TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

HAVELSAN
havelsan.com.tr

TEKNOLOJİ SOHBETLERİ 5

SİBER SAVAŞLAR VE GELECEĞİ

25 EYLÜL 2019

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

HAVELSAN Türk Silahlı Kuvvetlerini Güçlendirme Vakfı'nın bir kuruluşudur.


TEKNOLOJİ SOHBETLERİ 5
Ahmet Hamdi ATALAY
SİBER SAVA
VE
GELECE

HAVELSAN, Bilgi Teknolojileri ve İletişim Kurumu ve Türkiye Siber Güvenlik Kümelenmesi işbirliği ile düzenlenen Teknoloji Sohbetleri etkinliğinin beşincisi Siber Savaşlar ve Geleceği teması ile 25 Eylül 2019 tarihinde Bilgi Teknolojileri ve İletişim Kurumu ev sahipliğinde gerçekleştirilmiştir.

Teknoloji Sohbetleri etkinliği güncel teknolojilerin konuşulduğu, fikirlerin paylaşıldığı bir ortam oluşturmak amacıyla düzenlenmektedir. Bu kapsamda etkinlik teması alanında uzman katılımcılar tecrübelerini paylaşmaktadır. Bu sayede teknolojideki gelişmeleri gündemimizden düşürmemeyi ve gerçekleştirilen paylaşımlar ile ülkemize değer katan çalışmalar üretmeyi hedeflemekteyiz.

Günümüzde siber savaş ülkelerin ulusal güvenliğine yönelik en önemli tehditlerden biri haline gelmiştir. Ülkeler ordularında silahlı kuvvetlerinin yanı sıra siber güvenlik birimlerini de oluşturmaktadır. Amerika Birleşik Devletleri ve NATO dahil olmak üzere birçok ülke ve uluslararası kurum siber uzayı; kara, hava, deniz ve uzayın ardından beşinci savaş boyutu olarak tanımlamaktadır. Ülkeler siber güvenliklerini sağlamak için istihbarat toplamakta ve siber güvenlik kapasitelerini artırmaktadır. Ülkemizde de bu kapsamda siber güvenlik strateji ve eylem planlarının oluşturulması ve uygulanması, yerli ve milli çözümlerin geliştirilmesi, desteklenmesi ve yaygınlaştırılması, siber güvenlik ekosisteminin geliştirilmesi başta olmak üzere çeşitli çalışmalar gerçekleştirilmektedir.

Etkinlik kapsamında Türk Silahlı Kuvvetleri, kritik altyapıları yöneten kamu kurumları, Türkiye Siber Güvenlik Kümelenmesi üyesi firma temsilcileri ve akademisyenler tecrübelerini ve fikirlerini paylaşmıştır. Etkinliğe katkılarından dolayı Bilgi Teknolojileri ve İletişim Kurumu'na, HAVELSAN'a, Türkiye Siber Güvenlik Kümelenmesi'ne, tüm konuşmacı ve katılımcılara teşekkür ederiz.

AHMET HAMDİ ATALAY

HAVELSAN Genel Müdürü

Değerli konuklar; hepinizi saygıyla, sevgiyle selamlıyorum.

Sayın Başkanım, sayın komutanlarım, değerli katılımcılar... HAVELSAN olarak bugün beşincisini düzenlediğimiz Teknoloji Sohbetleri'ne hoş geldiniz diyorum.

Teknoloji Sohbetleri'ni bugün siber güvenlik ve siber savaş üzerine yapıyor olacağız. Ama bundan önce bu Teknoloji Sohbetleri'ni niye yapıyoruz, bir cümleyle değinmek istiyorum. Malum, Türkiye'nin bulunduğu bölge itibari ile de, dünyanın bulunduğu durum itibari ile de çok değişik gündemler var, çok değişik konular konuşuluyor. Ama biz bütün bu gündem ve konuların yanında teknolojiyi konuşmaya da bir takım ortamlar oluşsun istiyoruz. Teknoloji konuşmaya devam edelim, teknolojiyi gündemimizden düşürmeyelim. Bu fikirden hareketle Teknoloji Sohbetleri verdiğimiz ve ev sahipliğini BTK'nın (kendilerine çok teşekkür ediyoruz) yaptığı bu sohbetlerin bugün beşincisini yapıyoruz. Daha önce yine teknolojiler üzerine çeşitli sohbetler yapmıştık. Bu teknoloji sohbetleri sonunda da bir kitapçık ortaya çıkıyor. Bu kitapçıkta burada konuşulan konular da belgelendirilmiş oluyor. Buraya katılamayan ya da daha sonra geriye dönüp neler konuşmuştuk diye bakmak isteyenler için böyle de bir arşiv oluşturuyoruz. Türkiye'ye böyle bir değer katmaya çalışıyoruz.

Bugünkü konumuza gelecek olursak siber güvenlik, siber savaşlar; bu konular çok konuşuluyor. Konuşulmaya da devam edecektir, etmesi de gerekiyor. Çünkü, çok önemli. Malum, eskiden bütün savaş stratejileri kara, hava, deniz kuvvetleri üzerine kurgulanır, yapılırdı. Son dönemlerde, son yıllarda özellikle Amerika ve benzeri ülkelerde buraya bir dördüncü kuvvet olarak uzay da eklendi. Son zamanlarda da beşinci kuvvet siber alan da bu savaş alanlarından ya da kuvvetlerden biri haline getirildi. Amerika'da bir siber güvenlik komutanlığı var, yaklaşık beş altı yıl önce kuruldu. Çok şükür, bizde de Genelkurmayımızın bünyesinde bir Siber Güvenlik Komutanlığı var artık. Siber güvenlik deyince, komutanlık seviyesindeki bir işten bahsediyoruz ve dolayısıyla da ulusal güvenliğin, milli güvenliğin önemli unsurlarından birinden bahsediyoruz.

Bunun müsebbibi tabiri caizse bilgi ve iletişim teknolojilerinin geldiği durumdur. Bilgi ve iletişim teknolojilerini sektör olarak tanımlamak doğru değil, çünkü her sektörün kullandığı ya da içerdiği bir unsurdan bahsediyoruz. Bilgi ve iletişim teknolojilerinin bu kadar yaygınlaşması, hayatımıza girmesi ve hayatın her aşamasında yer alıyor olması ve aynı zamanda yapay zekâ, otonom sistemler, robotik sistemler gibi, bugün ve yakın gelecekte gündemimize gelecek yeni teknolojilerin bunun alt teknolojileri olması, bilgi ve iletişim teknolojilerine olan bağımlılığımızın giderek artmasına sebep olacaktır. Tabii bu bağımlılığın artıyor olması aynı zamanda verimlilik, etkinlik açısından bize çok önemli faydalar sağlıyor olmakla birlikte bir takım tehdit ve tehlikeleri de beraberinde getiriyor. Biz de bunları çok kabaca siber tehditler, bu konuda alınacak tedbirleri de siber güvenlik diye tanımlıyoruz.

Tabii bu işin bir de kritik altyapılar boyutu var. Demin de söylediğim gibi bilgi ve iletişim teknolojileri artık sektörden bağımsız; bütün sektörlerde, bütün altyapılarda altlık haline gelmiş durumda. Öyle olunca kritik altyapıların güvenliğinin sağlanması da çok önemli hale geliyor. Önümüzdeki günlerde, Bilgi Güvenliği Derneği olarak da kritik altyapılara ilişkin benzer bir çalıştay yapıyor olacağız. Bunu burada biraz daha detaylıca konuşuyor olacağız ama tabii kritik altyapılar da artık bilgi ve iletişim teknolojilerini çok yoğun kullandığı için kritik altyapılara yönelik tehditler de artıyor. O zaman bu ulusal güvenliğin önemli bir unsuru haline geliyor.

Zaman zaman konuşmalarımızın etkisini göstermek açısından çok kullanırız. Örnek, bir savaş uçağı, yaklaşık 100 milyon dolarlar civarında bedeli olan bir araç ve onun tahrip gücünü hepiniz tahmin edebiliyorsunuz. Hâlbuki bugün bilgi ve iletişim teknolojilerini ve siber tehditleri, siber silahları kullanarak belki 100 milyon dolarlık savaş uçağının yapabileceği olumsuz etki ya da yıkıcı etkiden çok daha fazlasını bir kötücül yazılım kullanan siber saldırıyla 100 dolarlık maliyetle gerçekleştirebiliyorsunuz.

Bir başka çarpıcı örnek olması açısından siber saldırı, bir yere siber anlamda saldırı yapmak için zaman, mekân diye bir bağımlılığınız yok. Dünyanın herhangi bir yerinden dünyanın başka herhangi bir yerine ve herhangi bir zamanda bu saldırıları yapabiliyorsunuz. Bir ülkenin bütün kritik altyapılarını çökertebiliyorsunuz. Geçmişte örnekleri var, hepsini saymaya lüzum yok ama işte Ukrayna'daki enerji sistemlerine verilen zararlar yakın geçmişte olduğu için biliniyor. Hatta Amerika'da çok ilan edilmiyor ama basına ufak da olsa düşüyor bazı eyaletlerde, bazı bölgelerde enerji sistemlerinin çöktürülmesi gibi. Bunlar bana sorarsanız böyle daha yoklama seviyesindeki işler. Yani iki ülke ciddi anlamda siber savaş noktasına gelse bütün altyapıyı ki Estonya hikâyesini hepimiz hatırlıyoruz; Rusya'nın Estonya Devleti'ni bir hafta gibi bir sürede tamamen işlemez hale getirdiğini 80'li, 90'lı yıllarda hatırlarız. Dolayısıyla siber tehditle alakalı, bu boyutta bir şeyden bahsediyoruz. Çok önemli bir konu. Bugün başka konuklar da bu konuyu gündeme getireceklerdir. Önemine binaen biz sohbetimizin bugünkü konusunu bu konuya ayırdık.

Burada benim altını çizeceğim birkaç konu var. Siber savaşlarda galip gelebilmek ya da siber savaşlarda daha güçlü olabilmek, ülkemizin ulusal güvenliğini güvence altına alabilmek için iki, üç konunun çok önemli olduğunu düşünüyoruz ve altını çizme gereğini hissediyorum. Birinci konu, yerli ve milli çözümlerin olmazsa olmaz olduğu bir alandan bahsediyoruz ve şöyle bir örnek veriyoruz; klasik, geleneksel savaş araçlarından, örneğin bir piyade tüfeğini ya da bir tankı, topu siz düşmanınızdan bile satın alsanız satın aldığınız andan itibaren Mehmetçik'in kontrolü altına verdiğinizde bu size hizmet eder. Ama bu siber dünya böyle bir dünya değil. Siz, sizi korusun diye aldığınızı düşündüğünüz bir siber güvenlik aracı alıyorsunuz ancak sizi korusun diye aldığınız o aracın bizatihi kendisi zafiyet ya da tehdit kaynağı olabilir. Ve bu sizin kontrolünüzde olmadan, sizin farkında olmadığınız bir zamanda size önemli zararlar verebilir. O yüzden biz şunu istiyoruz ve altını çizmek istiyoruz; siber güvenlikte tam güvenlikten bahsedebilmek için mutlaka yerli ve milli çözümlerimizi, ürünlerimizi üretiyor ve kullanıyor olmamız lazım.

İkinci konu da bu siber güvenlik bir zincir, bir sistem. Bunun teknoloji boyutu var, süreç boyutu ya da sistem boyutu ve insan boyutu var. Bu üç boyutun ve oluşan zincirin en zayıf halkası insan boyutu. Burada gerek kullanıcı seviyesinde, gerek yönetici seviyesinde, gerek teknik uzmanlık seviyesinde herkesin yapabilmesi gereken ve yapması gereken, alması gereken tedbirler var. Bu konuda hemen hemen her ülkede eksikler, açıklar ve zafiyetler var. Bizim ülkemizde de var. Çeşitli istatistikler var bu konuda, özellikle uzman açığı konusunda dünyada, kimi rakamlara göre 2 milyon, kimi rakamlara göre 3 milyon siber güvenlik uzman açığı var. Biz kabaca Türkiye'de bu gibi istatistiklerde %1 pay alıyoruz. Buraya göre bile bakarsak 20.000, 30.000 siber güvenlik açığımız olduğu ortaya çıkıyor. Ki biz Bilgi Güvenliği Derneği olarak geçmişte, 2015'te benzer bir hesap yapmıştık. Orada da aynı rakam çıkıyor. Gençler de var aramızda, bu vesileyle onlara da hatırlatmak

isterim; yeni bir meslek seçmek istiyorsanız hiçbir şekilde işsiz kalmayacağınız ve gelecekte çok başarılı işler yapabileceğiniz bir alan sizin için bu ve şu anda burada Türkiye'nin uzman açığı var. Biz de HAVELSAN şirketi olarak bunu çok derinden hissediyoruz. Başka kurum ve şirketler de hissediyordur. Dolayısıyla uzman yetiştirmemiz gereken bir alan. Aynı zamanda da top yekûn bilgi ve bilinç seviyemizi artırmamız gereken bir alan.

Son olarak, ulusal ve uluslararası iş birliklerinin çok önemli olduğu bir alan. Atatürk'ümüzün Kurtuluş Savaşı'nda söylediği veciz bir sözümüz vardır ya: "Hatt-ı müdafaa yoktur sath-ı müdafaa vardır." Ben bunun en geçerli olduğu alanların başında siber güvenlik alanı olduğunu düşünüyorum. Siber güvenlik alanında hiçbir kurum ya da hiçbir birim ya da hiçbir şehir, bölge "ben bütün tedbirlerimi aldım, artık hattımı kontrol altına aldım, ben artık güvendeyim." diyemez. Bütün sathı güvende değilse belli bir hattın güvende olmasından söz edilemez. O yüzden mutlaka kurumların ve daha üstünde de ülkelerin uluslararası iş birliklerinin çok önemli olduğunu düşünüyorum.

Siber tehditler, siber güvenlik gibi konuları iyilerle kötülerin mücadelesi olarak tarif ediyorum. Kötülerle iyilerin mücadelesi insanlık tarihi boyunca hep olmuştur. Bundan sonra da hep olacaktır. Burada kötüler genelde hep bir adım önde oluyorlar. İyiler de onu tedbir almak için geriden takip ediyorlar. En azından kötülere daha yakın olabilmek için, onlarla aradaki mesafeyi çok açmamak için hepimizin bilgi ve bilinç seviyemizi artırıyor olmamız lazım. Çünkü bu kötülerin tehditleri altında bütün insanlık var. Çünkü hepimiz artık "Connected World" olarak tanımlanıyoruz ve bağlantılı hale gelmiş bir dünyanın unsurlarıyız. Bu vesileyle bugün yapılacak bu toplantıların ülkemize hayırlar getirmesini diliyorum. Katkı verecek herkese de şimdiden çok teşekkür ediyor, hepinizi saygıyla ve sevgiyle selamlıyorum.

ÖMER ABDULLAH KARAGÖZOĞLU

BTK Başkanı

Türk Silahlı Kuvvetleri'nin değerli komutanları, kurumlarımızın değerli genel müdürleri, HAVELSAN'ın yöneticileri, kıymetli misafirlerimiz ve değerli basın mensupları; hepinizi şahsım ve kurumum adına sevgi ve saygıyla selamlıyorum. Konuşmama başlamadan önce Teknoloji Sohbetleri'nin düzenlenmesinde emeği geçen savunma, bilişim ve iletişim alanında ülkemizde güvenilir bir kaynak haline gelen HAVELSAN'a teşekkür ederim. Böyle verimli bir programa ev sahipliği yapmaktan duyduğum memnuniyeti de ayrıca belirtmek isterim.

Bildiğiniz gibi insanlık tarihi bilgi ve iletişim teknolojilerindeki gelişmeler sebebiyle belki de günümüze kadar geçirdiği en hızlı değişim ve dönüşüm süreçlerinden birine sahne oluyor. Gelişen teknolojiler, yaşamı ilgilendiren her alanı etkilerken dünya çapında ekonomik, politik, sosyal ve kültürel dönüşümlere de yol açıyor. Ayrıca yeni fırsatlar ve olanakları da beraberinde getiriyor. Ancak teknolojiler sunduğu fırsatların yanında riskleri de barındırıyor.

İnsan hayatının neredeyse her alanına hızlı ve sınırsız erişen teknolojiler, güvenlik açığının doğmasına ve güvenlik boyutunda yeni kaygıların

gelişmesine sebep oluyor. Web sitelerine, ağ sistemlerine, bilgisayarlara, sunuculara ve endüstriyel sistemlere yapılan saldırılar modern insanın kişisel güvenliği ile devletlerin ulusal güvenlikleri açısından büyük tehlikelere yol açıyor. Siyasi, askeri, ekonomik, coğrafi, demografik, bilişsel, teknolojik, sosyal ve kültürel alanları hedef alan siber saldırılar; ekonomik, fiziksel ve psikolojik anlamda yıkımlara neden olmasının yanında yaralanmalara, ölümlere ve büyük hasarlara sebep olabilecek kabiliyetlere de ulaşabiliyor.

Günümüzde siber savaş ülkelerin ulusal güvenliğine yönelik en önemli tehditlerden biri haline geldi. Devletler siber güvenliklerini sağlamak için istihbarat toplama ve siber kapasitelerini artırıyorlar. Ayrıca ordularında silahlı kuvvetlerinin yanı sıra siber güvenlik birimlerini de oluşturuyorlar.

Değerli konuklar, Türkiye son yıllarda siber uzay çalışmaları için kamu kurum ve kuruluşları, sivil toplum örgütleri ve özel sektör eliyle siber güvenlik stratejilerini geliştiriyor. Özellikle ulusal siber güvenlik stratejisi ve 2013-2014 eylem planı ve 2016-2019 ulusal siber güvenlik stratejisi ve eylem planı belgeleri, Türkiye'nin siber uzay faaliyetlerinde önemli adımlarından birisi. Siber uzay kapasitelerinin verimli ve koordineli olarak kullanılması bakımından kurumumuz bünyesinde faaliyet gösteren USOM'un önemli bir misyonu bulunuyor. Elektronik haberleşme işletmecileri tarafından USOM'a raporlanan siber saldırı sayıları 2016 yılında 8625, 2017 yılında 99.600 ve 2018 yılında 72.975 olarak kayıtlara geçti. 2019 yılında ise yarısında raporlanan saldırı sayısı 95.202 olarak kayıtlara geçti. Yapılan saldırıların %95'inden fazlasını DDoS ve Oltalama saldırıları oluşturuyor. Ülkemizi etkileyebilecek bu saldırılara karşı 7/24 müdahale esasına göre çalışan USOM ve USOM'un koordinasyonunda faaliyet gösteren SOME'ler etkin bir çalışma yürütüyor. USOM ayrıca kritik altyapı sektörleri ve kamu kurumları için sektörel SOME'ler kurmakla ve bunlara eğitim, koordinasyon sağlamakla siber güvenliğin sağlanmasında önemli bir rol oynuyor.

Güvenlik faktörü açısından ülkemizin içinde bulunduğu durum ve konum itibari ile yerli ve milli yazılım hassasiyetimiz kurum olarak önem verdiğimiz bir konu. Ülkemizde tamamen yerli ve milli imkânlarla geliştirilen AVCI, AZAD ve KASIRGA gibi yazılımlar bunun ispatı niteliğinde. Bu yazılımlar son kullanıcılara yönelik mağduriyetlerin engellenmesinde kullanıldığı gibi siber casusluk saldırılarına karşı da etkili tespitler yapabiliyor. BTK USOM olarak düzenlediğimiz siber yıldız yarışması, az önce bahsettiğimiz SOME'lere yönelik olarak düzenlediğimiz eğitimler, periyodik olarak yapılan istişare toplantıları ile siber güvenlik çalışmalarına katkıda bulunuyoruz.

Kıymetli misafirler, konuşmamı noktalamadan önce değinmek istediğim bir konu var. Ülkemizin güvenliği için tek başına veya milli güç unsurlarıyla birlikte siber alanda uluslararası hukuk ilkelerine bağlı kalarak kendine özgü kural, esas ve stratejileri doğrultusunda "ben de varım" diyen paydaşlarımızı desteklemeye her zaman hazırız.

Bu duygu ve düşüncelerle programın düzenlenmesinde emeği geçenlere teşekkür ediyor, hepinizi saygıyla selamlıyorum.

MUSTAFA ŞENOL

HAVELSAN
Yönetim Kurulu Başkan Vekili

Sayın Başkanım, başkanlarım, değerli hocalarım, komutanlarım, kıymetli katılımcılar hepinizi saygıyla selamlıyorum. “Siber Güvenlik, Savaş ve Caydırıcılık” konusundaki sunumumu perdede sunulan başlıklar altında yapmaya çalışacağım.

Hepinizin bildiği gibi bilgisayarın icadı sonucunda teknolojinin de gelişmesine paralel olarak bilgi ve iletişim sistemleri hayatımızın bir parçası hatta vazgeçilmesi olmuştur. Ve süreç içerisinde de bilginin daha etkin kullanılması, bilişim sistemlerinin daha etkin kullanılması, bilişim sistemlerinin kazanımlarının artırılması yönünde de siber güvenlik strateji ve politikaları çalışmaları bütün dünyada başlamış, ülkemizde de bu konuda çalışmaları yapılmış ve yapılmaya devam etmektedir.

HAVELSAN Genel Müdürümüzün de belirttiği gibi bilgi ve iletişim teknolojilerinin savaş alanlarına sağladığı kazanımlarla savaşlar da değişmiş ve 5. savaş alanı siber uzay ortaya çıkmış ve bütün dünya tarafından da kabul edilmiş durumdadır. Bilişim sistemleri ve bilgi iletişim sistemleri, teknolojinin gelişmesi ile pek çok kazanımlar getiriyor. Teknoloji gücümüz artıyor ama tehlikeler de beraberinde gelmekte. Hatta tehlikeler tedbir alınmadığı takdirde felaketler de getirebilir.

Siber uzayın yanında bu gelişmelere paralel olarak hayatımıza siber güvenlik, siber savaş, siber caydırıcılık gibi pek çok kavram da girmiş

bulunmakta. Bu kavramlara kısaca değineceğim, hepsini biliyorsunuz belki de ancak siber caydırıcılık konusunda bilgisi az olanlar vardır, o konuya da değineceğim. Ama bu kavramlara değinmeden önce HAVELSAN Genel Müdürümüz, Atatürk'ümüzün bir sözünden vurgu yapmıştı, ben de onun günün anlam ve önemini belirten 1920'lerde söylediği bir sözünü size vurgulamak istiyorum:

"Felaket başa gelmeden evvel önleyici ve koruyucu tedbirleri düşünmek lazımdır. Geldikten sonra dövünmenin yararı yoktur." Siber güvenliği önemseyelim, gerekli tedbirleri önceden düşünüp, felaket boyutuna ulaşmadan gerekli tedbirleri alalım diyoruz.

Siber Uzay / Bilgisayar ve füzelerden güneş ışınlarına kadar bilginin iletildiği düşünsel ortam.

Siber Saldırı / Taarruz, bilişim sistemleri kullanılarak yapılan her türlü tehdit veya hareket.

Siber Güvenlik / Savunma, siber ortamda olumsuz etkilerin önlenmesi, sistemlerin korunmasının ve devamlılığının sağlanması için alınması gereken tedbirlerin tümü.

Siber Savaş / Bilgi savaşı, siber ortamda siber risk ve tehditlere karşı ülkelerin kendi bilgi sistemlerini korurken, hedef ülke bilgi sistemlerini etkilemek için organize ettiği siber saldırılar.

Savaş için, savaş yapmak için bir güç gerekiyor. Yine ulusal hedeflerimize ulaşabilmek için, ulusal hedeflerimizi ele geçirebilmek için güçlerimiz 7 ayrı kategoride sıralanır. Ulusal gücümüzü oluşturan unsurlar gerekiyor. Günümüzde buna 8. unsur olarak siber güç, siber ortamda sahip olduğumuz bilişim sistemleri ve altyapıları ile bunların etkin olarak kullanılması yeteneği eklenmiş bulunmaktadır.

Siber uzay dediğimiz zaman sadece sanal boyutu, düşünsel boyutu aklımıza gelmemeli. Bunun fiziksel boyutu da bulunmakta. Siber uzayın güvenliği veya siber güvenlik dediğimiz zaman da bu değerli varlıklarımızın korunması aklımıza gelmeli.

Bilgi güvenliği ve siber güvenlik kavramları da tartışılmaktadır. Bunun için NATO Siber Güvenlik Kılavuzu'nda siber güvenlikle ilgili güzel bir tanım bulunmaktadır. Der ki: Devlet sırlarının korunması ve ulusal savunmanın sağlanması için temel esas siber güvenliktir. Yine en son strateji belgemiz olan 2016-2019 Ulusal Güvenlik Siber Stratejimiz'de, bilgi ve verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınabilmesi için gerekli tedbirler ve siber güvenlik olayı öncesi durumuna da herhangi bir olay olduğunda da döndürülmesini ifade eder şeklinde güzel bir tanım var. Bütün bu tanımlara baktığımız zaman bu sorunun cevabı, siber güvenlik günümüzde bilgi güvenliğinden çok daha geniş bir kavramı içermekte. Hele kâğıtsız bir ortama geçmeyi hedeflediğiniz ve kâğıtsız bir ortama geçtiğiniz bu dönemde siber güvenlik çok geniş bir kavramdır.

Siber risk ve tehditler dedik, biraz önceki tanımda da gördüğümüz gibi gizlilik, bütünlük ve erişilebilirlik bilgi güvenliğinin de kalbini oluşturan temel ilkeler. Bu ilkelerin herhangi birinin zarar görmesi durumunda güvenlik tam anlamıyla sağlanamamış olur ve bir güvenlik zafiyeti, bir güvenlik açığı oluşur. Bunların dikkate alınması gerekmektedir.

Ulusal Siber Güvenlik Strateji Bölgeleri'nde "Ortak Riskler" tanımlanmaktadır. Sosyal ağlara bağımlılık, kritik kurum, kuruluşların durumları, konumları, hedefli saldırılar – siber casusluk gibi, personel yetkinlik ve yetersizliği, koordinasyon eksikliği, ekonomik kaygılar ortak riskler olarak değerlendirilmektedir. Ulusal Siber Güvenlik Strateji Belgemiz'de belirtilen siber güvenlik risklerinde birinci sırada "Hedef odaklı saldırılar sonucunda kritik altyapılarımızın; enerji, ulaştırma ve benzeri kritik altyapı hizmetlerimizin kesintiye uğraması" yer alırken, "Kişisel bilgilerimizin, kamuya ait gizli bilgilerin saldırganların eline geçmesi yani bunların korunmasına yönelik riskler" ikinci sırada yer almaktadır.

Siber Güvenlik Strateji Belgemiz'de belirtilen amaç ve hedeflere baktığımız zaman birinci sırada; 5 Eylem Planımız'da da birinci sırada "Siber savunmanın güçlendirilmesi ve kritik altyapıların korunması", ikinci sırada "Siber suçlarla müdahale", üçüncü sırada "Farkındalık ve insan kaynağı geliştirme", dördüncü sırada "Siber güvenlik ekosisteminin geliştirilmesi" – kümelenme diyoruz biz ona –, beşinci sırada "Siber güvenliğin milli güvenliğe entegrasyonu" yer almaktadır. Bunlardan birinci sıradaki kritik altyapılarımızla ilgili korunma konusu devleti ve ulusal ekonomiyi, kritik altyapıları ve toplumu etkileyebilecek güçleri azaltmaya yöneliktir. Kritik altyapılar ülkeden ülkeye değişik konumlarda ve sayılarda tanımlanmaktadır. Ülkemizin strateji belgesinde bu altı grupta; elektronik haberleşme, enerji, su yönetimi, kritik kamu hizmetleri, ulaştırma, bankacılık ve finans şeklinde yer almaktadır.

Siber tehditler yönlerine göre, iç ve dış tehditler şeklinde tanımlanmaktadır. Yine bunlar kaynaklarına göre; insan kaynaklı, çevresel tehditler ve doğa kaynaklı tehditler şeklinde gruplanmaktadır. İç tehditlerde insanların bilgisiz, bilinçsiz, kötü niyetli hareketleri, dış tehditlerde de dışarıdan gelen tehditler değerlendirilmektedir. Günümüzde siber tehditlerin oranı % 80 iç tehditler, yani içimizden gelen tehditler ve % 20 dış tehditler şeklindedir. Siber tehditlerin kaynakları genç kuşak saldırganlardan, dış ülke yönetimlerine kadar sıralanmakta ve kurum çalışanları, yetkili kullanıcılar; yani içimizdeki tehditler ikinci sırada görünmektedir. Bunu dikkatinize sunuyorum. Ve bir soru soruyorum. Kurum, kuruluş temsilcilerimiz var, hepimiz kurum, kuruluşları temsil ediyoruz. "Siber saldırıya uğramayan kurum var mıdır?". Günümüzde iki türlü kurum vardır; siber saldırıya uğrayanlar ve siber saldırıya uğradığını bilmeyenler.

Siber güvenlik açıkları dediğimiz, bu saldırı kaynaklarının, saldırganların kullandığı güvenlik açıklarımız da alt yapı, çevreden, personelle ilgili açıklara kadar yazılım, dokümanlar, donanım açıklıklarını kapsar. Bunlardan istifade ederek saldırılar yapılmaktadır.

Tarihsel sürecine baktığımız zaman siber saldırılar ile ilgili çok ilginç bir durum söz konusudur. Başlangıçta çok basit olan saldırılar günümüzde çok karmaşık ve şiddeti çok ileri seviyelere gelmiş bulunmaktadır. Hem karmaşık, hem şiddetli, hem çeşitli. Her gün yeni bir saldırı türü ortaya çıkmaktadır. Peki, saldırıyı yapanların, saldırganların bilgi seviyesine baktığımızda nasıl bir durum söz konusudur. Burada başta çok yüksek bilgiler gerekirken şimdi iyice çok aşağı seviyelere inmiş durumdadır.

Saldırıların oranlarına baktığımızda en büyük oranı zararlı yazılımlar oluşturmaktadır. Maksatlarında da siber suçlar en fazla oranda yer almaktadır. Dünyada siber olayların meydana gelmesine göre ilk 20 ülke belirlendiğinde ülkemiz ilk onda yer almaktadır ve ilginçtir ki ülkemiz hem saldıran hem de saldırılan ülke olarak ilk ondadır.

Dünyadaki önemli siber saldırıları hatırlayalım:
- 2007'de Estonya saldırıları ve İsrail'in Suriye'ye siber güç destekli hava taarruzu,
- 2008'de Gürcistan'a yapılan siber saldırılar,
- 2010'da İran nükleer sistemlerine yapılan Stuxnet saldırısı,
- 2010'da Wikileaks olayı,
- 2011'de İran Silahlı Kuvvetleri'nin, ABD'ye ait bir insansız hava aracını sapasağlam yere indirmesi,
- 2014'te Sony şirketine yapılan saldırılar,
- 2016'da ABD'nin internet sistemine yapılan saldırılar,
- 2017'de ülkemizi de etkileyen fidye yazılımı saldırıları.

