TÜRK BİLİM ARAŞTIRMA VAKFI
TÜBAV
1995
TURKISH SCIENCE-RESEARCH FOUNDATION
TUBAV BILIM DERGISI

Yıl:2014 ,Cilt: 7, Sayı: 2, Sayfa: 16-31

KURUMSAL AĞ VE SİSTEM GÜVENLİĞİ POLİTİKALARININ ÖNEMİ VE BİR DURUM ÇALIŞMASI

Özgü Can[1*], M. Fatih Akbaş[2]

[1]Ege Üniversitesi Bilgisayar Mühendisliği Bölümü, Bornova-İzmir, Türkiye
[2]İzmir Kâtip Çelebi Üniversitesi, Bilgi İşlem Daire Başkanlığı, Çiğli-İzmir, Türkiye

Özet

Ağ ve sistem güvenliği politikaları, kurum ağında ve sistemlerde oluşabilecek durumları yetkili/güvenli ve yetkisiz/ güvensiz olmak üzere ikiye ayıran yazılı kurallar bütünüdür. Güvenlik politikaları gizlilik, bütünlük ve erişilebilirlik prensiplerini bir bütün halinde ele almaktadır. Kurumsal güvenlik politikaları, kurum bünyesindeki bilişim kaynaklarının güvenli bir şekilde nasıl kullanılması gerektiğine dair bir plan sunmakta ve kurumun bilgi güvenliğini tehdit eden durumların önüne geçebilmek için izlenmesi gereken kuralları belirlemektedir. Ağ güvenliği politikaları, sadece kurum dışından gelebilecek güvenlik tehditlerini değil, kurum içinden gelebilecek güvenlik tehditlerini de ele almalı ve güvenliği bir bütün halinde değerlendirmelidir. Bilişim kaynaklarına yönelik güvenlik tehditleri, kurum dışından olduğu kadar kurum içinden de kaynaklanabilmektedir. Bu nedenle, kurumsal güvenlik politikaları oluşturulması gerekmektedir. Güvenlik politikaları, kurum bünyesindeki bilişim kaynaklarının daha verimli kullanılmasını sağlamaktadır.Bu çalışma kapsamında; saldırı aşamaları açıklanmakta, saldırı yöntemlerine ve türlerine örnekler verilmekte, saldırılardan korunma mekanizmaları ayrıntılı olarak anlatılmaktadır.Saldırı türleri ile alt güvenlik politikaları ilişkilendirilerek, saldırı türlerine karşı uygulanacak güvenlik politikaları açıklanmaktadır. Ayrıca, kurumlar için ağ güvenliğinin önemine ve amacına değinilmekte, ağ güvenliği politikaları hazırlanırken dikkat edilmesi gereken durumlar açıklanmaktadır. Bu amaçla, İzmir Kâtip Çelebi Üniversitesi bünyesinde uygulanması düşünülen ağ ve sistem güvenliği politikası durum çalışması verilmektedir.

Anahtar Kelimeler: Güvenlik politikaları, ağ güvenliği, sistem güvenliği, güvenlik tehditleri.

IMPORTANCE OF INSTITUTIONAL NETWORK AND SYSTEM SECURITY POLICIES AND A CASE STUDY

Abstract

Network and system security policies are written rule sets which divide the states that may occur in institutional networks and systems as authorized/secure and unauthorized/insecure. Security policies handle confidentiality, integrity and availability in an integrated fashion. Institutional security policies present a plan of how must institutional information resources be used in a secure way and specify rules in order to prevent information security threats. Network security policies must not only evaluate the non-institutional security threats, but also threats that could come inside the institution and handle security in an integrated manner. Security threats to information resources may have its source inside the institutional as well as the non-institutional. Thus, institutional security policies should be created. Security policies provide an efficient usage of information resources inside the institution. In this work; threat phases are explained, threat methods and types are exemplified, threat protection mechanisms are explained in a detailed manner.Security policies that will be applied against the threat types are explained by correlating threat types and sub security policies. Besides, the importance and the objective of network security for institutions are mentioned, the noteworthy states during the creation of network security policies are explained. For this purpose, a case study of a network and system security policy, which is going to be used within theUniversity of Izmir Kâtip Çelebi, is being given.

Keywords: Security policies, network security, system security, security threats.

*E-posta: ozgu.can@ege.edu.tr

1. Giriş

Bilgi teknolojilerindeki hızlı gelişmeler ve internetin yaygın kullanımı sonucunda, kurumlar için bilgisayar ağlarının ve sunucuların güvenliğinin sağlanması önemli bir konu haline gelmiştir. Özellikle, bilgi-yoğun (knowledge-intensive) bir ortam sunan üniversite kampüs ağları; öğretim, araştırma ve yönetim alanlarında çok önemli bir rol oynamaktadır. Üniversiteler, kampüs ağlarını daha güvenli ve kararlı bir duruma getirmek için yüksek bütçeler ayırmakta ve ciddi yatırımlar yapmaktadırlar. Bu doğrultuda alınan güvenlik cihazları, daha çok kurum dışından gelen saldırıları engellemek amacıyla kullanılmakta ve kurum içi ağ güvenliği koruması ve kontrolü göz ardı edilmektedir. Bu nedenle, ağ güvenliğini tümüyle ele alan bütünleşik bir koruma sistemi oluşturulmalıdır [1].

Ağ güvenliğinin sağlanması, güvenlik politikalarının oluşturulması, hazırlanan politikaların uygulamaya konulması ve güvenlik duvarı politika yönetimi sistemlerinin kullanımı gibi konularda yapılan araştırmalarda, ağ güvenliğinin sağlanmasında güvenlik politikalarının merkezi ve önemli bir rol oynadığı belirtilmektedir [2]. Bu çalışmalarda, saldırı tespitinin yapılması, ağ trafiğinin analiz edilmesi ve ağın gözlemlenmesi gibi güvenlikle ilgili önemli kavramlara değinilmekte ve ağ güvenliği, bilgisayar sistemleri güvenliğinin bir alt kümesi olarak değerlendirilmektedir [3].

Bilgisayar ağlarına ve sunuculara içeriden veya dışarıdan yapılan saldırılar ya da kullanıcıların farkında olmadan yaptıkları hatalar, kurum için kritik olan bilgilerin yetkisiz kişiler tarafından okunmasına ya da değiştirilmesine neden olmaktadır. Bu nedenle, kurum ağı, bilgi güvenliğinin üç temel prensibi olan gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) kapsamında, içeriden veya dışarıdan gelebilecek tehditlerden korunmalıdır. Bu amaçla, ağ güvenliği politikalarının oluşturulması ve uygulanması kurumların bilgi güvenliğinin sağlanabilmesi için önemlidir.

Ağ ve sistem güvenliği politikalarının, kurumun bilişim kaynakları üzerinde herhangi bir güvenlik sorunu yaşanmadan önce oluşturulması önemlidir. Bir güvenlik politikası oluşturmanın en önemli adımı planlamadır. Planlama, kurumun güvenlik gereksinimleri göz önüne alınarak dikkatli bir şekilde yapılmalıdır [4]. Ağ güvenliği politikası, güvenli bir bilgisayar ağının nasıl olması gerektiğini tanımlayan ve ağ üzerindeki kaynakların kullanımını belirleyen yazılı kurallar bütünüdür. Politika, kurumun sahip olduğu bilişim kaynaklarını ve bilgiyi nasıl kullanacaklarını net bir şekilde belirtmektedir. Tüm politikaların tek bir dokümanda bulunması yerine, en üst seviyede genel kuralları barındıran bir bilgi güvenliği politikasının oluşturulması ve bu dokümanla diğer alt politikaların ilişkilendirilmesi önerilmektedir [5].

Bu çalışmada, bilgi kaynaklarına yönelik güvenlik tehditleri açıklanmakta ve bu tehditler doğrultusunda kurumsal güvenlik politikalarının önemine değinilmektedir. Bu amaçla, kurumsal güvenlik politikaları hazırlanırken dikkat edilmesi gereken unsurlar incelenerek, bilgi-yoğun üniversite kampüs ortamı için bir durum çalışması verilmektedir. Bu çalışmanın ikinci bölümünde, ağ güvenliği ile ilgili temel kavramlar tanımlanmakta, ağ güvenliği politikasının amacı, çeşitleri ve iyi bir güvenlik politikasının sahip olması gereken karakteristikler anlatılmaktadır. Üçüncü bölümde, ağ güvenliğini tehdit eden saldırı türlerinden ve bu saldırılardan korunma yollarından bahsedilmektedir. Dördüncü bölümde, bu çalışma kapsamında İzmir Kâtip Çelebi Üniversitesi'nde uygulanması düşünülen ağ ve sistem güvenliği politikasına yönelik bir durum çalışması verilmektedir.Beşinci bölümde, yedekleme ve iş sürekliliği kapsamında alınan önlemler anlatılmaktadır. Altıncı bölümde, gerçekleştirilen çalışma özetlenmektedir.

2. Güvenlik Politikaları ve Önemi

Bu bölümde, ilk olarak güvenlik ile ilgili temel kavramların tanımları verilmektedir. Temel kavramların açıklanmasından sonra güvenlik politikaları ve kurumsal güvenlik politikalarının önemi anlatılmaktadır.

2.1 Kavramlar

Güvenliğin üç temel prensibi olan gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability) kavramları ile ağ ve sistem güvenliğinde yaygın olarak kullanılan kimlik denetimi (authentication), inkâr edememe (non-repudiation), günlük kayıtları (logs) ve izlenebilirlik (accountability) kavramları aşağıda tanımlanmaktadır:

- *Gizlilik (Confidentiality):* Bilgiye ya da kaynağa sadece yetkili kişiler tarafından erişilmesi, yetkisiz kişilerin bilgiye ya da kaynağa erişiminin engellenmesidir.

- *Bütünlük (Integrity):* Verinin yetkilendirilmemiş bir şekilde değişiminin engellenmesidir. Verinin bozulması, değiştirilmesi ya da silinmesi gibi durumların önlenmesi amaçlanmaktadır.

- *Erişilebilirlik (Availability):* Bilginin sürekli ulaşılabilir ve kullanılabilir olması amaçlanmaktadır. Verilere erişim yetkisi olan kullanıcıların, ağlara, sunuculara ve veritabanı gibi uygulamalara güvenilir bir şekilde ulaşıp işlemlerini gerçekleştirmeleri sağlanmalıdır.

