Bütünleşik Güvenlik Bağlamında Siber

STM ThinkTech

ODAK TOPLANTISI

3 Kasım 2021

STM

STM ThinkTech
ODAK TOPLANTISI

TARİH: 3 Kasım 2021

MODERATÖR

(E) Korgeneral Alpaslan ERDOĞAN
STM ThinkTech Koordinatörü

KATILIMCILAR

Muhammet Sami ULUKAVAK
T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB), Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı

Prof. Dr. İbrahim ÖZÇELİK
Sakarya Üniversitesi, Kritik Altyapılar Ulusal Test Yatağı Merkezi Koordinatörü

Abdurrahman Emre ÖZKÖK
TÜBİTAK BİLGEM, Siber Güvenlik Hizmetleri Birim Yöneticisi

Enis Müçteba MEMİŞ
STM, Teknoloji Genel Müdür Yardımcısı

Güray YILDIZ
TUSAŞ, Yazılım Mühendisliği Direktörü

Ahmet Gökhan YALÇIN
Yapı Kredi Teknoloji, Bilgi Sistemleri Güvenlik Yönetimi Genel Müdür Yardımcısı

Mahmut KÜÇÜK
Türk Telekom, Siber Güvenlik Direktörü

Av. Ceyda CİMİLLİ AKAYDIN
Türkiye Bilişim Derneği, İstanbul Şubesi Yönetim Kurulu Üyesi

Çağlar ÇAKICI
Trendyol, Güvenlik Yöneticisi

Gökhan ÖNAL
LpsChain, Genel Müdür

Serbülend ZEREN
Trend Micro, Bölge Müdürü

(E) Korgeneral Alpaslan ERDOĞAN
STM ThinkTech Koordinatörü

ÜRETTİĞİMİZ VERİ VE BİLGİLERİ DE VATANIMIZI KORUDUĞUMUZ GİBİ KORUMALIYIZ

Günümüzde verinin üretilmesi kadar güvenli olarak muhafaza edilmesi, gerekli yer ve zamanda kullanılabilecek şekilde transfer edilmesi de önemle üzerinde durulması gereken bir husustur. Savunma ve güvenlik kapsamında fiziki güvenliğe paralel olarak siber güvenliği de öne çıkarmamız ve ürettiğimiz veri ve bilgileri de artık sınırlarımızı ve vatanımızı koruduğumuz gibi korumamız gerekmektedir.

Coğrafi konumumuz gereği kritik bir bölgede yer alan ülkemizin teknolojide yaşanan gelişmelere bağlı olarak karşı karşıya kaldığı risk ve tehditler her geçen gün farklılaşmakta ve bu risk ve tehditlerin tespit edilmesi de güçleşmektedir.

Karşı karşıya kaldığımız terör faaliyetlerinin farklı boyutlar kazanması, son zamanlarda yaşanan hibrid savaş konseptine de dahil edilebilen, siber harekât veya siber güvenlik alanında da tedbirler alınmasını zorunlu kılmaktadır.

Medyadan takip ettiğimiz ve yakın geçmişte örneklerini gördüğümüz kötü niyetli şahıslar, terör örgütleri veya devlet dışı aktörler tarafından yapılan siber saldırılar; şahısların, çokuluslu şirketlerin, uluslararası kuruluşların ve ülkelerin aciz duruma düşürülebileceğini göstermiştir.

Önceleri sadece bilgi teknolojilerinde siber güvenliğin sağlanması için tedbirler düşünülürken artık platformların, sensörlerin ve sistemlerin de siber güvenliğini dikkate almak durumundayız.

Günümüzde verinin üretilmesi kadar güvenli olarak muhafaza edilmesi, gerekli yer ve zamanda kullanılabilecek şekilde transfer edilmesi de önemle üzerinde durulması gereken bir husustur. Savunma ve güvenlik kapsamında fiziki güvenliğe paralel olarak siber güvenliği de öne çıkarmamız ve ürettiğimiz veri ve bilgileri de artık sınırlarımızı ve vatanımızı koruduğumuz gibi korumamız gerekmektedir.

Milli güvenliğin bir parçası olarak değerlendirilen siber güvenlik kapsamında ne gibi tedbirler alınabileceği de dahil olmak üzere bu konuların serbest bir şekilde tartışılması ve bir farkındalık yaratılması önem arz etmektedir.

