BİR KURULUŞUN BİLGİ SİSTEMİ GÜVENLİĞİ İÇİN BİR YAKLAŞIM

Hakan TAN | Bilgisayar Mühendisi
hakan.tan@barikat.com.tr

Ziya AKTAŞ | Başkent Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı
zaktas@baskent.edu.tr

Özetçe

Bilgisayar Mühendisliği alanındaki teknolojik gelişmeler bilgi sistemleri üzerinde işlenen ve paylaşılan bilginin boyutunu hızla artırmaktadır. Kamu kurum ve kuruluşları bu gelişmeleri takip ederek bilgi sistemleri sayılarını arttırmakta; temel görevlerini diğer kamu kurum ve kuruluşları ile bilgi paylaşım esasına göre bu sistemlerin üzerinde sürdürmekte ve vatandaşlara sunmaktadır. Özel sektörde de durum pek farklı değildir. Internet bankacılığı ile başlayan hizmetler bankacılık dışında hizmet veren firmaların artması ve güçlenmesi ile internet üzerinden her gün daha fazla kişi tarafından kullanılmaktadır. Bu trendin devam etmesi beklenmektedir. Bu nedenle bilgi sistemleri üzerindeki bilginin güvenliği ve hizmetlere erişilebilirlik bu hizmetleri veren kamu ve özel kurum ve kuruluşları için önem verilmesi gereken bir konu olmaktadır. Bu çalışmanın amacı bilgi sistemleri güvenliği kavramının araştırılarak sınırlarının tanımlanması ve mantıksal güvenlik alanında yararlı olabilecek güvenlik yazılımlarının kurum ve kuruluşlar tarafından nasıl kullanılabileceğinin özetlenmesidir.

Giriş

Çok sayıda kullanıcısı olan kamu ve özel kuruluşların ihtiyaçları ve verdiği hizmetler göz önünde bulundurulduğunda her kuruluşun iç ağlarında kendi çalışanlarına, internette ise dış kullanıcılara veya müşterilere çeşitli hizmetler sağladıkları bilinmektedir. Bu kapsamda kuruluşların çalışanlarına e-posta, dosya paylaşımları, internet erişimi, iç ağ portalleri ve üzerindeki web tabanlı uygulamalar gibi hizmetler verdikleri görülecektir. Dış dünya ile internet üzerinden verilen hizmetlerde ise mobil çalışanlara, müşterilere veya vatandaşlara çeşitli hizmetler sunulmaktadır. Birçok teknolojinin iç içe çalıştığı bu tarz ortamlarda işletim sistemleri ve bu sistemlerin üzerinde çalışan uygulamaların sahip olduğu güvenlik zafiyetleri kurumun bütün olarak güvenliğini tehdit etmektedir.

Yakın zamana kadar yürütülen bilgisayar korsanlığı aktiviteleri arkasındaki itici güç veya motivasyon ün, şan, şöhret iken, artık günümüzde bu itici güç çoğunlukla para ve nadir durumlarda da olsa ulusal çıkarlar olmaktadır. Motivasyonun niteliğindeki bu değişim yapılan saldırıların ve yazılan zararlı kodların da niteliğinde değişime sebep olması açısından oldukça önemlidir. Yüksek miktarda paranın el değiştirdiği yeni yeraltı ekonomisinin etkisi ile artık zararlı yazılımları yazanlar geçmiş zamanların tam tersine yazılımlarının kendilerini gizlemesi için çaba göstermektedirler. Bunun sebebi yarattıkları tehditlerin çözümlenmesini geciktirmek istemeleri ve bu süre zarfında yasa dışı kazançlarına devam etmek istemeleridir. Ulusal çıkarlar düşünülerek organize edilen saldırılara bakıldığında ilgili yazılımın yüksek yetenek ve bilgi seviyesi ile hazırlanmış oldukları fark edilecektir. McAfee güvenlik firmasının 2011 yılı içinde ortaya çıkardığı ve raporunu yayınladığı birden çok ülkeye ve bu ülkelerdeki kurumlara tek merkezden yapılan saldırılar ve izleme operasyonunun verileri internet ortamında gerçekleştirilen saldırıların ciddiyetini ortaya koymaktadır[1]. Aşağıdaki Tablo 1 ile bu operasyon kapsamında saldırıya uğrayan kuruluşların bulundukları sektörler gösterilmektedir[1].