- *Kimlik Denetimi (Authentication):* Bilgiye, sisteme veya ağa erişmek isteyen kişinin gerçekten iddia ettiği kişi olduğundan emin olunması gerekmektedir. Kullanıcıların kişisel bilgisayarlarında kullandıkları şifreler, bir sisteme erişilmek istendiğinde kullanılan kullanıcı adı ve şifre, günümüzde kullanımı giderek yaygınlaşan biyometrik sistemler de birer kimlik denetim mekanizmasıdır.

- *İnkâr Edememe (Non-Repudiation):* Veri iletişiminde mesajı gönderenin veya mesajı alanın, gönderdiği veya aldığı mesajı inkâr edememesi durumudur. Bu durumda, mesajın gönderilmiş olduğu ve alınmış olduğu garanti edilmektedir.

- *İzlenebilirlik (Accountability):* Ağ üzerinde veya herhangi bir sistem üzerinde gerçekleşen her türlü olayın, sonrasında incelenmek üzere kayıt altına alınmasıdır. Herhangi bir web sayfasına bağlanılması, sunucuya erişim, e-posta gönderimi gibi durumlar birer izlenebilirlik örneğidir. Depolanan olay kayıtları, ağa veya sisteme yönelik saldırı desenlerinin çıkartılmasında, saldırganların tespit edilmesinde ve alınması gereken önlemlerin belirlenmesinde kritik bir rol oynamaktadır.

2.2 Güvenlik Politikaları

Politika bir kurallar bütünüdür ve sistemin davranış seklini belirten bir durumdur [6].Bir servisi, kimin ve hangi koşullar altındakullanabileceğini, bilginin servise nasıl sağlanacağını vesağlanan bilginin nasıl kullanılacağını belirtir [7]. Kurum güvenlik politikası, kurumun sahip olduğu teknoloji altyapısına ve bilgi varlıklarına erişmesine izin verilen kişilerin uymak zorunda olduğu kuralların resmi olarak beyanıdır [8]. Bir sistem için veya sistemlerin oluşturduğu küme için "güvenli" tanımını yapan yazılı ifadelerdir. Güvenli olan bir sistem, yetkilendirilmiş bir durumda çalışmaya başlayan ve yetkilendirilmemiş duruma girmeyen sistemdir [9].

Ağ güvenliği politikaları, internet güvenliğini sağlayan cihazlar üzerinde gizlilik, bütünlük ve erişilebilirlik prensiplerini yerine getirmekte, trafik filtreleme ve kimlik denetimi gibi mekanizmaların uygulanmasını sağlamaktadır. Hazırlanan politikalar, güvenlik duvarları (firewall), saldırı tespit ve önleme sistemleri (intrusion detection and prevention system, IDS/IPS), web filtreleme (web filtering) ve uygulama kontrolü (application control) mekanizmaları gibi ağ güvenliğinin sağlanmasında kullanılan cihazlar üzerinde yürütülmektedir. Cihazlar üzerinde kuralların oluşturulması sürecinde dikkatli olunması gerekmektedir. Aynı hedefteki aynı işlem için farklı kurallar/politikalar tanımlanmış olabilir [6]. Böyle bir durumda çelişki meydana gelecektir. Ağ üzerindeki kuralların birbirleriyle olan etkileşimleri ve kural bağımlılıklarının olması tutarsızlığa, karmaşıklığa ve güvenlik açıklarının oluşmasına sebep olabilmektedir. Özellikle ağın büyüklüğü arttıkça karmaşıklık da artmaktadır. Bu nedenle, filtrelemenin söz konusu olduğu ağ güvenliği politikalarında, çelişen kuralların önüne geçmek için, geniş kapsamlı bir sınıflandırma yapılmalıdır [10].

Ağ ve sistem güvenliğinin sağlanması sürecinde; öncelikle risk analizi yapılmalı, takip eden süreçte ise güvenlik politikası oluşturulmalıdır. Bu doğrultuda, güvenlik duvarları, saldırı tespit ve önleme sistemleri, anti-virüs sunucuları gibi güvenlik mekanizmaları kullanılmalıdır. Bu süreç üç aşamada özetlenmektedir [11]. Bunlar;risk analizi çalışması, güvenlik ve kabul edilebilir kullanım politikasının oluşturulması ve güvenlik önlemlerinin alınmasıdır. Güvenlik politikası metni temel olarak aşağıda belirtilen başlıklara sahip olmalıdır [12]:

- Genel açıklama bölümü
- Politikaya neden ihtiyaç duyulduğuna dair amaç bölümü
- Politikanın neleri ve kimleri içine aldığını belirten kapsam bölümü
- Politika kapsamında belirtilen esaslara uyulması amacıyla hedef kitleye ilgili tavsiyeleri ve bildirimleri içeren bölüm
- Politika metninin ana kısmını oluşturan ve uyulması gereken esasları maddeler halinde ifade eden kurallar
- Teknik terimlerin açıklandığı tanımlar bölümü

- Politika metninin güncellenmesi gerektiği durumlarda ilgili değişiklerin yansıtılabilmesi için doküman versiyon numarası

Bilgisayar ağının tasarımını, bilginin gizlilik derecesini, kullanıcı haklarını ve sorumluluklarını bir bütün halinde ele alan güvenlik politikası ideal güvenliğin temelini oluşturmaktadır. Güvenlik politikalarının oluşturulmasında; kimlere, hangi sistemlere, ne zaman ve hangi yetkilerle izin verileceği, hangi aktivitelerin güvenlik riski oluşturacağı, kullanıcıların haklarının ve sorumluluklarının neler olacağı dikkat edilmesi gereken unsurlardır [13].Böylece, hazırlanan politika ile kurallar ve standartlar belirlenmektedir.

Güvenlik önlemi olarak, özellikle geniş ölçekli kurumsal ağlarda, güvenlik duvarı kullanımı çok önemlidir. Güvenlik duvarları, ağ güvenliğinin sağlanmasında kritik bir rol oynayan çekirdek (core) unsurlardır. Fakat ağ büyüdükçe buna bağlı olarak yazılan kuralların sayısı arttığından, karmaşıklık durumu da artmaktadır. Kuralların çelişmesi durumunda veya kuralların sıralamasına dikkat edilmediğinde, bir kuralın diğer bir kuralı etkisiz hale getirmesi gibi durumların engellenmesi gerekmektedir. Bu amaçla, bir takım algoritmalar ve teknikler geliştirilmiştir. "Firewall Policy Advisor" [14] adı verilen araç, güvenlik duvarı üzerinde bulunan kurallarla ilgili anormallikleri otomatik olarak keşfetmeyi sağlamaktadır. Bu araç ile aynı zamanda güvenlik duvarı üzerindeki kuralların yanlış yapılandırılmasından dolayı oluşabilecek zayıflıklar en aza indirilmektedir [14].

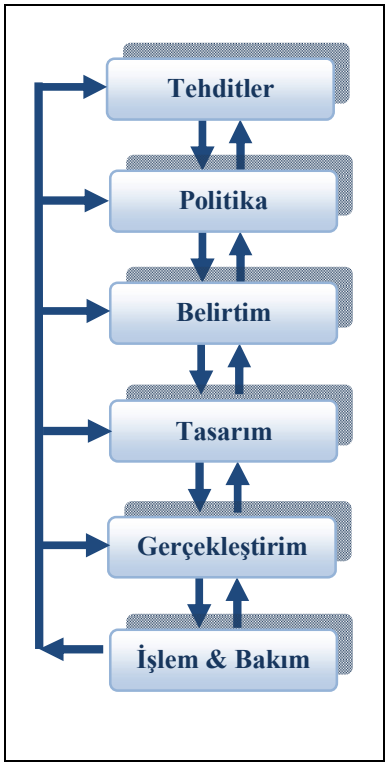
2.3 Kurumsal Güvenlik Politikalarının Önemi

B2B Internationalve Kaspersky Lab. tarafından yapılan "Global Kurumsal BT Güvenlik Riskleri 2013" [15] araştırmasında, 2013 yılı içerisindeTürkiye'de kurumların %92'sinde hassas veri kaybı yaşandığı belirtilmektedir. Araştırmada, kurum içi karşılaşılan en yaygın üç tehdidin, kullanılan yazılımlardaki güvenlik açıkları, insan hatası kaynaklı veri sızıntıları ve mobil cihazların kaybolması ya da çalınması olduğu belirtilmiştir. Ayrıca, çalışanların mevcut kurumsal güvenlik politikalarına her zaman uygun davranmadığı ve şirketlerin %47'sinin güvenlik politikalarının ihlâli durumlarında uygulanması gereken yaptırım ve disiplin işlemlerini net bir şekilde ortaya koymadığı ifade edilmektedir [15].

Güvenlik politikaları, kurumda güvenliğin önemini belirten unsurlardır. Yetkisiz erişim, kötü amaçlı kodların (malware) gönderilmesi, servislerde kesintiye uğratma (DoS ve DDoS atakları) gibi güvenliği tehdit eden durumlardan korunmak için öncelikle güvenlik politikalarının oluşturulması gerekmektedir. Bu durumlarda dikkate alındığında, güvenlik politikalarının kurumlara getirdiği önemli faydalar söz konusudur. Bunlardan bazıları aşağıda belirtilmektedir [16]:

- Kurum çalışanlarını ve üçüncü tarafları yasal sorumluluktan kurtarmaktadır.
- Kurumu; kuruma ait gizli bilgilerin, yetkisiz kişilerin eline geçmesi, ortaya çıkarılması ve değiştirilmesi durumlarına karşı korumaktadır.
- Kurumun bilişim kaynaklarının boşa kullanımını ve israfını engellemektedir.

Gelişen teknoloji ile birlikte sürekli olarak yeni tehditlerin ortaya çıkması, öncesinde güvenli olarak kabul edilen bir sistemi güvensiz hale getirebilmektedir. Bu nedenle, güvenlik çalışmaları bir yaşam döngüsü ile modellenmektedir. Şekil 1'degüvenlik yaşam döngüsü gösterilmektedir [17]. Güvenlik yaşam döngüsünde, her bir aşama önceki ve bu aşama boyunca bütün önceki aşamalara bir geri bildirim sağlamaktadır.Geribildirim için denetleme (auditing) kullanılmaktadır. Denetlemede, sistemin işleyişi ve analizi kaydedilmektedir. Böylece, analist problemleri belirleyebilmektedir.



Şekil 1.Güvenlik yaşam döngüsü.

