**İNTRODRUCTİON TO CYBERSECURİTY DERS NOTLARI**

**MODÜL 1**

**Siber güvenlik dünyası :**

Ağ bağlantılı sistemleri , verileri , dağıtmak ve zarara uğratmaya karşı koruyarak bireyleri ve devletleri diğital saldırılara korumaya yönelik çaba ..

* Kişisel: kimlik,veriler,işlem cihazları
* Kurumsal: kurum itibarı,veriler,müşteriler
* Devletler: ekonomik,iktisadi,ulusal

**Kişisel verilerin korunması :**

* Çevrimdışı bilgi: kaydolduğun yerler,kişisel yasam ile ilgili tüm bilgiler
* Çevrimiçi bilgi: sosyal kimlik

**Verilerin:** kişisel bilgiler eğitim kayıtları tıbbi kayıtlar vs.

**Verilerin nerede ? :** sunucu yerleşimi , randevu için sigorta şirkeri istemi mağaza bilgileri , reklam amaçlı 3. Kişiler ile paylaşım ..

**Akıllı cihazlar:** fittness giyilebilir cihazlar vs.

\*çevrimiçi bilgiler ücretsiz fakat sosyal medya reklamlarla ilerler !

**Bilgisayar korsanı ne istiyor? :** Kimlik ve para..

Kimlik hırsızlığı = uzun vadeli kazanç

ISS internet servis sağlayıcısı , arama motorları, sosyal medya vs reklamları için …

**Kurumsal veriler :**

**Organize veri türleri :**

Geleneksel : alışveriş , satış , işe alım, finansal temel organizasyonlar vs.

\*Nesnelerin interneti ( IoT) fiziksel nesnelerden oluşan geniş ağ , internete bağlı bulut ve depolama gerekli .

Küp : ( 1991 John McCumber ) 3 boyutu var ,

1: Bilgi koruma temel prensipleri :

* Gizlilik – yetkisiz kullanım
* Bütünlük – hash checksum
* Uygunluk – başka kişilerin erişimi engelleme

2: Her durumda bilgi koruma :

* İşleme – dolaşımda bulunur örn: veritabanı güncelleme
* Depolama – kalıcı depolama aygıtları
* İletim – aktarımdaki veriler

3: Veriyi korumak için önlem :

* Teknoloji – yazılım, donanım
* Politika prosedür – planlar kanunlar vs.
* Farkındalık eğitim-öğretim- bilgi sahibi olmak
* Kimlik avı çok yaygın
* Veri güvenliği sonuçları ağır örneğin itibar kaybı vs..

**Siber saldırganlar :** güvenlik açığından yararlanan birey yada gruplar ..

Saldırı türleri :

* Beyaz şapka: legal
* Gri şapka : bilgiyi amacı eşiğinde kullanan
* Siyah şapka: illegal

**Tehditler :**

İçeri: kayıtlı ve kayıtsız içeriden ağ veya tıklama örn.phısıng

Dışarı : sosyal mühendislik vs..

**MODÜL 2**

**Siber saldırıyı analiz etmek :**

**Kötü amaçlı yazılım türleri :**

* Casus yazılım
* Reklam yazılımı
* Arka kapı : yetkisiz erişim uzaktan
* Fidye yazılımları
* Scareware : korkutma yazılımı
* Rookit kök araç takımı : sistem değiştiren yazılım, güvenlik açıklarından yararlanır, tesbit edilmesi zordur.
* Virüs
* Truva atı : gerçek amacını maskeler , kötü amaçlı işlemler gerçekleştirir, kendini kopyalamaz.
* Solucanlar : karşılıklı olarak kendini kopyalar , yük taşır .

**Nasıl anlarsın?**

* CPU kullanım artışı
* Bilgisayar donuyor ve çöküyorsa
* Web tarama işlemi azalma
* Ağ bağlantısı sorunları
* Silinen dosyalar ve paralar
* İzinsiz e posta vs..

