T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
RADYO-TV VE SİNEMA ANABİLİM DALI

YENİ İLETİŞİM TEKNOLOJİLERİ VE KAMU KURULUŞLARINDA BİLGİ VE İLETİŞİM GÜVENLİĞİ (ERZİNCAN ÜNİVERSİTESİ ÖRNEĞİ)

YÜKSEK LİSANS TEZİ

DANIŞMAN
Yrd. Doç. Dr. Ahmet YATKIN

HAZIRLAYAN
Mehmet Akif BARIŞ

ELAZIĞ- 2009

T.C.
FIRAT ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
RADYO-TV VE SİNEMA ANABİLİM DALI

YENİ İLETİŞİM TEKNOLOJİLERİ VE KAMU KURULUŞLARINDA BİLGİ VE İLETİŞİM GÜVENLİĞİ (ERZİNCAN ÜNİVERSİTESİ ÖRNEĞİ)

YÜKSEK LİSANS TEZİ

Bu tez … /… /2009 tarihinde aşağıdaki jüri tarafından oy birliği / oy çokluğu ile kabul edilmiştir.

Danışman	**Üye**	**Üye**
Yrd. Doç. Dr. Ahmet YATKIN		

Bu tezin kabulü, Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun ..... / ..... /2009 tarih ve ..... sayılı kararıyla onaylanmıştır.

Doç. Dr. Erdal AÇIKSES

Enstitü Müdürü

ÖZET

Yüksek Lisans tezi

YENİ İLETİŞİM TEKNOLOJİLERİ VE KAMU KURULUŞLARINDA BİLGİ VE İLETİŞİM GÜVENLİĞİ

(ERZİNCAN ÜNİVERSİTESİ ÖRNEĞİ)

Mehmet Akif BARIŞ

Fırat Üniversitesi

Sosyal Bilimler Enstitüsü

Radyo-TV ve Sinema Anabilim Dalı

Elazığ- 2009, Sayfa: IX+107

Bu çalışmada; son yıllarda yaşanan teknolojik gelişmeler sayesinde oluşan yeni iletişim kanalları, bu kanalların kullanılmasıyla ortaya çıkan bilgi-iletişim güvenliği problemleri ve kamu kuruluşlarına yansımaları incelenmiştir. Bilgi ve iletişim güvenliği konusunda hazırlanan denetim raporları ve yapılan araştırmalara göre, makaleler veya konferans sunularında da ifade edildiği gibi güvenliğin sağlanması konusunda en zayıf halka insandır. Bu nedenle kamu kuruluşlarında personelin bilgi ve iletişim teknolojilerinin kullanımı ve güvenliği konusundaki yeterliliğinin sorgulanması gerektiği düşünülmektedir. Bu düşünceden yola çıkarak; çalışmada yeni iletişim teknolojilerine, yeni iletişim teknolojilerinde yaşadığımız güncel güvenlik problemlerine, kamu kurum ve kuruluşlarında güvenliğin önemine ve güvenliğin sağlanabilmesi için yapılması gerekenlere yer verilmiştir. Son olarak bilgi ve iletişim güvenliğinde anahtar rolü oynayan kamu personeli arasında bir anket çalışması yapılarak konu bu yönüyle irdelenmiştir.

Anahtar Kelimeler: Yeni İletişim Teknolojileri, Bilgi ve İletişim Güvenliği, Internet, Bilgisayar ve Internet Üzerinden İletişim

ABSTRACT
Master Thesis

NEW COMMUNICATION TECHNOLOGIES & INFORMATION AND COMMUNICATION SECURITY OF PUBLIC ORGANIZATIONS (CASE STUDY: ERZINCAN UNIVERSTY)

Mehmet Akif BARIŞ

Firat University
Social Sciences Institute
Radio-Tv and Cinema Main Branch
Elazığ- 2009, Page: IX+107

In this study, new communication channels generated via recent technological improvements; information-communication security problems occurred due to the use of these channels and their reflections on public institutions are examined. According to the control reports and investigations on information and communication security, the weakest link in maintaining security is human being as mentioned in articles or presentations at conferences. Therefore, I believe that we should question the use and security of information and communication technologies competence of the staff in public institutions. Regarding this, communication technologies, recent security problems met in these new communication technologies and the importance of security and what should be done to maintain security in public institutions are involved in the study. Finally, after a survey study conducted among the public staff who have a key role in information and communication security, the subject matter is examined concerning this.

Keywords: New Communication Technologies, Information and Communication Security, Internet, Communication on Computer and Internet

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

ÖNSÖZ

E-dönüşüm projesi çerçevesince hazırlanmış rehberde bilginin güvenliğine yönelik, "Kurumlar için en kritik varlık bilgidir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir. Kurum bünyesinden yaratılan, işlenen, depolanan, iletilen, imha edilen ve kullanılan bilgi ile kurumlar arasında iletilen bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak güvenliğin temel hedefidir. " ifadeleri kullanılmıştır. Kurum ve kuruluşlar teknolojik gelişmelere ayak uydurma sürecinde; verilerini elektronik ortama aktarma, kurum ağı oluşturma, internet bağlantısı kurma, iletişimi elektronik kanallar üzerinden sağlama gibi uygulamalarla işleyişlerini devam ettirmektedirler. Aynı süreçte bilgi yönetimi ile bilginin güvenli bir ortamda saklanmasına ve iletilmesine büyük önem verilmesi gerekmektedir.

Bu çalışmada, yeni iletişim teknolojileriyle birlikte kamu kuruluşlarında oluşan bilgi ve iletişim güvenliği riskleri tartışılırken; özellikle personel bazında risklere karşı alınabilecek önlemler araştırılmıştır.

Tezin hazırlanması sürecinde sabrını ve desteğini esirgemeyen danışman hocam Yrd. Doç. Dr. Ahmet YATKIN' a, anketi uygulamamda yardımcı olan Erzincan Üniversitesi yönetimine, ankete katılımcı olarak görüşlerini esirgemeyen Erzincan Üniversitesi personeline teşekkür eder, saygılar sunarım. Ayrıca her konuda olduğu gibi tez çalışmalarımda da yanımda olan, sonsuz anlayışı ve hoşgörüsü için eşime teşekkürü bir borç bilirim.

KISALTMALAR

BGYS	:Bilgi Güvenliği Yönetim Sistemi
DMZ	:Silahsızlandırılmış Bölge (Demilitared Zone)
DNS	:İsimlendirme Servisi
FTP	:Dosya Transfer Protokolü
GSM	:Global Mobil iletişim Sistemi
HTML	:Web sayfası script dili
IP	:Internet Protokolü
MSN	:Messenger Anlık ileti Programı
RBAC	:Rol Tabanlı Erişim Kontrolü
SKKD	:Servis Kurulum Kimlik Doğrulaması
SMS	:Kısa Mesajlaşma Sistemi
SSL	:Secure Socket Layer (Güvenlik bilgilerini doğrulama sertifikası)
TBD	:Türkiye Bilişim Derneği
UEKAE	:Ulusal Elektronik Kriptoloji Araştırma Enstitüsü
VTYS	:Veri Tabanı Yönetim Sistemi
E-	:Elektronik
s.	:Sayfa
S.	:Sayı
vb.	:ve benzeri

GİRİŞ

Yirminci yüzyılın ikinci yarısından itibaren bilgi ve iletişim teknolojileri alanında baş döndürücü gelişmeler yaşanmış, bilginin hızlı bir şekilde depolanmasına ve paylaşıma açılmasına yarayacak birçok yenilik keşfedilmiş ve bununla ilgili teknolojiler üretilmiştir. Teknolojik alanda ortaya çıkarılan her bir yenilik adeta diğer bir yeniliğin öncüsü ve habercisi olmuştur. Telefonlar, faks cihazları, radyo ve televizyonlar, bilgisayarlar, bilgisayar ağları ve internet haberleşmedeki gecikme sürelerini milisaniye seviyelerine kadar düşürmüş, küreselleşen dünya adeta bir teknokente dönüşmüştür. Böylece bu büyük teknokentte yaşamı kolaylaştıracak teknoloji ve cihazların üretilmesini ve kullanımının yaygınlaşmasını sağlayacak binlerce şirket kurulmuştur. Bu alanda faaliyet gösteren binlerce şirket de yeni yatırımlar yapmaya veya iş alanını geliştirmeye karar vermiştir. Bu aşamadan sonra artık bir gerçek vardır: İş dünyasında, ekonomik, siyasal ve hukuki alanlarda eski kural ve ilkeler birer birer geçerliliklerini kaybetmekte, yerini yenileri almaktadır. Artık bireyler, devletler, devletlerin oluşturduğu birlikler gibi tüm oluşumların yeni dünya düzeniyle entegre olarak varlıklarını sürdürebilmeleri için bu yeni kural ve ilkelere adapte olmaları gerekmektedir.

Bilgiyi biriktirme ve iletme ile ilgili bu kadar yenilik olurken, bireylerin ve organizasyonların bu yenilikleri alelacele kabullenmeleri ve işlerini kolaylaştırmak amacıyla uygulamaya başlamaları beraberinde bazı sakıncaları doğurmaktadır. Bu sakıncaların başında güvenlik, sağlık ve etik gibi konularda ortaya çıkan olumsuzluklar gelmektedir.

Haberleşme ve bilişimde temel sorun bilginin, iletinin güvenliğidir. İnternet gibi dünyanın hemen her noktasına açık erişimin sağlandığı bir ortamda bilgi güvenliği can alıcı bir öneme sahiptir. Teknoloji geliştikçe bilgi çoğalmakta, bilgiye erişim, paylaşma, koruma, eleme vb. önem kazanmaktadır.

Tüm bunların güvenli bir ortamda ve biçimde gerçekleşmesi için parola sorma, şifreleme gibi teknikler kullanılmaktadır (Sevgi, 28.04.2009).

İletişim ve haberleşmenin çok hızlanmasına karşın, bilginin iletilirken ve saklanırken bu kadar güvensiz olduğu hiçbir çağ görülmemiştir. Çünkü bilgi korsanlarının da teknolojiyi çok iyi takip ettiği çoğunlukla gözden kaçırılmaktadır. Bu nedenle en az bilgi korsanları kadar gelişmeler de yakından takip edilmeli, onlara karşı alınacak önlemler araştırılıp bu konuda çözümler ve stratejiler geliştirilmelidir.

Ülkemizde kurumlar, kuruluşlar, şirketler hızla teknolojik yeniliklerden yararlanmaya devam etmektedirler. Bunun ekonomik ve toplumsal hayata yadsınamaz yararlar getireceği düşünülmektedir. Şirketler, kurumlar ve kuruluşlar bilgilerini oldukça çağdaş ortamlara taşıyacaklar, büyük iştahla elektronik hizmetlerini sunacaklar, teknolojiyi kullanarak birçok açılım yapacaklar; fakat bunu yaparken belki özel ve gizli bilgilerinin, veri tabanı yönetim sistemlerinin güvenliklerini tehlikeye atacaklardır. Bu tehlikenin farkında olanlar bir dizi önlemler alacaklar ama her alınan önlemin bir süre sonra geçerliliğini yitirme ihtimaliyle karşı karşıya kalacaklardır. Bu konudaki en büyük saldırıların mağduriyetini ve güvenlik problemlerini bankaların yaşadığı bilinmektedir.

Bu kapsamda tüm kamu kuruluşlarında bilgi ve iletişim güvenliği konusunun bütün detaylarıyla -özellikle kurum personellerinin konuya yaklaşımı ve konu üzerindeki davranışlarının- irdelenmesi gerektiği düşünülmektedir. Çünkü her hangi bir kamu kurum veya kuruluşuna bağlı bir çalışanın kullandığı bilgisayarda veya iletişim aracında oluşabilecek küçük bir güvenlik açığı bile kuruma fazlaca olumsuz yansıyabileceği düşünülmelidir ve geniş kapsamlı bir güvenlik politikasının uygulanması gerektiği göz ardı edilmemelidir.

BİRİNCİ BÖLÜM

YENİ İLETİŞİM KANALLARI VE GÜVENLİK PROBLEMLERİ

İletişim teknolojisi ürünleri bugün dünyada, özellikle gelişmiş ülkelerde, insan hayatının her alanına girmiştir ve kullanımı giderek yaygınlaşmaktadır. Bu ürünler insan hayatını büyük ölçüde kolaylaştırmış, yeni iletişim kanalları açmıştır. Bugün insanlar eskiye göre daha fazla iletişim kurabilmekte, kısa sürede daha fazla bilgiye ulaşabilmekte, bu bilgileri depolayıp istediği anda kullanabilmektedir. Ancak, bütün teknolojik gelişmelerde olduğu gibi iletişim teknolojisinin büyük katkıları yanında, kişisel ve toplumsal hayat üzerinde olumsuz yönde bir takım etkilerinin olduğu bir gerçektir.

Bu bölümde gelişen teknolojiyle birlikte sistemler arasında oluşan yeni iletişim kanalları ve iletişim teknolojisinin en büyük zaafı olan bilgi güvenliği konuları ele alınmaktadır.

1. TEKNOLOJİK GELİŞMELER VE YENİ İLETİŞİM KANALLARI

Bulunduğumuz çağ küreselleşmenin de etkisiyle etkileşim, haberleşme, mesajlaşma, bilişim, telekomünikasyon gibi terimlerin yaygınlaşmasıyla tam bir iletişim çağı galine gelmiştir. Bilgisayarlı sistemlerin yardımıyla bilginin iletilmesi kolay ve hızlı hale getirilmiştir. Bu gelişmelerin temelini bilgi ve iletişim teknolojileri oluşturmaktadır.

Başlıca iletişim teknolojileri cihazları şunlardır:

— Telgraf
— Telefon
— Faks
— Teleks
— Radyo
— Televizyon
— Uzaktan kumanda
— Çağrı cihazı
— GSM
— Telsiz
— Trunk telsiz
— Bilgisayar
— Modem
— Video çalar
— Video kamera
— Video projektör
— Amplifikatör
— CD-ROM
— VCD
— DVD
— Matbaa
— Yazıcı
— Fotokopi Makinesi

Bilginin toplanması, işlenmesi, üretilmesi, düzenli ve sistematik olarak depolanması, aralarında ilişki kurularak doğru ve hızlı bir biçimde erişilmesi ve ağlar aracılığı ile iletilmesinde ve kullanım hizmetine sunulmasında yaralanılan iletişim ve bilgisayar teknolojilerini içine alan genel ifadeyi 'bilgi ve iletişim teknolojileri' olarak adlandırılmaktadır(Atılgan, 09.01.2009).

İletinin kaynaktan hedefe gönderilmesini sağlayan araçlar **iletişim kanallarını** oluşturmaktadır. Araçların kalitesi, güncelliği ve teknolojisi bu kanalların genişliğini ve mesajın iletilme hızını belirlemektedir.

İletişimde esas konu mesajın hedefe gönderilmesi ve mesaja ait geri beslenmenin sağlanmasıdır. Hedef ve kaynak arasındaki mesaj alış verişinin hangi yolla, en kısa zamanda nasıl sağlanacağı iletişim teknolojilerinin konusudur. İletiler **veri**, **enformasyon** ve **bilgi**den oluşabilir. Veri işlenmemiş gerçekler olarak tanımlanırken, düzenlenmiş veriler enformasyon olarak adlandırılmaktadır. Enformasyon yazılı, sözlü veya görsel bir mesajdır. Bilgi ise; kişisel anlamda düzenlenmiş enformasyondur, özümlenmiştir. İnsanlar ve sistemler arasında enformasyon akışı bilginin yaratılmasını sağlamaktadır.

Verinin iletilmesi konusunda ki durmak bilmeyen teknolojik gelişmeler ve yeni buluşlar iletişim hızını katlayarak artırmaktadır. Yeni iletişim teknolojilerinin en büyük sonuçlarından biri kitle iletişim araçlarının ortaya çıkması olmuştur. Bu araçlar sayesinde zaman ve uzay içinde sayısız tekrarlanabilen mesajlar büyük topluluklara iletilmesi sağlanabilmektedir.

Tek bir alıcı veya küçük yüz yüze iletişim araçlarının tersine, kitle iletişiminin çoğunluğu birbirini hiç görmez veya duymaz. Lazarsfeld'in kitle iletişim tanımında iki özellik vardır: a) Kitle iletişimi bir kişiye veya nüfusun dar bir bölümüne yönelik değil, büyük homojen olmayan bir kesimine, kitleye yöneliktir. b) Mesajın nüfusun büyük bir kesitine aynı anda ulaşabilmesi için,

teknik araçların kullanılması gerekir. Bu tanımlamaların kitle iletişim araçlarının daha çok 1960'lara kadar olan işleyişlerine göre yapıldıkları unutulmamalıdır. Lazarsfeld ve Schramm'ın tanımları, belirli bir mesajın benzer özellikler göstermeyen, farklı mekanlarda bulunan ve gönderici tarafından tanınmayan çok sayıda kişiye aynı anda aktarılması olarak tanımlanan kitle iletişimi ile; telefon, telgraf, teleks, veya mektup gibi iki nokta arasındaki iletişim biçimleri arasındaki geleneksel farklılıkları yansıtmaktadır (Geray, 2003: 17).

Tablo 1. İletişim Kanallarını Türüne ve Yönüne Göre Sınıflandırma

	Tek Yönlü	**İki Yönlü**
Yazılı İletişim	• Basın-Yayın (Dergi, Gazete vb.) • Tanıtım Yazıları ve İlanlar (Broşür, kartvizit, duyuru panoları vs.) • Elektronik Panolar Web siteleri (Tanıtım siteleri, açıklama ve duyuru siteleri, internet gazeteleri vb.)	• SMS (Kısa Mesajlaşma) • Elektronik Postalar • Anlık İleti Programları(MSN, Yahoo vb.) • Web Siteleri (Forum Siteleri, Paylaşım Sistemleri vb.) • Otomasyon Sistemleri (İntranet ve internet ortamında çalışan veritabanı programları)
Sesli İletişim	• Radyo • Ses kayıtları bulunan kaset, CD, kayıt cihazları • Sesli tanıtım ve ders kayıtları (Sesli tanıtımlar, dersler ve konferanslar) • Anonslar	• Telsizler • Telefonlar • Cep Telefonları • İp Telefonlar • İnternet üzerinden yapılabilen sesli görüşmeler. • Konuşmalı Elektronik Postalar
Görüntülü İletişim	• Televizyon • Video Kasetler • Filmler (Belgeseller, tanıtım filmleri vs.) • Video Konferanslar	• İnternet üzerinden yapılan görüntülü görüşmeler • Telekonferanslar • Görüntülü kablolu telefonlar (ev iş telefonları) • 3N görüntülü iletişim

Genel olarak tek yönlü veri akışı; haber, duyuru, tanıtım, bilgilendirme, ticari amaç içeren öğeler ve reklam gibi geri beslemesi olmayan veya geri

beslemesi aynı anda olması gerekmeyen ileti gereksinimlerinde kullanılır. Amaç, kaynak tarafında bulunan bilgileri veya mesajları hedef kitleye ulaştırmaktadır. Tanıtım ve reklamcılık bürolarının temel işleyişi bu şekildedir.

Çeşitli teknolojik, ekonomik ve toplumsal gelişmeler sonucu kitle iletişimi, telekomünikasyon olarak da tanımlanan iki nokta arasındaki iletişim, veri iletişimi gibi çeşitli iletişim biçimleri giderek birbirine dönüşmekte ve aralarındaki farklılık yok olmaktadır (Geray, 2002: 19).

Önceleri iki kişi veya iki topluluk arasında iletişim sadece yazılı veya uzaklığına göre işretleşmeler ile yapılmaktaydı. Ailesiyle mektuplaşan asker veya birbirine elçiler göndererek diplomasi sağlamaya çalışan krallar, padişahlar gibi örnekler çoğaltılabilir. Ancak elektriğin bulunması ile telefon ve telgraf hatları oluşturulmuş, haberleşmede bir başka deyişle bilginin iletilmesinde devrim yaratılmıştır.

Teknolojideki önemli gelişmelere yol açan en önemli buluşlar olarak sırasıyla yazı, kağıt, matbaa, telgraf, buharlı makine ve bilgisayarın icadı gösterilmektedir. Özellikle telgraf, telefon, teleks, televizyon ve internet şeklinde ortaya çıkan iletişim teknolojileri bilgi iletimi ve bilgi değişimini hızlandırmış ve bilgi ekonomisi gibi yeni kavramların doğmasına neden olmuştur(Ayhan, 2002: 6). Buna ek olarak bilişim teknolojileri ve iletişim teknolojileri gibi kavramlarda bu sürecin ardından daha yaygın kullanılmaktadır.

Teknolojik her yeni gelişme, bilginin daha çok kişiye ulaşmasına ve daha çok kullanılmasına öncülük etmiştir. İletişim teknolojilerindeki gelişmeler ile birlikte, bilgi kaynakları ve kayıtlı bilgide önemli artışlar olmuştur. Bilgi artık sadece basılı ortamda değil işitsel ve görsel iletişimi sağlayan cihazlarda dijital veriler halinde saklanabilmektedir.

1.1. Yazılı İletişim

Duygu, düşünce ve mesajların yazı olarak adlandırdığımız harf ve işaretlerle belli materyaller üzerinden karşılıklı olarak iletilmesine yazılı iletişim denilmektedir. Mektuplaşmalar, resmi yazışmalar bu iletişim türüne bilindik en eski ve hala günümüzde devam eden verilebilecek örneklerdir.

İlk matbaanın açılmasından sonra gazete ve mecmua gibi basılı yayınlarla haberleşmenin temelleri atılmış, yazılı iletişim günümüze kadar hızla gelişerek devam etmiştir. Basılı yayıncılık, fotoğrafçılık ve kağıt kalitesinin artırılmasıyla kitlesel iletişim alanında ayrıcalıklı konumunu devam ettirmiştir.

Özellikle 1985'lerden sonra basım ve yayın sektöründe ofset teknolojisinin iyice yaygınlaşması ve bilgisayar destekli tasarım ve imalat istemlerinin kullanılmasıyla yeniden yapılanma dönemi başlamıştır. Bu dönemde gerek ürün kalitesinin gerekse üretim hızının önemli ölçüde artması söz konusu olmuştur. Büyük hacimli ofset makineleri tipo makineleri ile yer değiştirmiş ve çok üniteli baskı firmalarının sayısı giderek artmıştır (Aras, 2004: 30).

Bununla birlikte yazılı ilanlar, duvar gazeteleri, reklam ve tanıtım broşürleri, kartvizitler, davetiyeler insanlığın mesaj ve haber iletme, iletişim kurma, bilgilendirme gibi sosyal ihtiyaçlarını karşılamak amacıyla defalarca kullanılmıştır. 'Söz uçar yazı kalır' sözünden yola çıkılacak olunursa insanlık her zaman yazılı iletişimi samimi ve güvenilir bir araç olarak görmüştür. Ayrıca kitaplar, dergiler ve benzeri yayınlar özellikle eğitim alanında kullanılarak bilgi paylaşımı kağıt üzerinden kolayca sağlanmıştır.

Ancak günümüzde kağıdın yerini artık elektronik ortamlar almaya başlamıştır. Cep telefonlarının üretilmesiyle önce SMSler(Kısa Mesajlaşma Sistemi), internetin yaygınlaşması ile birlikte elektronik postalar mektuplaşmanın yerini almaya başlamıştır.

Elektronik posta ya da kısa adıyla e-mail, bilgisayar ağlarında kullanıcılarının birbirleriyle yazılı olarak haberleşmesini sağlayan bir yoldur. Bilgisayar ağlarının oluşturulma nedenlerinden biri, kişilerin, bir yerden diğerine (hızlı ve güvenli bir şekilde) elektronik ortamda mektup gönderme ve haberleşme isteğidir. E-posta (electronic mail, e-posta), bu amaçla kullanılan servislere verilen genel addır. İletişim tarihinde devrim yapan elektronik postayı Ray Tomlinson adında MIT mezunu bir mühendis buldu. Tomlinson, ilk e-postayı 1971 yılında gönderdi. Tomlison, "E-posta toplumu değiştirmedi, sadece daha fazla iletişim kurmalarını sağladı" diyor. Elektronik posta Türkiye'ye, Türkiye Elektronik Posta Sistemi (TÜRKEP) ile 1993 yılında gelmiştir. Sistem, başlangıçta 5.000 kullanıcı kapasitesiyle hizmet vermeye başlamıştır (http://www.milligorusportal.com/, 04.03.2009).

MSN (Messenger) gibi anlık mesajlaşma programların geliştirilmesiyle elektronik ortamda yazışma yoluyla iletişim ve haberleşmenin son hızına kadar ulaşılmıştır. Ayrıca web siteleri üzerinde forumlar, bilgi ve görüş paylaşım ortamları yaratılarak internet üzerinden çoklu iletişim imkanları oluşturulabilmektedir.

Anlık ileti programları kurumlar için işleyişi kolaylaştıran özelliklere sahiptir. Acil çözüm gerektiren durumlarda kurumlar arası veya kurumlarla firmalar arası görüşmeler yapılarak müdahaleler yapılabilmektedir. İster masasında, ister evinde, isterse de yeni mobil çözümlerle birlikte seyahatte olsun diğer bir personelin iletişime açık olup olmadığı anlaşılabilmektedir. Yazılı gönderilen mesajın aynı anda karşı tarafta belirmesi ve geri bildirimin hemen olabilmesinin yanında, gelişmiş ürünlerle dosya aktarımı ve sesli, görüntülü iletişim gibi ek özellikler de sağlanabilmektedir.

İnternet bir yayın aracıdır. Kitle iletişiminde çok önemli bir adımdır. Artık kendine has özellikleri olan sui generis (nev'i şahsına münhasır) bir yayın

aracıdır. HTML "(Hiper Text Markup Language)" dokümanı olan web sayfası grafik ve sayısal kod tasarımından oluşturulur (Atamer, 2004: 447). İnternet gazeteciliği hem okurlar hem de gazeteciler için yepyeni bir haber ortamı yaratmıştır. Önceleri sadece tek bir kanaldan enformasyon alan okurlar online yayıncılık sayesinde dünyanın dört bir yanından bilgi alabilir hale gelmiştir. Bu durum gazeteciler içinde önemli bir avantaj haline getirmektedir (Akıncı, 2005: 57).

İnternet ile birlikte 1990'lı yıllarda başlayan ve çok hızlı yaygınlaşan internet gazeteciliği ile gazetenin sanal ortamda dünyanın her yerinden okunabilir olması ve okur ile online etkileşim sağlanması yazılı iletişimde gelinen noktanın dikkat çekici taraflarından biri olarak gösterilmektedir.

Günümüz teknolojisinin getirdiği kolaylıklardan istifade etmek amacıyla kurum ve kuruluşlar web siteleri üzerinden bilgilendirme ve tanıtımlarını elektronik yazılarla sağlamaktadırlar. Ve yine birçok kurum ve kuruluş verilerin saklanması, bilgi yönetim sistemlerinin oluşturulması ve otomasyon sistemlerinin kurulmasıyla işlemlerini yerel ağlar ve internet üzerinden gerçekleştirmektedir. Bu konuya internet bankacılığını, e-devlet işlemlerini, ticari faaliyet gösteren siteleri ve öğrenci otomasyonları gibi sistemleri örnek gösterilebilir.

Yazılı iletişimde ayrıca yazıcılar, tarayıcılar, fotokopi makineleri gibi yeni dönem teknolojinin buluşlarından olan cihazların büyük katkısı olduğunu belirtmek gerekir. Bu cihazlar sayesinde bilgi ve belgeler analog ortamdan dijital ortama, dijital ortamdan analog ortama rahatlıkla aktarılmakta ve çoğaltılmaktadır.