Sektör	Adet
Kamu	21
Enerji ve Üretim	6
Teknoloji	13
Finans	6
Sosyal Kuruluşlar	12
Savunma Sanayii	13

Tablo 1 'Operation Shady RAT' içerisinde saldırılan ve izlenen kuruluşlar.

Burada dikkati çeken ilk konu, saldırılan kurumlar düşünüldüğünde birçoğunun arkasında ekonomik sebeplerin yatmamasıdır. Bu durum bazı devletlerin diğer devletlere karşı yaptığı siber saldırılar konusunda bir ipucu niteliğindedir. Raporda bahsi geçen sektörlerdeki kuruluşların ortalama bir sene izlemeye ve veri kaçırılmaya maruz kaldıkları belirtilmiştir.

Bilgi Sistemleri Güvenliği

Bilgi sistemleri güvenliği erişilebilirlik, gizlilik ve bütünlük ilkeleri çerçevesinden düşünüldüğünde çok geniş bir yelpazede konuyu içeren bir alandır. Bu üç temel ilkenin hepsinin bir arada sağlanması ise bu geniş çalışma alanının her konu başlığında gerekli çalışmanın yapılması zorunluluğunu ortaya çıkarır. Örnek verilmek istenirse, bütünlüğü bozulmuş bir hasta veya finans bilgisinin erişilebilir olmasının ve gizliliğinin bir anlamı kalmamaktadır.

1.1. Güvenliği Sınıflandırmak

Vacca[2] bilgi sistemleri güvenliğini üç ana bölüme ayırmaktadır:

- Mantıksal Güvenlik
- Fiziksel Güvenlik
- Çevre Güvenliği

Mantıksal güvenlik bilgi sisteminin iletişim ağları vasıtası ile maruz kalabileceği tehditleri kapsamaktadır. Fiziksel güvenlik ise bilgi sistemlerini barındıran fiziksel altyapının güvenliğini tarif etmektedir. Fiziksel güvenliğin kapsamına sunucu ve istemci donanımları, sistem odası, sistem odasının bulunduğu bina, güç hatları gibi bileşenler girer. Çevre güvenliği ise fiziksel güvenlikle bir düşünülebilir, ayrıldığı nokta ise bilgi sistemini barındıran bina veya kampüs alanının sınırlarında alınacak güvenlik önlemleridir.

1.2. Mantıksal Güvenlik

Bu makalenin ana konusunu oluşturan mantıksal güvenlik iki alt guruba ayrılabilir:

- Uygulama Güvenliği
- Altyapı Güvenliği

Uygulama güvenliği, uygulamayı geliştiren yazılım ekibinin sorumluluğunda olan bir alandır. Burada yazılımcıların yazdıkları uygulama için geliştirme sırasında gerekli olan güvenlik seviyesine göre gereken önlemleri almaları beklenir.

Altyapı güvenliği ise bilgi sistemlerinin diğer sistemler ve kullanıcılar ile iletişim kurması esnasında alınabilecek önlemleri kapsar. Bu önlemler altyapı üzerinden geçen trafik üzerinde veya pasif olarak güvenlik personeline bilgi sağlayacak şekilde olabilir.

Bir bilgi sistemi katmanlı olarak düşünülürse yapılan sınıflandırmaların Şekil 1 de hangi katmanlara denk geldiği görülebilir[3].

