Bilgi güvenliği

Bilgi sistemlerinin ve bileşenlerinin hukuka aykırı veya yetkisiz her türlü müdahale veya etkiden korunması; bilgi ile ilgili yapılan her türlü işlemde bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin temini ve bu işlemlerin sadece yetkili kişiler tarafından yapılmasının sağlanmasına bilgi güvenliği denir.

Bilgi güvenliği, kurumsal varlıklar arasında belki de en önemli yere sahip olan bilginin tahribat, silinme, bozulma gibi zarar verici unsurlara ve olası saldırılara karşı korunmasını sağlayan birtakım uygulamaları kapsamaktadır[1]. Bilgi güvenliği, bilginin yetkisiz kişilerce kullanımının önlenmesi, doğruluk ve bütünlüğünün korunması ve yetkisi olan bireyler tarafından erişilmesini sağlamak şeklinde tanımlanmaktadır.

Bilgi merkezlerinde ve kar amacı gütmeyen kurumlarda ise bilgi güvenliği, ağ kaynaklarını kontrol edebilmek, kurumu siber tehditlere karşı koruyabilmek, gelebilecek saldırılara karşı bilgi sistemlerini koruyucu tedbirler almak ve saldırıları öngörebilmektir[2].

0.1 Bilgi Güvenliği İlkeleri Nelerdir ?

Bilginin sürekli korunmasını gerektiren üç temel ilke bulunmaktadır. Bu üç temel ilke gizlilik, bütünlük ve erişilebilirlik ya da süreklilik ilkesi olarak sıralanabilir.

Nitelik ya da ilkelerden biri olan gizlilik; bilginin yetkisi olmayan kişilerce erişilemez hale getirilmesini sağlamayı kapsamaktadır. Ancak bilgi hırsızları ve/veya sosyal mühendisler olarak bilinen saldırganlar bu bilgileri ve şifreleri izinsiz ve gizli şekilde elde edebilmektedirler. Şifrelerin ele geçirme, çalma ya da tahmin yöntemleriyle kırılması gizlilik ilkesine aykırı davranışlardır.

Bütünlük ilkesi göndericiden alıcıya iletilen bilginin değiştirilmeden ya da bozulmadan alıcıya ulaşmasını sağlamaya yönelik uygulamaları içerir[2] .

Erişilebilirlik ya da süreklilik ilkesi ise sistemin kurum içi ve kurum dışı kimselerce zarar verilmeden kullanılmasını ve sürekliliğin korunmasını sağlayan uygulamaları kapsar[3] .

Bu ilkeler ve benzer diğer önlemler bilgi merkezleri ve/veya diğer kurumlarda bulunan bilgileri ve kişisel verileri korumaya yönelik faaliyetlerdendir. Bu tür faaliyetler içinde bulunduğumuz bilgi toplumu çağının bir getirisi olan siber saldırı, kişisel verilerin ele geçirilmesi, bilgi hırsızlığı, kimlik hırsızlığı, veri madenciliği vd. suç türlerini önlemek amacıyla yapılmış ve yapılmakta olan önlemler olarak ele alınabilir.

0.2 Bilgi Güvenliğini Sağlamada Faydalanılan Süreçler

Bilgi güvenliği oldukça kapsamlı ve karmaşık bir süreçtir. Bilgi güvenliğinin sağlanması üç temel sürecin birlikte yürütülmesi ile yakından ilgilidir. Bu üç temel süreci yönetsel süreç, teknolojik önlem süreci, eğitim ve farkındalık süreci olarak tanımlayabiliriz.

Bunlardan biri doğru plan, strateji ve politikalarla doğru bilgi güvenliği yönetimi uygulamalarını kapsayan yönetsel süreç, ikincisi şifreleme, güvenlik duvarları, anti virüs yazılımları, yedekleme, denetim gibi teknik içerikli çözümleri kapsayan teknolojik önlem süreci ve son olarak kullanıcıların eğitim yoluyla bilgi güvenliği bilinci kazanmalarını sağlayan eğitim ve farkındalık sürecidir.

