Seferoğlu, S. S., Yıldız-Durak, H., Karaoğlan-Yılmaz, G. ve Yılmaz, R. (2018). Bilgi güvenliği farkındalığı ve bilgi güvenliği politikalarıyla ilgili bir inceleme. B. Akkoyunlu, A. İşman ve H. F. Odabaşı (Ed). *Eğitim teknolojileri okumaları 2018,* (3. Bölüm, ss. 29-43). TOJET ve Sakarya Üniversitesi, Adapazarı. [Çevrim-içi: http://yunus.hacettepe.edu.tr/~sadi/yayin/Kitap_ETO2018_Bolum3_29-43_BilgiGuvenligi.pdf, Erişim tarihi: 02.10.2018.]

3. BÖLÜM

BİLGİ GÜVENLİĞİ FARKINDALIĞI VE BİLGİ GÜVENLİĞİ POLİTİKALARIYLA İLGİLİ BİR İNCELEME

Prof. Dr. Süleyman Sadi SEFEROĞLU
Hacettepe Üniversitesi

Dr. Öğr. Üyesi Hatice YILDIZ DURAK
Bartın Üniversitesi

Dr. Öğr. Üyesi Fatma Gizem KARAOĞLAN YILMAZ
Bartın Üniversitesi

Dr. Öğr. Üyesi Ramazan YILMAZ
Bartın Üniversitesi

Özet

Günümüz bilgi toplumlarında bilişim teknolojileri sürekli gelişmekte ve değişmektedir. Bu gelişime paralel bir şekilde bu teknolojilerin kullanıcı sayısı da gün geçtikçe artmaktadır. Öte yandan bilişim teknolojilerinin kullanımı birçok kişi, kurum ve kuruluş için olmazsa olmaz türden bir durum haline gelmiş durumdadır. Bilişim teknolojilerinin söz konusu yaşamsal ve yoğun kullanımının büyük yararları bulunmaktadır. Ancak bu kullanımlar bazı olumsuz durumlara da yol açabilmektedir. Bu olumsuz durumlardan birisi de bilgi güvenliğine yönelik risk faktörlerinin ve bu tehdidin genişlemesidir. Teknolojinin bilinçsiz ve problemli kullanımı, bilgi güvenliği tehditlerinin çeşitlenmesi gibi nedenler bilgi güvenliğini sağlamanın zorlaşmasına yol açmaktadır. Bu nedenle ulusal ve uluslararası düzeyde olmak üzere kişisel ve kurumsal bilgi güvenliğinin sağlanması ve bilgi güvenliğiyle ilgili farkındalığın artırılması giderek daha önemli hale gelmektedir.

Bu gerekçeler doğrultusunda bu çalışmada bilgi güvenliği kavramıyla ilgili tanımlamaların, bilgi güvenliğinin kapsamının ve bilgi güvenliğiyle ilgili farkındalık durumunun incelenmesi, ayrıca ulusal ve uluslararası düzeyde bilgi güvenliği politikaları üzerine bir değerlendirme yapılması amaçlanmaktadır. Bu amaç doğrultusunda konuyla ilgili alanyazın incelenmiş, ulusal ve uluslararası politika belgeleri gözden geçirilmiştir.

Anahtar Sözcükler: Bilgi güvenliği, bilgi güvenliği farkındalığı, bilgi güvenliği politikaları.

Hazırlık Soruları

1. Bilgi güvenliği nedir?
2. Bilgi güvenliği farkındalığı neden önemlidir?
3. Bilişim teknolojilerinde bilgi güvenliğini sağlama konusunda alınabilecek önlemler neler olabilir?
4. Bireylerin bilgi güvenliği farkındalığını artırmanın önemini tartışınız.
3. Kullanıcıların bilgi güvenliği farkındalığını artırmak için ulusal ve uluslararası düzeyde neler yapılabileceğini tartışınız.

Giriş

İçinde bulunduğumuz bilgi çağında, bilgi ve iletişim teknolojileri (BİT) çok hızlı bir şekilde gelişmektedir. Bu gelişim, bu teknolojiler kullanılarak sunulan hizmetlerin ve uygulamaların yaygınlaşması ve kullanıcı sayısının artması anlamına gelmektedir. Günlük hayatta yapılması gereken birçok iş ve işlem BİT aracılığıyla hızlı ve kolay bir şekilde gerçekleştirilebilmektedir. Bu teknolojiler, özellikle günlük rutin işlerin gerçekleştirilmesi açısından büyük yararlar sağlasa da zaman içerisinde bilgi güvenliğine yönelik risk ve tehditleri de beraberinde getirdiği anlaşılmıştır. Yeni teknolojilerin yapısı ve uygulama alanları bilgi güvenliğiyle ilgili birtakım risk ve tehditlerin ortaya çıkmasına neden olmaktadır. Bilginin işlenmesi için kullanılan teknolojilerin güvenlik açıkları risk faktörlerinden birisidir. Diğer risk faktörü de kişisel bilgi güvenliğini sağlama farkındalığının düşük oluşudur. Bilgi güvenliğine yönelik risk ve tehditlerin azaltılması ve önlenmesi için bu faktörlerin göz önünde bulundurulması gerekir. Öte yandan sanal ortamlarda bilgi güvenliği tehditleri sayı ve kapsam olarak her geçen gün artmakta ve bu durum birtakım önlemlerin alınmasını gerekli kılmaktadır (Pricewaterhouse Coopers, 2015). Çevrim-içi ortamlardaki kötü niyetli kişi veya kurumlar, kişisel ya da kurumsal bilgi üzerinde etkili olabilmek için teknik ya da insani unsurlara ilişkin zayıflıkları kullanabilmektedirler (Blanding, 2004; Ulaştırma, Denizcilik & Haberleşme Bakanlığı, 2016).

Günümüzde, bireylerin ve kuruluşların en değerli varlıklarından birisi sahip oldukları bilgidir. Bilgi güvenliği, birey ya da kurumun bilgilerine izinsiz veya yetkisiz bir biçimde erişilmesi, kullanılması, silinmesi, değiştirilmesi ve açığa çıkarılmasını engelleme amaçlı alınan önlemler (Puhakainen, 2006) olarak tanımlanabilir. Bu bağlamda bilgi güvenliğinin hem bireysel ve hem de kurumsal düzeyde önemli olduğu söylenebilir. Bu nedenle de BİT araçlarının küreselleşmesi ile bu teknoloji ve sistemleri doğrudan veya dolaylı kullanan tüm birey ve kurumların bilgi güvenliğine katkıda bulunması gerekmektedir (Tsohou, Kokolakis, Karyda & Kiountouzis, 2008). Nitekim birçok kurum ve kuruluş bilgi güvenliğini sağlamak amacıyla en son teknolojileri kullandıkları halde yine de güvenlik ihlallerine maruz kalabilmektedirler. Artan bilgi güvenliği ihlallerinin sayısı ve etkisi şirketlere itibar, güven kaybı ve maddi kayıplar yaşatmaktadır. Bu nedenle bilgi güvenliğinin sağlanmasında insani faktörlerin önemine dikkat çekmekte yarar bulunmaktadır (Shropshire, Warkentin, Johnson & Schmidt, 2006). Nitekim alanyazında bireylerin ya da kurumların bilgi güvenliğinin sağlanmasında teknik önlemlerin tek başına yetersiz kaldığı belirtilmektedir (Furnell, Jusoh & Katsabas, 2006; Parsons, McCormac, Butavicius, Pattinson & Jerram, 2014; Pattinson, Jerram, Parsons, McCormac & Butavicius, 2012).

