Kütüphanelerde Bilgi Güvenliğinin Önemi

Doç. Dr. Semanur ÖZTEMİZ

Sunum Planı

- Bilgi güvenliği
- Kütüphaneler için bilgi güvenliğinin önemi
- Bilgi güvenliğini sağlamak için teknik çözümler ve farkındalık
- Örnek Bir Politika

Bilgi Güvenliği Nedir?

- Bilginin tahribat, silinme, bozulma gibi zarar verici unsurlara ve olası saldırılara karşı korunmasını sağlayan birtakım uygulamaları kapsamaktadır.
- Bilginin yetkisiz kişilerce kullanımının önlenmesi, doğruluk ve bütünlüğünün korunması…

Bilgi Güvenliği Nedir?

- Kurumsal bilgi kaynaklarını olası tehditlere karşı korumak
- Tehditler insan ya da doğa kaynaklı veya kurum içi ve kurum dışı
- Kurum içi tehditler: Bilgiye dayalı araçların yanlış ya da hatalı kullanımı, yazılım ya da donanım hırsızlığı…
- Kurum dışı tehditler: Virüsler, yığın (spam) iletiler, saldırganlar (hacker, sosyal mühendis gibi) ya da doğal afetler gibi nedenlerle ortaya çıkan tehditler…

Canbek ve Sağıroğlu, 2006, s.169

Bilgi Güvenliğinin Bileşenleri

- Bilgi güvenliğinin üç temel ilkesi bulunmaktadır. Bunlar:
  - Gizlilik
  - Bütünlük
  - Erişilebilirlik ya da süreklilik

Süreç Olarak Bilgi Güvenliği

- 1. Yönetsel süreç,
- 2. Teknolojik önlem süreci,
- 3. Eğitim ve farkındalık sürecidir.

Bilgi Güvenliği Neden Önemli?

- Etkili bir bilgi güvenliği
- kurumsal işleyişin süreklilik kazanması
- kurumsal itibarın artması…
- Bilgi güvenliği sağlanamamışsa maddi ve manevi kayıplar kaçınılmaz...

Teknoloji ve Bilgi Güvenliği

- Her teknoloji riskiyle birlikte gelir…
- Çeşidi ve miktarı her geçen gün artan bilgi teknolojileri
- Bir saldırı aracı veya hedef?

Teknoloji ve Bilgi Güvenliği

- Siber güvenlik
- Bir bilgisayar ya da bilgisayar grubunun bir sisteme veya ağa yetkisiz girmesi…
- Siber güvenlik algısı ve birbirinden farklı uygulamalar
- ABD için, siber uzay birimlerini/bölümlerini güvence altına almak için sağlanan önlemler...

Luiffjf vd. 2013, s. 6-7

Teknoloji ve Bilgi Güvenliği

- İngiltere için, bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa…
- Almanya için, sistemlere izinsiz girişleri engellemeye yönelik stratejiler..
- «engelleme» ve «güvence altına alma» orta noktası
- Siber güvensizliğin oluşturacağı maliyet…
- Güvenlik stratejilerine gereksinim

Kütüphanelerde Bilgi Güvenliği Riskleri

- Bilgi güvenliği kütüphaneler açısından da önemli…
- İnternetin sağladığı olanaklar…
- Sosyal mühendislerin kütüphane veri tabanlarına kolaylıkla erişmesi…
- Kütüphanelerde bulunan bilgisayarların fiziksel hasara ve kötü niyetli saldırılara karşı zayıf olmaları,
- Bilgi güvenliği bilincine ilişkin yetersizlikler…

Kütüphanelerde Bilgi Güvenliği Riskleri

- Kütüphane bilgi sistemlerindeki verilerin kazara veya kötü niyetle silinmesi
- Yetkisiz kişilerin sistemlere erişimi,
- Binanın hasar görmesi nedeniyle maddi kayıp ve ekstra fon ihtiyacı,
- Kütüphanelerdeki bilgi ve ağ sistemlerinin tahribatı,
- Kütüphanelere duyulan güvenin kaybı ve itibarın olumsuz etkilenmesi
- Kişisel bilgilerin ve paydaş verilerinin ifşa edilmesi,
- Telif hakkı ihlalleri,
- Kurumsal verilerin zarar görmesi…

Kütüphanelerde Bilgi Güvenliği Nasıl Sağlanabilir?