0.2.1 Bilgi Güvenliğini Sağlama ile İlgili TCK Maddeleri

Türkiye'de bilgi merkezlerinde bilgi güvenliğinin sağlanması konusu ile ilgili yasal düzenlemeler Türk Ceza Kanunu'nun 243 ve 244. maddelerinde yer almaktadır.

Türk Ceza Kanunu'nun 243. maddesi bilişim sistemine hukuka aykırı olarak girme suçunu; 244. maddesi ise bilişim sisteminin işleyişini engelleme, bozma, verileri yok etme veya değiştirme suçunu düzenlemektedir. Fakat bu konuda kamu kuruluşlarına ve özel kuruluşlara yol gösteren ya da birtakım önlemlerin alınması konusunda zorunluluk getiren yasal düzenlemeler bulunmamaktadır. Bu konuda yol gösterici olarak nitelendirilebilecek en önemli çalışma ve aynı zamanda ilk uluslararası sözleşme, 2001 yılında kabul edilen Avrupa Konseyi Siber Suçlar Sözleşmesi'dir. Avrupa Konseyi Siber Suçlar Sözleşmesi; siber suçları tanımlamakta, cezai soruşturma ve kovuşturma yöntemlerini belirlemekte ve üye ülkeler arasında işbirliği ve koordinasyonun geliştirilmesini sağlamayı amaçlamaktadır[4].

Bahsedilen bu yasal düzenlemelerin eksikliği, bilgi merkezleri ve diğer kurumların bünyesinde bulunan bilgilerin ve/veya kişisel verilerin korunması yönünde önemli bir sorun teşkil etmektedir. Bu sorunun çözümüne yönelik çalışmaların az olması ise başta biz bilgi uzmanları ve konu ile ilgili diğer tüm sorumluların bir eksikliğidir. Bu sorunun çözümüne yönelik çalışmaların sayısı artırılmalı ve bilgi merkezleri başta olmak üzere diğer kurumların bünyesinde bulunan veriler koruma altına alınmalıdır.

0.3 Bilgi Merkezlerinde Bilgi Güvenliği Nedir ve Neden Sağlanmalıdır ?

Elektronik ortamda yer alan bilgi, günümüzde bir varlık olarak algılanmalıdır. Özellikle elektronik bilgilerin yoğun olarak toplandığı kütüphaneler, arşivler, dokümantasyon ve enformasyon merkezlerinde; bilginin gizliliğinin ve bütünlüğünün bir varlık olarak korunması bilgi profesyonelleri tarafından uyulması zorunlu yükümlülükler haline gelmiştir.

Elektronik depolama ortamlarındaki binlerce önemli ve korunması zorunlu veri nedeniyle hemen her özel kuruluş ya da kamu kuruluşu gibi; bilgi merkezlerinin de günümüzde ve yakın gelecekte işlevsel doğası gereği siber saldırı denemelerinin öncelikli hedefleri arasında yer alacağı öngörülebilir[4].

Bilgi merkezlerindeki dijitalleştirilme çalışmalarının hız kazandığı ve elektronik ortamda oluşturulmuş bilgi oranının katlanarak arttığı düşünüldüğünde, bilgi merkezlerinin bilgi güvenliğinin sağlanması konusundaki sorumluluklarının da her geçen gün artmakta olduğu söylenebilir. Bilgi hizmetlerinde bilgi sistemlerine bağlılığın artması, tehditlere daha fazla açık olma anlamına gelmektedir. Bilgi merkezlerinde görülen bu bağlılıkla beraber oluşacak olası siber saldırı tehditleri, bilgi güvenliğinin sağlanması konusunda alınması gereken önlemler de artmakta ve bilgi merkezlerine düşen görev ve sorumluluklar daha da önem kazanmaktadır.

0.4 Bilgi Merkezlerinde Bilgi Güvenliği Nasıl Sağlanmalıdır ?

Bilgi teknolojilerinin kullanımının her geçen gün arttığı bilgi merkezlerinde özellikle elektronik ortamda bilgi erişimlerinin artmasıyla birlikte, bilgi merkezlerinde bulunan kişisel bilgilerin gizliliğine yönelik tehditler artacak ve güvenlik açıklarına yol açacaktır.