Sonuç olarak BİT'in sürekli geliştiği ve kullanıcı sayısının giderek arttığı günümüzde bu yeni teknolojiler hayatımızın olmazsa olmaz parçası haline gelmektedir. Ancak bu süreçte bilgi güvenliği risk ve tehditleri gibi olumsuz durumlar da ortaya çıkabilmektedir. Günümüzde bilgi güvenliği risk ve tehditleri bireysel ya da kurumsal ölçekte bir sorun olmaktan çıkmış ulusal ve uluslararası bir soruna dönüşmüş durumdadır. Çünkü teknik açıdan yaşanan zaaflar, teknolojinin bilinçsiz ve problemli kullanımı, bilgi güvenliğiyle ilgili farkındalığın düşük oluşu ve bilgi güvenliğiyle ilgili tehditlerin çeşitlenmiş olması gibi durumlar bilgi güvenliğini sağlamanın zorlaşmasına yol açmaktadır. Bu nedenle ulusal ve uluslararası düzeyde olmak üzere kişisel ve kurumsal bilgi güvenliğinin sağlanması ve bilgi güvenliğiyle ilgili farkındalığın artırılması önem kazanmıştır.

Çalışmanın Amacı

Bu gerekçeler doğrultusunda bu çalışmanın amacı bilgi güvenliği kavramıyla ilgili tanımlamaları, bilgi güvenliğinin kapsamını ve bilgi güvenliğiyle ilgili farkındalık durumunu incelemektir. Çalışmanın bir diğer amacı da uluslararası ve ulusal bilgi güvenliği politikaları üzerine bir değerlendirme yapmaktır. Bu amaçlar doğrultusunda konuyla ilgili alanyazın incelenmiş ve ayrıca ulusal ve uluslararası politika belgeleri gözden geçirilmiştir. Bu bağlamda sırasıyla "bilgi güvenliği kavramının tanımı ve kısa tarihçesi, bilgi güvenliğinin kapsamı, bilgi güvenliğiyle ilgili tehditler, bilgi güvenliği eğitimi ve bilgi güvenliği farkındalığıyla ilgili çalışmalar, uluslararası düzeyde bilgi güvenliği politikaları, Türkiye'de bilgi güvenliği politikalarına bakış ile tartışma, sonuç ve öneriler" başlıklarına yer verilmiştir.

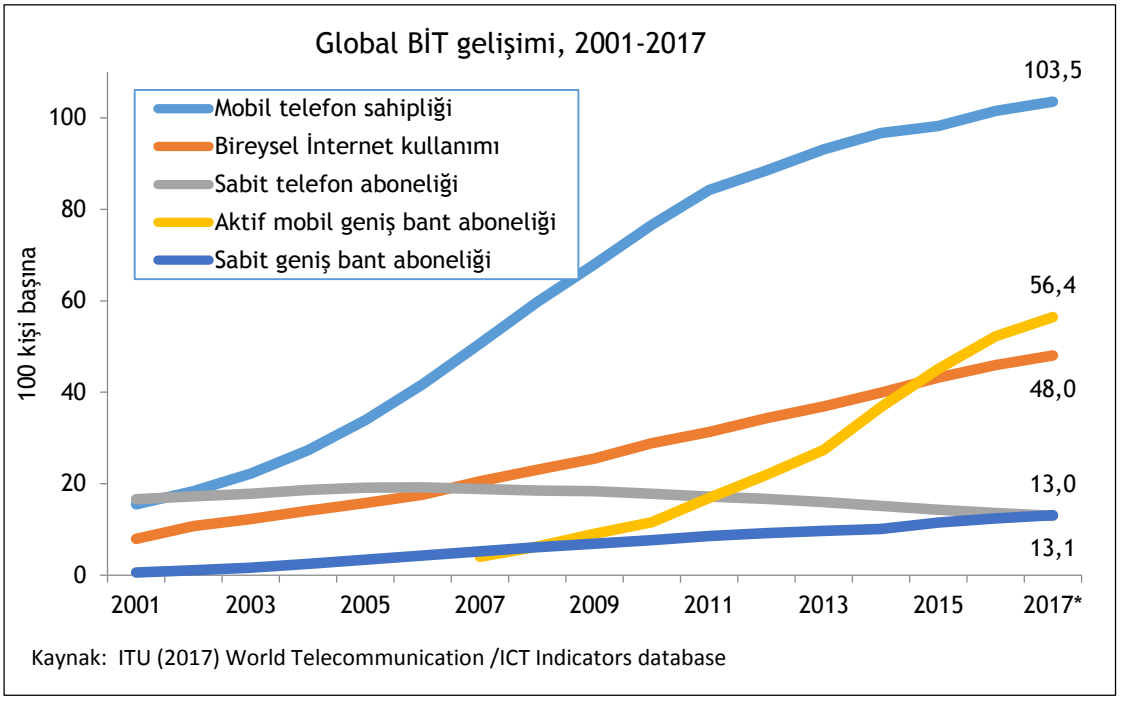
Bilgi Güvenliğiyle İlgili Kavramsal Çerçeve

Bilgi Güvenliği Kavramının Tanımı ve Kısa Tarihçesi

Bilgi toplumunda yaşanan dönüşüm, siber saldırılar, bilişim suçları, kişisel verilerin izinsiz kullanımını, bilgi/veri hırsızlığı ve siber zorbalık gibi birtakım bireysel ve toplumsal riskleri de beraberinde getirmiştir. Bu riskler ekonomik kazanç kayıplarına, hizmet sunumunda aksaklıklara ve bilgi toplumu dönüşümünün sekteye uğramasına neden olabilmektedir. Öte yandan bilgi toplumunda değerli bir şey olan bilgi, bilişim teknolojileri ile hızlı ve kolay bir şekilde paylaşılabilir niteliktedir. Bu nedenle bilginin çeşitli tehditlerden korunması, bireysel ve kurumsal düzeyde hayati derecede önemli bir konu olarak değerlendirilebilir.

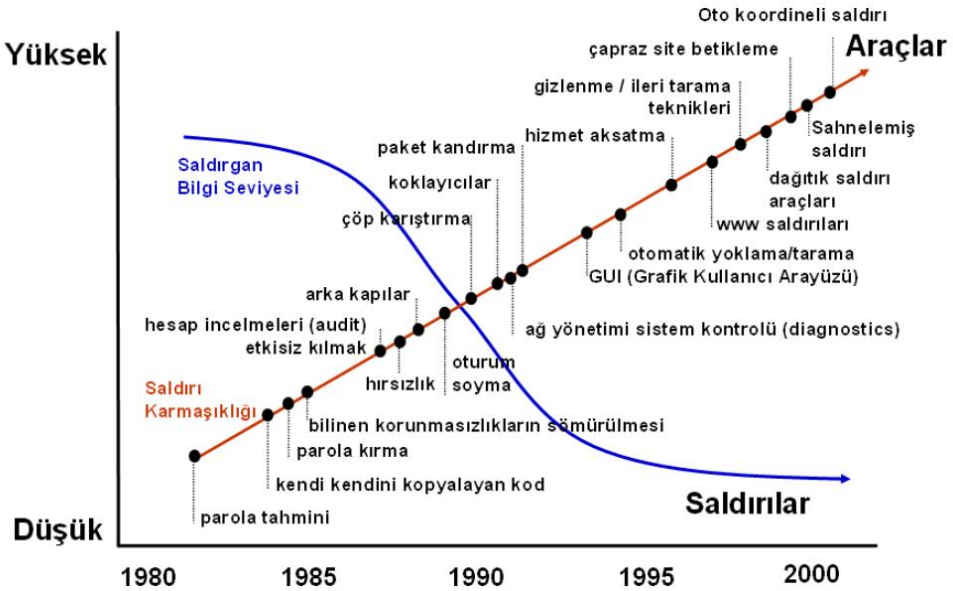
Bilgi güvenliği kavramı bilginin korunmasıyla ilgili çeşitli tedbirleri içerir (Canbek & Sağıroğlu, 2006). Örneğin bilgilerin elektronik ortamlarda taşınması/saklanması sürecinde amaç dışı kullanımlardan ve izinsiz erişimlerden korunması bilgi güvenliği kapsamındadır. Bilgi güvenliği ayrıca güvenli bir bilgi sisteminin oluşturulması ve bilginin istenmeyen kişi ya da kişiler tarafından elde edilmesini önleme girişimleri ve çabalarını da ifade eder.

