Necmettin Erbakan Üniversitesi

Bilgi Güvenliği
2022-2023 Güz Dönemi

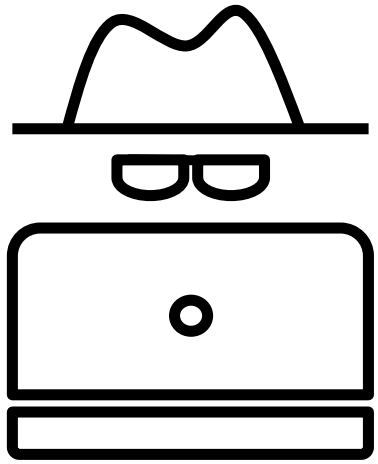
Dr. Alperen Eroğlu
aeroglu@erbakan.edu.tr

Hafta-2

Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler

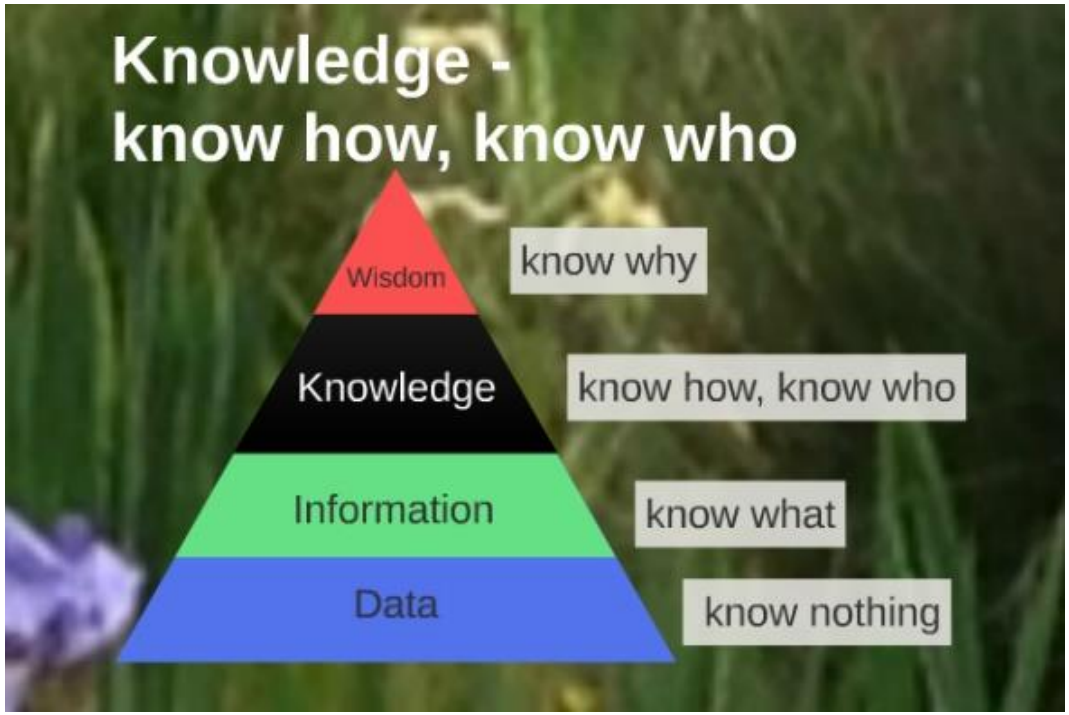
Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler

- Tanımlar
- Siber Saldırılar ve Türleri
- Karşılaşılabilecek Saldırılar ve Tehditler
- Siber Güvenlik Unsurları
- Saldırılara Karşı Koyma Adımları
- Nasıl Bir Siber Güvenlik ve Savunma
- Siber Güvenlik ve Savunmanın Önemi



Tanımlar

- **Veri,** bir durum hakkında, birbiriyle bağlantısı henüz kurulmamış bilinenler veya kısaca sayısal ortamlarda bulunan ve taşınan sinyaller ve/veya bitler olarak tanımlanabilir.



https://knowledgemaverick.files.wordpress.com/2016/05/knowledge-ecosystem.png

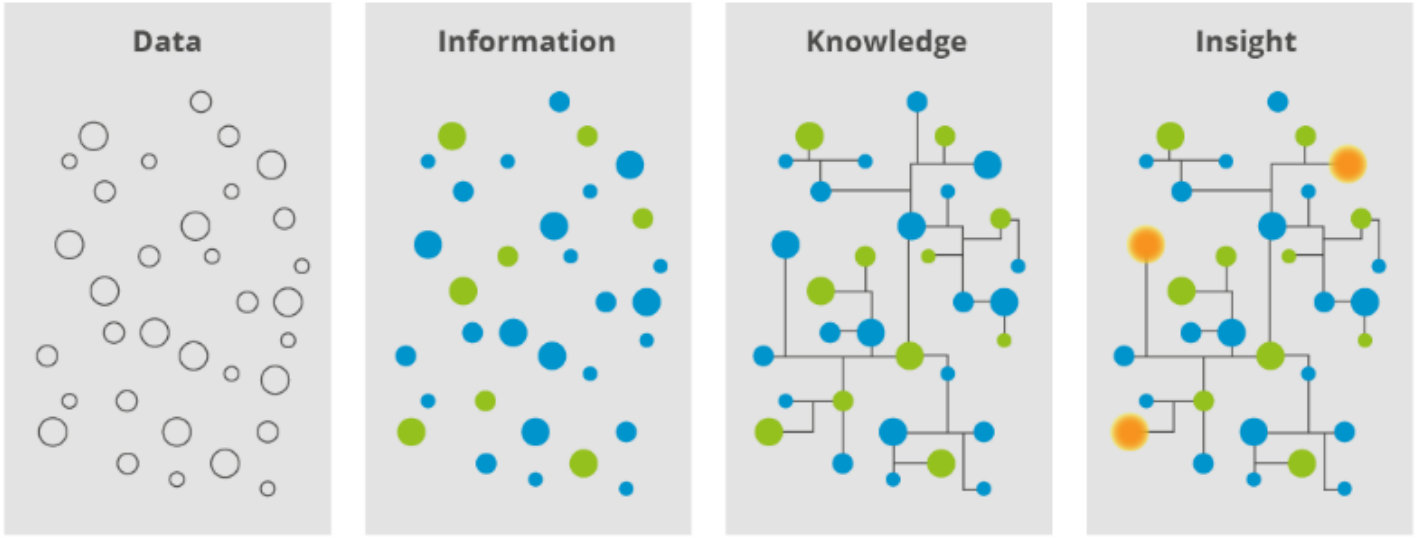
Tanımlar

- **Bilgi,** verinin bir üst formu olup, verinin değerlendirilmiş, analiz edilmiş, düzenlenmiş ve verinin belirli bir anlam ifade edecek forma dönüştürülmüş halidir. Claude Elwood Shannon bilginin; "belirsizliği giderdiğini" ve "bir konu hakkında var olan belirsizliği azaltan bir kaynak" olduğunu belirtmektedir.

https://www.endustri40.com/digitalization-dijitalizasyon-rehberi-siber-guvenlik/

Tanımlar

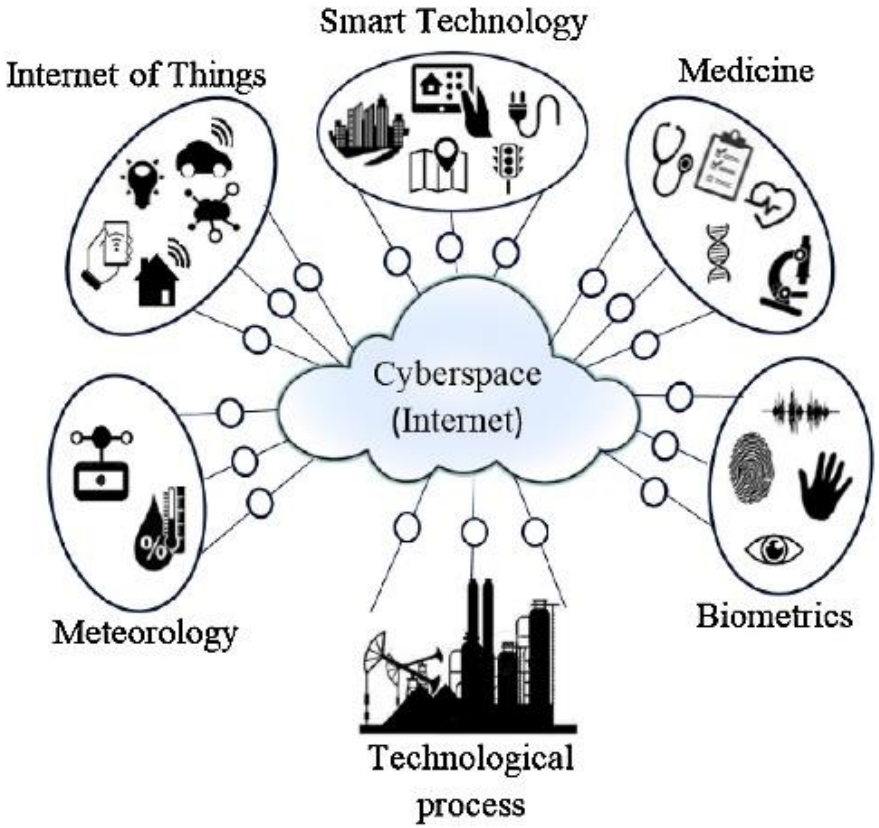
- **Özbilgi (knowledge),** tecrübe veya öğrenme şeklinde veya iç gözlem şeklinde elde edilen gerçeklerin, doğruların veya bilginin, farkında olunması ve anlaşılmasıdır. Diğer bir ifadeyle, ne, niçin, nasıl ve kim olduğunu bilmektir. Kısaca; olayı bilme, olayın altında yatan ilke ve yasaların farkında olma, bu olayı çözebilme becerisi, nevin nasıl yapılacağını kavramadır.



https://www.quora.com/What-is-the-definition-of-data-information-knowledge-and-wisdom-with-their-relation

Tanımlar

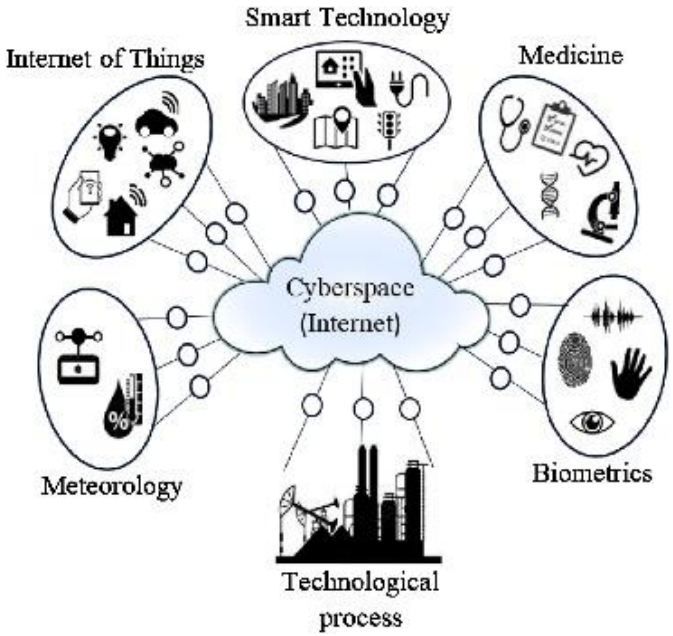
- **Siber**, tanım itibarıyla "elektronik ortamları" ifade etse de içerisinde çok farklı unsurları barındırmaktadır. Bu unsurların bulunduğu, işletildiği, yönetildiği ve geliştirildiği ortamlarda bulunan veriler; "bilgisayar, sunucu, cihaz, donanım, yazılım, protokol, algoritma, işlem, politika, süreç, laboratuvar ve sistem" gibi unsurları içermektedir. İnsanda, artık siber dünyanın önemli unsurlarından birisidir.



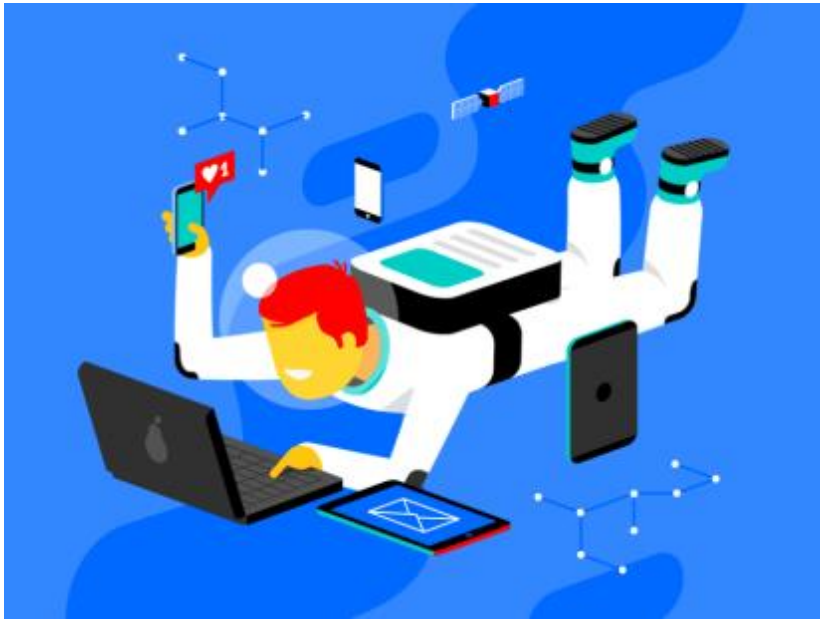
https://www.sciencedirect.com/science/article/pii/S0166361517304244#fig0005

Tanımlar

- **Siber uzay,** "siber alan" veya "siber dünya" olarak ta bilinmektedir. Siber uzay; ulusal strateji dokümanında "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam" olarak tanımlanmaktadır.



https://www.sciencedirect.com/science/article/pii/S0166361517304244#fig0005



https://dribbble.com/shots/4875999-Cyberspace

Tanımlar

- **Siber varlık,** siber ortamlarda bulunan, araçlar, işlemler, dokümanlar, planlar, dokümante edilmiş düşünceler, veriler veya bilgilerdir.