Üç ayda bir Siber Tehdit Durum Raporu yayınlayan STM'nin siber güvenlik alanında farkındalık yaratmak ve insan kaynağı geliştirmek amacıyla bu yıl yedinci kez 22-23 Ekim tarihlerinde düzenlediği "Capture the Flag (Bayrağı Yakala)" etkinliğinde 710 yarışmacı ve 394 takım; 24 saat boyunca siber ortamda kriptoloji, tersine mühendislik, web ve mobil uygulamalar gibi konularda kasıtlı olarak yaratılan sistem açıklarını bulmak için kıyasıya yarışma ve yeteneklerini sergileme imkânı bulmuşlardır.

STM ThinkTech olarak bu alanda katkı sunmaya çalıştığımız bir başka çalışmamız olan "Bütünleşik Güvenlik Bağlamında Siber" başlıklı odak toplantımızda öne çıkan kritik noktaları ve aşağıdaki sorular kapsamında aldığımız cevap ve önerileri bu raporumuzda sizlerle paylaşıyoruz.

1. Hâlihazırda içinde bulunduğunuz sektöre ilişkin siber uzayı nasıl tanımlıyorsunuz (önemli faktörler vb.)? Bu konuda en gelişmiş ülkelere ve ülkelerin güvenlik politikalarına örnekler verebilir misiniz?

2. Ülkemizde yaşanan siber saldırılar kapsamında alınan/alınması gereken önlemler nelerdir? Siber güvenlik alanında kamu ve özel sektör arasında nasıl bir işbirliği yapılmaktadır/yapılmalıdır?

3. Ekim 2021'de İran'da benzin dağıtım sisteminde meydana gelen teknik arıza sonucu benzinliklerin önünde uzun kuyruklar oluşurken, bunun siber saldırı kaynaklı olduğu Yüksek Ulusal Güvenlik Konseyi tarafından da teyit edildi. (Gerçekleştirilen saldırının ABD kaynaklı olduğu bilgisi mevcuttur.) Bu bağlamda siber saldırı kaynaklarının saptanması mümkün müdür? Mümkünse bu süreç nasıl işletilmektedir?

4. Devlet ve özel sektör tarafından üretilen ve kullanılan verilerin, güvenli bir şekilde yedeklenmesi, depolanması ve transferinde ne gibi yöntemler uygulanmaktadır? Veri güvenliği ile ilgili aşırı hassasiyet veri analitiğinde birtakım zorluklara yol açabilirken, aşırı korumacılık yerine daha esnek koruma modelleri bulunuyor mu?

5. Siber güvenlik dünyada daha çok "saldırı" yönü ile tartışılıyor fakat konunun operasyonel hazırlık yönü de yadsınamaz. Beklenmeyen şok durumlarında siber uzayda (enerji iletim, iletişim, banka işlemleri, online alışveriş siteleri vb.) yoğun talepler oluşuyor. Örneğin; yakın zamanda MTA/Ankara yerleşkesinde meydana gelen patlama sonrasında internet ve telefon kesintisi yaşandı. Bu tür potansiyel şok durumlarında talepleri karşılayacak sistemlerin operasyonel hazırlık seviyelerine ilişkin bilgi verebilir misiniz?

6. Pandemi sürecinde en büyük veri ihlallerine bakıldığında, ilk sırada MGM Resorts otel zincirinin müşteri verilerinin çalınması yer almaktadır. 2020 yılının Şubat ayında gerçekleşen olayda 142 milyondan fazla otel müşterisinin verilerine erişen hacker, bu bilgileri satılığa da çıkarmıştı. Bu tür ticari faaliyetlerde kullanılan kişisel verilerin ve ticari bilgilerin güvenliği nasıl sağlanmaktadır?

7. Ülkemizde bankacılık ve finans sektöründe etkisi yaygın olarak görülen siber olaylar yaşanıyor. Siber olayların sistem, kullanıcı, art niyetli saldırı vb. boyutları ile tanımlamasını nasıl yapıyorsunuz? Bu bağlamda sektöre ilişkin öne çıkan tedbirlerden bahsedebilir misiniz?

8. Haberleşme alanında en yaygın olarak kullanılmakta olan cep telefonu ve internet haberleşmesinde güvenlik açısından ne gibi tedbirler alınmaktadır? Örneğin bazı ülkelerde internet servis sağlayıcılar "walled garden" gibi önlemler alıyor. Bu tip önlemler ülkemizde de alınıyor mu? Bu konuda ne gibi çalışmalar mevcuttur?

