Ülke Bilgi Güvenliği

Yılmaz VURAL, Şeref SAĞIROĞLU

***Özet*— Kişisel ve kurumsal düzeyde stratejik bilgileri içeren ülke bilgi sistemleri, güvenlik tehditlerine karşı korunmalıdır. Ülke bilgi sistemlerimizde bilgilerin üretilmesi, işlenmesi, iletilmesi, depolanması ve paylaşılmasına bağlı olarak oluşabilecek güvenlik ihlallerini en aza indirgemek için kişisel ve kurumsal seviyede alınması gereken güvenlik önlemleri her geçen gün artmaktadır. Bu çalışmada, ülke bilgi güvenliğinin yüksek seviyede sağlanması için kurumsal ve kişisel bilgi güvenliğinin önemi, en zayıf halka olan insan faktörünün iyileştirilmesi için eğitimin önemi ve güvenlik süreçlerinin iyileştirilmesini sağlayan güvenlik testleri incelenmiştir. Son olarak ülke bilgi güvenliği hakkında genel değerlendirmeler yapılarak öneriler yapılmıştır.**

***Anahtar*— Bilgi güvenliği, kişisel bilgi güvenliği, kurumsal bilgi güvenliği, güvenlik testleri, ülke bilgi güvenliği**

***Summary*— National Information Systems that consist of strategic information at personal and enterprise level must be protected against threats. Personal and enterprise level security precautions are increasing day by day in order to decrease probable security threats that occur as a result of information being produced, processed, transferred, stored and shared on national information systems. In this paper, importance of personal and enterprise information security in order to provide national information security, importance of information security education and awareness in order to improve human factor which is the weakest link of security life cycle and security tests supplying improvements of security processes have been examined. Finally some evaluations about national information security have been performed.**

***Keywords*— Information security, enterprise information security, personal security, security testing, national information security**

I. GİRİŞ

Bilgi sistemlerinin kurumsal veya kişisel düzeyde kullanımının yaygınlaşması sonucunda hayatımız kolaylaşırken güvenliği yüksek seviyede sağlanan bilgi sistemlerine duyulan ihtiyaçlar da aynı oranda artmaktadır [1]. Ağ destekli bilgi sistemleri üzerinden haberleşen, sayıları hızla artan ve geniş kitlelerce ülke çapında kullanılan uygulamalar üzerinde tutulan bilgilerin değeri düşünüldüğünde bilgi güvenliğinin sağlanmasının önemi daha iyi anlaşılacaktır.

Ş. SAĞIROĞLU, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Ankara, ss@gazi.edu.tr

Y. VURAL, STM A.Ş., Ankara, yvural@stm.com.tr

Ayrıca geliştirilen yeni uygulamaların da beraberinde yeni güvenlik tehditlerini getirdiği düşünüldüğünde bilgi güvenliğinin sağlanmasının her geçen gün daha da zorlaştığı anlaşılacaktır.

Kamu veya özel kuruluşlara ait ağ destekli bilgi sistemlerinin birbirleriyle etkileşimi her geçen gün artmakta ve bu sistemler ülke bilgi sistemlerinin altyapısını oluşturmaktadır. Ülke bilgi sistemleri ülke güvenliği açısından önemli olan stratejik ülke bilgilerinin, ilgili kurumların kendi içinde veya başka kurumlar arasında paylaşılmasını ve kullanılmasını sağladığından ülke bilgi sistemlerinin güvenliğinin yüksek seviyede sağlanması ülke güvenliği açısından önemlidir.

Kişilerin ve kurumların sahip oldukları önemli bilgilerin yer aldığı ülke bilgi sistemleri istihbarat veya terör amaçlı yapılabilecek siber saldırılara karşı yüksek seviyede korunması gerekmektedir. Ülke bilgi güvenliğini tehdit eden unsurlar sadece elektronik ortamlarda yapılan saldırılarla sınırlı değildir. İnsan hataları, yangın, sel, deprem, terör saldırıları, sabotaj gibi istenmeyen olaylar veya doğal felaketler sonucunda da bilgiler ve bilgi sistemleri tamamen ya da kısmen zarar görmektedir. Ayrıca korunmasızlığın yanında korunma seviyesinin iyi belirlenememesi ve etkin güvenlik önlemlerinin alınamaması da beraberinde maliyet, performans ve verimsizlik gibi önemli diğer sorunlara yol açmaktadır.

Günümüzde elektronik ortamlarda meydana gelen güvenlik ihlâllerinden hemen hemen her gün bahsedilmektedir. Bu ihlallerden bir tanesi olan ve ülke bilgi güvenliği açısından önemli bir örnek olan "Estonyanın ülke bilgi sistemlerine karşı yapılan dağıtık temelli hizmet aksattırma saldırıları" sonucunda 1,3 milyonluk nüfusa sahip Estonya'daki kamu, banka ve medya internet siteleri, Rusya kaynaklı yüz binlerce bilgisayardan yapılan geniş kapsamlı, eşgüdümlü ve uzun süreli saldırılar sonucu çökertilmiş ve Estonyada hayat durma noktasına gelmiştir [2]. Bu saldırı devletler arasında yaşanan ilk siber soğuk savaş olarak tarihe geçmiştir.