- Bu bir bilgisayar, sunucu veya bir ağ cihazı olabileceği gibi kişisel, kurumsal veya ulusal veriler de olabilir. İnternete bağlı televizyon, cihaz, sistem veya araç olabileceği gibi veri tabanı, veri merkezi, veri kayıt sistemi veya kullanılan yazılımlar, donanımlar ve süreçler siber ortamdaki varlıklardır.

https://altitudebranding.com/use-digital-asset-management-protect-brand/cyber-assets-75267713_s/

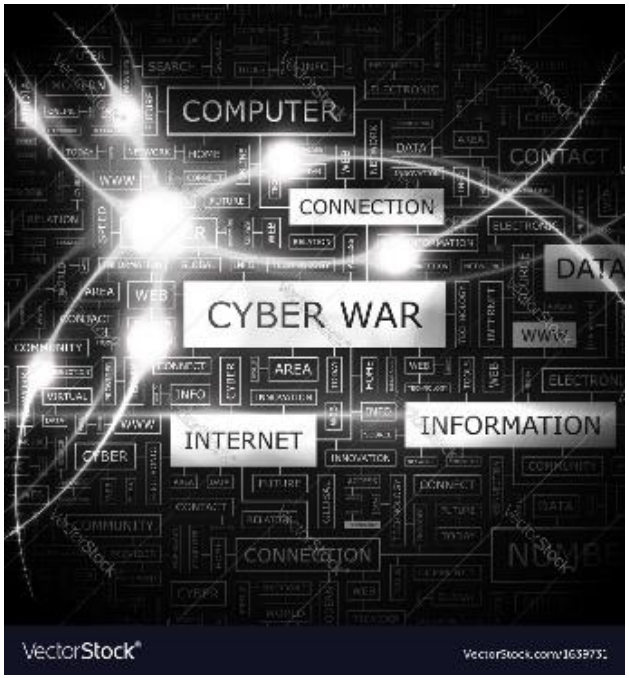
Tanımlar

- **Siber olay,** siber varlıkların bir şekilde etkilendiği, zarar gördüğü, ihlal edildiği veya çeşitli şekilde oluşan ve üzerinde işlem yapılan durumdur. Elektronik ortamlarda, işlenen verilerin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi, verilere zarar verilmesi, verilerin ele geçirilmesi veya buna teşebbüs edilmesi gibi konular buna verilebilecek örneklerdir. Bir siber saldırı sonucu elektriklerin kesilmesi, haberleşme sistemlerinde oluşan bir ihlal veya buna benzer bir durum, "siber olay" olarak ifade edilmektedir. ABD'de bir güvenlik enstitüsü bir siber olayı, "**sistematik yapılar veya fonksiyonlar üzerinde etkiye sahip değişikler**" olarak tanımlanmaktadır.

Tanımlar

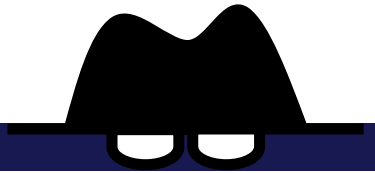
- **Siber savaş,** sahip olunan siber varlıkların; ulusal çıkarlar ve menfaatler çerçevesinde korumak için karşı tarafın bilişim sistemlerine zarar vermek, hizmetlerini durdurmak veya bozmak için bir başka ülkenin BT sistemlerini yavaşlatmak, bozmak, hizmetini aksatmak veya ele geçirmek amacıyla yapılan saldırılardır.

https://www.vectorstock.com/royalty-free-vector/cyber-war-vector-1639731



Tanımlar

- **Siber casusluk,** çoğunlukla elektronik ortamları kullanarak yapılan casusluğa verilen isimdir. Ülkelerin sahip olduğu internet, bilgisayar, cihaz, yazılım veya bunların bağlı olduğu ve hizmet verdiği ağlar ve sistemler üzerinde bulunan bilgi varlıklarının; elektronik ortamda oluşan açıklıklar, bulunan zafiyetler, sahip olunan tehditler, yapılan saldırılar, bilerek bırakılan açık kapılar ve kullanılan yazılım ve donanımlar üzerinden bilgi varlıklarını belirli bir çıkar için ele geçirme, bilgi sızdırma, amaca uygun faaliyetler yürütmekdir.



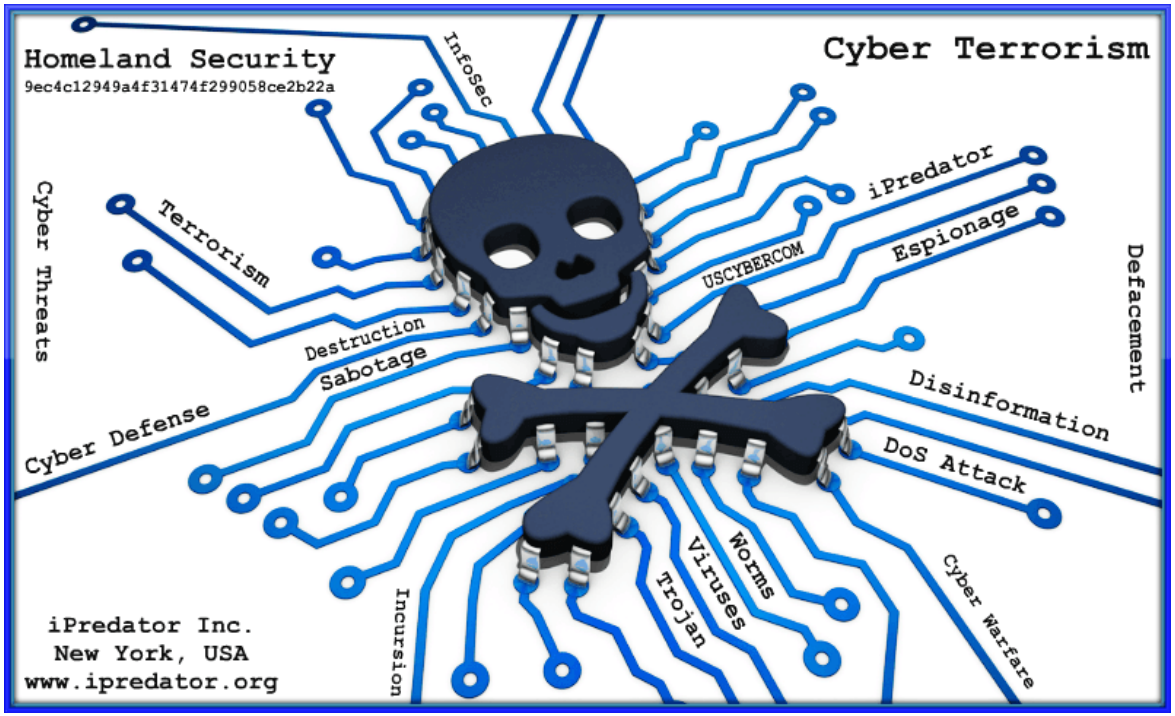
Tanımlar

- **Siber silah,** elektronik ortamda saldırı ve savunma amaçlı olarak kullanılabilecek her türlü araçtır. *"Kötücül amaçlı yazılım veya kod parçaları"* olarak ifade edilmektedir. NATO'ya göre siber silah, *"saldırı yeteneğine sahip olan ve karşıya zarar veren yazılım veya kod parçasıdır"*.

https://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/

Tanımlar

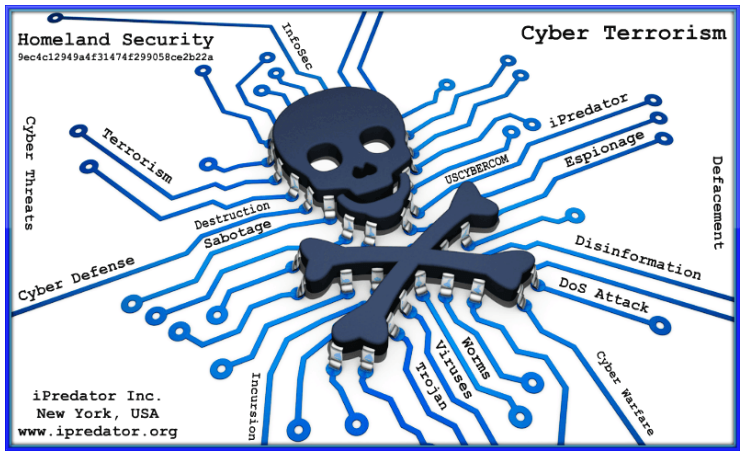
- **Siber terör, terörizm** ve **terörist,** Siber Terörle Mücadele: Tehditler ve Önlemler Ulusal Konferansı Sonuç Bildirgesinde (www.siberteror.org), siber terör ve terörizmle ilgili olarak terimlerin ve kavramların tekrar tartışılmasına ve tanımlanmasına katkı sağlamıştır.



https://www.ipredator.co/cyber-terrorism/

Tanımlar

- **Siber Terörizm**, *"terör örgütlerinin faaliyetlerinde siber ortamın sunduğu kolaylıkları, uygulamaları, araçları, altyapıları, teknik ve teknolojileri, boşlukları, zararlı yazılım ve içerikleri bulup kullanarak, tuzak kurarak veya yeni yöntemler geliştirerek hedefi doğrultusunda kişileri, toplumları veya ulusları yönlendirme, yıldırma, bezdirme, sindirme, zarar verme ve çıkar elde etme amacıyla yapılan faaliyetler"* şeklinde tanımlanmıştır.

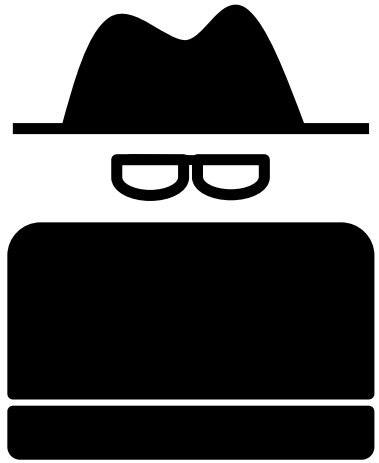


Tanımlar

- **Siber Terör**, *"siber ortamda bulunan her türlü hizmeti, açıklığı, altyapıyı, uygulamayı, zararlı yazılımları ve/veya içerikleri, her türlü boşluğu veya fırsatı kullanarak kişileri, toplumları, kurumları veya ulusları yönlendirme, yıldırma, bezdirme, sindirme veya zarar verme amacıyla doğrudan veya dolaylı olarak yapılan faaliyet"* olarak tanımlanmıştır.

Tanımlar

- **Siber Terörist**, *"siber ortamda bulunan her türlü hizmeti, açıklığı, altyapıyı, uygulamayı, zararlı yazılımları, boşluğu veya fırsatı kullanarak hedefi doğrultusunda kişileri, toplumları, kurumları veya ulusları doğrudan veya dolaylı olarak amacı doğrultusunda yönlendiren, yıldıran, bezdiren, sindiren veya zarar veren, çıkar elde eden, bu tür faaliyetlere yardım yapan veya destek veren kişi"* olarak tanımlanmıştır.



Tanımlar

- **Siber caydırıcılık,** *"sanal ortamlarda karşılaşılabilecek tehdit ve tehlikelere maruz kalmamak için saldırganlığı önleme, engelleme ve önlem alma girişimleri"* olarak ifade edilebilir. Diğer bir ifade ile *"saldırıları veya saldırganları amacından vazgeçirmek", "korkutarak cesaret kırmak ve vazgeçirmek için temel üstünlüklere sahip olma girişimlerinin tümü"* olarak ta tanımlanabilir.

https://siberbulten.com/makale-analiz/geleneksel-caydiricilik-kavramlarinin-siber-alanda-uygulanabilirligi-uzerine-bir-inceleme/

Tanımlar

- **Siber güvenlik,** *"siber ortamlarda karşılaşılabilecek tehdit ve tehlikeler ile oluşabilecek riskleri önceden öngörüp bunlara karşı önceden önlem alma girişimi", "siber varlıkların tehdit ve tehlikelerden korunması için doğru teknolojiler, yöntemler, çözümler, önlemler, politikalar, standartlar, testler gibi girişimlerin doğru amaç, hedef veya* şekilde kullanılarak *siber varlıkların veya sistemlerin istenilmeyen kişiler/sistemler tarafından elde edilmesini önleme girişimi"* veya *"siber ortamlarda oluşacak riskleri minimize etmek ve yönetmek"* olarak ta tanımlanabilir.

https://reciprocity.com/resources/what-is-cybersecurity/

Tanımlar

- **Bilgi güvenliği,** *"bilginin bir varlık olarak tehditlerden veya tehlikelerden korunması için doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak, bilgi varlıklarının her türlü ortamda istenmeyen kişiler tarafından elde edilmesini önleme girişimi"* olarak tanımlanır. Diğer bir ifadeyle, *"kişi ve kurumların BT kullanırken karşılaşabilecekleri tehdit ve tehlikelerin daha önceden analizlerinin yapılarak gerekli önlemlerin önceden alınmasını sağlama"* işlemleridir. Kısaca, "öneme sahip veya değerli bilginin korunmasına yönelik çabaların tümü" olarak tanımlanabilir.

