Kurumsal Elektronik Posta İletiminde Siber Güvenlik

Dr.Önder ŞAHİNASLAN, Dr.Ender ŞAHİNASLAN

***Özet*—Elektronik haberleşme kişi ve kurumların her an ihtiyaç duyduğu, fonksiyonel ve kanıt niteliği taşıyan hızlı bir haberleşme servisidir. Yaygın kullanımı, bilgilerin mahremiyeti ve değerli oluşu nedeniyle siber saldırganlar tarafından hedef seçilebilmektedir. Diğer taraftan bireysel ve kurumsal e-posta üzerindeki siber tehditler her geçen gün daha da artarak çeşitlenmektedir. Gerçek zamanlı olarak tehditleri engelleyebilmek optimize edilmiş sıkı bir güvenlik politikası ve aşamalı güvenlik yönetim süreciyle mümkündür. Zararlı etkileri olan, profesyonelce hazırlanmış yanıltıcı içerik ve yönlendirmeleri içeriklerden arındırılmış e-posta hizmetleri sunulmalıdır. Uzmanlaşan 'hacker' korsanlarına karşı uçtan uca siber güvenli mimarilerle desteklenerek maddi ve manevi kayıpların önüne geçilmelidir. Gönderici ve alıcı arasındaki iletilen özel bilgilerin mahremiyeti sağlanmalı, iletişim ve yedekleme şifreli(kripto) gerçekleştirilmelidir.**

Bu çalışma, siber saldırılara karşı daha güvenli bir elektronik haberleşme sisteminin nasıl yapılabileceğine dair kurumsal siber önlem ve çözümleri sunmayı amaçlar.

Anahtar Kelimeler: **E-Posta Yönetimi, Siber Saldırı ve Tehditler, Şifreleme, Bilgi Güvenliği, Spam Savunma**

CYBER SECURITY IN INSTITUTIONAL E-CORRESPONDENCE

Abstract **- Electronic communication, which is needed by both individuals and corporations at any moment bears legal quality of evidence, is a functional and quick correspondence. However, it may be exposed to Cyber attackers because of its widespread use, and secrecy and value of its data. Also, cyber threats to personal and institutional e-mail are variably increasing day by day. Yet, preventing the threats on a real time basis is possible with a strictly optimized security policy and a leveled security management. E-mail services, cleared of professionally produced misleading agents with malicious effects, must be offered. Those services must be protected with cyber-shielded architecture thoroughly against professional hacker pirates to prevent potential spiritual or material losses. Confidentiality of the data transferred between the sender and receiver should be secured; also correspondence and encrypted backup must be performed.**

The purpose of this study is to suggest institutional precautions and solutions for how a safer e-correspondence system against cyber attacks can be performed.

Keywords: **E-Mail Management, Cyber Attacks and Threats, Encryption, Information Security, Spam Defense**

I. GİRİŞ

İletişim çağı olan günümüzde saniyeler içerisinde elektronik haberleşme gerçekleşmektedir. Hızlı hayat akışı içerisinde yüz yüze görüşmelerin ve elden gönderilen iletiler yerini canlı ve kesintisiz bir dijital bilgi aktarım ortamına bırakmıştır. En popüler ve yaygın kullanım oranı bakımından e-posta ilk sıralarda yer almaktadır. Alman bilişim derneği Bitkom tarafından yaptırılan bir araştırmaya göre, kullanıcıların yüzde 88'i e-postanın yaşam kalitesini artırdığına inanıyor. Yüzde 89'u esnekliğe imkân tanıdığını, yüzde 84'ü ise bilgiye erişimini kolaylaştırdığını düşünüyor. Kullanıcıların yüzde 66'sı üretkenliğinin e-postayla arttığına inanırken, yüzde 61'i bu iletişim aracı sayesinde zamandan tasarruf ettiğini belirtmiştir[1].

İnternetin her alanında olduğu gibi e-posta kullanımında da siber saldırılara maruz kalınmaktadır. İstenmeyen eklenti, virüs ve içerik taşıyan e-postalar özellikle son kullanıcıları çok fazla mağdur etmektedir. Bu tür istenmeyen saldırılarla mücadeleyi sadece bireylere bırakmak sağlıklı bir çözüm değildir. E-posta sunucu hizmeti veren kurum veya kuruluşlar e-postalara gizlenmiş tehdit içerikli zararlılardan arındırılması için belli filtrelerden geçirmek durumundadırlar. Böyle yapılmadığı durumda hizmetten yararlanan üyeler spam tehditlerine maruz kalır. Sunucu üzerinde oluşan fazladan trafik oluşturma, posta kutularının gereksiz iletilerle aşırı büyümesi sonucu bakım ve yedekleme zorlaşır. Kullanıcı tarafında ise hem güvenlik riskine sebep olmakta hem de gereksiz zaman kayıplarına ve dikkat dağınıklılıklarına sebep olmaktadır.

