Siber Terörle bir Mücadele Modeli

Kerem ERSOY

Kerem ERSOY

Sibernet Ltd Şti Genel Müdür

ISACA-Ankara Dernek Başkanı

CISA, CRISC, CISSP, ISO 27001 LA, CEH

Basit zarardan savaşa

Her şey nasıl başladı?

- 1990'ların sonunda Web hizmetleri yaygınlaşmaya başladı. 2000'lerin başında yeni bir kavram ortaya çıktı. Buna Web yüzünün değiştirilmesi (*Defacement*) deniliyordu. Bu tür eylemler sadece bazı kişiler yapabildiği için keyif olarak yapılan siber "***vandallık***" eylemleri idi.
- İlerleyen yıllarda dünya bilgisayar korsanları "Hacker"lar ile tanıştı. Yapılan eylemler tek bilgisayardan bir ağa bağlı tüm alt yapıyı etkiler hale geldi.
- 2010 yılına geldiğimizde ise dünya "***Stuxnet***" zararlı yazılımı ile tanıştı.
- Stuxnet aynı zamanda dünyanın ilk "***siber silahı***" olarak adlandırıldı.
- Stuxnet ile artık web üzerinden yapılan eylemler sanal alemde verilen zarardan ibaret değildi Fiziksel olarak ekipman ve tesislere zarar verilmesi gündeme getirdi.: İlk defa fark edildiğinde Iran'ın uranyum zenginleştirme tesislerinin büyük kısmı virüs tarafından kullanılmaz hale getirildi.
- Bu tür eylemlere "***vandalık***" değil "***siber-savaş***" adı verildi.

Kısaca Tarihçe

- Kısaca bir ülkenin, başka bir ülkenin elindeki ekipman, tesis ve imkanları bilgisayar ağları kullanarak tahrip etmesine "***siber-savaş***" deniliyor.
- Siber Terörizm ise daha farklı bir rota izledi. Siber Terörizm tanımı ilk defa 2000 lerde yapılmış olsa da günümüzde oldukça sık duyduğumuz bir kavram.
- Dünyada "***Siber Terör***" ün üzerinde anlaşılmış tam bir tanımı yok. Ancak kısaca "ağ kullanılarak gerçekleştirilen", "Terör" yani yıldırma eylemi olarak tanımlayabiliriz.
- Siber Terör eylemlerinin en bilinenleri ise:
  - 2013'de yapılan Sony saldırısı: Sony' ye ait filmlerin kontratları, Sony'nin iç yazışmaları ve Sony çalışanlarının maaşları, ailevi bilgileri, adresleri yayınlandı. Sony gerek filimler gösterime sokamaması ve gerekse ortaya çıkan veriler ile ilgili sorunlar yüzünden büyük bir kayba uğradı.
  - Sürüngen Ekibi adı verilen ve kendisini "Siber Terörist" olarak tanımlayan bir grup Sony ve XBOX ağlarını noel tatili öncesi dev bir DDoS saldırısı ile durdurdu. ToR Projesi günlerce kapalı kaldı.
  - Kuzey Kore saldırısında 9,5 gün boyunca tüm Amerika ağ alt yapısı, bankalar ve kritik servisler durdu.
  - Dyn Sitesine düzenlenen DDoS saldırısı yüzünden Facebook, Twitter, Netflix'in de aralarında bulunduğu yüzlerce dünya devinin sitelerine günlerce ulaşılamadı.
  - Son başkanlık seçimlerinde Rus hacker'lar ABD'deki elektronik seçim sistemine sızmayı başardı ve bazı bölgelerde seçim sonuçlarını etkilemeyi başardı.

Kısaca Tarihçe

- Türkiye de bu tür saldırıların yabancısı değil:
  - Aralık 2015'de Nic.TR' ye düzenlenen DDoS saldırısında Türkiye'deki pek çok siteye, hizmete özellikle bankalara günlerce ulaşılamadı.
  - Nisan 2016'da Anonymus MERNİS verilerini çalıp yayınlandı.
  - Nisan 2016' da tüm yurt çapında 1 günlük elektrik kesintisi oldu. Ülkede iletişim, ulaşım ve üretim sektörleri etkilendi.
  - Geçtiğimiz ay içerisinde elektrik altyapısına düzenlenen saldırı yüzünden pek çok ilde zorunlu elektrik kesintileri yaşandı.
  - Enerji ve Tabii Kaynaklar bakanı Amerika kaynaklı pek çok "siber terör" salsırısnın durudurlarak altyapıya yapının etkilenmesine engel olunduğunu duyurdu.

Siber Terörizm nedir ?

- Siber Terörizm konusunda dünyada üzerinde anlaşılmış bir tanım yok. Pek çok akademisyen ve organizasyon Siber Terör tanımı yapmaya çalışıyor.
  - FBI, NATO, Birleşmiş Milletler, AB tamamında değişik tanımlar söz konusu.
- Bunun önemi nedir?
  - Ortak planlar yapmak, kararlar almak, eylem yapmayı zorlaştırıyor.
  - Problem: Terörün özellikle de siber terörün global bir konu olması dolayısıyla etkin mücadeleyi zayıflatıyor.
- Bu sunum boyunca siber terörü Ağ üzerinden gerçekleştirilen terör eylemi şeklinde kabul edeceğiz.
- Konuyu Siber ve Terör olarak ayırmak tanım kolaylığı sağlıyor.
- Siber tehditlere karşı, siber güvenlik stratejisi gerekiyor.