İnternet güvenlik şirketi McAfee firmasının 2007 yılı sonunda hazırladığı raporda gelecek on yılda dünyada güvenliğe ilişkin en büyük tehditlerden birinin, ülkeler arasında bilgi sistemleri üzerinde yaşanacak siber soğuk savaşların olduğu belirtilmiştir. Raporda yaklaşık 120 ülkenin, mali piyasalar, resmi bilgisayarlar sistemleri ve kamu hizmetleri alanında interneti kullanmak için çözümler geliştirdiğini ve istihbarat örgütlerinin diğer devletlerin ülke bilgi sistemlerini sürekli sınayarak zayıf noktalarını bulmak için yeni teknikler geliştirildiği vurgulanmıştır [3].

Bu ve benzeri siber tehditlerden ülke düzeyinde etkilenmeyi en aza indirmek için kurumsal ve kişisel düzeyde alınması gereken önemli güvenlik tedbirleri vardır. Ülke bilgi güvenliğinin aşamalarını oluşturan kurumsal ve kişisel bilgi güvenliğinin yüksek düzeyde sağlanması, ülke bilgi güvenliği politikalarının oluşturulması, yapılması gerekenler arasında ilk sırada gelmektedir. Kullanıcıların kişisel bilgi güvenliği konusunda bilinçli olmaları gerekirken, kurumların kurumsal bilgi güvenliği konusunda önlemler almaları ise yapılması gereken önemli görevler arasındadır [4].

Bu çalışmada takip eden bölümlerde stratejik ülke bilgilerinin yer aldığı ülke bilgi sistemleri açıklanmış, ülke bilgi sistemlerinin güvenliğinin sağlanmasında önemli aşamalar olan kişisel ve kurumsal bilgi güvenliği konuları ayrı başlıklar altında ele alınmış ve takip eden bölümlerde güvenlik testleri ve eğitimin önemi üzerinde durulmuştur. Son olarak ülke bilgi güvenliği konusunda değerlendirmeler yapılmış ve öneriler sunulmuştur.

II. Ülke Bilgi Sistemleri

Bilgi genellikle, bireyler veya kurumlar tarafından bir sorunun çözümü, herhangi bir çalışmanın başlatılması ya da bitirilmesi gibi faaliyetler sonucunda ortaya çıkarılan anlamlandırılmış verilerin bütününü ifade etmektedir. Bilgi kelimesinin menşei, Latincedeki herhangi bir şeye şekil vermek anlamına gelen "informare" kelimesinden gelmektedir [5]. Sözlük anlamıyla bilgi; "Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü" olarak tanımlanmaktadır [6]. Bilgi sistemleri donanımlar, yazılımlar, iletişim teknolojileri ve insan gibi alt bileşenlerden meydana gelmektedir. Bilgiler, bilgi sistemleri aracılığıyla üretilmeye, işlenmeye, taşınmaya ve depolanmaya başladıkça güvenlik tehditleri ve alınması gereken önlemler ise artarak farklılık göstermeye başlamıştır.

Ülke bilgi sistemleri bireylerden kurumlara kadar değişik seviyelerde ağ destekli ortamlarda bilginin yönetilmesi, iş verimliliğin ve bilgi akışlarının hızlandırılması, bireyler ve kurumlarla daha hızlı iletişimin kurulabilmesini sağlayan ulusal ve uluslararası kullanımı olan sistemlerdir [7]. Ülke Bilgi Sistemleri sayesinde ağ destekli ortamlarda bilginin üretilmesi, işlenmesi, taşınması ve saklanması sağlanarak bilgiye mekândan bağımsız olarak istenilen ortamlardan erişilmesi ve paylaşılması sağlanmıştır. Nüfus Vatandaşlık İdaresi MERNİS, Maliye İnternet Vergi Dairesi, Sosyal Güvenlik Kurumu Bilgi Sistemi, Meteoroloji Bilgi Servisleri, Coğrafi Bilgi Sistemleri ve Banka Bilgi Sistemleri ülke bilgi sistemlerimize ilk bakışta örnek olarak gösterilebilir.

Ülke bilgi sistemlerimizin birlikte çalışabileceği Ulusal Bilgi Sistemi ile ilgili çalışmalara ülkemizde devam edilmektedir. Ulusal Bilgi Sistemi ülke yönetimine yönelik stratejik bilgilerin ilgili kurumlar arasında ilişkilendirilmesi, paylaşılması ve yönetilmesini amaçlayan ülke bilgi sistemleri topluluğudur [8]. Ulusal Bilgi Sisteminin kurulmasıyla birlikte kurumsal bilgi sistemleri sistemlerin sistemi yaklaşımıyla ağ destekli bir ortamda birlikte çalışabilirlik kabiliyeti kazanacaktır.

Sistemlerin sistemi, birbirinden farklı sistemlerin tek başlarına gerçekleştiremeyecekleri işlevleri yapabilmek için ağ destekli ortamları kullanarak birbirleriyle uyumlu ve etkin şekilde çalışabilmesiyle oluşan sistemler kümesi olarak tanımlanmaktadır [9]. Sistemlerin sistemine verilebilecek en güzel örnek Internet'dir. İnternet yıllar içinde gelişmiş, yaygınlaşmış ve günümüzde dünyaya yayılmış bir bilgi sistemleri topluluğu haline gelmiştir.

