SİBER SAVAŞ

https://cybermap.kaspersky.com/ gerçek zamanlı siber tehditleri takip edebilirisiniz.

İçindekiler

5) Siber Savaşın Hukuki ve Etik Boyutları

a) Uluslararası Hukuk ve Siber Savaş

b) Siber Saldırılara Yanıt Hakkı ve Meşru Müdafaa

c) Uluslararası Anlaşmalar ve Düzenlemeler

d) Savaş Suçları ve Siber Savaş

e) Etik İkilemler ve Sivil Hedefler

6) Siber Güvenlik ve Savunma Stratejileri

a) Ulusal Siber Güvenlik Stratejileri

b) Kritik Altyapı Koruması

c) Tehdit İstihbaratı ve Erken Uyarı Sistemleri

d) Siber Savunma Birimleri ve Yetenekleri

e) Uluslararası İşbirliği ve Siber Diploması

f) Sıfır Güven (Zero Trust) Yaklaşımı

7) KAYNAKÇA

1) Giriş: Siber Savaş Nedir?

a) Tanımı , bir devletin, başka bir devletin bilgisayar sistemlerine zarara uğratmak ya da kesinti yaratmak üzere gerçekleştirilen sızma, saldırı faaliyetleridir.

Siber saldırı, potansiyel olarak kötü niyetli bir niyetle verilere, sistemin diğer kısıtlanmış alanlarına yetkisiz erişmeye çalışılır. Bilgisayardaki verileri, bilgisayar ağlarını, altyapılarını, kişisel bilgisayar cihazlarını veya cep telefonlarını hedef alır.

Siber saldırı, bireyler, guruplar, topluluklar veya gri şapkalılar arasında olmakla birlikte devletler arasında da olmaktadır ve bu "DEVLET DESTEKLİ HACKER'LAR" tarafından gerçekleştirildiğinde ise artık bir "siber saldırı DEĞİL bir siber SAVAŞ veya siber TERÖRİZM" olarak adlandırılır.

*Bir siber saldırıyı kolaylaştıran bir ürüne bazen siber silah denir.

b) Tarihsel Gelişimi

Siber güvenliğin tarihsel gelişimi İkinci Dünya Savaşı, Soğuk Savaş, Milenyum dönemleri olmak üzere üç evrede inceleyeceğiz.

- İkinci Dünya Savaşı Evresi, iki olay gerçekleştiği söylenebilir.

Bunlardan birinci olay Alan Turing ve Gordon Welchman tarafından geliştirilen BOMBE isimli elekro-manyetik makinenin Almanların Enigma kodlarının kırılmasında kullanılması olayıdır. Nazi Almanyası İkinci Dünya savaşı sırasında şifreli haberleşmesinde rotor mekanizmaları aracılığı ile olasılık üreten Enigma elekro-manyetik sistemini kullanıyordu. İngiliz matematikçi Turing Bombe adını verdiği şifre kırıcıyı tasarladı, daha sonra dönemin ünlü kod kırıcısı Welchman bu tasarımda değişiklikler yaparak kod kırma aşamalarını en aza indirgedi. BOMBE, Almanların şifreli haberleşmelerini deşifre ederek müttefiklere önemli stratejik üstünlük sağlamıştır.

İkinci olay ise ilk etik korsan olarak tarihe geçen Rene Carmille'nin Nazi Almanya'sının Fransa işgali esnasında delikli-kart makinelerinin Yahudilerin kişisel verilerini takip etmede kullanılmasını engellemesi olaydır. Rene Carmille delikli-kart bilgisayarı uzmanı ve Nazi işgali altındaki Fransa'daki direniş grubunun mensubuydu. Fransa'daki Vichy yönetiminin bilgi işleme amacıyla kullandıkları bilgisayarlara sahip olan Carmille, Nazilerin delikli-kart makinelerini Yahudilerin takibi için kullandıklarını tespit ettikten

sonra, makinelere bürokratik anahtarlar ekleyerek bu makineleri sabote etmiştir. Böylece pek çok insanın hayatını kurtarmıştır.

1960'lı yıllarda Amerikan hükümeti adına çalışan bilim insanlarının kendi aralarında haberleşmelerini sağlamak amacıyla kurulan internet, 1990'lı yıllara gelindiğinde yaygınlaşmaya başlamıştır. Bu nedenle ikinci dünya savaşı döneminde bildiğimiz manada ağlar üzerinden bilgisayar sistemlerine yapılan bir saldırıdan söz etmek mümkün değildir. Ancak örnek olaylar teknolojik imkânlar vasıtasıyla düşmanların kullandıkları cihazları etkilemenin mümkün olduğunu ve böylelikle düşman ülkelere stratejik avantajlar sağlamanın mümkün olduğunu göstermektedir. Burada örneklendirilen iki olay siber saldırı ve siber savaşların başlangıç noktasının karşı tarafın hassasiyetlerini istismar etmek üzerine kurulduğunu da bizlere göstermektedir.

- Soğuk Savaş evresi

Soğuk Savaş Evresi Batı ülkeleri ve Doğu ülkeleri arasında 1947–91 yılları arasında cereyan eden Soğuk Savaş bu dönemin karakteristiğini yansıtan ve gerçek manada siber savaşın başlangıcı olarak da kabul edebileceğimiz olay, 1982 yılında Rusya'ya ait Sibirya doğalgaz boru hattına Amerikan Merkezi İstihbarat Teşkilatı (CIA) tarafından gerçekleştirildiği iddia edilen saldırıdır . Sibirya doğalgaz boru hattı saldırısı Rus ajanlarının onu çaldığına inandırıldıkları bir yazılımın içine gizlenen Truva Atı aracılığı ile gerçekleştirilmiştir. Bu saldırıda kullanılan Truva atı yazılımı boru hattı bağlantıları ve kaynakları için standart basınç seviyesinin üzerinde basınç elde etmek için pompa hızları ve valf ayarlarının değiştirilmesinde kullanılmıştır .

- Milenyum evresi

2000–2010 yılları arasında meydana gelen önemli siber savaş maksatlı siber saldırılar dâhil edilmiştir. İnternet teknolojilerinde meydana gelen değişimler, yeni saldırı türlerinin ortaya çıkışı ile paralel olarak bu dönemde çok sayıda siber saldırı meydana gelmiştir. Bunlardan önemli etkileri olan ve zengin içeriğe sahip altı vaka seçilmiştir.

2007 yılı içerisinde Estonya devlet kurumları ve bankacılık sektörü başta olmak üzere özel işletmelere yönelik zombi bilgisayarlar vasıtasıyla DDos saldırıları yapılmıştır. Özellikle bankacılık ve lojistik sektörü hedef alan saldırılar Estonya'da hayati hizmetlerin aksamasına, maddi zararın oluşmasına ve prestik kaybına neden olmuştur. Bu saldırıların Tallinn'de bulunan Sovyet dönemine ait bir anıtın yer değiştirmesinden kaynaklı Rusya ile Estonya arasındaki siyasi gerilim esnasında gerçekleşmesi, siber saldırıların Rus hükümeti tarafından desteklendiği iddialarını güçlendirmiştir.