Tanımlar

- **Parola/Şifre,** bilgisayarlar ve bilgisayar sistemlere erişim güvenliğini sağlamak için kullanılan karakter dizileridir.

- Fransızca chiffre (şifre) ve parole (parola) sözcüklerinden Türkçemize geçmiştir.

- İngilizce sözlüklere bakıldığında ise hem şifre hem de parola anlamına gelen "password" kelimesi karşılığı olarak ifade edilmektedir. Çevirisi yapıldığında "geçiş veya erişim kelimesi" olarak ifade edilebilir. **Şifreler**, geri dönüştürülebilir veya dönüştürülemez metinlerden oluşur, aksi gerekmediği sürece ASCII karakterleri şeklinde olurlar. **Parola** ise, herhangi bir okunabilir, seçilmiş ve gizli tutulması gereken kelimedir.

Tanımlar

- **Reklam yazılımı (adware),** BT kullanıcı alışkanlıklarını izleyerek bunları merkezi bir noktaya aktaran, kullanıcıyı hedef üye sitelere yönlendirerek o sitelerin yüksek ziyaret oranlarına sahip olmalarını sağlamak gibi korsan işlemleri yerine getiren yazılımdır.

https://blog.getadblock.com/what-is-adware-ce135d866898

Tanımlar

- **Virüs,** işletim sistemleri de dahil olmak üzere kendini bir taşıyıcıya yerleştirerek yayılan kötücül kod parçasıdır. Tek başına çalışamadıkları için, aktif hale gelebilmeleri için taşıyıcı bir programa ihtiyaç vardır.

http://www.batuhankilinc.com/teknoloji/sinir-bozucu-bilgisayar-virusleri.html

Tanımlar

- **Kurtçuk (worm),** taşıyıcı kaynaklarını kullanarak tek başına ve farklı bilgisayarlar üzerinde de çalışabilen ve tam bir kopyasını oluşturabilen programlardır. Zararsız gibi görünürler, bulaştığı program veya bilgisayarın normal çalışmasını bozmadan işlerini veya görevlerini arka planda kullanıcının dikkatinden uzak bir şekilde yaparlar.

https://www.tech-worm.com/worm-solucan-nedir/

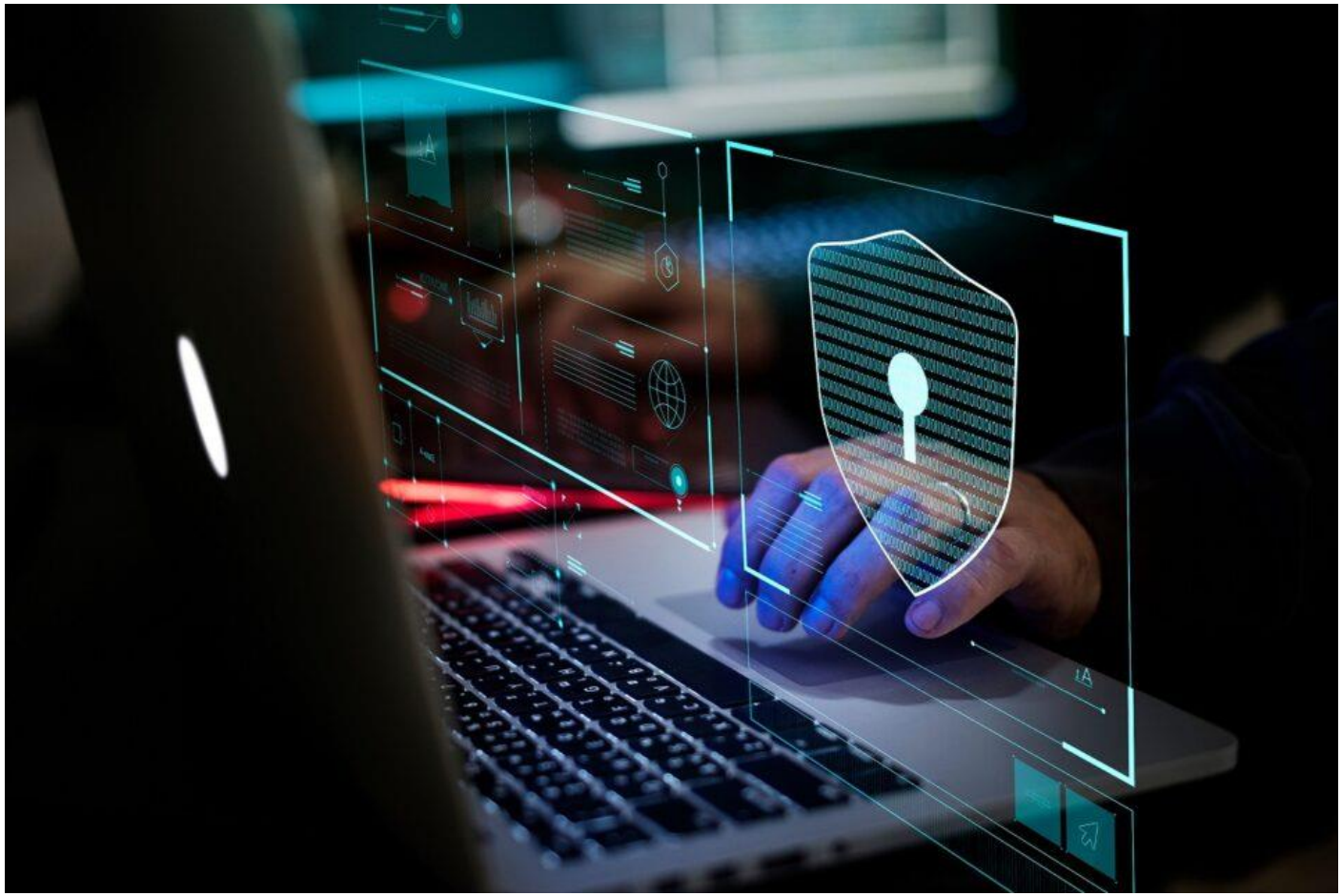
Tanımlar

- **Casus yazılım,** casusluk faaliyetlerini yapmak üzere geliştirilen kötücül amaçlı yazılımlardır. Bunlar, sadece bir fonksiyonu yerine getirmenin yanında tüm bilgisayar etkinliklerini takip edebilirler, saklayabilirler, raporlayabilirler, eposta ile 3. taraflara gönderebilirler veya sms atabilirler, ftp'ler ile topluca gönderebilirler, vb. pekçok işlemi yapabilirler.

https://www.cinarwbh.com/genel/casus-yazilim-nedir-ve-nasil-temizlenir/

Tanımlar

- **Saldırı,** en basit tanımlama ile siber ortamların **za**fiyete uğratılması veya suistimal edilmesi için yapılan girişimlerdir.



https://www.bthaber.com/en-cok-siber-saldiriya-ugrayan-ulkelerden-biri-de-turkiye/

Tanımlar

- **APT (Advanced Persistent Threat),** "gelişmiş sürekli tehdit", "hedef odaklı saldırı", "ileri düzey sürekli tehdit", "ileri düzey kalıcı tehdit", "ileri düzey saldırı" veya "ileri düzey tehdit" olarak literatürde bilinmekte ve bu isimler altında tanımlanmaktadır. Tanımlamalardan da anlaşılacağı üzere; ileri düzey, özel ve kapsamlı saldırıları içerisinde barındıran bir saldırıya verilen isimdir.

- Bu saldırı türüne bakıldığında; içerisinde sıfır gün saldırıları bulunan, işletim sistemi ve mimarilerinin zafiyetlerini kullanan, sinsice saklanan ve geleneksel metotlar ile bulunamayan, içerisinde casus yazılımlar olabilen, anti viral yazılımların tespit etmesinin mümkün değildir.

Tanımlar

- **APT (Advanced Persistent Threat)**

- Bu saldırılara en iyi örnek Stuxnet olarak verilebilir. Buna ilave olarak; Flame, DuQu, Wiper, Aurora, Nitro, ShadyRAT, Lurid, Night Dragon verilebilecek diğer örneklerdir. Bugün için 100'e yakın bu saldırı türüne örnek saldırılar bulunmaktadır.

https://www.csoonline.com/article/2615666/5-signs-youve-been-hit-with-an-apt.html

Tanımlar

- **Güvenlik modelleri;** siber güvenlikte farklı amaçlar için kullanılmaktadır. Bunlar, şifrelemelerde kullanılan teknikler veya algoritmalar olabileceği gibi protokoller, Bell-LaPadula, Harrison-Ruzzo-Ullman, Çin Duvarı, Biba, Clark-Wilson vb. güvenlik modelleri olabilir.

Tanımlar

- **Fidye yazılımı (ransomware),** son dönemde gündemde olan en önemli zararlı yazılım türü olup, oldukça geniş kitleleri etkilemiştir. Bu yaklaşım içerisinde; büyük oranda oltalama veya sazan avlama gibi zararlı yazılımlar barındıran web siteleri aracılığı ile dağıtılırlar. BT sistemlerine ise gönderilen bir e-posta ekine sıkıştırılmış (ZIP) bir dosya, PDF veya Word dokümanı olarak sistemlere bulaştırılırlar. Bu sistemin çalışma mekanizması incelendiğinde; BT sistemine giriş yapılması ile başladığı, bu erişim ile bir şifreleme yaklaşımı kullanılarak girilen veya erişilen sistemde bulunan dokümanlar şifrelenir. Şifreli doküman veya verilerin tekrar deşifre edilmesi için, fidyeci, kullanıcıya bir e-posta gönderir veya irtibat kurar. Gönderilen e-postada durumdan kullanıcı haberdar edilir. Bu durumdan kurtulmak için belirlenen tutardaki fidyeyi belirtilen hesaba, verilen zaman kısıtı içerisinde transfer edilmesi istenilir. Transfer teyidi yapıldığında ise fidyeci, şifreli dokümanı açmak için ihtiyaç duyulacak parolayı, ilgili kullanıcıya gönderir ve veriler deşifre edilir. Fidyecilerin kullandığı yöntem burada çok basit olarak veya en basit haliyle anlatılmıştır. Bunların farklı versiyonlarıda bulunmaktadır. WannaCry, Petya buna verilebilecek güncel örneklerdir.

Tanımlar

- **Sızma (penetration) testi,** BT sisteminin mevcut durumunu analiz etmek, varsa üzerinde barındırdığı zafiyetleri, tehditleri, açıklıkları veya zayıflıkları tespit etmek için yapılan ve son dönemlerde ise yapılması rutin haline gelen güvenlik testlerini içeren yaklaşımlarını ifade eder. Diğer bir ifade ile saldırganların sistem zafiyetlerini ve açıkıklarını öğrenmeden, BT sistemine sahip olan kişi veya kurumların, sahip oldukları bilgi varlıklarının ne kadar güvende olduğunu öğrenmeleri ve alınması gereken önlemleri önceden tespit etmek için yapılan testlere verilen isimdir. Son dönemde, kamu kurumlarının bu testleri yaptırmaya başlamaları, ulusal strateji ve eylem planı kapsamında bunun zorunlu hale getirilmesinin amacı ise güvenlik politikalarına ve standartlara uyumluluğu test etmek, varsa zafiyet ve açıklıkları belirlemek ve önceden gidermek, riskleri ve maliyetleri düşürmek, sistem performansını ve verimliliğini değerlendirmek, gelecekte karşılaşılabilecek olası saldırı, sızma ve istismar girişimlerini belirlemek ve önlemek, ve gelecek planları yaparak güvenliği daha etkin sağlamaktır.

Tanımlar

- **Zafiyet,** bir yazılım, donanım, sistem, süreç, tasarım ve üretim aşamalarında kaynaklanan algoritmik, mantık, tasarım, bakım veya test aşamalarında yapılan hatalardan kaynaklanabilecek ve istismara açık olan hususlara verilen addır. Zafiyetlerin, donanım, yazılım, tasarım ve işletimden kaynaklı olabileceği gibi insan faktöründen de kaynaklanabileceği de her zaman hatırda bulundurulmalıdır.

- **Güvenlik Açığı (Vulnerability)**
- Bir tehdit kaynağı tarafından istismar edilebilecek veya tetiklenebilecek bir bilgi sistemi, sistem güvenlik prosedürleri, iç kontroller veya uygulamadaki zayıflık.

