“SİBER GÜVENLİĞİN MİLLİ GÜVENLİK BAĞLAMINDAKİ ROLÜ”

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech **ODAK TOPLANTISI**

25 ARALIK 2019

KATILIMCILAR

Moderatör

(E) Korgeneral Alpaslan ERDOĞAN
STM ThinkTech Koordinatörü

Konuşmacılar

Kadir Murat BİÇER
STM Siber Güvenlik Müdürü

Borga ERBİL
HAVELSAN A.Ş. Siber Güvenlik Direktörü

Volkan ERTÜRK
Picus Security Kurucusu

Kubilay Onur GÜNGÖR
Multidisciplinary Cyber Struggle Academy Kurucusu

(E) Albay Kani HACIPAŞAOĞLU
CNK Global Consultancy Siber Güvenlik Direktörü

Mustafa ÖZÇELİK
SSB Siber Güvenlik ve Bilişim Sistemleri Grup Başkanı

Dr. Attila ÖZGİT
ODTÜ Enformatik Enstitüsü Siber Güvenlik Ana Bilim Dalı Öğretim Üyesi

(E) Tuğgeneral Mesut Bedri USTA
Turkcell İletişim Hizmetleri A.Ş. Kamu Savunma Teknolojileri Danışmanı

Mustafa YILMAZ
TR-TEST Test ve Değerlendirme A.Ş. Siber Güvenlik Direktörü

(E) Korgeneral Alpaslan ERDOĞAN

Siber güvenlik ve siber saldırılar kavramsal olarak ne ifade ediyor? Her yerde siber güvenlik, siber saldırı, siber terör diyoruz. İlk olarak kavramları tartışmak istiyoruz.

(E) Tuğgeneral Mesut Bedri USTA

Siber, sibernetikten geliyor. Bunun altını doldururken siber uzaydan, siber uzayın fiziksel katmanından bahsediyoruz. Buradaki herkes bu tanımları çok iyi bildiği için yeniden tanımlamak yerine biraz genişletmek isterim. Mesela Silahlı Kuvvetlerimizin kullandığı network'ün fiziksel katmanını oluşturan TAFICS sistemi, kapalı devre olduğu için güvenilir olduğuna dair yaygın bir kanı vardır. Her ne kadar İran'daki son Startnext olayından sonra bu biraz çökmüşse de ben hâlâ yüksek güvenlikli network'lerin kapalı devre olmaları gerektiğine inanıyorum. Tanımlamalardaki katmanlara baktığımızda artık yeni şeylerin söylenmesi gerektiğini düşünüyorum. Artık siber ortam dediğimiz şeyin, sadece fiber optik altyapı, ağ donanımları ve bilgisayarlardan oluşmadığını, elektromanyetik dalganın kullanıldığı her yerin siber tehdide açık ve siber güvenlik kavramına dahil olduğunu değerlendiriyorum. İşte bütün bu ortamı; yani bizim siber uzay ya da siber platform dediğimiz ortamdaki bütün katmanlarda (fiziksel katman-ağ katmanı-içerik katmanı-kod yazılım katmanı) güvenliği, bilişim sistemini saldırılardan korumayı, ortamda işlenen verilerin saklanmasını, veri bütünlüğünün sağlanmasını, erişimin güvence altına alınmasını, bütün bunların kayıtlanmasını biz siber güvenlik olarak tanımlıyoruz. Kablosuz sistemleri siber tanımının içine dahil etmek gerekmektedir. Mobil kullanıcıların, kablosuz sistemlerin bu kadar yaygınlaştığı günümüzde yönlendirilmiş antenler kullansanız bile Radyo Frekans (RF) sinyali bir siber güvenlik sorunu olarak ortaya çıkmaktadır.

Buradan siber saldırı kavramına bakarsak; Birleşmiş Milletler (BM) sanıyorum 51'inci maddesinde "Mutlaka devlet kökenli olması gerekmiyor, devlet dışı alandan da yapılsa siber saldırılar bir silahtır" der. Gerçi BM'de silah tanımı muallaktır ama 51'inci maddede siber saldırı bir silah olarak kabul ediliyor ve buna yönelik cevapların silahla verilebileceği de söyleniyor. Bizim TCK'da da 245 ve 246'ncı maddeler kapsamında her türlü bilgiye veya bilginin kullanıldığı alanlara -biraz önce tanımını genişlettiğimiz siber ortama- yönelik her türlü hukuk dışı girişimi siber saldırı olarak tanımlamak mümkün.

(E) Korgeneral Alpaslan ERDOĞAN

"Şahıslardan, devlet dışı organizasyonlardan veya terörist organizasyonlardan da gelse bu, saldırı olarak kabul ediliyor" diyorsunuz. Peki bunun -belki daha sonra da tartışırız- kaynağını belirlemek o kadar kolay mı?

(E) Tuğgeneral Mesut Bedri USTA

Siber saldırıların en önemli özelliklerinden biri, kaynağının belirsiz ve saldırı vasıtalarının kolay

"Siber uzay ya da siber platform dediğimiz ortamdaki bütün katmanlarda (fiziksel katman-ağ katmanı-içerik katmanı-kod yazılım katmanı) güvenliği, bilişim sistemini saldırılardan korumayı, ortamda işlenen verilerin saklanmasını, veri bütünlüğünün sağlanmasını, erişimin güvence altına alınmasını, bütün bunların kayıtlanmasını biz siber güvenlik olarak tanımlıyoruz. Buradan siber saldırı kavramına bakarsak; BM sanıyorum 51'inci maddesinde 'Mutlaka devlet kökenli olması gerekmiyor, devlet dışı alandan da yapılsa siber saldırılar bir silahtır' der. Bizim TCK'da da 245 ve 246'ncı maddeler kapsamında her türlü bilgiye veya bilginin kullanıldığı alanlara -biraz önce tanımını genişlettiğimiz siber ortama- yönelik her türlü hukuk dışı girişimi siber saldırı olarak tanımlamak mümkün."

(E) Tuğgeneral Mesut Bedri USTA

elde edilebilir olmasıdır. Ancak kolay yollarla elde edilen donanımla belirsiz kaynaklardan yapılabilmesi tehdidin varlığını ve sonuçlarını çok değiştirmiyor. Sonuçta hangi sektörde olursa olsun gerek kritik altyapı gerek güvenlik gerek silah, özellikle akıllı şebekelere yapılacak herhangi bir girişim siber saldırı olarak tanımlanıyor.

(E) Albay Kani HACIPAŞAOĞLU

Bu kavrama değişik bir açıdan ben de şöyle bakmak isterim: Siber güvenlik (*cyber security*) özellikle sivil sektörde çok yaygın olarak kullanılan bir tabir günümüzde. Ama bu toplantının çerçevesini düşündüğümüzde, sadece siber güvenlik kavramı altında bakmamak için bir görüş ortaya koymak uygun olur. Çünkü teknik olarak baktığımızda siber güvenlik dediğiniz şey, tamamıyla kendi sisteminizi korumak için aldığınız teknik önlemlerdir. Sistem üzerinde yaptığınız güvenlik ayarlamaları, parametrelerde yaptığınız ayarlar, koyduğunuz cihazlarla güvenliğinizi sağlıyorsunuz. Aynı fiziksel güvenliğinizi sağladığınız gibi. Ama milli güvenliğe olan etkisini üst seviyede ve genelde düşündüğümüzde NATO artık siber güvenlik demiyor. Barış, kriz ve savaş dönemlerini kapsayarak hem asker hem sivil kesimi içine almak üzere *cyber warfare* diye adlandırılıyor. Bu kavramı muharebe meydanına indirirseniz bunun adı *cyber operations diye tanımlanıyor, içinde siber güvenliği, siber savunması ve tabii siber taarruzu* var. Siber savunmayı bile iki safhaya ayırmak mümkün. Birisi içinde bulunduğunuz anda sistemlerinizi korumak için yaptığınız icraat -ki buna "pasif siber savunma" diyebiliriz; diğeri STM'nin de büyük katma değer yaratarak üzerinde çalıştığı "aktif siber savunma", yani proaktif olarak sistemlerimizi koruma gayreti. Biraz önce bahsettiğim gibi "siber harekât (*cyber operations*)" ya da en genel kapsamlı adıyla "siber savaş (*cyber warfare*)" sürecinin "siber taarruz (*cyber attack*)" denilen safhası var. Biz sivil tabirde genel bir anlatımla buna "siber saldırı" diyoruz. Ama ister "siber saldırı", ister "siber taarruz" diyelim, politik ve diplomatik dilde bu tabir farklı şekillerde ama tabii ki aynı anlam ve kapsamda ifade ediliyor. 2010'a kadar NATO, siber taarruzu hiç kullanmayıp sadece "siber savunma (*defence only*)" diyordu. Aradan bir müddet geçti; 2015-2016'dan sonra siber ortamdaki harekât için *respond appropriately* demeye başladı: "Uygun şekilde karşılık ver!". "Uygun şekilde karşılık verme"-nin içine takdir edersiniz ki her şey girer.

Toplantının müteakip saatlerinde yeri geldikçe açıklayacağım, şu anda NATO'da fiilen -fiziken geçen hafta İstanbul'da, bir ay önce de İzmir NATO Karargâhında- tatbikatlar uygulandı. Bunu sadece bir siber tatbikat değil insani yardım operasyonunu da içeren, Afrika'da geçen, komuta-kontrol, lojistik ve politik tarafı dahil bir tatbikat olarak düşünün. Bakıldığında artık bu kapsamdaki siber operasyon görevleri siber karşı taarruzu da kapsamak üzere "*Deter* (Caydırma)", sonra da "*Degrade*

(Gücünü azaltma)" ve "*Destabilize* (Çalışamaz/işlemez hale getirme)" ifadelerine dönüşüyor. Bunların hepsi aslında ofansif, yani taarruz/karşı taarruz ya da sivil tabirle saldırı kapsamındaki tabirler. Ama genelde politik/diplomatik seviyelerde *cyber offense*, *cyber attack* tabirlerini kendi yapacakları harekât içinde kullanmıyorlar. Zaten "saldırı" ya da "taarruz" günlük dilde ve taktik seviyelerde kullanılan ifadeler. Biraz önce bahsettiğim gibi seviye yükseldikçe ifade tarzı değişiyor ama niyet aynı. Bunu da böyle yapmak zorundalar çünkü hayatın gerçeği bu. Örneğin, NATO Genel Sekreteri 2018 yıllık raporuna çok açık bir şekilde yazmış: "NATO, artık siber olaylar dahil, elindeki her türlü imkân ve kabiliyeti karşılık vermek için kullanacak" diyor ve kullanıyor. Ama, NATO, yapısında şu anda organik olarak siber saldırı yeteneği olmadığı için bu tür bir icraat gerektiğinde bu kapsamdaki imkân ve kabiliyetini kullanmak için NATO'ya gönüllü olarak destek taahhüdünde bulunmuş olan yedi NATO ülkesinin siber taarruz timlerinin imkân ve kabiliyetlerinden faydalanıyor. Özetle, *Tallin Manual 2.0 On The International Law Applicable To Cyber Operations*, dört yıllık bir çalışma sonunda çıkan bir kitap. Burada diyor ki; "Yapacağınız siber harekât bir *Self Defence*, yani kendini savunma kapsamında mıdır ve *Proportionate*, yani size yapılan saldırı ile orantılı mıdır?" Temelde bu iki sorunun cevabı "evet" ise yapacağınız siber taarruz/karşı taarruz ya da saldırının uluslararası ortamda hukuksal dayanağı var demektir.

Sonuç itibarıyla, "siber güvenlik" işin en pasif güvenlik kısmı; "siber savunma" yapılan bir siber saldırıya karşı sistemlerimizi koruma kısmı, "siber taarruz/karşı taarruz" ya da "siber saldırı" ise uygun yöntem ve kurallarla aktif olarak karşılık vermek kısmıdır. Zaten bugün artık bütün planlama ve tatbikatlar, yani gerçeğin provası, tüm ülke kritik altyapılarına (su, sağlık, finans, enerji, ulaşım, telekomünikasyon gibi) yapılan siber saldırılarla başlıyor; sonra bildiğimiz klasik, konvansiyonel sıcak savaşla devam ediyor. Bu vesileyle, şu yanlış algıyı da düzeltmiş olalım: "Savunma" denilince konu siber bile olsa savunmanın bir asker işi olduğu yanılgısı var. Halbuki siber konusundaki savunma; barış, kriz ve savaş dönemleri de dahil tüm ülkede ağırlıklı olarak sivil kesim tarafından (kamu ve özel sektör) yürütülen bir faaliyettir. Çünkü belirttiğimiz gibi hedef, ülkenin enerji, finans, ulaşım ve sağlık gibi kritik altyapılarıdır. Dolayısıyla, "siber savaş (*cyber warfare*) kavramı barış, kriz ve savaş dönemlerini kapsayan; kendini koruma/savunmanın ötesinde siber karşı taarruzu da içine alan ve her dönemde ağırlıklı olarak ülkenin kamu ve özel sektörü ile sivil kesimi tarafından icra edilen milli güvenliğin ayrılmaz, hayati önemdeki bir parçasıdır. Bugün, dünyanın tüm gelişmiş ülkelerinin bu konuya bakışı böyledir.

(E) Korgeneral Alpaslan ERDOĞAN

Zaten genelde biliyorsunuz her ülkenin milli savunma bakanlıkları vardır. Hiçbir ülkenin saldırı bakanlığı ya da taarruz bakanlığı yoktur. Bütün ordular, bütün askeri teşkilatlar savunma için kurulmuştur sözde ama hepsinin bir saldırı planı da vardır. Bu aynen siber harekât için de geçerlidir.

(E) Albay Kani HACIPAŞAOĞLU

Tabii bu anlattıklarım Latince adıyla "de jure", yani hukuksal, resmi boyutu; bir de "de facto" dediğimiz gerçek hayatın pratikte uygulanışı var.

"Siber savaş kavramı, barış, kriz ve savaş dönemlerini kapsayan; kendini koruma/savunmanın ötesinde siber karşı taarruzu da içine alan ve her dönemde ağırlıklı olarak ülkenin kamu ve özel sektörü ile sivil kesimi tarafından icra edilen milli güvenliğin ayrılmaz, hayati önemdeki bir parçasıdır. Bugün, dünyanın tüm gelişmiş ülkelerinin bu konuya bakışı böyledir."

(E) Albay Kani HACIPAŞAOĞLU

Örneğin, Eylül 2018 tarihli ABD'nin Siber Güvenlik Strateji belgesinin önsözünde Trump diyor ki: "Ülkemin güvenliği ve refahı için siber güvenlik, siber savunma benim için çok önemli. Kim ülkeme kötücül yazılımlarla bir siber saldırı yaparsa, onu cezalandırırım." Bu kadar net. Yani Trump'a göre hangi kitapta ne yazdığının da bir önemi yok... Bu da dünyanın gerçeği.

(E) Korgeneral Alpaslan ERDOĞAN

Borga Bey, sizin ilaveniz var mı?

Borga ERBİL

Ufak ilavelerim olacak naçizane. Ben 1978 doğumluyum, 42 yaşındayım. Tecrübelere, deneyimlere çok inanıyorum. Ben henüz çocukken televizyonlar daha yeni yeni vardı. Siyah beyazdı, sonra renkli oldu. Evimize renkli televizyon geldiği günü hatırlıyorum. Üniversiteye ilk başladığım yıllarda internet omurgası daha yeni yeni şekilleniyordu 1996 yılında. Hatta 1993 yılında internet Türkiye'de ilk defa kullanılmaya başlandı. Bugün 27'nci yılındayız. Ama bu süreçte tabii elektronik entegre devreler hep vardı. Aslında hem bizde hem dünyada elektronik kartlar belli sistemlerde kullanılıyordu. Siber kavramı, işte yavaş yavaş internetle birlikte birazcık daha kendi içimizde köklerini salmaya başladı. Bir hocam vardır hatta, şöyle derdi: "Biz eskiden her şeyi konuşturmaya çalışıyorduk, şimdi her şeyi bloklamaya çalışıyoruz." Yani ilk başlarda özellikle çok yüksek meblağlar vererek wifi'larla sistemlerin birbiriyle konuşturulması sözkonusuydu. Şimdi ise bambaşka bir boyuttayız. Tabii 1993, sonra 90'lı yılların sonu, 2000'li yılların başında hep IT projeleri yapılmaya başlandı. IT alanında, bilgiye erişim teknolojileri alanında hep gizlilik-bütünlük-erişilebilirlik olarak bakılıyordu bu hususa. Evet gizlilik anlamında en popüler örnek şu meşhur 450 bin civarında kredi kartı ama *integrity*'ye bakıyorum, doktorun önüne giderken MR sonucunun değiştirilmesi örneği var. Şimdi bu bambaşka bir boyut *integrity*'de. İki gün içerisinde yerli otomobilimizin lansmanı yapılacak. O otomobili durdurabilmek konusu mesela şu an *availability* örneği olabilir.

(E) Korgeneral Alpaslan ERDOĞAN

Borga Bey, çok farklı bir şey söylüyorsunuz. İkinci Devrim otomobili vakası olur, Allah korusun. O otomobilin durdurulması konusu gibi hususlar kötü niyetli insanların aklına gelebilecek şeyler. Yani başladı, Allah korusun, köprünün ortasında durdurulursa, ikinci Devrim otomobili vakası yaşarız. İnşallah öyle bir şey olmaz diyelim.

Borga ERBİL

Ben elektromanyetik *compatibility* testlerini yapmış bir kişi olarak nasıl deaktive edildiğini iyi biliyorum. Dolayısıyla sadece deaktive edilmek değil, farklı şekilde yönlendiriyor olmak, bunların hepsi risk. Dolayısıyla aslında ben üniversite öğrencilerine *availability* dediğimiz noktada kendi evimizdeki robotların, endüstriyel sistemlerin kullanılabiliyor olması örneklerini veriyorum. Dolayısıyla IT'den uzaklaştığımızı bu anlamda görüyorum. Hafızam beni yanıltmıyorsa Türkiye'de 1 Nisan 2016'da 4,5G lansmanı yapıldı. Şimdi artık biz 5G konuşuyoruz, 6G hazırlıkları var. Yani dolayısıyla internet alanından yavaş yavaş mobiliteye, daha çok IoT'ye giden bir alanda artık siber, siber güvenlik, siber saldırı konuları daha sık gündeme gelmeye başladı. Elektrik nasıl şu an hayatın doğal bir parçasına dönüşmüşse zamanı geldiğinde bilgisayarlar da böyle olacak. Her yerde internet olacak ve onu kanıksamayacağız. Bu anlamda da 5G'nin de özellikle devreye girmesiyle artık bilgisayarlar kendi içinde konuşabiliyor olacak. Dolayısıyla bizim siber anlamda IT güvenliğini kanıksamamız lazım ama bir sonraki aşamaları konuşuyor olmak bana daha makûl geliyor. Teşekkür ediyorum.

(E) Tuğgeneral Mesut Bedri USTA

Onun için ben elektromanyetik dalganın altını çizdim. Dünyanın birçok yerinde tank halen esas muharebe vasıtası olarak değerlendiriliyor. Ancak

elektromanyetik dalgalar üzerinden yapılacak siber saldırılarla tankların etkisiz hale getirilmesinin yakın zamanda mümkün olacağını değerlendiriyorum. Bunları göz ardı etmemek lazım.

(E) Korgeneral Alpaslan ERDOĞAN

Kubilay Bey, bu konuda sizin ilaveniz var mı?

Kubilay Onur GÜNGÖR

Ben naçizane, tabii çok da haddimi aşmadan kavramlarla ilgili biraz muhalif taraftayım. Bizim zaten Cyber Struggle içerisinde yaptığımız şey de bir doktrin çalışması özünde. Dolayısıyla şu anda var olan tanımlara biraz eleştiride bulunuyoruz. Bu eleştirilerin özü de ilk önce şuna dayanıyor: Bir siber tanımı yapılırken -siber alan, siber dünya, siber uzay, vs- genelde cihazlar, elektromanyetik dalgalar, vs. üzerinden yapılıyor. Ancak biz daha çok yapı itibarıyla, yani doktrin itibarıyla siberi sanki vücudumuzun bir parçası gibi görüyoruz; dolayısıyla ayrı bir alanmış gibi düşünmüyoruz. Yani ayrı alan düşüncesi bize biraz konvansiyonel, daha gelenekçi bir yaklaşım gibi geliyor. Bu da mesela tanımı şu noktaya götürüyor: Kara, hava, deniz ve uzaya ek olarak beşinci alan siber gibi bir tanım var. Sanıyorum hâlâ NATO'da bilimsel tanım bu. Biz bundan ziyade aslında siberin bir *framework* olduğunu düşünüyoruz, ayrı bir alan değil. Şu an var olan bütün *domain*'leri kapsayan ve her biri için etki yaratabilecek bir alan olduğunu düşünüyoruz.

(E) Korgeneral Alpaslan ERDOĞAN

Yani diğer bütün alanlarla bütünleşik bir yapı mı demek istiyorsunuz?

Kubilay Onur GÜNGÖR

Evet, kesinlikle. Bu açıdan bakıldığında -mesela komutanım da belirsizlik üzerinde durdu- zaten siber faaliyetlerin kendisi belirsiz. Kuvvet yapısı belirsiz, bir saldırının süresi, nereden hangi kuvvet çarpanı ile geleceği, ne kadar süreceği belirsiz. Yani inanılmaz bir belirsiz ortamdan bahsediyoruz. Bu yapısı itibarıyla da aslında gayrinizami harbin doğasıyla bire bir örtüşüyor. Hatta terörden daha çok gayrinizami harbe benziyor. Terörde dahi, düşmanı tanımlama, hiç olmazsa bir çıkarım yapma, yani karşı taraf kabul etmese bile, bir

> *"Savaşla barış arasında bir ayrım da yok siberde. Siberle ilgili olarak zaten her şey belirsiz olduğu için aslında durum olarak bir savaş durumunda mısınız, yoksa barış durumunda mısınız; onu da bilmiyorsunuz. Bu çerçevede yapılan her türlü ofansif siber faaliyeti aslında etki odaklı harekât çerçevesinde değerlendiriyoruz. Demek ki bu sürecin aslında kavramsal olarak tamamıyla gayrinizami harp yahut asimetrik savaş çerçevesinde değerlendirilmesi ve kuvvet yapısının, personel yapısının da tıpkı bir özel kuvvet yapılanması gibi yeniden değerlendirilmesi gerektiğini düşünüyoruz."*
>
> **Kubilay Onur GÜNGÖR**

şeye vekalet ettiğini tespit edebilme gibi birtakım manevra kabiliyetlerine sahip oluyorsunuz. Ama siber faaliyetler terörden bile daha gayrinizami bir harp süreci. Öte yandan bu da siber savaş tanımını etkiliyor. Biz buna da muhalefet ediyoruz. Çünkü doğal olarak savaşın da bir geleneksel tanımı var. Savaşın bir öncesi var, savaş anı var, sonrası var ve bir bitişi var. Ancak siber taraf öyle değil. Hatta savaşla barış arasında bir ayrım da yok siberde. Siberle ilgili olarak zaten her şey belirsiz olduğu için aslında durum olarak bir savaş durumunda mısınız, yoksa barış durumunda mısınız; onu da bilmiyorsunuz. Sadece sezgisel olarak en fazla "Herhalde barıştayız" ya da "Herhalde birileri bize karşı bir siber faaliyet yürütüyordur muhtemelen" gibi çıkarımlarla ilerleyebiliyoruz. Bu çerçevede yapılan her türlü ofansif siber faaliyeti aslında etki odaklı harekât çerçevesinde değerlendiriyoruz. Bu da bizi şuna götürüyor: Demek ki bu sürecin aslında kavramsal olarak tamamıyla gayrinizami harp yahut asimetrik savaş çerçevesinde değerlendirilmesi ve kuvvet yapısının, personel yapısının da tıpkı bir özel kuvvet yapılanması gibi yeniden değerlendirilmesi gerektiğini düşünüyoruz. Bizim kendi doktrinimiz ve bütün çalışma şeklimiz de bunun üzerine kurulu.

(E) Korgeneral Alpaslan ERDOĞAN

Bu konuda ilavesi olan var mı?

(E) Albay Kani HACIPAŞAOĞLU

Söylediklerinize katılıyorum; ancak Kara, Deniz, Hava ve Uzay'dan sonra "Siber"in beşinci boyut/harekât alanı (*Domain*) olarak tanımlanması, olayların üzerine somut olarak gidilebilmesi için yapılan bir değerlendirme. Örneğin, siber de dahil bir harekâta etki edebilecek tüm psikolojik, sosyolojik, basın-yayın ve iletişim bilgilerini NATO *Information Enviroment* tanımı altında toplamış. Bu tanımı iyi incelediğinizde görüyorsunuz ki bilgi üstünlüğünüz ve gücünüz sayesinde "kinetik" etkiye gerek kalmadan birçok konuda inisiyatifi ve gücü elde bulundurabiliyor, ortamı lehinize çevirebiliyorsunuz. Yani, diğer bir ifadeyle, barış zamanı da savaşın içindesiniz, işte komutanımın belirttiği gibi bu olguya "hibrit (karma) savaş" denilmiş. Yani, sonuçta tanımlar bir yerde bir şeyin üzerine gidebilmek, sorunu ve çözümü ortaya koyabilmek için var.

Kubilay Onur GÜNGÖR

Ben bazen şöyle düşünüyorum: Bu tanımlar üzerine o kadar gidiliyor ki konvansiyonel bir yapılanmaya dönüşüyor, hantallaşmaya başlıyor.

(E) Albay Kani HACIPAŞAOĞLU

İşte konvansiyonel olmaması lazım.

Kubilay Onur GÜNGÖR

Mesela siber bir ordudan bahsediliyor. Ben bir adım daha ileri gidiyorum. Siberin ordu içerisinde

> *"Siberin ordu içerisinde bir ihtisas olması gerektiğini düşünüyorum. Örneğin bir özel kuvvet personeli nasıl dağ komando ihtisası alıyorsa, siber brövesi de takabilir. Ama aslında bir özel kuvvet personelidir."*
>
> **Kubilay Onur GÜNGÖR**

bir ihtisas olması gerektiğini düşünüyorum. Örneğin bir özel kuvvet personeli nasıl dağ komando ihtisası alıyorsa, siber brövesi de takabilir. Ama aslında bir özel kuvvet personelidir.

(E) Albay Kani HACIPAŞAOĞLU

O zaman işte o tanımları netleştirmek lazım. Yani, tanımları bu kadar genişletirseniz *baseline*'ı, temel referansları ve sınırları kaybedersiniz. Yani bu alanda çalışanlara ne görev vereceksiniz, kadro tanımı ne olacak, teşkilattaki yeri ne olacak, hangi görev tanımlarının alt kırılımları ne olacak? Onun için bir çerçeve çizmek zorundasınız. Yani çerçeveye her şeyi dahil ettiğinizde hem teknik hem yönetimsel hem de hukuki olarak belirsizlikler doğar ama bu tanımlamalar genişletilebilir belki.

Dr. Attila ÖZGİT

Kubilay Bey'in görüşlerine katılıyorum. Siber güvenlik çok net bir şekilde İngilizcesiyle *cross cutting* dediğimiz bir konumda. Yani bütün alanları yatay olarak kesiyor ve artık günümüzde bağlantılı dünya (*connected world*) dediğimiz dünyada siber güvenlik her cihazın içinde belli bir savunma kapasitesini sağlamak durumunda. Derslerde bir saydam olarak gösterdiğim "Kinetik vs. Siber Savaş" diye bir slayt vardır. Kinetik savaştaki şu olgu, siberdeki şuna karşılıktır şeklinde. IoT'ye kadar inmiş bir konudan bahsediyoruz. Yani illa ülke çapında bir askeri ya da terörist tehdide kadar gitmenize gerek yok. Buzdolaplarımızın, çamaşır makinelerimizin bundan beş sene sonra bağlantılı olduğunu düşünün. Fırınınızı *hack*'leyerek evde yangın çıkartmak, bir mahalleyi ciddi bir krize sokmak bile mümkün. Bütün bunlar tabii siber saldırı dendiği zaman aklıma şunu getiriyor: Belki biraz sistematik olarak saldırının arkasından yapılması gereken ya da korunmanın unsurları ve korunmadaki kriz yönetimi...

(E) Korgeneral Alpaslan ERDOĞAN

Yani 'resilience' olayına doğru gidiş mi hocam?

Dr. Attila ÖZGİT

Evet, tartışmanın yararlı olduğunu düşünüyorum. Ben 2015 yılının Aralık ayında Türkiye'nin belki de ilk ve en büyük siber saldırısını göğüslemiş biriyim. Oradan ekip olarak çıkarttığımız çok önemli dersler var. Gerçekten kriz durumunda, bugün internetin çok önemli altyapı bileşenlerinden olmakla beraber ayağınıza dolanan protokoller var. Mesela en basiti, DNS tabanlı çalışmak, kriz durumunda ciddi engel oluyor. Bu tür konuların da bence konuşulup önlemlerinin bir biçimde yeterince önceden alınması gerek. Tabii kriz yönetimi bir ön hazırlık gerektiriyor, bir de o anda sakin olmayı, koordineli olmayı gerektiriyor. Bir de bu

> *"Kriz yönetimi bir ön hazırlık gerektiriyor, bir de o anda sakin olmayı, koordineli olmayı gerektiriyor. Bir de bu büyüklükte siber saldırı ülke bazında düşünüldüğünde konu çok karmaşık bir hale geliyor. Gerçek bir sıcak savaşta bir genelkurmay başkanı altındaki bütün unsurları nasıl yönetecekse, bir siber saldırıda da bunun aynen o şekilde yönetilmesinin çok önemli olduğunu düşünüyorum."*
>
> **Dr. Attila ÖZGİT**

büyüklükte siber saldırı ülke bazında düşünüldüğünde konu çok karmaşık bir hale geliyor. Gerçek bir sıcak savaşta bir genelkurmay başkanı altındaki bütün unsurları nasıl yönetecekse, bir siber saldırıda da bunun aynen o şekilde yönetilmesinin çok önemli olduğunu düşünüyorum.