Belli sayının üzerinde kullanıcısı olan ağlarda istemci ve internet güvenliği sağlanmak durumundadır. Kurum içi veya dışında bir kullanıcıya iletilen e-posta gönderildiği bilgisayarın güvenliği kadar güvenli olabilir. Eğer bilgisayar yeterli düzeyde güncel güvenlik yazılımları ile korunamamışsa zaman içersinde spam saldırı ve yayma aracı haline dönüşebilir.

Tablo-1. E-Postalar üzerindeki spam yoğunluğu

Sektör	Yoğunluk(%)
Finans Kuruluşları	% 83
Eğitim Kurumları	% 67,3
Kimya/İlaç Sanayi	% 65,8
Ticari Olmayan Kuruluşlar	% 65,4
Tatil ve Konaklama	% 65,2

Mayıs 2013 yayınlanan Tablo-1'deki Symantec güvenlik araştırma sonuçlarına göre e-postalar üzerindeki spam yoğunluğu finans kurumlarından sonra en fazla eğitim kurumlarında görülmektedir[2]. Kurumlar kullanıcı taleplerini karşılamanın yanı sıra sahip oldukları bilgilerin güvenliğini de sağlamak zorundadır. ISO 27001 Uluslar arası bilgi güvenliği standardında da bilginin temel nitelikleri olan "gizlilik", "bütünlük" ve "erişilebilirlik" açısından korunması gerekliliği belirtilmektedir[3].

Şekil 1- Bilgi Güvenliğinde Sağlanacak Nitelikler

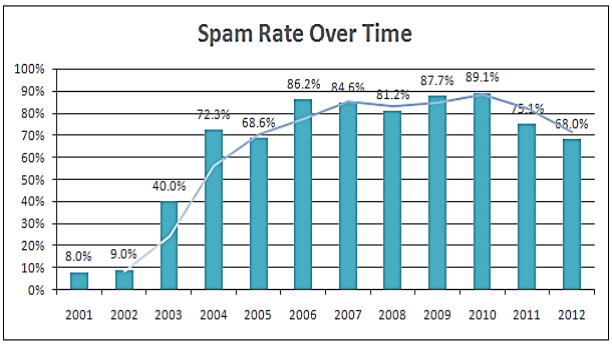
Elektronik haberleşme de karşılıklı iletilen bilginin bu temel güvenlik döngüsü esasında değerlendirilmesi gerekir. Yetkisiz erişimlerin engellenmesinden, veri bütünlüğünün korunmasından ve kolay ulaşılabilir olması sağlanmalıdır. Güvenli internet ve haberleşme servis ağı oluşturmak kurumların markalaşmasına da katkı sağlayacaktır. Korumasız ve güvensiz bir ortam iş gücü, finans, imaj kaybına ve kaynak israfına sebep olur. Güvenlik bakımından oluşabilecek zayıflıklar önceden tespit edilerek gerekli kontroller yapılmalı ve siber önlemler alınmalıdır[4].

Özellikle elektronik posta iletimi üzerinden yayılımını gerçekleştirilen kötü amaçlı yazılımlar oldukça tehlikeli ve zararlı fonksiyonları içerir hale gelmiştir. Trend Micro firmasının 2012 güvenlik raporuna göre kötü amaçlı yazılımlar dünya üzerinde endişe verici büyüklüğe ulaşmıştır.

Şekil 2 – Zararlı yazılımlardaki artış oranı

Şekil-2 incelendiğinde 2011 yılı ikinci yarısından itibaren on aylık büyüme oranı %60'dan fazla gerçekleşmiştir[5]. Sürekli artış gösteren bu tehditlerin bilgi varlıklarına yönelik gerçekleşmemesi için risklerin önceden fark edilmesi ve kurum ve/veya birey bilgilerinin zarar görmeden korunması kaçınılmazdır. Phishing (e-dolandırıcılık) saldırılarındaki artış yasal e-mail adresleri ile sahte ve yanıltıcı e-posta adreslerinin ayırt edilmesi gerekmektedir. Kullanılacak yazılımlarla kullanıcılar kendilerine gelen bir e-postanın güvenilir adresinden gelip gelmediğini doğrudan ayırt edebilmelidir. Bu sayede phishing ve sahte e-posta ile oluşacak riskleri azaltmaya yardımcı olur.

Symantec Güvenlik araştırma firmasının spam kaynaklı saldırılar konusunda yaptığı analiz sonuçları şekil-3'de görülmektedir. Saldırılar, %89 oranla en fazla 2010 yılında artış göstermiştir.



