

BİLGİ GÜVENLİĞİ SİBER GÜVENLİK

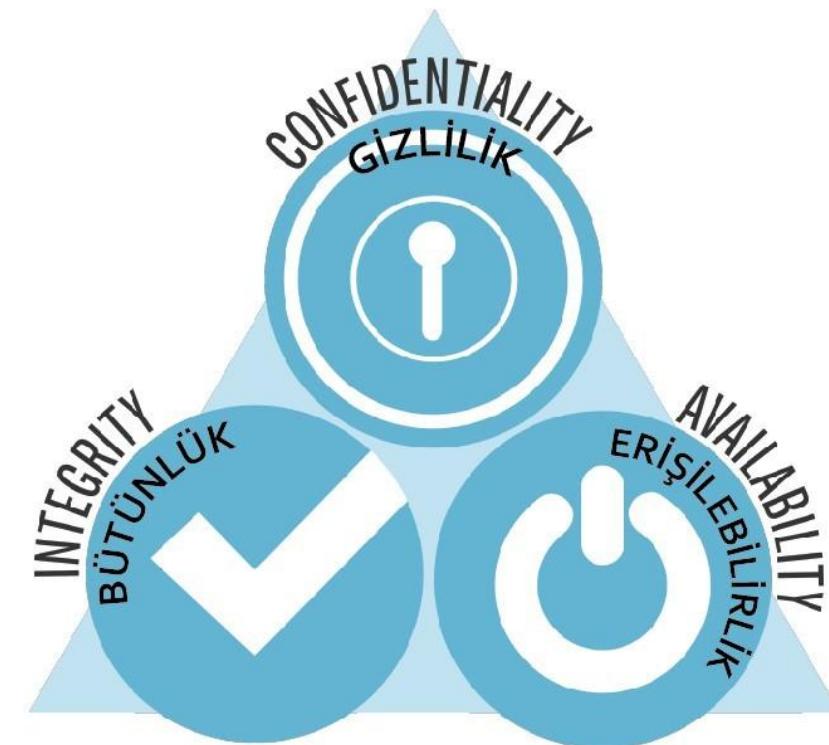
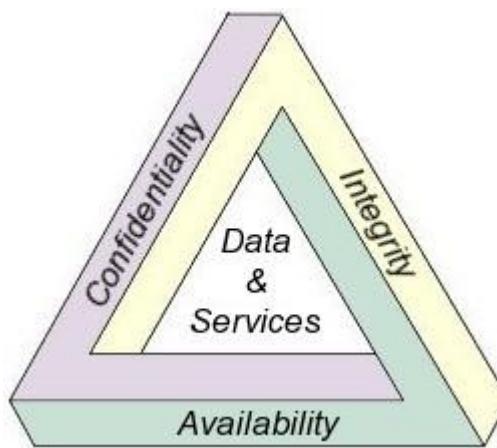
Öğr. Gör. Halil ARSLAN

Bilgi Güvenliği

- **Bilgi:** Bir kurumun kuruluşun veya organizasyonun faaliyetlerini yürütmekte kullandıkları verilerin anlam kazanmış haline denir.
- **Bilgi Güvenliği:** Öneme sahip bilginin korunması, bütünlüğünün sağlanması, erişebilir ve ulaşabilir olmasının sağlanması için alınan gereklili, önemler ve tedbirlerdir.
- Bilgi Güvenliği Yönetim Sistemi Standardı (ISO 27001)

CIA Üçlüsü (CIA Triad)

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



Bilgi Güvenliği

Gizlilik: Bilgilerin yetkisiz erişime karşı korunması

Bütünlük: Bilgilerin eksiksiz, tam, tutarlı ve doğru olması

Erişilebilirlik: Bilgilere yetkililere ihtiyaç duyulduğunda erişilebilir olması

Bilgi Güvenliği

- **Gizlilik - Confidentiality**

Herşeyi herkesten gizlemek değil, veriye/bilgiye sadece yetkisi onların ulaşılabilmesini sağlamak. Şifreleme gibi..

- **Bütünlük - Integrity**

Yetkisiz ve izinsiz değişikliklerin engellenmesi, verinin amacına uygun derecede doğru olması.

- **Erişilebilirlik - Availability**

Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması.

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur.**

(Bilginin sahibi, kullanan, sistemi yöneten, vb..)



Yetki paylaşılır, sorumluluk paylaşılmaz. Bilgi ise paylaşıldıkça artar.