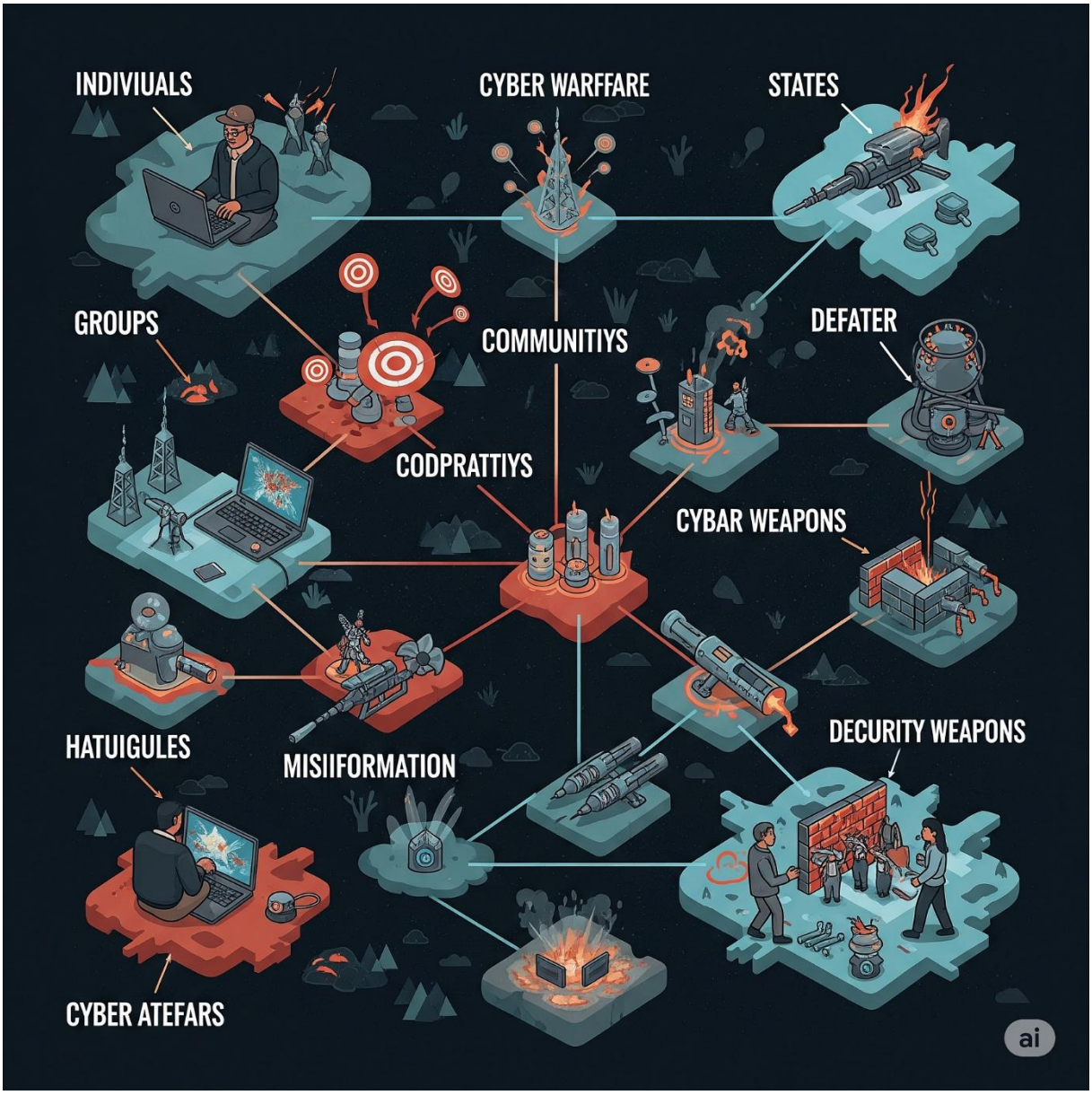
Ukrayna kaynaklı çevrimiçi devlet sitelerinin yanı sıra finans ve enerji şirketlerine ait sitelere 2017 yılında NotPetya fidye yazılımı ile yapılan saldırılar yaklaşık olarak 300 milyon dolarlık bir zarara neden olmuştur. CIA bu saldırının Rus askeri siber savaş birimlerince yapıldığını öne sürmüştür . Olumsuz sonuçlarının diğer ülkelere yansıması ve tehdidin uluslararası bir sorun haline gelmesi bu saldırıyı daha önceki saldırılardan farklı kılan unsurlardan birisidir .

İran'daki nükleer santrale yapılan Stuxnet veya Olimpik Oyunlar olarak bilinen saldırıdır. Saldırnın kaynağı hakkında kesin bir bilgi sahibi olunmasa da, saldırıyı İran ile politik anlaşmazlıklar içerisinde bulunan ABD veya İsrail tarafından gerçekleştirildiği öne sürülmektedir. Her ne kadar saldırı 2010 yılında gerçekleşmiş olsa da, bu eylem aslında 2006 yılında başlayan bir siber saldırı programının son halkasıydı. İran'ın uranyum zenginleştirme programını sekteye uğratmak maksadıyla denetim kontrol ve veri toplama (SCADA) sistemleri Haziran ve Temmuz aylarında gerçekleşen iki ayrı saldırı ile hedef alınmıştı. Harici bellek ile sisteme nüfuz eden bilgisayar solucanı, SCADA sistemlerini denetleyen Siemen Step 7 yazılımını hedef almıştır. Bu zararlı yazılım bir yandan bilgisayar kontrollü elektro-mekanik ekipmana hasar verecek komutlar yollarken, diğer yandan ana kontrol ünitelerine sahte geri beslemeler göndermiştir. Bu saldırının santralde bulunan 948 uranyum zenginleştirme santrifüjüne zarar verdiği tahmin edilmektedir.

Stuxnet saldırısı , bilgisayar sistemlerine harici bir donanım ile nüfuz etmiştir. Sistem bileşenlerindeki hassasiyetleri istismar ederek cihazların uzaktan kontrol edilebileceğini, kritik alt yapı ve tesislere bu yolla fiziksel zararlar verilebileceğini göstermiştir. Santralde görevli bir işçinin harici belleğinin enfekte edilmesiyle başlayan bu saldırı, bize insanların güvenlik hatalarının da bilgisayar sistemleri ve internet ağlarına ciddi hasarlar verilmesinde etkili olduğunu göstermiştir.

Rusya ve Gürcistan arasında devam eden savaş esnasında 2008 yılında Gürcistan'a yapılan siber saldırılar ise, Gürcistan'daki farklı sektörleri hedef alan siber saldırılar Estonya saldırısı benzeri ekonomik ve sosyal açıdan yıkıcı sonuçlar vermiştir.

2) Siber Savaşın Aktörleri



a) Ulusal Devletler ve Hükümetler

Devletler, siber savaşta saldırı kapasitesi geliştiren başlıca aktörlerdir.

- Ulusal Güvenlik: Siber saldırıları, ulusal güvenliklerini tehdit eden unsurlara karşı bir araç olarak kullanırlar. Örneğin, başka bir devletin kritik altyapılarına yönelik sızma, hasar verme veya işlevsiz bırakma eylemleri gerçekleştirebilirler.

