

Anayurt Güvenliğinin Sağlanmasında Bilgi Sistemleri Güvenliğinin Önemi

Yılmaz Vural, Mustafa Bayındır, Onur Tamer

STMA.Ş

yvural@stm.com.tr, mbayindir@stm.com.tr, otamer@stm.com.tr

Özet: Bilgiler, bilgi sistemleri aracılığıyla üretilmeye, işlenmeye, taşınmaya ve depolanmaya başladıkça bu ortamlarda alınması gereken farklı güvenlik önlemleri gündeme gelmiştir. Ulusal bilgi sistemlerinde muhafaza edilen ülke güvenliği açısından kritik olan bilgilerin güvenliğinin yüksek seviyede sağlanamamasından kaynaklanabilecek zafiyetler, anayurt güvenliğini tehdit etmektedir. Anayurt güvenliğinin yüksek seviyede sağlanabilmesi için, ülke bilgi varlıklarının değerinin iyi tespit edilerek korunma maliyetinin belirlenmesi, ülke bilgi güvenliği bilincinin topluma yerleşmesi, anayurt güvenliğinin parçası olan farklı sistemlere ait bilgi güvenliği yönetiminin geliştirilecek milli standartlar çerçevesinde gerçekleştirilmesi gerekmektedir. Bu önemden dolayı yapılan çalışmada bilgi sistemleri güvenliğinin yüksek seviyede sağlanması üzerine araştırma yapılmış ve anayurt güvenliği bakış açısıyla değerlendirilmiştir.

Abstract: As information is produced, processed, transferred and stored, several security measures are come into question. Weaknesses in ensuring the security of vital information, homeland security may be threatened. In order to ensure high level of homeland security, the national information assets and protection costs must be determined, information security consciousness must be increased and information systems that constitute the homeland security infrastructure must implement the information security standards that will be developed nationwide. In this paper, we researched providing high level of information security by relating it to homeland security concept.

Anahtar Kelimeler: Anayurt Güvenliği, Bilgi Güvenliği, Bilgi Sistemleri Güvenliği, Bilişim Güvenliği, Ülke Bilgi Güvenliği, Ülke Güvenliği.

1. Giriş

Bilgi; tarih boyunca insanoğlunun düşüncesini, yaşayışını, davranışını, gelişimini belirleyen faktörlerin başında gelen büyük bir güç olarak yerini korumuştur. Bilişim teknolojilerinin gelişmesi ve bilgi sistemlerinin hızla yaygınlaşmasıyla; bilginin yönetilmesi, iş verimliliğinin ve akışlarının hızlandırılması, çalışanlar ve diğer kurumlarla daha hızlı iletişim kurulabilmesi sağlanmıştır. Bilgi sistemlerinde bilginin üretilmesi, işlenmesi, taşınması ve saklanması sağlanmış ve bilgiye mekândan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmıştır.

Elektronik ortamlarda kişiler, kurumlar ve ülkelere ait kritik bilgilerin mahremiyetlerinin korunması, bilgi sistemlerinin kullanımının yaygınlaşması ve doğrudan veya dolaylı olarak yaşanan maddi ve manevi kayıpların oluşmaması için bu ortamlarda bulunan bilgilerin güvenliğinin sağlanması gereklidir. Hayatımızı kolaylaştırması iş ve işlemlerin hızlandırılmasına katkılar sağlayan bilgi teknolojileri insan hayatında günden güne daha da önem kazanmakta ve her geçen gün güvenliği üst düzeyde sağlanan güvenilir bilgi sistemlerine duyulan ihtiyaç artmaktadır [1].

Alınan birçok önleme geliştirilen birçok yeni donanım ve yazılım çözümüne rağmen bilgi

sistemlerine yönelik güvenlik saldırıları her geçen gün hızla artmaktadır. Bilginin gizliliğine, bütünlüğüne, erişilebilirliğine karşı yapılan saldırılar ciddi ve giderilemeyecek kayıplara yol açmaktadır. Bu kayıpları tamamen yok etmek mümkün değildir. Ancak önceden veya zamanında alınacak güvenlik tedbirleriyle kayıpları en aza indirmek mümkündür. Güvenlik sadece teknoloji problemi olarak değil aynı zamanda insan ve yönetim problemi olarak değerlendirilmelidir [2]. İnsan ve yönetim hatalarından kaynaklanan güvenlik ihlallerinin sebeplerine bakıldığında son kullanıcılardan ülke yönetimine kadar farklı kademelerde görev yapan kurum veya bireylerin ortak eksikliklerinin eğitim ve bilinçlendirme olduğu görülür.