Peki, ülkemizde hangi siber saldırılar olmuştur?
- 2008'de Bakü-Tiflis-Ceyhan boru hattımıza yapılan saldırı,
- 2009'da Atatürk Havalimanı bilgisayarlarını etkileyen saldırılar,
- 2011'de Telekomünikasyon İletişim Kurumu internet sitesinin devre dışı bırakılması,
- 2015'te 79 ilimizi etkileyen elektrik kesintisi,
- 2015'te 10 gün süreyle internet sistemimizi etkileyen saldırılar,
- 2016'da Sağlık Bakanlığı hastanelerine yönelik saldırılar,
- 2018'de internet bankacılığı döviz uygulamalarına yönelik saldırılar.

Bütün bu saldırılara baktığımız zaman siber saldırılarla haberleşme sistemlerinin devre dışı bırakılabileceği, şehrin trafik ışıklarının durdurulabileceği, ulaşım, su sistemlerinin bozulabileceği, bankacılık-finans sektörünün çökertilebileceği, doğal gaz boru hatları ve elektrik şebekelerinin büyük zararlar görebileceği, şehrin baraj kapakları açılarak sular altında kalabileceği ve nükleer santrallerin potansiyel bir atom bombasına dönüştürülebileceği ortaya çıkmaktadır. Evet, alın size siber savaş. Bunların bir de hep birlikte olduğunu düşündüğümüzde felaket söz konusu olabilir. Tabii bunların arkasında internetin icadı büyük rol oynamıştır, zaman - mekân kavramı ortadan kalkmış ve her şey bir tuşa basmaktan ibaret bir hale gelmiştir, bunun için küçük bir ağ bağlantısı yeterlidir. HAVELSAN Genel Müdürümüz 100 dolar dedi ama ben 50 dolar diyorum. 50 dolarlık bir ağla, 50 dolarlık bir sistemle uçak ve füzelerin verdiği zararlar verdirilebilir ve olay yerinde de olmaya hiç gerek yoktur. Kısaca bitler ve baytlar, mermiler ve bombalar kadar tahrip edici olabilir.

Siber savaş, bilgi savaşı, kavramları da çok farklı yerlerde kullanılmaktadır ama günümüzde Birleşmiş Milletler Terimler Sözlüğü'nde bunlar eş anlamlı olarak tanımlanmış durumdadır. Artık eş anlamlı olarak siber savaş daha geniş anlamda kullanılmaktadır. Düşmanın bilgilerine, verilerine zarar vermek, kendi bilgilerimizi de, bilgi sistemlerimizi de korumak anlamında Birleşmiş Milletler Terimler Sözlüğü'nde ifade bulunmaktadır. Geniş bir tanım olarak da devlet benzeri aktörler tarafından bilişim sistemlerine yapılan saldırılar ve bunlara karşı alınan güvenlik tedbirleri şeklinde tanımlayabiliriz. Tek başına da siber savaşlar yapılabilir. Hibrit savaş içerisinde, çok katmanlı savaş içerisinde diğer savaş teknikleri ile birlikte de bu kullanılabilir, yapılabilir. Ve klasik savaş ile karşılaştırdığımızda pek çok benzerlikler de içermekle birlikte üstünlükler de siber savaşta söz konusudur. Özellikle maliyet ve saldırı belirtileri konusunda. Maliyet düşük olabilir, saldırının farkına varılmayabilir.

Harekât çeşitleri ve özelliklerine baktığımızda klasik savaşta sadece silah, mermi farklılığı var. Siber savaşta ise silah, merminin yerini bilişim teknolojileri ve yazılımlar almış durumda. Ve düşünmemiz gereken çok önemli bir konu, henüz en güçlü ülkelerin en gelişkin siber silahlarını kullandığı türden bir siber savaş gerçeklemedi.

Caydırıcılık konusuna gelecek olursak; savaş önemli. Savaşı kazanmak, karşı tarafa isteklerimizi kabul ettirmek için gerekli. Ama savaşta mükemmeli, savaşı hep kazanmak olmayabilir. Milattan önce 500'lü yıllarda Çinli stratejist diyor ki: "En iyisi savaşmadan baş eğdirmektir." Ondan yaklaşık 1000 yıl sonra Anadolu topraklarımızda yaşayan Doğu Romalı ünlü komutan Belisarius diyor ki: "En mükemmel ve mutlu zafer şudur: Kendiniz bir zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmak." Siber güvenlik, siber saldırılar, taarruz demiştik buna bir de siber caydırıcılık eklenmiş durumdadır. Strateji belgelerimizde henüz yer almamakla birlikte dünyaya baktığımızda uluslararası strateji belgelerinde çok sık yer almaktadır. 2016 yılında da

Bilgi Teknolojileri ve İletişim Kurumumuza kanun hükmünde kararname ile şu görev verilmiş durumda: Kurumu, kurum ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması ve bu saldırılara karşı caydırıcılık sağlamak için her türlü tedbiri alır veya aldırır. Bu konuda da çalışmalarını Bilgi ve İletişim Kurumumuz biraz önce başkanımızın da değindiği gibi sürdürmekte. Yine aynı günlerde Başbakanımız da "siber saldırılarla caydırıcılık da geliştirilecek" diye ifade etmiştir. Nedir; genellikle korkutarak cesaret kırmak veya vazgeçirmek anlamında kullanılan "caydırmak" sözcüğünden çıkan caydırıcılık Türk Dil Kurumu sözlüğümüzde bir saldırganlığı önlemek ve engellemek için önlem alma işi olarak tanımlanmaktadır. Günlük hayatımızda biz bunun zaten içerisindeyiz. Hukukta suç işlemekten alıkoyma, diplomaside karşıdaki devleti emellerinden vazgeçirme, askeri anlamda da düşmanı herhangi bir hareketten vazgeçirmek için ortaya konan stratejidir. Caydırıcılık konusunda bir örnek verecek olursak silahlı kuvvetlerimizin internet sayfasında özellikle ikinci sırada vurgulanmıştır. 1998 yılında PKK Bölücü Terör Örgütü Başının Suriye'den çıkarılması ülkemizin caydırıcılık konusundaki tutum, davranış ve kararlılığı sonucu gerçekleştiğini hatırlarız.

Siber caydırıcılık konusuna bunlardan sonra gelecek olursak, karşı tarafa saldırılarda bulunmama konusunda gözdağı verme şeklinde tanımlayan Amerikalı akademisyen Libicki siber caydırıcılığı siber ortamda saldırganın eylemini boşa çıkarma veya cezalandırma yoluyla saldırıdan vazgeçirme şeklinde tanımlamıştır. Bu, geniş bir biçimde tanımlayacak olursak, düşmanı siber güç kullanarak maliyet / fayda hesaplamalarına yönelterek, faydalarını azaltıp masraflarını artırarak eylem yapmaktan kaçınmaya ikna etmek şeklinde tanımlayabiliriz. Ve siber caydırıcılık şiddeti nükleer ve fiziki caydırıcılıktan sonra gelmektedir.

Bütün bu yaşanan olaylara rağmen "Siber savaş, savaş mıdır değil midir?" ve "Siber savaşla siber caydırıcılık mümkün mü?" diye maalesef hala tartışılmaktadır. Nükleer savaşı önlemenin olmazsa olmazı olan caydırıcılığın siber savaşa uygulanamayacağı konuşulmaktadır. Hatta buna örnek olarak da ABD siber saldırılarda, strateji belgelerinde "ben basit askeri tedbirleri de kullanacağım" demesi gösterilmekte yani siber güçle caydıramıyor, askeri güçle caydıracak denilmekte. Ama gerçek olan şudur; hayatı kolaylaştıran siber güç aynı zamanda tehdit ve yaptırım aracı olarak kullanılabilir. Siber gücü savunma maliyetleri yüksek, taarruz maliyetleri düşük olacak şekilde formüle edebiliriz. En iyi savunma taarruzdur düşüncesiyle hareket edilerek en iyi şekilde kullanılabilir.

Siber caydırıcılıkta hedef devletten devlete, kurum / kuruluşlara, kişilere, toplumlara şeklinde olabileceği gibi tersine de olması mümkün. Ve siber caydırıcılık önleyici güvenlik tedbiri olarak kullanılabilmekte, tek başına kullanılabilmekte, diğer unsurlarla yine yaptırım aracı olarak kullanılabilmekte.
Siber caydırıcılık üç temel yöntemle sağlanır:

- Güçlü bir güvenlik ve savunma,
- Saldırganın tespiti, istihbarat yetenekleri ve bunun duyurulması,
- Saldırganın cezalandırılması.

Siber caydırıcılığa en güzel örneklerden birisi, 2014'te Sony şirketine yapılan saldırılardır. Sony tarafından 2014 yılında Kuzey Kore lideriyle ilgili "Röportaj" adlı film gösterime sokulmuş, Kuzey Kore'de tepkiyle karşılanması ve yapılan siber saldırılar sonucu film gösterimden kaldırılmıştı. Saldırılar önce e-postalarla kendini gösterdi. Şirket çalışanlarının kişisel verileri, bilgileri, yazışmaları internette yayınlanmaya başladı. 100 terabayttan fazla bilgi çalındı. Çekimi bile yapılmamış film senaryoları internet ortamında yayınlandı. Yöneticilere ve çalışanlara e-postalarla ve çeşitli yollarla tepki postaları gönderildi. Film oyuncularına, filmi vizyona sokmayı planlayan sinema salonlarına açıkça yine siber ortam kullanılarak tehditler yapıldı. ABD Federal Soruşturma Bürosu saldırılara karşı tedbir alınması gerektiği uyarısında bulundu. Kişisel verileri korunmadığı gerekçesiyle 15 bine yakın Sony çalışanı Sony şirketini mahkemeye verdi. Ülkenin en büyük sinema zincirleri filmin vizyona girdiği hafta filmi göstermekten vazgeçti. Sony, 90 milyon dolara mal olan filmi geri çekmekten başka çaresi kalmayınca, yayınladığı bildiriyle "ortaklarımızın kararını anlıyor, çalışanlarımızın ve sinemaseverlerin güvenliğine önem veriyoruz" diyerek bu filmi gösterimden kaldırdı. Tüm bu gelişmelerin ardından Sony şirketinin 210 milyon dolara yakın zararının ortaya çıktığı ifade edilmektedir. FBI, Kuzey Kore ile bağlantılı olduğunu ve şirketlerin hala risk altında olabileceğini açıklarken ABD yönetimi, ulusal güvenlik meselesi olarak konuyu değerlendirmiş, dönemin başkanı, saldırıların ardında Kuzey Kore'nin olduğuna inandıklarını söylemiştir. Bütün bu saldırı olayları 28 gün sürdü. 28 gün içerisinde Sony gibi uluslararası bir şirkete geri adım attırıldı. ABD'nin Temsilciler Meclisi Başkanı, "Sony'nin kararıyla ABD ilk siber savaş yenilgisini aldı." şeklinde ciddi bir ifade kullanmak zorunda kaldı. Kuzey Kore ise "Saldırı bize ait değil, ama olumlu karşılıyoruz" diye açıklama yaptı. Sonuçta siber saldırılarla, siber caydırıcılıkla hedefe ulaşılmış, "Küresel Dev" Sony bu filmi yayından kaldırmış, yani caydırıcılık sağlanmış, istekler kabul edilerek geri adım attırılmıştır. Bu saldırılar başarılı bir siber istihbarat yöntemleriyle gerçekleştirilmiştir. Eski çalışanlar kullanılmış, onların açıklarından istifade edilmiş, Sony'nin önceden tespit etmesine rağmen kapatmadığı güvenlik açıkları kullanılmış, hedef odaklı saldırılar yapılmıştır. Bunlara ek olarak psikolojik harekât yapılmış, teknoloji, medya, tanınmış artist - oyuncular kullanılmış ve caydırıcılık bu şekilde sağlanmıştır.

Sonuç olarak siber uzayda sınır tanımayan ve insanının tahayyül sınırlarını, hayal sınırlarını zorlayan gelişmeler yaşanmaktadır. Başlangıçta küçük çapta, zararsız

denilebilecek saldırılar, günümüzde teknolojinin gelişmesi ve internetin de yaygınlaşmasıyla siber savaş halini almış durumdadır. Siber ortamın tehlikelerinin farkında olan ülkeler buna yönelik olarak tedbirler geliştirmekte, stratejiler üretmekte, çözümler ortaya koymaktadır.

Siber savaşı küçümseyip bu konuda ciddi çalışmalar içerisinde olmayanlar, gerekli adımları atmayan ülkeler geç kalmıştır ve çok zor bir gelecek onları beklemektedir. Siber güvenliğin etkin şekilde sağlanması, siber gücün sağladığı imkân ve olanaklardan en iyi şekilde yararlanmak için çalışmalar aralıksız kararlılıkla sürdürülmelidir.

Siber güç kullanarak talep ve istekler karşı tarafa kabul ettirilebilir çünkü caydırıcılık(asimetrik etki) sağlamakta, bunu düşünmek zorundayız. Siber güvenliğin ve gücün artırılarak etkin yönetim ve denetim sağlanması için son ulusal siber güvenlik strateji belgemizde de belirtildiği üzere siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması kaçınılmaz bir zorunluluktur.

Önce Siber Güvenlik, yani siber savunma sonra siber saldırı yani taarruz ve caydırıcılık, ulusal güvenlik stratejileri bunun için oluşturulmalı ve karlılıkla uygulanmalıdır. Son sözümüz: “Siber caydırıcılıkta temel esas ve önemli olan; siber saldırıların / savaşın doğru zamanda, doğru hedefe yönelik, doğru teknik ve yöntemlerle icrasıdır.” Bunu yaptığımızda siber caydırıcılık sağlarız.

Beni sabırla dinlediğiniz için teşekkür ediyorum. Hepinizi saygı ve sevgiyle selamlıyorum.


Devletlerin birbirlerin
Moderatör:
Doç. Dr. Ahmet Hasan KÜLTÜKSÜZ
Tuğg. Engin ÇIRAKOĞLU
Dr. Alb. Hasan ÇİFCİ
İhsan ERDOĞAN

Moderator:
Doç. Dr. Ahmet Hasan KOLTUKSUZ
Yaşar Üniversitesi Bilgisayar Mühendisliği Öğretim Görevlisi

Tuğgeneral Engin ÇIRAKOĞLU
Jandarma MEBS Başkanı

Dr. Alb. Hasan ÇİFCİ
Hava Kuvvetleri Araştırma Merkezi Şube Müdürü

PANEL 1

Günümüzün ve Geleceğin Siber Savaşları

İhsan ERDOĞAN
Emniyet Siber Suçlarla Mücadele Daire Başkan Yardımcısı

Mustafa DAYIOĞLU
TÜBİTAK, Siber Güvenlik Direktörü

Doç. Dr Ahmet Hasan Koltuksuz:

Değerli başkanlarımızı, komutanlarımızı selamlıyorum. Üniversite yıllarında ders alırken hemen her hocamız ilgili konuda dersine başlamadan önce başlangıcı, o konunun geçmişine, yapılan önemli buluşlara ve bu buluşları yapan kişilere ayırıp geçmişe yönelik bir takım bilgiler aktarıyordu. Ben itiraf edeyim, o yıllarda pek bunun önemini kavramadım. Doktoramı yaparken aktif olarak araştırma hayatına girdiğimde fark ettim ki, bir konunun eğer ne şekilde geliştirildiğini, tarihsel bağlantılarını, klasik bir takım yapılan çalışmaları ve bu çalışmaları yapan insanların hangi amaçla, neyi düşünerek, neyi ne şekilde oluşturduklarını eğer incelemiyorsanız, bilmiyorsanız ya da daha açık bir deyimle, terimle yakın geçmişi bilmiyorsanız, çalıştığınız konuda o günü kavramak, o günü anlamak gerçekten mümkün olmuyor. Dahası günü de kavrayamadığınız, güncel teknolojileri ve bilimi yorumlayamadığınız için ileriye doğru da bakamıyorsunuz. İşte bu da bir vizyon eksikliği olarak sık sık karşımıza çıkan konulardan bir tanesi. Ben çok vaktinizi almayacağım, değerli panelistlerimiz size birçok konularda bilgi aktaracaklar. Tartışacağız biraz huzurlarınızda, ben siber savaşın bugün geldiğimiz noktadan itibaren geldiğimiz noktaya kadar bir takım köşe taşlarında neler var onları sizlere çok kısaca arz edeceğim.

Strateji ve taktik uzmanı, yazar, filozof, Çinli general Sun Tzu'nun hemen hemen her dile çevrilmiş "Savaş Sanatı" adında bir kitabı vardır. Okumanızı hararetle öneririm. Ve ilginçtir bu konuda birkaç sene önce bir yayınımız da olmuştu. Bugünkü siber savaşla Sun Tzu'nun ilkelerini karşı karşıya getirdiğinizde işte birkaç bin sene öncesinden dahi bugünlerin öngörülebildiğini görüp gerçekten insan ders alabiliyor.

Clausewitz, bugün anladığımız anlamda iki boyutlu savaşın mimarlarından bir tanesidir ve literatür olarak baktığımızda da "Savaş Üzerine" adlı kitabında çok net olarak karasal savaşların bugünkü itibariyle lojistiğinden tutun da sevk ve harekata kadar her şeyin gerçekten çok iyi tanımlandığını görürsünüz. Temin edip okumanızı bu konuda öneririm.

Hemen arkasından yine iki boyutlu alan savaşında bir savaş dâhisi var: Mustafa Kemal. Bir hat üzerindeki cephe savaşını hattan yeni tek boyuttan çıkarıp alan savunması ya da alan saldırısı olarak "Hatt-ı müdafaa yoktur sath-ı müdafaa vardır" sözüyle tanımlamıştır. Savaş doktrinlerini eğer incelerseniz Mustafa Kemal'in bu yaklaşımı iki boyutlu alan savaşları içerisinde köşe taşlarından bir tanesidir.

İki boyutlu alan savaşının teknolojik olarak nasıl geliştiği ya da teknolojiyle iki boyutlu savaşın nasıl iç içe girdiğini göstermesi açısından çok kritik çalışmalar var. Bunların bir tanesinde kabaca 40.000 km2'yi kontrol etmek için kaç askere ihtiyaç duyarsınız diye bir çalışma yapılmış. Tarih olarak 1865'te, Amerikan İç Savaşı'nın olduğu bu dönem telgraf var gündemde ve iletim hızı olarak da işte saniyede 20 bitlik bir hızınız var. Ve bu çerçevede bakıyorsunuz kontrol etmeniz gereken 10 km2'lik bir alan için kullanacağınız asker sayısı 40.000 olmuş. 10 km2'lik bir alan için 40.000 kişiyi kullanıyorsunuz. Tarihte hızla ilerlediğimizde 1.Dünya Savaşı geliyor 1914 yılında, teknoloji olarak telefon var. Bilgi iletim hızı 32 bite çıkmış durumda ve aynı şekilde 10 km2'yi kontrol etmek için artık gereken asker sayısı dramatik bir şekilde 38.000 - 40.000'den 4.000'e iniyor hemen çok kısa bir sürede. Tarih içinde ilerleyin, arkasından 2.Dünya Savaşı var. Bilgisayarın gerçek anlamda ortaya çıktığı bir dönemdir. Hız 71 bitlerde saniyede ve artık 10 km2 için 300 kişi çok rahatlıkla yeterli bir hale geliyor. Tabii ilerlerseniz günümüzde artık 10 km2 'nin kontrolü için artık insan falan kullanmıyorsunuz, bırakın 10 km2 'yi koca ülkelerin yüz ölçümlerine baktığınızda insansız kontrol edebilir hale geldik. Alan savaşının teknoloji ile iç içe girdiğinde nasıl değiştiğini görme açısından ilginç bir örnek.

3. boyuta geçerken yine bir vizyoner var; Mustafa Kemal Atatürk ve diyor ki: "İstikbal göklerdedir." Evet, doğrudur. Çünkü hâkim olduğunuz her yeni boyutla askeri gücünüz de çok ciddi bir biçimde, dramatik bir biçimde artıyor. Denizaltılar bir tarafta 3. boyutta suyun içinde hareket ediyorsunuz, suyun yüzeyinde değil. Ve aynı şekilde de sadece karada değil havadasınız. Dolayısıyla 3 boyutta savaş söz konusu. Bunlar savaş tarihi, savaş doktrinleri incelediğimiz zaman gördüğümüz kilometre taşları.

4. Boyut olarak hep uzaydan bahsettik. Uluslararası Uzay İstasyonu'nun, ISS'in finansmanını ağırlıklı olarak Amerika, Rusya, Kanada, Fransa, İngiltere yapıyorlar. Amerika'nın geçenlerde bir açıklaması oldu; "Ben ISS'i 2020 yılında da finanse edeceğim ama 2020'den sonra finansmanı kesiyorum, teknik destek veririm, lojistik destek veririm. Fakat herhangi bir finans desteği sağlamayacağım." Çünkü gerekçe olarak da NASA planları var. 2025'ten itibaren ayın etrafına uzay karakolları kurulması gündemde. Yani aslında bakacak olursanız uzay savaşında bir adım daha öteye gidiliyor. Hepimizin uydusu olan ayın etrafına birtakım karakollar kurulmaya başlanacak 2025'ten itibaren. ISS'in de finansmanından Amerika bu nedenle çekildi. Bu açıklama da geçen ay yapıldı.

5. Boyut olarak baktığımızda siber savaş ortamına, siber savaşa, siber uzaya gidiyoruz. Peki, bu yeni mi? Siber savaş aslında yeni değil. Bugün kullandığımız bütün bilgi işlem cihazlarının; bilgisayarlar, elinizdeki cep telefonları, hepsinde kullanılan bellek mimarisi John von Neumann'ındır. Ve John von Neumann 1949 yılında yaptığı bir konuşma - aslında 1946 yılında yapılmış bir konuşmadır- ölümünden sonra kâğıda geçirildi, 1949 yılına tarihleniyor, diyor ki; "Bakın siz benim bellek modelimi kullanacaksınız ama bu modele göre bellekte çalışan, bellekte olan herhangi bir program bir başka programa saldırabilir. Dahası yok edebilir. Ya da bir program bir başka program tarafından kontrol edilebilir." Tabii John von Neumann bunu söylediğinde kimseler pek bir şey anlamamış ama biz bugün bu problemi bilgisayar virüsleri olarak tanıyoruz. Yani aslına bakacak olursanız, 1949 yılından itibaren bunlar bizim önümüzdeydi.

Bilim kurgu yazarı John Brunner'ın, Shockwave Rider isimli Türkçe'ye de çevrilen kitabında, adına internet denmese de internet ortamı tanımlanmıştı ve bu ortamın içerisinde düğümden düğüme atlaya atlaya hiçbir şekilde yok edilemeyen, yok etmeye kalktığınızda tekrar kendi kopyasını üreten ve kendi kendini bir noktadan ötekine taşıyabilen programlardan bahsediliyor. Brunner bu programlara solucan ya da kurtçuk, İngilizcesine worm adını verdi. O gün bugündür biz solucan ya da kurtçuk ismini kullanıyoruz. Gelişmiş kitlelere uygun, bu işi bilen insanların eline geldiğinde "Evet ya, biz bunu yapabiliriz" düşüncesi oluşmasına sebep olmuştur. Gerçekten kendi adıma da söyleyeyim "ya bu solucan programı nasıl yazılır, ben bunu nasıl yapabilirim?" diye çalışma, bu kitabı okuduktan sonra bende başladı doktoramın ilk yılında. İlk yazdığım solucan programı da bu kitabın sonundadır.

William Gibson 1982'de yayınlanan Neuromancer adlı kitabında siber uzay terimini kullanır. Bugün çok iyi bildiğimiz bu ortam için Gibson: "Zihnin uzaysızlığında; ışık çizgileri, öbekler ve takımyıldızlar şeklinde düzenlenen veriler..." diyordu. Tam anlamıyla aslında internet bu. Ama işin ilginç tarafı bu 1982'de yazıldı ve eğer bu kitabı okursanız, yer altında bir mafya var ve bu mafya bugün adına Firewall dediğimiz programlarla geçitleri kontrol ediyor. Bugün kripto paralar, bitcoinler gibi paranın aktarılması diye kullandığımız şeyleri bu kitapta görebilirsiniz. Bir başka bakış açısıyla, aslında yazılım güvenliği, bilgisayar güvenliği eski adıyla bilgisayar insurance bir takım terimler 80'li, 90'lı yıllarda bunları çalışırken bu kitaplar aslında bize yol gösterdi. Bu anlamda hepsi son derece kritiktir. Siber savaş üzerine de tanım yapılmış bu çalışmada. Diyor ki "siber savaş siber uzayda, bilgisayarlar ve internetin kullanılmasıyla yapılan bir savaştır." Evet, siber uzayın tanımı varsa elinizde bu siber uzayın üzerinde de siz bir takım programları ötekine karşı saldırtıyorsanız şu ya da bu amaçla aslında yaptığınız şey bir siber saldırıdır. Bunu topyekûn yapıyorsanız bir siber savaştan da söz edilebilir.

Meşhur siber savaş örneklerinden biri Rusya'nın, Tallinn - Estonya'ya yaptığı saldırıdır. Bir Lenin heykelinin kaldırılması yüzünden başlayan tartışmaların sonucunda gerçekleşmiştir. Tarihte tamamen sayısal yönetimi oluşturan, devletin bütün birimlerinin sayısal ortama taşındığı ilk ülkedir Estonya. Bunlarla övünüyorlardı, hala da övünürler ama bu olaydan sonra Estonya'da pek çok birim çalışamaz hale geldi.

Amerika'nın, İran'ın Nükleer zenginleştirme tesislerine yaptığı saldırı. Bu aslında bizim Stuxnet dediğimiz saldırıdır. Bu saldırının sonucunda da bu nükleer zenginleştirmede kullanılan santrifüj pompaları kullanılamaz hale geldi ve İran'ın nükleer zenginleştirme programı 2 yıl kadar geriye gitti. Bunun dolar olarak kaybına bakacak olursanız da yüz milyonlarca doları İran kaybetti. Ama burada kritik olarak biz şunu öğrendik, böyle bir olayda siz donanımların, donanım birimlerinin, santrifüj pompalarının içinde dönüşü kontrol eden PLC gibi, kontrolünü ele geçirebilirsiniz. Belirgin bir hızdan sonra durması gerekirken durmadan devam ediyor ve santrifüj üreterek dağılıp gidiyor pompalar.

Bu olay bize şunu öğretti; demek ki dedik artık saldırı sadece yazılım ya da önlem sadece yazılımla olmayacak bunun bir donanım katmanı var, donanım tarafında da işleri bu hale getirmek mümkün. Bu anlamda tarihsel önemi bakımından bu Stuxnet saldırısı tarihe geçti. Tabii komutanlarımın gördüğü, bizim izlediğimiz şu, bunun üzerine bir sürü başka tehditler, başka bir sürü saldırılar var ama tarihsel açıdan bu kritik.

Birçok internet sitesi siber savaşları anlık olarak göstermeye çalışıyor. Aslına bakacak olursanız bu web sitelerinin hemen hepsi, Akamai hariç hemen hepsi anlık bilgi vermez, gerçek zamanlı bilgi vermez. Üç günlük, bir haftalık ya da bir aylık DDoS saldırılarını size gösterirler. Ama gerçek zamanlı olarak bilgi akışını sağlayan Akamai Grup çünkü bu grup zaten internet trafiğinin üçte ikisini ellerinde tutuyorlar. Dolayısıyla da gerçek zamanlı olarak kimin kime ne ölçüde hangi sıklıkla DDoS saldırısı yaptığını, sonuçların ne olduğu gibisinden bir takım veriler almak istiyorsanız bu siteler iyi ama Akamai'yı gerçekten öneririm. Diğerlerine de bakmanızda büyük bir fayda var. Evet, belki üç gün öncesinin ya da üç günün toplam saldırılarını görecek olursunuz bu sitelere girdiğinizde ama bu bize çok net bir fikir

verir. Siber savaş dediğimizde aslında gözünüzün görmediği, kulağınızın duymadığı ama ulus devletlerin birbirlerine karşı nasıl saldırdıklarını, arada sadece ticari şirketler değil ciddi bir biçimde ulus devletlerin tehdit güçleri de var. Daha görselleştirmiş olarak yakından izlemek mümkün. Umuyorum, inanıyorum ki çok yakın zamanda - birkaç seneyi bulacağını sanmıyorum - bu web siteleri içerisinde üç dört tane de Türk sitesi olacak. Kendi verilerimizi de oradan daha gerçekçi olarak izleyeceğiz.

Teşekkür ederim. Hepimizi ortak bir tarihsel geçmişte buluşturmak istedim ki değerli panelistlerimiz tartışmaları sırasında bizlere yol göstersinler. Hem bugünün değerlendirmesini daha sağlıklı alalım hem de ileriye doğru belki biz vizyonla çıkarız bu panelin sonunda.

Efendim tekrar teşekkür ediyorum. Şimdi panele sözü bırakacağım. Hasan Albayım yakınlarda bir kitap yazdı, "Siber Savaş" diye. Bakın Türk kitabımız var kitapçılarımızda. Dolayısıyla biz, Hasan Albayımdan bir dinleyelim. Nedir bu siber savaş, siber savaşın bileşenleri nedir, oyuncuları kimlerdir, savaşanları, askerleri kimlerdir? Hemen tanımları bir alalım onun üzerine de tekrar devam ederiz. Buyurun efendim.

Dr. Alb. Hasan Çifci:

Sayın Komutanım, değerli protokol üyeleri ve değerli katılımcılar; konuşmamı temel tanım ve kavramlar, siber savaşta neler olabilir, siber saldırıların maddi boyutu ve örnek saldırılar başlıkları altında arz edeceğim panelin bu bölümünde.

Siber ortam ya da siber alan, bazen siber uzay – cyber space olarak da adlandırılıyor, bu tamamen bildiğimiz uzaydan farklı bir kavram. Bu her türlü yazılım, donanım ve iletişim altyapısından meydana gelen, birbirine bağlı veya bağımsız sistemlerinin oluşturduğu sayısal ortamdır. Bu kara, deniz, hava ve uzayın yanı sıra "siber ortam" beşinci harekât alanı olarak kabul edilmektedir. Bu şu manaya geliyor; siz nasıl ki diğer alanlar için birlik geliştirip, teşkilat kurup, eğitim verip donatıyorsanız siber alan için de hem savunma hem de saldırı kabiliyetinizin olması gerekiyor.

Siber savaşın tanımına baktığımızda burada benim benimsediğim tanım, devletlerin birbirlerine karşı yürüttüğü siber saldırı faaliyetleridir. Diğerleri siber saldırı tanımına girmektedir. Eğer siber saldırının arkasında kimin olduğu çoğu zaman bilinmemekle beraber devletler bu işin içerisindeyse siber savaş ismi verilmektedir.