Tanımlar

- **Truva atı,** Bir casus yazılım türüdür. Genellikle başka bir dosyanın içerisinde saklanarak sisteme sızan ve sistemi ele geçiren bir saldırı türüdür. Mesela, bir resim olduğu düşünülen bir dosyaya tıklandığında, Truva atı yazılımı da devreye girmekte ve hedeflenen görevi yerine getirmektedir.

https://www.verigom.com/blog/trojan-nedir-trojan-virusu-nasil-temizlenir/

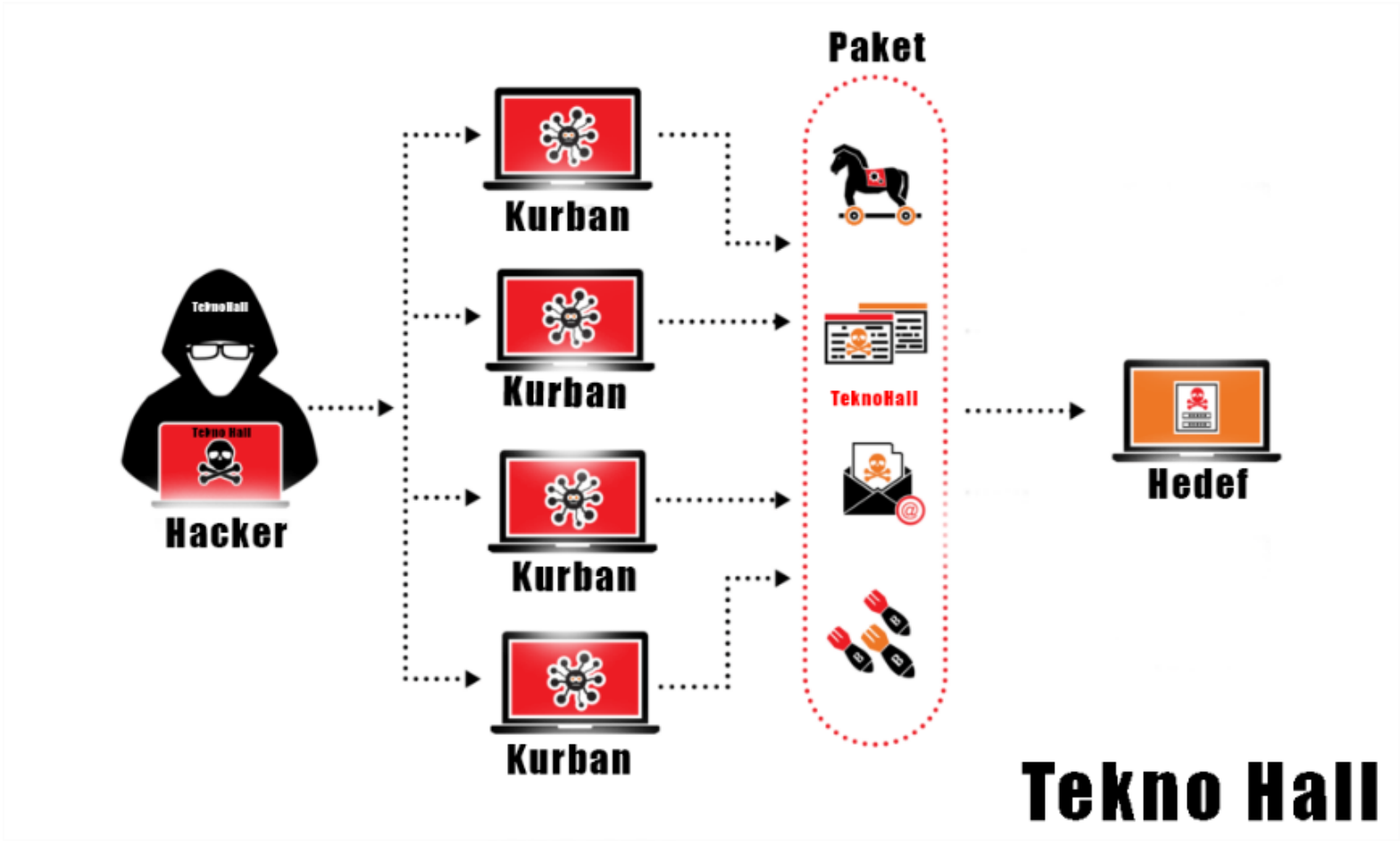
Tanımlar

- **Dağıtık Hizmet Engelleme (DoS, DDoS) saldırısı,** belirli bir internet sitesini erişilmez veya hizmet veremez hale getirme işlemidir. Bu saldırıda köle bilgisayarlar (botnetler (zombi ağı)) kullanılarak, sahip olunan çok sayıda köle bilgisayarın veya sistemin aynı anda hedeflenen bir hizmet için talep yoğunluğu oluşturarak, sistem erişilemez hale getirilir.

- Bu tür saldırılar, bir şirketin web sitesini sağlayan altyapı gibi, herhangi bir ağ kaynağı için geçerli olan belirli kapasite sınırlarından faydalanır. DDoS saldırısı, saldırıya uğrayan web kaynağına birden çok istek göndererek web sitesinin çok sayıda isteği işleme kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlar.

Tanımlar

- **Dağıtık Hizmet Engelleme (DoS, DDoS) saldırısı**



Tanımlar

- **Oltalama, Yemleme veya Sazan Avlama saldırısı (phishing),** günümüzde yapılan saldırılar doğrudan veya dolaylı olarak yapılmaktadır. Bu saldırının temel amacı; kullanıcıyı bir şekilde kandırarak bilgilerini, parolasını, kredi kart numarasını veya bunları alabileceği dolaylı bilgileri bir şekilde elde etmektir.

https://www.teknorun.net/worm-solucan-nedir/

Tanımlar

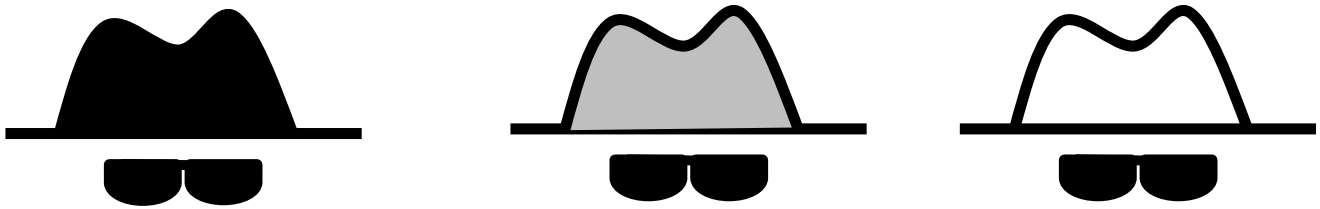
- **Oltalama, Yemleme veya Sazan Avlama saldırısı (phishing),**. Oltalama saldırısı, kullanıcıyı başka bir şey oluyormuş gibi kandıran ve sonuçta saldırganın belirlediği gizli amaca ulaşmada kullandığı bir saldırı türüdür. Mesela; kullanıcıya kendisini bir banka, bir kurum, bir şirket veya bir sosyal medya hesabından gelen bir e posta gibi göstererek; kredi kartı ekstresini tıklatma, parola yenileme mesajı gibi gösterme ve kişisel verileri elde etme, bir dokümanı indirmeni isteyerek bir kötücül yazılım indirtme, önemli bir hususu öne çıkararak bir linke tıklatma şeklinde gösterebilmektedir.

https://listelist.com/phishing-saldirisi-nedir/

Tanımlar

https://www.cisco.com/c/en/us/products/security/what-is-a-hacker.html#~how-hacking-works

- **Bilgisayar korsanı (Hacker),** günümüzde sistemlerin yapısını, çatısını veya işleyişini ihlal eden, zafiyetleri kullanarak çıkar elde eden, amacı veya işlevi dışında sistemleri kullanan, kullanıma açan veya zarar veren, genellikle yıkıcı, kötü amaçlı bilgisayar kullanıcılarına verilen isimdir



Cybercriminals

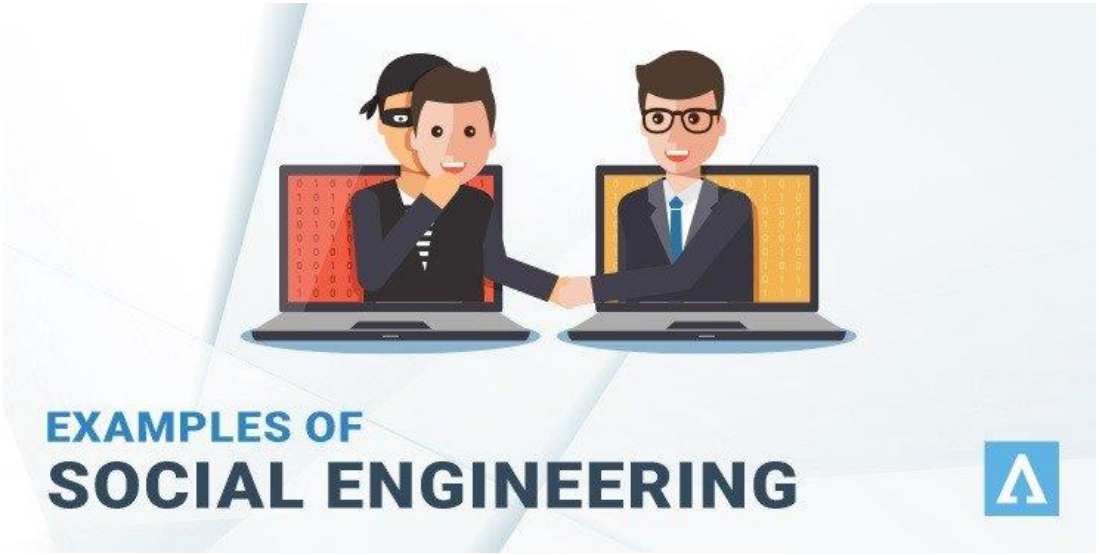
Ethical hackers

Hacktivists

Script kiddies

Tanımlar

- **Sosyal mühendislik ve saldırıları;** günümüzde bilinen dört önemli saldırı türünden birisidir. Bu saldırıların temel amacı; sistemlerin, bilgisayarların veya ağların suistimal edilmesi yerine, insanları yani kurbanları kandırmaya, duyguları istismar etmeye, zafiyetleri veya zayıflıkları kullanmaya dayanmaktadır. Bu saldırganlar; kurbanlarını başka birisi olduklarına ikna edenler, yakınlık kurarak sırlarını alanlar, güvenlik uzmanı olarak sistemlerini koruyacaklarını söyleyenler, kendilerini yardımsever olarak gösterenler, kişilere beklemedikleri samimiyeti ve desteği sunanlar, kişilerin zafiyetlerini iyi anlayanlar, bunlara verilebilecek örneklerden bir kaçıdır.



https://terranovasecurity.com/examples-of-social-engineering-attacks/

Tanımlar

- **Sıfırıncı gün saldırıları (Zero-day Attack):**

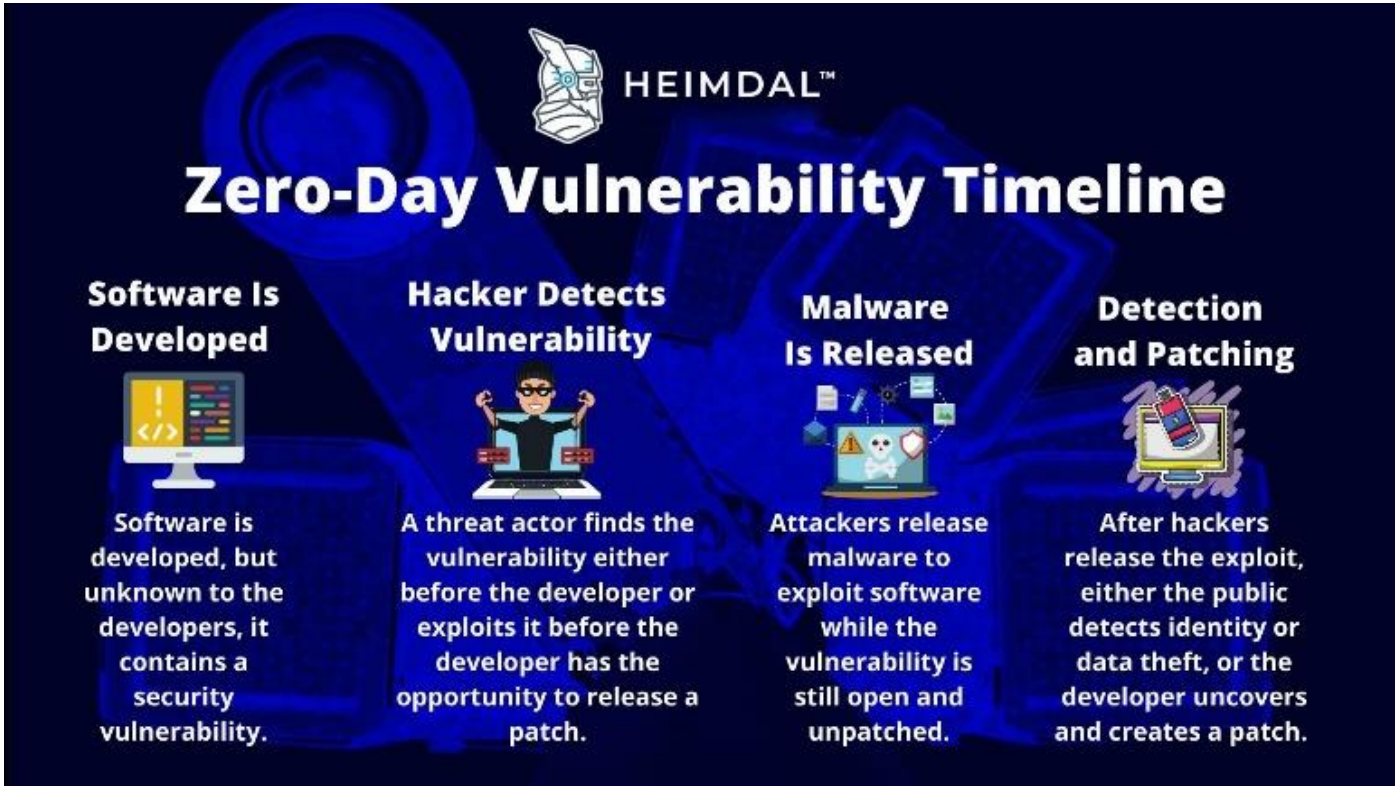
- "Sıfır gün", bilgisayar korsanlarının sistemlere saldırmak için kullanabileceği yakın zamanda keşfedilen güvenlik açıklarını tanımlayan geniş bir terimdir. "Sıfır gün" terimi, satıcının veya geliştiricinin kusuru henüz yeni öğrendiği gerçeğine atıfta bulunur - bu, düzeltmek için "sıfır günleri" olduğu anlamına gelir. Bilgisayar korsanları, geliştiricilerin sorunu çözme şansı bulamadan önce kusurdan yararlandığında sıfır gün saldırısı gerçekleşir.