Anayurt güvenliği, bir ülkenin ilgili tüm birimlerinin katıldığı bir ortaklaşa çalışmayı gerektirir [3]. Çalışan her sistemde olduğu gibi, bilgi anayurt güvenliğinde de hayati bir öneme sahiptir. Anayurt güvenliğinin parçası olan her kurum bilgi ve bilgi sistemlerine temelden bağımlıdır. Ayrıca doğru işleyen bir anayurt güvenlik sistemi, bilgiyi yatay ve dikey olarak paylaşan bilgi sistemlerinin oluşturulması ile mümkündür. Bilgi sistemlerinin tek tek güvenliğinin sağlanması kurumların işleyişinde hayati öneme sahip iken, anayurt güvenliği söz konusu olduğunda güvenlik ihlallerinin etkileri çok daha hayati olabilmektedir. Anayurt güvenliği bağlamında ele alındığında bilgi güvenliği artık ortak olarak ele alınması ve ortak politikalar belirlenmesi gerekli olan bir konu haline gelmektedir.

2. Bilgi ve Bilgi Sistemleri

Bilgi kelimesinin menşei, Latince'deki herhangi bir şeye şekil vermek anlamına gelen "informare" kelimesinden gelmektedir [4]. Sözlük anlamıyla bilgi; "Öğrenme, araştırma ve gözlem yoluyla elde edilen her türlü gerçek, malumat ve kavrayışın tümü" olarak tanımlanmaktadır [5]. Bilginin aktarılmasında ilk çağlardan başlayarak hikâyeler, masallar ve

destanlar aracı olmuş 12. yüzyıldan sonra da bilginin yaygınlaştırılmasında ve öğretilmesinde medreseler, üniversiteler ve kitaplar önemli roller üstlenmişlerdir. Bilgi sistemleri ise 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. Son dönemde iletişim ve işbirliğini son derece kolaylaştıran bilgi sistemlerinin gelişmesiyle bilgi çağı adı verilen yeni bir döneme girilmiştir. Bilgi çağında ülkeler bilgiyi en etkin biçimde bilgi sistemleri aracılığıyla kullanmaktadır. Bilgi çağında, savunma, eğitim, sanat, sağlık, iş yaşamı ve diğer alanlarda bilginin güvenli kullanımı ülkeler açısından önemli bir gereksinim halini almıştır. Güvenliği sağlanamayan ulusal bilgi sistemleri ülkeler açısından ciddi tehditlerin meydana gelmesine neden olmaktadır. Ulusal bilgi sistemlerinin ortak olarak kullanılmaya başlanmasıyla, bilgi sistemlerinde muhafaza edilen ve ülke güvenliği açısından kritik olan bilgilerin güvenliğinin yüksek seviyede sağlanması anayurt güvenliği açısından önem kazanmıştır

3. Anayurt Güvenliği

Geçtiğimiz yüzyılda dünyanın değişik yerlerinde ortaya çıkarak yayılan terör dalgası, 11 Eylül 2001 tarihinde Amerika Birleşik Devletleri'ni de etkilediğinde, başta Amerika Birleşik Devletleri olmak üzere tüm dünyada Anayurt Güvenliği konusu ve stratejileri tartışılmaya başlanmış ve güvenlik literatürüne bu kavram dahil olmuştur [6]. Anayurt Güvenliği kavramı iç içe birçok görevi ve misyonu da beraberinde getirmektedir. Devletin ve hükümetin çaba ve gayretleri yanında özel sektörün kendi alanındaki kabiliyetleri de bu alanda önem taşımaktadır. Hukuk, bilim ve teknoloji, bilgi sistemleri Anayurt Güvenliği kavramının temelini oluşturmaktadır.