Şekil-3 Son 10 Yıllık Spam Dağılım Oranı

Spam ile yapılan mücadele ve güvenlik tedbirleri geçtiğimiz 2 yılda etkisini göstermiştir [2]. Ancak belirgin bir düşüş olmasına rağmen pek çok şirketin ve bireylerin ciddi sorunu olmaya devam etmektedir. Mağdurların adres defterini, kimlik ve bankacılık bilgilerini karşı tarafa iletmekle kalmayıp, eklentilerindeki zararlı yazılımları kurdurarak bilgisayarı korumasız hale getirmektedirler. Yine 2012 Symantec raporuna göre dünyada her gün yaklaşık 100 milyar spam posta dolaşmaktadır. Siber saldırı araçlarını bu reklam postaları üzerinden gönderen spam tacirleri yılda 200 milyon dolar gelir elde etmektedirler. Mağdurlar ise milyar dolarlarca maddi kayıp ve işgücü israfına neden olmaktadır. Örneğin sadece Google, Microsoft ve Yahoo gibi şirketlerin sunucularına fazladan yüklenme ve bakım masrafı hariç kullandıkları anti-spam yazılımlarının toplam maliyeti 6.5 milyar dolardır[2]. Tüm bu artış rakamları bizlere kayıpları önleme adına e-posta yönetiminde bir takım siber güvenlik tedbirlerin alınması gerekliliğini göstermektedir. Sistemsel ve yazılımsal güvenlik çözümleri ile beraber son kullanıcı bilinçlendirme çalışmalarının yapılması gerekmektedir. Ayrıca e-posta iletiminde açık kaynak kodlu yazılım çözümleri üzerinden katmanlı yapıda, kurumsal siber güvenli uygulamalı güvenlik çözümleri anlatılmaktadır.

II. GÜVENLİ E-POSTA YÖNETİM SİSTEMİ

A. E-Posta Üzerinde Taşınan Siber Riskler

Günlük iş ve özel yaşantımızda sıklıkla kullandığımız e-posta hedef kişiye farklı veya aynı ağa ait sunucular üzerinden ulaşabilmektedir. İletilen postalar, güvensiz sunucularda okunma ve silinme riski taşıyabilir. Sunucular, günümüzde resmi geçerliliği de olan haberleşme

kanallarının dinlenmesi, taklit edilmesi, çoğaltılması gibi güvenlik açıklıklarına karşı güvenli olmak zorundadır. Çoğunlukla zararlı içerik taşıyan reklam türü spam postalar hem zaman ve kaynak israfına hem de zararlı eklentilerin taşınmasına neden olmaktadırlar[4]. Etkili bir siber güvenlik son kullanıcıya temiz bir posta kutusu iletişim hizmeti vermekle mümkündür. Güvensiz e-posta kullanıcıyı ve bağlı bulunduğu kuruluşu siber risk oluşturur. Kullanıcının da belli yükümlülükleri yerine getirmesinin yanı sıra asıl filtreleme ve risk önleme sunucu tarafında gerçekleştirilir.

1. İstenmeyen Elektronik Posta(spam)

Alıcı tarafın bilgisi ve talebi olmaksızın içeriğine çok fazla güvenilmeyen merak, korku, politik, reklam, kişisel veya ticari menfaat sağlamaya yönelik yüksek sayıda gönderilen ileti kopyalarıdır. Elektronik haberleşmede istenmeyen e-posta oranının arttığı bir dönemde spam saldırılarına karşı güvenli bir ağ trafiğinin olması gerekmektedir. Spam mesajlar internet üzerindeki trafiği arttırarak başta servis sağlayıcılar olmak üzere birçok internet servisi üzerinde gereksiz yük oluşturmaktadırlar

Spam iletilerinin masrafı gönderen açısından yok denecek kadar az olduğundan gönderilen iletilerde hedef kitle aranmaz ve bu tür mail'leri almak istemeyen binlerce kişi rahatsız edilir. Email spam listeleri gönderilerin taranması, sohbet gruplarının, üye listelerinin çalınması veya web üzerinden adres aramalarıyla oluşturulur

Günümüzde e-uygulamaların hızla yaygınlaştığı e-devlet, e-kurum, e-bankacılık benzeri kimlik doğrulama ekran girişlerinin phishing türü yanlış yönlendirmelerde hesap ve şifre bilgilerinin elde edilmesi yöntemi sıklıkla kullanılmaktadır. Bu tür yöntemi kullanan kişiler öncelikle ilgili kurumdan geldiği izlenimini veren sahte spam mailler göndererek kişileri tuzaklarına düşürmektedirler. Bu nitelikteki e-posta içerisinde gönderdikleri sahte link benzeri yönlendirmelerle gerçeğinden farklı bilgi giriş ekranlarına girdirmektedirler veya sahte düzeltme formları göndererek gerçek bilgileri elde etmektedirler. Spam e-postalarla mücadele öncelikle sunucularda taratılarak ayıklanmalıdır. Kullanıcı tarafında ise akıllı öğrenme yeteneklerine sahip spam tarama yazılımları ve önemsiz posta klasörlerinin iyi yapılandırılması ile etkili siber tedbirler alınmalıdır.

