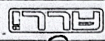


BSG



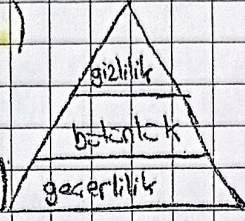
BSG 3 temel unsur içerir (CIA)

diğer unsurlar

1- gizlilik (confidentiality)

2- bütünlük (integrity)

3- erişilebilirlik (availability)
ulaşılabilirlik

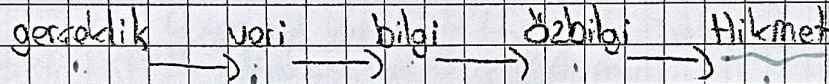


- inkar edememe (non repudiation)
- doğrulama (authentication)
- kanıt tutulması
- veri bütünlüğü
- süreklilik

• Veri → birbirleriyle bağlantısı koparılarak kurulmaması bilinir...

• Bilgi → verinin belli bir anlam ifade edecek şekilde düzenlenmiş haldedir.

• 2. bilgi → tecrübe veya öğrenme şeklinde veya gözlem şeklinde elde edilen gerçeklerin -değerlerin farklılığı -bilinmesi
→ asıl değerli olan özbilgidir.



TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistem Belgesi /Standartı

↳ bilgi gizliliği - bütünlük - erişilebilirlik sağlamak için verilen belge

Kötü Yarılm (Malware)

- Virüsler

- Trova Atları (Trojans)

- Arka Kapılar (Back doors)

- Tarayıcı sarma (Browser Hijacking)

- Korunmasızlık Sömürücüler (Exploit)

- phishing (soyan gülm)

- sniffer (kötüye)

- kondukl (spoof)

- password cracker

- Solucanlar (worms)

- Casus yazılım (spyware)

- Klavye dinleme (keylogger)

- Kötü kullandık Takımı (rootkits)

- Tarsanlar (wabbit)

- reklam yazılımı (adware)

- ağı torkını (Flood)

* phishing → olukl (phishing - arama)

* sniffing → sistem (sistem ve web)

* spoofing → sistem (facebook, net, ip)
hesap galm

Kötü Yazılım Belirtileri

Açılanmış dan arama motoru yerine başka bir arama motoru sonuçları çıkıyorsa

Baslangıç sayfası ayarları değişiyorsa

Favorites ve yet imleri değişiyorsa

int bağlantısı olmadı halde pop-up reklamlar

internet sayfasında bazı tuslar çalışmıyorsa (bir sonraki kutucuğa geçmeye çalışırken tab tuşu çalışmıyorsa)

Bilgisayar kapalı ikon bilgisayarın sabit disk lambası yanmıyorsa

Güvenlik tedbirleri

Kötü yazılımdan korunma
işletim sis. güncellemeleri
anti-spyware
Host (sunucu) bloklama
e-posta kontrolü
browser kullanımı
odis programları
güvenlik duvarı (firewall)

firewall
→ güvenlik duvarı

- Bilginin, programların, servislerin, ekipmanların veya haberleşme ağlarının yıkımı, hırsızlığı, yasadışı kullanımı, değiştirilmesi, kopyalanması da bilginin suçudur.

Bir bilginin suçu işlemediği nedenler arasında

moddi kazanç elde etmek

kisilerin itibarını salırmak

intimam olmak,

sosyal hayatta insanlara aktaramadığını sanal ortamda gerçekleştirilmek

karalamak veya

yokalanma ihtimalinin zor olduğunu düşünerek zebr amaçlı saldırı yapmak gibi sebepler ortaya çıkabilmek.

77

Hackerlar → beyaz sorkalı → iyi niyetli zarar vermeyen
→ siyah → kötü niyetli, karzaa elde etme
→ gri → yeme göre siyah veya beyaz

Bilism sistemlerine zarar vermek amaclı calisan kisi lere genelde cracker tanınmasına dahildirler

Lamer → bilgi yok.
Phreakers → kacak yasta, hacker donusu, programlama bilgisi yok
Script Kiddie → kontrol ve telefon hatlarının anıklaını kullanan hacker.
(kendini hacker yapar. Lamerden çok daha bilgili)

Siber zorbalık
elektronik zorbalık
elektronik iletişim zorbalığı

Adli bilism cesitleri

• Bilgisayar Adli bilismi (Computer Forensics)

→ harddisk, RAM, işletim sistemi araştırmaları

• Bilgisayar ağına yönelik A.B (Network Forensics)