BİT'in zamana bağlı olarak kullanım oranları artış göstermektedir. Şekil 1'de BİT'in yıllara bağlı kullanım ve sahipliğinde sürekli bir artış görülmektedir. Öte yandan alanyazına göre BİT'in zamana bağlı olarak kullanımının artması risk ve tehditlerin de paralel şekilde artmasına yol açmaktadır (ITU, 2011, 2015).



Şekil 1. Yıllara göre BİT Kullanım Durumunun Gelişimi

Bilgi ve iletişim teknolojilerinin kullanımı sürecinde bilgi güvenliğiyle ilgili olarak ortaya konulan çabalarda temel amaç, kişi ve kurumların BİT'i kullanırken tehdit ve tehlikelerin farkına varmalarını ve bu doğrultuda gerekli önlemleri almalarını sağlamaktır. Şekil 2'de görüldüğü üzere, bilgi güvenliği tehditleri zamana bağlı olarak ve gelişen teknoloji ile farklılıklar göstermektedir. Örneğin 1980'li yıllardan 2000'li yıllara doğru gidildikçe saldırgan bilgi seviyesinin düştüğü görülmektedir.



Şekil 2. Tarihsel Sürece Bağlı Saldırı Türleri, Saldırgan Bilgi Düzeyi ve Kullanılan Teknik Bilgi (Allen, 2001 akt. Canberk & Sağıroğlu, 2006)

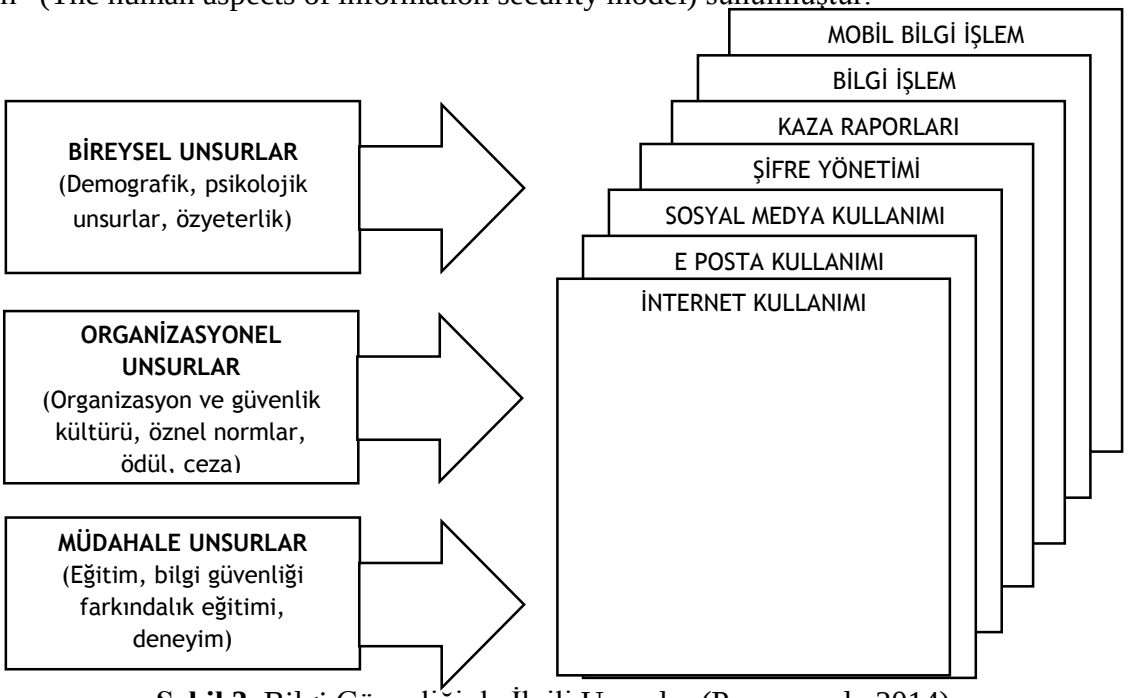
Zamana bağlı olarak saldırganın teknik bilgi düzeyi düştüğü halde giderek daha fazla sayıda saldırının yapıldığı görülmektedir. Bu durum, erişimi kolaylaşan yeni yazılımlar ve diğer

teknolojiler sayesinde saldırı yapmanın daha kolay hale gelmesiyle açıklanabilir. Başka bir ifadeyle bilgi ve iletişim teknolojilerindeki gelişmeler sayesinde karmaşık ve güvenli ortamlar kullanıma sunulmaktadır. Ancak bu yeni teknolojiler, kötü niyetli kişiler tarafından yeni tür saldırıların yapılması işleminde kullanılabilmektedir. Başka bir ifadeyle yeni teknolojiler sayesinde saldırıların yapılması işlemleri kolaylaşabilmektedir. Nitekim 1980'li yıllardan 2000'li yıllara doğru gidildikçe saldırı türlerinde de bir artış olduğu görülmektedir. Bu saldırı türlerinin artışının arkasında çok çeşitli nedenlerin olduğu söylenebilir. Bu nedenlere, ülkeler arasındaki gizli savaşların sanal alana taşınmış olması, büyük şirketler arasındaki güç savaşları, bilgi güvenliği alanında çalışan şirketlerin yeni pazar arayışları vb. durumlar örnek gösterilebilir.

Bilgi Güvenliğinin Kapsamı

Bilgi çağında bilgi güvenliğinin sağlanabilmesi için bilgi güvenliğinin kapsamı, bilgi güvenliği tehditlerinin tarihsel değişimi ve bilgi güvenliğinin sağlanmasında izlenilen yöntemlerin anlaşılması önemlidir. Geçmişten günümüze bilgi güvenliğinin sağlanması için fiziksel güvenlik, iletişim güvenliği, BİT sistemlerinin güvenliği ve ağ güvenliği konularında çalışmalar yapılmıştır (Maiwald, 2004). Kurum olarak bilgi güvenliğinin sağlanması, kurumun kâr etmesi, itibarını koruması, rekabet ve sürdürülebilir büyüme için sahip olduğu veya sahip olması gereken pazar, ürün, teknoloji ve organizasyona ait bilgilerin korunması anlamına gelir. Bilgi varlıklarının fiziksel olarak korunması, elektronik sistemlere istem dışı ulaşımının önlenmesi, BİT altyapısına erişimin kontrol altına alınması ve ağ güvenliğinin sağlanması ile mümkün olmaktadır (Meral, 2008; Vural & Sağıroğlu, 2008). Öte yandan bilgi güvenliğinin sağlanması; farklı formlardaki bilgilerin fiziksel önlemlerle korunmasının yanı sıra bireylerin bilgi güvenliği farkındalığını kazanması, bilgi güvenliğini sağlamaya dönük bilgi, tutum ve davranışları sergilemesi ile mümkün olmaktadır (Maiwald, 2004).