İyi bir güvenlik politikası çeşitli özelliklere sahip olmalıdır. Bu özellikler aşağıdaki gibi listelenmektedir [18]:

- Politika metni, basit ve açık olmalı, çok uzun olmamalıdır.
- Özel ve teknik tanımlamalar içermeyen kolay anlaşılabilir bir dille yazılmalıdır.
- Politika ve prosedür kavramları birbirinden ayırt edilmelidir.
- Kullanıcıların gerektiğinde sorularını sorabilecekleri güncel bir iletişim bilgisi içermelidir.

Bu maddelere aşağıda belirtilen özellikler de eklenmelidir:

- Güvenlik hedefleri açıkça belirtilmeli ve politika metni maddeler ile açıklanmalıdır.
- Politikanın, kurumun tüm çalışanları tarafından kolaylıkla erişilebilir olması önemlidir. Bu doğrultuda politika kurumun web sayfasında yayınlanmalıdır.
- Politikada, kurum çalışanlarının görev ve sorumluluklarına da yer verilmelidir.
- Politikaya uyulmayan durumlarda nasıl hareket edileceği açıklanmalı ve tanımlanmayan konularda kurumun tutumunu içermelidir.

Her kurum, güvenlik politikasını kendi ihtiyaçları doğrultusunda ve bireylerden bağımsız şekilde hazırlamalıdır. Güvenlik politikaları oluşturulurken üst yönetimin desteği mutlaka alınmalı ve politika çalışanlar tarafından benimsenmelidir. Üst yönetimin kurumda bilgi güvenliğini sağlama amacı, politikada bulunması gereken en önemli unsurlardan biridir. Üst yönetimin desteği, kurumda bilgi güvenliğinin sağlanmasında gereken kararlılığının gösterileceğini ifade etmekte ve kurum çalışanlarının bilgi güvenliğine daha çok önem vermesini sağlamaktadır [19].

Güvenlik politikası, ağ güvenliği yöneticisi tarafından kolay yönetilebilir, son kullanıcılar tarafından ise anlaşılabilir ve uygulanabilir olmalıdır. Politikanın sürekli güncellenebilir olması da dikkat edilmesi gereken önemli noktalardan biridir. Ayrıca, kurum bünyesinde güvenlik kültürünün geliştirilmesi için çalışanların bilinçlendirilmesi de önemli bir rol oynamaktadır. Bu doğrultuda, düzenlenen seminerler ve farkındalık eğitimleri güvenliğin öneminin kavranmasında etkili olmaktadır. Özellikle şifre seçimi, ekran kilitleme, doküman etiketleme ve fiziksel güvenlik (kapı güvenliği vb.) gibi konularda alınması gereken temel güvenlik önlemlerinin önemikullanıcılara anlatılmalıdır.

Bununla birlikte; kullanıcılara yönelik güvenlik ipuçlarını içeren posterlere basılmalı ve aylık olarak e-posta duyuruları gönderilmelidir.

3. Ağ Güvenliğini Tehdit Eden Saldırılar ve Önlemler

Ağ güvenliğini tehdit eden saldırılar, kuruma ait bir sistemin veya herhangi bir bilişim kaynağının zarar görmesine neden olabilecek istenmeyen olaylardır. Tehditler kaynakları açısından insan ve doğal afet kaynaklı olmak üzere iki gruba ayrılmaktadır. Doğal afet kaynaklı tehditlergenellikle önceden tespit edilemezler. Deprem, yangın, sel, vb. doğal afetler bu tür tehditlere örnektir.İnsan kaynaklı tehditler kötü niyetli olan ve olmayan davranışlardır. Kötü niyetli olmayan davranışlar; kullanıcının, sistemi dikkatsiz, bilinçsiz ve yeterli eğitime sahip olmadan kullanması sonucu yaşanan istem dışı problemlerdir.Kötü niyetli davranışlar ise ağ üzerindeki cihazlara veya sistemlere zarar vermek amacıyla yapılan kötü niyetli ve amaçlı davranışlardır. Bu tarz tehditler, sistemde bulunan güvenlik boşluklarından yararlanmaktadır.Bu bölümde, kötü niyetli davranışlar sonucu oluşan insan kaynaklı tehditler açıklanmaktadır.

3.1 Saldırı Çeşitleri

Bilgisayar ağlarına ve sistemlerine yapılan saldırılarda, kullanılan yöntem ve tekniklerin iyi bilinmesinin, saldırı karakteristiklerinin çıkarılmasının ve saldırgan profillerinin analiz edilmesinin güvenliğin sağlanması açısından alınacak önlemlerde faydalı olacağı belirtilmektedir [20]. Ağ ve sistem güvenliğini ihlâl eden saldırganlar, çeşitli yöntemlerle bu amaçlarını gerçekleştirmektedirler. Saldırıların karakteristiği dört ana başlıkta toplanmaktadır [21]:

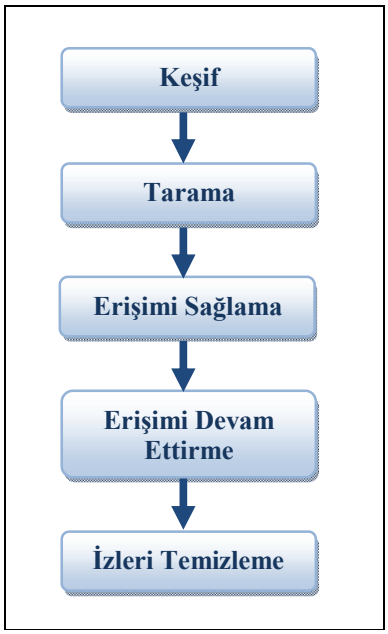
- *Engelleme (Interruption):*Kaynak ve hedef sistemler arasında bilgi akışı engellenmektedir. Böylece, bilgiye erişim engellenmiş olmaktadır. DoS, DDoS gibi servis reddi saldırıları örnek olarak verilebilir.

- *Dinleme (Intercept):*Kaynak ile hedef sistemler veya bilgisayarlar arasındaki iletişimin dinlenmesi yolu ile verinin okunmasıdır. Yetkisiz erişim durumu söz konusudur ve güvenliğin gizlilik prensibi ihlâl edilmektedir. Pasif bir saldırı türüdür. Ağda dolaşan paketlerin görüntülenmesi ve kaydedilmesi yöntemi olan ağ koklama (network sniffing) bu saldırıya örnektir.

- *Değiştirme (Modification):*Kaynak bilgisayardan hedef bilgisayara gönderilen verinin, araya giren saldırgan tarafından değiştirilmesi ve içeriği değiştirilen verinin hedef bilgisayardan geliyormuş gibi gönderilmesidir. Bu saldırı karakteristiğinde, güvenliğin bütünlük prensibi ihlâl edilmektedir. Bunun için virüsler, solucanlar ve truva atları gibi kötü amaçlı yazılımlar kullanılmaktadır.

- *Üretim/Uydurma (Fabrication):*Bu saldırı türünde, saldırgan tarafından üretilen yeni bir veri söz konusudur.Saldırı, hedefe sahte verilerin gönderilmesi yoluyla gerçekleştirilmektedir.

Şekil 2'de yer alan saldırı analizi, temel olarak;keşif, tarama, erişimi sağlama, erişimi devam ettirme ve izleri temizleme olmak üzere beş aşamada incelenmektedir [22].Keşif aşaması saldırıya hazırlık evresidir. Saldırı yapılacak hedef hakkında toplanabildiği kadar bilgi toplanmaktadır. Kurum çalışanlarının e-posta adreslerinin ele geçirilmesi bu aşamaya bir örnektir. Tarama, saldırı öncesi son hazırlıkların yapıldığı aşamadır. Keşif aşamasında elde edilen bilgiler ile çeşitli tarama işlemleri gerçekleştirilmektedir. Ağ topolojisinin çıkartılması, port tarama (port scanning), saldırıya açıklığı tarama (vulnerability scanning), sunucu üzerinde çalışan işletim sistemi hakkında bilgi edinmek gibi davranışlar bu aşamada yapılabilecek işlemlerdir. Erişimi sağlama, saldırının gerçekleştiği aşamadır. Saldırgan, tarama evresinde tespit ettiği açığı kullanarak sisteme sızmaktadır. Phyton, Perl gibi programlama dilleri ile yazılabilen ve sömürücü (exploit) adı verilen bu zararlı kod parçacıkları, sistemde veya programda bulunan açıklıkları kullanarak hedef sistemin komut satırını almayı, yetkisiz kullanıcılara yönetici yetkilerini kazandırmayı amaçlamaktadır.Erişimi devam ettirme aşamasında, saldırgan tarafından ele geçirilmiş olan sistemin açıklığının kullanılmasına devam edilmesi amaçlanmaktadır. Böylelikle, ele geçirilmiş olan sistem aracılığıyla saldırgan ağ üzerindeki diğer sistemlere de erişebilmektedir. Saldırgan, bu amaçla truva atları (trojan horse), kök kullanıcı takımları (rootkit), arka kapılar (backdoor) gibi zararlı yazılımları kullanarak istediği zaman sisteme sızma eylemini gerçekleştirebilmektedir.Son aşama olan izleri temizleme, yapılan saldırıya ait izlerin başkaları tarafından tespit edilmeden ortadan kaldırılması sürecidir. Saldırganın amacı yasal olarak işlemiş olduğu suça ait delilleri ortada bırakmamaktır.



Şekil 2. Bir saldırının analizi.

5651 sayılı "*İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi hakkında kanun*" kapsamında İzmir Kâtip Çelebi Üniversitesi'nde merkezi günlük kayıt (log) depolama ve raporlama sistemi kurulmuştur. Yapılandırması tamamlanmış ve kullanılmakta olan bu sistem ile işlenen günlüklerin özet fonksiyonları (hash) alınmakta ve zaman damgası (time stamp) ile damgalanarak dijital imza ile imzalanmaktadır. Anlık olarak (her saniye) yapılan bu işlem ile günlüklerin içeriğinin değiştirilememesi sağlanmakta ve inkâr edilemezlik ilkesi yerine getirilmektedir. Ayrıca, günlük dosyaları gün içinde belirlenen bir saatte Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nün (UEKAE) sağladığı zaman damgası servisi kullanılarak da damgalanmaktadır. Anlık olarak özet fonksiyonları alınıp imzalanan günlükler sistem üzerinde tutulmayıp, anlık olarak veri depolama ünitesine (storage) alınmaktadır. Özet fonksiyon algoritması (hash algorithm) olarak MD5 [23], imza algoritması (signature algorithm) olarak da RSA [24] kullanılmaktadır. Böylece, 128 bitlik özetler üreten tek yönlü şifreleme algoritması olan MD5 ile veri bütünlüğü sağlanmaktadır. Günlüklerin imzalanması için kullanılan RSA kriptosistemi ile de inkâr edilemezlik ilkesi yerine getirilmektedir.