Kubilay Onur GÜNGÖR

Aslında hocam çok güzel bir noktaya değindi. Bir özel kuvvet yapılanması gerekir derken işin bu noktasına değinmek istemiştim. Anonymous grubunun popüler olduğu bir dönem vardı. O dönemde ben global bir firmada *SOC* ve *Incident Management* süreçlerinin parçasıydım. Ana akım saldırılar oldukça uzun sürmüştü. Bu saldırı süreçlerinde, yoğun stres ve baskıdan dolayı rahatsızlanan, hastanede destek alan arkadaşlar olmuştu. Bu örnek, baskı ve yoğun stres altında ekip sevk ve idaresinin en az teknik bilgi kadar önemli olduğunu net bir şekilde açıklamaktadır. Bu nedenle 9-5 çalışan 30 kişilik ekiplerdense, tıpkı bir özel kuvvet gibi sayıca daha düşük ama etki yüzeyi daha büyük çevik ekipler kurulmalı, departmanlar ve faaliyetleri buna uygun tasarlanmalı. Yetkiler, otonomi ve doktrin bu çerçevede dizayn edilmeli.

(E) Korgeneral Alpaslan ERDOĞAN

Aslında çok kritik bir noktaya değindiniz. Silahlı Kuvvetlerde komando kursu, özel harekât kursu gibi standart kurslarımız vardır. Ama artık siber temel kursları, siber tekamül kursları, siber uzmanlık kurslarının da verilmesi lazım. Belki de siber uzman brövesi takması lazım. Artık yavaş yavaş bir branşa doğru gitmesi lazım. Evet, Siber Savunma Komutanlığımız var ama özel olarak buna doğru gidilen bir sürecin izlenmesi lazım TSK'da da.

> *"Baskı ve yoğun stres altında ekip sevk ve idaresi en az teknik bilgi kadar önemli. Bu nedenle 9-5 çalışan 30 kişilik ekiplerdense, tıpkı bir özel kuvvet gibi sayıca daha düşük ama etki yüzeyi daha büyük çevik ekipler kurulmalı, departmanlar ve faaliyetleri buna uygun tasarlanmalı. Yetkiler, otonomi ve doktrin bu çerçevede dizayn edilmeli."*
>
> **Kubilay Onur GÜNGÖR**

"Silahlı Kuvvetlerde komando kursu, özel harekât kursu gibi standart kurslarımız vardır. Ama artık siber temel kursları, siber tekamül kursları, siber uzmanlık kurslarının da verilmesi lazım. Belki de siber uzman brövesi takması lazım. Artık yavaş yavaş bir branşa doğru gitmesi lazım. Evet, Siber Savunma Komutanlığımız var ama özel olarak buna doğru gidilen bir sürecin izlenmesi lazım TSK'da da."

(E) Korgeneral Alpaslan ERDOĞAN

(E) Albay Kani HACIPAŞAOĞLU

Komutanım, aslında bir adım ileriye giderek şunu da söylemek lazım: Sizin söylediklerinize ve Atilla Hocamın *cross cutting* dediğine aynen katılıyorum; her tarafı etkiliyor. Ama şimdi zaten yapılara baktığımızda, şu anda mesela Silahlı Kuvvetler Muhabere Elektronik ve Bilgi Sistemler (MEBS) içinden siber ve elektronik harp konularını çıkardılar; kritik bir yetenek olduğu için üst düzey karar verme makamlarına bağladılar. Bu yetenekleri doğru analiz ve sentez edip değerlendirmek ve siber savaşta ya da siber savaşı da içine alan hibrit savaşta üstünlük sağlamak maksadıyla *Information and Knowledge Management*, *Information Operations* ve *Strategic Communications (STRATCOM)* gibi önemli kritik birimler kurdular. Bu kapsam içinde STRATCOM tanımı çok önemli; yapacağınız siber harekâtın, özellikle siber taarruza, saldırıya yönelik olan kısmında teknik ve hukuksal haklılığınızı ulusal ve uluslararası ortamda kabul ettirebilmeniz için sosyal medyanın ve psikolojik harekâtın uygun kullanımı var.

(E) Tuğgeneral Mesut Bedri USTA

Bir konuya açıklık getirmek isterim. Sanki siber güvenlik askeri bir alana sıkıştı kaldı. Orada kalmasın. Eğer siber güvenlik veya bunun milli güvenliğe etkisinden bahsediyorsak konunun sadece askeri bir yapılanma ve faaliyet olarak değerlendirilmesi bizi tamamen yanlış noktalara götürür. Silahlı Kuvvetlerin, brövesi olan siber güvenlik sınıfı kurması ve bunların siber güvenliğin kesin çözümü olarak nitelendirilmesi doğru olmaz. Evet, tehdidin askeri yönü vardır. Ancak bütün ülkede elektrik kesildiği zaman ağ güvenliğinizin tam olması, bilgiye erişmeniz ya da silahlarınızı kullanmanız da yaşayacağınız sıkıntıları ortadan kaldırmaz. Örnek olarak TAFICS, Silahlı Kuvvetlerin en önemli yeteneklerinden biridir. Ama elektrik kesildiği zaman belli bir saatten sonra bu yeteneği kullanmakta zorluklar yaşanır. Ya da Türk Silahlı Kuvvetleri Türkiye'nin üstündeki 300 noktadan uydu irtibatı sağlıyorken sivil askeri uydu yer istasyonlarında elektrik kesildiği zaman komuta kontrol sisteminiz zaafa uğrar. Dolayısıyla güvenlik sadece askeri bir alana sıkışmadan topyekûn milli güvenlik olarak ele alınmalıdır. "Siber Güvenlik ordusu kuralım, bir de bröve verelim, bunlar MEBS sınıfından da olmasın, siber güvenlikçi olsun" çözümünü çok da gerçekçi bulmadığımı ifade etmeliyim.

"Eğer siber güvenlik veya bunun milli güvenliğe etkisinden bahsediyorsak konunun sadece askeri bir yapılanma ve faaliyet olarak değerlendirilmesi bizi tamamen yanlış noktalara götürür. Silahlı Kuvvetlerin, brövesi olan siber güvenlik sınıfı kurması ve bunların siber güvenliğin kesin çözümü olarak nitelendirilmesi doğru olmaz. Evet, tehdidin askeri yönü vardır. Ancak bütün ülkede elektrik kesildiği zaman ağ güvenliğinizin tam olması, bilgiye erişmeniz ya da silahlarınızı kullanmanız da yaşayacağınız sıkıntıları ortadan kaldırmaz."

(E) Tuğgeneral Mesut Bedri USTA

(E) Korgeneral Alpaslan ERDOĞAN

Müsaade ederseniz şimdi ikinci konumuza geçiyoruz. İkinci konumuz siber güvenlik ve siber saldırı; devlet yönetimi, askeri envanter ve harbe hazırlık, finans, ekonomi, enerji, sağlık, eğitim, ulaştırma, haberleşme vb. alanları hangi büyüklükte, ne kadar süreyle, nasıl ve ne şiddette etkileyebilir ve olası etkiler nasıl yönetilebilir? Hocam buyurun, sizinle başlayalım. Biraz önce değindiğiniz 2015'in sonundaki en büyük siber saldırı örneği ile başlayalım.

Dr. Attila ÖZGİT

Ddos.tr yönetimi saldırısıydı. 15 gün sürdü. Tabii nokta tr'yi devirdiği zaman bir süre sonra ülke karanlığa bürünecekti, çünkü durum hiçbir nokta tr'li yere erişilmez hale gelecekti. Deviremediler. Zaten DNS doğası gereği bir miktar kendiliğinden karşı durabilir bir protokol. Onun da avantajını kullandık. 15 günün sonunda bizden vazgeçerek muhtemelen ayrıntısını BTK ve Ulaştırma Bakanlığının bildiği, kamu kurumları ile kamu ve özel sektör bankalarına bir hafta boyunca saldırılar yapıldı. Toplam üç hafta sürdü. Sonraki iki buçuk, üç yıl içinde bu saldırının kaynaklarına ilişkin kişisel görüşlerim oluştu, o ayrı bir hikâye. Olaya bu kadar büyük baktığınız zaman, demin söylediğimi tekrarlayacağım; bunun savunmasının, savunma stratejilerinin daha önceden yeterli tatbikatlarla bütün sektörler arasında yapılmış olması lazım. Bir de birbirinden kopuk, ayrı yönetimlere bağlı, kendi bilgisini devlet sırrı gibi saklayıp paylaşma eğilimli olmayan sektörlerin bir arada yönetebileceği süreçler değil bunlar. Bir kere bu anlayışın değişmesi lazım.

Bankanın, enerjinin günlük hayatta normal denebilecek trafiği nedir, bu nasıl modellenir, bu trafiğin anomali durumları nasıl anlaşılır? Bütün sektörler için bu yapılmalı. Ve özellikle kriz durumunda kim, nereye, nasıl raporlayacaktır? Bence olabildiğince güvenli ve otomatik savunma mekanizmalarının ortada olması lazım. Örnekleyecek olursak, bir operasyon merkezi düşünelim. Son beş, altı yıldır STM dahil önde gelen bütün savunma şirketlerimizin bir SoC Center'ı var. Bunun için de kendi dünyalarında, kendi verileriyle birtakım çalışmalar yapıyorlar. Tabii resmin tümünü göremiyorlar, her biri kendi dünyasındaki küçük resimleri görüyorlar. Aslında belki de her şey o resimlerin içinde yer alan küçük ipuçlarının toplu değerlendirmesinden geçiyor. Bugün büyük veri diye bir fırtına koparılıyor. Ben işin akademik tarafındaki biri olarak bu *buzz word*'leri hiç sevmiyorum. Yani büyük veri dediğiniz şey, makine öğrenmesi ile öğrenme teknolojisi. Büyük veri kimin elinde? Türkiye için bakacak olursak üç tane büyük operatörün elinde. Dünya için bakacak olursak 15 tane büyük telekom operatörünün elinde. Bunun yanında Google, Apple gibi insanları yönetebilen yerlerin elinde. Dolayısıyla aslında özünde makine öğrenmesi. Yani bütün bu alan, verinin büyüklüğü ve elinizde yaptığınız o istatistiki algoritmalarla bir başka algoritmayı aynı veri üzerinde karşılaştırabilmek. Senin küçücük verinden çıkarttığın algoritmanın başarımını ben nasıl ölçeceğim ki? Bir kere verinin paylaşılması lazım. Ülke yapay zekâ, makine öğrenmesi, büyük veri, analitik gibi uygulamalar yapacaksa burada üretilen algoritmaların hangisinin en iyi olduğunu bulmanın yolu ortak veriyi hepsine vermek. Ortak veriyi yaratırsınız, hepsi gelir yarışır. Bir tanesine bakarsınız, pırıl pırıl parlıyor. Müthiş sonuçlar çıkartır. Böyle anlarsınız. Verinin bu anlamda büyütülmesi, paylaşılması gerekiyor.

Türkiye'ye kaç noktadan girilir? Benim tahminim operatörlerin her birinin çok büyük beş, altı ana arteri olsa... Buraların üzerinden geçen trafiğe baktığınız zaman, Türkiye'nin üzerine doğru gelen bütün tehdidi görmeniz mümkün. Küçük bir pencereden küçük bir yere baktığınızda hâlâ bir şey görebilirsiniz ama ne kadar kaliteli sonuç çıkartabileceğiniz bence tartışmalı. Mesela burada muhatapları olduğu için bu soruyu yöneltiyorum. HAVELSAN, STM, bilmediğim başka SOC Center'lar, muhtemelen TÜBİTAK'ın vardır; bu kurumlar ellerindeki veriyi ortak bir havuza koymayı düşünürler mi? Temel tahminim, cevap hayır ya da çok zor. Niçin? Bence milli karakterimiz diyelim. Dolayısıyla benim kişisel gözlemim, sekiz sektörümüzle birlikte bu kadar büyük siber savunma yapacaksak bilgi paylaşımının bugün

olduğu yer kötü bir düzeyde. Bunu hiç değilse vasat bir yere çekmemiz lazım. Bir anlayış değişikliği gerekiyor.

Sonra teknik adımlar olarak konulara bakmak lazım. Eğer ülkenin tepesindeki kurumlar -Genelkurmay, MİT, Ulaştırma Bakanlığı, BTK, SSB gibi kriz durumunda ortak bir karara vardılar. Evet, şuradan şöyle bir saldırı geliyor. Duvarda ortak resim görmeleri gerekiyor. Biz bu ortak resmi 2015'te görememiştik. İki telekom operatörünü yan yana bile getiremedik. Aynı konferans görüşmesinin içinde bile onunla ayrı, öbürüyle ayrı konuştuk. Dolayısıyla ilk önce ortak bir resme ülke olarak bakabiliyor olmamız lazım. Bunun altyapısı da bilgiyi oraya doğru akıtıp konsolide etmekten geçiyor. Bunun teknolojisi için de reaksiyon olarak da çok hızlı adım atmanız lazım. Beş, altı tane önemli kurumun yetkilileri bir yerde problem olduğuna karar verirse hemen buna karşı bir önlem alınması lazım. Telefonla olabilecek bir şey değil. Bunların teknolojisinin otomatik olması güven ilişkisini de gerektiriyor. Yani merkezi bir yerden birtakım kritik *router*'lara "Şu *update*'i anında yap" diyebilmek için o *router*'ların o merkeze güvenmesi lazım. Dolayısıyla bu güven ilişkisinin altyapıda iletişim teknolojisi olarak kurulmuş olması lazım. Bu da bir çaba. Burada ayrı, özgün bir üründen, milli bir üründen bahsediyorum. Ama ülke çapında 40, 50, 100 ana arterden giren zararlı trafiği şak diye durduramazsınız. Bence bunların önlemlerinin şimdiden alınmaya başlanması lazım. Ve bunun önündeki en önemli temel engel milli kültürümüzün o olumsuz özelliği. Benim bilgim çok değerlidir, başım belaya girer, bu bilgiyi paylaşmayayım duygusundan yavaş yavaş farklı anlayışlara evrilmemiz lazım.

> *"Benim kişisel gözlemim, sekiz sektörümüzle birlikte bu kadar büyük siber savunma yapacaksak bilgi paylaşımının bugün olduğu yer kötü bir düzeyde. Bunu hiç değilse vasat bir yere çekmemiz lazım. Bir anlayış değişikliği bence gerekiyor."*
>
> **Dr. Attila ÖZGİT**

(E) Korgeneral Alpaslan ERDOĞAN

Yani bilgi kıskançlığından kurtulmamız gerekir sonucu mu çıkaralım hocam bundan?

Dr. Attila ÖZGİT

Evet. Namık Kemal Pak rahmetli, ODTÜ Fizik bölümü hocamız çeşitli nedenlerle teknolojik konularda da bizden fikir alıyor. Sonra TÜBİTAK Başkan Yardımcısı ve daha sonra da başkanı oldu. O yıllarda, "Biz ODTÜ'yüz, her şeyi çok iyi biliriz" diyen rahmetli Namık Hoca, TÜBİTAK koltuğuna oturduktan sonra, "Bu üniversiteler de ne yapar? Biz TÜBİTAK olarak her şeyi yaparız" duygusuna çok hızlı bir şekilde evrildi. Örgütlerde oluşan atmosfer, bireyleri tek tek etkisi altına alıyor. Dolayısıyla genel anlamda "Biz bu alanın en iyisiyiz" duygusu bir şekilde yerleşirse bunun gibi dükalıklar bir sürü yerde oluşmaya başlıyor. Dolayısıyla bu da bir örnek.

(E) Korgeneral Alpaslan ERDOĞAN

Hocam, aslında bu söylediğiniz husus davranış bilimlerinde "grubun birey üzerindeki normatif etkisi" diye adlandırılıyor. Yani gruba yeni giren bir bireyi öbür grup üyeleri anında şekillendiriyor.

Dr. Attila ÖZGİT

Cizre'deki bir sıcak savaşı yöneten kara kuvvetlerinin içinde oluşmuş böylesine bir duygu fazla sorun değil çünkü onların işini onlar çözecekler. Ama konuştuğumuz konu artık bu değil. Konuştuğumuz konu herkesi ilgilendiriyor. Dolayısıyla devletin içindeki değişik bakanlıkların ya da sektördeki iri kütlelerin bu anlayışı yıkmak için özel çaba göstermeleri gerektiğini düşünüyorum. Hem kendi içlerinde dikey olarak hem de

yatay olarak bütün sektörlerde. Dolayısıyla bütün bu üretilebilecek tekniklerin, teknolojilerin verimli kullanımı bana sorarsanız buradan geçiyor.

Volkan ERTÜRK

Bana sorduğunuz zaman, kuruma gelen zarar içerikli bir e-posta buradaki makineye virüs bulaştırdı. Bu ransomware bulaştırmaya çalışan, kötücül bir virüs ve adamın amacı para almak. Bu durum aslında ufak ekonomik kazanç amaçlı, saldırganın aynı anda yaptığı 100 bin saldırıdan bir tanesiydi. Bu bizim için aslında ülkenin siber güvenliğini etkileyen bir konu değil. Buna bir KOBİ'nin işini doğru yapmamasından kaynaklanan kaybettiği para ya da kaybettiği veri olarak bakıyoruz. Bunun bir finans kurumunda da, bir devlet kurumunda da çok benzer örnekleri olabiliyor. Konteks değiştiği zaman, kurum değiştiği zaman, devlete yapılan siber saldırı veya bir KOBİ'ye yapıldığında nasıl yorumlanıyor? O bankanın itibar kaybıdır. Benim çok bankacı müşterim olduğu için biliyorum, o banka siber saldırı yaşadığı zaman "Vatandaşın bize güveni azalıyor, marka güveni azalıyor, daha az para yatırıyor. Bizimle daha az çalışıyor. O yüzden siber güvenliğimizle kurduğumuz itibarımız bizim için çok önemli" diyorlar. Yani aslında orada ekonomik güdülenmeyle ilgili bir yaklaşım var.

Ama buradaki kontekste baktığımız zaman, aslında bu, ülkemize yapılan saldırıların izdüşümü olarak da yorumlanabilir. Açıkçası ben hep özel sektörde çalıştığım, bu saldırılar da yavaş yavaş daha sofistike hale geldiği ve etkileri arttığı için, yapılabilecek şeyler de arttığı için şöyle bakıyordum: Karşıdakinin bir motivasyonu var, bilgi çalmak. Niye; bilgiyi satar veya "Senden bunu aldım" diye tehdit eder, para kazanır. Ya da eskiden hobi amaçlı zarar veriliyordu. "Musa, Ayşe'yi seviyor" gibi şeyler yazılıyordu. Ama bu kontekste baktığımız zaman, düşman olarak tanımlanan kötü niyetli bir grubun, bir tüzel kişiliğin yaptığı ülke bazında bir faaliyet de olabilir. Bunun ülke çıkarlarına yönelik değil de oradaki bir kurumdan ekonomik kazanç veya bilgi elde etmek amaçlı yapılan bir saldırı olduğunun ayrımı nerede olacak? Çünkü aynı şeyi fiziksel örneği üzerinden de düşünebiliriz. Siber güvenlikte veya dijital dünyada sınır yok ama mesela biri Türkiye'nin sınır ülkelerinden birine gidip oradaki fırından bir ekmek çaldım ya da oradaki banka şubesini soydum dese bu bizim için bir hırsızlık olayı mıdır yoksa daha büyük bir olay mıdır? Veya oradaki ekip uçarak geldi, burada fiziksel olarak bir bankadan veya bir devlet kurumundan bir şey çaldı diyelim. Bu bir hırsızlık mıdır, yoksa bir düşman tarafından veya bilinmeyen bir güç tarafından yapılan askeri bir operasyon mudur? Bu çizgi benim için çok enteresan bir nokta.

Bence finans da, telekom da, bütün özel sektör buna ekonomiktir diye bakıyor. Böyle bakmak zorunda. Nasıl bakarsınız? Ben ne kadar gelir elde ediyorum, bunun ne kadarını itibarımı, güvenliğimi, altyapımı, dijital unsurlarımı korumak için harcıyorum? Bu yönetimin vereceği bir karardır. Yüzde 10'unu harcıyorsa, o zaman onun için 100 bin dolardır. 100 bin dolarla ne kadar güvenlik yapabiliyorsam o kadar yaparım diye bakacaktır. Çünkü daha fazlasını yapması anlamsız, işi kapatır. O zaman da gündeme ne geliyor? Ben kaç tane adam alırım buraya? Üç kişi alıyor, koyuyor oraya. Bu yeterli mi, değil. Neyin yeterli olduğunu bilmiyoruz. Ama ne kadarının yeterli olacağını düşünmeye gerek yok çünkü zaten hiçbir zaman o bütçeye sahip değiliz, hiçbir zaman öyle bir yatırım yapmak istemeyiz. O yatırımı, oradaki bilgi birikimini, oradaki süreçleri oturtacak zamanımız, enerjimiz yok gibi unsurlar devreye girecek. O yüzden birçok sektörde gerektiği kadar güvenlik, yapabildiğimiz kadar güvenlik, "Bizim çocuklar hallediyordur" kadar güvenlik anlayışı hakim oluyor. Devlet kurumlarına baktığımız zaman da konuya "Bize kadro vermiyorlar ki, kadro kesintisi var" veya "Sözleşmeli aldık, iki tane canavar arkadaş var, onlar her şeyi yapsın" şeklinde yaklaşıldığını görüyoruz. Devlet kurumunun ne kadar güvenliğe ihtiyacı olduğuna bakmak yerine, eldeki kadro, bütçe, kurum bütçesinden bilgi sistemlerine ayrılan bütçenin içerisindeki güvenlik payı gibi konular etrafında insanlar hareket etmeyi tercih ediyor. Daha üst bir bakışla bakıp "Bunlar bizim için kritik kurumlardır, bunlar bu şekilde davranmalı" gibi düşünen uzmanlarımız var ama bunun

pratiğe ne kadar inebileceği zor bir konu. Kaynak yetersizliği veya buraya kaynak ayırmamak tercihi sebebiyle de insanlar sıkışıyor.

Yönetimler güvenliğin kendileri için ne kadar önemli olduğunu anlamaya çalışıyor ama işlerini devam ettirecek kadar. Bilinmeyen bir tehdide karşı kimse korunmaya çalışmıyor çünkü insanlar korunamayacağını biliyor. "Bir devlet beni hedef alırsa zaten yapar" diye düşünüyorlar. İnsanlar "Finansal motivasyonu olan biri için en aşağıda duran meyve olmayayım, bana gelmesin de başkasına gitsin modunda davranıyor ve dışarıdan bakıldığında biraz daha dişli görünmeye çalışayım" diye düşünüyor. Mesela "Biz çok iyi güvenlik yapıyoruz, en iyi güvenlik operasyonu bizde" diye kimse beyanat vermez. Niye vermez? Hedef olmamak için vermez. Biraz daha gözükmeyelim, alçakgönüllü olalım. Bize kimler gelebilir? Buna ne kadar hazır olabiliriz, elimizden geleni yapalım şeklinde kalıyorlar. Burada Attila Hocamızın söylediği bilgi paylaşımı önemli. Ben o örneği şöyle veriyorum: Mesela ben kötü niyetli bir vatandaşım diyelim; çok bilinen bir platformla ilgili bir açıklık buldum, o açıklığı sömürecek bir kod yazdım. Bunu satmaya kalkışırsam birkaç milyon dolar değeri var piyasada. Niye? Çünkü bunu alanlar kullanabiliyor. Ama ben bunu satmayıp kullanmaya karar verdim. Diyelim ki finans sektörüyle ilgili, swift sistemine yönelik bir atak. 10 bin tane hedefleyeceğim banka var, Kodum hazır, kaç tanesine hemen aynı anda operasyon yapabilirim? Üç tane, bilemediniz beş tane. Aslında ben bu beş tanede amacıma ulaşmak için belki haftalar, belki aylarca çalışacağım. Geri kalan 9.995 banka için bir şey yapmayacağım şu an. Bu beş bankanın iki tanesinde hedefime ulaşırsam, üç tanesinde yakalanırsam ne olacak? Aslında bu yakalandığım an, yakalandığım zaman diliminde artık kimsenin bilmediği zararlı bir kod olmayacak ortada. O bilinen, yeni çıkmış bir teknik olacak. Oradaki paylaşım önemli oluyor. "Biz böyle bir teknik bulduk, böyle bir şey keşfettik altyapımızda" diye bu insanlar konuşmaya başlarsa geri kalan 9.995 tane banka bu teknikten etkilenmeyebilir. Çünkü onu öğrenip ona bağışıklık kazanmak için gerekli çabayı sarf edebilirler. O yüzden aslında iletişimi paylaşmak değerli bir şey. Ama diğer taraftan da paylaşmak zor bir şey. Mesela ben ABD'ye her gittiğimde büyük güvenlik üreticileriyle konuşuyorum; "Bizimle niye paylaşmıyorsunuz, zararlı

"Bence finans da, Telekom da, bütün özel sektör buna ekonomiktir diye bakıyor. Böyle bakmak zorunda. Nasıl bakarsınız? Ben ne kadar gelir elde ediyorum, bunun ne kadarını itibarımı, güvenliğimi, altyapımı, dijital unsurlarımı korumak için harcıyorum? Bu yönetimin vereceği bir karardır. Yüzde 10'unu harcıyorsa, o zaman onun için 100 bin dolardır. 100 bin dolarla ne kadar güvenlik yapabiliyorsam o kadar yaparım diye bakacaktır. Çünkü daha fazlasını yapması anlamsız, işi kapatır. O yüzden birçok sektörde gerektiği kadar güvenlik, yapabildiğimiz kadar güvenlik, 'Bizim çocuklar hallediyordur' kadar güvenlik anlayışı hakim oluyor. Devlet kurumlarına baktığımız zaman da konuya 'Bize kadro vermiyorlar ki, kadro kesintisi var' veya 'Sözleşmeli aldık, iki tane canavar arkadaş var, onlar her şeyi yapsın' şeklinde yaklaşıldığını görüyoruz."

Volkan ERTÜRK

bulduğunuz dosyaları bizimle paylaşırsanız aslında biz de öğreniriz" diyorum. Çünkü onların böyle paylaşım ortamları var. Dört, beş kurum bir araya geliyor. Her gün bir milyon tane dosya paylaşırsanız sizi oraya alıyorlar. Orada da şunu öğrendim. Aslında paylaştıkları müşterilerinin bazı bilgileri kritik oluyor çünkü *false positive* oluyor. Bunun içinde zararlı var diyor, adamın gerçekten bir standart word dokümanı, içindeki makro yanlış algılanmış. Aslında o paylaşımın içinde gerçekten Kişisel Verilerin Korunması Kanunu'nu (KVKK) etkileyebilecek veya belki kurumun ticari konumunu etkileyebilecek içerikler de olabiliyor. Yani zor bir konu. Biz her zaman haklı olmak zorundayız, biz her zaman doğru olmak zorundayız ki kalemizi koruyalım. Biraz daha üst akılla, üst bakış açısıyla belki önü alınabilir.

Kadir Murat BİÇER

Ben öncelikle ülkedeki siber güvenliğe bakış açısı için bir terim kullanmak istiyorum. İngilizce Türkçe karışık olacak biraz: "*Musibet based security*". Genelde bizdeki güvenlik anlayışında, başımıza bir olay geldikten sonra önlem alıyoruz ve musibetten sonra neler yapabileceğimizi değerlendiriyoruz. Musibetten önce neler yapılabileceğiyle ilgili Volkan Bey'in de özetlediği gibi üzerimizdeki bütçe, personel ve iş yükünün mümkün olduğu kadar fazla artmamasına yönelik konseptlerle ilerliyoruz. Sektörlerden hangisi kritik altyapıdır, hangisi devlet adına önemlidir, hangisi ne kadar etkilenirse devletin milli güvenliği veya devletin bekası o kadar etkilenir gibi bir ayrım çok zor. Geçmiş dönemde Estonya'daki saldırılar finans ağırlıklıydı ve devletin işleyişini etkiledi. Finans da etkileyecektir. Onun haricinde kamu kurumlarını da etkileyecektir. Emniyet ve güvenlik kuvvetlerini etkileyecektir ki en çok etkilenecek olanların başında enerji sektörü vardır. Bu anlamda genel olarak bizim kendi bakış açımızda STM Siber Füzyon Merkezi içerisindeki üç merkezden biri olan Siber İstihbarat Merkezi tarafında kamuya ait bazı bulgu ve bilgileri alıyoruz ve ilgili birimlerle de paylaşıyoruz. Ama bütün sektörün temsilcilerinin verileri ortak bir alanda paylaşmasıyla ilgili bir regülasyon olması veya talep gelmesi gerekir. Yoksa zaten bilgilerin "*need to know, need to share*" mantığında paylaşılmasında sıkıntı yok.

Siber istihbarat tarafıyla ilgili özellikle ilgi alanımıza giren, yani kapsamı belirleme, kapsamı küçültme anlamında baktığımız zaman genelde gov.tr, edu.tr, pol.tr, tsk.tr gibi biraz da kamu tarafında itibar kaybına sebep olabilecek veya kamu tarafında gizliliğin engellenmesine sebep olabilecek olayların tespiti, bunlara yönelik varsa bir aktivite, varsa bir grup, varsa farklı bir zararlı, bunların bilinip ilgili birimlerle paylaşılmasına yönelik bir efor paylaşılıyor. Siber istihbaratın burada önemli olduğunu da bazı olayların erken haber alınıp verilmesiyle görmüş bulunmaktayız. Mümkün olduğu kadar veri paylaşımı önemli ama kurumlar tarafında da siber istihbarata, özellikle siber tehdit istihbaratına önem verilmesi ve güvenlik anlayışında sadece interaktif ve reaktif

olunmamalı, aynı zamanda proaktif de yaklaşılmalıdır. Çoğunlukla İnteraktif güvenlik bileşenleri var. Mevcut duruma göre bir olay tespit ediliyor ve reaktif olarak da olaya müdahale ve diğer işlemler yapılıyor. Burada proaktif olarak istihbarat verisiyle beraber bu işlemlerin yapılabilmesini tavsiye ediyoruz.

