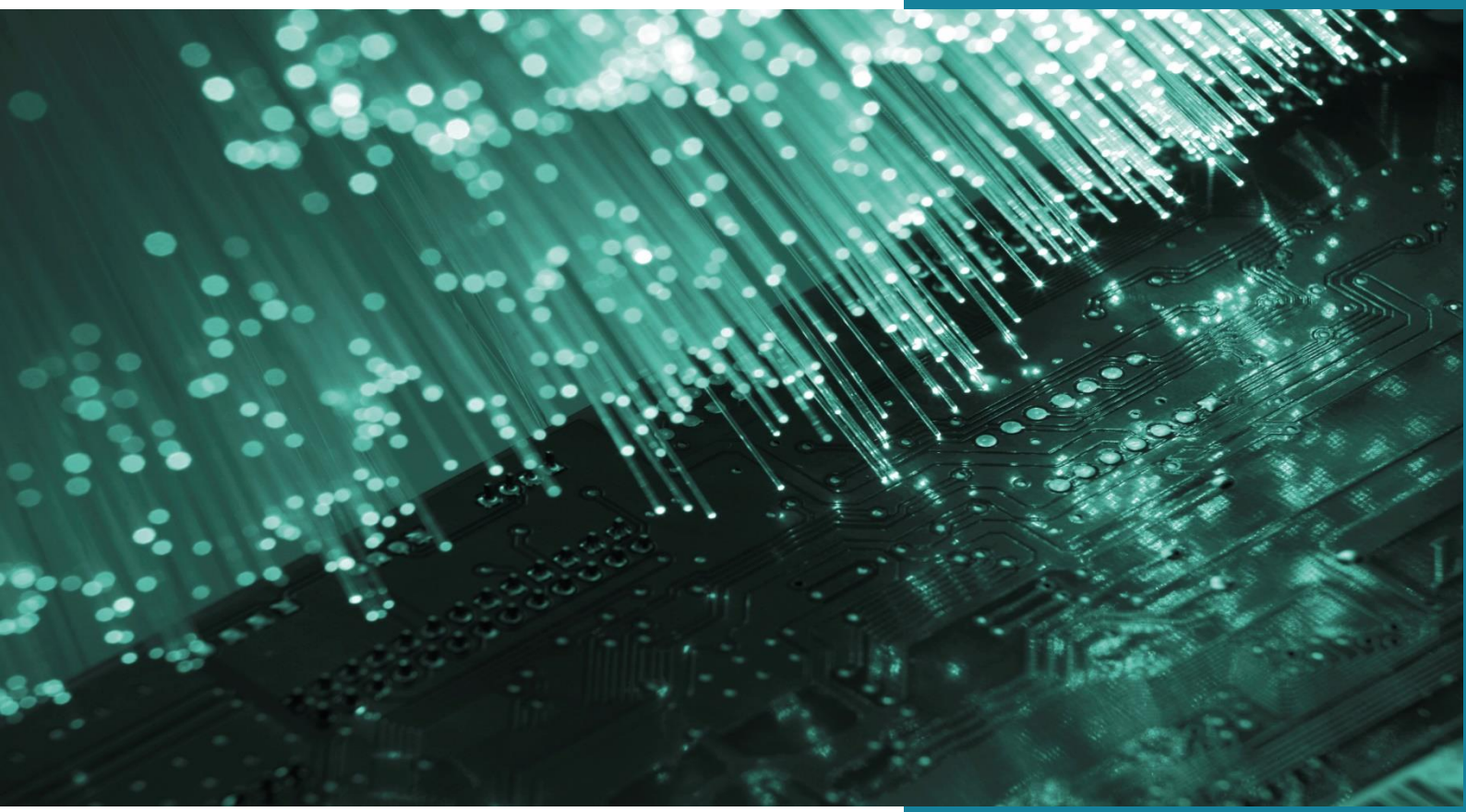
BİLİŞİM İNOVASYON DERNEĞİ

Siber Güvenlik Raporu



Hazırlayanlar

Ali KURTUL

M. Fatih ZEYVELİ

Yusuf İNCE

Kadir YILDIZ

Hüseyin YÜCE

Faruk YAKARYILMAZ

İçindekiler Tablosu

SİBER DÜNYADA BİLİŞİM GÜVENLİĞİ

GİRİŞ

Bilgi İşlem Teknolojileri, toplumu bir çok alanda etki altına alması ile birlikte kritik bir varlık olarak değerlendirilmiştir. Bu yüzden teknolojinin bu kadar etkin olarak kullanıldığı günümüzde, çeşitli problemler ile karşılaşılması kaçınılmazdır.

Bilgi güvenliği sadece kişisel bazda değil, toplumu oluşturan diğer kurumları da ciddi oranda ilgilendirmektedir. Firmalar ve devlet kurumları çerçevesinde bilgi ve bilişim güvenliği üzerinde kapsamlı çalışmalar yapılmakta ve bu konuda farkındalığın artırılması için çok ciddi araştırmalar yapılmaktadır.

Son zamanlarda bilişim sistemlerine ait saldırı ve güvenlik ihlalleri hızla artmaktadır. Yapılan araştırmalarda bilişim teknolojilerinin birer saldırı unsuru, kullandığımız sistemler de birer hedef haline geldiği vurgulanmıştır. Özellikle iletişim, banka hizmetleri, kamu faaliyetleri, savunma sistemleri, askeri sistemler ve ağ sistemleri gibi unsurlar ana hedef haline gelmiştir. Bu kapsamda bilgi güvenliğinin temel prensiplerine hâkim olma ve bunları pratik hayatta kullanmak oldukça önem kazanmaktadır.

Yaşamımızın her alanına derinlemesine giren teknoloji, sağladığı kolaylıkların ve faydaların yanı sıra bazı risk ve tehditleri de beraberinde getirmektedir. Bilgisayar ve ağlardaki açıklıkları fırsat bilerek sistemlerin çalışmalarına engel olmak, bilginin değiştirilmesine, çalınmasına, yok edilmesine zemin hazırlamak, maddi çıkar elde etmek amacıyla gerçekleştirilen siber saldırılar her geçen gün artmaktadır. Siber saldırıların hedefinde enerji, iletişim, sağlık, finans, barajlar, boru hatları gibi kritik altyapılar örnek verilebilir. Bu kritik altyapılara yapılan saldırıların boyut ve zararına bağlı olarak, zararın ve etkisinin sadece o sektöre olmayacağı, ayrıca paydaşlarının da etkilenebileceği aşikârdır. Yani risk ülkemizin bütünü ve bütünlüğü ile ilgilidir.

Bilişim İnovasyon Derneği olarak farkındalık oluşturma aşamasından teknoloji uygulamalarına kadar olan tüm süreçlere yönelik çalışmalarımızdan sadece biri olan bu raporun hedeflediği faydayı sağlamasını diliyoruz.

Siber Güvenliğe Giriş

SİBER GÜVENLİK KAVRAMLARI
SİBER GÜVENLİK

Tanımlara bakılarak; "siber" kavramı için, bilgisayar ve buna bağlı elektronik sistemlerden meydana gelen ortam, "bilişim" için ise bu meydana gelen teknolojik ortamlardan faydalanma anlamlarının çıkarılabileceği görülmektedir.

Siber güvenlik (Cyber Security); siber ortamda kurum kuruluş ve kullanıcıların varlıklarını korumak maksadıyla kullanılan araç, politika, güvenlik kavramları, risk yönetim yaklaşımları, güvenlik teminatları, faaliyetler, eğitimler, uygulamalar ve teknolojiler bütünüdür. Bu tanım kurum ve kuruluşların bilgi işlem donanımları, personel, altyapı, uygulamalar, hizmetler, elektronik haberleşme sistemleri ve siber ortamda iletilen ve saklanan tüm bilgileri kapsamaktadır *

SİBER SALDIRI

Siber saldırılar herhangi bir kullanıcının bilgilerini çalmaktan, ülkelerin stratejik önem arz eden sistemlerinin çalışmalarını engellemeye kadar çok geniş bir alanı risk altında bırakmaktadır. Bunun yapılması kasıtlı olabileceği gibi kasıtsız bir şekilde de olabilir. Siber tehditlerin virüs, casuslar, bilgisayar korsanları, terörist gruplar, yabancı ulusların istihbarat birimleri gibi birçok kaynaktan gelmesi muhtemeldir.

BULUT GÜVENLİĞİ

Bulut hayatımıza bir çok kolaylığı ile birlikte girdi. Masaüstünde yaptığımız işi, mobilden kullanabilmekte, arkadaşlarımızla paylaşabilmekteyiz.

Siber Sözcüğü

Siber sözcüğü "sibernetik" (Cybernetics) kelimesinin bir ön eki olarak kullanılmaktadır. "Siber" sözcüğü aynı zamanda kelimeyi kısaltmak amacıyla da kullanıldığı bilinmektedir.

Türkçede Siber Kavramı

Türkçede siber kavramının karşılığı olarak "bilişim" kelimesinin kullanıldığı görülmektedir.