Gizliliğin korunması ile ilgili yerel olarak bir bilgi merkezinde alınması gereken önlemler konusunda, American Library Assocation'ın belirlediği şablon üzerinden aşağıda yer alan temel hususlar örnek alınabilir. Buna göre;

Elektronik ortamda bulunan verilerin erişimi konusunu da içine alacak şekilde yazılı bilgi güvenliği ve gizlilik politikasının geliştirilmesi,

Bilgi merkezlerinde çalışan tüm bilgi profesyonellerinin hukuksal ve etik sorumluluklar konusunda eğitilmesi,

Bilgi profesyonellerinin yetkisiz erişimlerin tespiti ve gizliliğin ihlal edildiği bu tür durumlarda hangi birimlerle (bilgi işlem ve savcılık gibi) koordineli olarak çalışacağı konusunda bilgilendirilmesi,

Yapılan düzenlemelerle ilgili üyelik sürecinde ve sonrasında kullanıcıların bilgilendirilmesi. Bilgi güvenliği ve gizliliğin sağlanması konusunda kullanıcıların alacakları önlemlerin bildirilmesi,

Yapılan sözleşmelerin kütüphane politikalarına, kullanıcı gizliliğinin korunması ilgili etik değerlere ve hukuksal düzenlemelere uygun olması,

Küçük yaştaki bilgi merkezi kullanıcılarının ailelerinin de bilgi merkezinde geçerli olan gizlilik politikaları ile ilgili olarak bilgilendirilmeleri ve belirlenen politikalar dahilinde belirli bir yaşın altında (örneğin; Amerika'daki "Çocukların Çevrimiçi Gizliliğini Koruma Yasası" içinde 13 yaş sınırı olduğu gibi) bulunan küçüklerden ailesinin bilgisi dışında kişisel bilgi alınmaması, yerel bir bilgi merkezinin alabileceği uygulanabilir[4].

ALA'nın belirlemiş olduğu şablonu inceleyecek olduğumuz da bilgi merkezlerinde bilginin korunmasına yönelik birtakım çalışmaların bulunduğunu görmekteyiz. İçinde bulunduğumuz bilgi toplumunun bir getirisi olan teknolojik gelişmeler, beraberinde birçok problemi getirmiştir. Bu durumu bilgi merkezleri bünyesinde inceleyecek olursak bilgiye kolay erişim, bilgiye izinsiz erişim gibi problemleri sıralayabiliriz. Tüm bu tehditleri ortadan kaldırmak için ise tıpkı ALA'nın yapmış olduğu gibi çözüme yönelik şablonlar ya da daha farklı çözüm yolları belirlemeliyiz.

0.4.1 Bilgi Merkezlerinde Bilgi Güvenliği İçin Çözüm Önerileri

Kütüphanelerde bilgi güvenliğini sağlamanın teknik içerikli birtakım uygulamaları olmakla birlikte en önemli rol insana düşmektedir. Bu nedenle kütüphanelerde bilgi güvenliğine ilişkin bilinç ya da farkındalığın arttırılması kütüphane faaliyetlerinin amaca uygun ve sorunsuz bir şekilde yürütülmesinde büyük önem taşıyacaktır. Bu çerçevede verilecek bir farkındalık eğitiminin, bilgi güvenliği bilincinin arttırılmasında önemli bir rol üstleneceği düşünülmektedir.

Bilgi güvenliği ile ilgili sorumlulukların bir görev anlayışıyla yerine getirilmesinin güvenlik ihlallerinin azalmasında önemli bir rol oynayacağı düşünülmektedir.

Kütüphane personeli kullandıkları yazılımların güvenlik eklentilerinin güncellenmesi, anti virüs yazılımlarının kullanılması, saklanan verilerin yedeklenmesi gibi tedbir uygulamalarını gerçekleştirecek sosyal mühendislik saldırıları da dahil olmak üzere olası her türlü tehdide karşı kütüphane materyallerinin korunmasına katkı sağlayabilirler.

