BiltekCyber

Siber Güvenlik 101

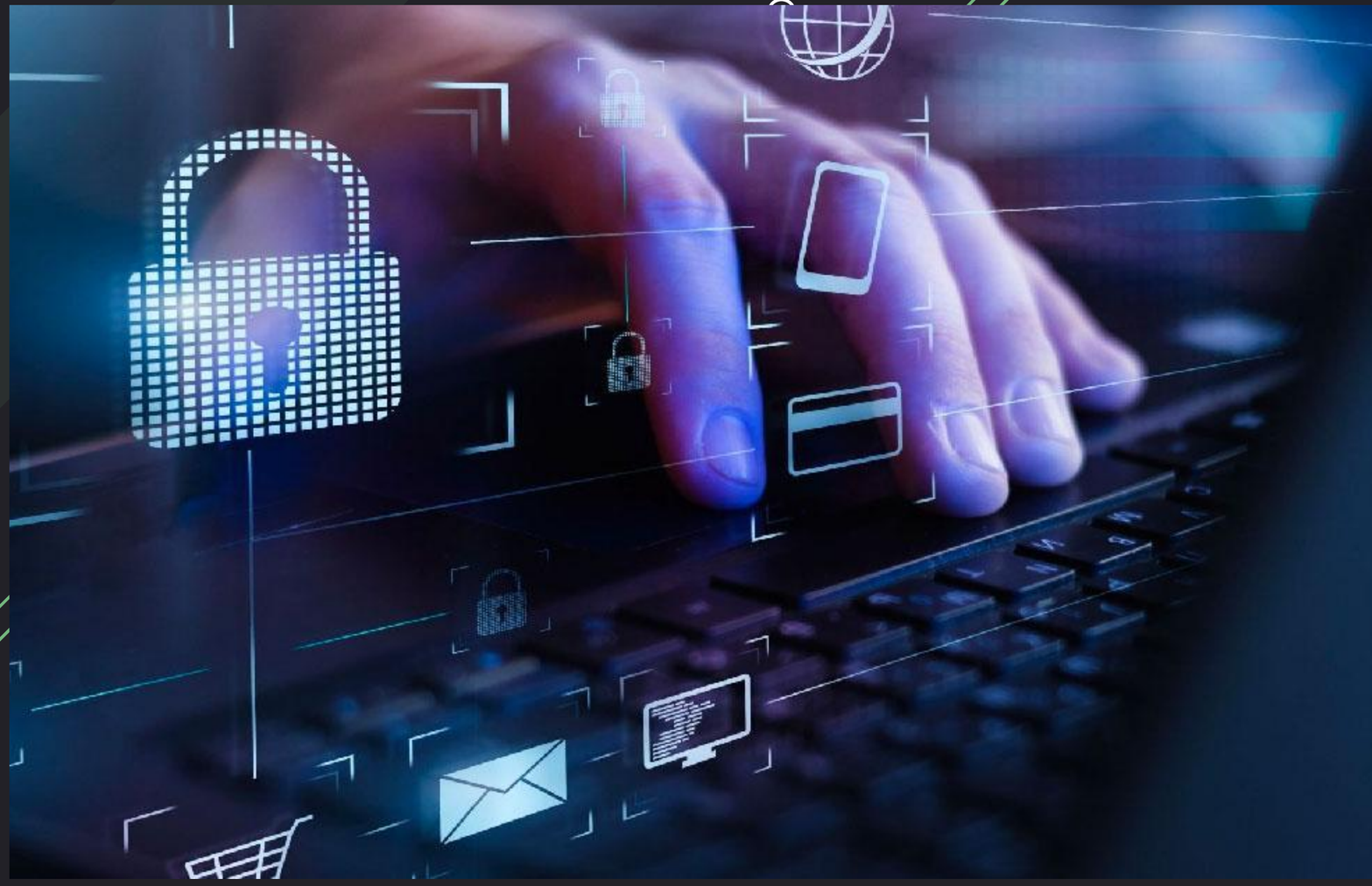
BiltekCyber

İçerik

BiltekCyber

Bilgi Güvenliği Nedir?

Bilgi güvenliği, (Gizlilik, Bütünlük ve Erişilebilirlik) bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma, veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemi.



BiltekCyber

Bilgi Güvenliği İlkeleri

1. **Gizlilik:** Gizlilik, bilginin sadece yetkililer tarafından erişilmesini sağlama ilkesidir. Sadece doğru kişiler bilgiye ulaşmalıdır.

2. **Bütünlük:** Bütünlük, bilginin değişmeden ve bozulmadan korunması gerektiği ilkesidir. Bilgi doğru ve güvenilir olmalıdır.

3. **Erişilebilirlik**: Erişilebilirlik, bilginin gerektiğinde sorunsuz bir şekilde erişilebilir olması gerektiği ilkesidir. Yetkili kişilerin bilgiye kolayca ulaşabilmesi önemlidir.

BiltekCyber

Siber Güvenlik Nedir?

Bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, ağları ve verileri kötü amaçlı saldırılardan koruma uygulamasıdır.

Bilgi teknolojisi güvenliği veya elektronik bilgi güvenliği olarak da bilinir.

