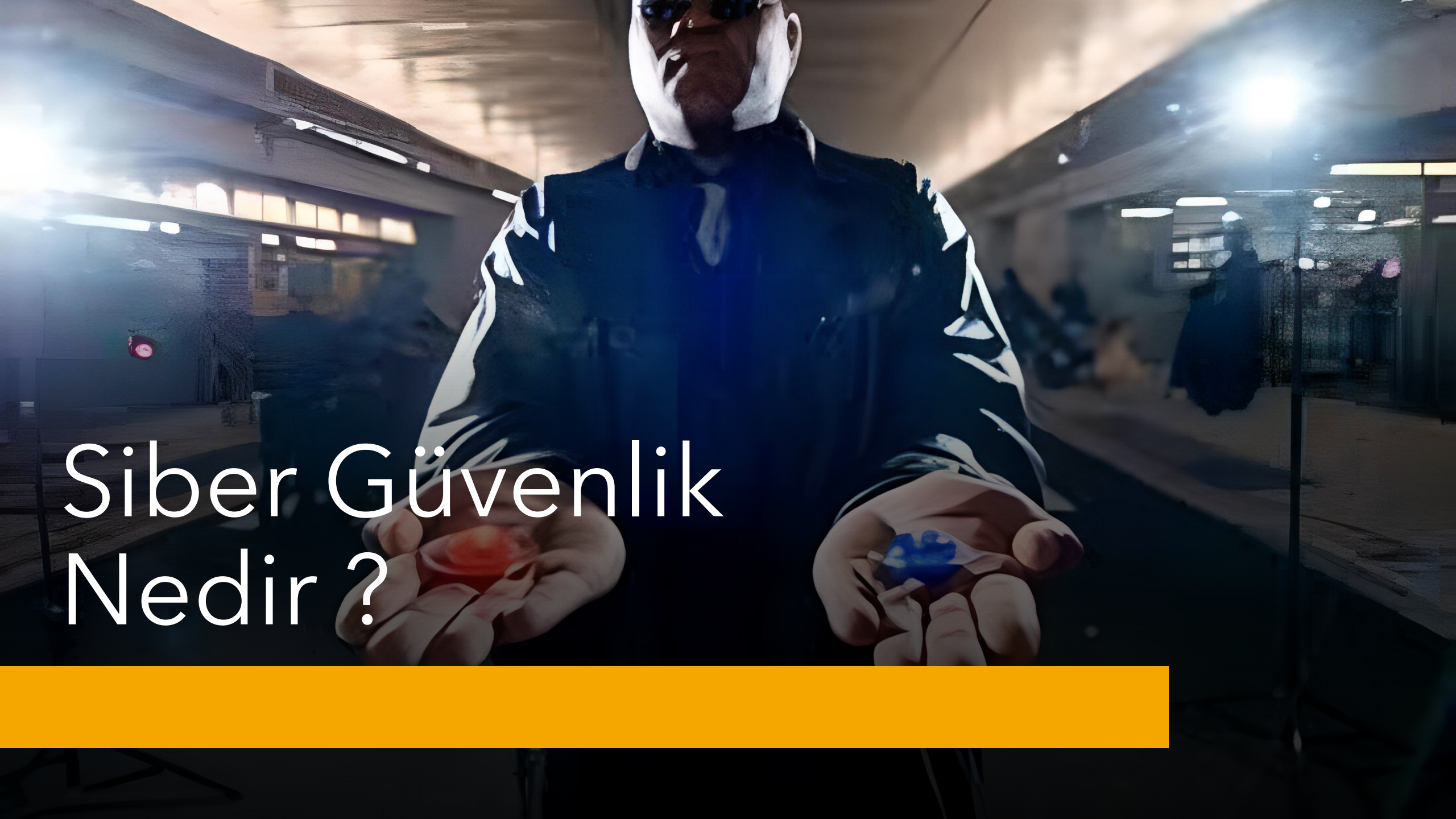


Siber Güvenlik Nedir ?

$who am i

İsmet Arslan

Cyber Securtiy Researcher

President at KMU Cyber Security Community

Mail : arslanismet@protonmail.com

Linkedin : arslanismet


Emniyet ?

Emniyet Nedir ?

- Fiziksel olan tehditlere alınan tedbirlerin genel ismidir.
- Reaktif (bir olay gerçekleştikten sonra) bir kavramdır.
- Polis gibi…

Güvenlik ?