Bilgi Sistemi Uygulamaları, Hizmetler	Uygulama Güvenliği
Veritabanları	
Hazır yazılımlar	
İşletim Sistemi	Alyapı Güvenliği
İç Network	
İnternet	
Fiziksel Ekipman, Personel, Tesis	Fiziksel Güvenlik

Şeki 1: Bilgi Sistemi Katmanları

Güvenlik Yazılımları

Kamu ve özel sektör kurum ve kuruluşları, güvenlik ihtiyaçlarına göre aşağıda kısaca özetlenmiş olarak verilen güvenlik yazılımlarını kullanabilirler. Güvenlik yatırımlarının kurumların ihtiyaçlarını karşılayacak şekilde yapılması önemlidir. İhtiyaçtan daha az veya daha fazla yapılan yatırım ve çabalar her zaman maddi ve manevi zararlar ile sonuçlanacaktır.

•Güvenlik Duvarı (Firewall): Güvenlik duvarları üzerlerinden geçen trafik için erişim kuralları belirlemek ve uygulamak amacı ile kullanılırlar. Üzerlerinde bulunan kural tablosu yardımı ile istenmeyen yere doğru giden belirli nitelikte trafiğin geçişi engellenebilir. Ana ağ segmentleri (veya bölümleri) içinde kullanılabilmeleri sayesinde segmentler arasında erişim kuralları uygulanabilir. Dış dünya ile bağlantıyı güvenlik duvarları sağladığından mobil kullanıcıların şifreli olarak bağlantı kurmalarına olanak sağlayarak açık ağlardan geçerken verinin gizliliğinin korunmasına yardımcı olur.

•Atak Önleme Sistemi (Intrusion Prevention System, IPS): Atak önleme sistemleri korunmak istenen ağ segmentlerinin bağlantıları üstüne konularak zararlı trafiğin kesilmesi sağlanır. IPS sistemleri trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği ararlar ve bulduklarında, paket düşürme, TCP bağlantısını

sonlandırma gibi eylemlerde bulunabilirler. Bu özelliklere ek olarak servis dışı bırakma saldırılarına karşı, istatistiksel ve manüel verilmiş sınırları işleterek koruma sağlayabilirler.

•Web Uygulama Güvenlik Duvar (Web Application Firewall): Web uygulama güvenlik duvarları IPS lere benzer bir görev üstlenir. Web hizmetlerinin çok yaygın kullanılması sebebi ile üretilen bu sistemler web hizmetlerine ve web sunucularına gelebilecek saldırıları önleyecek trafik imzaları bulundururlar. Bu özelliklerine ek olarak yazılım geliştirilirken önlem alınmamış konularda ek koruma getirebilirler. Web ara yüzünde bilgi girişi yapılan alanlar üzerinde istenilen kontrollerin veya girdi doğrulamasının yapılması bir örnek olarak verilebilir.

• Veritabanı Güvenlik Duvarı (Database Firewall) : Veri tabanı güvenlik duvarları veritabanına gelen sorguları inceler ve olası zararlı aktiviteleri tespit edebilir. Kullanıcı davranışlarını öğrenerek profil dışına çıkma durumlarında uyarı üretebilirler. Web ve veritabanı güvenlik duvarının beraber kullanımı ile kullanıcıların web üzerinde yaptıkları işlemlerin veritabanı üzerinde yarattığı iz düşümü takip edilebilir. Bu sayede uygulamaların veritabanına bağlandığı tek bir kullanıcı yerine gerçek kullanıcıların kimlik bilgileri ile eşleştirme yapılarak veritabanı operasyonları gerçek kişilere bağlanabilir.

• E-Posta Güvenliği (E-mail Security Gateway): Kurum sistemlerine dışarıdan gelen spam ve zararlı kodların önlenmesinde kullanılırlar. Ağ seviyesinde internete açık bir şekilde mail sunucu (Mail transfer agent, MTA) görevi ile de kullanılabilir. Aynı zamanda mail sunucuların üzerinde çalışan çeşitleri de vardır.