Kütüphane koleksiyonunda yer alan materyallerin ve internet araçlarının kullanımı kurumsal bir politika ile net bir şekilde ifade edilmelidir. Kural dışı kullanım için cezai yaptırımların uygulanmasının caydırıcı olabileceği düşünülmektedir.

Kütüphane kaynaklarının güvenli bir şekilde kullanılması hususunda kullanıcılara verilecek eğitimin karşılaşılan güvenlik sorunlarını azaltacağı düşünülmektedir. Bu amaçla özellikle kullanıcı eğitimi ya da rehberlik hizmeti veren kütüphanecilerin gerçekçi hedeflerle tasarlanmış

bir eğitim programı ile kullanıcılara gerekli eğitimi sunması çözümleyici olabilir.

0.5 Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı

Bilgi merkezlerinin yaşanabilecek olan her türlü siber tehdide karşı önlem alabilmesi, personelin ve/veya çalışanın bu tehdide karşı bilinçlendirilmesi için bilgi uzmanlarının kurumsal politikalar çerçevesinde farkındalık yaratması ve bunu personele kabul ettirmesi gerekmektedir.

0.5.1 Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı Yaratmanın Önemi

Bilgi merkezlerinde çevrimiçi kaynakların, kurumsal amaçların dışında kullanımı ve bunun sonucunda ortaya çıkacak riskler, verimlilik kayıpları ve zararlı yazılımlara maruz kalması ile birlikte bilgi merkezinin itibar kaybetmesi ve yasal yükümlülükler ile karşılaşması gibi sonuçlar ortaya çıkmaktadır. Bilgi merkezlerinde bilgi farkındalığı yaratmanın temel amacı, ağ kaynaklarının yanlış kullanımı sonucunda ortaya çıkacak sorunları kurumun güvenlik politikasına uygun olarak daha önceden öngörüp çözümler ortaya koymaktır.

Bilgi güvenliği farkındalığı, bilgi güvenliğini riske atan faktörlerden ve söz konusu faktörlere karşı ne tür önlemler alınabileceğini kapsayan güvenlik politikalarından haberdar olunması şeklinde tanımlanabilir[3].

Bilgi merkezlerinin adından da anlaşılacağı üzere en önemli varlığı olan bilgiyi, en etkin biçimde korumak, saklamak ve sağlamak zaruridir. Etkin bir bilgi güvenliği kurumsal işleyişin aktif ve sürekli olmasını ve kurumsal hedeflere ulaşmayı sağlamaktadır.

Teknolojinin gelişmesi ile birlikte bilginin uzaktan erişilebilir hale gelmesinin birçok yararının olmasının yanı sıra, bilgi sistemlerinin saldırılara açık hale gelmesine ortam hazırlamıştır. Sosyal mühendis olarak bilinen saldırgan grubunun kütüphane veri tabanlarına kolaylıkla erişip, kullanıcıların kimlik, adres, e-posta ve telefon bilgilerine ulaşabildiklerini öne sürmektedir[3]. Bilgi merkezlerinde bulunan donanımsal araçlar ağ saldırılarına karşı son derece zayıf olmasının yanında bilgi profesyonellerinin bazı ihmalleri sebebiyle saldırganların tehditleriyle karşı karşıya kalabilmektedir. Bu durum bilgi güvenliği için bilgi merkezi personelinin bu konuda bilinçlendirilmesi gerektiğini ortaya koymaktadır.

0.5.2 Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı Nasıl Sağlanır ?

Bilgi merkezlerinde bilgi güvenliği farkındalığı, bilgi profesyonellerinin hem bireysel hem de kurumsal olarak bilgi güvenliği bilincini yaratmaları, kurumsal bilgi güvenliği politikası oluşturmaları, bu konuda eğitimler ve bilgilendirmelerin aktif bir şekilde yapılması, personele belirli düzeylerde teknoloji bilgisinin verilmesi ve/veya seçilen personellerde bu özelliklerin aramasıyla ve bilgi güvenliğini kurumsal misyon olarak belirleme ile sağlanabilir.