→ ağ sistemleri ve iletişimine

• B. ağ cihazlarına y. A.B. (Network Device F)

→ yönlendirici, switch

• İnternet A.B (Internet F)

→ internet kaynakları ve internet sistemleri

• Bilgi A.B (Information F)

→ Bilgi olarak bilgisi içeren her türlü materyal, barındıran sistemler

Dünyadaki bilism suçları en çok Türkiye, Rusya, Brezilya oluyor.
Sebebi ise yeterli ceza sistemi olmaması

- Adli bilimde dijital delillerin kanıt olarak kullanılabilmesi için 4 safha vardır:

- Toplama (collection)
- inceleme (Examination)
- Gözlemleme (Analysis)
- Raporlama (Reporting)

Telsiz ağların avantajları

- Esneklik → bir gere bağlı kalmama (radyo)
- Kolay kurulum (zaman + para) → kablo döşeme ve masrafı yok
- Sağlamlık → kablo zararı yok

Telsiz ağların dezavantajları

- Güvenlik → radyo dalgalarının dinlenmesi ve verileri ele geçirilmesi kolay
- İletişim hızı → kabloluğa göre yavaş
- Standartlara uyum zorunluluğu → üretilen cihazların tüm dünya standartlarında olması gerekir.

• Telsiz ağların ilk 5 yılı için IEEE 802.11 geçerli olan tek güvenlik protokolüdür. (Güvenlik protokolleri → WEP, WPA, WPA2)

- Bluetooth - düşük maliyet ✓
 - " gürültü toleransı ✓
 - kararlı ses ve veri haberleşmesi sağlanması ✓
 - ortak standart yapısı ✓
 - tüm dünyada uyumlu olması ✓

WiMAX → son kullanıcıya kablo ve ADSL alternatifi olarak geniş band erişimi sağlayabilecek standart tabanlı kablosuz erişim teknolojisi.

→ interneti çok daha geniş alanlara yaymayı hedefler

E-ticaret güvenliği - SET ile SSL arasındaki farklar

- **SSL** de kart bilgilerini gönderen kişinin kart sahibi olduğu garanti edilmektedir.
- SET de edilir.

- **SSL** de kart ve PPS'un ait olduğu bankalar bu şekilde yapılır.

- **SSL** de kart bilgileri internet üzerinden şifrelenmektedir. Mağaza kart bilgilerini görebilir.
- SET de kart bilgilerini mağaza göremez. Sadece banka görebilir.

Bilgisayar güvenliği, veriyi korumak ve saldırıların (hackler) engellenmek için olabilecek tedbirlerin tamamlanması için.

Biz güvenliği ise iletişimin güvenliği ile ilgilidir.

Bilgi güvenliğinin en temel unsurları şunlardır:

- gizlilik (confidentiality)
- kullanılabilirlik (availability)
- kimlik doğrulama (authentication)
- bütünlük (integrity)
- inkar edilemezlik (non-repudiation)

- sorumluluk (accountability)
- erişim denetimi (access control)
- güvenilirlik (reliability)
- emniyet (safety)

} bilgi güvenliğini destekleyen unsurlar.

Gizlilik (confidentiality)

Bilginin sadece yetkili kişilerin - bilgisi kullanan - yaratılan tarafından bilinmesi.

Şifreleme (encryption), anahtar dağıtımı (key distributing) ile ilgili teknikler içerir.

availability
kullanılabilirlik (availability) Bilginin istenildiği zaman yetkili kişilerce kolayca erişebilir-kullanılabilir olmasıdır.

Kimlik kanıtama (authentication) = Bilgiyi gönderen-talan kişilerin gerçekten o kişiler olup olmasına ilişkin ilgilidir.

Bütünlük (integrity) = bilginin içeriğinin kötü niyetle ya da yanlışlıkla değiştirilip değiştirilmediği ile ilgilidir.

İnkâr edememe (non-repudiation) = bilgiyi oluşturmuş ya da kullanan kişinin daha sonra bunun reddedememesidir.

bu gereksinimler siberleme teknikleri ile sağlanabilir.

Sorumluluk (accountability) = belirli bir eylemin yapılmasından, kimin veya neyin sorumlu olduğunu belirlemesidir.

Güvenilirlik (reliability)

Bir bilgisayarın, bir bilginin veya iletişim sisteminin sorunlarına, tasarım gereksinimlerine sürekli ve kesin şekilde uyarak gelmesi ve bunu çok güvenli şekilde yapmasıdır.