9. Son zamanlarda sosyal medya platformlarında kişisel verilerin ele geçirmesiyle, kullanıcılardan yardım adı altında para istenerek birçok dolandırıcılık vakası yaşanıyor. Sosyal medyada teknolojinin kötüye kullanımı ve dolandırıcılık gibi suçların yasal olarak ne gibi karşılığı bulunmaktadır?

10. "Sosyal mühendislik" bilindiği üzere sıkça kullanılan bir saldırı tekniğidir. Bunu engellemeye yönelik efektif yaklaşımlar nelerdir?

11. Kamera görüntülerindeki kişilerin görüntülerinin yapay sinir ağları aracılığıyla kısmen veya tamamen değiştirilebildiği bir ortam türü olan "Deepfake", 2021 yılı içerisinde konuşulan siber tehditler arasında yer aldı. 2022 yılında hangi siber tehditlerin öne çıkacağını/tartışılacağını değerlendiriyorsunuz?

12. Siber güvenliğe ilişkin farkındalık ve bilinç oluşturma konusunda politika öneriniz var mıdır? Ayrıca STM ThinkTech tarafından gerçekleştirilecek bir sonraki odak toplantıya ilişkin tema/konu öneriniz var mıdır?

Saygılarımızla.

Muhammet Sami ULUKAVAK
T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı,
Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı

SİBER GÜVENLİKTE MİLLİ ÜRÜN KULLANIMINI ARTIRMAK ÇOK ÖNEMLİ

Siber güvenlikle ilgili en önemli tedbirler, son kullanıcıya ilişkin alınacak tedbirlerdir. Böylelikle muhtemelen siber güvenlikle ilgili sorunların yüzde 70-80'ini aşmak da mümkün olacaktır. Savunma sanayiinde son dönemde yaşanan hack'lenme vakalarının yine son kullanıcının çok kolay tespit edilebilir, öngörülebilir, bir miktar sosyal mühendislikle çok rahat elde edilebilir parolalar belirlemesi nedeniyle olduğunu görüyoruz. Bu nedenle çok basit uygulama, düzenleme ya da politikalarla tedbirler alabiliriz. Spektrumun bir ucu böyleyken, diğer ucu da aslında işin uygulanması zor ve çok para harcamanız gereken tarafıdır. SSB olarak milli ürün kullanımını artırmanın çok önemli olduğunu düşünüyoruz.

Ülkemizde yaşanan siber saldırılar kapsamında alınan ve alınması gereken önlemler kapsamında, öncelikle bir tedbirden bahsetmeden önce, tehdidin ne olduğunu anlamak gerekmektedir. Yani bir tedbir alacaksanız bir tehdit analizi yapmanız gerekiyor. Tehdidin en yoğun olduğu alanların ise son kullanıcıya dönük alanlar olduğunu görüyoruz. Onun için, tedbirin en önemli kısmı da son kullanıcıya dönük olan kısım oluyor. Biz ciddi bütçeler harcayarak birçok sistem ve teknoloji satın alıyoruz, yatırım yapıyoruz. Sadece T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) Siber Güvenlik ve Bilişim Sistemleri Dairesinde yürüttüğümüz projelerde yıllık 200 milyon dolara yakın bir harcamamız olduğunu görüyoruz. Hem kamu kurumlarının hem de kamunun dışındaki diğer siber güvenlik harcamalarına baktığımızda, çok yüksek meblağlar söz konusu. Güvenlik Operasyon Merkezleri (Security Operations Center -SOC) kuruyoruz; işi çok daha derinlemesine yapan firma, kuruluş ve kamu kurumları büyük ve sağlam ekipler kuruyor ama nihayetinde, son kullanıcının en zayıf halka olduğu bir noktaya gelip dayanıyorsunuz. Bu nedenle en önemli tedbirler, son kullanıcıya ilişkin alınacak tedbirlerdir. Böylelikle muhtemelen siber güvenlikle ilgili sorunların yüzde 70-80'ini aşmak da mümkün olacaktır.