**Sızma yöntemleri :**

* Sosyal mühendislik
* DOS servis engelleme : ağ hizmetinin kesilmesi , çok miktarda trafik veri trafiği ile ağ sekteye uğrar, kötü amaçlı biçimlendirilmiş paket gönderimi
* DDOS dağıtılmış dos : birden çok şifrelenmiş kanaldan aktarılır .
* BOTNET : güvenli olmayan web site , yüzbinlerce bota sahip olabilir.

**Yol üzerindeki saldırılar :**

* (MITM) ortadaki adam : cihaz kontrolü ele geçirme
* (MITMO) mobildeki adam : mobil cihaz bilgilerini ele geçirme

**SEO nun yükseltilmesi :** kötü amaçlı sitelere yönelik boru hattı .

**Wifi parolası kırma :**

**Parola saldırıları:**

* Püskürtme
* Sözcük saldırıları
* Kaba kuvvet : deneme yanılma
* Rainbow saldırısı : karma oluşturmak için kullanılan site belirleme
* Trafik müdahalesi : şifreyi açık okunabilir olarak saklarsanız yetkili ve yetkisiz erişim olur .

**Crack zamanları :**

**Gelişmiş kalıcı tehditler ( APT ) :**

Amacı: özelleştirilmiş yazılımları hedefin bir veya birden çok sistemine yaymak orada tesbit edilmeden kalmak , genelde devletler ..

**Güvenlik açığı kullanımları :**

* Donanım güvenlik açıkları
* Yazılım güvenlik açıkları
* Arabellek taşması
* Doğrulanmamış girdi
* Yarış koşulları
* Güvenlik uygulamalarındaki zayıflıklar
* Erişim denetim sistemi

**Kripto para birimi :**

* Blokchain sistemine kayıtlı
* 3. Şahıs müdahalesi olmaz
* Madencilikle doğrulanır

\*Kripto hırsızlığı : cryptojacking

**Tehdit türleri :**

* DDOS: birden fazla cihazın eş zamanlı olarak hedefin trafiğini arttırarak saldırı gerçekleştirmesi .
* Phısıng : oltalama , şifre ve link aracılığıyla
* Malware : kötü amaçlı yazılım kısatması , virüs , solucan , Truva atı , randsomware örn: keylogger
* Bruteforse : deneme yanılma .

**MODÜL 3**

Cihazı emniyetli hale getirmek için yap :

* Güvenlik duvarını aç
* Antivirüs – antispware yükle
* İşletim sistemi ve tarayıcı yönet
* Parola koruması ayarla

\*web tabanlı IoT cihaz tarayıcısı : shodan

\*SSID hizmet kurulum tanımlayıcısı : ağ tanımlama yolu

\*WPA2 şifreleme yapılması lazım .

Kracklerden kurtulmak için :

* Güvenlik güncellemeleri gelir gelmez yap
* Vpn kullan
* Anahtarların ağ modüllerine sahip tüm cihazlar için kontroller kullan (NIC)

Halka açık wifi :

* Wifi noktası geçerliliğini kontrol et
* ‘https’ olduğundan emin ol
* Vpn kullan
* Hassas veri paylaşımında yada kullanımında veri planı kullan

\*kullanmadığın zaman bluetoot kapat

\*Abd ulusal standartlar teknoloji enstitüsü (NIST) iyileştirilmiş parola kapsamı yayınlamış ;

- en az 8 en fazla 64 karakter ,

- yaygın olanları kullanma ,

- yazarken parolayı gör hata payını en aza indirmek için .

**Şifreleme EFS energy file system :**verileri şifreleyen Windows özelliği .

* Klasör seç
* Sağ tıkla ve özellikler de
* Gelişmiş tıkla
* Veriyi korumak için şifrele
* Korunanlar yeşil renkte .