Siber Terör Genel Tanımlar

- Terörü yapan kişiler, Teröristler gündeme geliyor.
- Terörist kısaca:
  - Politik bir ajandası olan,
  - Ya da belirli bir ülkenin çıkarları doğrultusunda hareket eden
  - Başka bir ülkedeki, ya da teroristin kendi ülkesindeki bazı gruplara kin güden
  - Onları ürkütmek, korkutmak ve böylece politik ajandasını onlara dayatmak, hareketlerini kontrol etmek, yaşam biçimlerini değiştirmek isteyen kişilere deniliyor.
- Ancak teröristlerin aksine "***siber terorist***" ler eylemi gerçekleştirdikleri yerde fiziksel olarak bulunmak zorunda değiller ve bomba ve silahlar yerine ağ ve iletişim sistemlerine sızmak, onların programlarını ve içeriklerini değiştirmek gibi yöntemler kullanıyorlar.
- Siber Terörizm ile mücadelede iki yöntem var:
  - Pasif Savunma
  - Aktif Savunma

Siber Terör Genel Tanımlar

- Kavramı alt parçalara ayırdığımız zaman siber terörizme karşı iki temel alanımız olduğunu görüyoruz:
  - Saldırılar iletişim ağları ve bilgi sistemlerine karşı yapıldığı için öncelikle "***siber savunma***" yapmak gerekiyor. "***Siber Savunma***" ağ ve kritik bilgi sistemlerinin dışarıdan gelen tehditlere karşı kuvvetlendirilmesi anlamına geliyor.
  - Ancak siber savunma yöntemleri *pasiftir*. Saldırganı engeller ya da yavaşlatabilir ancak saldırgana karşı aktif bir yaptırım uygulayamazlar.
  - Siber terör ile mücadele de tıpkı terörle mücadelede olduğu gibi:
    - Ortak eylem planı oluşturulması,
    - Faaliyetlerin koordine edilmesi (SIAM, SOME'ler oluşturulması vs.),
    - Önlem almak için gerekli çerçeve modellerin oluşturulması,
    - Gerekli yasal düzenlemelerin yapılması
    - Siber terör ulusal sınırları aştığı için yurtdışındaki benzer organizasyonlar ile ulusal düzeyde işbirlikleri yapılması

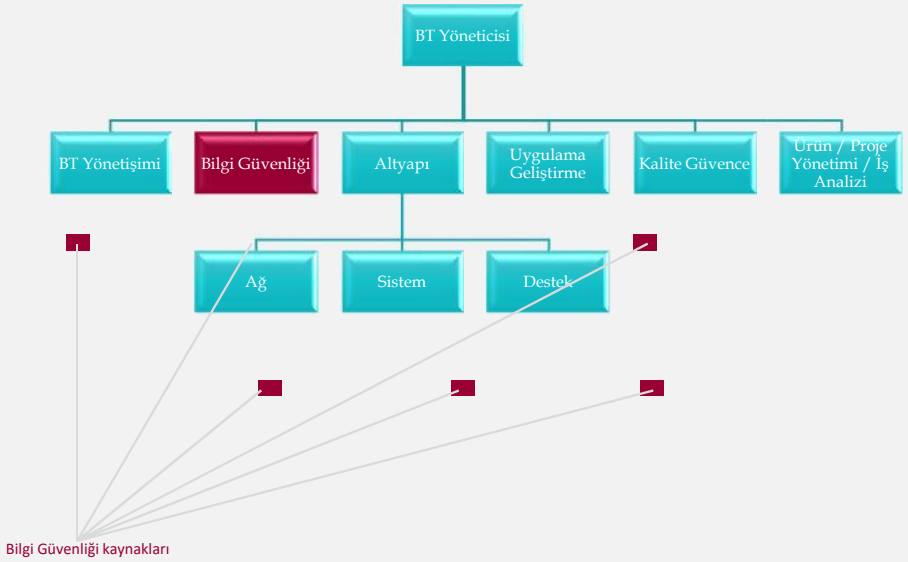
  gibi boyutları olması dolayısıyla devlet desteği olmasını gerektiriyor.
  - Devletin siber terörizm ile mücadelesi ise ***aktif mücadele*** olarak adlandırılır. Devlet saptanan terör saldırısını durdurma, yapanları cezalandırma ve/ve ya caydırma yetkisine ve gücüne sahiptir.

Alan 1 – Siber Savunma

- Öncelikle ister kamu, ister özel sektör olsun tüm kuruluşlarda siber güvenlik konusunda çalışan bir birim olmalıdır.

- Bu birim tüm diğer birimler ile bilgi alışverişinde olmalı.

