya bazı durumlarda tüm sistemler. Ek 43.2'de ayrıntılı olarak açıklandığı gibi, bir kullanıcı arayacak ve bağlanacaktır.



İnternet Kabulü

İnternet’in büyümesi olağanüstü olmuştur. İnternete ilk adımlarını atan insanların sayısından, iletişim teknolojilerindeki sıçramalara, İnternet kullanımı giderek daha yoğun ve daha fazla hale geldi.

doldurulur. İnternet, ticari ve kişisel iletişim için bir gereksinim haline geldi.

yenilik veya basit eğlence için. İnternet ile bir şekilde ilişkili olmayan işletmeler şimdi

genişletmek için kaldıraç kullanmaya çalışmak ve maliyetleri düşürürken müşteri memnuniyetini artırmak. Nadir değildir

bir kuruluşun varsayılan yükleme olarak yeni veya mevcut bir ofis için Internet bağlantısı içermesi için.

Buna karşılık, adanmış İnternet bağlantılarının ilk uygulayıcıları, bir kural olarak, tüm organizasyon. Ek 43.3'te gösterildiği gibi, uzak ofisler geniş bir alana girerek erişebilir İnternetin erişilebilir olduğu merkezi konuma ağ (WAN). Bu çok yaygın tasarım senaryosu İnternet trafiği ve gereklilikleri kapsam ve sıklık açısından sınırlı olduğunda tatmin edicidir. İnternet erişimi için gereksinimler arttıkça, WAN başlayana kadar bağlantıların sayısı doğru orantılı olarak artmıştır. acı çekmek. Bundan kısa bir süre sonra, doğrudan bağlantı maliyetleri azaldıkça ve İnternet gittikçe daha iş hayatının bir parçası daha önemli bir araç haline geldi ve daha fazla erişim gerekiyordu.

İnternetin geniş kabulü ve temel bir gereklilik olarak kabul edilmesi, İnternetin yoğunluğu ve çeşitliliği arttı. Günümüzde kuruluşların çeşitli erişim noktaları ve kaldıraçları vardır. diğer iç ağlardaki yükü azaltmak ve iç kullanıcılar için daha yüksek performans sağlamak için servis fazlalığı sağlamak gibi. Çok sayıda mevcut bağlantıdan yararlanarak, bir kuruluş VPN teknolojisini kullanarak, VPN'lerin dahil edilmesinden çok önce maliyeti makul olan bir hizmeti kullanırken iletişimi geliştirmek için uygulayabilir.

**Genişbant**

Günümüzde standart olan İnternete yüksek hızlı erişimin varlığından önce, tipik olarak yalnızca acı verici bir şekilde yavaş erişim sağlayan modemler ve telefon hatları vardı. Elbette, ISDN'ye sahip bazı ayrıcalıklı kullanıcılar için rahatlama sağlayan birkaç kullanıcı vardı. Ancak, erişim hala modemlere dayanıyordu ve düzgün çalışmak için bir kabus olabilirdi. Uzaktan erişimin ilk uygulayıcıları veri veya hizmet elde etmek için modem kullandılar. İnternet popülerleştikçe, modemler İnternete erişim için araç sağlayan bir İnternet servis sağlayıcısına (İSS) bağlanmak için kullanıldı. Her iki durumda da, sınırlı hız yetenekleri sıkıntılı

sabit.

Bugünün kişisel ve evden internete erişimi, tarihsel olarak yalnızca en büyük şirketlerin karşılayabileceği veya elde edebileceği pahalı hatlarla gerçekleştirilen hızlara erişebilir. Şu anda, ISS'ye bağlantı sağlayan ve evdeki veya küçük ofisdeki ana bilgisayara bağlanmak için Ethernet kullanan basit bir cihaz kurulabilir. Günümüzde erişim, bilgisayardan ayrı olarak sağlanmaktadır ve kontrol edilmektedir ve nadiren kullanıcı müdahalesi gerektirir. Fiziksel bağlantı ve iletişim ortamı kullanıcı ortamına karşı saydamdır. Genellikle, kullanıcı bilgisayarı açar ve Internet hemen kullanılabilir durumdadır. Bu, her biri sinyal sonlandırma noktası olmak için birlikte çalışan, kullanıcının sistemi ve modem ile ilişkili fiziksel bağlantının tam aksinedir.

ve bağlantıyı sağlamakla ilişkili tüm sorumlulukları üstlenmek.

Birçok iletişim teknolojisinde olduğu gibi (özellikle modem tabanlı uzaktan erişim konusunda),

Uzak cihazlara veya modemlere bağlantı sağlamak için sonlandırma noktası sağlanmalıdır. Çevirmeli

çözümler, uzak sistemin çevirip kurması için bir modem (sanal veya fiziksel) sağlanır

iletişim. Kablo bantları veya xDSL teknolojileri için de genişbant için benzer bir gereksinim bulunmaktadır: evdeki veya ofisteki uzak cihazlara bağlantı oluşturmak için bir sonlandırma noktası sağlanmalıdır.

Çekirdek sonlandırma noktası - VPN'lerin kabulü ile ilgili olarak -

Geniş bant ve modemler arasındaki farklılaşma faktörleri. Çalışanlara uzaktan çevirmeli erişim sağlamak için, bir sunucuya - veya bu konuda iş istasyonuna - tek bir modem takılabilir ve bir telefon hattı eklenebilir.

Uzak kullanıcı bir modem, telefon numarası ve bazı temel yazılımların kullanımı ile sağlanabilir; bir

sisteme ve hizmetlere geniş bir erişim sağlamak için bağlantı kurulabilir. Buna karşın, geniş bant uygulamaları daha karmaşık ve çok daha pahalıdır; bu nedenle, bugün yalnızca servis sağlayıcılar bu tür teknolojiyi uygularlar. Bir örnek Internet kablo servisidir; çok fazla şirket kendi iç uzaktan erişim çözümünü oluşturmak için kablo altyapısına erişemiyor.

Şu anda, geniş bant noktadan noktaya uzaktan erişim çözümleri için kullanılmıyor. Orada temel yatıyor

VPN'lerin çekiciliği: Bu ileri iletişim teknolojisini şirket kaynaklarına erişmek için kullanmanın bir yolu.

Sadece uygulama hızındaki büyük artış cazip değil, çünkü bazı uygulama gereksinimleri de olabilir.

modemlerin sağladığı sınırlı bant genişliği için harikadır, ancak teknolojinin bilgisayardan ayrılması, basitleştirilmiş ve ölçeklenebilir bir entegrasyon sağlar. Bu koşullar altında, geniş bant kurumsal kaynaklara erişim için son derece caziptir. Yüksek hızlı Internet'te gezinme ve kişisel geziler için geniş bant olması bir şeydir, ancak iş amacıyla aynı özelliklere sahip olması bir başkadır. Maalesef

Daha önce tarif edildiği gibi, genişbant teknolojileri karmaşık olmayan ve bir servis sağlayıcı kuruluşun iç kullanım için uygulamak için olanaksızdır. Sonuç, şu anda yalnızca İnternet erişimi sağlayan, yani VPN'lerin ortaya çıkmasına kadar olan yüksek hızlı bir iletişim çözümüdür.

**Genişletilmiş erişim**

İletişim yetenekleri arttıkça ve şirketler İnternet faaliyetlerini günlük prosedürlere entegre etmeye devam ettikçe, ikisini birleştirmek için VPN teknolojisinin oluşturulması kritikti. İnternete ve genişbant'a çevirmeli erişim, neredeyse her yerden ve yüksek hızlarla Internet'e erişim sağlar. Her ikisi de İnternete küresel erişime izin vermektedir, ancak şirket merkeziyle bağlantıyı sonlandırmanın uygun veya uygun maliyetli bir yolu yoktur. Genişbant erişimi İnternet ile yakından ilişkili olduğu ve doğrudan arama çözümlerinin etkisiz ve pahalı olduğu için, öngörülebilir tek çözüm özel sağlamak için Internet'i kullanmaktı. iletişim. Bu sonuçta kuruluşların mevcut internet yatırımlarına yatırımlarını çok yönlü uzak bağlantılara kullanmalarını sağladı. Nihai engel, gizlilik, bilgi bütünlüğü, erişim kontrolü, kimlik doğrulama, denetim ve bazı durumlarda reddedilmeme şeklinde iletişimin güvenliğini sağlamaktı.