Amerika Birleşik Devletleri'nde başlayan Anayurt Güvenliği kavramı, terör hareketlerinin sadece belli ülkelerle sınırlı olmayıp diğer ülkelerinde etkileyebileceğinin anlaşılması ile birlikte ülkeler arasında işbirliğine gidilmiş ve terör tüm boyutlarıyla tartışılmaya başlanmıştır. Anayurt Güvenliğini tehdit eden terör saldırıları incelendiğinde toplum yararına görülen birçok bilgi sistemi teröristler tarafından bir iletişim ve saldırı aracı olarak kullanılmış ve siber terörizm kavramı ortaya çıkmıştır.

Günümüzde birçok bilgi sistemi ülkeler açısından kritik bilgiler barındırmaktadır. Bu kritik bilgilerin güvenlik zafiyetlerinden ötürü siber teröristler tarafından kötüye kullanılması durumunda ülkeler açısından felaketler meydana gelebilir.

Siber teröristlerin kabiliyetleri ve ulusal bilgi sistemlerimizin korunmasızlığına bağlı olarak anayurt güvenliğini tehdit eden birçok saldırıyla karşılaşılabilir. Bir barajın kapaklarının istenmeyen bir zamanda açılması, askeri haberleşme sistemlerinin engellenmesi, kentin bütün trafik ışıklarını durdurulması, telefon santrallerinin kullanılmaz duruma getirilmesi, elektrik ve doğalgaz santrallerinin kullanılmaz hale getirilmesi, ulaşım ve su sistemlerini durdurulması, finans sektörünün çökertilmesi, acil yardım, polis, hastaneler ve itfaiyelere ait bilgi sistemlerinin çalışamaz duruma getirilmesi, anayurt güvenliğini tehdit eden bilgi sistemleri odaklı saldırılara örnek olarak gösterilebilir [7].

Anayurt güvenliğini tehdit eden bilgi sistemleri odaklı saldırılardan korunmak için bilgi sistemlerinin güvenliği yüksek seviyede sağlanmalıdır. Takip eden bölümde bilgi sistemlerinin güvenliği ele alınmıştır.

4. Bilgi Sistemleri Güvenliği

Bilgi sistemlerinin güvenliğinin sağlanması için, fiziksel güvenlik, haberleşme güvenliği, yayılım güvenliği, bilgisayar güvenliği, ağ güvenliği ve bilgi güvenliği konularında çalışma-

lar yapılmaktadır. Anayurt güvenliğini tehdit eden siber saldırılardan korunmak için ulusal bilgi sistemlerinin güvenliğinin yüksek seviyede sağlanması gerekmektedir. Bilgi sistemlerinin güvenliğinin sağlanabilmesi amacıyla yukarıda bahsedilen güvenlik önlemlerinin hepsinin bir arada düşünülmesi gerektiğinden bu önlemler takip eden alt başlıklarda kısaca açıklanmıştır.

4.1. Fiziksel Güvenlik

Geçmiş zamanlarda insanlar için önemli bilgiler, taşlara kazılarak saklanmış daha sonraları kâğıtlara yazılarak fiziksel güvenliği sağlanan ortamlarda saklanmıştır. Fiziksel güvenliğin sağlanabilmesi amacıyla, duvarlar örülmüş, kale hendekleri çekilmiş, giriş çıkışı kontrol eden nöbetçiler görev yapmıştır. Bilginin güvenliğini sağlamaya yönelik fiziksel önlemler alınmasına rağmen genellikle bu korumalar yeterli olmamış, bilgilerin çalınması veya istenmeyen kişilerin eline geçmesi engellenememiştir [8]. Geçmişten günümüze fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar, gelişen teknolojinin yardımıyla günümüzde de yapılmaktadır. Binaların etrafına çitlerin çekilmesi, bina içi ve dışının kameralarla izlenmesi, koruma duvarlarının yapılması, bina girişinde özel güvenlik görevlilerinin bulundurulması, önemli bilgilerin tutulduğu odaların kilitlemesi, önemli odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler günümüzde kullanılan fiziksel güvenlik önlemlerine örnek olarak verilebilir.