Siber tehdit kaynaklarına baktığımızda bunlar; bilinçsiz kullanıcılar, casuslar, organize suç örgütleri, terör örgütleri, siber korsanlar, ideolojik amaçlı gruplar ve devletler olduğunu görüyoruz. Bu tehditler neler peki? Bu tehditler; her türlü zararlı yazılım, yazılımın ötesinde tuzaklı donanımlar, oltalama saldırıları, internet servis saldırıları, hizmet dışı bırakma saldırıları ve gelişmiş siber tehditler.

Siber savaşta neler olabilir acaba? Biz hep siber savaş tarafını kullanıcı olarak önümüzdeki bilgisayara virüs bulaşması ve dosyalarımızın silinmesi olarak algılıyoruz çoğunlukla ama siber savaşta bunun -gerçekten örneklerini de birazdan arz edeceğim- gerçekten alt yapıyı önemli bir biçimde etkileyebilecek etkileri olabilir. Rafinerilerde ve nükleer tesislerde yangın çıkıp, patlama olabilir. 2010 yılında İran'ın nükleer tesislerine yapılan saldırı bunlardan bir tanesiydi. Fiziksel olarak tesisi hasara uğratmıştır. Hava trafik kontrol sistemlerinde meydana gelen hatalı ve zararlı çalışmalarından dolayı uçaklar havada çarpışabilir. Bankalar çalışmaz hale gelebilir, müşteri verileri çalınabilir, silinebilir. Trenler birbiriyle çarpışabilir, raylar yolundan çıkabilir, hatalı yönlere sevk edilebilir. Elektrikler kesilebilir ve elektrikle çalışan sistem ve ev aletleri bu süre boyunca kullanılamaz. Örneğin 2015 yılında Ukrayna'da elektrik santrali siber saldırıyla devre dışı bırakılmış, bir müddet elektrikler kesilmişti. Uydu sistemleri ele geçirilebilir. Uydulardan meteoroloji olarak, GPS seyrüsefer olarak, iletişim uyduları ve diğer uydular kullanılarak faydalanıyoruz. Bunlar düşürülebilir. Veya yörüngesinden çıkartılıp saptırılabilir. Petrol ve doğalgaz boru hatlarında patlamalar meydana gelebilir. Ve internet kesilebilir. İnternet üzerinde yapılan faaliyetlerin günümüzün küresel dünyasında hem hizmetin aksaması açısından hem de ekonomik açıdan milyar dolarlık değeri olduğu ortada.

Siber saldırıların maddi boyutuna baktığımızda 2015 yılında bu para senede 75 milyar dolarken önümüzdeki sene bunun 170 milyar dolara kadar çıkacağı değerlendiriliyor. Farklı kaynaklar farklı rakamlar vermekle beraber senede siber saldırılarının maliyetinin 400 ile 500 milyar dolar arasında değiştiği ifade ediliyor.

Bu kısımda örnek siber saldırılardan bahsederek gerçek resmi ortaya koymaya çalışacağım. 2009 yılında F-35 uçaklarının tasarımlarını içeren terabaytlar boyutunda verinin Çin'in yaptığı siber saldırılarla ele geçirildiği iddia edilmiş, 2015 yılında Amerikan Milli Güvenlik Ajansı NSA çalışanı Edward Snowden'in açıkladığı belgelerle de Çin'in 2007 yılından itibaren bu gizli belgeleri uçağı üreten Lockheed Martin firmasından çaldığına dair deliller basına yansımıştır. Burada terabaytlar boyutunda veri çalındıktan sonra iki uçak arasındaki benzerliği

görüyorsunuz. Ben de F-35 projesinde çalıştım, aviyonik sistem, dış görünüşü, düşük görünümlü hale getirebilmek için bazı şeyleri benzer yapmanız gerekiyor ama aviyonik sistemlerde de bir kısmında benzerlik olduğu basına yansımış durumda.

Stuxnet saldırısı fiziksel zarar vermesi açısından sürekli örnek verilebilecek bir saldırıdır. 1981 yılında Opera Harekatı'nda İsrail jetleri yapım aşamasında olan Irak -İran değil- Irak nükleer reaktörünü vurmuştu. Harekât yüksek risk altında, iki tane ülkenin hava sahasını kat ederek gerçekleştirilmiş ve büyük maliyetlere ulaşmıştır. Can kayıpları da olabilirdi.

2010 yılında ise dünyada çeşitli ülkelerde rastlanan Stuxnet adlı bir virüs İran'ın nükleer santraline sızmış, kumanda sistemlerini etkileyerek santrifüj adı verilen cihazların bir kısmı kullanılamaz hale getirmişti. Stuxnet ile beraber zararlı yazılımların kişisel bilgeleri çalma ya da bilgi sitemlerine zarar verme dışında, dış dünyaya kapalı kritik alt yapılara fiziki olarak zarar verebileceği ortaya çıkmıştır. Stuxnet sadece bilgisayarların değil endüstriyel kontrol sistemlerinin ve dış dünyaya kapalı sistemlerin hedef alınması ve bunda da başarılı olunması açısından çok önemli bir yere sahiptir. Stuxnet'i resmi olarak üstlenen ülke olmasa da İsrail ve Amerikalı uzmanlar tarafından geliştirildiğine yönelik birçok bilgi ve belge basına yansımıştır. Burada da görüldüğü üzere bombalarla yapılan saldırılar virüs kodlarıyla yapılmış ve belirli ölçüde başarıya ulaşılmıştır.

2012 yılından ve günümüzden bir örnek vereyim. 2012 yılında Aramco firması, Suudi sektör firmasına saldırı yapılıyor ve buradaki 30.000 bilgisayarın 4'te üçüne bulaşan virüs, bilgileri siliyor, yerlerine yanmış Amerikan bayrağı koyuyor. İranlı siber korsanlar (Kendilerine Shamoon ismi verilen "Adaletin Keskin Kılıcı") tarafından gerçekleştirilen bir saldırı.

Geçtiğimiz günlerde bir firmaya ait bir rafineri seyir füzesi, insansız hava aracı tarafından vuruldu. Bu defa fiziksel etkiler siber etkilerin çok üzerinde oldu. Ancak başarılı olsaydı siber etkileri daha kısa olmakla birlikte benzer bir etkiye yol açabileceği iddia edilmektedir.

Bir başka örnek; bankacılık sistemlerine yapılan saldırıydı ve yaklaşık 3 gün boyunca bu bankalara erişimde sıkıntılar yaşandı.

2014 yılında Türkiye'nin de aralarında olduğu 16 ülkeye siber saldırılar gerçekleştirildi. Burada hava yolları, enerji ve petrol firmaları, savunma sanayi firmaları ve Amerikan'ın Deniz Piyadeleri yani silahlı kuvvetlere ait intranet ağı hedef alındı. Saldırganlar kriptografi kodda "Şeytan gibi düşün melek gibi uygula!" şeklinde bir kodlama yapmışlardı.

Başka bir örnek baraj örneği. New York'ta 2013 yılında Bowman Barajı'na bir siber saldırı gerçekleştiriliyor. Kontrol sistemleri barajdan alınan su miktarını artırma görevi gördü ve tehlikenin ucuz atlatıldığı görülüyor. Ülkemizde de çok sayıda siber saldırılar oldu. 2015 yılında Mayıs ayında özellikle ülkemizin devlet kurumlarına ait internet sitelerine dağıtık hizmet dışı bırakma saldırıları düzenlenmiş, 3 gün boyunca internet hızı oldukça yavaşlamıştır. Saldırıların 12 farklı ülkeden geldiği görülmüştür.

İlk bölümde konuşmamı tamamlarken şunu arz etmek istiyorum, şimdiye kadar yaşanan tecrübelerden hareketle siber saldırıların kinetik saldırılar kadar etkili olabileceği görülmektedir.

Doç. Dr. Ahmet Hasan Koltuksuz:

Çok teşekkür ederiz. Jandarma MEBS Başkanımız da bizlerle, kendisine şunu soracağım; siber savaşları etkileyen faktörler neler, günümüzde siber savaşlar nasıl yapılıyor? Bu konuda bizi aydınlatabilirseniz çok sevinirim. Buyurun, efendim.

Tuğgeneral Engin Çırakoğlu:

Sayın Komutanım, değerli katılımcılar, öncelikle siber saldırılarda meşru müdafaa hakkından kısaca bahsetmek istiyorum. Çünkü ben görevi devraldığımda Jandarma Genel Komutanlığı'nda Siber Savunma Şube vardı. Bu şubenin ismini Siber Güvenlik Komutanlığı'na dönüştürdüm. Yani sadece savunma değil gerektiğinde taarruz etme yeteneğine de sahip. 2007 yılında bizden önceki konuşmacıların da söylediği gibi bu örnekleri siber dünyada, siber savaşlarda sıkça duyacaksınız, Estonya saldırısı çok önemli bir saldırıdır. Bilgi sistemlerini alt yapısına alan ve yaklaşık 85.000 botnet saldırısıyla yapılan bu saldırı sonucunda NATO bünyesinde oluşturulan çalışma grubu tarafından Tallinn rehberi hazırlanmıştır. Siber saldırıların bir kuvvet kullanımı olup olmadığını ele alan yaklaşımlardan, etki odaklı yaklaşım bu kabul edilmiştir ve siber saldırı etkileri bakımından bir konvansiyonel silahın kullanılmasıyla aynı sonuçlar ortaya çıkarıyorsa bir silahlı kuvvet kullanımı olarak tanımlanmış ve meşru müdafaa hakkının konvansiyonel silahların da dâhil olduğu bütün güç unsurlarıyla kullanılabileceğini ortaya

koymuştur. Dolayısıyla sadece savunmada kalmak yetmiyor, caydırıcı olması açısından sizin gücünüzü bilecekler ki saldırmayacaklar. Dolayısıyla bize saldırı düzenleyene saldırı düzenleyip bayrağımızı oraya koyma gücüne de sahibiz artık şükürler olsun.

Siber silahların kısıtlarından da kısaca bahsetmek istiyorum. Siber silahların kontrol edilmez özelliği bu silahların belirli bir süre sonra kullanan ülkede bile yayılma gösterdiğine işaret etmektedir. Örnek olarak biraz önce de bahsedilen İran'a yapılan Stuxnet saldırısı birçok ülkeye yayılmıştır, bunu biraz daha detaylı olarak söyleyeceğim. Siber saldırıda en yetkin ülkelerden bir tanesi ABD fakat savunmada yetersiz. Bu şuna benziyor çok usta taş atan birinin camdan yapılan bir sarayda oturması gibidir. Bumerang gibi, döner sizi vurur.

Siber saldırıları kısaca analiz edelim. Estonya saldırısının bir özelliği vardır; bu saldırı teknik gelişmişlik bakımından bir kasabanın binlerce askerle işgal edilmesine ya da aynı hedefe binlerce top mermisinin atılmasına benzetilebilir. Diğer bir deyişle bu saldırı teknik olarak aslında çok basit bir yapıya sahiptir. İran'a yapılan nükleer saldırı ise aslında çok detaylı bir istihbarat sonucunda yapılan, bir yazılımla yapılan bir saldırıdır. Bir tanesi basit bir saldırı, ülkeyi on gün boyunca felç etmiştir. Diğeri de önceden hazırlanan istihbarat bilgilerine dayalı yapılan bir yazılım. Bu ne demektir? Bu aslında alt detaya indiğinizde santrifüjün vantilatörünün normalden daha fazla çalışması bir süre sonra normalden daha az çalışması ve bu sayede santrifüjün devre dışa kalmasına yönelik bir saldırıdır. Bu saldırının bir başka özelliği daha vardır; bu saldırıda merkezi arıza tespit yazılımına sinyal göndererek "burada bir problem yok, santrifüj normal çalışıyor, endişe etmeyin" diye ayrıca bir bilgi gönderiyor. Zekice hazırlanmış bir yazılımdır. Bu da önemlidir. Aslında istediğiniz kadar tedbir alın, dünyanın en gelişmiş ülkesi olun birey en zayıf halka. Wikileaks belgelerinde gördük, ABD'nin 274 temsilciliğine gönderdiği kriptolu belgeler basına, internete sızdı ve ABD çok büyük bir prestij kaybetti.

Bir diğeri, aslında burada değinilmedi. Amerika Birleşik Devletleri Ulusal Güvenlik Ajansı tarafından Microsoft, Apple, Yahoo, Google, Facebook ve benzeri gibi büyük sosyal medya şirketlerine ait kullanıcıların kişisel verileri ele geçirildi. ABD 11 Eylül saldırısından sonra elektronik istihbarat toplama kaygılarını hızlandırdı. Bu kapsamda 2006-2007 yıllarında hayata geçirilen Yabancı İstihbarat Toplama Yasası genişletildi, Başkan Bush döneminde Patriot Yasası hayata geçti, PRISM Programı da bu çıkarılan yasanın sonucu ortaya çıktı. Edward Snowden sadece F-35'lerin bilgilerini çıkarmakla kalmadı, Obama yönetiminin de Bush yönetimiyle aynı çizgide olduğunu görünce bu açıklamayı yaptı. Daha sonra Hong Kong'a oradan da Rusya'ya gitti. Prizma Programı ile ilgili de şu anda sosyal medya şirketlerine üye olan hükümlü kişilerin sosyal medya verileri şu anda toplanıyor.

Günümüzde siber savaşlar, saldırılar nasıl yapılıyor kısaca buna değinmek istiyorum. Bu da malumunuz genel iletişime açık olan internet sitelerinin ana sayfalarını silmek veya değiştirmek, erişeme açık olan bu sitelerdeki dosyalara erişim sağlayıp bilgi hırsızlığı gerçekleştirmek ancak var olan dosyaları değiştirmemek, erişime açık olan sitelere saldırılar gerçekleştirerek erişilmez hale getirmek ki bu bizim için - güvenlik birimleri için önemlidir. Biz 24 saat esasına göre hizmet sunuyoruz, kolluk kuvvetiyiz. Sahil Güvenlik, Jandarma ve Emniyet 24 esasına göre, üstelik bu hizmetlerimizin % 75'ini e-Devlet'e taşıdık. Bizim için bu sistemlerin 24 saat esasına göre çalışması ve halka hizmet sunması esastır. Bunları güvenlik altında da tutmamız gerekiyor. Bir diğeri şahısların ve kurumların bilgisayarlarına virüs ve benzeri zarar verici yazılımlar yüklemek, bu yazılımlarla uzak sistemlere erişim sağlamak. Bu yolla sistemlere fiziksel zarar vermek, bilgi hırsızlığı yapmak. Elde edilen bilgiler ile siber suçlar işlemek, elde edilen bilgilerle başka alanları ilgilendiren suçlar işlemek. Siber ortamda yasal ya da gayri yasal propaganda gerçekleştirmek. Siber ortamı yasal olmayan faaliyetlerin organize ve koordine edildiği bir alan olarak kullanmak. Ve değişik şekillerde ele geçirilip köle haline getirilen bilgisayarları zamanı geldiğinde hedef ülkelere, hedef sitelere toplu olarak saldırıda kullanmak.

Gelecekte bizi bekleyen tehlike, nesnelerin internetinin genişlemesiyle siber dünyanın üstel olarak büyümesidir. Siber saldırın kaynağının tespiti maksadıyla saldırı için kullanılan kaynaklara sızılarak delil elde etmeye çalışmanın yasal açıdan uygun olup olmadığı da tartışılmalıdır. Yine biraz önce de söyledim. Bir botnet saldırısında, bir bankaya yapılan saldırıda acaba o bilgisayarı kullanan mı suçlu yoksa o saldırıları toplu olarak yönlendiren mi suçlu? Bunun da hukuki boyutlarının araştırılması gerekir. İleride bizi bekleyen tehlikeler bunlardır. Bu tür saldırıya uğrayan kurumlar tarafından yüklüce tazminata mahkûm edilme durumumuz vardır kişisel güvenliğimizi sağlamadığımız gerekçesiyle.

Siber güçlenme yarışında askeri ve kolluk kuvvetlerindeki birimlerin bizim yaptığımız gibi siber savunma değil, siber savunma artı taarruz birimlerine dönüştürülmesi gerekmektedir.

Doç. Dr. Ahmet Hasan Koltuksuz:

Teşekkür ederim. Siber savaş deyince biz doğal olarak askeri boyutta ve askeri bakış açısıyla bir takım yaklaşımlarda bulunuyoruz ama bir de siber suç kavramı var. Emniyetimizde Siber Suçlarla Mücadele Dairesi var ve Daire Başkan Yardımcısı bizlerle birlikte. Dolayısıyla ben kendisinden rica ediyorum, bir emniyet bakış açısıyla siber suçlarla ilgili nasıl bir tablo var karşımızda? Bu tabloya karşı nasıl mücadele ediyoruz, bu anlamda neler yapıyoruz? Bunları bizlerle paylaşırsanız çok seviniriz. Buyurun efendim.

İhsan Erdoğan:

Teşekkür ederim Hocam. Siber suç kavramı yeni bir kavram malumunuz. Bir 10 yıl geçmişi var. Bu tür suçlar özellikle internetin gelişmeye, yayılmaya başlamasıyla birlikte siber âlemde bu tarz suçların da işlenmesi ve bu işin mağdurlarının artması emniyet teşkilatının bu konuyla ilgili özel bir birim teşkil etmesi ihtiyacını ortaya çıkarıyor. Bununla ilgili bilgi işlem bünyesinde bir takım çalışmalar büro seviyesinde gerçekleştiriliyor. Daha sonrasında bugünkü boyutunda 2013 yılında Siber Suçlarla Mücadele Daire Başkanlığı boyutuna kadar ulaşıyor. Siber Suçlarla Mücadele Daire Başkanlığı bilişim suçlarla, siber suçlarla mücadele ediyor ve her ne kadar bu suçun tanımı henüz ceza kanunlarımızda yapılmamış olmasına karşın bilişim suçlarıyla ilgili birkaç madde şu anda Türk Ceza Kanunu'nda mevcut. 243, 244 ve 245.ci maddeler; orada bilişim sistemlerine yetkisiz erişim, bu sistemleri bozma, değiştirme, illegal olarak kullanma gibi birtakım suçlar kapsama alanına alınmışken onun yanında da kredi kartları, banka kartları, bunların suistimal edilmesi gibi birtakım suçlar da gene bilişim suçları kapsamına giriyor. Şimdi tabii bunlarla mücadele edebilmeniz için öncelikle güvenli olmanın ilk unsuru haberdar olmanız. Haberdar olduktan sonra da tabii üretebileceğiniz tepki oranında da gücünüz ortaya çıkıyor. Burada en önemli unsur tabii verilere erişim. Suça vakıf olduktan sora, öğrendikten sonra o suçların araştırılması, suçların tespit edilmesi bunlarla ilgili birtakım teknik çalışmaları gerektiriyor. O teknik çalışmalar da tabii veriler üzerinden yapılıyor. Şimdi maalesef ülkemizde bu veri toplama konusu - daha önce bu platformda da çok tartışıldı – kişisel veriler, bunların korunması vesaire gibi Avrupa'da tartışıldığı gibi ülkemizde de tartışılıyor. Bunlarla erişim noktasında Siber Suçlarla Mücadele Başkanlığı olarak birtakım sıkıntılar yaşıyoruz tabii. Ne kadar çok veriye erişebiliyorsanız o kadar çok analiz yapma şansınız, o kadar çok önleyici faaliyette bulunma şansınız ve siber suçları aydınlatma şansınız oluyor.

Siber savaş ya da saldırı anlamında bizim mücadele ettiğimiz alanlar içinde en önemlisi kritik alt yapılara saldırı ya da bilişim sistemlerine yetkisiz erişim ve bunlarda gerçekleştirilen bilgi hırsızlığı. Ya da fidye amaçlı birtakım CEO dolandırıcılığı dediğimiz tarzda suçlar. Bunları araştırırken biz ne yapıyoruz? En önemli unsur tabii bu saldırılan birimlerin bilişim cihazlarının imajlarının alınması gerekiyor. Ve bu imajların alınması için tabii donanım, yazılım gerekli. Bunların hepsi yabancı menşeli. Bunlar için çok önemli yatırımların yapılması gerekiyor. Bu yazılımların da tabii millileştirilmesi, yazılımların da yerlileştirilmesi bizim gelecekte aslında üzerinde durmamız gereken önemli unsurlardan bir tanesi. Buradan IP adreslerini tespit etmeye çalışıyoruz. IP adreslerinde No-IP var. No-IP'lerin de tabii tespit edilmesi oldukça zor bir hale geliyor. VPN kullanan çok, bu işlerle uğraşan, minareyi çalan tabii kılıfını hazırlıyor. Suçlular kendilerini gizlemek için ellerinden gelen her türlü tedbiri alıyorlar. Bunların tespiti noktasında o IP adreslerinin tespiti için işte BTK ile yazışmalar yapıyoruz ya da ilgili servis sağlayıcılarla yazışmalar yapıyoruz. Önemli bir süreç gerekiyor, zaman gerekiyor ve emek gerekiyor. Tabii bunlar zaman içerisinde tartışılır. Bunlara hızlı bir şekilde erişim, verilerin bir yerde toplanması, bunların analiz edilmesi için ortak bir veri havuzunun da oluşturulmasında fayda var. Yani özellikle siber suçlarla mücadelede ne kadar çok veriye sahipseniz o verilerin üzerinden yaptığınız analizler de o derece faydalı olma ihtimali yükseliyor. Bu tarz çalışmalar yapıyoruz ve özellikle kredi kartı ve banka kartı dolandırıcılıkları oldukça yaygın. Burada en önemli unsur tabii kişisel tedbirler, bireysel tedbirler. Fishing siteleri yine Türkiye'de bir hayli fazla, özellikle bankaların web sayfalarının kopyalanması ya da bunların sahte adreslerini oluşturarak insanların dolandırılması oldukça yaygın uygulanan bir yöntem. Bu konuda uyarılarımızı yapıyoruz. Bankaların BT birimleri de bununla ilgili çalışmalar yapıyorlar.

Mücadele konusu bireysel tedbirlerle yapılması gerektiği gibi aynı zamanda da özellikle kritik alt yapılara saldırı noktasında ulusal koordinasyon ve işbirliği gerektiren bir alan. Bu noktada da kurumların siber olaylara müdahale merkezlerinin oluşturulması ve o kurumlar arasında bir işbirliğinin, bir eşgüdümün sağlanması şu anda Türkiye'de önemli bir eksik olarak görülüyor. Ulaştırma Bakanlığımız bünyesinde ulusal siber olaylara müdahale merkezimiz var ama bunun biraz daha aktif olarak faaliyetlerini genişletmesi, diğer kurumları da kapsayacak, onların SOME'lerini

de kapsayacak bir takım çalışmalar yapılması şu anda en önemli eksiklik olarak görülüyor. Önümüzdeki dönemlerde inşallah bu tarz çalışmalar yapılır ve siber suçlarla mücadele noktasında daha iyi bir noktaya geliriz.

Doç. Dr. Ahmet Hasan Koltuksuz:

Sayın Erdoğan çok teşekkür ederiz. Bir siber savaşta, bir siber mücadelede bizi öne çıkaracak olan teknolojiler, alt bileşenler; özellikle donanım seviyesine indiğinde sizi avantajlı hale getirebilecek unsurlar gerçekten yeni bir konu, yeni bir çalışma konusu ve ben bu konuda TÜBİTAK'ın çok çalıştığını biliyorum. O nedenle Sayın Dayıoğlu'na sözü vermek istiyorum. Tahmin ediyorum bu konuda ne aşamada olduğumuzu ya da TÜBİTAK'ın bakış açısını kendi direktörlüğü nezdinde bizlerle paylaşacaktır. Buyurunuz efendim.

Mustafa Dayıoğlu:

Teşekkür ederim. Bu zamana kadar ki konuşmaların çoğunda siber saldırı örneklerinden bahsedildi. Fakat siber saldırıların geneline bakıldığında bunun teorik olarak bir sınıflandırılmasının yapılması gerekiyor. Mesela bu alan 90'lı yıllarda ilk ortaya çıktığında bu alanın ismi "Bilgisayar Güvenliği" idi çünkü bu alanın öncesi bilgisayardı. Bilginin depolandığı, işlendiği ve taşındığı yerler bu konunun alanıydı. 90'lı yıllardan sonra ağ kavramı gelmeye başladı. Bu alanın ismi oldu "Ağ Güvenliği". 2000'li yıllarda artık sadece bilgi depolanmaktan çıkmaya başlayıp özellikle internet sayfaları paylaşılmaya başlandı, "Bilgi Güvenliği" dediler. Takip eden gelişmelerle bu alan artık "Siber Güvenlik" olarak adlandırılmaya başlandı. İşte burada karşılaştığımız bir nokta bilginin esasında nerede işlendiği, nerede taşındığı ve nerede iletildiği konusu.

Bugüne baktığımızda şu anda BTK'nın yaptığı önemli bir çalışma var; 5G Türkiye'ye geldi, geliyor. 5G'nin gelmesi esasında siber saldırılarda çok önemli tehdit vektörlerine de işaret ediyor. Şimdi bu zamana kadar bir tabir vardı; internette insanlar birbirleriyle konuşuyordu sosyal medyayla. 5G ile birlikte nesneler birbirleriyle konuşmaya başlıyor. Yani herhangi ufak bir cihaz konuşuyor. İkinci noktası, donanım maliyetlerinde ciddi anlamda ucuzlamalar meydana geldi. Mesela 2000'li yılların başında 1500 dolar olan bir iş istasyonunu siz bugün 1,5 dolara alabiliyorsunuz. Gigahertz hızında işlemcisi var, en az 250 megabayt-gigabayt seviyesinde belleği var ve gigabayt seviyesinde depolama alanı var. 1,5 dolara aldığınız çok küçük ama çok büyük işler yapabiliyorsunuz. Hani insanı bu kadar ucuzlatmak mümkün değil. Doğuyor, büyüyor, belli bir yaşamı var. Ama bu sistemler, donanım teknolojileri geliştikçe ucuzlamaya başlıyor.

İkinci nokta özellikle bilginin işlendiği yerler değişmeye başladı. Eskiden koca koca veri merkezleri varken şimdi artık kurumlar veri merkezlerini terk edip bilgileri bulutlar üzerinde işliyor hatta tek bir veri merkezi yetmiyor dünya üzerinde yaygın bir şekilde dağıtmaya başlıyorlar. Tabii bunlar da saldırıları ve saldırganları esasında tehdit vektörlerini değiştirdi, değiştirmeye başladı. Bu durumdan mütevellit artık eski dünyadaki teknolojiler yerine yeni teknolojiler gelmeye başladı.

Biz TÜBİTAK olarak siber güvenlikle alakalı ürün ve teknoloji kriptoloji çalışmasına başlamıştık ve o çalışmaya başlarken öncelikle tehditlere baktık; tehditler neler, tehditlerin kaynağı neler, tehditlerin kullandığı araçlar neler ve hedefler neler. Ve bununla birlikte bir pazar analizi yaptık dünyada ve Türkiye'de ki hemen hemen rakamlar birbirine yakın. Şöyle söyleyelim; Türkiye'de IT'nin büyüme oranı yıllık %7 ekseriyetle. %7 ile %10 arası. Bazı zamanlar daha yüksek oluyor, kriz olunca biraz daha düşüyor. Siber güvenliğe harcanan yatırım oranı da IT'nin büyüme oranına paralel. Fakat IT'nin içinde yer alanlara baktığımızda veriyle ilgili kısımlar ciddi anlamda ve bulutla alakalı kısımlar %20'ler, 30'lar mertebesinde büyümeye başlıyor. Yani anladık ki artık herkes buluta taşınmaya başlıyor. Bu işin bir problemi, bir tarafı çünkü eski dünyadaki veri merkezinde kullanılan siber güvenlik ürün ve teknolojiler burada artık eskisi gibi çalışmıyor.

Diğer durum; buluta taşınmaya başlayınca bu sefer işlem gücünde hızlanma gerekiyor. İşlem gücündeki hızlanmalar da temelinde sürücü teknolojilerini değiştirdi, sürücüleri değiştirdi ve yazılım platformlarını değiştirdi. Mesela bizim bir açıklık geliştirmede en çok kullandığımız şeyler, durumlar yeni açıklıklar. Bakıyorsunuz mesela herhangi bir yazılımın yeni versiyonu çıkmış. O yazılım platformunun, burada isim zikretmeyeyim, herhangi bir marka rencide olmasın diye ve herhangi bir sürücü değiştiği zaman o sürücülerin değişmesinden kaynaklı da çok ciddi şeyler çıkıyor, bellekle alakalı açıklıklar çıkıyor ve biz bu açıklıkları sömürebilecek yazılım geliştirebiliyoruz. Sürücü teknolojileri eskiden terminalle iç içeyken artık kullanıcı uzayına çıkmaya başladı. Bu şu demek; kullanıcı uzayına çıktığı zaman kullanıcı donanıma direkt erişiyor anlamına geliyor ve donanımdaki açıklıkları kullanmaya başlıyor. Ve özellikle son zamanlarda ses getiren birçok açıklık genelde işlemci

platformlarından ve yonga setlerinden kaynaklanıyor. Mesela işlemci platformundan çıkan bir açıklık sayesinde normal kullanıcı hakkına sahipken orada bir anda yöneticiden daha yüksek olan kök kullanıcı hakkına çok rahat erişebiliyorsunuz ve bunun içinde saldırı tespit sisteminizin, güvenlik duvarınızın, anti virüslerinizin, hiçbir etkisi yok.

Diğer bir konu; mesela mobil platformlarda yonga setlerden ve özellikle kablosuz ve 3G modülleri üzerinde çıkan açıklıklarda uzaktan herhangi bir kod çalıştırabiliyorsunuz. Yani telefonunuz var, çok güvenli, çok güvenli bir ortam ama 3G modülüne o telefonu girip her yere ulaşabiliyorsunuz. Şimdi bunları düşündüğünüz zaman, artık bu dünyada sınır kavramı kalmadı. Eskiden standart bir veri merkezi varken ağ üzerinden, güvenlik duvarı üzerinden sınır güvenliği yapabiliyordunuz. Ama artık sınırlar kalmadı. Sınırlar kalmadığı için de burada teknolojik süre doldu gibi geliyor özellikle çevre ağ teknolojisi için. Ağ Erişim Kontrolünden çıktı kriptografiye dayanmaya başladı. Ve kriptografinin de en önemli şeyi kripto algoritmalarından ziyade anahtar üretmek. Yani siz ürettiğiniz anahtarı ne kadar güvenli üretip, ne kadar güvenli olarak saklarsanız sizin bu konularda, siber savaşta direnciniz artmaya başlıyor. TÜBİTAK olarak son yıllarda ülke için önemli gördüğümüz için biz bulut temelli güvenli anahtar, yönetim ve dağıtım servisi geliştirdik. Bu yarı bulut temelli, yarı bulutla alakalı bir konu. Çünkü buradaki anahtar yönetimi ve yönettiğiniz o anahtarları hem yazılım geliştirmelerde hem yazılım, fonksiyonlarda kullanabiliyorsunuz bulut üzerinde. Veri depolamada kullanabiliyorsunuz ve bunu birçok mobil araçlarda da kullanabiliyorsunuz. Bu ülke için önemli bir şeydi biz bu konuda çalışmalar gerçekleştirdik. Onun özellikle ilk örneği de safir deponun uygulama alanıdır. İşte orada Uygulama Programlama Arayüzleri(API) üzerinden biz kendi kripto kütüphanelerimizi, kendi kripto algoritmalarımızı geliştirdik.