• Yük Dengeleyici (Load Balancer): Yük dengeleyiciler erişilebilirliği en üst seviyede tutmak için yoğun istek gelen sunucular arasında yük paylaştırırlar. Eğer bu bir web sunucu ise SSL(secure sockets layer)'i kendi üstlerinde sonlandırarak sunucuları kriptolama yükünden kurtararak performans artışı sağlarlar.

• URL Filtresi ve Antivirus (Web Security Gateway): Kurum ağında çalışan istemcilerin internet erişimlerini düzenlemek amacı ile kullanılırlar. Bazı sitelere erişimin engellenmesi hem güvenlik hem de kurum politikası gereği istendiği durumlarda erişimi engelleyebilirler. Bu işlevi yaparken vekil sunucu şeklinde çalışıyorlarsa gelen trafik üzerinde zararlı yazılım taraması da yapabilirler.

• Web Cache Vekil Sunucusu (Caching Proxy Server): Kaşe (Cache) sunucuları URL filtreleri ile aynı sistemde olabildikleri gibi ayrı olarak da kullanılabilir. İnternetten çok defa aynı dosyanın indirilmesi durumunu engellemek amacıyla çok indirilen dosyaları üzerlerinde tutarak internet bant genişliği tasarrufu sağlarlar. Bu da erişilebilirliği artıracaktır.

• Transparan İçerik Yönlendiriciler (Transparent Redirection): Karmaşık ve büyük ağ yapılarında istemcilerin URL filtre gibi trafiğin yönlendirilmesi gereken yerlerde kullanıcı sistemleri üzerinde ayar yapılmadan gönderilmesini sağlayabilirler. Bu özellik ile kullanım kolaylığı sağlarken aynı zamanda da ayarların eksik yapılması ihtimalini ortadan kaldırarak her kullanıcının istenen vekil sunucuları kullanmasını garanti altına alırlar.

• Zafiyet Tarama Sistemleri (Vulnerability Scanner): Böyle bir sistem işletim sistemleri üzerindeki ve işletim sisteminde çalışan uygulamalar üzerindeki zafiyetleri otomatik taramalar ile bulur. Aynı zamanda yama eksikleri veya kurum politikasına aykırı yapılandırılmış sistemleri de tespit edebilir.

• Risk Analiz ve Önceliklendirme Sistemi (Risk Management Systems): Zafiyet tarama sistemlerinden sistem zafiyetlerini, güvenlik duvarı, ağ anahtarları ve yönlendiricileri gibi cihazlardan da yapılandırma ayarlarını toplayarak bir ağ modeli oluşturur. Oluşturulan ağ modeli üzerinden risk risk analizi yapılır ve önceliklendirilir. Bu sayede kısıtlı personel kaynaklarının nerelerde ilk önce kullanılması gerektiği ve en çok risk altında bulunan sistemler gibi bilgiler elde edilir

• Kayıt Toplama ve Korelasyon Sistemi (Security Information and Event Management, SIEM): Birçok güvenlik sistemi üzerlerinde meydana olaylar için çeşitli ortamlarda olay kayıtları tutarlar. Bu olay kayıtları her sistemin üzerinde olduğundan diğer sistemlerdeki olaylar ile ilişkilendirme işlemi çok zor olmaktadır. SIEM sistemleri dağıtık halde olan bu kayıtları bir yerde toplayarak korelasyon yapılabilir hale getirirler. Yazılan mantıksal kurallar sayesinde gerçek zamanlı korelasyon yapılabilir ve normalde tespit edilemeyen güvenlik olayları tespit edilebilir.

• Ağ erişim kontrolü (Network Access Control): Ağ erişim kontrolü sistemleri kurum politikalarına uymayan sistemlerin ağa dahil olmalarını engellemek amacı ile kullanılır. Bu sayede yabancı sistemlerin ve güvenlik durumu uygun olmayan sistemlerin iç ağı tehdit etmesi önlenir.