1.2. Sesli İletişim

Konuşmak, bağırmak, şarkı söylemek sosyal bir varlık olan insanın iletişim esnasında sıkça başvurduğu ihtiyaçlardır. Yaygın bir iletişim yöntemi

olan sesli iletişimde, duygu ve düşüncelerin etkili bir şekilde ve anlaşılır bir dille dinleyiciye ulaştırılması hedeflenmektedir. Bir yerden bir yere ses transferi ve sesin elektronik veri olarak kaydedilmesi teknolojik gelişmeler sayesinde sağlanabilmektedir.

Radyolar, ses kayıt cihazları, kasetler, CDler ve ses oynatıcıları kitle iletişimlerinde, habercilik sektöründe, reklam ve propaganda işlemlerinde büyük rol oynamışlardır. Beğendikleri sanatçıları, şarkıları kasetlerden dinleyebilmenin ve radyonun günlük yaşamda önemli yer almasına şahit olan eski kuşağın o günlerde sesli iletişimden dolayı yaşadıkları mutluluğu dile getirdiklerine sıkça şahit olmaktayız.

Radyo, yazılı kültürden basılı kültüre geçişteki süreçlere benzer bir şekilde, elektronik kültüre geçişi olanaklı kılan bir iletişim teknolojisi olarak, yeni egemenlik ilişkilerinin kurulmasına öncülük etmiştir. Sözü tekrar yazının önüne geçirmiş gibi yaparak kullandığı yeni söz ile eski kültürden ve onun egemenlik ilişkilerinden bir kopuşu simgeleyen radyo, bu kitleleşmiş kulaklara seslenebilmenin gücü ile dikkat çekmiştir (Atabek, 25.12.2008).

Hareket halinde iken iki yönlü haberleşme isteği "Gezgin (mobil) Haberleşme"nin oluşmasına neden olmuştur. Mobil iletişimin en yaygın kullanılan cihazları cep telefonları olmuştur. Cep telefonlarında GSM (Global System for Mobile Communications) standardını kullanılmaktadır. 212 ülkede 2 milyar insan tarafından kullanılan GSM Avrupa'da geliştirilmiş bir dijital telekomünikasyon standardıdır ve 1994'ten bu yana ülkemizde de dijital teknolojiyi kullanan cep telefonu ağlarından kullanılmaktadır (http://www.bilgiforum.com/329102/, 25.04.2009).

Kurulan mobil sistemlerle anlık sesli mesajlaşma imkanları kamu ve özel kuruluşlarına geçmişte büyük faydalar sağlamıştır. Kişiler arası iletişimi sağlayan telefonların yaygınlaşması ve cep telefonlarının piyasa sürülmesiyle

sesli iletişim kanalları çok büyük rağbet görmüştür. Bu rağbetle birlikte bu konularda büyük ticari sektörler ortaya çıkmış, binlerce kişi bu alanda iş fırsatı elde etmiştir. Bugün Telekom ve GSM şirketlerindeki çalışanların sayısı çok büyük rakamlara ulaşmıştır. Aynı zamanda dolaylı olarak sesli iletişim sektörüne hizmet veren özellikle elektronik cihazları üreten ve satan irili ufaklı yüzlerce işyeri sektörün büyüklüğünü gözler önüne sermektedir.

Ses verilerinin dijital ortama alınmasına ve paketler halinde bağlantılar üzerinde iletilmesine imkan sağlayan teknolojiler sayesinde internet ortamında kullanılabilen sesli iletişime yönelik yazılımlar geliştirilmiştir. Bu yazılımlar sayesinde sesli görüşmeler anlık olarak yapılabilmekte, sesli elektronik postalar elektronik adreslere gönderilebilmektedir. Bunun için bilgisayarlarda birer mikrofon ve hoparlörün takılı olması yeterlidir. İnternetle birlikte ortaya çıkan Voice IP, ve IP Telephonning ile sesli görüşme teknolojilerinde büyük gelişmeler kaydedilerek iletişim maliyetleri önemsenecek derecede düşürülmüştür. Çağımız iletişim teknolojisi uzak mesafeleri yakınlaştırarak iletişimde sesin büyüsünü ve etkileyiciliğini kullanma lüksünü günümüz insanına sunmaktadır.

1.3. Görüntülü İletişim

Gözler en iyi mesaj alan iletişim kanallarıdır. Yüz ifadesini, vücut hareketlerini, ortamı görmek iletişim ve haberleşme açısından çok önemlidir. Bir futbol maçını cep telefonuna mesaj alarak, radyodan dinleyerek ve televizyondan izleyerek canlı takip eden sırasıyla A, B, C şahıslarını düşündüğümüzde, C şahsının maç hakkında diğerlerine oranla çok daha fazla bilgiye sahip olduğunu gözlemleriz. Bunun nedeni görme duyularının daha fazla mesajı birden algılayabilmesidir. "Gözümle görmesem inanmam" diye halk içinde yaygın bir söz vardır. Bu söz görmenin bir konudaki ikna olmayı sağlamada en önemli faktör olduğunun göstergesidir. Uzaklardaki evladının

kaza geçirdiğini duyan bir annenin oğlunun iyi olduğu söylense dahi sesini duymak hatta mümkünse gözüyle görmek istemesi bu konuya verilebilecek örneklerdendir. Görüntülü iletişimin ve görüntülü yayıncılığın pahalı olmasına rağmen kısa sürede ilgi toplaması ve yaygınlaşması da görme duyularının iletişimdeki önemli rolünü ispatlamaktadır.

Fotoğraf makineleri, kameralar, videokasetler, video oynatıcıları, televizyonlar, sesten sonra görüntünün de veri olarak farklı ortamlara iletilebilmesini ve kaydedilebilmesini sağlamıştır. Bu cihazlara bağlı olarak filmler, belgeseller, tanıtım ve propaganda kayıtları, video ders ve konferanslar görüntülü ileti kanalları olarak günlük yaşamda yerini almıştır.

Sözlü, yazılı ve görsel mesajları bir arada iletme olanağı sağlayan ilk kitle iletişim aracı olan televizyon ilk yıllarından itibaren kitlelerin büyük ilgisini çekmeyi başarmıştır. 2 Kasım 1936 tarihinde dünyada ilk düzenli yayıncılığa başlayan televizyon kanalı BBC olmuştur (Yengin, 1994: 50). Ülkemizde ise 30 Ocak 1930'da Türkiye Radyo ve Televizyon Kurumu sayesinde ülkemiz insanı televizyon yayıncılığı ile tanışmıştır (http://www.zaman.com.tr, 22.02.2009). Özel kanalların da yayın hayatına başlamasıyla görsel basının, kitleleri bilgilendirmede ve yönlendirmede çok daha etkili olduğu görülmüştür.

İnternet üzerinden maliyeti çok daha düşük ve hızlı bir şekilde görüntülü görüşebilmek için yazılım firmaları tarafından geliştirilen yazılımlar ücretsiz olarak insanlığın hizmetine sunulmaktadır. Telekom'un sağladığı görüntülü iletişim imkanları maliyeti yüksek olmasına rağmen büyük rağbet görmesi de dikkat çekmektedir. Temmuz 2009'da üçüncü nesil (3N) iletişim teknolojisi kullanılarak ülkemizde mobil olarak çok hızlı bir şekilde iletişim sağlanabilecek. Bu sayede yazı ve ses datasına oranla daha büyük boyutta olan görüntü dataları çok daha kaliteli ve hızlı bir şekilde cep telefonlarına ve laptoplara kablosuz olarak iletilebilecektir.

2. İLETİŞİM GÜVENLİĞİNİ TEHDİT EDEN SALDIRI TÜRLERİ

Bilginin iletişim anında veya saklanırken güvenliği için üç ilke çok önemlidir: gizlilik, bütünlük ve erişilebilirlik. İletişim sırasındaki mesajın hedefe ulaşmadan bir başkası tarafından engellenmesi, ele geçirilmesi ve içeriğinin değiştirilmesi riski her zaman mevcuttur. Bu riske karşılık alınacak önlemler, kullanılacak çözümler ve yöntemleri iletişim güvenliği konusunu oluşturur.

Tarihte iletişim güvenliğini sağlamak için bir takım stratejilerin geliştirildiği ve çözümlerin uygulandığının örnekleri mevcuttur. Mesela; Sezar kendi adını verdiği bir şifre metodu kullanarak ilettiği bilgileri şifrelemiş, başkası tarafından ele geçirilse bile anlaşılamamasını sağlamıştır. Şifreli mesajlar özellikle askeri iletişimde kullanılmıştır. 2. Dünya savaşında Almanlar, Enigma adını verdikleri bir makine kullanarak askeri birliklerine şifreli mesajlar yollamışlardır. Aynı zamanda Japonlarda şifreli mesajlar kullanarak mesajlarının Amerikalılar tarafından anlaşılmamasını sağlamışlardır (Türkiye Bilişim Derneği, 2006: 4).

II. Dünya Savaşında sadece yazılabilen mesajlar kullanılmamıştır. Düşmanların, sesli mesajlarını dinlemelerine karşı önlem almak için Amerikalılar tarafından "Navaho Code Talkers" adlı şifre sistemi gerçekleştirilmiştir. Savaştan sonra da şifreli iletişimler devam etmiş ve Sovyetler Birliği tarafından "one-time pads" adlı şifre sistemi oluşturulmuştur (Türkiye Bilişim Derneği, 2006: 4).

Günümüzde ise; kişisel ve resmi işlemlerde veri iletişimi çoğunlukla elektronik ortamlarda ve bilgisayarlı sistemler aracılığıyla yapılıyor olduğu bilinmektedir. Bu nedenle bilgi ve iletişim güvenliği çok daha fazla önem kazanmıştır. Bu konuda oluşabilecek sorunlar ve alınması gereken önlemler sonraki bölümlerde detaylı olarak ele alınacaktır.

İletişim sistemlerinde iletinin kaynaktan hedefe; kayıpsız, sorunsuz ve mümkün olduğunca hızlı bir şekilde (zamanında) ulaştırılması amaçlanır. İletişim sisteminin kullanıldığı yer ve kullanılma amacına göre iletme işleminin gerçekleşmesi çeşitli önemler taşır. Önemin büyüklüğüne göre iletinin yolda başına gelebilecek tehlikeler ve saldırılar çeşitlenir. Saldırganın niyetine göre mesajın başına gelecek saldırıların türleri de farklı olur. Merak, maddi kazanç, kin, ün kazanma isteği gibi çeşitli nedenleri olan bu saldırıların amacı mesajın öğrenilmesine, değiştirilmesine, engellenmesine veya geciktirilmesine yönelik olabilir.

Bilgi ve bilgisayar güvenliğinde, karşı taraf, kötü niyetli olarak nitelendirilen kişiler (korsanlar veya saldırganlar) ve yaptıkları saldırılardır. Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak, zafiyete uğratmak, kişileri doğrudan veya dolaylı olarak zarara uğratmak, sistemlere zarar vermek, sistemlerin işleyişini aksatmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler saldırı veya atak olarak adlandırılmaktadır. Saldırganlar, amaçlarına ulaşmak için çok farklı teknikler içeren saldırılar gerçekleştirmektedirler. Saldırı türlerinin bilinmesi, doğru bir şekilde analiz edilmesi ve gereken önlemlerin belirlenmesi, bilgi ve iletişim güvenliği için büyük bir önem arz etmektedir (Canbek, Sarıoğlu, 2009: 168- 169).

Saldırgan, iletişim esnasında aşağıdaki durumlarda iletiye zarar vermeyi amaçlayabilmektedir.

1- Mesaj kaynak tarafında iletilmeye hazırlanıyorken (Örnek: Klavyeden bilgi giriş esnasında bilgilerin öğrenilmesi ve değiştirilmesi).

2- Mesaj kaynak ve hedef arasındaki veri yolunda iletilirken (Örnek: Hat dinleyici programlar ile verilerin çalınması).

3- Mesaj ulaştığı anda hedef tarafından çözümleniyorken (Örnek: Mail okuma programlarına bulaşan virüsler).

Saldırı tiplerini:

1) Saldırıda bulunan kişinin belirli verilere erişim sağlamak yerine yetkili kullanıcıların uygulamalara erişimini engelleyerek bilgi sistemleri kaynaklarını kilitlemesi olarak bilinen hizmetin engellenmesi.

2) İçeriden yapılan yetkisiz erişimle kritik bilgilerin değiştirilmesi ya da yok edilmesi tehlikesini içeren veri gizliliğinin bozulması.

3) Gizli bilgileri ele geçirmek için ağ parolalarına yetkisiz erişim yapan ve ana bilgisayarın ele geçirilmesi ile sistemin tamamen çökertilmesine neden olan, bilinen en tehlikeli saldırı türlerinden biri olan parola ve kök saldırıları olarak sınıflandırmak mümkündür.

2.1. Mesajın Ele Geçirilmesi

Mesajın kaynak veya hedef dışında üçüncü bir sistem ya da kişi tarafından alınması, kopyalanması şifreli ise çözülerek anlamlı hale getirilmesi mesajın ele geçirilmesidir. Mesajın ele geçirilmek istenmesi bilginin gizliliği ilkesini tehdit etmektedir.

Saldırganın mesajı ele geçirmek istemesinin birçok nedeni olabilir. Merak, bu nedenlerin içinde en iyi niyetli olanıdır. Mesajın içeriğini biliyor olmak için bu eylemin gerçekleştirilmiş olması bu riskin en iyimser halidir.

Diğer bir nedeni bilgiyi ele geçirmek, ele geçirdiği bilgiyi kötü niyetli olarak kullanmak ve başkalarına ulaştırmak olabilir. Bu yolla saldırgan, gizliliği önemli olan bir bilgiyi ifşa etmiş olur. Bilginin mahremiyeti açısından ülkemizde askeri kurumlar ve istihbarat kurumları gibi önemli yapılar

mevcuttur. Bu kurumlar kendi iletişimindeki bilgi ve mesaj güvenliğini sağmakla yükümlüdürler.

Mesajın ele geçirilmek istenmesinin en yaygın ve gerçekçi nedeni ise maddi menfaat sağlamaktır. Buna sıkça duyduğumuz, internetten banka hesaplarının ele geçirilmesi ve kredi kartı bilgilerinin çalınması olayları örnek verilebilir. İnternetten bankacılık işlemlerinin gerçekleştirilmesi, elektronik ticaretin yaygınlaşması gibi yenilikler, internet ağı üzerindeki özel veri trafiğini artırmaktadır. İnternet ortamında kaynak ve hedefler arasında dolaşan bu özel veriler, internet korsanlarının ve elektronik yollardan para hırsızlığıyla uğraşanların riskli saldırılarına çok kez maruz kalmışlardır.

Mesajı ele geçirmeye yönelik saldırıların temel amacı mesajın içeriğini öğrenmektir. Bu nedenle mesajları güvensiz ağlarda dolaştırırken şifrelenmiş, parçalara ayrılmış, sırası karıştırılmış şekilde iletilmesine yönelik güvenlik algoritmalarının kullanılması gerekmektedir. Algoritmalar ile kaynakta mesajın anlaşılmaz hale getirilip gönderilmesi ve hedefte çözülüp tekrar anlaşması sağlanmalıdır. Bu konudaki politikalar sonraki bölümlerde ele alınacaktır.

2.2. Mesajın Değiştirilmesi

Kaynaktan gönderilen mesajın hedefe ulaşmadan başka bir kişi veya sistem tarafından bozulması, eksiltilmesi veya arttırılmasıdır. Bu atak türünde mesajın içeriği saldırgan tarafından önemli değildir. Amaç hedefin hatalı veri elde etmesidir. Mesaj bir başka mesajla değiştirilir veya verilerin karşı tarafa yanlış bir şekilde ulaşması istenir.

Bu saldırıların birkaç nedeni olabilir. Birincisi hedefe mesaj kaynağının yerini şaşırtarak mesaja verilecek cevapların kendisine gelmesini sağlamak olabilir. Bu sayede hedefe ait özlük bilgilerini geri bildirimlerle toplamış olur. İkincisi; hedef veya kaynağa duyulan kin ve rekabete bağlı kıskançlık duyguları

ile gerçekleştirilmeye çalışan iletişimin engellenmesi amaçlanabilir. Ticari ilişkilerde, bankacılık işlemlerinde yapılan sahtekarlıklarda mesaj değiştirilmesi ve hedef saptırma kullanıldığı görülmektedir. Buna; bankalardan mail gönderiyormuş gibi internet kullanıcılarına mail atan ve gelen cevapları kullanarak hırsızlık yapan internet korsanlarını örnek gösterebiliriz. Bu saldırılardaki tehdit bilginin bütünlüğüne yöneliktir.

2.3. Mesajın Geciktirilmesi veya Engellenmesi

Bu tür saldırılarda da bir önceki mesajın değiştirilmesine yönelik saldırılardaki gibi mesajın içeriğinin korsan tarafından bilinmesi gerekmez. Önemli olan mesajın kaynaktan hedefe zamanında ulaşmasının engellenmesi veya hattın tamamen meşgul olmasını sağlayarak iletişimin koparılmasıdır. Bu durumda kaynak, hedeften mesajın ulaşıp ulaşmadığına dair bir mesaj alamayacağı için servisin kilitlenmiş olduğunu algılar. Dos (Denial Of Service) atakları bu türe örnek verilebilir.

Bu saldırılar kıskançlık veya düşmanlık duygularıyla yapılmış olabilir. Diğer bir nedeni ise kendini ispat etmeye çalışan ve bu alanda isim yapmaya çalışan kişi veya grup psikoloji olabilmektedir. Tehdit; bilginin gizliliğine yönelik değil, bilginin erişilebilirliğine veya iletişimin sorunsuz bir şekilde sağlanmasına yöneliktir.

İKİNCİ BÖLÜM

KURUMLARDA İLETİŞİM GÜVENLİĞİ İLE İLGİLİ PROBLEMLER

Günümüzde internet üzerinden iş ve bilişim süreçleri ilerledikçe güvenlik sistemlerine olan ihtiyaç giderek daha hayati bir öneme sahip olmaya başlamıştır. E-ticaret, tedarik zinciri yönetimi, uzaktan erişim gibi internet olanaklarının iş prosedürlerini kolaylaştırması, yüksek hızlı ses ve görüntü verileri taşıyan çoğul ortam uygulamalarının da haberleşme sistemlerine katılımı bu alanda yapılan yatırım maliyetlerini artırmıştır. Bununla birlikte yeni teknolojilerin kullanımından dolayı ortaya çıkan güvenlik problemlerini gidermek için ayrı bir harcama kalemi ortaya çıkmıştır.

Örgütler üzerinde yapılan bir araştırmaya göre örgütlerin %57'si bilgi iletişim teknolojilerinin ana işlemlerde yüksek bir etkisi olduğunu, %93'ü 3-5 yıl içinde çok etkili olacağını söylemektedir. Örgüt performansı ve verimlilik arasındaki ilişkileri inceleyen son araştırmalar ise, bilgi iletişim yatırımlarının pozitif ve önemli etkileri olduğunu, uzun dönemde ise faydalarının olduğunu saptamışlardır (Akıncı, 2005: 91).

Şirket ağlarında doğrudan maliyet ve ticari başarıya yönelik bir anlam taşıyan ağ sistemlerinin güvenliği, kurum ağlarında ulusal güvenlik boyutunda olumsuz etkilere neden olabilecek kritik bilgilerin korunması şeklinde kendini göstermektedir.

3. İLETİŞİM GÜVENLİĞİNİN ÖNEMLİ OLDUĞU KURUMLAR

Kurumlar iletişim güvenliğini her ortamda sağlamak zorundadır. Bilgiyi üreten, işleyen, ileten ve saklayan tüm kurumlar mevcut yazılımları, donanımları, ortamları ve insan kaynaklarını dikkate almalıdır. Bilgi güvenliği ile ilgili birçok insan kaynakları çalışmaları yapılmıştır. Çalışmalardan ortaya çıkarılan sonuçlar bilgiye ve bilgi güvenliğine verilen önemin yeterli

olmadığını, öneminin ancak olumsuz olayların ardından anlaşıldığını göstermiştir.

Gartner ve Deloittle gibi bağımsız araştırma kuruluşlarının raporları incelendiğinde; kurum ve kuruluşların güvenlik teknolojilerine yeterli ölçüde yatırım yapmadıkları görülmektedir.(Vural, Sağıroğlu, 2008: 508)

Geçmişte yaşanan önemli olaylardan görüleceği gibi iletişim güvenliğinin üst düzeyde sağlanabilmesi için standartlara uygun, yenilikçi, güncellenebilir ve devamlılık vadeden bilgi ve iletişim güvenliği sistemlerine kurumların ihtiyacı olduğu göz ardı edilemez bir gerçektir. Ülkemizde tüm kurumlar bilgilerini saklamak, iletmek ve haberleşmek için otomasyon sistemleri, haberleşme aracı yazılımlar ve kurumun büyüklüğüne göre Veri Tabanı Yönetim Sistemleri(VTYS) kullanmaktadırlar. Yani bilgiler, özel veriler ve iletiler artık elektronik ortamlarda tutulmaktadır ve iletilmektedir.

Bu bölümde ulusal güvenliği ilgilendiren askeri konuları, istihbarat konularını, dış ilişkileri, ekonomik, teknolojik, bilimsel, ticari ve diğer çok gizli, özel, hizmete özel, tasnif dışı gizlilik taşıyan bilgileri kendi içinde ve dışında iletime tabi tutan kurumlardan bahsedilecektir.

3.1. Ulusal Güvenliği İlgilendiren Kurumlar

Ulusal güvenliği sağlamak, suçları önlemek, terör ve organize suçlarla mücadele etmek, kamu düzeninin sağlanmasına yardımcı olmak, delil toplamak, yabancı hükümetlerin hâkimiyet kurmak amaçlı toplumsal ve sosyal yönlendirmelerine karşı koymak maksadıyla güvenlik kuvvetlerinin ve istihbarat teşkilatlarının bilgiye, bilgilerin güvenilirliğine ve güvenliğine ihtiyacı vardır. Bu kurumların bilgileri mutlaka daha değerli ve daha gizli olmaktadır. Bu nedenle bilgi güvenliğini kendi içinde ve iletimi esnasında

sağlamak için kurumsal ve ulusal bilgi güvenliği yönetim sistemine ihtiyaç vardır.

Resmî devlet kurumlarında, basın yayında veya sivil toplum örgütlerinde hatta kişilerde yalnız ülke ile ilgili değil, yabancı ülkelerle de ilgili bilgiler bulunur. Bunlardan da iyi bir bilgi yönetimi sistemi ile büyük faydalar sağlanabilinir. Örneğin, her hangi bir ülkenin millî arşivinde araştırma yaparak belge örnekleri almış bir araştırmacının hem getirdiği belgelerden, hem de edindiği kişisel bilgi ve deneyimlerden bir istihbarat elemanının istifade edeceği çok konu olabilir. Bu, ilgili araştırmacıyı sorgulamak anlamında değildir, bilgi yönetimi sistemi metodu içerisinde bilgileri kayıt altına alır ve bunu bilmesi gereken prensibi çerçevesinde paylaşıma sunarsınız. Faydalanmak isteyen herkes ve her makam bu bilgi birikiminden faydalanır. İstihbarat elemanları veya istihbarat teşkilatları için açıkta duran, ortalıkta dolaşan sayısız nitelikli belge ve bilgi mevcuttur. Ancak bunların ihtiyaç sahiplerince zahmetsizce elde edilmesini ve güvenliğini sağlamak bilgi yönetim sisteminin görevidir.

Tehlike ve tehdidin ne taraftan, nasıl geleceğini iyi hesaplamak, yeni tehdit unsurlarıyla mücadele edebilmek için istihbarat teşkilatlarının yeni bir savaş türü olan "Bilgi Savaşları"na hazır olması gerekiyor. Savaş Hârici Harekât (Operation Other Than War) kavramı olarak adlandırılan modern savaş kavramı hayatımızın her alanını kapsamaktadır. Dr John Alger, bilgi savaşını, "sahip olduğumuz bilgilerimizi, bilgi sistemlerimizi ve bilgi tabanlı yapılanmalarımızı korurken; rakibin bilgilerini, bilgi sistemlerini ve bilgi tabanlı yapılanmalarını etkileyerek bilgi üstünlüğünü sağlamamıza yarayacak her türlü faaliyetler" şeklinde tarif eder. Yine her şey gelip bilgi noktasında durmaktadır. Günümüzde yaşamanın, güçlü olmanın tek kaynağının bilgi olması hepimizi bilgili olmaya zorluyor. Bilgiyi tek başına üretmek, yığınlarla bilgi sahibi olmak da yeterli gelmiyor. Aynı sınırlar içerisinde görev ve

faaliyetlerini yerine getiren kurum ve kuruluşlar ile örtülü bilgiye sahip her ferdin ürettiği ve barındırdığı bilginin stratejik, sosyal, kültürel, ekonomik vb. değeri onları ancak düzenli kayıt altına aldığınızda ve hızlıca eriştiğinizde ortaya çıkıyor (http://www.bilisim2023.org, 2009).

Ülkemizin kurum ve kuruluşları ile bireylerin ürettiği bilgiyi yönetip, değerlendirecek, koruyup, hizmete sunacak altyapı, üstyapı ve sistemlerini kurması gerekiyor. Bilgi yönetim sistemini kurarken yalnız kendi coğrafyamız, ilgi ve hâkimiyet alanımızla sınırlı kalmayıp, bölgesel ve gelecekte küresel hâkimiyet alanlarımız olacağını, olması gerektiğini hesap edilmelidir.

3.2. Ekonomik ve Ticari İlişkiler İçeren Kuruluşlar

Bilgi güvenliği ticari rekabet ilişkileri ve elektronik para güvenliği açısından ticari kuruluşlar için çok önemlidir. Ticari bir kuruluşun günümüz dünyasında teknolojiden bağımsız varlığını sürdürebilmesi gibi, bilgi ve iletişim güvenliğini almadan başarılı olması mümkün görülmemektedir.

Bilginin dolaşımı ve paylaşımının küresel bir yapıya kayması, bilginin nüfuz mücadelesinde, ekonomik rekabette stratejik önem kazanmasına sebep olmuştur. Ekonomik amaçlar ve hedeflerle siyasî amaç ve hedefler paralellik göstermiş, uluslararası pazarda yer kapmak, kartelleşmek için her yol mubah görülmektedir. Küresel nüfuz sahibi olmak için askerî, kültürel, dinî, siyasî, psiko-sosyal vb. her alanda faaliyetler yoğunluk kazanmıştır. Örneğin; bir elektronik devi olan Fransız devi Thomson CSF firması Brezilya'daki yağmur ormanlarının uydu eliyle izlenebilmesi için Brezilya hükümetiyle görüşmelere başlamıştır ve bu sistemin çalışması için 800 milyon sterlin değerinde bir anlaşmayla ihaleyi kazanma noktasına kadar ilerlemiştir. Ancak devreye ECHELON girmiş, görüşme bilgilerini ele geçirerek, detaylarıyla birlikte bir Amerikan firması olan Raytheon Corp. Şirketine aktarmıştır. Sonuçta bu dev

ihaleyi Raytheon kazanmıştır. Fransızların kaybı tolere edilecek gibi değildir (http://www.bilisim2023.org: 04.05.2009).

İnternet bankacılığı, bankacılık hizmetlerinin internet üzerinden sunulduğu bir alternatif dağıtım kanalıdır. Türkiye' de bugün internet bankacılığı, herhangi bir banka şubesinin sağlayacağı hizmetlerin neredeyse hepsinden zaman ve mekandan bağımsız olarak çabuk ve kolayca yararlanmayı sağlar.