Şekil 3'te bilgi güvenliğinin insani açıdan kapsamını açıklayan "Bilgi Güvenliğinin İnsani Boyutu Modeli" (The human aspects of information security model) sunulmuştur.



Şekil 3. Bilgi Güvenliğiyle İlgili Unsurlar (Parsons vd., 2014).

Parsons vd. (2014) bilgi güvenliğiyle ilgili unsurları bir model önerisiyle ortaya koymuşlardır. Modelde bilgi, öncelikle "politika ve süreç bilgisi" olarak, daha sonra ise "politika ve sürece yönelik tutum ve öz-yansıtma davranışları" olarak kavramsallaştırılmıştır. Bu kavramsallaştırma İnternet kullanımı, e-posta kullanımı, sosyal ağ sitesi kullanımı, şifre yönetimi, olay bildirimi, bilgi işleme ile mobil bilişim işlemlerinde ve ortamlarında gerçekleşir. Bilgi, tutum ve davranış arasındaki ilişki, Şekil 3'te gösterildiği gibi "bireysel, örgütsel ve müdahale" şeklinde gruplanan birçok faktörden etkilenmektedir. Bireysel faktörler, "demografik, psikolojik ve özyeterlik"; organizasyonel faktörler, "organizasyonel ve güvenlik kültürü, öznel normlar, ödüller ve cezalar"; örgütsel müdahale faktörleri de "eğitim, bilgi güvenliği farkındalığı eğitimi, deneyim" gibi unsurlarla ilişkilidir. Bu faktörler bilgi güvenliğine dair bilgi, tutum ve davranışlar, farklı bilgi güvenliği politikaları ve süreçleriyle etkileşim içindedir.

Bilgi Güvenliğiyle İlgili Tehditler

Bilgi güvenliğiyle ilgili tehditler, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini olumsuz yönde etkileme durumu taşıyan riskler (Blanding, 2004) şeklinde ifade edilebilir. Tehditlerin bilgi sistemlerine zarar verecek düzeye erişmesinde bireysel ve teknik açıdan zafiyetler etkilidir. Öte yandan ITU (2011) bilgi güvenliğiyle ilgili tehditleri karakter, etki, köken ve aktörlere göre farklılaştırmaktadır. Bu tehditler;

a. Kazayla veya kasten tehditler
b. Aktif veya pasif tehditler
c. Tehdit kaynağı
d. Tehdit aktörü
e. Güvenlik açığı

şeklinde gruplanarak incelenebilir.

Örneğin, sistem veya yazılım hataları, fiziksel arızalar gibi kazayla ortaya çıkan tehditler, kasıtlı bir niyet olmaksızın ortaya çıkarken, kasıtlı tehditler, bir varlığın güvenliğine karşı gerçekleştirilmiş bilinçli eylemlerden kaynaklanmaktadır. Kasıtlı tehditler, bir bilgisayar ağını izlemede kullanılan izleme araçlarını kullanarak, özel sistem bilgisini kullanan karmaşık saldırıları içerir. Aktif tehditler, verilerin değiştirilmesi, yok edilmesi ve fiziksel ekipmanların imha edilmesi gibi, bir sistemin durumuna veya işletimine dair değişikliklerle sonuçlanan durumlardır. Pasif tehditler ise sistemin kaynaklarını etkilemeden bir sistemden bilgi toplanmasını amaçlayan bir tehdit türüdür. Öte yandan tehdit aktörünün herhangi bir tehdit kaynağı ile saldırıyı gerçekleştiren grup veya birey olduğu söylenebilir. Güvenlik açığı tehdit kaynakları ve tehdit aktörleri, çoğunlukla güvenlik kontrollerindeki zayıflıkları fırsat bilerek saldırıya geçmektedirler. Yazılım güncellemelerinin eksikliği veya zayıf güvenlik yapılandırması, personelin güvenlik ihlallerine karşı yeterli bilgiye sahibi olmaması ve bilgi güvenliği farkındalığı düşük olan BİT kullanıcılarının eylemleri bilgi güvenliği ihlallerinin oluşmasına neden olabilmektedir.

Öte yandan farklı tehdit kaynağından ortaya çıkan tehditler, uygun koşulların oluşmasıyla bilgi sistemlerine zarar verecek kusurları içeren zafiyetlere ve güvenlik ihlallerine yol açarak bilgi sitemlerine zarar vermektedir. Güldüren'e (2015) göre tehditler, tehdit kaynağı açısından bakıldığında;

a. Doğal afetler veya teknik arızalarla ilgili tehditler
b. Prosedürel eksiklerle ilgili tehditler
c. İnsan faktöründen kaynaklanan tehditler ve
d. Kötücül yazılımlarla ilgili tehditler,

şeklinde sıralanmaktadır.

Bilgi Güvenliği Eğitimi ve Bilgi Güvenliği Farkındalığıyla İlgili Çalışmalar

Bilgi güvenliği farkındalığı, bireylerin BİT kullanımında bireysel bilgilerini istenmeyen durumlardan korumak amacıyla gerekli güvenlik önlemlerini alma ve tehditlere karşı farkındalık sahibi olma durumudur (Vural & Sağıroğlu, 2008). Bu noktada bilgi güvenliği eğitimi ile bu konudaki ulusal ve uluslararası politikaların incelenmesi önem kazanmaktadır. Bilgi güvenliğinin insani açıdan kapsamını açıklayan ve Şekil 3'te sunulan modelde bilgi güvenliği eğitimlerinin önemi vurgulanmıştır. Öte yandan bilgi güvenliği ile ilgili araştırmaların yapılması, hem kullanıcıların bilgi güvenliği farkındalık düzeylerinin belirlenmesi ve hem de sunulacak bilgi güvenliği eğitimleri için ipuçları sunması açısından önemlidir.

Bilgi güvenliğini sağlamaya yönelik araştırmaların çoğunun güvenlik yazılımları ve modelleri oluşturma boyutlarında olduğu görülmektedir (Besnard & Arief, 2004; Mahabi, 2010; Vardal, 2009). Alanyazında insan faktöründen kaynaklanan bilgi güvenliği hatalarını belirlemeye ve bunları ortadan kaldırmaya yönelik araştırmaların son dönemlerde arttığı görülmektedir (Karaoğlan Yılmaz, Yılmaz & Sezer, 2014; Yılmaz, Karaoğlan Yılmaz, Öztürk & Karademir, 2017).

Stanton, Stam, Mastrangelo ve Jolton (2005) parola belirleme ile ilgili davranışlar üzerine bir çalışma yapmışlar ve parola belirleme davranışlarının bir örüntü taşıdığını raporlamışlardır. Mylonas, Kastania ve Gritzalis (2013) mobil cihazlardan uygulama indiren kullanıcıların genellikle ortamla ve indirecekleri uygulamayla ilgili olarak bir güvenlik kaygısı gütmedikleri sonucuna ulaşmışlardır. Araştırmacılar bu doğrultuda kullanıcıların uygulamanın yer aldığı ortama güven düzeylerine ilişkin kestirimlerde bulunulabilecek bir model geliştirmişlerdir. Öte yandan Magklaras, Furnell ve Brooke (2006) bir kurumun bilgi teknolojileri altyapısına kurum içinden yapılan saldırılar ve/veya kötü amaçlı kullanımlarla ilgilenmişlerdir. Bu amaçla sisteme yönelik kötü amaçlı kullanımlarla ilgili unsurlar tanımlanmaya çalışılmıştır. Araştırmacılar, bütün kötü amaçlı kullanımların analiz edilmesi ve tehditlerin önlenmesinde başvurulabilecek bir taksonomi geliştirmişlerdir.