İnternet'in küresel kabulü, kullanılabilirliği ve mevcut artan hızlar, çevirmeli bağlantı ile sınırsız erişim. Çevirmeli ağ kurmak için telefon sistemi kullanıldı. iletişim - ve telefonlar her yerde. Seri iletişimin kendisi, günlük bilgisayar korsanlarına müdahale etmesi zor olan ve bu nedenle nispeten güvenli olan özel bir devre üzerinden gerçekleştirildi. Artık İnternet her yerde olduğu için, artan hızlardan yararlanırken telefon şebekesinde var olan kullanılabilirliği çoğaltmak için kullanılabilir. İnternete bağlanmak için modem kullanılıyorsa, hız gerçekleştirilmez ve telefon sistemi bağlanmak için kullanılır, ancak yerel olarak; İnternet hala kullanılıyor ortak bağlantı ortamı için. Çevirmeli uzaktan erişim ile bile, bu hizmette büyük bir sıçrama oldu, çünkü birçok şirket tarafından sağlanan uzaktan erişim çözümünün yurtdışından bağlantısı zor olabilir. Politika ile sınırlandırılmadığı takdirde, telefon ekipmanı ve sistemleri bugün oldukları kalitede olmadığından ve uzun mesafeli yayınlar bağlantıyı engelleyeceğinden, maliyet bir sorun haline geldi. Buna karşılık, dünya genelinde telefon numaraları sağlayan çok büyük ISS'ler hariç, İnternet'e erişebilecek on binlerce ISS dünya çapında var. Son olarak, görünüşte bitmeyen erişim noktalarının sağlanmasına ek olarak, Dünya genelinde yüzlerce ISS için faturalandırma ve yönetim için merkezi bir nokta. Kullanıcı bakış açısına göre, dünyanın her yerinde büyük bir ISS var. Nihai engel, iletişimde olduğu gibi transit geçişe veya maruz kalmaya karşı korumayı sağlamaktı. telefon şebekesi üzerinden eski uzaktan erişim ile oluştu. Bunu doldurmak için VPN teknolojisi hemen kullanıldı. boşluk. genişletilmiş iletişim yetenekleri gelişine ve internet durumu ile everexpanding kurumsal varlığı kolayca desteklenebilir ve taşıma sırasında korunur.

**Her Zaman Bağlı**

Geçmişte, uzak bir kullanıcı merkezde modem bankasını arayabilir ve uzaktan servislere erişebilirdi kulak misafiri, aktarımın durdurulması veya kimliğe bürünme konusunda çok az endişe duyulması Barındırma sitesi açısından, maruz kalmayı azaltmak için güvenlik katmanları uygulanabilir. İletişim üzerindeki kontrolü artırmak ve tehditlere maruz kalmayı azaltmak için kimlik doğrulama, geri arama, zaman kısıtlamaları ve erişim kısıtlamaları kullanılmıştır. Bu koruma paketleri öncelikle iletişimin bire bir yönü nedeniyle mümkün olmuştur; Bağlantı kurulduktan sonra kolayca tanımlanabilir ve kontrol edilebilir. Gibi iletişimin kendisi kadarıyla, kamuya açık telefon sistemi üzerinden geçerken nispeten korunmuştur. özel devreler. Geniş bant teknolojisi, erişim cihazına bağlanmaya izin vermek için Ethernet'i kullanabileceği için, bilgisayar İnternet iletişimi için sadece "açık" olması gerekir (bkz. Ek 43.4). Bu büyük bir değişiklik gösterir bağlantının kurulmasından ve sürdürülmesinden bilgisayarın sorumlu olduğu geleneksel modem erişimi. Şu anda, tipik genişbant ile bağlantı, internet erişimine izin vererek erişim cihazında sürdürülmektedir. Ethernet arayüzündeki diğer sistemlerin durumundan bağımsız olarak bağlantı. Bilgisayardaki Ethernet arayüzü, kullanıcının onu başlatmasını, telefon numarasını bilmesini veya bağlantıyla ilgilenmesini gerektirmez. Tüm bu seçenekler işletim sistemi tarafından kontrol edilir; IP adresi bile otomatik olarak atanır. ISS, kullanıcıyla etkileşimi daha da azaltıyor. Artık İnternet bağlantısının sorumluluğu yalnızca erişim cihazına dayanmakta ve kullanıcıyı ve kullanıcının bilgisayarını bağlantıyı sürdürme ihtiyacından kurtarmaktadır. Son sistem sadece ağdaki bir düğümdür.

Erişim cihazına bağlı olan bilgisayarlar, Internet'e çok az korumasız veya korumasız olarak bağlanır.

Bir geniş bant sağlayıcısının bilgisayardaki kabloyu veya hattı ve Ethernet arabirimini takması çok yaygındır.

ve doğrudan güvenlik düzenlemesi olmadan sistemi bağlayın. Bu, temel uç sistemlere sahip olmamaya neden olur.

güvenlik kontrolü, uzun süre doğrudan Internet’e bağlanır. Fark

muazzam. İnternet üzerinde dolaşım yapan bir kullanıcının geçici bir örneği yerine, bir ISS'yi ararken IP adresi, trafik türü ve hatta bilgisayarın konumu uzun süre internete maruz kalır. Şirketler için doğrudan kullanıcı çevirmeli bağlantı desteği ile karşılaştırıldığında, pozlama şaşırtıcı. Belirgin fark, kullanıcının İnternete bağlı olmasıdır; oysa şirket tarafından sağlanan çevirmeli bağlantı servisi noktadan noktayadır. Bir sistem İnternet'e bağlandığında, türüne bakılmaksızın, bir şebekeye maruz kaldığı yaygın olarak kabul edilir.

muazzam tehdit sayısı. Ayrıca, bağlantının sürekli olduğu sürenin uzunluğu arttıkça kabul edilir.

kurulan, maruz kalma veya bulunma ve hedeflenme riski de artar. Güvenlik duvarları genellikle yerleştirilir

İnternet bağlantıları olan ağlar, ancak bunlar genellikle kesintili ana makinelerde görülmez.

İnternete bağlantı. Sebeplerden biri bağlantının niteliği olabilir - çok daha zordur

hareketli bir hedefi vurmak için. Ancak gerçek şu ki, bu yanıltıcı olabilir ve dolaşım sistemleri

özel bağlantıya sahip bir sistemle aynı şekilde. Kısacası, İnternet’e çevirmeli erişim,

tehditler için sistem ve özel bağlantılar aynı tehditlere de maruz kalır, ancak riski daha yüksektir

bu genellikle süreye atfedilebilir. İnternete bağlıysanız, her zaman veya her zaman, genişbant veya modem ile bağlı olup olmadığına bakılmaksızın saldırıya maruz kalırsınız; sadece öyle olur ki, her zaman bağlandığında, sen uçan bir ördek değil, oturan bir ördek olursun.

Kurumsal Ağlara Erişim

VPN teknolojisi, uzak kullanıcıların yararlanarak şirket kaynaklarına erişebilmelerini sağlayan son katalizördür.

internet. Bu doğal bir ilerlemeydi; İnternet her yerde. Telefon sistemi gibi, daha yüksek bant genişliği bağlantıları norm haline geliyor ve VPN teknolojisi iletimi şifreleme teknikleri ve kimlik doğrulama ile güvence altına alıyor

VPN’in başarısının büyük bir kısmı genişbant teknolojilerinin ortaya çıkışı ve bulunabilirliği ile ilişkilendirildi.

Yüksek hızlı erişim, İnternet’te dolaşıp daha hızlı şeyleri daha hızlı almanız için mükemmeldi ancak hepsi bu kadar.

Neredeyse bir gecede, genellikle 32K veya hatta 56K modemler gibi kişisel erişimle ilişkili bant genişliği internete 100 kat arttı. Kamu telefon sisteminden uzaklaşarak elde edilen daha yüksek erişim hızları ve özel geniş bant bağlantılarına modemler hızlı bir şekilde heyecan kaybedilmiş; Ancak, aynı zamanda, çoğu hizmetin kurumsal kaynaklara erişmesini istedi. Heyecan, erişim hızlarındaki büyük atılımdan kurtulduğundan, birçok kişi bunu uzaktan erişim için kullanmanın yollarını gördü. Bu işte

VPN teknolojisinin kaçtığını ve teknik toplumu absorbe ettiğini belirtmek

Olay yerindeki ilk istemci uzak yazılımdı. Bir ürün paketi, şirket sitesindeki İnternete bağlı bir cihazı ve dolaşım sistemine yüklenen istemci yazılımını içeriyordu ve bu da internet üzerinden şirket kaynaklarına uzaktan erişim sağladı. Uzaktan erişim çözümlerine çok fazla zaman ve para yatırıldı ve bu bugün de devam ediyor. Uzak istemci tabanlı erişim ile uyum içinde, VPN'lere yapılan acele, VPN sonlandırmasını sağlayan DSL ve kablo modem değiştirmelerine katıldı ve müşteriyi bir kez daha rahatlattı.

iletişimin sorumluluğundan sistem. VPN'ler şimdi teknik manzara boyunca genişbant erişiminin şiddetli bir rüzgarıyla itilen bir orman yangını.