• Sıfır Gün Zararlı Yazılım Tespit Sistemi (Zero Day Malware Protection System, Malware sandboxing): İmza tabanlı zararlı yazılım tespit sistemleri (Antivirüs) imza veri tabanlarında olmayan zararlı yazılımları yakalayamamaktadır. Günümüzde artan bir hacimde zararlı yazılımlar yazıldığından imza veritabanlarında yer almaları uzun süreler almaktadır ve bu arada geçen zamanda sistemler savunmasız kalmaktadırlar. Bu sistemler genelde şüpheli yazılımları ağ seviyesinde yakalayarak test sistemlerinde çalıştırırlar(Sandboxing). Çıkan sonuçlara göre imzasız olarak zararlı tespit edilen yazılımlar engellenebilir[4].

• Ağ izleme ve Performans Analiz Sistemi (Network Performance Management): Böyle bir sistem ağ trafiği üzerinden uygulama ve ağ performansı hakkında bilgi toplar. Bu sayede performans kaybı olaylarında bilgilendirme yapabilir ve bu durumlarda sorunun kaynağı ile alakalı detaylı bilgiyi ilgili personele sağlar[5].

• Veri Kaçaklarını Önleme Sistemi (Data Loss Prevention): Sistemler üzerinde bulunan hassas verinin izinsiz kurumlar dışına çıkartılmasına engel olur. Hem ağ hem de istemci seviyesinde çalışan modelleri vardır. İstemci üzerinde çalışan sistemlerde taşınabilir medya gibi kaynaklardan kaçakların önlenmesi için aygıt kontrolü yapan bileşenleri bulunur. Yazıcılar, CD-DVD yazıcı ve okuyucular, USB depolama cihazları örnek olarak verilebilir.

• Ağ Tabanlı Adli Bilişim Sistemi (Network Forensics): Bu sistemler pasif olarak ağ trafiğini yakalayarak trafik üzerinde derin paket incelemesi yapabilme olanağı sağlarlar [6]. Bu sayede sistemde meydana gelen olaylar ve sorunlar detaylı şekilde incelenebilir. Trafik kayıt edildiği için veri kaçaklarını önleme sistemlerine kaçak olması durumunda çıkan verinin niteliği hakkında bilgi sağlayarak yardımcı olurlar.

• Tek Yönlü Veri Transfer Cihazları (One Way Data Transfer): Genelde internete kapalı ağlara veri transferi yapılırken dışarı veri sızıntısını engellemek amacı ile kullanılırlar. Donanım tabanlı ürünler iki tarafa da kullanılan protokol çalışırmış gibi gösterirken donanım üzerinde bir yön haricinde ters yöne veri iletişimi fiziksel olarak engellerler[7].

• İstemci Güvenlik Ürünleri (Endpoint Security): İstemci üzerinde çalışan güvenlik ürünleri ağ seviyesinde çalışanlara destek olacak şekilde ek bir katman olarak görev yaparlar. Antivirus, IPS, Veri kaçakları önleme yazılımı, disk şifreleme örnek olarak verilebilir.

Güvenlik Risk Yönetimi

1.3. Risk Değerlendirmesi

Önceki bölümde kısaca özetlenen güvenlik yazılım ürünlerinin doğru seçimi ancak güvenlik risk değerlendirmesi yapıldıktan sonra yapılabilir. Risk değerlendirmesinin adımları sırası ile:

• Varlıkların tespiti ve değerlerinin belirlenmesi;

• Varlıklar zarar gördüğü zaman kurumun yaşayacağı zararın belirlenmesi;

• Tehditlerin ve tehditlerin olma olasılıklılarının belirlenmesi;

• Alınabilecek önlemlerin belirlenmesi;

• Hangi önlemlerin uygulanacağı kararı için fizibilite çalışması yapılması ve sonucuna göre uygun görülen güvenlik önlemlerinin uygulanması.

Güvenlik risk değerlendirmesi ilk defa yapıldıktan sonra periyodik olarak tekrarlanması gerekmektedir. Yaşam döngüsü şekilde yapılan risk değerlendirmeleri sistemlerin kullanılması, tasarımının yapılması veya uygulanmasını etkileyecektir[3].

