BİLGİSAYAR AĞLARINDA GÜVENLİK

Barış MUMCU, Elektrik Mühendisi
TRT Bilgi İşlem Dairesi Başkanlığı, Bilgisayar Ağları Grubu

Son yıllarda internetin ve internet üzerinden ticaretin gelişmesiyle birlikte, ağlar oluşabilecek saldırılara karşı zayıflık göstermeye başlamıştır. Ve ağların bu zayıflıkları, kritik iş uygulamalarında ürün kaybına ve şirketlerin ciddi anlamda zarar görmesine neden olmuştur. Bilgisayar virüsleri, DoS saldırıları, şirket çalışanlarının hataları, bilgisayar ağları üzerinde hala büyük bir tehlike oluşturmaktadır. Fakat bu ağ güvenlik açıklarını önlemek elbette ki mümkündür.

Günümüzde internet, gerek kişisel gerekse iş ilişkileri arasındaki bilgi akışını sağlayan, dünyanın en büyük iletişim aracı haline gelmiştir. İnternetin tüm dünyada böylesine yaygın kullanımı, güvenlik tehlikelerini de artırmaktadır. Önemli bir bilgi kaybı olabilir, gizlilik ihlal edilebilir (kredi kartı numarasının bulunması gibi) veya saatler hatta günler süren yükleme zamanları ortaya çıkabilir. İnternetteki bu tür güvenlik açıkları, insanları internete karşı güvensizleştirebilir ve web tabanlı şirketlerin sonunu hazırlayabilir. Bu yüzden şirketler, güvenliklerini her geçen gün arttırmakta ve yeni tehditlere karşı önlem almak amacıyla yatırımlarını sürdürmektedirler.

Bilgiye Yönelik Tehditler

Hackerlar

Herhangi bir hırsız araba çalınca, sadece bir tane araba sahibine zarar vermiş olur fakat bir hacker herhangi bir güvenlik açığından faydalanarak yüzlerce hatta milyonlarca kullanıcıyı ve şirketi zarara sokabilir. Hackerlar bir kişinin bilgisayarına ya da bir ağa izinsiz erişmek yoluyla zarar verir. İzinsiz erişimden kasıt, bir ağa ait bilgisayarın güvenlik şifresini kırıp, yetkilerini kullanmaktır. Bazı hackerlar, erişimini kazandığı bilgisayarın masaüstüne bir mesaj yazarak şaka amaçlı çalışsa da, bazıları tüm bilgisayar sistemini çökertebilir, bilgileri çalabilir ya da kullanılmaz hale getirebilir, web sayfalarını değiştirebilir ve şirketi ciddi zarar görmesine neden olabilir. Bu tür zarar veren hackerlara genelde *"cracker"* adı verilir.

Şirket Çalışanları

Çoğu güvenlik uzmanları, güvenlik açıklıklarını, ağı veya bilgisayarı kullanan şirket çalışanlarının başlattıklarını iddia etmektedirler. Şirket çalışanları, çoğunlukla ya şakayla, ya kötü niyetle ya da yanlışlıkla kendi şirketlerinin ağına veya önemli bilgilere zarar verirler. Şirketler genelde şubelerine de ağlarına erişim hakkı verirler ve şubede çalışan insanlar da, aynı şekilde güvenlik açıklarına yol açmaktadır. Bu yüzden, şirket, şubelerinin ve kendi çalışanlarının güvenliğini sürekli kontrol etmek zorundadır.

Örneğin bazı çalışanlar ağa bağlanmak için kullandıkları şifreyi, basit, crackerlar tarafından tahmin edilebilir şekilde seçerlerse, bu bir güvenlik açığı oluşturur. Veya yalnızca merkezde bir güvenlik duvarı ile korunan ve bu merkeze özel kiralık devre ile bağlı bulunan bir şubede, herhangi bir kullanıcının telefon hattı ile internete bağlanması da bir güvenlik açığı oluşturabilir.