Şirket ağına dizginsiz erişim sağlandıktan sonra, uzak siteler için nadir değildi veya

Normalde ayrıntılı güvenlik duvarlarının ve şirket sitesinde sağlanan diğer koruma paketlerinin koruması altında tutulan verileri kopyalamak veya açmak için kullanıcılar. Birçok uygulamada, VPN'ler, uygulamaların çalışmasını sağlamak için kullanılır.

normalde uzak sistemlerde kullanılamaz veya uzak ofislerdeki çalışanlara sağlamak için pahalı kaynaklar ve destek gerektirmez. Kısacası, VPN'ler, genellikle dahili ağda bulunan bir sistem için mevcut olan hemen hemen her şey için kullanılıyor. Satıcıların, iç ağda işlem yapıyormuş gibi yapmaları için teknolojiyi sattıklarını göz önünde bulundurarak bu beklenen bir durumdur. Bazı çözümler, Microsoft'un Windows İnternet Adlandırma Hizmeti'ni (WINS) ve NetBIOS özelliklerini, şirket sitesinde sanki sistemlerde ve kaynaklarda Etki Alanı taramasına izin vermek için ürünlerine dahil eder.

Temel olarak, VPN'ler uzaktan faaliyetleri iç faaliyetlere mümkün olduğunca sorunsuz bir şekilde entegre etmek için her derde deva olarak uygulanmaktadır. Nihai ürün, veriler ve uygulamalar kontrollü bir ortamın dışındaki sistemlerden yürütülmektedir.

**Erişim noktaları**

Tamamen iç ağlarda bulunan sistemler için iç hizmetlerin olması beklenir. Dahili ağ tipik olarak güvenlik politikaları ve prosedürlerinin uygulandığı kontrol edilen, korunan ve izlenen bir ortamdır. Hizmetlere ve verilere dahili olarak erişildiği için, bu iletişime maruz kalma veya tehdit biraz

Bilinen ve bir düzeyde kabul edilen. Çoğu kurum iç ağlar üzerindeki güvenlik tehditlerinin farkındadır, ancak saldırıya uğrarsa zararın değeri veya etkisi ile doğrudan orantılı bir risk seviyesi üstlenmiştir. Bunun çoğu basit nüfus kontrolüne bağlanıyor; Dahili kaynaklar için daha fazla risk üstlenirler, çünkü İnternette dahili olarak daha az insan vardır, etkileşim genellikle gereklidir (dolayısıyla bir ağ) ve istenirse her sistem izlenebilir. Temel olarak, bazı istatistikler bize iç ağların kurumsal verilere yönelik artan bir saldırı kaynağı olduğunu söylese de, kuruluşlar içinde bulunanları kontrol edebildiklerinden eminler

onların duvarları. Güvenlik politikaları olmayan ve kendilerini savunmasız olarak görebilecek örgütler bile

Güvenlik önlemlerini uygun gördüğü şekilde büyütmek ve uygulamak için her zaman yer olduğunu varsayınız. Bununla birlikte,

İnternet birçok kuruluşun gözünde çok daha büyük bir tehdit oluşturuyor ve bu bazı kuruluşlar için gerçek olabilir; her biri farklı. Temel nokta, İnternet'in bilinmeyen ve her zaman bir tehdit olacağı, oysa belirli önlemler alınabileceği - ya da riskin kabul edilebileceği - daha kolay bir şekilde iç ağda olmasıdır. Her durumda, dahili ağlar, bir işi desteklemek veya büyümek için bilgileri paylaşmak ve işbirliği yapmak için kullanılır ve bu da insanların Internet üzerinden evden istediği açık etkileşimidir.

VPN teknolojisi, varsayılan duruş ve kontrol erişiminin tam bir çelişkisidir. İç ağ,

uygulamaların, hizmetlerin ve verilerin bulunduğu yerlerde, güvenlik duvarları, prosedürler ve işlemler sayesinde güvenli kabul edilir

Yöneticiler tarafından denetlenen güvenlik, bir şekilde veya başka bir şekilde güvenliği sağlamaya odaklanmıştır. Ancak, doğası

VPN, kurumsal güvenliğin temel varsayımını ve anlaşılan güvenlik tutumunu olumsuzlar. Saldırganlar kim

sertleştirilmiş şirket güvenlik duvarları tarafından engellenmiş olabilir uzak VPN istemcilerini çok daha kolay hedefler bulabilir

aynı sonuçları sağlayabilir.

Genel olarak, yöneticiler sürekli güvenlik düzeltme ekleri uyguluyor, süreçleri güncelliyor ve performans sergiliyorlar

kritik sistemlerde güvenlik açıklarından korunmak için genel güvenlik bakımı. Bu arada, bu güvenlik açıkları, kullanıcılarının sistemlerini aynı bütünlükte sürdürmeleri daha az muhtemel olan son kullanıcı sistemlerinde kalmaktadır. İleri düzeyde bir kullanıcının kapsamlı bir koruma planı sunması durumunda,

uzak sistemler işletme sınıfı işletim sistemlerini çalıştırmaz ve kendiliğinden güvensizdir. Microsoft’un Windows 95 ve 98 platformları şu anda kişisel veya son kullanıcı sınıfı sistemlerin çoğunda kuruludur ve sınırlı güvenlik yetenekleri ve genel sağlamlık açısından iyi bilinmektedir. Bu nedenle, temel kusurlar sistemdeki uygulamalı güvenliği zayıflatır.

Ortak bir VPN uygulamasına katkıda bulunan özelliklerin çarpışması, şirket sitesinde uygulanan güvenlik altyapısının iptal edilmesiyle sonuçlanır. İnternete karşı korumanın neredeyse her yönü, bir kullanıcının bir VPN ile şirkete bağlandığı dakikada geçersizdir. Tek bir koruma noktası, yalnızca korunan ağ kaçınılan geçici ortamla etkileşime girmediğinde geçerlidir.

**Güvenlik Zarfı**

Bu muazzam maruz kalmayı tamamen kavramak için, bir güvenlik duvarı ve izinsiz giriş tespit sistemi ile İnternet'ten bölünmüş bir şirket ağı düşünün ve hatta silahlı güvenlik görevlilerinin özel bir sistem topluluğunun bulunduğu binayı koruduğunu düşünün. Ağdaki verilerin iç ağdayken açık alanda paylaşıldığını ve erişildiğini varsayalım. Katılan her sistem kuruluş tarafından eşit olarak korunur ve kontrol edilir.

Şimdi, sistemlerden birini kontrolsüz uzak bir yere götürün ve noktadan noktaya bir bağlantı kurun

modemlerle. Uzaktaki bilgisayar hala yalıtılmış durumda ve dışındaki güvenilmeyen sistemlere bağlı değil.

Telefon sistemi İletişimin kendisi göreceli olarak isimsizdir ve müdahalesi karmaşık olacaktır.

keşfedilirse. Bununla birlikte, VPN’lerde gördüğümüz gibi, şifreleme telefon sistemi üzerinden protokole uygulanabilir.

daha fazla koruma için.

Sonra, aynı sistemi uzak bir yere götürün ve İnternete bağlayın ve İnternet’e bir VPN kurun.

Şirket ağı. Artık sistem, bilgisayar kullanıldığında yapılan kontrolün ötesinde etkilere maruz kalmaktadır.

şirket ofisinde idi; yine de aynı erişime izin verilmektedir.

Yukarıdaki üç örnekte, bilgisayar kontrollü bir şekilde tutulurken güvenlikteki bozulma meydana gelir.

Uzak bir yere ortam ve çevirmeli erişim sağlanır. Riskler, çalınan sistemden değişiyor

telefon şebekesi üzerinden iletişim kurulurken iletimin yakalanma ihtimalinin yüksek olması, ancak sistemin genel güvenliği ve bilgiler göreceli olarak korunmaya devam etmektedir. Bununla birlikte, uzak bilgisayar İnternete yerleştirildiğinde, tehditlere maruz kalma ve çalışma riski artar

katlanarak.

Örneğin başında, sistemler yetkisiz kişilerden izole edilmiş bir koruma zarfında bulunur

koruma katmanları etkiler. Ardından, koruma zarfı uzaktaki çevirme sistemine kadar uzanıyoruz; anlaşılır bir şekilde, zarf zayıflamış, ancak bilginin korunmasını sağlamak için kesinlikle doğada var. Uzaktan çevirme sistemi, tahkimatlı çevre ortamı tarafından sağlanan korumanın bir kısmını kaybeder ve sınırlı tehditlere maruz kalır, ancak asıl önemli olan, şirket sitesi için güvenlik zarfı etkilenmemesidir.