Örnekleri ve detayları incelemek için Okuma Önerisi!!!!!

https://www.kaspersky.com.tr/resource-center/definitions/zero-day-exploit

Tanımlar

- **Sıfırıncı gün saldırıları (Zero-day Attack):**



https://heimdalsecurity.com/blog/zero-day-attack-exploit-vulnerability/

Tanımlar

- **Kayıtediciler (activity monitoring system);** sistem etkinliklerini takip etmek için geliştirilmiş yazılımlardır. Bir zararlı yazılıma dönüştürülebilirler. Hedef sisteme bağlı giriş ve çıkış cihazlarını (klavye, fare, monitör, yazıcı) takip ederler ve her hareketi kaydederek, sisteme izinsiz erişen kişi veya kişilere iletirler. Bu sayede, yazılan her şey karşı tarafa (3. tarafa) gittiği için kullanıcı adı ve parolalar, kredi kartı bilgileri ya da özel yazışmalar, 3. tarafların eline geçer.

Tanımlar

- **Yığın e-posta (spam mail);** istenmeyen e-postalara verilen isimdir. Genelde yasa dışı (ilaç, fidye, reklam, pornografik içerik içeren site vb.) ürünlerin reklamı yapmak için kullanılır. Son zamanlarda kimlik hırsızlığı sebebiyle oltalama saldırıları yapılmaktadır.

https://www.hosting.com.tr/blog/spam-mail-nedir-nasil-engellenir/

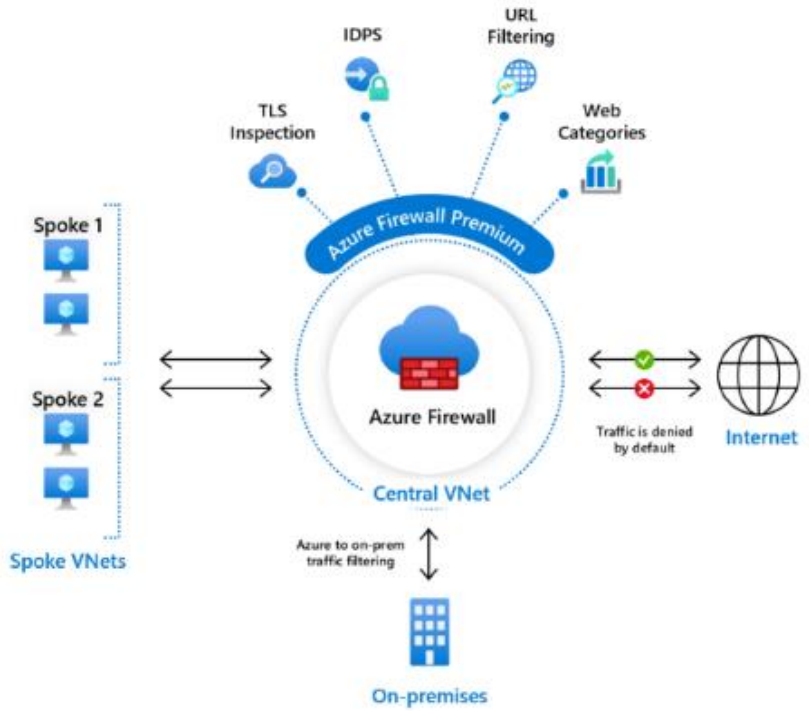
Tanımlar

- **Anti-virüs;** üzerinde işletim sistemi bulunan her bilgisayar veya telefon başta olmak üzere işletim sistemi olan neredeyse her sistemde kullanılabilen bir güvenlik çözümüdür. Bu yazılımlar, virüsleri ve zararlı yazılımları, imza adı verilen küçük kod parçalarına bakarak tanır ve bunlara karşı sistemin zarar görmesini önler

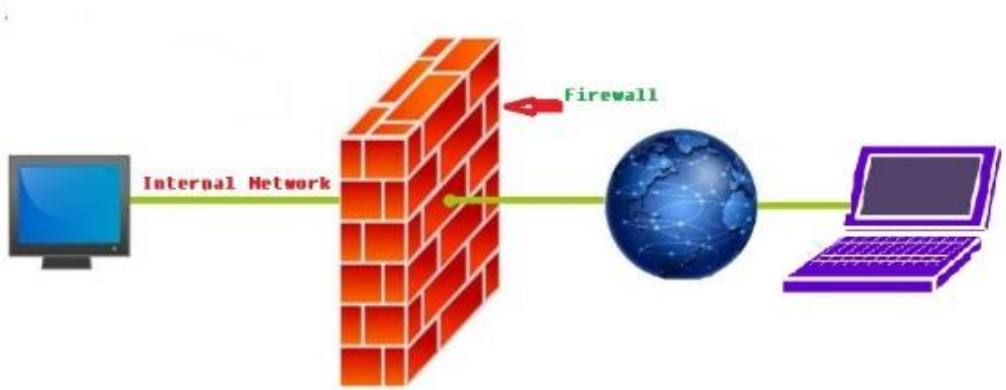
https://smartpro.com.tr/ucretsiz-olarak-kullanabileceginiz-antivirus-programlari/

Tanımlar

- **Güvenlik duvarı,** bir ağ içerisinde izin verilmeyen içten veya dıştan gelebilecek istekleri veya işlemleri, belirlenen kurallar çerçevesinden önleyen veya bloklayan, sistemleri kendi dışındaki işlemlerden korumak üzere kullanılan yazılım, donanım ya da her ikisinin birleşiminden oluşan çözümleri içeren güvenlik sistemidir.



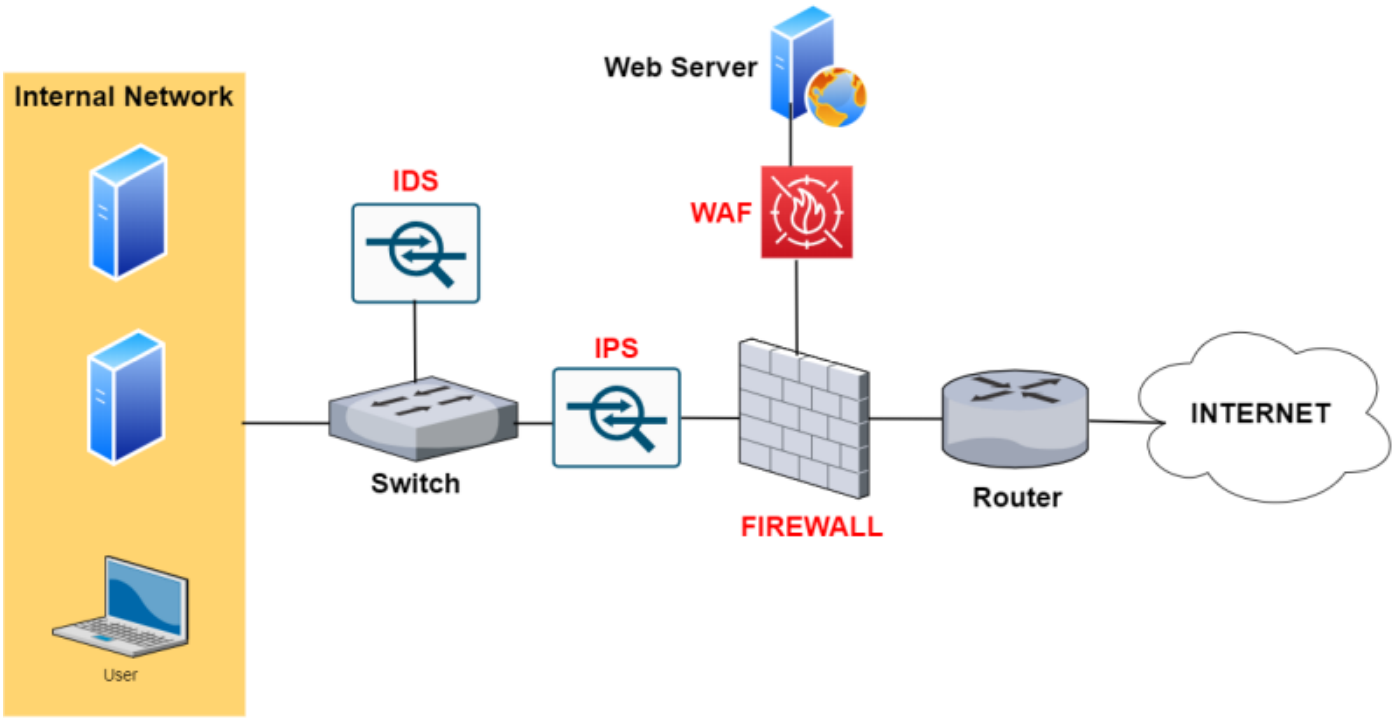
https://docs.microsoft.com/tr-tr/azure/firewall/premium-features



https://www.hosting.com.tr/blog/firewall-nedir/

Tanımlar

- **Saldırı tespit/Koruma sistemi (IDS/IPS);** bir bilgisayar, sunucu veya ağ sistemine yapılan saldırıları, izinsiz erişimleri veya sızmaları tespit ederek, bunu bir uyarıya (alert) dönüştüren ve sistemleri saldırılardan koruyan sistemlerdir.



https://forum.huawei.com/enterprise/en/comparison-and-differences-between-ips-vs-ids-vs-firewall-vs-waf/thread/763619-867

Tanımlar

- **İki adımlı kimlik doğrulama;** adından da anlaşılabileceği gibi kimlik doğrulama işlemini iki basamakta tamamlama işlemlerini kapsar. Bu doğrulama, kullanıcıların parola yanında ikinci bir erişim kontrol adımını sisteme ekleyerek, kullanıcının farklı bir şekilde sisteme giriş yapmasını sağlar. Örneğin, internet bankacılığında telefonlara gelen bir SMS, buna örnek verilebilir.

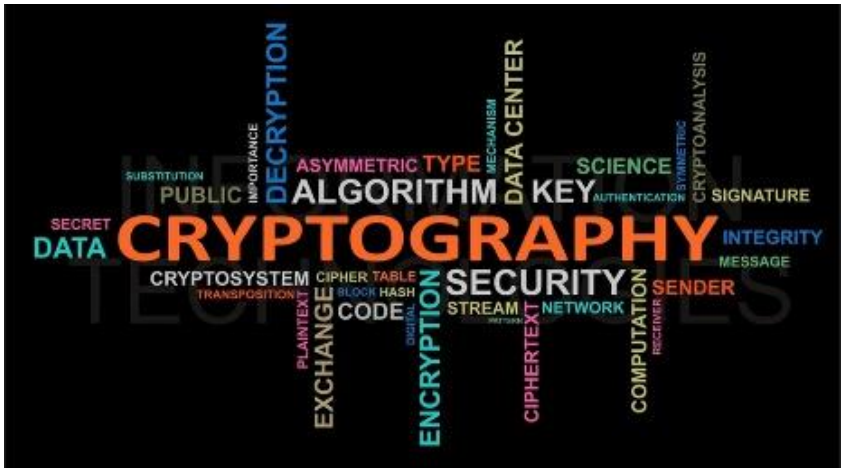
https://www.imperva.com/learn/wp-content/uploads/sites/13/2019/01/2fa-example.jpg

Tanımlar

- **Şifrebilim veya Şifreleme Bilimi (Kriptoloji);** veri, bilgi veya özbilginin şifrelenmesi, saklanması veya istenilmeyen kişilerin anlamasını zorlaştırma veya şifrelenmiş veri, bilgi veya özbilgilerin çözülmesi üzerine *çalışılan bilim dalıdır.*

- **Kriptografi**, geleneksel olarak, bilginin anlaşılabilir (normal olan) bir formdan/formattan anlaşılamaz bir forma/formata (okunamaz veya anlaşılamaz) hale dönüştürme yöntemlerini içermektedir.

Kriptoanaliz, kriptografik sistem mekanizmalarını ve yaklaşımlarını inceleme ve çözme bilimidir.



https://www.electronicdesign.com/technologies/embedded-revolution/article/21132412/maxim-integrated-cryptographic-implementations-hardware-vs-software

Tanımlar

Şifreleme algoritması; şifreleme ve şifre çözme işlemlerinde kullanılan algoritmaya verilen isimdir. Genel olarak değerlendirildiğinde şifreleme yaklaşımları, gizli anahtarlı ve açık anahtarlı olmak üzere ikiye ayrılır.