Türkçede "Bilişim" kelimesinin ifade ettiği anlam;

"İnsanların teknik, ekonomik ve toplumsal alanlardaki iletişimlerinde kullandıkları, bilim dayanağı olan bilginin, özellikle elektronik makineler aracılığıyla düzenli ve akılcı biçimde işlenmesi, bilginin elektronik cihazlarda toplanması ve işlenmesi bilimi" dir. *

Bulut teknolojisi bireyler ve kurumlara bir çok avantaj sağlamaktadır. Her yerden erişilebilen bu servisler ve verilerin yeterli güvenlik tedbirleri alınmadığı takdirde yetkisiz kişiler tarafından erişilebilir hale gelebileceği bilinmektedir. Hatta internet var olduğundan beri evrilerek gelişen her türlü tehlikenin bulut içinde mevcut olduğu söylenebilir.

Bulut teknolojisinin güvenlik kavramına kattığı yeni boyutlardan bahsetmek gerekirse, bulut öncesi dönemde kullanılan sistemleri, verileri kullanacak kişileri ve sistemler ile bağlantı şekillerini yönetebilme imkânı bulunuyorken artık herkesin her yerden erişebileceği, mobilitenin ön planda olduğu, hatta internetteki sistemler arası ilişkilerin yoğunlaştığı bir mimari ile karşı karşıya olunduğu göze çarpmaktadır. Bunun yanında bu verilerin bu kadar erişilebilir olması kötü niyetli kişileri de bu sistem ve verilere ulaşma konusunda daha hevesli ve etkili hale getirmiştir. Hatta bazen güvendiğiniz ve verileriniz emanet ettiğiniz firmanın basit bir hatası çok gizli verilerinizi herkese açık hale getirebilir. *

IOT GÜVENLİĞİ

IoT; bireysel tarafta giyilebilir cihazlar, sağlık gereçleri, akıllı ev ürünleri gibi değişik formatlarda karşımıza çıkmaktadır. İnternete bağlı sağlık gereçleri saldırıya açık hale gelmekte, evlerimizdeki akıllı televizyonlar mahremiyetimiz için tehdit oluşturabilmekte, akıllı araçlarımız ise birer güvenlik tehdidi haline gelmektedir.

Kalp pilleri hacklenebilmekte, insulin pompaları sadece 20$'lık cihazlarla devre dışı bırakılabilmektedir.

Wired sitesi bir grup hacker ile yaptığı testte bir aracın kontrolünün uzaktan tamamen ele geçirilebileceğini ve

Siber Savaş Kavramı

1990'ların başında ABD-Pentagon'da BİT sistemlerinin yaygın bir şekilde savunma sistemlerinde kullanılmasının meydana getirdiği zafiyetler konusunda endişeler dile getirilmesiyle başlamıştı. Richard A. Clarke, Robert K. Knake'in "Siber Savaş" adlı kitabında; 1994 yılında ABD savunma bakanlığı ve istihbarat organizasyonları arasında "Ortak Güvenlik Komisyonu" kurulduğunu. Bu komisyonda ağ teknolojilerinin gelişmesinin riskleri derinlemesine incelendiğini belirtmekteydi Komisyonun sonuç raporunda ise üç ana başlıktan bahsedilmekteydi;

"Bilişim sistemleri teknolojisi, bilişim sistemleri güvenliği teknolojisinden daha hızlı ilerliyor."

"Bilişim sistemlerinin ve ağlarının güvenliği bu on yılın en önemli güvenlik sorunu ve bu alanda karşılaşılan riskler konusunda yeterli bilince sahip değiliz."

"Pentagon'un yanında, özel sektöründe bilişim sistemlerine bağımlılığı ülkenin tamamının zayıflığını artırıyor."

araçların teknoloji kullanımının artmasıyla beraber bu tarz saldırılara açık hale geldiklerini ortaya koymuştur. (Greeenberg). 2014'te yayınlanan "Red Button" açığı ile milyonlarca akıllı TV'nin saldırıya açık olduğu ortaya çıkmıştır. *

Bunun yanında hastanelerde çalışmakta olan bir çok sağlık cihazı regulatif nedenlerle ve /veya firmaların izin vermemesi nedeniyle, çok eski işletim sistemleriyle kullanılmaktadır. Bu cihazlar, kritik bir çok güvenlik güncellemesi yapılmadığından, virus ve zararlı yazılımların saldırılarına açık bir şekilde çalışmaktadırlar

BÜYÜK VERİ / BİG DATA

Büyük veri; sosyal medya paylaşımları, ağ günlükleri bloglar, fotoğraf, video, log dosyaları vb. gibi değişik kaynaklardan toparlanan verilerin tamamının, anlamlı ve işlenebilir biçime dönüştürülmüş haline denir.

Siber güvenlik ile büyük veri ayrılmaz ikili olarak ortaya çıkmaktadır. Bu etkileşim her iki taraf açısından önemlidir. Siber güvenlik; öncelikle tüm etkileşimli cihazlardan toplanan bilgilerin ve güvenlik zafiyetleri ile ilgili bilgi, analiz ve yorumların saklanması ve anlamlandırılması için büyük veri teknolojilerine ihtiyaç duyar. Diğer açıdan bizzat büyük veri çözümlerinin bulut ortamında hizmet sunmaları nedeniyle, oluşan veri güvenlik zafiyetlerinin elden geçirilmesi, yorumlanması ve analizi de siber güvenlik açısından gereklidir.

KRİTİK ALTYAPI

İşlevlerini, kısmen veya tamamen, yerine getir(e)mediğinde, toplumsal düzenin sürdürülebilirliğinin ve/veya kamu

Kritik Altyapı

Bir kritik altyapı bileşeninin değeri, aşağıdaki üç parametre göz önüne alınarak tespit edilmelidir:

- Devre dışı kalması halinde oluşacak zararın büyüklüğü,
- Bu zarara yol açması muhtemel açıklıklar,
- Bu açıklıkları kullanabilecek tehditlerin gerçekleşme olasılığı.

Kritik altyapılarda kullanılacak olan risk analizi metodolojisinin belirlenmesi önemli bir kazanım olacaktır.

Bu değerlendirme temel alınarak oluşturulacak envanterde, oluşan zararın büyüklüğünün, açıklık miktarının ve tehdit olasılıklarının en aza indirgenmesi amacıyla uygulanacak risk hafifletme planları oluşturulmalı, bu planların başarısı ve uygulanması yakından takip edilmesi gerekmektedir.

Kamu kurum ve kuruluşları ile kritik altyapılarda bulunan verilerin kişisel veri, kritik altyapı verisi ve gizli veri olarak sınıflandırılması ve gizlilik seviyelerine uygun olarak bu verilerin saklanması ve paylaşılması gerçekleştirilmesi sağlanmalıdır.

hizmetlerinin sunumunun olumsuz etkileneceği ağ, varlık, sistem ve yapılar bütünü kritik altyapı olarak adlandırılmaktadır.

Telekomünikasyon, bankacılık ve finans, ulaştırma, enerji, sağlık hizmetleri, su yönetimi ve barajlar, kritik kamu hizmetleri, kritik üretim / ticari tesisler, tarım ve gıda ile kültür ve turizm Türkiye mevzuatında kritik altyapılar olarak tanımlanmıştır.

TEKNOLOJİ VE MAHREMİYET

İş ve süreçlerinin etkili ve verimli yapılmasına olanak sağlayan iletişim ve bilgisayar tabanlı bütün sistemleri kapsayan bilgi teknolojileri kavramı, bilgisayar teknolojisi ile sağlanabilen bilgi hizmetlerinin tamamı için kullanılabilmektedir. Dolayısıyla günlük yaşamın vazgeçilmez bir parçasıdır.

Bilgisayar teknolojisindeki gelişmelerin ise toplumlar üzerine doğrudan etkisi bulunmaktadır. Bu yüzden toplumların ekonomik refahından, sanayisine, sağlıktan eğitime kadar birçok alanda pozitif etkilerini gözlemlemek mümkündür.

Teknolojinin hayat ile olan bu iç içeliği ve sağladığı kolaylıkların yanı sıra gelen güvenlik boyutu farklı bir açıdan değerlendirilmesini kaçınılmaz kılmıştır, şöyle ki; insanlık tarihinin ilk çağlarından beri insanoğlu üç temel şeye ihtiyaç duymuştur. Yiyecek , barınma ve kendini güvende hissetme ihtiyacı. Dünya üzerinde her dönem güvenlik adına yeni yöntemler geliştirilmeye çalışılmış ve kurulan her devlet öncelikle kendini güvene alma ihtiyacı hissetmiştir.

Güvenliği ihmal etmenin diğer söyleniş şekilleri

“Bizim alnımız açık; gizlimiz saklımız yok.”

“Zaten herkesin her verisine ulaşılabiliyor.”

”Güvenlik önlemleri iş yapmamızı engelliyor.”

Bu güne kadar internetin gücü sürekli göz ardı edildi fakat 3G özelliği ile mobil cihazlarda internet kullanımı artmasıyla bilgi hırsızlığı, dolandırıcılık gibi olaylar artmaya başladı ve bu da güvenlik ihtiyacını doğurdu. 4.5G hızla hayatımıza girdi ve gelecek 1-2 yıl içerisinde internet ihtiyacımız şimdiye kadar olan ihtiyacımızın en az 10 katına çıkacak.