Güvenlik Nedir ?

- Proaktif (bir olay olmadan öncesi) bir konudur.
- Yalnızca görülen risklere karşı değil görülmeyen riskleri de bertaraf etmek içindir.
- Ordu, istihbarat gibi…


Siber ?

Siber Nedir ?

- "**Siber**" kelimesi İngilizce "**Cyber**" kelimesinden uyarlanıp kullanılmaya başlayan bir kelime olup "Bilgisayar ağlarına ait olan", "İnternete ait olan", "**Sanal Gerçeklik**" manalarına gelmektedir. Aslına bakılırsa interneti tanımlayan, bu sözcükten türeyen bir çok kelime mevcut. Siber kelimesi, bilişim sistemleri alt yapısında çalışan soyut ve geniş bir alt yapıdır. Biz kısaca siber alem diyoruz.

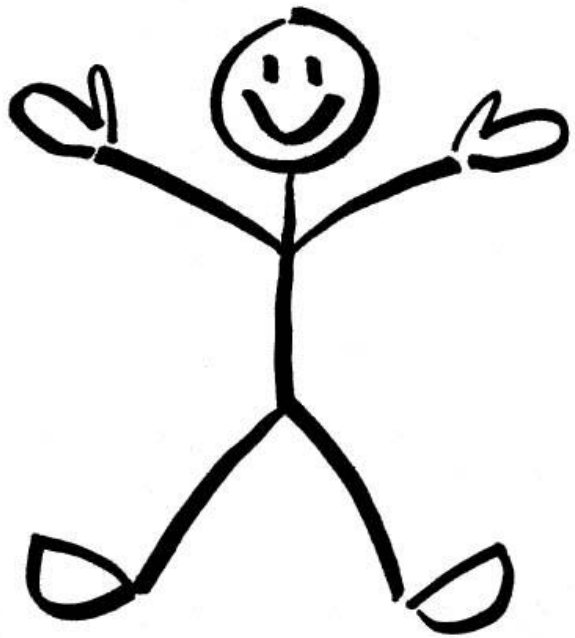
Siber Nedir ?

- Siber yalnızca Internet DEĞİLDİR, çok daha fazlasıdır.

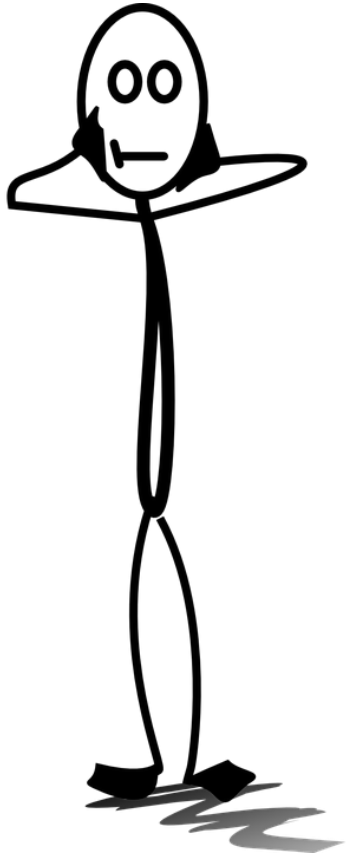
Veri nedir ?
Bilgi nedir?

Ne zaman güvenlik gerekir ?


DATA




DATA



Günün sonunda Siber Güvenlik nedir ?

İnternet'e bağlı sistemleri ve bu sistemlerle ilişkili verileri yetkisiz kullanım veya zararlardan korumak için

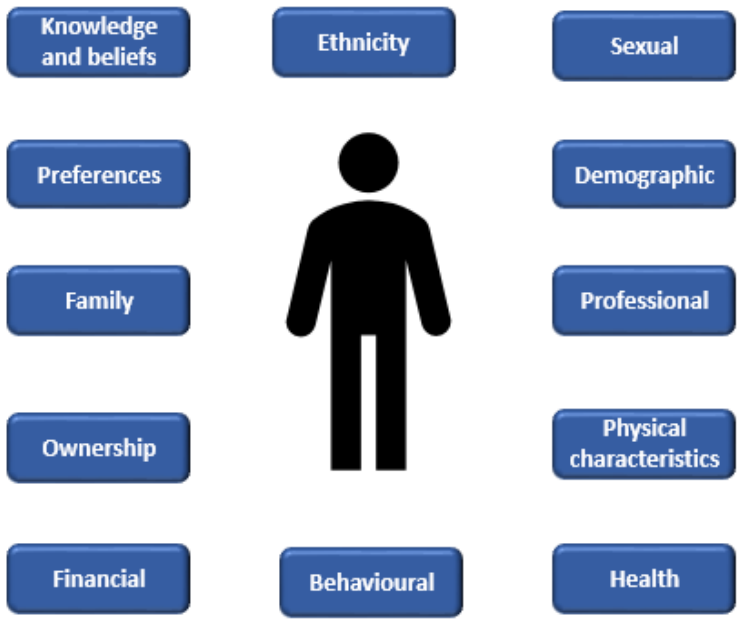
sürekli bir çabadır !