Bankalar başta olmak üzere ağ üzerinden paranın taşınmasını sağlayan tüm ticari kuruluşlara ait sistemler ileti güvenliğine yönelik saldırıların tehdidi altındadır. Bu konuda çok ciddi kriptoloji çalışmaları yapılmıştır. Şifreler, oturum ve IP kontrolleri, elektronik ve mobil imzalar derken korsanlar ve kuruluşlar arasında büyük bir bilgi güvenliği mücadelesi yaşanmaktadır. Vergi daireleri, sigorta şirketleri, online ödeme alan Tedaş, Telekom gibi şirketler bilgi güvenliğine dikkat etmesi gereken kuruluşlar arasında bulunmaktadır.

3.3. Eğitim, Sağlık ve Diğer Özel Hizmetleri Veren Kurumlar

Üniversiteler, hastaneler, rehabilitasyon merkezleri, kan bankaları, biyolojik araştırma merkezleri, enstitüler, insani yardım yapan dernekler, sendikalar gibi kuruluşlarda da bilgi kaynaklarının ve iletişim ağlarının güvenliği oldukça önemlidir.

Milli Eğitim Bakanlığı, ilköğretim okullarında öğretmenlere birer şifre vererek öğrencilerin notlarını internet üzerinden hazırlanan sisteme girilmesini sağlayan bir uygulama başlatmıştır. Böyle büyük veri tabanlarının özenle yedeklenmesi ve korunması sağlanmalıdır. Benzer şekilde üniversitelerdeki öğrenci otomasyonları ve personel bilgi sistemleri bilgilerine ulaşıldığında ya da değiştirildiğinde büyük problemlerle karşılaşılabileceğinden sürekli güvenlik düzeyleri arttırılmaya çalışılmaktadır. Geçmişte bu konuyla ilgili

büyük sorunlar yaşanmıştır. Üniversitelere ait veri tabanları kötü niyetli atakların hedefi olmuştur.

Hastanelerin ve diğer bir kısım sağlık kuruluşlarındaki bilgi edinme ve randevu sistemleri sanal ortama alınması beraberinde yine bilgi güvenliği sıkıntılarını ortaya çıkarmıştır. Bununla birlikte milli karakteri içeren verilere sahip ve biyolojik savaşa karşı mücadele veren araştırma merkezlerimiz ile enstitülerimiz veri ve ileti güvenliğini sağlamak durumundadırlar.

Yine birçok işleminde para kullanılan ve üyelerinin bilgilerinin çok özel olduğu sosyal dernekler ve sendikalar, korunaklı ağlara sahip olması gereken kuruluşlardandır. Bu tür kuruluşlar sürekli bilgi ve belge güvenliğini sağlamak için çaba sarf etmektedirler.

4. KURUMLARDAKİ BAZI GÜVENLİK AÇIKLARI

İletişim ortamlarının artması ve kullanımının yaygınlaşması sonucunda elektronik ortamlarda bulunan bilgilerin her geçen gün katlanarak artmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen elektronik uygulamaların ve işlemlerin fazlalaşması, ihtiyaç duyulan bilgilerin kablolu ve kablosuz ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir.

Özellikle ülkemizde, ne yazık ki, birçok kurum ve kuruluşun ve her seviyeden bilgisayar kullanıcısının çoğunlukla bilgi ve bilgisayar sistemlerine ve bilgi güvenliğine bakış açısının yeterli seviyede olmadığı tespit edilmiştir (4, 29). Kasım-Aralık 2004 tarihleri arasında yapılan bir araştırmada, 800 civarında ADSL abonesi ve 500'ün üzerinde şirketin güvenlik sisteminin denetlenmesi ile

gerçekleştirilen "Türkiye İnternet Güvenliği Araştırması" sonuçlarına göre şirketlerin %27'sinin bilişim sistemlerinde çok yüksek seviyede açıklar gözlenmiş, ADSL abonelerinin %72'sinin güvenlik duvarı yapılandırmalarında ciddi açıklar görülmüştür (Ersoy, 05.02.2009).

Kurum da yürütülen güvenlik politikalarından ve özellikle bu konuda yeterli donanım ve bilgiye sahip olmayan çalışanlardan kaynaklı oluşan açıklar kurumları ciddi tehlikelere sürüklemektedir. Bunun yanı sıra; saldırganların saldırı yapabilmeleri için gerekli olan yazılımlara internet üzerinden kolayca erişebilmeleriyle önemli ve gizlilik arz eden verilere, iletişim kanallarına ataklar son yılarda sürekli artış göstermektedir.

Güvenlik önlemleri, hiçbir zaman mükemmel değildir ve her güvenlik önleminin bazı zayıflıkları bulunabilmektedir. Güvenliğin sağlanması için zayıf noktalardan doğacak sorunların olabildiğince çözülmesi gerekmektedir (Karaarslan vd., 2008: 4). Bu zayıf noktalar genellikle insan kaynaklı açıklıklardır.

Kurum yöneticilerinin ve çalışanlarının (Bilişim Sistemleri Güvenliği El Kitabı, 2006: 9);

- Problemleri erteleyerek geçiştirmesi,
- Kısa dönemli günü kurtarmaya yönelik çözümlere yönelmesi,
- Kurumsal bilgi, iletişim ve prestijin ne kadar önemli olduğunu fark edememesi
- Güvenliğin işleme tarafına gerekli özeni göstermemesi, birkaç geçici çözüm uygulayıp dikkatli ve detaylı inceleme yaparak problemlerin ortadan kaldırılmasına izin verilmemesi,

- İş hayatı ile bilgi ve iletişim güvenliği arasındaki ilişkiyi yeterince kavramamış olması, fiziksel güvenliğe önem verirken yetersiz bilgi ve iletişim güvenliğinden kaynaklanabilecek tehlikeleri görememesi,
- Güvenlik sorumluluğunu yeterli güvenlik eğitimi almamış kişilere verip bu kişilere ne eğitim ne de iş yapmaları için yeterli zamanı vermemesi gibi tavırları sonucu hatalı ve özensiz ağ yapılandırmaları, web uygulamaları ile ilgili hatalar, kolay tahmin edilebilir şifre ve hesap adlarının kullanılması, zayıf loglar(günlükler) ve saldırı tespit sistemleri kullanılması, yetersiz güvenlik duvarı konfigürasyonları gibi güvenlik açıklarına yol açmıştır.

Kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasında insan faktörü önemli bir yere sahiptir. İnsan faktörü sayesinde birçok güvenlik denetimi devre dışı bırakılabilmektedir. Yeterli düzeyde eğitim almamış kurum çalışanları(yönetici, teknik sorumlu, son kullanıcı) veya kurumsal bilgi sistemleri üzerinde yetkili olan ve yerel saldırgan(internal hacker) olarak adlandırılan iyi niyetli olmayan üst derecede bilgiye sahip olan çalışanlar kurumsal bilgi güvenliğini üst düzeyde tehdit eden insan faktörleridir. Kurumsal bilgi güvenliği; insan faktörü, teknoloji ve eğitim üçgeninde devamlılık gerektiren ve bu üç unsur arasında tamamlayıcılık olmadığı sürece yüksek seviye bir güvenlikten bahsedebilmenin mümkün olamayacağı yönetilmesi zorunlu olan canlı bir süreçtir.

Bu konuya ait alt başlıklar anlatılırken Türkiye Bilişim Derneğinin hazırladığı Bilgi Sistemleri Güvenliği El Kitabı'ndan istifade edilmiştir.

4.1. Hatalı ve Özensiz Ağ Yapılandırmaları

Güvenlik açığı barındıran ağa sızabilen bir saldırgan, kurum ağına doğrudan erişim sağlayabilmekte ve yerel kullanıcı haklarına sahip olmaktadır. Bu nedenle ağın düzgün ve planlanarak yapılandırılması gerekmektedir. Ağ

üzerinde yapılacak iletişimde mesajların şifrelenerek gönderilmesi kurumun yararına olacaktır. Kullanıcıların internete erişim hakları kurumun lehine olacak bir şekilde düzenlenmelidir. Uzaktan kurumdaki sunuculara erişimlerde verilen yetkiler, yerel ağda sahip olunan yetkilerden çok daha az olmalıdır.

Eğer kurum birden fazla ve birbirinden farklı yerde birimlere sahip ise, merkez gövde ağı oluşturulmalı diğer birimler için ise sanal özel ağlar kurulmalıdır. Bu yapıda merkeze erişim için harici kimlik doğrulama sistemleri kullanılmalıdır. Sanal özel ağlara güvenli iletişim kanalları oluşturulmalıdır. Kullanılacak istemci yazılımları, internet kullanımı ile sanal özel ağ kullanımı arasında yalıtım yapılmalı ve istemcilerin internette farklı kaynaklara erişimi kısıtlanmalıdır.

Kablosuz ağ kullanılacaksa; bu ağın internet gibi güvensiz bir ağ olduğu göz önüne alınmalı, sinyal kalitesinde kısıtlamalara gidilmeli istemciler harici kimlik doğrulama sistemleri tarafından kontrole tabi tutulmalıdırlar. Kurum güvenlik politikası dahilinde, gezgin kullanıcıların sistemlerinde kurumda kullanılmamasına rağmen kablosuz ağ kartı bulunması engellenmeli ve istemci kurumda iken ağ kartının devre dışı olması sağlanmalıdır.

Sesli görüşmeleri sağlayan kurum telefon santrallerinin belli bir dışarıya erişim politikası uygulanarak, telefon görüşmeleri sağlanmalıdır. Kullanılacak santraller önemli görüşmeleri kayıt altına alabilmeli, kurum dışından sisteme girilip özel görüşmeleri dinlenmesi engellenmelidir. Voice IP, ip telephoning gibi sesli görüşme sistemlerini sağlayan özel ağlar; dinlenme, veri çalınması ve ses iletilerinin engellenmesi gibi saldırılara karşı koruma altına alınmalıdır.

4.2. Web Uygulamaları İle İlgili Hatalar

Kamu kurumlarının büyük bir kısmı; halkla ilişkiler, tanıtım veya bilgilendirmeler amacıyla kendi web sitelerini oluşturmuşlardır. Ayrıca online işlemlerin gerçekleştirilebilmesi amacıyla otomasyonlar web ortamına

taşınmıştır. Bilgilere webden ulaşılması nedeniyle; kurumların özel bilgileri izinsiz erişim riski altına girmiştir. Bu riski gidermek için bazı önlemler alınmalıdır. Bu önlemlerin başında kullanıcılara bazı kısıtlamalar getirilmesi gelmektedir.

Web uygulamalarını temel ve genel mantığı iletişime tabi tuttuğu verileri veri tabanı adı verilen kendine has sorgulama diline(SQL) sahip bir elektronik ortamda muhafaza etmesidir. SQL dilinde yapılan sorgular neticesinde verilerin saklandığı ortamda alınıp getirilerek web ekranında kullanıcılara gösterilmektedir. Saldırganlar SQL dilini kullanarak önemli verileri elde etmeye çalışırlar. Genel olarak problemler, uygulama geliştiricinin, SQL sorgularında anlam ifade edebilecek, UNION gibi kötü niyetli karakterlere karşı bir önlem almadığı zaman ortaya çıkmaktadır. Bu durum kullanıcıya önceden planlanmamış uygulama düzeyinde erişim sağlayabilmektedir. İçinde SQL sorguları barındıran birçok ürün SQL sorguları değiştirebilmesine karşı savunmasızdır. Saldırganlar SQL sorgularını değiştirme tekniklerini web sitelerine ve uygulamalara zarar vermek amaçlı kullanmaktadırlar. Bu tür saldırılar ile veri tabanı üzerinde eklemler yapılabilir, değişikler yapılabilir, veri tabanı yöneticisinin tüm haklarını elde edip bu haklar doğrultusunda sunucuda komut çalıştırabilirler. Bu nedenle web uygulamalarının tüm bileşenlerinde kullanılan değişkenler için kontroller oluşturulmalı ve değişkene atanması beklenen veri türü ile kullanıcı girdisi karşılaştırılmalıdır.

Web uygulamalarında oluşabilecek bir diğer açık, saldırganın hedef web sitesi aracılığıyla site ziyaretçilerinin sisteminde komut çalıştırabilmesine olanak tanımaktadır. Saldırı sonucu olarak site ziyaretçilerinin tarayıcılarında bulunabilecek güvenlik açıklarının kullanılması, bazı script dili komutlarının çalıştırılmasını mümkün kılmaktadır. Bu tür komutlar ile kullanıcıya ait site çerezleri alınabilir, kaydedilmiş şifreler çalınabilir veya tarayıcıda bulunabilecek güvenlik açıkları ile kullanıcı sistemi ele geçirile bilir. Ayrıca

elektronik ticaret veya bankacılık uygulamaları için sahte giriş ekranları oluşturularak ziyaretçilerin yanıltılması ve sonucunda kullanıcıya ait önemli verilerin ele geçirilmesi mümkün olabilir.

Web siteleri ve web tabanlı otomasyonların üzerinde çalıştığı ve ortak erişime sahip makinelere web sunucular denir. Çoğu kurum bu sunuculara ait yazılımları ve işletim sistemlerini güncellemektedir. Microsoft IIS ve ASF Apache gibi web sunucu yazılımlarının eski versiyonları birçok güvenlik açığı barındırmaktadır. Web sunucularının düzenli güncellenememesinin sebeplerinden en önemlisi, bu yazılımların parçası olduğu ticari ürünlerin kullanıyor olmasıdır. Web sunucuda yapılacak sürüm değişikliği veya güncellemeler, ürün firması tarafından desteğin kesilmesine neden olabilmektedir. Her iki web sunucusunda da saptanan güvenlik açıkları web sunucusun servis dışı kalmasına veya tüm sunucun ele geçirilmesine neden olmaktadır. Önceden belirlenmiş yapılandırma ile kurulan web sunucuları gerekli olmayan birçok bileşeni bünyelerinde barındırmakta ve gelecekte bu bileşenlere ait ortaya çıkabilecek güvenlik açıklarından etkilenebilmektedir.

Web sunucu yazılımlarının düzenli güncellenmeleri oldukça önemlidir, ayrıca gerekli olmayan tüm bileşenler (WebDAV, http, Frontpage Uzantıları, Yazıcı desteği, index oluşturma desteği ve örnek CGI uygulamaları) sistemden çıkarılmalıdır. Böylece gelecekte söz konusu bileşenler için duyurulacak güvenlik açıklarından etkilenilmeyecektir. Microsoft IIS web sunucusu için Microsoft URLScan aracı kullanılmalı ve tüm web istekleri içeriklerine göre süzülmelidir. Bir ters proxy aracılığıyla güvenlik açığı barındıran web sunucusuna doğrudan erişimin kısıtlanması, uygulama katmanında kullanılabilecek içerik denetim sistemleri, uygulama güvenlik duvarları veya, saldırı tespit sistemleri verimli sonuçlar üreten çözümlerdendir.

4.3. Saldırı Tespit Sistemlerinin Hatalı Kullanılması ve Zayıf Loglar

Saldırı tespit sistemleri etkin güvenlik için vazgeçilmez uygulamalardır; ancak hatalı yapılandırılmaları durumunda saldırganların ağ iletişimini aksatabilmesi için en önemli araçlardandır.

Tespit edilen saldırılara kontrolsüz tepkiler verilmesi durumunda;

- Saldırganlar saldırı tespit sisteminin türünü ve özelliklerini saptayabilir,
- Çokça yapılan saldırı ile kayıt veri tabanlarını doldurabilir,
- Ağda gereksiz bir ileti trafiği oluşturabilir,
- Saldırılarını gizleyebilir,
- Sahte saldırılar ile kritik görevdeki yönlendirici ve alan adı sunucularına erişimi kesebilir
- Veya güvenlik duvarı aracılığıyla saldırgan engelleme yapılıyor ise güvenlik duvarının kural tablosunu taşırabilir.

Ön tanımlı yapılandırmalarda, saldırı tespit sistemleri saldırı önleme yapmamaktadırlar, ancak optimizasyon yapılmamış bir çok sistemde kontrolsüz olarak saldırı önleme yapılmaktadır. Güncelleme ve tanımlamaları doğru yapılmamış, güncel yamalara uygulanmamış sistemlerde, farklı veri ve iletişim türleri seçilmesi durumunda saldırı tespit edilememektedir.

Ağ üzerinde bir süre saldırı tespit sistemi izleme durumunda çalıştırılmalı ve gelen mesaj trafiğine bağlı olarak saldırı tespit sistemi kural ve tepki optimizasyonu yapılmalıdır. Saldırı tespit sisteminin saldırı türlerine göre tepki vermesi sağlanmalı, zorunlu kalmadıkça tepki üretilmemelidir. Güvenilir sistemler tanımı oluşturulmalı önemli yönlendiriciler ve alan adı sunucuları ile kritik güvenlik sistemleri güvenilir olarak tanımlanmalıdır. Tepkiler öncelikle ICMP/TCP/UDP paketleri ile üretilmeli, çok sayıda saldırı olması durumunda tek bir işlem olarak ele alınmalı ve sürekli saldırılarda saldırgan sistem

güvenlik duvarı tarafından engellenmelidir. Paket ve iletişim analiz seçenekleri için önerilen yama ve yardımcı yazılımlar kullanılmalı, ürün geliştiricilerin hazırlamış oldukları rehber dokümanlarla karşılaştırılarak yapılandırmalar gözden geçirilmelidir.

Önemli bilgilerin saklandığı ve kuruma ait iletişim kanallarının işlemesini sağlayan sunucular üzerinde, erişimlere ve yapılan değişiklere dair kayıtlar tutulur. Bu kayıt dosyalarına bilişim literatüründe log dosyaları adı verilmektedir. Log dosyalarının nasıl tutulacağı iletişim ağını yöneten sistemciler tarafından ayarlanır. Bu dosyaların tutacağı kayıtlar satır satır ve anlaşır şeklide olmalıdır. Aksi bir durumda kayıtlar dosyadan okunur, yorumlanır ve aksiliğin hangi durumdan kaynaklandığı, hangi tarih ve saatte meydana geldiği, bu aksiliğe kimlerin sebep olduğu yorumlanabilir. Log dosyaları sunucu üzerinde en az veriler kadar, özel bir yere konulmalıdır. Çünkü saldırıyı gerçekleştiren saldırganın işlemi bitirdikten sonra düşüneceği ikinci işlem kendi izini kaybetmeye çalışmak olacaktır. Bu nedenle log dosyalarını bulup ya değiştirmeye çalışacak ya da silip saldırıyı yapanın tespit edilmesine engel olacaktır. Bu nedenle sistem ve ağ yöneticilerinin tutulan bütün loglara önem vermeleri gerekmektedir.

4.4. Kolay Tahmin Edilebilir Şifre ve Hesap Adlarının Verilmesi

Kurumda bulunan bilgisayarların, servis yöneticilerinin veya servislere özel kullanıcı hesaplarının kolay tahmin edilebilir şifrelere sahip olması, bir saldırganın kurum ağına yönelik kullanabileceği en basit saldırı yöntemidir. Özellikle yönlendirici yönetim şifreleri veya sunucu servislere ait kullanıcı hesaplarının şifreleri kolayca tahmin edilebilmektedir. Web temelli uygulamaların yaygınlaşması ile web temelli uygulamalar da şifre seçim hatalarından etkilenmektedir. Bir saldırgan, yönetim hesaplarının veya geçerli

bir kullanıcıya ait şifreleri ele geçirmesi durumunda, kurum ağına sınırsız erişim sağlayabilmekte ve istenen ağ iletişimini kolayca ele geçirilebilmektedir.

Şifre seçimi, kalitesi ve yönetimi konusunda kurum politikası oluşturulmalıdır. Başta sistem yöneticileri olmak üzere kullanıcıların şifre seçim kriterlerine uyumu, dizin hizmetleri veya alan denetçileri ile sağlanmalı ve kullanıcıların daha zor tahmin edilebilir şifre seçimleri yapmaları sağlanmalıdır. Özel uygulamalı alanlarda(sanal özel ağ, ERP yazılımları, bankacılık uygulamaları v.b.) harici doğrulama sistemleri veya sayısal sertifikalar kullanılmalıdır. Web temelli uygulamaların tasarımında, kullanıcı hesap yönetimi ve şifre seçimi hususunda beklenen kriterlerin uygulanması zorlayıcı olmalıdır.

4.5. Güvenlik Duvarı Konulmaması veya Hatalı Yapılandırılması

Güvenlik duvarları kurumların bilgi ve iletişim güvenliği sürecinde en önemli bileşenlerdendir. Kurumun işleyişini sağlayan veya yardımcı olan otomasyon sistemlerinin bulunduğu sunucuları içeren ağı, iç ve dış saldırılara karşı koruyan ve erişim hakları veren bir güvenlik duvarına bütün kurumlarda ihtiyaç duyulmaktadır. Özel istemci ve sunuculara verilmiş sınırsız erişim hakları, güvenlik duvarlarının önünde bulunan sunucu ve istemciler ile erişim denetim kuralları özelleştirilmemiş güvenlik duvarları, saldırganların kurum ağına sınırsız olarak erişimine imkan tanımaktadır. Yayınlanmış güvenlik açıklarının takip edilememesi veya yapılandırma hatası sonucu güvenlik duvarı tarafından korunmayan bir sistem, saldırganın kurum ağına girebilmesi için atlama noktası olabilmektedir.

Güvenlik duvarı tasarımı yapılırken, kurum ağında bulunan ve internet üzerinden hizmet sunacak sistemler Demilitarized Zone (DMZ-silahsızlandırılmış alan) denilen bölüme taşınmalı, yönlendirici ile güvenlik duvarı arasındaki ağa fiziksel giriş imkanları önlenmeli ve güvenlik duvarı

üzerinde düzenli kontroller yapılarak, özel haklar sağlayan kurallar devre dışı bırakılmalıdır. Özel amaçlar için güvenlik duvarının dışına yerleştirilmesi gereken sistemlerin yapılandırılmaları özelleştirilmeli, gerekmeyen servisler durdurulmalı, güvenlik yamaları tamamlanmalı ve güvenlik duvarı üzerinden ağa erişimlerinde hiçbir özel erişim kuralı belirlenmemelidir.

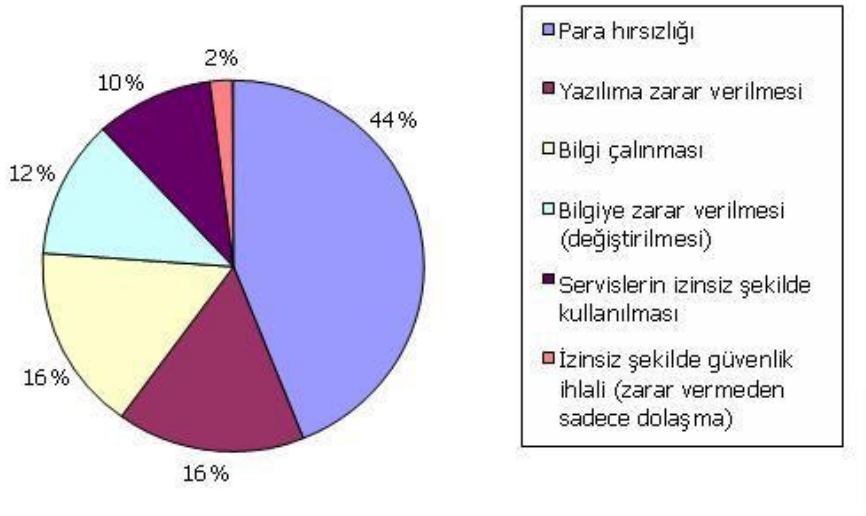
5. BİLGİ VE İLETİŞİM GÜVENLİĞİNİ TEHDİT EDEN SUÇLAR

Yapılan yasadışı eylemlere hukuki alanda suç adı verilmektedir. Günümüzün gelişen teknolojisinde işlenen suç türleri ve sayıları giderek artmaktadır. İnternet üzerinden gerçekleştirilen eylemler, kişi veya kurum bilgisayarlarına, iletişim cihazlarına, iletişim kanallarına ya da kurumsal ağlara ve sunuculara yapılan saldırılar ülkemizde bilişim suçları çerçevesinde yargılanır ve cezalandırılır.

Bilişim suçlularını suç işlemeye iten nedenler arasında geleneksel olarak bireyleri suç işlemeye götüren nedenlerden farklı, yeni bir neden görmek neredeyse olası değildir. İntikam alma duygusu, güce sahip olma, aç gözlülük, şehvet, macera veya "yasak meyveyi tatma" arzusu gibi geleneksel olarak bireyleri suç işlemeye götüren nedenler bilişim suçları anlamında da bireyleri suç işlemeye götüren nedenler olmaktadır (Özcan, 2004: 146).

Gartner Datapro Research şirketi tarafından yapılan araştırma sonuçları kurumsal bilgilerin nasıl, kimler tarafından tehdit edilebileceği ve zarar verebileceği konusunda ilginç sonuçlar vermektedir. Genel kanı ilk başlarda saldırıları yapanların genç ve kendilerine ün sağlamak isteyen bilgisayar hackerleri olduğu fakat zamanla bunların yerlerini daha çok maddi gelir sağlamayı amaçlayan organize örgütlerin aldığı görülmektedir.

Şekil 1. Bilgisayar Suçlarının Çeşitleri



(Kaynak: Bilgi Sistemleri Güvenliği El Kitabı)

Bilgi ve iletişimi tehdit eden bilişim sistemine yetkisiz girip verileri alma, bozma, değiştirme, yok etme veya erişilmez kılma gibi eylemler(http://www.bilgiguvenligi.gov.tr, 22.10.2008):

- Log dosyalarının değiştirilmesi,
- Gizli kanallardan bilgi sızdırılması,
- Ekipmanın tahrip edilmesi,
- Bilgin ele geçirilmesi,
- Kötü niyetli yazılımlar bulaştırılması,
- Mesajların yanlış yere veya geciktirilmesi,
- İletişim kanallarının gizlice dinlenmesi,
- Kurumlara ait bilgilerin özel amaçlarla kullanılması,
- Bilgi ve medya hırsızlığı,

- Bilgilere, yazılımlara, ekipmanlara yetkisiz erişilmesi gibi hüviyetlerde bulunabilir.

Bu tür eylemlerde bulunan kişi ve grupların para hırsızlığı, kin ve kıskançlık kaynaklı zarar verme, servislerin izinsiz kullanılması, izinsiz şekilde zarar vermeden dolaşma gibi amaçları olabilmektedir.

5.1. Para Hırsızlığı

Bankacılık ve elektronik ticaret işlemleri doğasında parayla ilgili işlemler barındırdığı için internet korsanlarının tehditlerinden en fazla etkilenen sistemlerdir. Bankacılık sektörünün interneti kullanmaya başladığı günden itibaren iletişim ağlarına yapılan "para hırsızlığı" amaçlı saldırılar giderek artmaktadır.

Elli yıl öncesinin meşhur Amerikan banka soyguncusu Willie Sutton'a sormuşlar: Niçin banka soymakta bu kadar ısrar ediyorsun? "Çünkü orası paranın bulunduğu yer " diye yanıtlamış Sutton. Kriminolojideki suçların fırsatları takip ettiği veciz bir şekilde açıklayan bu yanıttan yola çıkarak saldırıları en etkin yolunun suç işlemeye götüren fırsatların ortadan kaldırılması gerektiği ön plana çıkmaktadır (Özcan, 2004: 146). Fırsatların ortaya çıkmasında, diğer bir deyişle bilişim suçunun işlenmesinin önlenmesinde her şeyi devletten, polisten beklemek bizi istediğimiz sonuçlara götürmeyecektir. Bireyler ve kurumlar evlerini ve işyerlerini korudukları gibi bilgisayarlarını, şifrelerini, özel bilgilerini de yapılacak olası saldırılara karşı korumak zorundadır.