Diğer bir konu; özellikle yüksek hız çok önemli olduğu için iki tür erişim kontrolü vardır. Birisi isteğe bağlı denilen mekanizmadır. Kullanıcı ürettiği bilgiyi kendi sınıflandırır, kendi güvenlik önlemlerini alır. Bir de daha çok ihtiyaç duyulan zorunlu erişim kontrolü vardır. Bu da esasında sistem seviyesinde olması gereken şeylerden. Burada da temel nokta özellikle nesnelerin internetine dünya kaydığı için genelde bu Linux sistemlerinde, SELinux diye bahsedilen modül ki NSA geliştirmiştir. Biz şu anda o modülün yerli ve millisini geliştirmek üzere çalışıyoruz ve amacımız gerçek zamanlı işletim sistemlerine bizim gerçek zamanlı sistemlerini entegre edip savaş platformlarında zorunlu erişim kontrol mekanizması uygulayıp en azından o güvenlik politikalarını, özellikle uçtaki cihazlarda uygulanmasına olanak verecek konularda ağırlıklı olarak çalışmaya başladık. Özellikle melek yatırımcılarıyla yaptığımız bir çalışmada, yurt içi ve yurt dışında siber güvenlik alanında yeni ve özgün bir teknolojinin geliştirilmesi için yaklaşık 20 milyon dolar civarında bir bütçeye ihtiyaç olduğunu gördük. Bu 20 milyon dolar en azından 8-10 tane kritik teknolojiye ihtiyacınız olduğunda, özellikle 3 yıllık veya 5 yıllık periyotlarda en az 200 milyon dolar civarında bir bütçeye çıkıyor. Bunun devlet kaynakları ile finanse edilmesi çok kolay değil. Yani Amerika bile teknolojinin gelişimini özellikle melek yatırımcılar üzerinden finanse ediyor. Devletin vermiş olduğu destekler bu işin % 10'u kadar oluyor. Şimdi Türkiye'de özellikle bu tür teknolojilere sahip olunması için özellikle devletin kaynaklarına ya da ekstra yeni finansman kaynaklarına ve bu finansman kaynaklarının nasıl çeşitlendirildiğinin belirlenmesine ihtiyacımız var. İkincisi, bir ürün üretildiği zamanki durum. Siber güvenlikte bir ürün ürettiniz, sadece kamuyu hedeflediğinizde satacağınız sayılar 1000'ler mertebesinde oluyor. Ama globali hedeflediğinizde bazı yazılımlar var, 500 milyon tane indirilmiş, kullanılıyor. Şimdi burada da ne kadar çok ölçeklerseniz aslında birim maliyeti düşüyor. Özellikle de bizim global çapta; eğer siber güvenlik alanı, siber savaşlara karşı koyacaksanız global çapta bizim satabileceğimiz ürünleri geliştirmemiz gerekiyor. Birincisi finansman çeşitliliği, ikincisi bizim bu konuda nasıl müttefik ülkeler varsa silahlı kuvvetlerde, bu konuda siber müttefiklerle birlikte bu alanı çeşitlendirmemiz gerekiyor. Yoksa tek başına bir Arge'yi yaptığınız zaman, onun ürünleşme süreci ve o ürünün sürdürülebilirliği de önem arz ediyor.

Şimdi ben bu konuda biraz teknik noktadan farklı olarak bu iki konuda belki önümüzdeki günlerde siber savaşla birlikte siber müttefikler kavramının ele alınmasının önem arz ettiğini düşünüyorum. Çünkü şöyle söyleyeyim, mesela yonga setlerde açıklık çıkıyor, mikro işlemciler geliyor. Ortalama bir mikro işlemcinin geliştirme maliyeti yeni baştan 3 milyar dolar. Bizim onu ülke olarak geliştirebilmemiz şu anda o kadar mümkün değil. İkincisi donanımlarda arka kapılar çıkmaya başladı. Siz herhangi bir çip tasarlıyorsunuz, onu gidiyorsunuz yurt dışında ürettirdiğiniz zaman o çipin içine arka kapı yerleştirilebiliyor. Kriptografinin yanında kleptografi gibi çalma ile alakalı bilim dalları türemeye başladı. Ve donanımdan çıkan arka kapıları da sizin tespit edip önlemeniz çok zor. Özellikle biz askeri sistem tasarımlarında bu konuyla alakalı yöntemler üzerinde çalışıyoruz hatta başarılı olduğumuz birkaç yöntem de var. Şimdi bununla beraber donanıma hâkim olmanız gerekiyor. Genelde bu zamana kadar olan siber güvenlik çözümlerin çoğu yazılımsal çözümler. Yazılım güvenliği ile alakalı çözümler. Saldırılar da şu anda yazlımlar üzerinden. Ama artık bu iş nesnelerin interneti ile siber ve fiziksel sistemlere

kaydığı için burada donanıma da hâkim olmamız gerekiyor. O konuda da finansman çeşitliliği, pazar çeşitliliği ile birlikte bu işte siber müttefiklik konusu önem arz diyor. Siber müttefiklikle ilgili olarak şöyle bir şey var bizim ülkede: Mesela bir şirket bir alanda siber güvenlik ürünü geliştirdi ve başarılı oldu. Bizdeki birçok şirket aynı ürünü geliştirmeye çalışıyor. Bu sefer ne oluyor, zaten dar bir pazar var, o dar pazarda şirket sayısı da artıp kendi içlerinde anlamsız bir rekabete girilmeye başlanıyor. O yüzden bu konunun; özellikle siber güvenlikteki ürün konusunun ve müttefiklik konusunun kavram olarak bir oluşturulup, değerlendirilmesi gerektiğini düşünüyorum. Teşekkür ederim.

Doç. Dr. Ahmet Hasan Koltuksuz:

Biz de teşekkür ederiz, oldukça ilginç bir açıklama oldu. Bir bakıma da ben mutlu oldum çünkü herkesten fikir almış oldum. İkinci bölümde şimdi, biraz yakın geleceğe doğru, vizyonumuzu biraz ileriye doğru çevirip bakalım, neler bekliyoruz sorusuyla başlayacaktım. Zaten Mustafa Bey bize epey bir yolu açtı. Kişisel kanaatim, ben kendisini destekliyorum. Süratle Türkiye olarak - tabii şu anda oturup kendi işlemcimizi üretecek bir teknoloji yok. Artı bunun yatırımını yapmaya kalkarsak da yüzlerce milyar dolar ile karşı karşıya geliriz, ikinci bir Intel olma şansımız yok ama geç hiçten iyidir. Belki işlemcimiz olmayabilir ama FBGA üretip, biraz daha kalın olur belki, bilgisayarımızda, cep telefonumuzda hiç olmazsa bu anlamda - işlemci tarafında eksikliğimizi süratle kapatırız diye düşünüyorum çünkü gerçekten donanımda inanılmaz arka kapılar oluşmaya başladı. Birkaç ay evvel Intel'in ailesinde, işte i7'lerde, i9'larda bir komut keşfedildi. Intel "Unuttuk, kazara oldu" gibi bir açıklama yaptı ama basit bir işlemcinin içine bir komut öyle kazara unutulacak bir şey değildir devre tasarımı. Gayet güzel kripto analiz yapabileceğiniz, kripto analiz yapmakta kullanabileceğiniz komutlar çıkmaya başladı. Yani bunun anlamı şu; bilgisayarını şifreleyip güven altına, güvence altına aldığınızı zannettiğiniz verilerinizin dahi çok kolay, siz fark etmeden kırılıp, bunların yurt dışına taşınması mümkün. Ve bu giderek de artacaktır donanımlarda. Dolayısıyla bu anlamda bir şeyler yapabiliyor olmamız lazım.

Hal böyleyken ben tekrar Hasan Albay'a döneyim. Yakın gelecekte bizi neler bekliyor siber savaş anlamında, ne öngörüyorsunuz, ne düşünürsünüz, bizi nasıl aydınlatırsınız? Buyurun efendim.

Dr. Alb. Hasan Çifci:

Şimdi hocam örnek siber saldırılara baktığımızda bir ülke diğerlerini kötülüyor, hep doğu ülkesinden, şuradan bize saldırılıyor vesaire diye. Bizim bakışımız genelde Amerikan menşeli oluyor. Ama Amerika söylediği siber saldırıların mislini kendisi yapıyor. Ellerinde her marka, model güvenlik cihazı ve iletişim alma cihazlarına ait şablonlar var, onlara sızıyorlar. İletişim ağlarına tuzak yazılımlar ve tuzak donanımlar bırakıyorlar.

İki ülke örnek verdim. Geçenlerde Big Hack ya da Great Hack diye ortaya çıktı. Bu da küçücük bir çip, parmağın ucunda görebiliyorsunuz. Bu çip elektronik devrelere yerleştirilmiş durumda ve işin ilginç tarafı Amerika'nın devlet kurumlarından ve sivil firmalarından veri çalıyor. Devlet kurumlarından veri çalması biraz düşündürücü çünkü Amerika'nın Mustafa Bey'in biraz önce buyurduğu gibi Trusted Foundry Program diye donanımları test eden, içerisinde tuzak kapı var mı diye test eden programı var ve laboratuvarlarında bu donanımları test ediyorlar. Yani bugünden tohumları ekiyorlar, istedikleri zaman da, gelecekte herhangi bir zamanda da onu hasat edecekler.

Siber saldırıların etkileri konusunda iki uç boyut var. Bir tanesi bu fazla da önemli değil virüstür, yazılımdır diye konuşuluyor. Bir diğer senaryo da kâbus senaryosu, Sayısal Pearl Harbor. Japonların Amerikalılara 2. Dünya Savaşı başlatan – Amerikalılar açısından – saldırısı. Bugüne kadar gördüğümüz örneklerde siber saldırıların kinetik bir etkiye yol açacağı kesin bir şekilde ortaya konulmuştur. Burası nettir.

Gelecek teknolojileri siber savaşlara da, saldırı ve savunmalara da yön verecek. Burada endüstri 3.0 ve 4.0 teknolojileri, yapay zekâdan tutun da artırılmış gerçeklik, robotik de bunun içerisinde, eklemeli imalat bunun içerisinde, büyük veri analitiği bunun içerisinde. İlave olarak yapay zekâ ve robotiği ayrı bir şekilde düşünmek lazım. Kuantum teknolojileri hem bilgi işlemeye hem iletişime yön veriyor. Ve yeni nesil iletişim teknolojileri siber alanı şekillendirecek önemli teknolojiler arasında bu teknolojiler.

Peki, gidişat nereye doğru? Faydası var, sayısallaşma her alanda sayısallaşma. Akıllı cihazlar evlerimize giriyor, ceplerimizde var. Ama bu da tehditleri beraberinde getiriyor. Ne kadar sayısallaşıyoruz o kadar riske açığız, tehdide açığız.

Peki, gelecekteki eğilimler ne olacak? Belki virüs kodu değişecek, işletim sistemi sürümü değişecek,

yonga setinin adı değişecek ama daha hızlı saldırı ihtiyacı, eğilimi olacak. Daha hızlı tespit ihtiyacı olacak. Burada daha hızlı tepki vermemiz gerekecek. Ve daha hızlı iyileştirme yapmamız saldırılar sonrası gerekecek. Bunun için de çoğunlukla insanın aciz kaldığı durumlar ortaya çıkacak. Burada işte yapay zekânın, robotik sistemlerin, kendi başına karar verebilecek sistemlerin insanla birlikte çalışacağı bir ortama doğru süreç gidiyor.

Burada sonuç olarak siber alan kara, deniz, hava ve uzayın yanı sıra 5. bir harekât alanı olarak ortaya çıktı. Barış zamanında da sürekli olarak uygulanan bir saldırı yöntemi. Muhtemel bir savaşta da ilk olarak hedef alınan sistemlerin siber sistemler olacağı bütün uzmanlar tarafından dile getirilen bir husus.

Burada başarılı olabilmek için de teknoloji geliştirmekten tutun personel yetiştirmeye kadar her alanda yatırımlar yapılması gerektiğini değerlendiriyorum. Teşekkür ederim.

Doç. Dr. Ahmet Hasan Koltuksuz:

Engin Bey siz ne dersiniz benzer soru karşısında?

Tuğgeneral Engin Çırakoğlu:

Aynı zamanda emniyetle işbirliği açısından olayı ele alacağım. 2015 yılında enerji nakil hatlarına yapılan saldırı sonucunda, bizi tabii bunlar değişik tedbirler almaya yöneltti. Bu durumda enerjiye bağımlı olan iletişim altyapısı çöktüğünde ne yapabiliriz, terörle mücadelede nasıl yapabiliriz, yol kontrol noktalarında aranılan şahısların tespiti noktasında nasıl yaparız, emniyetle nasıl işbirliği yaparız konusuna yöneldik. Ve bununla ilgili tedbiri aldık, şu anda güvenlik nedeniyle altyapılarına inemeyeceğim ama Türkiye'de enerji altyapısı çöktüğünde Emniyet Genel Müdürlüğü ile aramızda ve tüm Türkiye'de güvenli bir kriptolu haberleşmeyi sağlayabilecek düzeydeyiz. Aynı zamanda hem veri tabanlarından sorgu yapıp aranılan şahısları yine kolaylıkla tespit edebilecek bir yapıyı gururla söylüyorum kurduk. Güvenlik nedeniyle alt detaylarına inmeyeceğim ama tamamı yerli ve milli çözümle olmuştur ASELSAN'ın da katkılarıyla. Tabii bu tür saldırılar bize karşı tedbir almayı da öğretiyor. Bizi de öğretiyor, eğitiyor.

Doç. Dr. Ahmet Hasan Koltuksuz:

Peki, çok teşekkür ederiz. Erdoğan Bey, siz kolluğun bir diğer mensubusunuz. Jandarmanın olduğu gibi Emniyet de bir başka tarafında ama belki de biz istatistiklere bakarak konuşuyoruz ama sizler birebir sahada yaşıyorsunuz siber problemleri. Bu problemlerden yola çıkarak muhtemel gelişmelere göre nasıl örneğin bir beş yıllık, on yıllık bir perspektifte neler öngörürsünüz bizlerle paylaşır mısınız lütfen?

İhsan Erdoğan:

Tabii ki paylaşırım. Şimdi önümüzdeki süreçte şu andaki mevcut siber alanda, siber uzayda, siber âlemde işlenen suçlar artarak devam edecek bunu öngörebiliyoruz. Yani geçtiğimiz yıllarda işlenen suçlara ve istatistiklere baktığımız zaman bir ivmelenme var. Kullanıcı sayısı her geçen gün artan bir ortamda buradan mağdurların sayısını da öngörebiliyoruz. Nedir; yine bilişim sistemlerine erişim noktasında, yine kritik kartların, banka kartlarının ve e-internet üzerinden yapılan dolandırıcılık konusunda, yine çocuk istismarı, yasadışı bahis vesaire gibi bu tarz konularda önümüzdeki süreçte de bu tarz suçlar artacak. Ama bunlara tepki üretilmesi noktasında bizim de şu anda, bunlarla mücadele edebilecek kritik altyapıları oluşturmamız gerekiyor. Bunlarla ilgili insan kaynağı, beşeri kaynak yetiştirilmesi, veri merkezlerinin oluşturulması, eşgüdümün, koordinasyonun diğer kurumlarla sağlanması ortak mücadele noktasında şu anda önemli çalışmalar var. Jandarma birimlerimizde, askeri birimlerimizde gene diğer BTK ve servis sağlayıcı diğer kurumlarımızla, diğer bakanlıklarımızla ortak çalışmalara devam ediyoruz.

Şimdi bizim asıl en önemli tehdit olarak gördüğümüz hususlardan bir tanesi, biliyorsunuz, "Supervisory Control and Data Acquisition" dediğimiz SCADA sistemlerine saldırı. Bu en önemli tehditlerden bir tanesi. Şimdi 11 Eylül malumunuz eş zamanlı, aynı anda uçakların belli hedeflere saldırması şeklinde gerçekleşmişti. Terör örgütlerinin şu anda böyle bir kapasitesi görünmüyor ama önümüzdeki 5 yıl içerisinde yine terör örgütlerinin mensupları kendilerini geliştirerek ya da birtakım hâkim güçlerin desteğiyle belki ülkemiz üzerinde bu tarz bir saldırı girişimi oluşturma ihtimalleri mevcut. Bunu bir istihbarat olarak söylemiyorum ama bu bir ihtimal. Yani bunu bir risk olarak göz önünde bulundurmak gerekir ve buna yönelik tedbirleri şimdiden almak

gerekir. Böyle bir saldırı olduğunda hava ulaşımına, hızlı tren ulaşımına ya da bilişim altyapısına eş zamanlı bir saldırı olduğunda neler yapabiliriz, bunların senaryolarının şimdiden tartışılması gerekir. Ve bununla ilgili ne tür tedbirler üretebiliriz, alternatif felaket kurtarma merkezlerimiz vesaire nasıl oluşturulabilir, bunlarla ilgili birtakım yatırımlar yapılması gerekiyor.

Bunun haricinde bir tehdit olarak da yine biliyorsunuz suçtan, yani suç işlenmesi ya da siber saldırıdan stratejik anlamda kazanım elde etme noktasında biz devletler düzeyinde bunu değerlendirdik. Siber savaştan özellikle devletler boyutunda bir bölgeye hâkim olma, bir alana hâkim olma. Orada hegemonya kurma ya da caydırıcılık noktasında o ülkeleri caydırılması gibi bir takım stratejik boyutları var ama öbür taraftan da bireysel anlamda da suç işleyenler gene bu uygulamadan çıkar sağlamak, menfaat sağlama, zenginleşme vesaire gibi bir takım amaçlarla hareket ediyorlar. Burada tabii en önemli unsur mali kaynak ya da para. Paranın transfer sistemlerine şu anda müdahil olabiliyoruz. Nedir, IBAN üzerinden transferi takip edebiliyoruz. Birtakım iletişim altyapılarına erişerek bunları takip etme şansımız oluyor fakat şu anda dünyanın bir gerçeği var; kripto paralar ve elektronik paralar. Maalesef bunlarla ilgili henüz dünya kadar ülkemizde bir regülasyon yok. Bunların kim tarafından üretildiği, kime gönderildiği, nasıl gönderildiği, niye gönderildiği, ne kadar miktar gönderildiği noktasında bir tespitimiz olmuyor. Önümüzdeki 5 yıl içerisinde de bu bize önemli bir sorun çıkaracakmış gibi görünüyor. Bununla ilgili de şimdiden tedbirler almak gerekir diye düşünüyorum. Teşekkür ederim.

Doç. Dr. Ahmet Hasan Koltuksuz:

Çok teşekkür ederiz, özellikle kripto para konusu kritik. Belki daha sonra tekrar geliriz ama tekrar teşekkürler efendim, sağ olun. Mustafa Bey, siz ne durumdasınız bu konuda, siz neler söylersiniz?

Mustafa Dayıoğlu:

Zaten sanayi 4.0 konuları ile birlikte fabrikalar otomasyona geçiyor, insansız fabrikalara doğru gitmeye başladı. Tabii bu özellikle yazılım sistemlerinin ağırlık kazanması anlamına geliyor. Şöyle bir istatistik var; normalde yazmış olduğunuz her bin satır kodda 1 tane açıklık oluyor. Eskiden böyle fiziksel siber sistemlerle ilgili toplam kod sayısı 5.000 – 10.000 civarındaydı ki 10.000 satır kodda 10 tane açıklığı kolaylıkla tespit edebiliyordunuz ama biraz evvel bahsedilen sistemlerde ortalama 20 milyon satır kod yürümeye başladı. Bu da şu demek; yani herhangi bir kaynak kodu analizi yaptığınızda 20 bin tane açıklık anlamına geliyor ki bizim bu sürücülerden vesairelerden gelen açıklarla birlikte, bunun önlenebilmesi için çeşitli önlemler alınması gerekiyor. Özellikle tasarım konularında; nasıl yazılım tasarımında müşteri gereklilikleri vardır, yazılım gereklilikleri olur. Bir de güvenlik gerekliği gibi güvenlik mühendisliği sürecinin olması gerekiyor.

Diğer bir konu; silahlı kuvvetlerde, askeri sistemlerde siber güvenlik. Biraz evvel donanımlarından bahsettik, o donanımların bazılarını kullanmak zorunda kalıyoruz doğal olarak. Burada bu donanımların tamamen güvensiz olduğunu kabul edip onun üzerine bizim güvenlik katmanları geliştirmemiz gerekiyor. Çünkü herhangi bir askeri sistem, en basiti GPS'ten örnek vereyim; bir GPS'i çok basit bir şekilde aldatabiliyorsunuz. GPS'i aldatmanızın size çok büyük etkileri olabiliyor sahada. Ve buna karşı şeyler de oluyor. O yüzden de güvenli tasarım konusu, yani bu açıklıkları çıkacak bazı platformlar bizim elimizde olmayacak. Biz dışarıdan bir şekilde tedarik edeceğiz ama bununla birlikte burada ciddi anlamda özellikle hem endüstriyel kontrol sistemlerinde hem de askeri sistemlerde – siber fiziksel sistem olarak biz onu adlandırıyoruz – bir güvenlik katmanına ve o güvenlik katmanı için ciddi bir güvenlik mühendisliği disiplinine ihtiyacımız bulunuyor. Yani yazılım mühendisliği gibi bir güvenlik mühendisliği de artık bu sistemlerin tasarım süreçlerinde.

Bizim ülkemizde şu anda sızma testi var. Sızma testi açıklığı bulabiliyor ama bulunan açıklığın çözümü bulunduğu kadar kolay olmayabiliyor. Bu konu üzerine çalışma yapılması önem arz ediyor. Biz de TÜBİTAK olarak Savunma Sanayi Başkanlığı ile birlikte siber akademi kapsamında güvenlik mühendisleri yetiştirmek üzere bir program başlattık. Sistemlerden başlıyor, temel seviye. Alan uzmanlığı başlıyor, uzmanlık seviye ve ileri olan uzmanlığında da artık bu güvenlik mühendisleri yetiştirip bu arkadaşları birçok yerde kullandırmamız gerekiyor. Ben teşekkür ederim.

Doç. Dr. Ahmet Hasan Koltuksuz:

İleriye dönük kısa dönemde çok ilginç dönüşler aldık. Bu konuda müsaade ederseniz ben de birkaç görüş arz edeyim. Ondan sonra tekrar panelistlerimize, belki eklemek istedikleri son şeyler olabilir, tekrar söz vereceğim.

Şimdi Moore's Resistance diye bilinen bir yasa vardır, Intel'in kurucusu Moore'un ortaya koyduğu. Her iki senede bir işlemci çıkar. Bizdeki transistör sayısı ikiye katlanır, fiyat yere iner diye fakat bu direnç öleli bir 10 yıl kadar oldu. Çünkü şöyle kritik bir gelişme yaşadık biz. Bir işlemcinin içine koyabileceğiniz transistör sayısı aslında onun fiziksel büyüklüğü ile alakalı. Şimdi 4 nanometreye kadar bunları küçültmek mümkün ama 4 nanometrenin altına indiğinizde bu sefer metrik uzaydan çıkıp kuantum uzayına gidiyorsunuz, orada da çok ciddi problemler var. Hesaplamalarda kararlılık yok oluyor. Yani işlemci büyüklüğü çok ciddi bir problem.

Bir diğer problemimiz hız. İşlemcilerimizin hızı. Orada da bir bariyerimiz var. Orada da bir 4 Gigahertz'lik bir hız bariyeri var. Onun üstüne çıktığınızda ciddi bir biçimde bir yanma gerçekleşiyor. Dolayısıyla işlemcinin de hızını artıramıyoruz. Bunlar teknik olarak şu an yaşadığımız problemler.

Ve bir 3. boyutta da, bakın insanlığın son 5000 senede ürettiği bilgiyi şu anda her gün üretir noktasındayız. Ve böyle olunca da bu bilgilerin depolanması başlı başına bir problem oldu. Artık sabit disklerle yetinilecek gibi değil durum. Başka ortamlarda kayıt yapabilmenin yolunu arıyoruz şimdi. Bunlar teknoloji ve bilimdeki üç temel problem. Önümüzdeki 10 yılı aslında belirleyecek olan problemler. Çünkü bunların her birinin çözümü teknolojide bizi yeni yeni boyutlarla karşı karşıya getirecek. Dolayısıyla da bunların savaş endüstrisinde siber savaş tarafına aktarılması yahut da ekonomiye eklemlenmesi farklı biçimlerde olacağından bu konularda Türkiye'nin de yavaş yavaş yerini alması gerekiyor diyebilirim. Çünkü bunlar masamızda olan problemler teknolojik olarak.

Eklemek istediğiniz başka bir şey olabilir mi acaba? Buyurun Komutanım...

Tuğgeneral Engin Çırakoğlu:

Fırsat bulmuşken bir konuya değinmek istiyorum. Jandarma Genel Komutanlığı olarak güvenle söylüyorum siber güvenlik alanında kullandığımız yazılımların %60'ı yerli. Yerli ve milli. Biz onları kullanmaktan korkmuyoruz. Burada hazır kamu ve kuruluşlarından gelen temsilciler var; sizler de kullanın. Hedefimiz önümüzdeki yıl %80'e çıkmak. Örneğin bir antivirüs programı var, ismini burada zikretmek istemiyorum. Bunlar yazılım tabanlı. Yani öğretilen virüsleri bulup yok ediyor. Sezgisel tabanlı; yani akıllı, öğrenen antivirüs programını aldık. Yerli ve milli, kullanıyoruz. Biz 24 saat esasına göre halka hizmet veriyoruz. Şu an verdiğimiz hizmetlerin %75'i e-devlet kapısında ve dijital platformda. Bu yılsonuna kadar vatandaşlarımıza verdiğimiz hizmetlerin %100'ünü e-devlete taşıyacağız. Her kurumun bilgisi kendisi için önemlidir, kritiktir. Bunu saygıyla karşılıyorum. Ancak bizim verilerimiz de değerlidir, kıymetlidir. Buna rağmen cesaretle bu ürünleri kullanıyorum. Siber kümelenmede yer alan şirketleri takip ediyorum. Yabancı ürünlerin yerine yaptığı ürün olduğu zaman hemen çağırıyorum, test ediyorum ve kullanıyorum. Kullanmaktan korkmayın. Bizim ürünlerimiz emin olun onların siber güvenlik ürünlerinden kat be kat iyi. Cesaretle kullanın. Teşekkür ederim.

Doç. Dr. Ahmet Hasan Koltuksuz:

Ben son olarak şunu arz etmek istiyorum. Birincisi biz panelistlere her şeyden önce fikirlerimizi paylaşma imkânı verdiği için HAVELSAN'a teşekkür ediyoruz. Bize ev sahipliği yapan Bilgi ve İletişim Kurumu'na da çok teşekkür ediyoruz. Ama bu iki güzide kurumumuz ötesinde vaktinizi ayırdığınız, bizi sabırla dinlediğiniz için sizlere de çok teşekkür ediyoruz efendim. Sağ olun, var olun.

DR. EMRE YÜCE

HAVELSAN
Kurumsal Siber Güvenlik
Hizmetleri Takım Lideri

GÜNÜMÜZ VE GELECEĞİN SİBER GÜVENLİK OPERASYON MERKEZLERİ

Siber saldırı nedir, nasıl gerçekleşir, bunlardan bahsedeceğim. Günümüzdeki ve gelecekteki beklentilerden bahsediyor olacağım. Temel bilgi güvenlik ilkeleri bozulduğunda bir saldırı gerçekleşmiş oluyor, bunu hepimiz biliyoruz. Gizlilik, bütünlük, erişilebilirlik ana temel maddeler. Saldırganların nasıl bir yol izlediğini bilmemiz gerekiyor, buna göre saldırıları analiz edebiliyoruz ve olası tehditleri tespit edebiliyoruz. Hedef hepimiziz. Verdiğimiz eğitimlerde şunu görüyoruz: “Benim kişisel bilgim yok, ben neden hedef olayım?” gibi bir izlenim var insanlarda. Ve mobil güvenlik eğitiminin özellikle sonunda şunu soruyoruz “cep telefonunuzu bize bir saatliğine şifresi açık bir şekilde, parolası olmadan verir misiniz?” diyoruz. Şu ana kadar “evet” cevabını alamadık bundan. Demek ki hepimizin kişisel bilgisi var. Telefonlarımızda fotoğraflarımız, mesajlarımız, e-postalarımız var. Dolayısıyla hepimiz hedefler olabiliriz, hepimiz atlama noktaları olarak kullanılabiliriz siber saldırılarda.

Günümüzde nasıl kullanılıyor? Aslında burada geçmişten, daha geçmişten bahsetmek gerekiyor. İlk bilgi işlem altyapıları oluşturulmaya başlandığında, bilgisayarlar oluşturulduğunda son kullanıcı güvenliği çok önemliydi. Dolayısıyla ilk hepimizin hatırladığı gibi antivirüsler, imza tabanlı çalışan antivirüs uygulamaları yaygın olarak kullanılıyordu. Daha sonra sınır güvenliği söz konusu olmaya başladı, dolayısıyla bir ağı bütün olarak korumak aslında söz konusu oldu. Güvenlik duvarları, saldırı tespit önlemle sistemleri ve ileri sandbox- kum havuzu- gibi teknolojiler ortaya çıktı. Daha sonrasında ilerleyen dönemde o kadar çok fazla bileşenimiz oldu ki bilgi sistem altyapılarında; bunların hepsi tonlarca log üretmeye başladı ve bunları analiz

etme ihtiyacı doğdu. Logları takip etmemiz gerekti. Bunlar da siber güvenlik operasyon merkezlerinin doğmasına sebep oldu. Bu birden fazla kişiden oluşan, birden fazla seviyede oluşan, bir de kişiden oluşan siber güvenlik operasyon merkezlerinden bahsediyoruz. Burada logların takip edilmesi, olaylara müdahale edilmesi, en önemli noktalardan bir tanesi kök neden analizi çünkü eğer bir siber olay için siz kök neden analizi yapmazsanız o siber olay sürekli başınıza gelmeye devam edecektir. 1 tane zararlı yazılım ağınıza bulaşmıştır, siz o zararlı yazılımı silip, bilgisayarları temizleyip koyduğunuzda o zararlı yazılımın sizin ağınıza tekrar bulaşma ihtimali çok yüksektir. Çünkü siz o zararlı yazılımın nasıl bulaştığını; kullanıcı hatası ile mi bulaştığını, yoksa sistemdeki bir açıklıkla mı bulaştığını tespit etmemişsinizdir. Örneğin buna kullanım senaryosu olarak kolay parolaları söyleyebiliriz. Kolay parola kullanımı, kolay tahmin edilebilen parolalar kullanıyorsa kullanıcılar bu kök nedenlerden bir tanesi olabilir. Buna yönelik bir çalışma yapmanız gerekiyor, dolayısıyla kök neden analizi önemli.