- ◊ Kütüphaneciler arasında işbölümü,
- ◊ Kütüphane personelinin eğitilmesi,
- ◊ Bir politikanın geliştirilmesi,
- ◊ Fiziksel güvenlik planlarının yapılması,
- ◊ Bilginin bütünlüğünün sağlanması,
- ◊ Bilgi erişim yollarının denetlenmesi.

Çözüm Yalnızca Teknik Mi?

- Teknik yegane çözüm değil!
- En önemli rol insana düşmektedir.
- Bilinç ya da farkındalığın arttırılması
- Gerçekçi hedeflerle tasarlanmış bir güvenlik yönetimi…

Kütüphanelerde Bilgi Güvenliği Yönetimi

- Olası tehdit ve risklere karşı alınacak önlemleri, bunların uygulanmasını ve denetlenmesini kapsayan sistematik bir süreçtir.
- Teknik önlemlerin yanı sıra politika, prosedür ve standartlar gibi önlemler…
- Güçlü bir bilgi güvenliği farkındalığı…

Kütüphanelerde Bilgi Güvenliği Farkındalığı

- Kütüphanelerde bilgi güvenliği farkındalığı için,
  - Etkili bir bilgi güvenliği politikası (bilginin güvenli kullanımı hakkında takip edilmesi gereken kurallar ve ilkeler),
  - Bilgi güvenliği eğitimi (seminer, konferans, tartışma platformları ve çeşitli kurslar aracılığıyla),
  - Teknoloji bilgisi (bilgisayarlar ve internet araçlarının güvenli ve doğru kullanımı)
  - Duyarlı personel…

Otorite Kuruluşların Önerileri?

- Kütüphanelerde gizliliği teşvik etmek için IFLA (2015),
  - Bilgi hizmetlerinde mahremiyetin korunmasını,
  - Dijital hakların savunuculuğunun desteklemesini,
  - Yetkisiz erişimi engellemek için önlemler alınmasını,
  - Kullanıcıların veri koruma ve mahremiyet konusunda eğitilmesini,
  - Medya ve bilgi okuryazarlığı eğitimlerinde veri koruma ve gizlilik konularına da yer verilmesini önerir.

Otorite Kuruluşların Önerileri?

- "IFLA İnternet Manifestosu" (2014)…
- Ağ bağlantılı bilgilere erişim ve güvenli dijital bilgi kullanımına ilişkin rehberlik,
- Herkesin bilgiye güvenli bir şekilde erişme ve paylaşma hakkına sahip olması gerektiğine ilişkin vurgu...

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Kütüphanenin ana kaynakları, personel ve kullanıcı bilgileri,
- ödünç alma bilgileri, kütüphane bilgi sistemleri içerisinde kayıtlı olan veriler,
- veri tabanı abonelik bilgileri, şifreler, e-posta adresleri,
- web sitesi verileri ve diğer tüm veriler = bilgi varlıkları

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Kütüphane bilgi güvenliği yönetim sisteminin işlerlik kazanmasını sağlamak,
- Bilgi güvenliğine ilişkin kurumsal politikalar hazırlamak,
- Bilgi güvenliğine ilişkin farkındalığı artırmak, elzemdir.
- Diğer önlemler?

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Veri işleme, depolama kapasitesine sahip güncel donanım,
- Cihazların şifrelenmesi, kritik öneme sahip taşınabilir cihazların güvenli bir şekilde saklanması,
- Bilgilerin kurum dışına çıkarılmaması, kaldırılan donanımların veri depolama birimlerindeki bilgilerin geri dönülemez şekilde silinmesi,
- Kullanım ömrünü tamamlamış olsa da bilgi içeren cihazları çevresel tehditlere karşı korumak,

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Kötü amaçlı web sitelerini kara listeye almak,
- Veri kaybını önlemek için yedekleme yapmak,
- Olası güvenlik ihlallerini belirlemek için kullanıcı işlemlerini inceleme ve bilgi işleme cihazlarını kötü amaçlı yazılımlara karşı otomatik olarak tarama,
- Teknolojik bilgi güvenliği önlemlerinin uygulanmasında kurumsal bilgi güvenliği yönetim araçlarının kullanımı,