2. Zararlı Eklenti ve Sahte Yönlendirmelere Sahip Elektronik Posta

Siber korsanların en belirgin phishing saldırı aracı haline gelmiştir. Posta gövde metninde gerçek kurum isim ve logoları üzerine verdikleri sahte tuzak adres linkleri ile yanıltılmaktadır. Özellikle spam postalarla birlikte taşınan virüs, trojan, worms benzeri gizli zararlı yazılımlar bilgisayarın kontrol dışı işlem yapmasından çok büyük bilgi kayıplarına kadar tehlikeli olabilmektedir. Çok değişik yöntem ve senaryolarla kişinin bilgisayarına gizli bir ajan yazılım olarak yerleşebilmektedir. Kendilerini faydalı bir program olarak göstererek kullanıcının onayını aldığından dolayı çoğu güvenlik önlemleri yetersiz kalabilmektedir.

Bilgisayara yerleşen zararlı bir yazılım kişinin Outlook'undan adres defterindeki tüm kullanıcılara kendi adında tuzak olabilecek zararlı eklentili ve yanıltıcı postalar gönderebilmektedir. Karşıdaki kişi gelen zararlı eklentiye sahip e-postanın tanıdığı ve güvendiği kişiden geldiği varsayımıyla rahatlıkla onay verebilmektedir. Bu şekilde bilgisayarlara yüklenebilen bir takım yazılımlar klavyeden girilen bilgileri, fare ve ekran görüntülerini saldırgan hedefe doğrudan göndermektedir. Zehirlenmiş PC olarak tariflenen bu bilgisayarlar üzerinden başkalarına ait binlerce reklam maili gönderilebilir. Uzak masaüstü servisini başlatarak saldırganın doğrudan erişmesini sağlar.

B. E-Posta Servis Hizmeti

Bilgi ve mesajların karşıdaki kullanıcıya elektronik iletişim araçları ile hızlı ve ucuz şekilde iletilmesidir. Oluşturulan bir e-postayı aynı anda çok fazla kişiye ulaştırmak mümkündür. İletilen mesajın ekinde doküman, ses, video gibi birden fazla dosya eki gönderilebilmektedir.

Kişilerin görsel ara yüzler kullanarak oluşturduğu elektronik bir mektubu bilgisayar ağları üzerinden taşınarak alıcı tarafa ulaşma işlemine e-posta denir. E-posta hizmeti sunucu ve istemci taraf olmak üzere iki bileşene sahiptir.

1. E- Posta Sunucusu

Bir ağ üzerinde çalışan bir veya birden fazla domain'e ait posta iletim ve dağıtım işlemini gerçekleştirebilen, çoklu kullanıcıya hizmet edebilen güçlü sistemleridir. Elektronik haberleşme servisleri üzerinden yapılan tüm iletim bilgilerini merkezi noktada toplar ve buradan ait olduğu hedef domainlere dağıtır. Hukuki durum ve bilgi güvenliği açısından yedekli bir yapıya sahiptir. Açık kaynak kodlu bazı e-posta sunucu yazılımları; Zimbra, Qmail, Send mail, Postfix

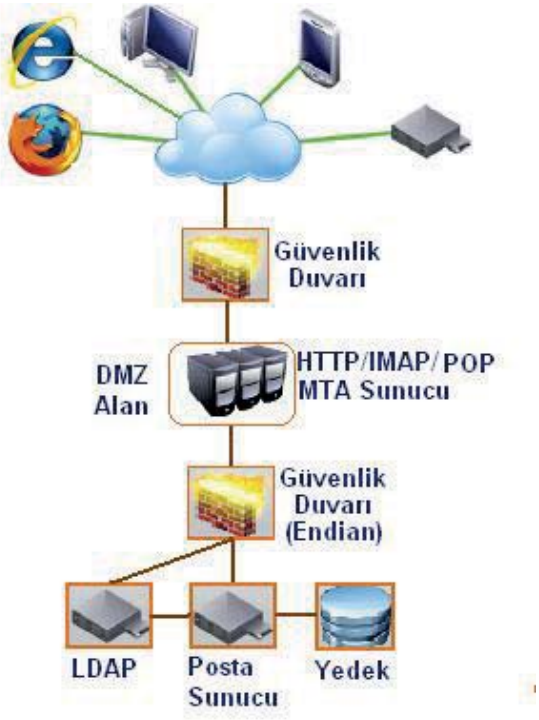
2. Elektronik Posta İstemcisi

İnternet kullanıcılarının e-posta yazma, gönderme, okuma ve silme işlemlerini gerçekleştirdikleri kullanıcı ara yüz servisleridir. Kullanıcılar bilgisayarlara kurulan yazımlar veya doğrudan browser üzerinden hesaplarına erişebilirler. Nestcape, k-mail, mozilla firefox, Thunderbird[3]

III. SİBER GÜVENLİ YAPILANDIRMA

A. Sistem Mimarisi

Bir kurumsal ağda, e-posta sunucusunun konumu, hangi kullanıcı grubunun izinli olacağı, merkezi yönetilebilir bir kimlik yetkilendirme ve trafik sınıflandırma sağlanmalıdır. Yeni nesil güvenlik cihazları kural ve politikalara bağlı izin tanımlarının yanı sıra saldırı önleme, virüs tarama, VPN bağlantı oluşturma, içerik filtreleme, spam ve virüs tarama gibi güvenlik fonksiyonları bütüncül şekilde konumlandırılmalıdır.