0.6 Bilgi Merkezlerinde Bilgi Profesyonellerinin Üzerine Düşen Görevler Nelerdir ?

Bilgi teknolojilerinin gelişimi ve bilişim dünyasının gelişimi ile doğru orantılı olarak sürekli kendini yenileyen ve geliştiren siber saldırı yöntemleri ve bu konu ile yine doğru orantılı olarak gelişim ve ilerleme göstermesi gereken bilgi güvenliği konusu, bilgi uzmanları açısından zorunlu bir konu ve sorunsal haline gelmiştir. Bilgi merkezlerinde sunulan erişim hizmetlerinin güvenliğinden yine bilgi uzmanları sorumlu olmuştur ve bu konudaki sorumlulukları siber saldırı tehditleri geliştikçe artacaktır.

Bilgi uzmanları, siber tehditleri engellemek için yerine getirmesi gereken sorumluluklarını hukuk kuralları çerçevesinde yerine getirmek ve bu kurallara uygun önlemler almak mecburiyetindedir. Bilgi uzmanlarının sorumlulukları sadece bilgilerin düzenlenmesi ve hizmete sunulması değildir.

Bilgi merkezleri ayrıca üyelerinin kişisel bilgilerinin güvenli olarak muhafaza edilmesine, üyelerin faydalandığı kaynaklardan elde edilebilecek özel hayatla ilgili bilgilerin gizliliğine özen gösterilmesi, meydana gelen bir suçun yetkili makamlara iletilmesi konularında genel cezai sorumluluklara sahiptir. Bilgi güvenliğinin sağlanması konusu, hukuk ve bilişim alanlarının her ikisinin de ortak konusudur ve bu disiplinlerden bir tarafın eksik kalması halinde kalıcı ve sürekli başarıya ulaşmak mümkün olmamaktadır. Bu nedenle teknik önlemlerinin hukuk kurallarına uygun olarak alınması önemlidir[4].

Bilgi profesyonelinin, bilgi güvenliğinin sağlanmasına yardımcı olmak için bu konudaki TCK maddelerini öğrenmeli, bilgi ve bilişim teknolojileri konusunda yeterli düzeye gelmeli, kurumsal faaliyetler için kullanılan ağ kaynaklarının güvenliğini sağlanması konusunda bilgiye sahip olmalı ve kurum içinde bu bilincin yaratılması için çaba göstermesi gerekmektedir.

0.7 Kaynakça

[1] Önel, D. ve Dinçkan, A. (2007). *Bilgi güvenliği yönetim sistemi kurulumu.* TUBİTAK UEKAE.

[2] Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güveniliği ve süreçleri üzerine bir inceleme. *Journal of Polytechnic, 3*(9), 165-174.

[3] Öztemiz, S. ve Yılmaz, B. (2013). Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı : Ankara'daki Üniversite Kütüphaneleri Örneği. *Bilgi Dünyası, 1*(14), 87-100.http://www.bby.hacettepe.edu.tr/yayinlar/dosyalar/105-829-1-PB.pdf adresinden erişilmiştir.

[4] Henkoğlu, T. ve Uçak, N. Ö. (2012). Elektronik Bilgi Güvenliğinin Sağlanması ile İlgili Hukuki ve Etik Sorumluluklar. *Bilgi Dünyası, 2*(13), 377-396.

1 Metin ve görüntü kaynakları, yazarlar ve lisans

1.1 Metin

- **Bilgi güvenliği** *Kaynak:* https://tr.wikipedia.org/wiki/Bilgi_g%C3%BCvenli%C4%9Fi?oldid=17197645 *Katkıda bulunanlar:* Tansu, Riker2000, Memty Bot, Cat, JAnDbot, Eldarion, Maderibeyza, Gerakibot, Gökçe Yörük, PSamathideS, Luckas-bot, Khutuck Bot, Dr. Coal, GhostLiving, Akil13, MastiBot, EmausBot, Lostar, Wall-e Bot, WikitanvirBot, FoxBot, MerlIwBot, KediÇobanı, Magawla61, E4024, Peykbot, Addbot, Kumkum, Yozer1, Zaitsév, Nbeksi, Rebuk, VolkanSert, Bbytayfa1 ve Anonim: 14

1.2 Resimler

1.3 İçerik lisans

- Creative Commons Attribution-Share Alike 3.0