Her kurumun ve kişinin bilgileri gizlidir. Kişisel ve ticari bilgilerin sır olarak saklanması gerekir. Örneğin bir firmanın ihale ile ilgili teklifleri, müşteri listesi, karlılığı ticari sırdır ve özenle saklanması gerekir.

Birçok kurum bilişim güvenliği ile ilgili danışmanlıklar ve önlemler almakta, ama alınan bu önlemler ve bilişim güvenliği kuralları işi yavaşlattığı nedeniyle delinebilmektedir.

Günümüze gelindiğinde ise güvenlik sıkıntıları ciddiyetini artırarak devam ettirmektedir. Teknolojinin gelişmesiyle beraber mahremiyet azalmıştır. Artık yazılımsal ve donanımsal cihazlarla dinleme ve izleme faaliyetleri çok kolay hale gelmiştir. Günümüzde de hem dünya basınında hem Türkiye basınında dinleme ve izleme faaliyetleri geniş yer bulmuştur. Özellikle Edward Snowden tarafından NSA'in internet, GSM ve uydu izleme altyapılarını basına sızdırmasından sonra güvenlik algısı baştan yazılmak zorunda kalmıştır. Cep telefonlarındaki merkezi denetim internet altyapısında mümkün olmadığından internet üzerinden suç işlemek çok daha kolaylaşmıştır ve teknik takibi bir o kadar zor olmaktadır.

Mahremiyet konusunu önemseyenler olduğu kadar önemsemeyen kitle de ciddi miktarda fazladır. Fakat insanın fıtratı gereği mutlaka mahrem kalması gereken bilgi ve verileri vardır ve önemsemediğini iddia eden kişiler bile bu konularda hassasiyet göstermelidirler. Bunu yanında modern batı ülkelerinin mahremiyet yaklaşımları çok farklıdır. Çoğu ülkede psikolojik itaat sistemi oluşturmak adına siyasi olarak sürekli izlenme algısı oluşturularak toplumu belli bir yönde kanalize etme yöntemini kullandıkları bilinmektedir.

Kişilerin neyi sevip neyi sevmediği, arkadaşlarının kimler olduğu, kendinin ve arkadaşlarının nerede yaşadığı, ne yediği, hastalıklarının neler olduğu, nerede ne zaman ne yapacağı bilinebilmektedir. Bu bilgiler art niyetli kişiler tarafından kullanıldığında çok tehlikeli sonuçlara sebep olabilir.

Günümüzdeki birinci sınıf dünya ülkeleri bugün siber güvenliğe ciddi miktarlarda yatırım yapmaktadır (ABD 19 Milyar $) ve devletler bu yatırımları ciddiye almazlarsa gelecekte kendilerini geri dönüşü olmayan bir çıkmazın içerisinde bulabilirler.

Bilginin yetkisiz kişilerin erişimine kapalı olması; mahremiyet (confidentiality) ve gizliliğin sağlanması bilişim güvenliğinin birinci kuralıdır.

SİBER SAVAŞ HUKUKU

Ortak savunma anlayışının siber alanda da geçerli olduğu fikri ve girişimi bir çok uluslararası belgede ifade edilmiştir. Estonya'nın başkenti Tallinn'deki CCDCOE'nin bir grup uzmana yazdırdığı ve 2013 yılında tamamlanan "Siber Savaşta Geçerli Uluslararası Hukuk üzerine Tallinn Makaleleri" adlı rapor bilim adamı ve uzmanların olması gerekeni değil cari uluslararası hukuku baz alarak konuya ilişkin yaptığı değerlendirmelerini yansıtmaktadır. Temel olarak siber ortamdaki savaş hukukunu analiz etmekte; "kuvvete başvurma hakkı" (egemenlik, devletin sorumluluğu, güç kullanımının yasaklanması ve meşru müdafaa, vb. konuları) ve "savaşta geçerli kurallar"ın (tarafsızlık hukuku, meşru hedefler, orantılılık,) siber alana nasıl uyarlanacağını incelemektedir. Rapor mevcut uluslararası hukuk düzenlemelerinde siber ortama yer verilmediği için ancak yeni anlaşmalar yapıldıktan sonra bu yeni alanın uluslararası hukuk düzenlemelerine tabi olabileceği nosyonunu reddetmektedir. Uluslararası savaş hukukunda geçerli kurallar siber ortamda da aynen geçerlidir.

Ülkemizde ve dünya genelinde internetin yaygınlaşması ve mobil cihazların akıllanmasıyla artık her bireyin internet üzerinden teknik takibinin yapılması mümkün hale gelmiştir. Yani cebinde akıllı cep telefonu olan her vatandaşın anlık mesajlaşmaları, telefon konuşmaları, GPS özelliği ile gün içerisinde bulunduğu lokasyonlar, çektiği fotoğraflar başta olmak üzere tüm hayatının izlenebilmesinin mümkün olduğu anlamına gelmektedir.

Toplanan bu bilgiler istihbarat, ticaret ve dolandırıcılık alanında kullanılabilir. Hatta düzenli olarak toplanan bu bilgiler toplum hakkında genel istatistikleri çıkarıp topluma yönelik istismar hareketleri gerçekleştirilebilir.

Örneğin insanların çoğunlukla ne tür yerlere gittiği, ne tür yiyeceklere yöneldiği, hangi hastalıkları barındırdığı gibi hayal gücüyle sınırlı olan her veri toplanıp işlenebilir.

Siber Riskler ve Yaşanmış Olaylar

SİBER SALDIRILAR VE TEHDİTLER

2016 yılı ile saldırılar daha yetenekli daha karmaşık ve daha yaratıcı hale geldi. Information Security Forum (ISF) tarafından, "2015 biterken 2016 yılında da siber tehditlerin büyüklüğü, şiddeti ve karmaşıklığın artması" dile getirilmiştir. Ayrıca kurum yetkililerinin belirttiği **2016 yılının siber risk yılı olacağı** tahmini büyük oranda doğrulanmıştır. *

Aşağıda listelenen tehdit türlerinin günümüz ve yakın geleceğin siber güvenliğini şekillendireceği söylenebilir.

SİYASİ SEBEPLİ SALDIRILAR

2015 yılının bilişim güvenliği risklerine baktığımızda dikkat edilmesi gereken ilk nokta ülkeler arası politikanın pek çok kamu ve özel sektör kuruluşların yüzleştiği siber tehdidin şekil ve şiddetinin temel belirleyicisi olduğudur.

Ülkeler arası ilişkilerde, siber caydırıcılığın 21. yüzyıl diplomasisinin bir aracı olacağı gittikçe daha açık hale gelmektedir.

Siber caydırıcılık vakaların aynı zamanda ticari işletmeleri hedef alması şirketleri telaşlandırmaktadır. İnternet artık modern toplumların omurgası haline gelmiştir.

Özellikle kritik altyapıların ulus-devletlerin caydırıcılık siber saldırıların yükünü taşımaları muhtemeldir. Kritik altyapılara yönelik siber saldırılarla gerçekleşebilecek kıyamet senaryoların gerçekleştirilme ihtimalleri çok azdır ama her şeye rağmen tehdit gerçek ve büyümeye devam etmektedir.

Risk Budur!

Siber tehditler geliştikçe ve daha sofistike oldukça, BT sistemlerinin güvenliğini sağlamak her zamankinden daha önemli hale gelmektedir. Hızla gelişen ve "Bulut", "Büyük Veri", "Nesnelerin Interneti" gibi yeni alanlara kayan bilişim dünyasının 2017 yılında ve sonrasında bu hızlı değişimin getirdiği güvenlik açıkları ile mücadele ettiği / edeceği söylenebilir. Ayrıca mobil ve kişisel cihazların yaygınlaşmasının (BYOD) kontrolü daha da zorlaştıracağı riski bir çok kurumun risk yönetim dokümanlarına girmiş durumdadır.

ABD – Çin Rusya

ABD şu anda doğrudan devlet tarafından işletilen medya kuruluşları ile bağlantılı web siteleri aracılığıyla resmi siber caydırıcılık politikasının inceliklerini ayarlarken, Çin askeri açık-açık siber orduyu kullanacağını belirtmiştir. Diğer taraftan Rusya, düzenli olarak stratejik rakiplerin ve eski müttefiklerin karar almalarını şekillendiren ve cezalandıran görünümlü misilleme operasyonlarıyla, siber caydırıcılık anlayışını zaten eyleme geçirmiştir. Aynı şekilde Kuzey Kore kendine yeten internet altyapısının dış siber saldırılardan göreceği zararı azaltmak ve hamle üstünlüğü elde etmek için belli düşmanlara karşı misilleme saldırılarında bulunmaktadır.

Siber Savaşların Yönü

Eskiden İran - ABD veya İran - İsrail arasında yoğun siber saldırılar beklenmekte idi. Şimdi İran - ABD Arası yakınlaşma ile bu beklenti azaldı. Ülkeler arası krizlere göre siber tehditlerin yönü değişebiliyor.