Erişim denetimi (access control)

bilgiye sadece erişim hakkı olan kullanıcıların ulaşabilmesidir. (iki tanımlanmış erişim hakkı)

bu amaç için firewall adı verilen yazılım ve donanım kullanılmaktadır.

Emniyet (safety)

Bir bilgisayar sisteminin veya yazılımın işlevsel ortamına gâmele olduğunda, kendisi veya gözetici olduğu ortam için istenmeyen potansiyel veya bifiil tehlike oluşturacak etkinlik-olayları önleme tedbirlerini içerir.

Güvenlik Düzeyleri

- 1- Kayıt alanı düzeyinde koruma
 - 2- Veri kaydı düzey kor.
 - 3- Uygulama programı düzey. Sorgulama / koruma
 - 4- Bilgisayara bağlanmayı sorg.
 - 5- Ağ kaynaklarını hizmet türleri açısından koruma
 - 6- Ağ girişi sorg / koruma
- en sıkı korumayı sağlar, iyi bir şifreleme ve şifre orantıları ile algoritması kullanılır.
- benzerler, biri ilgili uygulama prog. girişi, diğeri bilgisayar sistemine girişi denetler.
- genel olarak ağ dışından bağlanmayı - ağ üzerinden sunulan hizmetlere erişimi denetler.
- Firewall tarafından sağlanır koruma

Bir ağda güvenlik sağlanması yapılacaksa nerden korunması gerektiğine karar verilmelidir. Bunlar:

Veriler → (sizlilik - bütünlük - kullanılabilirlik)

Kaynaklar
Sorgular

Denetim → pasif

Engelleme
Değiştirme
Oluşturma } aktif - etkin saldırı türü kabul edilir.

email spoofing başka kullanıcı adına e-posta gönderilmesi
" bombardement

brexit-in verilen hizmetlerin closure dışı bırakılmasına yönelik saldırı

telnet attack uzaktan erişim protokolünün açıklandan faydalanır saldırı

NFS attack ağ dosyasına yapılır. ağ erişimi closure dışı bırakılır.

IP spoofing IP adres yanıltmasıyla yapılır

Intruder installed trojan horse prog → girilen sisteme daha sonra tekrar girilebilmesi - uzaktan yönetim için ajan prog. yerleştirilmesi

İletişim Protokollerini kullanan Saldırıları

- IP spoofing (sohtecilik)
- ARP attacks
- Rostgele (port) taraması
- UDP spoofing - sniffing (dinleme)
- Internet Routing Attack (yönlendirme saldırısı)
- Denial of ping
- ICMP attacks
- TCP dizi numarası saldırısı (TCP sequence number)
- Ortodaki adam sold.

İşletim sistemine özel Saldırıları

exploit denir → sistem tabanlı saldırı yani Unix için yapılan Windows

İşletim sistemleri seçilirken :

- Kurulum kolaylığı
- Donanım gereksinimleri, serice edilebilirliği
- Kullanım ve yönetimi
- Güvenlik
- Güvenlik
- uyumluluk
- Riyat ve destek

Uygulama katmanlı Saldırıları

DNS, SMTP, URS saldırıları

Verilerin giriş ile saldırıları

URL sohteciliği

Kötü niyetli Java ve ActiveX uyg. parçacıkları

Sistem Log solü (güvenlik dosyasına çok sayıda giriş yapılarak log dosyasının dolmasına ve sistemin kapatılmasına sebep olur)

Güvenlik Strajileri

- Önleme (prevention)
- tespit (detection)
- karşılık verme (response ya da reaction)

Güvenlik Duvarları

Paket Filtreleyici G.D (Packet filtering firewalls)

Devre Düzeyinde G.D (Circuit-level F.)

Uygulama Düz. G.D veya Vekil Sunucular (Application-Level F. or Proxy Server)

Paket filtreleyici güvenlik duvarları basit bir güvenlik adımı sağlarlar ve paketlerdeki veri içeriğine bakmazlar.

Devre D.G.D. duvarından geçen paketler için tek giriş noktasıdır. Dışarıdaki bilgisayarlar sadece bunun adresini bilirler. Böylelikle, ortasındaki ağ güvenli bir şekilde korunur.

Ayrıca asılama ve yetkilendirme yapılır. Verinin içeriğine bakılmaz.

Uygulama Düz. G.D. ise bilginin içeriğine bakarak paket geçişine karar verir. Asılama ve yetkilendirme kullanılır.

Gift-euli güvenlik duvarları daha güvenli bir yapı sunarken performans ve esneklik bakımından, perdelenmiş alt ağ g.d. daha düşük seviyededirler.