Bununla birlikte farklı sektörlerde farklı etkileri bulunmaktadır. Biraz önce söylediğimiz gibi geçmiş dönemdeki etkileri, mesela finans sektörüyle ilgili etkileri Estonya'da görüldü. Sağlık sektörüyle ilgili geçtiğimiz dönemde yaşanan Wannacry vakasıyla İngiltere'de birçok hastanede ameliyatlar yapılamadı ve sağlık sektörü direkt etkilendi. İngiltere ondan sonra sağlık sektörü tarafında olay olduktan sonra güvenlikçi personelin segmantasyon yapması gibi ilgili verileri kontrollü işlemeye başladı. İngiltere'deki sağlık olaylarından sonra segmantasyonlar yapıldı. Ama biraz önceki konuşmalarda gündeme geldi, Türkiye sağlık sektörü içerisinde benzer segmantasyonlar henüz tam olarak oturmamış durumda. Onu da bir başka projemiz içinde görüyoruz ve onları da zaten ilgili birimlerle paylaşıyoruz. Bunun haricinde, enerji sektöründeki saldırılar; -Ukrayna Kırım tarafındaki saldırılar gibi bundan birkaç ay öncesine kadar devam eden ve birkaç aydır biraz daha durağan olan Venezuela tarafındaki enerji santrallerindeki saldırılar ki Venezuela'nın içinde bulunduğu politik durumdan kaynaklandığı belirtiliyor, Veya herkesin çok çok iyi bildiği, Stuxnet tarafından nükleer santrallerde yapılan saldırılar- direkt milli güvenliği etkileyebilen saldırılar. Ama burada, hangi sektör milli güvenliği en çok etkiler, hangisi etkilemez boyutunda ayrım yapmak çok zor. O kapsamı belirlemek için de ülkemizde teşkilatlar, kuruluşlar, organizasyonlar da oluştu. Ulusal Siber Olaylara Müdahale Merkezi var; BTK bünyesinde görev yapıyor. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi çalışmalar yapıyor. Siber Güvenlik Kümelenmesi çalışmalar yapıyor. Bu anlamda, farklı gruplarla ele alınabilmesi ve artık son dönemde sıklıkla duyduğumuz "Cyber hygiene" konseptinde bu kritik kurumların güvenlik altyapılarının iyileştirilebilmesini önerebilirim.

Biraz önceki konuya ilave olarak, Kubilay Bey'in bahsettiği özel kuvvetler mantığında siber operasyon birliklerine bakış açısı mantık olarak güzel bir bakış açısı ama geçmişte piyade subayı ve hudutta çalışmış birisi olarak hudut güvenliğini unutmamak lazım derim. Yani özel kuvvetçi olacak ama hududa bakan biri de olacak. Yani hududa bakan birisi olmazsa özel kuvvetler tek başına yeterli olmaz, ne zaman ve hangi konumda görev alınacağını bilemez. Yani biz gözleme ve izlemeyi iyi yapabilmeliyiz ki, operasyon birliği, siber güvenlik operasyon kuvveti, kendine düşen görevi daha iyi ortaya çıkarabilsin.

(E) Albay Kani HACIPAŞAOĞLU

Olayı siber güvenliğin, siber savunmanın da ötesinde devlet olarak daha kapsamlı görmek lazım. Mesela şu anda *Cooperative Cyber Defence Centre of Excellence* (CCD COE)'da, milli olarak ülkelerin katılımıyla uluslararası bir organizasyonda yapılan siber güvenlik tatbikatları var; ama sözkonusu topyekûn ülke güvenliği olunca konuya daha önce açıkladığım şekilde daha yukarıdan ve çok daha kapsamlı bakmak gerekiyor. Bir sıcak savaştan önce kriz yönetim durumu olduğuna, devletin bütün teşkilatlarının bu kriz yönetiminin içinde olması gerektiğine, o kapsamda siber saldırılar, savunmalar planlanması ve icra edilmesi gerektiğine ve gerçekten bu şekilde uygulandığı zaman

> *"Sektörlerden hangisi kritik altyapıdır, hangisi devlet adına önemlidir, hangisi ne kadar etkilenirse devletin milli güvenliği veya devletin bekası o kadar etkilenir gibi bir ayrım çok zor. Finans etkileyecektir. Kamu kurumlarını da etkileyecektir. Emniyet ve güvenlik kuvvetlerini etkileyecektir ki en çok etkileyeceklerin başında enerji sektörü vardır."*
>
> **Kadir Murat BİÇER**

bizim şu anda yapmak istediğimiz siber tatbikatların, eğitimlerin veya saldırıların anlamının çok daha güzel çıkacağına inanıyorum. Bu doğrultuda, en kritik alanlardan biri "siber tehdit" istihbaratının olabildiğince ulusal olarak üretilip dışarıya olan bağımlılığımızın en aza indirilmesidir. Bunu HAVELSAN'da Siber Güvenlik Direktörüyken; 15 Temmuz 2016'dan 15 gün sonra, "*CIA registered*" bir Amerikan siber güvenlik firması olan FireEye ile birlikte iş ortakları olan ve siber tehdit istihbaratı üzerine yoğunlaşmış olan EyeSight firmasını ortak iş fırsatları konusunda ziyaret için gittiğimiz İrlanda'da çok net anladık. Özetle, tüm müşterilerinin bilişim sistemlerini siber tehdit ve saldırılara karşı izleyip korurken elde ettikleri çok değerli siber saldırı bilgileri öncelikle ABD istihbaratına akıyor; ticari bölümünde de uygun gördükleri kadarı çok yüksek maliyetlerle müşterilerine yıllık lisans ücreti karşılığı pazarlanıyor, hem de sizin sistemlerinize bağlanılarak... Bu durumu en kısa zamanda mümkünse ortadan kaldırmak, değilse en aza indirgemek zorundayız. Diğer bir ifadeyle, değişik siber tehdit ve saldırı bilgilerini oluşturan veritabanlarını biz geliştirip hizmete sunmalıyız; bunu yapabildiğimiz an gerçek anlamda "yerli ve milli" bir ürün ortaya koymuş oluruz.

Dr. Attila ÖZGİT

O günkü saldırıyı incelerken, birkaç operasyonel bilgiyi ayrıntılı vermek istiyorum. Trafik yönlendirmede çok temel bir konu vardır, teknik olarak *ingress egress filtering* deniyor. *Router*'ınıza giren trafiğin sizin *domain*'inize doğru geri ittiriyor olması lazım. Bu paketlerin içinde size doğru olduğunun gösterilmesi lazım. Dışarı çıkan paketlerin de sizin IP'lerinizden çıkması lazım ve bunun giriş çıkış denetim filtrelerinin olması lazım. Bunun olmaması nedeniyle trafiğin yaklaşık yüzde 35'i bu şekliyle Türkiye'nin içinde başımıza beladır. Bunu sonra operatörlerle konuştuk. Türk Telekom'un altyapısı, tabii muhtemelen teknolojinin de zaman içinde hızlı evrilmesi nedeniyle çok sistematik yapılmış değil. Doğal olarak bir şeyin üstüne biraz daha koyuyorsunuz ve birtakım teknik adamlar IP altyapısının *network* segmantasyonlarının hangi IP'lerden, nereden nereye nasıl geçeceğiyle ilgili planlamalar yapıyorlar. Bence hepsi transitti ama Türk Telekom altını çize çize "Biz transit operatörüz, sadece Türkiye trafiği taşımıyoruz, dolayısıyla giren çıkan transit trafikse biz buna karışamayız" diyordu. Ama bunu da anlamanın yolu var. Transit trafiğini öyle bir yere *network partition* yaparsın ki oradan geçirirken

istiyorsan o kuralları uygulamayabilirsin. Ama hiçbir yerde bu filtreleme yok. Şimdi gerekçe şu: "Biz transit operatörüz, biz böyle bir şey yapamayız." Ancak cevap bu değil. Teknik bir adam oturacak, Türkiye çapında çok büyük bir IP *network*'ü tekrar *ingress egress filtering*'e uygun bir şekilde bir yapılandıracak. Teknik adam doğal olarak bu işten kaçıyor. Belki kendi de haklı. "Günlük zaten 40 bin tane derdim var, tutup bir de böyle büyük bir lokmayla uğraşmaya kalkarsam ben bunun altından nasıl kalkarım" diye düşünüyor. Ama pratik olarak sonuç; emniyetin içinde, Türk Telekom'un içinde değişik yerlerde kendi kendine saldırılar başlıyor. Emniyetten bize o dönemde bir yazı geldi, "ODTÜ'den bize saldırıyor musunuz, çok acele cevap verin" diyor. Hayır, ele geçen bot'lar tamamen sahte paketler yaratıyorlar, *spoof* paketlerin tümü faraş gibi geçiyor Türk Telekom *network*'ünden. Bu bile bana sorarsanız bugün hâlâ Türkiye'nin temel sorunu. Çünkü büyük ölçekli bir saldırı başladığı anda bu yeteneğin olmaması arka planda inanılmaz bir arka plan gürültüsü yaratıyor. Bu durumu anlatmaya çalıştık ama hâlâ bundan bir ders alınmadığını düşünüyorum. Bunun özeti şu: ODTÜ kapısına koyduğu bir cihaza filtreleme yapmalı. İçeri giren paketin hedef adresi içerideki ODTÜ adresi olmalıdır, ODTÜ'den dışarıya çıkan bir paketin kaynak adresi mutlaka ODTÜ'lü olmalıdır. Siz bu filtrelemeyi yaptığınız zaman içinizden dışarıya *spoof* paket yollamazsınız. Herkes kapısının önünü bu biçimde süpürdüğü zaman söylediğim bu arka plan gürültüsü çok çok azalır ki kriz durumlarında zaten *signal/noise* arasındaki farkı anlayabilmek için de vakit harcıyorsunuz.

IP based DNS kullanmayan, başka protokol kullanmayan *IP based* bir plan olması lazım çünkü DNS kriz durumunda ayağınıza dolanıyor. Bir yere *DNS request* kullanıyorsunuz, cevap alamıyorsunuz. Cevap alamadığınız için bekliyorsunuz. Biz bunu nereden öğrendik? Kendi iç *network*'ümüzde trafik istatistikleri üreten ve her beş dakikada bir değişik trafik karakteristiklerini bize yollayan yazılım çalışmamaya başladı. Çünkü DNS *resolution* yapıyordu. Sözel telefon iletişimi bu durumlarda inanılmaz sıkıntılı bir şey. Çok sayıda adamın birbirleriyle değişik ikililer halinde konuşmaları ve o konuşmaların sonucunda işlem yapılması ve o işlemlerin yukarıya eksik gedik yansıtılması. Niye derseniz aralarında telefonla konuşurken çok komik bir şey oldu. Artık üzerinden çok vakit geçtiği için konuşabiliyorum, o zamanlar sıkıntılıydı. Turkcell'in bir mühendisiyle arada konuşulurken şöyle gözlem anlatılıyor: Gözlemde "şu boy paketler alıyoruz" deniyor. Karşı taraftaki mühendis "o boydaki paketleri drop et" diye bir kural koyuyor. Bir kere çok hızlı verilmiş bir karar. Analiz etmek lazım. Turkcell'in DNS *request*'lerine giden boy, turkcell.com.tr ve kendisini *resolve* edememeye başladı. Dolayısıyla telefon iletişimi dünyanın bu tür durumlarda bence kaçınılması gereken bir durum. Saldırı yüzeyini genişletmek için her kurumun bir *contingency* planının olması lazım. Çünkü özellikle DDOS türü yerlerde saldırı belli noktalara yoğunlaşıyor. O noktaların, o makinelerin *float* edebilmesi, hızlıca IP değiştirebilmesi, o makinelerden çok sayıda alınması, böylece karşı tarafın işini iyice zorlaştırma gibi yöntemlerin çok önceden planlanmış ve kenarda hazır vaziyette bekler olması lazım. Koordinasyon çok önemli.

(E) Korgeneral Alpaslan ERDOĞAN

Dünya siber güvenliği nasıl takip ediyor, bu konuda en gelişmiş ülkeler ve güvenlik uygulamaları nelerdir, uluslararası teşkilatlarla siber harekât ya da siber operasyon işbirlikleri nasıl yürütülmektedir? Görüşlerinizi rica ediyoruz.

Mustafa ÖZÇELİK

İlk oturumda kavramları konuştuk. Sınır kavramının değiştiği aşikâr. Yani konvansiyonel anlamda sınır ortadan kalktı. Hepimiz IoT'yi konuşuyoruz. Cihazlarımızı bireyler olarak aslında hepimiz kendi organizasyonlarımızda kullanıyoruz. Hepsi sınırın bir muhatabı oldu. Olayın savunma tarafında muhataplar böyle. Saldırı tarafında da aslında muhataplarda inanılmaz bir değişim var. Konvansiyonel anlamda saldırı ve savaş bakımından devletleri konuştuk, biraz terörizm

konuşuldu. Kubilay Bey terörizmden daha öngörülemez bir şey olarak bahsetti, kesinlikle katılıyorum. Terörizmde dahi aslında muhatabınız belli. Ama siber saldırılarda muhatap da inanılmaz bir belirsizlik içinde. Tabii bütün bunlar hepimiz için daha öngörülmesi zor bir sonuç doğuruyor. Tabii bu devletler açısından. Organizasyonlar ya da bireyler açısından baktığınızda ciddi bir tehdit algısı oluşturuyor. Tabii tehdit ve fırsat kavramları birbirini tetikleyen şeyler. Tehdit ne kadar büyükse üreticiler anlamında, şirketler anlamında aslında müthiş büyük bir pazarın ortaya çıktığı aşikâr. Bugün siber güvenlikle ilgili yapılan harcamalarda projeksiyon olarak trilyon dolarları konuşmaya başladık ve bu bakımdan inanılmaz eksponansiyel bir artış var. Tabii dünyadaki hazırlık seviyelerine baktığımızda NATO'dan örnekler verildi, bir miktar ABD'yi konuştuk. Olayı Doğu ve Batı biraz farklı algılıyor. Bir soğuk savaş devam ediyor. Savaş ve barış kavramları da çok iç içe geçmiş durumda. Bugün NATO'daki toplantılarda - Doğu Bloku çok açık bir şekilde bir tehdit olarak algılanıyor; Doğu tarafına gittiğinizde de Batı inanılmaz bir tehdit olarak algılanıyor. Geriye kalan bölge de aslında savaşın daha fazla cereyan ettiği bir bölge. Ukrayna'yı konuştuk, belki İran'ı konuşuyoruz. Venezuela aslında caydırıcılık seviyesine ulaşmış büyük aktörlerin savaşlarını icra ettiği yeni alanlar olarak ortaya çıkıyor. Yine Soğuk Savaş döneminden, konvansiyonel bir örnek olacak belki ama bir dönem SSB'de uydu fırlatma işlerinde görev alma imkânı bulmuştum ve Ukrayna'yı ziyaret ettik. Ukrayna, Sovyetler Birliği döneminde roket imalatında önemli bir noktaydı. Dinyeper şehrinde fabrikalarını gezerken dediler ki, "Bizim geliştirdiğimiz bir roket var, Batılılar da şeytan diyor". Şeytan demelerinin sebebi şu: Bu roket, Sovyet rejiminin çok farklı noktalarından çok farklı sensörlerden sürekli veri alıyor, sinyal kesildiği anda bu ABD'nin, Rusya'ya inanılmaz bir füze saldırısı başlattığı, kritik tesislerini vurmaya başladığı anlamına geliyor. Kritik tesislerden o füzeye link koptuğu an, füze havalanıyor. Füze bir yeri vurmak için havalanmıyor. Sadece Rusya Federasyonu'ndaki bütün füzeleri ateşlemek üzere havalanıyor ki birçoğunun nükleer başlığı var, ABD'deki birçok kritik noktayı hedef almış vaziyette. Ben Soğuk Savaş kavramını orada daha iyi hissetmiştim. Çünkü bahsettiğimiz tek bir füze bile ABD'nin bir şehrine inanılmaz tahribat verebilecek. Yani bugün biraz siber güvenlik jargonuyla ddos saldırısı gibi bir durum. Ateşlenen binlerce füzenin yüzde 90'ını bile engelleseniz -ki ABD o dönem o kadar da yetkin değildi- kalan yüzde 10'u ABD'ye inanılmaz tahribatlar verebilecek seviyede. Buradan şu çıkarımı rahatlıkla yapabiliyorsunuz: Evet, Rusya'nın ABD ile, ABD'nin de Rusya ile doğrudan savaşma ihtimali yok. O yüzden savaş başka yerlerde cereyan etti, halen cereyan ediyor. Siber caydırıcılık burada çok önemli bir unsura dönüşüyor. Rusya'yı konvansiyonel anlamda caydırıcı hale getiren, bugün birçok kısıta rağmen dünyada hâlâ söz sahibi yapan şey aslında savunma sanayiindeki üretim kabiliyeti. Yani teknolojik olarak hâlâ dünyaya birçok noktada liderlik yapıyor olması. Mesut Bedri Paşam aslında biraz elektronik harple bağladı. Bugün Suriye'de dünyanın belki de gelmiş geçmiş en büyük elektronik harbi icra ediliyor ve bu harpte ABD'lilerin açıkça söylediği bir şey var: "Ruslar bizden daha iyi durumda. Hatta 10 yıl onların gerisindeyiz. Çünkü şu an birçok sistemi hatta maalesef bizim unsurlarımızı da bir şekilde etki altına almış oluyor.

(E) Korgeneral Alpaslan ERDOĞAN

İsrail'in Suriye'ye karşı icra ettiği elektronik harbi de unutmamak gerekiyor. İsrail çok önemli bir elektronik harp kapasitesi ve yeteneği olan bir ülke. Sık sık hava saldırıları oluyor, gidip istediği noktayı vurup gelebiliyor. Bu da sanki biraz elektronik harbi Rusya'dan daha iyi kullanıyor izlenimi veriyor. Zarar görmeksizin Suriye'nin içerisindeki hedefleri vurup dönebiliyor, orada hava savunma sistemlerini etkisiz hale getirebiliyor. Dolayısıyla elektronik harp deyince İsrail'i de düşünmemiz gerekiyor.

Mustafa ÖZÇELİK

Kesinlikle. Zaten dünyada verilen örneklerden birini de İsrail'e bağlayacağım. Caydırıcılık çok önemli ve bu caydırıcılığı sağlamanız için sizin

teknolojik olarak dünyada liderlik edenler arasına girmeniz gerekiyor. Bu elektronik harpte de böyle, artık siber güvenlikte de böyle. Bunun başka yolu yok. Başkalarının teknolojisini kullanarak sizin dünyada siber güvenlikle ilgili "Ben kendimi güvende hissediyorum" deme ihtimaliniz bulunmuyor. Mesela siber güvenlikte insan boyutunu epey konuştuk. İnsanların bilgi paylaşımını, hazırlık seviyesini artırmasını konuştuk. Aslında bence o konuda hep yine teknolojiye, otomasyona gelip dokunuyor. Bugün 80 milyon Türk insanının hepsinin eline silah versek ve silah kullanmayı öğretsek biz konvansiyonel anlamda ne kadar güçlü bir ülke oluruz, biraz soru işareti. Bir etkisi var mıdır, evet. Ama etkisi neye olur? Bugün bizi Suriye'de iç güvenlik operasyonlarında da etkin kılan nedir diye baktığımızda aslında kendimizin geliştirdiği insansız sistemleri görüyoruz. Burada da teknolojik anlamda odaklanılması gereken konunun işin otomasyon boyutu olduğunu düşünüyorum. Picus, ATAR Labs gibi yerli ürünlerimiz çok güzel örnekler. Tabii dünyada teknolojik anlamda da söz sahibi ülkeler aslında çok iddialı yaklaşıyorlar. Burada İsrail örneğine gelelim. İsrail'e baktığınızda aslında biraz uç bir örnek. Kendisi büyük bir pazar değil ama dünyada siber güvenlik ürünlerine baktığınızda en etkin birkaç ülke arasında yer edinmiş durumda. Bunun altyapısını incelediğinizde dışarıdaki dünyadaki kendi yatırımcılarının bu alana öncelik vermesi, devlet politikası olması gibi çok önemli unsur var ama hepsinin altında İsrail'in bir devlet politikası dahilinde kendi insan kaynağını, kendi ekosistemini, kendi inovasyonunu siber güvenliğe yönlendirmesinin, siber güvenliği öncelik altına almasının yattığını düşünüyorum Aslında teknolojik anlamda yerli ve milli bir hamle yapıyor ve bunu uzun vadeye yayıyor. Rusya için durum biraz daha farklılaşıyor. Pazarda çok etkin değiller ama kendileri zaten bir pazar. Rusya ve Çin örneğine baktığınızda ise bu ülkeleri siber güvenliğin biraz daha istihbaratın kontrolünde gittiği, teknolojiyle istihbaratın biraz tetiklediği bir yer olarak görüyorum. Kurduğumuz temaslarda da bunu ifade ediyorlar, yavaş yavaş bir açılım içerisindeler. Dünyaya teknoloji satma noktasına hazırlanıyorlar. ABD yine her alanda olduğu gibi bu konuda da iddialı. Zaten dünyada yaptığı operasyonlarla da kendi büyük firmalarıyla da bu ligin hâlâ ilk sırasında. Burada Hollanda güzel bir örnek bence. Hollanda'da Hague Security Delta'yı ziyaret etme fırsatımız olmuştu. Hollanda olaya biraz daha *business* gözüyle bakıyor: Dünyadaki siber güvenlikle ilgili startup'ları Hollanda'ya çekme ve bu konuda iddialı bir hub oluşturma noktasında epey yol katetmiş durumdalar. Biz aslında Türkiye olarak neler yapıyoruz, neler yapmalıyız bağlamında düşündüğümüzde aslında bütün bu örneklere baktığımızda ilk olarak milli güvenlik boyutuyla kendi teknolojimizi geliştirmek zorundayız. İkincisi Türkiye'deki tek problemimiz güvenlik problemi değil. Bugün aslında ekonomik krizle boğuşuyoruz, genç nüfusumuzu beyin göçü anlamında dışarıya kaybetmenin verdiği üzüntü var, onu nasıl yönetebileceğimizi konuşuyoruz. Tüm bu sorunlara baktığımızda siber güvenlik aslında birçok problemi çözebilecek yeni nesil bir alan olarak ortaya çıkıyor. Hollanda'yla konuştuğumuzda Haque Security Delta bir rakam vermişti. Haque Security Delta'daki firmalarda kişi başına düşen ciro 2018 rakamıyla 500 bin avro. Bakıldığında inanılmaz bir katma değer. Bizim Türkiye'de en övündüğümüz, teknolojik katma değerimizin en yoğun olduğu savunma sanayiimizdeki rakamlarımızda bunun beşte birine ancak ulaşabiliyoruz. O yüzden Savunma Sanayii Başkanlığımız olarak bu konuda hem güvenliğimizi garanti altına almak hem de dünyada inanılmaz büyüyen bir pazar, genç nüfusun kanalize edilebileceği doğru bir teknolojik alan olduğu bakış açısıyla ekosistemi nasıl geliştirebileceğimize odaklandık ve çeşitli sektörel analizler ve bu konudaki paydaşlarla bir araya gelme neticesinde Türkiye Siber Güvenlik Kümelenmesi oluşumunu doğurdu.

Kümelenme olarak 2017-2018 yıllarında yaptığımız analizlerde şunu gördük: Akademiyle, özel sektörle, kamuyla ayrı ayrı görüştük ve çeşitli problemler aslında ortaya konuldu. Bu problemlerden biri paydaşlar arası etkileşim problemimiz. Yani biz birbirimizi yeterince tanımıyoruz, birbirimizle doğru etkileşim kanalları oluşturamıyoruz ve herkes kendi adacığında kendi dünyasını

"Savunma Sanayii Başkanlığımız olarak bu konuda hem güvenliğimizi garanti altına almak hem de dünyada inanılmaz büyüyen bir pazar, genç nüfusun kanalize edilebileceği doğru bir teknolojik alan olduğu bakış açısıyla ekosistemi nasıl geliştirebileceğimize odaklandık ve çeşitli sektörel analizler ve bu konudaki paydaşlarla bir araya gelme neticesinde Türkiye Siber Güvenlik Kümelenmesi oluşumunu doğurdu. Kümelenme olarak 2017-2018 yıllarında yaptığımız analizlerde şunu gördük: Akademiyle, özel sektörle, kamuyla ayrı ayrı görüştük ve çeşitli problemler ortaya konuldu. Paydaşlar arası etkileşim bir problem olarak çıktı. İnsan kaynağı eksikliğini gidermek ciddi bir ihtiyaç. Kamunun belki kendi kaynakları, kısıtlarıyla da alakalı ama özel sektör de bu problemi yaşıyor. Bir diğeri de sertifikasyon konusuydu."

Mustafa ÖZÇELİK

kurtardığını iddia ediyor. Ama büyük resme baktığımızda aslında birçok kadük yapı görüyoruz. Bunu kamu kurumları için de özel sektör için de akademi için de söyleyebiliriz. İnsan kaynağı eksikliğini gidermek ciddi bir ihtiyaç. Kamunun belki kendi kaynakları, kısıtlarıyla da alakalı ama özel sektör de bu problemi yaşıyor. Bir diğeri de sertifikasyon konusuydu.

(E) Korgeneral Alpaslan ERDOĞAN

Kamu kesimi insan kaynakları konusunda sıkıntı yaşıyor. Kadro ve maaş düşüklüğünün bütçe sıkıntısından dolayı olduğunu biliyoruz da, özel sektördeki sıkıntının sebebi de yine aynı mı, yoksa Volkan Bey'in vurguladığı gibi herkesin düşük bütçeler ayırarak kendisine yeterli emniyeti sağladığı düşüncesi mi?

Mustafa ÖZÇELİK

Aslında buradaki konu finansal kaynaktan ziyade siber güvenliğin çok hızlı büyüyen bir alan olması ve yetişmiş insan kaynağının sadece Türkiye'de değil, tüm dünyada büyük bir problem olması. Kaynağı çekememe bir problem; kamunun, özel sektörün kendi içinde bununla ilgili çözmesi gereken şeyler var ama totalde baktığınızda da, bütün problemlerinizi çözseniz de, iyi maaşlar da verseniz -bütün kamu için söylüyorum- insan kaynağı kısıtı bütün dünyada bir gerçek. Türkiye'nin de bir gerçeği; yetişmiş beyinlerinizin dışarıya kaçmasını engelleyemiyorsunuz. Havuzu bir şekilde doldurmanız gerekiyor ama bir taraftan da boşalıyor, bunu hızlı bir şekilde çözmemiz gerekiyor.

Sertifikasyon konusu da şöyleydi: Diyoruz ki, "yerli milli ürünlerimizi kullanmak zorundayız, teknolojik olarak liderlik etmek zorundayız." Yerli ürünler var mı var. Bugün Türkiye siber güvenlik kümelenmesinde 106 üyeye ulaştık. Bunların hepsi Türkiye'de mühendislik eforu sarf etmiş insanlar. Bunların arasında iyi firmalarımız da var, biraz daha küçük ölçekli firmalar da var ama kullanıcı şunu söylüyor: "Ben yerli bir üreticiye şans veriyorum. Bir ürünle ilgili sorunlar yaşıyorum. Söylediği fonksiyonları yerine getirmediğinin üç, beş ay sonra farkına varıyoruz. Ürün yeterliliği noktasında ciddi problemler yaşıyoruz." İkincisi, "iyi bir mühendislik şirketi, iyi bir ürün ortaya koymuşlar. İhtiyacımıza hızlı cevap veriyor. Bir yıl çok mutluyuz. Ama bir yıl sonra bir sabah uyandığımızda firmanın personeli yok. Neden, firma batmış." Sürdürülebilirlik problemimiz var. Burada da kamu şunu söylüyor: "Bir otorite bunları sertifiye etsin." Yani bu şirket finansal anlamda, süreç yönetimi anlamında, yazılım geliştirme anlamında nasıldır? Ürün güvenilirliği nedir? Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bir genelge yayınladı. (Backdoor) Arka kapı açıklığı var mı yok mu taahhüt altına alalım. Şimdilik belki taahhütle bir adım atıldı, devamı da gelecektir ama bu kamu tarafında ciddi bir endişeydi. Yerli sistem, yerli ürün alıyorum ama bu arka tarafta bir şeyleri tetikliyor mu? Her zaman kötü niyetli olmak zorunda değil. Yani yazılım anlamında iyi bir yazılım geliştirmediyseniz içerisinde zafiyetler

barındırıyor olabilir, sertifikasyonla bundan da emin olmak istiyor.

Özel sektör de problem olarak şunu söyledi: "Ben pazara erişim problemi yaşıyorum. Yerli milli rüzgârı estiği söyleniyor ama o rüzgâr bize dokunmuyor, ben kamuya mal satamıyorum. Kamuya mal satamadığım zaman yurtdışına da satamıyorum. Çünkü yurtdışında bana 'Sen sağlık sektöründe bir satış yapmaya çalışıyorsun ama Türkiye'deki Sağlık Bakanlığına ya da sektörüne satış yaptın mı?' diyorlar." Yapmadığını söylediğinde senden niye alayım sorunsalı yaşanıyor. Bu problemleri adreslemek üzere aslında Türkiye Siber Güvenlik Kümelenmesi faaliyetlerine başladı. Neler yaptığından kısaca bahsedeyim. Bu problemleri adresleyecek başlıkları oluşturduk. Bir de "Biz etkileşim oluşturmalıyız" dedik. Aslında kümelenmelerin bir katalizör olması, arzla talebi birleştiriyor olması gerekiyor. Şimdiye kadar her yıl yaptığımız ve yapmayı planladığımız üç tane zirvemiz var. Zirvelerimiz etkileşim oluşturmadaki ana faaliyetlerimiz. Birincisi, kendi içimizde düzenlediğimiz bir sektör zirvesi. Bir araya gelerek sektörel problemleri masaya yatırıp konuştuğumuz, problem yaşadığımız alanları ve kümeyi tartıştığımız bir zirve. Diğeri kamu siber güvenlik zirvesi. Burada kamuyla sektör unsurlarını bir araya getirip müşteri üretici buluşmasını sağlıyoruz. Üçüncü olarak da Uluslararası Siber Güvenlik ve Savaş Konferansı'nı icra ediyoruz. Bu konferansla uluslararası alanda bir marka olabileceğimize inanıyoruz. SSB himayelerinde bugüne kadar üç kez düzenlenmişti, Kasım 2019'da dördüncüsünü düzenledik. Bundan sonra her yıl tekrar edecek. Bunu yavaş yavaş bir fuara da dönüştürüyoruz ve uluslararası ivme giderek artıyor.

(E) Korgeneral Alpaslan ERDOĞAN

Mustafa Bey, böyle çok kalabalık bir etkinlikte herkes söz alamadığı için belki herkesin sesi duyulamayabilir. Acaba bunu bir haftaya yaysanız, gün gün bölseniz herkes sesini duyurabilse... Böyle bir şey olabilir mi?