Bazı çalışanlar da yanlışlıkla internetten ya da floppy diskten bir belge yüklerken bilgisayara virüs bulaştırabilirler ve kendi bilgisayarına bulaştırdığı virüsün farkına varmadan ağ içindeki diğer bilgisayarlarla bilgi alışverişi ile, bu virüsü tüm ağa yayabilirler. Bu da ağ için bir tehlike oluşturur. Bu soruna karşı alınabilecek önlem, tüm bilgisayarlara virüs koruma programı yüklemek ve bir belge yüklerken ekrana uyarı mesajları gelmesini sağlamaktır.

Ayrıca bazı çalışanlar, ki bu kişiler genellikle kovulmuş ya da şirket içinde aşağılanmış kişilerdir, kendi ağ yetkilerini kullanarak ve bilerek tüm ağa virüs bulaştırabilir ya da önemli bilgileri yok edebilir.

Snoops denilen bazı çalışanlar da vardır ki, bir casus gibilerdir. Diğer

çalışanlarla arasındaki rekabet nedeniyle, erişim yetkisine sahip olmadığı birtakım gizli bilgilere ulaşmaya çalışırlar. Mesajlara ya da maaş bilgilerine erişmek masum olabilir ancak önemli ve gizli finansal bilgilere ulaşmak, o şirket için büyük tehlike oluşturabilir.

Bilinen Güvenlik Delikleri

Bazı bireyler ya da gruplar, bir ağı korumak için yeni yollar bulmanın gerek olmadığını, gelen zararların kolaylıkla bilinen problemlerden kaynakladığını savunmaktadırlar. Hackerların verdikleri zararlardan yola çıkarak güvenlik açıklarını iyi bir şekilde sıralamışlardır.

Örneğin kısa zaman önce SANS enstitüsü ve NIPC, en kritik on internet güvenlik açığını özetleyen bir liste hazırlamışlardır. Birçok şirket bu listeyi kullanarak önem sırasına göre kendi ağlarındaki tehlikeli açıkları kapatmaya çalışmıştır. En son 2001 yılında, Cisco Systems'in araştırmalarıyla bu liste güncellenmiştir ve en kritik yirmi güvenlik açığı olarak listelenmiştir. Bu yirmi zayıflığı üç kategoride ele almışlardır:

Genel Zayıflıklar, Windows Zayıflıkları ve Unix Zayıflıkları.

Zararlı Kodlar

Kullanıcılara zararlı virüsler bulaştırmak kolaydır. Birçok hacker bu yolla bir ağın performansını düşürebilir.

Virüsler

Virüsler en çok bilinen güvenlik tehlikelerindendir. Kendini kopyalayabilen ve bazı olaylarla aktif hale gelebilen bir bilgisayar programıdır. Örneğin, macro virüs denilen virüsler sürekli tekrar eden uygulamalara (e-posta işlemi gibi) kendini yapıştırır ve o uygulama her başlatıldığında aktif hale geçer ve zarar verir. Yaptığınız işlemi kesen bazı virüsler de vardır. Örneğin, klavyede özel bir harfe her basışınızda ekrana bir mesaj çıkması gibi. Ayrıca önemli bilgilerin bulunduğu dosyaları silen ya da sistemi yavaşlatan bazı zararlı virüsler de vardır. Aynı zamanda virüsler bir bilgisayardan diğerine geçerek tüm ağa yayılabilirler ve ağı çökertebilir ya da yavaşlatabilirler.

Trojan Horse Programları

Bu programlara trojans da denilebilir. Bunlar genelde bilgisayar oyunları gibi zararsız hatta bazen yararlı sayılabilecek programlardır. Fakat zararlı oldukları durumlar da vardır. Bir bilgi dosyasını silebilir ya da bilgisayarı daha başka saldırılara karşı savunmasız bırakabilir. Ancak, internetten trojan horse programı yüklediğiniz zaman ya da e-posta ekini açarak bulaşabilir. Ne trojan horse, ne de virüsler e-postanın kendisinden değil, içerdiği dosya eki çalıştırıldığında bulaşabilir.