- Casusluk ve İstihbarat: Siber casusluk faaliyetleri ile diğer devletlerin gizli bilgilerine, askeri planlarına, teknolojik sırlarına veya diplomatik yazışmalarına erişmeye çalışırlar.
- Etki Operasyonları: Yabancı kamuoyunu etkilemek, dezenformasyon yaymak veya politik istikrarsızlık yaratmak amacıyla siber operasyonlar yürütebilirler.
- Devlet Destekli Hacker Grupları: Kimi zaman doğrudan kendi birimleri aracılığıyla, kimi zaman da dolaylı olarak, devlet destekli hacker grupları veya siber suçluları kullanarak siber saldırılar düzenlerler. Bu durum, sorumluluğun üstlenilmesini zorlaştırır ve "inkar edilebilir" bir saldırı imkanı sunar.

Devletler aynı zamanda siber tehditlere karşı savunma mekanizmalarını oluşturan ve güçlendiren ana aktörlerdir:

- Ulusal Siber Güvenlik Stratejileri
- Kurumsal Yapılandırma
- Altyapı Güçlendirme
- Uluslararası İşbirliği
- Siber Ordu/Komutanlık Kurulumu

ile devletlerin savunma mekanizmaları ile güvenliği sağlarlar.

b) Devlet Destekli Hacker Grupları

Rusya: Fancy Bear ve Cozy Bear

Rusya'nın en bilinen hacker gruplarından Fancy Bear (APT28) ve Cozy Bear (APT29), ABD seçimlerine müdahale, Avrupa'daki siyasi manipülasyonlar ve NATO ülkelerinin sistemlerine sızma operasyonlarıyla tanınıyor. Genellikle kimlik avı (phishing) saldırıları, kötü amaçlı yazılımlar ve sıfır gün açıklarını kullanarak hedeflerine ulaşıyorlar.

Çin: APT41 ve Hafnium

Çin merkezli APT41 ve Hafnium, küresel çapta ekonomik casusluk yapmak ve endüstriyel sırları çalmak için faaliyet gösteriyor. Bu gruplar özellikle teknoloji şirketlerine, savunma sanayisine ve akademik araştırma merkezlerine sızarak kritik verileri ele geçiriyor. Çin hükümetinin doğrudan desteğiyle çalıştıkları iddia edilen bu hackerlar, siber casuslukta oldukça ileri teknikler kullanıyor.

Kuzey Kore: Lazarus Group

Kuzey Kore'nin en bilinen hacker grubu olan Lazarus Group, finansal saldırılarla ülkeye ekonomik kazanç sağlamayı hedefliyor. 2017'deki WannaCry fidye yazılımı saldırısı, Sony

Pictures hacklenmesi ve büyük çaplı kripto para hırsızlıkları bu grubun eylemlerine örnek olarak gösterilebilir.

İran: APT33 ve Charming Kitten

İran destekli APT33 ve Charming Kitten, özellikle Orta Doğu'daki rakip ülkelerin altyapılarını hedef alıyor. Enerji sektörüne yönelik saldırılar, muhaliflerin takibi ve propaganda amaçlı siber operasyonlar bu grupların uzmanlık alanlarından. Bu gruplar, genellikle devletlerin politik hedeflerine hizmet eden operasyonlar yürütüyor. Amaçları sadece bilgi çalmak değil, aynı zamanda psikolojik savaş taktikleriyle toplumları manipüle etmek.

c) Terör Örgütleri ve Suç Grupları

Siber güvenlik, dijital dünyadaki tehditlere karşı korunma süreçlerini kapsayan geniş bir alan olarak tanımlanırken; siber terörizm, siyasi amaçlar güden terör gruplarının siber uzayı kullanarak gerçekleştirdiği veya tehdit ettiği saldırıları ifade ediyor. Bu iki kavramın farklı aktörler (bireyler, suç grupları, devletler, terör örgütleri) tarafından kullanılabileceği unutulmamalıdır.

Dipnot: Siber uzay, terimi bilgisayarların ve onu kullanan insanların İnternet ve benzeri ağlar içinde kurduğu iletişimden doğan sanal gerçeklik ortamını anlatan metaforik bir soyutlamadır. Siber uzay kavramı Türkçede zaman zaman "siber ortam" olarak da kullanılmaktadır.

Siber terörizmin ana ayırt edici özelliği, saldırıların doğrudan fiziksel şiddet içermemesi ve siber altyapı (yazılım, donanım, ağlar) üzerinden gerçekleştirilmesidir. Siber terörizmin geleneksel terörizm gibi can kaybına yol açmasa da günlük hayatı etkileyebilecek, ulusal güvenlik sorunlarına ve maddi kayıplara neden olabilecek ciddi sonuçlar doğuracaktır. Terör örgütlerinin siber alanı propaganda, iletişim, finansman, istihbarat ve saldırı gibi çeşitli amaçlarla kullandığı belirtiliyor.

Siber terörizmin potansiyel hedefleri arasında enerji**,** telekomünikasyon**,** askeri sektörler**,** finansal altyapı **ve** kritik kamusal hizmetler gibi geniş bir yelpaze bulunuyor. Bu saldırılarla terör örgütleri, hedef toplumlarda korku, panik ve güvensizlik oluşturmayı, hedef ülkeyi itibarsızlaştırmayı ve güç gösterisi yapmayı amaçlıyorlar.

Terör örgütü olarak tanımlanmış örgütler listesi

Bir dizi ulusal hükûmet ve iki uluslararası kuruluş, terörist olarak tanımladıkları örgütlerin listelerini oluşturmuştur. Aşağıdaki tanımlanmış terörist örgütleri listesi, mevcut ve eski ulusal hükûmetler ve hükûmetler arası kuruluşlar tarafından terörist olarak tanımlanan örgütleri listeler.

aşağıdaki linkten ulaşabilirsiniz.

Terör örgütü olarak tanımlanmış örgütler listesi - Vikipedi Vikipedi, özgür ansiklopedi
Bir dizi ulusal hükûmet ve iki uluslararası kuruluş, terörist olarak tanımladıkları...tr.wikipedia.org

3) Siber Savaşın Amaçları ve Hedefleri

a) Kritik Altyapıların Hedeflenmesi (Enerji, Su, Telekomünikasyon, Finans)

Siber saldırılar yıllardır bireyleri ve şirketleri hedef alıyor , onları hazırlıksız yakalayıp hassas verileri çalmayı çalışıyor.

İnsanlar ve altyapılar giderek daha fazla bağlantıya bağımlı hale geldi. Uzaktan çalışma ve Nesnelerin İnterneti devrimi gibi gelişmeler , bu birbirine bağlı olma eğilimini hızlandırdı ve siber suçluların saldırması için daha fazla kapı açtı .

örnekler;

Sömürge Boru Hattı Petrolü 2021

Tehdit**:** 5 milyon dolar fidye, petrol ve gaz kıtlığı
Şüpheli**:** Rus hacker grubu DarkSide
Tetikleyici**:** Bilinmiyor

Ukrayna'nın Elektirik şebekesi 2022

Tehdit**:** Elektrik kesintileri
Şüpheli**:** Rus hacker grubu 'Sandworm'
Tetikleyici**:** Kötü amaçlı yazılım saldırısının ardından gelen izinsiz giriş saldırısı

KillNet 2022–2023

Tehdit**:** Sağlık, enerji ve savunma sektörlerinde kesintiler
Şüpheli: Rusya yanlısı hacker grubu KillNet
Tetikleyici: DDoS

Pensilvanya Su Sistemi 2023

Tehdit: Su temini ve kalitesi
Şüpheli: İranlı hacker grubu " Cyber Av3ngers"
Tetikleyici: Kötü amaçlı yazılım saldırısının ardından gelen izinsiz giriş saldırısı

Hollanda: Güneş Panelleri 2024

Tehdit**:** Elektrik kesintileri, mali kayıplar, ulusal güvenlik
Şüpheli: Etik " Hollandalı " bilgisayar korsanları
Tetikleyici: Nesnelerin İnterneti (IoT) cihazlarındaki sıfırıncı gün güvenlik açıkları.