E-posta güvenliğine Yönelik Tehditler

Gizlilik adımındaki etkililik

Her türlü
pistlik

Brute force (Kaba kuvvet)

Fake Mail

Phishing

Keylogger (Trojan)

Uygulama zafırları

Sosyal mühendislik

XSRF - CSRF - XSS → saldırıyan SS: kodları sileye enjekte dımaı

Clickjacking → Browser güvenlik ağıdır

Sosyal müh.: İnsan ve PC tabanlı, örnekleri: sahte mail, web sitesi benzeri yapıp bilgi alma, reklama tıklama para kazan, firma yetkilisi tutma

Etheral = TCP/IP mesajlarını analiz:

Wireshark, bilgisayara bağlı olan her türlü ağ kartlarındaki (ethernet kartı veya modem kartı) tüm TCP/IP mesajlarını analiz eden bir programdır.

- sebebe probleminde sorun çözüme
- güvenlik problemlerini sınırlamak
- uygulamaya konan protokollerde oluşan hataları anlamak veya arındırmak
- ağ probleminin nereden bilgileri öğrenilebilir amacıyla kullanılır

Wireshark =

Birçok işletim sistemine uygundur.
Yerel ağ üzerindeki paketleri tutar, ayrıntılı şekilde paketlenen bilgileri gösterir.

- Tutulan bilgileri kaydedebilir.
- Gösterdiği kriterlerde paket arar, filtreler.
- Gösterdiği istatistikleri kullanıma sunar.
- Birçok protokol için şifre çözüme desteği sunar.

Wireshark bunlarla kullanılabilir:

- Ağ trafiği tespiti
- Veri madenciliği
- Saldırı tespiti
- Port tarama tespiti
- Virüslerin buluşup bulmadığını veya Denial of Services (DoS) saldırıları bulma
- Bağımlı sorunu tes
- Çoşuk yolum tes

Linux

Neden Linux =

- Hız
- Yönetim
- Güvenlik
- Sağlamlık

Özellikleri

- Birçok kullanıcı desteği
- Çok güçlü olması
- Çok istemci desteği

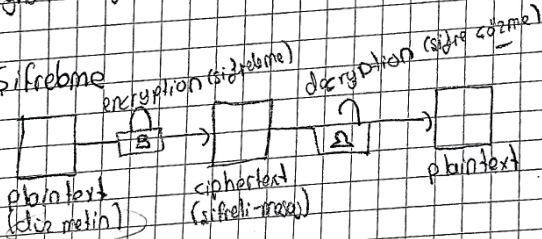
- TCP/IP desteği
- Dosya yapısı
- Kabuklar (shell)

5.1

Ağ üzerinden yapılan saldırı türleri:

- İfşaat - açığa çıkarma (disclosure): mesajın içeriğinin herhangi birisine verilmesi veya uygun kriptografik ortamda sahip olmama
- Trafik analizi: bağlantı sıklığı, sayısı, bağlantısız ortamda ise mesajların sayısı, uzunluğu belirlenebilir.
- Gerçekçi gizleme (masquerade): hileli bir kaynaktan ağa mesaj gönderme, saldırgan, gerçek kullanıcıdan mesaj getiriyormuş gibi yapabilir.
- İçerik değiştirme (Content Modification)
- Sıra Değiştirme (Sequence " ")
- Zamanlamayı Değiştirme (Timing " ") mesajları geciktirme veya yenileri yollama
- İnkarcılık (repudiation) alınan veya gönderilen mesajın kaynak tarafından inkar edilmesi

Sifreleme



$$K = 2$$

$$B = 1$$

Sifreleme Algoritmaları

- Simetrik Sif. Alg.
- Asimetrik Sif. Alg.

Simetrik Sif. Alg. Basit

- Bir tane gizli anahtar vardır. (sifreleyen ve sifreyi çözen)
- Hızlıdır. (simetrik > asimetrik)
- Elektronik cihazlara uygulamak daha kolaydır
- Anahtarın büyüklüğü - bit sayısı önemlidir.

Simetrik

Kuvvetli Yönleri

- Hızlıdır
- Donanım ile birlikte kullanılabilir
- Güvenlidir

Zayıf Yönleri

- Güvenli anahtar dağıtımı zordur.
- Kapasite sorunu vardır.
- Kimlik dağıtım ve bütünlük ilkeğini güvenli şekilde gerçekleştirilmeli zordur.