- Simetrik yaklaşım olarakta bilinen gizli anahtarlı yaklaşımda, şifreleme ve şifre çözme için tek bir anahtar kullanılır. En popüler gizli anahtarlı şifreleme yaklaşımı veri şifreleme standardı olarak isimlendirilen DES (Data Encryption Standard)'dir.

- Asimetrik olarakta bilinen açık anahtarlı yaklaşımda, kullanıcı bir çift anahtara yani hem açık bir anahtara hem de gizli bir anahtara sahiptir. Bu anahtarlar, özel (private) veya gizli ve genel (public) veya açık olarak ta isimlendirilir. Açık (genel) anahtar herkese açıkken, gizli (özel) anahtar ise sadece kişiye özeldir. Şifreleme açık anahtarla yapılırken, şifre çözme işlemi gizli anahtarla yapılmaktadır. Bunun terside mümkündür. Açık anahtarlı şifreleme yaklaşımlarında en popüler yaklaşım RSA (Rivest, Shamir ve Adleman)'dır.

Tanımlar

Düşman (tehdit ajanı) – Adversary:

Zararlı faaliyetler yürüten veya yürütme niyetinde olan kişi, grup, kuruluş veya hükümet.

Saldırı (Attack):
Bilgi sistemi kaynaklarını veya bilgilerin kendisini toplamaya, bozmaya, reddetmeye, imha etmeye veya yok etmeye çalışan her türlü kötü niyetli faaliyet.

Karşı önlem (Counter measure):
İstenmeyen veya düşmanca faaliyetlerin operasyonel etkinliğini bozmayı veya casusluk, sabotaj, hırsızlık veya hassas bilgi veya bilgi sistemlerine yetkisiz erişimi veya bu sistemlerin kullanımını önlemeyi amaçlayan bir cihaz veya teknik.

Tanımlar

Risk
Bir işletmenin potansiyel bir durum veya olay tarafından ne ölçüde tehdit edildiğinin ölçüsü ve tipik olarak 1) durum veya olay meydana geldiğinde ortaya çıkacak olumsuz etkiler ve 2) gerçekleşme olasılığı.

Güvenlik Politikası (Security Policy)
Güvenlik hizmetlerinin sağlanması için bir dizi kriter. Sistemler ve veriler için bir güvenlik koşulu sağlamak için bir veri işleme tesisinin faaliyetlerini tanımlar ve kısıtlar.

Tehdit (Threat)
Organizasyonel operasyonları (misyon, işlevler, imaj veya itibar dahil), organizasyonel varlıkları, bireyleri, diğer organizasyonları veya ulusu bir bilgi sistemi aracılığıyla yetkisiz erişim, bilginin yok edilmesi, ifşa edilmesi, değiştirilmesi yoluyla olumsuz etkileme potansiyeli olan herhangi bir durum veya olay ve/veya hizmet reddi.

Tanımlar

Ulusal Siber Olaylara Müdahale (USOM), 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı kapsamında, ulusal ve uluslararası koordinasyonun sağlanması için kurulmuştur. USOM, hem ulusal ve uluslararası koordinasyon görevini yürütmekte hem de internet aktörleri, kolluk güçleri, uluslararası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişimi gerçekleştirmektedir. Aynı zamanda, ülkemize karşı yapılan saldırıları yakınen takip etmekte, önlemler almakta ve 2000'e yakın Kurumsal SOME ile bu görevi başarıyla yürütmektedir.

https://www.usom.gov.tr/

Tanımlar

Siber Olaylara Müdahale Ekibi (SOME), ülkemizde USOM ile işbirliği içersinde çalışan, kurum ve kuruluşların sorumluluğunu yürüten birim veya ekibe verilen isimdir. Bir siber saldırının tespit edilmesi, tespitin USOM'a bildirilmesi, USOM'dan gelen uyarıların veya bildirimlerin yerine getirilmesi, giderilmesi için atılması gereken adımları bilen ve bunu yerine getiren yetişmiş uzmanları tanımlar. Ulusal Siber Güvenlik Stratejisi ve Eylem Planında SOME'ler, "kurumlarına doğrudan ya da dolaylı olarak yapılan veya yapılması muhtemel siber saldırılara karşı gerekli önlemleri alma veya aldırma, bu tür olaylara karşı müdahale edebilecek mekanizmayı ve olay kayıt sistemlerini kurma veya kurdurma ve kurumlarının bilgi güvenliğini sağlamaya yönelik çalışmaları yapma veya yaptırmakla yükümlü" ekiplerdir. Ayrıca, ulusal strateji dokümanı kapsamında meydana gelen siber olayların önlenmesi, zararlarının azaltılması, kurum BT sistemlerinin kurulması, işletilmesi veya geliştirilmesi ile ilgili çalışmalarda teknik ve idari tedbirler konusunda da ilgili birimlere öneriler sunabilmektedirler.

Tanımlar

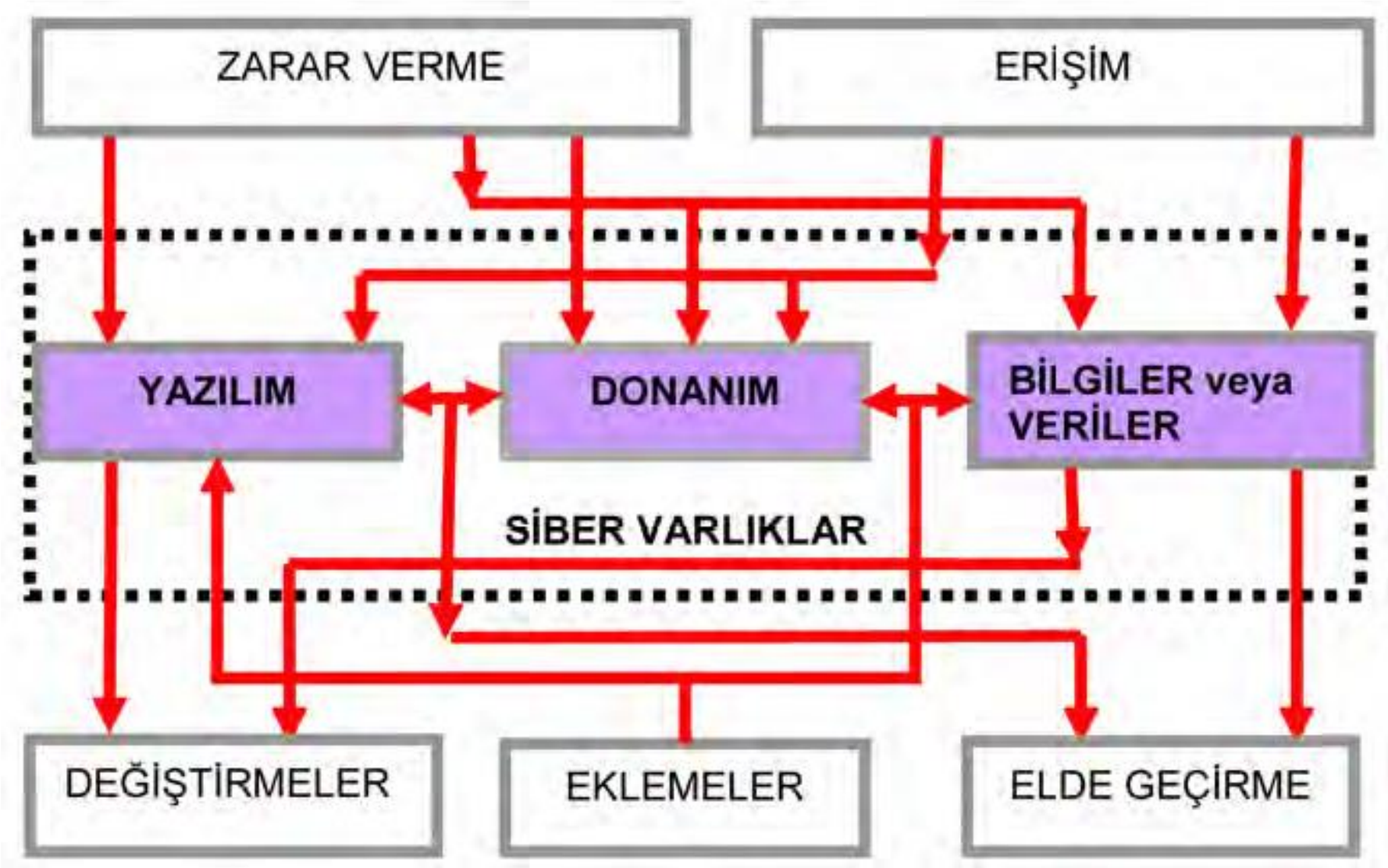

Ulusal Siber Organizasyon Yapısı
https://www.usom.gov.tr/faydali-dokumanlar
KAMU
ÖZEL
USOM
TR-CERT
Kurumsal Some
Sektörel Some
Denetleyici ve Düzenleyici Kurum
Kurumsal Some
Diğer Kurumlar²
Bakanlık
İlgili veya Bağlı Kurum
Özel
www.usom.gov.tr

Tanımlar

https://www.usom.gov.tr/faydali-dokumanlar

Siber Saldırılar ve Türleri

Saldırı Türleri



Karşılaşılabilecek Saldırılar ve Tehditler

APT, casus program sızmaları, açık portları kullanma, TCP/IP korsanlığı, virüsler, casus yazılımlar, kötücül yazılımlar, yığın e-postalar, solucanlar, oltalama veya sazan avlama (phishing), botnetler, sosyal mühendislik saldırıları, yapay zeka saldırı araçları, vb. bunlardan bazılarıdır.

Karşılaşılabilecek Saldırılar ve Tehditler

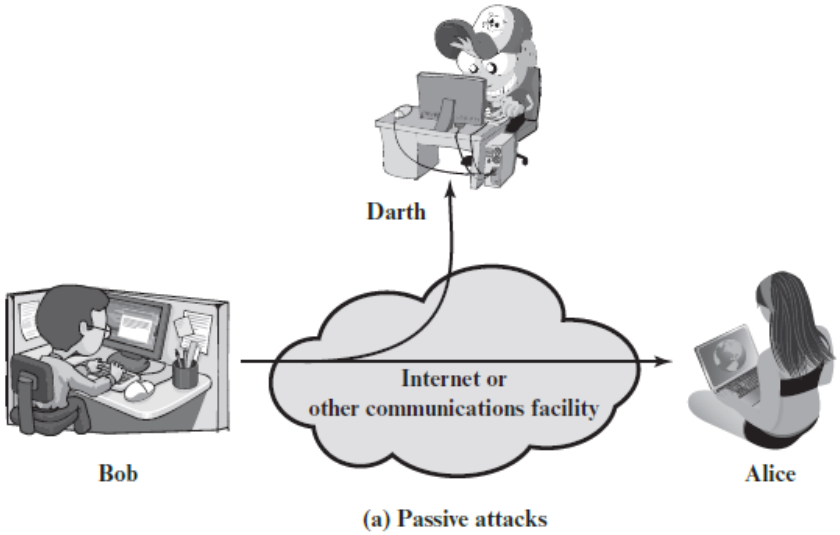
Literatür incelendiğinde; bunların farklı şekillerde **sınıflandırıldığı** bilinmektedir. Bu sınıflandırmalar aktif ve pasif olarak yapılmaktadır. Bunlar;

- **Pasif** : Dinleme
- **Aktif** : Engelleme, değiştirme, üretim

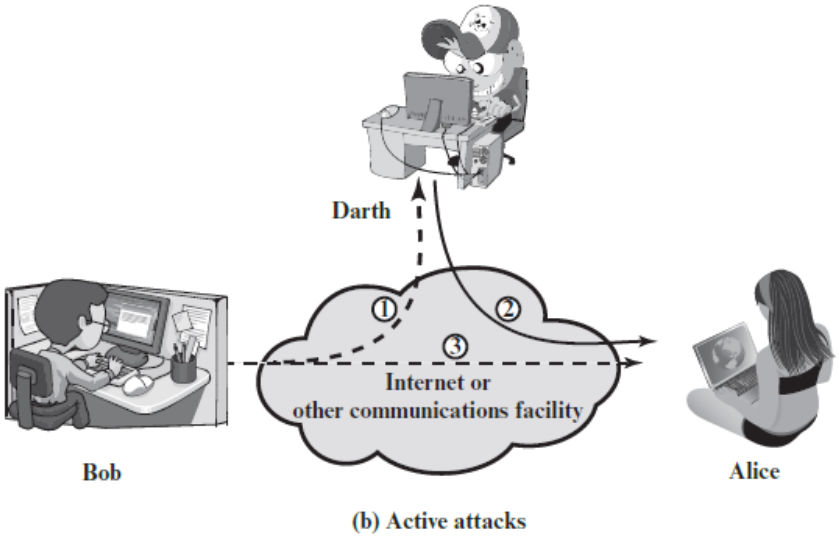
olabileceği gibi
- iç ortamlardan (iç ağdan) veya
- dış ortamlardan (dış ağdan)

yapılan saldırılar olarakta sınıflandırılmaktadır.