Mustafa ÖZÇELİK

Planımız 2020 Kasım ayında, bir hafta boyunca, sadece Ankara'da değil, İstanbul'da da bir Cyber Week yapmak. Mesela bu sene bir hacker konferansını da aynı hafta içerisinde düzenledik. STM'nin CTF programını uluslararası hale getirmekle ilgili STM'yle temaslarımız var. Ülkedeki siber güvenlikle ilgili ön plandaki etkinlikleri bir araya getirdiğimiz, daha ses getirici, uluslararası anlamda da fark oluşturabilecek bir etkinlik düzenleme düşüncemiz var. Etkileşim oluşturmamız bunlarla sınırlı değil, bir de Siber Kafe'miz var. Siber Kafe'deki amacımız da biraz daha alt

segmentlerde buluşmaları sağlamak. Yani biraz daha teknoloji bazlı.

Bugüne kadar ne yaptık? Mesela EPDK ile enerji sektöründe siber güvenlik etkinliği yaptık. 30'un üzerinde enerji dağıtım şirketi geldi. Siber güvenlikteki özellikle de IOT tarafındaki firmalarımızı bir araya getirdik. Finans sektörüne siber güvenlik yaptık. BDDK, İstanbul'da 50 bankayı çağırdı. Bizim de yaklaşık 50 firmamızla katılım anlamında bir ilki gerçekleştirdik. Bunu savunma sanayiinde, adli bilişim tarafında yaptık. Şimdi e-ticaret ve sağlık tarafında devam edeceğiz. Bu silsile devam edecek. Etkileşim oluşturmada küme aslında belirli bir yola girdi. Bu anlamda güzel geribildirimler de var ama daha iyiye gitmesi, sürekli iyileşmesi gerektiğinin farkındayız. Pazara erişim yine önemsediğimiz bir konuydu. Pazara erişimde hem yurtiçi hem yurtdışı pazarla ilgili faaliyetlere başladık. Yurtiçinde kamudaki Bilgi İşlem Daire Başkanlığımıza kümenin tanıtımını yapmayı hedefledik, onları ziyaret ediyoruz. Bir envanter çalışması yaptık. Yine Türkiye'de bir ilk. Bir katalog çıktı. Türkiye Siber Güvenlik Kümelenmesi üyelerinin ürünlerini tek bir katalogda topladık, İngilizce versiyonunu da yaptık. Artık karar alıcıların, sipariş vereceklerin önüne bir katalog koyabilir durumdayız. Online ortamda da bunu paylaşıyoruz.

DMO ile bir işbirliğimiz oldu. DMO'nun tekno kataloğu biliyorsunuz özellikle de yerelde birçok kamu kurumunun doğrudan hızlı bir şekilde alımını sağlıyor ve aslında fena bir kanal değil bakıldığında. Onlarla bir noktaya geldik ama biraz daha iyiye gitmesi gerektiğine inanıyorum. Oradaki konumuz da şu: Tekno kataloğa daha hızlı siber güvenlik ürünlerimizin konulması için bir hamlemiz var. Bir yandan yurtdışını önemsiyoruz. Firmalarımızı yurtdışında fuarlara götürdük. Hollanda'ya, Dubai'ye, çeşitli noktalara gittik, bunlar devam edecek. Burada biraz daha SSB'nin ve özellikle de STM, HAVELSAN dahil olmak üzere savunma sanayiindeki büyük şirketlerimizin de desteklerini almak istiyoruz. Çünkü kümelenme dediğiniz sadece bir kurumun destekleyerek ayakta tutabileceği ya da büyütebileceği bir yapı değil. Aslında bütün unsurların kaslarını kullanarak sinerji oluşturması gereken bir alan. Burada HAVELSAN ve STM'nin özellikle yurtdışındaki kaslarını kullanmaya çalışıyoruz, destek oluyorlar sağ olsunlar. Bu sene hem fuarlar noktasında hem de yurtdışındaki ofisler üzerinden oradaki işlerin takip edilmesiyle yurtiçindeki ürünlerimizi yurtdışına daha fazla konumlandırma gibi düşüncelerimiz var. Çünkü sürdürülebilirlikte çarkın dönmesi için finansın artması gerekiyor. Yeteneğe erişim çok önemli bir konu. Orada üniversitelerle ciddi bir etkileşime girmiş durumdayız. Geçen sene Eylül ayında Ankara'da HAVELSAN, STM ve Siber Savunma Komutanlığımızı ziyarete gittik, 19 üniversiteden siber güvenlik kulüpleri geldi. O gün bizim erişebildiğimiz 19'du, bugün bu sayı 50'ye yaklaştı. 50 üniversitedeki siber kulüplerle işbirliği içerisindeyiz, bir siber güvenlik kulüpler birliği de kurduk. Onların üzerinden 2019 yılında üniversitelerde 2000'in üzerinde öğrenciye siber güvenlikle ilgili çeşitli seminerlerle eğitimler verdik. İstanbul ve Ankara'da daha fazla kesime daha detaylı eğitimler verebilmek için yaz ve kış kampları düzenledik. 2019'un son çeyreğinde Elazığ ve Zonguldak'ta Cyber Anadolu diye bir program başlattık, akabinde Mersin'de ve İzmir'de devam etti. Şimdi farklı illerle devam edecek. Buradaki amacımız da eğitimler ve CTF'i birleştirip bölgedeki yetenekleri keşfetmek. Bölgedeki yetenekleri niye önemsiyoruz? Şöyle bir anekdot anlatmak istiyorum: Geçen sene Elazığ'da bir eğitime gittik. Elazığ Fırat Üniversitesi hem mühendislik konusunda iyi bir üniversite hem de siber güvenlikle ilgili ilk ihtisas programını açmış bir üniversite. Türkiye'de adli bilişimle ilgili altyapıları, hocaları var. Kimin vizyonudur bilmiyorum ama güzel bir noktaya gelmiş bir üniversitemiz ve bu, öğrencilerde de karşılık bulmuş. Anadolu ve özellikle Ankara'daki üniversitelerle de kıyasladığımda öğrenci farkındalığının da yüksek olduğu bir yer. Kocaman bir anfiyi doldurabiliyorlar. Bir akşam eğitimden sonra soru cevap kısmı oldu. Çocuklar akşamın sonunda bize bir hediye takdim ettiler. Hediye şu: Bu arkadaşlar çeşitli bug bounty (ödül avcılığı) programlarına katılıyorlar. Ben açıkçası bayağı etkilenmiştim, o yüzden paylaşmak istiyorum. Facebook veya Starbucks gibi şirketlerin "Benim sistemlerimde bir zafiyet bulursanız size 1000 dolarlık kahve çeki veriyorum, istediğiniz gibi harcayın" gibi programlarını takip edip yarışıyorlar ve buralardan ufak

tefek paralar kazanıyorlar. Bu arkadaşlar buralardan kazandıkları paralarla bizim ekibin adına Türk Silahlı Kuvvetlerini Güçlendirme Vakfına bağışta bulunmuşlar. Bizim isimlerimizin yazdığı vakfın bağış mektubunu bize takdim ettiler. Ben çok etkilendim ve çocuklara şunu söyledim: "Bizim Ankara'dan beklediğimiz tek şey motivasyon." Yani Ankara'dan özellikle devlet yöneticilerinin buraya gelip, "Biz sizin farkınızdayız" demeleri bizim için yeterli. Yoksa herhangi bir eğitici ihtiyacı da duymuyor bu çocuklar. Zaten artık online platformlar var, kendilerini geliştirebiliyorlar ya da zaten para kazanıyorlar. Kazandıkları paraları bu arada şahsi amaçlı da harcamıyorlar. Tamamen üniversitedeki aktivitelere harcıyorlar.

Aslında bunu yetkinliğe erişerek bırakmak istemiyoruz. Fikir marka döngüsünü de oluşturduk. Fikirleri yarıştıralım, yeteneğe erişelim. Çeşitli staj programları da yapıyoruz. Bu yıl kümelenme öğelerinde 100'ün üzerinde öğrenci sektörde staj imkânı buldu. Bunlar firmalarımızda yer alsın, yeni startup'lar oluşturalım. Şu an İstanbul Teknopark'ta yeni yapılan bölümde yaklaşık 2000 metrekarelik bir kuluçka alanını bize tahsis edecekler. 2021 itibariyle tamamen siber güvenlikle ilgili bir kuluçka oluşturacağız. Globalde marka oluşturmak istiyorsak bu tarz adımlar atmalıyız. "2000 metrekareyi nasıl dolduracaksınız" diye sorulabilir ama ben dolduracağımızı düşünüyorum. Doldurduğumuz gün globale çıkmak için daha emin adımlarla gittiğimiz gün olacaktır diye düşünüyorum. Burada vurgulamaya çalıştığım şey şu: Bu işin olmazsa olmazı inovasyon. Dünyada açık inovasyon diye tabir edilen teknolojik dönüşüm artık startup'lar üzerinden gelişiyor. Bizim de kümelenme olarak önem verdiğimiz konu bu inovasyonu geliştirelim, startup sayısını artıralım. Büyük firmalarımızla etkileşim oluşturalım, müşteriyle buluşturalım, büyütelim gibi bir döngümüz de var.

(E) Korgeneral Alpaslan ERDOĞAN

Çok güzel, teşekkürler. Müsaade ederseniz diğer arkadaşlarımız da bu konuda görüşlerini söylesinler. Son sözlerinizi alalım.

Mustafa YILMAZ

Kani Bey de Kadir Murat Bey de siber istihbaratla alakalı önemli bir hususa değindi. Kani Bey'in şöyle bir ifadesi vardı: "Siber istihbarat bilgisi üretmemiz lazım." Bu önemli ve gerçekten çok değerli bir ifade. Biz TR-TEST olarak, SSB'nin başlattığı Türkiye Siber Güvenlik Kümelenmesi, Siber Güvenlik Ürünleri Test ve Sertifikasyon Projesi kapsamında tehdit istihbarat üreticilerini bir araya getiriyoruz. Onların bize toplantının başında söylediği ilk cümle buydu: "Bizim ürünlerimiz siber istihbarat verisi olmadan hiçbir zaman anlamlı bir şeye dönüşmeyecek. Ürünlerimiz, istihbarat verileri ile entegre olunca, bu veriler bize sağlanınca anlamlıdır" diye ifade etmişlerdi. O anlamda destekleyici bir ifade olarak belirtmek istiyorum.

Kamu perspektifinden birkaç hususa değinmek istiyorum. Birlikte çalışabilirlik veya kurumların kendi korumacı politikaları hakikaten zaman zaman ülkemize siber güvenlik stratejisi noktasında sıkıntı oluşturabiliyor. Biz mesela TSE'deyken ülkenin bir hususta dolayı kendi güvenli kripto algoritmalarının bir listesini çıkartmak gerekiyor dediğimizde çok parçalı bir yapı olmasından dolayı zaman zaman muhatap bulamadığımız durumlar olabiliyordu. Şöyle düşünüyorum, bir strateji belgesi üretme noktasında ülke olarak çok büyük bir sıkıntı yaşamıyoruz ama strateji belgelerinin

"Bu işin olmazsa olmazı inovasyon. Dünyada açık inovasyon diye tabir edilen teknolojik dönüşüm artık startup'lar üzerinden gelişiyor. Bizim de kümelenme olarak önem verdiğimiz konu bu inovasyonu geliştirelim, startup sayısını artıralım. Büyük firmalarımızla etkileşim oluşturalım, müşteriyle buluşturalım, büyütelim gibi bir döngümüz de var. "

Mustafa ÖZÇELİK

uygulanabilirliği, denetlenmesi, burada belirtilen görevlerin idamesi noktasında sıkıntı yaşıyoruz. Cumhurbaşkanlığı Dijital Dönüşüm Ofisiyle birlikte bunların biraz toparlanıp tek bir yapıdan yürütülmesinin faydalı olacağını düşünüyoruz.

Bu sorunuza özellikle standart boyutuyla değinmek istiyorum. Uluslararası teşkilatlarla standart boyutuyla işbirliğine baktığımızda aslında bunun çalışmaları çok önceden yapılmış. *Common Criteria* denilen bir standarttan bahsedeceğim. ISO / IEC 15408 diye geçen bir standart. *Common Criteria* Türkçeye "Ortak Kriterler" diye çevrilmiş. Burada ülkelerin aslında çıkış noktası şu: Avrupa'da ITSEC var. Yani kendi güvenlik standartları var. ABD'de yanlış hatırlamıyorsam TCSEC, Kanada'da CTCPEC gibi standartlar var. Avrupa'daki bir üretici ITSEC'ten giriyor, benim ürünüm güvenli diye bir sertifika alıyor ama bunu ABD'ye satmak istediği zaman -20,30 yıl önceden bahsediyorum- şöyle bir şeyle karşılaşıyordu: "Avrupa'da ITSEC'ten almışsın ama benim

"Kamu perspektifinde, birlikte çalışabilirlik veya kurumların kendi korumacı politikaları hakikaten zaman zaman ülkemize siber güvenlik stratejisi noktasında sıkıntı oluşturabiliyor. TSE'deyken ülkenin bir hususta dolayı kendi güvenli kripto algoritmalarının bir listesini çıkartmak gerekiyor dediğimizde çok parçalı bir yapı olmasından dolayı zaman zaman muhatap bulamadığımız durumlar olabiliyordu. Şöyle düşünüyorum, bir strateji belgesi üretme noktasında ülke olarak çok büyük bir sıkıntı yaşamıyoruz ama strateji belgelerinin uygulanabilirliği, denetlenmesi, burada belirtilen görevlerin idamesi noktasında sıkıntı yaşıyoruz."

Mustafa YILMAZ

ülkemde de TCSEC diye bir standart var, bundan da geçmen lazım." Dolayısıyla bu üreticilerin emek, zaman, maliyet israfına yol açıyor. Aynı şekilde ABD'deki bir üretici de Avrupa'ya gittiğinde, "Bizim ITSEC var, hele bundan bir geç" yaklaşımı vardı. Ülkeler, "Biz bir araya gelelim, ortak bir kriter oluşturalım ve bu ülkedeki standart gereksinimlerini bunun içine koyalım" demişler ve "Ortak Kriterler" adı verilen ortak bir standart oluşturmuşlar. Bu anlamda da bir uluslararası anlaşma imzalamışlar ve 31 ülke bu anlaşmaya taraf. Yanlış hatırlamıyorsam BM'nin kabul ettiği 180 civarı ülke var. Bu anlaşmayı imzalayan 31 ülke ama bu 31 ülkenin profiline baktığımızda dünyaya yön veren ülkeler olduğunu görüyoruz. Birkaç örnek vereyim, Amerika kıtasında ABD, Kanada, Avrupa'ya geldiğimizde İngiltere, Fransa, Almanya, Hollanda, İspanya, İsveç gibi ülkeler var. Türkiye var. Asya tarafında Güney Kore, Japonya, Singapur, Malezya, Hindistan gibi ülkeler bu anlaşmaya taraf. Ve burada da sertifika üretici ülke ve sertifika tüketici ülke diye ikili bir yapı var. Türkçeye biraz değişik çevrilmiş. Yani kimi ülkelerin verdiği sertifikalar bu anlaşmaya taraf olan 31 ülkede belirli bir seviyeye kadar tanınıyor. Kimilerinin verdiği sertifikalar da sadece ulusal bazda tanınıyor. Onlar da belli bir denetimden geçtikten sonra sertifika üretici ülke konumuna gelebiliyor. Türkiye olarak bu anlamda iyiyiz, onu söyleyebilirim. Ülkemiz tarafından verilen sertifikalar 31 ülkede belirli bir seviyeye kadar geçerli, tanınan konumdayız.

(E) Korgeneral Alpaslan ERDOĞAN

Burada yetkili kurum kim? TSE mi?

Mustafa YILMAZ

Burada yetkili TSE ve onun dışında da başka bir yer de olamaz. Çünkü sebebi de şu: Uluslararası anlaşmada, "bunu bir hükümet kuruluşu yapar" diyor. Zamanında TSE tarafından imzalanmış ve bu anlaşmaya taraf olunmuş, aktif bir şekilde faaliyetler yürütülüyor.

(E) Korgeneral Alpaslan ERDOĞAN

Peki, TR-TEST'in konumunu burada nasıl oturtacağız?

Mustafa YILMAZ

Birazdan ona geleceğim. TR-TEST yerli üreticilerle alakalı çalışma yapıyor. Ortak Kriterler, uluslararası anlamda bilgi teknolojileri ürün güvenliği işbirliği anlamında en fazla kabul görmüş bir çalışma. Bir de şunu söyleyeyim, uluslararası anlamda bu işe önem verilmesi noktasında da ilginç. Daha önceki görevim itibarıyla zaman zaman bizimle aynı işleri yapan yerlere denetime gittiğimde şunu görmüştüm. Mesela Güney Kore'de bu organizasyonun bende bıraktığı algı bizim TÜBİTAK benzeri bir yapımız ile onların istihbarat ajansının birleşimi olan bir yapı kurmuşlar ve bu faaliyetleri onlar yapıyor. Yanlış hatırlamıyorsam Güney Kore'nin Ulusal Siber Güvenlik Stratejisi 2006 yılında çıkmıştı. Ben gittiğimde 2011 yılıydı ve bizim hâlâ çıkmamıştı. Bizde 2013'te çıktı. Mesela İspanya'da faaliyetleri, onların istihbarat ajansı içerisinde kurdukları bir yapı yapıyordu. Hatta denetimlerde biz CV'leri incelemeyi talep ettiğimizde, istihbarat olduğundan dolayı dosyaları bize bırakmıyorlardı, takip ediyorlardı. Orada Ortak Kriter belgesine imza atan kişi bakan düzeyindeydi. Ve biz şaşırdık, çünkü bizde bir müdür atıyor. Ve resmi gazetelerinde yayınlanıyor o belge. Almanya örneğine geçersek, orada da BSI diye bir yapı var. BSI da büyük bir siber güvenlik enstitüsü. Bizim bu yaptığımız işi yapan belki 20 kişilik bir ekip var ama genel anlamda tüm ülkenin siber güvenliğine yön veren çalışmalar yapıyorlar. Tabii Avrupa ülkelerinin ayrıca bu standartlar noktasında işbirliği anlamında SOGIS denilen bir yapıları var. SOGIS noktasında bilgilerini karşılıklı olarak belirli bir seviyeye kadar tanıyorlar. Her ne kadar buralar teknik alan deseler de biraz politik durumlar da oluyor. Mesela şöyle bir şey olmuştu: "SOGIS'e biz de girelim Türkiye olarak" dediğimizde toplantılarda biraz "*This is not a political issue*" deseler de bize *off the record* olarak,

"Siz AB ülkesi değilsiniz o yüzden zor" diyorlardı. Öyle yapılar var.

Ülkeler dünyada siber güvenliği nasıl takip ediyorlar noktasında İsrail'den çok bahsedildi. İsrail ile ilgili hususta bu anlamda bir tez bulmuştum. Sadece birkaç cümleyi okumak istiyorum. Özellikle dünyada siber güvenlikte en iyi olan ülkeler olarak genel itibariyle ABD, Rusya, Çin, İsrail gösteriliyor. "Dünyada en iyi siber güvenlik ve savunma stratejisine sahip ülkelerden biri olarak kabul edilen İsrail siber saldırılarla mücadele konusunda askeri ve istihbarat kaynaklarının imkân ve kabiliyetlerini birleştirmiştir. İsrail kritik hükümet sistemlerinin herhangi bir siber tehditten etkilenmemesi için iç ağ, intranet gibi internetten bağımsız olarak çalışabilen ve genellikle hassas ve gizli bilgileri taşıyan ağlar üzerinde çalışmaktadır" diyor. İlk oturumda biraz konuşulmuştu. "Uzun süredir siber savaş kapasitesine sahip askeri birlikler yetiştiren İsrail, siber savaşçılarını sadece teknik bilgi düzeylerine bakarak değil aynı zamanda fiziksel savaşma yeteneklerine bakarak seçmektedir. Seçilen siber komandolar hedef ülke içerisine sızarak gerektiğinde düşman teknolojisinin keşfini yapabilecek doğru hedefleri bulup fiziksel tahribat yapabilecek şekilde yetiştirilmektedir."

(E) Korgeneral Alpaslan ERDOĞAN

Burada Kubilay Bey'in söylediği yere geldik işte.

Kubilay Onur GÜNGÖR

Bir parantez açayım mı? Bu bahsedilen kurum Unit 8200 diye geçiyor İsrail'de. Unit 8200'den ben pek çok insanla görüştüm yurtdışında. Bizim sertifikalarımızla ilgilenmişlerdi, hatta bir dönem de bağlantıda olan bir firma partnerlik için görüşmek istemişti. Fakat o zaman Mavi Marmara vs. olduğu için ben de kabul edemedim; konjonktür de uygun değil demiştim. Onların kabul ettiği şey şu: Cyber Struggle'ın multidisipliner siber komando tanımlaması, şu an yeryüzünün en iyi eğitimi. Henüz Unit 8200 bu aşamada değil. Ayrıca onlar zaten askeri personel için bu çok disiplinli sistemi kullanmakta. Daha sonra buradan çıkan kişilerin globalde desteklenmesiyle çeşitli markalar oluşturulmakta. Bunu kendileri de söylüyorlar. ABD Navy Seals da aynı şeyi söylüyor. Henüz Türkiye'ye söyletemedik ama bir ara söyleyecektir. O yüzden o yetiştirme konusunda içiniz rahat olabilir. Biz Türkiye olarak onlardan daha iyiyiz. Sadece daha organize değiliz. Yani arkamızda bir hükümet desteği yok. Özel kurum olarak onlardan daha iyiyiz. Tek eksiğimiz işte o koordinasyonun ve ulusal önceliğin olmayışıydı. Onun haricinde bir problemimiz yok.

(E) Tuğgeneral Mesut Bedri USTA

Bu arada Türk Silahlı Kuvvetleri olarak o kadar çok mütevazı olmayalım, silahlı kuvvetlerde halen piyade subaylarından, ODTÜ'de siber güvenlik eğitimi almış bir bölüm var. Hep İsrail'i örnek veriyoruz ama ülke olarak TSK'nın da hakkını verelim. Bizde de, piyade ya da komando eğitimi almış siber güvenlik eğitimi almış subaylarımız var. Öte yandan TSK'nın da şu anda siber güvenliği yapan muhabere sınıfında ya da MEBS sınıfının görev tanımlarında piyade gibi savaşmak zorunluluğu vardır.

Kubilay Onur GÜNGÖR

Bir güzel şey de şu: Mesela bu bahsedilen Unit 8200 çok eski bir birimdir. Ama bu tarz bahsedildiği şekilde kapsamlı bir multidisipliner metodolojiye dönüşüm Cyber Struggle'ın kurulmasından bir buçuk ay sonradır. Cyber Struggle böyle bir metodolojiyi dizayn edip sivil kullanımına açan ve klasik askeri eğitimin de ötesine götüren ilk organizasyondur. Şu an herkesten iyiyiz. O konuda içiniz rahat olabilir.

Kadir Murat BİÇER

Burada ben bir ilave yapmak istiyorum. İsrail'de Unit 8200, Çin'de Unit 61398 var. Genelde bu tarz yapılar biraz daha saldırı ağırlıklı ve yapılan

işlemlerin biraz daha gizli kalması için kurulan yapılar. Yaptıkları işlemlerin belli olmaması için birlik isimleri numarayla tanımlanır. Diğer ülkelerde de benzer yapılar isim yerine numara altında yer almakta ve tanımlanmaktadır. Burada esas olan bu grupları veya bu personeli buraya dedike etmek veya ilgili eğitimleri aldırıp insanları bu konularda motive edip yetiştirmek. Önemli olan bu tarz inisiyatiflerin gösterilip bu tarz birimlerin kurulmasına yönelik harekete geçilmesi. Milli Savunma Bakanlığı ve savunma mantığı altında bunlar yapıldığı zaman biraz daha aktif savunma tarafında kalır. Yani belli bir yetkinlik kalacak şekilde bir bakış açısı gündeme geliyor. Siber, direkt Silahlı Kuvvetlerin ilgi alanında değildir. Genel etkileyiş olarak zaten milli güvenliği direkt etkileyen bir unsur olduğundan dolayı Silahlı Kuvvetlerin tek başına bu konu hakkında sorumlulukları yakalaması da zordur. Bu kapsamda, silahlı kuvvetler dahil tüm birimlerin vereceği ortak bir karar sonrası bu tarz yetkinlikler silahlı kuvvetler bünyesinde de olabilir, dışında da olabilir. Çünkü ülke içerisinde farklı birimlerde de bu tarz yetkinlikler mevcut. Ortak bir birim olabilir, kurulabilir. Bu şekilde kurulanlar ve belli bir şekilde çalışanlar mevcut. Bunların biraz daha yapılandırılıp kendi görev ve sorumluluklarının kapsamı ortaya çıkarılıp yetkilendirilmesiyle olabileceğini düşünüyorum.

"İsrail'de Unit 8200, Çin'de Unit 61398 var. Genelde bu tarz yapılar biraz daha saldırı ağırlıklı ve yapılan işlemlerin biraz daha gizli kalması için kurulan yapılar. Diğer ülkelerde de benzer yapılar isim yerine numara altında yer almakta ve tanımlanmaktadır. Burada esas olan bu grupları veya bu personeli buraya dedike etmek veya ilgili eğitimleri aldırıp insanları bu konularda motive edip yetiştirmek. Önemli olan bu tarz inisiyatiflerin gösterilip bu tarz birimlerin kurulmasına yönelik harekete geçilmesi. Siber, direkt Silahlı Kuvvetlerin ilgi alanında değildir. Silahlı kuvvetler dahil tüm birimlerin vereceği ortak bir karar sonrası, bu tarz yetkinlikler silahlı kuvvetler bünyesinde de olabilir, dışında da olabilir. Çünkü ülke içerisinde farklı birimlerde de bu tarz yetkinlikler mevcut. Ortak bir birim olabilir, kurulabilir. Bu şekilde kurulanlar ve belli bir şekilde çalışanlar mevcut. Bunların biraz daha yapılandırılıp kendi görev ve sorumluluklarının kapsamı ortaya çıkarılıp yetkilendirilmesiyle olabileceğini düşünüyorum."

Kadir Murat BİÇER

Kubilay Onur GÜNGÖR

Mesela Unit 8200'deki personel aslında salt askeri, silahlı kuvvetler, istihbarat servislerini içermiyor. Unit 8200'deki personelin birçoğu, belki yüzde 80'i belirli bir süre görev yaptıktan sonra yurtdışında belirli yerlerde özel sektörde çalışmaya başlıyorlar. Mesela bugün CheckPoint diyorsunuz, kurucularının içinde Unit 8200 var. Recorded Future diyorsunuz, taktik istihbarat sağlıyor, kurucularının içinde Unit 8200 personeli var. Yani İsrail'in böyle bir stratejisi de var. Unit 8200'ü okul gibi kullanıp orada yetiştirdikten sonra global siber güvenlik lobisi yaratmaya çalışıyor ve birbirlerine destek oluyorlar. Bu yüzden de hızla yatırım alıp hızla ürün satma süreçlerinde önemli katkıları oluyor. Yani olay sadece silahlı kuvvetler çerçevesinde değil. Bizim rakibimiz olabilecek ülkeler zaten sivillerini de böyle özel tim gibi yetiştirmeye başlıyorlar.

Mustafa YILMAZ

Son olarak insan kaynağıyla alakalı bir cümle söylemek istiyorum. Türkiye Bilişim Sanayicileri Derneği'nin her yıl bilgi ve iletişim teknolojileri pazar verileri yayınlanır. Ben de elimden geldiğince bakarım. 2018 pazar verilerine baktığımızda şöyle bir soru var: "Sektör gelişimi için en önemli

"Türkiye olarak Asya Pasifik bölgesinde birtakım ülkelerle sadece ürün konumlandırma, ürünü tanıtma anlamında değil ama stratejik yakın işbirlikleri yapıyoruz. Tabii olayın ticari boyutu, başka farklılıkları var ama stratejik işbirlikleri anlamında da SSB ile adımlar atılabilirse kurumsal anlamda çok büyük sinerji doğar. Çünkü siber tehdit istihbaratı olabilir, belli saldırılara karşı ortak savunma olabilir, bu anlamda hem NATO nezdinde hem Tier 1 operatörlerde hem belli bölgelerdeki özel işbirliklerinde oldukça fazla fırsat görüyorum."

Borga ERBİL

gördüğünüz üç sorunu belirtir misiniz?" diyor. Bu benim son üç yıldır takibimde ve üç yıldır hiç değişmiyor. Her zaman nitelikli işgücü açığı öncelikli bir husus. Sektörde paranız da olsa zaman zaman insan kaynağı noktasında ciddi bir sıkıntımız söz konusu.

Borga ERBİL

Olayın uluslararası boyutu mutlaka görüşülmeli. Fırsatlar ve tehditler bu anlamda daha iyi analiz edilmeli. Bu aslında uluslararası bir işbirliği. Ben üçüncü madde kapsamında özellikle birkaç hususa değinmek istiyorum. NATO'da CCD COE kapsamında birtakım tatbikatlar yapıldı. Biz bunlara iştirak ediyoruz. Benzer bir şekilde geçen hafta da BTK'da CyberShields gerçekleştirildi. Burada 17 ülke, 20 takım yarıştık. Bu tip mekanizmalarla işbirliklerine bakmak faydalı olabilir. Bir de son ICWC'de Malezya ve Pakistan'dan iki uluslararası konuşmacımız da vardı. Malezya'dan General Tan Sri katıldı. Kendisi özellikle işbirliklerinin altını çizdi. Türkiye olarak Asya Pasifik bölgesinde birtakım ülkelerle sadece ürün konumlandırma, ürünü tanıtma anlamında değil ama stratejik yakın işbirlikleri yapıyoruz. Biz de HAVELSAN olarak o projede çok aktifiz. Tabii olayın ticari boyutu, başka farklılıkları var ama stratejik işbirlikleri anlamında da SSB ile adımlar atılabilirse kurumsal anlamda çok büyük sinerji doğar. Çünkü siber tehdit istihbaratı olabilir, belli saldırılara karşı ortak savunma

olabilir, bu anlamda hem NATO nezdinde hem Tier 1 operatörlerde hem belli bölgelerdeki özel işbirliklerinde oldukça fazla fırsat görüyorum.

(E) Korgeneral Alpaslan ERDOĞAN

Kani Albayım, bu soru kapsamındaki bilginizi alacağım ama aynı zamanda dördüncü konumuz olan Türkiye'de şimdiye kadar yaşanan örnek siber saldırılara da değinelim.

