T.C. SAĞLIK BAKANLIĞI
SAĞLIK BİLGİ SİSTEMLERİ
GENEL MÜDÜRLÜĞÜ

Sağlık Bilgi Sistemlerinde Siber Güvenlik

Ders İçeriği

- Temel Kavramlar
- Yasal Düzenlemeler
- Dikkat Edilmesi Gereken Hususlar
- Örnek Olaylar

Siber Kavramı

- İnternet’e ait olan
- Bilgisayara ait olan
- Sanal gerçeklik

Siber (cyber) terimi **sibernetik** kökeninden gelmektedir. Tam bir kelime anlamı yoktur. İlk olarak **1958** yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleyen Sibernetik biliminin babası sayılan **Louis Couffignal** tarafından kullanılmıştır. (Yunanca kybernétes: dümenci)

Bilgi Güvenliği Tehdit Kaynakları

- **İç Tehditler**
  - ✓ Bilgisiz ve bilinçsiz kullanıcılar
  - ✓ Kötü niyetli çalışanlar

~% 80

~% 20

- **Dış Tehditler**
  - ✓ Meraklılar, genç kuşak saldırganlar
  - ✓ Profesyonel suçlular
  - ✓ Endüstri ve teknoloji casusları
  - ✓ Dış ülke yönetimleri

Bilgi Güvenliğinde İnsan Faktörü

Bilgi güvenliği açıklıklarının/risklerinin büyük bir kısmının teknik önlemler ile sağlanıyor gibi bir algı olsa bile insan faktörü bilgi güvenliğinin en önemli halkasıdır.

Ve zincir en zayıf halkası kadar güçlüdür.

BGYS Birimi Görev ve Sorumlulukları

- Sağlık Bilgi Sistemleri Genel Müdürlüğünün ISO 27001 tabanlı Bilgi Güvenliği Yönetim Sistemini (BGYS) işletilmesi,
- Bilgi güvenliği ile ilgili standartların belirlenmesi, ilgili mevzuatın hazırlanması ve yayımlanması,
- Bilgi güvenliği farkındalık çalışmalarının yapılması (eğitim, seminer, çalıştay vb.),
- Bilgi güvenliğinin en uç noktalara kadar yaygınlaştırılması için eylem planlarının hazırlanması ve takibi,
- Merkezi bilgi güvenliği ihlal olayları yönetiminin yapılması.

SOME Birimi Görev ve Sorumlulukları

- Açıklık tarama ve sızma testlerinin yapılması/yaptırılması,
- Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve diğer kaynaklar (Emniyet, MİT, açık istihbarat sağlayan kuruluşlar, «darkweb» tarama) tarafından yapılan bildirimlerin (BGYS birimi ile koordineli olarak) takip edilmesi,
- Bilişim sistemleri ile ilgili teknik açıklıkların takip edilmesi, kritik açıklıklar konusunda ilgili taraflara bildirim yapılması,
- Siber olaylarla ilgili teknik inceleme yapılması, adli bilişim faaliyetlerine destek verilmesi,
- «Sektörel SOME» faaliyetlerinin yürütülmesi.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi

- **Sistematik yönetim yaklaşımı:** Kurumda bilgi güvenliğinin sağlanması için sistematik bir yaklaşım oluşmasını sağlar. İşleri tesadüfe bırakmaz.
- **Bilgi varlıklarının farkına varma**: Kurumda hangi bilgi varlıklarının olduğu belirlenir. Korunmayan hiçbir varlık kalmaz.
- **Sahip olunan varlıkların korunması:** Varlıklara yönelik riskler belirlenir. Kuracağı kontroller ile koruma metotları belirlenir ve uygulanır.
- **İş Sürekliliği:** Bir felaket halinde sistemlerin en az etkilenecek şekilde sürekliliği sağlanmış olur.

Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzu

https://bilgiguvenligi.saglik.gov.tr/Home/Mevzuat

Bilgi Güvenliği / Siber Güvenlikle

İlgili, hastane yöneticileri düzeyinde bilinmesi gereken

Yasal Düzenlemeler, Standartlar ve Diğer Mevzuat

Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler)

Ocak 2018

- **İdari Tedbirler**
  - Kişisel Veri İşleme Envanteri Hazırlanması
  - Kurumsal Politikalar (erişim, bilgi güvenliği, kullanım, saklama, imha vb.)
  - Sözleşmeler
  - Gizlilik Taahhütnameleri
  - Kurum İçi Periyodik ve/veya Rastgele Denetimler
  - Risk Analizleri
  - Kurumsal İletişim (kriz yönetimi, bildirimler, itibar yönetimi vb.)
  - **Eğitim ve Farkındalık Faaliyetleri**
  - VERBİS'e Bildirim

- **Teknik Tedbirler**

  - Yetki Matrisi
  - Yetki Kontrol
  - Erişim Logları
  - Kullanıcı Hesap Yönetimi
  - Ağ Güvenliği
  - Uygulama Güvenliği
  - Şifreleme
  - Sızma Testi
  - Saldırı Tespit ve Önleme Sistemleri
  - Log Kayıtları
  - Veri Maskeleme
  - Veri Kaybı Önleme Yazılımları
  - Yedekleme
  - Güvenlik Duvarları
  - Güncel Anti-Virüs Sistemleri
  - Anahtar Yönetimi
  - Silme, Yok Etme veya Anonim Hale Getirme

Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Rehberi (Taslak)

Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

Hastane Yöneticileri Ne Yapmalı?

Hastanelerde Neler Yapılabilir?

- **İdari Tedbirler**
  - Bilgi güvenliği yetkilisi, bilgi güvenliği ekipleri (multi-disipliner bir ekip)
  - Bilgi güvenliği politikaları, dokümantasyon (erişim ve yetki kontrolü vb.)
  - Bilgi güvenliği farkındalık eğitimleri (yılda en az bir kez)
  - İhlal olayı yönetimi
  - Fiziki ve çevresel güvenlik tedbirleri
  - Gizlilik sözleşmeleri (çalışanlar, stajyerler, tedarikçiler)
  - ISO 27001 BGYS (özel hastaneler) / BG Politikaları Kılavuzu (devlet hastaneleri)

Hastanelerde Neler Yapılabilir?

- **Teknik Tedbirler**
  - Etki alanı yönetimi, grup politikalarının uygulanması
  - Ağ yönetimi, segmentasyon (kullanıcılar / sunucular / tıbbi cihazlar)
  - Zararlı yazılımlar ile mücadele
  - Yama yönetimi
  - Veri yedekleme (SBYS verileri, kritik veriler)
  - Sunucu/sistem odası güvenliği
  - Tıbbi cihaz güvenliği (Bilgi Güvenliği Politikaları Kılavuzu Madde 9.11)
    - Hastanelerin Bilgi İşlem/Biyomedikal Birimleri Tarafından Takip Edilmesi Gereken Hususlar
    - Tıbbi Cihaz Tedarik Planlaması Yapan Birimler Tarafından Dikkat Edilmesi Gereken Hususlar

Yaygın Hatalar / Örnek Olaylar