

Neden , Ne Kadar Güvenlik ? ve Güvenlik Politikaları

Lisans

Bu döküman **Fatih Özavcı** tarafından yazılmıştır. Güvenliğin gerekliliği , yapılması gereken yatırımın boyutlarını ve bir güvenlik politikasının genel ölçekte nasıl hazırlandığını tartışmak üzere yazılmıştır. Yazarın haklarına saygı duyarak her türlü kaynakta yazılması ve yayınlanması serbesttir.

Neden Güvenlik ?

Hergün birçok şirket teknolojinin ne kadar ilerlediğini görüp bir şekilde bundan faydalanmak ve iş akış süreçlerini hızlandırmak yada revize etmek ister. Bir işletmenin konusu , büyüklüğü ne olursa olsun bugün en az 2-3 bilgisayarı yada farklı bölgelerdeki şubeleriyle haberleşme sistemleri vardır. Şirketler optimum kaynaklarla maksimum verim istediklerine göre de bu durum bir süre sonra kaçınılmaz olur. Bugün şehirlerarası yada uluslararası bir şirket olma kaygısı gütmeyen ayakta kalmak mümkün değildir, bu yüzden olsa gerek , şirketler şube veya merkezlerini bir network ile birleştirmeyi ve telefon, fax, e-posta sistemleri kurarak düşük maliyet ile hız kazanmayı istemektedirler. Tabiki bu durum bazı risklerde içerir. Örneğin telefon maliyetimizi düşürmek için 2 bölge arasında kurduğunuz ağ üzerinden bu işlemi gerçekleştirmeniz durumunda görüşmelerinizi bir çalışanınız sniffer kullanarak yakalaması ve Cisco her ne kadar yasalarla engellemeye çalışsada sesli görüşmelerinizi dinlemesi, stratejik kararlar içeren e-postalarınızın internette elden ele gezmesi, piyasaya çıktığında size milyon dolarlar kazandıracak ürününüzün planlarının bir bilgisayar korsanı tarafından ele geçirilmesi sonrada açıklanması hatta rakibinize yüksek meblağlara satılması gibi riskler sizi bekleyebilir. Ancak ortada bir gerçek vardır. Kimse evine bir hırsızın girmesini, mutfağında bir şeyler yiyip koltuğunda televizyon seyretmesini, giderken de annesinden kalan gerdanlığı götürmesini doğal karşılayamaz. Bu durumda şu soru akılları kurcular; Ne kadar güvenliğe ihtiyacımız var ?

Önce Bütçemizi Belirleyelim

Amerika`da yapılan bazı araştırmalara göre şirketler ortalama olarak karlarının 3`te 1`i kadarını güvenliğe harcamışlardır. Aklınızdan "Benim sadece bir sitem var ve onuda sadece müşterilerim sorduğunda var diyebilmek için yayına soktum." gibi bir düşünce geçiyorsa müşterileriniz yeni hazırladığınız ürününüzü görmek için sayfanıza geldiğinde bir kaç huri resmi yada acelece yazıldığı her halinden belli küfürlerle karşılaştığında ne hissettiklerini düşünün. Demek ki kayıp her zaman maddi olmuyor, prestijde kaybedilebiliyor. Bu yazıda bahsi geçen her olay dünyanın çeşitli yerlerinde ki şirketlerin başından geçmiştir, çoğu sabah uyandığında sayfasının yeni halini görmüş ve sizinde tahmin edeceğiniz gibi biraz kızmışlardır. Sizde onların sayfalarını ve muhtemel başınıza gelebilecekleri öğrenmek isterseniz *Security Space* sitesinin arşivler bölümüne bir uğrayın. Şimdi "Ne harcamalıyım da böyle durumlar başıma gelmesin" diyorsanız (ki bu artık aynı dili konuştuğumuz anlamına gelir) kaybedeceğimiz şeyleri düşünün ve sonra da 2 ile çarpın böylece harcamanız gereken tutarı buldunuz. Neden 2 ile çarptık dersiniz en kötüyü düşünmek yaşamaktan farklıdır derim. Peki bütçemize karar verdiğimizize göre bu bütçeyi hangi stratejik bölümlere aktaracağız ?

Nerelerde Güvenliğe İhtiyacımız Var ?

Neler yaptığımızı ve şirketimizin bilgi sistemleri altyapısını nasıl oluşturduğumuzu bilirsek almamız gereken önlemleride düzenli olarak saptama imkanımız olmaktadır. Şirketiniz şubeleri yada müşterileriyle özel olarak haberleşmek için sanal bir çalışma ağı kurmak istiyor mu ? yada Böyle bir ağa sahip mi ? Önemli yazışmaları e-posta yoluyla gönderiyormusunuz ? Çalışanların internette göntüllerince gezmesine , ICQ , IRC ve e-posta yoluyla arkadaşlarıyla haberleşmesine ne oranda izin veriyorsunuz ? Bir web sayfanız , şirket e-postalarınız için bünyenizde bulundurduğunuz bir posta sunucunuz var mı ? Önemli çalışmalarınızı kaydettiğiniz bir veritabanı sunucunuz var mı ? Bazı önemli görüşmelerinizi sesli yada videolu olarak internet üzerinden yapıyormusunuz ? Peki sektörünüzde ismini çok duyurmuş bir şirketmişiniz ? Bu sorulardan birine bile cevabınız evet ise saldırı altındasınız ve aramıza hoş geldiniz. Sizin bugün kendinize sorduğunuz soruların çoğu daha önce birileri tarafından cevaplandı, tek yapacağınız bu cevaplardan uygun olanları seçmek :