Önceleri bankaların elektronik para trafiğini sağlayan sistemlerine, veritabanlarına, otomasyon barındıran sunucularına yönelik saldırılar yapılmaktaydı. İnternet bankacılığı işlemleri bankalar tarafından başlatıldığından itibaren bu saldırılar çoğunlukla internet kullanıcılarına yönelmiştir. Bunun en büyük nedenleri kullanıcıların bilgisayarlarına yapılan

saldırıların farkına varamamaları, bilgisayarlarında bulunan açıkları önemsememeleri, bankacılık işlemlerinde kullandıkları şifreleri ve yetkileri kendisi haricinde kullanılamaması için yeterli çaba sarf etmemeleridir. İnternet bankacılığı hususunda birçok suç işlendiğini, internet korsanlarının ve örgütlerinin yakalandığı haberlerinin medyadan çokça işitilmektedir. İnternetteki zafiyetlerden ve sesli görüşmelerde yapılan dinlemelerden kaynaklı birçok mudiinin banka hesaplarının boşaltıldığı, çoğu zaman hırsızların yurt dışında olduğu için yakalanamaması nedeniyle mağdur oldukları bilinmektedir.

Korsanlar yasal olmayan yollardan elde ettikleri verileri anlamlandırarak, şifreli ise şifrelerini çözerek bankaları ve banka müşterilerini mağdur etmektedirler. Bunu iki farklı yoldan yapabilirler:

1- Telefon bankacığı yoluyla, müşteri hakkında kendisine sorulan soruların tümünü doğru yanıtlayarak,

2- Ürettikleri korsan banka kartına bu bilgileri yükleyerek ve ATM'lerde kullanmak suretiyle müşteriye ait hesabı boşaltabilirler.

Diğer dikkat edilmesi gereken bir husus ise kredi kartlarıdır. E-ticaret işlemleri yapan bir çok web sitesi müşteriye tahsilatı kredi kartları ile yaptırmaktadır. Kredi kartı bilgilerinin web üzerinden girilmesi yüzünden çok kişi online alışveriş mağduru olmuştur. Bu nedenle şirketler ve bankalar bu işi daha sıkı tutmaktadır. Müşteri internetten alışverişini yaparken kredi kartı ödeme safhasına geldiği anda firma veya banka tarafından SSL güvenlik sertifikası desteği olan sayfalarda kart bilgi girişi sağlanmaktadır.

5.2. Duygusal Kaynaklı Zarar Verme

İletişime ve bilgiye yönelik saldırılar aşağıdaki bahsedilen duygulara sahip olan kişi veya gruplar tarafından yapılabilir:

Ün kazanma arzusu ile bilişim konusunda bilgi ve becerilerini göstermek için verilen zararlardır. Bu tür gruplar özel şirketlerin ve kamu kuruluşlarının sistemlerine girerek veya sistemlerini ele geçirerek ses getirecek eylemler yapmaktadır.

Kin ve düşmanlık güttüğü örgütlerin sistemlerine yapılan saldırılardır. Ya da eski çalıştığı ve sorunlu ayrıldığı kuruma çalıştığı döneme ait bilgileri de kullanarak zarar vermek isteyen kişilerin yaptığı saldırılardır.

Kıskançlık duygusuyla rekabet içinde olduğu kişi veya grupların bilgi ve iletişim ağını zarara uğratma amacı ile gerçekleştirilen eylemler olabilir.

Merak duygusuyla sadece yetkisiz bir şekilde sistemde dolaşarak bilgi elde edilmek istenmesi de duygusal kaynaklı zarar verme kategorisinde incelenmektedir.

5.3. Servislerin ve Yetkilerin İzinsiz Kullanılması

Servisler bilgi ve iletişim sistemlerinin hizmetleridir. Otomasyon sistemleri, işletim sistemleri, internet, intranet sistemlerde bulunabilen kişilere sağlanan başlıca servislerdir. Her sisteme ait veya sistemin servislerine ait kullanıcı tanımlamaları olmalıdır. Kullanıcıların ihtiyaçlarına göre tanımlamalarına karşılık şifreler ve bu şifrelerle sisteme giriş yaptıklarında yetkiler tanımlanmıştır. Servislerin kullanılması şifreler ve yetkiler dahilinde olmalıdır. Eğer korsan bu yöndeki güvenlik açığını fark etmişse bunu istismar edebilir. Yani servisleri, hakları, kullanıcı rollerini yetkisiz kullanma yoluna gidebilir.

Bu tür açıkların kapatılması için ‘admin’ veya ‘root’ adı verilen en yetkili kullanıcının güvenliği en ciddi şekilde alınmalıdır. Çünkü bütün kullanıcı tanımları, hak ve yetkilerin verilmesi bu kullanıcı üzerinden yapılmaktadır.

Sistemlere yapılan saldırı kayıtlarına bakıldığında en fazla saldırıyı 'root' ve 'admin' kullanıcılarının aldığı görülmektedir.

5.4. Zarar Vermeden Ağda Dolaşma

Daha çok merak duygusuna ve kendini ispat etme düşüncesine bağlı olarak yapılan bu saldırılar, izinsiz bir şekilde güvenliğin aşılması veya ihlal edilmesidir. Bu saldırıları gerçekleştirenler sisteme herhangi bir zarar verme niyetinde değillerdir. Sistemin güvenliğinin ne derece aşılabildiğini göstermek amacında olabilirler ve bunu sistem yöneticilerine iletip açıklarını bildirirler. Bunu yaparken bilgi ve iletilerin içeriklerini gizlilik derecelerini önemsememeksizin öğrenmiş olabilirler.

6. BİLGİ VE İLETİŞİM GÜVENLİĞİNİ TEHDİT EDEN KİŞİLER

Kredi kartları, bilgisayarlar, internet sistemleri v.b. ileri teknoloji ürün ve hizmetleri, insanların artık oturdukları yerden banka işlemleri yapmalarından tutunda alışveriş yapmalarına kadar birçok işi gerçekleştirmelerini sağlamaktadır. Buna bağlı olarak da suç tipleri değişmiş; hırsızlıklar, dolandırıcılıklar, bilgi ve mesaj hırsızlığı ve diğer bilişim suçları da geçmiş yıllara göre artmıştır.

Bilişim Suçları Araştırma Büro amirliğinin verilerine göre bilişim suçları diye tanımlanan ve kredi kartları internet v.b. ileri teknolojiler kullanarak işlenen suçlar 1998 yılından sonra %100'lük artışlarla giderek tehlikeli boyutlara ulaşmıştır. Bu suçların arasında lisans haklarına aykırı çoğaltmalar, sahtecilik, bilgisayar sabotajları, yasa dışı yayınlar gibi kanunsuzluklar da yer almaktadır. Bilişim suçlarının kapsamında yer alan suçların bir kısmı da bilgisayar ortamındaki bilgilere yönelik yapılan saldırılardır. Banka sistemleri, özel ve gizli güvenlik ve çeşitli resmi kayıtlar bu saldırıların potansiyel olarak yöneldiği yerler olmaktadır (Bozkurt, 2004: 258).

Bilişim suçlarının birçoğu macera arayan kişiler tarafından bilinmeyeni keşfetme duygusuyla işlenir. Bilişim alanında suç işleyebilmek için gerekli teknolojik bilgi düzeyinin yüksekliği göz önüne alınırsa, kompleks yapıdaki bilgisayar güvenlik sistemlerine zarar verme yoluyla, suç faillerinin kendilerini ispatlama güdüsü veya bir meydan okuma güdüsü ile hareket ettikleri de unutulmamalıdır.

6.1. Hackerlar

'Hack' ingilizce bir kelime olup 'kesmek', 'yarmak' anlamlarına gelir (http://www.babylon.com, erişim tarihi: 19.02.2009). İngilizcedeki –er takısı fiilin ardından geldiğinde eylemi yapan kişi manası verir. 'Hacker' kelimesi çok sıkça kullanılır olduğundan okunuşuyla 'hekır' olarak dilimize geçmiştir. Kelime manası ve terminolojideki intibası kötü olsa da, bu yeteneğe sahip insanlar iyi işlere yönlendirildiği zaman bilişim konusunda çok fayda sağlarlar.

Hacker yetenekli ve zeki bilgisayar kurdudur. Gerçek yeteneği ise bilgisayar ve iletişim güvenliği üzerinedir. Mantıksal programlama bilgisine sahip kişilerdir. Bilgi ve yeteneğini kötüye kullanarak sistemlere sızan, virüs yazan ya da yayan, ulaştığı sistemlere, ağ yapılarına ve bilgisayarlara zarar veren kişiler hacker olarak adlandırılmıştır. Ama bu kişilerin eğlenmek, zarar vermek, ün kazanmak ve maddi çıkar elde etmek gibi amaçları olabilir.

Bu kişiler sistemlerdeki açıkları kendileri bulurlar. Hazır bilgiyi alıp kullanmaktan ziyade, edindikleri bilgilerle yeni yazılımlar, yeni bilgiler üretmek gibi meziyetleri vardır. Bu nedenle hep aranan ve istenen adam özelliklerindedirler.

6.2. Lamerlar

Hacker olmak için veya olduğunu göstermek için çaba sarf eden fakat yetenek bazında yetersiz kişilerdir. Hackerların yaptığı saldırıları taklit ederek

verdikleri zararlardan pay çıkarmaya çalışırlar. Gerçekte bilgi güvenliği mantığına yönelik bir birikime sahip değillerdir. Bu nedenle güvenlik konusunda yazılım geliştiremezler, saldırılarında var olan yazılımları kullanmaya çalışırlar. Amaçları eğlenmek, hayranlık uyandırmak ve ün gibi kavramlardır.

6.3. Crackerlar

Daha çok programcılık bilgisi gelişmiş kimselerden oluşurlar. Kriptoloji alanında buldukları bütün kaynaktan istifade ederler. Tüm şifreleme algoritmalarını ve sistemlerini öğrenmeye çalışırlar ve ters mantık geliştirmeye çalışırlar. Özellikle Reverse Engeneering dediğimiz, son ürün uygulama dosyası halindeki programları, değiştirmek konusunda yeteneklidirler. Genellikle ücretli olan veya deneme sürümü bulunan programları yazdıkları diğer programcıklarla ücretsiz hale getirerek yasa dışı bir eylemde bulunmuş olurlar.

6.4. Kötü Niyetli Sistem Yöneticileri

Bilişim suçu işleyenler içinde beklide en tehlikeli olanlardır. Bu kişiler zaten kurumda çok kritik noktalarda yetki sahibi oldukları için birçok şey onların elindedir ve işledikleri suçları gizleyebilirler. Bu nedenle kurum yöneticileri ve patronlar bu konuma getirecekleri kişileri ciddi mülakatlardan geçirmelidirler ve işe alındığından itibaren belli periyotlarda bu kişilerden rapor isteyip, raporları dikkatlice izlemelidirler.

Özellikle çoğunluğu devlet kuruluşu olan birçok örgüt sistem yöneticileri tercihlerinde yeterince ince eleyip sık dokumamaktadırlar. Bu nedenle kötü niyetli sistem yöneticilerinden kaynaklan, tespiti ve telafisi diğerlerine nazaran çok daha zor olan bilişim suçları giderek artmaktadır.

6.5. Fiziksel Sabotajcılar

Bir bilişim sistemine zarar vermek isteyen, saldırıyı teknolojik yollarla yapamayan ve sisteme fiziksel olarak yakınlığı bulunan kötü niyetli kişilere fiziksel sabotajcılar denilmektedir. Bu kişilerin saldırıları, bağlantıyı koparma amaçlı ileti yollarına zarar verme, sinyal alıcı ve vericilere engel olma gibi eylemlerin yanı sıra hard disk, yedekleme üniteleri gibi verilerin saklandığı ortamlara karşı düzenlenmektedir.

Bu türlü saldırıların olma ihtimali düşünülerek kurumlar tarafından B planları oluşturulmamış ise bilişim hizmetleri kesintileri uzun süreli yaşanabilmektedir. Bu nedenle kurumlar her türlü fiziksel sabotajı göz önünde bulundurarak hemen devreye koyabilecekleri ikinci bir sistemi hazırda bulundurmalıdırlar.

ÜÇÜNCÜ BÖLÜM

KURUM VE KURULUŞLARDA BİLGİ VE İLETİŞİM GÜVENLİĞİ İÇİN ALINAN ÖNEMLER VE UYGULANAN POLİTİKALAR

Bilgi ve iletişim güvenliği denince salt polisiye tedbirlerle erişimin denetlenmesi ve bilginin üçüncü şahıslara karşı korunması da algılanmamalıdır. Bilgi kaybının önlenebilmesi, kurum bilgi işlem merkezinin yangın, deprem gibi herhangi bir afet ile kullanılmaz hale gelmesi durumunda da hizmetin devam edebilmesi, bilgi işlem yöneticisinin çözmesi gereken karşılaşma olasılığı yüksek en önemli sorunlardan biridir.

Günümüz dünyasında kişiler, kurumlar ve hatta ülkeler için özellikle parasal değeri olan veya menfaat sağlanabilecek her türlü kıymetli bilginin dost olmayan kişi, kurum veya ülkelerin eline geçmesi son derece tehlikeli olabilir. Sırf bu yasal olmayan müdahaleler için eğitilmiş ve ayrılmış kaynakların bulunması ve kişi veya kurumların planlarını ellerine geçirdikleri bu bilgileri üstünlük sağlayacak şekilde kullanabilmeleri ağ güvenliğinin ve sonuçta ortaya çıkan bilgi ve kişisel hakların korunmasının, ne kadar önemli olduğunu ortaya koymak için yeterlidir.

Kişisel bilgilerimiz ve çalıştığımız kurumun sahip olduğu bilgilerin etkileşimli bilgisayar ağları ortamında kullanıma açılması değişik riskleri de beraberinde getirmektedir. Bu bilgilerin erişim yetkisi olan kişi veya kişilerin kullanımına açılırken yetkisiz ve kötü niyetli kişilerin müdahalelerinden de korunması gerekmektedir. Bu amaçla politikaların oluşturulması ve güvenlik için gerekli donanımların ve yazılımların kurulması bilgi işlem merkezi yöneticilerinin önderliğinde tüm kurum yönetimi ve çalışanlarının katkılarıyla gerçekleştirilmelidir. Aksi takdirde gerekli bilgi paylaşımı ve transferi güvenliğine sahip olmayan bir ağ ile veri tabanını internet ortamına açmak,

davetsiz misafirleri kolayca içeriye buyur edecek ve kurumumuz için hayati bilgilerin ilgisiz ve yetkisiz kişilerin eline geçmesini sağlayacaktır.

Bu süreçte standartların da önemi büyüktür. Tüm kurumların ortak gereksinimlerine yanıt verecek ve temel güvenlik önlemlerini eksik bırakmayacak şekilde tasarlanmış standart uygulamalar gerek riskleri gerekse sorumlulukları azaltacaktır. Aynı şekilde bilgi teknolojileri dünyasında benimsenmiş olan kriterlerin kurumların alım kararlarında da değerlendirilmesi sağlıklı bir seçim için yön gösterici olacaktır.

7. KURUM VE KURULUŞLARDA BİLGİ VE İLETİŞİM GÜVENLİĞİ

Bilgiye sürekli erişimin sağlandığı bir ortamda, mesajın göndericisinden alıcısına kadar gizlilik içerisinde bozulmadan, değişikliği uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi ve iletişim güvenliği olarak tanımlanabilir. Kurum ve kuruluşlarda ise bilgi ve iletişim güvenliği, bilgi varlıklarının tespit edilerek zafiyetlerin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizleri yapılarak önlemlerin alınması ile sağlanabilir.

Kamu kurum ve kuruluşları gerek işleri hızlandırma ve bürokrasiyi azaltma gerekse teknoloji maliyetinin insan gücü maliyetinden daha düşük olması gibi gerekçelerle süratle yeni ortama uyum sağlamaktadırlar. İşte bu bağlamda bilgi ve iletişim güvenliği büyük önem kazanmaktadır.

Bir kurumda bilgi güvenliğini etkin bir şekilde sağlamak amacıyla çeşitli kurallar ve metotlar uygulanabilir. Bu kural ve metotlar kurumun tehdit ve açıklarını analiz ederek risklerinin farkına varmasından teknik güvenlik çözümlerini sisteme entegre etmesine sözleşmelerde bilgi güvenliğini de ele

alan düzenlemeler yapmasından, kullanıcıların bilgi güvenliği farkındalığını arttırmaya kadar çok çeşitli alanlarda uygulanabilir (Öztürk, 2008: 5).

Kurumsal bilgi güvenliğinin sağlanmasının önemli gerekçeleri ana hatlarıyla aşağıda belirtilmektedir (Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı):

- Güvenlikle ilgili tehdit ve risklerin belirlenerek etkin bir risk yönetiminin sağlanması ve kurumsal itibarın korunması,
- İş sürekliliğinin sağlanması,
- Bilgi kaynaklarına erişimin denetlenmesi,
- Personelin, yüklenicilerin ve alt yüklenicilerin güvenlik konusunda bilinç düzeyinin yükseltilmesi ve önemli güvenlik konularında bilgilendirilmesi,
- Bilgi varlıklarının gizliliğinin bütünlülüğün ve doğruluğunun sağlanması,
- Kurumsal bilgi varlıklarının kötü amaçlı olarak kullanma ve/veya suiistimal edilmesinin engellenmesi,
- Bilgilerin güvenli bir şekilde üçüncü taraflara ve denetçilere açık olmasının sağlanması,
- Bilgi sistemlerini kullanan kişilerin umursamazlığından, planlanmış taciz, bilinçsiz kullanım veya bilmeden yanlışlıkla suiistimal etme gibi nedenlerden dolayı oluşabilecek donanım, yazılım ya da bilgisayar ağlarında meydana gelebilecek arızalara karşı korunması.

Kurum ve kuruluşlarda güvenlik için fiziksel ve sanal bazı katmanlar üzerinde önlemler alınmaktadır. Bu bölümde Türkiye Bilişim Derneğinin yayınladığı Bilişim Sistemleri Güvenliği El Kitabından istifade edilerek ağ, sunucu, internet ortamı ve personel bilgisayarlarında alınan güvenlik tedbirlerinden bahsedilecektir.

7.1. Ağ Güvenliği

Kurumlarda bilgisayar, yazıcı, tarayıcı, sunucu gibi birden fazla cihazın arasında kanallar oluşturarak iletişimin sağlandığı yapıya kurum ağı denilmektedir. Kurum ağları çalışma organizasyonu ve koordinasyon açısından büyük fayda sağlamaktadır. Bu şekilde oluşturulan ağlar genel olarak yerel ağ olarak adlandırılmaktadır. Bir yerel ağını oluşturan cihazlar kablolu veya kablosuz olarak birbirleriyle iletişim kurabilirler.

Günümüzde kurumlar için yerel ağ kavramı artık, iç ve dış ağ ayrımı yapılmaksızın, kurumdaki herhangi bir kişiye, herhangi bir yerden erişebilmek anlamında genişlemiştir. Ama bu genişlemeye paralel olarak, güvenlik uzmanları da ağlarına karşı olan tehditlerle başa çıkabilmek için daha komplike güvenlik politikaları uygulamak zorunda kalmaktadırlar. Bu tehditlere karşı alınabilecek çözümlerin başında önemli ağ kaynaklarını internetten veya yerel ağdan gelebilecek saldırılardan korunması gelmektedir.

Ağ yöneticilerinin en önemli görevlerinden biri ağ geçitleri üzerinden iç sistemlere yapılması muhtemel saldırıları önceden kestirmek ve buna yönelik tedbirleri almaktır. FBI tarafından yapılan araştırmalara göre 2001 yılında dünya üzerinde güvenlik açıkları nedeniyle gerçekleşen maddi kayıp 15 milyar dolar civarındadır. Araştırmacılar bu rakamın 2002 yılında 1.5 kat arttığını belirtmektedirler. Bu açıdan bakıldığında ağa saldırıların dış kaynaklı olması ihtimali yüksek görünse de dünya üzerinde kayıtlı vakalara göre büyük çoğunluğu içeriden yetkisiz erişimlerle gerçekleştirilmektedir. San Francisco'daki Computer Security Institute tarafından yapılan bir araştırmaya göre %60-80'i içerideki kullanıcıların yanlış yöneliminden kaynaklanmaktadır. O halde ağ tasarlanırken dışarıdan gelen saldırıları içeri girmeyi engelleyecek, içerideki kullanıcıların da yetkileri dışında erişimlerini kısıtlayacak bir mekanizma göz önüne alınmalıdır (Tağmaç, 2003: 44).

Ağ güvenliğini sağlayabilmek için Güvenlik Duvarları (Firewall), Saldırı tespit Sistemleri (IDS) ve Rol Tabanlı Erişim Kontrolleri (RBAC) kullanılabilir (Bilişim Sistemleri Güvenliği El Kitabı). Ağ üzerinden erişim kontrolü, mevcut ağ kaynaklarını korumak için en temel yoldur. Ölçeklenebilir kapsamlı erişim denetimi kuralları sayesinde, ağ güvenliği yöneticileri ağ bağlantıları için kaynak sistem, hedef sistem, ağ trafik türü ve uygulama zamanını belirlemek suretiyle esnek ağ erişim hakları belirleyebilirler.

Komple bir ağ güvenliği çözümü üretmek için erişim kontrollü koruma tedbirleri tek başına yeterli değildir. Komple bir ağ güvenliği çözümü için aşağıdaki maddeler sağlanmalıdır.

- Ağ kullanıcılarının kimliklerinin belirlenmesi,
- Aktarım esnasında veriyi şifreleme,
- Cihazlara verilen IP numaralarını optimize kullanma,
- Ağ trafiğinin tümünün içeriğine güvenlik politikasını uygulama,
- Yapılan saldırıları gerçek zamanlı olarak belirleme ve önlem alma,
- Denetim bilgilerinin tümünün kayıtlarını tutma(Loglama İşlemleri).

Güvenilir ve performanslı bir ağ kurmak için hem ağ içi haberleşmede hem de ağın dış dünya ile haberleşmesinde trafik yoğunluğunun artması, içerden ve dışarıdan yetkisiz erişim veya önemli bir verinin saklanması gibi durumlarda hiçbir zafiyet oluşturmadan ağ güvenliğini sağlayan güçlü bir sistem kurmak gerekir. Bu sistem hem kullanılan ağ cihazlarının hem de bu cihazlar üzerinde çalışan uygulama programlarının iyi bir konfigürasyonla seçilmesi ve çalışmasının devamı ile mümkündür.

7.2. Kablosuz Ağ Güvenliği

Kablosuz iletişim; kablosuz iletişim sağlayan modemler, erişim noktaları ve bilgisayarlarda bulunan Ethernet kartları sayesinde gerçekleşir. Data paketleri hava yoluyla dalgasal sinyaller halinde kablosuz cihazlar arasında iletilir. Verilerin kablo içinde elektriksel olarak değil, güvensiz bir ortamda iletilmek istenmesi beraberinde ciddi güvenlik sorunlarını getirmiştir. Çünkü bilgiler korumasız biçimde saldırılara açık haldedir.

Kablosuz ağ güvenliğini sağlamak için üç temel maddenin üzerinde durmak gerekir:

1- Kullanıcı doğrulaması; yetkisiz kişilerin erişim noktalarını kullanarak veri gönderip almasını engellemek amacıyla yapılır. Kullanıcı doğrulama için Erişim Noktaları; Servis Kurulum Kimliği Doğrulaması (SKKD) ve MAC Adres Filtreleme veya Anahtar Doğrulaması gibi yöntemlerden birini veya bir kaçını kullanırlar.

SKKD temel olarak alfanumerik karakterlerden oluşan bir isimdir. Kablosuz ağı bir veya birden fazla erişim noktasının servis verdiği segmentlere bölmeye yarar. Aynı segmentte yer alan kablosuz istemcilere o segmentteki erişim noktasının ismi girilir. Bir istemci birden fazla erişim noktasından hizmet alacaksa bu erişim noktalarının isimleriyle konfigüre edilir. Kablosuz bir istemcinin bir erişim noktasından servis almak için doğru servis ismini sunması gerektiğinden, SKKD basit bir şifrenin sağladığı ölçüde erişim kontrolü sağlar.

MAC adresi istemcilerin kablosuz ağ kartlarının sahip oldukları adreslerdir. Yani erişim noktalarından servis talep ederken MAC adresleriyle başvururlar. Bu noktadan yola çıkılarak bir erişim noktasına erişebilecek istemcilerin ağ kartlarının MAC adreslerinin listesi erişim noktasına girilip bunlar dışındaki istemcilerin kablosuz ağa dahil olmaları engellenerek de kullanıcı doğrulaması sağlanabilir. MAC adres filtrelemesi olarak bilinen bu

yöntemin dezavantajı her erişim noktası için ayrı ayrı elle girilen MAC adresi listelerini güncel tutmanın zorluğu ve girilebilecek adres sayısının sınırlı olmasıdır. Ayrıca bazı yazılımlar aracılığıyla bir ağ kartının adresi değiştirilebildiğinden ağa erişim hakkı bulunan bir kartın adresinin çalınması durumunda yetkisiz kişiler doğrudan ağa erişebileceğinden bu yöntem tek başına yeterli bir kullanıcı doğrulama mekanizması değildir.

Diğer bir yöntem olan Anahtar Doğrulaması ise istemcinin daha önce erişim noktasına girilmiş olan gizli bir anahtara sahip olması temeline dayanmaktadır.Erişim noktasına istemcinin gönderdiği mesaj yanlış anahtarla şifrelenmiş veya hiç şifrelenmemişse istemci ağa dahil edilmez. Bu yöntemin dezavantajı ise şifreleme anahtarının statik olması yani, önceden elle erişim noktasına ve istemciye girilmesin gerekmesi ve sonradan da otomatik olarak değiştirilememesidir.

2- Verinin gizliliği sağlanmalıdır. Yani kablosuz ağlarda verilere üçüncü kişiler tarafından erişilse bile içeriğinin anlaşılmamasının yolu veririnin şifrelemesidir. Bu şifrelemeyi sağlayan standartlar mevcuttur. Bu standartlardan başlıca olanları WPA, WEP, WEP2 dir.

3- Mesaj bütünlüğü olmalıdır. Veriler havadaki sinyaller yoluyla iletildiği için kesintiye uğrama riski taşımaktadır. Bu nedenle mesajlar iletilirken bir bütünlük taşmalıdır. Kesinti bile olsa tekrar bağlantı sağlandığında iletiler bütünlük içinde kaldığı yerden devam edebilmelidir.

Kablosuz ağ kullanan kurumlar alınan bütün önlemlere rağmen zaaf olacağı için kablosuz ağlarını yerel ağlarından ve veri tabanlarından izole edecek şekilde kurmaları daha güvenli olacaktır.