Şekil-4 Güvenli E-Posta Sunucu Yerleşimi

Sunucu ile istemci arasında uçtan uca şifreli mesajlaşma sağlanır. Proxy sunucu, DMZ bölge oluşturma, LDAP dizin erişim güvenlik doğrulaması, SSL/TLS Güvenli aktarım katmanı, SMTP/IMAP/POP vb. basit posta aktarım servisleri Şekil-4 de olduğu gibi güvenlik duvarı arkasında konumlandırılabilir.

1. Ağ Yapılandırması

Ağ üzerinde tek bir noktada güvenlik denetimi yapılması, günümüz siber saldırıları için oldukça yetersiz kalmaktadır. Farklı yöntemlerle savunma tedbirlerinin alınması, gelebilecek tehlikenin aşamalı olarak engellenmesini sağlar. Her kurumun kendi bilgi varlıkları ve e-posta sunucu uygulamaları risk düzeyine göre ağ güvenlik yaklaşımı farklılaşır. Aktif cihazlar, güvenlik duvarı, port yapılandırılması, IP-MAC filtreleme, log kayıtlarının tutulması gibi unsurlar sunucunun bağlı bulunduğu ağda denetim ve kontrol altında tutulmalıdır.

2. Sunucu Yapılandırması

E-posta domain, web, veritabanı, DNS, yedekleme gibi bir veya birçok uygulamayı aynı anda servis eden ve çok sayıda kullanıcıya 7x24 hizmet sağlayan sunucular siber tehditlere karşı korunaklı olmalıdır. Üzerindeki işletim sistemi ise sunucu yönetimi ile birlikte diğer uygulama ve servislere de yön veren siber güvenliğin sağlanmasında çok büyük fonksiyona sahiptir. İşletim sistemi kaynaklı açıklık ve açıklık için tedbir alınmadığı sürece bilgi varlıkları üzerinde siber güvenlik riski oluşturur. Yapılan çalışmada açık kaynak kodlu kolay kurulum ve yönetilebilirliği açısından Centos işletim sistemi tercih edilmiştir. Posta yönetim uygulama sunucu yazılımı olarak açık kaynak kodlu zimbra bütünleşik uygulama modülü tercih edilmiştir. Tümleşik uygulama olarak; Open Ldap Postfix, Apache-Tomcat, Mysql, Clamav, Spamassassin, Dspam uygulamalarını içerir[8]. Hazır Postfix MTA posta iletim aracı etkindir. Amavisd - Virüs ve spam koruması için güncel ve fonksiyonel bir içerik filtreleme aracıdır. Kurulum aşamasında tümleşik uygulamalar isteğe bağlı olarak doğrudan ücretsiz kurulumu gerçekleştirilebilir.

3. Spam ve Zararlı Eklentilerden Koruma

Kötü amaçlı yazılım ve phishing eklentilerle siber saldırı bugünün dijital ortamında oldukça yaygındır. Bu kuruluşların hassas bilgileri elde veya kötü amaçlı yazılım içeren girişiminde mesajlardan kullanıcıların koruması önemlidir.

ClamAV , ödüllü açık kaynak anti virüs sistemidir. Uygulamada açık kaynak kodlu Zimbra e-posta yönetim paketi kullanıldı. Siber tehdit zararlılarından(anti-virüs, anti-worm, anti-phishing) korumasını en üst düzeyde siber güvenlik oluşturmak için günde birden çok online güncelleme gerçekleştirmektedir.

Reklam ve tuzak olabilecek spam iletileri önlemede açık kaynak kodlu modül olan SpamAssassin ve DSPAM filtreleme araçları kullanılmalıdır. Zimbra açık kaynak posta sunucu kurulumunda bu modüllerde etkin hale gelmektedir. Bu araçlar posta sunucusu kullanıldıkça sürekli öğrenme yeteneğine bağlı olarak güvenlik performansı artmakta ve kendi veritabanlarını optimize etmektedirler. Ayrıca belli domainler veya spam kaynağı etki alanları tanımlanarak çok yetenekli spam kısıtlama ve ayıklama seçenekleri mevcuttur.

4. Ağ ve İnternet Trafiğini İzleme

Ağdaki paketlerin ileri düzey yönetilebilirliğini sağlayan Iptables, OpenBSD Paket Filter gibi açık kaynak yazılımları ile TCP/IP trafik routing, ethernet protokolü ve MAC filtreleme, bant genişliği yönetimi ile NAT işlemleri yapılmalıdır. Ağ paket trafik analizi ve çok özellikli saldırı tespiti engelleme yazılımı(Etherial, Ettercap), ağ güvenliği denetimi ve trafik dinleme amaçlı sniffer programı kullanımı ile olası siber saldırı durumlarına karşı denetlenmelidir. Ayrıca Nmap(Network Mapper) ile basit anlaşılır bir grafik arabirimi sayesinde çok amaçlı ağ araştırma ve port tarama gerçekleştirilmektedir. Uygulamada Squid proxy ve Dansguardian içerik filtreleme programını ile erişim iz kayıtları(log)'nı analiz etmek için sarg reports yazılım araçları kullanılmıştır.