ABD Sağlık Sistemleri 2024

Tehdit: Sağlık hizmetlerinin aksaması
Şüpheli: Rus Blackcat/ALPHV fidye yazılımı grubu
Tetikleyici: Fidye yazılımının izlediği izinsiz giriş saldırısı

b) Bilgi Hırsızlığı ve Casusluk

Siber casusluk, muhtemelen stratejik, politik veya finansal avantaj elde etmek amacıyla gizli bilgilere yetkisiz erişimdir. Çoğunlukla, hassas bilgileri çalmak amacıyla bilgisayar sistemlerine, ağlarına veya cihazlarına sızan devlet destekli gruplar veya bağımsız bilgisayar korsanları tarafından yürütülür. Daha çok finansal kazançlara odaklanan siber suçun aksine, siber casusluk genellikle devlet kurumları, askeri kuruluşlar, şirketler veya araştırma kurumlarından bilgi toplamakla ilgilidir.

c) Propaganda ve Dezenformasyon Faaliyetleri

Propaganda ve dezenformasyon faaliyetleri, siber güvenlikle olan ilişkisi, dijital ortamda gerçekleştirilmeleri ve siber saldırılarla iç içe geçebilme potansiyellerinden kaynaklanır.

Propaganda, belirli bir fikri, ideolojiyi veya kişiyi desteklemek amacıyla yapılan sistematik bir yayma faaliyetidir. Dezenformasyon ise kasıtlı olarak yanlış veya yanıltıcı bilgi yayma eylemidir ve genellikle kamuoyunu manipüle etmeyi hedefler. Her ikisi de dijital ortamda, özellikle sosyal medya platformları aracılığıyla yaygınlaşır. Bu noktada siber güvenlikle doğrudan bir bağ oluşur.

-Sosyal Medya Manipülasyonu

-Sosyal Mühendislik ve Kimlik Avı

-Kritik Altyapı ve Hizmetlere Yönelik Tehditler

-Güven Aşındırma ve Kutuplaşma

-İtibar Yönetimi ve Kurumsal Güvenlik

Propaganda ve dezenformasyon faaliyetleri, siber saldırıların bir öncüsü, tamamlayıcısı veya bağımsız bir tehdit unsuru olarak siber güvenlik ekosisteminde önemli bir yer tutar. Bu nedenle, siber güvenlik stratejileri geliştirilirken bu tür bilgilendirici manipülasyon faaliyetlerine karşı da önlemler alınması büyük önem taşımaktadır.

d) Askeri Operasyonlara Destek ve Köstek Olma

Siber güvenliğin önemli bir kısmını askeri siber güvenlik önlemleri oluşturmaktadır. Günümüzde hibrit savaş içinde siber unsurların kullanılması yanında, birçok askeri hedefe yapılan saldırılara siber saldırı unsurlarının da eşlik ettiğini görmekteyiz. Özellikle askeri istihbarat unsurlarının önemli bir kısmının artık siber saldırı ve istihbarat araç ve yöntemleri kullandığı bilinmektedir. Bu nedenle, bir güvenlik ittifakı olarak NATO da, 2007'de Estonya'ya yönelik gerçekleştirilen siber saldırıdan sonra öncelikle siber uzaya dönük savunma odaklı bir strateji geliştirmiştir. Kritik altyapıların korumalarını esas alan

bu yaklaşım, 2008'de Rusya'nın Gürcistan'da ülkenin hem kara askeri güçlerini hem de bilgisayar ve iletişim altyapısını hedef alan saldırısıyla birlikte daha da derinleşti ve bu tür saldırılara karşı önlemler geliştirebilmek amacıyla 14 Mayıs 2008'de Estonya Tallinn'de Siber Savunma Mükemmeliyet Merkezi kuruldu. Ardından NATO'nun 2016 Varşova Zirvesi'nde siber uzay kendi başına bir 'askeri operasyon sahası' olarak kabul edildi. Böylece NATO sadece saldırılara karşı üyelerini savunmak amacıyla tasarladığı siber savunma stratejisinden, siber saldırıyı da içine alan bir yaklaşıma doğru evrildi. Bu gelişme sonrasında üye ülkeler de askeri yapıları içinde siber uzayda savaşabilecek birlikler tesis etmeye başladılar. Siber uzayın ayrı bir operasyon alanı olarak kabul edilmesi, siber saldırılara nasıl karşılık verilebileceği gibi teknik soruları gündeme getirdi. Özellikle ABD'de 'siber saldırılara fiziksel cevap verilip verilmeyeceği' yönünde hararetli tartışmalar olurken, Washington, Amerikan askeri güçlerinin kişisel bilgilerini Twitter aracılığıyla duyuran DAEŞ'li bir siber saldırgana (hacker) insansız hava araçları ile saldırı düzenleyerek bu konudaki ilk örneği oluşturdu. 6 Mayıs 2019'da da İsrail ordusu, siber saldırı gerçekleştiren HAMAS'a karşı bu saldırıların yapıldığını iddia ettiği Gazze'deki bir binayı bombalayarak karşılık verdi. Böylece siber saldırılara karşı fiziksel cevap verilebileceği konusunda belirgin örnekler ortaya çıkmış oldu.

Askeri siber organizasyonların ve operasyonların hızla gelişmesine karşın uluslararası hukukun bu konuda yetersiz kaldığı ve henüz gelişmekte olduğu görülmektedir. Askeri siber organizasyonların karar vericilerinin bu bağlamda uluslararası hukukun gelişiminde yönlendirici rol oynayabilmek için siber diplomasi sahasında çalışan kurumlarla işbirliği yapmaları gerekmektedir.

e) Ekonomik Sabotaj

2018 yılında siber suçların küresel ekonomiye maliyeti yaklaşık 600 milyar dolar olarak tahmin edilmektedir. Bu rakam, 2014 yılındaki 445 milyar dolarlık zarara kıyasla %34'lük bir artışı temsil etmektedir. Avrupa ekonomisinin %0,84'ü siber suçlardan etkilenmiştir.

Siber suçların büyük bir kısmı (%80), devlet destekli organize suçlar olarak nitelendirilmektedir. Siber saldırılar savunma (yılda 16.1 milyon dolar) ve finansal hizmetler (11.5 milyon dolar) sektörlerinde yüksek maliyetlere yol açmaktadır.