Vandallar

Vandal, bir yazılım uygulama programıdır. Tek bir dosyayı da silebilir, ağ sisteminin önemli bir parçasını da silebilir. Web sayfalarını daha çekici kılmak için Active-x veya java applet gibi bazı programlar mevcuttur, fakat bu programlar bilgisayara yüklendiği taktirde, Vandal aktif hale gelebilir.

Ağ Saldırıları

Üç kategoride incelenir:

1.Keşif Saldırıları

Bir bilgisayar ağını tehlikeye sokmak için, hackerların daha sonra kullanmak üzere bilgi toplama aktivitesidir. Ağların potansiyel zayıf yanlarını bulmak ve kaynaklarını belirlemek için kullanılan, sniffer ya da scanner gibi yazılım araçlarıdır. Bu yazılım daha çok yöneticiler için geliştirilmiştir. Şifresini unutan bir çalışanın şifresini çözmek için kullanılır fakat yanlış ellere geçerse, tehlikeli bir silah olabilir.

2.Erişim Saldırıları

Bir ağ alanındaki yetki servisi ve file transfer protocol (FTP) fonksiyonlarındaki zayıflıklar ile ilişkilidir. Gizli bilgilere, e-posta hesaplarına, veritabanına giriş kazanmak için kullanılır.

3.DoS Saldırıları (Denial of Service)

DoS saldırıları, bir bilgisayar sisteminin tamamıma ya da bir kısmına erişimi engeller. Farklı ağlardan ya da internetten büyük boyutta, yığın olarak bilgi gönderilerek oluşur.

Bilginin Ele Geçirilmesi

Herhangi bir bilgisayar ağına gönderilen bilgi, o bilgiyi almaya yetkisi olmayan kişilerce ele geçirilebilir. Bu kişiler iletişimi gizlice gözetleyebilirler ya da gönderilen bilgi paketini değiştirebilirler. Bunu bir-

çok metod kullanarak yapabilirler. Örneğin IP spoofing yöntemi. Bilgi iletişiminde, bir alıcının IP numarasını kullanarak sanki o alıcıymış gibi gönderilen bilgileri istediği gibi kullanabilir.

Sosyal Mühendislik

Gizliliğin, ağ güvenliğini sağlamada yaygın bir rolü vardır. Bilinmeyen bir şifreyi bulmak, herhangi bir çalışana yeni bir yetki vermek gibi işleri yürütür.

İstenmeyen E-postalar

Spam denilen bu tür e-postalar, reklam amaçlı mesajlar içerir ve tüm e-posta sahiplerine gönderilebilir. Çok zararlı değildir fakat sıkıntı veren bir işlemdir. Alıcının zamanını alır ve dolayısıyla şirketlerin para kaybına yol açar ve de iş amaçlı kullanılacak olan alan meşgul edilmiş olur.

Güvenlik Araçları

Şirketler, gelişmiş yazılımlar, firewall ya da intrusion detection system (IDS) gibi güvenlik araçlarını ne kadar kullanırlarsa kullansınlar, insan hatalarından dolayı oluşan problemlerden asla kurtulamazlar. Bu yüzden güvenlik iki kategoriye ayrılmıştır: İnsan güvenliği ve teknik güvenlik.

Çalışanlar aynı anda farklı yerlerden ağa bağlanmaya çalışabilir ya da ağ bağlantısını koparmadan şirketten ayrılabilirler. Bunlara benzer problemler yüzünden ağ bozulabilir, güvenlik açıklıkları meydana gelebilir.