Ulusal bilgi sisteminin bu yaklaşım çerçevesinde oluşturulması sonucunda kazanılacak bir çok olumlu kabiliyetin yanında güvenlik, performans ve yönetim gibi temel sorunlarında dikkate alınması ve çözümlenmesi gerekmektedir. Tüm bu sorunların çözümünde ise bilgi güvencesi (information assurance) kavramı ön plana çıkmaktadır.

Bilgi güvencesi bilginin güvenliği, performansı ve yönetimi gibi temel konuların birlikte çözümlenmesini sağlayan çözümler kümesi olarak tanımlanmaktadır [10]. Bilgi güvencesi sayesinde ülke bilgi sistemlerinin ağ ve bilgi altyapılarının bütünleşmesi sağlanacaktır. Bilgi güvencesi kurumsal bilgi sistemlerinin birlikte çalıştığı ülke bilgi sistemlerinin tamamında sağlanmalıdır. Ülke bilgi güvenliğinin yüksek seviyede sağlanabilmesi için kurumsal bilgi güvenliğinin ülke genelinde yeterli koruma seviyesinde sağlanması önemlidir. Bundan dolayı takip eden bölümde kurumsal bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik açıklamalar yapılmıştır.

III. Kurumsal Bilgi Güvenliği

Kurumsal bilgi, kurum içinde üretilen veya kuruma dışarıdan gelen, o kurumla ilgili kayıtlı ya da kayıtsız her türlü bilgiyi ifade etmektedir. Kurumsal bilgi, bireysel bilgilerin toplamının yanı sıra, diğer kurumlar tarafından kolayca taklit edilemeyecek şekilde insan, teknoloji ve yönetim ilkeleri arasında üretilen bilgi kaynaklarını ifade etmektedir [11].

Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde iletilmesi süreci bilgi güvenliği olarak tanımlanmaktadır [12]. Kurumsal bilgi güvenliği ise, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerinin alınması ve güvenlik süreçlerinin standartlara göre yönetilmesidir [13].

Kurumsal bilgi güvenliği, ülke bilgi güvenliğinin sağlanmasında önemli bir aşamadır. Kurumsal bilgi güvenliği sağlanmadıkça, ülke bilgi güvenliği sağlanamayacaktır. Kurumsal Bilgi güvenliğinin sağlanması, planlanması, tasarlanması, gerçekleştirilmesi, işletilmesi, izlenmesi, denetlenmesi, sürdürülmesi ve geliştirilmesi için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası

Kurumsal Bilgi Güvenliği Yönetim Sistemi (KBGYS) olarak tanımlanmaktadır [14].

Kurumlar açısından önemli bilgilerin ve bilgi sistemlerinin korunabilmesi, risklerin en aza indirilmesi ve sürekliliğinin sağlanması, KBGYS'nin kurumlarda hayata geçirilmesiyle mümkün olmaktadır. KBGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

Sadece teknik önlemlerle (güvenlik duvarları, atak tespit sistemleri, antivirüs yazılımları, anticasus yazılımlar, şifreleme, vb.) kurumsal bilgi güvenliğinin sağlanması mümkün değildir. KBGYS; insanları, süreçleri ve bilgi sistemlerini içine alan ve üst yönetim tarafından desteklenen bir yönetim sistemidir. Kurumsal bilgi güvenliği insan, eğitim, teknoloji gibi birçok faktörün etki ettiği yönetilmesi zorunlu olan karmaşık süreçlerden oluşmaktadır.

Kurumsal Bilgi Güvenliği sadece teknoloji problemi olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir [15]. Kurumlarda insan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan üst yönetime kadar farklı kademelerde çalışan insanların ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür. Kurumun stratejik hedeflerini belirleyen en üst seviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek çok önemlidir. Bilgi güvenliğinin sağlanması için gerekli olan idari ve mali kararların verilebilmesi amacıyla yönetim tarafından bilgi güvenliği birimi kurulmalıdır. Bu birim tarafından güvenlikle ilgili stratejik kararlar zamanında ve doğru bir şekilde alınmalıdır. Yönetim tarafından bilgi güvenlik biriminin kurulması ve etkin bir yapıda çalışması yönetimin kurumsal bilgi güvenliğini sahiplendiğinin ve desteklediğinin önemli bir göstergesidir.

Kurumsal bilgi güvenliğinin üst seviyede sağlanmasına yönelik süreçlerinin oluşturulması, yönetilmesi ve yapılandırılması amacıyla yapılan standartlaşma çalışmaları dünyada ve ülkemizde hızla sürmektedir. Standartlaşma konusuna öncülük eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul görerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir [16].

Kurumsal bilgi güvenliğinin sağlanması ülke bilgi güvenliğinin yüksek seviyede sağlanması için önemli bir aşama olmasına rağmen tek başına yeterli değildir. Ülke bilgi güvenliğinin yüksek seviyede sağlanması için ülke bilgi sistemlerini kullanan son kullanıcıların güvenliği yani kişisel bilgi güvenliği de sağlanmalıdır. Bundan dolayı takip eden bölümde kişisel bilgi güvenliğinin yüksek seviyede sağlanmasına yönelik açıklamalar yapılmıştır.