3.2 Kötü Amaçlı Yazılım Saldırıları

Kötü amaçlı yazılım saldırıları, saldırı analizinde dördüncü aşama olarak belirtilen erişimi devam ettirme aşamasında kullanılmaktadır. Virüsler, solucanlar, truva atları, kök kullanıcı takımları, arka kapılar, sömürücüler, tuş kaydedici (keylogger) yazılımlar ve casus yazılımlar (spyware) temelinde bilgisayar sistemlerine zarar vermek amacıyla yazılmış kötü amaçlı yazılımlardır. Bu yazılımlar karakteristik özelliklerine göre ayrışmaktadırlar:

- *Virüsler (Viruses):*Kendilerini çalıştırılabilir programlara veya dosyalara iliştirebilen programlardır. Kendilerini çoğaltabilme özelliğine sahiptirler. Virüslerin etkilerini gösterebilmeleri için öncelikle kullanıcı tarafından çalıştırılmaları gerekmektedir. Çalıştırıldıktan sonra çoğalarak yayılırlar ve sisteme zarar verirler. İleri seviye virüsler kendilerini oluşturan kod parçacığını değiştirebilme yeteneğine sahiptir.

- *Solucanlar (Worms):*Solucanlar, virüslerin bir alt kümesi olarak nitelendirilmektedirler. Virüslerden ayrıldıkları nokta ise yayılmaları ve çalışmaları için kullanıcı tarafından herhangi bir programın çalıştırılmasına gerek olmamasıdır. İnternette sayfalar arasında gezinirken istenmeden otomatik olarak açılan reklamların linklerine tıklanması sonucu solucanlar bilgisayarlara yüklenebilmektedir. Özellikle, ağ üzerinden diğer sistemlere veya bilgisayarlara bulaşabilme durumları solucanları, virüslere kıyasla daha tehlikeli yapmaktadır. Solucanlar, ağ üzerindeki kaynakların yüksek miktarda tüketimine de sebep olmaktadırlar. Fakat virüsler gibi silme işlemi gerçekleştiremezler.

- *Truva Atları (Trojan Horses):*Aslında yararlı gibi görünen, fakat arka planda kötü niyetli bir şekilde çalışarak kritik bilgileri dışarıya gönderen casus programlardır. Truva atları çalıştırıldığında; bir arka kapı

oluşturularak saldırgana ait dışarıda bulunan sunucu ile bağlantı kurulmaktadır. Saldırgan, şifrelere, e-posta adreslerine, kredi kartı bilgilerine, kişisel belgeler gibi yetkisi olmayan bilgilere erişebilmekte ve bunları kendine yönlendirebilmektedir. Truva atları, kendilerini virüsler gibi kopyalayamazlar. Truva atının gereken işlevini yerine getirebilmesi için öncelikle çalıştırılması gerekmektedir.

- *Kök Kullanıcı Takımları (Rootkits):*En tehlikeli grup olarak nitelendirilen kök kullanıcı takımları bulundukları sistemde kendilerini çok iyi gizleyen programlardır. Kök kullanıcı takımları kendilerini işletim sisteminin derinliklerine saklarlar ve tespit edilebilmeleri güçtür. Bu saldırıda, sistem dosyalarının değiştirilmesi amaçlanmaktadır. Kök kullanıcı takımları, genellikle sistemde bulunan çekirdek (kernel) açıkları kullanılarak, kök (root) yetkisinin kazanılması sonucu bulaşmaktadırlar. Anti-virüs yazılımları kök kullanıcı takımlarını tespit etmekte zorlanmaktadır. Tespit edilse dahi sistemden temizlemek güç olduğundan anti-virüs yazılımlarına ek olarak bir takım güvenlik yazılımları kullanılmalıdır. Bu doğrultuda, sadece kök kullanıcı takımlara yönelik geliştirmiş bazı anti-virüs programlarımevcuttur. Bu kötü amaçlı yazılımlardan korunmak için, kuruma ait bilgisayarlarda, dördüncü bölümde belirtilen anti-virüs politikası uygulanmalıdır.

3.3 Servis Reddi (Denial of Service) ve Dağıtık Servis Reddi (Distributed Denial of Service) Saldırıları

Servis reddi (Denial of Service, DoS) saldırısı, sunucuların veya servislerin aşırı yüklenme sonucu kullanıcılara hizmet veremez hale getirilmesidir. Erişim sağlama evresinde kullanılan bu tip saldırılarda yetkisiz erişim veya sistemin kontrolünü ele geçirmeye yönelik saldırılardan farklı olarak hizmetin kesilmesi veya yavaşlatılması amaçlanmakta, bant genişliğinin tüketilmesi ve CPU'ya aşırı yüklenilmesi hedef alınmaktadır. Hafıza bloğu taşması saldırısı (buffer overflow attack), ölüm ping'i (ping of death), syn saldırısı (syn attack) servis reddi saldırısı örnekleridir:

- *Hafıza Bloğu Taşması Saldırıları (Buffer Overflow):* Değişkenlere (int, char vb. veri tiplerine) varsayılandan daha büyük veriler girilmesi sonucu hafıza taşmasına sebep olan saldırı türüdür. Örneğin, 5 byte veri taşıyabilecek bir değişkene 10 byte kopyalamak hafıza taşması sonucunu doğuracaktır. Bu tipteki saldırılar, programların kilitlenmesine ve yanıt veremez duruma gelmesine neden olmaktadır.Hafıza taşırma saldırılarının önüne geçmek için güvenli fonksiyonlar kullanılmalıdır. Örneğin, "**`strcpy`**" fonksiyonu yerine "**`strlcpy`**" fonksiyonu tercih edilmelidir. Ayrıca, Assembly, C ve C++ yerine bellek taşması kontrolü yapan C# ve Java gibi diller tercih edilmelidir [25].

- *SYN Saldırısı (SYN Attack):*Syn paketleri, istemci ile sunucu arasındaki **`tcp`** trafiğini başlatmak için gönderilen ilk paketlerdir. Syn saldırısında, sunucuya aşırı miktarda syn paketi gönderilerek sunucunun hafıza alanın dolması sağlanmaktadır. Paketlerdeki kaynak IP adresleri geçersizdir ve her gönderilen pakette kaynak IP adresi değiştirilmektedir. Sunucu, gerçek olmayan bu isteklere yanıt vermekle uğraşırken, gerçekten hizmet etmesi gereken kullanıcılara yanıt verememektedir. Syn çerezleri (syn cookies), syn saldırılarına karşı korunmak için kullanılan etkili bir tekniktir.

- *Ölüm Pingi Saldırısı (Ping Of Death):*Ölüm pingi saldırısı (Ping of Death, PoD), bilgisayar sistemlerine 65535 byte'dan büyük bir paket gönderildiğinde oluşan bir saldırı tipidir. Hedef IP adresine kötü amaçlı olarak büyük boyutlu **`icmp`** (internet control message protocol) paketlerinin gönderilmesidir. Ping paketinin boyutu varsayılan olarak 32 byte'dır. Komut satırından yazılabilecek bir komutla (**`ping 192.168.1.1 –t –l 65500`**) hedefe istenen büyüklükte paket boyutu gönderilebilmektedir.

Dağıtık servis reddi (Distributed Denial of Service, DDoS) saldırısı, *zombie* adı verilen birçok köle bilgisayarın bir araya gelerek hedef sisteme dağıtık mimaride ve planlı olarak saldırmasıdır. Erişim sağlama evresi kapsamında koordineli bir şekilde ve dağıtık olarak gerçekleştirilen bu saldırı türü, verilen hizmetin durdurulmasını ve yavaşlatılmasını amaçlamaktadır. Çok fazla sayıda köle bilgisayar kullanılarak yapılan saldırılarda; yüksek bant genişliğine sahip ağda bulunan sunucular gelen servis isteklerine cevap verememektedir. DDoS saldırısında amaç;DoS saldırısında olduğu gibi, ağ bant genişliğinin ve sunuculara ait kaynakların tüketilmesidir. Ancak, DDoS saldırıları, dağıtık yapıda ve çok sayıda köle bilgisayar ile koordineli bir şekilde yapıldığı için DoS saldırılarına nazaran daha tehlikelidir. Bu nedenle, DDoS engellenmesi zor olan bir saldırı biçimidir.

Yaygın olarak gerçekleştirilen DDoS saldırısı türlerinden biriKöle Bilgisayarlar Ağı (Botnet) saldırısıdır. Saldırgan, kendi amaçları doğrultusunda kullanmak istediği bilgisayara kötü amaçlı yazılımlar yükleyerek bilgisayarı internet

robotuna (bot), diğer bir deyişle köle bilgisayar haline getirmektedir. Bot haline gelen bilgisayarlar uzaktan aldıkları komutlarla bir takım zararlı görevleri gerçekleştirmektedir. Bu süreçte, kullanıcı saldırı yaptığının farkında değildir. Köle bilgisayar durumuna gelmiş bilgisayarların oluşturduğu ağa *botnet* denmektedir. Sunuculara saldırmak, istenmeyen e-postalar (spam) göndermek gibi amaçlar doğrultusunda kullanılmaktadır.

Yük dengeleme (load balancing) ve balküpü (honeypot) teknikleri ile DDoS saldırılarının etkileri minimize edilebilir. Yük dengeleme bir işin iki veya daha fazla kaynak arasında paylaştırılmasıdır. Sunucuda bir problem yaşandığında diğer sunucu devreye girerek verilen servislerin devamlılığı sağlanmaktadır. Ayrıca, yük birden fazla sunucu ile dengelenerek performans artışı da sağlanmaktadır. Bu nedenle, özellikle web ve DNS gibi kritik sunucularda yük dengeleme tekniği kullanılmalıdır. Balküpleri, bilgi sistemlerine yapılan saldırıların tespit edilmesi için kurulmuş tuzaklardır. Saldırganın ne tip davranışlarda bulunduğunu gözlemleyen ve analiz eden uygulamalardır. Balküpü uygulaması farklı tipteki saldırı çeşitlerini kendi üzerine çekeceğinden dolayı yapılandırma aşamasında dikkat edilmeli ve trafik kontrol altında tutulmalıdır. TÜBİTAK Ulak-CSIRT bünyesinde yürütülen çalışmalar sonucunda ULAKNET omurgasına bir balküpü uygulaması yerleştirilmiştir. Bu servis kapsamında, balküpü trafiği üzerinde yapılan analiz sonuçlarına ulaşılabilmektedir [26].