1.4. Zafiyet ve Sızma Testleri

Oluşturulan güvenlik mimarisi ile birlikte sistemin beklenen şekilde çalıştığı durumda alınan güvenlik önlemlerinin etkinliğinin belirlenmesi önemli bir konudur. Sistem altyapısına ve işletim sistemlerine entegre edilmiş güvenlik önlemleri her ne kadar belirli bir seviyede güvenlik getirse de asıl önemli olan, bu yazılımları kullanan, yapılandıran ve sürekli izleyen güvenlikten sorumlu personeldir. Bu sebeple sızma veya penetrasyon testi olarak anılan, sistemin son haline iç ağdan ve dış ağdan test saldırıları düzenlenir. Açıklıklar bulunmaya çalışılır ve bulunan açıklıklar raporlanır. Periyodik olarak yapılan sızma testleri ile güvenlik sistemlerinin yapılandırmaları ve etkinlikleri istenilen seviyede tutulmaya çalışılır.

Sızma testlerine ek olarak hizmet veren sunucuların ve üzerlerinde koşan uygulamaların açıklarının da tespit edilmesi ve alınabilecek bir önlem varsa alınması gerekir. Zafiyet testleri, sızma testleri gibi insanlar tarafından yapılabileceği gibi, bu işe özel olarak yazılmış otomatik araçlar kullanılarak da yapılabilir. Otomatik

araçlar kullanıldığında bu testler daha sık yapıldığından kurum sistemlerinin zafiyet durumları geçen zaman göre incelenebilir ve iyileşme ya da kötüleşme durumlarından ilgili kişiler haberdar edilebilir.

Tasarım

Bilgi sistemlerinin tasarım ve gerçekleştirilmelerinde mimari olarak katmanlı mimariler ile modüler yapının avantajlarından faydalanılır. Fakat bu sadece esnek yapının avantajlarını değil aynı zamanda güvenlik önlemlerinin alınmasında da kolaylık ve olanak sağlar. Web ara yüzü, uygulama sunucusu ve veritabanı sunucusu şeklinde tasarlanmış bir bilgi sisteminde bileşenler arası çalışmada bahsedilen güvenlik bileşenleri kullanılabilir.

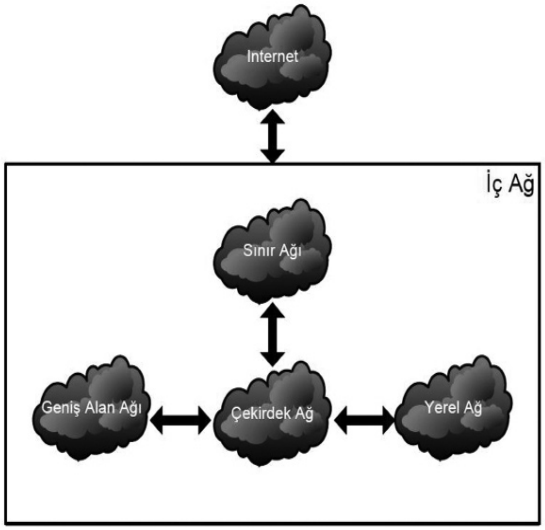
Bu makalede yukarıda bahsedilen şekilde tasarlanmış bir uygulama ile servis veren ve aynı ağda kullanıcılarını da barındıran sanal bir kurum için güvenlik önlemlerinin tasarlandığı bir yüksek lisans tez çalışması özetlenmiştir[8]. Güvenlik mimarisi tasarlanırken genel ağ segmentleri birbirlerinden güvenlik duvarları ile ayrılmıştır. En genel olarak aşağıdaki ağ segmentleri (bölümleri) belirlenmiştir:

- Internet
- Sınır Ağı
- Yerel Ağ
- Çekirdek Ağ
- Geniş Alan Ağı

Bu ağ bölümleri arası geçişler erişim kuralları ile düzenlenmiştir. En az yetki prensibi ile gerekli erişimler dışındaki tüm erişimlerin engellendiği varsayılmaktadır.