IV. İNSAN FAKTÖRÜ (KİŞİSEL BİLGİ GÜVENLİĞİ)

Çalışma kapsamında incelenen, bilgi güvenliğiyle ilgili yapılan raporlar, anketler, kitaplar ve makalelerde bilgi güvenliğinin sağlanmasındaki en zayıf halkanın insan faktörü olduğu gösterilmiştir [17-23].

İnsan faktöründen kaynaklanan zafiyetlerin saldırganlar tarafından kullanılması, teknolojik olarak tüm güvenlik tedbirlerinin alınmasına rağmen bilgi güvenliği ihlallerinin yaşanmasına neden olacaktır. Bu ihlaller ülke bilgi güvenliği açısından önemli sorunlara yol açacaktır.

Kişisel bilgi güvenliğini tehdit eden, insan faktöründen kaynaklanan hatalar ve alınması gereken önlemlerden bazıları aşağıda başlıklar halinde özetlenmiştir.

Güvenlik politikaları ihlali: Bilgi Sistemlerindeki bilgilere erişim hakkı olan her kullanıcının yöneticiler tarafından onaylanan Bilgi Güvenliği politikalarına uyması gerekmektedir. Güvenlik politikaları son kullanıcılar tarafından çoğu zaman bilerek veya bilmeyerek ihlal edilmektedir. Güvenlik politikalarının ihlal edilme sebeplerinin başlıcaları, kullanıcı alışkanlıkları, uygulanamayacak yaptırımlar, bilinçsizlik olarak tespit edilmiştir. Politika ihlallerinin önüne geçebilmek için kullanıcıların genel bilgi güvenliği konusunda eğitilmesi ve güvenlik politikalarının uygulanabilir ifadeler içermesi gerekmektedir.

Bilgi aktarımı: İnsanlar genellikle tanımadıkları kişilere sohbet esnasında birçok önemli bilgiyi farkında olmaksızın iletmektedir. Hiçbir kullanıcı ortam fark etmeksizin (e-posta, telefon, faks, yüzyüze, vb.) kimliğinden emin olmadığı kimselere hiçbir konuda bilgi vermemelidir. Örneği hiçbir teknoloji kullanılmadan bir kurum çalışanlarından alınacak bilgilerle tüm kurumsal bilgi güvenliği kontrollerinin aşılabileceği hiçbir zaman unutulmamalıdır. Başlangıçta önemsiz gibi görünen küçük bilgiler bir araya geldiğinde, içinde gizli bir bilgiyi barındıran ciddi bir güvenlik açığına dönüşebileceğine dair örnekler her geçen gün artmaktadır. Bilinmeyen kişilere bilgi aktarılmaması için kullanıcıların özellikle sosyal mühendislik konusunda eğitilmesi gerekmektedir.

Şifrelerin kâğıtlara yazılması: Şifreleme politikaları, kırılması güç olan şifrelerin kullanıcılar tarafından kullanılmasını ve düzenli aralıklarla bu şifreleri değiştirilmesini zorunlu kılmaktadır. Şifrelerin güçlü olması, içerdiği karakterlerin karmaşıklığıyla doğru orantılıdır. Güçlü şifrelerin kullanılmasıyla birlikte kullanıcıların bu şifreleri hatırlama problemleri ortaya çıkmaktadır. Kullanıcılar, bu durumda şifrelerini hatırlayabilmek amacıyla görebilecekleri bir yere şifrelerinin yazılı olduğu kâğıdı asmaktadır. Bu durum ilgili kullanıcı şifresinin kötü niyetli başka bir kişi tarafından okunarak kullanılmasıyla güvenlik ihlalinin oluşmasına sebep olacaktır. Bu durumların meydana gelmemesi için kullanıcılara şifre seçimi ve hatırlanmasıyla ilgili eğitimler verilmelidir.

Güvenilir olmayan yazılımların kullanımı: Güvensiz yazılımlar illegal olarak kopyalanmış veya internetteki

güvenilir olmayan sitelerden indirilmiş, lisanssız yazılımlar olup içerisinde bilgisayara zarar verebilecek virüs, truva atı, tuş kaydedici ve her türlü kötü amaçlı yazılımları barındırabilen programlardır. Güvenilir olmayan yazılımlar, ziyaret edilen web sitelerinin kayıtlarını tutarak başkalarına gönderen, istenmeyen reklâm pencerelerinin gelmesini sağlayan, bilgisayar içerisinde yer alan kişisel dosyaları başkalarına gönderebilen, bilgisayarın performansını düşüren ve internet erişimini gereksiz yere meşgul eden istenmeyen yazılımlardır. Güvenilir olmayan yazılımların kullanımı sonucunda, birçok güvenlik ihlali meydana gelmektedir. Bu tür ihlallerin önüne geçebilmek için kullanıcılara güvenilir olmayan yazılımların ne olduğu ve bu yazılımlardan nasıl korunulacağı konusunda eğitimler verilmelidir.

