YBS-319

Bilgi Sistemleri Güvenliği

1. Hafta Dersi

23.09.2021

Notlandırma

- 2 Ödev, her biri % 15 ağırlıkta, toplam => % 30
- 1 ara sınav => % 30 (7. veya 8. hafta)
- Final sınavı => % 40

Ara sınav ve final sınavı çoktan seçmeli 25 soru.

Bilgi Sistemleri Güvenliği

- Temel amacı bilgiyi korumaktır.
- Bilgi Sistemi: Bir kurumun ve şirketin faaliyet gösterebilmesi için gerekli olan bilgilerin saklandığı, erişildiği, işlendiği, yeni bilgilerin üretildiği sistemdir.
- Bilgi Sisteminin Güvenliğini sağlamak şirketler için büyük önem taşır.

KVKK

- Kişisel Verileri Koruma Kanunu
- Kişisel Verileri Koruma Kurumu ilgili kanuna göre (KVKK) faaliyet göstermektedir.

> “İşlenen kişisel verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirir

Siber Saldırı (Cyber Attack)

* 18.03.2021 tarihinde kimliği veri sorumlusunca belirlenemeyen şahıs ya da şahıslarca Yemek Sepetine ait bir web uygulama sunucusuna erişildiği,

* Normal şartlarda yetkisiz bir erişim olduğunda uyarı veren araç üzerinde sorun kaydı oluştuğu ancak bir aksaklık nedeniyle yetkisiz erişimin o an fark edilemediği,

* 25.03.2021 tarihinde gelen alarmlar incelendiğinde şüpheli bir davranışın tespit edildiği,

* Yemek Sepetine ait bir web uygulama sunucusu üzerinde bir açıklık bulunduğu, bu açıklıktan yararlanılarak, uygulama kurulduğu ve komut çalıştırılmak suretiyle sunucuya erişilebildiği,

* Saldırıyı yapanlar tarafından sunucu üzerinde kullanıcı oluşturularak veri toplanmaya çalışıldığı ve uzaktaki sunuculara trafik gönderildiği,

* İhlalden 21.504.083 kişinin etkilendiği,

* İhlalden etkilenen kişisel verilerin kısmi olarak veri sorumlusunca belirlendiği ve söz konusu verilerin kullanıcı adı, adres, telefon, e-posta, şifre, IP bilgileri olduğunun değerlendirildiği,

Yemek Sepeti veri ihlali duyurusu

Konu Başlıkları

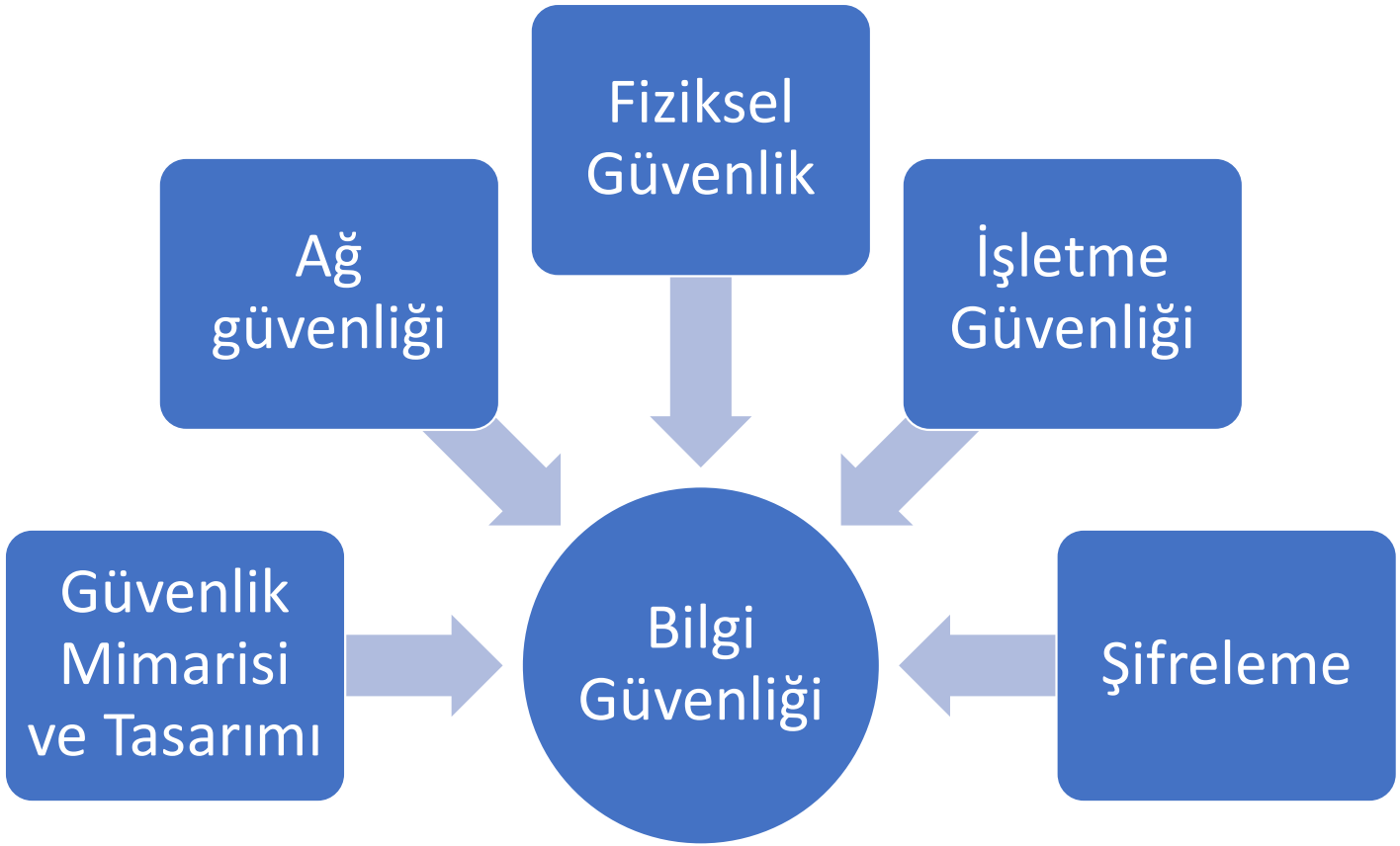
- Bilgi Sistemleri Güvenliğine Giriş
- Bilgi Güvenliği Prensipleri
- Risk Yönetimi
- Varlık Yönetimi
- Erişim Kontrolü
- Zararlı yazılımlara karşı güvenlik
- BT (Bilgi Teknolojileri) sistemlerinde (diğer) tehdit ve zayıflıklar
- Ağ sistemleri (Network Zones)
- Bulut (Cloud) servislerinin güvenliği