Kişisel Veri

Çevrimiçi ve Çevrimdışı Kimliğiniz

- Çevrimdışı Kimliğiniz
  - Evde, okulda veya işte düzenli olarak etkileşim kuran kimliğiniz.
- Çevrimiçi Kimliğiniz
  - Siber alandaki kimliğiniz

Kişisel Veriler



Tıbbi Kayıtlar

Fiziksel, zihinsel ve diğer kişisel bilgiler

Reçeteler

Eğitim Kayıtları

Notlar, sınav puanları, alınan dersler, ödüller ve dereceler

Devamlılık

Disiplin raporları

İstihdam ve Finansal Kayıtlar

Gelir ve giderler

Vergi kayıtları – maaş çekleri, kredi kartı ekstreleri, kredi notu ve bankacılık ekstreleri

Geçmiş istihdam ve performans bilgileri

Veriler Nerede ?

Tıbbi Kayıtlar:

- Hastane, doktor ofisi, sigorta şirketi

Tüketim Bilgilerimiz:

- Mağaza sadakat kartları
- Online alışveriş siteleri

Kişisel Bilgilerimiz:

- Sosyal medya hesaplarımız

Bilgisayarımız ve diğer cihazlarımız


KVKK
KİŞİSEL VERİLERİ KORUMA KURUMU

Varlıklar Ne Zaman Güvenli Kabul Edilir ?

Confidentialty (Gizlilik):

- Genel olarak mahremiyetin sağlanması diyebiliriz.
- Bireyler için söyleceksek, kişisel verilerin, yaptığı haberleşmelerinin başkaları tarafından görülememesidir.
- Kurumlar olarak düşünürsek kurumsal verilerin sadece kurum içerisinde yetkisi olan kişiler tarafından görülmesinin sağlanmasıdır.
- Gizlilik öncelikle **kimlik denetimi** ile sağlanır. Bu sayede yetkisi olmayan kişiler bu verilere ulaşamaz. Kimlik denetiminin yanı **sıra kriptolama (şifreleme) teknolojile**ri de bu amaçla kullanılmaktadır. Kriptolama teknikleri, ağ üzerinden geçen verilerin üçüncü şahısların eline geçmesi durumunda okuyabilmelerini engller.

Kimlik Denetimi (Authentication)

Kimlik Denetimi (Authentication)

Klasik denetim :

