SİBER GÜVENLİK - GİRİŞ

Ankara Üniversitesi

Giriş

- Bir iletişim ve paylaşım ortamı olarak ortaya çıkan internet, kısa sürede tüm dünya coğrafyasını etkisi altına almıştır.
- Özellikle 21. yüzyıl dünya coğrafyasının internet ağı ile iç içe geçtiği bir yüzyıl olmuştur ve olmaya devam etmektedir. Çünkü tüm dünya insanları internet sayesinde birbirleriyle yüksek hızda iletişim kurmuş durumdadır.
- Aynı zamanda önemli ticari, siyasi, ekonomik ve sosyo-kültürel alanlarda uluslararası ilişkiler alanında devletler arasında güçlü bir bağ oluşmuştur.

Giriş

- İnternetin üç temel varlığı vardır:
  - Bilgisayarlar,
  - Kullanıcılar,
  - Ağlar.
- Sürekli değişen bilgisayar teknolojileri ve çeşitli yeteneklere sahip olmaya başlayan kullanıcı kesimleri sayesinde ağ teknolojilerinin geliştiği gözlemlenmiştir.
- Ağ teknolojilerinin gelişen ve yaygınlaşan bu kullanımları, önemli güvenlik sorunlarını da beraberinde getirmiştir. Bu nedenle kurum, kuruluş ve bireylerin varlıklarının korunması amacıyla siber güvenlik ortamı sağlanmaya çalışılmıştır .

Giriş

- Siber kelimesi, altyapısı bilgi sistemleri olan ağlara verilen isimdir.
- Siber güvenlik, bilgi sistemlerinde kurum, kuruluş ve kişiler tarafından kurulan iletişim, yaşam, bütünleşme, maddi veya manevi varlıkların, verilerin elektronik ortamdaki güvenliğinin, bütünlüğünün ve gizliliğinin korunmasıdır.
- Özetle, altyapısı bilgi sistemlerinin bulunduğu siber ağlar üzerinde sanal hayatın güvenliğinin sağlanması, veri bütünlüğünün ve mahremiyetinin korunması siber güvenlik adı altında korunmaktadır.

Giriş

- Siber güvenliğin öncelikli amacı internet ortamında kişi ve kurumların verilerini güvence altına almaktır. Bu hayati konunun farkında olunmaması ciddi tehditlere yol açabilir.
- Örneğin, kötü amaçlı bir kişi ağ üzerinden cihazlara sızarak verileri ele geçirebilir veya kredi kartı bilgileri, kullanıcı kimlik-parolaları gibi kullanıcı kimlik bilgileri çalınabilir. Bireylere, kurumlara, büyük şirketlere ve hatta devlet çapında mali zarar verebilir.
- Son araştırmalara göre siber saldırılar dünya ekonomisine milyarlarca dolara mal oluyor. Günümüzde siber saldırılar sadece basit bilgisayar saldırıları olarak değil, arkalarında büyük gruplar, şirketler ve eyalet hükümetlerinin olduğu bir tür büyük iş olarak görülebiliyor.
- Bu örneklerin her biri bir siber saldırıdır ve ancak iyi bir siber güvenlik politikası ile korunabilir.

Güvenlik Problemi/Çözüm

- Son yıllarda İnternet kullanımı hızla artmıştır ve artmaya da devam etmektedir.
- Bireyler ve şirketler, gerçek dünyadan ziyade siber alanda birden fazla günlük işlem gerçekleştirir. Dijital ortamın yaygın kullanımı nedeniyle olağan suçlar da dijital ortama taşınmaktadır.
- Son zamanlarda siber suçlular, saldırıları otomatikleştirmek ve saldırıların etkisinden yararlanmak için hizmet olarak siber saldırıları kullanmaya başlamışlarıdr. Saldırganlar, donanım, yazılım ve iletişim katmanlarında bulunan güvenlik açıklarından yararlanırlar.
- Bulut bilişim, Nesnelerin İnterneti (IoT), sosyal medya, kablosuz iletişim ve kripto para birimleri gibi yeni teknolojilerin ortaya çıkması da güvenlik sorunlarını gündeme getirmiştir.