Mesela Şii din adamı Nimr al-Nimr'in Arabistan'da 2 Ocak 2016 da idam edilmesi ile 3 Ocakta askıya alınan İran - Suudi Arabistan diplomasisinden sonra Suudi Arabistan'a yönelik saldırıların artması bekleniyordu. *

Bu haberden birkaç ay sonra ABD'li ağ güvenliği şirketi Palo Alto araştırmacılarının açıklamasına göre, kendilerini OilRig diye adlandıran bir siber casusluk topluluğunun Suudi Arabistan'ın mali ve savunma amaçlı teknolojik kurum ve kuruluşlarını hedef aldığı belirtildi. *

UYGULAMALARIN BİLİNEN GÜVENLİK AÇIKLARI

Uygulamalarda bulunan güvenlik açıkları BT departmanları için en büyük tehditlerden biridir.

Yazılımların düzenli olarak güncellenmesi gerekir. Tüm yazılımların dışarıya açılan yönlerinin güvenlik kontrollerinin yapılması gerekir.

MOBİL CİHAZ RİSKLERİ

Mobil cihazlar hızla gelişmektedir ve birbiri ile yarışan üreticiler fazla kontrol yapamadan hızla yeni ürünler piyasaya sürmektedirler. Bu hız birçok güvenlik açığını beraberinde getirmektedir. Ayrıca mobil cihazlar üzerine kurulan uygulamalar da hem kişisel veriler için hem de kurum uygulamaları için ciddi tehdit olmaktadır. Hem ev (çocuklar ve oyun) hem de iş için kullanılan uygulamalar kurumlar için tehdit haline gelmiştir.

Uygulamaların Güvenlik Açıkları

HP'nin 2015 Siber Risk Raporu, 2014'de yaşanan ihlallerin %44'ünün iki ile dört yıllık güvenlik açıklarından kaynaklandığını tespit etti. Bu, sıkıntının ne kadar büyük olduğunu göstermektedir. *

Türkiye'de Fidye Yazılımları

Genellikle sosyal mühendislik tekniklerin de faydalanır. Ülkemizde CrypteLocker virüsü Turkcell, Türk Telekom Faturası gibi görünerek bir çok kullanıcıya ciddi zararlar verdi ve vermeye devam ediyor. Geçtiğimiz yıl birçok kişi fidye ödeyerek bu tür saldırganlardan verilerini geri aldı. Bu fidye kazancının artmasından dolayı bu tehditlerin bu yıl artması bekleniyor. *

FİDYE YAZILIMLARI (RANSOMWARE)

Fidye yazılımın etkisinin 2016 yılının ilk çeyreğinde arttığı göze çarpmaktadır. En son CryptoWall v3 tehdidi dünya çapında yüzbinlerce kullanıcıya 325 milyon ABD dolarına mal olmuştur. Bu tür saldırı; önemli dosyaları şifreleyip, fidyeyi ödeyene kadar verilere erişim engeller.

HEDEF ODAKLI KİMLİK AVI

Siber Suçlular en az direnç gösterecek olan yolu seçerler. Genellikle sizin değerli verilerinize ulaşmalarının en kolay yöntemi, içerden birisini anahtarları teslim etmesi için kandırmaktır. Akıllı bir kod ile değil, bir telefon veya maille insanlar kandırılabilmektedir. Resmi görünümlü mesajlar ve web siteleri arttıkça veya güvenilir kaynaklardan geliyormuş görünümlü iletişimler oldukça, kimlik avları devam edecektir.

Çözüm için sadece potansiyel hedefleri tehlikeler hakkında eğitmek yeterli değildir. Gerçek zamanlı gözlemleme ve tarama sistemleri ile engelleme sistemleri ile farkındalık eğitimlerini de içeren bütünleşik bir bakış açısı gerekmektedir.

IoT RİSKLERİ

Henüz ülkemizde çok yaygınlaşmamış olsa da çeşit çeşit mobil cihazlar ve giyilebilir teknolojik cihazların kullanılmaya başlandığı görülmektedir. Bu cihazların her biri siber suçlular için yeni potansiyel açıklar sunar.

Nesnelerin İnterneti sadece mobil ve giyilebilir cihazlar anlamına gelmemektedir. Hemen her türlü cihaz yavaş yavaş ağa bağlanmaya başlamıştır. Bağlanabilirlik,

Hedefe Yönelik Kimlik Avı

Özellikle yüksek güvenlik yetkisine sahip olanların veya üst düzey yöneticilerin hedeflenmesi artıyor. Örneğin, siber suçlular bir CEO'nun hesabına girebilirlerse, hasara yol açıp hassas verileri ifşa edebilirler.

Buluttaki Güvenlik Riskleri

Bulut (Cloud)'da bulunan kullandığımız hizmetler arttıkça, BT departmanları gözetim ve kontrollerini kaybedebilmektedir. Çalışanlar ihtiyaç duydukları hizmetleri BT'yi atlayarak almakta ve bu süreçte güvenlik protokolleri ve sistemleri gözardı edildiğinden ciddi bir tehlike oluşmaktadır. Bazen de kullanılan bulut hizmetlerin güvenliği hizmetinin BT tarafından verilmesi istenmekte, bu hem BT yükünü artırmakta hem de dış ortamlardaki sistemleri kontrol etmek çok zor olmaktadır.

hayatımızın ve işletmelerin her köşesine yayılırken, veri kontrolü çok daha zor hale gelmektedir.

Nesnelerin İnterneti bazı heyecan verici iş fırsatların habercisi olabilir, ama sınırlı ve güvenli erişim sağlamak konusunda dikkatli olmamız gerekir. Hassas veriler şifrelenmeli, erişimi kısıtlanmalı ve erişimlerin izlenmesi gereklidir. Kurumsal cihazları yönetmek ve gerektiğinde erişimlerini engelleyebilmek önemlidir.

YAŞANMIŞ GLOBAL SALDIRILAR

XKeyscore, PRISM, ECHELON, Carnivore, DISHFIRE, STONEGHOST, Tempora, Frenchelon, Fairview, MYSTIC, DCSN, Boundless Informant, BULLRUN, PINWALE, Stingray ve daha ismini bile bilmediğimiz onlarca gizli proje…

11 Eylül 2001'de ABD'de ikiz kulelere ve diğer birçok hedefe yönelik olarak gerçekleştirilen terör saldırıları, teröristlerin internet ve dijital ortamdan etkin bir şekilde yararlanmış oldukları gerçeği ile birlikte, bir ülkeye yönelik gerçekleşmesi muhtemel bir dijital "Pearl Harbor" saldırısı ile ortaya çıkabilecek "dijital felaket" senaryolarının ciddiyetle konuşulmasını sağladı. Siber saldırılarla devletlerin kritik altyapılarına verilebilecek zararın milli güvenlik endişeleri ile ilişkilendirilmesi ile birçok ülke siber güvenlik stratejilerini ulusal güvenlik belgelerine eklediler.

ESTONYA ÖRNEĞİ

Estonya, yaygın internet kullanımı, günlük hayatta bir çok kamu ve özel hizmetin, altyapı hizmetlerinin internet

Bilgi ve Bilginin Gücü

Beyaz Saray'ın Siber Güvenlik Danışmanı olan Richard Clarke'ın sözleri durumu özetler niteliktedir;

"Casusluk artık çok kolaylaştı. Eskiden Washington'daki Rus Elçiliği'nde çalışan bir KGB ajanının bir FBI ajanı ayartması çok zordu. Ama şimdi Moskova'da oturuyorsun. Ve hiçbir risk olmadan binlerce sayfa çalabiliyorsun. Eskinin casuslarına artık gerek yok. Eskiden Sinop'ta büyük bir kulemiz vardı. Rusya'daki konuşmaları dinliyorduk. Ama şimdi buna ihtiyaç yok. Kimse radyofrekansı kullanmıyor. Ulusal Güvenlik Ajansı'nın (NSA) Maryland'deki kampüsünden bütün dünyadaki internet trafiğini izliyoruz. Bu konudaki bütçe Pentagon'a ait olduğundan, NSA ve Pentagon neredeyse tek bir kuruluş gibi çalışıyor. Amerikalı asker Sinop'a gitmesine gerek kalmadan her işini masasından halledebiliyor." *

Bu yaklaşımın gerçek dünyadaki yansımalarına gelince;
Dünya ülkelerinin maruz kaldığı ilk kayda değer siber saldırıların tarihinin 90'lı yılların sonlarından başlatılabileceğini söylenebilir.

üzerinden sunulması ile dünyada siber bağımlılığı en yüksek ülke olarak kabul edilmektedir. Rusların Estonya'ya karşı 27 Nisan 2007 tarihinde başlattığı siber saldırılar değişen şiddet seviyelerinde 23 Mayıs 2007 tarihine kadar devam etti. Internet üzerinden verilen kamu hizmetlerini çalışmaz duruma getiren saldırılara karşı önlem olarak Estonya hükümeti yurtdışı internet iletişim kapasitesini 2 Gbps'ten 8 Gbps'e çıkardı. Kamu ve özel sektör kuruluşları sunucu ve iletişim kapasitelerini artırarak saldırıları göğüslemeye çalıştılar. Estonyanın NATO'dan yardım istemesi ile oluşturulan çeşitli yardım ekipleri Estonya'da görev yapmaya başladılar.