(E) Albay Kani HACIPAŞAOĞLU

Siber olaylara dünyanın nasıl baktığı konusunda ilave olarak şunu da söyleyebilirim: Dünyanın gelişmiş kısımları artık uyanıyor. Artık bu işi bir MEBS olayı, bir IT, ICT olayı olmaktan farklı görüyorlar -ki biraz önce arz ettiğim gibi NATO teşkilatlarında siberle ilgili bölümleri çıkartıp daha üst komuta kademelerine, hatta politik kademelere bağladılar. Çünkü bu konunun multidisipliner bir yapısı var. Örneğin NATO harekâtında siber konuları, komuta kademelerinin en çok ihtiyaç duyduğu *Commander's Critical Information Requirement* listesinde, yani "olmazsa olmaz"lardan biri. Bu doğrultuda, altı çizilmesi gereken bir husus şu: Dünyanın gelişmiş ülkeleri artık siber harekât ya da siber savaş kapsamındaki olayları, sadece bilişimcilerin baktığı teknik konular olmaktan çok öte olaylar olarak görüp algılıyor ve değerlendiriyor. Ayrıca, ister özel sektör ister kamu, ister asker ister sivil herkes artık "Bu işler teknik adamların işi, gidin onlara sorun" fikrinden uzaklaşmalılar. Siber kapsamındaki konular artık kamu ve özel sektörde en üst seviye yönetici, amir ve yönetim/icra kurullarının birinci derece sorumluluğu altındadır. Üst düzey yönetimlerin siber konusundaki sorumlulukları doğal olarak teknik değil; ancak bu konunun önemini doğru algılamak, gereken seviyede destek vermektir. Geçen yıl Aon firmasının davetlisi olarak İstanbul Conrad Otel'de katıldığım risk yönetimi etkinliğinde siber risk yönetimiyle ilgili konularda konuşmuştum. Yapı Kredi'nin genel müdür yardımcılarından biri risk yönetimi sorumlusu. LC Waikiki'de genel müdür yardımcısı seviyesinde bir sorumlusu var ve özetle, "Eğer bir firmanın cirosu yıllık 300 milyon doların üzerindeyse o firmada mutlaka bir risk yönetimi birimi olmalı ve siber risk yönetimi de bunun içinde olmalı" diyorlar. "Aksi takdirde, bu işi yönetemezsiniz" deniliyor. Bunu böyle algılamak lazım.

"Dünyanın gelişmiş ülkeleri artık siber harekât ya da siber savaş kapsamındaki olayları, sadece bilişimcilerin baktığı teknik konular olmaktan çok öte olaylar olarak görüp algılıyor ve değerlendiriyor. Ayrıca, ister özel sektör ister kamu, ister asker ister sivil artık herkes 'Bu işler teknik adamların işi, gidin onlara sorun' fikrinden uzaklaşmalılar. Siber kapsamındaki konular artık kamu ve özel sektörde en üst seviye yönetici, amir ve yönetim/icra kurullarının birinci derece sorumluluğu altındadır. Üst düzey yönetimlerin siber konusundaki sorumlulukları doğal olarak teknik değil; ancak bu konunun önemini doğru algılamak, gereken seviyede destek vermektir."

(E) Albay Kani HACIPAŞAOĞLU

Volkan ERTÜRK

Neden risk yönetimi diyorlar, orayı biraz daha açalım. Çünkü siber güvenlik henüz mümkün değil. Yani ben güvenliğimi her boyutuyla sağlayamayacağım, o zaman eksikliklerimi, risklerimi önce tanımlayayım, önceliklendireyim, kritik olandan başlayayım.

(E) Albay Kani HACIPAŞAOĞLU

Tabii ve nasıl en aza indirgeriz durumu var. Nasıl sıfırlarız şeklinde bir yaklaşım yok, zaten bu

mümkün de değil. Siber risklerin de içinde bulunduğu risk yönetimi çalışmalarını Dünya Ekonomik Forumu (WEF) da yapıyor. WEF'in 2018-2019 raporuna baktığınızda gerek önemi gerekse etkisi açısından doğal afetlerden sonra ikinci sırada siber tehditler geliyor. Keza, ABD'nin Homeland Security teşkilatı da yaptığı tehdit ve risk değerlendirmesinde nükleer saldırılardan sonra ikinci sıraya stratejik seviyelerdeki siber tehdit ve riskleri koymuş. Siber suçların sebep olduğu zararlar konusunda yapılan araştırmalarda da Marsh & McLennan, McAfee gibi firmaların raporlarına baktığınızda, 2014'te siber suçların verdiği zarar 445 milyar dolar, 2017'de 600 milyar dolar olarak doğal afetlerden de daha fazla. 2019 sonu itibarıyla 2 trilyon dolar olan bu zararların 2021'de de 6 trilyon dolara ulaşacağı tahmin ediliyor. Bu zararlara, bilişim sisteminin donanım ve yazılımında ortaya çıkan hasarların yanında kurum ve firmaların mülkiyet hakları, saygınlığı, itibarındaki kayıplar gibi çok önemli kayıplar da dahil. Konuyu toparlamak gerekirse, öncelikle bu konu sadece teknik bir konu değil; diğer taraftan, sadece askerin işi de değil. Devlet seviyesinde ele alınması gereken kapsamlı bir iş. Bu konuda son olarak belirtmek istediğim bir husus da 24 Aralık 2019 itibarıyle resmî gazetede yayımlanan genelge, Akıllı Şehirler Strateji ve Eylem Planı Genelgesi. Bu genelgeyi Çevre ve Şehircilik Bakanlığı çıkardı. 412 sayfalık bu strateji ve eylem planının içerisinde 87 yerde siber konusu geçiyor.

(E) Korgeneral Alpaslan ERDOĞAN

Teşekkür ederim. Türkiye'de yaşanan siber olaylara giriş yaparsak bugüne kadar neler yaşandı veya kapsamlı siber saldırılar nelerdi?

(E) Albay Kani HACIPAŞAOĞLU

Garanti Bankası da dahil birçok banka DDoS saldırısına uğradı. Bunun ilkini de Atilla Özgit hocam yaşamıştı. Yaşanan bu olay hakkında özetle şu hususlara dikkat çekmek isterim: Bu işin geri planının sadece teknik ya da ekonomik olmadığını değerlendiriyorum. Bu olay gerçekleştiğinde tarih 15 Aralık 2015 idi ben HAVELSAN'da Siber Güvenlik Direktörüydüm. Beni kim aradı biliyor musunuz? Çok ilginç bir olay yaşadık. ABD'nin Ankara büyükelçiliğindeki *Political Advisor* olan ABD'linin danışmanı olan Türk bir kadın aradı beni. "ODTÜ'deki olayı biliyor musunuz? ODTÜ'dekilerin bu işte ne kadar zaafı var?" şeklinde ilginç sorular aldım. Tabii alması gereken uygun cevabı aldılar.

Burada şunu da belirtmek gerek. Malum, istatistikler eskiden bir siber saldırının yapıldığını ve hasarını anlamak için 271 gün geçtiğini söylüyorlardı, şimdi bu süre 251 güne düştü. Büyük bir siber saldırının olduğundan ortalama ne kadar zaman sonra oradaki insanlar uyanır: 251 günlük bir süre var. Çünkü siber saldırganların *Kill Chain Methodogy* gibi uyguladıkları yedi safhalı bir süreç var. Hedefledikleri bilgi sistemi için sosyal mühendislik, oltalama ve benzer yöntemlerle girdikleri sistemin elde ettikleri bilgilerini örneğin Arnavutluk'ta bir sistem üzerine koyup müteakiben Deep/Dark webde satışa çıkartıyorlar. Bugün dünya istatistiği bu. 251 günde bile hâlâ kendisine yapılan siber saldırıdan hiç haberi olmayan

"Siber suçların sebep olduğu zararlar konusunda yapılan araştırmalarda Marsh & McLennan, McAfee gibi firmaların raporlarına baktığınızda, 2014'te siber suçların verdiği zarar 445 milyar dolar, 2017'de 600 milyar dolar olarak doğal afetlerden de daha fazla. 2019 sonu itibariyle 2 trilyon dolar olan bu zararların 2021'de de 6 trilyon dolara ulaşacağı tahmin ediliyor. Bu zararlara, bilişim sisteminin donanım ve yazılımında ortaya çıkan hasarların yanında kurum ve firmaların mülkiyet hakları, saygınlığı, itibarındaki kayıplar gibi çok önemli kayıplar da dahil."

(E) Albay Kani HACIPAŞAOĞLU

kurumlar da var, haberi olup duyurmayanlar da! Bunlar yaşanan ve bizlerin de zaman zaman tanık olduğumuz ve devlete faturasının çok ağır olabileceği konular.

Kadir Murat BİÇER

Ben hak veriyorum, burada özellikle farkına varmayan kurumlar olabilir. Herhangi bir şekilde bilgisi ortaya çıkmamış saldırı olabilir -ki mesela fidye saldırısında onunla ilgili eğer gerekli bütçe varsa, fidyenin verilip o saldırının kamuya duyurulmadan kendi içerisinde üstünün kapatıldığını biliyoruz. Ben burada başka bir bakış açısıyla yaklaşmak istiyorum. Siber saldırılar genelde, yine STM Siber Füzyon Merkezi tarafındaki yapılan çalışmalardan hareketle söyleyebilirim, konjonktürel gelişmelere bağlı olarak ülke kaynaklarına karşı artabiliyor veya azalabiliyor. Yanlış hatırlamıyorsam, 22 Ocak 2018'de Zeytin Dalı, Afrin harekâtı başladı, yaklaşık iki ay sürdü. Biz o dönem içerisinde gov.tr, bil.tr, edu.tr, com.tr uzantılı sitelerimiz ve ülkemizin büyük altyapılara sahip kritik kurumlarına baktığımızda saldırıların genelde sosyal medyada örgütlendiğini, belli saldırı gruplarının belli komiteler altında, belli hashtag'lerle bir araya gelerek belli bir süre boyunca siber saldırı başlattığını, bu saldırıların ağırlıklı olarak hizmet engellemek amaçlı "dağıtık servis dışı bırakma" dediğimiz DDoS saldırıları şeklinde yapıldığını ve Afrin operasyonunun başarıya ulaştığı dönemde saldırının en üst seviyelere ulaştığını gördük. Konu hakkındaki raporlarımızı ilgili yerlerle paylaştık. 9 Ekim 2019'da başlayan Barış Pınarı Harekâtı'nda da yine gördüğümüz manzara aynı oldu. Bizim ülke olarak bütün milli unsurlarımızla beraber bir arada bulunarak yapmış olduğumuz bir harekâtta, o harekâta katılmayan ama ülke içerisindeki hizmetlerin verilmesinde etkinliği olan kurumlara karşı siber saldırı yapıldığını, saldırıları da harekâta karşı çıkan grup veya oluşumların özellikle sosyal medyada bir araya gelerek organize ettiğini söyleyebiliriz -ki biraz önce ismi verilen bankaya yapılan saldırı da aynı dönemdeydi. Bu bankaya yapılan saldırı da benzer mantıkla yapıldı. Aynı anda başka kurum ve bankalara da saldırılar olduğunu tespit ettik ama özellikle POS işlemleri bakımından yüksek seviyede olmasından dolayı bu bankanın adı ön plana çıktı. POS işlemlerinin yapılamaması ve genelde müşteri alışkanlıklarına karşılık vermemesinden dolayı ilgili bankanın ve operatörlerin ismi çıktı. Bunu şöyle bağlamak istiyorum: Siyasi konjonktürle beraber bizim kendi altyapılarımıza da hibrit savaşın bir parçası dediğimiz siber saldırıların yapıldığı bir gerçek. Bu anlamda özellikle kritik altyapı sahibi olan kurumların da konjonktürel gelişmelere bağlı olarak kendi ekiplerini artırmalarını, kaynaklarını farklı yöntemlerle bir araya getirmelerini veya biraz önce bahsettiğim segmantasyon gibi bazı bilgilerin aktarılmasının engellenmesi gibi önlemleri almalarını tavsiye ederiz.

> *"Siber saldırılar genelde, yine STM Siber Füzyon Merkezi tarafındaki yapılan çalışmalardan hareketle söyleyebilirim, konjonktürel gelişmelere bağlı olarak ülke kaynaklarına karşı artabiliyor veya azalabiliyor. Özellikle kritik altyapı sahibi olan kurumların konjonktürel gelişmelere bağlı olarak kendi ekiplerini artırmalarını, kaynaklarını farklı yöntemlerle bir araya getirmelerini veya biraz önce bahsettiğim segmantasyon gibi bazı bilgilerin aktarılmasının engellenmesi gibi önlemleri almalarını tavsiye ederiz."*
>
> **Kadir Murat BİÇER**

(E) Albay Kani HACIPAŞAOĞLU

Bu konuda teknik olarak iş başındayken genelde yaşadığımız husus hep şöyleydi: Bir kurum yetkilisi kurumuna bizi davet ediyor ve sistemlerine bir sızma testi yapmamızı istiyordu. Her seferinde bilgi sistemlerindeki zafiyetlerin bir sızma testiyle önüne geçilemeyeceğini belirtiyor, bu sürecin

> *"Türkiye'ye yapılan bu saldırılar genelde kamuoyuna paylaşılmak yerine arıza olarak nitelendiriliyor. Oysa kamuoyuyla paylaşarak alınacak tedbirler topyekûn değerlendirilmelidir. Bunların üstünü örtmek yerine paylaşmak ve ortak çözüm aramak her kurumun hedefi olmalıdır."*
>
> **(E) Tuğgeneral Mesut Bedri USTA**

kriter ve standartları olan çok daha kapsamlı bilimsel bir süreç olduğunu anlatmak zorunda kalıyorduk. Çünkü doğru yaklaşım, "Teknoloji, İnsan, Süreç" bağlamında gerçekleştirilecek test ve prosedürler silsilesi. Örneğin, bizim ISO 27.001 dediğimiz güvenlik test süreci bile aslında belirttiğim bu bilimsel sürecin sadece bir parçası.

(E) Tuğgeneral Mesut Bedri USTA

Türkiye'ye yapılan siber saldırılar konusunda bir şey daha eklemek istiyorum: 2008'de Bakü-Ceyhan Petrol Boru Hattı'nda basınç yükseltildi. 31 Mart 2015'te Van hariç 44 ilde elektrik kesildi. Atilla Hocamın bahsettiği Türkiye'nin tr uzantılı bütün sitelerine bir Ddos saldırısı oldu. Geçen aylarda Bakan Yardımcımız Ömer Fatih Sayan da "Türkiye'ye çok saldırı oldu. Yüzde 99'u dağıtık servis" dedi. Ama sorun ne biliyor musunuz? Türkiye'ye yapılan bu saldırılar genelde kamuoyuna paylaşılmak yerine arıza olarak nitelendiriliyor. Oysa kamuoyuyla paylaşarak alınacak tedbirler topyekûn değerlendirilmelidir. Bunların üstünü örtmek yerine paylaşmak ve ortak çözüm aramak her kurumun hedefi olmalıdır.

(E) Korgeneral Alpaslan ERDOĞAN

Bazı sistemler veya altyapıya eklentiler birbirlerinden farklı, koordinasyonsuz şekilde yapıldığında bu durum bir açık yaratıyor mu? Mesela basıncın yükseltilip boru hattının patlatılması kamera görüntü sisteminin üzerinden yapıldı diye hatırlıyorum. Hatta eve hizmetçiyi kontrol etmek için döşenen kamera sisteminden erişilip, evde yangın çıkartılması gibi durumlar da yaşanıyor. Dolayısıyla belki evin elektrik sistemine sonradan bir şey ilave edilmesi veya önce boru hattı sistemi yapılıp sonradan bunun emniyeti için kamera görüntü sistemi koyulması gibi birbiriyle koordine edilmeden yapılanlar da sıkıntıya yol açıyor.

(E) Albay Kani HACIPAŞAOĞLU

Örneğin, bir barajın tüm çalışmasını kontrol eden ve genelde SCADA olarak bilinen "Endüstriyel Kontrol Sistemleri (ICS: Industrial Control Systems)" kendi içinde kapalı bir sistem dahi olsa en azından sistem güncellemeleri için bir noktada internete bağlı olduğundan güvenlik zafiyetleri oluşuyor. Dolayısıyla, işlettiğiniz tüm bilişim sistemlerini ve endüstriyel kontrol sistemlerini bütünsel bir yaklaşımla güvenlik testlerine ve yapılanmalarına tabi tutarsanız muhtemel saldırılardan en az etkilenecek durumda olursunuz.

> *"Örneğin, bir barajın tüm çalışmasını kontrol eden ve genelde SCADA olarak bilinen Endüstriyel Kontrol Sistemleri (ICS: Industrial Control Systems), kendi içinde kapalı bir sistem dahi olsa en azından sistem güncellemeleri için bir noktada internete bağlı olduğundan güvenlik zafiyetleri oluşuyor. Dolayısıyla, işlettiğiniz tüm bilişim sistemlerini ve endüstriyel kontrol sistemlerini bütünsel bir yaklaşımla güvenlik testlerine ve yapılanmalarına tabi tutarsanız muhtemel saldırılardan en az etkilenecek durumda olursunuz."*
>
> **(E) Albay Kani HACIPAŞAOĞLU**

(E) Korgeneral Alpaslan ERDOĞAN

Siber güvenlik hangi sektör ve alanları etkilemektedir? Kubilay Bey önce sizin katkınızı alacağız. Bu konuda Borga Bey'in ve Volkan Bey'in de katkılarını alacağız.

Kubilay Onur GÜNGÖR

Öncelikle şunu söyleyebilirim: Bu söyleyeceğim hem koordinasyon konusuna bir atıf olacak hem de günün en başında konuştuğumuz paradigma değişimiyle alakalı konulara atıf olacak. Bir taraftan da bütün süreci konvansiyonel görme problemi var. Yani savunma planlaması yaparken bu konuda hem ülke hem özel sektör olarak Soğuk Savaş yıllarındaki gibi tehdit odaklı savunma planı yapar durumdayız. Hatta sosyal medyada da hep siber tehditler, hep tehdit tadında ilerliyor. Bundan ziyade, yetenek bazlı veya olay odaklı planlamalara geçmememiz gerektiğini düşünüyorum. Bu personel tarafında yetenek bazlı senaryolar oluşturmak için hibritleşmeyi yine o özel kuvvetler açısından beraberinde getirecek çünkü çok minik, çok taktiksel kalıyor tehditlere hazırlanmak. Örneğin SQL Injection tehdidi için savunma yapmak ya da savunma planını böyle küçük taktiksel şeyler üzerine oturtmak çok efektif olmuyor. Onun yerine bir olay olacak, ne zaman olacak bilmiyorum, kim yapacak bilmiyorum, hangi kuvvetle gelecek bilmiyorum, ne kadar sürecek bilmiyorum ama benim buna hazırlanmam gerekiyor. Bu çerçevede ilerlemesi gerekiyor. Hangi sektör ve alanları etkilemektedir deyince de belki ben biraz daha şahin bakıyor olabilirim bu konuya, benim için etkilemediği bir alan yok. Benim şahsen tanıdığım bir arkadaş vardı ABD'de otelde ölü bulundu. Hatta basına da yansımıştı bir güvenlik konferansından önce. Çalıştığı konu kalp pillerini uzaktan durdurma üzerineydi.

(E) Korgeneral Alpaslan ERDOĞAN

Kendisinde kalp pili mi vardı yoksa?

Kubilay Onur GÜNGÖR

Kendisinde yoktu ama ölü bulundu. O düzeye kadar indi. Mesela şu an Çin mikroçiple haberleşme üzerine insan deneyleri için izin aldı. Yani beyne takılan iki çiple iki farklı insanın hiç konuşmadan haberleşme süreci başladı. Bunların hepsi kötü niyetli insanlar için cennet, bizim için de yeni savunma alanları. Dolayısıyla ayrım yapma şansımız kalmadı, aklımıza ne geliyorsa her şeyi etkiliyor. Aslında

"Burada artık siber dünya demek yerine siber yaşama doğru bir tanım yapmak faydalı olabilir. Yaşam çünkü sibere doğru kayıyor. Dolayısıyla hayatta günümüz problemleri neyse, bunların hepsinin siber yansımaları olacak. Ya günümüzdeki suç siberde yeni bir alan olarak işlenecek ya da siberin kendine ait suç modelleri de olacak. Dolayısıyla bir kayış var. İki tarafı da barındırıyor. Kesinlikle ayırma şansı kalmıyor diye düşünüyorum."

Kubilay Onur GÜNGÖR

burada artık siber dünya demek yerine siber yaşama doğru bir tanım yapmak faydalı olabilir. Yaşam çünkü sibere doğru kayıyor. Dolayısıyla hayatta günümüz problemleri neyse, bunların hepsinin siber yansımaları olacak. Ya günümüzdeki suç siberde yeni bir alan olarak işlenecek ya da siberin kendine ait suç modelleri de olacak. Dolayısıyla bir kayış var. İki tarafı da barındırıyor. Kesinlikle ayırma şansı kalmıyor diye düşünüyorum.

(E) Korgeneral Alpaslan ERDOĞAN

Teşekkürler Kubilay Bey. Borga Bey, buyurun.

Borga ERBİL

Askeri alan bu değişimlerden son derece fazla etkileniyor. Ben olayın sadece defansif olduğunu düşünüyorum. Askeri alanda sadece merkezde değil, taktik alana doğru giden, yani sahaya doğru giden, ofansif bazlı planlamalar, yapılanmalar var. Siber güvenlik saldırı ekipleri artık belli ülkelerin silahlı kuvvetleri tarafından özel olarak tasarlanıyor. Bununla ilgili yürüyen projeler dahi görmekteyiz. Bunun haricinde tabii kamu ciddi anlamda etkilenen önemli bir sektör. Türkiye'de e-devlet süreci çok önce başladı. Bu anlamda Türksat ev sahipliğini yapıyor. Ancak önce bir parantez açıp, *false-positive* de diyebiliriz belki ama mesela alt-üst soy sorgulama servisi açıldığında aslında bir nevi saldırı altında kaldı. Hizmet almaya çalışan kişiler aslında bilinçdışı bir saldırı gerçekleştirmiş oldu. Bunlar da kaos yaratabilecek, inişler çıkışlar yaratan durumlara sebebiyet vereceği için illa kötü niyetli olmayabilir -yani halkın belli durumlardaki taleplerindeki artışlar azalışlar da bu anlamda değerlendirilebilir- diye düşünüyorum. E-Ticaret'in olabildiğince elektronikleştiğini düşünürsek onlar da siber güvenlikteki durumlardan olabildiğince etkileniyorlar. Finans-ekonomi zaten aşikâr. Parasal zararı en çok yaşayabilecek ve deneyimleyen oyuncular olduğu için çok ciddi yatırımlar yapıyorlar. Prestij kaybı onlar için önemli kayıplara yol açıyor.

Haberleşmenin pek çok boyutu oluyor; data haberleşmesi, ses haberleşmesi ve hele ki IoT haberleşmesi. Bu anlamda ben servis sağlayıcı ya da Telekom sektörünün çok çok önemli bir noktada olduğunu düşünüyorum. Etkilenen birimler arasında direkt bazı siyasi partiler ya da politik görüşlerini açıklayan politik kurumlar, düşünce kuruluşları olabilir. Medyada birkaç saniyenin bile önemi var. Bir haberi bir gelişmeyi en hızlı şekilde aktarmak amaç. Üç-beş dakika sonra duyurduğunuzda bir anlamı kalmıyor. Bu anlamda onlar da hem kendi hizmetlerini ayakta tutmak hem de olan biteni hızlıca aktarmak adına bu konuya son derece önem verirler. Örneğin seçimlerde pek çok deneyim yaşadık. Haberleşmede haberleşmeyi kesebilirsiniz, enerjide enerjiyi kesebilirsiniz. Hatta enerji kesintisinin olduğu 31 Mart 2015 tarihinde ben Ankara'daydım. Bir servis sağlayıcının çalışanıydım. Öğlen 12:30 civarı Ziraat Bankasına gittim, hizmet veremez hale gelmişti. Neden dedim, jeneratörünüz yok mu? Var ama mazotu bitti dediler. Yani hizmet veremez hale gelmişlerdi. Öğleden sonra 14:30 gibi kriz merkezi kurulduğunu gördüm kendi biriminde. Çünkü baz istasyonlarının da mazotları bitmeye başlamıştı ve lojistik anlamda o kadar fazla baz istasyonuna aynı anda o kadar mazot dağıtmak gibi bir operasyon düşünülmemişti. Dolayısıyla enerjiyi vurursanız Telekom, Telekom'u vurursanız başka şeyler böyle

domino etkisiyle gidiyor. Bir de tabii Türkiye'de 15 Temmuz 2016 musibetinden çok çok önce bu durumlar ortaya çıktığı için aslında enerji sektörü kendi korumasını daha sıkı başlattı. Biz hep güvenliğe kuzey-güney trafiğinde bakarken biraz daha artık içimizde bakmaya başladık. Yani erişim anlamında kablolu kablosuz kimler erişebiliyor, içeride neler olup bitiyor, sadece IT değil OT tarafında neler olup bitiyor? Bu anlamda ben son beş yılda enerji alanında son derece üst seviyede bir farkındalık ve koruma içgüdüsü gözlemliyorum ve alınan aksiyonları gözlemliyorum. Hatta bunların merkezîleştirilmesi noktasında da bazen son dönemde kurulan uluslararası şirketler de dahil biz şirketler kuruyoruz. Örneğin Botaş International var. Sadece kamu değil onlarla ilişkili bazı özel şirketler de olabiliyor. 20'nin üzerinde birim var. Bunların siber güvenliğini merkezîleştirici bir adım atıldı. Bu anlamda aslında aksiyonların doğru olduğunu düşünüyorum.

Bir hususu daha belirtmek istiyorum. Haberleşmeyi kesiyorsunuz, enerjide enerjiyi kesiyorsunuz, finans sektöründe döviz kuruyla oynayarak kısa süreli manipülasyonlar yapıyorsunuz ancak binlerce gün içeride kalabilen bazı atak türleri var. Çok sonra içeride bir şeyler yapıldığı ortaya çıkabiliyor. Vatandaşların sağlığı milli güvenlik konusudur değil mi? Ya da gençlerimizin, çocuklarımızın eğitimi bir milli güvenlik konusu olabilir çünkü kademeli olarak yanlış yere çocuklar yönlendiriliyorsa, yani yetenekli çocuklar yeteneklerinden saptırılacak şekilde farklı eğitim kanallarına gönderiliyor olabilir. Aslında hasta olmayan bireylerin verileriyle oynanarak hem o bireyin toplumdan düşürülmesi hem de sağlık harcamalarının artırılması da bence bir milli güvenlik problemi. Ben belirli hastanelerimizde veri kayıpları olduğunu biliyorum. Dolayısıyla vatandaşın geçmiş sağlık verilerinin korunamıyor olması milli güvenlik açısından bir problem olabilir.

(E) Korgeneral Alpaslan ERDOĞAN

Volkan Bey sizin de kısaca finans ve bankacılık konusundaki görüşlerinizi alalım.

Volkan ERTÜRK

Biraz daha pragmatik veya biraz daha somut konuşmak istiyorum. Problemi değil çözüm yaklaşımlarını konuşmak istiyorum. Sektör bazlı konuştuk, oraya katkım çok daha sınırlı olur. Elon Musk'ın Space X'in yapım sürecinde bir lafı vardır: "Benim bir roketin prototipini yapmamla gerçeğini yapmam arasındaki eforum 100 kattır." Bir versiyonunu yapmakla, bunu sürekli üretilebilir hale getirmek arasındaki efor farkı. Şimdi Kubilay Bey başarılarını anlattı, gururlanıyoruz kendisiyle, çok inanılmaz şeyler yapıyor ama bizim ülke olarak Kubilay'ı yetiştirmek için eforumuz çok sınırlı. Kendi başına yetişmiş bir arkadaş. Bayırda açan inanılmaz güzellikte bir çiçek gibi. Asıl amaç Kubilaylar yetiştirebilecek bir fabrika üretebilmek. Biraz böyle bakmamız gerekiyor.

Siber güvenlik start up'ları yetiştirebilecek miyiz? Önemli olan konu bu bence. Biraz buna kafa yormak lazım. Şimdi sertifikalandıralım bunları, önceliklendirelim de; asıl bunları üretmeye odaklanmak kıymetli. 8200 mesela; insanlar üç sene boyunca veya kaç sene zorunlu hizmeti varsa orada çalışıyor, siber güvenlik alanında özel operasyonlarını yapıyor, orada kullandığı teknolojiyi sonra gidip ticarileştiriyor. Aslında zeytini sıkıyor, sızma yağını kendi tüketiyor, posasını da al bunu ticarileştir buradan para kazan, bizim farklı sektörler kazansın şeklinde kullanıyorlar. Üç, dört sene sonra piyasaya giren bir teknoloji oluyor. Ama biz duyunca "Adamlar neler düşünmüş" diyoruz. Baktığınız zaman burada bir çark dönüyor aslında. Bizim de böyle çarklar kurabilmemiz çok kıymetli. İkinci konu da siber savaş içinde olup olmadığımız tartışılabilir. Peki pragmatik olarak ne yapacağız, somut adımınız ne burada? Tatbikat yapalım, insanları bir araya toplayalım veya yönergeler yazalım, insanlar buna uysun ama bütçesi var mı, onu destekleyecek donanımı var mı? İnsan eksiğimiz var biliyoruz, teknoloji olarak hep ihraç ediyoruz, kullanımda da çok iyiyiz, bunları da söylüyoruz. Peki ama pragmatik olarak siz yapın diye kurumlara görevler, ödevler vermenin dışında buradaki insanları biz nasıl destekleyeceğiz? Merkezi idare ne yapacak? Belki buralardan bakmak lazım. Ben şuna inanıyorum, start up'da

"Siber güvenlik start up'ları yetiştirebilecek miyiz? Önemli olan konu bu bence. Biraz buna kafa yormak lazım. Şimdi sertifikalandıralım bunları, önceliklendirelim de; asıl bunları üretmeye odaklanmak kıymetli. İkinci konu da siber savaş içinde olup olmadığımız tartışılabilir. Peki pragmatik olarak ne yapacağız, somut adımınız ne burada? Tatbikat yapalım, insanları bir araya toplayalım veya yönergeler yazalım, insanlar buna uysun ama bütçesi var mı, onu destekleyecek donanımı var mı? İnsan eksiğimiz var biliyoruz, teknoloji olarak hep ihraç ediyoruz, kullanımda da çok iyiyiz, bunları da söylüyoruz. Peki ama pragmatik olarak siz yapın diye kurumlara görevler, ödevler vermenin dışında buradaki insanları biz nasıl destekleyeceğiz? Merkezi idare ne yapacak? Belki buralardan bakmak lazım."

