

Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması
Ar. Gör. Enis Karaarslan*, Abdullah Teke**, Prof. Dr. Halil Şengonca**
{enis, ateke, sengonca}@bornova.ege.edu.tr
*Ege Üniv. Uluslararası Bilgisayar Enst., **Ege Üniv. Bilgisayar Müh.

ÖZET

Ağ güvenlik politikası, kısaca bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili stratejinin resmi şekilde yazılı olarak ifade edilmesidir. Bu bildiride güvenlik politikalarının kurumlar için önemi belirtilmekte ve bilgisayar ağlarında uygulanması için gereken çalışmalara değinilmektedir. Ege Üniversitesi'nin 2001-2002 döneminde gerçekleştirdiği ağ güvenlik duvarı (firewall) ve virus duvarı (viruswall) projesi ile gerçekleştirdiği güvenlik politikasına da göndermede bulunmaktadır.

1. AĞ GÜVENLİK POLİTİKASI NEDİR?

Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet'e uyarlamışlardır. Eskiden kilitli odalarla sağlanan güvenlik kavramı, bilgisayar ağları ve İnternet gibi ortamların gündeme gelmesiyle boyut değiştirmiştir. İnternet yasalarla denetlenemeyen bir sanal dünyadır. Bu sanal dünyada saldırganlar bilgiye ulaşmada ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir. Kurumlarda oluşan kayıplar maddi olabileceği gibi güven yitirme gibi manevi zararlar da olabilmektedir. Bu tür durumlarla başa çıkabilmek için bazı kuralların belirlenmesi gerekmektedir.

Kurumların kendi kurmuş oldukları ve İnternet'e uyarladıkları ağlar ve bu ağlar üzerindeki kaynakların kullanılması ile ilgili kuralların genel hatlar içerisinde belirlenerek yazılı hale getirilmesi ile ağ güvenlik politikaları oluşturulur. Güvenlik politikasının en önemli özelliği yazılı olmasıdır ve kullanıcıdan yöneticiye kurum genelinde tüm çalışanların, kurumun sahip olduğu teknoloji ve bilgi değerlerini nasıl kullanacaklarını kesin hatlarıyla anlatmasıdır [1]. Ağ güvenlik politikaları mümkünse sistem kurulmadan ve herhangi bir güvenlik sorunuyla karşılaşmadan önce oluşturulmalıdır. Bu aynı zamanda, kurulu olan bir sistemin güvenlik politikasını oluşturmaktan daha kolaydır. Güvenlik politikası olmadan güvenli bir bilgisayar ağı gerçekleştirilemez. Bu kadar öneme sahip olmasına rağmen Amerika'da güvenlik politikalarının gerçekleştirilme oranı sadece %60'larda kalmakta, Türkiye için bu oran daha da düşmektedir [2].

Ağ güvenlik politikaları, kurumların yapılarına ve gereksinimlerine göre değiştiğinden bir şablondan söz etmek mümkün değildir. Bu bildiride güvenlik politikası oluştururken dikkat edilmesi gerekenler belirtilmiştir. Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların

konuya veya teknolojiye özgü olmasıdır [3]. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar aşağıda sıralanmıştır [4]:

1. Kabul edilebilir kullanım (acceptable use) politikası
2. Erişim politikası
3. Ağ güvenlik duvarı (firewall) politikası
4. İnternet politikası
5. Şifre yönetimi politikası
6. Fiziksel güvenlik politikası
7. Sosyal mühendislik politikası

1.1. Kabul Edilebilir Kullanım (Acceptable Use) Politikası

Ağ ve bilgisayar olanakların kullanımını konusunda kullanıcıların hakları ve sorumlulukları belirtilir. Kullanıcıların ağ ile nasıl etkileşimde oldukları çok önemlidir. Yazılacak politikada temelde aşağıdaki konular belirlenmelidir [5][6]:

- Kaynakların kullanımına kimlerin izinli olduğu,
- Kaynakların uygun kullanımının nasıl olabileceği,
- Kimin erişim hakkını vermek ve kullanımı onaylamak için yetkili olduğu,
- Kimin yönetim önceliklerine sahip olabileceği,
- Kullanıcıların hakları ve sorumluluklarının neler olduğu,
- Sistem yöneticilerin kullanıcılar üzerindeki hakları ve sorumlulukların neler olduğu,
- Hassas bilgi ile neler yapılabileceği.