Biometrikler

Hemen hemen tüm şirketler çalışanlarını takip etmek ve güvenliği artırmak için gelişmiş teknolojiler kullanmaktadırlar. Güvenlik risklerini en aza indirmek için kullanıcıların elektronik ve de fiziksel bakımdan nerede olduğunu bilmek ve öngörülen güvenlik işlemlerini uygulayıp uygulamadıklarını bilmek önemlidir.

Biometrik güvenlik sistemi sayesinde, çalışanların parmak izlerinden, ellerinden, yüzlerinden ve gözlerinden kimlik saptama işlemi yapılabilir. Fakat bu sistem çok pahalıdır ve hükümetler ya da çok büyük şirketler tarafından uygulanmaktadır.

Magnetic-strip sistemleri

Bu işlem daha ucuz olup, verimli sayılabilecek bir takip sistemidir. Bir çalışanın başka bir binada olup, diğer binada o kişinin bilgisayarından ağa ya da fiziksel sistem kaynaklarına girilip girilmediğini takip ederek güvenliği sağlar.

Güvenlik Uzmanı

Şirket çalışanları güvenliği sağlayabilecek kapasitede olmayabilir. Ağ güvenliği ve uygulamaları çok geniş ve karışık bir problem olduğu için, tüm çalışanların güvenlik gereksinimlerini anlamalarını sağlamak çok zaman alıcı ve zor bir iştir. Bunun yerine, gelişmiş yazılım ve donanım araçlarını kullanabilen, özel bilgi gerektiren işlemleri yürüten, bir güvenlik uzmanına ihtiyaç vardır.

Güvenlik Yöntemleri

Verimli olmak için, güvenlik metodları geniş ve tüm ağa hakim bir yapıda olmalıdır. Gelebilecek tehlikeler ve güvenlik açıkları önceden belirlenirse, güvenliği sağlamak daha kolay olacaktır.

Güvenliği sağlamak için gelişen teknolojiler çok çeşitlidir. Hazır bir antivirüs paket programı da olabilir ya da gelişmiş bir ağ güvenlik donanım aygıtı da olabilir. Bunlara örnek, firewall'lar ve IDS'ler verilebilir.

Ağdaki kullanıcılar arasındaki uzaklık, güvenliği olumsuz yönde etkiler. Bazı kullanıcılar erişimlerini yoldayken ya da internet aracılığıyla gerçekleştirebiliyorlarsa, bu hackerların da erişimine olanak sağlayabilir. Bu yüzden, kullanılan teknoloji sadece erişim yetkisi olan kullanıcıların erişimine izin vermelidir.

Honeypot'lar

Honeypot'lar, hackerların hedeflerini şaşırtarak, kaynaklara ulaşmalarını engelleyen bir sistemdir. Bunlar fonksiyonel olarak bir bilgisayardır fakat normal bir kullanıcı değillerdir. Gelen tehlikelere yanlış hedef belirlerler. Bir tehlike anında alarm verir ve yönetici bu alarmla birlikte hackerlardan gelen mesajları iptal eder ya da alarmı kapatıp IDSyi aktif hale getirir.

Honeypot'ın iki çeşidi vardır: sacrifice box ve service simulator.

Sacrifice box, herhangi bir aktivite olduğunda onu başka bir ağ kaynağına yönlendiren, tam fonksiyonelli bir işletim sistemi içerir. Service simulator ise ağ dışı olayları ve server hareketlerini izleyen bir yazılım uygulamasıdır. Sadece dıştan erişimi kısıtlar ve daha ucuzdur. Eğer ağın ihtiyaçları kesin bir alarmsa, service simulator fiyat olarak daha avantajlıdır. Eğer ağ yapısı geniş ise sacrifice box daha verimlidir. Bu çözümler kullanılıyorsa, ağın güvenliği sürekli kontrol ediliyor demektir.