4.2. Haberleşme Güvenliği

Karşılıklı bilgi alışverişinde güvenli bir haberleşme ortamını oluşturmak üzere yapılan faaliyetlerin ortak adı haberleşme olarak adlandırılır [9]. Haberleşme anında fiziksel olarak bilgilerin güvenliğinin sağlanması, güvenlik açısından yeterli değildir. İletişim sırasında bilginin hedefe ulaşmadan önce başka kişiler tarafından ele geçirilmesi ve içeriğinin öğrenilmesi riski her zaman vardır. Haberleşme güvenliğinin sağlanmasında kullanılan yöntemler tarih boyunca

ca değişmemiş fakat bu güvenliği sağlamak için kullanılan teknikler ve yöntemler sürekli olarak gelişmiştir. Haberleşme güvenliğinin sağlanmasında kriptografi ve steganografi yöntemleri kullanılmaktadır [10-15].

4.3. Yayılım Güvenliği

Yayılım güvenliği, elektronik sistemlerin meydana getirdiği yayılımların yetkisiz kişilerce ele geçirilip analizinin önlenmesidir [16]. Tüm elektronik cihazlar çevreye elektromanyetik sinyal yayarlar. Elektromanyetik sinyaller havadan radyoelektrik dalgalar olarak, elektrik dağıtım veya telefon şebekesine elektriksel gürültü olarak, çeşitli kabloların yüzeylerinden iletilen elektromanyetik dalgalar olarak yayılırlar [17]. Her türlü istem dışı yayılımın kaydedilerek bilgi/veri analizi yapılması şeklindeki bilgi elde etmeye bağlı yayılım güvenliğine karşı koruma sağlamak için Tempest (Transient Electro Magnetic Pulse Emanation Standard) adı altında bir standart geliştirilmiştir. Yayılım güvenliği için Tempest sertifikalı cihazlar kullanılmalı, elektromanyetik dalgalara gürültü adı verilen anlamsız dalgalar katılmalı, binalar inşa edilirken Tempest kurallarına göre binaların dış yüzeyleri özel zırhlarla giydirmeli (faraday kafesi), dışa bakan pencere sayıları sınırlı olmalı, kabloların geçtiği kanallar yine özel zırhlarla kaplanarak korunmalıdır.

4.4. Bilgisayar Güvenliği

Bilgisayarların ortaya çıkması ve kullanımının yaygınlaşmasıyla birçok veri ve bilgi, bilgisayar ortamlarında tutulmaya başlanmıştır. Fiziksel güvenlik, yayılım güvenliği ve haberleşme güvenliğinden sonra bilgisayar güvenliği, bilgi sistemlerinin güvenliğinin sağlanması açısından önem kazanmıştır. 1970'li yılların başında David Bell ve Leonard La Padula bilgisayar güvenliğine ilişkin bir model geliştirmişlerdir [18-19]. Bu model 1983 yılında ABD Savunma Departmanı 5200.28 nolu bu standardı kabul etmiş ve Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-Trusted Computer System Evaluation Criteria) adlı kitabın (Tu-

runcu Kitap-Orange Book) oluşmasını sağlamıştır [20]. Bu kitapta, bilgisayar sistemlerinin güvenliğini test etmek için oluşturulan güvenlik seviyeleri anlatılmıştır [21].

4.5. Ağ Güvenliği

Güvenli Bilgisayar Sistemi Değerlendirme Kriterleri (TCSEC-DoD Trusted Computer System Evaluation Criteria) ağ sistemlerinin güvenliği için geliştirilmediğinden 1987 yılında TCSEC'in güvenilir ağ yorumlaması (Trusted Network Interpretation) adını verdiği Kırmızı Kitap (Red Book) yayımlanmıştır [22]. Kırmızı Kitap, Turuncu Kitaba ek olarak bilgisayar ağları ve bileşenlerinin güvenliğiyle ilgili konuları da içermektedir. Bilgisayarlar, ağlar aracılığıyla kablolu veya kablosuz olarak birbirleriyle iletişim kurmaktadır. Kablolu ve kablosuz ağ ortamlarının güvenliğinin sağlanmasıyla ilgili güvenlik duvarları, saldırı tespit sistemleri gibi farklı çözümler geliştirilmiştir.