4) Siber Saldırı Türleri ve Teknikleri

a) DDoS (Hizmet Reddi) Saldırıları

Dağıtılmış hizmet reddi (DDoS) saldırısı, genellikle ana sunucunun hizmetlerini geçici olarak kesintiye uğratarak veya ekleyerek, çevrimiçi bir hizmeti veya web sitesini kullanıcılar için erişilemez hale getirmek için yapılan kötü amaçlı bir girişimdir.

b) Malware (Kötü Amaçlı Yazılım) ve Virüsler

Zararlı yazılım, kötü amaçlı yazılım veya malware, bilgisayar ve mobil cihazların işlevlerini bozmak, kritik bilgileri toplamak, özel bilgisayar sistemlerine erişim sağlamak ve istenmeyen reklamları göstermek amacı ile kullanılan yazılımdır.

c) Fidye Yazılımları (Ransomware)

Fidye yazılımı çalışmaya başladığında, yerel ve ağ depolamasını tarayarak şifrelenecek dosyaları arar. İşletmeniz veya bireyler için önemli olduğunu varsaydığı dosyaları hedefler.

d) Kimlik Avı (Phishing) ve Sosyal Mühendislik

Kimlik avı, siber korsanların e-posta yoluyla kullanıcı veya şirket bilgilerini çalmak için kullandığı sosyal mühendislik tekniklerini tanımlar. Kimlik avı saldırıları en çok, kullanıcılar bunun olduğunun farkında olmadığında etkilidir.

e) Sıfır Gün (Zero-Day) Açıkları

Sıfır gün açığı, henüz bir çözümü olmayan bir güvenlik açığından faydalanan bir saldırıdır. “Sıfır gün” tehdidi olarak adlandırılır çünkü kusur keşfedildikten sonra, geliştirici veya kuruluşun bir çözüm bulması için “sıfır gün” süresi vardır.

f) Tedarik Zinciri Saldırıları

Tedarik zinciri saldırısı , tedarik zincirindeki daha az güvenli unsurları hedef alarak bir kuruluşa zarar vermeyi amaçlayan bir siber saldırıdır . Tedarik zinciri saldırısı, finans sektöründen petrol endüstrisine ve hükümet sektörüne kadar her sektörde meydana gelebilir.

g) APT (Gelişmiş Sürekli Tehdit) Grupları

Gelişmiş sürekli tehdit (APT), genellikle bir grup becerikli bilgisayar korsanı tarafından hazırlanan ve uzun bir süre boyunca devam eden sofistike ve sistematik bir siber saldırı programıdır.

5) Siber Savaşın Hukuki ve Etik Boyutları

a) Uluslararası Hukuk ve Siber Savaş

Uluslararası hukukta silahlı çatışmalarda hukuka uygun araç ve yöntemlerin kullanılması ve savaş başladıktan sonra bazı kurallara uyulması uluslararası antlaşmalar ile belirlenmeye çalışılmıştır. Bu kurallara uyulmaması durumunda ise devletlerin sorumluluğu gündeme gelecektir ve kurallara uymayan devlete karşı bazı yaptırım metotları uygulanabilecektir.

Bir siber savaş durumunda mevcut kuralların, siber savaş için geçerli olup olmayacağı meselesini değerlendirmeye aldığımızda, mevcut kurallardan ilki savaş alanı ve savaşın ilan edilmesi ile ilgilidir. Bu iki kural çerçevesinde siber savaş esnasında devletlerin ülkesel alanı da savaş alanı olarak kabul edilebilecektir. Savaş ilan edilmesi meselesi ise uluslararası hukukta zorunlu olmadığı için, siber savaş durumunda da herhangi bir ilanda bulunma zorunluluğu yoktur. Siber savaş ile ilgili en önemli meselelerden birisi, silahlı çatışmalar hukukunda belirtilen savaşçı tanımının, siber savaşçılar için uygulanmasının zorluğudur. Siber savaşçılar genellikle silahlı kuvvetler mensubu olmayı, sivil vatandaşlar olmaktadır. Ancak yine de bu durum silahlı çatışmalar hukuku kuralları bu kişiler için de geçerli olup, devletlerin bu kişiler üzerinde de denetim ve kontrol yetkisi bulunmaktadır. Son olarak kara, deniz ve hava da silahlı çatışmaların yürütülmesi de yine siber savaş için de geçerli olacaktır. Burada dikkat edilmesi gereken esas nokta, siber saldırılardan kullanılan siber enstrümanların silahlı bir saldırının etkisini doğuracak sonuç yaratması beklenmektedir. Günümüzde NATO ve BM gibi uluslararası kuruluşlar siber savaş ile ilgili bazı kuralların oluşması yönünde çalışmalar gerçekleştirmektedir. Bu zamana kadar herhangi bir siber savaş gerçekleşmemiştir. Ancak daha önce de değindiğimiz üzere teknolojinin her geçen gün hızlı bir şekilde gelişmesi, ilerleyen yıllarda savaş konseptini de değiştirebilecektir diyebiliriz.

- **Devlet Sorumluluğu:** Bir devlet, kendi topraklarından kaynaklanan siber saldırıları önlemekle yükümlü müdür? Evet .
- **Kuvvet Kullanımı:** kesin birşey söylenmemektedir. Az sonra okuyacağınız *b) Siber Saldırılara Yanıt Hakkı ve Meşru Müdafaa bölümünde ayrıntılı cevaplanmaktadır.*
- **Kanıt Toplama ve Yargılama:** Sınır ötesi siber suçlarda kanıt toplama, faillerin tespiti ve yargılanması süreçleri uluslararası işbirliği gerektirmektedir.

b) Siber Saldırılara Yanıt Hakkı ve Meşru Müdafaa

Siber savaşa IHL'nin (Uluslararası İnsancıl Hukuk) nasıl uygulanacağı sorusu, ancak bir devletin "siber saldırılar" olarak algıladığı durumlara yanıt olarak yasal olarak "güç" kullanabileceği belirlendikten sonra ele alınabilir. Bu belirleme, bir devletin uyuşmazlık çözüm aracı olarak meşru olarak ne zaman güç kullanabileceğini ve kullanamayacağını dikte eden yerleşik "çatışma yönetimi" normları ve prosedürleri olan J*us ad bellum bağlamında yapılmalıdır* .

Jus ad bellum , Birleşmiş Milletler Sözleşmesi, Sözleşme'nin yorumları ve Sözleşme ile birlikte ve bazen de Sözleşme'den önce geliştirilen uluslararası örf ve adet hukuku tarafından yönetilir.

“Kuvvet kullanımı”, “kuvvet tehdidi” veya “silahlı saldırı” terimleri Birleşmiş Milletler Sözleşmesi’nde tanımlanmamıştır. Ancak uluslar, olumsuz ticaret kararları, uzay tabanlı gözetleme, boykotlar, diplomatik ilişkilerin kesilmesi, iletişimin engellenmesi, casusluk, ekonomik rekabet veya yaptırımlar ve ekonomik ve politik zorlama gibi belirli dostça olmayan eylemlerin, etkilerinin ölçeği ne olursa olsun, kuvvet kullanımı seviyesine ulaşmadığını anlar. Silahlı saldırı; ilan edilmiş savaş, toprak işgali, deniz ablukası ve yurt dışında topraklara, askeri güçlere veya sivillere karşı silahlı kuvvet kullanımını içerebilir. Ancak, saldırgan siber operasyonların nasıl değerlendirilmesi gerektiğine dair emsal bulunmamaktadır.