- Müşterilerinizi yada merkezlerinizi internet üzerinden birleştirmek istiyorsunuz ama güvenli olsun diyorsunuz ; VPN (Virtual Private Network - Sanal Özel Ağ) çözümleri kullanmalısınız.
- Önemli yazışmalarınızı e-posta ile yapıyorsunuz , sadece göndereceğim kişi okusun diyorsunuz ; e-maillerinizi PGP ile şifrelemelisiniz.
- Çalışanlarınızın istemediğiniz sayfalara girdiğini görmek istemiyorsunuz ve bu şekilde ağ trafiğinizi arttırmalarını istemiyorsunuz ; Content Filter (İçerik Kontrol) çözümleri kullanmalısınız.

- Ağınıza istemediğiniz kimselerin girmesini istemiyorsunuz, çalışanlarınızın da internette sizin izniniz olmayan hizmetlerden yararlanmasını istemiyorsunuz ; Firewall çözümleri kullanmalısınız.
- Web sayfanız var , Posta sunucunuz var , Veritabanı Sunucunuz var ve bunları korumak istiyorsunuz ; Firewall kullanmanız yeterli değil, tüm yazılımları elden geçirmeli , yamalarınızı güncel olarak takip etmeli ve uygulamalısınız.
- Ağınızın toplam güvenlik bütünlüğünü belirlemek ve bu şekilde ağınızda olası tehlikeleri saptamak istiyorsunuz ; Firewall , sunucularınız ve ağınızın tamamının güvenliğinin devamlılığını görmek istiyorsunuz ; otomatik açık tarama araçlarını kullanmalı ve düzenli olarak ağınızı elden geçirmelisiniz.
- Önemli görüşmelerinizi internette yapıyorsunuz ve güvenli olsun diyorsunuz; VPN çözümleri kullanmalısınız hatta bu görüşmeleri şifreli yapan programları kullanmalısınız.
- Size kimlerin saldırdığını görmek istiyorsunuz, saldırıların içeriden mi dışarıdan mı geldiğini belirlemek istiyorsunuz ; IDS (Intrusion Detection System - Saldırı Tespit Sistemi) çözümlerini kullanmalısınız.
- Siz ve çalışanlarınıza hergün yüzlerce mail geliyor, ayrıca çalışanlarınız her ay dergilerden programlar bulup bilgisayarlarına yüklüyor virus bulaşırsa diyorsunuz ; Anti-Virtüs sistemleri kurmalı düzenli güncellemeli ve ağınızın tamamını incelemelere dahil etmelisiniz.
- Çalışanlarınızın bir kısmına notebook verdiniz , dışarıdan da çalışmalarına devam ediyorlar ve sizin ağınıza girerek çeşitli görevlerini yerine getiriyorlar ; kesinlikle VPN kullanmalı mümkünse RADIUS, SecureID ve Tokenlar gibi harici onaylama sistemleri kullanmalısınız. Ayrıca çalışanlarınızın sistemine girebilecek kişilerin sizin sisteminize sızabileceğini düşünerek kişisel güvenlik ürünlerinin de kullanımı tavsiye edilir.
- Ağınızda ve sunucularınızda neler olduğunu düzenli görmek, yöneticilerinizin neler yaptığını bilmek istiyorsunuz ; Raporlama yazılımları kullanmalısınız ve bu raporları düzenli olarak inceleyecek kişileri görevlendirmelisiniz.
- Şirketinizde kötü niyetli insanlar var mı ? ağınıza zarar verir mi ? ağınız gereksiz trafiklerle meşgul ediliyor mu ? görmek istiyorsunuz ; Sniffer kullanmalısınız.

Şimdi ise hepsinden önemli bir sorumuz var , ve bu soru ilk cevaplanması gereken sorudur : "Bir Güvenlik Politikamız Var mı ?"

Peki niçin bu en önemli soruyu en son sorduk ; çünkü bu sorunun cevabını ararken yukarıdaki cevapları kullanacak ve hangilerine ihtiyacım var sorularının cevaplarını inceleyeceğiz. İçlerinde olmazsa olmaz ürünler olduğu gibi sizinle hiç ilgisi olmayan ürünlerde vardır. Aşağıda bahsi geçecek ürünler sizin güvenliğiniz için saldırganların önüne bir zincir çıkarırlar ; ancak unutmayın ki bir zincir en zayıf halkası kadar güçlüdür. O yüzden sistem güvenliğinizi bir bütün olarak düşünmelisiniz. Sadece bir Firewall kurmak ve yönetimiyle hiç ilgilenmemek yada güncellemediğiniz bir anti-virus sistemi kurmak güvende olduğunuz yanılsamayı yaratmaktan farklı bir işe yaramaz. Dolayısıyla ilgilenmediğiniz ürünlere 100.000 \$ yatırım yapmak pek de mantıklı değildir. Şimdi güvenlik politikamızı üzerine kuracağımız bileşenlerimizi tek tek inceleyelim ve önem sırasına göre dizelim.