Gerçekte, uzak sistemlerin doğrudan arama yapmasına izin verme riskleri tipik olarak

yetkisiz erişim, genellikle telefon sistemi aracılığıyla kazanılır. Kurumsal uzaktan kumandaya telefon numaraları sağlar

kullanıcıların erişebilmesi için bu sayılara gezegenin her yerinden erişilebilir. Saldırganlar, hedef uzaktan erişim numaralarını dahil etme olasılığı yüksek olan telefon numarası aralıklarını kolayca ve hızlı bir şekilde belirleyebilir. Menzil bilindikten sonra, her numarayı saldırgandan çok az veya hiç müdahalede olmadan test etmek için bir telefon tarama veya “savaşçı arama” programı kullanılabilir. Bununla birlikte, bu riskleri kontrol altında tutmayı başaran birçok faktör vardır. Geri arama, gelişmiş ve çok katmanlı kimlik doğrulama, kapsamlı günlük kaydı, zaman kısıtlamaları ve erişim kısıtlamaları saldırgan için zorlu bir hedef oluşturmak için birleştirilebilir. Sadece tek bir erişim noktası ve uzaktaki sistem yalıtımlı olduğunda, güvenlik zarfı sağlam ve somut kalır. Elbette, bozunma derecesi, şirketteki tek erişim noktasının güvenliği ve uzaktaki sistemin izolasyon düzeyi ile doğrudan ilgilidir.

Bir VPN'nin istihdamının İnternet üzerinden kurumsal bağlantı sağladığı son senaryoda, çevirmeli erişim çözümlerinden daha büyük veya eşit olmasa bile, güvenlik çok yüksek olarak algılanmaktadır. Neden olmasın? Aynı özelliklere ve tartışmalı olarak aynı güvenliğe sahip oldukları görülüyor. Çevirmeli bağlantı çözümlerinde iletişim nispeten korunur, şirkette sonlandırma sağlayan sistem güvence altına alınabilir ve yetkisiz erişimi azaltmak için doğrulama önlemleri alınabilir. VPN'ler de bu özelliklere sahiptir ve kapsamlı bir güvenlik zarfı elde etmek için kullanılabilir.

Ne yazık ki, VPN normalde bulunmayan bir güvenlik cephesi olan şeffaf bir zarf sunmaktadır.

VPN'ler bir protokol olarak çok başarılı olmasaydı, bu yoğunluk. Kurumsal olarak sağlanan zarf, uzaktaki sistemin güvenlik ve koruma istihdamının kontrolünü kazandığı gerçeğinden dolayı VPN'lerle bir kırılma noktasına kadar uzanıyor. Güvenlik zarfının artık olmadığı çok açık olacak

şirket tarafından verilen veya yönetilen ancak bunun yerine uzaktaki sistem artık tüm güvenlik denetleyicileridir - yerel olarak

ve kurumsal içine. Uzak bir sistem İnternete bağlanır ve İnternet topluluğunun geri kalanıyla iletişim kurmak için ISS'den bir IP adresi alır. İnternetteki bir yerde, şirket ağındaki dahili ağa erişim sağlayan bir VPN ağ geçididir. Uzak sistem veri paylaşmak için VPN'i kurdukça, şirket tarafından alınan güvenlik önlemlerini tamamen aşabilecek bir dizi güvenlik açığı ortaya çıkmıştır.

normalde güvenlik zarfını sağlıyor olacaktı. İnternete bağlanma noktasında

fark edilmiş güvenlik yuvarlanması gerçekleşiyor ve uzaktaki sistem hakim, jüri ve muhtemelen

şirket güvenliğinin cellatı.

Uzak sistem, ana bilgisayar sisteminin bir yönlendirici görevi görmesine ya da bilgilerin İnternet'ten özel ağa iletilmesine izin vermeyen çok sağlam bir VPN çözümü kullanmış olabilir. Bir adım daha ileri gitmek için, VPN çözümü sınırlı güvenlik duvarı yetenekleri veya sınırlamak için filtreleme konseptleri kullanabilir.

dahili ağa erişim. Bununla birlikte, muhtemelen VPN istemcisi veya güvenlik duvarı tarafından sağlanan koruma

yazılım kullanıcılar tarafından kapatılabilir ve sonunda onları saldırıya açabilir. Bir paket olabilir halinde

Kullanıcının koruma paketini kapatamadığı durumlarda uygulanan güvenlik açığı olacağı varsayılabilir.

Bunu düzeltmek için bir yama gerektiren ortaya çıkar.

Bu senaryo oldukça yaygındır ve güvenlik duvarı ve çevre güvenliği için neredeyse her gün meydana gelir

Yöneticiler sadece sınırlı sayıda güvenlik duvarına yetişmeye çalışıyorlar. Dikkat eksikliği göz önüne alındığında

normalde birçok kuruluşta güvenlik duvarı bakımına bakıldığında, yalnızca dağılmanın hayal edilebileceği tahmin edilmektedir.

uzaktaki sistemin güvenlik duvarı yazılımında güvenlik açıkları bulunduğunda güvenlik

**Güvenlik açığı kavramları**

Tam olarak yeterli hale getirilen algılanan kurumsal güvenliğin imhasının uç noktasını tam olarak anlamak

teknoloji ve süreçlerin miktarları, uzak sistemin açık ve maruz kaldığını bilmek gereklidir.

internet. Bazı durumlarda, geniş bantta olduğu gibi, pozlama sabittir ve uzun süre

tahmin edilebilir - bir saldırganın en büyük varlığı.

İnternet, çok sayıda insan ve teknoloji yüzünden, başka bir şey değilse, bir tehdit denizidir.

anonim olarak başkalarına, özellikle hazırlıksız olanlara zarar vermek için kullanılabilir. Bir kaç tane var

farklı kullanımlar için olan ve iletişimdeki farklı katmanları etkileyen farklı saldırı türleri. İçin

Örneğin, hizmet reddi (DoS) saldırıları, yalnızca yıkıcı bir amaç olan bir sistemin veya hizmetin kullanılabilirliğini ortadan kaldırmak için tasarlanmıştır. DoS saldırıları düşük seviye iletişim özelliklerinde zayıflıklardan yararlanır,

Bir protokol güvenlik açığı veya uygulamanın kendisinde bulunabilecek üst düzey zayıflıklar gibi. Diğer bazı saldırılar çok özel uygulamalara sahiptir ve erişim sağlamak veya bilgi edinmek için belirli durumlar için tasarlanmıştır. Bu saldırıların uygulama hatalarından ve tuhaflıklarından yararlanarak görülmesi gittikçe yaygınlaşıyor. Sonuçlar, sistem bilgilerini almak veya hatta ana bilgisayarı uzaktan kontrol etmek için özel olarak tasarlanmış uygulamalardır.

Trojanlar, çoğunlukla popüler işletim sistemlerinde ve çok becerikli programlayıcılardaki büyük zayıflıklar nedeniyle çok karmaşık ve kullanımı kolay hale geldi. İnternette oturan tipik bir sistem, yalnızca sisteme erişmek, ana bilgisayar sisteminin bölümlerini uzaktan kontrol etmek, yerel olarak depolanan verileri elde etmek ve klavye girişi toplamak için kullanılamayan, ancak ana bilgisayar ne zaman saldırganı bilgilendirebilecek bir Trojan kurmuş olabilir. sistem

çevrimiçi ve erişime hazır. Bazı durumlarda, bilgiler çevrimdışı toplanabilir ve ne zaman saldırgana gönderilebilir.

İnternet bağlantısı kurban tarafından kurulur. En kötü senaryoyu temsil eden bu güvenlik açığıdır ve ne yazık ki, etkilenen tipik bir ev sisteminin yaygın olduğu bir durumdur.

Truva atının tamamen yüklenemediği veya uygulanamadığı bir durumda, bir saldırgan yeterli erişim sağlayabilir,

geçici olsa bile, hedeflenen sistem veya kullanıcı hakkında hayati bilgiler toplamak, sonuçta daha

daha iyi sonuçlar veren saldırılar. Anti-virüs programlarının ve ana bilgisayar tabanlı güvenlik duvarı uygulamalarının yapabileceği söylenebilir.

Kullanıcının güvenlik açıklarını azaltmasına ve onları keşfetmesine yardımcı olmalarına ve muhtemelen onları gidermelerine yardımcı olma. Ne yazık ki, bu tür uygulamaların uygulanması, bakımı ve günlük güvenli kullanımı kullanıcının elindedir. Bununla birlikte, uzman personel ile rafine, son derece teknik ortamları korumak, Internet'e yayılmış çok daha az uzak sistemleri korumak için yeterince karmaşıktır.

**Çözümler**

Elbette, VPN'lerin uygulanmasıyla sunulan güvenlik ikilemine kolay bir çözüm yoktur.