5. Güvenlik Duvarı Yapılandırma

Dış ağlardan iç ağa gelecek veya içeriden dışarıya çıkacak IP'ler ve izin verilecek portlar, veri trafiğnin yönü tanımlanarak hedef sistemlere yönlendirilir. Domain, E-posta, Port veya IP bazında kısıtlamalar ve yasaklamalar getirilebilir. System Access kısmından interface'ler arasında hangi trafiklerin geçebileceği tariflenir. Uygulama da kullanılan Endian Firewall oldukça gelişmiş açık kaynak kodlu yazılımları bir araya getirerek bir paket çözümü sumaktadır. Kolay yönetilebilir web ara yüzünden DHCP, içerik filtreleme, anti spam, firewall, OpenVPN ve IDS gibi

bir yönetilebilir birçok bileşene sahiptir. Endian'da LAN, WAN, DMZ ve WIFI olmak üzere 4 ayrı ara yüz tanımı yapılabilmektedir[9]. Küçük ve orta ölçekli işletmelerde interneti kolayca dağıtıp paylaştırılabilecek ağın yanı sıra e-posta sunucusunu da kontrol altında tutabileceğimiz Linux tabanlı açık kaynak kodlu güvenlik duvarıdır. Dışarıdan gelebilecek saldırı ve botlara karşı etkin tarama modülleri ile tedbir niteliğidir. Veri iletişim sistemlerine karşı siber saldırıları en az indirebilecek güvenli, kullanımı ve sistem ayarları kolay yapılabilen bir sunucu tabanlı güvenlik yazılımdır.

B. E-Posta Mahremiyeti ve Gizlilik

E-posta hesabı pek çok üyeliklerde doğrulama ve aktivasyon aracı olarak kullanılmaktadır. Siber âlemde hesap bilgileri ve parolalar çok kıymetlidir. Sunucu ve bireysel posta kutularımız ile arada iletilen verinin gizlilik ve güvenliği oldukça önemlidir[10]. Aşağıda belirtilen hususlara dikkat etmek gerekmektedir.

1. Kimlik Doğrulama

Kişisel veya kurumsal mahremiyet gerektiren verilere erişim, izleme, kontrol ve düzenleme belli seviyelerde kimlik doğrulama gerektiren işlemlerdir. Günümüzde karmaşık yapıda şifre doğrulamanın yanı sıra iris, parmak izi gibi kişisel sağlık bilgilerine dayalı veya elektronik çipli doğrulama kullanılabilmektedir. E-posta servislerinde de LDAP benzeri yapılarla eşleme yapılabilmektedir[11].

2. Erişim ve Yetkilendirme

E-Posta uygulamaları içersinde bulunan bazı yan uygulamalar kullanıcının sahip olduğu yetkilere bağlı olarak işlem görürler. Yöneticiler belli posta gruplarına erişim ve yetkilendirme ayrıcalıkları tanıyabilmektedirler. Hesap geçerliyse ve bağlantı için yetki verilmişse, sunucu bağlantıyı posta erişim ilkelerine ve kullanıcı hesabı özelliklerine göre kabul eder. Yapılan uygulamada zimbra sunucusu içersinde class-of-service (COS) modülü üzerinden ayrıntılı ve güvenli yetkilendirme seçeneklerine sahip olduğu görülmüştür[8].

3. Şifreleme

Güvenli Sunucu Sertifikası (SSL - Secure Sockets Layer) ağ üzerindeki veri iletişiminde siber güvenliğin sağlanması amacıyla kullanılmaktadır[12]. Son yıllarda gelişmiş algılama ve yakalama teknikleri kullanılarak ağ trafiği üzerindeki değerli verilerin bilgisayar korsanları tarafından ele geçirmektedirler. E-posta iletişimine yönelik gerçekleşebilecek saldırılar ve ele geçirebilen verilerin maddi ve manevi değeri ölçülemez. O nedenle haberleşme iletileri başta olmak üzere kritik niteliklere sahip verilerin iletimi mutlaka şifreli mimari üzerine kurgulanmalıdır.

4. Dijital İmzalama

E-posta iletişiminde yüksek siber güvenlik sağlamak amacıyla kurumsal yapılarda kullanılmalıdır. Dijital imzalar göndereni doğrulamak ve iletilen mesajın bozulmamış olmadığını kanıtlar. Dolayısıyla bütünlük doğrulanır[13].

5. Yedekleme

E-posta sistem dosyaları ve posta kuruları yasalara uygun güvenli damgalama süreçleri kullanılarak kriptolu şekilde yedeklenir[14]. Kullanım yoğunluğu ve süreçlerin risk düzeyine bağlı olarak belli saatlerde günlük, haftalık ve birden fazla ortama, hızlı dönüş yapılabilecek şartları da sağlayacak şeklinde yedekleme yapılır.