Karşılaşılabilecek Saldırılar ve Tehditler



(a) Passive attacks

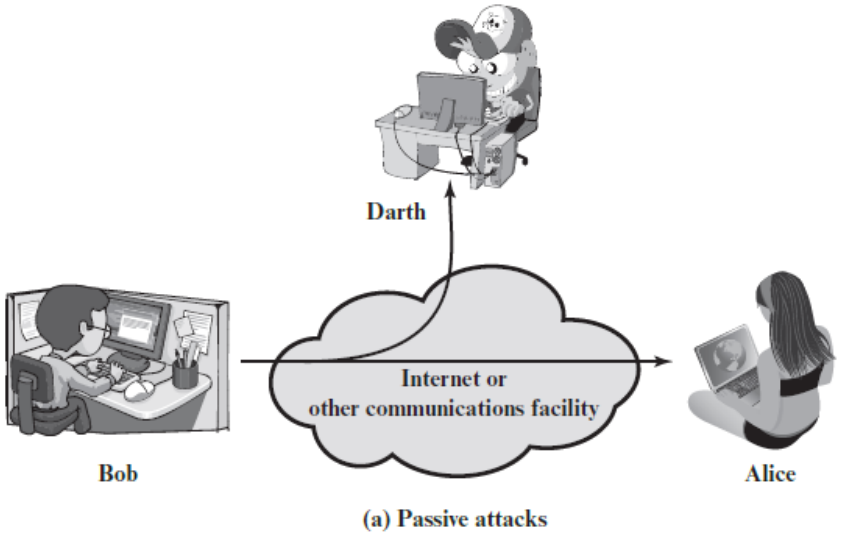


(b) Active attacks

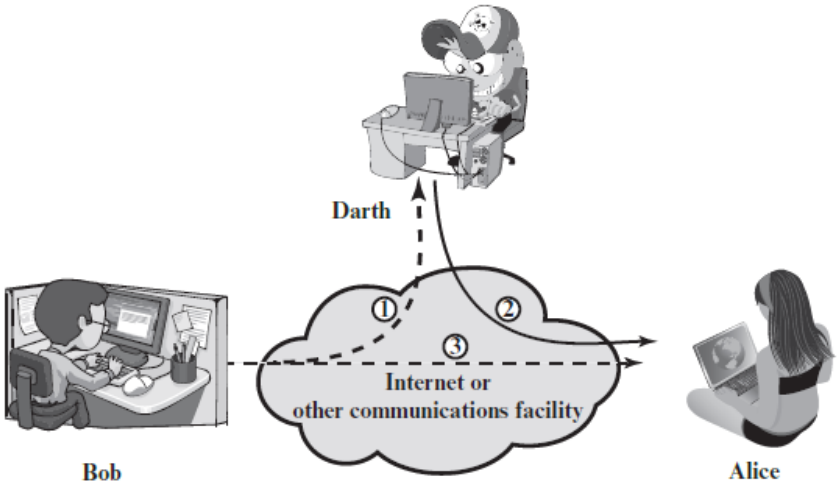
Pasif Ataklar:

Trafik analizi
Mesaj içeriğinin serbestliği

Karşılaşılabilecek Saldırılar ve Tehditler



(a) Passive attacks



(b) Active attacks

Aktif Ataklar:

Bir varlık farklı bir varlık gibi davrandığında bir maskeli balo (**masquerade**) gerçekleşir (Şekil 1.2b'deki yol 2 aktiftir)

Yeniden oynatma (Replay), bir veri biriminin pasif olarak yakalanmasını ve ardından yetkisiz bir etki oluşturmak için yeniden iletilmesini içerir (yol 1, 2 ve 3 aktif).

Mesajların değiştirilmesi basitçe, meşru bir mesajın bir kısmının değiştirilmesi veya mesajların yetkisiz bir etki yaratmak için ertelenmesi veya yeniden sıralanması anlamına gelir (yol 1 ve 2 aktif).

Hizmet reddi (DoS), iletişim olanaklarının normal kullanımını veya yönetimini engeller veya ket vurur (yol 3 aktif).

Karşılaşılabilecek Saldırılar ve Tehditler

Son zamanlarda yapılan saldırılar değerlendirildiğinde, saldırıların;

- otomatik yapılan saldırılar
- manuel olarak yapılan saldırılar ve
- hibrit saldırılar

ve/veya

- zeki saldırılar ve
- zeki olmayan saldırılar

ve/veya

- düşük riskli saldırılar,
- orta riskli saldırılar,
- yüksek riskli saldırılar
- kritik veya riskli saldırılar

Karşılaşılabilecek Saldırılar ve Tehditler

ve/veya

- ileri düzey kalıcı saldırılar (APT)
- geçici olan saldırılar

ve/veya

- kablolu sistemlere yapılan saldırılar
- kablosuz ortamlara yapılan saldırılar

ve/veya

- bilinen yöntemlerle yapılan saldırılar
- bilinmeyen yöntemlerle yapılan saldırılar (sıfır gün saldırıları)

ve/veya kullanılan işletim sistemlerine göre yapılan saldırılar

- Linux
- Unix
- Microsoft
- iOS

Karşılaşılabilecek Saldırılar ve Tehditler

ve/veya kullanılan yaklaşımlara göre yapılan saldırılar

- Kriptografi,
- Steganografi,
- Kuantum

ve/veya

- otomatik araçlar kullanılarak yapılan saldırılar,
- yeni geliştirilen araçlarla yapılan saldırılar

ve/veya

- profesyonel saldırganlar tarafından yapılan saldırılar veya
- uzman olmayanların yaptıkları saldırılar

ve/veya

- delillendirilebilen (cezalandırılan) saldırılar
- delillendirilemeyen (cezalandırılamayan) saldırılar

Karşılaşılabilecek Saldırılar ve Tehditler

ve/veya kullanılan yaklaşımlara göre yapılan saldırılar

- Kriptografi,
- Steganografi,
- Kuantum

ve/veya

- otomatik araçlar kullanılarak yapılan saldırılar,
- yeni geliştirilen araçlarla yapılan saldırılar

ve/veya

- profesyonel saldırganlar tarafından yapılan saldırılar veya
- uzman olmayanların yaptıkları saldırılar

ve/veya

- delillendirilebilen (cezalandırılan) saldırılar
- delillendirilemeyen (cezalandırılamayan) saldırılar

Karşılaşılabilecek Saldırılar ve Tehditler

Bu sınıflandırmaların temelinde dikkate alınan kriterler incelendiğinde ise;

- saldırganlar, hedefler, risk seviyeleri, kullanıcılar,
- bilim dalı, sistemler, ortamlar,
- verilen zararlar, cihazlar, yazılımlar, altyapılar,
- işletim sistemleri, hedef ülkeler ve ortamlar,
- verilen veya alınan hizmetler,
- faydalanılan araçlar, teknikler ve teknolojiler,
- kritiklik seviyeleri, ve
- ihtiyaç duyulan yetenekler

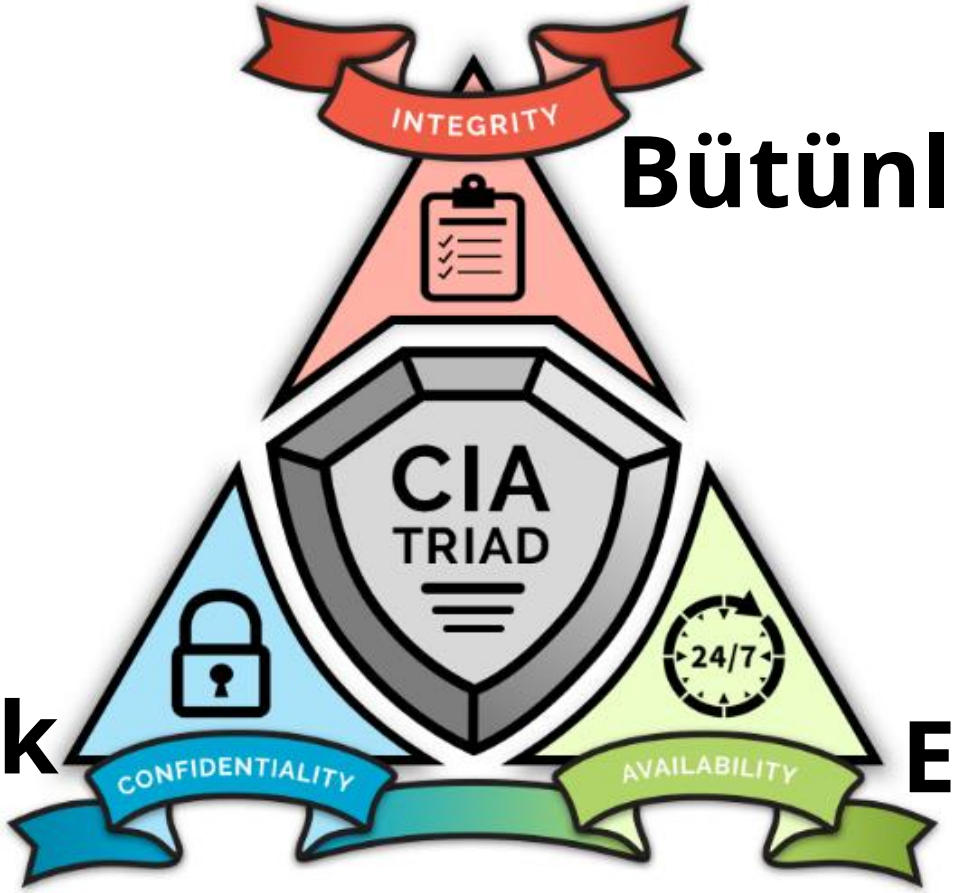
Karşılaşılabilecek Saldırılar ve Tehditler

Genel olarak değerlendirdiğimizde ve literatür incelendiğinde ise bilgisayar sistemlerinde karşılaşılabilecek tehditler;

- sistemlere izinsiz erişim,
- sistemlere ve verilere zarar verme,
- verilerde değişiklik yapma ve
- veri üretimi

olmak üzere dört farklı başlık altında gruplanmıştır.

Siber Güvenlik Prensipleri



Bütünlük

Gizlilik

Erişilebilirlik

https://spanning.com/blog/cia-triad-best-practices-securing-your-org/

Siber Güvenlik Prensipleri

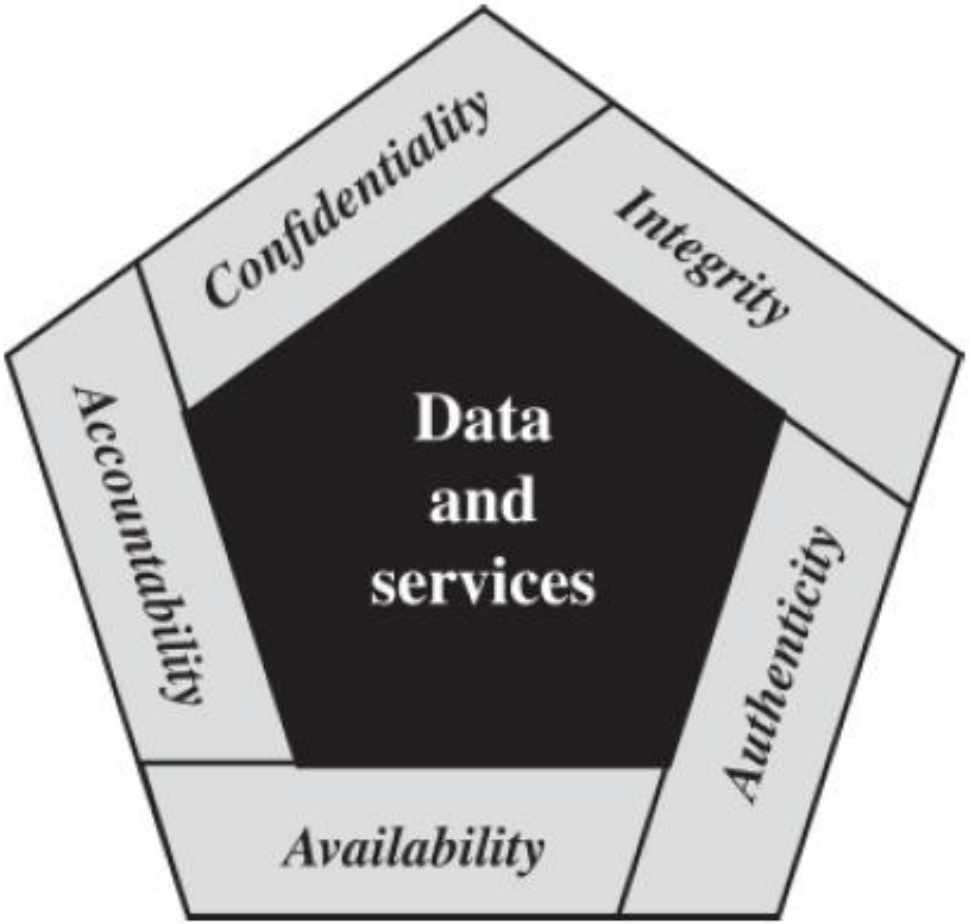
Bilgisayar Güvenliği: Donanım, yazılım, firmware ve işlenen, depolanan ve iletilen bilgiler dahil olmak üzere bilgi sistemi varlıklarının (Assets) gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan önlemler ve kontroller.

Veri gizliliği: (Data confidentialty) Özel veya gizli bilgilerin yetkisiz kişilere verilmemesini veya ifşa edilmemesini sağlar. (Privacy - Gizlilik) Bireylerin kendileriyle ilgili hangi bilgilerin toplanabileceğini ve saklanabileceğini ve bu bilgilerin kim tarafından ve kime açıklanabileceğini kontrol etmelerini veya etkilemelerini sağlar.