Bilgi Güvenliği Kategorileri

- **Ağ güvenliği** (Network security)
- **Uç/Son nokta** veya **Kullanıcı güvenliği** (Endpoint security)
- **Veri güvenliği** (Data security)
- **Uygulama güvenliği** (Application security)
- **Kimlik ve Erişim Yönetimi** (Identity and access management)
- **Güvenlik yönetimi** (Security management)
- **Sanallaştırma ve bulut** (Virtualization and cloud)

Bilgi Güvencesi

- Information Assurance, IA

Bilgi sistemlerinin ;

- Kullanılabilirliğini,
- Bütünlüğünü,
- Doğrulanmasını,
- Gizliliğini ve
- İnkar edememe

Özellikini sağlar. Bilgi güvenliğini de içine alır.



Siber Güvenlik

- Siber uzayda organizasyon ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünüdür.

Kaynak: Uluslararası Telekomünikasyon Birliği (ITU)

Siber Güvenlik (Cyber Security)

- Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.
- Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır.

Hack

- Kırmak,
- Küçük parçalar koparmak,
- Açık yönlerini ortaya çıkarmak,
- Açıklığı kullanmak.

Anlamlarında kullanılır.

Hacking

- Sistem veya programın açığından yararlanıp erişim sağlamak, değiştirmek veya silmek.
- Açıklığı kullanma işlemidir.

Hacker



- Sistemlere sizabilme yeteneğine sahip, programlama bilgisi üst düzeyde olan ağ ve sistemlerin işleyişini iyi bilen, gerektiğinde sosyal mühendislik yapabilen, hacking araçlarını tanıyan ve bunları gerektiği zaman geliştirebilen kişilerdir.

Siber Korsan

- Etik, kültür, etnik veya siyasi özelliklerine göre farklılar göstermektedir.
- Siyah Şapkalı Hacker, Gri Şapkalı Hacker, Beyaz Şapkalı Hacker, Haktivist, Cracker, Phreaker, Lamer, Script Kiddie

Hackerların Şapka Renkleri

Siyah Şapkalı Hacker

- Kötü amaçlı, zarar vermek veya para odaklı,
- Sistemleri ele geçirmek veya yok etmek için,
- Saldırı gerçekleştiren, tehlikeli bilgisayar korsanıdır.
- Sisteme erişimi engelleme, bilgi değiştirme, gizli bilgi çalma gibi faaliyetlerde bulunurlar.



Beyaz Şapkalı Hacker

- Etik hacker,
- Aynı bilgi ve beceriye sahip, İyi niyetli,
- Açıklığı tespit eden, uyarın veya önleyen,
- Sistem güvenliğinden sorumlu personel,
- Ahlaklı siber korsandır.



Gri Şapkalı Hacker

- Sistemlere sizma ve giriş yapan,
- Kötü amaç olmayıp, merak için,
- Yasallık sınırlarında saldırganlık faaliyeti olan,
- Zaman zaman tehlikeli faaliyetler içerisinde,
- Yaptıkları hukuk karşısında suç teşkil eden,
(Sisteme sizme, girme vb.) Siber korsanlardır.



Ek Tanımlamalar

Cracker

- Bilgisayar programlarının kopya korumalarını kırrarak, bu programların izinsiz olarak dağıtımına imkan veren veya bu yolda çıkar sağlayan kişilere denir. (Yazılım korsanı)
- Lisansların iptali veya serial-key temini,



Hacktivistler

- Hacker + Aktivist = Hacktivist
- Kendilerine göre, toplumsal sorun veya yanlış politik durum olarak gördükleri konulara dikkat çekmek için sistemlere saldıran kişi veya gruplardır. (sanal protestocu)
 - Wikileaks,
 - Anonymous,
 - RedHack,
 - Cyber-Warrior,
 - Ayyıldız Tim,
 - SEA vb.



- Başkalarının önceden yazdığı betik(script) kodları veya programları çalıştırır, övünür,
- Ağ, sistem, yazılım, programlama gibi konularda bir bilgiye sahip olmadan,
- Atak yapmaya çalışan kişilerdir.

(Lamer: Özenti, basit)



Script Kiddie

- Yeterli bilgisi olmadan hazır araçlarla saldırı düzenleyen (genelde genç yaşıta-çocuk) kişilere verilen isimdir. (Betikçiler-BetikKerataları)
- Tıpkı lamer'lar gibi ama bir miktar bilgi sahibi,
- Kötü niyetli, zarar verme amaçlı,
- Teknik detay ve programın nasıl çalıştığını bilmez, ama kullanımını bilenlerdir.



Phreaker

- Telefon iletişim hatlarına erişip,
- Uzun süreli Ücretsiz görüşme, vb. amaçlı,
- Telefon kıräcileridir.



- Çaylak, okula yeni başlayan,
- Bilişimde veya programla da yenilere denilir,
- Betik keratalarından bir basamak üstte,
- Kendini öğrenmeye adamış bilişim korsanı adaylarıdır.