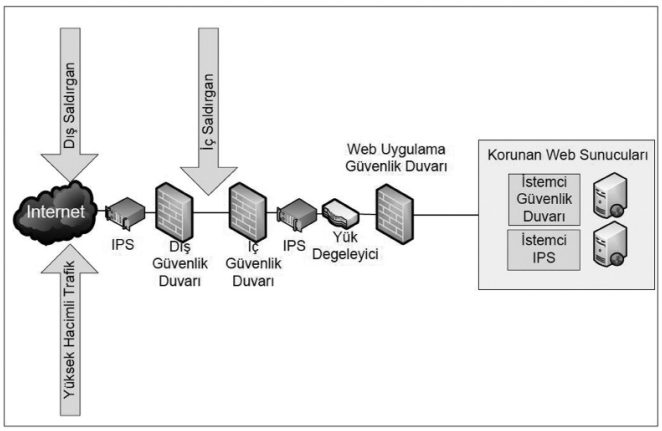
Şekil 2'de yukarıda belirtilen ağlar arası iletişim yolları mantıksal olarak görülmektedir. Internet haricinde diğer kesimler kurum iç ağı olarak kabul edilmiştir.

Sınır ağı internetten doğrudan ulaşılması gereken e-posta sunucuları, DNS sunucuları gibi sistemlerin bulunduğu bölümdür. Çekirdek ağda dışarıdan doğrudan erişilmeyecek tüm sunucular bulunur. Yerel ağ ile geniş alan ağında da kullanıcı sistemleri bulunmaktadır. Geniş alan ağı mobil kullanıcıları ya da uzak ofisleri temsil etmektedir.



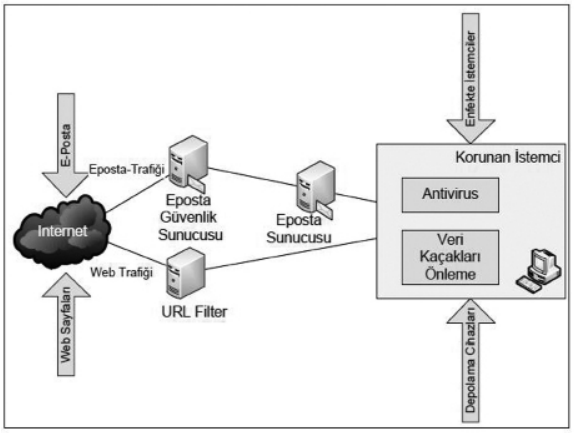
Şekil 2: Genel Ağ Segmentleri

Tanımlanan ağ segmentlerinde güvenlik önlemleri için katmanlı güvenlik mimarisi tanımlanmıştır. Katmanlı güvenli mimarisi saldırgan ve hedef arasına birden fazla güvenlik önlemi koyarak sağlanır. Bu sayede katmanlar arasından gelebilecek tehditler sonraki katmandaki güvenlik önlemleri ile engellenebilir. Şekil 3 ile korunmak istenen bir web sunucu ile internet arasında alınan önlemler mantıksal bir şema ile gösterilmiştir. Bu senaryoda internet tarafından başlamak gerekirse öncelikle dış güvenlik duvarı tarafından istenmeyen yöndeki trafik kesilecektir. Bilinen ataklara karşı koruma sağlayan IPS sistemleri ile hem internet tarafından hem de diğer ağlardan gelecek trafik engellenebilmektedir. Bu önlemlere ek olarak yük dengeleyici ile erişilebilirlik artırılmakta web uygulama güvenlik duvarı ile de daha karmaşık web tehditlerine karşı koruma sağlanmaktadır. En son katman savunma olarak istemci IPS ve istemci güvenlik duvarı kullanılmıştır. Bulunduğu ağdan gelecek olası bir saldırı bahsedilen ağ cihazlardan geçmeyeceği tek savunma olarak istemci güvenlik ürünleri kalmaktadır. Uygulanan bu katmanlı yapı ile saldırıların gelebilecekleri tüm yerler ve nitelik olarak bilinen saldırıların birçoğu engellenebilecektir



Şekil 3: Katmanlı Savunma için Mantıksal Yapı

Şekil 4 içinde ise istemcilere bulaşabilecek zararlı yazılımların geliş vektörlerine göre alınmış önlemler görülebilir.