Herath ve Rao (2009), normatif inançlar ve bilgi güvenliği politikalarına uyma niyetleri gibi potansiyel olarak bilgi güvenliği davranışlarına etki eden değişkenleri incelemiştir. Bununla birlikte, bu çalışmalar çalışma grubunun genel bilgi güvenliği bilincini/farkındalığını belirlemeye dönük değildir. Ünver, Canbay ve Mirzaoğlu (2009) yaptıkları araştırmada bilgi güvenliği zafiyetlerine vurgu yaparak, Türkiye'de internet üzerinden işlem yapmak için kullanılan TC Kimlik numarası ile kullanıcıların tüm kişisel bilgilerine erişilebildiğini, bu durumun da önemli güvenlik sorunlarını beraberinde getirdiğini ifade etmektedirler.

Karjalainen (2011) tarafından yapılan çalışmada bilgi güvenliği davranışları teknoloji kabul modellerine göre incelenmiştir. Söz konusu bu çalışma sonucunda teknoloji kabul modellerinin

sunduğu değişkenler bağlamında bilgi güvenliği davranışları incelendiğinden çalışmanın önemli sınırlılıklar taşıdığı belirtilmiştir. Vroom ve von Solms (2004) tarafından yapılan çalışmada, bilgi güvenliği farkındalığında kurumsal düzeyde bilgilendirmenin, politikaların, kişilik özelliklerinin, dahil olunan örgüt kültürü gibi birçok faktörün önemli olduğu vurgulanmıştır. Marinos (2013) yaptığı araştırmada saldırıların en fazla; indirilen programlar, zararlı yazılımlar, oltalama, sahte içerikli e-postalar, bilgi sızdırma ve fiziksel zarar şeklinde olduğunu ifade etmiştir.

Karaoğlan Yılmaz, Yılmaz ve Sezer (2014) tarafından yapılan çalışmada üniversite öğrencilerinin güvenli BİT kullanım davranışları belirlenmeye çalışılmıştır. Araştırmada öğrencilerin güvenli BİT kullanım davranışları sergilediği sonucuna ulaşılmıştır. Bununla birlikte bu davranış düzeyinin gelişen ve değişen teknolojik koşulların oluşturduğu yeni durumlara yanıt vermede yetersiz olduğu görülmektedir. Yapılan analiz sonuçları öğrencilerin, bilgisayara erişim güvenliği, zararlı programlar ve korunma yolları, sosyal mühendislik, parola güvenliği, dosya erişim ve paylaşım güvenliği, internet ve ağ güvenliği, e-posta güvenliği, yedekleme yapma gibi konularda temel düzeyde ve en popüler olarak bilinen güvenlik önlemlerinden yalnızca bir ya da birkaçını aldığını, diğer güvenlik önlemlerini ise almadıklarını göstermektedir.

Keser ve Güldüren (2015) tarafından yapılan çalışmada yükseköğretim kurumlarında çalışan öğretim elamanlarının bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirilmiştir. Çalışmada geliştirilen bu ölçek "saldırı ve tehditler" ile "kişisel verilerin korunması" şeklinde iki alt boyuttan oluşmuştur. Çalışma sonucunda ölçeğin geçerliğinin ve güvenirliğinin sağlandığı görülmüştür.

Güldüren, Çetinkaya ve Keser (2016) tarafından yapılan "Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması" başlıklı çalışmada ortaöğretim kurumlarında öğrenim gören öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemeye yönelik bir ölçek geliştirilmiştir. Bilgi güvenliği farkındalık ölçeğinin alt boyutları "saldırı ve tehditler", "mahremiyet" ve "kişisel verilerin korunması" olarak belirlenmiştir. Bu çalışma sonucunda ortaöğretim kurumlarındaki öğrencilerin bilgi güvenliği farkındalık düzeylerini belirlemek amacıyla geçerlik ve güvenirliği sağlanmış bir ölçek geliştirilmiştir. Ayrıca, bu ölçekle elde edilen verilere göre öğrencilerin bilgi güvenliği farkındalıkları ile cinsiyetleri arasında anlamlı bir farklılığın olduğu bulunmuştur. Bu bağlamda erkek öğrencilerin bilgi güvenliği farkındalıkları kadınlarınkine göre daha yüksek çıkmıştır.

Bilgi Güvenliği Politikaları

Uluslararası Düzeyde Bilgi Güvenliği Politikaları

Bilgi güvenliği eğitimine ve uygulanan politikalara bakıldığında ülkeler arasında farklı uygulamalar olduğu görülmektedir. Avrupa Birliği kapsamındaki ülkeler ile Amerika Birleşik Devletlerinde bireylerin bilgi güvenliklerini sağlamak amacıyla teknik anlamda birçok ulusal güvenlik standardının uygulandığı görülmektedir. Örneğin Amerika Birleşik Devletleri'nde, Ulusal Güvenlik Ajansının başkanlığında kurulan siber güvenlik biriminde, siber güvenlik tehditlerini izleme ve bunlarla mücadele etmek amacıyla çeşitli faaliyetler yürütülmektedir.

Çeşitli devletlerin mevcut siber güvenlik politikalarını geliştirmeleri veya gözden geçirmeleri için uluslararası bir takım stratejiler ortaya koydukları görülmektedir. Örneğin, Amerika Birleşik Devletleri açısından bakıldığında mevcut politikaların; siber tehditleri azaltma, caydırıcılık,

uluslararası katılım, olaya müdahale, esneklik ve geri kazanım politikaları ve faaliyetlerini kapsadığı görülmektedir. Bu süreçte küresel bilgi ve iletişim teknolojisi altyapısının güvenliği ve istikrarı ile ilgili olarak bilgisayar ağ sistemlerinin, bilgi güvenliği merkezlerinin, diplomasinin, kolluk kuvvetleri, ordu ve istihbarat birimlerinin işbirliği içinde çalıştıkları görülmektedir. Öte yandan Kuzey Kore'nin ise ulusal bilgi güvenliğini sağlamak amacıyla son yirmi yıldır siber güvenlik uzmanlarının yetiştirilmesine yönelik eğitimler sunduğu ve ayrıca İngilizcede "Certified WhiteHat Hacker" olarak adlandırılan kendi beyaz şapkalı bilgisayar uzmanlarını yetiştirdiği görülmektedir (Leyden, 2010; Zorz, 2010).

İngiltere'de, ülkeye yönelik siber saldırı ve tehditlerin artması ile birlikte 2009 yılında "Siber Güvenlik Stratejisi' başlıklı bir strateji belgesi yayınlanmıştır. Siber Güvenlik Stratejisi'nde ulusun siber sağlığının korunması ve ulusal kritik siber altyapının korunmasının önemine vurgu yapılmaktadır. Bu bağlamda İngiltere'de siber saldırıları izleyecek, analiz edecek ve önlemeye yönelik tedbirler alacak bilgi güvenliği uzmanlarından oluşan savunma ekipleri kurmaya karar verilmiştir. İngiltere'deki Siber Güvenlik Operasyon Merkezi siber güvenlik konusunda yeni bir hükümet stratejisinin bir parçası olarak görülmeye başlanmıştır. Bu merkezin Amerika Birleşik Devletleri'ndeki eşdeğer merkezlerle koordineli çalışarak saldırıları belirleme ve önlemler alma konusunda birlikte hareket ettikleri ifade edilmektedir (Phahlamohlaka, Jansen van Vuuren & Coetzee, 2011).