Kurumun yapısına göre başka maddeler de eklemek mümkündür. SANS Enstitüsü'nün oluşturduğu politika şablonu için bakınız [7]. Türkiye'de üniversitelerin İnternet bağlantısını sağlayan Ulakbim'in kabul edilebilir politikası için bakınız [8].

1.2. Erişim Politikaları:

Erişim politikaları kullanıcıların ağa bağlanma yetkilerini belirler. Her kullanıcının ağa bağlanma yetkisi farklı olmalıdır. Erişim politikaları kullanıcılar kategorilere ayrıldıktan sonra her kategori için ayrı ayrı belirlenmelidir. Bu kategorilere sistem yöneticileri de girmektedir. Sistem yöneticisi için erişim kuralları belirlenmediği takdirde sistemdeki bazı kurallar sistem yöneticisinin yetkisine bırakılmış olacağından, bu sistem üzerinde istenmeyen güvenlik açıkları anlamına gelebilecektir.

1.3. Ağ Güvenlik Duvarı (Firewall) Politikası:

Ağ güvenlik duvarı (network firewall), kurumun ağı ile dış ağlar arasında bir geçit olarak görev yapan ve İnternet bağlantısında kurumun karşılaşabileceği sorunları çözmek üzere tasarlanan çözümlerdir. Ağın dışından ağın içine erişimin denetimi burada yapılır. Bu nedenle erişim politikaları ile paraleldir. Güvenlik duvarları salt dış saldırılara karşı sistemi korumakla kalmaz, performans artırıcı ve izin politikası uygulayıcı amaçlar için de kullanılırlar. Bu çözümler yazılım veya donanımla yazılımın bütünleşmesi şeklinde olabilir. Güvenlik duvarlarının grafiksel arabirimleri kullanılarak kurumun politikasına uygun bir şekilde erişim kuralları tanımlanabilmektedir. Güvenlik duvarı aşağıda belirtilen hizmetlerle birlikte çalışarak ağ güvenliğini sağlayabilmektedir [9]:

- Proxy: Proxy bir bağlantı uygulamasında araya giren ve bağlantıyı istemci (client) için kendisi gerçekleştiren bir hizmettir. Proxy'nin kullanımı, uygulama temelli (application-level) güvenlik duvarı olarak da adlandırılabilir. Bu tür bir uygulama

aynı zamanda kimlerin bu hizmetleri kullanacağını belirlemek ve performans amaçlı olarak bant genişliğinin daha etkin kullanılmasını sağlamak için de kullanılır.

- Anti-Virus Çözümleri: HTTP, FTP ve SMTP trafiğini üzerinden geçirerek virüs taramasını yapmayı ve kullanıcıya gelmeden önce virüslerden temizlemeyi hedefleyen sistemlerdir.
- İçerik Süzme (content filtering): Çeşitli yazılımlarla ulaşılmak istenen web sayfalarını, gelen e-posta'ları süzmeye yarayan sistemlerdir.
- Özel Sanal Ağlar (Virtual Private Network-VPN): Ortak kullanıma açık veri ağları (public data network) üzerinden kurum ağına bağlantıların daha güvenilir olması için VPN kullanılmaktadır. İletilen bilgilerin şifrelenerek gönderilmesi, Genel/Özel (Public/Private) anahtar kullanımı ile sağlanır. VPN kullanan birimler arttıkça daha sıkı politika tanımları gerekli hale gelmektedir.
- Nüfuz Tespit Sistemleri (Intrusion Detection Systems-IDS): Şüpheli olayları, nüfuz ve saldırıları tespit etmeyi hedefleyen bir sistemdir. IDS, şüpheli durumlarda e-posta veya çağrı cihazı gibi yöntemlerle sistem yöneticisini uyarabilmektedir.

Bu servislerin hepsinin konfigürasyonu ve kullanacakları kuralların belirlenmesi güvenlik politikasına uygun olarak yapılmalıdır.