Çok Basit Tedbirlerle Çok Önemli Siber Saldırılar Önlenebilir

Son zamanlarda, Instagram hesaplarının hack'lendiğini duyuyoruz. İlk sorduğum soru şu oluyor: Çift faktörlü doğrulama kullanıyor musunuz? Hack'lenen kişilerin hepsi kullanmadığını söylüyor. Şu ana kadar bu tür yöntemleri kullanıp da sıkıntıya uğrayan kurum ya da kişi duymadım; varsa da çok sınırlı sayıda olduğunu düşünüyorum. Bunun nedeni de yine yedekleme mevzusudur. "Introduction to Cyber Engineering" gibi bir çalışma olsa, kitabın birinci sayfasında "Verileri yedekleyin" yazar. Siber güvenliği sadece bilgisayarınıza giremediğiniz veya verilerinizin fidye yazılımı için kilitlendiği bir ortam gibi düşünmemek gerekiyor. Yeri geliyor, çok büyük firmalar gözünüzün içine baka baka sizin verinize erişmenizi engelliyor. Örneğin WhatsApp bunu yapıyor, veriye giremiyorsunuz. Bu da bir nevi siber saldırıdır. Aslında yedeklemiş olsanız bu saldırıyı da önlemiş olacaksınız. Benim özellikle burada vurgulamak istediğim konu şu: Çok basit tedbirlerle çok önemli siber saldırılar önlenebilir. IT operasyonunu yürüten birimler olarak biz şunun farkında oluyoruz: Bilgi Güvenliği Yönetimi Sistemi (BGYS) politikaları gerçekten uygulanabilse siber güvenlik risklerini ciddi oranda azaltmış olacak. Biz parolaların belli periyotlarda güncellenmesi için bir politika oluşturuyoruz. Genellikle son kullanıcılarımız, "Çok sık parola değiştirmeyi zorunlu tutuyorsunuz" diyorlar. Halbuki son dönemde yaşanan hack'lenme vakalarının yine son kullanıcının çok kolay tespit edilebilir, öngörülebilir, bir miktar sosyal mühendislikle çok rahat elde edilebilir parolalar belirlemesi nedeniyle olduğunu görüyoruz. Bu nedenle çok basit uygulama, düzenleme ya da politikalarla tedbirler alabiliriz.

Spektrumun bir ucu böyleyken, diğer ucu da aslında işin uygulanması zor ve çok para harcamanız gereken tarafıdır. SSB olarak milli ürün kullanımını artırmanın çok önemli olduğunu düşünüyoruz. Savunma sanayiinde, siber güvenlikten önce epeyce bir yol katetmiş vaziyetteyiz ama siber güvenlik sektöründe, savunma sektörünün 15 sene gerisindeyiz gibi görünüyor. Fakat yavaş yavaş ilerliyoruz. 2016 yılında çeşitli siber güvenlik ürünlerinin milli olanlarını bulmak için bir araştırma yaptığımızda, pek çok alanda buna ilişkin bir ürünün olmadığını görmüştük. Şu anda iki firma geliyor, diyor ki; "O ürünü biz yaptık". Bir de değil iki firma geliyor. Onun için ciddi bir ivmelenme kazanmış vaziyetteyiz ama milli ürün kullanımını artırmanın çok önemli olduğunu düşünüyoruz.

Bu kapsamda, SSB olarak da pek çok proje yürütüyoruz. SİSAMER bunlardan bir tanesi. Bu çalışmaları mutlaka uçtan uca yapmak gerekiyor, çünkü atak vektörleri de olgunlaşıyor. Yani siber saldırıların, aslında saldırıya uğrama ihtimali olanlar için bir avantajı şu: Siber saldırılar genellikle tek kullanımlıktır. Çünkü bir saldırı yapıldığında, ya bir yama geçer onu kapatırsınız ya da o siber saldırıya yönelik bir tedbir alırsınız. Böylelikle çok iyi takip etmeyen, bu konuda güncellemeleri yapmayan, yamaları edinmeyen kurum ve kişilere ancak bu saldırılar ikinci defa yapılabilir. Ama tek kullanımlık siber silahlar olgunlaştığında sizin daha bütüncül ürünlerle kendi tedbirinizi geliştirmeniz gerekiyor. Bu da mutlaka birbirleriyle entegre milli çözümlerden geçiyor.