BM Şartı’nın 2. maddesinin (4) numaralı fıkrasının gerçek anlamı konusunda uluslararası hukukçular ve hukukçular arasında görüş ayrılıkları bulunsa da, bu hüküm bir devletin uluslararası toplumda başka bir devlete karşı “güç” kullanmasını veya bu tehdidi savurmasını yasaklamaktadır. Şart’ın 39. ve 42. maddelerinde, güç kullanımına ilişkin bu yasağa yalnızca iki istisna yer almaktadır: Güvenlik Konseyi tarafından yetkilendirilen eylemler ve BM Şartı’nın 51. maddesi uyarınca meşru müdafaa eylemleri.

c) Uluslararası Anlaşmalar ve Düzenlemeler

Siber suçlarla mücadele ve siber güvenliğin sağlanması amacıyla birçok uluslararası anlaşma ve girişim bulunmaktadır. Bunlardan en önemlileri şunlardır:

- Avrupa Konseyi Siber Suç Sözleşmesi (Budapeşte Sözleşmesi)
- Birleşmiş Milletler (BM) Çerçevesi
- Şanghay İşbirliği Örgütü (ŞİÖ) Uluslararası Bilgi Güvenliği Alanında İşbirliği Anlaşması
- Afrika Birliği Siber Güvenlik ve Kişisel Verilerin Korunması Sözleşmesi
- Uluslararası Telekomünikasyon Birliği (ITU)
- Küresel Siber Güvenlik Gündemi (Global Cybersecurity Agenda / GCA)
- Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA)
- NATO
- ISO/IEC 27000 Serisi Standartları
- NIST Siber Güvenlik Çerçevesi

d) Savaş Suçları ve Siber Savaş

Siber savaş , bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirilen sızma faaliyetleridir.

Siber savaşın potansiyel etkileri ,

Kritik altyapılarda bozulmalar, havacılık ve uydu sistemlerinde aksaklıklar, finans sektöründe durmalar, ulaşım sistemlerinde sorunlar, elektrik şebekesinde kesintiler meydana gelir.

Savaş suçu kriterleri olarak ise ,

Orantısız zarar,

(Siber saldırılar planlanırken veya uygulanırken, potansiyel olarak orantısız zarara yol açabilecek her türlü olasılık dikkate alınmalıdır. Eğer bir saldırının sivil kayıplara neden olabileceği önceden tahmin edilebiliyorsa, bu saldırıyı uygulamak sadece stratejik bir hataya değil, aynı zamanda bir savaş suçuna yol açabilir.)

Ayrım gözetmeme,

(Devlet X'in başlangıçta sadece askeri bir hedefi vurmayı amaçlamış olsa da sivil altyapıya ve yaşama yönelik büyük ve orantısız zararlar vermiştir. Bu tür bir saldırı, uluslararası hukuk bağlamında açıkça bir savaş suçu olarak kabul edilecektir. Ayrım gözetmeme ilkesinin ihlali, sadece etik ve hukuki sonuçlar doğurmakla kalmayıp, aynı zamanda uluslararası toplumda ciddi diplomatik yıkımlara yol açabilir.)

Uluslararası hukuk,

(Colonial Pipeline "ABD'deki kritik altyapıya yönelik kamuoyuna açıklanan en büyük siber" saldırı gibi olaylar, uluslararası hukukun siber saldırılara uygun bir yanıt geliştirebilmesi için derinlemesine analiz ve güncellemelerin kaçınılmaz olduğunu gösteriyor. Yeni teknolojiler ve siber tehditler, mevcut hukuki çerçevelerin yetersiz kaldığı alanlara işaret ediyor. Dolayısıyla, devletlerin ve uluslararası kuruluşların bu konudaki yasal boşlukları dolduracak mekanizmalar geliştirmesi, giderek daha acil bir hale geliyor.)

Türkiye'nin siber güvenliği: tehditler, zafiyetler ve stratejik ihtiyaçlar

(Türkiye'nin uygulayabileceği en etkili strateji, devlet destekli siber güvenlik inisiyatiflerini özel sektör ve uluslararası ortaklarla daha etkin bir şekilde koordine etmektir. Ayrıca, mevcut yasal çerçeve ve yaptırımların siber tehdit ve saldırıları caydıracak şekilde güncellenmesi, Türkiye'nin siber alandaki savunma kabiliyetini artıracaktır.)

e) Etik İkilemler ve Sivil Hedefler

Siber güvenlik etiği, Etik siber güvenlik uygulamaları, veri koruma ve siber güvenliği düzenleyen yasal ve düzenleyici çerçevelere bağlı kalarak bireylerin, kuruluşların ve toplumun haklarını ve çıkarlarını korur.

Etik sorunlar ise, gizlilik ihlalleri, gözetim ve izleme, siber güvenlik kaynak tahsisi, şeffaflık ve açıklama sorunları ile karşılaşılmasıdır.

Etik ikilemler ise , tehditler ve riskler, gizlilik, kullanıcı gizliliği maalesef ki ikilemleri arasında kalınmaktadır.

Siber güvenlik profesyonellerinin karşı karşıya kaldığı etik ikilemler, mesleki görevler ile ahlaki yükümlülükler arasında hassas bir denge gerektiriyor.

Siber güvenlikte sivil hedefler, siber saldırıların odak noktası haline gelebilen, doğrudan askeri olmayan ancak toplumsal yaşamın ve ekonominin işleyişi için kritik öneme sahip kişi, kurum, altyapı ve verileri ifade eder. Bu hedeflere yönelik saldırılar, ciddi toplumsal ve ekonomik sonuçlar doğurabilir.

Siber güvenlikte sivil hedeflerin korunması, hem devletlerin hem de bireylerin ortak sorumluluğundadır. Bu, güçlü siber güvenlik altyapılarının oluşturulması, siber güvenlik farkındalığının artırılması ve uluslararası işbirliğinin güçlendirilmesiyle mümkündür.

6) Siber Güvenlik ve Savunma Stratejileri

a) Ulusal Siber Güvenlik Stratejileri

Türkiye'de şuanda uygulanan Ulusal Siber Güvenlik Stratejisine (2024–2028) https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf

buradan ulaşabilirsiniz.

b) Kritik Altyapı Koruması

b.1) Siber Güvenlik Önlemleri: Güçlü güvenlik sistemleri, düzenli güvenlik testleri, ağ izolasyonu

b.2) Fiziksel Güvenlik: Erişim kontrolü, gözetim sistemleri, acil durum planları

b.3) Doğal Afetlere Karşı Dayanıklılık: Altyapı güçlendirme, yedek **s**istemler

b.4) Ulusal ve Uluslararası İşbirliği: Paydaşlarla koordinasyon, uluslararası standartlar

b.5) Eğitim ve Farkındalık: Personel eğitimi, toplum farkındalığı

c) Tehdit İstihbaratı ve Erken Uyarı Sistemleri

Siber tehdit istihbaratı, bir kuruluşun sistemlerine yönelik mevcut veya gelecekteki siber saldırıları tespit etmek için kullanılan bilgilerdir.

Klasik güvenlik anlayışında saldırıları tespit etme amaçlı IDS, SIEM, Firewalls gibi ürünler kullanılmaktadır.