Güvenlik Problemi/Çözüm

- Dağıtılmış hizmet reddi (DDoS) saldırısı, kimlik avı, ortadaki adam saldırısı, parola saldırısı, uzaktan saldırı, ayrıcalık yükseltme ve kötü amaçlı yazılım saldırısı gibi çeşitli farklı siber saldırılar vardır.
- Yeni nesil saldırılar ve savuşturma teknikleri nedeniyle, mevcut koruma sistemleri (Firewall, saldırı tespit sistemi, antivirüs yazılımı, erişim kontrol listesi vb.) bu gelişmiş saldırıları tespit etmede artık etkili değildir.
- Bu nedenle, siber güvenlik alanındaki saldırılara karşı yenilikçi ve daha uygulanabilir çözümler bulunmasına acil bir ihtiyaç vardır.

Güvenlik Problemi/Çözüm

- Makine öğrenimi, derin öğrenme, bulut platformları, büyük veri ve blok zinciri gibi trend teknolojilerin birlikte kullanılması, mevcut ve gelecekteki siber saldırılar için umut verici çözümler olabilir.
- Bu teknolojik çözümler, kötü amaçlı yazılımları, saldırı tespitini, spam tanımlamayı, DNS saldırı sınıflandırmasını, sahtekarlığı tespit etmeyi, gizli kanalları tanımayı ve gelişmiş kalıcı tehditleri ayırt etmeyi sağlamaya yardımcı olabilir.
- Ancak bazı umut verici çözümler, özellikle makine öğrenimi ve derin öğrenme, akıllı siber saldırılara karşı çözümler önerirken dikkate alınması gereken kaçınma tekniklerine karşı dirençli değildir.

Temel Tanımlar

- **Bilgi:** Verilerin anlam kazanmış halidir.
- **Güvenlik:** Toplumsal yaşamda düzenin aksamadan yürütülmesi.
- **Bilgi Güvenliği:** Fiziksel veya elektronik bilgilerin yetkisiz erişimini, kullanımını, ifşasını, değiştirilmesini, gözden geçirilmesini, kaydedilmesini veya imha edilmesini önleme uygulamasıdır. Bilgi güvenliğinin temel amacı, verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumaktır.

Temel Tanımlar

- **Siber:** Cyber kelimesinden uyarlanmış, İnternet ve bilgisayar ağlarının tamamını kapsayan sanal ortam.
- **Siber Güvenlik:** Siber güvenlik, bilgisayarları, sunucuları, mobil cihazları, elektronik sistemleri, bilgisayar ağlarını ve verileri kötü niyetli saldırılardan koruma uygulamasıdır.
- Veri-, bilgi- ve ağ güvenliği, saklanan verilere veya iletilen verilere yetkisiz erişimi, kullanımı, değişikliği veya imhayı önlemeyi amaçlarken; siber güvenlik, uçtan uca bilgi akışlarını kapsayan çok daha geniş bir uygulama alanına sahiptir.

Temel Tanımlar

- **Veri güvenliği,** dijital verilerin tüm yaşam döngüsü boyunca yetkisiz erişim, değişiklik veya ifşadan korunmasıdır.
- **Ağ güvenliği,** iletişim ortamlarında iletilen verilerin yanı sıra bilgisayar ağlarının gizliliğini, bütünlüğünü ve erişilebilirliğini korumaktır.
- Geçmişte veri veya bilgi güvenliği terimi çokça kullanılırken günümüzde ağırlıklı olarak siber güvenlik kullanılmaktadır.

Temel Tanımlar

- **Etik:** Ahlâk ile ilgili (meslek ahlakı), karakter/kültür olarak doğru tutum ve davranışlardır.
- **Hack:** Bir sistemin işleyiş kurallarının dışına çıkabilmektir. (Bir açıklığı kullanmak)
- **Hacker (siber korsan):** Bilişim alanında üst düzey bilgisi ile yazılım geliştiren/kullanan ve aradığı bilgiye erişen kişidir.
- **Hacking:** Bir sistemin açıklarından faydalanarak izinsiz erişim sağlamak veya sistemi ele geçirmektir.