7.3. Sunucu Güvenliği

Sunucular bir kurumda işleyişle ilgili gereksinimlere cevap veren gelişmiş bilgisayarlardır. Sunucular kullanıcılarına çalışma nedenlerine göre bilişim hizmetleri sunarlar. Sunucular farklı türlerde olabilir:

- İnternet erişim sunucusu; kurum bilgisayarlarının kontrollü bir şekilde üzerinden internete çıkarıldığı bilgisayardır. Bu sunucuyu kullanan kurumlarda, kullanıcı bilgisayarlarının ağ ayarlarına, internete erişebilmek için varsayılan ağ geçidine internet erişim sunucusunun ip numarası girilmelidir.
- E-posta sunucuları; varsa kuruma ait elektronik posta hizmetlerini sağlayan bilgisayarlardır. Bu sunucular sayesinde kurum personeli kendilerine, kuruma ait uzantıya sahip e-posta hesapları oluşturabilir, hesaplarına gelen postaları okuyabilir ve gönderimde bulunabilir.
- Veri tabanı sunucuları; kuruma ait tüm verilerin bulunduğu sunuculardır. Korunmasına azami derecede önem verilmelidir. Otomasyonlar ve yazılımlar sayesinde girilen veriler bu sunucu üzerinde depolanır. Bu sunuculara yetkilerine göre kullanıcılara erişim hakları verilir. Veriler üzerinde okuma, değişiklik yapabilme, ekleyebilme veya veriyi silebilme gibi yetkiler kullanıcı bazında işaretlenir.
- Web ve Uygulama Sunucuları; kurumda çalışan yazılımların ve internet sitesinin üzerinde bulunduğu bilgisayarlardır. Bu sunucular aracılığıyla kurum bilgileri web ortamına taşınabilir, yazılımların yayımlanması sayesinde ise kurum personellerinin kurum işleyişinin bilgisayarlar üzerinden yürütülmesini sağlarlar.
- Bu sunucular dışında dosya paylaşımını sağlayan FTP sunucuları, tüm ağ trafiğine ait hareket kayıtlarını tutan loglama sunucuları, ip dağıtan DHCP sunucuları, bilgisayarların internete çıkışında isim sağlayan DNS

sunucuları, kullanıcı bilgisayarları virüs ve türevlerinden koruyan Anti-virüs sunucuları gibi sunucular kurum ağlarında bulunabilen diğer türlerdendir.

Kurum ağını dışarıdan gelen saldırılara karşı güvenli hale getirmek için iyi tasarlanmış bir çevre ağının varlığı önemlidir. Böyle bir ağ aynı zamanda iç ağın diğer ağlara karşı saldırılarda kullanılmasını önlemeye de yarar. En yaygın kullanılan çevre ağ öğesi güvenlik duvarıdır.

Çevre ağ yapısında sunucular DMZ (Silahsızlandırılmış Bölge) adı verilen ikinci bir ağ yapısında bulundurularak güvenlik duvarı sayesinde extra güvenlik ilkeleri sağlanarak korunur.

Kurum ağının sunucuları çoğu zaman fiziksel olarak farklı yerlerde bulunduğundan sistem yöneticisi tarafından uzaktan erişimle konfigüre edilirler. Uzaktan erişim işlemi de güvenlik açısından zayıf bir noktadır ve güçlendirilmelidir. Bunun için telnet, rlogin, rsh uygulamaları yerine, açık anahtar yapısı ile yüksek güvenlik sağlayan ssh uygulamaları tercih edilmelidir.

Kurumdaki kullanıcıların çeşitli hizmetlere erişmek için kullandıkları kimlik ve parola bilgilerini bir yerde tutmak, hep aynı kimlik doğrulama mekanizmasını kullanmak, hem kullanım kolaylığı hem de takip açısından tercih edilmesi gereken bir seçenektir. Diğer yandan merkezi bir yapı, saldırıları tek bir noktaya odaklatacağından bu sunucunun yüksek güvenlikli olmasını gerektirir. Erişimlerin merkezi kontrolü için tercih edilebilecek bir uygulama LDAP (Lightweight Directory Access Protocol)'dur. Açık kaynak sürümleri de yaygın olarak kullanılan LDAP aynı zamanda kullanıcı bilgilerinin kurum içinde kolayca paylaşımı için de kullanılır.

Veri tabanlarına yönelik tehditler sunucunun ele geçirilmesi, veri hırsızlığı, verilerin değiştirilmesi ve geciktirme saldırıları olarak özetlenebilir.

Veritabanına yönelik saldırılar kurum dışından olacağı gibi, verilerin bir kısmına erişim hakkı bulunan kurum içi kullanıcıların erişim hakkına sahip olmadıkları veriye ulaşmaları şeklinde de olabilir. Böyle bir yapı veri tabanın sunucusunun profillerine ve rollerine göre konfigüre edilmesini gerektirir.

İnternet üzerinden posta gönderme hizmetini sağlayan e-posta sunucularının güvenliğinin sağlanması için: Anti-spam, mesaj filtreleme ve pgp veri şifreleme algoritmaları gibi önlemler; e-posta hizmetlerine yönelik olan tehditlerden postanın yolda okunması, e-posta kutularının mesaj bombardımanına tutulması, sahte postaların oluşuturulup gerçek alıcılara gönderilmesi, spam virüslern yayılması, e-posta sunucusunun ele geçirilip başka saldırılar için kullanılması gibi tehlikelere karşın tedbirlerin alınması gerekir.

Her ne kadar güvenlik duvarı gibi önlemlerle kurum ağı dışarıya karşı korunsa da, tüm bu duvarlar kurumun diğer hizmetlerine entegre olarak çalıştığından, web sunucusunun zayıflığı doğrudan kurum sistem yapısının zayıflığı olarak ortaya çıkar. Web sunucusu saldırıları, sunucuyu çökertmekten, şifrelerin eline geçirilmesine kadar geniş bir spektrumu kapsar. Güvenli bir web hizmeti için güvenli yazlım esaslarına göre tasarlanmış ve kodlanmış bir web sunucusuna gereksinim vardır. Bununla birlikte dinamik içerikli web hizmetlerinin kurum içi hizmetlerle entegrasyonu güvenlik gerekleri göz önünde bulundurularak yapılmalı, ancak gerekli minimum hizmet web servisine entegre edilmelidir. Son olarak da sunucunun savunma mekanizması zayıflık test eden uygulamalarla test edilmelidir.

Dosya paylaşımı için kullanılan dosya sunucularına erişim de güvenli yollarla yapılmalı, şifrelerin açık gönderildiği FTP gibi protokoller yerine sftp, scp protokolleri gibi güvenli protokoller seçilmelidir.

7.4. Internet Güvenliği

Kurumlarda, hızla gelişen haberleşme teknolojisiyle ilgili yenilikleri takip etmek, güncel veriyi daha pratik yollarla elde ederek verimliliği artırmak amacıyla personelin bilgi iletişimini internet üzerinden sağlanması vazgeçilmez bir unsur haline gelmiştir.

Başlangıcında yalnızca akademik amaçlı bir araştırma ağı olan Internet, bugün gelinen noktada önemli toplumsal dönüşümlere altyapı sağlar duruma gelmiştir. Ancak ilk yıllarda lüzumsuz ya da önemsiz olarak nitelendirilebilen güvenlik konusu, Internet'e bağlı kurum sayısı arttıkça ciddi bir problem haline gelmiştir. Internet'in temeli oluşturan protokollerin büyük bölümünün güvenliğe pek az önem verilerek tasarlanmış olması bu yaklaşımı doğrular niteliktedir. Internet'in ilk yıllarından itibaren önemsiz sayılan güvenlik konusu, özellikle 1988 yılındaki Morris Kurdu faciası ile dikkatleri üzerine çekmiştir. Kurt, başarılı biçimde binlerce bilgisayara sızmayı başarmış ve bu bilgisayar sistemlerini çalışmaz hale getirmiştir (Pasin, 2002: 1).

Kurumlar, çalışanlarına araştırma, kendilerin geliştirme ve yeniliklerden haberdar olma amacıyla İnternet'e çıkma olanağı tanımaktadır. Internet, bilgiye erişmenin ve araştırma yapmanın en hızlı, en kolay, en güncel yoludur. Fakat korumasız bir ağ olduğu için her türlü saldırılara açıktır ve mutlaka güvenliğinin sağlaması gerekmektedir.

Web sitelerinin kullanımının yaygınlaşmasıyla birlikte dolayı bu sitelere yapılan saldırılar en yaygın saldırı biçimlerinden biri olmuştur. Özellikle Web sitesini kıran saldırganlar bu siteye bağlanan kişileri kolaylıkla kendilerine yönlendirebilir ve kişilerin bilgilerini ele geçirebilirler. Web sitesinin gerçekte bağlanılan Web sitesi olduğundan emin olunması gerekmektedir. Dolayısıyla, Web sitelerinin ve bu sitelere bağlanan kişilerin kimliklerini ispat edebilmeleri ve güvenli olarak birbirleriyle iletişim kurabilmeleri için elektronik kimlik

belgelerine ihtiyaçları vardır. Elektronik kimlik (E-kimlik) belgeleri, kişilerin, kurumların ve Web sunucularının internet üzerinde kimliklerini ispatlamak için kullandıkları elektronik dosyalardır. Temeli çift anahtarlı kriptografi teknolojisine dayanan bu belgeler, sahiplerine ait kimlik bilgilerinin yanısıra sahiplerinin elektronik açık anahtar bilgisini de içermektedir. Bu açık anahtar bilgisinin belirtilen kişi, kurum ya da Web sunucusuna ait olduğunu garanti etmektedirler.

Bilgi İşlem Merkezleri için veri ve sistemlerinin güvenliğini sağlamak kadar yedekleme sistemlerini kurmakta çok büyük önem taşımaktadır. Temel olarak bilgi kayıplarının dört ana sebebi vardır. Bunlar donanım arızaları, yazılım hataları, insandan kaynaklanan olaylar (sabotaj, saldırı) ve doğal afetler (deprem, sel)'dir. Bu sebeplerden dolayı oluşabilecek bilgi kayıplarını en alt düzeye indirmenin ve sistemin devamını sağlamanın yolu yedekleme sistemleri kurmaktır. Bilgilerin kopyalarının çeşitli ortamlarda tutulması sistemin ya da herhangi bir kopyanın bozulması durumunda geri dönüş için çok önemlidir. Düzenli olarak yedek almak ve yedeklerin çalıştığından emin olmak iyi bir yedekleme için mutlaka olmak zorundadır. Yedekleme Sistemlerindeki en önemli kararlardan bir tanesi de güvenilir, hızlı, kullanılabilir ve güncel bir sistemin kurulmasıdır. Dolayısıyla yedeklenmiş bir bilgi herhangi bir bozulma olmadan yıllarca saklanabilmelidir. Yapılan işi aksatacak bir olayla her zaman karşılaşılabilir ve her an bir yedeğe ihtiyaç duyulabilir. Bu nedenle karşılaşılabilecek herhangi bir soruna önceden hazırlıklı olmak ve önlemini almak gerekmektedir.

7.5. Kişisel Bilgisayar Güvenliği

Kuruma ait tüm bilgisayar kullanıcıları kendi verilerinin ve iletişimin güvenliğini almakla yükümlüdürler. Yönetimin ve bilgi işlem biriminin aldığı tedbirlerin yanında kurum personeli de; giriş şifreleri oluşturmak, kişisel

güvenlik duvarı kullanmak, virüslere karşı kullanımla ilgili dikkati göstermek gibi sorumlulukları da yerine getirmelidirler.

Kurumsal ortamlarda bilgisayar sisteminin düzgün çalışabilmesi, potansiyel sorunlara karşı korunması, meydana gelebilecek olaylarda en kısa zamanda ve en az kayıpla ayağa kalkılabilmesi için alınması gereken önlemleri, virüslere karşı alınacak önlemler ile birlikte düşünmek gerekmektedir.

Virüslere karşı en genel koruma yöntemi anti-virüs programlarının kullanılmasıdır. Anti-virüsler, virüslere karşı korunmada oldukça etkilidirler ama hiçbir zaman %100 koruma sağlayamazlar. Virüsün özellikleri, anti-virüs programının özellikleri, güncelleme sıklığı, düzenli ve gerektiğinde virüs taramasının yapılması gibi birçok faktör virüsten korunmayı etkiler. Yani, virüslere karşı korunmada hiçbir zaman sadece anti-virüs ile korunma yeterlidir diye düşünülmemelidir.

Bilgisayar güvenliğinin sağlanması için akıllı kart ve akıllı anahtar gibi karmaşık ve pahalı çözümler kullanılabilir. Bu çözümlerin yanı sıra her kullanıcının rahatlıkla uygulayabileceği çözümler de mevcuttur. Örneğin, bilgisayarlara açılış şifresi koymak ve bu şifreyi gerekli durumların dışında başkaları ile paylaşmamak alınması gereken önlemlerden birisidir. Aynı zamanda şifreli ekran koruyucuları kullanılmalı ve bu ekran koruyucularının devreye giriş süreleri uygun bir şekilde ayarlanmalıdır.

Kişisel bilgisayarlarda yedekleme işlemi de çok önemlidir. Kullanıcılar hiç ummadıkları anlarda sistemlerinin çökmesi ve diğer nedenlerle bilgilerini kaybetme riskiyle karşı karşıya kalmaktadırlar. Bu nedenle kurum çalışanları önemli belgelerini belirli periyotlarda düzenli olarak yedeklemelidirler. Yedeklerine ihtiyaç duyulan zamanda kolayca ulaşabilmeleri için tarihli bir şekilde tasnif ederek kaydetmelidirler. Verilerini bilgisayarlarının güvenli bir

sürücüsünün dışında ayrıca harici bir belleğe de kopyalarının oluşturulması daha faydalı olacaktır.

8. KURUM VE KURULUŞLARDA BİGİ VE İLETİŞİM GÜVENLİĞİNE YÖNELİK UYGULANAN POLİTİKALAR

Kurumsal bilgi ve iletişim güvenliği politikası, kurum ve kuruluşlarda bilgi ve iletişim güvenliğinin sağlanması için tüm güvenlik faaliyetlerini kapsayan ve yönlendiren talimatlar olup kurumsal bilgi kaynaklarına erişim yetkisi olan tüm çalışanların uyması gereken kuralları içeren belgelerdir. Bilgi ve iletişim güvenliği politikaları her kuruluş için farklılık gösterse de genellikle çalışanın bilgi ve belgenin gönderilmesi ve saklanmasındaki sorumluluklarını, güvenlik denetim araçlarını, amaç ve hedeflerini kurumsal bilgi varlıklarının yönetimini, korunmasını dağıtımını ve önemli işlevlerin korunmasını düzenleyen kurallar ve uygulamaların açıklandığı genel ifadeleri içermektedir.

Güvenlik politikaları kurum ve kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür (Kalman, 2003: 36).

Bilgi güvenliği politikaları, bir kurumun değerli bilgilerinin yönetimini, korunmasını, dağıtımını ve önemli işlevlerinin korunmasını düzenleyen kurallar ve uygulamalar bütünüdür (Tuğlular, 2003: 1).

Kurumsal bilgi ve iletişim güvenlik politikaları kuruşların ihtiyaçları doğrultusunda temel güvenlik ilkelerinin (gizlilik, bütünlük ve erişilebilirlik) bazıları üzerinde yoğunlaşabilir. Örneğin askeri kurumlarda bilgi ve iletişim güvenlik politikalarında genellikle gizlilik ve bütünlük ihlalinin engellenmesi amaçlanmaktadır. Erişebilirlik de önemlidir ancak birinci planda gizlilik ve bütünlük gelmektedir. Askeri bir savaş uçağının kalkış zaman bilgilerinin onaylanıp yürürlüğe girmesi için düşmanlar tarafından görülmemesi (gizlilik)

ve değiştirilmemesi (bütünlük) gereklidir. Bir diğer örnek ise kar amacı gütmeyen işletmelerde uygulanan bilgi ve iletişim güvenliği politikalarında genellikle erişebilirlik ve bütünlük ihlalinin engellenmesi amaçlanmaktadır. Gizlilik unsuru da önemlidir ancak birinci planda erişebilirlik ve bütünlük önemlidir. Üniversite sınavının açıklandığı yüksek öğretim kuruluşunda uygulanan güvenlik politikasında öğrencileri sınav açıklandıktan sonra istediği zaman diliminde (erişebilirlik), doğru bir şekilde (bütünlük) sınav sonuçlarına bakabilmelidirler.

İyi bir güvenlik politikası, kullanıcıların işini zorlaştırmamalı, kullanıcılar arasında tepkiye yol açmamalı, kullanıcılar tarafından uygulanabilir olmalıdır. Politika, kullanıcıların ve sistem yöneticilerinin eldeki imkanlarla uyabilecekleri ve uygulayabilecekleri yeterli düzeyde yaptırım gücüne sahip kurallardan oluşmalıdır. Alınan güvenlik önlemleri ve politikayı uygulayan yetkililer veya birimler yaptırımları uygulayabilecek idari ve teknik yetkilerle donatılmalıdır. Politika kapsamında herkesin sorumluluk ve yetkileri tanımlanarak kullanıcılar, sistem yöneticileri ve diğer kişilerin sisteme ilişkin sorumlulukları, yetkileri kuşku ve çelişkilere yer bırakmayacak biçimde açıkça tanımlanmalıdır. Politikalar içerisinde uygulanacak olan yasal ve ahlaki mahremiyet koşulları ile elektronik mesajların ve dosyaların içeriğine ulaşım, kullanıcı hareketlerinin kayıt edilmesi gibi denetim ve izlemeye yönelik işlemlerin hangi koşullarda yapılacağı ve bu işlemler yapılırken kullanıcının kişisel haklarının nasıl korunacağı açıklanmalıdır. Gerekli durumlarda istisnalar ve alternatif uygulamalar açıklanmalıdır.

Saldırıların ve diğer sorunların tespitinde kullanıcıların, yöneticilerin ve teknik personelin sorumluluk ve görevleri ile tespit edilen sorun ve saldırıların hangi kanallarla kimlere ne kadar zamanda rapor edileceği güvenlik politikalarında açıkça belirtilmelidir. Sistemlerin gün içi çalışma takvimleri,veri kaybı durumunda verinin geri getirilmesi koşulları gibi kullanıcının sisteme

erişmesini sınırlayan durumlara politikalar içerisinde yer verilmelidir.Bu durumlarda kullanıcıya, izlenmesi gereken yolu anlatacak ve yardımcı olacak kılavuzlara da yer verilmelidir.

Bu bölümde Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(UEKAE) tarafından oluşturulan Bilgi Yönetim Sistemlerinde Risk Yönetim Süreci Kılavuzundan istifade edilerek; kurumlarda uygulanan bilgi ve iletişim güvenliği politikalarını, risk analizleri, seminer ve eğitim çalışmaları, gerekli yazılım ve donanımın sağlanması, güvenlik yapısının oluşturulması ve kayıt tutulması gibi başlıklar altında incelenip değerlendirilmektedir.

8.1. Risklerin ve Oluşabilecek Etkilerinin Belirlenmesi

Kurumun bilgi ve iletişim güvenliği bakımından oluşabilecek tehditleri önceden kestirebilmesi, işleyişin ve verimliliğin zarara uğramaması için bir takım analizlere ihtiyacı vardır. Hangi bilgi varlıklarının korunacağı, kurumun iletişim kanallarının saldırılara ve dinlemelere karşı nasıl izole edileceği belirlendikten sonra, oluşabilecek istenmeyen durumlara karşı nasıl bir yol izleneceği risk yönetimi sürecinde ele alınmalıdır. Risk yönetimi sürecinde öncelikle iyi bir analiz yapılması gerekir.

Risk analizinin ilk adımı kapsam belirlenmesidir. Kapsamın ilk aşamada doğru kurum hedeflerine uygun olarak belirlenmesi ileride gereksiz çaba harcanmasını önler ve risk analizinin kalitesini arttırır. Kapsamda risk analizine tabi her şey açık olarak belirtilmelidir. Örneğin risk analizinde dikkate alınacak bütün bilişim teknolojisi varlıkları (yazılım, donanım gibi), personel, tesisler, operasyonlar açıkça belirtilmelidir. Örnek bir kapsam şu şekilde olabilir. “Bu risk analizi kurumun muhasebe işlemlerinde kullanılan tüm donanım, yazılım ve personeli kapsar.” Bu durumda muhasebe işlemleri için kullanılan tüm sunucular, kullanıcı bilgisayarları, işletim sistemleri, veri tabanı yazılımları,

uygulamalar ve tüm bunları kullanan ve yöneten kurum personeli risk analizi içinde yer alır.

Diğer bir adım, varlık belirlemesidir. Varlık sistemin bir parçası ve kurum için değerli olan her şeydir. Varlık kurum için değerli olduğundan her şeydir. Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nün 2007 yılında çıkardığı Risk Yönetim Süreci Kılavuzu'na göre aşağıdaki örnekler varlık olarak nitelendirilebilecek değerlerdir.

- Bilgi,
- Donanım,
- Yazılım,
- Haberleşme cihazları,
- Dokümanlar,
- Üretilen mallar,
- Servisler (hizmetler),
- Mali Değerler,
- Personel,
- Kurumun prestiji veya imajı.

Bütün bu varlıklar aynı zamanda bir kurumun eksik kaldığı takdirde, işleyiş, verimlilik veya büyüme bakımından ihtiyaç duyacağı argümanlardır. Bu varlıklar belirlenirken anketlerden, birebir görüşmelerden, incelenen dokümanlardan ve otomatik tarama araçlarından istifade edilebilinir.

Bir başka analiz adımı da tehditlerin belirlenmesidir. Tehdit herhangi bir kaynağın kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. Tehditler deprem, su baskını gibi doğal veya elektrik kesintisi, sızıntılar gibi çevresel olabileceği gibi bilinçli veya bilinçsiz şekilde yapılan insan kaynaklı da olabilmektedir.

Tablo 2. Açıklık Türleri ve Temel Sebepleri

Açıklık Türü	Temel Sebepler
Altyapı ve Çevreyle İlgili Açıklıklar	• Binada yeterli fiziksel güvenliğin olamaması • Girişlerde yetersiz fiziksel kontrol • Yıpranmış güç kaynakları • Depremde yıkılma riski taşıyan yapılar • Şifrelenmemiş / zayıf şifrelenmiş kablosuz ağlar
Donanımlarla İlgili Açıklıklar	• Periyodik yenilemenin yapılmaması • Voltaja değişiklerine, toza, neme, ısıya duyarlılık • Periyodik bakım eksikliği • Değişim yönetimi eksikliği
Yazılımlarla İlgili Açıklıklar	• Yama yönetimi eksikliği / yetersizliği • Kayıt yönetimi eksikliği / yetersizliği • Kimlik tanımlama ve doğrulama eksiklikleri • Şifre yönetimi yetersizliği • Şifre veritabanlarının korunamaması • Erişim izinlerinin yanlış verilmesi • İzinsiz yazılım yüklenmesi ve kullanılması • Saklama ortamlarının doğru silinmemesi • Dokümantasyon eksikliği/yetersizliği • Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi • Yazılımların yeterli test edilmemesi
Haberleşmeyle İlgili Açıklıklar	• Korunmayan haberleşme hatları • Hat üzerinden şifrelerin açık olarak iletilmesi • Telefon hatlarıyla kurum hatlarına erişim • Ağ yönetimi yetersizliği
Dokümanlarla İlgili Açıklıklar	• Dokümanların güvensiz saklanması • Dokümanların kontrolsüz çoğaltılması • Dokümanların imha edilmemesi
Personel İle İlgili Açıklıklar	• Eğitim eksikliği (Personel hataları) • Güvenlik farkında lığı eksikliği • Donanımların ve yazılımların yanlış kullanılması • İletişim ve mesajlaşma ortamlarının kullanımını düzenleyen politikanın eksikliği/yetersizliği • İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması

Kaynak: UEKAE- Risk Yönetim süreci Kılavuzu

Güvenlik açıkları; sistem prosedürlerinde, tasarımda, uygulamada veya iç kontrolde bulunan ve bilişim güvenliğini ihlal edebilecek zafiyet hata veya kusurlardır. Sistemdeki açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir.

Yukarıdaki tabloda belirtilen tehditlerin, açıklıkları gerçekleme olasılıklarını azaltacak veya ortadan kaldıracak kontrollerin hali hazırda uygulanıp uygulanmadığı veya bu kontrollerin uygulanmalarının planlanıp planlanmadığı incelenmelidir. Uygulanan veya uygulanması planlanan kontroller açıklıkların gerçekleşme olasılıklarını düşüreceği için olasılık değerlendirilmesinde ve dolayısıyla risk derecelendirilmesinde önem kazanacaktır.

Risk analizinde bir açıklıktan dolayı oluşabilecek tehlikelerin olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirilmesi yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi ve mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulur.

Tablo 3. Üç Seviyeli Bir Olasılık Değerlendirmesi

Olasılık Seviyesi	Olasılık Tanımı
Yüksek	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesini engelleyecek kontroller bulunmamaktadır veya etkisidir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçekleşmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçeklenmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

Kaynak: UEKAE- Risk Yönetim Süreci Kılavuzu

Olasılığın değerlendirilmesinden sonra risk derecelendirilmesi yapabilmek için etki analizi yapılmalıdır. Etki analizinde herhangi bir riskin gerçekleşmesi halinde yaşanacak olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde değerlendirilebilinir.

Tablo 4. Üç Seviyeli Bir Etki Değerlendirmesi

Etki Derecesi	Etki Tanımı
Yüksek	Açıklığın gerçeklenmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir. Kurumun çıkarları Misyonu ve prestiji büyük zarar görebilir veya etkilenebilir.
Orta	Açıklığın gerçeklenmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir.
Düşük	Açıklığın gerçeklenmesi durumunda: Kurumun bazı varlıkları etkilenir. Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

Kaynak: UEKAE- Risk Yönetim Süreci Kılavuzu

Etki analizi de yapıldıktan sonra artık muhtemel riskler derecelendirebilir durumdadır. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelerine göre yapılır. Risk bir tehdidin bir açıklığı gerçekleme olasılığının, açılığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonunudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır. Bu

fonksiyonuna bağlı olarak oluşan değerlere bağlı olarak risklere ait derecelere bir tanım koyulur ve o riske ait seviye belirlenerek olması sonucunda yapılaması gerekenler belirlenir. Derecelendirmenin tanımlanması kurum yönetiminin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir.

Tablo 5. Risk Dereceleri ve Tanımları

Risk Derecesi	Risk Açıklamasıve Yapılması Gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içerisinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önem alınıp alınmayacağı sistem sahibi veya sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

Kaynak: UEKAE- Risk Yönetim süreci Kılavuzu

Risk yönetiminde diğer bir aşama risk işleme aşamasıdır. Bu aşama risk ve etki analizinde belirlenen risklerin nasıl işleneceğine karar verilmesi, yapılacakların önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur. Risklerin tamamen ortadan kaldırılması için bütün kontrollerin yapılması çoğu zaman kurum için mali açıdan imkansızdır. Yönetim, riski azaltmak istediğinde sisteme gelebilecek zararı en aza indirmek için “en düşük maliyetli” ve “en uygun” kontrolü seçmekle sorumludur.

Risk yönetiminin son aşaması ve diğer aşamaları da kapsayan değerlendirme ve takip safhalarıdır. Risk yönetimi bir döngüdür ve burada belirlenen risk analizi ve risk işleme süreçleri periyodik olarak uygulanmalıdır. Bu sayede uygulanan kontrollerin amacına ne kadar ulaştığı belirlenmiş olur. Ayrıca bilişim teknolojileri çok hızlı değiştiği için kurum sistemine dahil olan varlıkların risk yönetimine dahil edilmesi önem arz etmektedir. Bunlara ek olarak zaman içerisinde kurumun iş hedefleri, iş yapma şekli ve önem verdiği konular değişebilir. Bütün bu değişiklikler varlıklarda, varlıkların değerlendirilmesinde, açıklıklarda ve tehditlerde değişiklik olmasına neden olur. Risk yönetim döngüsünün sürekli olarak işletilmesi tüm bu değişikliklerin getirdiği risklerin yönetim tarafından farkına varılmasını ve ele alınmasını sağlayacaktır.

8.2. Kişilere Sorumluluklarıyla İlgili Eğitim Verilmesi

Bilgi Güvenliği denetim raporları, makaleler veya konferans sunularında da ifade edildiği gibi güvenliğin sağlanması konusundaki en zayıf halka **insan**dır. Bilgi ve iletişim güvenliği uzmanlarının kanaati de bu yöndedir. İnsan faktörü uygun ve yeterli seviyede güvenliğin sağlanmasında anahtar roldedir. Bu sebeplerden ötürü kurum varlığı olan insan üzerinde daha büyük dikkatle durulması gerekmektedir. Bu bağlamda Kurumsal Bilgi ve İletişim Güvenliği Politikaları kapsamında her seviyedeki kurum çalışanının güvenlik konusundaki sorumluluklarını kavramasını sağlayacak bir bilinçlendirme sürecinin oluşturulması zorunludur.