Farkındalık önemli. İnsan, teknoloji ve süreç üç tane temel bileşeni bizim bilgi sistem altyapılarımızın. Bu üçünü de sağlıklı bir şekilde oturtmanız lazım. Güzel güvenlik cihazlarınız olması lazım, onları doğru şekilde ayarlamamız lazım. Süreçlerinizin düzgün yapılandırılmış olması lazım, işe giren personelin ve işten ayrılan personelin düzgün bir şekilde bu süreçleri tamamlaması lazım. Parola politikalarınız, internet kullanım politikalarınız, e-posta kullanım politikalarınız bunların hepsi süreçlere dâhil. Ama son nokta insan kaynağı. İnsan kaynağının da eğitilmiş olması gerekiyor. Buna en güzel örnek finans birimlerinde veya insan kaynakları birimlerinde çalışan personel. Burada çalışan personel genelde ellerindeki bilginin ne kadar değerli olduğunun farkında olmuyorlar. Bu farkındalığı yaratmamız gerekiyor. Siber güvenlik operasyon merkezlerinde günümüzde karşılaştığımız problemler bunlar.

Peki, neler yapıyoruz siber güvenlik operasyon merkezlerinde? Proaktif, yani önceden tehditleri öğrenip bunlarla ilgili izleme ve uyarı gerçekleştiriyoruz. Siber tehdit istihbaratı topluyoruz ve bunu kurumlarla paylaşıyoruz. Olay müdahale raporlama, servis sürekliliği takibi, açıklık takibi ve eğitimler de diğer hizmetlerimiz arasında.

HAVELSAN olarak bu hizmeti nasıl gerçekleştiriyoruz, bundan bahsedelim. Planlama ile başlıyoruz, bir boşluk analizi bunu takip ediyor. Yani mevcut durumda o kurum ne durumda, bunu tespit ediyoruz ve nerde olması gerektiğini söylüyoruz. Günün sonunda arada neler yapması gerektiğine dair bir danışmanlık hizmeti veriyoruz. Daha sonra o kurumu korumaya başlıyoruz. Politikalar üretiyoruz, insan kaynağına eğitimler sağlıyoruz veya insan kaynağı eksikse bununla ilgili danışmanlık sağlıyoruz. Bir siber olay gerçekleştirildiğinde de müdahale çalışmalarını gerçekleştiriyoruz.

Ek olarak bir siber olay sonucunda, biz, zararlı bir yazılım elde ettiysek onun analizini gerçekleştiriyoruz. İstihbaratı, yaygınlaştırma ve eğitimler de diğer başlıklarımız. Eğitimler artı yaygınlaştırma diye bahsediyoruz çünkü sadece eğitimle de olmuyor. Kuru kuruya insanları bir araya toplayıp bir şeyler anlattığınızda o salondan çıktıklarında bu bilgiler akıllarından çıkabiliyor. Bu sizde çıkmayacak bu örneği verdiğim için. Fakat yaygınlaştırma ile bunu destekliyoruz. Yaygınlaştırma çalışmalarımız neler; mesela ortalama taktik hatları gerçekleştiriyoruz. Dolayısı ile kurumdaki personel gerçekten bir siber saldırıya maruz kalmış oluyor. Afişler, broşürler ve diğer çalışmalarla bunları destekliyoruz.

Gelecekte neler olacak? Daha önce söylediğim gibi uç nokta güvenliği ile başladı her şey. Daha sonrasında sınır güvenliğine geçti. Daha sonra bilgi çok hızlı bir şekilde artmaya devam ediyor. Dolayısıyla hepimizin dilinde olan büyük veri, büyük verinin analiz edilmesi. Veriniz sizin ham olarak elinizde olması aslında bir şey ifade etmiyor. O bilgiyi sizin, o veriyi sizin anlamlandırabiliyor olmanız gerekiyor. Gelecekteki siber güvenlik operasyon merkezlerinde karşılaşılacak durumlardan en önemlilerinden bir tanesi bu. Bu bilgi benzer şekilde bizim elimizde olduğu gibi saldırganların da elinde var. Dolayısıyla anlık olarak değişen zararlı yazılımlar, anlık olarak değişen oltalama e-postaları gözlemleyebiliyoruz. Kişiyi hedefleyen oltalama e-postaları gözlemlemeyi bekliyoruz ilerleyen dönemde.

Makine öğrenmesi veya yapay zekâ aslında beklediğimiz teknolojiler arasında. Burada şöyle sıkıntılar var. Her şeyi makine öğrenmesi ve yapay zekâ ile yaptıramıyoruz maalesef. Neleri yaptırabiliriz? Otomatikleştirebileceğimiz şeyleri veya daha çok öğrenebileceğini bildiğimiz, elimizde deneysel veri olan kısımları tabii ki yapabiliriz. Saldırı izleme ve uyarıyı, yazılım hatalarının öğrenilmesi, yazılımların geliştirilmesi yapay zekâ ile gerçekleştirilebilir. Fakat insan faktörünün her zaman olması gerektiği konular da mevcut. Bunların başında yönetmelikler geliyor. Uyumluluk çalışmaları ve etik anlayışı geliyor.

Siber güvenlik operasyon merkezlerinde orkestrasyon ve analiz çalışmaları artış göstermekte. Eskiden bir SIEM (Security Information and Event Management System) koyuyorduk merkeze. Bu logları topluyordu, ilişki üretiyordu. Artık onun bir aşama sonrasına, SOAR'a geçiyoruz. SOAR, eski tanımlı security operations analysis and reporting olarak geçiyor. Fakat bunda da durum değişiyor. Artık "security ochestration, analytics and response"a dönüyor. Dolayısıyla sizin güvenlik cihazlarınızı siber güvenlik operasyon merkezlerinden yönettiğiniz, anlık siber olaylara karşı bir aktif aksiyon gösterdiğiniz durumlara geçiyoruz. Bunları analiz ettiğiniz durumları gözlemlemeye başlayacağız gelecekte.

Şifreleme önemli bir konu. Kuantum kriptografi ile beraber kuantum kriptografinin yaygınlaşması durumunda bugün kullandığımız birçok şifreleme algoritması aslında geçersiz hale gelecek. Örneğin bankacılık uygulamalarında SSL alt yapılarını kullanıyoruz, SSL'i kullanıyoruz varsayılan protokol olarak, bu geçersiz hale gelecek. Dolayısıyla iletişimimiz aslında güvensiz hale gelmiş olacak. Dolayısıyla burada kuantum sonrası kriptografiyi düşünmemiz, algoritmaları düşünmemiz gerekecek.


Hasan Hüseyin ÖZBENLİ
SSB Siber Güvenlik
Kümelenmesi Koordinatörü
Sarp SERTCAN
Yüksek Seçim Kurulu
Bilgi İşlem Daire Başkanı
Dr. Mehmet SONGUR
ASKİ Bilgi İşlem Başkanı

Moderator:
Gökhan EVREN
UAB Haberleşme
Genel Müdürü

Özgür ÖZTÜRK
Haberleşme Genel
Müdürlüğü Siber Güvenlik
Daire Başkanı

Yakup ŞIVKA
Anadolu Ajansı Bilişim
Sistemleri Direktörü

PANEL 2

Yeni Nesil Kurumsal Siber Güvenlik ve Kritik Alt Yapıların Korunması

Hasan Hüseyin
ÖZBENLİ
SSB Siber Güvenlik
Kümelenmesi Koordinatörü

Sarp SERTCAN
Yüksek Seçim Kurulu
Bilgi İşlem Daire Başkanı

Dr. Mehmet SUNGUR
ASKİ Bilgi İşlem Başkanı

Gökhan Evren:

Teşekkür ederim. Kritik altyapılar bildiğimiz üzere siber güvenliğimizde en önemli altyapıları, en önemli yapı taşları. Bu altyapılara yapılabilecek bir saldırı kamu hizmetlerinin doğrudan etkilenmesine neden olabileceği ve kamu hizmetlerinin sürekliliğinin sunulmasını engelleyebileceği için, özel bir önem atfettiğimiz bir alan. Ve siber güvenlikle ilgili bu bütüncül bakış açısında öncelikli alanlar olarak belirlediğimiz altyapılar diyebiliriz. Bu doğrultuda ülkemizde 2013 yılında belirlenmiş kritik altyapılar söz konusu. Bunlar elektronik haberleşme sektörü, enerji sektörü, finans, ulaştırma ve su yönetimi ve kritik kamu hizmetleri. Kritik kamu hizmetlerinin altında da birçok alt kırılım söz konusu.

Ülke olarak siber güvenlik alanındaki faaliyetimize özellikle son birkaç yıl içerisinde yeni bir ivme kazandırmış durumdayız. Geçtiğimiz aylarda İTÜ'nün bir siber güvenlik endeksi yayınlandı. Bunu takip etmiş olanlar aramızda vardır mutlaka. GCI dediğimiz bu endeks her yıl yayınlanıyor ve 2018'teki veriler esas alınarak yapılan bu puanlandırmaya göre – 175 ülke bu puanlamaya giriyor – bu ülkeler arasında ülkemiz 2018 yılında Avrupa genelinde 10. sırada yer aldı, önemli ülkelerin önünde yer aldı. İtalya, Almanya, Danimarka gibi ülkelerin önünde yer aldı. Dünya genelinde de bir önceki endekse göre 43. sıradan 20. sıraya yükseldik. Bu endekste genel olarak nelere dikkat ediliyor; tabii kurumlardan, bakanlıklardan veri toplanıyor ve bu veriler detaylı şekilde kaynaklarından, referanslarından teyit ediliyor. Bu endeks içerisinde yasal ve mevzuatsal altyapının ağırlığı, bunun etkinliği, teknik kabiliyetleri, ülke genelinde siber güvenlikle ilgili sorumlu kuruluşların teknik kabiliyetleri, organizasyonel yapının etkinliği, verimliliği, uzman insan kaynağı kapasitesinin inşasına yönelik çalışmalar ve bununla ilgili gelişmeler(bir önceki döneme göre), siber güvenlikte ülke içi paydaşlarla ve uluslararası paydaşlarla olan işbirlikleri ve bu işbirliğine yönelik anlaşmalar, çalışmalar, toplantılar, veri alışverişleri gibi hususların varlığı irdeleniyor ve buna göre bir skorlama, bir puanlama yapılıyor. Bu bağlamda söz konusu endekste yapmış olduğumuz bu sıçrama, geçtiğimiz yıllarda yapılan çalışmaların etkinliğini, verimliliğini önemli derecede ortaya koyan bir göstergedir diye düşünüyorum.

Ülkemizde Siber Güvenlik Organizasyonu'nun kuruluşu 2013 yılına kadar dayanıyor. 2013 yılında Ulusal Siber Olaylara Müdahale Merkezi kuruldu ve ardından kritik kurum, kuruluşlarımızdan başlamak üzere Siber Olaylara Müdahale Ekipleri oluşturuldu, oluşturulmaya da devam ediyor. Şu an itibariyle SOME sayısı 1200'e yaklaşmış durumda. BTK binamızda USOM'un Siber Güvenlik Operasyon Merkezi var ve bu merkezde hem süreç olarak hem de altyapı ve yazılım imkânlarıyla SOME'ler ile iş birliği ve bağlantılarımız devam ediyor. Burada tespit edilen ülke genelindeki tehditler ilgili kurum, kuruluşlarla anlık olarak 7/24 paylaşılıyor. Bu belirtmiş olduğumuz 1200'e yakın SOME'miz ve bunlara kayıtlı 3500 civarında siber güvenlik uzmanı doğrudan, birebir güvenlik bildirimleri gönderiyor.

Geçtiğimiz dönem içerisinde 2013-2014 yıllarını kapsayan bir eylem planı yürürlüğe konuldu. Daha sonra da ikinci eylem planı siber güvenlikle ilgili, 2016-2019 eylem planı. Bunların yürütücülüğünü, koordinasyonunu bakanlığımız yaptı. Önemli kurumlarımız, paydaşlarımız burada önemli fonksiyonlar icra ediyor.

Önümüzdeki dönem için de eylem planı hazırlıklarımız devam ediyor. Geçmiş dönemde siber tehditlere, saldırılara hazırlık anlamında tatbikatlar da gerçekleştirildi. Yine bunların koordinasyonunu BTK ve Bakanlığımız olarak icra ettik. 4 tane ulusal, 1 tane uluslararası tatbikat yaptık. Bu senenin sonu içinde yeni bir uluslararası tatbikat hazırlıklarımız devam ediyor. Bu anlamda teknik altyapı senaryolarının hazırlanmasını tamamladık. Organizasyonel süreçleri tamamladıktan sonra inşallah sene sonunda güzel bir etkinlik olacak. Bunun için de tatbikatın altyapısı yine buradaki yerli-milli imkânlarımızla geliştirildi ve bundan sonra da müteakip etkinliklerde, tatbikatlarda tekrar tekrar kullanılabilecek önemli bir altyapıya da kavuşmuş olduk.

SOME ekiplerimizin önümüzdeki dönemde, siber olaylara müdahale ekiplerimizin olgunluk seviyelerinin değerlendirilmesi ve iyileştirilmesine yönelik çalışmalarımızı da hızlandırıyoruz. Bu noktada belirli olgunluk değerlendirme yöntemleri var. Bu yöntemlerde, bu Framework'lerde ön plana çıkan hususlar özellikle insan kaynağı, SOME ekiplerinin insan kaynağının ne derece yeterli olduğu, yetkin olduğudur. İkinci olarak teknik altyapısının ve kabiliyetlerinin ne derece etkin ve verimli olduğu ve Üçüncü olarak da süreçler. Siber olaylara karşı hazırlık ve olay anında yürürlüğe koyulacak, konulacak süreçlerin varlığı ve bu süreçlerin etkinliği ve verimliliği yine olgunluk değerlendirme yöntemimizde ön plana çıkan hususlar olacak.
Bu noktada panelistlerimizin özellikle bu hususlarda ortaya koydukları çalışmaları ve gelişmeleri konuşmalarında vurgulamalarını önemle rica ediyorum. İlk olarak Ulaştırma Bakanlığımızdan Daire Başkanı Sayın Özgür Öztürk'e sözü vermek istiyorum. Özellikle USOM'un yaptığı çalışmaları, bakanlığımızın yaptığı çalışmaları özetlemesini rica ediyoruz.

Özgür Öztürk:

Bakanlığımızın ulusal siber güvenlik anlamındaki görevleri 5809 sayılı kanunla; ulusal anlamda politika belirleme, stratejilerin oluşturulması ve bu stratejiler kapsamında eylem planlarının geliştirilmesi, bu eylem planlarının ilgili ve sorumlu kuruluşlarla koordinasyonlu bir şekilde tamamlanmasına yönelik sürecin yönetilmesi işlemlerini yürütüyor. Bir taraftan da USOM eliyle operasyon faaliyetleri yürütmeye devam ediyor. Mevcut eylem planı içerisinde 5 ana stratejik konu belirlenmiş durumda. Bunlar içinde

kritik alt yapıların korunması elbette bulunuyor. İnsan kaynağının arttırılması ve farkındalığının oluşturulması. Siber suçlarla mücadele edilmesi. Siber güvenliğin ulusal güvenliğe entegrasyonu hususları yer alıyor.

USOM ne gibi faaliyetler yürütüyor? USOM, siber olaylara müdahale noktasında siber tehditlerin tespit edilmesi, çeşitli kritik altyapıların ve ülkemizin siber uzayına yönelik kaynakların taranmak suretiyle zafiyetlerin belirlenmesi, risklerin tespit edilmesi ve bu tespitler neticesinde ilgili kurum-kuruluşlara yönelik alarmların, uyarıların yürütülmesi. Çeşitli noktalarda duyuruların yapılması ve olayın koordinasyonlu yürütülmesi faaliyetlerini içeriyor. Tabii gerektiğinde, çok kritik durumlarda bünyemizde bulundurduğumuz ekiplerle yerinde olay müdahale koordinasyonu da bu çerçevede işletiyor. Dolayısıyla siber olaylara müdahale kapsamında ulusal koordinasyonu sağlama görevlerini ve faaliyetlerini USOM kapsamında yürütüyoruz.

USOM'un altında belirlenen sektörler, kritik altyapılar var. Bu sektörler ve altyapılarda kurulan sektör SOME sayısı şu anda 14 olmak üzere ve kurumsal siber olaylara müdahale ekipleri, 1294 civarında. Bütün bu USOM, sektörel SOME ve kurumsal SOME organizasyonu içerisinde ülkemizin siber alanda ve kritik altyapılarına yönelik faaliyetler 7/24 durmaksızın, her an koordinasyon içerisinde devam ettirmekteyiz.

USOM'un temel faaliyet alanlarını 4 ana başlıkta toparlıyoruz. Kapasite inşası bu programlardan bir tanesi. Hızlı tespit ve erken önleme sistemlerinin geliştirilmesi ve adaptasyonu bir başka başlık. Yine siber güvenliğe ilişkin, siber tehditlere ilişkin tehdit istihbaratının edinimi, üretimi, paylaşımı son derece önemli bir konu. Ve tabii ki kritik altyapıların korunması yine temelde yürüttüğümüz 4 ana başlık içerisinde yer almakta. Şu anda hâlihazırda USOM koordinasyonunda bütün siber olaylara müdahale ekipleri ve bu ekiplerde görevli uzman arkadaşlarımız tamamen ulusal iç kaynaklarda geliştirilmiş olan SOME iletişim platformu üzerinden anlık olarak bütün uyarıları, alarmları, ihbarları çift yönlü olarak etkileşim içerisinde, güvenli bir ortamda sürdürebilmektedir. 2017 yılında hayata geçirdiğimiz SOME iletişim platformu, bizim anlık olarak SOME'lerle iletişimimizi sağlayan bir platform.

Kapasite inşası dediğimiz zaman, eğitim faaliyetlerini bir taraftan yürütüyoruz. Ülkemizdeki hem kamu kurumlarında hem kritik altyapılarında bulunan özel kuruluşlardaki siber olaylara müdahale ekipleri içerisindeki insan kaynağımızın düzeyinin yükseltilmesi, ülkemiz açısından ihtiyaç duyulan siber güvenlik uzman kaynağının da bir taraftan temin edilmesi, yetiştirilmesi faaliyetlerini içeriyor. Bu çerçevede kamu kurumlarımıza yönelik hem genel eğitimler verdiğimiz gibi hem de sektör spesifik olmak üzere; enerji, sağlık vb. alanlarında da eğitim veriyoruz. Ayrıca kamuya açık eğitimler düzenliyoruz. Son 3 yıl içerisinde, siber güvenliğin çok çok farklı alanlarında, IOT güvenliğinden zararlı yazılım analizine birçok alanda, 50'yi aşkın sınıfta 3000'in üzerinde kişiye eğitimler düzenledik.

Bir başka üstlendiğimiz faaliyet "Siber Yıldız" yarışmaları. Bu 2017 ve 2019 olmak üzere 2 defa düzenlediğimiz bir yarışma. 30.000'e yakın başvuru almış ve yarışmacıların 24 saat kıyasıya mücadele ettiği bir Siber Yıldız yarışması. Burada tespit ettiğimiz yetenekli gençlerin hem ülke adına kamu kurumlarında ihtiyaç duyulan pozisyonlara yerleştirilmesi hem de tespit ettiğimiz yetenekli ve dereceye girmiş yarışmacıların USOM bünyesinde istihdam edilmesine yönelik çalışmalarımızı sürdürüyoruz.

Bir başka uygulamamız yine tamamen iç kaynaklarla geliştirdiğimiz Fetih Siber Talimhane Uygulaması. Burada da bireysel olarak uygulamalı bir laboratuvar ortamında siber güvenlik uzmanlarının kendilerini deneyebilecekleri, test edebilecekleri, kendilerini geliştirebilecekleri bir ortam sunuyoruz. Siber Yıldız yarışmasından çıkan 150 kişilik bir grupla ilk fazda eğitimini aldık. Bundan sonra da gerek kamu kurumlarında gerekse bu tür faaliyetlerden gelen arkadaşlarımızı bu tür eğitimlere dâhil ediyor olacağız.
İkinci önemli başlığımız hızlı tespit ve erken müdahale sistemlerinin geliştirilmesi. Tabii insan kaynağını oluşturmanız gerekiyor. Teknolojiyi bunun yanında kullanmamız gerekiyor. Dolayısıyla USOM bünyesinde Avcı, Azad, Kasırga gibi değerleri belki de yüz milyonlarca lira olacak uygulamaları yine iç kaynaklarla geliştiriyoruz. Avcı uygulamamızla zararlı yazılımlar bulaşmış sistemleri, bunların komuta kontrol merkezlerini ve ele geçirilmiş olan sistemleri tespit ederek bunları ilgililerileriyle iletişime geçip gerekli önlemlerin alınmasını sağlıyoruz.

Yine Azad uygulamamız yeni nesil uygulamalar dediğimiz makine öğrenmesi, yapay zekâ temelli uygulamalarız. Burada da Botnetlere dahil olmuş sistemlerin tespit edilmesi noktasında çok çok önemli adımlar atıyoruz.

Kasırga uygulaması bir başka uygulamamız. Burada 7/24 ülkemizin internete açık kaynaklarının taranması, zafiyetlerin tespit edilmesi, hizmet sürekliliği açısından kontrol edilmesi ve ilgili taraflarla iletişime geçirilerek anlık olarak buna tepki verilmesi yürüttüğümüz faaliyetler arasında.

Kritik alt yapıların korunmasında ne tür faaliyetler yapıyoruz? Siber güvenlik operasyon merkezini kurduk. Avcı'dan, Kasırga'dan, Azad'dan gelen veriler hem kendi uzman ekiplerimiz tarafından tespit edilen zafiyet ve veriler hem SOME'lerimizden gelen bilgiler hem de dış paydaşlarımızdan aldığımız tespit ve istihbaratları konsolide edilmesi suretiyle vakit geçirmeksizin, 7/24, anlık olarak olaya müdahale imkânı sağlıyoruz.

Bunun yanında ülkemizin elektronik haberleşme altyapısına yönelik herhangi bir kesinti ya da hizmet sürekliliği açısından oluşan problemlerin tespiti ve bunu operatörlere anlık olarak iletişime geçmek suretiyle gerekli çalışmaların yapılması kapsamında güvenlik operasyon merkezimiz faaliyetlerini yürütüyor.

Kritik altyapıların korunmasına yönelik yine zararlı yazılım analiz laboratuvarımız var. Burada analizlerimizi gerçekleştiriyoruz. Dijital kayıt inceleme, servis inceleme, zararlı bağlantıların tespiti, sızma testlerinin yapılması ve bu yaptığımız faaliyetler neticesinde de çeşitli alarmların üretilmesi, uyarıların yayınlanması, duyuruların yapılması şeklinde faaliyetlerimizi özetleyebiliriz. Yaptığımız bu faaliyetler neticesinde kurum ve kuruluşlardaki kritik ve acil olarak ele alınması gereken zafiyetleri tespit ediyoruz. Bugüne kadar yaklaşık 3 yıl içerisinde 7 binin üzerinde bir zafiyet tespit etmişiz. Ve bu zafiyetler ilgili kurumlarla, kuruluşlarla vakit geçirilmeksizin irtibata geçilmek suretiyle gerekli önlemlerin alınması sağlanmış durumda.

Yine zararlı bağlantılar tespit edilerek çeşitli IP'ler, domainler, oltalama amacı ile kullanılan ya da başka amaçlarla kullanılan zararlı bağlantılar tespit edilerek, operatör seviyesinde bu zararlı bağlantıların engellenmesi sağlayıp vatandaşlarımızın, kurumlarımızın, özel sektörümüzün bunlardan etkilenmesinin önüne geçiyoruz.

Kritik altyapılarımızla 7/24, ülkemizin siber uzayını yaklaşık 16 milyon IP'yi taramak suretiyle gerekli zafiyet ve izleme işlemlerini yine gerçekleştiriyoruz. Bu kapsamda USOM'a kazandırılan imkânlarla birçok zafiyet tespit edilerek ilgililerliyle paylaşmış durumdayız.

Tehdit istihbaratı edinimi, üretimi, paylaşımı yine önemli gördüğümüz hususlardan bir tanesi. Bu kapsamda gerek yurtiçi paydaşlarımızdan gelen istihbarat bilgileri, gerek kendi ekiplerimiz içerisinden tespit edilen istihbaratlar ve gerekse uluslararası FIRST, CAMP, ITU-IMPACT, MISP, TI gibi organizasyon ve kuruluşlardan elde ettiğimiz istihbaratlar değerlendirilmek suretiyle olay tespit edilmesi halinde önlemler zaman geçirilmeksizin alınmaktadır.

Gökhan Evren:

Teşekkür ederiz Özgür Bey'e verdiği bilgiler için. Şimdi sırada Anadolu Ajansımız var. Ardından da hemen YSK'ya söz vermek istiyorum. YSK tarafından Daire Başkanımız Sarp Sertcan. İkisi de önemli altyapılarımız, göz önünde olan altyapılarımız. Kritik dönemlerde hizmet sürekliliği çok önemli olan sistemleri yönetiyor bu Daire Başkanı arkadaşlarımız ve ekipleri. Öncelikle Anadolu Ajansı'na, Yakup Bey'e sözü vermek istiyorum. Sistemlerinizin güvenliğini ve sürekliliğini sağlamak için yaptığınız çalışmalar hakkında az önce örneğini verdiğimiz teknoloji, insan kaynağı ve süreçler bağlamında çalışmalarınızı bizimle paylaşır mısınız?

Yakup Şıvka:

Anadolu Ajansı, hepinizin de bildiği gibi üretim kapasitesi ve etik kapasitesi bakımından değerlendirildiğinde dünyanın en büyük ajansları arasında. Bugün 100'ün üzerinde ülkede muhabir barındırıyoruz ve 13 ayrı dilde dünyaya yerinden yayın yapıyoruz. Gerçekten büyük bir operasyon ve bu operasyonu yürütmek büyük külfet aslında. Ama böyle bir operasyonu yürütecek ekibin arka planında teknoloji geliştirmek de ayrı bir zorluk.

Haberciler özgürlüğüne çok düşkün insanlar. Yani onlar için sizin sınır dediğiniz şeyler onlar için araştırma sahaları. Bugün internette birçok kamu kurumunda yasak dediğimiz, belli kategorilerde engellediğimiz bir site ya da bomba eğitimi veren siteler haber için araştırma alanı. Dolayısıyla da oralara da girmek istiyorlar. Haberciler biraz da hani üst yöneticilere de yakın olma sebebiyle çok sınırlara gelen insanlar değiller. Kural koyamıyorsunuz onlar için. Mümkünse hiç şifre koymadan sistemlere girelim istiyorlar. Basit de olsa şifreyi kullanmak istemiyorlar. Sizin yaptığınız her adım habercilikle ilgili haberin gecikmesine sebep olan, onların sözleriyle tırnak içinde engel olan, sert konan, yokuşa sürülen konular haline geliyor. Dolayısıyla özgürlükle güvenlik arasında bir denge gütmeniz gerekiyor. Ne kadar çok özgürlük verirseniz insanlara bu siber güvenlikte o kadar çok ödün veriyorsunuz. Özgürlüğü ne kadar kısarsanız o kadar güvenli hale geliyorsunuz fakat bu sefer de habercilikle ilgili işin icra edilmesi anlamında birçok engel çıkarmış oluyorsunuz. Biz yaşadığımız bu süreçte habercilerle orta yolu bulmaya çalıştık. Ne aşırı güvenli bir ortam ne aşırı özgür bir ortam. Öncelikle ilk geldiğim dönemlerde hatırlıyorum şifrelerle ilgili ciddi sıkıntılar yaşamıştık çünkü bütün sistemlerimiz farklı farklı şifrelere sahip ve ben monitörler üzerinde farklı sistemler için şifreler olduğunu görüyordum. Çünkü unutuyorlar, hatırlayamadığı için monitörler üzerine yapıştırılmış şekilde bulunuyordu. Öncelikle bu yapıyı bir toparladık. Single sign on dediğimiz tek şifre mekanizmasıyla bütün uygulamaların girişi yapılabilen bir yapıya geçtik. Bu haberciler için büyük kolaylık. Ama bir taraftan da büyük bir risk aslında. Niye, çünkü eline aldığı şifre her türlü sisteme erişebildiği için kaybedildiği anda büyük bir zafiyet aynı zamanda, büyük bir risk barındırıyor. O şifrenin daha karmaşık olması, daha büyük olması gerekiyor. Onun belli sürelerle değişilmesi zorunluluğu gerekiyor. Bütün bunlar haberciler için alışılması zor olan alanlardı. Bunu zamanla ve riskin büyüklüğünü anlata anlata, farkındalığı artıra artıra habercilere kabul ettirdik. Şu anda belli dönemlerle zor şifreleri değiştirmeye alıştılar. Bunun bir sonraki aşamasını güvenlik anlamında belli bir yıldan sonra buna ancak geçebildik. O da OTP dediğimiz ikinci doğrulama mekanizması. Haberciler zaten bir şifre kullanmaya imtina eden insanlar diğer taraftan ise bir şifre giriyorsunuz, yetmiyor ayrıca bir donanım üzerine ikinci bir kod üreterek sisteme girmelerini söylüyorsunuz. Tabii bunun çok acı örnekleri olduğu için mutlak kabullenmek zorunda kaldılar. Şu anda bütün sistemlerimiz OTP entegrasyonu ile birlikte ayrıca mobil cihazlar üzerinde ürettiğimiz kodlar ile giriş yapılıyor. Tabii mobil cihazlar üzerinde üretilen o kodu üreten uygulamanın da güvenliği önemli. Biz burada da o uygulamayı da kendi içimizde geliştirerek aslında güvenliği uçtan uca tamamlamış olduk.

Bununla ilgili kötü örnekler de var. Katar Haber Ajansı'na bir siber saldırı düzenlendi. O saldırıda Katar Emiri ağzından bir haber yayınladı Katar Haber Ajansı, devlet ajansı aracılığıyla. Ve bildiğiniz o körfez krizi o haber sebebiyle çıktı. O haberde hem Suudi Arabistan Prensi'ne hem de Amerikan Başkanı'na ağır ifadeler de bulunuyordu. Bir taraftan da İran'ın dost ülke olduğundan bahsediyordu. O haberin hemen akabinde zaten Arabistan büyük bir refleks gösterdi ve Mısır, Birleşik Arap Emirlikleri ve Arabistan'ın blok oluşturduğu grup Katar'a karşı ambargo başlattı. Hatta bir dönem işgale kadar gidiyordu Türkiye müdahale etmese. Katar Emir'i çıktı "ben yapmadım, sistemlerimiz etkilendi" dediği halde bir taraftan aslında "minareyi çalan kılıfını bulmuş" misali onu bahane ederek istedikleri ambargoyu koymaya başladılar.