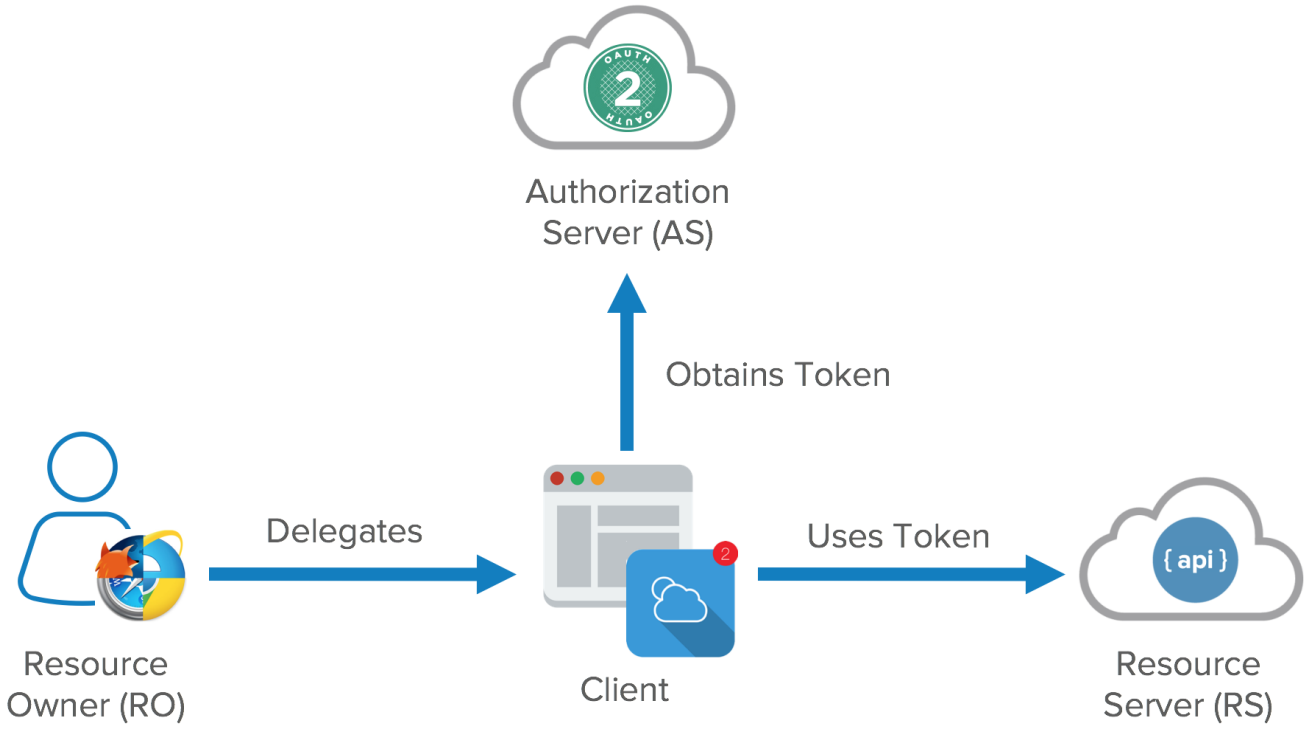
- Kullanıcı adı / Parola

Modern kimlik denetimi:

- MFA (Çok faktörlü kimlik doğrulama)
- Biyometrik Doğrulama (parmak izi, avuç izi, yüz veya ses tanıma)

Açık Yetkilendirme (OAuth 2.0 / Open Authorization)

- Son kullanıcının kimlik bilgilerinin kullanıcı parolasını açığa çıkarmadan üçüncü taraf uygulamalara erişmesini sağlayan açık standart sistemdir.



Integrity (Bütünlük):

- Bütünlük verinin yetkisiz kişiler tarafından değiştirilmesinin engellenmesidir. Veri aktarımında sıranın değmiş olması bile bütünlüğü bozar.
- Üçüncü şahıslar tarafından verinin değiştirilip değiştirilmediğinin anlaşılması için konrtol numaraları kullanılır. Bu kontrol numaraları hash algoritmları ile hesaplanır. Bu algoritmalar matematiksel olarak sabit bir uzunlukta bir kontrol numarasının (özet) oluşturulmasını sağlar. En önemli özelliği geriye döndürülemez olmalarıdır. Popüler olanlarına MD5, SHA-1, SHA-256, SHA-512 örnek verilebilir.

MD5 örneği:

Kontrol Edilecek Metin	MD5 hash'i
Ödenecek miktar 17 ₺	**db4e88b7f509cf14d74be0c66a58808f**
Ödenecek miktar 1337 ₺	**04436c488d6431e5c70208b2fdc0da52**

Availability (Erişilebilirlik) :

- Uygunluk (kullanılabilirlik) olarak da çevirebileceğimiz bu kavram, yetkili kişilerin ihtiyaç duyduklarında sistem kaynaklarına ve verilerine ulaşabilmeleridir.

- Erişeblirliğin devamı için;
  - Donanımların bakım ve kontrol altında tutulması,
  - Yazılımların bakım ve kontrol altında tutulması,
  - Sistem yedeklerinin doğru biçimde alınması,
  - Büyük kurum ve kuruluşlarda afet kurtarma planlarının bulunması,

  gibi çözümler sağlanmalıdır.