Türkiye Siber Güvenlik Kümelenmesi Kuruldu

Kamu ve özel sektör işbirliği noktasında, SSB olarak 2018 yılında, Türkiye Siber Güvenlik Kümelenmesini kurduk. Kümede şu anda 192 firmamız bulunuyor. 20-25'e yakın da üyelik

süreci devam eden firmamız var. Burada ciddi bir işbirliği imkânı oluyor. Tabii bu da bir tekamül meselesidir; "Bugün bir kümelenme kurduk, bütün firmaları bir araya getirdik, hadi çalışsın" demekle olmuyor. Biz ilk senelerde sektördeki firmaları bir araya getirerek, onlara ilişkin etkinlikler düzenleyerek ekosistemdeki sinerjiyi ortaya çıkarmak üzere faaliyetler gerçekleştirdik. 2021'in başından itibaren kümelenmede bir vizyon değişikliği oldu. Etkinlik odaklı bir yapılanmadan stratejik faaliyetlere odaklı bir yapılanmaya geçildi. Böylelikle belki ürün odaklı, belki firmalar odaklı ama olgunlaşma sürecinin başında olan firmalara yön gösterebilecek çeşitli faaliyetlerin planlamasını yapıyoruz; kısa zamanda inşallah bunların duyurusunu yapacağız.

Ayrıca firmalara "jet hızlandırma" programları da uyguluyoruz. Firmasını kurmuş ya da henüz firmasını kurmasa da ciddi bir fikri yeni olgunlaştırma aşamasında olan arkadaşlar arasından belirli kriterler dahilinde seçim yapıyoruz. Kısıtlı sayıda firmaya ya da start-up'a destek veriyoruz. Bu destekler teknik bilginin de ötesindedir. Örneğin pazara girdiğinde hangi alana girmeli, fiyatlaması ne olmalı, coğrafi olarak nerelerde bulunmalı ya da odaklanmalı gibi konularda destek vererek olgunlaşma sürecinin ilk aşamalarında daha hızlı ilerleyebilmeleri için onlara fayda sağlıyoruz. Tabii bunları çeşitlendirecek ve artıracak şekilde, uçtan uca gelişim sürecinin tamamına bu desteklerin verilmesi gerekiyor. ThinkTech'in düzenlediği panelimiz gibi çalışmalardan çıkacak sonuçları da mutlaka değerlendirip kendi karar mekanizmalarımıza katacağız.

Verilerin İşlenmesinde Uygulanan Yöntemler

Verinin yedeklenmesi, depolanması, transferi; yani verinin işlenmesi konusunda iki önemli konu var. Birincisi iş sürekliliği, ikincisi de gizlilik/güvenlik. İş sürekliliği anlamında şunu hatırlayabiliriz: 2017 yılında Danimarkalı lojistik şirketi MAERSK hack'lendi ve kendi IT altyapısını 17 saat kullanamadı. Bunun MAERSK'e 300 milyon dolara yakın maliyeti oldu. Bu, şu anlama geliyor: Eğer siber güvenlik anlamında iş sürekliliğini sağlayamazsanız çok ciddi maliyetlerle karşılaşabilirsiniz. Bunun için STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) ile de birlikte ve bağımsız olarak iş sürekliliği merkezleri kuruyoruz.

Gizlilik tarafına geldiğimizde, savunma sanayii ağırlıklı olduğumuz için sistemlerimizi, özellikle de IT altyapılarımızı hem intranet hem internet olarak farklı güvenlik seviyelerine sahip ağlar şeklinde yapılandırıyoruz. Bazen dış dünyayla bütün ilişiği kesilmiş kapalı ağla çok gizli seviyede, hatta şu anda TSK'da kullanılan TAFFICS gibi kendi fiziksel altyapımızı dahi kendimizin oluşturduğu farklı güvenlik seviyesindeki ağlar kullanıyoruz. Elbette burada data diyot, sanal hava boşluğu gibi yapılar gündeme geliyor çünkü sadece ağları birbirinden ayırmanız yetmiyor, mutlaka ağlar arasında da veri paylaşımı yapmanız gerekiyor. Bunun için politikalar geliştirebileceğiniz ve bu politikaları uygulayabileceğiniz yapılar kurgulanıyor. Örneğin, şu anda SSB'de de farklı güvenlik seviyelerinde ağlarımız var. Verilerimizi gizlilik seviyesine göre farklı ağlarda işliyoruz. İki ağ arasında veri geçişi ihtiyacı olduğunda da ağ geçidi sistemleri kullanıyoruz. Bu, bir ürün olmak zorunda değil. Şu anda data diyot veya sanal hava boşluğu gibi ürünlerimiz var ama onun dışında terzi işi çözümler de olabiliyor. Örneğin, şu anda NATO'nun Hava Komuta Kontrol Sistemi (NATO Air Command And Control System -NATO ACCS) ile tüm Türkiye'de Hava Kuvvetlerinin HvBS sistemi arasında bir veri alışverişi yapılması lazım. Bunun için özel olarak geliştirilmiş bir çalışmamız var.