Şimdi sistemlerinizi bu şekilde kullanıcı eğitimi anlamında güvenli hale getirmek sadece bir uygulamayla ya da şifre yönetimi ile mümkün değildir. Bütün sistemlerin uçtan uca bir güvenlik mekanizmasıyla donatılması gerekiyor. Yani şöyle söyleyebilirim; çok güzel bir Firewall'unuz var, yeni nesil Firewall. Güvendeyim diyebilir misiniz? Hayır, diyemezsiniz. Sistemlerin en uçtan, son kullanıcıdan, antivirüs sisteminden başlamak üzere, akabinde bahsettiğim OTP sistemleri, network erişim sistemleri-NAC dediğimiz, akabinde sanal web sunucu sistemleri, sonra WAF dediğimiz uygulama güvenliği sistemleri, SIEM dediğimiz log ürünleri ve nihayetinde içerik filtreleme, IPS, IDS ve Firewall sistemlerinin birbirleriyle uçtan uca entegre ve birbirini tamamlayan ürünler olması gerekiyor. Maalesef bağımsız çalışan ürünler olduğu zaman da bu zafiyetleri yaşıyoruz. SIEM'de aldığınız bir log ürünü topladığı bir logdan çıkaracağı yorum Firewall için bir komut haline gelebilmeli ve ona göre bir önlem alabilmeli. Dolayısıyla aynı ürün serisini kullanmanın avantajları ya da farklı ürün serisi olsa bile entegre çalışabilen ürünleri kullanmanın avantajları burada çıkıyor. Biz Anadolu Ajansı olarak şu anda uçtan uca diyebileceğim bir şekilde birbirini tamamlayan ve entegre çalışan bir güvenlik mekanizmasına sahibiz.

Gökhan Evren:

Teşekkür ediyoruz Yakup Bey'e verdiği bilgiler için. Özellikle habercilik alanındaki güvenlik önlemlerinin zorluğu noktasındaki deneyimlerini paylaştı bizlerle. Şimdi Yüksek Seçim Kurulu'ndan, Bilgi İşlem Daire Başkanı Sarp Sertcan Bey'e sözü verelim. YSK sistemi de yine çok kritik bir altyapı. Özellikle verdiği hizmet ve hitap ettiği kesimin büyüklüğü tüm Türkiye'ye hitap eden bir altyapı. Bu anlamda yapmış olduğunuz çalışmaları ve siber güvenlikle ilgili önlemlerinizi bizlerle paylaşır mısınız?

Sarp Sertcan:

Yüksek Seçim Kurulu seçim hizmetlerini yürütürken SEÇSİS Bilişim Sistemi ve Otomasyon Sistemi'ni kullanıyoruz. Bu otomasyon seçim sistemi de güvenilirlik ve şeffaflık kavramı üzerinde, iki unsur üzerinde kurulmuş bir kurumsal sistem mimarisi üzerinde tasarlanmış durumda. Bu tasarımda en önemli unsur, sistemin internete kapalı bir ortamda gerçekleşmesi. Yani biz herhangi bir internetle, internet tabanlı bir faaliyet ile iletişim sağlamıyoruz.

Burada seçim dönemi boyunca bütün sistemlerde üretilen bilgilerin kopyası, daha sonra seçmen bilgilendirme ve siyasi parti bilgilendirme kapsamında internet tarafındaki bir ortama aktarılıyor. O ortamdan da tekrar seçim hizmetlerinin gerçekleştirilmesi sağlanıyor. 2007'den beri bu tasarımla beraber 15 genel seçim ve 2700'e yakın da ara seçim gerçekleştirmiştir. Bu süreçlerle ilgili olarak da bizim verdiğimiz hizmet bu kapsamda dünyada sayılı başarılı ve güvenilir bir sisteme sahip olduğumuz söylenebilir. Diğer seçim kurullarıyla iletişime geçtiğimizde bizim ne kadar sağlam bir sisteme sahip olduğumuzu görmekteyiz. Ve bu sistemi de tabii özellikle seçim günü siber faaliyet olaylarına daha sıkılaştırma ve daha fazla SOME ekiplerimizle, süreçlerimizle faaliyetlerimizi arttırıyoruz ve her zaman sistemi güvenilir kılma noktasında faaliyetlerimizi sürdürüyoruz.

Gökhan Evren:

Teşekkür ederiz Sarp Bey. 2014 yılında bir veri tabanının yayınlanması durumu söz konusu olmuştu. Aslında biz de bizzat gittik, o tarihte USOM ekibimizle birlikte YSK'da incelemelerde bulunduk. YSK Başkanımız, ilgili genel müdür yardımcısı ve teknik ekiplerle toplantılar yaptık, sistemlerde de inceleme yaptık. Önemli bir paydaşla da çalışıyor aslında. YSK uzun yıllardır HAVELSAN şirketimizle çalışıyor. Aslında mevzuat gereği, yasal zorunluluk olarak YSK'nın siyasi partilerle paylaştığı bir seçmen veri tabanı var, onunla ilgili bilgi verebilir misiniz?

Sarp Sertcan:

Yasa değişikliğinden sonra, seçim döneminde hızlı, sağlam, verimli, efektif bir şekilde yapılmasından ziyade bizim veri tabanımız her zaman güncel olarak MERNİS Adres veri tabanıyla güncel bir şekilde alışveriş yapıp hemen bilgi alışverişiyle seçimlere hazır oluyoruz. Ama daha sonraki süreçlerde, 2010'dan sonraki, 5980 sayılı kanun değişikliğiyle, siyasi partilerin bilgi iletilmesi konusunda biz internet ortamında bilgi alışverişini yapıyoruz. Ama bu süreçte onlara verdiğimiz web servisleriyle, protokolle şu anda onlara taratılmış tutanakları da imzalanmış tutanakları da veriyoruz. Yani komple kendilerinin o sistemini de siber olaylara karşı koruyoruz. Ama veri tabanı bağlamında, onlara yasa karşılığı bizim sunduğumuz bir SİPPORT siyasi parti portalımız var, biz bu portaldan veriyoruz. Orada yasa gereği o yapılması gereken bir durum onu da herhangi bir yasanın emrettiği şekilde kurumumuzun da verdiği karar gereği paylaşılıyor.

Gökhan Evren:

Teşekkür ederiz. Şimdi ASKİ Genel Müdürlüğümüzden Bilgi İşlem Yöneticimiz Mehmet Sungur'a sözü vermek istiyorum. Belediyeler özellikle kamuya hizmet eden, çok sayıda, direkt doğrudan vatandaşın hizmet aldığı birçok şirketi olan oluşumlar. ASKİ de bunlardan bir tanesi. Son dönemde ülkemizde de çeşitli yurt dışındaki ülkelerde de; örneğin Amerika'da geçtiğimiz aylarda birçok belediyenin kullandığı yazılımlarda, ortak olarak kullandığı belediye yazılımlarında olan zafiyetlerden faydalanan saldırganlar, hizmetlerin kesintiye uğramasına neden oldu. Bu noktada belediyelerimiz de SOME ekiplerini kurdu. USOM'la doğrudan temas halinde çalışıyor. ASKİ olarak bu noktada sizin faaliyetleriniz nelerdir? Hizmet sürekliliği, siber güvenlik açısından önlemleriniz hakkında bilgi verir misiniz?

Dr. Mehmet Sungur:

Ben sıra dışıyım diyen var mı? Normal insanlara benzemiyorum, normal insanlardan biraz farklı düşünüyorum diyen... 1, 2 evet 3.sü de benim. Çünkü normalde inşaat mühendisliği okudum. 1993 yılında eve bir bilgisayar aldım, orada bütün hayatım değişti. İnşaat mühendisliğini tamamen bıraktım, o günden sonra asla bir inşaat işi yapmadım. 2004 yılındaysa DNA ile tanıştım o günden sonra da Harvard Medical School ile 10-15 yıldır ortaklaşa yürüttüğümüz birkaç proje var.

Arkadaşımız az önce Katar'ın yaşadıklarını anlattı. Gençlerimiz her konu hakkında, özellikle siber güvenlik konusunda, duydukları ya da gördükleri her haberi mantık süzgecinden geçirip, sorgulamalı, doğruluğu kanıtlanmamış ifadelerin, kendilerini yönlendirmesine asla izin vermemelidir.

Siber Güvenlikle ilgili üç unsurdan bahsedildi. Verilerin sıkıştırılması, kırılamayacak şifrelerin oluşturulması ve büyük veri. Biraz önce de farklı düşünmekten bahsetmiştim. Bu üç konuda geliştirilecek yeni yaklaşımlarda doğadan ilham alabilir miyiz, bunu gençlerimiz düşünmelidir. Örneğin kırılamayan tek şifre DNA'dır. Bakın DNA sadece adenin, guanin, sitozin, timin'den oluşur. Ama 7,5 milyar insanın hiçbirinin DNA'sı birbirini tutmaz. Kanser hücresiyle uğraştık Harvard'da yaklaşık 10 yıl, kanser hücresi biliyorsunuz bir DNA zinciridir. Adenin, guanin, sitozin, timin diye gider, bir şifredir bu. Bu şifrenin bittiği yer kanserli hücrenin olduğu yerdir. Eğer siz şifreyi tahmin edebilirseniz, oraya nelerin geldiğini tahmin edebilirsiniz, böylelikle o şifreyi çözersiniz. Böylelikle kanserle uğraşan veya ben bugünden sonra şifre yazacağım diyen kişi ve arkadaşlar daha çok genetik algoritmayla ilgilenseler ve şifrelerini bunun üzerine yazarlarsa iyi olur diye gençlere fikir veriyorum.

Şimdi gelelim ASKİ'ye ve su güvenliğine. Ankara önümüzdeki yıllarda 2023–2030 ve ondan sonraki yıllarda çok aşırı derecede kurak yıllar yaşayacak. Ama tabii bundan önce aşırı derecede yağışların olacağı yıllar da olacak. O aşırı derecede yağışların olduğu yıllarda suları depolayacağız, kurak olduğu yıllarda kullanacağız. Dünya Su Polisi diye bir şey kurulacak, bu kesin. Kaçınılmaz bir son. Artık suyu kafanıza göre kullanamayacaksınız. Başka ülkeden de bir polis gelip sizi uyaracak. Eğer siz suyunuzu dışarıdaki saldırılara ve içerideki saldırılara güvenli hale getirmezseniz, artık su da bulamazsınız. Özellikle gençlerimizi teknik detaylarla boğmak istemedim açıkçası onu söyleyeyim. Teşekkür ediyorum.

Gökhan Evren:

Mehmet Sungur Bey'e çok teşekkür ediyoruz. Farklı bir bakış açısıyla izleyicilerimizi, dinleyicilerimizi kısa bir rahatlattı. Şimdi sırada Savunma Sanayii Başkanlığı'ndan Siber Güvenlik Kümelenmesi Projesi'nin koordinatörü Hasan Hüseyin Özbenli'ye sözü vermek istiyorum. SSB, yaptığı çalışmalarla yerli ve milli teknolojilerin mevcut durumu, paydaşları nasıl bir iş birliği içine sokarız, burada arz ve talebi nasıl buluştururuz, aynı zamanda bu Kobilerimizi nasıl destekleriz gibi çalışmaları yürütüyor. Bununla ilgili bizimle bilgi paylaşır mısınız?

Hasan Hüseyin Özbenli:

Savunma Sanayi Başkanlığı bildiğiniz üzere silahlı kuvvetlerin ve kamu kurumlarının güvenlik ihtiyaçlarını karşılamak, tedarik etmek amacıyla kurulan bir kurum. 15-20 yıldır yürüttüğü sanayileşme politikalarıyla platformlar tarafında %70'e varan yerlilik oranını yakalamış durumdayız. Artık milli uçaklar, milli muhabere uçakları, milli tank, milli helikopter gibi platformlara yönelik çalışmaları siz de basından şahit oluyorsunuzdur. Tabii fiziksel güvenlik, sınır güvenliği ya da platform güvenliğinin yanında siber güvenlik de Savunma Sanayi Başkanlığı'nın gündeminde bir süredir. Çünkü bu konuyla ilgili de Silahlı Kuvvetlerimizin ihtiyaçları bize geliyor ve buna yönelik Siber Güvenlik ve Bilişim Sistemleri Grup Başkanlığı olarak projeler yürütüyoruz.

Tabii biz 2017 yılında siber güvenlik alanında sektör analizleri yaptığımızda bu alanda bir yabancı hegemonyasının olduğunu gördük ve sektör olarak neler yapabiliriz, sektörümüzde hangi firmalar var, hangi ürünler var, bunlarla ilgili çalışmalar neler bunlarla ilgili bazı çalışmalar yaptık. Şimdi tabii panel konusu kritik altyapılar. Kritik altyapılarda seçim güvenliği konusu konuşuluyor, su güvenliği konuşuluyor. Diğer taraftan ulaşımdı, savunmaydı bunların hepsi kritik altyapılara giriyor. Ve bu kritik altyapılarda yerli – milli teknolojilerin kullanılması gerçekten çok önemli bir husus. Ancak güvenliğimizin bu şekilde sağlanabileceğini düşünüyorum. Çünkü hani şöyle bir benzetme yapmak

istiyorum; bir kale inşa etmişsiniz, çok büyük yatırımlar yapmışsınız, içinde kritik varlıklarınızı koruyorsunuz ama bu kalenin kapısına yabancı bir asker koymuşsunuz. Surlarına yabancı askerleri yerleştirmişsiniz. Gerekçeniz ne bunu yapmakla, gerekçeniz de bu askerlerin dünyadaki en kabiliyetli, en donanımlı askerleri olduğunu düşünüyorsunuz. Ve diyorsunuz ki hani yerli ya da kendi askerimiz bu konuda yetersiz bu yüzden ben bunlarla çalışıyorum diyorsunuz. Böyle bir güvenliğin gerçekten de söz konusu olmadığını düşünüyoruz.

2017 yılında biz sektör çalıştayları yaptık. Kamu kurumları çalıştayı yaptık. Kamu kurumlarının siber güvenlikle ilgili ihtiyaçları, sorunları neler? Özel sektörün neler? Akademinin neler gibi farklı paydaşlarımızla bir araya geldik. Ve ortaya bir kümelenme modeli çıktı. Kümelenme, siber güvenlik kümelenmesi adını verdiğimiz bu model tamamen siber güvenlik sektörünün yerli – milli sektörün geliştirilmesi amacıyla oluşturulmuş ve savunma sanayi icra komitesinden çıkmış bir kararla 5 yıllık bir proje aslında. Bu alanda, baktığımızda 45 firmayla yola çıktığımız zamanlarda, o zaman bize de sorsalar, siber güvenlik alanında çalışan kaç tane firma var, bu kadar firma olduğunu biz bile bilmiyorduk. Herkesin bildiği, çalıştığı, çevremden duyduğum 45 – 50 civarında firma vardı ama şu anda siber güvenlik alanında ürün geliştiren, hizmet üreten, eğitim veren 128 tane firma var. Bunların yanında bir sürü de başvuru var. Bu başvurular da tabii değerlendiriliyor. Tabii sektörümüzün gelişmesi, ekosistemin gelişmesi önemli. Yani hakikaten bu 128 firma içerisinde çok başarılı firmalar var. Yani globalde ürün satan, onlu rakamlarda milyon Euro'luk yatırımlar alan, firmalarımız da var. Ancak sonuçta şu noktaya geliyor, bir firma ne kadar güçlü olursa olsun sonuçta hangi ekosistemdeyse ya da hangi ülkedeyse oranın ekosistemiyle anılıyor nihayetinde. Bizim amacımız aslında burada hem bahsettiğim yerli – millilik noktasında yabancı hegemonyasını kırmak hem de bu firmalarımızın, ürünlerimizin globalde rekabet edebileceği seviyeye gelmesini sağlamak. Yurt dışına gidiyorlar, "Türkler de mi siber güvenlikle ilgili bir şeyler yapıyor?" diyorlar. Yani bunu kırmak en nihayetindeki amacımız diyebiliriz.

Şimdi sektörle ilgili, pek tabii firmalarımızla ilgili analizler yapılıyor, firmalarımızın performansları nasıl artırılabilir ya da toplu olarak sektörün performansı nasıl en üst noktaya getirilir, onunla ilgili çalışmalar yapıyoruz. Bunun yanında biz insan kaynağına da nasıl en hızlı şekilde ulaşırız, orada da siber güvenlik kulüpleri ile bir araya geliyoruz. İlk çağırdığımızda, siber güvenlik kulüplerine ulaştığımızda, 12 siber güvenlik kulübü vardı üniversitelerde. Ama şu anda 43 tane siber güvenlik kulübü var. Onlarla birlikte de eğitim faaliyetleri yapılıyor. Bu biraz sektörle ilgili bir şey. Sektörümüzde şu anda 4000 – 5000 aralığında bir siber güvenlik uzmanı sayısı var gibi rakamlar alıyoruz ama tabii bu rakamlar sürekli değişkenlik de gösteriyor. 180 tane ürün, 400 tane hizmete ve eğitime yönelik bir katalog çalışmamız da mevcut. Yani bunu gittiğimiz kamu kurumlarında, buluştuğumuz paydaşlarımızla da paylaşıyoruz. Kataloğumuzda ürünlerin bir taksonomisi var, birçok ülkenin siber güvenlik yol haritasını görmüşsünüzdür. Bu da bizim ülkemizin aslında bir ürün haritası diyebiliriz. Farklı ürün ailelerinde hangi ürünlere sahip olduğumuzu gösteren bir harita. Bunun ayrıntıları zaten kataloğun içerisinde mevcut.

Burada sektörle yaptığımız çalıştaylarda aslında 4 temel strateji üzerinde biz faaliyetlerimizi yürütüyoruz. Paydaşlar arası etkileşim, insan kaynağının geliştirilmesine yönelik çalışmalar, sektör kapasitesinin artırılması ve pazara erişim gibi çalışmalar yürütürüz. Bunun dışında aslında sektördeki fikirlerin filizlenmesini hedefliyoruz. Burada firmaların yetkinliklerinin artırılması, vasıflı iş gücünün artırılması, firmalarımızın teknolojik kabiliyetlerinin artırılması ve globalde rekabet edebilecek seviyeye gelmeleri gibi hedeflerimiz mevcut.

Paydaşlar arası iletişim konusunda kritik altyapılarda hep bahsedilen enerji sektörü, ulaşım sektörü, savunma sektörü, finans sektörüyle bizim siber güvenlik sektörümüzü bir araya getiriyoruz. Yani müşteriyle bir nevi üreticiyi bir araya getirerek böyle sektör odaklı etkinlikler yaptık. EPDK ile beraber enerji sektörüyle siber güvenlik etkinliği yaptık. BDDK ile beraber finans sektörüne siber güvenlik, savunma sektörü, yine burada BTK'da yaptığımız ulaştırma sektörü ile ilgili etkinlikler yapıyoruz.

Bunun dışında farklı çalışma gruplarımız mevcut. İhracatı nasıl geliştirebiliriz, teknolojik liderlik nasıl yapabiliriz, burada teknolojilerimizi nasıl artırabiliriz bununla ilgili çalışmalar var. Ürünlerin sertifikasyonu ile ilgili çalışmalar başlamış durumda. Yani bu 128 tane ürün gerçekten ürün mü? Firewall var ama gerçekten Firewall'un yeteneklerini gösteriyor mu, o fonksiyonları yerine getiriyor mu ve burada bir test sertifikasyon mekanizması oluşturduk. Bunu projelendirdik ve ürünlerimiz test edilmeye başlandı şu anda. Ürün aileleri altında burada fonksiyonel kriterler ortaya çıkarıldı. Test kriterleri ortaya çıkarıldı ve 6 aydır devam eden yoğun bir çalışmanın sonucunda da ürünlerimiz artık bir savunma sanayi iştiraki olan TRTest tarafından da etiketlenecek.

İnsan kaynağı tarafında eğitimlerin verildiğini söylemiştim, bu 43 üniversite kulübü ile birlikte son 10 ayda üniversiteler ile beraber yaptığımız kamplarla birlikte 2000'e yakın öğrenciye eğitim verilmiş durumda ve bu eğitimleri sektördeki firmalarımız veriyorlar. Kümelenmeye üye olan firmalar veriyor. Burada da hakikaten tohumları attığımızı düşünüyoruz ve bunların yeşereceğine de inanıyoruz. Diğer bir taraftan bu insan kaynağı ile ilgili ya da Türkiye'nin global arenada sesinin duyurulmasıyla alakalı bir proje başlattık. Orada da mesela "Biz Senin Yanındayız" şeklinde, destek vermek amacıyla Black Hat, Def Con gibi konferanslarda sunum hakkı kazanan uzmanları masraflarını karşılayarak bu platformlarda Türkiye'nin adını duyurmasını hedefliyoruz. İşte bu yıl 3 kişiyi Def Con'a gönderdik. Bunun gibi çalışmalarımız mevcut.

Pazara erişimle ilgili kamu kurumlarına yapılan ziyaretler var. Kullanılabilirlik anlamında etkisi olması açısından, burada katalogdaki ürünler anlatılıyor. Firmalarımızın globalde yer alması amacıyla Hollanda'ya bir siber güvenlik eğitimine geçen yıl 30 tane firmamızı götürdük. Bu yıl Dubai'ye götüreceğiz. Almanya'ya keza yine götürdük. Bunun dışında yurt dışında temsil kabiliyetleri kazanmaları için küme olarak, sektör olarak yurt dışına da aslında seferler düzenliyoruz.

1 yılda neler yaptık derseniz, işte burada aslında bahsettiğim şeyler. 1000'in üzerinde hatta şu anda 2000'e yaklaştı sektör etkinlikleri, çalışma grupları, eğitim faaliyetleri gibi birçok alanda etkinliğimiz var. Web sitemizden, sosyal medyadan çalışmalarımızı takip edebilirsiniz.

Bir de yakın zamanda yapacağımız bir uluslararası Siber Savaş&Güvenlik konferansı var SSB himayelerinde. Ona da ben sizi davet etmek istiyorum, buradan duyurusunu yapmak isterim. 20 - 21 Kasım'da uluslararası arenada, hatta şöyle söyleyeyim, yurt dışında bizi temsil eden Türklerin de ağırlıklı olduğu bir konferans olacak. Hepinizi beklerim.

Gökhan Evren:

Çok teşekkür ediyoruz bütün katılımcılarımıza ve dinleyicilerimize. Panelimizi bu şekilde sonlandırıyoruz.


HAVELSAN
HAVELSAN
HAVELSAN

PROF. DR. KEMAL BIÇAKCI

TOBB Ekonomi ve Teknoloji Üniversitesi Bilgisayar Mühendisliği Öğretim Görevlisi

GÜNÜMÜZ ve GELECEĞİN KİMLİK DOĞRULAMA YÖNTEMLERİ

Hoş geldiniz. Ben kimlik doğrulama ile ilgili konuşacağım ve uzmanlık alanım da bu. Kimlik doğrulama niye önemli bir problem? Günümüzde nasıl yapılıyor? Gelecekte nasıl yapılması öngörülüyor? Bu konuları konuşacağım.

Eğer sadece bir tek şeyi not almak gerekiyorsa benim konuşmamdan şu notu alın: Rob Joyce NSA. Youtube'a gidin, Rob Joyce NSA olarak yazın ve 35 dakikalık bir video geliyor. Bu videoyu lütfen dikkatlice izleyin. Bu Rob Joyce denilen kişi, NSA Özel Erişim Operasyon Şefi. 2013 yılına kadar Edward Snowden dokümanları ifşa olmadan önce böyle bir birimin varlığı bile bilinmiyormuş. 2016 yılında bu arkadaş bir konuşma yapıyor ve konuşmanın ana fikri şu: "Neler yaparsanız, biz sizi daha zor kırarız, daha zor hack ederiz." Oradan ben sadece bir alıntı yaptım. Orada diyor ki: "Sıfırıncı-gün saldırıları denilen şey; zero day attack diye bir şey var. Ne demek zero day attack; yani o güne kadar daha bilinmeyen bir açıklık. Ve bu açıklığı kullanarak tabii sızılabilir ama bu açıklıkları kullanmamıza gerek kalmıyor. Niye; çok daha rahat, çok daha kolay hedefli oltalama saldırıları diye bir şey var. Yani mail atıyorsunuz, onun parolalarını alıyorsunuz ve bu sayede zaten parolayı almış olmak, kimlik bilgilerini çalmış olmak çoğu zaman yeterli oluyor ve çok daha kolay bir işlem. Öyle

olunca biz genelde bu şekilde başarı oluyoruz" diye anlatıyor. İşte ben de tam olarak bu problemle ilgileniyorum yani acaba şu an günümüzde % 90 - 99 belki parolalara bağlı olan kimlik doğrulamayı nasıl daha güvenli hale getiririm. Bununla ilgili rakamlar var ama ben sadece bir anekdot anlatayım. Bizim okulda bir de siber güvenlik yüksek lisans programımız var. Oraya bir arkadaş başvurmuştu seneler önce. Kendisi TÜBİTAK'ta sosyal mühendislik test takımında görevliymiş. Hedefleri saldırganların kullandığı psikolojik manipülasyon teknikleri yardımıyla kullanıcılardan bir takım hassas verileri toplamak? Şöyle yürüyor iş; kurumla anlaşıyorsunuz, anlaşmayı imzaladıktan sonra diyorsunuz ki biz telefon açacağız, şu kadar kişiye ve bakalım parolalarını veriyorlar mı vermiyorlar mı test edeceğiz. Merak ettim, hani nasıl başarı oranlarınız nedir? Atıyorum 25 kişiye telefon açtınız ne kadarının parolasını toparlayabiliyorsunuz? Hocam % 100'ü aştığımız oluyor dedi. Dedim yanlış mı anlaşıldı, sorumu tekrar ettim. "Ne demek %100'ü aştığımız oluyor?" "Hocam şöyle oluyor" dedi. "Biz telefonu açıyoruz. İşte falanca probleminizden dolayı bize parolanız lazım diyoruz. Biz teknik iletişimden arıyoruz diyoruz, ondan sonra kişi parolasını veriyor. Ondan sonra da, ofisteki arkadaşımın da aynı problemi var diyor, telefonu ona uzatıyor. Biz günün sonunda 25 kişiye telefon açmışız, 30 tane parola toplamışız. Yani %100'ü aşmak bu demek."

Şimdi bu olayla ilgili iki türlü yorum yapılabilir. Bir tanesi şu; kullanıcılar bilinçsiz, kullanıcılar gelişigüzel tıklıyorlar, gelişigüzel veri paylaşıyorlar. Biz ne yapalım, onları eğitelim. Bununla bir yere kadar yol alabilirsiniz. Bir diğeri de acaba kullanıcılar gelişigüzel davransalar da güvenli çalışan kimlik doğrulama sistemleri kurgulayabilir miyiz? Benim esas konum o. Yani kullanıcılar kendi ağzıyla parolasını verecek, kendi ağzıyla her şeyi verecek buna rağmen biz güvenli kalacağız. Olabilir mi böyle bir şey? Şimdi iki faktörlü doğrulama var değil mi? SMS ile elektronik bankacılık uygulamalarında size tek kullanımlık parola geliyor, tek kullanımlık parolayı da giriyorsunuz. İki faktörlü doğrulama yeterli mi? Gerekli ama yeterli değil. O parolalar da yine benzer sosyal güvenlik saldırılarıyla saldırganların ellerine geçebiliyor. Bu tür haberler basına da yansımış durumda. O zaman bizim iki faktörlü doğrulamanın da ötesinde başka bir yaklaşım sergilememiz lazım. Artık o yaklaşımın da özü şu; kimlik doğrulama bir makine öğrenme problemi. Biz çok farklı kaynaklardan kimlik doğrulamayla ilgili bilgi topluyoruz. Ne zaman girmiş, nasıl girmiş, nereden girmiş. Tüm bilgiler ışığında bir anomali tespit etmeye çalışıyorsunuz. Yani bu kimlik doğrulama örneği gerçekten doğru bir örnek mi yoksa bu bir saldırı olabilir mi? Bu örneği bir makine öğrenme problemi halinde inceliyorsunuz ve bu inceleme esnasında toplayacağınız bilgilerin önemli kısmı davranışsal biyometri ile ilgili kısımlar oluyor. Fiziksel biyometri biraz daha fazla bilinen bir şey. Parmak izi gibi, iris gibi. Davranışsal biyometri biraz daha az biliniyor; örneğin benim yürüyüş tarzım, klavyeyi tuşlamam ya da cep telefonunu swipe yapmam da aslında bana özgü. Bana özgü davranışlar sayesinde acaba kimlik doğrulaması yapabilir miyiz? İşte bizim araştırma olarak uzmanlaştığımız ve şirketimizde projeler ürettiğimiz alan bu davranışsal biyometri konusu. Yani normal klavyelerde bu işi yapabilirsiniz ya da mobil tarafa geçersiniz dokunmatik dinamiğinde mobil telefon üzerinde de yani siz evinizde tuttuğunuz mobil telefonda öyle sensörler var ki özel olarak üretseniz belki on binlerce dolara mal edeceğiniz bir telefon elinizde tutuyorsunuz. Ve o telefonda bir sürü sensör var, kulağınıza götürürken ayrı şekilde götürüyorsunuz, yürürken ayrı şekilde orada datalar toplanıyor vesaire. Dolayısıyla tüm bu dataları toplama imkânı ve kimlik doğrulamada kullanma imkânı var.

Ne tür avantajları var böyle bir sistemin, yani davranışsal biyometri kullanan bir sistemin? Bir kere güvenlik avantajları, ikinci faktör, üçüncü faktör olarak kullanabiliyorsunuz. Tamamen pasif olarak yani arka planda, yani kullanıcı daha bu işin farkında olmadan, normal hareketlerini yaparken, normal kullanım esnasında da pasif bir şekilde doğrulama yapabiliyorsunuz. Sürekli doğrulama yapabiliyorsunuz. Bu ne demek; diğer tüm kimlik doğrulama sistemleri sizi kapıya kadar, kapıda kontrol ediyor. İçeriye girdikten sonra bir kontrol yok. Ama bu dediğim davranışları yani klavyenin tuşlanması, swipe hareketleri. Biz mesela elektronik bankacılık uygulamasına girdiğinizde hala devam ettiğiniz hareketler bunlar. Bu hareketler esasında süreklidir, bir doğrulama mümkün ve risk tabanlı bir servis. Yani 0-1 değil, 1 ile 100 arasında bir skor üretip ve bu skorla bizim risk tabanlı bir doğrulama servisi kurmamız mümkün. Herhangi bir özel donanımı yok, maliyet avantajları da söz konusu oluyor.