Virüs Koruma Yazılımı

Antivirüs yazılımı, düzgün bir şekilde kurulmuşsa ve düzenli olarak yenileniyorsa, virüs tehlikelerini

önceden bilebilir. Geniş ağ yapılarında da önceden virüsleri haber verir. Ağdaki tüm bilgisayarlar aynı sürüm antivirüs paketini kullanmalı ve bakımını yapmalıdır.

Güvenlik Politikası

Herhangi bir ağ kurulduğunda, ister LAN ister WAN olsun, ilk yapılması gereken şey, temel güvenlik politikalarını kurmaktır. Güvenlik politikası, programlanmış ve alanı kontrol eden güvenlik ekipmanları içeren kurallardır.

Politikalar, ağa giren kişilerin erişimini kontrol etmeli ve bu kişilere sadece yetkileri dahilindeki bölgelere girmelerine izin verilmelidir. Şifreler, insanların yetkilerini belirler. Örneğin bir yönetici tüm ağ bölgelerine erişebilirken, bir teknisyen maaş bilgilerine erişememelidir.

Bu politikaları birey ya da bir grup kurar ve yönetir. Bu grubun ağdaki tüm bölgelere erişim yetkileri vardır. Bu yüzden tamamıyla güvenilir ve bilgili kişiler olmaları gerekir. Aksi taktirde, potansiyel bir tehlike oluştururlar.

Eğer kimse bu politikaları anlamaz ve bilmezse, hiçbir işe yaramaz. Varolan politikaları değiştirebilmek, yenileyebilmek ya da ek güvenlik önlemleri alabilmek için etkili bir mekanizma kullanılmalıdır.

Kimlik Teknolojileri

Politikaları kurduktan sonra, kullanıcıları tanımlamak ve erişim yetkilerini belirlemek de güvenlik için çok önemlidir.

Şifreler

Ağ yapıları mutlaka şifre girişli, kontrollü olmalıdır. Ağa sadece kullanıcı adı ile şifresini doğru giren kullanıcılar erişebilmelidir. Fakat insanlar şifrelerini koruyamadıkları sürece ağ güvenliğinden pek söz edilemez. Çoğu kullanıcı doğum günü, telefon numarası gibi basit şifreler kullanır ve hiç değiştirmezler ve de şifrelerini gizli tutmazlar. İyi bir şifreleme yöntemi şöyle olmalıdır:

- *Şifre düzenli aralıklarla değiştirilmelidir,*
- *Şifre mümkün olduğunca anlamsız kelime ya da rakamlardan seçilmelidir,*
- *Çok gerekli olmadığı sürece şifre hiç kimseye söylenmemelidir.*

Dijital Sertifikalar

Dijital sertifikalar, kişi tanımlamaları için kullanılan elektronik ehliyet ya da pasaportlara benzer. Genelde internette güvenlik için tanımlamalarda kullanılır. (VPN'ler gibi)

Erişim Kontrolü

Bir kullanıcı şifresiyle ağa erişmeden önce, şifresinin geçerli olup olmadığı kontrol edilir. Şifresi geçerli ise, erişimin kontrol sunucusu tarafından bu kullanıcının erişim hakları belirlenir. Yani, ağda hangi alanlara girip giremeyeceği belirlenir.

Firewall (Güvenlik Duvarı)

Özel ağ kaynaklarına erişimi kısıtlayarak güvenlik politikalarını uygulayan ağ yapılarında kullanılan, yazılım veya donanım çözümleridir. Kapı kilidine benzetilebilir. Bir odayı sadece anahtarı olan kişilerin açabileceği gibi, ağdaki bir alana da sadece şifresi aracılığıyla erişim hakkına sahip olan kullanıcı girebilir. Firewall dış dünya ile ağ arasındaki koruyucu bir katmandır. İzinli girişler arasındaki bilgi alışverişini herhangi bir gecikmeye maruz bırakmadan yapar. Ayrıca, ağa girmeye çalışan herhangi izinsiz bir materyale karşı filtre görevi yapar, ağa girişe izin vermez. Daha sonra, izinsiz ağa girmeye çalışanları, yöneticiye rapor eder.