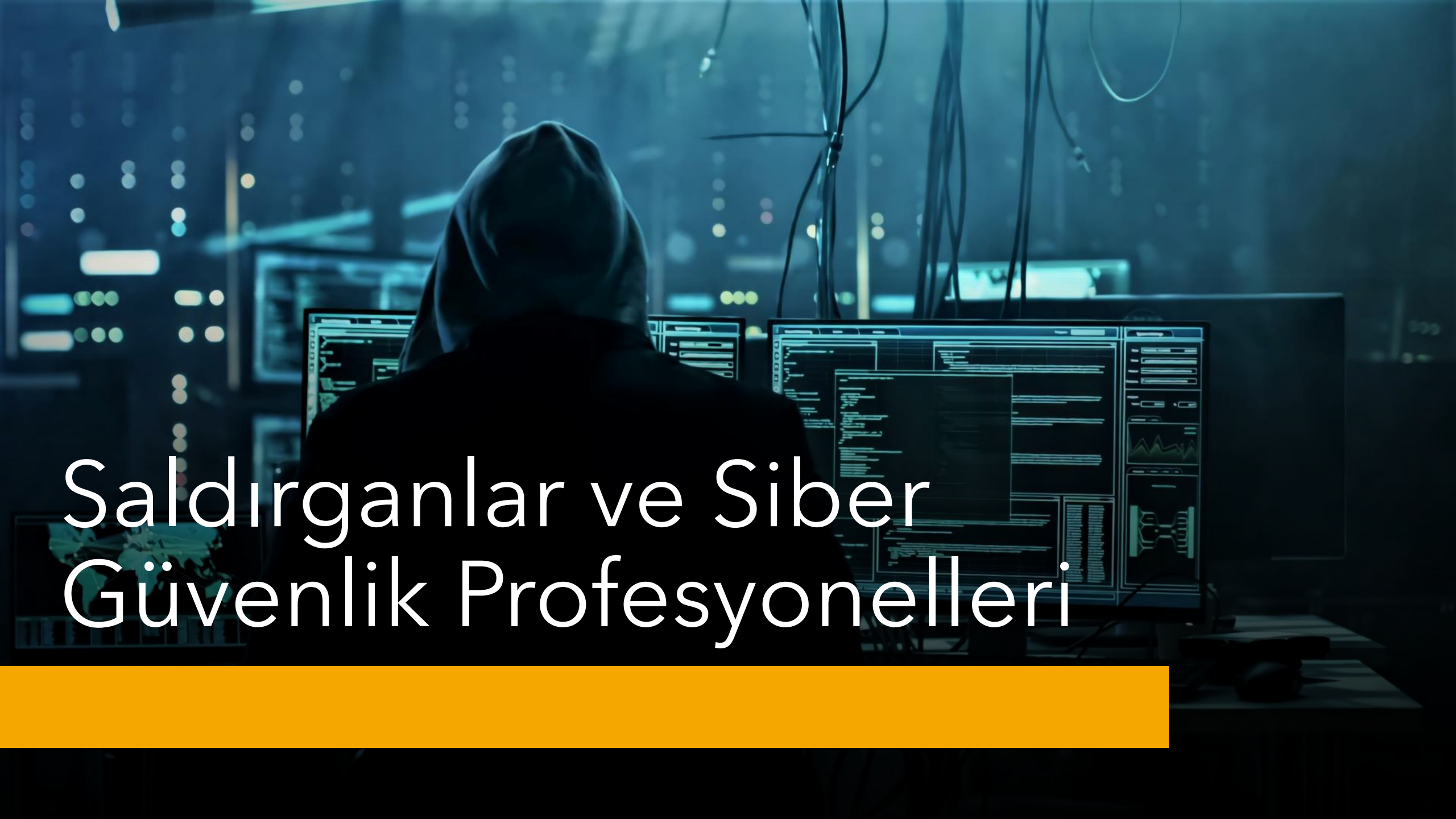
Availability (Erişilebilirlik) :

- Erişlebilirliğin devamı için ;

  - DoS (Denial of Service) veya DDoS (Distributed Denial of Service) saldırılarına karşı önlemler alınmalıdır.

  - Ransomeware'lere karşı önlemler alınmalı. Bir playbook oluşturulmalı.

Hack && Hacker ???



Saldırganlar ve Siber Güvenlik Profesyonelleri

Kim bunlar ?