Güvenlik Politikasının Bileşenleri

Firewall : Bir kişisel kullanıcı da olsanız, küçük bir şirkette olsanız , dünyada söz sahibi bir şirkette olsanız tüm bilgisayarlarınızın korunması için en temel şarttır. Ücretsiz olan Firewall' lardan 100.000 \$ gibi rakamlara ulaşan çözümler ve geniş bir yelpaze mevcuttur. Ama kesinlikle ucuz olan Firewall kötü , pahalı olan Firewall ise iyidir gibi bir yaklaşıma girmemelisiniz, çünkü iki tarafında içinde aksini kanıtlayabilecek oranda istisna mevcuttur.

Burada esas önemli olanlar Firewall' un mimarisi , kullanım zorluğu , performansı ve fiyatıdır. Genel olarak 2 tür Firewall piyasada bulunmaktadır ; Application Proxy seviyesinde çalışan Firewall' lar ve Stateful Inspection olarak çalışan Firewall' lar. Arada hybrid denilen ve ikisininide destekleyen Firewall' larda vardır. Application Proxy olanlar gelen paketlerin içeriye gitmesine izin vermez ve o paketi alarak, içeriye kendisi gönderir. Böylece paketlere daha çok müdahale şansı kazanırsınız. Stateful Inspection Firewall' lar ise paketlerin hedeflerine ulaşip cevapların dönüşüne kadar her durumunu izler ancak paketlerin içeriğine bakmaz. Yoğun olmayan ağlarda Proxy Firewall' lar tercih edilmektedir , yoğun ağlarda ise Stateful Firewall' lar tavsiye edilir, çünkü Proxy Firewall' lar doğası gereği bir miktar yavaş çalışmaktadırlar.

Kullanım kolaylıkları da seçim konusunda önemli bir etkidir. Örneğin her pakete yeterince müdahale şansımızın olup olmadığı ve bunun ne kadar kolay bir ortamdan yapıldığı gibi. Kullanımı kolay Firewall' larda yöneticinin uzmanlık seviyesi fazla önem arzetmezken , kullanımı zor olan Firewall' lar gerçekten işinin ehli insanlar isterler. Zorluk ile gelen/giden paketlere müdahale ve yönetim gücü doğru orantılıdır. Genelde sisteminizin yapısı ve önemi gereği en az 1 yada 2 adet Firewall yöneticisi bulundurarak sisteminizi güvenli hale getirebilirsiniz.

Anti-Virüs Sistemleri : Anti-Virüs sistemleri çoğu kişi tarafından önemsenmezler ; ancak bugün herkesi şaşırtacak oranda gelişmiş virüs yapıları ve zeka seviyeleri karşısında onları önemsemeyen kişileri attıkları çılgınlarla farkedebilirsiniz. Güvenliğin en önemli parçalarındandır. 3 açıdan stratejiktir;

- 1. Kullanıcılarınızın hepsinin bilgisayarına yüklenmeli
- 2. Firewall'unuz ile uyum içerisinde çalışabilmeli, ftp, http, smtp gibi protokollerde gönderilen dosyaları inceleyebilmeli ve bu işlemler sırasında hızlı olabilmeli
- 3. Posta sunucunuzda çalışabilmeli ve gelen-giden e-posta trafiğinizi incelemeli, performans kaybı yaratmamalıdır.

Bütün bunlara ek olarak düzenli güncellenebilirliği , bütün bu işlemlerin tek bir arabirim aracılığıyla yapılabilmesi , otomatize edilebilirliği bir anti-virüs sistemini öne çıkaran diğer etkenlerdir. Fiyat olarak hepsi birbirine yakındır, yukarıdaki kriterler onları öne çıkarır. Genelde bütün bunları takip edebilecek bir yönetici olması şarttır; ancak fazlası gerekli değildir.

IDS-Saldırı Tespit Sistemleri : Sisteminizin ne şekilde saldırılara maruz kaldığını ve bunların ne ölçüde engellenebilir olduğunu görmeni sağlar. Çok çeşitli şekillerde çalışanları , değişik fiyat yelpazesinde olanları vardır. Genelde Sunucu Tabanlı ve Ağ Tabanlı olarak ikiye ayrılırlar, Özel bir uygulama için geliştirilmiş olanları da mevcuttur. Sunucu tabanlı çalışanlar yardımcıların yüklendiği bilgisayarları kontrol ederler. Ağ tabanlı olanlar ise tüm ağınızdaki dinler ve saldırı işaretleri yakaladığı hareketleri size raporlar. Her ikisinde de tek konsoldan yönetilebilmesi tercih sebebidir.