3.4 Sosyal Mühendislik Saldırıları

Sosyal mühendislik (social engineering) saldırıları, etkileme ve ikna yöntemlerinden faydalanarak kişiye istenilen işlerin yaptırılması veya istenen bilgilerin ele geçirilmesi sanatı olarak tanımlanmaktadır. Erişim sağlama evresinde gerçekleştirilen bu tip saldırılarda genellikle güvenlik unsurunun en zayıf halkası olarak bilinen insan faktörü kullanılmaktadır. İnsanların inanç, güven, vicdan, korku ve yardım etme duyguları kullanılarak yapılan bilgi hırsızlığı olarak da ifade edilebilecek olan sosyal mühendislik tekniği en tehlikeli saldırı tiplerinden biridir. Saldırganın, kurum içi bir çalışan izlenimi uyandırarak kurum çalışanlarına sorular sorması ve bir takım bilgilere ulaşmaya çalışması, kişilerin acıma duygularından faydalanarak ve aceleci bir dil kullanarak yardım talebinde bulunması gibi senaryolar sosyal mühendislik saldırısı örnekleridir.

Ağ ve sistem güvenliğini sağlamak için güvenlik duvarı, saldırı önleme sistemleri, anti-virüs yazılımları kullanımının yanı sıra bu tip saldırılardan korunmak için çalışanlara öncelikle güvenlik eğitimleri verilerek bilgilendirilmeleri ve bilinçlendirilmeleri gerekmektedir. Bu doğrultuda, sosyal mühendislik saldırılarından korunmak için dördüncü bölümde yer alan şifre politikası, kurum bünyesinde uygulanmalıdır.

Oltalama saldırısı (phishing), bilgisayar tabanlı bir sosyal mühendislik saldırı çeşididir. Saldırgan, genellikle sahte e-postalar göndererek kişilerin şifre ve kredi kartı gibi önemli bilgilerini çalmayı amaçlamaktadır. Kullanıcıları tuzağa düşürmek için gönderilen sahte e-postanın içeriğinde, genellikle bir `url` adresi bulunmaktadır. Bu adres bağlantısına tıklandığında, kişi farklı bir sayfaya yönlendirilmektedir. Örneğin, saldırgan herhangi bir bankaya ait resmi web sayfasının birebir taklidini yaparak, kullanıcının farkında olmadan ilgili alanlara kredi kartı bilgilerini yazmasını sağlamakta ve bu bilgileri arka planda istediği bir adrese yönlendirmektedir. Saldırgan, kişiye e-postanın yetkili ve resmi bir yerden gönderildiği hissini uyandırmaktadır. Ancak, e-postanın içeriği dikkatle incelendiğinde resmi olmayan bir dil kullanıldığı, cümlelerde anlatım bozukluklarının bulunduğu fark edilecektir. Kurumlar kullanıcılarını, e-posta yoluyla kendilerinden kişisel bilgilerinin istenmeyeceği ve bu tarzda gelen e-postalara kesinlikle cevap yazılmaması gerektiği konusunda bilgilendirmelidir. Bu tarz saldırılarla mücadele edebilmek için,dördüncü bölümde anlatılan e-posta ve anti-virüs politikaları izlenmelidir. Ek olarak, bu tarz saldırıların önüne geçmek için, e-posta sunucusunun önüne konumlandırılmış olan e-posta güvenlik cihazı (e-mail security gateway) kullanılmalıdır.

Kurumların bünyesinde bulunan bilgi teknolojilerini saldırılara karşı koruyabilmek için; güvenlik duvarı, saldırı tespiti ve önleme sistemleri, web filtreleme sistemi kullanılması, tüm bilgisayarlara anti-virüs kurulması, erişim denetimi düzeneklerinin uygulanması, sanal yerel alan ağı (virtual local area network, VLAN) yapılandırılması, erişim denetim listesi (access control list, ACL) oluşturulması ve kriptografik tekniklerin kullanılarak şifreleme yapılması gerekmektedir.

4. Ağ ve Sistem Güvenliği Politikası İçin Durum Çalışması

Ağ güvenliği formel politika kurallarını temel almalıdır [27]. Ağ güvenliğinin sağlanmasında etkin politikaların yazılması gereklidir. Bu amaçla; [28] çalışmasında ağların güvenliğinin sağlanması ve etkin bir şekilde yönetilmesi için takip edilmesi gereken standart kurallar ve politikalar açıklanmakta, [29] çalışmasında ise kampus ağ

güvenliğinin sağlanmasına yönelik bir araştırma yer almaktadır.Bu bölümde, İzmir Kâtip Çelebi Üniversitesi bünyesinde uygulanması düşünülen ağ ve sistem güvenliği politikası kapsamında taslak olarak hazırlanan politika kurallarına yer verilmektedir. Bu doğrultuda; politikanın amacı ve genel kuralların yanı sıra internet erişimi ve kullanım politikası, sunucu güvenliği politikası, e-posta politikası, şifre politikası, anti-virüs politikası ve sanal özel ağ politikası alt politikalarına değinilmektedir. Ağ ve sistem güvenliği politikasını oluşturacak olan bu alt politikaların;amaçları, kapsamları ve içerdikleri kural maddeleri taslağı sunulmaktadır.

Farklı kurumların farklı güvenlik ihtiyaçları söz konusu olabilmektedir. Bu güvenlik ihtiyaçlarına yönelik olarak; Kabul Edilebilir Kullanım Politikası, İnternet Erişimi Politikası, Sunucu Güvenliği Politikası, E-Posta Politikası, Şifre Politikası, Anti-Virüs Politikası, Sanal Özel Ağ Politikası, Kimlik Doğrulama Politikası, Kablosuz Erişim Politikası, Misafir Erişim Politikası ve Mobil Cihaz Politikası gibi çeşitli politikalar tanımlanabilmektedir.Kurumlar, güvenlik ihtiyaçları doğrultusunda bu politika çeşitlerinin bir kısmını veya tamamını kendi bünyelerinde uygulamaktadırlar.

Durum çalışması kapsamında; Türkiye Cumhuriyeti İçişleri Bakanlığı Bilgi Güvenliği Politikaları Yönergesi [30], Türkiye Cumhuriyeti Sağlık Bakanlığı Kurumsal Bilgi Güvenliği Yönetim Politikası Yönergesi [31], Gediz Üniversitesi Bilgi ve İletişim Kaynakları Kullanım İlkeleri Yönergesi [32] ve California Üniversitesi'nin kampüs politikaları [18] incelenmiştir.İzmir Kâtip Çelebi Üniversitesi yapısını temel alanağ ve sistem güvenliği politikası durum çalışmasında, öncelikli olarak uygulanması düşünülen genel kurallar ana hatlarıyla belirlenmektedir. Uygulanması düşünülen politikanın amacı ve genel kuralları belirlendikten sonra, alt politikalarda detaylandırmalar yapılmaktadır.

4.1. Amaç ve Genel Kurallar

İzmir Kâtip Çelebi Üniversitesi bünyesinde, ağ ve sistem güvenliğinin sağlanması kapsamında bilişim kaynaklarının nasıl kullanılması gerektiğine yönelik genel kurallar aşağıda maddelerle anlatılmaktadır.

Amaç: Ağ ve Sistem Güvenliği Politikası, İzmir Kâtip Çelebi Üniversitesi bilişim kaynaklarının işleyişlerini, Türkiye Cumhuriyeti'nin ilgili yasalarına ve ULAKNET'in ilgili politikalarına uygun şekilde ve güvenli kullanılması için gerekli kuralları belirlemeyi amaçlamaktadır.

Genel Kurallar:

1. İzmir Kâtip Çelebi Üniversitesi bilişim kaynakları, Türkiye Cumhuriyet yasalarına ve bunlara bağlı yönetmeliklere, üniversite yönetmeliklerine aykırı faaliyetlerde bulunmak amacıyla kullanılamaz.
2. İzmir Kâtip Çelebi Üniversitesi bilişim kaynakları, kurum işlerinin yürütülmesi ve akademik çalışmalar için kullanılmalıdır.
3. İzmir Kâtip Çelebi Üniversitesi bünyesinde, internet erişim hizmetinin alındığı Ulusal Akademik Ağ (ULAKNET) politikalarına uyulmalıdır.
4. İzmir Kâtip Çelebi Üniversitesi bilişim kaynaklarının kullanımı esnasında, kaynakların kullanıcılar arasında adil paylaşımı sağlanmalıdır. Diğer çalışanlara bilişim kaynaklarını kullanım olanağı vermeyecek şekilde trafiğin oluşmasına karşı ve kaynaklara zarar verebilecek tehlikelere karşı güvenlik önlemleri alınmalıdır.
5. İzmir Kâtip Çelebi Üniversitesi bilişim kaynaklarının kullanımı esnasında, ağ ve sistem güvenliğini ihlâl eden durumlara ve girişimlere ilişkin kayıtlar kimlik denetimi mekanizması kullanılarak tutulmalıdır.
6. İzmir Kâtip Çelebi Üniversitesi bilişim kaynakları, genel ahlak kurallarına aykırı, müstehcen ve fikri mülkiyet haklarını ihlâl edici materyal üretmek, barındırmak ve iletmek amacıyla kullanılamaz.
7. İzmir Kâtip Çelebi Üniversitesi bilişim kaynakları, ülkenin birlik ve beraberliğine, bölünmez bütünlüğüne aykırı siyasi, dini, etnik propaganda yapmak amacıyla kullanılamaz.
8. Kurum işlerinin ve akademik çalışmaların sağlıklı bir şekilde yürütülmesi için mesai saatleri içinde uçtan uca iletişim (peer-to-peer, P2P) trafiği yapmak yasaktır.
9. Kurum bünyesinde hiçbir birim veya kullanıcı, İzmir Kâtip Çelebi Üniversitesi Bilgi İşlem Daire Başkanlığı'nın belirlediği IP adresleri dışında bir IP adresi atayamaz.
10. Kullanıcılar, İzmir Kâtip Çelebi Üniversitesi bilişim hizmetlerinden yararlanmaya başladığı andan itibaren bu politikada yer alan maddelere uyacağını kabul ve taahhüt eder. Aksi yönde bir tutum tespit edildiği takdirde internet erişimi ve e-posta kullanımı hakkının sona erdirileceğinin bilincindedir. Kullanıcılar, belirtilen kurallara uymadığı takdirde tüm hukuki ve idari işlemlerden kendisi sorumlu olur.