Kurumsal Bilgi ve İletişim Güvenliği Eğitimi süreci (Önel, 2008: 5):

- Bilinçlendirme ve eğitim konularının seçilmesi
- Bilinçlendirme ve eğitim materyalleri için kaynak bulunması
- Farklı metotlar izleyerek eğitim materyallerinin hazırlanması

- Bilinçlendirme sürecinin etkinliğinin değerlendirilmesi
- Değişen teknoloji ve kurum öncelikleri konusunda güncel kalınması

gibi aşamalardan oluşabilmektedir.

Bir kurumdaki yöneticilerin, teknik personelin ve diğer çalışanların bilgi ve iletişim güvenliği konularındaki sorumluluklarıyla ilgili bilinçlenmeye ihtiyaçları vardır. Bilinçlendirme çalışmaları bir takım eğitim faaliyetleri, toplantılar ve seminerler içermelidir. Bahsi geçen tüm kurum bireylerinin:

- Kurumun misyonu doğrultusunda görev ve sorumluklarını anlamaları,
- Kurumun bilgi ve iletişim politikası, prosedür ve uygulamalarını anlamaları,
- Sorumlu oldukları bilişim kaynaklarını korumaya yönelik yönetimsel, operasyonel ve teknik açıdan gerekli asgari bilgi seviyesine sahip olmaları gerekmektedir.

Başarılı ve etkin bir bilgi ve iletişim güvenliği bilinçlendirme süreci oluşturulabilmesi için bu alandaki görev ve sorumlulukların açık ve net bir biçimde belirlenmesi gerekmektedir. Olgunlaşmış bir bilinçlendirme süreci, bu görev ve sorumlulukların sahipleri tarafından doğru anlaşılması, bilinmesi ve uygulanması ile mümkündür. Bilgi ve iletişim güvenliği bilinçlendirme süreci içinde en üst seviyeden en alt seviyeye kadar çalışanların katılımını gerektirmektedir.

Üst yönetim, güvenlik bilinçlendirme sürecinden nihai olarak sorumlu olan taraftır. Kurumun üst yönetimi bir bilinçlendirme süreci oluşturulmasına yönelik kararlılığını ortaya koymalıdır. Bu süreçte başarıya ulaşma konusunda üst yönetimin durum ve yaklaşımı son derece önemlidir.

Bilgi ve İletişim Güvenliği Yöneticileri, kurum üst yönetimi tarafından bilinçlendirme sürecinin oluşturmasını yönetmekle görevlendirilen kişilerdir. Bu kişiler eğitim stratejilerini belirler, gerekli finansmanı sağlarlar ve bilinçlendirme sürecini takip ederler.

Bölüm Yöneticileri, bilgi ve iletişim güvenliği bilinçlendirme ve eğitimi sürecinin gereklerine personelinin, uymasını sağlamakla sorumludurlar.

Diğer Kurum Çalışanları, bu süreçteki en büyük ve önemli hedef kitledir. Kurum içindeki işler yürütülürken yapılan hataları ve bilgi sisteminde oluşabilecek açıklıkları en aza indirmek onların elindedir.

Kurum personeli, yüklenici firma personeli, yarı zamanlı personel, stajyerler, diğer kurum çalışanları, iş ortaklarının çalışanları, destek alınan firmaların personeli kısaca kurumun bilgi varlıklarına erişim gereksinimi olan herkes kurumun Bilgi ve İletişim Güvenliği konusundaki sorumluluklara sahip olmalıdır.

Bu süreçte öncelikle kurum personelinin ne tür bilinçlendirilme ve eğitime ihtiyaç duyduğu tespit edilmelidir. Tespit için (Önel, 2008: 13):

- Kurumsal anketler
- Belirlenen tüm kritik personel gruplarıyla yüz yüze yapılacak görüşmeler ile personelin günlük görevleri kapsamında gerçekleştirdiği aktivitelerin ve bilgi sisteminin hangi amaçlarla kullandıklarının öğrenilmesi
- Kurum çapında bugüne kadar düzenlenmiş bilgi ve iletişim güvenliği eğitim faaliyetlerinin gözden geçirilmesi
- Geçmişte yaşanmış güvenlik ihlali olaylarının incelenmesi (servis dışı bırakılma, web sayfasının değiştirilmesi, sisteme yapılan yetkisiz girişler, başarılı virüs saldırıları)
- Bilgi sistemine erişimi olan kullanıcıların hesap dökümünün alınması

- Geçmişte yapılmış denetimlere ait raporlardaki bulguların incelenmesi
- Bilgi sisteminde yapılan teknik ve alt yapısal değişikliklerin sürekli takip edilmesi
- Akademik çevrelerde ve eğitim kurumlarındaki bilgi ve iletişim güvenliği alanında takip edilen son gelişmelerden haberdar olunması şeklinde yöntemler kullanılmaktadır.

İhtiyaçlar belirlendikten sonra bu doğrultuda bir eğitim stratejisi belirlenmelidir. Strateji belirlenirken hangi personelin kurslara tabi tutulacağı, hangi personel ile bire bir ilgilenilmesi gerektiği, ne tür etkinliklerle bilinçlendirme yapılacağına karar verilmelidir.

Hedef kitleye bilinçlendirme ve eğitim çalışmaları yılda en az bir kez yapılmalıdır. Programın hedefine ulaşması açısından süreklilik gereklidir. Bilişim güvenliği konusunda daha çok sorumluluğa sahip personel (sistem yöneticileri, ağ yöneticileri, bilgi güvenliği sorumluları v.b.) için bu periyot daha sık olmalıdır.

Kurumsal Bilgi ve İletişim Güvenliği Yönetimi Politikası'nın önemli bir öğesi olan bilinçlendirme ve eğitim süreci boyunca; kurum içinde kimlerin bilgi ve iletişim güvenliği konusunda başarıyla eğitildiği, kimlerin hala eğitime ihtiyaç duyduğu, katılımcıların eğitim materyallerini nasıl değerlendireceği ve kurumun katılımcıların eğitimi ve diğer faaliyetlerden gerçekten bir kazanım sağlayıp sağlamadığı tespit edilmelidir.

8.3. Güvenliği Sağlayacak Yazılım ve Donanımın Temin Edilmesi

Kurumsal iletişimde güvenliği sağlamak için öncelikle gerekli donanım ve yazılım sistemlerinin temin edilmesi gerekmektedir. Gelişmiş özelliklerde servis sağlayıcılar, ağ donanımları, otomasyonlar ve telefon görüşmeleri için iyi bir santral bu konuda yapılması gereken yatırım kalemleridir. Güvenliğin daha

fazla ön planda olduğu kurumlarda ise sinyal bozucu, şifreleme sistemleri, büyük yapılandırılmış bilgi yedekleme üniteleri gibi daha etkin donanım elemanları kullanılmaktadır.

Fortune dergisinin ilk 500 kategorisinde bulunan üst düzey yöneticilerin iletişim teknolojilerine olan tutumlarını değerlendiren bir çalışma, çoğunluğun interneti takip ettiğini ortaya koymuştur. İnternet günümüz iş dünyasının devamlılığının anahtarı gibi görülmekte ve her geçen gün büyümektedir. Gerçekten de e-postanın bir numaralı iletişim teknolojisi olması beklenmektedir. 200 işletmenin yetkilileriyle görüşülmüş ve aşağıdaki topolojilerin bir örgütün başarısında önemli olduğu tespit edilmiştir (Telephony, 2000: 34):

İnternet	%90
Kurum Şebekeleri ve intranet	%78
E-mail	%75
Kablosuz İletişim	%64
Taşınabilir bilgisayarlar	%60
Ses, veri ve imgelerin yöndeşmesi	%54
Fax	%11

Kurumlar bilgisayar ve yeni teknolojiler üzerinden iletişim ağlarını oluştururken ihtiyaçlarına göre performans ve maliyet dengesini göz önüne almalıdır. Bunu yaparken bilgi ve iletişim güvenliğini sağlayacak faktörlere de yeterli önem verilmelidir. Güvenliği sağlayacak donanım ve yazılımlar:

Anahtarlama cihazları yerel alan ağlarında temel iletişimi sağlayan cihazlardır. Anahtarlama cihazlarından gelişmiş olanları birçok güvenlik mekanizmasını da bünyesinde barındırmaktadır. Kimlik doğrulama, port güvenliği, servis kontrolü gibi güvenlik tedbirlerini almaya imkan sağlayan özellikler bulunabilmektedir.

Yönlendiriciler iç ağı dış dünyaya (internete) bağlamak amacıyla kullanılması gereken cihazlardır. Bu cihazlar üzerinde bulunan güvenlik duvarı, kural oluşturma tabloları, port ve ip kontrol listeleri sayesinde dış ağdan gelecek saldırılara karşı önlemler alınması sağlanabilir.

Saldırı tespit sistemleri ağa yapılan saldırıları tespit edip sistem yöneticilerini bilgilendirerek gerekli önlemlerin alınmasını sağlamaktadır. Bununla birlikte **saldırı engelleme sistemleri** ise ağa yapılan saldırıları haber verdiği gibi engelleme yeteneğine de sahiptirler.

Güvenlik duvarı ise bir bilgisayar ağında, ağ kullanıcılarının güvenli bir şekilde dış ağa erişebilmesi ve bunun yanı sıra dış ağdaki kullanıcıların ağdaki servislere zarar vermeden izinler dahilinde kullanabilmesini sağlayan cihazlardır. Bu cihazlar üzerindeki yazılımlar sayesinde iletişim güvenliğini sağlama yeteneğine sahiptirler ve yazılımları günün şartlarına göre güncellenebilmektedir.

Bilgi güvenliğinde kişisel bilgisayarlar ve diğer cihazlar da çok önemlidir. Bilgisayarlar ve üzerinde ki yazılımlar gerekli güvenlik protokollerini desteklemelidir. Kişisel bilgi güvenliğini sağlamak amacıyla virüslere ve benzeri zararlı yazılımlara karşı antivirüs programları yüklenmiş olmalıdır.

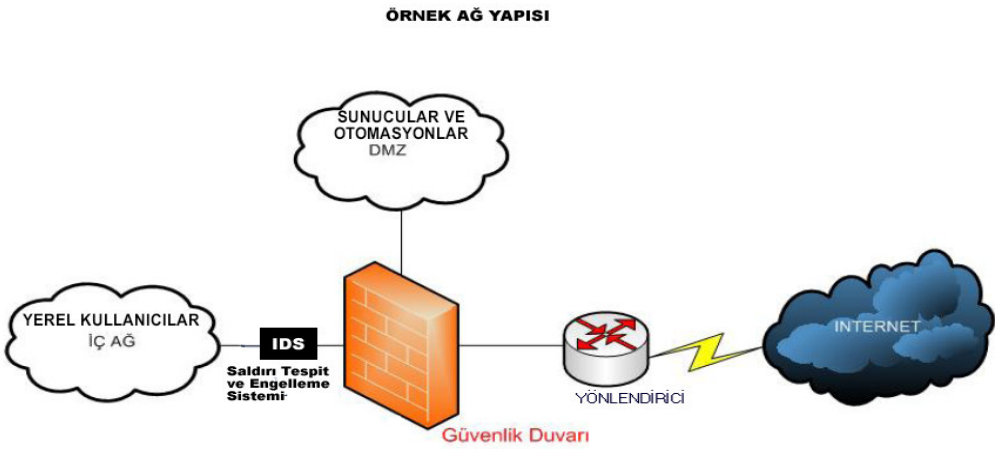
Tüm bu cihazların üzerindeki yazılımların lisanslı olması önemli bir ayrıntıdır. Birçok kurum ve personel bu ayrıntıyı es geçmektedir. Fakat güvenlik suçu ile karşı karşıya kalınan durumlarda ancak yazılımların lisanlı olması halinde hak aranabileceği unutulmamalıdır.

8.4. Güvenlik İçin Gerekli Yapının Kullanılması

Günümüzde kamu kuruluşlarının ve diğer örgütlerin büyük bir kısmı resmi yazışmalarını, sorgulamalarını, çağrı sistemlerini, otomasyon sistemleri ile bilgi aktarımlarını, sesli ve görüntülü görüşmelerini internet üzerinden veya

oluşturulmuş kiralık hatlar üzerinden gerçekleştirmektedirler. Bu aktivitelerin gerçekleştirilebilmesi için güvenli bir ağ yapısına ve dışarıya erişim cihazlarına ihtiyaç duyulmaktadır. Kurumlarda oluşturulacak iletişim altyapısı; bilginin gizliliğinin, erişebilirliğinin ve bütünlüğünün korunmasını sağlayacak temel ağ elemanlarını barındırmalıdır ve bu elemanlar yerli yerince kullanılmalıdır. Şekil 2'de örnek bir ağ yapısında cihazlar, yerel ağ, sunucular ve internetin nasıl konumlandırılabileceği gösterilmiştir.

Şekil 2. Kurumların Oluşturabileceği İnternete Açılan Örnek Bir Ağ Yapısı



Şekle göre, güvenlik duvarı, yönlendirici vasıtasıyla sağlanan internet bağlantısından gelecek saldırılara karşı sunucuların bulunduğu ağı (DMZ) ve yerel kullanıcıların bulunduğu içi ağı korumaktadır. Saldırı tespit ve engelleme sistemi (IDS) ise yerel kullanıcılar veya onlara ait bilgisayarları kullanarak zarar vermeye çalışan dış kullanıcılar tarafından sunuculara yapılacak saldırıları tespit eder, bilgi verir, önlemeye çalışır ve kayıt altına alır.

Şekilde ki yapıya benzer yapılar ihtiyaca göre daha fazla genişletilebilir. Kuruma ve kurumdaki bilgilerin değerine göre güvenlik duvarı veya saldırı tespit sistemleri birden fazla kullanılabilir. Yönlendirici ve diğer cihazlar

üzerine daha gelişmiş yazılımlar ve şifreleme sistemleri kurularak farklı önlemler alınabilir.

8.5. Log Tutulması ve Logların Takibi

Güvenlik tedbirleri için ve oluşabilecek olumsuzluklar sonrasında gerekli işlemlerin yapılabilmesi için log kayıtları çok önemlidir. Log kayıtları, kullanılan iletişim teknolojileri üzerindeki tüm iletişim trafiğini listeleyen denetim kayıtlarıdır. Bu kayıtlar cihaz içinde tutulduğu gibi ayrı bir log sunucusunda da saklanabilir. Denetim kayıtlarındaki listelenmiş bilgiler log sunucusu üzerinde incelenerek yapılan erişimler takip edilebilir veya yapılan şüpheli bağlantılar daha ayrıntılı incelenebilir. Denetim kayıtları yapılan erişimlerin kanıtları niteliğindedir. Bu nedenle denetim kanıtlarının kötü niyetli birinin eline geçmesi, sisteme yapılan saldırılara ait ipuçlarının yok olması anlamına gelebilir. Denetim kayıtları belli periyotlarda cd ve dvd gibi ortamlara alınarak muhafaza edilmesinde büyük yarar vardır.

9. ERZİNCAN ÜNİVERSİTESİNDE BİLGİ VE İLETİŞİM GÜVENLİĞİNE YÖNELİK ARAŞTIRMA

Bu araştırma işlenilen konunun örnek bir kamu kurumu ile somutlaştırılmasına ve tezin önerisinde düşünülen ve öngörülen bir takım fikirlerin doğruluğunun tespitine ışık tutmaktadır. Kamu kurumlarının, özellikle üniversitelerin gelişen bilgi ve iletişim teknolojileri takip ederken yapılan güncellemelerin kapsamına çalışanların da dahil edilmesi hususunda verilecek kararların önemini ortaya koyan bir araştırma niteliğindedir.

Uygulama sürecinde katılımcıların tamamına yakını düzenlenen anketin sorularını özveri ile cevaplamıştır. Düzenlenen anketin soruları bir birini tamamlayıcı niteliktedir ve bütünlük arz etmektedir. Bu nedenle cevaplarında tutarsızlık görülen veya yarım bırakılan anketler analize tabi tutulmamıştır.

9.1. Araştırmanın Amacı

Daha önceki bölümlerde gelişen teknolojiyle kurumların bilgi ve iletişim sağlama aracılarının da değiştiğini, kurumların işleyişinin online sistemlere dönüştüğünü ve kurumlardaki bilgisayar ve internet kullanıcılarının büyük yüzdelere ulaştığını, buna bağlı olarak kurumun ve kurum çalışanlarının bilgilerinin daha güvensiz ve saldırılara açık ortamlara taşındığı belirtilmektedir. Hat dinlemeler, mesaj çalmalar, virüsler, izinsiz veritabanı erişimleri gibi saldırıların bilinçsiz kurum çalışanlarını defalarca zor durumda bıraktığı görülmektedir. Kuruma ait özel verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayan güvenlik politikalarının sadece teknik düzeyde kalamayacağı hatta çoğunlukla çalışanların bu konuda bilinçlendirilmesi gerektiği bir gerçektir. Son yıllarda kalite çalışmalarının kurumun bilgi işlemi, basın yayın birimi ve eğitimcilerin birleşimi sonucu oluşturulan kurullarla yapılması kalite çalışmalarıyla bilişim konularının iç içe olduğunu göstermektedir.

Araştırmanın amacı, Erzincan Üniversitesi personelinin bilgi teknolojilerine ve yeni iletişim kanallarına yaklaşımları konusundaki mevcut durum saptamasını yaparken, bu kanallara olan güveninin dengede olup olmadığı sorularına da cevap aramaktır. Kurum personeli birçok kişisel işini ve kurumu ilgilendiren işlemleri (kişisel ve kurumsal e-devlet işlemleri, online bankacılık işlemleri, telefon bankacılığı, internet ortamında sohbet, e-posta kullanımı gibi) iş anında kullandığı bilgisayarlardan ve iletişim gereçlerinden gerçekleştirmektedir. Bu anketle kurum çalışanlarının bahsedilen işlemleri gerçekleştirirken bilinç düzeyleri, deneyimleri ve demografik özellikleri ile yeni iletişim teknolojilerine ve güvenlik konularına yaklaşımları arasındaki ilişki araştırılmıştır.

9.2. Araştırmanın Yöntem ve Sınırlılıkları

Araştırma Erzincan Üniversitesi'nin personeline uygulanan bir anketle gerçekleştirilmiştir. Hazırlanan anket soruları kurum personeline yazılı bir şekilde elden ulaştırılarak cevaplamaları sağlanmıştır. Araştırmada idari ve akademik kadroya sahip yönetici, teknik personel ve diğer pozisyondaki çalışanlar görüşlerini belirtmişlerdir.

Araştırmanın bulguları, yalnızca bu örneklem ile benzer koşulları taşıyan örneklemlere genellenebilir. Araştırma kesitsel olduğundan, kesitsel araştırma deseninin tüm dezavantajları bu araştırma için de geçerlidir. Araştırmanın sınırları, ülkemizdeki kamu çalışanları evreninden Erzincan Üniversitesi'nde çalışan, işyerinde kuruma ait bilgisayarları ve diğer iletişim araçlarını kullanan personel olarak belirlenmiştir.

9.3. Araştırmanın Hipotezleri

H1: Kurum çalışanları yeni iletişim kanallarını yoğun bir şekilde kullanmaktadırlar. Buna karşın personel internet ortamındaki iletişime güven duymamaktadır. (Varsayım)

H2: Kurumlarda şifre oluşturma işlemlerine personel tarafından yeterli önem verilmemektedir. (Varsayım)

H3: Kurum çalışanlarının önemli bir kısmı şifrelerini çaldırma, veri kaybı, virüsten zarar görülmesi gibi bilgi ve iletişim güvenliği konusunda kötü tecrübeler yaşamıştır. (Varsayım)

H4: Personel türü (Akademik/İdari) yeni iletişim teknolojilerine olan yaklaşımı değiştirmektedir.

H5: Çalışma/hizmet süreleri yeni iletişim teknolojilerine olan yaklaşımı değiştirmektedir.

H6: Yaş aralığı yeni iletişim teknolojilerine olan yaklaşımı değiştirmektedir.

9.4. Veri Toplama Aracı

Araştırmada tanımlayıcı ve açıklayıcı veriler elde etmek amacı ile hazırlanan ve 42 sorudan oluşan bir anket kullanılmıştır. Anket soruları 3 gruptan oluşmaktadır.

İlk grupta çalışanın demografik özelliklerini belirttiği yaş, cinsiyet, kadro türü, unvan gibi bilgileri isteyen sorulardan oluşmaktadır.

İkinci gruptaki sorular personelin bilgisayar ve internet kullanım yoğunluğunu ölçecek nitelikteki sorulardır. Bu bölümde aynı zamanda kullanıcının dikkat göstermesi gereken online işlemleri kullanıp kullanmadığını anlamaya yönelik sorular sorulmuştur.

Üçüncü gruptaki sorular ise; kurum çalışanının bilgi ve iletişim güvenliği ile ilgili başından geçen istenmeyen olaylara (veri kaybı, şifre çaldırma gibi), konuya yaklaşımı ve konuyla ilgili alışkanlıkları saptamaya yöneliktir.

Ankete katılan 238 kişiye ait veriler SPSS 16.0 programına girilerek analize tabi tutulmuştur. Analiz yapılarak elde edilen bulgular yine bu programın verdiği sonuçlar ile elde edilmiştir.

9.5. Veri Analizi

Veri analizi yapılırken hipotez 1, hipotez 2 ve hipotez 3 için ankette ilgili sorulara verilen cevapların frekans dağılımları hesaplanmıştır. Hipotez 4, hipotez 5 ve hipotez 6 için doğruluk kontrolü ki-kare testi ile yapılmıştır ve çapraz tablolar verilmiştir.

- ✓ 238 kişinin katıldığı anketteki ilk grup sorulardan elde edilen demografik bulgular Tablo 6'da,

- ✓ Personelin internet ortamındaki yeni iletişim kanallarını kullanım yoğunluğu Tablo 7'de,
- ✓ Web üzerinde ki yazılımları ve otomasyonları kullanım oranları Tablo 8' de,
- ✓ Günümüz iletişim teknolojileri ile birlikte ortaya çıkan yeni iletişim metotlarına duyulan güvene ilişkin verilen cevap dağılımına ise Tablo 9'da yer verilmiştir.

Tablo 6. Katılımcıların Demografik Özellikleri

	Sayı	**Yüzde**
Cinsiyet		
Erkek	185	77,7
Kadın	53	22,3
Yaş Aralığı		
20-25	40	16,8
26-30	72	30,3
31-40	55	23,1
41-50	50	21,0
51 ve üstü	21	8,8
Medeni Hal		
Evli	149	62,6
Bekar	89	37,4
Personel Türü		
Akademik	124	52,1
İdari	114	47,9
Çalıştığı Birim		
Rektörlük	59	24,8
Enstitü	6	2,5
Fakülte	98	41,2
Yüksekokul	16	6,7
Meslek Yüksekokulu	59	24,8
Unvan		
İşçi	12	5,0
Memur	62	26,1
İşletmen	7	2,9
Teknisyen	11	4,6
Tekniker	7	2,9
Mühendis	2	0,8
Yönetici	10	4,2
Uzman	9	3,8
Okutman	8	3,4
Arş. Gör.	31	13,0
Öğr. Gör.	43	18,1
Yrd. Doç.	34	14,3
Doç.	1	0,4
Prof.	1	0,4

Tablo 7. Personelin İnternet Üzerindeki İletişim Kanallarını Kullanma Yoğunluğu

E-Posta hizmetlerini kullanıyor musunuz?		
	N	**%**
Evet	226	95,0
Hayır	12	5,0
Toplam	238	100,0
Anlık ileti programlarını kullanıyor musunuz?		
	N	**%**
Evet	218	91,6
Hayır	20	8,4
Toplam	238	100,0
Internet üzerinden sesli ve görüntülü görüşme yapıyor musunuz?		
	N	**%**
Evet	158	66,4
Hayır	80	33,6
Toplam	238	100,0

Tablo 7' de 2000'li yılların en fazla kullanılan iletişim kanalı olarak öngörülen E-posta kullanımının personel arasında %95 gibi bir orana ulaştığı görülmüştür. MSN, Yahoo Massenger gibi anlık ileti programlarının ise %91,6 oranlarında kullanıldığı sonucuna varılmıştır. Sohbet imkanı sağlayan yazılımlara eklenen yeni özelliklerle birlikte ortaya çıkan internet üzerinden sesli ve görüntülü görüşmeler kurum personelinin %66'sı tarafından tercih edildiği saptanmıştır.

Tablo 8' de; çalışanların %67,2'sinin kimlik numarası sorgulama, taşıt vergisi ödeme, seçimlerde sandığını öğrenme gibi e-devlet işlemlerinden yararlanıyor olmasının yanında internet üzerinden tüm bilgilerini girerek alış veriş yapıyor olması(~%40) ve bankalarının sunduğu internet bankacılığı işlemlerinden faydalandığı gözlemlenmektedir (~%60).

Tablo 8. Çalışanların Web Uygulamalarını Kullanma Yoğunluğu

Web ortamındaki e devlet islemlerinden faydalanıyor musunuz?		
	N	**%**
Evet	160	67,2
Hayır	78	32,8
Üyelik isteyen web sitelerine tüm bilgilerinizi girerek üye olur musunuz?		
	N	**%**
Evet	38	16,0
Hayır	200	84,0
İnternet üzerinden alışveriş yapıyor musunuz?		
	N	**%**
Evet	94	39,5
Hayır	144	60,5
Cep telefonunuza ait online işlemleri yapıyor musunuz?		
	N	**%**
Evet	62	26,1
Hayır	176	73,9
İnternet bankacığı işlemlerini kullanıyor musunuz?		
	N	**%**
Evet	109	45,8
Hayır	129	54,2

Tablo 9'daki oranlar; Tablo 7 ve Tablo 8'de ki bulgularla birlikte **1. Hipotez 1'**i doğrular niteliktedir. Personelin %69,3'lük gibi büyük kısmı günümüz iletişim kanallarından hiçbirini güvenli bulmamaktadır. Tablo 9'dan elde edilen diğer bulgular ise;

- Personelin %79,4'ü internet üzerinden alış verişi güvenli bulmamaktadır.
- Personelin %70,6'sı internet bankacılığı işlemlerini güvenli bulmamaktadır.

- Personelin %80'ni internet üzerinden yapılan görüşmeleri güvenli bulmamaktadır.

Tablo 9. Kurum Çalışanlarının Yeni İletişim Kanallarına Yaklaşımı

Günümüz iletişim teknolojilerinden hangisini daha güvenli buluyorsunuz?		
	N	**%**
Telefon	37	15,5
SMS	14	5,9
Internet üzerinden görüşmeler	5	2,1
Hiçbiri	165	69,3
Hepsi	17	7,1
İnternet üzerinden alış veriş güvenliği hakkındaki fikriniz nedir?		
	N	**%**
Güvenli buluyorum ve kullanıyorum	24	10,1
Güvenli bulmuyorum fakat kullanıyorum.	68	28,6
Güvenli buluyorum ama yine de kullanmıyorum.	25	10,5
Güvenli bulmuyorum ve kesinlikle kullanmıyorum	121	50,8
İnternet bankacılığı işlemlerinin güvenliği hakkında fikrinizi belirtir misiniz?		
	N	**%**
Güvenli buluyorum ve kullanıyorum	41	17,2
Güvenli bulmuyorum fakat kullanıyorum.	83	34,9
Güvenli buluyorum ama yine de kullanmıyorum.	29	12,2
Güvenli bulmuyorum ve kesinlikle kullanmıyorum	85	35,7
İnternet üzerinden yapılan yazılı, sesli, görüntülü görüşmelerin güvenilirliği konusunda fikriniz nedir?		
	N	**%**
Güvenli buluyorum ve kullanıyorum	26	10,9
Güvenli bulmuyorum fakat kullanıyorum.	140	58,8
Güvenli buluyorum ama yine de kullanmıyorum.	24	10,1
Güvenli bulmuyorum ve kesinlikle kullanmıyorum	48	20,2

Hipotez 2, yapılan araştırmaya göre doğrudur. Çünkü Tablo 10'da kurum personeli %37,4 gibi önemli bir kısmı bilgisayarlarının açılışına şifre oluşturmamaktadır ve online işlemler için -ki bu işlemler internet ortamında olduğundan saldırılara açıktır- yeterince karmaşık şifreler kullanmamaktadır. Ayrıca "Şifrelerinizi yeterince sık değiştiriyor musunuz" sorusuna verilen cevaplardan %66,4 'ü "Hayır" şeklindedir.