4.6. Bilgi Güvenliği

Bilgi güvenliğinin sağlanabilmesi için daha önceki alt bölümlerde anlatılan güvenlik önlemlerinin tamamının birlikte değerlendirilmesi gerekmektedir. Bilgi varlıklarının fiziksel olarak korunması için fiziksel güvenliğin, iletim halindeki bilgilerin güvenliğinin sağlanması için haberleşme güvenliğinin, elektronik sistemlerden istem dışı yayılan sinyallerin kullanılarak önemli bilgilerimize ulaşılmaması için yayılım güvenliğinin, bilgisayarlarımıza erişimin kontrol altına alınması için bilgisayar ve ağ güvenliğinin sağlanması gerekmektedir [23].

4.7. Bilgi Sistemleri Güvenliği Farkındalığı (İnsan Boyutu)

Bilgi sistemlerinin güvenliğiyle ilgili yapılan çalışmalarda (raporlar, anketler, kitaplar, makaleler, vb.) vurgulandığı gibi bilgi sistemlerinin güvenliğinin sağlanmasındaki en zayıf halkanın insan faktörü olduğu belirlenmiştir [24]. Örneğin, görevi nedeniyle telefonda hangi bilginin verilip verilmeyeceği konusunda farkındalığı olmayan bir görevliden telefon

görüşmeleriyle alınacak bilgiler siber saldırı yapabilmek için gerekli olan saldırıların bir parçasını oluşturabilir. Yüksek seviyede bilgi sistemlerinin güvenliğinin sağlanması için insan faktörü dikkate alınmalı ve bilgi sistemleriyle doğrudan veya dolaylı olarak ilişkide bulunan tüm görevliler bilgi güvenliği konusunda eğitilmelidir.

5. Sonuçlar

Anayurt güvenliğinin sağlanması, güvenlikle doğrudan veya dolaylı olarak ilgili tüm kurum ve kuruluşların hatta bireylerin bir arada ortak çalışması ile mümkündür. Kurumlar ve kuruluşlar arasındaki ortak ve etkin çalışma ise günümüzün dinamik dünyasında ancak beraber ve etkin bir şekilde çalışan bilgi sistemleri ile sağlanabilmektedir. Bilgi sistemlerinin birlikte çalışabilirliği bir çok güvenlik tehdidini de beraberinde getirmektedir. Bilgi sistemlerinin korunmasızlığından kaynaklanabilecek zafiyetlerin siber teröristler tarafından kullanılması anayurt güvenliğini yüksek düzeyde tehdit etmektedir.

Anayurt güvenliğini tehdit eden bilgi sistemleri odaklı saldırılardan korunmak için güvenli bilgi sistemlerine ihtiyaç duyulmaktadır. Güvenli bilgi sistemlerinin ortak verileri etkin bir şekilde kullanarak anayurt güvenliğini ilgilendiren hususlarda uygun tehdit analizleri ile olası saldırıları yaşanmadan önce haber vermelidir. Güvenliğin doğasında yer alan “en zayıf halka” kuralı bilgi sistemlerinin güvenliği içinde geçerlidir. Bu çalışmada vurgulandığı gibi bilgi sistemlerinin güvenliğinde de en zayıf halka olan insan faktöründen doğabilecek tehditlerin en aza indirgenmesi için insanlar eğitilmeli ve bilinçlendirilmelidir.

Güvenliği yeterince sağlanamayan bilgi sistemleri anayurt güvenliğini doğrudan olumsuz olarak etkilediğinden bilgi sistemlerinin güvenliğinin bu yazıda özetlenen önlemler dikkate alınarak en üst seviyede sağlanması gerekmektedir. Ülkemizde anayurt güvenliğinin

sağlanması için öncelikle ulusal bilgi sistemlerimizin birlikte çalışabilir güvenli sistemler haline getirilmesi sağlanmalıdır. Ayrıca anayurt güvenliği konusunda her kesimden kurumlarımız, kuruluşlarımız ve insanımız eğitilmeli ve bu konuda ortak çalışmalar yapılması gerektiği değerlendirilmiştir.