4.2. İnternet Erişimi ve Kullanım Politikası

*Amaç:*İzmir Kâtip Çelebi Üniversitesi bünyesinde güvenli internet erişiminin sağlanabilmesi için gereken standartları belirlemektir.

*Kapsam:*Bu politika, İzmir Kâtip Çelebi Üniversitesi bünyesindeki akademik ve idari birimlerdeki tüm çalışanları ve öğrencileri kapsamaktadır.

Maddeler:

1. İzmir Kâtip Çelebi Üniversitesi internet kaynakları, TÜBİTAK ULAKBİM politikasında belirtilen şekilde kullanılmalıdır.
2. İzmir Kâtip Çelebi Üniversitesi internet kaynakları, hiçbir şekilde yasa dışı kullanılamaz, kurum çıkarlarıyla çelişemez ve kurumun iş aktivitelerini engelleyemez.
3. İzmir Kâtip Çelebi Üniversitesi internet kaynakları öncelikli olarak resmi kurum işlerinin ve akademik çalışmaların yürütülmesinde kullanılmalıdır.
4. İzmir Kâtip Çelebi Üniversitesi bilgisayar ağı, güvenlik duvarı üzerinden internete erişebilmelidir. Ağ ve sistem güvenliğini sağlamak amacıyla kullanılan güvenlik duvarı kurum ağı ile internet arasında bir köprü görevi görmekte, kurum ağının iç yapısını dışarıdan gizlemekte ve kontrollü erişim sağlamaktadır.
5. Kurumun politikaları doğrultusunda web, url ve içerik filtreleme sistemleri kullanılmalıdır. İstenilmeyen siteler (pornografi, kumar, madde bağımlılığı, şiddet içeren vs.) yasaklanabilmelidir.
6. Kurumun ihtiyacı doğrultusunda Saldırı Önleme Sistemi (Intrusion Prevention System) kullanılmalıdır. Ayrıca Servis Reddi (Denial of Service, DoS) adı verilen saldırılara karşılık belli eşik değerleri (threshold) belirlenerek DoS sensörleri oluşturulabilmelidir. Anormallik durumlarında e-posta ile ağ güvenliği yöneticisi bilgilendirilmelidir.
7. Kurumun bünyesinde Anti-Virüs sunucuları ve/veya Ağ Geçidinde Anti-Virüs (Anti-Virus Gateway) sistemleri kullanılmalıdır. İnternete giden ve internetten gelen tüm trafik (özellikle HTTP, HTTPS gibi web trafiği, SMTP, SMTPS, POP3, POP3S, IMAP, IMAPS gibi e-posta trafiği, FTP, FTPS, IM gibi dosya transferi trafiği) virüslere karşı taranmalıdır.
8. Kurumun ihtiyaçları doğrultusunda, uygulamalar, hizmetler ve protokoller için imza içeren Uygulama Kontrolü (Application Control) mekanizması kullanılarak trafikte kullanılan uygulamalar (Remote Access, P2P, Proxy, Botnet Uygulamaları vs.) tespit edilebilmeli ve gerekli tedbirler alınabilmelidir.
9. Yetkilendirilmiş kişiler internete çıkarken tüm servisleri kullanabilme hakkına sahip olmalıdır.
10. İzmir Kâtip Çelebi Üniversitesi Bilgi İşlem Daire Başkanlığı'nca yazılı olarak izin verilmedikçe ağın izlenmesi, port taraması ve kullanıcıların kendine ait olmayan veriyi almaya çalışması yasaktır.
11. İzmir Kâtip Çelebi Üniversitesi'ne ait kritik bilginin ortaya çıkmasını veya kurum servislerinin ulaşılamaz hale gelmesine neden olacak tüm aktiviteler yasaktır.

4.3. Sunucu Güvenliği Politikası

*Amaç:*Bu politikanın amacı, kurumun sahip olduğu sunucuların güvenliği için gereken sorumluluklara ve yapılandırmalara ait standartların belirlenmesidir.

*Kapsam:*Bu politika, kurumun sahip olduğu tüm sunucular için geçerlidir.

Maddeler:

1. Kurumda bulunan sunucuların yönetiminden sadece sunucuyla ilgili yetkilendirilmiş kişiler sorumludur.
2. Sunucu kurulumları, yapılandırmaları, yedeklemeleri ve güncellemeleri sadece sorumlu kişiler tarafından yapılmalıdır.
3. Sunuculara ait bilgilerin yer aldığı bir Excel tablosu oluşturulmalıdır. Bu tabloda sunucuların isimleri, IP adresleri, görevleri, işletim sistemi sürümleri vb. bilgiler bulunmalıdır.
4. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
5. Sunucu üzerinde çalışan servislere ve uygulamalara erişimler, güvenlik duvarı üzerinde belirlenen kurallar doğrultusunda sağlanmalıdır.
6. Güvenli olmayan servis ve protokoller, daha güvenli olan servis ve protokoller ile değiştirilmelidir
7. Yetkisiz kişilerin sunuculara erişip erişemediği periyodik olarak test edilmelidir.

8. Servislere erişim kayıtları, gerektiğinde incelenmek üzere merkezi bir günlük kayıt sunucusuna (log server) gönderilmelidir.
9. Sunucular üzerinde çalışan işletim sistemleri ve diğer yazılımlar belirli zamanlarda güncellenmelidir.
10. Sunucular üzerinde anti-virüs yazılımı yüklü olmalıdır. Anti-virüs güncellemeleri otomatik olarak yapılmalıdır.
11. Sunucuların sorumluları "**`administrator`**" ve "**`root`**" gibi genel sistem hesapları kullanmamalıdır.
12. Sunuculara erişim için oluşturulan şifreler, şifre politikasında belirlenen standartları sağlamalıdır.
13. Sunuculara bağlantılar güvenli kanallar (SSH, SSL, IPSec vb.) üzerinden yapılmalıdır.
14. Sunuculara ait bağlantılar normal kullanıcı hatlarından yapılmamalıdır. Sunucu VLAN'larının tanımlı olduğu port'lardan bağlantı sağlanmalıdır.
15. Sunuculara sadece lisanslı yazılımlar kurulmalıdır.
16. Sunucular üzerinde zararlı yazılımlar (malware, spyware vb.) çalıştırılmamalıdır.
17. Sunucular üzerinde çalışan uygulamalar kaydedilmeli ve kayıtlar saklanmalıdır.
18. Web, DNS, e-posta vb. sunucuların disk yedekleri günlük değişenler en az 75 gün, haftalık tam yedekler ise en az 10 hafta olmak üzere saklanmalıdır.
19. Kayıtlar, sunucu üzerinde tutulmalarının yanı sıra ayrı bir merkezi günlük kayıt sunucusunda da saklanmalıdır.
20. VPLEX, birden fazla depolama ünitesinin (storage) yedekli bir şekilde çalışmasını depolama sanallaştırma yöntemi ile yapan ağdan yalıtılmış, sadece disk üniteleri ile bağlantılı çalışan bir sistemdir. Disk ünitesinin herhangi birinde fiziksel bir sorun oluştuğunda, sistem kesintiye uğramadan, işlemler diğer disk ünitesinde devam edebilmelidir. Kuruma ait dağıtık yapıda bulunan birden fazla veri merkezinin tümü tek bir depolama altyapısında olacak şekilde yönetilebilmelidir.
21. Sunucular, ağ alt yapısı, elektrik, sıcaklık ve nem değerleri düzenlenmiş, tavan ve taban güçlendirmeleri yapılmış, yedekli olarak çalışabilecek klimaların bulunduğu ve fiziksel olarak korunmakta olan sistem odalarında bulunmalıdır.
22. Sistem odalarına girişler ve çıkışlar, kimlik denetimi mekanizmasına (parmak okuyucu vb. biyometrik yöntemler) sahip olmalı ve oluşan kayıtlar merkezi günlük kayıt sunucusunda tutulmalıdır.

4.4. E-Posta Politikası

*Amaç:*Kuruma ait uzantı (**`ikc.edu.tr`**) ile oluşturulan e-postalar resmi bir kimlik taşımaktadır. Bu politikanın amacı İzmir Kâtip Çelebi Üniversitesi e-posta hizmetine yönelik kuralları ortaya koymaktır.

*Kapsam:*Bu politika kurum uzantılı e-posta hesapları ile oluşturulan e-postaların doğru şekilde kullanımını içermektedir ve tüm kullanıcıları kapsamaktadır.

Maddeler:

1. Kullanıcı hesaplarına ait şifreler ikinci bir şahsa verilmemelidir.
2. Kurum ile ilgili olan gizli bilgi, gönderilen mesajlarda yer almamalıdır. Buna e-posta ekinde gönderilen dosyalar da dâhildir.
3. Kullanıcı hesapları, ticari ve kâr amaçlı olarak kullanılmamalıdır.
4. İstenmeyen e-postalar (spam), oltalama e-postaları (phishing) gibi zararlı e-posta'lara cevap yazılmamalıdır.
5. Kullanıcılar, e-posta hesapları ile uygun olmayan içerik barındıran mesajlar (pornografi, madde bağımlılığı, ırkçılık, siyasi propaganda, fikri mülkiyet içeren belgeler vb.) göndermemelidir.
6. Kullanıcılar e-postalarının içeriğinde dile getirdiği tüm ifadelerin kendisine ait olduğunu kabul edip, suç teşkil edebilecek, tehditkâr, yasadışı, hakaret edici, küfür veya iftira içeren, ahlaka aykırı mesajların yollanmasından sorumludur.
7. E-posta kişisel amaçlar için kullanılmamalıdır.
8. Kullanıcılar, kullanıcı adı ve şifresini girmesini isteyen bir e-posta geldiğinde, bu e-postalara herhangi bir işlem yapmaksızın ağ güvenliği yöneticisine haber vermelidir.
9. Kullanıcılar, kurumsal e-postalarının, kurum dışındaki kişiler ve yetkisiz kişiler tarafından görülmesini ve okunmasını engellemelidir.
10. Kaynağı bilinmeyen e-posta ekinde gelen dosyalar kesinlikle açılmamalı ve tehdit unsuru oluşturabilecek e-postalar ağ güvenliği yöneticisine haber verilmelidir.
11. Akademik ve idari çalışanlar için e-posta hesapları **`ad.soyad@ikc.edu.tr`** şeklinde açılmalıdır. Eğer iki isim söz konusu ise **`ad1ad2.soyad@ikc.edu.tr`** şeklinde veya herhangi bir ismin sadece baş harfi

kullanılacak şekilde kısaltılarak açılmalıdır. İki soyadı söz konusu ise **ad.soyad1.soyad2@ikc.edu.tr** şeklinde açılmalıdır.