Bununla birlikte bilgi güvenliğinin sağlanmasında kullanıcı farkındalığının geliştirilmesine yönelik politikalar da teknik anlamda alınan önlemler kadar önemli bir boyut olarak görülmektedir. Bunun dışında gelişmekte olan ülkeler ile az gelişmiş ülkelerde ise kullanıcıların bilgi güvenliğinin sağlanması amacıyla daha çok teknik önlemlerle çözümler üretilmeye çalışıldığı görülmektedir. Amerika Birleşik Devletleri, Kanada, İngiltere, Güney Kore gibi gelişmiş ülkelerde bilgi güvenliği politikalarının belirlenmesi sürecine; ekonomik, politik, askeri, psikolojik vb. gibi birbiriyle ilişkili çok sayıda boyut gözetilerek yaklaşılmakta ve bilgi güvenliği stratejileri bu boyutlar dikkate alınarak belirlenmektedir.

Gelişmiş bilgi ve iletişim teknolojisi altyapısı ve insan gücüne sahip olan Güney Kore'nin ulusal bilgi güvenliği politikalarına bakıldığında bir dizi eylemin ve alınması gerekli önlemin öne çıktığı görülmektedir. Bu politikalar; "siber güvenliğin desteklenmesinde ilgili yapıların kurulmasını kolaylaştırmak; siber güvenlik tehditlerinin ve güvenlik açıklarının azaltılmasının sağlamak; devlet ve özel sektör arasındaki işbirliğini ve koordinasyonu desteklemek; siber güvenlik konusunda uluslararası işbirliğini teşvik etmek ve güçlendirmek; kapasite oluşturma ve siber güvenliğin kültürünü teşvik etmek; uygun teknik ve operasyonel siber güvenlik standartlarına uyumu teşvik etmek" (Phahlamohlaka, Jansen van Vuuren & Coetzee, 2011) şeklinde listelenebilir.

ABD'de, ulusal siber politikasının asgari olarak "yönetim, mimari, davranış normları, kapasite geliştirme" gibi dört ana unsuru dikkate alması gerektiği öne sürülmektedir:

> Yönetim: İlgili politikaların geliştirilmesi ve yürütülmesinde hükümet yapılarının etkin rol alması gerekmektedir. Bu unsur, çeşitli birim ve kurumlarla yetki sahibi olmanın sonucu olan örtüşmeleri ve sorumlulukları gözden geçirmeyi içerir.

Mimari: Mimari yapı gelecekte ihtiyaç duyulacak en uygun sistem karakteristikleri için mevcut bilgi ve iletişim sistemlerinin ve altyapısının performans, maliyet ve güvenlik özelliklerinin yanı sıra stratejik planlamalara hitap eder. Bu unsur standartlar, kimlik yönetimi, kimlik doğrulama ve ilişkilendirme, yazılım güvencesi, araştırma ve geliştirme, tedarik ve tedarik zinciri risk yönetimini içerir.

Davranış Normları: Hukuk, yönetmelik ve uluslararası antlaşmalar ve teşebbüs gibi unsurların yanı sıra, siber uzayda davranış standartlarını kolektif olarak sınırlandıran ve tanımlayan en iyi uygulamalar gibi fikir birliğine dayalı önlemleri de ele alır.

Kapasite Geliştirme: Bu unsur, daha fazla siber etkin ve yetkin bir millet olmak için gereken kaynakların, faaliyetlerin ve yeteneklerin toplam ölçeğini kapsamaktadır. Bunlar arasında kaynak gereksinimleri, araştırma ve geliştirme, kamu eğitimi ve farkındalığı, uluslararası ortaklıklar, vatandaşlık ve işgücü ile geleceğin dijital bilgi ve iletişim altyapısının inşa edilmesini sağlayan tüm diğer faaliyetler yer almaktadır (Phahlamohlaka, Jansen van Vuuren & Coetzee, 2011).

Kanada'nın ulusal siber politikasının anahtar öğelerinin ise; uluslararası, sektörler arası stratejilerin önemli olduğu görülmektedir. Bu bağlamda uluslararası, sektörler arası çeşitli paydaşlarla bilgi paylaşımına ve işbirliklerinin geliştirilmesine önem verilmektedir. Hükümet, bu ilişkileri ve ortaklıkları cesaretlendirmede, ilerlemeyi analiz etmede ve yeni gelişmeleri izlemede rol oynamaktadır. Yine bir başka önemli nokta, hesap verebilirlik ve uygun davranış çizgilerini belirleyerek bilgi güvenliğini sağlama konusudur. Bu kapsamda Kanada kamusal farkındalığı geliştirmek amacıyla siber okuryazarlığın teşvik edilmesine önem vermekte ve bu doğrultuda uygulamalar gerçekleştirmektedir.

Türkiye'de Bilgi Güvenliği Politikalarına Bakış

Türkiye'deki bilgi güvenliğiyle ilgili uygulamalara bakıldığında ilk olarak "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" başlıklı doküman göze çarpmaktadır (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2013). Daha sonra, gelişen teknolojik alt yapı, saldırı sayısı ve çeşitliliğinin artması, uluslararası politikalardaki değişimler gibi sebeplerle strateji ve eylem planının güncellenmesine ihtiyaç duyulmuş ve Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından "2016-2019 Ulusal Siber Güvenlik Stratejisi" hazırlanmıştır (Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, 2016). Bu dokümanda, stratejik siber güvenlik amaçları ve eylemleri kapsamında; siber savunmanın güçlendirilmesi ve kritik altyapıların korunması, siber suçlarla mücadele, farkındalık ve insan kaynağı geliştirme, siber güvenlik ekosisteminin geliştirilmesi ve siber güvenliğin milli güvenliğe entegrasyonu gibi boyutların yer aldığı dikkatleri çekmektedir.

Türkiye'nin bilgi güvenliği politika ve stratejilerine bakıldığında Amerika Birleşik Devletleri, Kanada, İngiltere, Güney Kore gibi gelişmiş ülkelerin bilgi güvenliği politikalarının belirlenmesinde de rol oynayan; ekonomik, politik, askeri, psikolojik, bilgi/eğitim/farkındalık gibi öğelerin birbiri ile entegrasyonunu sağlamaya yönelik adımların atıldığı görülmektedir. Bu bağlamda Milli Eğitim Bakanlığı tarafından "Bilişim Teknolojileri ve Yazılım" dersi kapsamında öğrencilerin bilgi güvenliği farkındalıklarını artırmaya yönelik kazanımlara yer verildiği, ayrıca çeşitli kamu kurum ve kuruluşlarının personelinin bilgi güvenliği farkındalıklarını artırmak için

hizmet içi eğitim etkinlikleri planladıkları/uyguladıkları görülmektedir. Öte yandan kullanıcı farkındalığının artırılmasına yönelik olarak, Bilgi Teknolojileri ve İletişim Kurumu ile Aile ve Sosyal Politikalar Bakanlığı gibi kurum ve kuruluşların çeşitli kongre, sempozyum ve çalıştay gibi etkinlikler düzenledikleri ve ayrıca kamu spotları hazırladıkları görülmektedir. Fiziksel ve teknik alt yapının güçlendirilmesiyle ilgili olarak da Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından "Ulusal Kamu Entegre Veri Merkezi Projesi" kapsamında kamu kurumlarının veri merkezlerinin güvenilir alt yapılar içerisinde saklanabilmesine yönelik çalışmalar başlatılmıştır. Bu arada ABD ve İngiltere örneklerinde olduğu gibi beyaz şapkalı bilgisayar korsanları yetiştirmek ve bunların ulusal güvenlik süreçlerinde kullanılmasını sağlamak amacıyla da Bilgi Teknolojileri ve İletişim Kurumu tarafından Ulusal Siber Olaylara Müdahale Merkezi isimli bir birim kurularak çalışmalara başlandığı görülmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2015). Ayrıca benzer amaçlar doğrultusunda Türk Silahlı Kuvvetleri bünyesinde Siber Savunma Komutanlığı kurulmuştur.