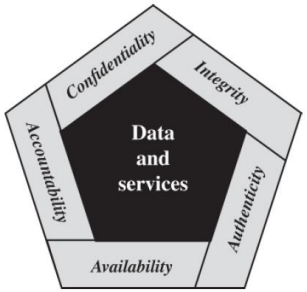
Bütünlük: Bu terim birbiriyle ilişkili iki kavramı kapsar: **Veri bütünlüğü**: Bilgi ve programların yalnızca belirli ve yetkilendirilmiş bir şekilde değiştirilmesini sağlar. **Sistem bütünlüğü**: Bir sistemin amaçlanan işlevini, sistemin kasıtlı veya kasıtsız yetkisiz manipülasyonundan arınmış bir şekilde yerine getirmesini sağlar.

Kullanılabilirlik: Sistemlerin hemen çalışmasını ve sadece yetkili kullanıcılara hizmet verilmesini sağlar.

Siber Güvenlik Unsurları



Siber Güvenlik Unsurları



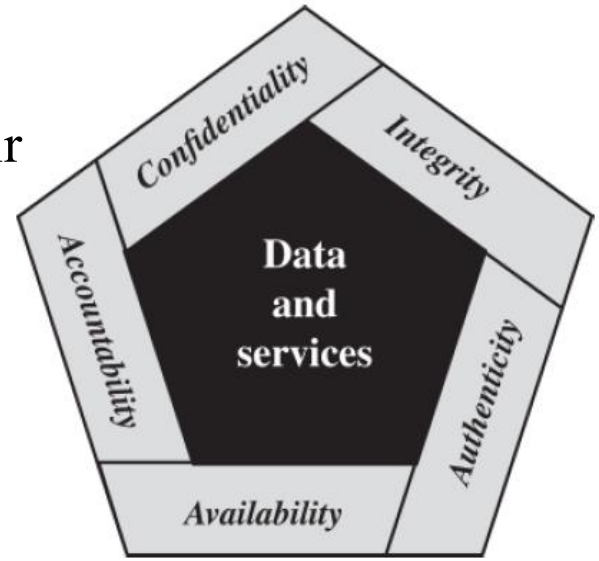
Confidentiality (Gizlilik) , "verilerin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etmektir". Diğer bir ifade ile "verilerin erişim yetkisi olmayan kişilerce elde edilmesini önleme girişimleridir". Bu unsur, şifreleme algoritmaları kullanılarak sağlanmaktadır.

Integrity (Bütünlük), siber güvenlik unsurlarından bir diğeridir. "Verilerin ve işleme yöntemlerinin doğruluğunu ve içeriğin değişmezliğini sağlamak" veya "verinin bir ortamdan diğerine değişmeden gönderildiğini doğrulamak" olarak tanımlanabilir. Özetleme (parmakizi) fonksiyonları kullanılarak veya farklı fonksiyonlar kullanılarak sağlanır.

Erişilebilirlik, "yetkilendirilmiş kullanıcıların bilgiye ve ilişkili kaynaklara erişim hakkına sahip olmalarının garanti edilmesi", "yetkilendirilmiş kullanıcıların sistemlere güvenli ve sürekli olarak erişmelerinin garanti edilmesi" veya "hizmetin sürekliliğinin sağlanması için gereken önlemleri alma girişimi" olarak tanımlanmaktadır.

Siber Güvenlik Unsurları

Authenticity (Kimlik Doğrulama): Gerçek olma ve doğrulanabilir ve güvenilir olma özelliği; bir iletimin, bir mesajın veya mesajı oluşturanın geçerliliğine olan güven. Bu, kullanıcıların söyledikleri kişi olduklarının ve sisteme gelen her girdinin güvenilir bir kaynaktan geldiğinin doğrulanması anlamına gelir. Örneğin, Bu unsur, elektronik imza ile sağlanır.



Accountability (Sorumluluk): Bir varlığın eylemlerinin o varlığa özel olarak izlenmesi gereksinimini oluşturan güvenlik hedefi. Bu, reddedilmeme, caydırıcılık, hata yalıtımı, izinsiz giriş algılama ve önleme ve eylem sonrası kurtarma ve yasal işlemi destekler. Gerçekten güvenli sistemler henüz ulaşılabilir bir hedef olmadığından, bir güvenlik ihlalini sorumlu bir tarafa kadar takip edebilmeliyiz. Sistemler, güvenlik ihlallerini izlemek veya işlem anlaşmazlıklarına yardımcı olmak için daha sonraki adli analizlere izin vermek için faaliyetlerinin kayıtlarını tutmalıdır. Bu unsur, açık anahtar altyapısı ve zaman damgası ile sağlanır.

Saldırılara Karşı Koyma Adımları

(1) Yapılan saldırıları önlemek için bir saldırı tespit ve koruma sistemi yaklaşımı gereklidir. Bu kurulmalıdır.
(2) Tehdidi saptama için bir sistem gereklidir. Bu sistem kurulmalıdır.
(3) Yapılan saldırıların ne zaman, nasıl, kim veya kimler tarafından yapıldığı saptanır. Bunun için kayıtları analiz edecek bir sistem kurulur veya uzmanlıklardan faydalanılır.
(4) Saldırılara karşı koyma (reaksiyon gösterme) işin önemli ve son adımıdır. Saptanan ve tespit edilen tehditler bu adımda giderilir. Karşılaşılan tehditler ortadan kaldırılır ve verilen zararlar giderilir. Sistem kayıplardan arındırılarak, önceki haline dönüştürülür.

Nasıl Bir Siber Güvenlik ve Savunma

“yüzde yüz bir güvenliğin” hiçbir zaman sağlanamayacağı yaklaşımıyla, varlıklar (yazılım, donanım, veri, süreç, uzmanlık, vb.) değerleri oranında ve sadece değerleri geçerli olduğu sürece korunmalıdır !!!

Nasıl Bir Siber Güvenlik ve Savunma

BT sistemlerinin; fiziksel güvenlikten haberleşme güvenliğine, yayınım güvenliğinden bilgisayar güvenliğine, ağ güvenliğinden bilgi güvenliğine, cihaz güvenliğinden sistem güvenliğine, yazılım güvenliğinden donanım güvenliğine, bulut ortamlarının güvenliğinden siber güvenliğe kadar birçok tedbirin alınması gerektiği bilinmeli ve korunacak olan siber varlıkların sınıfına, ortamına veya değerlerine göre gerekli güvenlik seviyeleri belirlenmeli ve koruma sağlanmalıdır.

Siber güvenlikte temel hedef; güvenliği **mükemmele yakın sağlama** olmalı, riskler iyi belirlenmeli, giderilmeye çalışılmalı ve iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak, belirlenen **siber güvenlik felsefesi** kapsamında çalışmalar yürütülmelidir

Nasıl Bir Siber Güvenlik ve Savunma

BT sistemlerinin; fiziksel güvenlikten haberleşme güvenliğine, yayınım güvenliğinden bilgisayar güvenliğine, ağ güvenliğinden bilgi güvenliğine, cihaz güvenliğinden sistem güvenliğine, yazılım güvenliğinden donanım güvenliğine, bulut ortamlarının güvenliğinden siber güvenliğe kadar birçok tedbirin alınması gerektiği bilinmeli ve korunacak olan siber varlıkların sınıfına, ortamına veya değerlerine göre gerekli güvenlik seviyeleri belirlenmeli ve koruma sağlanmalıdır.

Siber güvenlikte temel hedef; güvenliği **mükemmele yakın sağlama** olmalı, riskler iyi belirlenmeli, giderilmeye çalışılmalı ve iyi bir risk yönetimi yapılmalı, mevcut teknikler, teknolojiler, politikalar, standartlar ve çözümler uygulanarak, belirlenen **siber güvenlik felsefesi** kapsamında çalışmalar yürütülmelidir

Nasıl Bir Siber Güvenlik ve Savunma

- Bir güvenlik politikası oluşturulmalı ve uygulanmalıdır.
- Gereği kadar koruma prensibi uygulanmalıdır.
- İyi bir risk analizi ve yönetimi yapılmalıdır.
- Sistemlerde oluşabilecek hataları, eksiklikleri ve açıklıkları gidermek için zaman zaman testler (sızma testleri) yapmak ve tüm zafiyetleri gidermek gerekmektedir.

Nasıl Bir Siber Güvenlik ve Savunma

- Sistemleri kullanan her kullanıcıya en az hak verme yaklaşımı benimsenmelidir. Bir kullanıcıya ihtiyaç duyacağı hakları vermenin karşılaşılabilecek problemleri azaltacağı unutulmamalıdır.

- Siber güvenlik standartları (ISO 270XX Serisi Standartlar) yakınen takip edilmeli ve uygulanmalıdır. Bunlara ilave olarak, yakın olan diğer standartlardan da mutlaka faydalanılmalıdır.

- Elektronik ortamların her zaman güvensiz ortamlar olabileceği unutulmadan, sahip olunan bilgi varlıklarının yedeklenmesi veya kurtarılmasına yönelik sistemler (Felaket Kurtarma Merkezi) kurulmalı ve işletilmelidir.

Nasıl Bir Siber Güvenlik ve Savunma

- Güvenli sistem bileşenlerini tanımlama ve güvenlik gerektiren bileşenlerin sayılarını en aza indirgeme temel amaç olmalıdır.

- Siber güvenlik sistemlerini kuran, işleten, yöneten ve güncelleyenlerin güvenlik uzmanları olduğu unutulmadan, siber güvenlik uzmanlarının kendilerini geliştirmelerine fırsatlar verilmeli, bu birimlere daha fazla insan kaynağı ayırılmalıdır. Güvenliği teknik ve teknolojilerin yardımıyla insanların sağladığı veya ihlal edildiği de unutulmadan gerekli tedbirler alınmalıdır.

Siber Güvenlik ve Savunmanın Önemi

- Siber ortamlar, farklı verilerin, ortamların, sistemlerin, belge ve bilgilerin, süreçlerin, standartların, politikaların ve en önemlisi kritik yapıların bulunduğu ortamlardır. Bu ortamlardaki verilerin boyutu, kapsamı, çeşitliliği artmakta ve bu verilerden değer elde etme ise yaygınlaşmaktadır. Bununla beraber, bu verilerin ihlali, kötüye kullanımı, istismar edilmesi de arttığından, verilerin korunması da gereklidir.

- Veri koruma artık hukuki sonuçlar da doğurmaktadır. Kanun ve yönetmeliklerin uygulanması, yasal yükümlülüklerin yerine getirilmesi için önemlidir ve bir zorunluluktur.

- Siber ortam verilerinin; gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması hem rekabet gücünü artırma hem de ticari imajı korumak ve sürdürmek için bir zorunluluktur.

Siber Güvenlik ve Savunmanın Önemi

- Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları artırmaktadır. Ayrıca, yeni teknolojiler, altyapılar, kullanılan algoritmalar, uygulamalar ve hizmetler sürekli değişmekte ve gelişmekte, beraberinde yeni saldırılarıda getirmektedir. Bunlardan dolayı, oluşabilecek tehdit ve tehlikeleri gidermek, güven tesis etmek ve siber güvenliği üst seviyelerde tutmak için de önemlidir.

Siber Güvenlik ve Savunmanın Önemi

- Siber ortamlarda; online alışveriş sistemleri, bankacılık sistemleri, elektrik-üretim ve dağıtım tesisleri, akıllı şebekeler, cep telefonu opretatörleri, SCADA sistemleri, haberleşme sistemleri, doğal gaz kontrol ve aktarma sistemleri, hava trafik kontrol merkezleri, bilgisayar ve iletişim sistemleri, buna benzer kritik altyapılar ve ağlar, kritik yazılımlar ve buna benzer pekçok alanda yer alan uygulamalar ve sistemler bulunmaktadır. Bu ortamlara yapılacak saldırılar, ulusal hizmetlerin aksamasına, karmaşa, karışıklık veya kaosa sebebiyet verebileceğinden, siber güvenliğin sağlanması olmazsa olmalar arasındadır.

Siber Güvenlik ve Savunmanın Önemi

- Yapay Zeka, Nesnelerin İnterneti, Büyük Veri, Derin Öğrenme, Kuantum Hesaplama gibi yeni yaklaşımların, teknolojilerin, bakış açılarının ve uygulamalarının hızla artış gösterdiği günümüzde yeni tehdit ve tehlikelerin oluşacağı dikkate alındığında, siber güvenliğe ve savunmaya daha fazla ihtiyaç duyulacağı için önemlidir.

Siber Güvenlik ve Savunmanın Önemi

Kullanıcılar ve sistemler için siber güvenliğin sınırları; tarafların verilerini, kendilerini ve sistemlerini güven içinde hissetmeleri için gerekli ve düzenleyici politikalar doğrultusunda ve hukuki zorunluluklar çerçevesinde belirlenir. Güvenliğin bir kurum veya kuruluşun faaliyete geçmesiyle başladığı, varlığını sürdürdüğü zaman içerisinde süreklilik arz ettiğini belirtmekte fayda vardır.

Bilişim teknolojilerini kullanan her seviyedeki personel, kurum ve kuruluş, *"siber güvenlik kavramını bilmek, farkındalığını oluşturmak ve politikalarını belirlemek, siber varlıklarını, itibarlarını ve saygınlıklarını korumak"* zorundadır

Sorular

Bir sonraki ders Siber Güvenliğin Temelleri – 1 (Şifre Bilim (Kriptografi), Kullanılan Teknikler) konusuna giriş yapılacak.