Bilgisayarların fiziksel güvenliğinin sağlanmaması: Genellikle kullanıcılar koruma önlemi almaksızın bilgisayarlarının başından ayrıldığında kötü niyetli insanlar bu durumu değerlendirerek bilgisayarı zararlı amaçlar için kullanmakta ve güvenlik ihlalleri meydana gelmektedir. Fiziksel güvenlik zafiyetinden faydalanarak bilgisayarı kullanan kötü niyetli kişi gizli bilgiler içeren dosyaları dışarıya e-posta aracılığıyla gönderebilir, bilgisayar üzerindeki bilgileri silebilir, değiştirebilir ve o anki kullanıcının yetkisi ölçüsünde birçok işlemi kötücül amaçlar için yapabilir. Bilgisayarların fiziksel güvenliğinin sağlanmasıyla ilgili olarak; kullanıcılar bu konuda bilinçlendirilmeli bilgisayarların başından ayrılan kullanıcıların en azından parola korumalı ekran koruyucusu kullanmaları bilgisayarlara fiziksel olarak yapılabilecek saldırıların en aza indirgenebilmesi açısından önem arz etmektedir.

Bilgisayarların yönetici hakkıyla açılması: Kullanıcılar kurum içerisinde kendilerine tahsis edilmiş olan kişisel bilgisayarlarını, herhangi bir kısıtlama olmaksızın kullanmak amacıyla genellikle yönetici haklarına sahip olan hesaplarla kullanmaktadırlar. Bu durum, bilgi güvenliğinin sağlanmasında önemli ilkelerden biri olan "en az yetki" prensibinin (principle of least privilege) ihlali anlamına gelmektedir. Yönetici haklarına sahip bir hesapla bir kullanıcının bilgisayarında oturum açılması, güvenlik ihlali meydana geldiğinde bilgisayar üzerinde yönetici işlemlerini yapma yetkisine sahip olacağından güvenlik ihlalinin etkisi çok daha büyük olacaktır. Bu tür ihlallerin etkisini azaltmak için kullanıcıların ihtiyaçlarını karşılayacak kısıtlı haklara sahip olan hesaplar tanımlanmalı ve bu hesaplarla kullanıcıların oturum açmaları zorunlu hale getirilmelidir. Bu önleme ek olarak kullanıcılara yönetici haklarına sahip hesaplarla oturum açmalarının gereksizliği ve zararları anlatılarak, kısıtlı haklara sahip olan hesapları kullanmaları yönünde özendirici ve bilgilendirici eğitimler verilmelidir.

Bilinçsiz e-posta kullanımı: Kurum çalışanları tarafından kullanılan iletişim araçlarının başında e-posta gelmektedir. Günümüzde kötücül yazılımlar çoğunlukla e-postalar aracılığıyla yayıldığından, e-posta kullanımının önemi artmıştır. Bilinçsiz e-posta kullanımı sonucunda bilgi güvenliği ihlalleri meydana gelmektedir. Kullanıcıların tanımadığı kişilerden gelen şüpheli e-postaları açmaması, e-posta eklerini virüs taramasından mutlaka geçirmesi, e-posta aracılığıyla kişisel gizli bilgilerini (internet bankacılığı hesap bilgilerini, kimlik bilgileri, kullanıcı hesap bilgileri) kimseye vermemesi gibi e-posta kullanımında dikkat edilmesi gereken hususlar konusunda kullanıcılar bilinçlendirilmeli ve eğitilmelidir. Bu eğitimler sonucunda e-posta kullanımından kaynaklanacak zafiyetler en aza indirgenecektir.

Genel anlamda bilgi güvenliğinin sağlanmasında en zayıf halka olan insan faktöründen meydana gelen zafiyetlerin giderilmesinde eğitim önemli bir rol oynadığından ülke bilgi güvenliğinin sağlanmasında eğitimin önemi ayrıntılı olarak takip eden bölümde incelenmiştir.

V. EĞİTİM

Ülke bilgi güvenliğinin sağlanması açısından önemli olan eğitimler ve bilinçlendirmeler farklı yöntemlerle ülke bilgi sistemlerini her seviyede kullanan kişilere düzenli olarak verilmelidir. Bu yöntemler bilinçlendirmeler, toplantılar, web üzerinden eğitimler, e-posta yoluyla kullanıcılara bildirimler, yazılar ve duyurular, seminerler, bültenler ve güvenlik posterleri şeklinde olabilir.

İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bilgi güvenliği eğitimleri riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. Farklı bilgi seviyesindeki insan gruplarının, bilgiyi ve bilgi kaynaklarını koruma konusunda üzerilerine düşen sorumlulukları anlaması ve yerine getirmesi, bilgi güvenliğinin sağlanması ve insan faktöründen kaynaklanan zafiyetlerin en aza indirgenmesi açısından kritik bir öneme sahiptir.