Estonya'nın yanısıra Almanya, İtalya, Letonya'nın katılımıyla CCD COE kurulmuştur. NATO'nun 2008 yılındaki Bükreş zirvesinde siber savunma siyaseti kabul edilerek bunu geliştirecek yapılar ve gerçekleştirecek otoriteler oluşturulmasına karar verildi. Zirveden sonra NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority) Brüksel'de kurulmasına karar verildi. Bunun yanısıra Ekim 2008'de NATO bünyesinde Estonya Tallinn merkezli Siber Savunma İşbirliği Mükemmeliyet Merkezi (CCD COE - Cooperative Cyber Defence Centre of Excellence) kuruldu.

Estonya, Gürcistan ve daha sonra Ukrayna'ya yönelik siber saldırılarda yoğun olarak kullanılan DDOS (Distributed Denial of Service - Dağıtık Servis Dışı Bırakma) saldırıları sunucu kapasitelerinin ve ağ kaynaklarının doldurularak hizmet veren sistemlerin hizmet veremez duruma getirilmesidir. Zararlı yazılımlar

Estonya Saldırıları ve Siber Milat

Estonya'ya yönelik siber saldırılar uluslararası güvenlik bakımından bir milat oldu. Estonya saldırısından sonra siber saldırılar ve savaşlar konusunu gündemlerine aldılar. Siber saldırının hangi durumlarda kanuna karşı bir suç olarak değerlendirilip hangi durumlarda savaş sebebi sayılacağı konusu tartışmaları yapılmaya başlandı. Siber saldırıların savaş sebebi (casus belli) sayılabileceği hususu daha sonra 2012 yılında ABD başkanı Obama tarafından açıkça dile getirildi.

Daha güçsüz Bir Örnek; Gürcistan

Ağustos 2008'de Gürcistan ile Rusya arasında çıkan çatışmalar beraberinde yine siber saldırıları getirdi. 7 Ağustos 2008 akşam saatlerinde Gürcistan'a karşı gerçekleşen siber saldırıların verdiği zararın etkisi Gürcistan enformasyon alt yapısının Estonya kadar gelişmiş olmaması nedeniyle sınırlı kaldı.

aracılığı ile farkında olmadan botnetlere (robot ağ) dahil olan zombi bilgisayarlar aracılığı ile gerçekleştirilen bu saldırılara karşı önlem almak sofistike teknikler ve yüksek maliyetler gerektirmekle birlikte önlemler her türlü saldırıya karşı her zaman yeterli olmayabilir. Bu yüzden esnek ve alternatif çözümlerin yanısıra uluslararası işbirliği son derece önemlidir. Ukrayna'ya yönelik olarak Aralık 2015'te gerçekleşen saldırılarda enerji ağına yönelik siber sabotajla ülke saatlerce karanlığa gömüldü.

TÜRKİYE'DE YAŞANMIŞ SALDIRILAR

Siber saldırılara Türkiye'nin de önemli oranda maruz kaldığı ve zaman ilerledikçe bu tür saldırılarla çok daha fazla karşılaşılacağı kaçınılmazdır. Özellikle 2015 yılının aralık ayında gerçekleşen ve Türkiye'nin isim çözümleme altyapısına (nic.tr) yapılan siber saldırı sonucunda tr uzantılı sitelere yurtdışından erişimlerde ciddi sıkıntılar yaşanmıştır. Bu saldırının arkasında kimlerin olduğu tartışılırken Anonymous adlı uluslararası hacker grubu bu saldırıyı üstlenmiş, akabinde saldırılarının devam edeceğini ve hedef olarak da Türkiye'nin finans, ulaşım gibi kritik altyapılarını aldığını belirten bir mesaj yayınlamıştır. Bu noktadan sonra Türkiye'de siber saldırı açısından bir ilk yaşanmış, Anonymous grubu Türkiye'deki birçok bankaya siber saldırı gerçekleştirmiş ve bu bankalardan bazılarında ciddi hizmet kesintisi yaşanmıştır. Bu saldırıların en önemli özelliği ise; ilk defa bu kadar net bir şekilde bir siber saldırı nihai anlamda vatandaşların hayatını etkilemiş olmasıdır. Çünkü çalışmayan bankacılık sistemleri, ATM cihazları, POS makinaları bir siber saldırının gerçek hayatı nasıl etkileyebileceğinin en belirgin göstergelerindendir.

Ülkemizin yaşadığı siber saldırılar çeşitlilik olarak da farklılık gösteriyor. Örneğin 2016 yılının Mart ayında İstanbul'da yaşayan ve toplu taşıma araçlarını kullanan vatandaşlar bu araçlardaki bilgilendirme ekranlarında bir hacker tarafından bırakılan mesajla güne başladılar. Vatandaşları bilgilendirme amaçlı kullanılan sisteme sızan hackerlar bu sistemi kullanan bütün araçlarda gösterilecek bir mesaj yazmış ve sistemden çıkmışlardı.

Bahsi geçen bu olaydan önceki 15 gün içinde Türkiye'de yaşanan terör saldırıları göz önünde bulundurulduğunda, hackerların vatandaşlar üzerinde çok olumsuz tepkiler doğurabilcek başka türlü (sahte ihbar mesajları vb) mesajlar yazmaları halinde oluşabilecek kaos ve kargaşa çok daha yıkıcı etkilere sahip olabileceği görülmüştür.

Türkiye'deki kamu kurumlarının da ciddi şekilde siber saldırılara uğradığını ve özellikle kritik bilgilerin yer aldığı kurumların hedef olarak seçildiğini de biliyoruz. 2015 yılının başlarında **Suriye Elektronik Ordusu** isimli grup, aralarında Türkiye Cumhuriyeti Cumhurbaşkanlığı, Dışişleri Bakanlığı, Milli Savunma Bakanlığı ve Hava Kuvvetleri Komutanlığı gibi kurumların olduğu e-posta hesaplarını hacklediğini duyurdu. Her ne kadar yayınlanan veriler nispeten eski tarihli veriler olsa da bir siber saldırının gerçekleştirildiği ve bunun başarıya ulaştığı söylenebilir. Ülkemizin mevcut konjonktürde ne kadar kritik bir rol

üstlendiği göz önünde bulundurulursa hem iç hem de dış kaynaklı bu tarz saldırıların daha da artacağı ve şekilleneceği söylenebilir. *

Sadece Türkiye'de değil bütün dünyada siber saldırıların her geçen gün artış gösteriyor olması, bu saldırıların birçoğunda farklı türdeki birçok gizli bilginin de saldırganların eline geçme riskini artırmaktadır. Bu saldırılarda hedef olarak devlet kurumları, finans şirketleri, elektronik ticaret siteleri gibi bir çok farklı kurum veya şirket bulunmaktadır.

*

Siber Güvenliğin Geleceği

SİBER GELECEĞE HAZIRLIK, 2023 VİZYONU, 2023'te SİBER GÜVENLİK NEREYE GELECEK?

GÜNÜMÜZ SAVAŞLARI SİBER SAVAŞ HALİNE Mİ DÖNÜYOR?

Konvansiyonel savaşların artık neredeyse hiç gerçekleşmeyeceği, iki silahlı ordunun karşılıklı tank ve top atışları ve piyade birlikleri ile bir savaşa girişmeyecekleri artık toplumların da malumu… Bunun yerine orduların artık tamamı bilişim sistemleri ile yönetilen silahlar kullanacakları ve savaşın tarafları yeni açılan ve adına 5. cephe denilen **siber uzay**da da mücadele etmek zorunda kalacakları öngörülmektedir. Hatta 5. cephedeki güç diğer cephelerdeki güç için de belirleyici olacaktır.

DÜNYADA GÜVENLİK YAKLAŞIMLARI

Artık siber savaşların ülkelerin geleceğini belirleyeceği söylenebilir. Bu söylemi doğrulamak adına gelişmiş ülkelerin ve uluslararası oluşumların siber savaşlara ve siber güvenliğe yaklaşımları kısaca şöyle ifade edilebilir;

AB

Uluslararası bilişim suçları ve bilgi güvenliği politikaları ile ilgili olarak Avrupa Konseyi tarafından hazırlanan en önemli hukuki belgelerden biri 185 sayılı Siber Suçlar Sözleşmesi (SSS)'dir (European Council, 2001). 2001 yılında kabul edilerek 2004 yılında yürürlüğe giren ve sonradan Türkiye'nin de katıldığı (TBMM'de 02.05.2014 tarihli ve 6533 sayılı kanun ile onaylanıp yürürlüğe girdi) 47 ülke tarafından (ABD, Japonya, Kanada, Güney Afrika, Avrupa Konseyi üyeleri ve diğer Avrupa ülkeleri)

CIA Başkanı Leon Panetta'ın aşağıdaki ifadesi hem günümüzün hem de geleceğin durumunu özetler mahiyettedir;

"İnternet üzerinden, hükümet birimlerimize saldıranlara karşı en ufak bir tahammül göstermeyeceğiz. Savunmamız da karşı saldırılarımız da en sert biçimde gerçekleşecek… Soğuk Savaş bitti ama teknoloji savaşları başladı." *

5. Cephe; Siber Uzay

Orduların artık tamamı bilişim sistemleri ile yönetilen silahlar kullanacakları ve savaşın tarafları yeni açılan ve adına 5. cephe denilen **siber uzay**da da mücadele etmek zorunda kalacakları öngörülmektedir. Hatta 5. Cephedeki güç diğer cephelerdeki güç için de belirleyici olacaktır.

imzalanan SSS; bilgi merkezlerini ve bireyleri korumayı hedef almakta ve zararlı kodların üretilmesi/dağıtılması konusunda uluslararası bir çerçeve oluşturmaktadır (Bozkurt, 2010).