Veri güvenliği:

\*verileri yedekle

\*ev ağı kullan (yerel ağ)

\* (NAS) depolama cihazları

\*AWS amazon web services gibi bulut depolama hizmetleri ..

Verileri kalıcı olarak nasıl sileriz ? :

* Microsoft : S delete
* Mac : Secure empty trash
* Linux : shred

Veya depolama aygıtını yok etmek ..

Notlar :

* Hizmet şartlarını oku ve anla
* Veriler ile ilgili haklar neler
* Verileri birleştirebilir miyim
* Sağlayıcı verilerle ne yapar ?
* Hesaplar kapanınca verilere ne olur ?
* Varsayılanı kabul etmek yerine gizlilik ayarı seç
* Paylaşılan kişiyi sınırla
* Güvenlik politikaları incele
* İki faktörlü doğrulama ve karmaşık şifre

Açık yetkilendirme ( AOUTH) üçüncü taraf uygulama geçiş için parolanızı kimlik bilgilerinizi kullanmaya yönelik olanak sağlayan bir uygulamadır (Google ile giriş gibi )

* Gizli modda çerezler saklanmaz
* Güvenli şifre uygulamaları kullan
* https ile erişin

SOCIALACCESSNOW uygulaması güvenlik geliştirmenin gerekli olup olmadığını vurgular .

**MODÜL 4**

Siber güvenlik cihazları ve teknolojileri :

**Güvenlik araçları** :

* yönlendirici ( router ) : trafiği sağlar , ağ bölümlerini birbirine bağlar
* güvenlik duvarları : ağ trafiğini derinlemesine inceler kötü amaçlı yazılımları tesbit eder ,
* saldırı önleme sistemi : ( IPS ) kötü amaçlı trafiği engeller engelleyen trafik imzası kullanır .
* VPN sistemleri : şifrelenmiş tünel kullanılmasına olanak tanır .
* Antimalware ve antivirüs : kötü amaçlı kodu tanımlamak ve engellemek için davranışsal analiz kullanır .
* Diğer güvenlik cihazları : sistemler web ve e posta , şifre çözme cihazları , istemci erişim kontrol cih vs.

**Güvenlik duvarları :**

Firewall :

* Ağ katmanlı güvenlik duvarı
* Taşıma katmanlı güvenlik duvarı
* Uygulama katmanlı güvenlik duvarı
* Bağlama duyarlı ( profile göre )
* Proxy sunucusu (web içerik filtre )
* Test Proxy sunucusu
* Ağ adres çeviricisi ( NAT ) -özel adres gizler
* Host tabanlı – portlar ve sistem servisi filtre

\*nat : kaynak hedef ıp

\*Proxy : web içeriği sınırlama

\*host : tek işletim sistemi

Port tarama : bağlantı noktası numarası

Kötü niyetli kullanılabilir

Zenmap port tarama uygulaması .

* IDS saldırı tesbit sisemleri ve izinsiz giriş önleme sistemleri
* IPS ağ üzerinde dağıtılan güenlik önlemleridir.
* IDS ağ trafiğini izler kötü iz arar görevi tesbit etmek ve raporlammaktır.ıds tarafından ağ yavaşlatılır genelde çevrimdışı yerleştirilir kopyalanır ve bir anahtar tarafından yansıtılır .
* IPS şebekeyi engelleyebilir , en iyi bilineni snort tur . sondajları tesbit edebilir , saldırıyı algılayabilir ve port taraması gerçekleştirebilir . log analizi için 3. Taraf araçlara entegre olur .

**En iyi güvenlik uygulamaları :**

* Risk değerlendirmesi yapma
* Güvenlik politikası oluşturma
* Fiziksel güvenlik önlemleri
* İnsan kaynakları güvenlik sistemleri
* Yedeklemeleri güçlendirin ve test edin
* Güvenlik yamaları ve güncelleştirmeler
* Erişim kontrolleri kullanın
* Olay müdahalesini düzenli olarak test et
* Ağ izleme, analiz ve güvenlik prog uygula
* Ağ güvenliği cihazları uygula
* Antivirüs
* Kullanıcı eğitimi ( sans enstitü)
* Herşeyi şifrele

**Davranış tabanlı güvenlik :**

\*honeypot : saldırganı cezbeden sanal bir tesbit aracıdır. Saldırgan bilgilerini yakalayıp analiz edebilir.