Şekil 4: Zararlı Yazılım Geliş Yolları ve Önlemler

Zararlı yazılımlar için de katmanlı mimari kullanılmıştır. İstemcide çalışması gereken zararlı yazılımların geliş vektörleri internet den eposta ve internet kullanımı, depolama cihazları ve diğer enfekte sistemler olarak özetlenebilir. Eposta ve web için güvenlik yazılımları vekil sunucu şeklinde konumlandırılarak zararlı yazılım taraması yapmaktadırlar. Sistemlere ağ üstünden geçmeyen yollar ile gelmesi durumu için Veri Kaçakları Önleme Yazılımlarında bulunan ya da tek başına kullanılabilen aygıt yönetme yazılımı ile depolama aygıtlarının kullanılması yasaklanmıştır. Bu sayede depolama cihazları ile istemciye zararlı yazılım bulaşması engellenmiştir. Bu yolların dışında, ortamda bulunan diğer bir enfekte sistem de kendini başka sistemlere göndererek yayılmayı seçebilir. Burada da antivirus yazılımı zararlı kodu imzalarında var ise engelleyecektir.

Sonuç

Kamu ve özel sektörde sayısı ve boyutu hızla artan bilgi sistemlerinin gerektiği oranda güvenliğinin sağlanması günümüzde büyük önem kazanmıştır. Katmanlı savunma mimarisi ile birden çok katmanda güvenlik kontrolü yapılabilir. Katmanlı yapı ile birden fazla savunma noktaları oluşturularak saldırganları yavaşlatmak ve her atak vektörünü karşılayacak bir önlem konuşlandırılmış olabilmektedir.

Bu makalede altyapı güvenliğinin artırılması özellikle ele alınmıştır. Fakat diğer güvenlik alanları da aynı zamanda oluşturulmalıdır. İnsan faktörü ve fiziksel güvenlik toplam güvenlik mimarisinde vazgeçilemeyecek noktalardır.

Herhangi bir kurum ve kuruluş için güvenlik yatırımları yapılmadan önce risk analizi çalışması yapılarak ancak gerektiği kadar güvenlik yatırımı yapılması uygun bir yaklaşım olacaktır.

Teşekkür

Yazarlar, bilgi sistemleri güvenliği alanına katkıda bulunan tüm meslektaşlarına teşekkürlerini sunarlar.

Kaynakça

[1] Alperovitch, D. “Revealed: Operation Shady RAT”, McAfee, 2011.

[2] Vacca, J. “Computer and Information Security Handbook” Morgan Kaufmann, 2009.

[3] Sommerville, I. “Software Engineering”, Addison-Wesley, 2007.

[4] FireEye Web MPS Datasheet, http://www.fireeye.com/resources/pdfs/FireEye_Web_MPS_ds.pdf

[5] Riverbed Cascade, http://www.riverbed.com/us/products/cascade/

[6] Packet Capture, Wikipedia, http://en.wikipedia.org/wiki/Packet_capture, 09.2011.

[7] Unidirectional Network, Wikipedia, http://en.wikipedia.org/wiki/Unidirectional_network

[8] Tan. H. “Kurum ve Kuruluşların Bilgi Sistemi Güvenliği ve Bir Uygulama”, Yüksek Lisans Tezi (Danışman: Prof. Dr. A. Z. Aktaş), Başkent Ü. Bilgisayar Müh. Bölümü, 2011.