Host tabanlı olanlar genelde 5 yardımcı lisansıyla gelirler daha fazlası ayrıca talep edilir. Her yardımcı sizin önemli bir sunucunuza yüklenir (Posta , Web , Veritabanı sunucuları gibi) ve bu sistemdeki sizin belirlediğiniz dosya yada hareketleri izler, gerekirse müdahale edebilir. En önemli seçim yardımcılarının tüm sunucularınıza yüklenmesi ve eşit kriterlerde güvenliği garanti edebilir olmasıdır. Ağ tabanlı sistemler ise ağınızdaki olası saldırıları dinler , gerekirse bağlantıları keser hatta Firewall yada Router'ınızda bu durum için değişiklikler yapabilir. En az 2 noktayı dinleyebilmelidir.

- 1) Firewall ile internete giden Router arasındaki trafik
- 2) Yerel ağınızdaki trafik Host tabanlı sistemler ile Ağ tabanlı sistemlerin tek bir arabirimden kontrol edilebilirliği önemlidir. Ayrıca ölçeklenebilir olması , yani daha sonra eklenecek sunucularınıza yüklenmesi , eklemek yeni ağlardaki performansı ve bunların ortaya çıkaracağı maliyet kararın aşamalarındandır. Ücretsiz olan IDS'lerde yeterince kullanışlıdır ama ciddi olarak uzmanlık gerektirmektedirler.

Bu konuda maddi yatırım yapmak istemiyor olsanız bile en azından bir ücretsiz IDS yükleyerek sisteminizde neler olup bittiğine bakmalıyız, böylece alakasızca insanların size saldırdığını gördüğünüzde belki fikriniz değişebilir. IDS'lerle ilgili bir önemli noktada tutulacak kayıtların korunması, sürekli incelenmesi, raporlanması ve gerekli önlemlerin alınmasıdır. En az 1 kişi yönetim için bulunmalıdır. Mümkün ise 2 kişi sorumlu olmalı ve 2. kişi düzenli olarak raporları incelemelidir.

VPN-Sanal Özel Ağ : İki ağın yada 2 sistemin arasındaki veri trafiğinin bir sniffer ile dinlenememesi için trafiği şifreleyen ve internet gibi güvenilmeyen bölgeden bile güvenilir veri akışı sağlayan sistemlerdir. Farklı platformlarda, donanım yada yazılım olarak yapılabilir ; önemli olan hızı mümkün olduğunca az etkilemesi , desteklenen şifreleme standartları, performans ve lisans ücretleridir. Loglarının düzenli olarak incelenmesi gerekir. Ayrıca veriyi şifrelerken aslında girilebilecek bir kapı da açtığından harici onaylama yöntemleri (RADIUS, SecureID gibi) kullanılabilir.

İçerik Filtreleme Yazılımları : Çalışanlarınızın internetten yeterince faydalanması bazen iş verimini düşürmektedir. Bazen girilmesini istemediğiniz, şiddet , sex, oyun ve siyaset sitelerini engellemek isteyebilirsiniz. Bu durumda içerik filtreleme yazılımları kullanılmalıdır. Genelde bir veritabanı tutup sürekli güncelleyerek size geniş bir seçim yelpazesi sunar. Seçimlidir, gerekliliği tartışılabilir, belirleyici olan unsurları lisans bedelleridir.

Otomatik Açık Tarayıcılar : Ağınızdaki tüm bilgisayarların güvenliğini kontrol etmek ve kullanıcıların yada sunucuların güncel açıklarını taramak istiyorsanız kullanışlıdır. NAI'in CyberCOP'u , ISS'in Internet Scanner'i ve Axent'in Netrecon'i öne çıkanlardır. Ücretsiz kullanılabilen Nessus, Saint ve Sara gibi alternatifler de mevcuttur. Belirleyici unsurları güvenlik açıklarını takip etme hızı , mevcut güvenlik açığı veri tabanlarının büyüklüğü, rapor mekanizmaları ve lisans bedelleridir. Düzenli olarak çalıştırılan bir tarayıcı ile sürekli olarak olası riskleri takip edebilirsiniz.

Ağ İzleme Araçları : Ağınızdaki neler olduğunu anlamak için çeşitli programlar kullanmalısınız. Trafiğin ağırlıklı bölümünü hangi servislerin kullandığı , elemanlarınızın önemli dökümanları şifreleyerek gönderip göndermediği ve içerideki elemanlarınızın ağı meşgul eden saldırılar yada bilinçsiz kullanımlar yapıp yapmadığını görmek için sniffer denilen bu programlar kullanılır. Genelde sorun giderme amaçlı kullanılır. En ünlüsü NAI'in Sniffer ürünüdür. Seçimlidir; ancak ağ yöneticilerinin en temel yardımcılardır.

Raporlama Araçları : IDS , Otomatik Açık Tarayıcıları , VPN , Sniffer ve Firewall'ların loglarını daha anlaşılır kılarlar. Düzenli raporlar ile ihtiyacınız olan bilgileri saptayıp tüm logları incelemenizi engellerler. Genelde yöneticilerin önemli yardımcılarındandır. Webtrends ve Crystal Reports en ünlüleridir. Logları düzenli incelenmeyen IDS ve Firewall'lar ancak sizi %20 koruyabilir, esas amaç olan sistematik saldırıları ancak tutulan kayıtlardan farkedebilirsiniz.