Bunun dışında veriyi korumak, veriyi paylaşmamak demek değil. Veriyi mutlaka paylaşmanız ve bunun usulünün belirlenmesi lazım. Bunun için veri sızıntısı önleme sistemleri, veri etiketleme sistemleri kullanılabilir ki biz "Test ve Sertifikasyon Projesi" kapsamında şu anda hâlihazırda iki tane DLP ürününü sertifiye etmiş durumdayız. Milli veri etiketleme ürünlerimiz var. Bunlar çok rahat kullanılabilir. Tabii tek bir kurumun kendi içindeki veri işleme sürecinden bahsediyoruz ama birbirinden bağımsız, farklı lokasyonlarda ya da aynı kurum veya teşkilatın taşra ve genel merkezi arasındaki veri haberleşmesine baktığımızda da burada yine kullanıcıya özgü bulut sistemleri veya kiralık hatlar şeklinde fiber, dark fiber altyapıları kullanılıyor. Şu anda savunma sanayii firmalarıyla SSB arasında SAVNET adını verdiğimiz bir yapı kurduk. 2016, 2017 yıllarında kamu kurumları arasında KAMUNET altyapısı kurulmuştu. SAVNET de benzer bir yapıdır. Bunun da ötesinde sadece iletim güvenliği (transec) değil aynı zamanda haberleşme güvenliği (comsec) anlamında da verinin güvenliğinin sağlanması gerekiyor. Aynı zamanda, diyelim ki SAVNET ağımızda bu güvenliği sağladık, SAVNET ağının bağlandığı uç noktadaki yerel ağda da mutlaka bir güvenlik sağlamanız gerekiyor. Bunun için de SAVNET ağına bağlı bir uç noktadaki yerel ağda güvenlik gereksinimlerinin sağlandığının teşhis edilmesi için"Siber Hijyen" dediğimiz bir projemiz var. Aslında bu noktada, Tesis Güvenlik Belgesi adında kurumsallaşmış bir yapı var. Tesis güvenlik belgesinin bir cüzü olacak şekilde, belki siber güvenlik belgesi de verilebilir. Böylelikle firma veya kurumların veri işleme için birbirleriyle güvenli haberleşebilmesi amacıyla bir ortam teşkil edilmiş olabilir.

> "SSB olarak 2018 yılında Türkiye Siber Güvenlik Kümelenmesini kurduk. Burada şu anda 192 firmamız bulunuyor. 20-25'e yakın da üyelik süreci devam eden firmamız var."