Bilgi güvenliği eğitimlerinin temel hedefi, bilgi kaynaklarının gizlilik, bütünlük ve erişilebilirliğin sağlanması konusunda yapması gereken görev ve sorumluluklar konusunda insanları eğitmektir. Bilgi güvenliği eğitimleriyle insanlar sadece bilginin korunması konusunda nasıl katkı sağlayabileceklerini değil aynı zamanda bilginin neden korunması gerektiğini de öğrenmelidir. Çalışanlar hatalı davranışlarının ülke bilgi güvenliği üzerinde yaratabileceği etkiyi eğitimler aracılığıyla açıkça anlamalıdır. Kullanıcı bilinçlendirme çalışmaları, güvenlik ihlallerinin maliyetini azaltmaya ve kontrollerin kurumun tüm bilgi kaynakları üzerinde dengeli uygulanmasına yardımcı olacaktır.

Güvenlik farkındalık eğitimlerinin amacı, güvenlik ve güvenlik kontrollerinin önemi hakkında ülke bilgi sistemleri kullanıcılarında ortak bir bilinç oluşturulmasıdır [24]. Bilinçlendirme mesajları basit ve açık olmalı, bilinçlendirme eğitimleri insan gruplarının anlayabileceği basit bir formatta verilmelidir.

Çoğu kurumda güvenliğin sağlanması için yapılması gereken kısıtlamaların kullanıcıların alışkanlıklarıyla ters düşmesinden dolayı güvenlikle ilgili yaptırımların uygulanmasında geç kalınmaktadır. Güvenlik uygulamaları başından itibaren uygulanamadığından zamanla her kullanıcının, güvenliğe dikkat etmeksizin farklı kullanım alışkanlıkları edindiği görülmüştür. Bu durum bilgi güvenliği

bilinçlendirme eğitiminin uygulanmasını zorlaştırarak, kullanıcılarda güvenlik uygulamalarına karşı direnç oluşmasını sağlamaktadır. Çünkü sadece kullanıcıları eğitmek değil aynı zamanda eski alışkanlıklarından kurtarmak gerekmektedir.

Kullanıcılara göre kurum güvenlik önlemleri olmaksızın bugüne kadar gayet iyi çalışmıştır ve hiçbir sorunla karşılaşmamıştır. Yeni güvenlik önlemleri hayatı zorlaştırıcı gereksiz değişiklikler olarak görülür. Bilinçlendirme eğitimleri güvenlikle ilgili bilgi vermenin yanında kullanıcı alışkanlıklarından nasıl kurtarılacağı göz önüne alınarak hazırlanmalı akıcı ve eğlenceli bir içerikle kullanıcılara sunulmalıdır.

Çalışma kapsamında yapılan araştırmalarda çoğu kurumda güvenlik bilinçlendirme programının olmadığı görülmüş, olan kurumlarda ise genellikle kullanıcıları bilgi güvenliğinin neden önemli olduğu konusunda eğitmeyi başaramadığı tespit edilmiştir. Eğitimin başarılı olabilmesi için kullanıcıların kafasındaki neden sorusunun cevabı kullanıcıyı ikna edecek şekilde verilmelidir Başarılı bir eğitim sonrasında kullanıcıların şifreleme politikasına sahip çıkarak yeni politikanın uygulanmasında gayretli olacakları görülecektir. Pek çok kullanıcı, bilgi ve bilgi kaynaklarının korunmasının önemi konusunda yeterli bilgiye sahip değildir. İyi tasarlanmış ve sonuçlandırılmış bilinçlendirme ve eğitim çalışması güvenlik zincirinin en kırılgan halkası olan insan faktörünün güçlendirilmesine büyük katkı sağlayacaktır.

Ülke Bilgi Güvenliğinin sağlanmasındaki kurumsal ve kişisel bilgi güvenliği aşamalarından sonra insan faktöründen kaynaklanan zafiyetleri en aza indirgeyen eğitim unsuru üzerinde durulmuştur. Ülke bilgi güvenliği süreçlerinin işlerliğinin kontrol edilebilmesi için güvenlik testlerine ihtiyaç duyulduğundan güvenlik testleri takip eden bölümde açıklanmıştır.

VI. Güvenlik Testleri

Ülke Bilgi Güvenliğinin sağlanmasında temel unsurlar olan insan faktörü ve eğitim önceki bölümler içerisinde alt başlıklar halinde incelenmiştir. Bilgi güvenliğine etki eden unsurların bir bütün olarak saldırgan gözüyle sınanması, zafiyetlerin tespit edilerek giderilmesi için yapılacak düzeltmelerin ve sıkılaştırmaların belirlenmesi, güvenlik testlerinin ülke bilgi güvenliğinin sağlanmasındaki önemini özetlemektedir.

Güvenlik testleri, bilgi sistemlerinin başına olumsuz bir durum gelmeden önce, sistem açıklarını sınayarak belirlemek ve alınabilecek karşı tedbirlerin önceden düşünülmesinde kullanılan önemli bir erken uyarı sistemidir. Güvenlik testlerinin başarılı olabilmesi için bilgi sistemlerinin güvenliğine etki eden faktörlerinin ağırlıkları dikkate alınarak sistemlere özgü farklı senaryolar geliştirilmesi gereklidir. Güvenlik testleri için geliştirilen senaryolar kullanılan teknolojilere, kullanıcıların bilgi düzeylerine, bilgi güvenliği seviyesine, bilgi güvenliği bileşenlerinin dozuna göre farklılık gösterebilir.