NATO

NATO'nun 2008 yılındaki Bükreş zirvesinde siber savunma siyaseti kabul edilerek bunu geliştirecek yapılar ve gerçekleştirecek otoriteler oluşturulmasına karar verilmiştir. Zirveden sonra NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority) Brüksel'de kurulmasına karar verilmiş, bunun yanı sıra Ekim 2008'de NATO bünyesinde Estonya Tallinn merkezli Siber Savunma İş birliği Mükemmeliyet Merkezi (CCD COE -Cooperative Cyber Defence Centre of Excellence) kurulmuştur.

AMERİKA

2009'da ABD Başkanı Obama, siber tehditleri ABD'nin karşısındaki en ciddi ekonomik ve ulusal güvenlik sorunu olarak göstermiş, ABD'nin 21.yüzyıldaki huzur ve refahının siber güvenliğe dayandığını söylemiştir. ABD'nin siber güvenlik için 2017 bütçesinde ayırdığı tutar 19 milyar USD olmuştur.

http://fortune.com/2016/02/09/obama-budget-cybersecurity/

ÇİN

Çin Halk Cumhuriyeti, 2011 yılında Mavi Ordu isimli siber savaş biriminin varlığını açıklamıştır.

http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/

Siber riskler gelecekte uluslar arası ittifakların da öncelikli maddeleri arasında olacaktır.

Bu çerçevede;

2001 de AB mevzuatında dillendirilen Siber Gündeme önem atfedilmeye başlanmıştı. Ardından NATO nun 2008 yılında gündeme almasıyla birlikte bilinen ittifakların gündemine oturdu. Teknolojiye yön veren ülkeler tarafından büyük bütçelerin ayrılması bu yeni cephenin farklı boyutlarını da gözler önüne sermekteydi. Bundan itibaren bir çok ülke siber cepheye devasa bütçeler ayırmaya başladı.

Amerika Örneği

2009'da ABD Başkanı Obama, siber tehditleri ABD'nin karşısındaki en ciddi ekonomik ve ulusal güvenlik sorunu olarak göstermiş, ABD'nin 21.yüzyıldaki huzur ve refahının siber güvenliğe dayandığını söylemiştir. ABD'nin siber güvenlik için 2017 bütçesinde ayırdığı tutar 19 milyar USD olmuştur.

RUSYA

Rusya devlet başkanı Putin'in imzaladığı 2016 Ulusal Güvenlik Stratejisi'nde enformasyon savaşına da dikkat çekilmiş ve uluslararası etki yaratmaya uğraşan gizli servislerin oldukça aktif olduğuna vurgu yapılmıştır.

İNGİLTERE

2010 yılında yayınlanan Ulusal Güvenlik Stratejisinde siber saldırılar, uluslararası terörizm ve uluslararası askeri krizlerle aynı kategoride değerlendirilmiş ve stratejinin önsözünde Başbakan Cameron siber saldırıların Britanya'ya ölümcül hasarlar verebileceğini belirtmiştir. 2016 yılında siber güvenlik için ayrılan bütçe 1,9 milyar sterlin olmuştur.

*

BİLİŞİMİN GELECEĞİNDEKİ YENİ RİSKLER

BULUTA BAĞIMLILIK

Kurumlar bir buluttan sunucu alıp kullanarak, yazılım alıp kullanarak ihtiyaçlarını hali hazırda karşılamaktalar. Günümüzde bilişim altyapısının tamamını buluta taşıma hedefinde olan kurumlar bile mevcuttur. Yakın gelecekte bir çok kurumun verilerinin bulutta olacağı aşikardır. Bu da aslında ticari sır kapsamında olduğunu varsaydığımız bir çok kritik verinin internette olmasını, bazı verileri bir ülkede iken başka verilerinin başka ülkede olduğu, global kompleksliğe sahip mimariler ortaya çıkabilecektir. Yani muhasebe sistemi bir ülkede, müşteri ilişkileri (CRM) verileri başka bir ülkede olabilecektir.

Buluttan servis alma artık hayatımızın ayrılmaz birer parçası haline gelmiştir

Bireyler maillerini, kontaklarını, fotoğraflarını, dosyalarını bulutta tutmaya, trafik bilgisini buluttan almaya kadar bir çok işini internet üzerindeki bulut servislerinden yapmaktadırlar. Bu bağımlılığın daha da artarak bulut destekli olmayan hiç bir işimiz kalmayacak bir noktaya geleceğiz.

İnternete ve özellikle de buluta olan bağımlılık

Uluslararası arası ilişkilerde stratejik bir silaha dönüşebilecektir. Önümüzdeki yıllarda bu teknolojileri elinde tutan ülkelerin diğerlerine karşı hem ekonomik hem de stratejik olarak üstünlükleri olacağı kaçınılmazdır.

Birçok kurumun ve neredeyse tüm bireylerin buluttan kullandığı mail, dosya paylaşımı gibi servislerin kapatılması durumunda, kurumların en önemli iletişim araçlarından birinin çalışmaması sonucu kaybedecekleri ticaret potansiyeli oldukça yüksek olacaktır. Bunun devamlılık arz etmesi durumunda hem kurumlar hem de bireyler hafızalarını kaybetmiş olacaktır.

Herkesin trafikte kullandığı navigasyon sistemleri, kendisini kullanan kullanıcıların verilerini toplayarak anlamlı trafik verileri üretmektedirler. Bu verilere dayanarak kullanıcılarına optimum rotayı önermektedir. Bu sistemler kişilerin konum bilgilerine sahip büyük verileri sürekli işlemektedirler. Tabii ki bu büyük veri istihbari manada da kullanabilecektir. Kim kiminle hangi sıklıkta görüşmekte, kim evine, işine giderken hangi rotaları kullanmaktadır gibi veriler çok kolay elde edilebilecektir. Ya da bütün veriler manipüle edilerek, kasten, bir şehirdeki trafik yanlış yönlendirmeler ile daha karmaşık hale getirilebilecektir.

Bulutun yaygınlaşmasıyla beraber ülkemizi bekleyen olası siber tehditlere örnek vermemiz gerekirse: Bir ülkeyle olan ilişkilerde yaşanabilecek gerilim veya kopma o ülkeden alınan bulut servislerinin yavaşlatılması veya durdurulması ile sonuçlanabilir. Bu da o ülkeden servis alan birey veya kurumlarının işlerinin aksamasına hatta durmasına neden olabilecektir. CRM servisi alan bir firmanın müşteri ile olan bağının kopması ve satışlarının kısa vadede azalması orta uzun vadede durması gibi durumlarla

Buluta Bağımlılığın Olası Etkilerine Bir Örnek;

CRM servisi alan bir firmanın müşterisi ile olan bağının kopması ve satışlarının kısa vadede azalması orta uzun vadede durması gibi durumlarla sonuçlanabilir.

Biletleme, check-in gibi uçuş operasyonlarını buluttan sağlayan bir havayolu şirketi için bilet satamamak, uçaklara yolcu alamamak gibi sonuçlar sadece havayolunu değil, tüm ülke ulaşımını kaotik bir noktaya sokabilecektir.

IoT: Nesnelerin İnterneti

Sürekli olarak nabzımızı ve tansiyonumuzu ölçen gömlekler, alışveriş listemizi kendisi belirleyip, internetten sipariş eden buzdolapları, gitmek istediğimiz yere bizi kendisi götüren otonom arabalar, bizi sesimizden tanıyan, asistanımız haline gelmiş akıllı televizyonlar yakın gelecekte hepimizin hayatının birer parçası haline gelecek.

sonuçlanabilir. Biletleme, check-in gibi uçuş operasyonlarını buluttan sağlayan bir havayolu şirketi için bilet satamamak, uçaklara yolcu alamamak gibi sonuçlar sadece havayolunu değil, tüm ülke ulaşımını kaotik bir noktaya sokabilecektir.

NESNELERİN İNTERNETLE OLAN GELECEĞİ

Teknolojinin bu kadar hayatımızın içerisine girmesi ve bu teknolojilerin internet bağımlılıklarının her geçen gün artması bizleri de internetten gelebilecek saldırıların birer hedefi haline getirebilecektir. Bu saldırılar kişisel bilgilerin çalınması, özel hayata müdahale gibi günümüzde de yaygın olan amaçlar içerebileceği gibi çok daha karmaşık hedefler içerebilecektir. Sağlık bilgilerinizin çalınmasının yanında bir devlet adamının internet bağlantılı kalp piline yapılabilecek bir suikast, bir rakibin arabasına kaza yaptırıp ticari üstünlük sağlama veya akıllı şehirlerdeki sensörlerin hatalı bilgi üretmesini sağlayarak şehirde kaos yaratma gibi farklı hedefler içerebilecektir.