1.4. İnternet Politikası:

Kurum bazında her kullanıcının dış kaynaklara yani İnternet'e erişmesine gerek yoktur. İnternet erişiminin yol açabileceği sorunlar aşağıdaki gibidir[10]:

- Zararlı kodlar: Virüs veya truva atı (trojan) gibi zararlı yazılımların sisteme girmesine yol açabilir. Virüslerden korunmak için her kullanıcının makinasına bir antivirüs yazılımının kurulmasını sağlamak veya İnternet (http, email, ftp) trafiğini sunucu(lar)da tarayıp temizledikten sonra kullanıcıya ulaştırmak gibi önlemler alınabilir. Sistemde güvenlik açıklarına neden olacak truva atlarını engellemek için güvenlik duvarlarında kesin kurallar konulmalıdır.
- Etkin Kodlar: Programların web üzerinde dolaşmalarına olanak sağlayan Java ve ActiveX gibi etkin kodlar saldırı amaçlı olarak da kullanılabilir. Java, denetim düzenekleri ile bu tür saldırıların gerçekleşmesini önleyen bazı olanaklar sunmasına karşın ActiveX için aynı şeyden söz etmek mümkün değildir. Bu nedenle bu kodların kullanıma ilişkin ayarlar İnternet tarayıcısı üzerinde yapılmalıdır.
- Amaç dışı kullanım: İnternet hattı, kurumun amacı dışında da kullanılabilir. Film, müzik gibi büyük verilerin İnternet'ten çekilmesi hat kapasitesini gereksiz yere dolduracağından kurumun dış kaynaklara erişim hızında yavaşlamalara yol açabilecektir.
- Zaman Kaybı: İnternet ortamında gereksiz web sitelerinde zaman geçirmek kurum çalışanlarının iş verimini azaltabilir. Bunu engellemek için kurum politikasında bazı kullanıcılara İnternet erişimi verilmeyebilir veya İnternet erişimi öğle molası gibi belirli saatlerle kısıtlanabilir. Farklı bir çözüm ise web erişimini denetim altına almak ve ulaşılabilecek web sitelerini belirlemektir. Bu denetimler farklı kullanıcı gruplarına farklı şekillerde uygulanabilir.

Kurumda dış kullanıcılardan (çalışanlar, ortaklar, müşteriler veya diğerleri) kimlerin kurum ağındaki hizmetlere erişebilecekleri ve ne tür erişim haklarına sahip oldukları tanımlanmalıdır.

1.5. Şifre Yönetimi Politikası:

Şifreler kullanıcıların ulaşmak istedikleri bilgilere erişim izinlerinin olup olmadığını anlamamızı sağlayan bir denetim aracıdır. Şifrelerin yanlış ve kötü amaçlı kullanımları güvenlik sorunlarına yol açabileceğinden güvenlik politikalarında önemli bir yeri vardır. Sistem yöneticileri kullanıcıların şifre seçimlerinde gerektiği yerlerde müdahale etmelidirler. Basit ve kolay tahmin edilebilir şifreler seçmelerini engellemek için kullanıcılar bilinçlendirilmeli ve programlar kullanılarak zayıf şifreler saptanıp kullanıcılar uyarılmalıdır. Her hesap için ayrı bir şifre kullanılmalı ve şifreler sık sık değiştirilmelidir [11]. Kullanıcılar şifrelerinin çalındığından kuşkulandıklarında yetkili birimlere haber vermeli, gereken önlemleri almalıdır. Şifre seçimi ve kullanımı konusunda ayrıntılı bilgi edinmek için bakınız [12]. Şifrenin seçilmesi ile birlikte kullanıcının sorumluluğu bitmez, çünkü yeterli kaynak ve zaman olduğunda her şifre kırılabilir [1]. Ayrıca kurumlar güvenlik politikalarında şifre seçimi ile ilgili aşağıdaki kısıtlamaları belirleyebilmektedirler:

- Şifrenin boyutu ve içeriği: Kurum, sistemlerde kullanılacak şifrenin uzunluğunu (en az 7-8 karakter) ve içeriğinin ne olması gerektiğini (rakam ve harflerin birer kombinasyonu) belirleyebilmektedir.
- Süre dolması (eskime) politikası: Süresi dolan şifreler kullanılamamakta ve kullanıcılar yeni şifre almak zorunda kalmaktadır. Böylece şifreler üzerinde bir denetim düzeneği kurulmuş olmaktadır.
- Tek kayıt ile herşeye erişim (Single Sign On-SSO) politikası: Kullanıcı, tek bir şifre ile ağ üzerindeki kendisine erişim izni verilen bütün uygulamalara ulaşabilmektedir. Kullanıcının birçok şifreyi birden hatırlamak zorunluluğu olmadığı için son kullanıcılar için kullanışlıdır.