Gelişmiş teknoloji ile bile, kuruluşlar bilgisayar korsanlarını durduramaz. Sistemlere erişmeye devam ediyorlar

görünürde kolaylıkla korunan ağlarda. Bunun çoğu zayıf tasarıma bağlanabilir, aradaki boşluklar

bakım, yanlış yapılandırma veya basit cehalet. Her durumda, çevreye odaklanarak,

yetkisiz erişim hala endişe verici bir oranda gerçekleşiyor. Binlerce olmasa da yüzlerce bu senaryo göz önüne alındığında

İnternetteki uzak bilgisayarlardan, onları korumak için ne yapılabilir? Bir iç ağ varsa, basitçe ifade

soruna en iyi çaba harcandığında korunamazlar;

evde ve yolda kitleler.

Her türlü sağlam güvenlik uygulamasında olduğu gibi, bilgilerin korunmasında bir güvenlik politikası çok önemlidir. belirtme

bilgi erişimi için veri erişim kısıtlamaları ve işletme parametreleri,

bilgi. Başka bir deyişle, uzaktan çalışma için belirli bir bilgi türüne ihtiyaç duyulmazsa, o zaman uzak

erişim sistemleri bu bilgiye veya sisteme erişim sağlamamalıdır. Sadece genişliği azaltarak

uzaktan erişim çözümü tarafından sağlanan erişim, veriler doğal olarak korunabilir. Neyin sınırlandırılması uygulaması

aslında uzak kullanıcılar tarafından erişilebilir durumda, iç ağı VPN topluluğundan koruyan görünen VPN aygıtlarının arkasındaki güvenlik duvarları şeklinde gerçekleşmiştir. Ne yazık ki, bu tasarımın çok büyük kısıtlamaları var ve erişim esnekliği açısından VPN'in ölçeklenebilirliğini sınırlayabilir. Bir başka olasılık da dahil olma

VPN erişim cihazında kullanılan filtreleme yöntemlerinin listesi. Enjekte edilen trafiği kontrol etmek için filtreler oluşturulabilir

dahili ağa bağlanılır ve bazı durumlarda filtreler gerçek kimliği doğrulanmış kullanıcılar veya gruplarla ilişkilendirilebilir.

Erişim ne kadar kısıtlı olursa olsun, bir noktada uzaktaki bir kullanıcı hassas bilgiler ister ve herkes

Kullanıcılar için uygulama hizmetleri bu “özel durum” ile karşı karşıya kalmıştır. Bu nedenle, teknoloji devralmak zorundadır

bilgiyi korumak için. Tıpkı iç ağlarımızı İnternetten korumak için güvenlik duvarlarına baktığımızda,

Uzaktaki sistemleri, özel bilgilerin bilinmeyene aktarılmasından korumak için teknolojiyi tekrar arayın.

Ana bilgisayar tabanlı koruma yazılımının uygulanması tamamen yeni değildir, ancak saldırıların sayısı artmaktadır.

kişisel sistemler varlıklarının farkındalığını arttırdı. Bununla birlikte, bu uygulamalar nokta çözümleridir ve güvenliği sağlamak için ölçeklenebilir, esnek veya merkezi olarak kontrol edilen veya yönetilen bir çözüm değildir. Temel olarak, her kullanıcı, gerçekleştirdiği güvenlik duruşundan sorumludur.

**Sonuç**

VPN'ler son derece değerli olabilir; zamandan, paradan tasarruf sağlayabilir, erişimi genişletebilir ve kuruluşların iletişimde en üst düzeyde esneklik kazanmasını sağlayabilirler. Ancak, bir VPN tarafından sağlanan özel bağlantı sanal bir arka kapı açabilir. Saldırganlar. Hassas verilerin bir VPN'den geçmesine izin veren kuruluşlar, bu bilgileri bir Korunan iç ağda bulunmayan tehditlerin bolluğu. Her biri kendi bağlantı kurma, bağlantıyı sürdürme ve genellikle iç ağda bulunan hizmetleri sağlama yöntemlerine sahip birçok VPN ürünü türü vardır. Maalesef, uzaktaki sistem VPN üzerinden merkez ofisle özel bir iletişimde bulunmuyorsa, sistem son derece savunmasız sayılabilir. İnternet hayatlarımıza ve günlük aktivitelerimize nüfuz edecek şekilde büyüdü, ancak her zaman kumda toplam asimilasyondan ayrılmanın ölçülebileceği bir çizgi çizildi. Güvenlik duvarları, modemler, yönlendiriciler, filtreler ve hatta tarayıcılar gibi yazılımlar İnternete görünür bir erişim noktası sağlayabilir. Teknoloji daha yaygın hale geldikçe, İnternet ve özel ağlar arasındaki sınır belirsizleşmeye başlayacaktır. Maalesef, uygun öngörüler olmadan, güvenlik önlemlerinin tahsisi ve azaltma süreçleri bilgi terörizmindeki ilerlemelere ayak uyduramayacak. Düzgün bir şekilde planlanmamış ve kontrol edilmemişse, görünüşte güvenli bir şekilde bir tahkimat haline getirilmiş görünmesi diğer tüm korumayı olumsuz etkileyebilir; Bir kalenin duvarları doğrudan yanlarına gelmeyen bir saldırıya karşı etkisiz olacaktır.

---------------------------------------------------------------------------------------------------------------------

**Çerezler ve Web Hataları: Ne Onlar ve Birlikte Nasıl Çalışırlar?**

Çerezler nedir ve Web hataları nelerdir? Çerezler, bakkalda bulduğumuz ve yemeyi sevdiğimiz çerezler değildir. Aksine, World Wide Web’de bulunan çerezler, bir Web sitesi tarafından oluşturulan ve bilgisayarınızın sabit diskine gönderilen küçük, benzersiz metin dosyalarıdır. Çerez dosyaları, her tıkladığınızda fare tıklatma seçimlerinizi kaydeder

İnternete gir. Bir Tekdüzen Kaynak Bulucu (URL) yazdıktan sonra, tarayıcınız bu sunucuya bağlanır

ve belirli bir Web sitesinin monitörünüzde görüntülenmesini ister. Tarayıcı sabit sürücünüzü arar

Siteden zaten bir çerez dosyanız olup olmadığını görün. Bu siteyi daha önce ziyaret ettiyseniz, benzersiz tanımlayıcı

Daha önce çerez dosyanızda kayıtlı olan kod tanımlanır ve tarayıcınız çerez dosyası içeriğini tekrar o siteye aktarır. Artık, sunucunun daha önce o siteyi ziyaret ettiğinizde seçtiğiniz şeyin bir geçmiş dosyası var. Bunu daha önce görebilirsiniz; çünkü önceki seçimleriniz ekranınızda vurgulanır. Bu siteyi ilk defa ziyaret ediyorsanız, size bir kimlik atanır ve bu ilk çerez dosyası sabit diskinize kaydedilir.

Web hatası, Web sayfasındaki veya kimlerin okuduğunu izlemek için tasarlanmış bir e-posta iletisindeki bir grafiktir.

Web sayfası veya e-posta mesajı. Bir Web hatası, e-postanın İnternet Protokolü (IP) adresini sağlayabilir.

alıcı, alıcının bu bilginin ifşa edilmesini istemesini isteyip istemediğini. Web hataları bilgi sağlayabilir

Bir mesajın ne sıklıkla iletilip okunduğuna bağlı olarak. Web hatalarının diğer kullanımları

takip eden detaylar. Ayrıca, Web hataları ve çerezler birleştirilebilir ve hatta bir kişininkiyle senkronize edilebilir

e. Web kullanımına göre araştırılacak olumlu, olumsuz, yasadışı ve etik olmayan konular var

böcekler ve kurabiyeler. Bu detaylar da takip ediyor.

Çerez Nedir?

Sadece son birkaç yılda çerezler tartışmalı bir konu haline geldi, ancak daha önce de belirtildiği gibi, bu tür değil

markette "Oreos" veya "Famous Amos" ismini taşıyan çerezlerin listesi.

bir Web sitesi ile bir bilgisayarın sabit diski arasında geçen bilgiler. Her ne kadar çerezler oluyor

daha popüler bir konu olarak, çerezlerin zor durumda tutulduğunun farkında olmayan birçok kullanıcı var.

sürücüler. Çerezlere aşina olanlar, internet gizliliği ve ahlakı konularını gündeme getiriyor. çok

DoubleClick, Inc. gibi şirketler de, şu soruyu soran davalara açıldı: İnternet şirketleri çok mu ileri gidiyor?

Başlamak için, çerezlerin temelleri açıklanmalıdır. Netscape için Lou Montulli, kurabiyeyi 1994 yılında icat etti. O zaman, bir kurabiye icat etmenin tek nedeni, çevrimiçi alışveriş sepetlerini sağlamaktı. Neden “cookie” adı? “Çerezler… İyi mi Kötülük?” Başlıklı bir makaleye göre, ilk bilgisayar korsanlarının Andy Williams’ın TV programında gösteriye başladıkları söyleniyor. Ayı kıyafetli bir adamın Williams'dan bir kurabiye almak için her türlü hileyi denediği ve “Çerezler olmaz! Şimdi değil, asla değil… HİÇ! ”Bir bilgisayar korsanı“ çerez ayı ”adını ve sinir bozucu anabilgisayar bilgisayar operatörlerini konsollarını devralarak ve“ WANT COOKIE ”mesajı görüntüleyerek aldı. çerez, ”ve çerez ayı bir teşekkür ile cevap verirdi. “Kurabiye”, operatörün sinirlerine zarar vermek dışında hiçbir şey yapmadı. Böylece “çerez” adı ortaya çıktı.