Bilgi güvenliği ihlallerinin kontrollü bir şekilde tespit edildiği teknik testlere ek olarak teknik olmayan testler de yapılmalıdır. Teknik olmayan güvenlik testlerinin başında sosyal mühendislik testleri gelmektedir. Sosyal mühendislik, yalan söyleme ve ikna etme üzerine kurulan inandırma ve bilgi toplama sanatıdır [25]. Sosyal mühendislik testlerinden sonuç alabilmek için farklı yöntemler kullanılmaktadır. Bu yöntemlerden en çok kullanılanı telefon yoluyla taklit ve ikna yöntemidir.

Güvenlik testlerinin yapılmasında dünyada yaygın olarak bilinen birçok açık kaynak standart ve kılavuzlar (OSSTMM, NIST, OWASP, v.b.) vardır. Güvenlik testleri yapılırken bu kaynakların kullanılması güvenlik testlerinin başarısı açısından önemlidir.

Bu çalışmada ülkemizde güvenlik testlerinin henüz yaygınlaşmadığı ve kurumlar tarafından kurumsal bilgi güvenliğinin sağlanmasında önemli bir bileşen olduğunun bilinmediği tespit edilmiştir. Bu durum güvenlik testlerinin kurumlara katkılarının, sağlayacağı farkındalığın ve güvenlik seviyesinin artırılmasına katkısının ülkemizde pek bilinmediğinin ve yeterince önem verilmediğinin göstergesidir.

VII. Sonuçlar ve Değerlendirmeler

Ülke bilgi sistemleri, e-devlet uygulamaları aracılığıyla kişisel veya kurumsal ihtiyaçlar doğrultusunda kurumsal bilişim altyapılarını kullanarak hizmet vermektedir. Geçmiş yıllarda saldırılar hedef gözetmeksizin yapılmaktayken günümüzde nokta hedefi gözeten ve ülke bilgi sistemlerini hedef alan bilinçli saldırılar yapılmaktadır. Ülke bilgi güvenliğini zaafa uğratmaya hatta yıkmaya çalışan, bireyler ve kurumlar üzerinde maddi manevi büyük zararlara yol açan bilgi güvenliği tehditlerinin engellenmesi için kişisel ve kurumsal seviyede bilgi güvenliği sağlanmalıdır. Ülke bilgi sistemlerinin bilgi güvenliği süreçleri uluslararası standartlara göre yönetilmelidir.

Ülke bilgi sistemleri ülkeler açısından kritik bilgiler barındırmaktadır. Bu kritik bilgilerin bilgi güvenliğinden kaynaklanan zafiyetlerden dolayı siber saldırılara uğraması sonucunda ülkeler açısından telafisi mümkün olmayan durumlarla karşılaşılabilir. Bir barajın kapaklarının yetkisiz bir şekilde istenmeyen bir zamanda açılması, sivil veya askeri haberleşme sistemlerinin aksatılması, elektrik ve doğalgaz santrallerinin kullanılmaz hale getirilmesi, bankacılık, sağlık ve eğitim sektörlerine ait bilgi sistemlerinin çökertilmesi ülke güvenliğini tehdit eden bilgi sistemleri odaklı saldırılara örnek olarak gösterilebilir. Ülke güvenliğini tehdit eden bilgi sistemleri odaklı saldırılardan korunmak için ülke güvenlik politikaları oluşturulmalı ve bu politikalara göre ülke bilgi güvenliği sağlanmalıdır.

Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak yapılacak güvenlik testleriyle kayıpları en aza indirmek mümkündür. Ülke bilgi sistemlerine yönelik yapılacak güvenlik testlerinin ulusal bir otorite tarafından

oluşturulan güncel ulusal güvenlik politikalarına uygun olarak yapılması gerekmektedir. Ülkemizde güvenlik testlerini ücretsiz yapan devlet destekli merkezler oluşturulmalı ve güvenlik testlerine yönelik milli yazılımlar geliştirilerek kullanılmalıdır.

Bilgi güvenliğinde "güvenliğiniz en zayıf halkanız kadardır" ilkesi gözönüne alındığında ülke bilgi güvenliğini oluşturan halkalar içerisinde en zayıf halka olan insan faktöründen kaynaklanan zafiyetlerin giderilmesi için bilgi güvenliği eğitimi ve bilinçlendirmesi, ilköğretimden üniversiteye kadar eğitimin her aşamasında verilmelidir. Burada özellikle sivil toplum kuruluşlarına, Milli Eğitim Bakanlığına ve üniversitelere büyük görevler düşmektedir.

Ülke güvenliğini tehdit eden siber saldırıların bilinmesi, bilgi güvenliğinin sağlanmasına yönelik ülke stratejilerinin geliştirilmesinde önemli bir role sahiptir. Bilgi sistemlerine yönelik olarak yapılan planlı saldırılar incelendiğinde; saldırıların kişi düzeyinden ülke düzeyine kadar çok geniş bir yelpazede gelişmiş teknikler kullanılarak yapıldığı tespit edilmiştir. Ülke bilgi güvenliğinin sağlanması amacıyla, saldırı türlerinin takip edilmesi, saldırganların kullandığı gelişmiş yöntemlerin saptanması, ülkemizde ve dünyada bu konuda yapılan araştırmaların, raporların ve çalışmalar ile tespit edilen açıkların yakından takip edilmesi ve zamanında giderilmesi gerekmektedir.