Kaynaklar

- [1] Schmidt, A. H., “Building a mosaic of security for a better world”, Security Matters, Aspatore Books, U.S.A., 24-26 (2004).
- [2] 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).
- [3] Office of Homeland Security, “National strategy for homeland security” (2002).
- [4] Rocha, L. M., Schnell, S., “The Nature of Information-Lecture Notes”, Indiana University, Bloomington, 1, (2007).
- [5] İnternet: Türk Dil Kurumu “Güncel Türkçe Sözlük” http://www.tdk.gov.tr/TR/SozBul.aspx?7F6E10F889243_3CFFAAAF6AA849816B2EF4376734BED947CDE&Kelime=bilgi
- [6] İnternet: Wikipedia, “Anayurt Güvenliği”, http://tr.wikipedia.org/wiki/Anayurt_guvenligi.
- [7] İnternet: Özcan, M., “Siber Terörizm ve Ulusal Güvenliğe Tehdit Boyutu”, <http://www.turkish-weekly.net/turkce/makale.php?id=87>
- [8] Maiwald, E., “Network Security: A Beginner’s Guide Summary”, McGraw-Hill Osborne Media, California, 4-11, (2003).
- [9] İnternet: “Communication” <http://en.wikipedia.org/wiki/Communication> [10] İnternet: Wikipedia “Kriptografi” <http://tr.wikipedia.org/wiki/Kriptografi>

- [11] Yerlikaya, T., Buluş, E., Buluş, N., “Kripto Algoritmalarının Gelişimi ve Önemi”, Akademik Bilişim 2006, Pamukkale Üniversitesi, 2, (2006).
- [12] Bilişim Sistemleri Güvenliği El Kitabı Çalışma Grubu “Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0” Türkiye Bilişim Derneği Yayınları, Ankara, 4, (2006).
- [13] Sağıroğlu, Ş., Tunçkanat, M., “Gizli bilgilerin internet ortamında güvenli olarak aktarımı için yeni bir yaklaşım” Popüler Bilim Dergisi, 9(105), 21-24, (2002).
- [14] İnternet: Wikipedia “Steganografi” <http://tr.wikipedia.org/wiki/Steganografi>
- [15] Sağıroğlu, Ş., Tunçkanat, M., Altuner, M., “Kriptolojide Yeni Bir Yaklaşım Resimli Mesaj”, Telekomünikasyon Ekseni Dergisi, Telekomünikasyon Kurumu, 2(2):22-24, (2002).
- [16] Baykal, N., “Bilgi Teknolojisinin, Ulusal Güvenlik ve Ulusal Güvenlik Stratejisi ile İlgili Boyutu”, Hava Harp Akademileri Sempozyumu, 12, (2005).
- [17] Sevgi, L., “Elektromanyetik Uyumluluk-Elektromanyetik Kirlilik”, Elektrik Mühendisleri Odası Dergisi, 23, (2000).
- [18] İnternet: Wikipedia “Tempest” <http://en.wikipedia.org/wiki/TEMPEST>
- [19] Bell, D., La Padula, L., “Secure Computer System: Unified Exposition and Multics Interpretation”, The MITRE Corporation Technical Report ESD-TR-75-306, Bedford, 5, (1975).
- [20] Abrams, D. M., Joyce, V. M., “Trusted System Concepts”, Computers & Security, 14(1):45-56, (1995).
- [21] Department of Defense, “Trusted Computer System Evaluation Criteria”, DoD 5200.28-STD, Washington, 3-8, (1985).
- [22] Lehtinen, R., “Computer Security Basics, 2nd Edition”, O’Reilly, Sebastopol, 302, (2006).
- [23] Sharp, E. D., “Information Security in the Enterprise”, Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., Auerbach Publications, New York, 1199-1200, (2004).
- [24] Vural, Y., “Kurumsal Bilgi Güvenliği ve Sızma Testleri” Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 40, 2007.