Türkiye'de bilgi güvenliğinin sağlanması ile ilgili olarak atılan bu adımların bilgi/eğitim/farkındalık, ekonomik, politik, askeri ve teknik alt yapı anlamında adımlar olduğu söylenebilir. Bununla birlikte bilgi güvenliğinin psikolojik boyutları ile ilgili adımların ise üniversitelerce yürütüldüğü söylenebilir. Üniversitelerde, bireylerin bilgi güvenliği farkındalıklarını tespit etmek ve bu farkındalık üzerinde etkili değişkenleri belirlemeye yönelik gerçekleştirilen araştırmalar bu bağlamda yürütülen çalışmalara örnek olarak verilebilir. Bu çalışmaların birbiri ile koordineli bir şekilde, kurumlar-arası işbirliğiyle, bilgi paylaşımı sağlanarak ve bu doğrultuda geleceğin ihtiyaçları kapsamlı olarak belirlenerek yürütülmesi durumunda daha işlevsel sonuçlara ulaşılacağı açıktır.

Tartışma, Sonuç Ve Öneriler

Bilgi güvenliği, bir varlık türü olarak bilginin izinsiz veya yetkisiz bir biçimde erişimini, kullanımını, değiştirilmesini, ifşa edilmesini, ortadan kaldırılmasını, el değiştirmesini ve hasar verilmesini önlemek olarak tanımlanabilir. Bu tanımdan hareketle bilgi güvenliğinin, "gizlilik, bütünlük ve erişilebilirlik" olarak isimlendirilen üç temel unsurdan meydana geldiği söylenebilir (Puhakainen, 2006; akt. Güldüren, 2015). Bu bağlamda bilgi güvenliği politika ve stratejileri, "bilginin gizliliği, bütünlüğü ve erişilebilirliği" gibi unsurlar göz önüne alınarak geliştirilmektedir. Bununla birlikte "bilgi güvenliği" birçok disiplini de içerisinde barındıran karmaşık, bütüncül ve disiplinler arası bir süreçtir. Bu duruma bağlı olarak bilgi güvenliğiyle ilgili tehditler; karakter, etki, köken ve aktörlere göre farklılaştırmaktadır (ITU, 2011). "Bilgi güvenliği farkındalığı" ise bireylerin, BİT kullanımında kişisel bilgilerini tehlikelerden korumak amacıyla gerekli güvenlik önlemlerini alma ve tehditlere karşı farkındalık sahibi olma durumu olarak ifade edilir. Alanyazında bilgi güvenliğini sağlamaya ve bilgi güvenliği farkındalığını belirlemeye yönelik araştırmalar bulunsa da bu araştırmaların önemli bir kısmında bilgi güvenliğinin, güvenlik yazılımları ve modelleri oluşturma boyutlarında ele alındığı görülmektedir (Besnard & Arief, 2004; Mahabi, 2010; Vardal, 2009). Bununla birlikte alanyazında insan faktöründen kaynaklanan bilgi güvenliği hatalarını/farkındalığını belirlemeye ve bunları ortadan kaldırmaya yönelik araştırmaların son dönemlerde arttığı görülmektedir (Karaoğlan Yılmaz, Yılmaz & Sezer, 2014; Yılmaz, Karaoğlan Yılmaz, Öztürk & Karademir, 2017).

Bilgi güvenliği konusuna uluslararası düzeyde bakıldığında, ABD, Kanada, İngiltere, Güney Kore gibi gelişmiş ülkelerin bilgi güvenliği politikalarının ve stratejilerinin belirlenmesi sürecine; ekonomik, politik, askeri, psikolojik, bilgi/eğitim/farkındalık gibi farklı öğeler bağlamında yaklaştıkları, bu süreçte konunun temel öğeleri arasındaki entegrasyonu sağlayarak bütüncül bir sistem ortaya koymaya çalıştıkları görülmektedir. Bu nedenle Türkiye'de bilgi güvenliğinin sağlanmasına yönelik planlamalar yaparken de bilgi güvenliği sisteminde yer alan tüm unsurların dikkate alınarak, birbiri ile koordineli olacak şekilde bütüncül sistemlerin ortaya konulmasının önemli olduğu söylenebilir.

Türkiye'de bilgi güvenliğini artırmaya yönelik mevcut çalışmaların, henüz kullanıcı farkındalığının geliştirilmesi ve teknolojik alt yapının iyileştirilmesi boyutunda olduğu söylenebilir. Kullanıcı farkındalığını geliştirmek amacıyla Milli Eğitim Bakanlığının "Bilişim Teknolojileri ve Yazılım" dersinin bazı kazanımlarında bilgi güvenliği farkındalığına yer verildiği görülmektedir. Bununla birlikte eğitim sürecinin her aşamasında buna yönelik kazanımlara yer verilmesi, kazanımların güncel tehdit ve saldırı durumları göz önüne alınarak güncellenmesi de bir o kadar önemli bir boyuttur. Bu nedenle "Bilişim Teknolojileri ve Yazılım" dersi öğretim programlarının yapılandırılması sürecinde bunların göz önünde bulundurulması gerekir.

Bilgi güvenliği birçok halkadan oluşan bir zincir olarak görüldüğünde bu zincirin en zayıf halkasının insan faktörü olduğu söylenebilir. Bu nedenle insan faktörü boyutunun güçlendirilmesi yalnızca resmi öğretim kurumlarında kazandırılacak bilgi ve beceriler şekilde düşünülmemelidir. Özellikle yetişkinlerin de toplumsal yaşamın her alanına girmiş olan teknolojiyle iç içe olduğu günümüzde, onların bu konuyla ilgili farkındalıklarını artırmaya yönelik yaşam boyu öğrenme programları düzenlemek ve ayrıca kamu spotları hazırlamak kullanıcı farkındalığı ile ilgili olarak göz önüne bulundurulması gereken bir diğer önemli noktadır.

Bilgi güvenliği konusu teknolojik alt yapı açısından da ele alınabilir. Bu bağlamda Türkiye'deki internet alt yapısının, veri depolama merkezlerinin, bilgisayar ve telefonlarda kullanılan işletim sistemi, program ve uygulamaların da güvenliğinin sorgulanarak, bunlara yönelik önlemlerin alınmasının gerekli olduğu söylenebilir. Özellikle de işletim sistemi, iletişim ve anti-virüs programlarıyla ilgili olarak yerli yazılımların üretilmesinin ve kullanımının desteklenmesinin önemli olduğu anlaşılmaktadır.

Bilgi güvenliğinin sağlanması ile ilgili önemli hususlardan bir diğeri ise politika ve stratejilerin belirlenmesinde paydaş kurum ve kuruluşların bir araya gelerek ulusal politika ve stratejileri belirlemeleridir. Nitekim gelişmiş ülkelerin bilgi güvenliği stratejilerinde dikkat çeken en önemli noktalardan biri konuyla ilgili kurum ve kuruluşlar arasında işbirliği, bilgi paylaşımı ve koordinasyonun sağlanmış olmasıdır. Hatta uluslararası kurum ve kuruluşlar da bu sürece dahil edilmeye çalışılmaktadır. Türkiye'deki kurum ve kuruluşların her birinin bilgi güvenliği konusunda belli bir amaç ve çaba içerisinde oldukları, ancak uygulamalar arasında entegrasyonun sağlanmasında problemler yaşandığı dikkatleri çekmektedir. Bu nedenle Türkiye'de sürdürülebilir bir strateji ve eylem planının ortaya konulmasında bu hususun da dikkate alınması gerekir.