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Ağ güvenliği önlemlerini almak:
  - Yasaklı sitelere erişimin engellenmesi,
  - Ağ teknolojisi ve cihazların kayıtlarının tutulması,
  - Kurumsal ağa bağlı kullanıcılara ait donanımların erişimlerinin tehditlere karşı kontrol edilmesi
  - Güvenli uygulamaların yüklü olduğu cihazların kullanımı

Kütüphanelerde Bilgi Güvenliği Önlemleri

- Veritabanlarının güvenilir yönetimi için merkezi kimlik doğrulama sistemleri,
- Bilgilerin kritiklik derecesine göre sınıflandırılması ve şifrelenmesi,
- Veri depolama ortamlarındaki bilgilerin farklı depolarda yedeklenmesi,
- Kişisel bilgilerin tedarikçilerle paylaşılmasında sözleşme kurallarına uyulması,
- Tedarikçi ve kullanıcıların birim ile ilişkilerini sonlandırmaları durumu?
- Kişisel bilgilerin kullanılmasına ilişkin onay alınması,
- Güvenlik performanslarının artırımına yönelik uygun stratejiler ve politikalar

Örnek Bir Politika Neleri Kapsamalı?

- Kütüphane, herhangi bir amaçla saklanan gizli bilgilerin yetkisiz erişime karşı korunmasını sağlamak için her türlü makul önlemi almalıdır.
- Kütüphanenin, gizli bilgilerine erişmenin, bunları işlemenin, paylaşmanın Kişisel Verilerin Korunması Kanunu'na uygun olma sorumluluğu vurgulanmalıdır.
- Bu politika kütüphanedeki tüm elektronik bilgi kaynakları, personel, kurum, kullanıcı ve paydaş bilgileri, ağ ekipmanı ve yazıcılar gibi çevre birimleri için eşit derecede kapsayıcı

Örnek Bir Politika Neleri Kapsamalı?

- **Görev Ve Sorumluluklar**
- Kütüphane yöneticisinin rehberliğinde, E-kaynaklar ve dijital hizmetlerden sorumlu kimseler ve bilgi işlem yetkilisi gibi ilgili diğer sorumlular
  - Oturum açma erişimini yetkili kullanıcılarla kısıtlama,
  - Güncel yazılım yamalarını ve anti-virüs yazılımı,
  - Sistem yedeklemelerini sağlama ve sürdürme,
  - Güvenlik duvarlarını etkinleştirme ve kullanma,
  - Bilgi işlem sistemleri, ekipmanları ve ağlarında düzenli güvenlik taramaları,
  - Farkındalık eğitimleri ve materyali sağlama.

Örnek Bir Politika Neleri Kapsamalı?

- **Yetkili Kullanıcılar**
- Bilgilerin gizliliğinin, bütünlüğünün, kullanılabilirliğinin ve mevzuata uygunluğunun korunması…
- Erişim için kullanıcı adı ve şifresi,
- Gizli bilgilerin, şifrelerin veya diğer erişim mekanizmalarının kaybolması, çalınması veya ifşa edilmesi durumu…

Örnek Bir Politika Neleri Kapsamalı?

- Ekran koruyucu veya kilitleme özelliğini kullanma…
- Mobil cihazların kontrolü düzenli olarak sağlanmalıdır.
- Gizli bilgileri aktarmak için şifreli dosyalar kullanılmalıdır.

Örnek Bir Politika Neleri Kapsamalı?

- **Kütüphane Yöneticileri**
- Kurumsal bilgi güvenliği politikasının ve bireysel sorumlulukların personele açıkça iletilmesini ve yeterince takip edilmesini sağlamaktan nihai olarak sorumludur.
- Personelin kötü amaçlı yazılım tehlikesini, … teknik kontrolleri anlaması…
- Personelin çalışma düzenine ilişkin değişiklikleri bilgi işlem sorumlusuna bildirmek,
- Yetki düzenlemelerinin gözden geçirilmesini sağlamak.

Örnek Bir Politika Neleri Kapsamalı?