- En önemli paydaşlar:
  - BT yönetişimi,
  - Uygulama Geliştirme,
  - Ağ yönetimi
  - Sistem Yönetimi,
  - Destek



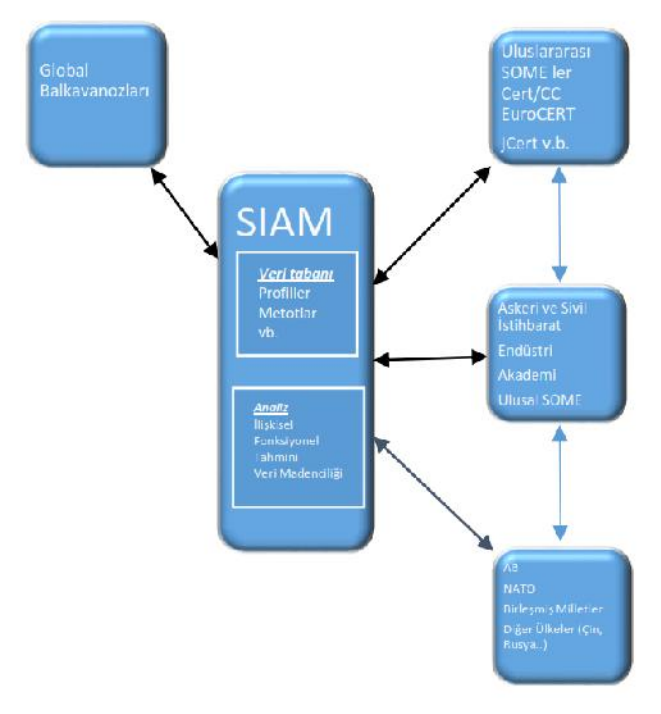
Alan 2 – Terör ile Mücadele

- Terörle mücadelenin diğer ayağı ise yasal düzenlemelerdir.
- Devlet seviyesinde organizasyon gerektirir.
  - Yurt içindeki teröristlerin bulunup yargılanması için hukuki düzenlemeler,
  - Ulusal eylemler için planlama ve kanuni düzenlemeler,
  - Ulusal ve uluslar arası kurumlar ile koordinasyon ve iş birliği sağlanması

  gibi düzenlemeler yapılması gereklidir.
- Gerekli düzenlemelerden bazıları:
  - Siber terörizmin, terör eylemi olarak ceza kanunlarında yerin alması
  - Siber Olaylara Mücadele Organizasyonu (SOME) için düzenlemeler
  - Siber İstihbarat Analiz Merkezi (SIAM) organizasyonu için kanuni düzenlemeler
  - Diğer ülkelerde bulunan uluslar arası kuruluşlar (AB, NATO v.b.), SOME ve SIAM lar ile ilgile devletler ile iletişim.

Alan 2 – Terör ile Mücadele Modeli

Siber İstihbarat Analiz Merkezi (SIAM)



Siber İstihbarat Analiz Merkezi (SIAM)

- Organizasyonda veri işleme için veri tabanı ve veri madenciliği olanakları ile ilgili uzmanlık gerekmektedir.
- Ulusal Paydaşlar ile iletişim SOME'ler, milli ve Askeri istihbarat, Akademi ve İş dünyasının temsilcileri yer alır.
- Uluslararası paydaşlar, organzasyon ve Devletler ile uluslararası SOME ler ile iletişim.
- Global olarak çalışan "***Bal Kavanozları***"ndan gelen bilgilerin değerlendirilmesi işlemleri yapılır.

Siber Terör ile Mücadele Problemler

- Global olarak kabul görmüş bir Siber Terör tanımı yok

- Ortak zeminde buluşma güçlükleri:
  - Terörist / Özgürlük Savaşçısı
  - Bir takım ülkelerin diğerlerine yapılan eylemlerin arkasında olamsı ve bizzt desteklemesi

- Global olarak kabul görmüş bir hukuki çerçeve yok:
  - Siber terör eylemleri nelerdir?
  - Verilecek cezalar ve sınırları
  - Caydırıcılık

Siber Terör ile Mücadele Global Çözüm Nedir?

- Uluslararası ilişkiler ve ortak platform ve dil geliştirilmesi:
  - Tanımlar (BM, AB konseyi)
  - Hukuki Çerçeve
- Altyapının sürekli taranması ve anormallik tabanlı izleme:
  - Altyapının izlenmesi ve denetlenmesi caydırıcı olabilir.
- Teknoljik altyapı yatırımları ile "Siber Güvenliğin" sürekli artırılması:
  - Yatırım ve altyapı gereksinimleri yüzünden gelişmekte olan ülkelerde uygulama güçlükleri oluşabilir.
- Siber Terörizm'in etkisi genel olarak ne olduğunun bilinmemesi ve bunun yarattığı korku:
  - Bilinçlendirme ve eğitim faaliyetleri
  - Siber güvenlik ve farkındalık programlarına entegre edilmeli
  - Tüm eğitim kurumlarında öğretilerek yaygınlaştırılmalı

Sorular / Öneriler ?

Teşekkürler