PGP : NAI'nin en ünlü ürünlerindedir. Tüm posta ve dosya transferlerini şifreli olarak yapar sadece gönderdiğiniz kişideki anahtar bu şifreleri açabilir. Her işletim sistemi için ve neredeyse her posta programı için sürümleri mevcuttur. Ticari, Ticari olmayan ve Açık kodlu versiyonları mevcuttur. <http://www.pgpi.com> adresinden indirilebilir ve daha detaylı bilgi alınabilir.

Kişisel Güvenlik Yazılımları : Eğer ağınıza dışarıdan bağlanan kullanıcılarınız varsa onların güvenliği diğer yazılımlarınızın sağladığı güvenlik kadar önemlidir. Onların bilgisayarlarını ele geçiren kişiler sizin ağınıza sızmak için kapı bulmuş olurlar. Bu yüzden bu kullanıcılarınızın bilgisayarlarında da , kişisel Firewall , anti-virüs , vpn , pgp , secureid yada tokenlar gibi güvenlik çözümleri gerektiği oranda kullanılmalıdır.

Bu ürünlerin mantıklı olması gereken harcama oranlarında önemlidir. 5 bilgisayarlı ağınıza için 50.000 \$ lik bir Firewall almak ve 2 güvenlik uzmanını bu işe yöneltmek yanlış olur. Dünya üzerinde pek çok şirket ücretsiz güvenlik programları ve önlemleri ile güvenlik seviyelerini %95 seviyesine çekmektedirler. En çok maliyet üreten Firewall , IDS, güvenlik açığı tarayıcıları, VPN ve anti-virus gibi sistemlerin her birinin pahalı olanları kadar başarılı ücretsiz alternatifleri de bulunmaktadır. Ancak sonuçta önce bu ücretsiz güvenlik ürünlerini bulmalısınız, daha sonra kullanımlarını öğrenmeli ve size özel çözümler üretmelisiniz. Bu da uzman güvenlik yöneticileri gerektirmektedir. Açıkçası bana programlardan bilgili sistem ve güvenlik yöneticilerine yatırım yapmak daha mantıklı gelmektedir. Sonuçta kullanımı kolay ve ücretli bir web server olan IIS (Ücreti alındığı işletim sistemine dahildir.) 2 senede en çok açığı çıkan hatta sisteme direk erişim veren bir program iken , Apache kısmen daha zor yönetilebilen ama çok daha güvenli ve ücretsiz bir programdır. Ama sadece Windows kullanabilen bir sistem yöneticisine Apache, Roxen gibi alternatifler var demek sadece tepki almaya yarar, bu durumda elindeki sistemi nasıl güçlendirebileceğini anlatmak daha faydalı çözümler çıkarabilir. Demek ki öncelik yetmişmiş işgücü veya dış kaynak kullanımından geçmektedir.

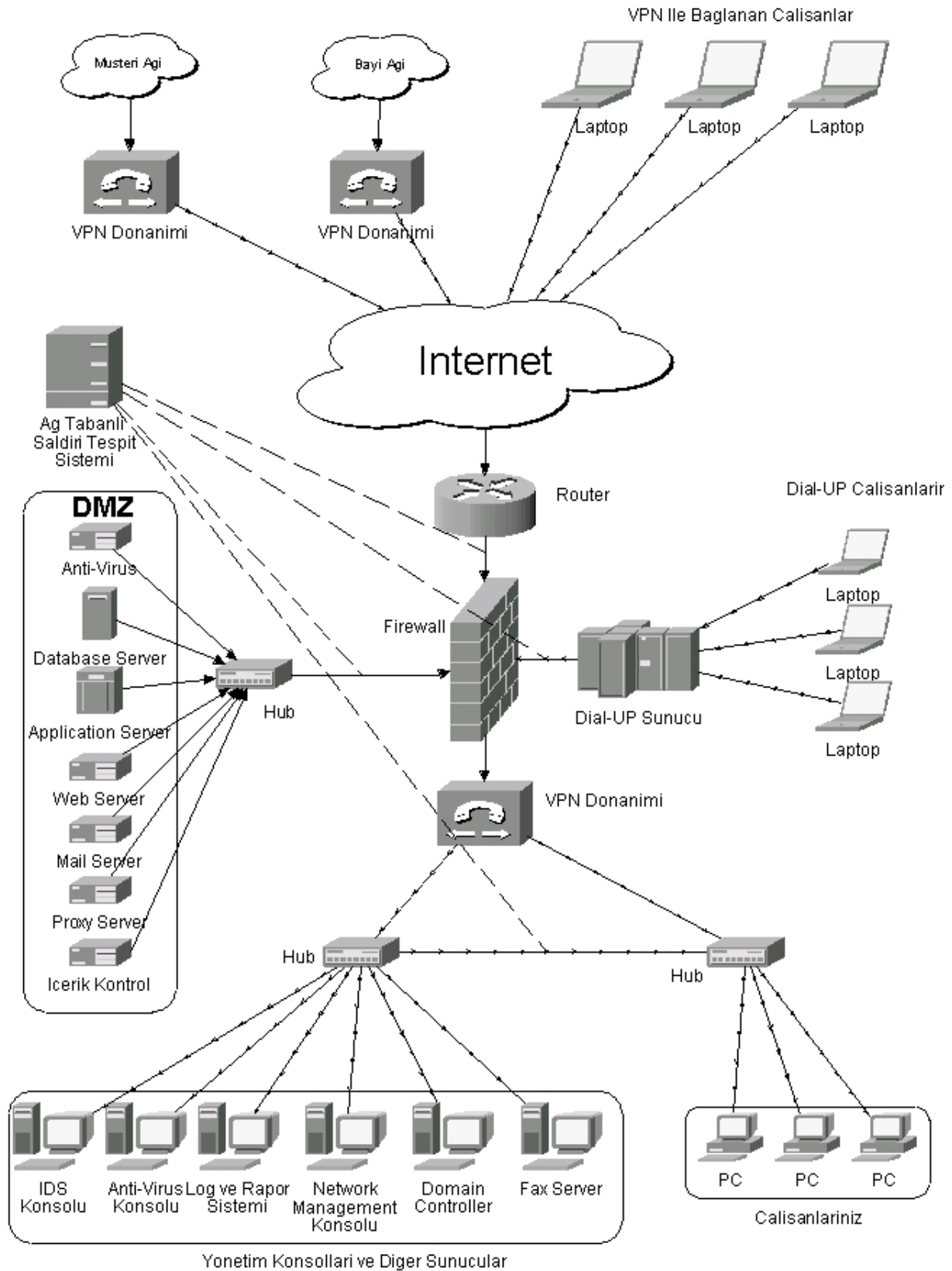
Bütün bu işlemleri yaptıktan sonra da sisteminizi Penetration Test dediğimiz sistem güvenliğinizi zorlayacak testlerle incelemeniz ve size saldırıların izleyebilecekleri muhtemel yolları görmeniz gerekmektedir. Artık güvenlik politikamızı oluşturabiliriz.