C. Elektronik İletişimde Uygulanması Gereken Siber Güvenlik Politikaları

I. *E-Posta Politikası*

- Kurum e-postaları uygunsuz ve amaç dışı üyeliklerde kullanılamaz,
- Kurum saygınlığını zedeleyecek, taciz niteliğinde postalar için kullanamaz,
- Spam türü zincir e-postalar oluşturup, sahte ve zararlı eklentiler gönderemez,
- Kaynağından emin olunmayan e-postalar cevaplanmaz, başkasına gönderilmez,
- Kurumla ve işle bağdaşmayan uygunsuz iletiler kalıcı olarak silinir,
- Kullanıcı kendi e-postasından ve doğabilecek hukuki suçlardan sorumludur.
- Kullanıcılar, tanımadıkları kimselerden gelen, cazip öneriler içeren e-postaları açmamalı, gerektiğinde sistem ve güvenlik yöneticilerini vakit kaybetmeden konu hakkında bilgilendirmelidirler.

II. *Şifre Politikası*

- Ağda yetkilendirilmiş bir personelin e-Posta kullanıcı adı ve şifresi paylaşılamaz,
- Kullanıcı e-posta hesabının bilinçli amaç dışı kullanımdan doğabilecek zarardan sorumludur,
- Belli sürelerde şifre oluşturma kurallarına göre şifre değişmesi zorunludur,
- Bilgisayardan uzaklaşması halinde e-posta oturumu kapatma alışkanlığıdır,
- E-Posta kullanıcı adı ve şifreler üzerinden bazı program yetkilerinin verildiği ve sahipliğidir,
- Gizli belgelerin e-posta ortamlarında mutlaka şifreli şekilde iletilmesi gerekliliğinin önemli olduğu[15].

III. *Ağ ve İnternet Kullanım Politikaları*

- Kullanıcılar kurum internetini bilinçli kullanmalı, amaç dışı ve sistemlerin çalışmasını engelleyecek şekilde kullanmamalı,
- Kuruma ait bilgisayar, MAC ve IP adresi kullanılarak oluşturulan trafikten, o zaman dilimindeki kullanıcı olan kişi sorumludur,
- Kuruma ait sunucu sistemlerine karşı siber tehdit oluşturmamalıdır,
- Kurum ağından telif hakları ihlal edici yasal olmayan materyal edinmemek,
- Gerçek dışı endişe veren, yanıltıcı e-posta iletimde bulunmamak,
- Kullanılan cihazı ve ağa zarar verebilecek e-postaları açmamak, virüslü ve şüpheli iletilerden uzak durmak,
- Bilgi kaynaklarını yetkisiz ve izinsiz kullanmamak

IV. SONUÇ VE ÖNERİLER

Kurumları ve bireyleri sahte, spam, zararlı eklentiler yoluyla siber saldırılara neden olabilecek bilgi hırsızlığına karşı korumak için, sonuçta aşağıda belirtilen siber güvenlik önlemlerinin alınması gerekmektedir;

- E-posta kanalıyla hesap ayrıntılarını isteyen, kişisel ve gizli kalması gereken bilgiler asla verilmemelidir.
- Ağa bağlı son kullanıcıların e-postalarını takip ettiği bilgisayarda mutlaka güncel bir anti virüs olmalıdır.
- Bilgisayarın güvenlik duvarı uyarı konumunda etkin şekilde olmalıdır.
- İşletim sistemi yamaları yapılmış ve güncellenmiş olmalıdır.
- Son kullanıcıların spam, phishing, malware, worm türü zararlılar konusunda bilinçli olması için uyarı ve eğitimler düzenlenmelidir.
- Yazılım yüklenmesini gerektiren e-postalara karşı tedbirli ve bağlantılı ek kurulumlar iptal edilmelidir.
- İlginç ve beklenmedik e-postaların kendisi, eklentisi ve bağlantıları açılmamalıdır.
- E-posta isimleri veya listesi web sayfalarında açık ve doğrudan kullanılabilir şekilde yayınlanmamalı, en azından aradaki @ işareti resim veya at şeklinde değiştirilmeli.
- Posta sunucularında gelen giden veri trafiği ve posta kutuları üzerinde mutlaka anti-spam, anti-virüs, anti-worm, anti-phishing gibi yazılımlarla zararlılar ayıklanmalıdır.
- Posta sunucusu deneyimli personel tarafından sunucu işletim sistemi siber güvenliği eksiksiz sağlanmalıdır[16].
- Kullanıcılara ait posta kutuları, belli periyotlarda, kriptolu ve şifre korumalı şekilde yedeklenmelidir.
- Posta sunucusu SSL sertifikasına sahip olmalı, kullanıcılar web mail hizmetini https:// ile başlayan adres satırı kullanılarak veri trafiği kriptolu şeklide gerçekleşmelidir.
- Posta sunucusu üzerinde istem dışı aşırı posta gönderim trafiğine karşı uyarı ve koruma sistemi olmalıdır.
- İleti trafiği ve oturum açma bilgileri gerçek zamanlı kaydedilerek analizi yapılmalıdır.