Asimetrik

Kuvvetli Yönleri

- (B-tiler), kimlik dağıtım ve gizlilik hizmeti güvenli bir şekilde sağlanabilir.
- Anahtar kullanıcı tarafından belirlenir.

Zayıf Yönleri

- Sifreler uzun olduğu için algortma yavaş çalışır
- Anahtar uzunluğunun korunması gerekir

• Asimetrik şifrelemenin kurulması simetrikten daha zordur.

• İki anahtarlı şifrelemeden dolayı inkar edemeyi sağlayan sayısal imza gibi yeni yöntemler geliştirilmiştir.

• Anahtarları kullanarak bilgileri çözme işlemi CPU zamanının çok fazla olması (bu zaman ile uzunluğu ile dşsel olarak artar)

Simetrik Şifreleme Alg.

- DES (data encryption standard)
- Triple DES
- IDEA (international data ency Alg)
- Twofish
- IRON
- AES
- RC4
- MD5
- SHA

Asimetrik Şifreleme Alg

- DH (diffie helman)
- RSA
- DSA (digital signature Algorithm)
- Elliptik eğri A. (ECC)

• Günümüzde simetrik ve asimetrik şifreleme birlikte kullanılmaktadır (melez)

DNS: Domain Name System DOS: Disk Operating System

IP Sıtçılığı (IP spoofing)

sahte kaynak IP adresi ile paketlerin gönderilmesidir

TCP SYN paketi ile Saldırı Saldırının amacı bağlantı kurmak değil sunucu kaynaklarını yormak ve kapasiteyi dolduraktır. Sunucu gerçek kullanıcılar tarafından erişilemez olur.

IP servisi durdurma Saldırısı (Smurf) = hedef bilgisayara ping isteginde bulunulur. Ancak ping hedef makinenin ip'sinden geliyormuş gibi hazırlanmıştır. Bu durumda da ağ üzerindeki tüm makineler, hedef makineye ping atar. hedef makinenin boğulması kesilir.

Arp Saldırıları (Address Resolution Protocol) =

mac flooding → hedef bilg. ARP tablosunun yanlış bilgilerle dolmasını sağlayarak, hedef bilg. göndermeye paketlerin saldırının istediği adrese gitmesini sağlar.

man in the middle → saldırı, sahte ARP cevaplarının kendine kendi bilgisayarının MAC adresini yazarak hedef bilg. akan tüm paketleri kendi istinden geçirip bircok bilgiye ulaşabilir.

Denial of Services → amaç, hedef bilg. akan paketleri dinlemek değil, hedef bilg. servisi deli bırakma (DOS saldırısı) yapmaktır.

• Arp saldırılarından korunabilmek için alınabilecek önlemler:

- Statik veya dinamik ARP koruması kullanılması
- ARP sınırlama

5.2

Kriptografi: Bilgiyi şifreli hale dönüştürme işlemi

Kriptanaliz: Bir şifreleme sistemini veya sadece şifreli mesajı inceleyerek şifreli mesajın orijinal halini elde etmeyi amaçlayan kriptoloji disiplini.



Sezar Şifreleme

metin alfabe de kendinden sonra gelecek 3. haffli yer değiştirilerek oluşturulmaktadır

Pigpen (mason) şifrelemesi

Vigenere Sistemi → dünyanın en büyük casusluk ağı

PROMIS (Dava yarelin sistemi) →

ENIGMA → elektromekanik bir şifre çözme makinesidir.

Steganografi → yarıca "gizlemis yazı"

↳ resim, ses, video ortamlarına bilgiler gizlenebilir.

↳ Bilgi gizleme

Hash

hash fonksiyonu gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir.

Hash Fonk. geri dönüşüm olmayan bir fonk.

Gör bilinen hash fonk → MD-4, MD-5, SHA-1

MD-5 (message-digest algorithm 5)

Tek yönlü (gerek arandadır) şifreleme tekniğidir. (128 bitlik çıktı)

SHA-1 (secure hash algorithm)

Tek yönlü. Veriler 160 bit uzunluğundadır.

Web alanında geniş kullanımı vardır.

SHA-2 adı altında hazırlanmış 224, 256, 384, 512 bit uzunluğunda çıktıları üreten cihazları vardır.

DES (Data Encryption Standard)

RSA açık anahtar uygulaması (asas sayı)

BitLocker Şifreleme

The logo features the letters 'H' and 'K' in a large, bold, serif font. The 'K' is stylized with a winged design on its right side. The background is dark blue with a faint, light blue geometric pattern of overlapping triangles in the upper left corner.

HK

SOWACODEHK.COM.TR