Güvenlik Politikası Oluşturmak

Burada oluşturulacak güvenlik politikası mümkün olduğunca basit ve genel tutulmaktadır. Siz kendi deneyimleriniz, elinizdeki imkanlar ve bilginiz çerçevesinde size özel çözümleri bu dökümandan yola çıkarak oluşturabilirsiniz. Önce güvenli bir ağ altyapısı hazırlamalıyız. Daha sonra elimizdeki ürünleri gerekli noktalara yerleştirmeliyiz. Güvenli bir ağ yapısı oluşturarak politikamıza başlayalım.

- Öncelikle çalışanlarınıza, müşterilerinize ve internetteki potansiyel ziyaretçilerinize ne tür servisler vereceğinizi belirlemelisiniz. Şirketiniz bünyesinde Posta , Web , Veritabanı , Alan Adı Sunucuları ve Alan Denetçileri (Domain Controller) bulundurup bulundurmayaçağınıza karar vermelisiniz. Uygulama sunucusu ve Terminal sunucusu kullanılıp kullanılmayacağı da önemli bir etkidir. Bu sunucularda maliyet/güvenlik oranına uygun uygulamalar kullanarak başlamalısınız. Örneğin Posta sunucusu olarak Posix (Linux, *BSD, *nix sistemler) üzerinde çalışan Qmail sunucusu sizin için iyi bir alternatiftir. Hatta Yahoo ve Hotmail bile bu sistemle çalışmışlardır. Web sunucusu olarak ise tercihinizi Apache'den kullanmanızı öneririm, çünkü güvenliği , performansı ve ücretsiz olması çok ciddi artılarındandır. Mümkün ise Web sunucunuzda Posix tabanlı bir sistem olarak seçmelisiniz. Veritabanı sunucusu olarak MySQL iyi bir performans sergilemektedir. Alan Adı sunucunuz güvenlik açısından sizin önemli parçalarınızındandır, mümkün ise DNS sunucunuzun çokça açığı bulunan Microsoft DNS yada BIND yerine DjbdNS gibi güvenliğiyle öne çıkan ücretsiz bir ürün olmalıdır. Alan Denetçisi olarak ise Novel ve NDS yapısı , Microsoft ile Active Directory yapısı , Posix bir sistem ile Samba yada NIS yapısı sizin için bir alternatiftir. Bu yapılar içinde hepsinin kendine göre güvenlik sakıncaları vardır ; ancak gerek yerel ağınıza kullanılacak olması gereksede tüm ağınıza güvenlik ile ilgili yönetimini tek bir arabirimden yapabilecek olması sizin için gerekliliğini ortaya koyar. Seçimi iyi kullanabildiğiniz sistemden yapmanız önerilir. Terminal sunucularınız ve uygulama sunucularınız amaçlarınız doğrultusunda şekillenecek bir işletim sistemi uygulama ikilisi yaratacaktır.