BiltekCyber

Bilgi Güvenliği ile Siber Güvenlik Arasındaki Farklar

Siber güvenlik ve bilgi güvenliği terimleri benzer kavramları ifade etse de, bazı farklılıklar içerirler.

Siber Güvenlik, dijital sistemlerin korunması ve siber tehditlere karşı savunmanın odaklandığı bir alandır. Bilgi Güvenliği ise siber güvenliği içerirken fiziksel dokümanlar, iş süreçleri, insana dayalı güvenlik riskleri ve daha fazlasını kapsar.

BiltekCyber

Hack ve Hacker Kavramları

"Hack," genellikle bilgisayar sistemlerine veya yazılımlara izinsiz erişim sağlama, değiştirme veya manipüle etme işlemi olarak tanımlanır.

"Hacker," kendisini bilgisayar sistemleri ve ağlarının içine girerek, değiştirerek veya bilgilere erişerek test eden veya keşif yapan bir kişiyi tanımlayan geniş bir terimdir.

BiltekCyber

Hacker Metodolojisi

Hacker metodolojisi, bir bilgisayar sistemi veya ağa izinsiz erişim sağlama veya güvenlik açıklarını sömürme amacı güden kişilerin izlediği belirli bir adım ve yaklaşım sırasını ifade eder.

- Keşif (Reconnaissance): Hedef sistem veya ağ hakkında bilgi toplama aşaması. Açık kaynak istihbarat, tarama ve diğer yöntemlerle hedef hakkında veri toplanır.

- Tarama (Scanning): Hedef sistemler üzerinde açıkları tespit etmek ve daha fazla bilgi almak amacıyla taramalar yapılır. Port taramaları ve servis sürüm tespiti gibi teknikler kullanılır.

BiltekCyber

Hacker Metodolojisi

- Sızma (Gaining Access): Hedef sistemlere veya ağlara izinsiz erişim sağlama amacı güden aşama. Şifre kırma, güvenlik açıklarını sömürme veya sosyal mühendislik gibi teknikler kullanılabilir.

- Denetim ve Kontrol (Maintaining Access): Bir kez içeri girildiğinde, erişimi sürdürmek için backdoorlar veya kök erişim araçları kullanılabilir.

- Saldırıları Gizleme (Covering Tracks): Hackerlar, faaliyetlerini gizlemek için izlerini silmeye veya log kayıtlarını değiştirmeye çalışabilirler.

BiltekCyber

Şapkalarına Göre Hackerlar

"Hackerlar"ın farklı "şapkalara" ayrılması, hackerlerin amaçları, etik kurallara uyumları ve faaliyetlerinin doğası açısından sınıflandırılmasını kolaylaştırmak için kullanılan bir kavramdır. Bu şapkalar, bir hackerın niyetine, motivasyonuna ve faaliyetlerini belirtir.

- **White Hat Hacker (Beyaz Şapkalı Hacker):** Bu hackerlar bilgisayar sistemlerinin ve ağlarının güvenliğini test etmek ve savunmak amacıyla etik olarak çalışırlar. Genellikle şirketlerin güvenlik açıklarını tespit etmek veya siber saldırılara karşı savunma stratejileri geliştirmek için istihdam edilirler.

BiltekCyber

Şapkalarına Göre Hackerlar

- **Black Hat Hacker (Siyah Şapkalı Hacker):** Bu hackerlar kötü amaçlı olarak bilgisayar sistemlerine ve ağlara sızarak, kişisel kazanç veya zarar verme amacı güderler. Kredi kartı bilgilerini çalmak, fidye yazılımı dağıtmak veya diğer kötü niyetli faaliyetlerde bulunmak gibi suçlu amaçlarla çalışırlar.

- **Gray Hat Hacker (Gri Şapkalı Hacker):** Gray hat hackerlar, genellikle izinsiz olarak sistemlere girebilirler, ancak amacı zarar vermek değil, güvenlik açıklarını tespit etmek veya sahiplerine dikkat çekmek olabilir. Bu nedenle, etiklikleri konusunda bazen tartışmalı olabilir.

BiltekCyber

Parola Güvenliği

Güçlü parola güvenliği, siber saldırılara ve hesap ihlallerine karşı koruma sağlar. Parola güvenliğinin nasıl sağlanabileceği konusundaki bazı temel prensipler:

- Uzun ve Karmaşık Parolalar Kullanın
- Kişisel Bilgilerden Kaçının
- Her Hesap İçin Farklı Parola Kullanın
- Sembol, Rakam, Büyük-Küçük Harf İçeren Parolalar Tercih Edin

BiltekCyber

Kaynakça

1-https://www.nist.gov/cyberframework
2-https://tr.wikipedia.org/wiki/Bilgi_güvenliği
3-https://www.cisa.gov/cybersecurity
4-https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security
5-https://en.wikipedia.org/wiki/Hacker
6-https://en.wikipedia.org/wiki/Security_hacker

BiltekCyber

Hazırlayan

Adı: Yahya
Soyadı: Çakıcı
Fakülte: Mühendislik ve Doğa Bilimleri Fakültesi
Departman: Yazılım Mühendisliği 2.Sınıf

Linkedin: https://www.linkedin.com/in/yahya-çakıcı-584004256/