Volkan ERTÜRK

"Araba üreteceksen önce iki tekerlekli ittirilebilen scooter yap, onun problemini gör, üç tekerleklisini yap sonra motorlu bir tane mobilet yap" derler. Yani aşama aşama üret. İki tekerlekli scooter'ı bir haftada yaparsın. Arabayı iki yılda yapacaksan bile en azından her zaman elinde çalışan bir prototip olur. Pratik olarak mesela Kubilay "Tehdit odaklı bakmayalım; olay odaklı, yetenek bazlı bakalım" dedi. Mesela bir tane olay seçilsin. Örneğin, elektrik. Elektrik bizim için çok kritik.

(E) Tuğgeneral Mesut Bedri Usta

Bir parantez açalım, Cambridge Üniversitesi'nin ABD için yaptığı araştırmada ABD'deki siber saldırıların yüzde 32'si elektrik sistemlerine yönelik olmuş.

Volkan ERTÜRK

Elektrik sisteminin güvenliği için ulusal bazlı neler yapılabilir? Bu olay elektrik sistemimizi hedef alıyor. Bunun içinde özelleştirilen yapılar da var. TEDAŞ var. Somut olarak buradaki sistemin güvenlik seviyesini bir birim artırmak için neler yapacağız? Elektrik dağıtımını almak iyi olabilir belki. Ufak bir şeyle başlayalım, onu iyileştirelim, ondan sonra onun başarı hikâyesini yapalım. Bir değişim ajanı yapalım, onun etrafında daha büyük şeyleri hayata geçirmek için çabalayalım.

(E) Korgeneral Alpaslan ERDOĞAN

Çok teşekkür ederiz, çok güzel bir yaklaşım. Diğer bir konumuz olan, siber güvenlik yazılımları ve programlarının testleri nasıl yapılmaktadır? Test prosedürleri nasıl belirlenmektedir? Bunu da spesifik olarak -TR-TEST'in artık yeni konularından birisi olduğu için- Mustafa Bey size soruyoruz. Eğer ilave katkı olursa Kadir Murat Bey'den de katkı alabiliriz.

Mustafa YILMAZ

Bahsi geçen testlerin nasıl yapılması gerektiği ve tespit aşamasından bahsedecek olursak, daha iyi anlaşılması açısından konuyu belki bir üst çerçeveye taşımak daha farklı olabilir. Test faaliyeti aslında bir nevi uygunluk değerlendirme faaliyetidir. Uygunluk değerlendirmesinin de İSO'da tanımı şu şekilde geçer: "Bir ürün, proses, sistem, kişi ve kuruluş ile ilgili belirli şartların karşılandığının ispatı." Bu ürün de olabilir, proses de olabilir, kişi ve kuruluş da olabilir. Tabii uygunluk değerlendirmesinin alt kırılımları var. Birkaçından bahsedeyim. Birinci taraf, bu hizmeti sağlayanın kendini geliştirme sürecinde yaptığı testler veya faaliyetler olarak değerlendirebiliriz. İkinci taraf da hizmeti yapan taraf var ama hizmeti kullanan bir kişi veya o hizmeti satın almayı düşünen bir kişi tarafından yapılan şey. En kıymetlisi üçüncü taraf uygunluk değerlendirme faaliyetidir. Bu da şu demektir: Konu veya hizmetten bağımsız olarak üçüncü taraf tarafından yapılan bir faaliyettir.

Bunun altında uygunluk değerlendirmesinin birkaç formu var. Test bunlardan bir tanesidir. Bir diğeri belgelendirmedir. Bir diğeri de *inspection* denilen, muayene olarak çevrilen bir faaliyettir. Ana formları bu şekildedir. Yani uygunluk değerlendirmesi ile birlikte bu faaliyetler ihtiyaca binaen yapılır. Tabii biraz önce Kani Bey aslında biraz değindi; bizim ülkemizde siber güvenlik testi deyince genellikle sızma testi olarak algılanıyor ve onunla sınırlı kalıyor. Sızma testi belirlenen sistemin güvenlik açısından analiz edilmesi, sistemin güvenlik açıklarının, güvenlik boşluklarının bulunması, bu açıklıklardan faydalanarak sistemlere sızılması şeklinde ifade edilir. Burada hedeflerden biri de kötü niyetli kişiler tarafından istismar edilmesini önlemektir. Tabii bunun yetkili ve yasal olarak yapılması önemlidir.

Ülkemizde ve dünyada da ciddi çalışmalar vardır. Bunlardan bahsedecek olursak; STM'nin de kurucu üyeleri arasında yer aldığı European Cyber Security Organisation -ECSO diye bir organizasyon var. Bu organizasyon Belçika'da 2016 yılında kurulmuş kâr amacı gütmeyen ve kendi kendini finanse eden bir kuruluş. ECSO'nun altında bazı çalışma grupları var. Açıkçası ben bu çalışma gruplarını eskiden beri incelerim. Benim âcizane kanaatim, *Working Group 1*, bu anlamda belki dünyadaki en kapsamlı çalışmalardan biri. Standardization Certification And Supply Change Management diye bir çalışma grubu var...

(E) Korgeneral Alpaslan ERDOĞAN

STM olarak biz katılıyor muyuz bu gruplara?

Kadir Murat BİÇER

Evet, STM üye olarak bu çalışmalara katılıyor. ECSO'da altı alt çalışma grubu var. Bu altı grup içerisinde farklı sorumluluk alanlarındaki çalışmalar devam ediyor. Bu çalışma gruplarında; standardizasyon, pazarlama, eğitim ve farkındalık ve yeni teknolojiler gibi siber güvenliğin farklı fonksiyonlarına yönelik çalışmalar yürütülüyor. Biz de bu çalışma gruplarına katılmaya çalışıyoruz. STM, ayrıca tüm grupların bağlı olduğu yürütme

"STM'nin de kurucu üyeleri arasında yer aldığı European Cyber Security Organisation'da (ECSO) altı alt çalışma grubu var. Bu altı grup içerisinde farklı sorumluluk alanlarındaki çalışmalar devam ediyor. Bu çalışma gruplarında; standardizasyon, pazarlama, eğitim ve farkındalık ve yeni teknolojiler gibi siber güvenliğin farklı fonksiyonlarına yönelik çalışmalar yürütülüyor. Biz de bu çalışma gruplarına katılmaya çalışıyoruz. STM, ayrıca tüm grupların bağlı olduğu yürütme kurulunda da görev alıyor. Toplantılarına dahil oluyor. Buradaki toplantılar ağırlıkla Belçika'da ve birer günlük çalışma grubu toplantıları şeklinde gerçekleşiyor. Yapılan faaliyetlerin çoğu zaten AB'nin siber güvenlik operasyonlarına yönlendirici oluyor."

Kadir Murat BİÇER

kurulunda da görev alıyor. Toplantılarına dahil oluyor. Buradaki toplantılar ağırlıkla Belçika'da ve birer günlük çalışma grubu toplantıları şeklinde gerçekleşiyor. ECSO konusu açıldığı için ben devam etmek istedim. Yapılan faaliyetlerin çoğu zaten AB'nin siber güvenlik operasyonlarına yönlendirici oluyor.

Mustafa YILMAZ

ECSO Working Group 1'in altında bu standardizasyon ve sertifikasyon ile alakalı kapsamlı bir dokümanı var. Dediğim gibi biz zaman zaman işimiz gereği test ve sertifikasyon uygunluk değerlendirme faaliyetleriyle bir fikir sahibi oluyoruz, ülkelerle görüşüyoruz vs. ama burada tüm ülkedeki özellikle Avrupa'daki ve dünyadaki yapıyı standardize etmişler. Birkaç başlıktan bahsedeceğim. Genel IT ürünleri için standartlar ve şemalar var; Fransa'dan, Ortak Kriterlerden, Singapur'da yapılan çalışmalardan bahsediyor. Endüstri 4.0 ve diğer alanlardaki standartlardan bahsediyor. Enerji ağları ve akıllı şebekeler alanındaki standartlardan ve yapılardan bahsediyor. Telekom, medya ve içerikle alakalı, ödeme endüstrisiyle alakalı standartlardan bahsediyor. Bunların bir kısmı bazı ülkelerde bir kısmı bizim ülkemizde de yapılıyor, birazdan örnek vereceğim. Kriptografik modüller, IoT uygulamaları, IoT ürünleri, Bulut Servis Sağlayıcıları gibi farklı farklı standartlar var; konu uzun olduğu için detayına girmeyeceğim. Servis sağlayıcılar ve organizasyonlar ekseninde IT alanında bunlardan bahsediyor. 27001 gibi standartlar da bu çalışmaların içerisinde. Hakikaten kapsamlı bir şey.

Peki, biz bunlardan hangilerinde varız diye konuşacak olursak, şunu söyleyeyim. Çok detaylı bir şey. Her ülke hepsinde yok ama Ortak Kriterlerde biz ülke olarak bu işin içerisinde yer alıyoruz. Bu test mekanizması nasıl işliyor, ondan bahsedeyim. Burada bir belgelendirme kuruluşu var, bir laboratuvar var, bir de üretici var. Üçlü bir sacayağından oluşuyor. Üretici diyor ki, "Benim bir ürünüm var ve ben bu ürünle alakalı şöyle bir güvenlik seviyesinde olduğunu iddia ediyorum" diyor ve belgelendirme otoritesine başvuruyor. Belgelendirme otoritesi de üreticiye kendisinin onay verdiği laboratuvarlardan birini seçmesini söylüyor. Tabi laboratuvarlar için ön koşullardan birisi de ISO IEC17025 laboratuvar akreditasyonunu almak. Sonra bu üçlü döngü ve değerlendirmeler başlıyor. Ortak kriter süreci hakikaten çok kapsamlı. Şöyle örnek vereyim ben sertifika alması bir buçuk, iki yılı bulan ürünlere bizzat şahit oldum. Belirli seviyeler var. EAL (Evaluation Assurance Level) 4 seviye diye bir seviye var, zaten her şey normal şartlar altında gitse ve tüm taraflar bilinçli bir şekilde hareket etse de orada yedi sekiz ayı bulur. Bu test sürecinde altı ana başlık var. Bir tanesi ürünün tanımlandığı, tehditlerin, varsayımların tanımlandığı bir doküman var, buna bakılıyor. Ürünün yaşam döngüsüne bakılıyor. Kılavuz dokümanlarına bakılıyor, test yapılıyor ve ürüne yönelik *hacker* saldırısı gibi bir saldırı gerçekleştiriliyor. Aslında baktığımız zaman test sürecinde T sıfır anından (ürünün başlangıç

anından), nihai aşamaya kadar olan süreçlerdeki döngülere bakılıyor ve değerlendiriliyor. Bu kıymetli. Ama bunun dezavantajları da var. Uzun zaman alıyor, ciddi bir emek ve ciddi bir maliyet de getiriyor. Yurtdışında özellikle bizim temasta bulunduğumuz ülkelerde şunu gördük: Eğer üretici yurtdışına ürünü satacaksa genellikle "Git, ortak kriter sertifikasını al" diyor; "31 ülkede de geçerli". Eğer ülke içindeki pazarda satmayı düşünüyorsan, çok kritik bir ürün değilse, "Gel benim farklı bir sertifikasyonumu yap" diyor.

Bu noktada biz TR-TEST olarak şu çalışmayı yapıyoruz: Siber güvenlik kümelenmesinde 136 tane üye firmalardan bahsedildi. Bu üye firmalarımızın çeşitli ürün gruplarında ürünleri var. Biz ne yapıyoruz bu çalışmamızda? Yerli ve milli ürün ve hizmet sunanların test kısmını organize ediyoruz. Bunu yaparken de ilk yaptığımız şey şu: Üreticilerle beraber ürün grubu bazında toplantılar yapıyoruz. Yani *firewall*'cu kaç tane var ülkemizde? Diyelim yedi tane var. Yedisini bu ortamda toplayıp bir günlük çalıştay yapıyoruz. Ve kriterleri oluşturmaya çalışıyoruz. *Firewall* da altı ay gibi kısa bir sürede farklı farklı ürün gruplarında 47 tane çalıştay organize ettik. 47 çalıştay da 47 iş günü demek. 47 iş gününde Firewall'u, SIEM 'iDLP'si, uç nokta güvenliği, tehdit istihbarat, güvenli mesajlaşma, zafiyet yönetimi gruplarının kriterlerini tamamladık. Biz bir taraftan da bu kriterleri ülkemizde test edebilecek mevcut altyapılardan da teklifler alıyoruz. Bu teklifleri alıp SSB ile birlikte değerlendirdikten sonra bu laboratuvarlarla sözleşme yapıyoruz, sözleşmeden sonra da test sürecini başlatıyoruz. Bu anlamda *firewall* DLP ve SIEM de süreçleri başlattık, diğerlerinden de teklifleri topluyoruz. Test süreci nasıl işleyecek? Kriterler oluşturuldu, laboratuvarın ilk işi bu kriterlerin nasıl test edileceğine dair çalışmayı yapıyor. Yani bir test metodolojisini oluşturuyor. Test metodolojisini oluşturduktan sonra biz tekrar üreticileri bir araya topluyoruz, "Sizin ürününüz bu test metodolojisine göre test edilecek, uygun mudur" diye mutabakat toplantısıyla madde madde üzerinden geçiyoruz ve ardından test sürecini başlatıyoruz. Ülkemizden soruda bahsi geçen yerli ürün ve hizmetlere karşı yürütülen test sürecini bu şekilde organize ediyoruz. Bunu neden böyle yaptık? Güney Kore, Fransa, İspanya gibi ülkelerde de benzer yapılar var. Güney Kore ihracatçılar için ortak kriterleri şart koşarken, kendi içindeki yapı için de aynı bizim yaptığımız gibi çalışmayı onlar daha önce yapmışlar.

(E) Korgeneral Alpaslan ERDOĞAN

Bizim bu kapsamda test yaptığımız kaç tane ürün oldu?

Mustafa YILMAZ

Sürecini başlattığımız üç ürün grubu var. *Firewall*, SIEM ve DLP. Yalnız şöyle bir sıkıntı var. Biz laboratuvarlarla belirli bir noktaya getirdik ama açık konuşmak gerekirse yerli üreticilerimiz kriter oluşturma sürecindeki hızı test sürecinde maalesef göstermiyorlar. Biz, "Bunu sizlerle birlikte oluşturduk, bir an önce teste getirin" diyerek biraz sıkıştırıyoruz açıkçası. Ürün gruplarını şu an bekliyoruz. Diğer ürün gruplarında da tekliflerimizi ve değerlendirmelerimizi yapıyoruz. Ama yerli üreticilerimiz biraz teste getirme noktasında yavaş davranıyor. SSB'nin bu anlamda ciddi bir finansman desteği var. Ayrıca şunu da belirtmek lazım; biz ülke olarak siber güvenlikte uygunluk değerlendirme faaliyetlerine ciddi bir önem vermek durumundayız.

Kadir Murat BİÇER

Mustafa Bey de bahsetti, TS/ISO15408 Ortak Kriterler, bu konuda uluslararası geçerliliği olan bir sertifikadır. Yazılım test konusunda eğer ihracat ve globalde tanınmak gibi niyet varsa biz olaya bu şekilde yaklaşıyoruz. Zaten STM olarak Şubat 2019'dan bu yana Ortak Kriterler test laboratuvarımız devrede ve testlerimizi yapıyoruz. Onun dışında, sızma testlerine paralel söylemek istediğim teknik testler de var. Burada da kaynak kod analizi ve güvenli yazılım geliştirme, özellikle güvenli yazılım oluşturmada ilk yazılım geliştirme sürecinin başlangıcından itibaren önem arz ediyor. Genelde

önce uygulamayı yapıyoruz, arkasından güvenliği için uğraşıyoruz ya da uygulamanın başına bir şey geldiği zaman güvenlik aklımıza geliyor. Uygulama hep önden gittiği için, uygulama henüz daha yayınlanmadan önce testlerin, sadece sızma testi olarak değil de kaynak kodunun analiz edilmesi, uygulama içerisinde herhangi bir atak yüzeyi olup olmadığının incelenmesi ve yapılan bir iyileştirme varsa o iyileştirmeler yapıldıktan sonra yazılımın piyasaya çıkmasını öneriyoruz.

(E) Korgeneral Alpaslan ERDOĞAN

Bizim burada kendi laboratuvarımızda mı gerçekleştiriyoruz bu testleri, yoksa akredite olan laboratuvarları kullanarak mı yapıyoruz?

Kadir Murat BİÇER

Eğer ki ortak kriterler test merkeziyle ilgili EAL 4+ seviyesinde bir güvenlik sertifikasyon ihtiyacı varsa, kendi laboratuvarımızda gerçekleştiriyoruz. Burada laboratuvarın fiziksel olarak da belirli yükümlülükleri var, onları da yerine getirmemiz gerekiyor. Oradaki kodların saklanması, giriş çıkışlar ve her türlü dokümantasyon bulunması dahil

"STM olarak Şubat 2019'dan bu yana Ortak Kriterler test laboratuvarımız devrede ve testlerimizi yapıyoruz. Onun dışında, sızma testlerine paralel söylemek istediğim teknik testler de var. Burada da kaynak kod analizi ve güvenli yazılım geliştirme, özellikle güvenli yazılım oluşturmada ilk yazılım geliştirme sürecinin başlangıcından itibaren önem arz ediyor. Genelde önce uygulamayı yapıyoruz, arkasından güvenliği için uğraşıyoruz ya da uygulamanın başına bir şey geldiği zaman güvenlik aklımıza geliyor. Uygulama hep önden gittiği için, uygulama henüz daha yayınlanmadan önce testlerin, sadece sızma testi olarak değil de kaynak kodunun analiz edilmesi, uygulama içerisinde herhangi bir atak yüzeyi olup olmadığının incelenmesi ve yapılan bir iyileştirme varsa o iyileştirmeler yapıldıktan sonra yazılımın piyasaya çıkmasını öneriyoruz."

Kadir Murat BİÇER

"Ortak Kriter alanında Türkiye'de laboratuvarlar var. Biri TÜBİTAK'ın BİLGEM'i, biri STM, biri BEAM Teknoloji, bir de Certby diye bir firma ve TSE içinde de Ortak Kriterler Lab'ı var. Hepsi TÜBİTAK'tan ISO IEC 17025 Laboratuvar akreditasyonunu almış, aynı zamanda TSE tarafından lisanslanmış firmalar. TSE'nin yurtdışında çalıştığı ABD'de CygnaCom diye bir laboratuvar var. İspanya'da Epoche ve Espri Hollanda'da Brightsight BV diye bir laboratuvar var."

Mustafa YILMAZ

-ki onlar da TSE tarafından belirli dönemlerde denetleniyor. Ama bunun haricinde söylediğim kaynak kod analizi veya yazılım güvenliği gibi teknik testlerle ilgili çalışmaları, kurumlar genelde kodlarını dışarı çıkarmak istemediği için kurumların yerinde, kendi kaynaklarımızı oraya götürüp orada gerçekleştiriyoruz. Ama Ortak Kriterler için testleri kendi laboratuvarımızda yapıyoruz.

Mustafa YILMAZ

Ortak Kriter alanında Türkiye'de laboratuvarlar var. Biri TÜBİTAK'ın BİLGEM'i, biri STM, biri BEAM Teknoloji, bir de Certby diye bir firma ve TSE içinde de Ortak Kriterler Lab'ı var. Hepsi TÜBİTAK'tan ISO IEC 17025 Laboratuvar akreditasyonunu almış, aynı zamanda TSE tarafından lisanslanmış firmalar. TSE'nin yurtdışında çalıştığı ABD'de CygnaCom diye bir laboratuvar var. İspanya'da Epoche ve Espri Hollanda'da Brightsight BV diye bir laboratuvar var.

(E) Albay Kani HACIPAŞAOĞLU

Toplantıya katkısı olacak bir dipnot düşeceğim. Şimdi bu testler ürün bittikten sonra yapılıyor. Fakat işin enteresan tarafı şu: Siber güvenlikte ürün geliştirmiş birisi olarak arz ediyorum; burada "Ortak Kriter" dediğimiz konuda güvenlik testleri EAL 1, 2, 3, 4, 5 diye geçiyor. EAL diye geçen, *Evaluated Assurance Level*, yani güvenlik değil, güvenirlik seviyesi. Dolayısıyla, güvenliği de kapsayan ve değişik seviyelerde üretilecek ürünün güvenirliği konusunda uzun ve zor testler. Bu nedenle, siber güvenlik ürünü geliştirme sürecinde bu testlerdeki kriterlerin göz önünde bulundurulması, ürün tamamlandığında yapılacak test ve sertifikalandırma için kolaylık ve avantaj sağlıyor.

Volkan ERTÜRK

Ben sertifikasyonlara inanmıyorum. Sebebi de şu: Teknolojiler çok hızlı şekilleniyor. Amazon'un web sitesinin güncelleme frekansının hızını biliyor musunuz? Bir saniye. Yani her saniye yeni bir versiyon çıkıyor. Bu kadar hızlı *deployment*'lar var, çevik geliştirme yaklaşımları var. Her hafta kod çıkartma, yani her hafta ürün versiyonunu güncellemeyen firmalara yavaş firma, dinozor deniyor. O yüzden, şöyle bir konu var, sizin bu teste soktuğunuz yazılımın versiyonu sabit bir yazılım...

(E) Korgeneral Alpaslan ERDOĞAN

11-12 ay sürünce o sistem çoktan eskimiş oluyor.

Volkan ERTÜRK

Eskimiş oluyor. Mesela ben eskiden ticari ürünlerden satıyordum; şu versiyon bizde şu sertifikaya sahip. Ama ben o versiyonda kalmak istemiyorum ki, o versiyonun özellikleri eski kalıyor. Ben yeni özellik istiyorum. O zaman bunu kuracaksın ama oraya geçeceksem o test edilmemiş.

Mustafa YILMAZ

Dediğiniz problem güncel ve gerçekçi bir problem. Sertifikaların geçerliliğiyle alakalı konu, Ortak Kriterler uluslararası toplantılara katıldığımızda en fazla tartışılan ve sonuç alınamayan, her yıl

da gündem olan konulardan biridir. Hiçbir zaman çözülemiyor, ülkelerin farklı yaklaşımları var. Şu an son halini bilmiyorum ama İngiltere'nin mesela bir ara şöyle bir yaklaşımı vardı: "Ben sertifikayı veriyorum ama bu sertifika sadece o an itibarıyla geçerli". Çünkü yeni tehditlere, yeni güncel saldırılara cevap vermiyor. Güney Kore üç yıllık bir süreç veriyordu. Ülkemizde de öyle yapılıyordu. Sertifikan üç yıl geçerli ama yeni bir tehdit çıkarsa benim üreticiyi çağırma hakkım var. Gerekirse teste sokma hakkım var.

Volkan ERTÜRK

Bu beklediğimiz pragmatik ve somut faydayı sağlamaktan uzak çünkü...

Mustafa YILMAZ

Siber güvenlik doğası, bilişim ürünlerinin doğası. Mesela bir bakanlığa ürün geliştiren adam bana diyor ki, "Hocam sen bana bunu söylüyorsun ama sen söyledikten iki saat sonra ben yazılımı güncelliyorum, çünkü bakanlık sürekli mevzuat yayınlıyor." Böyle bir husus var. Fakat "Sertifikalara inanmıyorum" hususunu kesinlikle kabul edemiyorum. Sertifikaların kesinlikle çok önemli olduğunu düşünüyorum.

Volkan ERTÜRK

Ben teste sokacağım ürünün bir versiyonunu hazırlarım, veririm; ertesi gün yeni versiyon yaparım.

Mustafa YILMAZ

Orada da etki analizi raporu gibi bir yaklaşım var. Her ne kadar sizin dediğinizi karşılamasa da şöyle bir şey var: "Sen güncelleme mi yaptın, bana etki analizi raporunu getir" diyor. Burada güvenliği etkileyen fonksiyonlar var mı, yok mu; bakılıyor. Eğer varsa güvenlik testine girmesi gerekiyor ama dediğiniz doğru, çok efektif olmuyor. Sertifikanın şöyle bir faydası var: Sertifika üçüncü tarafa, alıcı tarafa bir güven tesis ediyor.

(E) Korgeneral Alpaslan ERDOĞAN

Güven tesis ediyor mu, çok fazla güvenilir mi? Devam eden o güncellemeler kapsamında demek ki geçerlilik süresi çok da fazla uzun olamıyor. Belki de İngilizlerin yaklaşımı bu kapsamda daha doğru. "Ben sana bu sertifikayı şu anda veriyorum" diye.

Kadir Murat Biçer

Bu sadece Ortak Kriterler için değil, bütün test faaliyetleri için geçerli. Sızma testini bugün yaptırdığınız zaman da, o sızma testi o anda yapılmış, anlığın fotoğrafını çeker. Ertesi gün güncelliği garanti değildir.

Volkan ERTÜRK

Sürekli değerlendirmeye geçiliyor, o yüzden pentest otomasyonu gibi şeyler konuşuluyor.

Kadir Murat Biçer

Zaten pentest otomasyonu Bugshield platformu gibi. Bizim zafiyet bulma, sürekli sızma testi Bugshield platformuyla bu faaliyetlerin belirli dönemlerde yapılmaması, sürekli yapılması hedefleniyor. Çünkü regülasyonlara baktığınız zaman finans kuruluşları olsun, enerji dağıtım şirketleri olsun, bankalar olsun, bunlar belli dönemlerde yılda iki defa sızma testi yaptırıyor. Ama regülasyon sadece o dönem değil o gün yaptırdığını kapsar. Sürekliliği yoktur. Bu maalesef her sektörde karşımıza çıkıyor ve biz de bu testlerin sürekliliği için BugShield platformumuzu öneriyoruz.

Dr. Attila ÖZGİT

Ben de aykırı bir cümle söyleyebilir miyim? Ülkede üretilen yazılım belli bir sayısal noktaya gelsin de test tek dersimiz olsun.

(E) Korgeneral Alpaslan ERDOĞAN

Diğer bir konu; siber güvenliğe sosyolojik ve psikolojik boyutlarıyla bakıldığında siber suçlu olma hali, suçlu davranışının arkasındaki kök nedenler nelerdir?

Kubilay Onur GÜNGÖR

Biz mesela sertifika programında da kriminolojiye girerken ilk önce bir soru cümlesiyle başlıyoruz: "Siber suçlar kriminal aktivitenin devamı mıdır, yoksa kendine has ayrı bir kriminal alan mıdır?" Bazı kişiler aslında siber suçlu ama siber saldırıya yönelik bir bilgileri yok. Mesela adam normal hayatında da dolandırıcı ve şöyle diyor: "Siber diye bir şey çıkmış, internet diye bir şey çıkmış ben buradan da kandırırım adamları" diyor. Aslında bir kanal olarak kullanıyor. Kendisi sadece siber suçlu değil, suçlu zaten. Bazı durumlarda da siberin kendine has suç yarattığı alanlar ve yöntemler var. Şimdi hal böyle olunca, normalde kinetik hayatta insanı suça iten faktörler neyse bunların hepsi siber dünya için de geçerli.

Burada daha çok iki noktada genelleme yapılabilir... Yapısal teoriler, suçu açıklayan teoriler var; bir de öğrenmeye yönelik teoriler var. Yapısal teorilerde her zaman ilk söylenen şey aslında sosyolojik; toplumlarda bazı insanlar istedikleri şeylere kolaylıkla, rahatlıkla ulaşırken bazıları ne yaparsa yapsın ulaşamıyor. Bu da onlarda bir tansiyon yaratıyor. Ve bu tansiyon ya bireysel suça dönüşüyor ya da bu tansiyonu ortak yaşayan insanlar bir araya geliyor, bir şekilde organize suça dönüşüyor. Bunun haricinde statü veya toplumun başarı kriteri, başarı tanımı yine suçun oluşmasına destek oluyor. Bazı toplumlar, örneğin ABD' de mafyanın çok yükseldiği ailelerin olduğu dönemlerde "başarı eşittir para, başarı eşittir güç" kodlaması aslında suç oranını ciddi şekilde artırıyor. Çünkü insanlar bulunduğu ortamlarda statü sahibi olmak istiyorlar, gücü elinde bulundurmak istiyorlar vs. Bunun haricinde aslında en önemli şeylerden biri de şu: Bir suçun oluşabilmesi için suçun ortamının var olması gerekiyor, o suçun bilinmesi gerekiyor ve ilgili motivasyonunun paylaşılması gerekiyor. Burada siber dünyayı ayıran en önemli şeylerden biri aslında suçlunun suça daha hızlı karışmasını sağlaması. Normalde kinetik hayatta diyelim ki siz hayatınızda hiç ateş etmemişsinizdir ya da düğünlerde havaya ateş etmişsinizdir ama gidip kadın cinayeti işliyorsunuzdur. Ama siber dünya öyle değil, siber dünyada siz sanki bir polis gibi taktik eğitim alıyorsunuz ve bu eğitimin aynısı aslında suç için de kullanılıyor. Dolayısıyla suçu nasıl işleyeceğinizi çok iyi öğreniyorsunuz. Bu durum suça karışmayı gittikçe hızlandırıyor.

Bunun haricinde şunu söyleyebilirim: Bir de olayın politik, siyasi, etnik tarafları var. Yine orada da suçun bir başka açıklaması da başarısız sosyalleşme olarak ele alınıyor. Başarısız sosyalleşmenin sonucunda çeşitli etnik yapılar veya politik tabanlı görüşler bir şekilde yine tansiyon oluşturup politik ya da etnik suçlara yönelebiliyor. Birbiriyle çelişen değerler yine insanları suça teşvik ediyor. Yine suçun aslında öğrenildiği yer çoğunlukla organize alanlar. Bu kısmı gerçekten çözülmesi çok zor bir problem çünkü aslında suç organize örgütlerin içerisinde öğreniliyor ama biz bunları güvenlik diye öğretiyoruz, çünkü öğretmek zorundayız. Bireylere, bireysel güvenliği öğretmek için gayrinizami harp öğrettiğinizi, silah kullanmasını ve bomba yapmasını öğrettiğinizi düşünün, sonra da suçla mücadele etmeye çalıştığınızı düşünün. Aslında sürekli kendi suçlumuzu yetiştiriyoruz... Dolayısıyla o bir ikilem içerisinde ilerliyor, bu da suça yönelik önemli bir konu.