- Tüm sunucularınız üzerinde bildiğiniz sistemleri kullanmanız tercih edilmelidir. Tanıdığınız bir Windows işletim sisteminde yapabileceğiniz güvenlik ayarları onu standart kurulmuş bir Linux'a göre daha güvenli yapabilir. Posix sistemlerin en büyük avantajı sistem çekirlerinde dahi değişiklik yapılabilir olması , uygulamaların çoğunun açık kodlu olması sebebiyle kodundan gerekli güvenlik önlemlerinin alınabilmesi, yönetimini sağlayan kişilerin genellikle üst düzey uzmanlık seviyesinde olmalarıdır. Eğer bu tür bir sistem üzerinde bilginiz yok ve eğitim almak gibi bir düşünceniz varsa en azından bu süre zarfında bildiğiniz işletim sistemlerini tercih etmelisiniz ; çünkü uygulamalarınızı ve işletim sistemlerinizi zayıf hale getiren açıkların en büyüğü varsayılan kurulumla devam etmektir.
- İşletim sistemleriniz ve uygulamalarınız üzerindeki servislerden işinize yaramayan yada bilmediğiniz servisleri tamamen kapatın. Çünkü bilinmeyen yada kullanılmayan servisler saldırganların genelde bildikleri ve kullandıkları servislerdir. Bu ayrıntı onlara ciddi bir avantaj kazandırmaktadır. Bu avantajı lehinize çevirebilmenin en önemli yolu bildiğiniz ve kullandığınız servislerin dışındaki tüm servisleri kapatmaktır.
- Ağınızda switch'li bir yapıyı tercih etmelisiniz, gerçi günümüzde artık her yapı switch'ler üzerine inşa edilmektedir ama ciddi bir ayrıntıdır. Günümüzde sniffer aracılığıyla switch'li ağlarda dinlenebilmektedir ve bu konuyla ilgili önlemlerde almanız gerekmektedir, ancak tüm switch'li ağı dinlemek ancak port kopyalama dediğimiz ayarların switch'ler üzerinden yapılmasıyla olabilir. Switch'li ağların güvenliğiyle ilgili olarak *Sniffer ve Switch'li Ağların Güvenliği* yazımızı okuyabilirsiniz.
- Sunucularınızdan stratejik önem içerenleri mutlak suretle DMZ (DeMilitarize Zone-Yarı Güvenlikli Bölge) bölümüne aktarmanız ve Firewall üzerinden yerel ağ ve internet ile iletişimini gerekli olanlar dışında kesmelisiniz.
- Ağınızda farklı bölümler farklı ağları temsil etmeli ve bu ağların arasındaki iletişim, yetkiler oranında gerçekleşmelidir. Böylece yetkisiz kötü niyet kullanımını önlemiş olursunuz. Bu ağları Firewall aracılığıyla kontrol ederek aralarında tam bir yalıtım sağlamalı ve gereklilikler dışında iletişim kurulamamalıdır. Unutmayın ağınızda gereksiz yada tehlikeli hiçbir trafik akmamalıdır.
- Bir dikkat edilmesi gereken nokta da dışarıdan çalışanlarınızın , müşterilerinizin , bayilerinizin ağınıza ulaşımının sürekli izlenmesi ; bu girişlerin ve veri akışının güvenli bir şekilde gerçekleşmesi ve haklarında gereklilikler üzerinde olmamasıdır. Unutmayın ki çalışanlarınız, müşterileriniz yada bayileriniz içinde kötü niyetli kişiler olabileceği gibi onların sistemlerine giren bir saldırganda onlarla aynı haklara sahip olacaktır.
- Çalışanlarınızın ICQ, IRC, Napster gibi programlar kullanmasına izin verip vermeyeceğinizde ciddi bir güvenlik sorunudur. Bu sistemlerdeki açıklar o kişilerin çalışanlarınızın bilgisayarlarına sızabilmesini sağlamaktadır ve içeride bu şekilde kontrolü ele geçirilmiş bir bilgisayar artık Firewall'larınızın da arkasında durmaktadır ve durdurabileceğiniz tek sistem sadece IDS'lerinizdir ki onlarda bazı durumlarda çaresiz kalmaktadırlar. Ayrıca bu programların yaratacağı trafikte küçümsenmemelidir, özellikle ICQ yarattığı oturum sayısı ile ağınızda ciddi bir yavaşlamaya sebep olabilir.
- Posta sunucunuzun ve Alan Adı sunucunuzun içeride olması size pek çok avantaj sağlayacaktır. Çalışanlarınızın sistemleri herhangi bir isim sorgulaması için internete çıkmayacak sadece o sunucuya gideceklerdir, böylece bu hizmeti Firewall üzerinden sadece sunucuya ve oda içeriden dışarıya olmak üzere açabilirsiniz, bu da size ciddi bir güvenlik artışı sağlar. Mail sunucunuz için ise durum biraz daha farklıdır ; çalışanlarınızın e-maillerini sizin sunucunuz aracılığıyla alması tüm e-maillerin kontrol edilebilmesine , virüs taramasından geçirilebilmesine olanak tanır ve böylece yalıtılmış bir ortam sağlanmış olur.
- Kullanıcılarınızın hakları gerekli olan kaynaklara, yazıcılara, veritabanlarına ulaşabilecek seviyeden yukarı olmamalıdır. Şifre kurallarınızı (En az 8 karakterli şifre olsun, ayda bir değiştirilsin gibi) ve çalışanlarınızın haklarını bir güvenlik poliçesi ile kullandığınız Alan Denetçileri aracılığıyla tüm sistemlere ulaştırmalısınız.
- Ağınızda DMZ'de bulunacak bir önbellek yazılımı ile HTTP ve FTP isteklerini filtrelemeli, çalışanlarınız sadece o sistemden sayfaları çağırabilmeli ve dışarıya sadece o sistem çıkabilmeli. Böylece HTTP ve FTP isteklerini de tek bir sistemde toplayarak ve o sisteme de sadece içeriden dışarıya çıkış izni vererek birçok saldırıyı engellemiş oluruz.
- Bir anti-virüs politikası oluşturmalısınız ; sürekli güncellemeleri takip etmeli , tüm kullanıcılarınızda , posta sunucularınızda yüklü olmasını ve gerekli olan tüm trafiği izlemesini sağlamalısınız. Ağınızdaki Truva Atı, Virüs gibi zararlı programlar en büyük tehlikelerdendir, çok çabuk yayılır ve ağınıza büyük ölçüde zararlar verebilir.
- Ağınıza yapılan tüm saldırıları izlemeli , raporlamalı ve önlemler almalısınız. Firewall , IDS gibi programların tuttıkları kayıtlar sizin için hayati öneme sahiptir.
- Tüm önemli sunucularınız için yıkımdan kurtarma planları yapmalısınız, düzenli yedekler almalı ve bu yedekleri kontrol etmelisiniz. Tüm sistemlerinizin zarar gördüğü durumda yedeklerinizin işe yaramadığını görmek kabus gibi bir durumdur.
- Bir saldırı altında olduğunuzda yada bir saldırı başarılı olduğunda neler yapacağınıza önceden karar vermeli ve düzenli olarak sistemlerinize saldırılar yaparak kontrol etmelisiniz.
- Düzenli olarak otomatik güvenlik tarayıcıları kullanarak ağınıza elden geçirmeli, güncel açıkları aramalı ve zayıf noktaları saptamalısınız. Bu güvenlik tarayıcılarını düzenli olarak güncellemenizdir.
- Stratejik sunucularınız hardenning denilen işletim sistemi ve uygulamanın güçlendirilmesi işleminden geçmiş olmalıdır. Tüm açıkları kapatılmış, tüm yamalar yapılmış ve diğer önlemler alınmış olmalıdır.