Veri Analitiğinde Esnek Koruma Modelleri

Veriler depolanmaya ve bunlardan anlamlı çıktılar sağlanmaya başladığında sizin mutlaka o veriyi korumanız ve veriyi işlerken "özellikle bilmesi gereken" prensibine göre hareket etmeniz gerekiyor. Veri analitiğinin nesilli bir yapısı vardır. Descriptive/Betimleyici/Betimsel olarak tanımladığımız Veri Analitiği 1.0'da, var olan veriden size bir şeyi tanımlayıcı bilgi elde edebilirsiniz. Diognastic dediğimiz 2.0'da verinin teşhis edilmesi söz konusu. 3.0 ve nihayet 4.0 var. Prescriptive dediğimiz 4.0'da da sizin bir sorununuz var, verinin o soruna ilişkin size bir çözüm önermesi anlamına geliyor. Veri analitiğinde sıkılaştırılmış veri politikalarını kullanırken genellikle daha düşük seviyeli nesilli veri analitiği yapıyorsanız daha büyük sıkıntıyla karşılaşıyorsunuz. Ama Veri Analitiği 4.0'a gittiğinizde artık veriler toplulaştırılıyor ve siz münferit bir ajana ilişkin bilgiye sahip olamıyorsunuz. Bu nedenle veri analitiğinde daha üst nesillere gittiğinizde veriyi daha rahat kullanabileceğiniz bir pozisyon oluyor. Bu nedenle veri analitiğinde daha prescriptive metotlara geçişi önerebilirim. Örneğin Avrupa İstatistik Ofisi (Eurostat) dışarıya veri sağlarken, online ortamda sadece belli kısıtlarda veriyor ya da tüm parametrelerde arama yapmanıza imkân vermiyor. Çünkü siz bir firma ya da bir ülkeye ilişkin çok spesifik veri elde edebilirsiniz. Bu Eurostat için istenmeyen bir durum. Araştırmacılar genellikle Lüksemburg'a, Eurostat'ın merkezine gitmek zorunda kalıyorlar. Oraya gidildiğinde de veriyle ilgili yine çıktı alabilmeniz için ya da soft bir versiyon alabilmeniz için belli onay mekanizmalarından geçmeniz gerekiyor. Kısacası, dünyada veri analitiğinde, verinin kullanımı için teknik metotlardan ziyade daha idari tedbirler alınmış vaziyette. Biz de benzer şekilde veri anonimleştirme yapabiliriz veya idari tedbirlerle birlikte hem kamu verilerinin hem de özel sektördeki verilerin kullanıma açılması mümkün olabilir. Veri analitiğinde bu şekilde yöntemler kullanılabilir.

KamuNet'teki Verilerin Yedeklenmesi Projesi

Ulaştırma ve Altyapı Bakanlığı tarafından başlatılan KamuNet ilk başta hizmete özel gizlilik derecesindeki verilerin kamu kurumları arasındaki paylaşımı için yapılmıştı. Daha sonra internet üzerinden hizmete özel verilerin mail ortamında paylaşılabileceğine ilişkin bir düzenleme yapıldı. Böylece KamuNet bir miktar baypas edilmiş oldu. Yani KamuNet'in kurulmasıyla amaçlanan hedef, internet üzerinden bu düzenlemenin yapılmasıyla gerçekleştirilmiş oldu. Bu noktadan sonra, ayrıca bir veri merkezi ihtiyacı olup olmadığı belki tartışılabilir.

SAVNET'in Güvenliğinin Sağlanması Çok Önemli

SSB olarak SAVNET'in kurulumu, işletilmesi ve güvenliğiyle ilgili bütün sorumluluğu almış durumdayız. SAVNET'in güvenliğinin sağlanması çok önemli. Her bir veri aktarımında iki

> "Siber güvenlikte tedbirlerimizi periyodik olarak alabilecek bir mekanizma kurgulamak gerekiyor. Siber güvenliğin de havacılık gibi belli sertifikasyonları olması gereken ve bunların ancak belirli otoriteler tarafından onaylandıktan sonra kullanılabileceği bir noktaya gelmesi gerektiğini düşünüyorum."

taraflı kriptolama yapıyoruz. Yazılım kriptosu değil doğrudan donanım kriptosu kullanıyoruz. Aynı zamanda çeşitli yazılım kriptoloma ya da tünel mekanizmaları, VPN gibi çeşitli metotlar kullanıyoruz. Ama onun da ötesinde, ağa erişim kontrol cihazlarımız oraya tanımlanmış vaziyette; o ağa yetkisiz bir erişim olduğunda mutlaka buna ilişkin siber güvenlik tedbirlerini almış vaziyetteyiz. Ama bizim sıkıntımız SAVNET'in iletim aşamasında değil SAVNET'in eriştiği noktadaki yerel ağ kısmında ortaya çıkıyor. Çünkü o ağı kontrol etmek sizin elinizde değil. Diyelim ki bir savunma firmamızın yerel ağı ile SAVNET bağlantısı yaptınız. Bu bağlantının o noktadaki güvenliğinin sağlanması, ilgili firmanın kendi BT ya da siber güvenlik ekiplerinin kontrolündedir. Biz bu nedenle "Siber Hijyen Projesi"ni başlattık. Yani o noktada da güvenliği sağlamanız gerekiyor ki, transfer etmek istediğiniz verinin güvenliğini de almış olabilesiniz. Onun için biz şu anda SAVNET'te hizmete özel verileri paylaşıyoruz. Gizli verileri paylaşabilmek için siber hijyen gerekliliği arıyoruz. Tabii ki savunma sanayii olması nedeniyle birkaç hizmete özel bilginin aynı anda kullanılması gizli bir bilgi olabilir. Bu anlamda biz SAVNET'te hizmete özel bilgileri paylaşıyoruz, hizmete özel mail paylaşımı yapıyoruz, hizmete özel bulut depolama hizmeti veriyoruz ama onun ötesinde "gizlilik seviyesinde" paylaşım yapabilecek çalışmaları yapıyoruz. Siber hijyenle birlikte onu da sağlamış olacağız.