12. Akademik ve idari çalışanların e-posta hesapları için oluşturulan ilk şifreler rastgele olarak şifre politikasında belirtilen kombinasyona göre üretilmelidir.
13. Öğrenciler için e-posta hesapları **ogrno@ogr.ikc.edu.tr** şeklinde açılmalıdır. Öğrenciler için ilk şifre TC Kimlik numaralarıdır.
14. Kullanıcı şifreleri şifre politikasında belirtildiği gibi en az 10 karakterden oluşmalı, en az 1 büyük harf, en az 1 küçük harf ve en az 1 rakam içermelidir.
15. Kurumsal e-postalar, yetkili kişilerce hukuksal açıdan gerekli görülen yerlerde önceden haber vermeksizin denetlenebilir.
16. Kullanıcılar e-postalarına erişirken, kullanıcı adı ve şifresini açık metin olarak okunabilecek şekilde taşıyan HTTP, SMTP, POP3, IMAP vb. protokolleri kullanmamalıdır.
17. Virüs, solucan (worm), truva atı (trojan horse) gibi zararlı kodlar içeren e-postalara ve oltalama (phishing) e-postalarına karşı korumak için e-posta sunucusunun önüne e-posta güvenlik cihazı (e-mail security gateway) konumlandırılmalıdır.
18. E-posta güvenlik cihazı üzerinde, kurum uzantısına (**ikc.edu.tr**) sahip e-postalar ile e-posta sunucusunun ip adresi ilişkilendirilerek spoofing saldırıları (e-posta taklitçiliği) engellenmelidir.
19. Gönderilen veya alınan e-postalarda ek boyutu en fazla 50 MB olmalıdır.
20. E-posta eklerinde, doküman dosyalarına (pdf, doc vb.), resim dosyalarına (jpg, png, vb.) ve sıkıştırılmış (içeriği okunabilir) dosyalara izin verilmelidir.
21. Gelen e-postaların ekinde izin verilmeyen çalıştırılabilir dosya türleri mevcutsa (exe, bat, vb.) mevcutsa e-posta güvenlik cihazı devreye girerek bu ekleri kaldırmalı ve sadece mesajın içeriği kullanıcıya iletilmelidir.
22. Giden e-postaların ekinde izin verilmeyen çalıştırılabilir dosya türleri mevcutsa (exe, bat, vb.) bu e-postalar, e-posta güvenlik cihazına gelmeden, e-posta sunucusu (e-mail server) tarafından doğrudan reddedilmelidir.
23. Sunucu üzerinde bulunan e-postaların belli bir süre sonra otomatik olarak silinmesinden dolayı yedekleme ve arşivleme yapılması tavsiye edilmektedir.

4.5. Şifre Politikası

*Amaç:*Bu politikanın amacı güçlü bir şifre oluşturma standardı belirlemektir.

*Kapsam:*Bu politika, İzmir Kâtip Çelebi Üniversitesi bünyesindeki tüm kullanıcıları kapsamaktadır.

Maddeler:

1. Sistem hesaplarına ait şifreler (root, administrator vb.) altı ayda bir periyodik olarak yenilenmelidir.
2. Kullanıcılara, şifrelerini başkaları ile paylaşmamaları ve kâğıtlara yazmamaları konusunda bilgilendirme yapılmalı ve şifre güvenliğinin sağlanması ile ilgili farkındalık kazandırılmalıdır.
3. Şifre en az on (10) karakterli olmalıdır.
4. Şifre içerisinde en az 1 büyük harf, en az 1 küçük harf ve en az 1 rakam bulunmalıdır.
5. Şifre oluşturulurken sıralı karakterler (abcde, 12345, qwert vb.) kullanılmamalıdır.
6. Şifre, kullanıcı için bir anlam ifade eden kelimeler (araba plakası, tuttuğu takım, doğum tarihi vb.) içermemelidir.

4.6. Anti-Virüs Politikası

*Amaç:*Bu politika, kuruma ait bilgisayarların virüslere ve benzeri zararlı yazılımlara karşı korunması sağlamak amacıyla anti-virüs kullanımının standartlarını belirlemektedir.

*Kapsam:*Bu politika, İzmir Kâtip Çelebi Üniversitesine ait tüm bilgisayarları kapsamaktadır.

Maddeler:

1. Kuruma ait tüm bilgisayarlarda anti-virüs yazılımı yüklü olmalıdır.
2. Kuruma ait tüm bilgisayarlarda otomatik olarak haftalık virüs taraması yapılmalıdır.
3. Anti-virüs güncellemeleri gün içinde belli aralıklarla anti-virüs sunucusu aracılığı ile yapılmalıdır.

4. Harici veri depolama cihazları bilgisayarlara takıldığında anti-virüs yazılımı devreye girerek otomatik olarak tarama işlemini gerçekleştirmelidir.
5. Bilinmeyen veya şüpheli kaynaklardan dosya indirilmemelidir.
6. Yerel ağdaki bilgisayarlara virüs bulaştığı fark edildiğinde, ağ güvenliği yöneticisi bu bilgisayarları ağdan çıkartabilmelidir.
7. Kullanıcılar, anti-virüs yazılımını hiçbir sebepten dolayı bilgisayarlarından kaldıramaz.
8. Kurum bünyesinde zararlı yazılımlar (virüsler, solucanlar, truva atları vb.) oluşturmak ve dağıtmak yasaktır.

4.7. Sanal Özel Ağ (Virtual Private Network, VPN) Politikası

*Amaç:*Bu politikanın amacı, İzmir Kâtip Çelebi Üniversitesi ağına Sanal Özel Ağ (Virtual Private Network, VPN) ile dışarıdan erişilmesine ilişkin standartları belirlemektir.
*Kapsam:*Bu politika, İzmir Kâtip Çelebi Üniversitesi ağına dışarıdan VPN ile bağlanacak kurumları, firmaları ve kurum içindeki tüm kullanıcıları kapsamaktadır.

Maddeler:

1. İzmir Kâtip Çelebi Üniversitesi ağına erişmesi gereken kurumlar ve/veya kişiler VPN teknolojisini kullanmalıdır. VPN teknolojisi, veri bütünlüğünün ve gizliliğin korunmasını ve erişim denetiminin sağlanmasını mümkün kılmaktadır. VPN teknolojileri SSL, PPTP, L2TP, vb. protokollerinden birini içermelidir.
2. Sadece kurumun onay verdiği kullanıcılar VPN'yi kullanabilir.
3. Bağlantı bilgileri başka kişiler ile paylaşılmamalıdır.
4. VPN hesabının açılabilmesi için İzmir Kâtip Çelebi Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından hazırlanan VPN talep formunun eksiksiz olarak doldurulması ve imzalanması gerekmektedir.
5. VPN talep formunda erişilmesi gereken IP adresi ve port bilgisi yazılmalı, kurum ağına dışarıdan erişim nedeni açıkça belirtilmelidir.
6. Firmalara açılan VPN hesapları 30 gün ile sınırlıdır. 30 gün sonunda hesaplar kapanmaktadır. Erişimin devam etmesi gerektiği durumlarda talepte bulunularak hesap tekrar aktif hale getirilmektedir.

4.8. Uygulama ve Ceza

İzmir Kâtip Çelebi Üniversitesi bünyesinde uygulanacak olan bu politikaların uygulanması ve cezai durumları aşağıdaki gibidir:

1. İzmir Kâtip Çelebi Üniversitesi bilişim kaynaklarının kullanımı ile ilgili konularda bilişim kaynaklarını kullanıma sunan birimler ve Bilgi İşlem Dairesi Başkanlığı, kurum bünyesinde uygulanan Ağ ve Sistem Güvenliği Politikasına, ULAKNET Kullanım Politikasına ve 5651 Sayılı Kanun kapsamında belirtilen diğer politika ve prosedürlerde yer alan esaslara uyulmayan tüm durumlarda; *Kullanıcı sözlü ve yazılı olarak uyarılır, kullanıcıya tahsis edilmiş kaynaklar süreli veya süresiz olarak kullanımından alınır, soruşturma ve diğer yasal süreçler başlatılır ve sonuçları uygulanır*.
2. Uygulanacak yaptırımların düzeyi veya sırası, politika kapsamında belirtilen esaslara uyulmayan durumların tekrarına, verilen zararın büyüklüğüne ve bilişim kaynaklarının tamamında oluşturulan olumsuz etkiye bağlı olarak belirlenir.
3. Politika kapsamında belirtilen esasların ihlâli kurum dışı kaynaklı ise ilgili durum elde edilen kanıtlar ile birlikte adli makamlara bildirilir.

4.9. Onay ve Yürürlülük

Belirtilen Ağ ve Sistem Güvenliği Politikası, İzmir Kâtip Çelebi Üniversitesi Senatosunca kabul edildiği tarihte yürürlüğe girer:

1. Ağ ve Sistem Güvenliği Politikası, altı (6) ayda bir İzmir Kâtip Çelebi Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından gözden geçirilir ve değişiklikler söz konusu ise gerekli güncellemeler yapılarak İzmir Kâtip Çelebi Üniversitesi Bilgi İşlem Daire Başkanlığı tarafından onaylanır.
2. İzmir Kâtip Çelebi Üniversitesi bilişim kaynaklarını kullanan kullanıcılar, Ağ ve Sistem Güvenliği Politikası maddelerini kabul eder.