Ve bu konu tabii çalışılıyor. Avrupa Birliği'nde mesela elektronik bankacılık regülasyonunun içine girmiş durumda. Yani ikinci bir faktör olarak davranışsal biyometri geçerli. Bizim ülkemizde de BDDK'nın taslak yönergesinde bu konuyla ilgili yapılan çalışmalar var, davranışsal biyometri ile ilgili. Ülkemizde de güzel gelişmeler oluyor.

Şimdi biz bu konuda ne yaptık? Bilinen bilgileri, yani diyelim benim kimlik bilgilerimi siz çaldınız. Siz aynı şekilde yani doğru şekilde giriyorsunuz, sistem sizi içeriye almıyor. Ama ben o bilgileri girdiğimde sistem beni içeriye alıyor. Niye çünkü benim girdiğim gibi siz giremiyorsunuz. Ben parolamı çaldırsam, kullanıcı ismimi çaldırsam, pinimi çaldırsam, her şeyimi çaldırsam dahi benim gibi giremeyeceğiniz için sistem sizi kabul etmiyor dolayısıyla tamam eğitim önemli ama bakın öyle sistemler var ki siz ağızınızla kimlik bilgilerinizi paylaşsanız dahi güvenli kalabilen veya güvenliği artıran sistemler mevcut. Çok teşekkür ederim ilginiz için.


HAVELSAN
HAVELSAN
HAVELSAN

Moderator:
Doç. Dr. Bilgin METİN
Boğaziçi Üniversitesi

Ahmet Cengiz GÜRAY
HAVELSAN

Burak ÇİFTER
Bilge SGT

Celil ÜNÜVER
Trapmine

PANEL 3

Siber Güvenliğimize Güç Katan Çözümlerimiz

Burak DAYIOĞLU
Atar Labs

Özdemir ŞARMAN
Kron

Eyüp ÇELİK
Ekon Bilişim

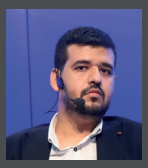
Doç. Dr. Bilgin Metin:

Öncelikle hoş geldiniz diyorum. Ben Bilgin Metin. Yönetim Bilişim Sistemleri Bölümü, Boğaziçi Üniversitesi öğretim üyesiyim. Aynı zamanda Boğaziçi Üniversitesi'nde BÜSİBER'in yöneticiliğini yapıyorum. Burada en önemli konuşulan konulardan biri ekosistem ve bu ekosistemin en önemli ana oyuncuları ise yerli siber güvenlik teknoloji üreticileri. Bu yüzden de ayrıca da çok mutluyum çünkü biz BÜSİBER'i kurduğumuz zaman önümüze 2016-2019 siber güvenlik stratejisini aldık ve neler yapmamız lazım diye oraya bakarak hareket ettik. Orada üniversitelere verilen bazı roller vardı. Bunların hepsini oynamaya çalıştık. Orada üniversitelere yetişmiş insan gücü kazandırmaları diyordu bunun üzerine yaz kampları ve kış kampları düzenledik. Hiç yaz kampımıza ya da kış kampımıza katılan var mı burada dinleyicilerimizden? Onları gördükçe mutlu oluyorum. Biz İstanbul Kalkınma Ajansı destekli bir proje olarak kuruldu, 2016 Aralık'ta faaliyetlere başladık. Hemen 2017 Ocak'ında bir siber kampı düzenledik. Bu zamana kadar şöyle bir baktığımızda 10 tane siber kamp yapmışız. Sonra 2016-2019 strateji belgesine baktığınız zaman üniversitelerin kamu kurumlarıyla sıkı ilişkiler kurması gerektiğini söylüyor. Bu aşamada da daha önce BTK'da da kamu kurumlarına yönelik eğitimler verdik. Boğaziçi Üniversitesi'nde belediyelere, hastanelere yönelik ücretsiz eğitimler verdik. Üniversitelere yönelik ücretsiz eğitimler verdik. Yine BTK sağ olsun davet etti, burada enerji sektörüne yönelik eğitimler verdik. Böylece strateji belgesindeki bir maddeyi daha yerine getirmiş olduk. Bu alandaki üniversite – sanayi işbirliklerinin önemli olduğunun altı çizilir; o alanda da mümkün olduğunca üreticilerle ve yerli üreticilerle bir araya gelmeye çalıştık. Ve 2107 yılının 8 Mayısı'nda "Siber Güvenlik'te Yerli ve Milli Çözümler" zirvesini Üniversitemizde gerçekleştirdik. Sonra yine strateji belgesine baktığımız zaman toplumda farkındalık oluşturacak etkinlikler yapmalı, çalışmalar yapmalı diyordu. Bu alanla ilgili olarak da üniversitemizde kişisel verilerin korunması ve KVKK noktalarında zirveler yaptık.

Bu alanda özellikle geçtiğimiz günlerde İstanbul Kalkınma Ajansı bir fizibilite açmıştı ve biz oraya Siber Operasyon Merkezi Fizibilite Projesi diye bir projeyle başvurduk. Ülkemizde yeterince yetişmiş insan kaynağı yok. Firmalarda farkındalık oluşsa ve eleman almak isteseler bunu alacak insan kaynağı yok. Ve bu durumda siber operasyon merkezlerine gidecekler ama siber operasyon merkezlerinin sayısı yetersiz ve desteklenmeye de ihtiyacı var. Dolayısıyla biz burada özellikle de yerli ve milli firmalarla bir araya gelerek yerli-milli çözümler sunan bir operasyon merkezimiz olsun ve siber operasyon merkezleri de bir araya gelerek hangi konuda destekleri varsa onlara destek vermek noktasında iş birlikleri yapıyoruz. Mesela şimdi Koç Sistem'in bir operasyon merkezi var, onlarla iş birliği anlaşması yapıldı ve orada işe alınacak arkadaşlara eğitimler de vereceğiz. Bu şekilde hem yerli üreticilerle hem kamu kurumlarıyla hem genç arkadaşlarla bir araya gelerek bir sinerji ortaya koyacağımıza inanıyorum. Burada da özellikle genç arkadaşları görmek beni çok çok mutlu etti.

Siber güvenlikte yerli ve milli çözümlerin kullanılmasının önemini herkes anlamış vaziyette. Bu manada yerli ve milli çözümlere güvenmemiz ve var olan sorunların bir şekilde aşılması gerekiyor. Burada çok değerli yerli-milli çözüm üreticileri de var. Ben sözü sırayla onlara vermek istiyorum. Özellikle siber savaş genelinde yerli-milli çözümlerin oynadığı rol üzerine değerli görüşlerini almak istiyorum.

Öncelikle Celil Hocamdan başlayayım. Hocam bu konuda ne düşünüyorsunuz, değerli görüşlerinizi almak isteriz. Özellikle zararlı yazılım konusunda çözümleriniz var ve bunlar çok önemli rol da oynuyor. Daha önceki sunumlarda gördük Stuxnet gibi zararlı yazılımların neler yapabildiğini. Ya da şirketlere özel APT saldırıları geldiği zaman bunu standart yazılımlarla durduramayacağımızı da gördük. Bu alanda sizin değerli düşüncelerinizi almak isteriz.



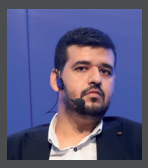
Celil Ünüver:

Öncelikle organizasyon sahiplerine, HAVELSAN'a, BTK'ya teşekkür ederim davetleri için. Bilgin Hocama da teşekkürler. Siber güvenlikte gerçekten yerlileşme ve millileşme önemli bir rol oynuyor. Özellikle artık siber alan aynı zamanda siber güvenlik çözümleri dünya geneline baktığımızda artık bir politika aracı. Hatta yaptırımlara dahi maruz kalabiliyor. Biz Trapmine olarak bu uç nokta güvenlik kısmında aslında yer alıyoruz. Yeni nesil uç nokta güvenliği çözümü üretiyoruz. Zararlı yazılım ve exploit bazlı hatalara karşı. Daha çok davranış temelli, davranış analizi temelli ve yapay zekâ tabanlı çözüm üretmeye çalışıyoruz. Uç nokta güvenliği kısmında son yıllarda örnek vermek gerekirse politik birkaç olay oldu. Haberlerde duymuşsunuzdur zaten; örnek vermek gerekirse Amerika'da Kaspersky toplandı, yaptırıma maruz kaldı ve yasaklandı. Yine aynı şekilde Avrupa Birlik Komisyonu bu ürün için, bu firma için benzer kararlar aldı. Burada aslında söylemek istediğim bu firma aslında casusluk yaptı değil. Böyle bir iddiada bulunuyorlar ancak kanıtlanmış bir şey değil. Aslında mevzu Amerika ile Rusya'nın çekişmesi ve bundan da teknoloji firmalarının da yaptırım gibi sonuçlara maruz kalması ki bir başka mobil üretici benzer durumlara maruz kaldı yine bu Play'a, Android'e erişememek gibi. Bu noktada yerli ve milli çözümler oldukça kritik bir önem arz ediyor. Bugün özellikle baktığımızda globalde kullanılan pek çok güvenlik çözümü, Türkiye'de de çok yaygın olanlar aslında birçok Amerikan, İsrail ve benzeri ülkelerin savunma sanayi firmaları tarafından satın alındı. Yani daha önceden siber güvenlik firması olan birçok ürün bugün baktığımızda Raytheon gibi firmalar tarafından satın alındı. Bildiğiniz gibi Raytheon, Patriot füzelerinin

üreticisi. Bugün mesele F-35 krizi olduğunda benzer bir şekilde aslında kullandığımız diğer çözümleri veya farklı yabancı menşeli, Amerikan menşeli siber güvenlik ürünlerini kullanmamıza da bir ambargo gelebilir. Nasıl F-35'lere yönelik bir ambargo geldiyse, alamadıysak benzer ambargolar kullandığımız pek çok yabancı teknoloji için gelebilir. Bu noktada birçok üründe aslında yerli muadil bir çözüm olması ülkelerin siyasi, ekonomik ve savunma gücü için kritik bir önem arz ediyor. Ben bu şekilde düşünüyorum hocam.

Doç. Dr. Bilgin Metin:

Teşekkür ederim düşünceleriniz için. Gerçekten de daha önce böyle ambargolar oldu hani, yıl 1998. O zaman iş hayatına yeni atılmıştım. Armada Bilgisayar'da Cisco mühendisiyim, VPN için 56 bit DES algoritması kullanmanıza izin veriyorlar. 168 bit lisansını satmıyorlar. Hani orada önemli bir noktaya değindiniz. Siber güvenlik ürünleri için de böyle ambargolar olabilir.



Celil Ünüver:

Aslında zaten katsayı yaptırımlarının detaylarına baktığınızda yani umarım böyle bir durumla karşılaşmayız ama katsayı yaptırımlarının içerisinde aslında siber güvenlik ürünleri de var. Yani sadece silah sanayi, savunma sanayi ürünlerine yaptırım değil bir ülkeye bu yaptırım uygulandığında onun içinde siber güvenlik ürünleri de dâhil edilebiliyor Amerika tarafından. Dolayısıyla gerçekten kritik bir önem arz ediyor kullandığımız bütün ürünlerin yerli bir muadilinin olabilmesi.

Doç. Dr. Bilgin Metin:

Çok teşekkür ediyoruz. Sizlere Siber Operasyon Merkezleriyle ilgili bir fizibilite projemiz olduğundan bahsetmiştim. Buradaki bizim proje paydaşlarımızdan birisi HAVELSAN. HAVELSAN da ülkemizdeki Siber Operasyon Merkezlerinden birisini kurdu. Biz de onlarla iş birliği yapmanın, bir sanayi – üniversite iş birliği yapmanın mutluluğunu yaşıyoruz. Özellikle ben şimdi HAVELSAN İş Geliştirme ve Satış Müdürü Sayın Ahmet Cengiz Güray'ı dinlemek istiyorum. Çünkü HAVELSAN'ın da çok sayıda yerli ve milli çözümleri var. Dolayısıyla bu alandaki ülkemizin en önemli oyuncularından bir tanesi.

Ahmet Cengiz Güray:

Teşekkür ederim Hocam. Öncelikle bu saatte bizi dinliyorlar, çok teşekkür ederim. Gerçekten siber güvenliğe gönül vermiş arkadaşlarımız, yöneticilerimiz sağ olsunlar. HAVELSAN adına tabii ki birçok uygulamamız var ama söze başlarken girdiğinizde ekosistem... Şöyle bakıyorum hepsi ekosistemimizde olan firmalar. Bu bize gurur veriyor. Ama bu gururu, burada görmüşsünüzdür beyaz tişörtlü bir sürü arkadaşım var, ben bunlarla yaşıyorum. Sağ olsun onlar iyi ki var ve biz bu gururu yaşayabiliyoruz, yöneticilerimiz var, o yüzden yaşıyoruz. Biz iyi bir eleman yetiştiren, ülkemize hizmet etmeye çalışan, ekosistemiyle sinerjik çalışmalar yapmaya çalışan bir hizmet sunmaya çalışıyoruz. Bunun içerisinde üniversitelerimiz de var. Sabahtan beri ben etkinliği izliyorum aslında. Tam bir hikâye gibi. Giriş var, gelişme var. Şimdi de sonuç. Girişte konuşmaların hepsi siber güvenliğin günümüzde, dünyada bakışı, tanımı, tanımlamasıyla ilgiliydi. Farkındalığı vardı. Daha sonra yöneticiler geldi, neler yaptıklarını anlattılar. Bunların arasında Türk yazılımlar, Türk çözümler de vardı, olmayan da vardı. Şimdi de onların nasıl yapacağını anlatan bir ekosistem grubuyuz. Biz belki HAVELSAN'ız ama onlar da bizim ayrılmaz parçalarımız. Biz çalışanlarımıza bu konuda eğitimle, destekle 7/24 Siber Operasyon Merkezimizde, ürünlerimizle hizmet etmeye çalışıyoruz. Ama dikkat ettiğimiz bir konu var; sevgili paydaşlarımızın girdiği konularda onların emeklerine saygı duyarak onlara destek olup onlarla birlikte çözümler üretmeye çalışıyoruz. Bu konuda da bütün ekosistemdeki firmalara açığız. Herkese eşit şekilde yaklaşıyoruz. Bize ürünlerini getirebilirler, çözümlerini getirebilirler. O beyaz yakalı arkadaşlarım bunları incelerler, gerekli olanlara biz gerekli desteği her zaman HAVELSAN olarak vermeye hazırız çünkü yöneticilerimiz de bize bu vizyonu veriyorlar.

Burada bazı notlar aldım, müsaadenizle. Tanımlamalar var. İşte diyoruz ki: savunma, saldırma, caydırma. Yapay zekâ, kuantum algoritması. Arkasından bu tespit, tepki ve iyileştirme. Yapay zekâ otonom sistemler. Ne mutlu ki biz bunların hepsini yapabiliyoruz. Bunların birçoğunu bizim paydaşlarımız, birçoğunu da arkadaşlarımızla yapıyoruz. Ama çözemediğimiz pek çok şey varmış, onu da öğrendim bu arada: kripto para. Bunun için de herhalde bir çalışma başlatırız yakın zamanda.

Burada bazı ürünlerimiz de var tabii ki. Bu ürünler zamanla yatırımla başlanmış, şu anda da sektörde değişik kamu kurumlarında, kuruluşlarında hizmet olarak veriyoruz. Bunların hizmetini verebilmek çok önemli çünkü Türkiye'de yabancı ürünlerin en büyük sıkıntısı aldıktan sonra başlıyor. Nasıl bunun hizmetini vereceksiniz? Bir güncelleme geldiği zaman buna ne kadar güvenebileceksiniz? HAVELSAN'ın aslında bu konuda çözümü çok kuvvetli diye düşünüyorum. İşte SIEM ürün ailemiz var, Katip, Gözcü ve Kahin. Bunların hepsi müşterinin nitelik, nicelik ve bütçesine göre konumlanabilir yerli ve milli yazılımlarımız. Arkasından Bariyerimiz var. Bir DLP ürünümüz. Son derece güzel, yerli veri sızma ürünümüz var. Kalkanımız var, web uygulama ürünümüz var. Aynı şekilde bir ASTARİZ var tamamen yapay zekâ, tamamen yerli ve milli; gururla söylüyoruz. Ve en önemlisi kriptolu iletişimimiz var, bir

telefonumuz var. Bunu da gün geçtikçe piyasalarda hızla duyacağınıza inanıyorum.

HAVELSAN gerçekten iyi bir yazılım evi, iyi bir paydaş, iyi bir ekosistem ortağı olduğunu düşünüyorum. Hem üniversite hem firmalar olarak. Çok teşekkür ederim.

Doç. Dr. Bilgin Metin:

Ben teşekkür ederim. Bizim bir önceki siber kampımızda HAVELSAN, sponsorlarımız arasındaydı. Gerçekten üniversitelere yapılan akrediteleri de destekliyorlar sektöre yetişmiş iş gücü katılması noktasında çok çaba sarf ediyorlar. Ben şimdi Bilge Siber Güvenlik Teknolojileri yöneticisi Burak Bey'i dinlemek isterim, bu konudaki değerli görüşlerini almak isterim.

Burak Çifter:

Siber güvenlikle savunma hatta diplomasi iç içe geçmiş durumdadır. Yerlileşmedeki ihtiyacımız teknik veya taktiksel taarruz gibi veya savunma gibi taktiksel seviyeden çıkmış ve stratejik bir hal almış durumda. Çünkü bazı diplomatik gerginliklerde dahi yaşadık biz bunu geçmiş yıllarda hatırlarsınız hepiniz. Diplomatik bazı gerginliklerde karşıdakine verdiğiniz cevaplar belli bir düzeye kadar sözlü cevaplar. Bir üzerine çıktığınızda başka seviyede yani elinizde ne kadar kozunuz varsa o kadar elinizi güçlendirip ve ne gerginliği istiyorsanız yükseltip istiyorsanız da karşı tarafın cevap verememesi adına bir caydırıcı olarak kullanıyorsunuz. Artık siber saldırılar da diplomatik gerginliklerin çatışmaya kadar vardığı noktayı düşünürsek eğer aradaki kademelerden bir kaçı haline gelmeye başladı. Gerginlikler belirli bir seviyeye geliyor belki bir çatışmaya dönmeden önce sözlü münakaşalardan sonra artık ülkeler arası öncelikli tırnak içerisinde "devletlerin kesinlikle desteklemediği" bir şey de olsa işte hacker grupları arasında bazı savaşlar, daha sonrasında devlet sitelerine belki kamu hizmetlerine yönelik bazı saldırılar gibi devam ediyor, başlıyor. Haliyle yerli çözüm ihtiyacımız bizim kendimizi savunmamız gereken devletlerden aldığımız güvenlik çözümlerinin bağımlılığını ortadan kaldıracak. Yani bugün X bir ülkeden aldığımız elbette ki bizi bu ülkeye karşı korumayacak ve onunla yaşadığımız bir gerginlikte ciddi bir yaptırım da bunun içerisinde olabilir, bu ürünleri artık tedarik edememek veya o üründen mevcut olarak elimizde veya sistemlerimizde kullanmışsak karşılıklı bir çıkar çatışması durumunda bizim aleyhimize kullanılacak bir hale de gelebilir.

Ben yerli ürünlere yönelik desteklerin aslında artık sadece yerliyse alalımdan ziyade "yerlisine olmasına ihtiyacımız var ve bu bizim için bir parasal veya sadece millilik duygusuyla hareket ettiğimiz bir motivasyonla ilerlediğimiz bir şey değil stratejik olarak bağımsız, kendi kararlarını verebilen bir devlet olabilmenin gerekliliğiyle beraber gelen bir durum. Kendi kararlarımızı verdiğimiz anda çıkar çatışması sonucunda eğer belirli ürünleri tedarik edemiyorsanız, belli teknolojilerden mahrum kalıyorsanız veya bunlar size -çok özür diliyorum- nimet gibi sunulup böyle çok özel izinlerle size takdim edilebiliyorsa ve bunun karşılığında bazı tavizler vermek durumunda kalıyorsanız hatta ve hatta bunun sonucunda dahi aslında parasını vererek ve belli tavizler vererek o ürünü aldığınız ülkenin yani o menşein karşı kendi sistemlerinizi savunmasız halde bırakıyorsanız bu konunun hiçbir anlamı yok. Kendi kararlarınızı veremeyecek durumdasınız demek ve onlar için işte ilk sunumlarda da vardı, Sayın Komutanım sanırım arz etmişti, savaşın en güzel olanı hiçbir cebir ve güç kullanmadan karşı tarafın yapmamasını istediğiniz şeyi yapmasını engellemek. Yani sizin istediğiniz noktaya gelmesini sağlamak. Bu durumda tabii siber güvenlikle siber savunma aşırı diyebileceğimiz şekilde iç içe geçti. Hâlihazırda ağ merkezli savaş dediğimiz, ağ tabanlı savunma veya savaş sistemleri artık çok yaygın olarak kullanılıyor. Günümüzde bile farklı ülkelerle teknoloji transferi veya yeni ürünler almamızdaki en büyük sorunlar olarak bu gösteriliyor çünkü networkleri nasıl birbirinin içerisine geçireceğiz veya NATO uyumlu mu veya değil mi veya güvenlik standartlarına uyumlu mu değil mi gibi kaygılar ortaya çıkıyor. Bu sebeple kendimize ait, kendimize özel çözümlerimizin olması artık "olsun, çok iyi olur, olmasına ihtiyacımız var"dan ziyade olmazsa olmaz noktasında. Bu artık bağımsızlığın bir gereği olmuş durumda.

Bununla beraber tabii sertifikasyonlar çok önemli. Biz her ne kadar yerli ürünler geliştiren üreticiler olsak da hala aslında sertifikasyon mercileri temel olarak, TSE burada olsa da uluslararası bir sertifikasyon standartı uyguluyoruz. Onların gerekliliklerini uyguluyoruz. Ve onlardan sadece onay almış ve onlardan akredite olan sertifikalarla piyasaya çıkabiliyoruz. En büyük örneklerinden birisi işte ortak kriterler gibi, işte bunun gibi aslında Türkiye'de çok da fazla yerli üreticiler tarafından çok rağbet görmüyor. Belki zorluğundan dolayı, belki hitap ettiği pazarın bunun çok gerektirmemesinden dolayı olan sertifikasyon süreçleri var. Aslında belki TRtest de aramızda olsaydı çok güzel olurdu, burada da görüyorum onların olmadığını. Bu konuda da güzel bir girişim başlatıldı bildiğim kadarıyla SSB tarafından. TRtest diye bir sertifikasyon amacıyla yerli bir şirket de kuruldu. Belki buranın birazcık daha aktif hale gelmesi, çok hızlı bir biçimde faal hale gelmesi bu ekosistemde, HAVELSAN da dâhil olmak üzere, siber küme de dâhil olmak üzere. Bu tarafta daha etkin bir çalışma aslında son kullanıcıları ve kurumları da daha rahat ettirecek. Bugün TSK'ya bir ürün götürdüğümüzde mutlaka şunu sormak durumunda kalıyor: Sertifikaları var mı, TÜBİTAK tarafından güvenlik kontrolleri yapıldı mı, güvenlikle ilgili sertifikasyon onayları tamam mı? Hâlbuki yerli ürünlerle ilgili bunlar ya tek elde toplanmalı ya kolaylaştırılmalı ya da yerli bir

güvenlik standartlarının belli güvenlik seviyelerine kadar, hizmete özel, gizli, çok gizli seviyelerine kadar artık bunlar nasıl düzenleniyorsa, her kademe için belki farklı güvenlik standartlarının milli bir sertifikasyon çatısı altına toplanarak ilerletilmelidir. Ben zannediyorum ki yerli ürünlerin hem kendilerinin olgunlaşması "hem de ürün yaptık, bitti; şimdi ne yapacağız?" değil de bir hedef koyarak "biz bir ürün yapacağız ve şu standartlara göre yapmak zorundayız" diye kendilerini bilgilendirmesi ve bu ürünlerin yaşaması ve ticari bir değere dönüşmesi lazım. Bunun için de müşteri desteğine ihtiyacımız var. Bunu sağlamak adına da bu sertifikasyonlara sahip ürünler kurumlar tarafından daha güvenilir addedilecektir, bunu sağlayacaktır. Belki bu taraftan da birazcık daha çalışmaların hızlanması ve sonuç elde edilmesi hepimiz adına faydalı olur. Biz bu desteği sağ olsun çoğunlukla HAVELSAN'dan aldık. Ürünlerimizin denetimini de, ürünlerimizin testlerini de, gerçek ortam testleri dahil, HAVELSAN'ın ekibi gerçekleştirdi ve bize eksikliklerimizi veya yol haritamızla ilgili desteklerini sundular. Bunun için de tekrar teşekkür ediyorum zaten. Ama böyle bir açık olduğunu aslında görmüş oluyorum.

Doç. Dr. Bilgin Metin:

Çok teşekkür ediyoruz. Şimdi Atar Labs. kurucusu Burak Dayıoğlu'na söz vermek istiyorum. Onun da özellikle siber operasyon merkezi gibi çok sıcak bir alanda güzel bir ürünü var. Hocam siz nasıl değerlendirirsiniz operasyon merkezlerinin durumunu?

Burak Dayıoğlu:

Öncelikle etkinliğe ev sahipliği için BTK ve HAVELSAN'a çok teşekkür ediyoruz. Şimdi izin verirseniz önce geniş perspektiften alıp Celil Bey'in başladığı gibi siber güvenlikte yerli-milliyi nasıl görüyoruz, ondan başlayayım. Sonra da Atar'da biz ne yapıyoruz, hangi problemi nasıl çözmeye çalışıyoruz, bunun Türkiye için nasıl bir anlamı vardır, yerli üreticiler bugün ne tür güçlükler yaşıyor, bunlardan söz edeceğim.

Siber güvenlikte yerli-milli diyoruz ama bence bu bir tekno-milliyetçilik konusu. Yani her türlü teknolojinin Türkiye'de üretildiği bir zemine doğru ilerlemeye ihtiyacımız var. Bir şeyleri biz üretmediğimiz sürece o teknolojinin kimin tarafından ne zaman, nasıl kullanılacağını bilmiyoruz. Az önce size ne örnek vereceğimi düşünürken trafik lambalarını yöneten sistemi de yurt dışından aldığınızda da aynı riskiniz var. Birileri ülkeler arasında bir problem çıktığında o lambaların başka şekilde uzaktan çalışmasını kumanda ediyor olabilir. Hastanedeki MR cihazı için de aynı şey geçerli. MR'larınız başka çıkıyor olabilir ya da size ışın tedavisi veren cihaz vermesi gereken dozun üzerinde, çok üzerinde doz veriyor olabilir. Dolayısıyla hani konumuz aslında sadece siber güvenliği millileştirme yerlileştirmek değil ama şüphesiz ki şemsiyesi altında bulunduğumuz etkinlik itibariyle biz onu siber güvenlikle ilgili bakış açısına bakıyoruz. Ben aynı zamanda İnnovera'nın da kurucusuyum. Türkiye'deki en büyük güvenlik entegratörü firmalardan bir tanesiyiz. Gözlemlediğimiz bir tane problem var; biz her birimiz farklı marka güvenlik ürünü alıyoruz ama o güvenlik ürünlerimiz birbiriyle konuşmuyor. Yakup Başkan da söz etmişti o ürünleri bir arada çalıştırmak için çok insana ihtiyacımız var. Bilgin Hocamların düzenlediği gibi yaz kamplarına, bir sürü farklı kuruluş düzenliyor ve fakat yetiştirdiğimiz insan adedi beklentinin çok altında kalıyor ve biz hiçbir zaman beklentiyi karşılayacak bir yere doğru gitmiyoruz. Yani gayretimiz insan kaynağı açısından mümkün olduğunca açığı kapatalım ama tamamen kapatmak mümkün olmayacak gibi görünüyor. Biz de bunun üstüne 2017'nin Eylül'ünde Atar Laboratuvarlarını kurduk, orada otomatik tehdit analizi ve yanıt verme, adını ATAR koyduğumuz teknolojiyi geliştiriyoruz. Hâlihazırda 115 - 116 güvenlik programını bir araya getiren, bunları konuşturan, bunlara merkezi komuta kontrol sağlayan bir imkân sağlıyoruz. Saldırıların çok fazla olmasıyla mücadele edeyim diyorsunuz; günde 500 – 600 saldırı alarmı alıyorsanız hangisine bakacaksınız diye soruyoruz, hiçbirine bakamıyoruz diyorsunuz. Biz bunlara bakabilir hale gelmenizi sağlıyoruz.

Saldırılar çok hızlandı. Zararlı yazılımı bir koyuyorsunuz ağın ortasına, on dakika içerisinde yapacağının hepsini yapıyor. On dakikada ben ekranda yanıp sönen bir şeyleri bile görmüyorum. Oralarda hem saldırı hızı hem saldırıların hacmiyle mücadele etmeye katkı sağlayan, az adamla çok iş yapmaya imkân sağlayan bir teknoloji kümemiz var. 50 kişilik, farklı yetkinlikleri olan bir askeri kitleyi bir araya getirdiğinizde ilk yapacağınız şey bir komuta kontrol hiyerarşisi kurmaktır. Bu 50 kişiyi nasıl komuta kontrol edeceğiz, kimin ne zaman, neyi yapacağını, nerede yapacağını nasıl belirleyeceğiz. Biz siber savunma için komuta kontrol altyapısı geliştiriyoruz özetle. O komuta kontrol altyapısı az sayıda uzmanın daha etkin çalışmasını sağlıyor. Bilgin Hocamın da söz ettiği gibi uluslararası iş birlikleri niteliğinde pazara gitmeye çalışıyoruz. Kendi başınıza gidebileceğiniz yer son derece limitli oluyor.

Bugün uluslararasına çıkmış olan Celil Beylerin şirketi, bu tarafta, Kron'un saha durumundan göreceğiniz gibi, Türkiye'de, biz yurtdışından daha zor projeler gerçekleştiriyoruz. Yurtdışı işlerimiz hepimiz açısından çok daha hızlı gidiyor.