Öneriler

TÜRKİYE'NİN SİBER GÜVENLİK GELECEĞİNE İLİŞKİN ÖNERİLER

DEVLET
A- GÜVENLİK İLE İLGİLİ REGÜLASYONLAR

Oluşturulan stratejilerin takibi ve güncel tutulması

Aralık 2012 de Siber Güvenlik Kurulu tarafından hazırlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" Bakanlar Kurulu'nun Haziran 2013 tarihli kararı ile yayımlanmıştır. Eylem planına yapılan bir çok eleştiri bir tarafa; ilk olması, farkındalık oluşturması, bürokrasinin konuya dahil olması gibi daha temel konularda fayda sağladığı inkar edilemez.

2013-2014 Eylem planının en temel eksiği, 2016-2019 Ulusal Siber Güvenlik Stratejisi çalıştayında da vurgulandığı gibi takip, kontrol ve raporlamanın olmamasıydı.

Nato, AB, ABD ve diğer yapılanmaların siber güvenlik çalışmaları takip edilmeli, eylem planları ve stratejiler sürekli olarak güncellenmelidir.

Olay yönetimi (USOM, SOME)

USOM, bağlı sektörel SOME'ler ve kurumsal SOME'ler hiyerarşisinin verimli ve değer üreten bir konuma gelmesi için yetişmiş insan kaynağı ve güvenli iletişim altyapılarının sağlanması gerekmektedir.

USOM - sektörel SOME - kurumsal SOME işleyişindeki diğer temel ihtiyaç olan güvenli iletişim konusunda uluslararası standart olan STIX, TAXII gibi standartların kullanılacağı alt yapı oluşturulmalı ve kurumlar arasında güvenin tesis edimesi için süreçleri, sorumlulukları ve müeyyideleri de tarifleyen mevzuat oluşturulmalıdır.

USOM biriminin yaptırım gücünün olmaması önemli bir eksikliktir. USOM'un yaptırım gücü elde edebilmesi için bazı düzenlemeler gerçekleştirilmelidir.

Stratejik Planlar

Stratejik planların ve bağlı eylem planlarının hayata geçirilmesi için gerçekçi tarihler ve ölçüm kriterleri belirlenmeli ve bunlar üzerinden mutlaka müeyyideler belirlenmelidir. Takip, konrol ve raporlama süreçlerinde kullanılacak güvenli yöntemler devreye alınmalı paylaşılacak verilerin güvenliği garanti edilmelidir.

USOM ve İnsan Kaynağı

Yetişmiş insan kaynağına sahip olunmadan sistemin işletilmesi mümkün değildir. Bu amaçla USOM'da bizzat istihtam edilecek kaynakların yanında özel durumlarda aktif görev alacak yetişmiş insan kaynakları ile özel sözleşmeler, devlet adına görevlendirmeler ve gönüllülük esası ile aktif irtibat kurulmalıdır. Bu çalışmanın ilk adımı olarak yetişmiş insan kaynağının tespiti amacıyla envanter çalışması yapılmalı ve sonuçlar kolluk kuvvetleri ve istihbarat birimlerince filtrelenmelidir.

Bilgi Güvenliği Yönetim Sistemi (BGYS) ve ISO 27001

ISO 27001 BGYS sistemlerinin merkezinde değer varlıkları ve risk yönetimi vardır. Ülkenin varlık envanteri düşünüldüğünde kritik altyapılar öncelikli olmak üzere tüm kurumların varlıkları milli değer varlığıdır.

Kurulumların bu standardın gereklerini yerine getirecek hale getirmesi için gerekli çalışmalar yapılmalıdır.

Tatbikatların ve Güvenlik Testlerinin Etkinlik ve Kalitesinin Arttırılması

Gap (boşluk) analizleri ve Penetrasyon Testlerinin (sızma testleri) nin daha etkin yapılabilmesi için ilgili kurum ve kuruluşların yetkinlikleri değerlendirilmelidir. Kritik bilgilere ulaşabilen bu kuruluşların koordinasyonu ve elde ettikleri anonim verilerin bir merkeze iletimi sağlanmalıdır. Bir sistemin varlıklarını tehdit eden riskler aynı zamanda sistemi geliştiren unsurlarsa ülkenin siber altyapısında meydana gelebilecek ihlaller güvenlik sisteminin güncelliğini tetiklemelidir.

İş Sürekliliğinin sağlanması ve İş Sürekliliği Yönetim Sistemi (İSYS)

Sistem sürekliliği ve güncelliği sistematize edildiği zaman ortaya çıkan değer iş sürekliliğidir.

ISO 22301 maddeleri ile standardize edilmeye çalışılan İş Sürekliliği Yönetim Sisteminin kapsamı kurumların içi ile sınırlı kaldığında, alınmış olan tedbirlerin koordinasyonundan bahsedilemez. Zira kurumlar her zaman birbirinin paydaşı olmasa da benzer özelliklerinden dolayı birbirine destek verebilir. Bir kurumda sağlanamayan bir süreklilik benzer bir kurumun da problemidir. Veya bir kurumda elde edilen bir iş sürekliliği başarısının diğer kurumlara model olabilmesinin yolu da kurumların iş sürekliliği koordinasyonunu sağlamasından geçmektedir.

Kurumlarda iş sürekliliği ile ilgili İş Sürekliliği Yönetim Sistemi çalışmaları yapılmalı ve yapılan çalışmalar ve tecrübeler kurumlar arası koordinasyon ile paylaşılmalıdır.

BGKM (Bilgi Güvenliği Koordinasyon Merkezi) Yapılanması

USOM uhdesinde yürütülen SOME ler, daha çok ihlal olaylarını koordine etmek üzere tasarlanmış ve bunun dokümantasyonunu hedeflemiştir. İhlal yönetiminden daha kapsamlı olmak üzere BGYS başta olmak üzere yönetim sistemlerindeki boşluk verilerinin de USOM benzeri bir merkeze akması, merkezden yönetilebilmelidir. Bu risk analizlerini de daha anlamlı kılacaktır. Bu noktada bir BGKM (Bilgi Güvenliği Koordinasyon Merkezi) benzeri bir yapılanmaya gidilebilir.

İSKM (İş Sürekiliği Koordinasyon Merkezi) Yapılanması

Bir Önceki maddede belirtilen BGKM (Bilgi Güvenliği Koordinasyon Merkezi) benzeri bir yapılanmanın uhdesinde veya münferit olarak koordinasyon yapacak bir İSKM (ş Sürekiliği Koordinasyon Merkezi) benzeri bir yapılanmaya gidilebilir.

Farkındalık Eğitimleri

Bilişim güvenliğindeki temel tehditlerden biri de bilinçsiz kullanıcılardır. Kurumların, firmaların, kişilerin, gençlerin, çocukların, velilerin bilgiyi koruma, güvenli paylaşma, bilişimin sağlıklı kullanımı gibi konularda eğitilmesi gerekmektedir. Düzenli eğitimler organize edilmeli, bu eğitimler zorunlu yapılmalı ve başarısı bir takım yöntemlerle ölçülmelidir.

B- ALTERNATİF AĞLAR, KAMU ENTEGRE VERİ MERKEZLERİ

Alternatif ağlar

İnternete çıktığınız anda, ne kadar güvenlik tedbiri alırsanız alın hiçbir zaman %100 güvende olamazsınız. Bunun yanında devlet hizmetlerin birbiriyle entegre çalıştığı e-devlet altyapılarının kesintisiz çalışma ihtiyacı aşikardır. İnternet üzerinden gelebilecek saldırılar, tehditler bu servislerin kesilmesine neden olabilecektir.

Bu saldırılardan korunabilmek yada en azından etkisini azaltabilmek adına, kamu kurumlarının sadece karşılıklı haberleşme, bilişim servislerinden faydalanma amacıyla özel ağlar kurmaları internet alt yapısında olabilecek olası kesinti yavaşlamalardan devlet hizmetlerinin kesintisiz bir şekilde çalışmalarına imkan tanıyacaktır.

Kamu Entegre Veri Merkezleri

Kamu entegre veri merkezleri kamuya hizmet vermek üzere tasarlanmış büyük veri merkezleridir. Bu veri merkezleri internete, kamu alternatif ağlarına ve tabii ki kamu kurumlarının birbirlerine kolay erişim sağlaması adına kritik tesisler olacaktır. Bunun yanında standartları belli olmayan bir çok kamu veri merkezine parçalı yatırımlar yapılması yerine yatırımın merkezileşmesi ve standartları yüksek veri merkezlerinin kurulması esas olarak kabul edilmelidir. Burada fiziksel güvenlik katmanından, ağ, uygulama ve bilgi güvenliği gibi değişik katmanlarda güvenlik kurgulanarak kamu kurumlarının en üst seviyede güvenlik hizmeti aldığı garanti altına alınmalıdır. Kamu entegre veri merkezlerinin kamu kurumları arasındaki alternatif ağların merkezinde olması da bu güvenliği bir kat daha arttıracaktır.

Bilgi Güvenliği Firmalarının Koordinasyonu

Danışmanlık, Analiz, Test ve Belgelendirme benzeri hizmetleri veren kurum, kişi ve kuruluşların ulaştığı kritik bilgileri ve anonim verilerin bir merkezde toplanması sağlanmalıdır. Hizmet veren kuruluş ve kişilerin ilgili verilerden faydalanabileceği bir özellikte olmaldır.

Veri merkezleri konusuna ayrıca değinilecektir.