**Çerez İçeriği**

Tanımlama bilgileri ilk keşfedildiğinde, bu tanımlama bilgilerinin sabit sürücünüzdeki bilgileri tarayabileceği ve şifreleriniz, kredi kartı numaralarınız veya bilgisayarınızdaki bir yazılım listesi gibi ayrıntılar alabileceği söylentileri ortaya çıktı. Bir çerezin çalıştırılabilir bir program olmadığı ve doğrudan bilgisayarınıza hiçbir şey yapamayacağı açıklandığı zaman bu söylentiler reddedilmiştir. Basit bir ifadeyle, çerezler tarafından oluşturulan küçük, benzersiz metin dosyalarıdır.

bir Web sitesi ve bir bilgisayarın sabit diskine gönderildi. Bir isim, değer, son kullanma tarihi ve

kaynak site. Başlık bu bilgiyi içerir ve tarayıcıdan önce belgeden kaldırılır

görüntüler. Tarayıcınızda görünüm veya belge kaynağı komutlarını çalıştırsanız bile bu başlığı göremezsiniz. Başlık, oluşturulduğunda çerezin bir parçasıdır. Sabit diskinize takıldığında, başlık bırakılmıştır. Tanımlama bilgisinden kalan tek bilgi sunucu ile ilgilidir ve başkası yoktur.

Bir başlık örneği aşağıdaki gibidir:

Set-Cookie: NAME=VALUE; expires=DATE; path=PATH;

domain=DOMAIN\_NAME; secure

ADI = DEĞER gerekli. NAME, çerezin adıdır. VALUE'nin kullanıcı ile ilgisi yoktur; Kaynak sunucunun göndermeyi seçtiği bir şeydir. DATE, çerezin sabit diskinizde ne kadar kalacağını belirler. Son kullanma tarihi yok, Web tarayıcısından çıktığınızda çerezin kullanım süresinin sona ereceğini belirtir. DOMAIN\_NAME, çerezi gönderen ve tarayıcı bu sunucudan bir dosya istediğinde bu çerezin bir kopyasını alacak olan sunucunun adresini içerir. Çerezin geçerli olduğu etki alanını belirtir. PATH, bir çerezin sunucuya ne zaman geri gönderileceğini daha fazla tanımlamak için kullanılan bir özelliktir. Secure, çerezin yalnızca güvenli bir kanal kullanılıyorsa gönderileceğini belirtir. Birçok farklı tipte çerezler kullanılır. En yaygın tür, ziyaretçi çerezi olarak adlandırılır. Bu tutar bir siteye kaç kez döndüğünüzü izleyin. Hangi sayfaların birden fazla alan Webmaster’ı uyardığı ziyaretler. İkinci bir çerez türü, bir kullanıcının sayfanın nasıl yükleneceğine ilişkin seçtiği değerleri depolayan tercih edilen bir çerezdir. Özelleştirilmiş ana sayfaların ve site kişiselleştirmenin temelidir. Sayfada hangi renk şemalarını tercih ettiğinizi veya bir aramadan kaç sonuç sevdiğinizi hatırlayabilir. Alışveriş sepeti çerezi, çevrimiçi siparişi ile popüler bir tanesidir. Bir çerez aracılığıyla size bir kimlik değeri atar. Öğeleri seçtiğinizde, bu öğeyi içerir sunucudaki kimlik dosyasında. En ünlü ve tartışmalı olan, izleme çerezidir. Bu benzer alışveriş sepeti çerezi, ancak kimlik dosyanıza öğe eklemek yerine, ziyaret ettiğiniz siteleri ekler. Satın alma Hedefli pazarlama için alışkanlıklar toplanır. Potansiyel olarak, şirketler tarafından sağlanan e-posta adreslerini kaydedebilirsiniz. kullanıcı ve sizi hakkında topladıkları bilgilere dayanarak sizi spam. Çerezler sadece veriler dolaşırken kullanılır. Tarayıcınıza bir URL yazdıktan sonra, sunucu ve bu Web sitesini ister. Tarayıcı, zaten bir çerez dosyanız olup olmadığını görmek için makinenize bakar siteden. Bir çerez dosyası bulunursa, tarayıcınız çerezdeki tüm bilgileri o siteye gönderir. URL. Sunucu bilgileri aldığında, artık alışverişinizi keşfetmek için çerezi kullanabilir. tarama davranışı Çerez alınmazsa, size bir kimlik atanır ve makinenize şu şekilde gönderilir: sonraki ziyaretinizde kullanılacak bir çerez dosyası.

**Çerezler hakkında olumlu şeyler**

Öncelikle, çerezlerin amacı, göz atma geçmişinizdeki bilgileri takip etmektir. Bir kullanıcı çerezleri kullanan bir siteye eriştiğinde, kullanıcının tarayıcısına en fazla 255 bayt bilgi iletilir. Kullanıcı bir dahaki sefere siteyi ziyaret ettiğinde, çerez sunucuya geri gönderilir. Çerez, kullanıcının ziyaret ettiği sayfaların bir listesini veya kullanıcının önceki ziyaretlere dayanarak görüntüleme modellerini içerebilir. Çerezler sayesinde, bir site kullanım modellerini izleyebilir ve siteye giriş yaptıklarında görüntülenen bilgileri kişiselleştirebilir.

İkincisi, çerezler pazarlamacılara bilgi hazinesi sağlayabilir. İnternet çerezleri kullanarak, çevrimiçi işletmeler, belirli tüketicilerin ihtiyaçları ve ilgi alanlarıyla alakalı reklamları hedefleyebilir. Hem tüketiciler hem de

pazarlamacılar çerezleri kullanmaktan yararlanabilirler. Pazarlamacılar daha yüksek bir Tıklama Oranı izleyicisine ulaşırken, müşteriler yalnızca ilgilerini çeken reklamları görüntüleyebilir. Ayrıca, çerezler tekrarlı reklamları engelleyebilir. Internet

Focalink ve DoubleClick gibi pazarlama şirketleri, bir İnternet kullanıcısının aynı reklamları tekrar tekrar görmek zorunda olmadığından emin olmak için çerezler uygular. Ayrıca, çerezler, kullanıcıların internette gezinme alışkanlıklarını inceleyerek pazarlamacılara tüketici davranışlarını daha iyi anlamalarını sağlar. NCR, Inc. ve Sift, Inc. gibi ileri veri madenciliği şirketleri, çerez dosyalarındaki müşterilerle ilgili bilgileri analiz edebilir ve tüm tüketicilerin ihtiyaçlarını daha iyi karşılayabilir.

Bir çevrimiçi sipariş sistemi, bir kişinin ne almak istediğini hatırlamak için çerezleri kullanabilir. Örneğin, eğer bir

müşteri bir sitede bir kitap aramak için saatlerce alışveriş harcıyor ve sonra aniden çevrimdışı olmak zorunda

müşteri siteye daha sonra geri dönebilir ve ürün hala alışveriş sepetinde olacaktır.

Site kişiselleştirme, çerezlerin bir diğer yararlı kullanımıdır. Diyelim ki bir kişi CNN.com sitesine geliyor ama

herhangi bir spor haberini görmek istemiyor; CNN.com bu kişinin bunu bir seçenek olarak seçmesine izin veriyor. O andan itibaren

(çerez sona erene kadar), kişinin CNN.com'da spor haberlerini görmesi gerekmez.

İnternet kullanıcıları şifrelerini ve kullanıcı kimliklerini saklamak için çerezleri kullanabilirler, böylece bir dahaki sefer oturum açmak isterler

Web sitesine parola veya kullanıcı kimliği girmeleri gerekmez. Ancak, çerezlerin bu işlevi

bilgisayar diğer kullanıcılar arasında paylaşılıyorsa, güvenlik riski oluşturabilirsiniz. Hotmail ve Yahoo, bazı ortak

Bu çerez türünü kullanan siteler, e-posta kullanıcıları için daha hızlı erişim sağlamak için kullanılır.