Konu Başlıkları

- Ağ güvenliği (Network Security)
- Ağ İzolasyonu (Network Isolation)
- Kablosuz Network Güvenliği (Wireless Network Security)
- Güvenlik Değerlendirmeleri ve Testleri
- Network Tarama Araçları
- Şifreleme (Cryptography)
- Olay Yönetimi (Incident Response), Disaster Recovery (Felaket Kurtarma), ve İşin Devamı (Business Continuity)
- Personel Politikaları (BT odaklı)

Bilgi Güvenliği Alanları-1

Bilgi Güvenliği Alanları-2

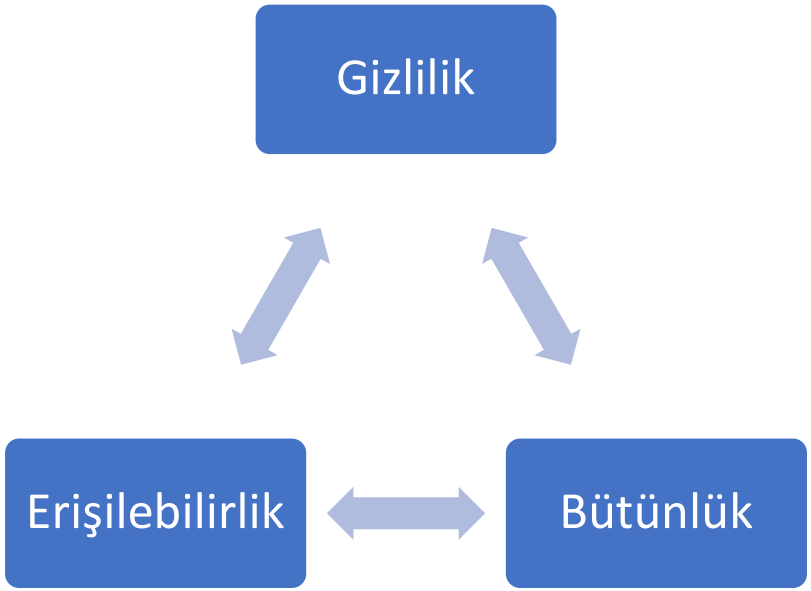


ISO 27001 – Bilgi Güvenliği Yönetim Sistemi

- Bilgi güvenliği yönetiminde uluslararası bir standarttır.
- ISO: International Standards Organization

CIA Üçlüsü (CIA Triad)

- Confidentiality (Gizlilik)
- Integrity (Bütünlük)
- Availability (Erişilebilirlik)



CIA

GİZLİLİK

- Bilgiye yetkisiz erişimleri engellemek
- Doğrulama, erişim kontroleri ve şifreleme ile sağlanır

BÜTÜNLÜK

- Bilginin (veri) değiştirilmediğini ve zarar görmediğini kontrol eder
- Hashing

ERİŞİLEBİLİRLİK

- Gerekli olduğu zaman bilgiye erişim olabilmelidir.
- Yedekleme ve Yedek Sunucular