Sonuç olarak elektronik posta iletiminde etkili bir siber güvenlik sunucunun doğru yapılandırılması ile başlar, son kullanıcının dikkat ve özenli kullanımı ile gerçek başarıya ulaşılabilir.

KAYNAKÇA

[1] http://www.bitkom.org/ - Mart-2012

[2] Symantec Intelligence Report, Symantec Corporation, http://www.symantec.com- Mayıs-2013

[3] E Şahinaslan, A Kantürk, Ö Şahinaslan, E Borandağ; Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, Akademik Bilişim 2009, Şanlıurfa, S.1

[4] The Horizon Scan 2013, "Council of Europe Recommendation" No. Rec (2006) 4 of the Committee of Ministers to memberstates on research on biologicalmaterials of humanorigin, https://wcd.coe.int/ViewDoc.jsp?id=977859

[5] http://www.trendmicro.com/how-big-will-the-android-malware-threat-be-in-2012/- Şubat 2013

[6] Ö Şahinaslan, E Şahinaslan M Razbonyalı, Open Source Administration Software and Implementation Results for ensuring Electronic Communication and Information Security Gediz University ISCSE 2010, Kuşadası, S.2

[7] National White Collar Crime Center, 2009 Internet Crime Report, US Department of Justice, http://www.ic3.gov - May 2010

[8] http://www.zimbra.com/- Mayıs 2013

[9] http://www.endian.com/en/community/ Nisan 2013

[10] TS ISO/IEC 17799, Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri - Kasım 2002, S.1.

[11] Ö Şahinaslan, E Şahinaslan, A Kantürk,; Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık, III. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu 2010, Ankara, S.4

[12] http://windows7news.com/2010/04/09/microsoft-security-intelligence-report-vol-7

[13] http://www.linuxhelp.net- Nisan 2013

[14] Ö Şahinaslan, E Borandağ, E Can, E Şahinaslan; Zibra Sunucu ile Birlikte Yönetim Sistemi, Akademik Bilişim 2009, Şanlıurfa, S.1

[15] http://www.howtoforge.com/- Nisan 2013

[16] Thomas R. Peltier, "Information Security Risk Analysis", Asset Protection and Security Management Handbook, Information Technology Control and Audit, CRC Press, London, 2005

BIYOGRAFILER

Dr. Önder Şahinaslan – Bilgi teknolojileri alanındaki yaklaşık 18 yıllık eğitim, birikim ve iş geliştirme becerilerine sahiptir. Bilgisayar Programcılığı ve Mühendislik eğitiminden sonra Bilgisayar Mühendisliği ve İşletme(MBA) alanında çift yüksek lisansın ardından Siber Güvenlik alanında Bilgisayar Mühendisliği doktora eğitimini tamamlamıştır. 1995 yılında bilgisayar sektöründe eğitmen ve teknik danışman olarak çalışma hayatına başladı. MEB'e bağlı özel öğretim kurumlarında uzman öğreticilik ve yöneticilikte bulundu. 2000 yılında katıldığı Maltepe Üniversitesi'nde sırayla Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi, Bilgi İşlem Daire Başkanı olarak çalıştı. Halen Bilişim Bölüm Başkanı ve Öğretim Görevlisi olarak görev yapmaktadır.

Bilgi ve bilgi teknolojileri, siber güvenlik, ağ ve sunucu sistem yönetimi, açık kaynak kodlu uygulama ve çözümler, sızma test ve denetleme araçlarının kullanımı, ağ ve sunucu güvenliği belli başlı çalışma alanlarını oluşturmaktadır.

1975 doğumlu evli ve 2 çocuk sahibi olan, özel yaşamında spora ve sosyal aktivitelere önem veren, ailesiyle birlikte vakit geçirmekten hoşlanan araştırmacı bir kişiliğe sahiptir.

Dr. Ender Şahinaslan - 1972 yılında Sivas ili Gürün ilçesinde doğdu, evli ve üç cocuk babasıdır. Trakya Üniversitesi Bilgisayar Mühendisliği Lisans, Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği bölümünde 'Yazılımda Kalite Modellerinin Değerlendirilmesi' adlı çalışmayla Yüksek Lisans, Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde 'Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi' adlı çalışmayla doktora programını tamamladı.
1996 yılında Gazi Üniversitesi'nde başladığı çalışma hayatına Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Araştırma Görevlisi, Maltepe Üniversitesi Öğretim Görevlisi, Sabancı Üniversitesi Bilgi Teknolojileri Birimi'nde Uygulama Sorumlusu olarak devam etti. 2004 yılında Bank Asya Yazılım Geliştirme Müdürlüğü'nde başladığı göreve, Organizasyon Kalite ve Sistem Geliştirme Müdürlüğünde devam etti halen Bilgi Güvenliği, BT Risk ve Uyum Müdürü olarak çalışmaktadır. ISO 27001 LA, ITIL Fv3 ve CRISC sertifikalarına sahiptir.