Change Management (Değişim Yönetimi)

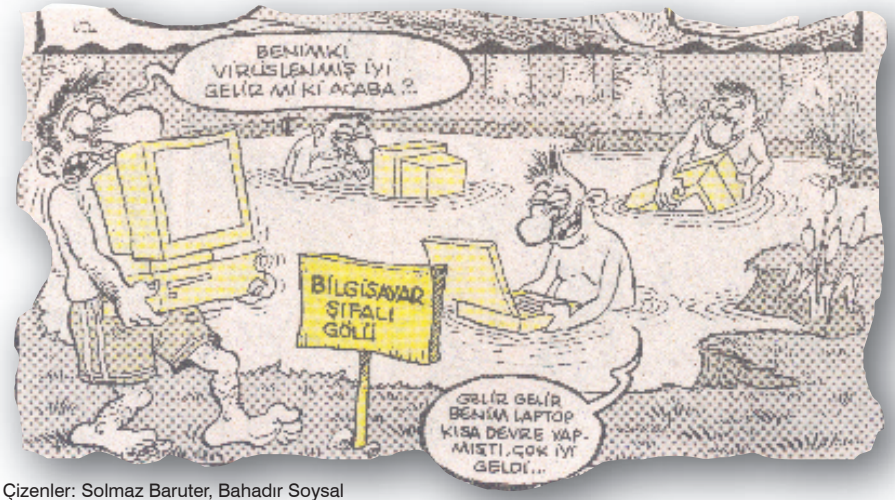
Değişim Yönetimi, ağ operatörleri tarafından geliştirilen yöntemler bütünüdür. Değişim yönetimi yazılımları geliştiren şirketler, ağda değişiklik olduğunda ya da ağın daha verimli olmasına ihtiyaç duyulduğunda, teknisyenler ile onarım sağlarlar. Fakat bu yöntem, genelde güvenlik aracı olarak küçümsenir. Ağ üzerinde yapılan değişiklikler, özel ya da acil change-ticket prosedürlerine bağlı kalınarak yapılmalıdır.

Enkriptolama

Bu teknoloji, mesajların izinsiz bir başka kişi tarafından okunmasını ya da müdahale edilmesini engeller. Bir ağ üzerinden gönderilen bilgiyi korur ve bunun için matematiksel bir algoritma kullanır.

Enkriptolama teknolojisi, VPN teknolojisinin ihtiyacı olan gerekli güvenliği sağlar. VPN, gizli bağlantı sağlayan, internet gibi bir ağ teknolojisidir. VPN bilgi alışverişinin güvenilirliğini Enkriptolama ile sağlar.

Enkriptolama'nın birçok çeşidi vardır. Bunlardan bazıları daha güvenlidir. Amerikan hükümeti, son yıllarda yeni bir Enkriptola-



Çizenler: Solmaz Baruter, Bahadır Soysal
Penguen Mizah Dergisi

ma standardı olan Triple DES ve AES'yi geliştirmiştir. AES temel olarak daha önceki metodolojilerden daha güvenli, daha hızlı ve daha verimlidir. Ve önemli bir avantajı da, maliyetinin düşük olmasıdır.

Saldırı Tespit Sistemleri

Şirketlerin, ağlarına izinsiz girmeye çalışanlar için kullandıkları firewall gibi teknolojiler tek başına pek yeterli sayılmamaktadır. Bu yüzden, riskleri ve güvenlik açıklıklarını azaltmak için Intrusion Detection System (IDS) kullanımı da yaygınlaşmıştır.

IDS, ağı sürekli olarak gözetim altında tutar, ağ içindeki bilgi paketlerini inceler, hacker saldırısı gibi izinsiz girişlerin olup olmadığını kontrol eder ve ağın bozulmasına fırsat vermeden kullanıcıların neden olduğu güvenlik açıklıklarını belirler. İznsiz bir giriş bulduğunda, yönetim konsoluna bir alarm göndererek bu aktiviteyi bildirir ve genellikle router gibi diğer sistemlere izinsiz girişi kesmesi için emir gönderir.