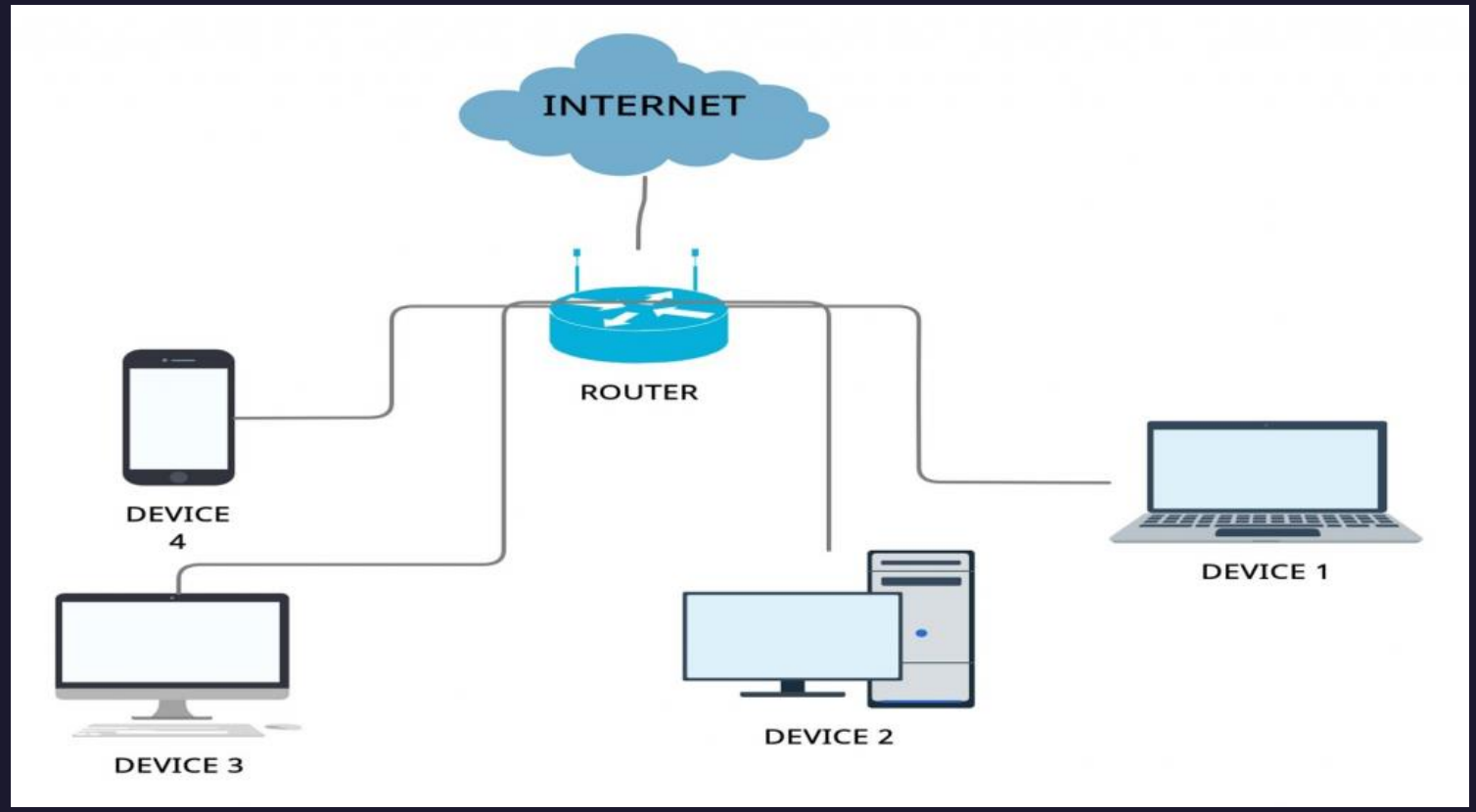
Saldırgan Türleri

- Amatörler
  - Sistemler ve programlama hakkında bilgisi olmayan, yalnızca araç kullanan kişiler. (Script kiddies)
- Siber Güvenlik Profesyonelleri (Beyaz Şapka / White Hat)
- Suçlular (Gri-Siyah Şapka/ Grey-Black Hat)