5. Yedekleme ve İş Sürekliliği

Kurumlar, bilgi teknolojilerine yaptıkları yatırımlara karşılık en yüksek verimi almayı amaçlamaktadır. Günümüzde verilerin güvenliği, yedeklenmesi ve yönetilebilirliği, bilgi sistemlerinin kesintisiz bir şekilde çalışmaya devam etmesi kurumlar için kritik derecede öneme sahiptir. Kurum bünyesinde verilen hizmetlerin herhangi bir nedenden dolayı kesintiye uğraması, olası veri kayıpları ciddi problemlere neden olmaktadır. Bu problemler, sadece maddi kayba değil aynı zamanda prestij ve zaman kaybına da neden olmaktadır. Bu nedenle, yaşanması muhtemel problemlere karşılık önceden planlama yapılması ve gereken önlemlerin alınması gerekmektedir. İzmir Kâtip Çelebi Üniversitesi bünyesinde sunulan web, e-posta, DHCP, DNS, UBS (Üniversite Bilgi Sistemi) ve benzerikritik hizmetlerin kesintisiz olarak çalışması ve yedeklemelerinin yapılması için donanımsal ve yazılımsal çözümler kullanılmaktadır.Bu doğrultuda kullanılan VPLEX cihazı ile birden fazla depolama ünitesinin (storage) yedekli bir şekilde çalışması sağlanmaktadır. Böylece kritik verilerin ve servislerin bulunduğu disk ünitesinin herhangi birinde fiziksel bir sorun oluştuğunda, sistem herhangi bir kesintiye uğramadan, işlemler diğer disk ünitesinde anlık olarak devam edebilmektedir.Bununla birlikte, fiziksel olarak yedekli çalışan sistemlerde oluşabilecek herhangi bir hata durumunda veri kaybı yaşanmadan sistemin çalışan son haline en kısa sürede getirilebilmesi için RecoverPoint [33] çözümü kullanılmaktadır. VPLEX ile bağlantılı olarak çalışan RecoverPoint ile veriler anlık olarak geri getirilebilmekte ve böylece iş sürekliliği sağlanmaktadır.Ayrıca, profesyonel dosya yedekleme (file backup) çözümü olan Avamarile günlük olarak eklemeli yedekler (incremental backup), haftalık ve aylık olarak ise tam yedekler (full backup) alınmaktadır. Özetle, VPLEX ile fiziksel yedekleme sağlanırken, anlık geri dönüş ve sıfır veri kaybı amacıyla kullanılan RecoverPoint ile de iş sürekliliği sağlanmaktadır. Dosya yedekleme amacıyla kullanılan Avamar ile de verilerin profesyonel olarak uzun vadede saklanması sağlanmaktadır.Mevcut veri merkezimizdeki yedekleme sistemi ve iş sürekliliği çözümlerinin yanı sıra deprem, sel, yangın gibi doğal afetleri göz önünde bulundurarak ayrı bir lokasyonda felaket kurtarma sistemi (disaster recovery) kurulması planlanmaktadır.

6. Sonuçlar

Ağ ve sistem güvenliği politikaları, güvenli bir ağda olması gereken unsurları tanımlayan ve kurumların bilgi güvenliğinin sağlanması için ilgili yönergeleri içeren yazılı metinlerdir. Bununla birlikte kurumların kültürünü yansıtan ve yaşayan dokümanlardır. Güvenlik politikaları; gizlilik, bütünlük ve erişilebilirlik ile ilgili tüm prensipleri ele almalıdır. Ortaya çıkan yeni güvenlik tehditleri, güvenlik politikalarının sürekli olarak kontrol edilmesi ve güncellenmesi gerekliliğini ortaya koymaktadır. Kurumsal ağlarda bilgi güvenliğinin sağlanması kurumun saygınlığı açısından büyük bir önem arz etmektedir. Öncelikle bilginin sahibi ve bilgi işlem daire başkanlığı olmak üzere, tüm kurum çalışanları bilgi güvenliğinden sorumludur. Bu çalışmada, bilişim kaynaklarına yönelik saldırı yöntemleri, saldırı çeşitleri ve korunma mekanizmaları detaylı olarak anlatılmış vesaldırı türlerine karşı uygulanması gereken alt güvenlik politikalar açıklanmıştır. Ayrıca, güvenlik prensipleri bir bütün olarak ele alınmış ve kurumlar için güvenlik politikalarının önemi anlatılmıştır. Bu kapsamda, İzmir Kâtip Çelebi Üniversitesi için hazırlanan ağ ve sistem güvenliği politikası taslağı durum çalışması olarak sunulmuştur.

Kaynaklar

[1]X. Wang, S. Zhang., "Research about Optimization of Campus Network Security System", Procedia Engineering, CEIS 2011, Vol. 15, 1802-1806, 2011.
[2]R. Macfarlane, W. Buchanan, E. Ekonomou, O. Uthmani, L. Fan, O. Lo, "Formal security policy implementations in network firewalls", Computers&Security, Vol. 31, Issue 2, 253-270, 2012.
[3] G. A. Marin, "Network Security Basics", IEEE Security and Privacy, Vol. 3, Issue 6, 68-72, 2005.
[4]E. Karaarslan, A. Teke, H. Şengonca, "Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması", İletişim Günleri, 2003.
[5]S. Barman, "Writing Information Security Policies", Sams Publishing, 240 pages, 2001.
[6] Ö. Can, M. O. Ünalır, "Ontoloji Tabanlı Bilgi Sistemlerinde Politika Yönetimi", Gazi Üniversitesi Bilişim Enstitüsü Bilişim Teknolojileri Dergisi, Cilt 3, Sayı 2, 2010.
[7]L. Kagal, T. Finin, M. Paolucci, N. Srinivasen, K. Sycara, G.Denker, "Authorization and Privacy for Semantic Web Services",IEEE Intelligent Systems, 19(4), 50-56, 2004.
[8] B. Fraser, "Site Security Handbook", http://www.ietf.org/rfc/rfc2196.txt, 1997. (Son Erişim: Mayıs 2014)
[9] M. Bishop, "Introduction to Computer Security", Addison-WesleyProfessional, 784 pages, 2004.
[10]E. Hamed, E. Al-Shaer, "Taxonomy of conflicts in network security policies", IEEE Communications Magazine,

Vol. 44, Issue 3, 134-141, 2006.
[11] E. Karaarslan, "Kampüs Ağ Yönetimi", Akademik Bilişim, 2005.
[12]InstantSecurityPolicy, "IT Security Policy Guide", http://www.instantsecuritypolicy.com/Introduction_To_Security_policies.pdf. (Son Erişim: Mayıs 2014)
[13] İ. Soğukpınar, "Veri ve Ağ Güvenliği", Ders Notu, http://obs.iszu.edu.tr/dosyalar/DersMateryal/bilgiguvenligidersnotu1.pdf. (Son Erişim: Mayıs 2014)
[14] E.S. Al-Shaer, H.H. Hamed, "Modeling and Management of Firewall Policies", IEEE Transactions on Network and Service Management, Vol. 1, Issue 1, 2-10, 2004.
[15]KasperskyLab, http://www.kaspersky.com/tr/about/news/virus/2014/Turkiyede-isletmeler-tehdit-altinda, 2014. (Son Erişim: Mayıs 2014)
[16]Pro-G Bilişim Güvenliği ve Araştırma Ltd., "Bilişim Güvenliği", http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf, 2003. (Son Erişim: Mayıs 2014)
[17]M. Bishop, "Computer Security: Art and Science", Addison-Wesley Professional, 1136 pages, 2002.
[18] UC Davis Administrative Policy Office, "Guide to Writing and Maintaining CampuswideAdministrativePolicy", http://manuals.ucdavis.edu/resources/GuidetoWritingPolicy.pdf. (Son Erişim: Mayıs 2014)
[19] G. Öztürk, "Bilgi Güvenliği Politikası Oluşturma Kılavuzu", UEKAE BGYS-0005, 2008.
[20]G. Canbek, Ş. Sağıroğlu, "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23, (1-2), 1 – 12, 2007.
[21] J. H. Allen, "The CERT Guide to System and Network Security Practices", Addison-WesleyProfessional, 447 pages, 2001.
[22]K. Burlu, "Bilişimin Karanlık Yüzü", Nirvana Yayınları, 477 sayfa, 2013.
[23] R. Rivest, "The MD5 Message-Digest Algorithm", http://tools.ietf.org/pdf/rfc1321.pdf, 1992. (Son Erişim: Mayıs 2014)
[24]W. Stallings, "Cryptography and Network Security: Principles and Practice", Prentice Hall, 5th Edt, 744 pages, 2010.
[25] Y. Atlas, "Arabellek Taşması Zafiyeti (Buffer Overflow)", TUBİTAK BİLGEM, 2013.
[26]ULAKNET Servisleri Balküpü, http://www.ulakbim.gov.tr/ulaknet/servisler/balkupu. (Son Erişim: Mayıs 2014)
[27]R. Macfarlane , W. Buchanan, , E. Ekonomou , O. Uthmani, L. Fan, O. Lo, "Formalsecuritypolicyimplementations in network firewalls", Computers& Security, 31(2), 253–270, 2012.
[28] J. G. Kolo, U. S. Dauda, "Network Security: PoliciesandGuidelinesforEffective Network Management", Leonardo Journal of Sciences, Issue 13, 7-21, 2008.
[29] X. Wang, S. Zhang, "Researchaboutoptimization of campus network securitysystem", ProcediaEngineering, CEIS 2011, Volume 15, 1802–1806, 2011.
[30]Türkiye Cumhuriyeti İçişleri Bakanlığı,"Bilgi Güvenliği Politikaları Yönergesi"http://www.icisleribilgiislem.gov.tr/ortak_icerik/bilgiislem/8%20Bilgi%20G%C3%BCv.%20Pol.%202.2012.pdf. (Son Erişim: Mayıs 2014)
[31]Türkiye Cumhuriyeti Sağlık Bakanlığı,"Bilgi Güvenliği Politikaları Yönergesi"http://bilgiguvenligi.saglik.gov.tr/files/BilgiG%C3%BCvenli%C4%9FiPolitikalar%C4%B1Y%C3%B6nergesi.pdf. (Son Erişim: Mayıs 2014)
[32]Gediz Üniversitesi, "Bilgi ve İletişim Kaynakları Kullanım İlkeleri Yönergesi"http://www.gediz.edu.tr/Dosyalar/Yonergeler/bilgi_ve_iletisim_kaynaklari_yonergesi.pdf. (Son Erişim: Mayıs 2014)
[33]RecoverPoint, "RecoverPointDisasterRecoveryand Data Protection",http://www.emc.com/collateral/software/data-sheet/h2769-recoverpoint-ds.pdf(Son Erişim: Eylül 2014)