\*siber tehdit savunması çözüm mimarisi

Net akış (netflow) teknolojisi ağda akan veriler hakkında bilgi toplamak için kullanılır. Netflow toplayıcılarına gönderilir.90dan fazla özniteliğe bakabilir.

**SIZMA TESTİ :**

Pen testi diye geçer . sistem savunmasını geliştirmek için kullanılır . 5 adımda :

* Planlama :

Pasif ve aktif ayak izi ve güvenlik açığı araştırmaları hedef sistem hakkında bilgi.

* Tarama :

Potansiyel erişim noktası belirlemek için port taraması , güvenlik açıkları , hedefle aktif bağlantı

* Erişim kazanma :

Yük ile sömürü paylaşılması , varlıklara yönelik fiziksel engellerin aşılmas , sosyal mühendislik, web yayılma açığı, yazılım ve donanım açıklar , erişim kontrolü ihlalleri, zayıf parolalı wifiler .

* Erişim onaylama:

Arkakapı,Truva atı , rookitler kullanır . kendisini belli etmez.

* Analiz ve özet:

Ürün politika ve eğitimlerde güncelleme içeren rapor.

**Etki azaltmak için yap :**

* Sorun bildir
* Samimi ve sorumlu ol
* Detay ver
* Sebebini bul
* Öğrenilen dersleri uygula
* Tekrar tekrar kontrol et
* Eğit ve eğitil .

**Risk yönetimi :**

Riski sürekli tanımlayan ve denetleyen organizasyonların tümü.

\*maliyet koruduğun varlıktan fazla olmamalı ..

* Riski çerçeveleyin : tehditleri belirle
* Değerlendirme : ciddiyeti belirleyin , bazıları organizasyon durdurur bazıları küçük rahatsızlıklar verir.
* Yanıt verme : eylem planı geliştirin
* İzleme: azaltılan her riski sürekli gözden geçirin.

**(CSIRT) bilgi güvenliği olay müdahale ekibi :**

\*securty playbook derlenmelidir .

\*tehdite verilen yanıtın nasıl tanımlanacağı

\*içeri ve dışarı trafiği açıkla ve tanımla

\*özet bilgiler sağla

\*önemli istatistik ve ölçümlere hızlı erişim

\*tüm ilgili veri kayıplarını ilişkilendir.

**Olay tesbiti önlemeye yönelik araçlar:**

(SIEM) güvenlik bilgileri ve olay yönetimi saldırının erken tesbitini kolaylaştırmak için ağdaki güvenlik cihazlarından tüm verileri toplar ve analiz eder .

(DLP) veri kaybı önleme sistemi hassas verilerin ağdan çalınımını önlemek için tasarlanmıştır . verileri 3 farklı durumda izler ve korur :kullanımdaki veriler , hareket halindeki veriler , beklemedeki veriler ..

**MODÜL 5**

**İş arama uygulamaları :** mdeed,linkedin,monster,careerboilder

**Sertifikalar :**

* cısco certified support tecnıcıan (ccst) –giriş seviye
* Comptia securty + ,
* (CEH) cc council certified etichal hacker
* Isc2 certified information systems securty proffessonel (cıssp) :en tanınan en popüler , 5 yıl sektör tecrübesi ,
* Cısco certified cyberops associate : operasyon merkezlerinde cyber securty analistlerinin ihtiyaç duyduğu beceriyi doğrular.

\*Cyberseek :arz talep durumunu ayrıntıı bilgi veren uygulama . maaşlar , yeterlilik belgeleri ve beceri setleri hk. bilgi verir.