Çerezler, “E-Ticaretin‘ Çerez Canavarı ’Görüntüsünün Yok Edilmesi” bölümünde açıklanan avantajlarına sahiptir. Çerezler, belirli tüketici ihtiyaçları ve ilgi alanlarıyla alakalı reklamları hedefleyebilir. Bu, yüzlerce uygunsuz ve istenmeyen reklamları uzak tutarak bir kullanıcıya yarar sağlar. Çerezler tekrarlayan afiş reklamları önler. Ayrıca, çerezlerin kullanımı yoluyla, şirketler tüketici davranış alışkanlıklarını daha iyi anlayabilirler. Bu, pazarlamacıların çoğu tüketicinin ihtiyaçlarını karşılamasını sağlar. Çerezler, söz konusu bilgisayardaki kullanıcının sitesinde saklanır. Çerezleri devre dışı bırakmak kolaydır. Internet Explorer 4.0'da Görünüm, Internet Seçenekleri komutunu seçin ve Gelişmiş'i tıklayın.

sekmesini tıklayın ve Tüm Çerezleri Devre Dışı Bırak seçeneğini tıklayın.

**Çerezlere İlişkin Olumsuz Konular**

Çerez teknolojisini kullanma konusundaki ana kaygılar güvenlik ve gizlilik konularıdır. Bazıları çerezlerin bir güvenlik riski, gizlilik istilası ve İnternet için tehlikeli olduğuna inanıyor. Çerezlerin etik olup olmaması, kullanıcılar hakkındaki bilgilerin nasıl toplandığına, hangi bilgilerin toplandığına ve bu bilgilerin nasıl kullanıldığına dayanır. Bir kullanıcı bir Web sitesine her giriş yaptığında, servis sağlayıcı, işletim sistemi, tarayıcı tipi, monitör özellikleri, CPU tipi, IP adresi ve en son hangi sunucunun oturum açtığı gibi bilgileri verir.

Çerezlerin kötüye kullanılmasının iyi bir örneği, bir kullanıcının bir bilgisayarı diğer kullanıcılarla paylaştığı durumdur. Örneğin, bir İnternet kafede, insanlar bilgisayarın sabit diskinde depolanan son kullanıcının çerez dosyasına göz atabilir ve önceki kullanıcı hakkında hassas bilgileri potansiyel olarak açığa çıkarabilir. Bu, Web geliştiricilerin çerezleri kötüye kullanmamalarının ve bir kullanıcının çerez dosyasında hassas olabilecek bilgileri saklamamalarının kritik olmasının bir nedenidir. Birinin Sosyal Güvenlik numarası, annenin kızlık soyadı veya bir çerezdeki kredi kartı bilgileri gibi bilgileri saklamak, İnternet kullanıcıları için bir tehdittir.

Çerezlerin çevrimiçi işletmeler ve Web kullanıcıları için neler yapabileceğinin dezavantajları ve kısıtlamaları vardır. Bazı İnternet tüketicileri, çerezlerin neler yapabileceği hakkında birçok efsaneye sahiptir, bu yüzden çerezlerin yapamayacağı şeyleri belirtmek çok önemlidir:

• Bir kullanıcının sabit diskinden bilgi çalmak veya zarar vermek

• Sabit diski yok edecek bitki virüsleri

• Bir siteden diğerine olan hareketleri izlemek

• İzinsiz kredi kartı numaralarını al

• Kullanıcıyla başka bir bilgisayara seyahat edin

• Tüketiciler bu bilgileri sağlamadıkça isimleri, adresleri ve diğer bilgileri takip edin

kendi isteğiyle

**Web Hata Nedir?**

Bir Web hatası, Web sayfasını veya e-posta mesajını kimin okuduğunu izlemek için tasarlanmış bir e-posta mesajındaki bir grafiktir. Çerezler gibi, Web hataları, Web sitelerinin ve reklamverenlerin siber ortamdaki ziyaretçilerin yerlerini izlemelerine yardımcı olan elektronik etiketlerdir. Ancak, Web hataları sayfada aslında görünmez ve çok daha küçüktür - cümle sonunda dönemin büyüklüğü hakkında. Melissa virüsünün yaratıcısının izini sürmesiyle bilinen, www.privacyfoundation.org adresinin Baş Teknoloji Sorumlusu Richard Smith, Web hata tekniğini ortaya çıkarmak için kredilendirildi. Smith'e göre, “Genellikle şeffaf bir resim olarak ve yalnızca 11 piksel boyutunda ayarlanmış bir Web hatası, Web sayfasını veya e-postayı kimin okuduğunu izlemek için tasarlanmış bir Web sayfasındaki veya e-posta iletisindeki bir grafiktir. mesaj. ”Meconomy.com Baş Teknoloji Sorumlusu Craig Nathan’a göre,

11 piksel Web hatası “bir işaret gibi, bu yüzden bir Web sayfasına her tıkladığınızda bir ping veya geri arama

Sunucu "Merhaba, ben buyum ve ben buyum" diyor.

Çoğu bilgisayarda, bir afiş reklamı görüntülendiğinde, bir kişinin sabit diskine yerleştirilen çerezler bulunur veya

bir kişi çevrimiçi bir hizmet için kaydolur. Savvy Web sörfçüleri, bir banner reklam gördüklerinde izlendiklerini biliyorlar. Ancak, insanlar Web hatalarını göremez ve çerez önleme filtreleri onları yakalamaz. Bu nedenle, Web hataları, çevrimiçi olarak banner reklamlarının bulunmadığı bölgelerde veya kişilerin izlenmesi beklenmeyen sitelerde, sörfçüleri takip edebilir.

Bir Web böceği örneği http: www.investorplace.com adresinde bulunabilir. Adresinde bulunan bir Web hatası var.

sayfanın en üstünde. Internet Explorer'da Görünüm, Kaynak veya Netscape'de Görünüm, Sayfa Kaynağı'nı seçerek görebilirsiniz

işyerinde kod. Aşağıda gösterildiği gibi, kod “Yatırımcı Yeri” ziyaretçisi hakkında bilgi verir.

reklam ajansı DoubleClick:

<IMG SRC=“http:ad.doubleclick.net/activity;src=328142;

type=mmti; cat=invstr;ord=<Time>?”WIDTH=1

HEIGHT=1 BORDER=0>

Bir Web sayfasındaki hataları kontrol etmek de mümkündür. Sayfa yüklendikten sonra, sayfanın kaynak kodunu görüntüleyin.

Sayfada WIDTH = 1 HEIGHT = 1 BORDER = 0 (veya

GENİŞLİK = “1” YÜKSEKLİK = “1” SINIR = “0”). Bu, küçük, şeffaf bir görüntünün varlığını gösterir. Eğer

Bu etiketin gösterdiği görüntü, geçerli sunucudan başka bir sunucuda (yani, IMG etiketi metni

SRC = “http: //”), büyük olasılıkla bir Web hatası.

**Gizlilik ve Diğer Web Hata Sorunları**

DoubleClick veya Match Point gibi reklam ağları, İnternet’in çeşitli bölgelerinin yanı sıra, dünyanın çeşitli bölgelerinde bulunan kişilerin sayısının “bağımsız bir hesaplamasını” geliştirmek için Web hatalarını (“İnternet etiketleri” olarak da adlandırılır) kullanır belirli bir Web sitesine Reklamverenler, Web siteleri içindeki istatistiksel sayfa görünümlerini de hesaba katarlar. Bu, içeriğin etkinliğini planlama ve yönetmede çok yararlıdır, çünkü bir hedef pazar bilgisi araştırması sağlar (yani, kullanıcıların siteye yaptığı ziyaretlerin sayısı). Bu aynı

reklam ağları, bir kişinin ziyaret ettiği sitelerin kişisel profilini oluşturmak için Web hatalarını kullanabilir. Bu bilgi

ne tür reklamların gösterileceğini belirlemek için bir veritabanı sunucusunda depolanabilir ve çıkarılabilir

kullanıcı. Buna “yönlendirilmiş reklamcılık” denir.

E-posta mesajlarında kullanılan web hataları daha da istilacı olabilir. Web tabanlı e-postada, Web hataları kullanılabilir

Bir e-posta mesajının ne zaman okunup okunmadığını belirlemek için. Bir Web hatası, cihazın IP adresini sağlayabilir.

alıcı, alıcının bu bilginin ifşa edilmesini istemesini isteyip istemediğini. Bir kuruluş içinde, bir Web hatası

Bir mesajın ne sıklıkla iletildiği ve okunduğu hakkında bir fikir verebilir. Bu, bir reklam kampanyasının etkinliğine ilişkin istatistikleri döndürmek için doğrudan pazarlamaya yardımcı olabilir. Web hataları, birinin önemsiz e-posta iletisini görüntüleyip görüntülemediğini tespit etmek için kullanılabilir. Bir mesajı görmeyen kişiler gelecekteki postalar için listeden çıkarılabilir.