Tablo 10. Kurum Çalışanlarının Şifre Kullanma Alışkanlıkları

İşletim sistemleriniz için giriş şifresi kullanıyor musunuz?		
	N	**%**
Evet	149	62,6
Hayır	89	37,4
Tüm online işlemler için yeterince karmaşık şifreler oluşturuyor musunuz?		
	N	**%**
Evet	114	47,9
Hayır	124	52,1
Şifrelerinizi yeterince sık değiştiriyor musunuz?		
	N	**%**
Evet	80	33,6
Hayır	158	66,4

Hipotez 3'teki kanıya bağlı olarak Tablo 11'den elde edilen bulgular şunlardır:

- 238 personelden 11'inin kredi kartı veya internet bankacılığı hesap bilgileri çalınarak maddi zarara uğratılmıştır.
- Personelin %66,8'i virüs ve benzeri zararlı yazılımlardan etkilenmiştir.
- Personelin %51,3'ü, yani yaklaşık her iki kişiden birinin bilgisayar ortamındaki verileri kaybolma veya bozulma gibi olumsuz etkilere maruz kalmıştır.

Personellerin bilgi ve iletişim güvenliği konusunda sıkıntılar yaşadığı anlaşılmaktadır.

Tablo 11. Kurum Çalışanlarının Bilgi Güvenliği Konusundaki Deneyimleri

E-posta ve benzeri internet kullanım şifreleriniz kötü niyetli kişiler tarafından ele geçirildi mi?		
	N	**%**
Evet	27	11,3
Hayır	211	88,7
Virüs, trojan, spy gibi zararlı yazılımlara maruz kaldınız mı?		
	N	**%**
Evet	159	66,8
Hayır	79	33,2
Bilgisayarınızdaki önemli veri ve bilgileri yedekliyor musunuz?		
	N	**%**
Evet	198	83,2
Hayır	40	16,8
Bilgisayarinizdaki önemli veri ve bilgilerin kaybolması veya bozulması olaylarına maruz kaldınız mı?		
	N	**%**
Evet	122	51,3
Hayır	116	48,7
Kötü niyetli mailler aldınız mı ve bilgisayarınıza zarar verdi mi?		
	N	**%**
Evet	72	30,3
Hayır	166	69,7
Kötü niyetli anlık ileti adınız mı ve zarar verdi mi?		
	N	**%**
Evet	68	28,6
Hayır	170	71,4
Kredi kartı ve hesap bilgileriniz kötü niyetli kişiler tarafından ele geçirildi mi?		
	N	**%**
Evet	11	4,6
Hayır	227	95,4

Hipotez 4'te öne sürülen akademik ve idari personelin genel olarak yeni iletişim teknolojilerine ve bilgi - iletişim güvenliği konularına farklı yaklaşımlar içinde olduğunu aşağıdaki tablolar göstermektedir. 12- 27 numaralı tablolarda ki-kare testi uygulanarak verilen ilişkiler analiz edilmiştir. Tablolarda kullanılan kısaltmalar E: beklenen değeri, C: çıkan değeri ifade etmektedir.

Tablo 12. Personel Türü * E-Posta Hizmetlerini Kullanma Dağılımı

E-posta hizmetlerini kullanıyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	121	3	124
		E	117,7	6,3	124,0
	İdari	C	105	9	114
		E	108,3	5,7	114,0
Toplam			226	12	238

P=0.54 >0.005 olduğundan aralarında anlamlı bir ilişki bulunmamaktadır. Hem akademik hem de idari personel e-posta hizmetlerini yoğun bir şekilde kullanmaktadırlar. E-posta kullanımı kuruluşlar ve çalışanlar için birçok avantaj getirmiştir. E- posta ile birlikte;

- ✓ Dosya ve resim iletişimi,
- ✓ Toplu gönderimler ile duyuru, reklam, propaganda yapılabilmesi,
- ✓ İnsan kaynakları ve bilgi edinme başvurularının yapılabilmesi ve alınabilmesi,
- ✓ Elektronik imzanın kullanarak resmi yazışmaların yapılabilmesi
- ✓ Gönderilen ve alınan mektupların istenilen sayıda istenildiği kadar saklanabilmesi ve ihtiyaç duyulduğu anda okunabilmesi,
- ✓ Cep telefonu sayesinde posta geldiğinde anında haber alınabilmesi,

gibi avantajların oluşması elektronik postanın çağımızın en popüler iletişim aracı olmasını sağlamıştır.

Tablo 13. Personel Türü * Anlık İleti Programlarını Kullanma Dağılımı

Anlık ileti programlarını kullanıyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	119	5	124
		E	113,6	10,4	124,0
	İdari	C	99	15	114
		E	104,4	9,6	114,0
Toplam			218	20	238

P=0.011 < 0.05 olduğundan söz konusu ilişki anlamlıdır. Tablo 13'te çaprazlama sonucu akademik personelin çıkan değeri (C) istenilen değerden (E) yüksek olduğu görülmektedir. Buna göre; anlık ileti programlarını akademik personelin daha yoğun kullandığı anlaşılmaktadır.

Tablo 14. Personel Türü * Görüntülü ve Sesli Görüşme Oranları

İnternet üzerinden görüntülü ve sesli görüşme yapıyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	92	31	124
		E	81,8	41,7	124,0
	İdari	C	65	49	114
		E	75,2	38,3	114,0
Toplam			157	80	238

P=0.010 < 0.05 olduğundan ilişki anlamlıdır. Akademik personel internet üzerinden görüntülü ve sesli görüşmeyi daha fazla kullanmaktadır.

Tablo 15. Personel Türü * E- Devlet İşlemlerinden Faydalanma Oranları

Web ortamındaki e devlet işlemlerinden faydalanıyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	94	30	124
		E	83,4	40,6	124,0
	İdari	C	66	48	114
		E	76,6	37,4	114,0
Toplam			160	78	238

P=0.003 < 0.05 olduğundan ilişki anlamlıdır. Akademik personel E-Devlet

işlemlerinden daha fazla faydalanmaktadır. E-Devlet işlemlerinden kasıt TC Kimlik numarası sorgulama, vergi miktarını öğrenme, ikamet bilgisi alma gibi online işlemlerin gov.tr uzantılı web siteleri üzerinden yapılmasıdır. İdari personelin bu tür online işlemler yerine daha çok klasik yöntemleri kullanmaya devam ettiği gözlemlenmektedir.

Tablo 16. Personel Türü * İnternet Üzerinden Alışveriş Yapma Dağılımı

İnternet üzerinden alışveriş yapıyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	68	55	123
		E	48,3	74,7	123,0
	İdari	C	25	89	114
		E	44,7	69,3	114,0
Toplam			93	144	237

P=0.000 < 0.05 olduğu için ilişki anlamlıdır. Akademik personel internet üzerinden alışverişi daha fazla tercih etmektedir.

Tablo 17. Personel Türü * İnternet Bankacılığı İşlemlerini Kullanma Dağılımı

İnternet bankacılığı işlemlerini kullanıyor musunuz?		Evet	Hayır	Toplam
Personel Türü	Akademik	67	57	124
		56,8	67,2	124,0
	İdari	42	72	114
		52,2	61,8	114,0
Toplam		109	129	238

P=0.008 < 0.05 olduğu için ilişki anlamlıdır. İnternet bankacılığı işlemlerini de akademik personel daha fazla kullanmaktadır.

Tablo 18. Personel Türü * İşletim Sistemleriniz İçin Giriş Şifresi Kullanma Dağılımı

İşletim sistemleriniz için giriş şifresi kullanıyor musunuz?		Evet	Hayır	Toplam
Personel Türü	Akademik	85	39	124
		77,6	46,4	124,0
	İdari	64	50	114
		71,4	42,6	114,0
Toplam		149	89	238

P=0.048 < 0.05 olduğu için anlamlı bir ilişki bulunmaktadır. Akademik personel şifre oluşturma işlemlerine daha fazla önem vermektedir. Bilinç düzeyinin güvenli giriş sağlama düşüncesine etkisi olduğu düşünülmektedir.

Tablo 19. Personel Türü * Tüm Online İşlemler İçin Karmaşık Şifreler Oluşturma Oranları

Tüm online işlemler için yeterince karmaşık şifreler oluşturuyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	65	59	124
		E	59,4	64,6	124,0
	İdari	C	49	65	114
		E	54,6	59,4	114,0
Toplam			114	124	238

P=0.145 > 0.05 olduğu için anlamlı bir ilişki bulunmamaktadır.

Tablo 20. Personel Türü * Şifrelerini Yeterince Sık Değiştirme Dağılımları

Şifrelerinizi yeterince sık değiştiriyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	49	75	124
		E	41,7	82,3	124,0
	İdari	C	31	83	114
		E	38,3	75,7	114,0
Toplam			80	158	238

P=0.044 < 0.05 olduğu ilişki anlamlıdır. Akademik personeller idari personele göre şifrelerini daha sık değiştirmektedir.

Tablo 21. Personel Türü * Virüs, Trojan, Spy Gibi Zararlı Yazılımlara Maruz Kalma Oranları

Virüs, trojan, spy gibi zararlı yazılımlara maruz kaldınız mı?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	89	35	124
		E	82,8	41,2	124,0
	İdari	C	70	44	114
		E	76,2	37,8	114,0
Toplam			159	79	238

P=0.090 > 0.05 olduğundan anlamlı bir ilişki mevcut değildir.

Tablo 22. Personel Türü * Bilgisayarlarındaki Önemli Veri ve Bilgileri Yedekleme Dağılımları

Bilgisayarınızdaki önemli veri ve bilgileri yedekliyor musunuz?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	104	20	124
		E	103,2	20,8	124,0
	İdari	C	94	20	114
		E	94,8	19,2	114,0
Toplam			198	40	238

P=0.771 > 0.05 olduğundan ilişki anlamlı değildir.

Tablo 23. Personel Türü * Bilgisayarlarındaki Önemli Veri ve Bilgilerin Kaybolması Veya Bozulması Olaylarına Maruz Kalma Oranları

Bilgisayarınızdaki önemli veri ve bilgilerin kaybolması veya bozulması olaylarına maruz kaldınız mı?			Evet	Hayır	Toplam
Personel Türü	Akademik	C	75	49	124
		E	63,6	60,4	124,0
	İdari	C	47	67	114
		E	58,4	55,6	114,0
Toplam			122	116	238

P=0.003 < 0.05 olduğundan anlamlı bir ilişki bulunmaktadır. Akademik personelin daha fazla veri kaybolması veya bozulması olaylarına maruz kaldığı gözlemlenmiştir. Bu olaylara virüsler, bilgisayarın düzgün kapatılmaması, elektrik beslemesinde yüksek voltaj gibi etkenler neden olabilmektedir.

Tablo 24. Personel Türü * Günümüz İletişim Teknolojilerine Güven Duyma Dağılımları

Günümüz iletişim teknolojilerinden hangisini daha güvenli buluyorsunuz?			Telefon	SMS	Int. Üz. Grş.	Hiçbiri	Hepsi	Toplam
Personel Türü	Akademik	C	18	6	2	93	5	124
		E	19,3	7,3	2,6	86,0	8,9	124,0
	İdari	C	19	8	3	72	12	114
		E	17,7	6,7	2,4	79,0	8,1	114,0
Toplam			37	14	5	165	17	238

P=0.226 > 0.05 olduğundan anlamlı bir ilişki yoktur.

Tablo 25. Personel Türü * İnternet Bankacılığı İşlemlerinin Güvenliği Hakkında Belirtilen Fikirler

İnternet bankacılığı işlemlerinin güvenliği hakkında fikrinizi belirtir misiniz?			Güvenli buluyorum ve kullanı-yorum	Güvenli bulmuyoru m fakat kullanı-yorum.	Güvenli buluyoru m ama yine de kullan-mıyorum	Güvenli bulmuyoru m ve kesinlikle kullan-mıyorum	Toplam
Personel Türü	Akademik	C	24	52	13	35	124
		E	21,4	43,2	15,1	44,3	124,0
	İdari	C	17	31	16	50	114
		E	19,6	39,8	13,9	40,7	114,0
Toplam			41	83	29	85	238

P=0.028 < 0.05 olduğundan anlamlı bir ilişki bulunmaktadır. Akademik personeller internet bankacılığına güven duymadıklarını ama yine zorunlu olarak kullandıklarını daha baskın olarak belirtmişlerdir. İnternet bankacılığı işlemlerinde yaşanan dolandırıcılık olaylarının personeli etkilediği görülmektedir.

Tablo 26. Personel Türü * İnternet Üzerinden Alışveriş Güvenliği Hakkında Belirtilen Fikirler

İnternet üzerinden alış veriş güvenliği hakkındaki fikriniz nedir?			Güvenli buluyorum ve kullanıyorum	Güvenli bulmuyor um fakat kullanı-yorum.	Güvenli buluyorum ama yine de kullan-mıyorum.	Güvenli bulmuyor um ve kesinlikle kullan-mıyorum	Toplam
Personel Türü	Akademik	C	18	53	10	43	124
		E	12,5	35,4	13,0	63,0	124,0
	İdari	C	6	15	15	78	114
		E	11,5	32,6	12,0	58,0	114,0
Toplam			24	68	25	121	238

P=0.000 < 0.005 olduğundan anlamlı bir ilişki mevcuttur. İdari personeller yoğunluklu olarak internet üzerinden alış verişe güven duymadıklarını ve kesinlikle kullanmadıklarını belirtmişlerdir. Elektronik ticarette alıcı ve satıcı birbirini görememesi, para ödendikten sonra ürünün gönderilmesi, alış veriş esnasında önemli bilgilerinin çalınma ihtimalinin olması gibi nedenler duyulan güveni etkilemektedir.

Tablo 27. Personel Türü * İnternet Üzerinden Yapılan Yazılı, Sesli, Görüntülü Görüşmelerin Güvenilirliği Konusunda Belirtilen Fikirler

İnternet üzerinden yapılan yazılı,sesli,görüntülü görüşmelerin güvenilirliği konusunda fikriniz nedir?			Güvenli buluyorum ve kulanı-yorum	Güvenli bulmuyorum fakat kulla-nıyorum.	Güvenli buluyorum ama yine de kullan-mıyorum.	Güvenli bulmuyorum ve kesinlikle kullan-mıyorum	Toplam
Personel Türü	Akademik	C	13	81	12	18	124
		E	13,5	72,9	12,5	25,0	124,0
	İdari	C	13	59	12	30	114
		E	12,5	67,1	11,5	23,0	114,0
Toplam			26	140	24	48	238

P=0.109 > 0.05 olduğundan aralarındaki ilişki anlamlı değildir.

Hipotez 5'te kamu personelinin çalışma yıl sayısı ile yeni iletişim teknolojilerine ve bilgi – iletişim güvenlik konusuna yaklaşımları arasında ilişki olduğu görüşünü belirtilmektedir. Personelin tecrübe kazandıkça ve edindiği gözlemlerle zamanla teknolojik hususlardaki davranışları da farklılaşmaktadır kanısındayım. 28- 41 numaralı tablolar ile bu ilişkinin doğruluğu analiz edilmiştir

Tablo 28. Çalışma Yılı Sayısı * E-Posta Hizmetlerini Kullanma Dağılımı

E-posta hizmetlerini kullanıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	109	5	114
		E	108,3	5,7	114,0
	6-10	C	23	1	24
		E	22,8	1,2	24,0
	11-15	C	26	0	26
		E	24,7	1,3	26,0
	16-20	C	27	1	28
		E	26,6	1,4	28,0
	21 ve üstü	C	41	5	46
		E	43,7	2,3	46,0
Toplam			226	12	238

P=0.297 > 0.05 olduğundan anlamlı bir ilişki bulunmamaktadır.

Tablo 29. Çalışma Yılı Sayısı * Anlık İleti Programlarını Kullanıyor Musunuz?

Anlık ileti programlarını kullanıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	109	5	114
		E	104,4	9,6	114,0
	6-10	C	24	0	24
		E	22,0	2,0	24,0
	11-15	C	25	1	26
		E	23,8	2,2	26,0
	16-20	C	27	1	28
		E	25,6	2,4	28,0
	21 ve üstü	C	33	13	46
		E	42,1	3,9	46,0
Toplam			218	20	238

P=0.000 < 0.05 olduğu için anlamlı bir ilişki mevcuttur. Tablo ya göre; personelin anlık ileti programlarının kullanımı çalışma yılı sayısı arttıkça düşmektedir.

Tablo 30. Çalışma Yılı Sayısı * Görüntülü ve Sesli Görüşme Yapma Oranları

Görüntülü ve sesli görüşme yapıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	80	34	114
		E	75,2	38,3	114,0
	6-10	C	19	4	24
		E	15,8	8,1	24,0
	11-15	C	16	10	26
		E	17,2	8,7	26,0
	16-20	C	16	12	28
		Ê	18,5	9,4	28,0
	21 ve üstü	C	26	20	46
		E	30,3	15,5	46,0
Toplam			158	80	238

P=0.048 < 0.05 olduğundan anlamlı bir ilişki bulunmaktadır. Tabloda ki verilere göre; 0– 10 çalışma yılına sahip, yani iş hayatının başında olan personel, 10 yıl üstü çalışanlara göre internet üzerinden görüntülü ve sesli iletişim kurmayı daha fazla tercih etmektedirler.

Tablo 31. Çalışma Yılı Sayısı * E- Devlet İşlemlerinden Faydalanma Dağılımı

Web ortamındaki e devlet islemlerinden faydalanıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	80	34	114
		E	76,6	37,4	114,0
	6-10	C	21	3	24
		E	16,1	7,9	24,0
	11-15	C	19	7	26
		E	17,5	8,5	26,0
	16-20	C	13	15	28
		E	18,8	9,2	28,0
	21 ve üstü	C	27	19	46
		E	30,9	15,1	46,0
Toplam			160	78	238

P=0.015 < 0.05 olduğu için anlamlı bir ilişki mevcuttur. 0- 15 yıl çalışma tecrübesine sahip kurum çalışanları E-Devlet işlemlerine daha fazla rağbet göstermektedirler.

Tablo 32. Çalışma Yılı Sayısı * İnternet Üzerinden Alışveriş Yapma Oranları

İnternet üzerinden alışveriş yapıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	42	71	113
		E	44,3	68,7	113,0
	6-10	C	16	8	24
		E	9,4	14,6	24,0
	11-15	C	13	13	26
		E	10,2	15,8	26,0
	16-20	C	10	18	28
		E	11,0	17,0	28,0
	21 ve üstü	C	12	34	46
		E	18,1	27,9	46,0
Toplam			93	144	237

P=0.014< 0.05 olduğu için anlamlı bir ilişki bulunmaktadır. 0- 5 yıl çalışma tecrübesine sahip personeller internet üzerinden alışverişi daha fazla tercih etmektedirler.

Tablo 33. Çalışma Yılı Sayısı * İnternet Bankacılığı İşlemlerini Kullanma Dağılımı

İnternet bankacığı işlemlerini kullanıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	43	71	114
		E	52,2	61,8	114,0
	6-10	C	15	9	24
		E	11,0	13,0	24,0
	11-15	C	16	10	26
		E	11,9	14,1	26,0
	16-20	C	11	17	28
		E	12,8	15,2	28,0
	21 ve üstü	C	24	22	46
		E	21,1	24,9	46,0
Toplam			109	129	238

P=0.049 < 0.05 olduğundan anlamlı bir ilişki bulunmaktadır. Tablodaki verilere göre genel olarak çalışma yılı sayısı arttıkça internet bankacılığı işlemlerinin kullanımı da artmaktadır.

Tablo 34. Çalışma Yılı Sayısı * İşletim Sistemleri İçin Giriş Şifresi Kullanma Dağılımı

İşletim sistemleriniz için giriş şifresi kullanıyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	67	47	114
		E	71,4	42,6	114,0
	6-10	C	16	8	24
		E	15,0	9,0	24,0
	11-15	C	21	5	26
		E	16,3	9,7	26,0
	16-20	C	19	9	28
		E	17,5	10,5	28,0
	21 ve üstü	C	26	20	46
		E	28,8	17,2	46,0
Toplam			149	89	238

P=0.231 > 0.05 olduğundan anlamlı bir ilişki mevcut değildir.

Tablo 35. Çalışma Yılı Sayısı * Tüm Online İşlemler İçin Yeterince Karmaşık Şifreler Oluşturma Oranları

Tüm online işlemler için yeterince karmaşık şifreler oluşturuyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	59	55	114
		E	54,6	59,4	114,0
	6-10	C	9	15	24
		E	11,5	12,5	24,0
	11-15	C	16	10	26
		E	12,5	13,5	26,0
	16-20	C	13	15	28
		E	13,4	14,6	28,0
	21 ve üstü	C	17	29	46
		E	22,0	24,0	46,0
Toplam			114	124	238

P=0.208 > 0.05 olduğu için anlamlı bir ilişki bulunmamaktadır.

Tablo 36. Çalışma Yılı Sayınız * Şifrelerini Yeterince Sık Değiştirme Oranları

Şifrelerinizi yeterince sık değiştiriyor musunuz?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	37	77	114
		E	38,3	75,7	114,0
	6-10	C	7	17	24
		E	8,1	15,9	24,0
	11-15	C	11	15	26
		E	8,7	17,3	26,0
	16-20	C	7	21	28
		E	9,4	18,6	28,0
	21 ve üstü	C	18	28	46
		E	15,5	30,5	46,0
Toplam			80	158	238

P=0.606 > 0.05 olduğundan anlamlı bir ilişki bulunmamaktadır. Son üç tabloya göre personelin şifre alışkanlıklarını çalışma tecrübesi değiştirmemektedir.

Tablo 37. Çalışma Yılı Sayısı * Virüs, Trojan, Spy Gibi Zararlı Yazılımlara Maruz Kalma Dağılımı

Virüs, trojan, spy gibi zararlı yazılımlara maruz kaldınız mı?			Evet	Hayır	Toplam
Çalışma yılı sayınız	0-5	C	84	30	114
		E	76,2	37,8	114,0
	6-10	C	16	8	24
		E	16,0	8,0	24,0
	11-15	C	20	6	26
		E	17,4	8,6	26,0
	16-20	C	19	9	28
		E	18,7	9,3	28,0
	21 ve üstü	C	20	26	46
		E	30,7	15,3	46,0
Toplam			159	79	238

P=0.049 < 0.05 olduğu için anlamlı bir ilişki bulunmaktadır. 6 ile 20 yıl arası çalışanlar virüsten ve benzeri zararlı yazılımlardan daha fazla etkilenmişlerdir.

Tablo 38. Çalışma Yılı Sayısı * Bilgisayarınızdaki Önemli Veri ve Bilgileri Yedekleme Oranları

Bilgisayarınızdaki önemli veri ve bilgileri yedekliyor musunuz?			Evet	Hayır	Toplam
Çalışma yıl sayınız	0-5	C	99	15	114
		E	94,8	19,2	114,0
	6-10	C	22	2	24
		E	20,0	4,0	24,0
	11-15	C	22	4	26
		E	21,6	4,4	26,0
	16-20	C	25	3	28
		E	23,3	4,7	28,0
	21 ve üstü	C	30	16	46
		E	38,3	7,7	46,0
Toplam			198	40	238

P=0.008 < 0.05 olduğundan anlam bir ilişki bulunmaktadır. 21 ve üstü yıldır çalışan personelin yedek alma alışkanlıkları daha az olduğu anlaşılmaktadır.

Tablo 39. Çalışma Yılı Sayınız * İnternet Üzerinden Alışveriş Güvenliği Hakkında Belirtilen Fikirler

İnternet üzerinden alış veriş güvenliği hakkındaki fikriniz nedir?			Güvenli buluyorum ve kulanı-yorum	Güvenli bulmuyo rum fakat kullanı-yorum.	Güvenli buluyorum ama yine de kullan-mıyorum.	Güvenli bulmuyoru m ve kesinlikle kullan-mıyorum	Topla m
Çalışma yılı sayınız	0-5	C	11	31	13	59	114
		E	11,5	32,6	12,0	58,0	114,0
	6-10	C	6	11	2	5	24
		E	2,4	6,9	2,5	12,2	24,0
	11-15	C	2	12	4	8	26
		E	2,6	7,4	2,7	13,2	26,0
	16-20	C	1	4	2	21	28
		E	2,8	8,0	2,9	14,2	28,0
	21 ve üstü	C	4	10	4	28	46
		E	4,6	13,1	4,8	23,4	46,0
Toplam			24	68	25	121	238

P=0.009 < 0.05 olduğu için anlamlı bir ilişki mevcuttur. Verilere göre; 6- 15 çalışma yılı deneyimine sahip personel internet üzerinden alış verişi güvenli bulmamalarına rağmen daha fazla kullandıkları anlaşılmıştır. 16 ve daha üstü personelin genel seçimi ise 'Güvenli bulmuyorum ve kesinlikle kullanmıyorum' şeklindedir.

Tablo 40. Çalışma Yılı Sayınız * İnternet Bankacılığı İşlemlerinin Güvenliği Hakkında Belirtilen Fikirler

İnternet bankacılığı işlemlerinin güvenliği hakkında fikrinizi belirtir misiniz?			Güvenli buluyorum ve kulanı-yorum	Güvenli bulmuyorum fakat kullanı-yorum.	Güvenli buluyorum ama yine de kullan-mıyorum	Güvenli bulmuyorum ve kesinlikle kullan-mıyorum	Toplam
Çalışma yılı sayınız	0-5	C	18	30	19	47	114
		E	19,6	39,8	13,9	40,7	114,0
	6-10	C	7	11	2	4	24
		E	4,1	8,4	2,9	8,6	24,0
	11-15	C	8	12	3	3	26
		E	4,5	9,1	3,2	9,3	26,0
	16-20	C	1	10	4	13	28
		E	4,8	9,8	3,4	10,0	28,0
	21 ve üstü	C	7	20	1	18	46
		E	7,9	16,0	5,6	16,4	46,0
Toplam			41	83	29	85	238

P=0.006 < 0.05 olduğundan anlamlı bir ilişki mevcuttur. 6 yıl üstü çalışma tecrübesine sahip personel internet bankacılık işlemlerini güvenli bulmadıklarını ama yine de kullanmak durumunda olduklarını daha yoğun belirtmektedirler. Tablodaki verilere göre; 0- 5 çalışma yılı tecrübesine sahip yeni çalışanların ise online bankacılık işlemlerini güvenli bulmadıkları ve kesinlikle tercih etmedikleri tespit edilebilmektedir.