1.6. Fiziksel Güvenlik Politikası

Bilgisayar veya aktif cihazlara fiziksel olarak erişebilen saldırganın cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişerek (tapping) hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal güvenlik önlemlerinin hiç bir kıymeti bulunmamaktadır. Kurumun ağını oluşturan ana cihazlar ve hizmet sunan sunucular için alınabilecek fiziksel güvenlik politikaları kurum için belirlenmelidir. Cihazlar için alınabilecek fiziksel güvenlik önlemleri için bakınız [13].

1.7. Sosyal Mühendislik Politikası

Sosyal mühendislik, kişileri inandırma yoluyla istediğini yaptırma ve kullanıcıya ilişkin bilgileri elde etme eylemidir. Sistem sorumlusu olduğunu söyleyerek kullanıcının şifresini öğrenmeye çalışmak veya teknisyen kılığında kurumun içerisine fiziksel olarak sızmak veya çöp tenekelerini karıştırarak bilgi toplamak gibi değişik yollarla yapılabilir. Kurum çalışanları kimliğini kanıtlamayan kişilere kesinlikle bilgi aktarmamalı, iş hayatı ile özel hayatını birbirinden ayırmalıdır. Kurum politikasında bu tür durumlarla ilgili gerekli uyarılar yapılmalı ve önlemler alınmalıdır [4] [11].

2.KURUMUN İHTİYAÇLARININ BELİRLENMESİ

Güvenlik Politikalarının oluşturulması sırasındaki ilk adım olarak bu politikanın kurumun hangi gereksinimlerine yönelik oluşturulacağı belirlenmelidir. Politikanın oluşması için aşağıdaki aşamalar yerine getirilmelidir [1] :

- Korunacak nesnelerin belirlenmesi: Bu yazılım ve donanım gibi bilgisayar kaynakları olabileceği gibi, bilgisayarla ilgili olmayan ve kurum için hayati öneme sahip yazılı belgeler olabilir. Ağ güvenliği söz konusu olduğunda etkin iletişim cihazları ve sunucular (server) belirlenmelidir. Ağ üzerinden hizmet veren sunucuların kimlere ne hizmeti verdiği, hangi protokolleri kullandığı, bu sunucuları yöneten kişilere (admin) ulaşım için kullanılacak e-posta adresi ve telefon gibi bilgilerin ağ güvenliği ile uğraşan birime dilekçe ile verilmesi sağlanmalıdır. Örnek bir dilekçe için <http://security.ege.edu.tr/dilekce.htm> adresine bakılabilir. Her birimin bilgisayar işlerinden sorumlu yerel sistem yöneticilerine, birim yöneticilerine telefon ve/veya resmi yazı ile ulaşmalı ve sunucu bilgileri toplanmalıdır. Ağ trafiği izlenerek de ulaştırılmayan bilgiler edinilebilir.
- Kime karşı korumanın yapılacağıın belirlenmesi: Korunmak istenen kaynaklara kimler tarafından zarar verilebileceği tüm durumlar göz önünde bulundurularak belirlenmelidir. Bu İnternet üzerinden veya kurum içinden saldırıda bulunan kişiler olabileceği gibi, dikkatsizlik yapan bir kurum çalışanı da olabilir.
- Bilgileri saklama yönteminin belirlenmesi: Kurumların ellerindeki bilgilerin nasıl tutulduğunu ve bu bilgilerin nasıl aktarıldığını belirlemeleri gereklidir. Örneğin bir kurumda tüm bilgiler sözlü olarak aktarılırken, bir başka kurumda bilgilerin aktarımı için resmi yazılar gerekli olabilir.
- Bilgilerin arşivlenmesi ve yedeklenmesi: Kurumlar bilgi kayıplarını en aza indirmek için yedekleme ve eski bilgilere daha sonra erişebilmek için arşivleme yapmalıdır. Kurumlarda ne tür bilgilerin yedekleneceği, hangi sıklıkla yedek alınacağı, yedeklemenin kimler tarafından yapılacağı kurallarla belirlenmelidir.
- Kurum içerisinde sorumlulukların belirlenmesi: Kurum çalışanlarının görev alanları ve güvenlik politikaları üzerindeki sorumlulukları belirlenmelidir. Güvenlik politikasında sorumluluk alan gruplar aşağıdaki gibidir [1]:
 - Yönetim: Yönetim, güvenlik politikasını oluşturmak ve uygulanmasını sağlamak için güvenlik bölümünün oluşturulmasından sorumludur.
 - Güvenlik Bölümü: Bu bölümün sorumlulukları ise güvenlik politikasını oluşturmak, yayınlamak, uygulanmasını sağlamaktır. Bir diğer görevi ise çalışanları politika konusunda bilgilendirmek ve eğitmektir.
 - Kullanıcılar: Kullanıcılar güvenlik politikaları ile belirlenen kurallara göre davranmak zorundadırlar.
- Yaptırım gücünün belirlenmesi: Güvenlik politikasının uygulanabilir olabilmesi için yaptırım gücünün olması gerekir. Aksi takdirde politika kağıt üzerindeki bir belgeden öteye gidemez. Yaptırım amacıyla yasalardan veya kuruma ilişkin kurallardan yardım alınabilir.