Erken Uyarı Sistemleri genellikle tek bir yazılımdan ziyade, farklı güvenlik teknolojilerinin birleşimiyle oluşur. Bunlardan bazıları şunlardır:

- **Saldırı Tespit Sistemleri (IDS — Intrusion Detection Systems):** Ağ trafiğini veya sistem günlüklerini izleyerek bilinen saldırı imzalarına veya anormal davranışlara göre tehditleri tespit eder.
- **Saldırı Önleme Sistemleri (IPS — Intrusion Prevention Systems):** IDS'in yeteneklerine ek olarak, tespit ettiği saldırıları otomatik olarak engelleyebilen sistemlerdir.
- **Güvenlik Bilgileri ve Olay Yönetimi (SIEM — Security Information and Event Management) Sistemleri:** Farklı güvenlik cihazlarından gelen günlükleri ve olay verilerini toplar, ilişkilendirir ve analiz eder. Bu sayede karmaşık saldırı paternleri tespit edilebilir ve uyarılar oluşturulur.
- **Veri Kaybı/Sızıntısı Önleme (DLP — Data Loss Prevention) Sistemleri:** Hassas verilerin yetkisiz kişiler tarafından dışarı çıkarılmasını veya paylaşılmasını engeller.
- **Uç Nokta Güvenliği (Endpoint Security):** Bilgisayarlar, sunucular ve mobil cihazlar gibi uç noktalarda zararlı yazılımları, yetkisiz erişimleri ve diğer tehditleri tespit ederek engeller.
- **Güvenlik Düzenleme, Otomasyon ve Yanıt (SOAR — Security Orchestration, Automation and Response) Sistemleri:** Güvenlik operasyonlarını otomatikleştirerek ve olaylara yanıt sürelerini kısaltarak güvenlik ekiplerinin verimliliğini artırır. SIEM sistemlerinden gelen uyarıları alarak otomatik yanıt senaryolarını tetikleyebilir.
- **Tehdit İstihbaratı Platformları:** Bilinen siber tehditler, saldırgan teknikleri, taktikleri ve prosedürleri (TTP'ler) hakkında güncel bilgiler sağlayarak, güvenlik ekiplerinin potansiyel saldırılara karşı daha hazırlıklı olmasını sağlar.
- **Davranış Analizi Sistemleri:** Kullanıcı ve varlık davranışlarını (UEBA — User and Entity Behavior Analytics) analiz ederek normalin dışındaki şüpheli hareketleri tespit eder.

d) Siber Savunma Birimleri ve Yetenekleri

Siber savunma birimleri, devlet kurumlarının, kritik altyapıların ve genel olarak bir ülkenin siber uzaydaki güvenliğini sağlamakla görevli, özel olarak eğitilmiş ekiplerdir.

Siber güvenliğin yönetim ve koordinasyonunda kilit rol oynayan kurumlar şunlardır:

- **Siber Güvenlik Kurulu:** Cumhurbaşkanı tarafından başkanlık edilen bir kuruldur.
- **Siber Güvenlik Başkanlığı:** Siber Güvenlik Kurulu'nun aldığı kararları uygulamaktan sorumlu olan bir başkanlıktır.
- **Bilgi Teknolojileri ve İletişim Kurumu (BTK):** Siber güvenliğin düzenlenmesi ve ulusal siber olaylara müdahale konularında önemli bir kurumdur.
- **Ulusal Siber Olaylara Müdahale Merkezi (USOM):** BTK çatısı altında faaliyet gösteren USOM, ulusal ve uluslararası siber tehditleri tespit etmek, izlemek, analiz etmek ve bertaraf etmek için kamu ve özel sektörle koordinasyonu sağlar.
- **Genelkurmay Başkanlığı (Türk Silahlı Kuvvetleri):** Askeri sistemlerin siber güvenliğinden sorumlu birimlere sahiptir. Daha önce Siber Savunma Komutanlığı gibi yapılanmalar kurulmuştur.
- **Emniyet Genel Müdürlüğü (Siber Suçlarla Mücadele Daire Başkanlığı):** Siber suçların tespiti, önlenmesi ve soruşturulması konularında adli ve kolluk faaliyetlerini yürütür.
- **Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK):** Milli kripto çözümlerinin geliştirilmesi, Ar-Ge faaliyetleri ve siber tehdit tespit sistemleri (honeypot) gibi konularda aktif rol oynamaktadır.

Sadece devlet kurumları değil , devlet kurumlarının yanında Türkiye'de siber savunmamızı geliştirmek için başka aktörler de bulunmaktadır, bunlar:

- **Siber Güvenlik Kümelenmesi:** Kamu, özel sektör ve akademi iş birliğini destekleyen, siber güvenlik ürün ve hizmetlerinin geliştirilmesini teşvik eden bir yapıdır.
- **Üniversiteler ve Araştırma Merkezleri:** Siber güvenlik alanında insan kaynağı yetiştirme, Ar-Ge projeleri yürütme ve bilimsel çalışmalar yapma konusunda önemli bir rol üstlenirler.
- **Özel Sektör Firmaları:** Siber güvenlik çözümleri geliştiren, siber güvenlik danışmanlığı ve hizmetleri sunan firmalar da ülkenin siber savunma kapasitesine katkıda bulunurlar.

e) Uluslararası İşbirliği ve Siber Diploması

Siber güvenlik alanı, küresel bir etki alanına sahiptir ve bu nedenle tek bir kurum veya kuruluş tarafından belirlenen kurallarla yönetilmesi mümkün değildir. Bunun yerine, dünya genelinde siber güvenlik kuralları ve standartları, çok paydaşlı bir yaklaşımla çeşitli uluslararası kuruluşlar, hükümetler, özel sektör, sivil toplum kuruluşları ve teknik topluluklar tarafından ortaklaşa oluşturulur ve geliştirilir.

Uluslararası Kuruluşlar ve Hükümetlerarası Yapılar

- Birleşmiş Milletler (BM)
- Uluslararası Telekomünikasyon Birliği (ITU)
- Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC)
- Avrupa Birliği (AB) Kurumları

-Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA)

-NIS Direktifi (Ağ ve Bilgi Sistemlerinin Güvenliği Direktifi) ve NIS2 Direktifi

-GDPR (Genel Veri Koruma Tüzüğü)

- NATO (Kuzey Atlantik Antlaşması Örgütü)
- G7/G20 Ülkeleri

Uluslararası Kuruluşlar ve Hükümetlerarası Yapılar Nedir?

-Birleşmiş Milletler (BM): Siber güvenliği uluslararası güvenlik gündeminin önemli bir parçası olarak ele alır. Özellikle Siber Alan Güvenliği Hükümet Uzmanları Grubu (GGE) ve Açık Uçlu Çalışma Grubu (OEWG) gibi platformlar aracılığıyla siber alanda sorumlu devlet davranışları ve uluslararası hukukun uygulanması üzerine tartışmaları yürütür.

-Uluslararası Telekomünikasyon Birliği (ITU): BM'nin uzmanlaşmış bir kuruluşu olan ITU, bilgi ve iletişim teknolojileri (BİT) alanında uluslararası standartlar geliştirir. Siber güvenlik, ITU'nun Küresel Siber Güvenlik Gündemi (GCA) kapsamında ele aldığı önemli bir konudur ve ülkelerin siber güvenlik kapasitelerini geliştirmelerine yardımcı olur.

-Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC): Bu iki kuruluş, geniş bir yelpazede uluslararası standartlar geliştirir. Siber güvenlik alanında özellikle **ISO/IEC 27000 serisi** (Bilgi Güvenliği Yönetim Sistemleri) ve **ISO/IEC 27032** (Siber Güvenlik Rehberi) gibi standartlar, kuruluşların bilgi güvenliği risklerini yönetmeleri ve siber güvenlik stratejileri oluşturmaları için temel oluşturur.

-Avrupa Birliği (AB) Kurumları: AB, siber güvenliği bölgesel düzeyde düzenleyen önemli bir aktördür.

-Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA): AB'nin siber güvenlik ajansı olarak görev yapar. Üye devletlerin siber güvenlik kapasitelerini artırmalarına yardımcı olur, risk değerlendirmeleri yapar ve siber güvenlik politikaları için tavsiyelerde bulunur.

-NIS Direktifi (Ağ ve Bilgi Sistemlerinin Güvenliği Direktifi) ve NIS2 Direktifi: AB genelinde ağ ve bilgi sistemlerinin yüksek düzeyde güvenliğini sağlamayı amaçlayan yasal çerçevelerdir. Kritik sektörlerdeki kuruluşlar için güvenlik gereksinimleri ve olay bildirim yükümlülükleri getirir.

-GDPR (Genel Veri Koruma Tüzüğü): Veri ihlallerinin bildirimini zorunlu kılarak ve kişisel verilerin korunmasına ilişkin sıkı kurallar getirerek siber güvenliği dolaylı olarak etkiler.

-NATO (Kuzey Atlantik Antlaşması Örgütü): Siber savunma kapasitelerini geliştirmeye ve siber saldırılara karşı kolektif savunma stratejileri oluşturmaya odaklanır.

-G7/G20 Ülkeleri: Bu ekonomik gruplar, siber güvenliği küresel ekonomik istikrar ve kalkınma açısından önemli bir konu olarak ele alır ve siber suçla mücadele ile siber alanda işbirliği konularında politikalar geliştirir.

- Ulusal Kuruluşlar ve Yasal Çerçeveler

-ABD — Ulusal Standartlar ve Teknoloji Enstitüsü (NIST)

-Çeşitli Ülkelerin Ulusal Siber Güvenlik Ajansları/Merkezleri (USOM, BSI)

- Sivil Toplum Kuruluşları, Sektör Birlikleri ve Teknik Gruplar

-ISACA, ISC^2, SANS Institute

-Cloud Security Alliance (CSA)

-FIRST (Forum of Incident Response and Security Teams)

-APWG (Anti-Phishing Working Group)

f) Sıfır Güven (Zero Trust) Yaklaşımı

Geleneksel BT ağ güvenliği, ağ içindeki herkese ve her şeye güvenir. Sıfır Güven mimarisi ise kimseye ve hiçbir şeye güvenmez.

Sıfır Güven güvenliği, özel bir ağdaki kaynaklara erişmeye çalışan her kişi ve cihaz için, ağ çevresinin içinde veya dışında olmalarına bakılmaksızın sıkı kimlik doğrulaması gerektiren bir BT güvenlik modelidir. ZTNA , Sıfır Güven mimarisiyle ilişkili ana teknolojidir; ancak Sıfır Güven, birkaç farklı ilke ve teknolojiyi bünyesinde barındıran bütünsel bir ağ güvenliği yaklaşımıdır .

Geleneksel BT ağ güvenliği , kale ve hendek kavramına dayanır . Kale ve hendek güvenliğinde, ağın dışından erişim sağlamak zordur, ancak ağ içindeki herkese varsayılan olarak güvenilir. Bu yaklaşımın sorunu, bir saldırganın ağa erişim sağladıktan sonra, içerideki her şey üzerinde tam kontrole sahip olmasıdır.

Kale ve hendek güvenlik sistemlerindeki bu güvenlik açığı, şirketlerin verilerinin artık tek bir yerde olmamasıyla daha da kötüleşiyor. Günümüzde bilgiler genellikle bulut sağlayıcıları arasında dağılmış durumda ve bu da tüm ağ için tek bir güvenlik kontrolü sağlamayı zorlaştırıyor.

Sıfır Güven güvenliği, ağın içinden veya dışından hiç kimseye varsayılan olarak güvenilmemesi ve ağdaki kaynaklara erişmeye çalışan herkesin doğrulama yapması gerektiği anlamına gelir. Bu ek güvenlik katmanının veri ihlallerini önlediği kanıtlanmıştır . Araştırmalar, tek bir veri ihlalinin ortalama maliyetinin 3 milyon doların üzerinde olduğunu göstermiştir . Bu rakam göz önüne alındığında, birçok kuruluşun artık Sıfır Güven güvenlik politikasını benimsemeye istekli olması şaşırtıcı değildir.

7) KAYNAKÇA

- https://cybermap.kaspersky.com/
- https://tr.wikipedia.org/wiki/Siber_sald%C4%B1r%C4%B1
- https://dergipark.org.tr/en/download/article-file/1114311
- https://organikinsan.com/siber-savaslar-ve-devlet-destekli-hacker-gruplari-dijital-tehditler-nereye-gidiyor/
- https://dergipark.org.tr/en/download/article-file/2811668
- https://www.anapaya.net/blog/top-5-critical-infrastructure-cyberattacks
- https://trguvenlikportali.com/wp-content/uploads/2019/11/SiberGuvenlik_SalihBicakci_v.1.pdf
- https://cahitcengizhan.com/siber-suclarin-kurumsal-ve-ekonomik-etkisi-2/
- https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/what-is-a-dos-attack-denial-of-service/
- https://tr.wikipedia.org/wiki/Malware#:~:text=Zararl%C4%B1%20yaz%C4%B1l%C4%B1m%2C%20k%C3%B6t%C3%BC%20ama%C3%A7l%C4%B1%20yaz%C4%B1l%C4%B1m,g%C3%B6stermek%20amac%C4%B1%20ile%20kullan%C4%B1lan%20yaz%C4%B1l%C4%B1md%C4%B1r.
- https://www.trendmicro.com/tr_tr/what-is/ransomware.html
- https://www.trendmicro.com/tr_tr/what-is/phishing.html#:~:text=Kimlik%20av%C4%B1%2C%20tipik%20olarak%2C%20siber,bunun%20oldu%C4%9Funun%20fark%C4%B1nda%20olmad%C4%B1%C4%9F%C4%B1nda%20etkilidir.
- https://www.cloudflare.com/learning/security/threats/zero-day-exploit/
- https://en.wikipedia.org/wiki/Supply_chain_attack
- https://www.forcepoint.com/tr/cyber-edu/advanced-persistent-threat-apt
- https://tasam.org/Files/Icerik/File/yeni_dunya_ekonomi_ve__guvenlik_mimarisi__IGK2019_5_(11)_pdf_45c49710-c0fc-4b5f-8688-7faf1998ee60.pdf
- https://www.scirp.org/journal/paperinformation?paperid=109997
- https://tr.wikipedia.org/wiki/Siber_sava%C5%9F
- https://pkf.com.tr/siber-saldirilar-savas-sucu-derinlemesine-bir-analiz/
- https://www.ollusa.edu/blog/cybersecurity-ethics.html

- https://www.cybersecurity.com.tr/kritik-altyapilarin-korunmasi/#:~:text=Kritik%20Altyap%C4%B1lar%C4%B1n%20Korunmas%C4%B1%20%C4%B0%C3%A7in%20Al%C4%B1nacak%20%C3%96nlemler&text=D%C3%BCzenli%20G%C3%BCvenlik%20Testleri%3A%20Sistemlerin%20g%C3%BCvenlik,kar%C5%9F%C4%B1%20etkili%20bir%20savunma%20sa%C4%9Flar.
- https://www.checkpoint.com/cyber-hub/cyber-security/what-is-threat-intelligence/
- https://www.bgasecurity.com/makale/siber-saldirilar-i%CC%87cin-erken-uyari-sistemi/
- https://www.cloudflare.com/learning/security/glossary/what-is-zero-trust/