Bir çerez yardımıyla, Web böceği bir makineyi, açtığı Web sayfasını, ziyaretin başladığı zamanı ve diğer ayrıntıları tanımlayabilir. Reklam hizmetleri sunan bir şirkete gönderilen bu bilgiler daha sonra satın almak üzere aynı reklam ağındaki bir başka şirket sayfasını ziyaret edip etmediğini belirlemek için kullanılabilir.

bir şey ya da diğer materyalleri okumak için. DoubleClick'teki küresel teknoloji başkan yardımcısı David Rosenblatt, “Çevrimiçi mağazalarında tüketici faaliyetlerini bir araya getirmenin bir yolu” diyor. Ancak, tüketici bekçileri için,

Web hataları ve diğer izleme araçları, çevrimiçi bilgisayar kullanıcılarının gizliliği ve özerkliği için artan bir tehdit oluşturuyor.

Microsoft Word belgelerine Web hataları eklemek de mümkündür. Bir Web hatası bir yazara izin verebilir

Bir belgenin nerede ve ne sıklıkla okunduğunu izleyin. Ek olarak, yazar nasıl “tıkandığını” izleyebilir

doküman bir kişiden diğerine veya bir organizasyondan diğerine geçirilir.

Word belgelerinde Web hatalarının olası kullanımlarından bazıları şunlardır:

• Bir şirketten gizli belge sızıntılarını tespit etmek ve izlemek

• Haber bültenlerinin ve raporların telif hakkı ihlalini izlemek

Bir basın bülteninin dağıtımını izlemek

• Bir Word belgesinden yeni bir belgeye kopyalandığında metin alıntılarının izlenmesi

Web hatalarını, Microsoft Word'deki bir belgenin bir görüntü dosyasına bağlanabilmesi için mümkün kıldığı;

uzak bir Web sunucusunda bulunur. Çünkü Web hatalarının sadece URL'si bir belgede kayıtlı değil.

Asıl görüntü, Microsoft Word, görüntüyü her defasında bir Web sunucusundan almalıdır

açıldı. Bu görüntü bağlama özelliği daha sonra uzaktaki bir sunucuyu ne zaman ve nerede izleyeceği konumuna getirir.

belge dosyası açılıyor. Sunucu, açılan bilgisayarın IP adresini ve ana bilgisayar adını bilir.

döküman. Bir ana bilgisayar adı genellikle bir işletmenin şirket adını içerir. Bir evin ana bilgisayar adı

Bilgisayarda genellikle kullanıcının İnternet servis sağlayıcısı adı bulunur. İzin veren özelliğin kaldırılması

Microsoft Word'deki Web görüntülerine bağlantı oluştururken, iyi bir önleyici çözüm olduğu görünmüyor. Ek olarak

Word belgelerine, Web hataları Excel 2000 ve PowerPoint 2000 belgelerinde de kullanılabilir.

**Web Hatalarının ve Çerezlerinin Senkronizasyonu**

Ek olarak, Web hataları ve tarayıcı çerezleri belirli bir e-posta adresine senkronize edilebilir. Bu numara

Bir Web sitesine, gelen kişilerin kimliklerini (artı onlar hakkında diğer kişisel bilgileri) tanımalarını sağlar.

Site daha sonraki bir tarihte. Bunu daha fazla açıklamak için, bilgisayarınıza bir çerez yerleştirildiğinde,

başlangıçta yerleştirilen çerez, okuyabilen tek kişidir. Teoride, iki ayrı bölge ayrı yerleştirirse

Bilgisayarınızdaki benzersiz bir çerez, birbirlerinin çerezlerinde depolanan verileri okuyamazlar. Bu genellikle

örneğin, bir site yakın zamanda diğer siteyi ziyaret ettiğinizi söyleyemez. Ancak, durum

bilgisayarınıza yerleştirilen çerez, bu site tarafından bir siteye gönderilen bilgileri içeriyorsa, çok farklıdır.

reklam ajansının sunucusu ve bu ajans her iki Web sitesi tarafından da kullanılır. Bu sitelerin her biri bir Web hatası veriyorsa

Her iki siteyi de her ziyaretinizde, bilgileri reklam ajansının bilgisayarına geri bildirme sayfasında,

Sizinle ilgili ayrıntılar bilgisayarınızda depolanan bilgileri kullanarak reklam ajansına geri gönderilecektir.

Her iki çerez dosyası grubuna göre. Bu, bilgisayarınızın sitelerin her birini ziyaret eden bir bilgisayar olarak tanımlanmasını sağlar.

Bir örnek bunu daha fazla açıklayacaktır. Web sörfçü Bob olduğunda, bir sayfa yükler veya bir e-posta açar. bir Web hatası içerir, bilgiler “şeffaf GIF” i içeren sunucuya gönderilir. Yaygın bilgiler gönderilirken, Bob’un bilgisayarının IP adresini, tarayıcı türünü, görüntülenen Web sayfasının URL’sini, görüntünün URL’sini, ve dosyanın erişildiği zaman. Ayrıca, Bob’un gizliliğini en çok tehdit edebilecek olan sunucuya potansiyel olarak gönderilmek, bilgisayarında bulunan ve önceden belirlenmiş bir çerez değeridir.

Önceden varolan bir çerezin niteliğine bağlı olarak, adresinden bir sürü bilgi içerebilir. e-posta adreslerine ve kredi kartı bilgilerine kullanıcı adlarını ve şifreleri. Örneğimize devam etmek için, Bob Belirli bir reklam ajansının sunucusunda barındırılan şeffaf bir GIF içeren Web Sitesi # 1’i ziyaret ettiğinde bir çerez alabilir. Bob, aynı reklam ajansının sunucusunda barındırılan şeffaf bir GIF içeren Web Sitesi # 2'ye gittiğinde de başka bir çerez alabilir. Ardından iki Web sitesi, Bob’un etkinliğini, reklamverene rapor eden çerezler aracılığıyla çapraz referans bulabilir. Bu etkinlik devam ettikçe, reklamveren Bob’un kişisel olmayan bilgileri olarak kabul edilenleri stoklayabilir tercihler ve alışkanlıklar ve aynı zamanda, Bob’un kişisel toplanma potansiyeli var. bilgi de.

Standart çerez kodları aracılığıyla, farklı sunucuların çerezlerini ve Web hatalarını senkronize ederek bu bilgilerin World Wide Web'de paylaşılmasını sağlaması kesinlikle teknik olarak mümkündür. Eğer bu gerçekleşirse, bir kişinin belirli bir Web sitesini ziyaret etmesi birçok İnternet’e yayılmış

sunucular ve birinin gizliliğinin istilası sonsuz olabilir.

**Sonuç**

Çerezlerin ve Web hatalarının temelleri tanımları, içerikleri, kullanışlılığı, gizlilik kaygılarını ve senkronizasyonu içerecek şekilde sunulmuştur. Çerezlerin ve Web hatalarının gerçek kodunun birkaç örneği gösterildi

Okuyucunun onları nasıl tanımlayacağını öğrenmesine yardımcı olmak için. Çerezlerin ve Web hatalarının işletmelerdeki birçok olumlu kullanımı

tartışılmıştır. Ayrıca, çerezler ve Web hataları ile ilgili gizlilik ve diğer konular incelenmiştir. Sonunda,

Web hatalarının ve çerezlerinin (Word belgelerinde bile) senkronizasyonu tartışıldı.

Ancak, tartışmalarımız öncelikle yalnızca günümüzde tanımlandığı, depolandığı ve kullanıldığı için çerezler ve Web hatalarıyla sınırlandırılmıştır. Çerez ve Web böcek meta verileri (verilerle ilgili depolanan veriler) sayesinde

Bilgisayar sistemlerinin birçok platformunda bireysel kullanıcı davranışları hakkında bilgi izlenebilir.

Bir gün çerez ve Web böcek madenciliği yazılımını her türlü farklı anormalliği filtreleyen görebiliriz ve

çerez ve Web böcek depolarından tüketici trendleri! Şimdiye kadar gördüklerimiz sadece bahşiş olabilir

buzdağı. (Texas A&M Üniversitesi - Corpus Christi'deki MIS öğrencilerine özel teşekkürler

Bu araştırmaya katkıları: Erik Ballenger, Cynthia Crenshaw, Robert Gaza, Jason Janacek, Russell

Laya, Brandon Manrow, Tuan Nguyen, Sergio Rios, Marco Rodriquez, Daniel Shelton ve Lynn Thornton.)

1. http://www.webparanoia.com/cookies.html

2. http://theblindalley.com/webbugsinfo.html

3. <http://www.privacyfoundation.org/education/>

4. http://ciac.llnl.gov/ciac/bulletins/i-034.shtml

5. http://ecommerce.ncsu.edu/csc513/ student\_work/tech\_cookie.html

6. http://www.rbaworld.com/security/computers/ cookies/cookies.shtml

7. http://www.howstuffworks.com/cookie2.ht

<http://www.pusulasecurity.com/hizmetlerimiz/guvenlik-duvari-firewall/>

<https://tr.wikipedia.org/wiki/G%C3%BCvenlik_duvar%C4%B1>