Bir başka temel zorlandığımız nokta da özellikle İsraillilere çok imreniyorum. İsrail'den niye çok güvenlik firması çıkıyor diyoruz, firmayı İsrail'de kurmuş olsaydım ilk gittiğim kamu kuruluşlarından 8-10 tanesi ürünlerin liste fiyatından hemen ürün almaya razı oluyorlar çünkü ilk bir ayağa kalkması lazım firmanın, işte bir gelir elde edebildiğini birilerine

göstermesi lazım ki onu Amerika'ya taşısınlar, Avrupa'ya taşısınlar. Bizde hepimiz açısından tam tersi oluyor. Eyüp bugünlerde birebir aynısını yaşıyordur. Atıyorum hani 100 bin dolarlık bir teknoloji diye götürüyoruz, "Eyüp'çüğüm sen bana bunu ücretsiz ver, bak ben sana referans müşteri olacağım"larla kamu kuruluşları bize gelmeye çalışıyor. Halbuki ne bileyim Turkcell'in, TürkTelekom'un referansından daha önemlisi bankaların, savunma sanayisinin referanslar açısından. Bunları anlatmakta çok zorlanıyoruz. Liste fiyatlarından falan almalarını beklemiyoruz kamu kuruluşlarının ama % 99 indirim yaptığımız, hibe ettiğimiz, hediye ettiğimiz yerler de bizim şirket olarak ayağa kalkmamızı, uluslararasına çıkarken yatırımcı aradığımızda, Angel şirketlerin masasına oturmamıza ciddi şekilde engel oluyor. Oraları biraz iyileştiremediğimiz durumda buradan bugün çıkarttığımızı düşündüğümüz şirketlerin de uzun soluklu olamadığını göreceğimizden endişeliyim. Ve bu endişeyle de bu turu kapatayım ben. Teşekkür ederim.

Doç. Dr. Bilgin Metin:

Teşekkür ediyorum ben de. Şimdi burada sözü Kron firmasından Özdemir Bey'e vermek istiyorum. Sizin de değerli görüşünüzü almak isteriz.

Özdemir Şarman:

Teşekkür ederim. Öncelikle bize ev sahipliği yapan ve bu panele katılan tüm katılımcılara teşekkür ediyorum değerli zamanlarınızı ayırdığınız için. Ben önce Kron kimdir, bundan çok kısaca bahsetmek istiyorum ve bu kuruluşumuz olan 2007 senesinden bu yana bugünlere gelene kadar yaşadığımız yolda, nerelere geldiğimizi, neler yaşadığımızı çok kısaca anlatıp sonrasında da bugün tüm panelistlerin aktardığı işte doğrulama nedir, kimlik doğrulama nedir, yeni güvenlik tehditleri, zamanla değişen güvenlik tehditleri ve biz bunlarla nasıl başa çıkacağız, değişen saldırı vektörleri nedir, bunlarla nasıl baş edebiliriz? Bu konularda da bazı bilgiler paylaşmak istiyorum.

Kron, 2007 senesinde kurulan, tamamıyla %100 yerli ve milli bir Türk şirketi. Telekom operatörleri ve servis sağlayıcılarının yazılım ve donanımsal isteklerini ve ihtiyaçlarını hem yurtiçinde hem de yurtdışında karşılıyoruz. Bütün panelistler, katılımcılar, yerli ve milli üreticiler bir takım yaşadığımız zorluklardan bahsettiler. Doğru. Hepimiz bir takım zorluklar yaşıyoruz. Biraz önce çok güzel bir şey söylediniz. Bir satış ağının oluşması çok önemli ve diğer yabancı üreticilerin bu kadar yaygın olmalarının asıl nedeni ürünlerinin bizim ürünlerimizden daha iyi olmaları değil, daha çok tanınmaları ve satış pazarlama ağlarında daha aktif olmaları, daha çok bilinmeleri. Belki de Türk üreticilerinin en büyük problemi pazarlama konusunda olan eksikliğidir. Ben bunu kendi adımıza da söylüyorum. Evet, çok ciddi bir yol aldık, çok ciddi referanslarımız var ama bugün baktığınız zaman CISCO'nun pazarlama ağı çok daha etkin çalışır. Bu bir yolculuk, bu bir süreç. Ama biz bunu ülkece öğreniyoruz, yerli yazılımcılar olarak, Türk üreticiler olarak ve öğrendiğimiz noktada çok efektif sonuçlar elde edebiliyoruz. Zaten ürünlerimiz kalite anlamında yurtdışındaki ürünlerle çok rahatlıkla rekabet edebiliyor. Hatta geliştirdiğimiz pek çok ürünle özellikle yabancı üreticilerin ürünlerini geride bırakabiliyoruz. Çok daha etkili özellikler geliştirebiliyoruz fakat bugün konuşan bütün panelistlerin üzerinde durduğu ortak bir nokta vardı; güvenlik kalıcı bir durum değildir. Değişken bir durumdur ve genellikle de bozulma eğilimindedir; yani güvenli diye bir şey yoktur; sadece güvenli bir an olabilir. Ve bu genellikle de hep bozulma eğilimine girer. Bunu – işte biraz önce Burak Bey de bahsetti – bir saldırı geldiği zaman 10 dakika içerisinde ekranı göremezsiniz, farkına bile varamayabilirsiniz. İşte biraz önceki öğretim görevlimiz dedi ki çok basit yöntemlerle insanların parolalarını almak mümkün ve bu parolaları alarak istediğiniz işlemleri yapabiliyorsunuz. Bunların hepsi doğru ve gerçek. Burada önemli olan noktaların birincisi farkındalık. Farkındalık güvenliğin belki de ilk temel ilkesi. İkincisi ise entegrasyon. Günümüzde hiçbir ürün tek başına bir güvenliği uçtan uca sağlayamaz. Sadece diğer ürünlerle ne kadar entegre olabilirse ve ne kadar beraber konuşabilirse o denli size güvenliği vadedebilir ama yine de hiçbir ürün ya da hiçbir ürün kümesi tamamıyla, %100 bir güvenlik sunamaz. Sadece sizin hayatınızı kolaylaştırır ve yapabileceği en yüksek farkındalığı oluşturmaya çalışır. Şimdi burada bir güvenlikten bahsedebilmek için belki de ilk önemli olan konu doğrulama. Yani bir şeyi yetkilendirmeden önce onun ne olduğunu doğrulamanız gerekiyor. Doğrulama eskiden sadece sistemlerdeki yetkili kullanıcılarla gösterilirken, ölçeklenirken artık günümüzde sadece kullanıcıların parolaları yeterli olmuyor. Neden? Çünkü artık sadece bilgi teknoloji ağlarında çalışan bizim gibi insanlar değil artık akıllı şehirlerden bahsediyoruz. Nesnelerin internetinden bahsediyoruz. Birbirleriyle konuşan nesnelerin internetinden bahsediyoruz; yani insan öğesi dışında da aslında doğrulama ihtiyacı olan ve bizim yabancı olduğumuz pek çok sistem bulunuyor. İşte diğer panelistler trafik lambalarından, işte SCADA sistemlerinden, enerji sistemlerinden bahsettiler. Bunların hepsi yine bir doğrulama ve yetkilendirme içeren sistemler. Fakat doğrulamada sizin bir parolanızı çaldırmanız ya da bir uygulamanın parolasının ele geçirilmesi günümüzde son derece kolay bir işlem. Burada diğer katılımcıların da aktardığı gibi çoklu kimlik doğrulama, biyometrik doğrulama yaptığınız zaman süreci evet kısmen bir parça daha esasında zorlaştırıyorsunuz. Ama bu yine tamamıyla, %100 bir çözüm size sağlamıyor. Burada doğrulama faktörlerinin artırılması gerekiyor.

Biz Kron olarak çok katmanlı kimlik doğrulamayla ilgili çok ciddi çalışmalar yaptık ve single connect diye bir ürün ailemiz var. Bu ürün ailesi içerisinde doğrulama, parola kasaları, yetkili kullanıcı oturum yönetimi,

network doğrulama Triple Play ürünleri yani Tacacs'lar ve Radius'lar, KVKK ve GDPR'a istinaden veri tabanı erişimlerinin yönetilmesi, maskelenmesi ya da hassas verilerin keşfi gibi ürünleri içeren bir veri tabanı, erişim yönetim katman ailesi ve bu robotik proses otomasyonu da sağlayan bir yetkili ürün ailemiz var. Fakat en önemli nokta bütün kullanılan uygulamaların, ister bir SIEM uygulaması olsun, ister bir Endpoint ister bir DLP; güvenlikte kullandığınız uygulamalar birbirleriyle doğru şekilde konuşmuyorlarsa orada sizin bir konudan anında haberdar olmanız, onunla ilgili doğru aksiyonu hızlı bir şekilde alabilmeniz mümkün değil.

Biz siber küme mensubu olan yerli üreticiler olarak öncelikle kendi aramızdaki iletişimleri oldukça artırdık ve birbirimizle konuşabileceğimiz entegrasyonlar yapmaya önem gösteriyoruz, önem veriyoruz. Çünkü ne kadar ürünlerimiz ve çözümlerimiz birbirleriyle konuşabilirse aslında size o kadar daha yüksek oranda bir güvenlik sağlamış oluyoruz. Fakat güvenliği sağlamakla sadece konu bitmiyor çünkü güvenlik doğrulamasını yaptıktan sonra artık atak vektörlerinin sadece dışarıdan değil aynı zamanda içeriden de gelebileceğini pek çok örnekten gördük. Biliyorsunuz önceki yıllarda bankalarda swift işlemlerinde çeşitli güvenlik açıkları oluştu ve hem Türkiye'den hem de yurtdışından bazı bankalarda ciddi parasal ve finansal kayıplar yaşandı. Biz bu konuda bankalarda, çoklu kimlik doğrulamada ürettiğimiz ürünlerle kendilerine bir çözüm sağladık ama sadece finans sektörüne has bir durum değildi. Bu enerji şirketlerinde de yaşanıyordu, büyük holdinglerde de yaşanıyordu, kamu kurumlarında da, üniversitelerde de yaşanıyordu. Belki burada yerli ve milli üretici olmanın en önemli noktası beyin göçünü ki bence ülkemizde en önemli problemlerden biridir beyin göçü, bunu engellemek. Çünkü bizim amacımız, siber küme üyesi bütün şirketlerin amacı, bu oluşmaların amacı beyin göçünü de engellemek ve tersine bir beyin göçünü gerçekleştirmek. Ülkemizde siber güvenlik anlamında yetişen insan sayısı bizim ihtiyaçlarımızı karşılamaktan uzak. Ve biz ne kadar bu değerli iç kaynaklarımızı kendi içimizde tutabilirsek esasında ülke olarak da o kadar başarılı bir ülke olacağız ve sadece tüketen değil aynı zamanda da kendi ihtiyaçlarını üreten ve yurtdışına satabilen bir konuma geleceğiz.

Burada desteklerini gösteren hem kamu kuruluşlarına hem özel sektördeki tüm kişilere bize olan güvenleri için çok teşekkür ediyorum. Güvenlik bir yolculuk, bir süreç. Bu süreçte sürekli olarak geliştirme yapmak zorundasınız çünkü sürekli değişiyor. Bundan dolayı hepimizin gelişime açık olması ve farkındalığımızı da çok yüksek tutması, aralıksız araştırması ve kendimizi de geliştirmesi gerekiyor. Ve biz bu açıdan tüm katılımcılara ve bu kümelenmede yer alan bütün herkese de çok teşekkür ediyoruz. Benim şu an için aktarmak istediklerim bunlar.

Doç. Dr. Bilgin Metin:

Çok teşekkürler. Ben en son, sözü Eyüp Bey'e vermek istiyorum. Sizin de değerli düşüncelerinizi alalım lütfen.

Eyüp Çelik:

Öncelikle bugünkü organizasyonda emeği geçen herkese ve dinleyenlere teşekkür ediyorum. Güzel bir etkinlik olmuş. Herkes siber saldırılardan, siber savaşlardan, zararlı yazılımlardan çok çok bahsettiği için aynı şeyleri tekrarlamak istemiyorum. Şöyle bir noktadan bakıyorum; biz yerli ve milli yazılımlar, yerli ve milli ürünler üzerine konuşuyoruz. Bunları sadece Türkiye'de tutup yerli ve millilik kavramını sadece Türkiye'de yerleştirmenin çok doğru bir yaklaşım olmadığını düşünüyorum. Artık ürettiğimiz yerli ve milli ürünlerin globalleşmesi taraftarıyım, geliştirdiğimiz ürünleri de bunu baz alarak geliştirdik. Dolaysısıyla biz Türkiye'de bir şeyler üretip, ürettiğimiz şeyi dünyadaki diğer büyük üreticilerin yaptığı aynı pazarlama taktikleri kullanarak diğer ülkelere yayılmayı hedefledik ve ana stratejimizi bunun üzerine kurduk. Bunun meyvelerini de yemeye başladık. Birçok ülkeye satış yapmaya başladık.

Şimdi burada temel sorunlardan biri şu; biz siber savaşları çok konuşuyoruz, yıllardır konuşuyoruz ama siber savaşlarda en büyük problem sizin savaşacak elemanınız ne kadar var? Bu soru bizim için çok önemli bir noktaya geliyor. Eğer savaşacağınız ülkenin teknik personel sayısı, kalifiye eleman sayısı sizin ülkenizden çok fazlaysa yeteri kadar mücadele veremeyeceksiniz. Bu da başlı başına bir problem yaratıyor dolayısıyla bizim gözlemlediğimiz -uzun yıllardır sektörü ve üniversiteleri gözlemliyoruz- birçok Hocamın da düzenlediği, işte Boğaziçi Üniversitesi'nde düzenlediği birçok benzer etkinlik de biz de rol alıyoruz, uzmanlarımızı gönderiyoruz, kalifiye eleman yetiştirmek için elimizden geleni yapıyoruz. Ama bu noktada bizim bu mücadeleyi sadece bir kampla kazanamayacağımızı anladıktan sonra öbür tarafta bir yenilik getirme ihtiyacı duyduk ve bunu Priviahub isimli bir ürünümüzle yapmaya başladık. Dünyada iki tane rakibimizin bulunduğu cyber range platform geliştirdik. İşte herkesin girip üye olabildiği, hem kurumsal bacağının olduğu hem de herkese açık versiyonunun olduğu bir platform geliştirdik. Bu platformun üzerinde yaklaşık 130'un üzerinde makine var ve bu makinalar gerçek dünyanın benzer senaryoları ile oluşturuldu. İşte içerisinde SCADA senaryoları, bankaların bankacılık senaryoları, swift sistemler veya APT gruplarının tekniklerini kullanarak sızmaya olanak veren sistemler var. Kullanıcılar burada, bu sistemler üzerinde hem teknik bilgi ve pratiklerini geliştirebiliyorlar, mesleki dezenformasyonu engelliyoruz ve hızlı öğrenmeyi sağlıyoruz. Aynı zamanda biz kullanıcıların hangi

kategorilerde, hangi alanlarda ne kadar ilerleyebildiğini ölçümleyip, raporlayıp, ona doğru eğitimi verecek platformu geliştirdik. Bu platformla birlikte biz bütün siber güvenlik tarafında çalışan; ofansif, defansif adli analiz ve benzeri alanlarda çalışan bütün ekipleri bu platform üzerinde hem pratik yapabilmelerine olanak veriyoruz hem de eksik oldukları taraflarını tamamlamalarına olanak verdiğimiz bir platform olarak hayata geçirdik ve birçok ülkenin savunma bakanlığına da bu ürünlerimizi satmaya başladık. Onlar da kendi ülkelerindeki adamlarını yetiştirmek için bu tarafta bizden destek alıyorlar.

Burada bizim için önemli olan noktadan yola çıkarak bir savaşı sadece bir zararlı yazılım ya da başka bir şeye indirgemek yerine kalifiye personel, işi bilen, teknik anlamda ve pratikte işi bilen ve yapabilen insanlar yetiştirmeye çalışıyoruz.

Biz aynı zamanda iki tane ürün geliştirdik. Bir diğer geliştirdiğimiz ürünümüz de Avcı isminde. Bu da Burak Hocamların yaptığı orkestrasyonun bir benzerini yapıyor ama o yaptığı orkestrasyonu siber güvenlik tarafında kullanılan offense ürünlere yönelik gerçekleştiriyoruz. Dünyada yaklaşık 35 tane üreticinin merkezi bir yerde yönetilmesini ve burada çıkan zafiyetleri geçmişe dönük bakıp kontrol edebileceğimiz yeni bir mekanizma geliştirdik. Böylece bir kurumun zafiyetinin yıl içerisinde hangi tarafa yükseldiğini ya da risklerinin artıp, düştüğünü ölçümleyebiliyoruz. Aynı zamanda biz bunu sektörel olarak da kurumlar bize bilgi göndermeye, onay verdiklerinde; ürün üzerinden bilgi gönderdiklerinde, onay verdiklerinde ülke bazında ve sektör bazında raporlar oluşturabiliyoruz. İşte bankacılık sektöründe en çok karşılaşılan güvenlik açıklıkları nelerdir, bir açıklıkla karşılaştıktan sonra onun giderilme yöntemleri, giderilme süreleri, reaksiyon süreleri gibi birtakım raporları hem ülke seviyesinde hem de sektör seviyesinde oluşturup, düzenli olarak bu raporlarımızı müşterilerimize gönderebildiğimiz bir yapı kurduk. Teşekkür ediyorum.

Doç. Dr. Bilgin Metin:

Özellikle Bilgi ve Teknoloji Kurumu'na, HAVELSAN'a bu organizasyonu düzenledikleri için teşekkür ediyorum. Ve her şeyden önce sizlere teşekkür ediyorum, bu saat oldu hala bizleri dinliyorsunuz.


elil UNUVER
rapmine Siber Güvenlik
eknolojileri
Burak DAYIOĞLU
Atar Labs
Özdemir ŞARMAN
Kron
Hüseyin Alp ONAT
Ekon Bilişim

BERKE ÇAPLI

NATO Bilim ve Teknoloji Organizasyonu Araştırma Komitesi Başkanı

SİBER GÜÇ DESTEKLİ ÇOK KATMANLI HARP

Çok katmanlı harpten bahsedeceğim size bugün. Aslında ilk önce fark ettiğim bir unsuru söylemek istiyorum, o da başlığımız siber savaş ama çok fazla siber savunma konuştuk. Siber saldırı hakkında bir şey söylemiyoruz çünkü söyleyemeyiz, çünkü yasalarda karşılığı yok.

5. Katman'ı ben biraz açmak istiyorum. NATO için 5. Katman sadece siber uzayla sınırlı. Almanya daha çok yeni doktrinlerini değiştirdi ve buna elektromanyetik spektrum ve bilgi ortamı dedi. Bilgi ortamı dediğimiz ne; halkın kafasının içi diye adlandıralım. Oraya doğru genişlemeye başladılar. Peki, Rusya'ya baktığımızda onlar ne anlıyor? Bütün bunun adına stratejik katman deyip tüm bilgi uzayını dâhil ediyor ve olayı harbin dışında barış dönemine de dahil ediyor. Yani olayı politik bir savaşa çekiyor.

Peki, çok katmanlı harp ne? Bu beş katmanı da eş zamanlı tek bir etki için kullanmak anlamına geliyor. Bir örneğine bakalım Ukrayna'dan, bir kente zırhlı araçlar girecek. Gerçek bir olay bu. Polislerin sokağa çıkıp engel teşkil etmelerini istemiyorlar. Ne yapıyorlar, siberden polislerin telefonlarını ve isimlerini çalıyorlar veri tabanından. Arkasından GSM kulelerini kullanarak bütün o telefonlara mesaj

gönderiyorlar. “Yarın sokağa çıkma, çıkmazsan hiçbir şey olmayacak.” Bu kısmı ne, psikolojik harp. Ertesi gün de fiziksel etki yani kinetik etki dediğimiz oluyor ve zırhlı araçlar kente gidiyor. Polisler sokağa çıkıyor mu, hayır. İşte çok katmanlı harp bütün katmanların tek bir etki için kullanılması böyle bir şey.

Bir diğer örnek Suriye’den, ünlü bir gazeteci, savaş gazetecisi bölgeden sürekli haber yapıyor, katliamları gösteriyor. Bilgi ortamını kirletiyor mu bu kişi, saldırganların gözünden, evet. Ortadan kaldırılması gerekiyor, nasıl kaldırıyorlar? Her gün uydu telefonu ile bağlanıp haber yaptıklarını biliyorlar mı, biliyorlar. Uydu telefonu sinyalini buluyorlar ve o sinyali hedefleme olarak kullanıp füze saldırısı yapıyorlar ve gazeteciyi öldürüyorlar. Bu kişi bir sivil. Yani politik harp dediğimiz nokta tam burada devreye giriyor.

20.000 tane veri inceledik Suriye ile ilgili, bütün harbi modellemeye çalıştık ve siber bilgi harbi olaylarını da grupladık. Siber ve bilgi olaylarını, birden fazla olayın aynı anda olduğunu, sivil yardım örgütlerinin kaçırıldığını ve öldürüldüğünü görüyoruz. Siber harbin ve bilgi harbinin denk geldiğini görüyoruz. Önemli bir soru, “bütün mantığımız birlikteliği korumaya yönelikken sivilleri kim koruyacak operasyon yaparken?”

NATO’nun yeni kavramı Meskûn Mahal Harbi ile ilgili geliştirdikleri kavram, şu anda ülkeler arasında dolaşıyorlar. Ne diyor bize; 2035’e doğru dünya nüfusunun %62’si meskûn mahalde yaşayacak. Çarpık kentleşme ve güçsüz yönetimden dolayı buraları tehdit noktaları olacak ve bu tehditler ilerleyip uluslararası tehditler haline gelecekler. Venezuela bunlardan bir tanesine örnek. Olduğu anda, ne diyor: %62’si meskûn mahalde yaşıyorsa burada ne demeye getiriyorlar, meskûn mahallerde savaşacağız diyorlar. Ve şu soruyu soruyor, 10 milyonluk bir nüfusta %1’i sizi sevmese nasıl kontrol altına alacaksınız?

Gelecek savaştan bahseden çok güzel iki kitap; bir tanesi Afganistan’ı örnek alıyor, bir diğeri de Bosna Hersek’i örnek alıyor. Ne söylüyorlar bize? Kuvvet çarpanı olarak şehir. Kuvvet çarpanı nedir, çok askeri bir terim. Nedir, klasik mantık, saldıran üç olması gerekiyor, 3K olması gerekiyor, savunma 1K ise. 1K savunan ne yapıyor, şehri çarpan olarak kullanıyor, kendi gücünü artırıyor. Diyor ki mesela Out of the Mountains kitabında, Mumbai terörist saldırısında, teröristler önce trafiği kullandı. Trafiğe istedikleri şekilde yön verdi polislerin ulaşmasını engelleyecek şekilde, ondan sonra terör saldırısını gerçekleştirdiler. Sonra soruyor, “Brezilya’daki gecekondu mahalleleri, Jamaika’daki garnizon toplumlar” diyor çünkü oraya kimse giremiyor. “Buraları nasıl kontrol edeceğiz?” diyor. Ve arkasından şu soruyu söylüyor. Diyor ki “Sen artık tepeyi de ele geçirdin ve askeri hedefler kalmadı.” diyor. Normatif sistemler diye bir kelime kullanıyor, bu nedir insanların kafalarında geliştirdikleri sistem. Mesela adalet algısı. Afganistan’dan bir örnek veriyor. Amerika geldi diyor, adalet nedir, mahkemeler olacak, bağımsız yargı sistemi, nerede, şehir merkezinde. Köy nerede, şehir merkezine 100 km ötede. Gece ne yapıyor, gece olunca Taliban geliyor, kendi yargı sistemiyle sorunu çözüyor ve gidiyor. Halk neye bakar, halk sorunun çözümüne bakar. Diyor ki o zaman bizim bunu normatif sistemler üzerinden rekabetçi kontrol ile bunları kontrol etmeye çalışacağız diyor. Askeri hiçbir şey söylemiyor. İnsan, bilişsel kısmından bahsediyor sadece gelecek harbi için.

Diğeri de General Rupert Smith, bir İngiliz generali, Bosna’da şunu söylüyor, diyor ki; biz oraya bir kuvvet gönderdik hiçbir kullanma niyeti olmadan. Gönderdiğin kuvveti nasıl kullanman gerektiği sorusunu soruyor ve şununla bitiriyor aslında “Savaş artık yok!”, “Savaş bitti” demiyor. Endüstriyel savaş bitti diyor. Artık patates tarlalarında, kentlerden uzak tankların tanklarla çarpıştığı bir savaş modeli yok diyor. İnsanların içinde savaşacağız diyor.

Peki, bu siber için ne demek? Bir; sosyal medya analizi birkaç defa geçti buradan. Niye bu PRIZMA izinleri verildi, niye bu veriler toplanıyor çünkü bu ordular, bu kuvvetler insan kafasını anlamaya çalışıyor. Çünkü geleceğin böyle olacağını biliyorlar. Veya bir şehrin içerisindeki dijital sistemler karşı tarafın bunu güç olarak kullanmasına engelleyebilecek hale geliyor.

General Michel Yakovleff diyor ki; “Batının savaş anlayışı iflas etmiş bir yöntemdir.” Daha önemlisi yine kendi sözleriyle “Ahlaki olarak iflas etmiş bir yöntemdir.” Afganistan’dan bir örnek veriyor, önüme bir rapor geldi diyor, bir veya iki Ak-47‘li bir makinalı tüfekli saldırgandan dolayı hava desteği çağrılıyor, hava desteğinin karşısında 1 ya da 2 kişi var dikkat edin. 8 ton patlayıcı atılıyor. Şu anda Suriye’de kullanılan patlayıcı miktarı yaklaşık 4.000 tondan daha fazla diyor ve şunu soruyor; “Bu şehirlerde önümüzdeki 20 sene kim, nasıl yaşayacak?” Ahlaki olarak iflas etmiştir dediği bu. Bütün dünyadaki ordular artık küçük diyor, niye, başından beri anlattığım gibi şehirlerden dolayı. Çözüm nerede diyor, robotik teknolojiler olarak gösteriyor. Ama burada şunu söylüyor, robotlar askerin yerini alacak demiyor. Askerin etrafında bir robotik çevre kurulacak diyor. Önden giden dronelar, arkasına sakladığımız ateş unsurları, bu ne demek, yine hemen arkasından siberle ilgileniyorsanız robot dediğiniz sistemler, siber sistemler.

Türkiye için gelecek ne diye baktığımız zaman çok katmanlı harbin biz neresindeyiz, bir bunu sormamız

gerekiyor. Diğer tarafta sadece taktik sahadan uzak sivil dijital spektruma baktığımız zaman Stuxnet, Estonya, Black Enerji çok konuşuldu ama ne yapmamız gerekiyor? Çok güzel bir kitap var Orta Asya'dan Mustafa Kemal'e kadar Türk Ordusu diye. Bir Amerikalı yazarla Türk subay yazmış. Orada şunu der: "1700'lerdeki en büyük sorun Türklerin – uzmanlarının diyeyim – sürekli Osmanlı ile ilgili problemleri yazması kitaplar halinde ve çok güzel. Gerçekten çok güzel problemi anlatırlar. Sonunda bir sayfa çözüme ayırmasıdır."

Diğer taraftan taktik sahaya siber ineceği zaman şu soruyu sordular, İngiltere'de bir harp oyununda, "biz Facebook'un verisine nasıl ulaşacağız?" dediler. Biz bir şey istediğimiz zaman bize verecekler mi? Yasalardaki karşılığımız ne? Tabiri caizse kollarını nasıl bükeceğiz? Veya ben şu kadar veriyi inceliyorum sahada, hangi kuvvetle? Hiçbir ordu yedek sistem olarak tutamaz. Maliyetler konuşuldu zaten. Özel sektör. Özel sektörün taktik sahada var olması gerektiği bir dönemden bahsediyoruz. Buna hazır mıyız?

Son olarak da çatı kurum. Rusya'ya baktığımızda, Çin'e baktığımızda, Hollanda'ya baktığımızda, Almanya'ya baktığımızda bir çatı kurumunun olduğunu görüyoruz. Bu konuşmaları BTK'da yaptığımıza göre niye bizde BTK olmasın sorusunu ben sorayım. Sonunda bir sayfa ayırmam lazım ya çözüme, o da benim olsun.

Çalışma komitemizin geliştirdiği Hibrit Savaş Oyunu'yla HAVELSAN ekibi ve TSK'nın katılımıyla gelecek savunma ön izlemesini, öngörüsünü araştırmaya çalışacağız. Türkiye'de de bir ilk olacak. Arkasından da yayın yapacağız. Yayını elimden geldiğince yaymaya çalışacağım. Ve umarım o bir sayfa çözümü en azından bir 10 sayfaya çıkartacağız. Geç olduğu için çok hızlı geçtim. Ama istediğiniz yerde, istediğiniz zamanda bana ulaşıp, istediğiniz soruyu sorabilirsiniz. Dinlediğiniz için teşekkür ederim. Geldiğiniz için teşekkür ederim.

DOÇ. DR. İZZET GÖKHAN ÖZBİLGİN

HAVELSAN Siber Güvenlik Direktörü

HAVELSAN olarak teknoloji sohbetlerinin devamını yapacağız. Bu etkinliğe destek verdiğiniz için çok teşekkür ediyoruz. HAVELSAN Siber Güvenlik Ürünleri ve Çözümlerinin ses getireceğine inanıyoruz. Lokal ve global çözümler üretmeye devam edeceğiz. Bu etkinliğin gerçekleştirilmesinde rol alan herkese hepinizin huzurunda teşekkür ediyorum.

TEKNOLOJİ SOHBETLERİ 5

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

HAVELSAN
havelsan.com.tr


KNOLOJİ
OHBETLERİ 5
SİBER SAVAŞLAR
HAVELSAN
havelsan.com.tr

Ürün ve hizmetlerimiz ile ilgili bilgi almak için;
info@havelsan.com.tr

HAVELSANResmi www.havelsan.com.tr havelsan_resmi

Uzaktan Çalışma Güvenlik Hizmetleri Paketi

Yeni çalışma düzeninizi HAVELSAN deneyimine emanet ederek iş sürekliliğinizi güvenli bir şekilde sağlamaya devam edin.

Uzaktan Çalışma Güvenlik Analizi:

- Süreç ve Politika Analizi
- Mimari ve Yapılandırma Analizi
- Yetki ve Rol Tanımlamaları Analizi
- Uzaktan Çalışma Güvenliği Farkındalık Eğitimi

Uzaktan Çalışma Güvenlik Testleri:

- Personel Farkındalığı - Oltalama Saldırıları
- Personel Bilgisayar Güvenliği - HAVELSAN Tarafından Geliştirilen Araçlar ile Otomatik Sıkılaştırma
- Sızma Testleri
- Dağıtık Servis Dışı Bırakma (DDoS) Testleri

Uzaktan Çalışma Sistemleri Olay Yönetimi:

- Sistemlerin Gerçek Zamanlı İzlenmesi
- Kullanıcı Aktivitelerinin İzlenmesi
- Siber Olay Müdahale Danışmanlığı
- SIEM (Güvenlik Bilgi ve Olay Yönetimi) Danışmanlığı

OSCP|OSCE|OSWE|CISSP|GREM|GPEN|CEH|CISM|CISA|ISO27001

TÜRKİYE SİBER GÜVENLİK KÜMELENMESİ

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

HAVELSAN
havelsan.com.tr

TEKNOLOJİ SOHBETLERİ 5

www.teknolojisohbetleri.com