3. RİSK ANALİZİ ve GÜVENLİK MATRİSLERİNİN OLUŞTURULMASI

Risk analiziyle kurumun ağına, ağ kaynaklarına ve verilere yapılabilecek saldırılarla oluşabilecek riskler tanımlanır. Amaç değişik ağ bölümlerindeki tehdit tahminlerinin belirlenmesi ve buna uygun bir düzeyde güvenlik önlemlerinin uygulanmasıdır. Oluşabilecek tehditin önemine ve büyüklüğüne göre üç düzey kullanılabilir; Düşük Risk, Orta Risk, Yüksek Risk. Riskler tanımlandıktan sonra sistemin kullanıcıları tanımlanmalıdır. Kullanıcı türleri aşağıdaki gibi sınıflandırılabilir [14]:

- Yöneticiler: Ağ kaynaklarını yönetme sorumluluğundaki iç kullanıcılar.
- Öncelikliler (privileged): Kullanıcılardan daha fazla erişim hakkına gereksinim duyan iç kullanıcılar.

- **Kullanıcılar:** Genel erişim hakkına sahip iç kullanıcılar.
- **İş Ortakları:** Bazı kaynaklara erişim gereksinimi duyacak dış kullanıcılar.
- **Diğer:** Dış kullanıcılar veya müşteriler.

Risk düzeyleri ve kullanıcı türleri tanımları kullanılarak, her ağ sistemine erişim tipi güvenlik matrisi dediğimiz yapılarda tanımlanır. Güvenlik matrisi her sistem için hızlı bir başvuru ve sonraki güvenlik ayarlamaları için başlangıç noktası oluşturur. Güvenlik matrisi içeriğine göre çeşitli biçimlerde olabilir. Çizelge 3.1’de ağ sistem elemanlarının risk düzeylerine göre sınıflandırılması yapılmıştır [14]:

Sistem	Tanım	Risk Seviyesi	Kullanıcı Tipi
Ağ geçidi (router)	İnternet erişimini sağlayan ağ cihazı	Yüksek	Cihaz konfigürasyonu için yöneticiler; veri aktarımı için bütün kullanıcılar
Ağ cihazları (switch)	Ağ iletimi cihazları	Orta	Cihaz konfigürasyonu için yöneticiler; veri aktarımı için bütün kullanıcılar
Ağ güvenlik duvarı	Ağ güvenliği	Yüksek	Cihaz konfigürasyonu için yöneticiler; veri aktarımı için bütün kullanıcılar
Veritabanı Uygulaması	Ağ uygulaması	Orta veya Yüksek	Sistem yönetimi için yöneticiler; veri güncelleme-leri için “öncelikliler“; veri erişimi için kullanıcılar; diğerlerine kısmi erişim hakkı.