Tablo 41. Çalışma Yılı Sayınız * İnternet Üzerinden Yapılan Yazılı, Sesli, Görüntülü Görüşmelerin Güvenilirliği Konusunda Belirtilen Fikirler

İnternet üzerinden yapılan yazılı, sesli, görüntülü görüşmelerin güvenilirliği konusunda fikriniz nedir?			Güvenli buluyorum ve kulanı-yorum	Güvenli bulmuyoru m fakat kullanı-yorum.	Güvenli buluyorum ama yine de kullan-mıyorum.	Güvenli bulmuyoru m ve kesinlikle kullan-mıyorum	Toplam
Çalışma yılı sayınız	0-5	C	13	68	13	20	114
		E	12,5	67,1	11,5	23,0	114,0
	6-10	C	3	16	1	4	24
		E	2,6	14,1	2,4	4,8	24,0
	11-15	C	2	17	5	2	26
		E	2,8	15,3	2,6	5,2	26,0
	16-20	C	2	20	1	5	28
		E	3,1	16,5	2,8	5,6	28,0
	21 ve üstü	C	6	19	4	17	46
		E	5,0	27,1	4,6	9,3	46,0
Toplam			26	140	24	48	238

P=0.106 > 0. 05 olduğu için anlamlı bir ilişki bulunmamaktadır.

Hipotez 6'da hipotez 5'ki çalışma yıl sayısının konuya yaklaşımı değiştirdiği düşüncesinden yola çıkılarak öne sürülen yaş aralığının da kamu kurumlarında yeni iletişim teknolojilerine ve bilgi- iletişim güvenliğine yaklaşımı değiştirdiği varsayımı yapılmaktadır. Fakat hipotez 4 ve 5 için yapılan ki kare analizleri hipotez 6 için uygulandığında ortaya çıkan ilişkili bir sonuç olmadığı anlaşılmaktadır. 1 – 2 çaprazlamanın dışındaki bütün testler, yaş ile konuya yaklaşım ve davranışlar arasında doğrudan bir ilişki olmadığını göstermektedir.

DÖRDÜNCÜ BÖLÜM

GENEL DEĞERLENDİRME

Bu bölümde konuyla ilgili araştırılan kaynaklardan edinilen bilgilerle ve anket çalışmasından elde edilen bulgularla sonuç değerlendirilmesi yapılarak öneriler sunulmaktadır.

Bulgular

1- Yeni iletişim teknolojileri sayesinde haberleşme ve iletişim kanalları farklılaşmıştır. Verilebilecek bazı örnekler şu şekildedir:

- Mektup ve telgraf ile iletişim yerini elektronik posta, cep telefonundan kısa mesaj, anlık ileti programları gibi elektronik ortamlarda iletişime bırakmıştır.
- Sabit telefonlar üzerinden iletişim yerine mobil (hareketli) çözümler olan cep telefonları veya internet üzerinden sesli ve görüntülü görüşme yoluyla iletişim tercihleri artmıştır.
- Gazete, dergi gibi basılı yayınlara alternatif oluşturan internet gazeteciliği ve online dergiler rağbet görmüştür.
- Tanıtım, yazıları, ilanlar ve duyurular internet ortamına taşınarak e-postalar ve web siteleri üzerinden yapılmaya başlanmıştır.

2- Kurumların iletişim teknolojilerini kullanma oranları giderek artmaktadır. Kurum yöneticileri hızlanma ve verimliği sağlamak için bazı yatırımlar yapmışlardır:

- Kurumsal iletişim ağları oluşturulmuştur.
- Personelin kullanımına bilgisayar verilmiştir.

- İhtiyaca göre otomasyonlar temin edilerek bilgi depolanması ve iletimi elektronik ortamlarda yapılmaya başlanmıştır.
- Bilgilendirme ve halkla ilişkiler çalışmaları için web siteleri oluşturulmuştur.

3- Kurumların yeni iletişim teknolojilerine geçişinde bazı sıkıntılar yaşanmaktadır. Bu sıkıntılardan en önemlileri:

- Bilgi teknolojilerinin kullanımı ve bilişim güvenliği konusunda yeterli bilgiye sahip olunmaması,
- Kağıt üzerinde ki kayıt ve bilgilerin elektronik ortama alınırken kayıpların yaşanması,
- Geleneksel yöntemlerden vazgeçemeyen personelin acemilikler yaşaması,
- Yeni yöntemlere geçilirken yeterli kurumsal desteğin alınamaması,
- Ortaya çıkan problemlere yeterince hızlı ve kalıcı çözümler getirilememesi.

4- Yeni iletişim teknolojileri beraberinde bilgi ve mesaj güvenliği sıkıntılarını getirmiştir. Kurum ağına içerden veya dışardan yapılan saldırılar, gerek personelin bireysel iletişimini gerekse kurumun özel bilgilerini tehdit etmektedir.

5- Bilgi ve iletişim güvenliği sürekli gelişen teknoloji ortamında hiçbir zaman tam olarak sağlanamamıştır. Bilgiye yönelik yapılan saldırılar sürekli var olan engelleri aşmak için geliştirildiği için yeni çözümlerin bulunması gerekmektedir.

6- Kurum yöneticileri bilgi ve iletişim güvenliğini sağlayacak alt yapı çalışmalarına yeterli yatırımı yapmamaktadır. Bilgi ve iletişim

güvenliği için gelişmiş santrallere, güvenlik duvarlarına ve saldırı tespit sistemlerine ihtiyaç duyulmaktadır.

7- Kurum personeli bilgi güvenliği hususunda yeterli eğitime sahip değildir. Yapılan ankette, kurum personelinin bilgi yetersizliği nedeniyle bilgisayarlarında virüs ve benzeri zararlı yazılımların etkilerine maruz kalma ve buna bağlı olarak bilgi kaybı yaşama oranları bir hayli yüksek çıkmıştır. Yaklaşık her 3 personelden 2'sinin zararlı bir yazılıma maruz kaldığı ve her 2 personelden 1'inin ise bilgi kaybı yaşadığı tespit edilmiştir.

8- Güvenlik açıklıkları çoğunlukla yeterli eğitime sahip olmayan veya kötü niyetli personel nedeniyle ortaya çıkmaktadır. Kurum personeli, kullandıkları bilgisayarlardan internet bankacılığı ve online alışveriş işlemlerini gerçekleştirmektedirler. Bu nedenle kurum ağı, internet korsanlarının saldırılarına birçok defa maruz kalabilmektedir. Ayrıca; kurum içinde bilgi ve menfaat elde etmek isteyen kötü niyetli çalışanlar, kullanıcı bilgisayarlarına ve sunucularına yetkisiz erişim yaparak kurumu zor durumda bırakabilmektedirler.

9- Kurum çalışanları şifre oluşturma ve muhafaza etme konusunda gerekli özeni göstermemektedir. Anket çalışmasında; şifre oluşturma ve güvenlik için şifrenin belirli aralıklarla değiştirme konusunda akademik personelin idari personele oranla daha fazla bilinçli olduğu gözlemlenmektedir.

10- Kurum çalışanlarının iletişim güvenliği sorunlarına yol açacak ve bilgi kaybına yol açacak zararlı yazılımlardan korunma hususunda yeterli bilince sahip olmadığı görülmektedir. Bu sorun öncelikle yönetimden kaynaklanmaktadır. Çünkü henüz birçok kurum antivirüs çözümü için herhangi bir çaba sarf etmemektedir. Kurum çalışanlarının ise lisansız

programlar kullandıkları ve bu programların nasıl kullanacağı konusunda yeterli bilgiye sahip olmadıkları gözlemlenmiştir.

11- Kurum çalışanlarının yeni iletişim teknolojilerine güven duymadıkları ve buna rağmen riskler göze alarak iletişim kanallarını kullandıkları ya da riskler nedeniyle yeni iletişim teknolojilerinden uzak durmaya çalıştıkları anlaşılmaktadır.

Sonuç

Bilgi çağının gereksinimlerinden birisi bilginin paylaşımıdır. Buna bağlı olarak günümüzde iletişim teknolojileri sayesinde bilginin yer değiştirmesi ve haberleşme oldukça hızlanmış ve yoğunlaşmıştır. Radyo, televizyon, telefon, bilgisayar ve internet aracılığıyla kitlesel ve kişiler arası iletişim oldukça yaygınlaşmıştır. Getirdiği kolaylıklar ve avantajlar nedeniyle kurumların da kendini adapte etmeye çalıştığı yeni teknolojik sistemler, bugün bilginin gizliliğini, bütünlülüğünü ve erişilebilirliğini tehdit eden risklerin etkisi altındadır. Bunun başlıca nedenlerinden biri bilgi hırsızlığını ve sahteciliğini yapan kişilerin var olduğu ve var olmaya devam edecek olmasıdır.

Bu tez çalışması ile aşağıda belirtilen üç ilişki sorgulanmıştır.

- ✓ Yeni iletişim teknolojileri – Kamu kuruluşları
- ✓ Kamu kuruluşları – Gelişen teknolojide bilgi ve iletişim güvenliği
- ✓ Kamu çalışanları – Bilgi ve iletişim güvenliği bilinç düzeyi

Kamu kuruluşlarında yeni iletişim teknolojilerinin kullanımıyla hiyerarşik kademeleşmeyi ve orta kademeyi azaltan ya da ortadan kaldıran, daha çok katılıma yer veren, dışa dönük, şeffaf yapıların etkinlik kazandığı öne sürülmektedir. Yeni iletişim teknolojileri kamu kurumlarının geleceği ile ilgili belirsizliklerin azaltılmasında ve geleceğe hazırlanarak etkinliğin artırılmasında önemli olanaklar sunmuştur. Yeni teknolojiler sayesinde vasıflı işgücünün

kendini göstermesi kolaylaşmış, hizmet çeşitliliği ve verimliliği artmış, örgütler hem kendi içinde ağlara oluşturmuş hem de küresel iletişim ağlarına bağlanmış, büyük kütleli bilgiler veri tabanlarında toplanarak kullanışlı hale getirilmiştir.

Kurumsal bilgi güvenliğini tehdit eden saldırıların bilinmesi, bilgi güvenliğin sağlanmasına yönelik kurumsal stratejilerin geliştirilmesinde önemli bir role sahiptir. Bilgi ve iletişim sistemlerine yönelik olan saldırılar incelendiğinde, saldırıların çok geniş bir yelpazede yapıldığı, otomatik teknikler kullanılarak saldırıların kolayca yapılmasının sağlanmasında önemli artışların görüldüğü tespit edilmiştir. Zararlı yazılım üreterek kurum ağlarına zarar vermek isteyenler daha gelişmiş araçlarla çalışmaya başlamışlardır. Bu nedenle kurumsal bilgi ve iletişim güvenliğini sağlamanın dinamik bir süreç olduğu ve süreklilik arz ettiği anlaşılmaktadır. Bu nedenle geleceğe dönük, kendini yenileyen bilgi ve iletişim güvenliği politikalarının oluşturulması gerekmektedir.

Her konuda olduğu gibi bu konuda da çözüm eğitimden geçmektedir. Yüksek seviye bir kurumsal bilgi ve iletişim güvenliği için teknoloji-eğitim-insan üçgeninde bir yönetim yaklaşımı dikkate alınmalıdır. Yöneticiler hangi oranda önemli veri kaynağına ne miktarda güvenlik yatırımı yapacağını hesap edebilmelidir. Bu hesaba yardımcı olacak teknik elemanlarda konuya gerekli önemi göstererek üstlerini teknik konularda bilgilendirmelidirler. Bilgi ve iletişim güvenliğinin en zayıf halkası olan diğer personeller ise iyi bir bilinçlendirme politikasıyla eğitilmelidir. Güvenlik ve iş yapabilirlik dengesi göz önünde tutularak personele iletişim teknolojilerini ve bilgisayarlarını kullanma konusunda sınırlı yetkiler verilmelidir.

Öneriler

- Kurumlar yeni iletişim teknolojilerini tercih ederken geleceği düşünerek, yatırım yapmalıdırlar, günü birlik çözümlerden kaçınmalıdırlar.
- Kurumlar bilgi ve iletişim güvenliği altyapısını oluştururken belli bir planlamaya gitmeli, güvenlik ve maliyet dengesini korumalıdırlar.
- Mutlaka bilgi kaynakları bir derecelendirilmeye tabi tutularak, risk değerlendirilmesi yapılmalıdır.
- Kurumlara alınan özellikle bilgi güvenliğine katkıda bulunacak teknik personelin bilgileri ve ahlaki davranışları göz önünde tutulmalıdır.
- Kurum çalışanlarının yeni iletişim teknolojilerine genelde güvensiz yaklaşımlarından dolayı bilinçlendirme çalışmaları yapılarak yeni iletişim teknolojilerine duyulan güven ve bilgi güvenliği dengesi sağlanmalıdır.
- Kriptoloji, şifre oluşturma, şifre yi belli aralıklarla değiştirme konularında personele eğitimler düzenlenmesi gerekmektedir.
- Devlet bünyesinde veya devlet desteğiyle oluşturulan bilgi ve iletişim örgütleri (Ulusal Kriptoloji Araştırma Enstitüsü, Türkiye Bilişim Güvenliği Derneği vb.) bulunmaktadır. Kurumlar bu örgütlerle yakın ilişkiler içinde olmalı bu kurumları web sitelerinden sürekli takip etmelidirler.
- Yapılan anket çalışmasında personel türleriyle ve çalışma yılı sayısıyla bilgi güvenliği bilinç düzeyinin ilişkili olduğu tespit edilmiştir. Kurumlar kendi bünyelerinde böyle anketleri veya yüz yüze görüşmeleri gerçekleştirip, sonuçlarına göre eğitim stratejisi uygulamalıdırlar.

KAYNAKÇA

Adair, J. (2003), "Etkili İletişim", Babıali Kültür Yayıncılığı, İstanbul

Anan, A. (2000), "İnternet El Kitabı", Sistem Yayınları, İstanbul.

Aras, F.E. (2004), "Basım ve Yayım Sektöründe Yeni Teknolojilere Dayalı Yeniden Yapılanma Süreci İstanbul Örneği", Gazi Üniversitesi Mühendislik Fakültesi, Cilt 19, No:1, s. 30.

Akıncı Vural, Z. B. (2005), "Bilgi İletişim Teknolojilerinin Örgütsel Yansımaları", Nobel Yayınevi, Ankara.

Atabek, Ü. (25.12.2008). "Yeni Medya ve Gelecek Yönelimleri", http://www.mediaif.emu.tr/pages/atabek/docs/yenimedya.html.

Atamer, Y. (2004), Türkiye Bilim Şurası, "İnternet ve Hukuk", İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

Atılgan, D. (09.01.2009), "İletişim Teknolojileri Çağında Değişen Bilgi Hizmetleri", http://acikarsiv.ankara.edu.tr/fulltext/864.htm.

Ayhan, A. (2002), "Dünden Bugüne Türkiye'de Bilim ve Geleceğin Teknolojileri", Beta Dağıtım, İstanbul.

Bozkurt E. (2004), "Siber Terörizm", 1. Polis Bilişim Sempozyum Kitapçığı, S.258, Ankara.

Canbek G. ,Sarıoğlu Ş. (2009), "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, s. 168- 169.

Ersoy E. (05.02.2009), "İnternette, Virüs, Spam, Bireysel Savunma", http://ab.org.tr/ab06/bildiri/11.doc, S.5- 6.

Geçikli F. (2008), "Halkla İlişkiler ve İletişim", Beta Yayınları, İstanbul

Geray, H. (2003), "İletişim ve Teknoloji", Ütopya Yayınevi, Ankara.

Gümüş, A. (2004), "İletişim Çalışmaları İçin Bilgisayar Ortamında İletişim", Değişim Yayınları, Ankara.

Housman, E. M., "The Nature of Information", Bulletin of the American Society for Information Science

Kalman S. (2003), "Web Security Field Guide", Cisco Press, S.36, Indianapolis

Karaarslan E., Akın G., Fetah V. (2008), "Kurumsal Ağlarda Zararlı Yazılımlarla Mücadele Kılavuzu", S.4, Ankara.

Lance S., Ron, L. (2002), "Surveying the Electronic Landscape: an Introduction.", Communication and Cyberspace: Social Interaction in an Electronic Environment.

Önel D. (2008), Bilgi Güvenliği bilinçlendirme süreci Oluşturma Kılavuzu, S.5-13, Gebze.

Özcan M. (2004), "Siber Terörizm", 1. Polis Bilişim Sempozyumu Kitapçığı, S.146, Ankara.

Öztürk G. (2008), Bilgi Güvenliği Politikası Oluşturma Kılavuzu, S.5, Gebze.

Pasin Ş. (2002), "Çok Algılayıcılı Saldırı tespit Sistemleri", Gebze Yüksek Tekonoloj Enstitüsü Bil. Müh. Veri ve Ağ Güvenliği Dersi Projesi, S.1.

Sevgi, L. (28.04.2009), "Değişen Dünyada Elektronik Savaşlar Bilgi Güvencesi ve Ulusal Savunma", TMMOB Elektrik Mühendisleri Odası Dergisi, Sayı:411, http://www3.dogus.edu.tr/lsevgi/.

Tağmaç H. (2004), "Siber Terörizm", 1. Polis Bilişim Sempozyum Kitapçığı, S.258, Ankara.

Telephony (2000), "Which Technologies Are Critical to an Organization's Succes?", August 21, Vol.239, Issue 8, p.34.

Timisi, N. (2003), "Yeni İletişim araçları ve Teknolojileri ve Demokrasi", Dost Kitapevi Yayınları, İstanbul

Törenli N. (2005), "Yeni Medya, Yeni iletişim Ortamı", Bilim Sanat Yayınları, Ankara

Tuğlular T. (Ekim 2003), "Üniversitelerde Bilgi Güvenliği Politikaları", Ulaknet Sistem Yönetimi Konferansı Bildiri Kitapçığı.

Türkiye Bilişim Derneği (2006), "Bilgi Sistemleri Güvenliği El Kitabı", s.4- 9, Türkiye Bilişim Derneği Yayınları, Ankara.

Türkiye Bilimsel ve Teknik Araştırma Kurumu (2004), "Ulusal Bilim ve Teknoloji Politikaları, 2003- 2023 Strateji Belgesi", Versiyon 19 (2 Kasım 2004) TÜBİTAK, Ankara

Vural Y. , Sarıoğlu Ş. (2008), "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", Gazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi, Cilt:23, No:2, S.507- 522, Ankara.

Walther, B. (1996), "Computer Mediated Communication: Impersonal, Interpersonal and Hyperpersonal Interaction.", Communication Research 23

Wang, R., Kon, H., Madnick, S. (1993), "Data Quality Requirements Analysis and Modelling", Ninth International Conference of Data Engineering, Vienna, Austria.

Wellman, C. (2004), "The Internet in the Everyday Life: An Introduction." The Internet in the Everyday Life, London

Yengin, H. (1994), Ekranın Yayınları, Der Yayınları, İstanbul.

http://www.bilgiforum.com/329102/, "GSM Nedir?", Erişim Tarihi25.04.2009

http://www.bilgiguvenligi.gov.tr/stip, "Bilişim Güvenliği", Erişim Tarihi: 2.10.2008.

http://www.babylon.com, Online Sözlük, Erişim Tarihi: 19.02.2009.

http://bilisim2023.org/index.php?option=com_content&view=article&id=83:sthbarat-ve-blg-yoenetm-2-&catid=7:goerueler&Itemid=18, "İstihbarat ve Bilgi Yönetimi II" , Erişim Tarihi: 04.05.2009.

http://www.milligorusportal.com/showthread.php? t= 26389, Erişim Tarihi: 03.04.2009

http://www.zaman.com.tr/haber.do?haberno=643716, "TRT, 31 Ocak'ta 40. yaşını kutlayacak", Erişim Tarihi: 22.02.2009.

ÖZGEÇMİŞ

Yazar, 19.07.1981 Pertek doğumlu olup Erzincan'da ikamet etmektedir. Eğitim ve öğretim sürecini Elazığ'da tamamlamıştır. Fırat Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünü 2005 yılında tamamlayarak 2007 yılında Fırat Üniversitesi İletişim Fakültesi Radyo-Televizyon ve Sinema Bölümünde yüksek lisans eğitimine başlamış ve devam etmektedir. Evli ve bir çocuk babası olup, Erzincan Üniversitesi'nde uzman olarak çalışmaktadır.

Mehmet Akif BARIŞ

EKLER

(EK-1) ANKET FORMU

Fırat Üniversitesi Sosyal Bilimler Enstitüsü, Radyo - TV- Sinema Bölümü Yüksek Lisans (Master) programı çerçevesinde "**Erzincan Üniversitesi'nde Bilgi Ve İletişim Güvenliği**" konulu tez çalışmamın temelini oluşturacak bilgilere ulaşmak amacıyla tarafımızca hazırlanan soru kağıdı sunulmaktadır. Sizlerin kişisel ve mesleki nitelikteki bilgi, tecrübe ve görüşlerinden yararlanmaksızın böyle bir çalışmanın başarılı olmasının mümkün olamayacağını özellikle belirtmek isterim. Sorulardan hiçbiri herhangi bir şekilde kişisel değerlendirmeler yapmak ya da kişi ile ilgili bir takım özellikleri ortaya çıkarmak gibi bir amaç taşımamaktadır. Ankete katılımınızdan dolayı teşekkür ederim.

M. Akif BARIŞ

1- Cinsiyetiniz
[ ] Erkek [ ] Kadın

2- Yaşınız
[ ] 20- 25 [ ] 26 - 30 [ ] 31 – 40 [ ] 41 – 50 [ ] 51 ve üstü

3- Personel Türü
[ ] Akademik [ ] İdari

4- Çalıştığınız Birim
[ ] Rektörlük [ ] Enstitüler [ ] Fakülte [ ] Yüksek Okullar [ ] Meslek Yüksek Okulları

5- Unvanınız
[ ] İşçi [ ] Memur [ ] İşletmen [ ] Teknisyen [ ] Tekniker
[ ] Mühendis [ ] Yönetici [ ] Uzman [ ] Okutman [ ] Arş. Gör.
[ ] Öğr. Gör. [ ] Yrd. Doç. [ ] Doç. [ ] Prof.

6- Medeni Haliniz
[ ] Evli [ ] Bekâr

7- Çalışma Yılı Sayınız
[ ] 0 - 5 [ ] 6 - 10 [ ] 11 - 15 [ ] 16 - 20 [ ] 21 ve üstü

8- Bilgisayar kullanarak çalışma yılınız
[ ] 0 - 5 [ ] 6 - 10 [ ] 11 - 15 [ ] 16 - 20 [ ] 21 ve üstü

9- İnternet kullanarak çalışma yılınız
[ ] 0 - 5 [ ] 6 - 10 [ ] 11 - 15 [ ] 16 - 20 [ ] 21 ve üstü

10- Kendinize ait bilgisayarınız var mı?
[ ] Evet [ ] Hayır

11- Evinizde internetiniz var mı?
[ ] Evet [ ] Hayır

12- E-Posta hizmetlerini (hotmail, gmail gibi) kullanıyor musunuz?
[ ] Evet [ ] Hayır

13- Anlık ileti programlarını (msn, yahoo Messenger gibi) kullanıyor musunuz?
[ ] Evet [ ] Hayır

14- İnternet üzerinden görüntülü ve sesli görüşmeler yapıyor musunuz?
[ ] Evet [ ] Hayır

15- Kurumunuza ait web üzerinden otomasyon kullanıyor musunuz?
[ ] Evet [ ] Hayır

16- Kurumunuz ağında çalışan otomasyon kullanıyor musunuz?
[ ] Evet [ ] Hayır

17- Kurumunuza bağlı bir web posta adresi (@erzincan.edu.tr uzantılı) kullanıyor musunuz?
[ ]Evet [ ] Hayır

18- İnternet üzerinden forumlara ve gazete haberlerine yorum yazıyor musunuz?
[ ] Evet [ ] Hayır

19- Web ortamındaki e-devlet (TCNO sorgulama, vergi borcu ve kredi borcu sorgulama gibi) işlemlerinden faydalanıyor musunuz?
[ ] Evet [ ] Hayır

20- İnternet üzerinden alış veriş yapıyor musunuz?
[ ] Evet [ ] Hayır

21- İnternet üzerinden kredi kartı bilgilerinizi girerek alışveriş yapıyor musunuz?
[ ] Evet [ ] Hayır

22- İnternet bankacılığı işlemlerini kullanıyor musunuz?
[ ] Evet [ ] Hayır

23- Üyelik isteyen internet sitelerine bütün bilgilerinizi girerek üye olur musunuz?
[ ] Evet [ ] Hayır

24- Cep telefonunuza ait online işlemleri internetten yapıyor musunuz?
[ ] Evet [ ] Hayır

25- İşletim sisteminiz için giriş şifresi kullanıyor musunuz?
[ ] Evet [ ] Hayır

26- Kullandığınız otomasyonlar için giriş şifresi oluşturuyor musunuz?
[ ] Evet [ ] Hayır

27- Tüm online işlemleriniz için yeterince karmaşık şifreler oluşturuyor musunuz?
[ ] Evet [ ] Hayır

28- Şifrelerinizi yeterince sık değiştiriyor musunuz?
[ ] Evet [ ] Hayır

29- Kurumdaki bilgisayarınızda antivirüs programı kullanıyor musunuz?
[ ] Evet [ ] Hayır

30- Kurumdaki bilgisayarınızda kişisel güvenlik duvarı kullanıyor musunuz?
[ ] Evet [ ] Hayır

31- Kötü niyetli mailler aldınız mı ve bilgisayarınıza zarar verdi mi?
[ ] Evet [ ] Hayır

32- Kötü niyetli anlık ileti aldınız mı ve bilgisayarınıza zarar verdi mi?
[ ] Evet [ ] Hayır

33- E-posta ve benzeri internet kullanım şifreleriniz kötü niyetli kişiler tarafından ele geçirildi mi?
[ ] Evet [ ] Hayır

34- Virüs, trojan, spy, gibi zararlı yazılımlara maruz kaldınız mı?
[ ] Evet [ ] Hayır

35- Bilgisayarınızda ki önemli veri ve bilgilerinizi yedekliyor musunuz?
[ ] Evet [ ] Hayır

36- Bilgisayarınızdaki veri ve bilgilerin kaybolması veya bozunması olaylarına maruz kaldınız mı?
[ ] Evet [ ] Hayır

37- İnternet üzerinden kredi kartı ve hesap bilgileriniz kötü niyetli kişiler tarafından ele geçirildi mi?
[ ] Evet [ ] Hayır

38- Günümüz iletişim teknolojilerinden hangisini daha güvenilir buluyorsunuz?
[ ] Telefon [ ] SMS [ ] İnternet üzerinden görüşmeler.
[ ] Hiçbiri [ ] Hepsi

39- İnternet Bankacılığı işlemlerinin güvenilirliği konusunda fikrinizi belirtir misiniz?
[ ] Güvenli buluyorum ve kullanıyorum.
[ ] Güvenli bulmuyorum fakat kullanıyorum.
[ ] Güvenli buluyorum ama yinede kullanmıyorum.
[ ] Güvenli bulmuyorum ve kesinlikle kullanmıyorum.

40- İnternet üzerinden alış veriş güvenliği konusunda fikriniz nedir?
[ ] Güvenli buluyorum ve kullanıyorum.
[ ] Güvenli bulmuyorum fakat kullanıyorum.
[ ] Güvenli buluyorum ama yinede kullanmıyorum.
[ ] Güvenli bulmuyorum ve kesinlikle kullanmıyorum.

41- İnternet üzerinden yapılan yazılı, sesli ve görüntülü görüşmelerin güvenilirliği konusunda fikriniz nedir?
[ ] Güvenli buluyorum ve kullanıyorum.
[ ] Güvenli bulmuyorum fakat kullanıyorum.
[ ] Güvenli buluyorum ama yinede kullanmıyorum.
[ ] Güvenli bulmuyorum ve kesinlikle kullanmıyorum.

42- Güvenli iletişim konusundaki fikir ve önerilerinizi kısaca özetler misiniz?

[_____

_____

_____]