Temel Tanımlar

- **Etik Hacker:** Bilgi ve yeteneğini etik kurallar çerçevesinde kullanan kişilerdir. Zayıflığı tespit eden ve bu güvenlik açığını kapatmaya yardımcı olan kişidir.
- **Etik Hacking:** Sistemin açık ve tehlikeli yönlerini ortaya çıkarmak için yapılan erişim veya ele geçirme işlemi. (Sızma Testi)
- **Saldırı:** Saldırganların kötü niyetli amaçları için uyguladıkları (siber) faaliyetlerdir.
- **Savunma:** Bilişim sistemlerini siber tehditlere karşı korumak için alınan önlemlerdir.

Temel Tanımlar

- **Tehdit:** Bir sistem veya kuruluşta zarara neden olabilecek istenmeyen bir olayın potansiyel olarak nedenidir.
- **Zafiyet (Vulnerability):** Saldırgana fırsat verebilecek, yazılım, donanım ve prosedürlerdeki açıklıklar, güvenlik boşluklarıdır.
- **Şifre:** Gizliliği olan şeylerin açılması, kullanılması veya iletilmesi için gerekli olan işaretler (harf, rakam, sembol, vb.) bütünüdür. (8F10D078B2799206CFE914B32CC6A5E9)
- **Parola:** Gizlilik ortamında tanıma veya iletişim için gerekli anahtar (kelime) ifadedir. (Gizli) pArola123

Temel Tanımlar

- **Kriptoloji:** Şifre Bilimidir. Belge veya mesajın şifrelenip iletilmesi ardından deşifre edilmesini gerçekleştirmektir (İletişimde gizlilik bilimi) (Kriptografi-Kriptoanaliz)

- **Adli Bilişim (Forensic):** Bilişim sistemleri üzerinden elde edilen nesnelerinin (yazı, resim, program vb.) mahkemede sunulmak üzere (delillerin) toplanması, saklanması, derlenmesi, analizi ile ilgili standartların ve işlemlerin bütünüdür.

Temel Tanımlar

- **Network(Ağ):** İki veya daha fazla bilgisayarın kablolu ya da kablosuz iletişim araçları üzerinden yazılım ve donanım bileşenleriyle birbirine bağlanması ile meydana getirilen sistem bütünüdür.
- **Server(Sunucu):** Bir ağ üzerinde, program veya bilgiyi, farklı kullanıcılara/sistemlere paylaştıran/dağıtan donanım veya yazılıma verilen genel isimdir.
- **Linux:** Unix işletim sistemine fikirsel ve teknik anlamda atıfta bulunarak geliştirilmiş açık kaynak kodlu, özgür ve ücretsiz (destek hariç) bir işletim sistemi çekirdeğidir. (GNU-GPL) (Unix türevidir.)
- **Kali Linux:** Sızma testleri için geliştirilmiş Debian tabanlı bir linux dağıtımıdır. Backtrack 5 devamı niteliğindedir.

Temel Tanımlar

- **Pentest (Penetrasyon-Sızma Testi):** Belirlenen bilişim sistemlerine mümkün olabilecek her yolun denenmesi ile sızılması.
- Kurumların kendi iletişim alt yapısı, sunucu, uygulama veya sistemlerine uyguladıkları sızma testleridir.
- Test sonucu tespit edilen açıklıkların raporlanması ve yöneticilere iletilmesi işlemleridir.
- **Pentester:** Sızma testi yapan uzman kişi.

Temel Tanımlar

- **Metasploitable:** Güvenlik açıkları hakkında bilgi sağlayan, sızma testleri ve IDS imza gelişmesinde yardımcı olan bir framework projesidir.
- **Exploit:** Sistemler ve servisler üzerinde yer alan güvenlik açığının kullanılmasını sağlayan araçlara denilmektedir.
- **Payload:** Hedef sistem veya servis üzerinde çalıştırılması istenen kodlara denir. (Exploit işleminin ardından)

Güvenlik

- **Hiçbir zaman güvenlik %100 değildir!**

- Siber Güvenlik
  - İnternet güvenliği
  - Ağ güvenliği
  - Bilgisayar güvenliği
  - Mobil güvenlik
  - Siber Savaş