Çizelge 3.1: Ağ Sistem Elemanlarının Risk Seviyesi Sınıflandırılması

Ayrıca kurum kullandığı IP/IPX ağlarını ve hangi alt ağların (subnet) hangi alt bölümler için kullandığını belirlemesi gerekmektedir. Bölümlerin hangi diğer bölümlere hangi protokolleri kullanarak erişim yapacağı da güvenlik matrisi ile belirlenebilmektedir.. Örneğin Çizelge 3.2’de hangi birimin (alt ağın) hangi birime erişim hakkı olduğu belirtilmektedir. Bu çizelgeye göre; bilgi işlem ve idari bölümler diğer bütün ağlara ulaşabilirken, diğer birimlerin erişimleri kısıtlanmaktadır. Bu tür çizelgeler daha ayrıntılandırılarak birimlerin kendi içlerinde sunucu(server), protokol, kişi tabanlı erişim tanımlamaları da yapılabilir.

	Bilgi İşlem	ArGe	Muhasebe	Satın Alma	İdari	İnternet
Bilgi İşlem	√	√	√	√	√	√
ArGe		√				√
Muhasebe			√			
Satın alma			√	√		
İdari	√	√	√	√	√	√

Çizelge 3.2: Birimlerin Birbirlerine Ağ Üzerinden Erişim Hakları

4. GÜVENLİK POLİTİKASININ UYGULANMASI

Kurumun gereksinimlerinin belirlenmesi ve risk analizi sonucunda güvenlik politikası bir sorumlu veya bir kurul tarafından oluşturulmaktadır. Güvenlik politikası uygulanmadan önce aşağıdaki koşullar sağlanmalıdır:

- Politika hazırlanırken katılım sağlanmalıdır: Güvenlik politikası oluşturulurken mümkün olduğunca çok kişinin katılımı sağlanmalıdır. Kullanıcılar ile çeşitli toplantılar yapılarak kurallar şekillendirilmelidir. Ama bunun mümkün olmadığı durumlarda en azından birimlerin yerel sistem yöneticileri ve sunucuların yöneticileri ile iletişim sağlanmalıdır. Ege Üniversitesi Network Yönetim Grubu, oluşturduğu “adminduyuru” listesi ile bu birimlere e-posta aracılığı ile ulaşmaktadır. Yakın bir zamanda da güvenlik politikasının tartışılabileceği forum gibi ortamların oluşturulması planlanmaktadır.
- Politika standartlara uyumlu olmalıdır: Kurumların güvenlik ortamları bazı nedenlerle birbirinden kopuk ve parçalı hale gelebilir. Bu durumlara örnek olarak şirket birleşmeleri ve bölünmeleri verilebilir. Ayrıca ortak kurumlar, çalışanlar ve müşterilere hizmet ulaştırmak da gerekecektir. Sonuç olarak her bir bölüm için ayrı politikalar oluşturulması gerekebilmektedir. Farklı güvenlik uygulamalarının ve politikalarının birbiriyle uyumlu çalışmasının gerekliliği güvenlik politikalarını tanımlarken bazı standartların kullanılmasını gerektirmektedir. Bu konudaki standartlara örnek olarak IETF’in “Security Policy Specification Language“ (SPSL), Sun Systems’in “Generic Security Services API“ (GSSAPI) ve “Pluggable Authentication Modules“ (PAM) verilebilir.
- Yönetimin onayı alınmalı ve politika duyurulmalıdır: Bu tür güvenlik politikalarını devreye almadan önce kurum yönetiminin onayı alınmalı, mümkünse kurum yöneticisi tarafından bu güvenlik politikası resmi yazı ile bütün birimlere duyurulmalıdır. Bu yazıda güvenlik politikasının oluşturulma nedenleri ve güvenlik politikasının ana hatları verilmeli, daha ayrıntılı bilgi için kullanılacak erişim bilgileri de belirtilmelidir. Yönetimsel destek alınmayan ayarlamaların ve kısıtlamaların birçok soruna yol açabileceği unutulmamalıdır. Aynı zamanda bir web sayfası aracılığı ile kullanıcıların her an güvenlik politikasına erişebilmeleri sağlanmalıdır. Ege Üniversitesi’nde <http://security.ege.edu.tr/guvenlik.php> adresinden kullanılan güvenlik politikasına ulaşılabilen ve duyuru düzenekleriyle değişiklikler kullanıcıya ulaştırılmaktadır.
- Acil durum politikası oluşturulmalıdır: Güvenlik matrisinde özellikle risk düzeyi yüksek olan sistemlerin bir saldırı veya doğal afet sonucunda devre dışı kalması durumunda ne tür önlemlerin alınacağı acil durum planı oluşturularak belirlenmelidir. Bu tür planın sistem yedeklemesine gereksinim duyacağı açıktır. Sistemde önemli bilgilerin düzenli olarak yedeklenmesine de önem gösterilmelidir.