Bütün bu bileşenler elimizde olduğuna göre artık ağımızın da yapısını çizmeliyiz. Böylece stratejik noktaları daha iyi görebiliriz. Şeklimizde genel olarak hazırlanmış bir güvenli ağ yapısı görünmektedir ; ancak bu yapıyı kendi sistemlerinizde birebir uygulamak yerine kendinize göre özelleştirmeniz ve bütçenize göre düzenlemeniz gerekmektedir.

Tüm yerel ağdaki sistemlerinizde ve uzaktan bağlanan çalışanlarınızda anti-virüs yüklü olmalıdır. Uzaktan bağlanan kullanıcılarınızda ve Dial-Up ile size bağlanan çalışanlarınızda Token, SecureID , Kişisel Firewall ve VPN İstemcilerinden gerekenler yüklü olmalıdır. Müşteri ve bayilerinizin ağlarını VPN donanımlarıyla ağınıza ulaştırmalı ve kontrolü bu donanımların seri numaraları ile yapmalısınız. Ayrıca o ağlardan ve uzaktaki kullanıcılarınızdan gelebilecek olası tehlikelere karşı erişim hakları gereklilikler ölçüğünde kısıtlanmış olmalıdır. DMZ ile ağımızdaki tüm önemli sistemlerde HIDS (Sunucu Tabanlı Saldırı Tespit Sistemi) yüklü olmalıdır. DMZ ile ağınız arasındaki trafik gereklilikler ölçüsünde sınırlandırılmalı. Firewall tüm bu iletişimi kaldırabilecek oranda güçlü olmalı. NIDS (Ağ Tabanlı Saldırı Tespit Sistemi) ise Router ve Firewall arasını, Yerel ağ ve Dial-Up arasını, Yerel ağınızı ve DMZ bölümlerini aynı anda dinleyebilmelidir.

Sonuç

Sonuç olarak ağımızın performanslı ve güvenli olması için politikalarınız, kurtarma planlarınız ve tasarımınız mükemmel yakın olmalıdır. Bu bileşenleri mutlak suretle yakınınızda ulaşabileceğiniz yerlerde buldurmalısınız. Bütün bu işlemleri adım adım yaptığımızı göre şimdide gerçek bir saldırganın neler yapabileceğini düşünmelisiniz, böylece göremediğiniz riskleri de yakalamış olursunuz. Bunun için Penetration Testleri yaptırmanız , böylece göremediğiniz risklerde ortaya çıkmış olur. Düzenli olarak güvenlik zayıflıklarını yayınlayan listelerini takip etmeli , kullandığınız sistemleri güncel tutmalısınız. Bunların bir kısmını çalışanlarınıza bir kısmında dış kaynak yoluyla yaptırıp gerçekten %99 güvenli bir ağa kavuşabilirsiniz. Güvenlik önemlidir, düşük maliyetlede sahip olunabilir, bu yüzden gerekli önlemleri almayı asla küçümsemeyin.