- **Genel Politikalar**
- Bilgi güvenliğinin sağlanmasından tüm yetkili kullanıcılar sorumludur.
- Sunucu güvenliği bilgi işlem sorumlusu ve ilgili diğer sorumlular tarafından kontrol edilir.
- Sunucu güvenlik mekanizmalarına diğer tüm kullanıcıların önceden izin alınmaksızın erişmesi yetkisiz erişim olarak değerlendirilmelidir.

Örnek Bir Politika Neleri Kapsamalı?

- Ağ kaynaklarına erişmeden önce tüm kullanıcıların ağda kimlik doğrulaması yapılması gerekir.
- Bilgi güvenliği eğitimi, bilgisayarların, yazılımın ve ağ bilgi kaynaklarının kullanımı…
- Bilgi güvenliği raporları düzenli olarak kütüphane yönetimi tarafından incelenmelidir.

Örnek Bir Politika Neleri Kapsamalı?

- **Yürürlük**
- Kullanıcılar bu politikaya uymadığında,
- kütüphane ağında depolanan, işlenen veya iletilen bilgiler, gizlilik, bütünlük veya kullanılabilirliğin kabul edilemez kaybı…
- Bilgi güvenliği ihlalleri soruşturulmalı ve yaptırımlar disiplin işlemleriyle sonuçlanabilmelidir.
  - **Güvenlik İhlali**
- Gizli bilgileri içeren herhangi bir fiili veya şüphelenilen güvenlik ihlali
- e-kaynak/dijital hizmetler
- İhlali tespit etmek, düzeltmek ve tarafları bilgilendirmek için gerekli müdahaleler yapılmalıdır.

Öneriler

- Kurumsal bilgi güvenliği yönetimi araçlarının kullanılmasını mümkün kılacak alt yapı olanaklarının sağlanması
- Fiziksel ve çevresel güvenlik tedbirlerinin uygulanması.
- Örneğin güvenlik kameraları, ziyaretçi girişlerini daha verimli kaydedebilir ve genel güvenliği artırmak amacıyla da kullanılabilir
- Gerektiğinde acil durum anahtarlarını kullanmak
- Güvenli bilgi= Güvenli kurum algısı

Öneriler

- Bilgi güvenliğine dayalı problemlerin yalnızca teknik yöntemlerle çözümlenebileceği düşüncesi ile mücadele…
- Güvenlik açığı yazılım ya da donanımdan çok insan faktörüne bağlı olarak ortaya çıkmaktadır.
- İnsan faktörünü aşan bir saldırganın antivirüs yazılımlarını, güvenlik duvarlarını ya da saldırıları rapor eden sistemleri aşması…

Öneriler

- Güvenlik risklerinin indirgenmesinde insan kaynaklı hataların giderilmesi…
- Teknolojinin bugün geldiği noktada Yapay zekâ odaklı kullanıcı analizlerinin çıktıları,
- Kişisel verilerin anonimleştirilmesini mümkün kılar.
- Kişisel veya hassas bilgiler…
- Mahremiyet hakkı ve veri koruma mevzuatı
- Kütüphaneler tüm bunları gözeten bilgi güvenliği uygulamalarını benimsemeli.

Kaynakça

- Altıntaş, F. F. (2022). G7 ülkelerinin siber güvenlik performanslarının analizi: ENTROPİ tabanlı MABAC yöntemi ile bir uygulama. Güvenlik Bilimleri Dergisi, 11(1), ss 263-286, doi:10.28956/gbd.1109776
- ITU. (2020). Global cyber security index. Geneva: ITU Publication.
- Kavak, A. Ve Odabaş, H. (2023). The impact of information security management guide utilization on technological and institutional information security measures in university libraries in Türkiye. The Journal of Academic Librarianship, 49(6). https://doi.org/10.1016/j.acalib.2023.102800
- Luiijf, E., Besseling, K., ve de Graaf, P. (2013). Nineteen national cyber security strategies. Int. J. Critical Infrastructures, 9(1/2), 3-31.
- Öğün, M. N., ve Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. Güvenlik Stratejileri, 9(18), 145-181.
- Öztemiz, S. Ve Yılmaz, B. (2013). Bilgi merkezlerinde bilgi güvenliği farkındalığı: Ankara'daki üniversite kütüphaneleri örneği. Bilgi Dünyası 14 (1), 87-100, 2013. 24, 2013.
- Shaker Library (2024). https://shakerlibrary.org/policies/administrative-policies/information-security-policy/