Alternatif Bağımsız Ağlar

Bu altyapı NATO TAFICS adı ile ülkemizde de kurulu olan altyapı gibi fiziksel olarak bağımsız bir altyapı olmak durumundadır. Paylaşımla bir altyapıda VPN gibi teknolojilerle kurulmuş ağlar internet altyapılarını kullanan ağlarla ortak altyapıyı kullanabilecekleri için burada yaşanabilecek kesinti, yavaşlama ve güvenlik risklerini üzerinde barındıracaktır. Böyle bir ağın NATO TAFICS'den temel farkı sadece belirli büyük şehir merkezlerinde ve kamu entegre veri merkezlerinde olmasının yeterli olmasıdır. NATO gibi yaygın bir coğrafyaya hitap etmesi gerekmeyecektir.

Kamu entegre veri merkezleri tasarlanırken unutulmaması gereken önemli konu ise kritik altyapıları belirli merkezlerde toplarken bu merkezde olabilecek bir kesintinin etkisinin çok daha yüksek olacağı unutulmamalıdır. Bu sebeple kamu entegre veri merkezleri tasarlanırken dağıtık yapıda tasarlanmalı ve bu merkezlerde çalışacak uygulamalarında dağıtık yapıda çalışabilir olması sağlanmalıdır. Bu veri merkezlerinden herhangi birisinde olabilecek kalıcı veya süreli, tam veya kısmi kesintilerinin etkisi bu dağıtık mimariden dolayı azaltılabilecektir. Dağıtık mimari gündeme geldiğinde ise büyük şehirler içerisinde alternatif lokasyonlar olacağı gibi alternatif illerinde bu mimari içerisinde yer alması gereklilik olacaktır. Bu iller seçilirken veri merkezi yer seçim kriterlerinin analitik bir şekilde değerlendirilip, uygulanması yapılacak veri merkezi yatırımının uzun vadeli bir yatırım olduğu bilinciyle yapılması gerekmektedir.

Siber Uzayda Ülke Sınırlarının Korunması

Günümüzde internetin yaygınlaşması ve hayatın bir parçası haline gelmesiyle beraber artık ülkeler arası sınırların internet üzerinden kalktığı bir dünyadayız. Ülkeler eskiden yollar üzerinden sınır kapıları ile birbirlerine bağlı iken artık fiber kablolar ile birbirlerine bağlı hale geldiler. Bu gelişmeler, iletişim, ekonomi gibi birçok alanda kolaylıklar sağlarken bağımlılıkları da arttırır hale getirmiştir.

DDoS saldırıları yapısı itibariyle dağıtık kaynaklardan belirli hedeflere doğru gelmektedir. Bant genişliğini veya servise hizmet veren donanım katmanlarının kapasitesini doldurup hedefteki servisin hizmet veremez hale gelmesini hedeflemektedirler. Günümüzde korunma yöntemi olarak çoğunlukla telekom operatöründen bu servise gelen trafiğin temizlenmesi tercih edilmektedir. Bir alternatif olarak yurtdışında bu servisi veren trafik temizleme merkezlerine trafiğin yönlendirilip temizlenmesi de söz konusudur. Birinci seçenekte maliyet ve yönetim kolaylığından dolayı dolayı bu temizleme noktaları omurgada son noktada yer almaktadır. Buda gelen zararlı, saldırı trafiği Türkiye'nin bütün haberleşme altyapısında taşımak manasına gelmektedir. Bunun yerine bu saldırı trafiği ülkeye trafiğin girdiği noktalarda temizlenmesi daha yaygın ve etkili bir çözüm olacaktır.

Kamu Entegre Veri Merkezleri

Kamu entegre veri merkezleri kamuya hizmet vermek üzere tasarlanmış büyük veri merkezleridir. Bu veri merkezleri internete, kamu alternatif ağlarına ve tabii ki kamu kurumlarının birbirlerine kolay erişim sağlaması adına kritik tesisler olacaktır. Bunun yanında standartları belli olmayan birçok kamu veri merkezine parçalı yatırımlar yapılması yerine yatırımın merkezileşmesi ve standartları yüksek veri merkezlerinin kurulması esas olarak kabul edilmelidir.

Bu merkezlerde özellikle kritik altyapıları ilgilendiren veriler yeni riskler gözetilerek barındırılmalıdır.

Siber Uzayda Ülke Sınırlarının Korunması

Ülkemiz dışındaki siber savaşların ülkemizin altyapısını ve cihazlarını kullanmaması için ülkemizin siber sınırlarını koruyucu tedbirler alınmalıdır. Farkındalığı arttırmak, yeni yatırımlar veya Çin örneğindeki gibi trafiği koruma tedirleri ile sınırlar korunabilir.

Saldırıların asıl kaynağında yok edilebilmesi bu tarz saldırılar ile mücadele etmenin en etkin yoludur. Bu mücadeleyi daha etkin yapabilmek adına tüm dünyadaki Telekom operatörleri arasında iş birliktelikleri oluşturulmalı ve saldırı anlarında saldırı amaçlı trafiklerin geldiği noktalar bu iş birliktelikleri ile oluşturulmuş savunma zincirleriyle saldırıyı oluşturan zombi bilgisayarların olduğu ülkeye kadar ulaşılarak o ülkelerde bu saldırıların oluşması engellenmelidir.

Bunun yanında Çin örneğinde olduğu gibi tüm ülkenin internet giriş çıkışlarının güvenlik duvarları ile kontrol altına alan ülkeler de mevcuttur. Bu uygulamanın artıları ve eksileri ile ayrıca tartışılması daha faydalı olacaktır.

C- YERLİ DONANIM VE YAZILIMI TEŞVİK EDECEK POLİTİKALAR
SEKTÖR
SEKTÖR ÖNERİLERİ ve YERLİ POLİTİKALAR

Sipariş Desteği

Yerli ürünler fazla büyüyemeden sonlanıyor. Bir ürünü yaşatan ve geliştiren müşteridir. Yabancı ürünler kadar yetenekli olmasa da yerli ürünleri satın alarak onların gelişmesi sağlanabilir. Yerli bilişim güvenliği ürünlerini kurumlara öneren, tanıtan etkinlikler düzenlenebilir, kamuda bütçeden belli oranda yerli ürün zorunluluğu getirilebilir.

Vizyon Eğitimleri

Bilişim, sektörü çok hızlı şekil değiştiriyor. Sektör yön değiştirdikçe tehditler de farklılaşıyor ve artıyor. Bilişim güvenliği sektörünün doğru bir şekilde yönlendirilebilmesi için ürün ve marka bazlı olmayan eğitimlerin ve/veya seminerlerin yapılması gerekiyor. Büyük veri, bulut, nesnelerin interneti, giyilebilir teknolojiler vb birçok yeni teknoloji var. Bunlara yönelik olası tehditler ve çözüm yöntemleri için öncelikle bilişim firmalarının vizyonunu geliştirici etkinlikler planlanmalıdır.

SEKTÖR İLİŞKİLERİNE YÖNELİK ÖNERİLER

Sipariş Desteği

Yerli üretimi desteklemek üzere adımlar atılmalı, bu adımlar atılırken inovatif motivasyonun ihmal edilmemelidir. Unutulmamalıdır ki ürünleri ve firmaları yaşatan en önemli faktör müşteridir.

Rekabetin Sağlanması ve Vizyon Gelişimine Destek

Devlet yerli üretimin müşterisi oluyorken bir yandan da üreticilerin sayısını arttırıcı, var olanların da vizyonunu geliştirici çalışmalar yürütmelidir.

TÜBİTAK, TÜRKSAT, HAVELSAN, TSE gibi kurumların sektöre rakip olan değil, sektöre yol gösteren, sektöre rekabeti açarak iş yaptıran bir şekilde yapılanmaları gerekmektedir. Ticarete rekabetin doğrudan şekil vermediği ortamlar girişimciliği ve inovasyonu bitirecektir.

Personel Desteği

İnsan kaynağı ihtiyacını karşılamak üzere sektöre TUBİTAK benzeri kurumlar üzerinden düzenli eğitimler verilmelidir.

Devletin Özel Sektöre Rakip Olmaması

Kamuya bağlı kurumların kendilerinin birtakım çözümler ürettiği veya üretmeye çalıştığı görülmektedir. Bilişim güvenliği sektörü çok dinamik, çok hızlı değişen bir sektördür. Kamu reflekslerinin bu değişime ayak uyduramıyor olduğu malumdur. Ayrıca kamu kurumlarının kendi yapmaya çalıştıkları çözümler rekabetten beslenmediği için kalite sorununa sahiptir. Bu tür çözümlerin bizzat devlet tarafından sağlanmaya çalışılması ve hatta bu etkinliklerin rekabeti olumsuz yönde etkilemesi sektöre destek vermekten öte zarar vermektedir.

TÜBİTAK, TÜRKSAT, HAVELSAN, TSE gibi kurumların sektöre rakip olan değil, sektöre yol gösteren, sektöre rekabeti açarak iş yaptıran bir şekilde yapılanmaları gerekmektedir.

Personel Eksikliği

Sektörde bilişim güvenliği uzmanı ihtiyacı vardır. Üniversitelerde ilgili bölümlerin TÜBİTAK SGE bünyesinde düzenli bilişim güvenliği eğitimleri verilebilir.