Bir de öğrenme teorileri var, sosyal öğrenme vs. Burada da modadaki bir kıyafeti taklit etmek gibi suçu taklit etmek yatıyor. Siber dünya bunun için çok uygun. Suça ittirmede şu da önemli: Mesela terör bölgesinde taş atan çocukları görürdük televizyonlarda eskiden, yüzleri hep gülerdi dikkat ettiyseniz. Çünkü aslında o taşı atıp arka tarafa gittiği zaman mahallenin ağabeyi ona "Aferin" der ve çoğunlukla taş atarken oyun oynadığını zanneder, yaptığı şeyin bir suç olduğunu bilmez. Dolayısıyla bulunduğu o yapıda o hareket normalize edilmiştir ve ödüllendirmeye başlamıştır. Siber dünyanın doğasında bu da var. Siz bir yeri *hack*'lediğiniz zaman, mesela Red Hack örneği... Aslında bir suç işleniyor ama toplumun belirli bir

kesimi bu suçu yüceltebiliyor, ödüllendirebiliyor. Veya bir yerleri *hack*'lemek dâhilik, çok büyük bir yeteneğin bir sonucuymuş gibi düşünülüp kişileri buna teşvik edebiliyor. Yine toplumsal mimleme de suça itebiliyor. Bazı uyanıklık ya da dolandırıcılık durumlarında bunları yapan için "Aa ne zeki adam" derler ya, o mantıkla siber dünya buna çok uygun. Yaptığınız herhangi bir siber faaliyetin suç unsuru oluşturmasıyla sıradan halk ilgilenmiyor. Onu şöyle mimliyor "Aa, zeki çocuk, nasıl düşünmüş, cingöz" vs. sürekli bir olumlama var, bu da otomatikman itiyor.

"Bir suçun oluşabilmesi için suçun ortamının var olması gerekiyor, o suçun bilinmesi gerekiyor ve ilgili motivasyonunun paylaşılması gerekiyor. Burada siber dünyayı ayıran en önemli şeylerden biri aslında suçlunun suça daha hızlı karışmasını sağlaması. Siber dünyada siz sanki bir polis gibi taktik eğitim alıyorsunuz ve bu eğitimin aynısı aslında suç için de kullanılıyor. Dolayısıyla suçu nasıl işleyeceğinizi çok iyi öğreniyorsunuz. Bu durum suça karışmayı gittikçe hızlandırıyor."

Kubilay Onur GÜNGÖR

(E) Korgeneral Alpaslan ERDOĞAN

Teşekkürler. Şunu sormak isterim: Siber güvenlik ve siber saldırıyı etkileyen önemli faktörler nelerdir? Örneğin, yetişmiş insan kaynağı, eğitim, fiziksel altyapı, mevzuat vs. çerçevesinde değerlendirmenizi almak isteriz.

Dr. Attila ÖZGİT

Yine aykırı bir cevapla başlayayım. Türkiye olarak insan, yetişmiş insan kaynağı, eğitim, fiziksel altyapı ve mevzuat, hepsinden sınıfta kaldık.

Siber Akademi diye SSB'nin başlattığı oluşumun ilk döneminde epey bir katkı vermiştim. Sonra o nereye evrildi takip etmedim ama oradaki

değerlendirmelerimizde yukarıdan aşağı doktora seviyesinde bilgi sahibi olmaktan işin teknisyeni olmaya kadar giden insan gücünün her yerinde eksiğimiz olduğunu gördüm. Bunları yetiştirmek için kurulan yapıların zayıflığı -ki örnekleyecek olursak, kendi üniversitem dahil bugün önde gelen üniversitelerimizde siber güvenlik adına üç, beş hocayla sınırlı yapılar görüyorsunuz. Tabii bu çok sayıda öğrenciyi yetiştirmek için yeterli değil. Bir de çok hızlı gelişen bu alanda özellikle pratik eğitim vermek için bir pratisyene, yani işin akademisyenlerine değil de daha güncel, pratik alanda yaşayan eğitimcilere ihtiyacımız var.

(E) Korgeneral Alpaslan ERDOĞAN

Silahlı Kuvvetlerde buna "alaylılar" diyoruz hocam. İşin akademik tarafından değil de pratikten, uygulamadan gelenler.

Dr. Attila ÖZGİT

Aslında tam anlamıyla bire bir alaylıyla da örtüşmüyor. Evet bir kısmı alaylı ama bir kısmı da başka disiplinlerde okumuş ama hızla bu alana devşirilebilecek insanların siber güvenlik alanında pratik bir şekilde eğitilmesi önemli. Piramit gibi bir yapıya baktığınızda bunun her yerinde çok ciddi eksik var. Doktora, *master* düzeyinde işin mekteplilerini eğitmeye kalktığınızda bile işgücünüz yok. Önce öğretim üyesi almanız lazım; üç, beş sene sonra eğitimin kalitesini ve sayısını arttırmanız lazım, kendi rektörlüğünüzün gündemine girip siber güvenliğin o üniversite içinde önemli bir şey olduğunu anlatmanız lazım. Sonra YÖK'e gidip, "Bu alan için ayrı kontenjan istiyorum" demeniz lazım. Dışarıya insan kaçırmayacak biçimde, belki bu konuya önem veren bazı üniversiteler, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, SSB gibi işin devlet tarafından sahip unsurlarını da yanlarına alarak, "100-200 adet doktoralı, yüksek lisanslı çok kaliteli adam yetiştireceğim, burs vereceğim, bursun kaynağını nereden bulacağım?" diyerek YÖK'ten kadro istenebilir. Belki o kaynak YÖK olmayacak, SSB ya da Cumhurbaşkanlığı olacak. Ama öyle bir yapı kurmalısınız ki bundan bir sene önce bir anda Hollanda'ya giden 600 tane ASELSAN mühendisi gibi bir olguyu bir daha bu ülkede yaşamayasınız. Dolayısıyla "Siber güvenlik yetenekleri kazandıktan sonra da ben herhangi bir Avrupa ülkesine giderim" anlayışı tabii ki olmamalı. İyi para verip, iyi üniversitelerde iyi eğitim aldırıp sözleşmelerle bağlayıp ve iş garantisi vererek bunu modellemeniz lazım.

"Türkiye olarak insan, yetişmiş insan kaynağı, eğitim, fiziksel altyapı ve mevzuat, hepsinden sınıfta kaldık. Yukarıdan aşağı doktora seviyesinde bilgi sahibi olmaktan işin teknisyeni olmaya kadar giden insan gücünün her yerinde eksiğimiz olduğunu gördüm. Bunları yetiştirmek için kurulan yapıların zayıflığı -ki örnekleyecek olursak, kendi üniversitem dahil bugün önde gelen üniversitelerimizde siber güvenlik adına üç, beş hocayla sınırlı yapılar görüyorsunuz. Tabii bu çok sayıda öğrenciyi yetiştirmek için yeterli değil. Bir de çok hızlı gelişen bu alanda özellikle pratik eğitim vermek için bir pratisyene, yani işin akademisyenlerine değil de daha güncel, pratik alanda yaşayan eğitimcilere ihtiyacımız var."

Dr. Attila ÖZGİT

Kadir Murat BİÇER

Burada bir katkı yapmak istiyorum. Hocam programların ya da lisans programlarının açılmasından bahsetti. Güzel bir örnek olarak Adli Bilişim mühendisliğiyle ilgili lisans programı olan Fırat Üniversitesini vereyim. Lisans programları şu anda yurtdışında yaygınlaşmaya başladı. Ülkemizde de adımlar atıldı, hatta siber güvenlik liseleri kurulması konuşuluyor ki yurtdışında birkaç gelişmiş ülkede bunlar mevcut. Siber

güvenliğin eğitim boyutunda biraz daha düşük yaşlara inmesi, en azından farkındalık derslerinin arttırılması için Milli Eğitim Bakanlığının yaptığı çalışma var. Bunlar, hep bizim yeni yetişecek nesle yönelik yapmış olduğumuz çalışmalar.

Bir de mevcut neslimize göre bazı çalışmaların yapılması gerektiğine inanıyorum. Özellikle 50-55 yaş üzeri Facebook'la tanışmış, WhatsApp'ı görmüş, interneti birazcık öğrenmiş, Instagram'ı bir iki paylaşım yaparak görmüş olan kullanıcılar, şu anda tam o siber saldırganların parayla ilgili motivasyonlarına hitap eden kesim. Hedef kitle. O kesim genelde de kurumsal bir kültür içerisinde de olmadığı için genellikle emekli veya yaşlı, kendi işini yapan, kurumsal bir güvenlik aidiyeti içerisinde de olmadıkları için bu tarz bilinçlendirme ve farkındalık faaliyetlerinden de uzak kalıyorlar ve bu kitle içerisinde bu tarz siber suçlardan mağdur olanlar çok fazla. Ve yine mağdur olmaya devam edeceklerdir. Ama bu kitlenin bilinçlendirilmesi işi de farklı zorlukta. Diğer kurumsal çalışanların bilinçlendirilmesi biraz daha kolay, farkındalık programlarıyla yapılabiliyor ama bu kitlenin bilinçlenmesine yönelik belki kamu spotu şeklinde bazı konuları, temel bilgileri verebilecek, özellikle sosyal medyayı nasıl kullanabileceğiyle ilgili, oltalama saldırılarına karşı nasıl önlem alabileceğiyle ilgili temel bilgileri sunacak ortamların oluşturulmasının bu kitleyi siber saldırganların hedef kitlesi olmaktan kısmen çıkaracağını düşünüyorum. Sadece genç nüfus değil, yaşlı nüfus da siber güvenlikte farkındalık ve eğitim için hedef kitle olmalı kanaatindeyim.

"Özellikle 50-55 yaş üzeri Facebook'la tanışmış, WhatsApp'ı görmüş, interneti birazcık öğrenmiş, Instagram'ı bir iki paylaşım yaparak görmüş olan kullanıcılar, şu anda tam o siber saldırganların parayla ilgili motivasyonlarına hitap eden kesim. Hedef kitle. O kesim genelde de kurumsal bir kültür içerisinde de olmadığı için genellikle emekli veya yaşlı, kendi işini yapan, kurumsal bir güvenlik aidiyeti içerisinde de olmadıkları için bu tarz bilinçlendirme ve farkındalık faaliyetlerinden de uzak kalıyorlar ve bu kitle içerisinde bu tarz siber suçlardan mağdur olanlar çok fazla. Ama bu kitlenin bilinçlendirilmesi işi de farklı zorlukta. Diğer kurumsal çalışanların bilinçlendirilmesi biraz daha kolay, farkındalık programlarıyla yapılabiliyor ama bu kitlenin bilinçlenmesine yönelik belki kamu spotu şeklinde bazı konuları, temel bilgileri verebilecek, özellikle sosyal medyayı nasıl kullanabileceğiyle ilgili, oltalama saldırılarına karşı nasıl önlem alabileceğiyle ilgili temel bilgileri sunacak ortamların oluşturulmasının bu kitleyi siber saldırganların hedef kitlesi olmaktan kısmen çıkaracağını düşünüyorum."

Kadir Murat BİÇER

Mustafa YILMAZ

Mevzuatla ilgili bir iki cümle eklemek isterim. Ülkemizde 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı vardı. Ardından 2016-2019 versiyonu çıkartıldı. Şu an 2020 ve sonrası için bir ulusal siber güvenlik stratejisi eylem planı ihtiyacı var. Duyduğumuz kadarıyla Cumhurbaşkanlığı Dijital Dönüşüm Ofisi bu anlamda çalışıyor. Rehber çalışmaları var, bu da çıkarsa en azından faydalı olur. Yetişmiş insan kaynağı, eğitim gibi konu başlıkları hepsi bu strateji belgesinin altında olan başlıklar, ona yönelik politikalar oluyor. Bu strateji belgesi çıktıktan sonra da uygulanması ve denetlenmesi noktasında ciddi bir emek sarf edilmesi gerektiğine inanıyorum. Çünkü denetlemediğiniz şeyi kontrol edemiyorsunuz. Bir de denetlenen tarafın perspektifiyle yaklaşmak istiyorum. Denetlenen tarafın da bu görevleri yapabilmesi için bunun planlaması yapılmalı. Çünkü o kişilerin günlük operasyonlarını

bırakıp bir nevi bu stratejik hedeflere yönelik bir çalışma yapabilmesi için buradan belki ayrılabilmesi, bir insan kaynağının buraya dedike edilebilmesi ihtiyacı var.

(E) Korgeneral Alpaslan ERDOĞAN

Teşekkürler. Siber güvenlik ve siber saldırı konularındaki yatırım ihtiyaçlarına yönelik Türkiye'de ve dünyada neler oluyor? Bu konuda katkılarınızı rica edelim.

(E) Tuğgeneral Mesut Bedri USTA

Baktığınız zaman dünyada en büyük pazar haline gelmeye başladı. O kadar ki şu an neredeyse dünyadaki en büyük insan gücünün ayrıldığı yer siber, siber güvenlik ya da bilişim alanı olmaya başladı. Bizim ülkemizde de öyle. Piyasadaki en rahat iş bulanlar siber güvenlik alanındaki uzmanlar. Nicelik olarak çok olmak bir şeyi değiştirmiyor. Sektörde bir nitelik sorunu olduğunu da görmek lazım. Dünya bunu aşmak için önce bir yatırım planlaması yapmış. İnsan kaynağı planlaması yapmış. Malezya geleceğe yönelik siber alanda personel yetiştirmek için özel bir birim kurmuş, sırf bunun için çalışıyor. Kore yatırımlarını oturtmuş, bilişim alanındaki yatırımlarını yönlendirecek bir grup kurmuş. Bizde her şeyden önce bir organizasyon oluşturmak lazım. Bu işin sahibinin ve yatırımları kimin yöneteceğinin belirlenmesi gerekiyor. SSB bu işleri kısmen yapıyor, siber kümelenme vs. var ama akademik tarafta biraz boşluk var. Bu alanda yatırımları yönlendirecek kurumlara ihtiyaç var. Siber güvenlikten bahsediyoruz değil mi? Ama Telekom altyapımızdaki donanımın yüzde 80'e yakını yabancı şirketlerin. İşletim sistemimiz var mı? TÜBİTAK'ta geliştirilen Pardus var, HAVELSAN bunu ticarileştirmeye çalışıyor ancak halen sınırlı kullanım mevcut. Güvenlik duvarı çok küçük. Şirketlerin "Biz bunu yaptık" dediği birtakım ürünler var. CM öyle. Dolayısıyla siber güvenlik alanında ürün geliştirme sıkıntımız var.

Birçok kurumumuz siber harekât merkezi ya da operasyon merkezi kurarak "Bakın herkes Türkiye'ye saldırıyor, Türkiye hedef ülkelerde ilk 10'da" bilgisi veriyor. Oysa bunların genel güvenliğe katkısı oldukça sınırlı. Bizim yatırım ihtiyaçlarımızı yönlendirmiyor. Bizim ürün yelpazesine ihtiyacımız var. Bunun için de üretime dönen yatırımlar gerekiyor. Eğer Türkiye son 10 yılda hâlâ markalaşmış bir *switch* üretmemişse, hâlâ bir *router* üretmemişse bu bir planlama eksiği gibi görülmektedir. Milli ve yerli ürün konusu yanlış anlaşılmasın, prematüre bir ürün çıkartıp, "Benim ürünüm var, niye kullanılmıyor?" denmemeli. Eğer ürünün sürekliliği, veri bütünlüğünü, erişilebilirliği, güvenliği

"Siber güvenlikten bahsediyoruz ama Telekom altyapımızdaki donanımın yüzde 80'e yakını yabancı şirketlerin. İşletim sistemimiz var mı? TÜBİTAK'ta geliştirilen Pardus var, HAVELSAN bunu ticarileştirmeye çalışıyor ancak halen sınırlı kullanım mevcut. Güvenlik duvarı çok küçük. Bizim ürün yelpazesine ihtiyacımız var. Bunun için de üretime dönen yatırımlar gerekiyor. Eğer Türkiye son 10 yılda hâlâ markalaşmış bir switch üretmemişse, hâlâ bir router üretmemişse bu bir planlama eksiği gibi görülmektedir. Yazılım alanında bizim siber uzayı kodlama alanında da, hâlâ yabancı kaynaklı birtakım başka yazılımlar kullanıyorsak, adli bilişim için hâlâ ABD'li bir şirketin yazılımını kullanıyorsak, veri kurtarmak için hâlâ böyle bir şey yapıyorsak mutlaka oturup bir düşünmemiz lazım. Yani işin özü üretime yönelik çalışmalar yapmak lazım, yoksa harekât merkezi kurarak ekranlarda ne kadar saldırı olduğunu göstermek çözümün parçası olmuyor. Sadece bilgi toplamaya yarıyor."

(E) Tuğgeneral Mesut Bedri USTA

tam olarak sağlamıyorsa, yüzde 98 bağlantı sağlamıyorsa "Benim milli ürünüm var!" demek yeterli değil. Markalaşmış ürünlerden söz ediyorum. Bizim üretim altyapısı çok iyi olan şirketlerimizin bu alanda biraz yatırım yapıp ürün çıkartması gerektiğine inanıyorum. Yazılım alanında bizim siber uzayı kodlama alanında da, hâlâ yabancı kaynaklı birtakım başka yazılımlar kullanıyorsak, adli bilişim için hâlâ ABD'li bir şirketin yazılımını kullanıyorsak, veri kurtarmak için hâlâ böyle bir şey yapıyorsak mutlaka oturup bir düşünmemiz lazım. Yani işin özü üretime yönelik çalışmalar yapmak lazım, yoksa harekât merkezi kurarak ekranlarda ne kadar saldırı olduğunu göstermek çözümün parçası olmuyor. Sadece bilgi toplamaya yarıyor.

"Dünya siber güvenlik pazarının 2025 yılında 250 milyar dolar civarında olması öngörülüyor. Türkiye'nin 2019 siber güvenlik tarafındaki yatırımları yaklaşık 120 milyon dolar civarında. 2025 yılında da bunun 200-220 milyon dolar civarında olması bekleniyor. Dünyaya göre binde bir seviyelerinde. Biz şu an kendi ekosistemimiz içindeki ürünlerin konumlanması anlamında kendimize yetecek kadar yaptığımız için firmalar içeride çok rahat pazar bulamıyor. Firmaların da bu konudaki serzenişi, sektörde yer alan global vendor'lerin tek bir ürünle değil tüm güvenlik bileşenleriyle suit olarak komple gelmeleri. Ortalama bir sistem odasında yönetilen farklı işlemler için 30-35 arasında güvenlik bileşeni var. Böyle olunca da yerli ekosisteminde herhangi bir ürünün araya girme ihtimalinin zor olduğunu söyleyebilirim. Burada ülke olarak biraz daha siber güvenlik yatırımlarının artırılmasının, yatırımların da yerli ekosistem içerinde değerlendirilmesine yönelik çalışmaların genişletilmesinin, Siber Küme ve TR-TEST'in çalışmalarıyla yönlendirilmesinin bütün ürünlerdeki olgunluk seviyesini artıracağını düşünüyorum."

Kadir Murat BİÇER

Kadir Murat BİÇER

Esasında pazar olduğu zaman ürünü geliştirenler çok daha rahat hareket edip kendini çok daha iyi bir konuma getirebiliyorlar. O pazarın oluşturulması önemli.

Dünya siber güvenlik pazarının 2025 yılında 250 milyar dolar civarında olması öngörülüyor. Raporlara baktığımızda, Türkiye'nin 2019 siber güvenlik tarafındaki yatırımları yaklaşık 120 milyon dolar civarında. 2025 yılında da bunun 200-220 milyon dolar civarında olması bekleniyor. Dünyaya göre binde bir seviyelerinde. Bazı ülkeler çok aşırı yatırım yaparken, bazı ülkeler kendine yetecek kadar yapıyor, bazıları hiç yapmıyor. Biz şu an kendi ekosistemimiz içindeki ürünlerin konumlanması anlamında kendimize yetecek kadar yaptığımız için firmalar içeride çok rahat pazar bulamıyor. Firmaların da bu konudaki serzenişi, sektörde yer alan global vendörlerin tek bir ürünle değil tüm güvenlik bileşenleriyle suit olarak komple gelmeleri. Ortalama bir sistem odasında yönetilen farklı işlemler için 30-35 arasında güvenlik bileşeni var. Böyle olunca da yerli ekosisteminde herhangi bir ürünün araya girme ihtimalinin zor olduğunu söyleyebilirim. Burada ülke olarak biraz daha siber güvenlik yatırımlarının artırılmasının, yatırımların da yerli ekosistem içerinde değerlendirilmesine yönelik çalışmaların genişletilmesinin, Siber Küme ve TR-TEST'in çalışmalarıyla yönlendirilmesinin bütün ürünlerdeki olgunluk seviyesini artıracağını düşünüyorum.

(E) Tuğgeneral Mesut Bedri USTA

Şirketlerin ürünlerini önce kendilerinin kullanması gerekiyor. Pardus'u TÜBİTAK geliştirdi

ama TÜBİTAK Pardus'u ne kadar kullandı? HAVELSAN şu anda aldı, işletim sistemi ticarileştiriyor. Kendisi kullanmalı. Şimdi ASELSAN değişik güvenlik seviyelerindeki ağları birbirine bağlayacak bir arayüz yapıyor. ASELSAN bu ürünü internetle kendi görev alanının içinde bağlayıp kullanmalı. Pazardaki müşteri, "Önce sen kullan da ben öyle alayım" der. Dolayısıyla ürün geliştirenlerin pazara sunacağı ürünü öncellikle kendilerinin kullanacağı kadar güvenli hale getirmeleri lazım.

Borga ERBİL

Değişim yönetimi aslında son derece hassas ele alınması gereken bir yönetim boyutudur. Bununla ilgili değişimi bir anda tamamen herkese yayamıyorsunuz. Önce değişimi kabullenecek, içeride anlatacak, değişim yapacak temsilciler bulmak gerekiyor. Her kurum kendi çözümünden önce kendi içinde sindire sindire deneyip birkaç tane de kritik kurumdaki ilgili ekiplerden geri besleme alacağı şekilde çeşitlendirirse iş yürüyor. Biz siber güvenlik alanında HAVELSAN olarak bütün ürünlerimizi şu an kendimiz kullanıyoruz. Üstelik, TÜBİTAK'ta, STM'de bizim bazı ürünlerimiz şu an test ediliyor. Kritik kurumlarda tamamen yaygın bir şekilde kullanım da olmayabilir. Dar alanlarda birtakım özel testler de yapılıyor olabilir ama tabii ki nihai hedef yaygınlaştırmaktır. Ana prensibimizin bu olduğunu özellikle vurgulamak isterim. Pardus konusuna TÜBİTAK yanlış bilmiyorsam 2005 yılında başladı. Bu çok uzun bir hikâye.

"Şirketlerin ürünlerini önce kendilerinin kullanması gerekiyor. Pardus'u TÜBİTAK geliştirdi ama TÜBİTAK Pardus'u ne kadar kullandı? HAVELSAN şu anda aldı, işletim sistemi ticarileştiriyor. Kendisi kullanmalı. Şimdi ASELSAN değişik güvenlik seviyelerindeki ağları birbirine bağlayacak bir arayüz yapıyor. ASELSAN bu ürünü internetle kendi görev alanının içinde bağlayıp kullanmalı. Pazardaki müşteri, 'Önce sen kullan da ben öyle alayım' der. Dolayısıyla ürün geliştirenlerin pazara sunacağı ürünü öncellikle kendilerinin kullanacağı kadar güvenli hale getirmeleri lazım."

(E) Tuğgeneral Mesut Bedri USTA

Kamuda dijital dönüşüm konusunda son derece başarılı olmuş pek çok yöneticimiz bunu denedi; çeşitli kamu kurumlarında bir tane de değil onlarca yerde denendi. Dolayısıyla çıkarılmış dersler var. Katılıyorum her kurum Pardus'u kullanarak yaygınlaştırmalı.

(E) Tuğgeneral Mesut Bedri USTA

Şimdi Turkcell olarak "Yaani" adı altında yerli bir mail servisi yaptık. AFAD'da kullanılıyor. Savunma kuruluşlarında sırf yerli bir şey kullanılsın diye neredeyse bilabedel kuracağız. Yeni yeni tamamlanmaya başladı. İlla exchange kullanmak zorunda mı yani, işte var milli.

Volkan ERTÜRK

Ben bu coğrafyadaki insanlar olarak çok hızlı düşündüğümüzü ve çok zeki olduğumuzu düşünüyorum ama çok hızlı düşündüğümüz için durup bir şey uygulayacak zamanımız olmuyor. ABD'de çıkan bir ürün gördüğümüz zaman "Ben bunu düşünmüştüm" diye kalıyoruz ama adamlar yapmış oluyor. Bu biraz şunu getiriyor; bir şeyi yapmak istiyorsak aslında arkasında durmalıyız. Kişilerden, kurumlardan bağımsız olarak bunu strateji haline getirmeliyiz. Bir şeyin çıkması için üç, beş, 10 sene ne gerekiyorsa arkasında durmalıyız. Çin'in başarısı, Kore'nin başarısı, makro politikalarının 10, 50, 60 yıllık uygulamaların sonucunda geldiğini siz benden daha iyi biliyorsunuz. Picus'ta da bizim yaptığımız buydu aslında. Biz bir şeyi çözeceğiz dedik, başka hiçbir şey yapmayacağız dedik. Altı yıl bitti, yedinci yılımızdayız. Lisans faturası dışında biz hiçbir şeye fatura kesmedik, başka hiçbir şey de yapmıyoruz, tek ürünümüz var. Bu kümelenme etkinliklerinde diğer firmaların konuşmalarını da dinliyorum, arkadaşlarımız da var. "Biz iki yıllık firmayız, dört ürünümüz var. Bir tanesi siber istihbarat ürünü, bir tanesi şöyle bir milli ürün" diyorlar. Bir ürünün prototipini yapmak çok kolay ama o üründe derinleşmek, o üründe farklı dikeylerdeki ihtiyaçları anlayıp ona uygun çözüm sunabilmek, müşterinin arkasında olabilmek zor bir şey. Piyasadaki insanlara ve kurumlara da empati yapabilmek önemli. Yerli milli alın tamam da oradaki insanın yönetmesi gereken bir operasyonu var. Hayatta kalmaya çalışıyor. Şu an siber güvenlik alanında çalışan birçok birim hayatta kalmaya çalışıyor, sürekli yangın söndürüyorlar. Tabii ki destek olmak için yapılacak faaliyetler var ama oradaki insanın işine yaramazsa bir yere satarsın, iki yere satarsın; sonrası gelmez. Öyle olunca da ayakta kalamazsınız.

İnsan gücü yetiştirmekte de benzer duruma bakıyorum ben. Bir tane kamp yaptım, iki tane etkinlik yaptım, insanlara iki gün bir şey öğrettim. Aslında insanlara bir tatlı veriyorsunuz, çok hoşuna gidiyor lezzeti, kandaki şekeri yükseltiyor, çok iyi hissettiğini söylüyor ama sonra daha kötü noktaya geliyor. O yüzden bu işin daha sistematik şekilde, uzun yıllar içerisinde ele alınması önemli. Kurumlar tarafından bakarsak da gidip yöneticiden, yönetimden, yönetim kurulundan, genel müdürden bütçe alıyorsunuz ve bu bütçeyi güvenlik için harcıyorsunuz. Diyelim bir bankasınız, 10 milyon dolar aldınız siber güvenlik alanında harcamak için. 10 milyon istiyorsunuz, kurum 8 milyon dolar veriyor. 8 milyon doları danışmanlık için, teknolojinizi yenilemek için, içerideki insan kaynağını çalıştırmak için harcıyorsunuz. Günün sonunda başınıza bir şey geldiğinde yönetim size şunu söylüyor: "Ben sana o parayı verdim ama ne oldu? Bak *hack*'lendik." Globaldeki istatistiğe göre CTO'ların, güvenlik yöneticilerinin ortalama çalışma süreleri 13 ay civarında. Çıkma sebepleri ya *burn out* alıyorlar, istifa ediyorlar ya da başlarına bir şey geliyor, işlerinden oluyorlar. Bu konjonktürde içeride olanı, sıkıntıyı dışarı yönetime aktarmak, yönetim tarafına anlatıp onların desteğini almak zor bir konu. Burada da mesela savunulabilir güvenlik programı konuşulur. Bu programı da ne kadar defansif yapabiliriz, nasıl ispatlayabiliriz? Çünkü her şeyin arkasında matematik var. Belli temeller üzerine koyup biz bunun daha iyi iletişimini nasıl sağlayabiliriz iş dünyasında. Çünkü iş dünyasının şunu anlaması lazım: Yüzde 100 güvenlik mümkün değil.

(E) Korgeneral Alpaslan ERDOĞAN

Terör dalgası olarak da kabul edilen siber terörün siber saldırılardan farkı ve geçmişine ilişkin örnekleri milli güvenlik boyutuyla değerlendirmek üzere Kadir Murat Bey ve Kubilay Bey'den katkılarını rica edeceğiz.

Kadir Murat BİÇER

Siber terörü hibrit savaşın bir parçası olarak görüyoruz. Malumunuz ülkemizin terörizmle mücadelesi uzun yıllardır devam ettiği için siber terörizmle ilgili farkındalığı yüksek ülkelerden bir tanesiyiz. Bunun da temel aktörlerinden bir tanesi Genelkurmay bünyesinde olan Terörizmle Mücadele Mükemmeliyet Merkezinin açtığı programlar ve bu programlara çağırdığı uzmanların verdiği seminer ve eğitimler diyebilirim. Geçmiş dönemlerde bizler de bazı eğitimleri vermiştik. Siber terörizm, teröristlerin siber ortamı normal bir vektör gibi kullanmasıyla ortaya çıkıyor. Ve siber teröristler siber ortamı, normal terörizme göre çok daha rahat, çok daha etkin, çok daha kolaylıkla kullanabiliyor. Çünkü sınır veya bir güvenlik doğrulama veya bir güvenlik katmanı olmadığı için direkt siber ortamda istediği hedefle bir araya gelebiliyor. Burada, ağırlıklı olarak biraz önce gündeme gelen Barış Pınarı ve Zeytin Dalı Harekâtlarında örneğini gördüğümüz bazı terörist grup ve organizasyonların sosyal medyada, deep web tarafında, forum sayfalarında, ilgili zamanların ve mekânların adres bazında -IP bazında da olabilir- paylaşıldığını ve yapılan organizasyonlarla ilgili aktivist olarak tanıtılan faaliyetlere sempati duyan kesimin de yapılan siber terör faaliyetine bilinçsiz olsa da dahil olduğunu görüyoruz. Burada geçmişten bugüne alınmış tedbirlere göre en azından siber ortamdaki terörizmin kullanılmasına yönelik aktör sayılarının biraz daha azaldığını ama kalan aktörlerin de kullanılan *hashtag*'ler ya da kullanılan komüniteleri etkin kullanmasından dolayı daha etkin hareket ettiğini söyleyebilirim.