Yansıtma Soruları

1. Ulusal düzeyde bilgi güvenliği farkındalığı oluşturulması için neler yapılabileceğini tartışınız.
2. Ulusal ve uluslararası düzeyde uygulanan bilgi güvenliği politikalarını, bilgi güvenliği risk ve tehditlerini ortadan kaldırma yeterliği açısından karşılaştırınız.
3. Tüm eğitim düzeyleri açısından bakıldığında Türkiye'deki bilgi güvenliği eğitiminin yeterli olup olmadığını tartışınız.
4. Bilgi güvenliği tehditlerine maruz kalındığında bireysel ve kurumsal düzeyde yapılması gerekenleri tartışınız.
5. Bilgi güvenliği risk ve tehditlerinden korunmak için bireysel ve kurumsal düzeyde alınması gereken önlemleri açıklayınız.

Kaynaklar

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. Computers & Security, 23(3), 253-264.

Bilgi Teknolojileri ve İletişim Kurumu (2015). USOM ve kurumsal SOME'ler. 08.03.2018 tarihinde https://www.btk.gov.tr/tr-TR/Sayfalar/SG-USOM-ve-Kurumsal-SOME adresinden erişildi.

Blanding, S. F. (2004). An introduction to LAN/WAN security. Information security management handbook (Fifth Edition). New York: Auerbach Publications.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3), 165-174.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. Computers & Security, 25(1), 27-35.

Güldüren, C. (2015). Yükseköğretim kurumlarındaki öğretim elemanlarının bilgi güvenliği farkındalık düzeylerinin değerlendirilmesi. Yayımlanmamış doktora tezi. Ankara Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Güldüren, C., Çetinkaya, L., & Keser, H. (2016). Ortaöğretim öğrencilerine yönelik bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. İlköğretim Online, 15(2), 682-695.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. European Journal of Information Systems, 18(2), 106-125.

ITU (2011). ITU National cybersecurity strategy guide. 08.11.2017 tarihinde http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf adresinden erişildi.

ITU (2015). Global cybersecurity index & cyberwellness profiles report. 08.11.2017 tarihinde http://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf adresinden erişildi.

ITU (2017). ITU World telecommunication / ICT Indicators database. 08.03.2018 tarihinde http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx adresinden erişildi.

Karaoğlan Yılmaz, F. G., Yılmaz, R., & Sezer, B. (2014). Üniversite öğrencilerinin güvenli bilgi ve iletişim teknolojisi kullanım davranışları ve bilgi güvenliği eğitimine genel bir bakış. Bartın Üniversitesi Eğitim Fakültesi Dergisi, 3(1), 176-199.

Karjalainen, M. (2011). Improving employees' information systems (IS) security behavior: Toward a meta-theory of IS security training and a new framework for understanding employees' IS security behavior. Academic dissertation. University of Oulu, Faculty of Science, Department of Information Processing Science, Finland.

Keser, H., & Güldüren, C. (2015). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. K.Ü. Kastamonu Eğitim Dergisi, 23(3), 1167-1184.

Leyden, J. (2010). South Korea sets up cyber warfare unit to repel NORK hackers. 08.03.2018 tarihinde http://www.theregister.co.uk/2010/01/12/korea_cyberwarfare_unit/ adresinden erişildi.

Magklaras, G. B., Furnell, S. M., & Brooke, P. J. (2006). Towards an insider threat prediction specification language. Information Management & Computer Security, 14(4), 361-381.

Maiwald, E. (2004). Fundamentals of network security. McGraw Hill: Burr Ridge, IL.

Mahabi, V. (2010). Information security awareness: System administrators and end-users perspectives at Florida State University. Unpublished doctoral dissertation, Florida State University.

Marinos, L. (2013). ENISA Threat landscape 2013: Overview of current and emerging cyber-threats. Heraklion: European Union Agency for Network and Information Security Publishing. 11.03.2018 tarihinde https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport adresinden erişildi.

Meral, M. (2008). Siber savunma: Ülkeler ve stratejiler. 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Aralık 2008, Ankara. 08.03.2018 tarihinde http://www.iscturkey.org/s/2226/i/2008-posters-03.pdf adresinden erişildi.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. Computers & Security, 34, 47-66.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q). Computers & security, 42, 165-176.

Pattinson, M., Jerram, C., Parsons, K., McCormac, A., & Butavicius, M. (2012). Why do some people manage phishing e-mails better than others? Information Management & Computer Security, 20(1), 18-28.

Phahlamohlaka, L. J., Jansen van Vuuren, J. C., & Coetzee, A. J. (2011). Cyber security awareness toolkit for national security: An approach to South Africa's cyber security policy implementation. 21.02.2018 tarihinde https://researchspace.csir.co.za/dspace/bitstream/handle/10204/5162/Phahlamohlaka_2011.pdf?sequence=1&isAllowed=y adresinden erişildi.

Pricewaterhouse Coopers (PWC) (2015). Turnaround and transformation in cybersecurity: Key findings from The Global State of Information Security Survey 2016. 18.02.2018 tarihinde https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf adresinden erişildi.

Puhakainen, P. (2006). A design theory for information security awareness. Academic dissertation. University of Oulu, Faculty of Science, Department of Information Processing Science, Finland.

Shropshire, J., Warkentin, M., Johnston, A., & Schmidt, M. (2006). Personality and IT security: An application of the five-factor model. AMCIS 2006 Proceedings, 415, 3443-3449.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. Computers & Security, 24(2), 124-133.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating information security awareness: Research and practice gaps. Information Security Journal: A Global Perspective, 17(5-6), 207-227.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, Ankara. 08.03.2018 tarihinde https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FBTDNewFolder%2FSiber+Güvenlik%2F2_1_Strateji+Eylem+Planı+2013-2014.pdf adresinden erişildi.

Ulaştırma, Denizcilik ve Haberleşme Bakanlığı (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. 08.03.2018 tarihinde http://www.udhb.gov.tr/doc/siberg/2016-2019guvenlik.pdf adresinden erişildi.

Ünver, M., Canbay, C., & Mirzaoğlu, A. G. (2009). Siber güvenliğin sağlanması: Türkiye'deki mevcut durum ve alınması gereken tedbirler. Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ankara. 08.03.2018 tarihinde http://www.academia.edu/download/45165390/Siber_Guvenligin_Saglanmasi__Turkiyedeki_Mevcut_Durum_ve_Alinmasi_Gereken_Tedbirler.pdf adresinden erişildi.

Vardal, N. (2009).Yükseköğretimde bilgi güvenliği: Bilgi güvenlik yönetim sistemi için bir model önerisi ve uygulaması. Yayımlanmamış doktora tezi. Gazi Üniversitesi, Eğitim Bilimleri Enstitüsü, Ankara.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. Computers & Security, 23(3), 191-198.

Vural, Y., & Sağıroğlu Ş.(2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23(2), 507-522.

Yılmaz, R., Karaoğlan Yılmaz, F.G., Öztürk, T., & Karademir, T. (2017). Lise öğrencilerinin güvenli bilgisayar ve internet kullanım farkındalıklarının incelenmesi: Bartın ili örneği. Pegem Eğitim ve Öğretim Dergisi, 7(1), 83-114.

Zorz, Z. (2010). South Korea preparing for cyber war. 08.03.2018 tarihinde http://www.net-security.org/secworld.php?id=8722 adresinden erişildi.