Genel olarak kullanıcı tabanlı ve ağ tabanlı olmak üzere iki çeşit IDS vardır. Kullanıcı tabanlı sistemler, bir sunucuya ya da masaüstüne kurulur ve buradan kütük dosyalarında herhangi bir olay ya da değişiklik olup olmadığını kontrol eder. Genellikle kullanıcıdaki trafiği kontrol eder. Ağ tabanlı IDSler (NIDS) ise ağ trafiğini bir sensör yardımıyla kontrol eder. Bu sensör tüm bilgi paketlerini toplar, paketlerin başlıklarını ve bilginin kendisini, herhangi bir saldırı var mı diye kontrol eder.

Ağ Taraması

Ağ taraması, evden çıktıktan sonra belirli aralıklarla kapı-pencerenin açık olup olmadığını kontrol etmeye benzer. Ağ sistemini sürekli denetler, ağ güvenliğinde herhangi bir açıklık varsa ortaya çıkarır. Riskleri bulmaya ve anlamaya yardımcı olur.

Yönetilebilir Güvenlik Hizmetleri

Ağ güvenliğini öğrenmek ve güvenlik açısından bir adım daha öne geçmek hem zaman alıcı, hem de pahalıdır. Maliyet ve zamandan kazanmak açısından güvenlik risklerini belirleyen firmalardan destek almak mantıklı olacaktır.

Bir de security intelligence service'lar vardır. Bunların farkı, sadece güvenlik açıklarını, riskleri belirlemekle kalmaz, aynı zamanda teknik destek ile güvenliği sağlarlar. 24 saat güvenlik kontrolleri sağlayabilirler.

Diğer Servisler

Ağ Denetimi 24x7x365

Tecrübeli güvenlik mühendisleri tarafından ağın güvenliği sürekli olarak denetlenir.

Firewall Konfigürasyonu/ Kurulum Desteği

Ağa firewall konfigürasyonu ve kurulumu yapılır.

Zayıflık Tespiti (Vulnerability Assessment)

Bir güvenlik çözümü uygulanmadan önce ve sonra, geniş bir zarar, güvenlik açığı tespiti yapılır. Ayrıca belirli aralıklarla yeni bir zayıflık olması durumuna karşı zarar tespit çalışması yapılır.

Aylık Kullanım/Raporlama

Ağ aktivitelerinin takip edilebilmesi için detaylı ve güvenilir bir özet rapor hazırlanır ve güvenlik politikalarını tanımlamada destek sağlanır.

Web Sitesi Filtreleme

Web erişim zamanını ve performansını artırmada yardımcı olur.

Virüs Koruması

Ağa virüs bulaşmasını önler ve varolan virüslerin yayılmasını engeller.

Siber Sigorta

Güvenlik açığından ortaya çıkabilecek kayıplara karşı şirketlerin sigortalanabileceği yeni bir kavramdır. Çoğu şirket müşteri bilgilerine izinsiz erişim nedeniyle bu kayıplara maruz kalmaktadır. Bu nedenle sigortalama işlemi gün geçtikçe yaygınlaşmaktadır. Şirketler herhangi bir kayıp karşısında finansal açıdan ne kadar zarar görebileceklerini hesaplayarak bu miktar üzerinden sigortalanabilirler. Bunu hesaplarken olası tüm riskler ve şirketin büyüklüğü göz önünde bulundurulur. Örneğin, web sitesinden bir müşterinin kredi kartı numarası bir hacker tarafından bulundu ve müşteri bu durumda kaybını şirketten almak hakkına sahip. Eğer şirket bu tür bir duruma karşı sigortalanmışsa, müşterinin kaybını sigorta öder.