> *"Siber terörü hibrit savaşın bir parçası olarak görüyoruz. Malumunuz ülkemizin terörizmle mücadelesi uzun yıllardır devam ettiği için siber terörizmle ilgili farkındalığı yüksek ülkelerden bir tanesiyiz.Bunun da temel aktörlerinden bir tanesi Genelkurmay bünyesinde olan Terörizmle Mücadele Mükemmeliyet Merkezinin açtığı programlar ve bu programlara çağırdığı uzmanların verdiği seminer ve eğitimler diyebilirim."*
>
> **Kadir Murat BİÇER**

Kubilay Onur GÜNGÖR

Her ne kadar NATO içerisinde terörizmle ilgili birtakım şeyler söyleniyor olsa da, yazılı da olsa parayı veren düdüğü çalıyor gibi bir yaklaşımı var terör kavramının. Güçlü olan her kimse kendi teröristini de rahat bir şekilde tanımlayabiliyor. Fakat bunun yanı sıra aslında terörist faaliyetlerin siber dünyadaki en önemli avantajlarından birisi, bir kere etki odaklı harekât. Etki yüzeyi neredeyse bir patlayıcı kullanma, bir ateşli silah eylemi yapma kadar ve neredeyse daha fazla etki yaratacak seviyede. Bunun haricinde doğrudan bir iletişim kanalı üzerinde cereyan ettiği için korku yaratmak gibi terörün bilişsel yanlarını da rahatlıkla kullanabiliyor. Ve bunları kullanacağı hedefleri çok daha hızlı ve detaylı spot edebiliyor. Öte yandan keşif aşaması da önemli. Sözgelimi bir karakol baskını olmadan önce neredeyse bir ay keşif yapılıyor ama o baskının en büyük özelliği keşif yapacak kişinin oraya gitmek zorunda olması. Dolayısıyla bir risk var. Yakalanma riski, deşifre olma riski, başarısız olma riski var ama burada keşif aşamasında da terörist kendisini kolaylıkla saklayabiliyor. Hem hızlı hedef tespit edebiliyor hem etki odaklı kalabiliyor hem kendi risklerini minimize etmiş durumda hem hâlâ halka mal olabiliyor. Bu işin operatif bölümü. Bir de işin eğitim

tarafı var. Çok daha hızlı eğitim verebiliyorlar. Örgüt içerisindeki iç eğitimler, çok daha geniş kitlelere eğitim verebiliyorlar. Elemanlama tarafında da çok daha hızlı, çok daha büyük coğrafyalarda faaliyet yürütüp çok fazla eleman toplayabiliyorlar. Dolayısıyla siber dünyanın azımsanamayacak avantajı var. Bütün bunların yanı sıra bir de algı oluşturabiliyorlar. Algının oluşması için ne lazım? Duyu organına verinin gelmesi lazım. Siber hepsine hitap ediyor. İstediğiniz manipülasyonu yaparak istediğiniz duyu organına rahatlıkla ulaşabiliyorsunuz. Bütün bunlar birleştiğinde belki de yakın gelecekte olmasa da orta vadede teröristin fiziksel eylem yapma ihtiyacı bile gittikçe azalacaktır. Adam niye canını tehlikeye atsın ki, zaten benzeri bir katma değeri -kendi çapında katma değeri- burada yaratabiliyor diye düşünüyorum.

(E) Albay Kani HACIPAŞAOĞLU

Vurgulamak istediğim hususları şöyle özetleyeyim: Siber savunma ve siber harekât/siber savaş konuları askerden çok kamu ve özel sektör olarak sivil toplumun işi. Süreç, barış, kriz ve savaş olmak üzere tüm yaşamı kapsıyor, muharebe meydanındaki askerin siber savunması bu işin sadece bir kısmı. Sonuçta sorun ülke olarak hepimizin sorunu, sorumluları da her seviyedeki amir ve yöneticiler. Bu farkındalık çok önemli. Konuyu en üst yönetim seviyesinde sahiplendiremezseniz etkin sonuç alabilmek sözkonusu değil. Şimdi "siber terör" kavramına gelince, siber terörün siber saldırılardan çok ayrıldığı bir nokta var. Devleti ya da büyük kitleleri hedef alırsanız kinetik etki yaratacak sonuçlar da ortaya çıkar. Yani öldürmeye, yok etmeye, hasar vermeye yönelik sonuçlar çıkar, bu da siber terördür. Örneğin, bir üretim bandında üretilecek bir yiyeceğe ya da ilaca bir şekilde siber saldırıyla müdahil olur da kitlelere zarar vermesine neden olunursa bu bir siber terördür. Bir hava kontrol sisteminin bilişim sistemine, hava kontrol sistemi yazılımına müdahil olunur da sistemin çalışması bozulur ya da değiştirilirse sonuç yine bir siber terördür. Dolayısıyla, bu işin hafife alınacak bir tarafı yok. Sonuç itibarıyla da siber savaş ülkenin bütününü, en azından büyük kitleleri kinetik etkisi de dahil olumsuz olarak etkileyecekse bu bir siber saldırıdan ziyade bir siber terördür. Son bir değerlendirme olarak Gartner raporlarına

"2019 yılında dünyada siber konusundaki harcamalar; donanım, yazılım, insan, eğitim ve siber sigortalar dahil 124 milyar dolar. Ama aynı yılda siber suçların dünyaya verdiği zarar 2 trilyon dolar. Bu şu demek: Birçok bilişim sistemi için ya siber güvenlik önlemleri alınmamış ya da yetersiz veya yanlış alınmış."

(E) Albay Kani HACIPAŞAOĞLU

referansla şunu belirtmek isterim: 2019 yılında dünyada siber konusundaki harcamalar; donanım, yazılım, insan, eğitim ve siber sigortalar dahil 124 milyar dolar. Ama aynı yılda siber suçların dünyaya verdiği zarar 2 trilyon dolar. Bu şu demek: Birçok bilişim sistemi için ya siber güvenlik önlemleri alınmamış ya da yetersiz veya yanlış alınmış. Dolayısıyla, 124 milyar dolarlık siber güvenlik yatırımı yapıyorsunuz, buna rağmen 2 trilyon dolarlık zarar görüyorsunuz. İşaret etmek istediğim son husus, bugün Pardus olarak ortada olan işletim sisteminin yetersizliği. Sadece kişisel bilgisayarlarda çalışan ve en önemli kısım olan çekirdeği (Kernel) üzerinde hiçbir kontrolümüzün, denetimimizin olmadığı Pardus... Pardus'un kurumsal ilk versiyonunu Millî Savunma Bakanlığı olarak 2000'li yılların başında kurduk ve kullandık. Hem de Türkiye'nin 785 yerinde, bütün *server* seviyesindeki sistemlerde olacak şekilde. Pardus'un benzer şekilde ikinci kurumsal kullanıcısı da EPDK'dır, üçüncüsü de Merkez Bankasıdır. Dolayısıyla, bu kavramları doğru yerine oturtturmak lazım, üst kademelerdeki yöneticileri doğru bilgilendirmek lazım.

(E) Korgeneral Alpaslan ERDOĞAN

Teşekkür ederiz. Attila hocamdan, hibrit savaş ve bilgi harekâtının bir parçası olarak siber harekâtın ulusal ve uluslararası etkilerini değerlendirmek üzere katkılarını rica edelim.

Dr. Attila ÖZGİT

Ben Kani Komutanımın bıraktığı yerden devam edeyim. Gerçekten bütün cihazlarda bir kere milli ya da yerli bir işletim sistemimizin -milli çünkü çok abartılı bir niteleme; çok fazla olaylardan geçmiş anlamını taşıyor. ABD'de kamuda kurumlar arası bilgi değişimi olayını nasıl hallettmişler? ABD'li sistemi kuruyor, gerisine karışmıyor. Tabii kaynak da bol, demiş ki özel sektöre. Bize bire bir uyacak bir şey değil ama örnek olsun diye anlatıyorum. Özel sektöre, "Buyurun problem bu. Alın bir kamu kurumunu yanınıza, ihtiyaçlarını belirleyin. Onların ihtiyacını giderecek olan yazılımı geliştirin, her şeyiyle bize verin. Adamlar da bize ayrı rapor etsinler. Bu bizi şu seviye de mutlu etti, bu seviyede etmedi vs. Sonra biz değerlendireceğiz" diyor. Hiç pazara bakmıyor. Pazar birbiriyle yarışarak -ki bence düzgün yarışma budur zaten- çözüm üretiyor; sonra nasıl seçtiğini, gerisini takip etmiyor. Böyle bir süreç. Bunlar ABD'li tabii. Dünyanın bütün kaynaklarını elinde tutan bir yer. Dolayısıyla bu tür işleri bu tür yöntemlerle çok rahat çözebiliyorlar. Türkiye'de böyle bir şeyi çöz demeye kalktığınızda, zaten birbirimizin ayağına basma konusunda yeterince becerikliyiz, bir de üstüne paraları harcayıp bütün kaynakları tüketip sonra tükettiğimiz kaynakla çıkarttığımız ürün arasında ters orantılı bir durumla karşılaşma noktasına kadar gidebiliriz. Ama bu bağlamda da şunu öneriyorum ben: Neoliberal ekonomilerin sözünü ettiği vahşi pazar psikolojisinin yöntemleri Türkiye'ye uygun değil. İyi bir hibrit bulmamız lazım. Neoliberal söylemlerle zamanında terk ettiğimiz merkezi planlamacı yaklaşımımızın bir kısmını siber güvenlik alanında göstermeliyiz çünkü deminden beri eleştirdiğimiz gibi elimizde kaynak yok. Elimizde kaynağın olmadığı bir yerde kıt kaynaklarımızı yapay yarışmalarla, yapay rekabetlerle tüketiyoruz. Bu nedenle bir miktar merkezcilik lazım. Mesela Pardus kadar çok zengin şeyler tanımlamak yerine bir milli, güvenliği artırılmış bir Linux çekirdeği. Bunun için yeteneği olan kimdir? TÜBİTAK BİLGEM'dir, HAVELSAN'dır. Her kimse! Sektör de itiraz etmiyor buna.

"Neoliberal ekonomilerin sözünü ettiği vahşi pazar psikolojisinin yöntemleri Türkiye'ye uygun değil. İyi bir hibrit bulmamız lazım. Neoliberal söylemlerle zamanında terk ettiğimiz merkezi planlamacı yaklaşımımızın bir kısmını siber güvenlik alanında göstermeliyiz çünkü deminden beri eleştirdiğimiz gibi elimizde kaynak yok. Elimizde kaynağın olmadığı bir yerde kıt kaynaklarımızı yapay yarışmalarla, yapay rekabetlerle tüketiyoruz. Bu nedenle bir miktar merkezcilik lazım. Mesela Pardus kadar çok zengin şeyler tanımlamak yerine bir milli, güvenliği artırılmış bir Linux çekirdeği. Bunun için yeteneği olan kimdir? TÜBİTAK BİLGEM'dir, HAVELSAN'dır. Her kimse! Sektör de itiraz etmiyor buna."

Dr. Attila ÖZGİT

(E) Albay Kani HACIPAŞAOĞLU

Ama çekirdek?

Dr. Attila ÖZGİT

Çekirdek tabii. İhtiyacı tanımlayanın yetileri bile bu ülkede bir problem. Tanımlamayı boş verin, o tanımlamayı kâğıda dökme becerisi, bunun adil yapılma hali de yok. Dolayısıyla düzgün, aklıselim bileşenler tanımlamamız lazım. Mesela bir küçük *embedded* Linux bu ülke için şart. Yarın öbür gün bu ülkede IoT geliştireceksek, bir tane kendimizin yerli, güvendiğimiz, kaynak kodunun Devlet Denetleme Ofisinin ya da STM, TR-TEST gibi güvenilir kurumların kasasında durduğu bir *embedded* Linux. Çok iyi tanımlanmış temel ihtiyaçları ortaya koyup o ihtiyaçlar için de bütün herkesi bir yarışmaya sokup birbirlerinin ayaklarına gereksiz basma noktasına getirmeden bu bileşenleri çözdürebilmemiz lazım.

Kubilay arkadaşımızın söylediği gibi terörü isteyen istediği gibi tanımlıyor, gücünüz doğrultusunda terör tanımı yapabiliyorsunuz. Dolayısıyla o terminolojiye de çok fazla takılmanın yararlı olmadığını düşünüyorum. Zaten siber güvenlik dediğimiz ekosistemin içinde temel sınıfına giren bir şey varsa onun uzmanları var. Ben onun uzmanlarından biri değilim. Uzmanlar zaten alıp bunu o terör *domain*'inde konuşup yapar. Siber güvenliğin toplumsal farkındalık bacağını ayrı bir yere koymalıyız. Kimdir, hangi bakanlıktır bilmiyorum; hayal edemiyorum. Milli Eğitim Bakanlığı tabii ki doğal muhatabı. Bugün itibarıyla başlasalar, bir sene içinde müfredat oluştursalar, bir yıl sonra başlatırlar eğitimini. Milli Eğitim Bakanlığında 12-13 yıl eğitiminin içine yedirilmiş bir siber güvenlik müfredatı bugün yapılsa hiç değilse bir adımdır. Bunun daha iyisini yapan ülkeler olabilir. Ama onun yanına yaklaşayım, o ülkeden daha da iyisini yapayım demeye ne vaktimiz ne lüksümüz var. Yani makul, çok eleştirilmeyecek kadar izlenim veren bir çözümü pragmatik bir şekilde uygulamaya başlamak lazım. Ve hep dikkat edin –meli –malı diye konuşuruz. Yani bu gerçekten çok ciddi bir sıkıntı. İnterneti Türkiye'ye getirdiğimiz yıllar benim ilk bilgisayarla tanışmam falan 80'li yıllar, yaklaşık 40 yıla yakın oluyor. Bir zamanlar bilişim, bilişim okuryazarlığı nasıl yaygınlaştırmalı denirdi. Bu kendiliğinden geldi, biz çözmedik problemi. Biz biraz daha beklersek bir 10 yıl daha, siber güvenlik de kendiliğinden çözülecek.

Borga ERBİL

Ben gerçekten artık sahada aksiyon görüyorum. Öğrenilmiş çaresizliklerin üstünde artık aksiyonlar -bizzat kendi kurumumda da- görüyorum. Yetkin bir yönetici olarak bu konuyla ilgili aksiyonlar alabiliyorum, üst yönetimin desteği var, ilgili kurumlarımızın desteği var. Üç aylık projeler değil, üç yıldan beri geliştirilen projeler. Hatta karar babaları burada, yol haritasını çizen, uygulayanlar burada, sözde sahada aksiyon var. Ürün sahada, son kullanıcıya gittiğinde değerli, ticari boyutları olması da değerli. Aksiyon var hocam. Daha da aksiyonlar gelecek, bence bu aksiyonların nasıl

hızlandırılacağı ve nasıl daha verimli hale getirileceğini konuşmalıyız. Esas hedefimiz ne ve bu hedefe daha hızlı, daha etkin ulaşmak için işbirliği ama rekabet bağlamında işbirliği yapalım.

Milli arenada biz birlikteyiz. Milli birtakım projelerde artık belli kurumlarımız karar vericilerle birlikte, ilgili idari birimlerle birlikte ortak hareket etmeye başladı. Dolayısıyla bu benim göğsümü kabartan milli bir duruş. Biz HAVELSAN olarak ürünlerimizle, hizmetlerimizle ama EAL (*Evaluation Assurance Level*) 4 sertifikası alarak, ama TR TEST sertifikası alarak bunu artık net bir şekilde ortaya koyuyoruz. İşbirliğinden yanayız. Yurtiçinde, yurtdışında bunun çok değerli olduğunu düşünüyoruz. Stratejik adımları atarken de kim neye odaklanacak? Birtakım savaşlara gerek yok, akıllı adımlar tarafındayız. Pazarlara gidiyoruz. Yurtdışı pazarları ihracat anlamında çok önemsiyoruz. APAK, Ortadoğu, Kuzey Afrika, bizim için dünyanın her yerinde fırsatlar var. Bu anlamda yatırımlarımız devam edecek. Gerçekten her şeyi kendimiz yapacağız diye bir kural yok. Ekosisteme çok inanıyoruz. Demin Volkan hocamın ifade ettiği gibi, küçük veya orta ölçekli firmalar bir konuda derinleşebilir ama bunları bir milli rota doğrultusunda bir araya getirmek, senkronize etmek, işbirliği yapar hale getirmek gerek. Sonuçta birinin çıktısı birinin girdisi olabilir hocam, bu anlamda bir orkestrasyonu yapabilecek idari ve mesela birtakım vakıf şirketleri gibi ilerlemelerle bence net sonuçlara gideriz.

Mustafa YILMAZ

Ben çok hızlı bir şekilde millilik ve yerlilikle alakalı bir hususa değinmek istiyorum. Burada dört ana eksene odaklanılabileceğini düşünüyorum. Birincisi, var olan ürünlerin belirli bir olgunluğa ulaşması noktasında bu önem arz ediyor. Çünkü ülkede halihazırda firewall, SIEM, DLP vb. farklı siber güvenlik ürünleri var. Bunların belli bir olgunluğa ulaşması önemli. İkincisi, kamunun ve özel sektörün en çok yakındığı nokta olan bakım destek süreçleri. Adam ürünü geliştiriyor, yapıyor, hemen satıyor ama sonra bakım destek süreci olmadıktan sonra muazzam şikâyetler oluyor. Kamu da tabiri caizse "Ağzım yandı" diyor, bir daha kullanmak istemiyor. Bakım destek süreçleri çok önemli. Üçüncüsü, kamu sahipliği; yani bunların kendi bünyemizde kullanılması. Ve

dördüncü olarak da yeni ve öncelikli alanlarımıza firmalarımızın yönelmesi o alanda bir farklılık yaratabilir. Odaklanmak lazım. Picus başarılı bir örnek. Son cümle şunu da düşünmek lazım: Bu zaman alan bir şey. Yani siber güvenlik kümelenmesindeki siber güvenlik firmalarının yanlış hatırlamıyorsam yaş ortalaması altıydı. Gerçekten çok küçük ve yeni bir sektör. Zaman alacaktır. Doğru adımlarla, doğru stratejilerle ama hemen sonucu belki göremeyecek şekilde beklemek gerektiğini düşünüyorum.

(E) Albay Kani HACIPAŞAOĞLU

İki notum var. Birincisi, tanımların önemini vurgulayarak başladık, aynı önemi vurgulayarak bitirelim. Tanım ve tarifleri, kriter ve standartları belirleyip sahiplenemezsek ötesi sadece boşuna emek, zaman ve para kaybı ve bir kaos. *Cyber Operations* dediğimiz siber harekât muharebe meydanını kapsar; *Cyber Warfare* dediğimiz siber savaş ise barış, kriz ve savaşta olmak üzere tüm ülkeyi kapsar. Yani siber konusunda, barış zamanında da savaş yaşıyoruz. Bunu aklımızdan hiç çıkarmayalım. İkinci not, çok güzel şeyler tartışıyoruz. –meli –malı demesek de –ecek –acak diyoruz ancak siber güvenlik stratejisini iyi bilen ve katkı verenlerden biriyim. Zamanında da bu stratejiyi geliştiren yetkililere söylemiştim, denetimi ve özellikle de yaptırımı olmayan işlerden çok sağlıklı ve verimli sonuçların alınamayacağını. Sorumlusu, miadı ve yaptırımı belli olmayan işten genelde tatminkâr sonuç çıkmaz.

(E) Tuğgeneral Mesut Bedri USTA

Hibrit savaş deyince benim aklıma hep Ulu Önder'in "Hattı müdafaa yoktur sathı müdafaa vardır" sözü geliyor. Artık savaş sadece cephede değil, her yerde var. Dolayısıyla müdafaa sadece askeri tarafta değil, dolayısıyla siber alanın da bu alanda genişlediğini başlangıçta söyledim. Artık siber alanı sadece IT altyapısı olarak düşünmeyip bütün iletişim altyapısına elektromanyetik dalgaların, kablo sistemlerinin hepsini dahil edecek bir şekilde genişletmek gerekiyor ve bilginin paylaşılmasının da önemini bir kere daha vurguluyorum. Bakü-Ceyhan boru hattındaki patlamayı siber saldırı değil, elektrik deyip halının altına süpürmek yerine bu bilgilerin bir yerde toplanıp, paylaşılmasının ve bunlara çözüm üretilmesinin önemli olduğunu düşünüyorum. Son olarak da mutlaka organizasyon ve teşkilat gerekiyor. Yani insan kaynağıyla beraber hakikaten bu işi kim ele alacak, sorumlusu kimdir, nereye geldik, nereye gidiyoruz, tüm bunları değerlendirecek bir organizasyon yapısına acil ihtiyacımız var. Sonuçta artık hattı müdafaa yok, sathı müdafaa var. Sivil, asker; herkes siber suçlara, siber teröre ve siber savaşa karşı tedbir almak durumunda.

Kadir Murat BİÇER

STM olarak zaten Türkiye'nin büyük siber güvenlik projelerini yönetiyoruz ve yönetmeye devam edeceğiz inşallah. Bununla birlikte siber güvenlik kümelenmesi veya diğer TR-TEST çalışmalarında da yer alıyoruz. Ben burada şunu eklemek istiyorum. Konuştuğumuz konular zaten kritik altyapılar ve milli güvenliğimize etki edebileceğini

> *"Gömülü donanım, gömülü sistemlerin güvenliğini de bizim sağlamamız lazım -ki üzerinde çalışan sistemlerin güvenliğini tam almış olalım. O anlamda genelde üzerinde çok alan uzmanlığı bulunduramadığımız ve bazı konularda takıldığımız gömülü sistemlerin, entegre sistemlerin mümkünse kendi tarafımızdan en azından geliştirilmesi ama kendimiz tarafından geliştirilmeyen sistemlerin de ne yaptığının anlaşılabilmesine yönelik güvenlik testlerinin yapılması da hedeflerimizden biri olmalı."*
>
> **Kadir Murat BİÇER**

değerlendirdiğimiz konular. Endüstriyel Kontrol Sistemleri (EKS) ve IoT tarafı bu anlamda kesinlikle bizden beklenen en büyük zorluklardan biri olacaktır. Bu kapsamda Sakarya Üniversitesiyle yapmış olduğumuz EKS Test Yatağı Merkezi projemiz var. Önümüzdeki yılın ilk yarısında bitirmeyi hedefliyoruz. O projeyle de su ve elektrik sistemlerinde kullanılan EKS ürünlerinin güvenlik testinin yapılmasını hedefliyoruz. Ayrıca IoT dediğimizde, evlerde artık sıklıkla kullanmış olduğumuz donanımların güvenliğine ve yine sağlık sektörüne yönelik bir proje geliştiriyoruz ve bunu da Başkent Üniversitesi desteğiyle yapıyoruz. Sizin dediklerinize katılıyorum, yıllardır aynı şeyleri konuşuyoruz. Gömülü donanım, gömülü sistemlerin güvenliğini de bizim sağlamamız lazım- ki üzerinde çalışan sistemlerin güvenliğini tam almış olalım. O anlamda genelde üzerinde çok alan uzmanlığı bulunduramadığımız ve bazı konularda takıldığımız gömülü sistemlerin, entegre sistemlerin mümkünse kendi tarafımızdan en azından geliştirilmesi ama kendimiz tarafından geliştirilmeyen sistemlerin de ne yaptığının anlaşılabilmesine yönelik güvenlik testlerinin yapılması da hedeflerimizden biri olmalı.

Volkan ERTÜRK

Ben değişimin bireyde başladığına inanıyorum. O yüzden başka bir taraftan bir şey beklemeden yapabildiğimiz kadarını yapmamız değerli. 80-20 kuralı da çok kıymetli. O yüzden baktığımız zaman her şey birbirine zincirleme bağlı. O başkasından bir şey bekliyor, o başkasından. Bizim

"Ben değişimin bireyde başladığına inanıyorum. O yüzden başka bir taraftan bir şey beklemeden yapabildiğimiz kadarını yapmamız değerli. Bu masanın etrafındaki insanlar birlikte ne yapabilir, bireysel olarak herkes kendi alanında ne yapabilir, bence onlara odaklanmalıyız. Çok büyük problemlerin bir anda çözülebileceğine inanmıyorum. Ufak değişimlerle, büyüyen kartopu etkisiyle büyük problemlerin çözülebileceğine inanıyorum."

Volkan ERTÜRK

elimizde sahip olduğumuz, üretebildiğimiz, düşünebildiğimiz şeylerle aksiyon almamız önemli. Bu toplantı notlarının ve buradan çıkacak önerilerin daha ileri gitmesi için neler yapabileceğimiz de önemli. Ben konuya öyle bakıyorum. Bu masanın etrafındaki insanlar birlikte ne yapabilir, bireysel olarak herkes kendi alanında ne yapabilir, bence onlara odaklanmalıyız. Çok büyük problemlerin bir anda çözülebileceğine inanmıyorum. Ufak değişimlerle, büyüyen kartopu etkisiyle büyük problemlerin çözülebileceğine inanıyorum. Zaten çözülebilseydi bu duruma gelmezdi, belki sorunlar hiç bu kadar büyümezdi. Çünkü sektör de çok hızlı, dünya da çok hızlı bu alanda. O yüzden zaten "Biz oturup bir eylem planı yapalım üç yılda bunu çözeceğiz" dediğimiz durumda, eylem planı bittiği zaman zaten eskimiş olacak. O yüzden bence aksiyon, kararlılık ve heyecan gerekiyor.

"Mesela Türkiye'de ilk kez davet edildik böyle bir konuşmaya. Normal şartlarda Türkiye'de bu konuşmalar için yabancılar davet ediliyor. O yabancıların bir kısmı yurtdışında bizi dinliyorlar. İstiyorum ki bu konuşmalar havada kalmasın. Sahip çıkalım birbirimize ve o şekilde ilerleyelim. Mesela Linux'tan bahsettik. Şu an 'Milis Linux' diye bir Linux var. Çekirdeği dahil her şeyi yerli. Bugün Arch Linux'tan da Debian'dan da daha hızlı. Bilfiil bizim topluluğumuzdan da bu Linux'a katkı sağlanıyor. Bir de bunun güvenlik versiyonu var, onun adı da 'Komutan Linux'. Bunlar hazır aslında. Sadece birbirimizden haberimiz yok. Haberi olanlar da -hasetlik mi diyeyim, başka bir şey mi diyeyim- bazen başkalarına iletmiyorlar. Bir şekilde kopuk, birbirimize destek olmadan, yok etmeye çalışarak ticaret yapıyoruz. Önce bunu çözmemiz gerekiyor, bunu çözersek çok hızlı ilerleyeceğiz."

Kubilay Onur GÜNGÖR

Kubilay Onur GÜNGÖR

Ben iki şey söyleyebilirim. İlki tamamlayıcı olacak. Burada eğer bu konuyu uluslararası ya da ulusal güvenlik çerçevesinde ele alacaksak, insanlar hiç olmazsa konu ulusal güvenlikse birbirlerine destek olma tarafında ilerleyebilirler. Bir şekilde globalleşme ya da marka yaratma sürecinde daha yapıcı rekabet ya da daha yapıcı bir destek içerisinde olmamız gerekiyor. Bir ekosistem oluşması gerekiyor. Mesela Cyber Struggle örneğinden gideyim. Biz naçizane bu konuları biraz daha doktrin seviyesinde de ele almaya çalışıyoruz. Mesela Türkiye'de ilk kez davet edildik böyle bir konuşmaya. Normal şartlarda Türkiye'de bu konuşmalar için yabancılar davet ediliyor. O yabancıların bir kısmı yurtdışında bizi dinliyorlar. Ukalalık olarak algılamayın. İstiyorum ki bu konuşmalar havada kalmasın. Sahip çıkalım birbirimize ve o şekilde ilerleyelim. Mesela Linux'tan bahsettik. Şu an "Milis Linux" diye bir Linux var. Çekirdeği dahil her şeyi yerli. Bugün Arch Linux'tan da Debian'dan da daha hızlı. Bilfiil bizim topluluğumuzdan da bu Linux'a katkı sağlanıyor. Bir de bunun güvenlik versiyonu var, onun adı da "Komutan Linux". Bunlar hazır aslında. Sadece birbirimizden haberimiz yok. Haberi olanlar da -hasetlik mi diyeyim, başka bir şey mi diyeyim- bazen başkalarına iletmiyorlar. Bir şekilde kopuk, birbirimize destek olmadan, yok etmeye çalışarak ticaret yapıyoruz. Önce bunu çözmemiz gerekiyor, bunu çözersek çok hızlı ilerleyeceğiz.

Dr. Attila ÖZGİT

Ben bir açıklama yapayım. –meli –malı nitelemesinden dolayı çok özel bir olumsuzluk algılanmasın. Gerçekten öyle bir ekosistemin içinde yaşamayı hayal ediyorum ki gereksiz zaman

tüketmeyeyim, gereksiz yarışmalar, gereksiz kaynak tüketmeler olmasın. Olabildiğince, becerebildiğimizce... Geçmiş kaydımız çok iyi değil, o nedenle de bu –meli –malı'lardan artık kurtulalım ve düzgün hedeflerle yürüyelim. Her bir start up'ın 999 tane belki kaybetmişi var. Onların içinde hiç mi değerli fikir yok? Tabii ki var ama o pek güzergâhını bulamamış. Doğru toprak ve doğru gübrenin üstünde, doğru olasılık teori sonuçlarıyla yeşerememiş. Dolasıyla Türkiye o anlamda artık vakit kaybetmesin, o nedenle de artık bu –meli –malı'lardan kurtulalım dileğimi belirtmek adına söylemiştim.

Borga ERBİL

İki vektör STM ve HAVELSAN şu an ikisi de aynı yöne gidiyor. Mesela NATO'da NSAD Anlaşması imzalandı. İkisi de aynı yöne bakıyor, bunları toplayabilirsek işte tam dediğiniz olacak. Bileşke vektörden bahsetmiyorum aynı yöne bakan, aynı yere gitmek isteyen iki vektörden bahsediyorum.

(E) Korgeneral Alpaslan ERDOĞAN

Çok verimli ve son derece önemli konularda fikir ve tespitlerin ortaya çıktığı bir toplantı oldu. Katkılarınız için çok teşekkür ediyoruz.

STM
www.stm.com.tr
/STMDefence

thinktech
STM Teknolojik Düşünce Merkezi
thinktech.stm.com.tr
/STMThinkTech