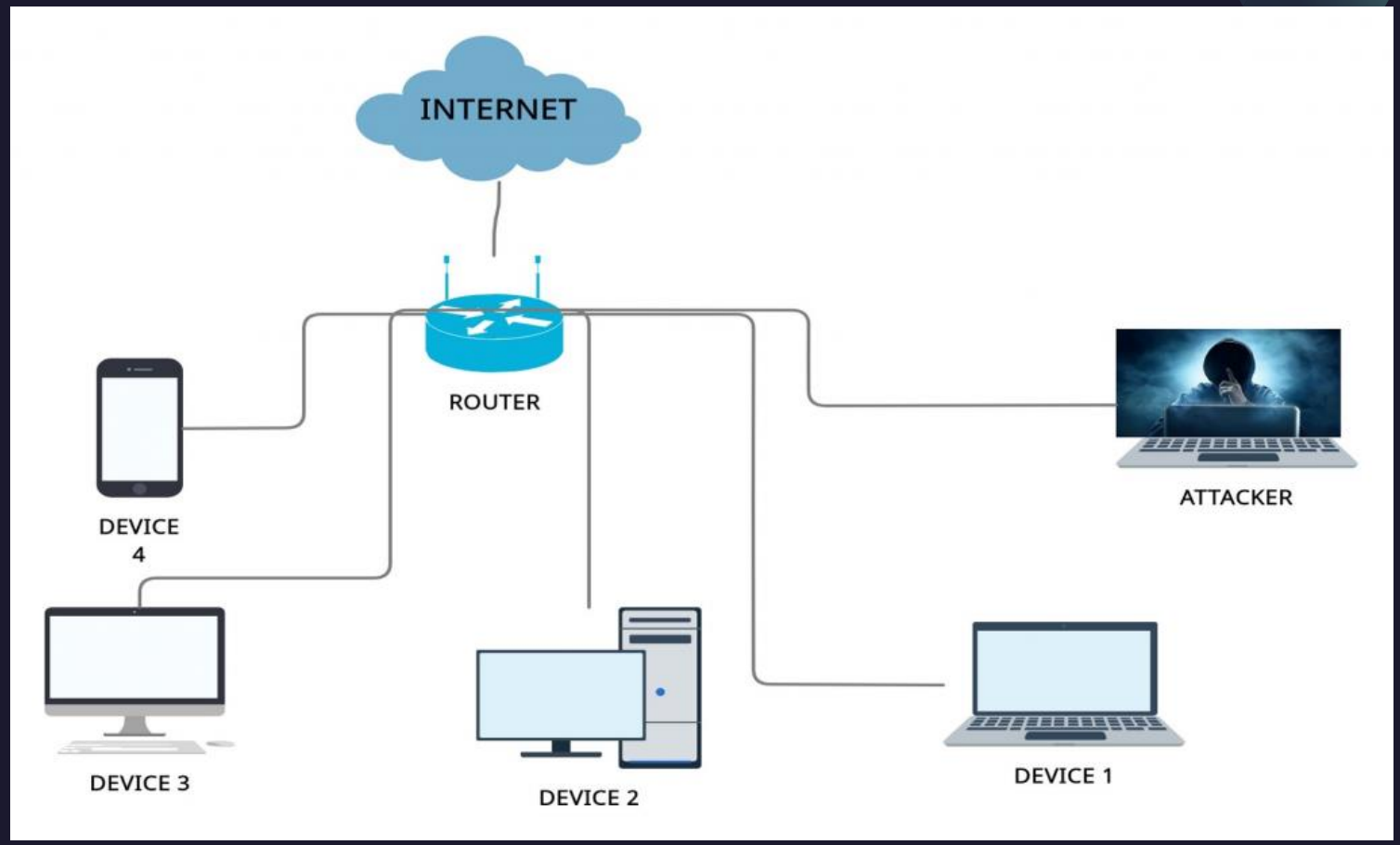
ARP Spoofing / ARP Poisoning

- ARP (Address Resolution Protocol) protokolü MAC adreslerinin çözümlenmesini sağlar. Yani IP adreslerini MAC adreslerine çevirir. Bu çevirme işlemini yapabilmek için MAC adreslerini ve IP adreslerini cahce denilen bir tabloda tutar. ARP protokolü OSI modelinin 2. katmanında (Data-Link) çalışır.
- ARP Spoofing (ARP Kandırmacası)/ARP Poisoning(ARP Zehirlenmesi) ise ARP paketlerinin kullanılarak yerel ağa bağlı olan cihazların gönderdiği paketlerin bu cihazların kandırılmasına ve kandırılmış cihazların ağ trafiğini izlenmesine ve manipüle edilmesine imkan veren saldırıdır.

- Şekildeki LAN’a bir saldırganın dahil olduğunu varsayalım.



- Saldırgan router’a “ben device 1’im” diye broadcast paketleri gönderir. Router ARP tablosunu belirli aralıklarla bu gelen mesajlara göre düzenlediği için bir süre sonra device 1 olarak artık saldırgan cihaz tutulmaya başlar.



Sorular ?

Teşekkürler