Politikalar oluşturulduktan ve duyurulduktan sonra uygulanmalıdır. Politikada belirtilen kuralların uygulanması için korunacak sistemler üzerinde veya ağ cihazlarında gerekli teknik ayarlar yapılmalıdır. Örneğin güvenlik matrisinde oluşturulan erişim kuralları ve hangi sunuculara hangi protokoller üzerinden erişilebileceği güvenlik duvarı veya erişim listeleri (access-list) yöntemleri kullanılarak oluşturulmalıdır. Fakat daha önemlisi ayarlanan güvenlik sistemleri sık sık sınanmalı, risk haritası çıkarılmalı, sistemin zayıf noktaları saptanıp gerekli önlemler alınmalıdır. Logların incelenmesi ile güvenlik politikasının amacına ulaşip ulaşmadığı anlaşılabilir.

5.SONUÇ

Bilgisayar ağlarında güvenlik politikasının uygulanması kritik önem taşımaktadır. Kurumsal güvenlik için öncelikle yazılı olarak kurallar belirlenmelidir. Bir güvenlik politikası yaratmanın en önemli adımı planlamadır. Güvenlik politikası oluşturulurken kurumun en alt düzeylerine kadar inerek gereksinimler belirlenmelidir. Aynı zamanda oluşturulan politikalar dikkatli bir şekilde uygulanmalıdır. Güvenlik politikasının etkin olması için üst yönetimin desteği sağlanmalı ve kurumun çalışanları kullanılan politika konusunda bilgilendirilmelidir.

Güvenlik politikaları bir kez hazırlanıp sonra değişmeyen kurallar değildir. Güvenlik politikası değişen tehditlere, zayıflıklara ve kurum politikalarına göre yeniden değerlendirilmeli ve gerekli değişiklikler yapılmalıdır.

KAYNAKLAR

- [1] Scott Barman, Writing Information Security Policies, New Riders Publishing, 2001
- [2] Lütfi Yelkenci, Güvenlik Politikasız Güvenlik Nereye Kadar?, 2002, <http://www.guvenlikhaber.com/koseyazisi.asp?ID=8>
- [3] The SANS Security Policy Project, <http://www.sans.org/resources/policies>, 2003
- [4] Türker Cambazoglu, Bilişimde Güçlü Güvenlik Politikalarından Ne Anlıyorsunuz? (I-II) <http://www.bilisimrehber.com.tr>
- [5] How to Develop a Network Security Policy , An Overview of Internetworking Site Security, Sun Microsystems
<http://www.sun.com/software/whitepapers/wp-security-devsecpolicy/>
- [6] J.P. Holbrook, J.K. Reynolds, The Site Security Handbook, RFC 1244, Jul-01-1991, <http://rfc.net/rfc1244.html>
- [7] Acceptable Use Policy Template, SANS Enstitute,
http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf
- [8] Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) "Kabul Edilebilir Kullanım Politikası" Sözleşmesi, <http://www.ulakbim.gov.tr/ulaknet/AUP.uhtml>
- [9] Karaarslan Enis, Ağ Güvenlik Duvarı Çözümü Oluşturulurken Dikkat Edilmesi Gereken Hususlar, Akademik Bilişim 2003
- [10] 10 Tips for Creating a Network Security Policy, <http://secinf.net>
- [11] Burç Yıldırım, Burak Dayıoğlu, Kurumsal Güvenlik, <http://www.dikey8.com/>
- [12] Ege Üniversitesi Network Güvenlik Grubu, Şifre Seçimi,
<http://security.ege.edu.tr/dokumanlar.php>
- [13] Karaarslan Enis, "Network Cihazlarının ve Sistemlerinin Güvenliği", inet-tr 2002 Konferansı
- [14] Network Security Policy: Best Practices Whitepaper, Cisco Systems,
<http://www.cisco.com/warp/public/126/secpol.pdf>