Sonuç olarak; ülke bilgi güvenliğinin sağlanmasına yönelik yapılan çalışmaların ve alınması gereken önlemlerin yeterli olmadığı, kişisel ve kurumsal düzeyde bilgi güvenliği bilincinin ve eğitiminin toplumumuza tam olarak yerleşmediği ve ülkemizde yüksek seviyede ülke bilgi güvenliğinin sağlanamadığı dikkate alındığında, bu çalışmada sunulan hususlara dikkat edilmesi ve yapılan önerilere uyulması gerekmektedir.

KAYNAKLAR

[1] Thow-Chang, L., Siew-Mun, K., and Foo, A., "Information Security Management Systems and Standards" Synthesis Journal, 2(2):5,8 (2001).
[2] Sandham, D., "News", Communications Engineer Publication 5(4):3-8, (2008).
[3] İnternet: "McAfee Virtual Criminology Report" http://www.mcafee.com/us/research/criminology_report/default.html (09.11.2008)
[4] Vural, Y., "Kurumsal Bilgi Güvenliği ve Sızma Testleri", Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 15-20, (2007).
[5] Rocha, L. M., Schnell, S., "The Nature of Information-Lecture Notes", Indiana University, Bloomington, 1, (2007).
[6] İnternet: Türk Dil Kurumu "Güncel Türkçe Sözlük" http://www.tdk.gov.tr/TR/SozBul.aspx?F6E10F8892433CFFAAF6AA849816B2EF4376734BED947CDE&Kelime=bilgi
[7] İnternet : "National Information Systems Advisory Panel- Computer-Based National Information Systems" http://govinfo.library.unt.edu/ota/Ota_5/DATA/1981/8109.PDF (09.11.2008).
[8] İnternet: "Türkiye Ulusal Bilgi Sistemi:Genel Esaslar" www.hssgm.gov.tr/stratejikyonetim/egitim_dokumanlari/turkiye_ulusal_bilgi_sistemi_esaslari.pdf (09.11.2008)
[9] Krygiel, J., "Behind the Wizards Curtain: An Integration Environment for a System of Systems" DoD C4ISR Cooperative Research Program,Washington, 9-11 (1999).
[10] İnternet: Wikipedia, "Information Assurance", http://en.wikipedia.org/wiki/Information_assurance (09.11.2008)
[11] Bhatt, G. D., "Knowledge Management in Organizations: Examining the Interaction between Technologies, Techniques and People", Journal of Knowledge Management, 5 (1):71, (2001)
[12] Vural, Y., Sağıroğlu, Ş., Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, ISC Turkey Uluslararası Katılımlı Bilgi Güvenligi ve Kriptoloji Konferansi, Ankara, 191-199, Aralık 2007
[13] Vural, Y., Sağıroğlu, Ş., Gazi Üniv. Müh. Mim. Fak. Der. 23(2), 507-522, (2008)
[14] Türk Standardları Enstitüsü, "Bilgi güvenliği yönetim sistemleri", TSE-TS 1779- 2, Ankara, 3, (2005).
[15] Mitnick, K. D., Simon, L. W., Wozniak, S., "The Art of Deception: Controlling the Human Element of Security", Wiley Publishing, New York, 17-18 (2003)
[16] İnternet: Wikipedia, "ISO/IEC 27001", http://en.wikipedia.org/wiki/ISO_27001 (09.11.2008)
[17] İnternet: CERT "Historical Statistics" http://www.cert.org/stats/historical.html (09.11.2008)
[18] Dunlevy, J. C., "Information Security Strategies: A New Perspective", CERT, Pittsburgh, 15, (2006)
[19] Internet: World Stats "Top 20 Countries With The Highest Number Of Internet Users" http://www.internetworldstats.com/top20.htm (17.03.2007)
[20] Symantec Corp., "Symantec Internet Security Threat Report Trends for July–December 07" Symantec Volume XII, Cupertino, 24-64 (2008).
[21] Gordon, L. A., Loeb, M. P., Lucyshyn, W., Richardson, R., "CSI/FBI, Computer Crime and Security Survey", FBI Computer Security Institute, 1- 26, (2005).
[22] Koç.net Haberleşme Teknolojileri ve İletişim Hizmetleri A.Ş., "Türkiye İnternet Güvenliği Araştırma Sonuçları 2005", Koç.net, İstanbul, 5- 12, (2005)
[23] İnternet: "Information Security Awareness" http://www.massachusetts.edu/SecurityAwareness/securityawareness.html (9.11.2008)
[24] Morales, L.; Dark, M., "Information Security Education and Foundational Research", System Sciences, HICSS 2007. 40th Annual Hawaii International Conference, Hawaii, 269 (2007).
[25] Mitnick, K. D., Simon, W. L., "Aldatma Sanatı", Nejat Eralp Tezcan, ODTÜ Yayıncılık, Ankara, 303, (2006).