Sürdürülebilir Güvenlik Farkındalığı Oluşturmalıyız

Farkındalık ve bilinç oluşturmamız gereken konulardan biri sürdürülebilir güvenliktir. Bugün aldığımız tedbirler bugünün tehditlerine karşı bir koruma sağlıyor, yarın eskimiş oluyor. Onun için siber güvenlikte tedbirlerimizi periyodik olarak alabilecek bir mekanizma kurgulamak gerekiyor. Siber güvenliğin de havacılık gibi belli sertifikasyonları olması gereken ve bunların ancak belirli otoriteler tarafından onaylandıktan sonra kullanılabileceği bir noktaya gelmesi gerektiğini düşünüyorum -ki bugün common criteria bunlardan bir tanesidir. SSB olarak yürüttüğümüz Test ve Sertifikasyon projesi kapsamında hâlihazırda 11 ürün grubundan 19 ürünü test ettik ve sertifika verdik. Bu ürünler sadece güvenlik kriterleri değil aynı zamanda performans ve fonksiyonalite anlamında da belli kriterleri sağlıyor. Tabii bunun olgunlaştırılması gerekiyor. Yani common criteria gibi çok daha derinlikli ve bazı senaryoların ön tanımlı olarak üreticiler tarafından tanımlandığı, sonra bunun kavram ispatının yapıldığı bir tarzda değil ama daha jenerik kriterlerin belirlenerek test edildiği bir ortam var. Şu anda biz bunların ulusal kriter olması için çalışıyoruz. Hâlihazırda belli seviyelerde testi geçen 19 ürün arasında A, B ve C sertifikası alanlar var.

NATO'nun Estonya Tallin'deki Siber Güvenlik Mükemmeliyet Merkezindeki en önemli aktivitelerden biri tatbikatlardır. Burada düzenlenen siber güvenlik tatbikatlarının Türkiye ayağını Genelkurmay Başkanlığı Siber Savunma Komutanlığından yürütüyoruz. Bu tatbikatların sadece askeri odaklı olmaktan çıkarılıp yaygınlaştırılması çok faydalı olabilir. Kırmızı Takım, Mavi Takım, Sarı Takım, Gri Takım, Beyaz Takım gibi farklı fonksiyonalitesi olan ekiplerin bir arada çeşitli tatbikatlar yapması, sürdürülebilir güvenlik anlamında faydalı olacaktır. Diğer taraftan ödül avcılığı da aslında sürekli bir sızma testi anlamına geliyor.

Prof. Dr. İbrahim ÖZÇELİK
Sakarya Üniversitesi, Kritik Altyapılar
Ulusal Test Yatağı Merkezi Koordinatörü

SİBER GÜVENLİK, ULUSAL GÜVENLİĞİN VAZGEÇİLMEZ BİR PARÇASI

Siber saldırılarda ortak nokta, toplum ve devlet düzeninin bozulma durumunun söz konusu olması. Toplum ve devlet düzeninin bozulması, can ve mal kayıplarının oluşması noktasında baktığımızda, bunun tanımı kritik altyapıların güvenliğine giriyor. Bir kritik altyapının bu anlamda siber saldırıya uğraması sonucunda ortaya çıkabilecek hasar ve bir problemin diğer kritik altyapıları ne kadar etkileyebileceğiyle ilgili ülkemizin çalışmalar yapması gerekiyor.

Siber uzay, dijital dünyaya bağlı olan cihaz ve sistemlerin oluşturduğu bir uzay olarak değerlendirilebilir. Literatürde çok farklı tanımlar söz konusu olmakla birlikte, ben bunlardan özellikle Ulusal Siber Güvenlik Strateji Dokümanı'nda yayınlanmış olanını ifade etmek istiyorum.

Siber uzay; tüm dünyaya ve uzaya yayılmış bilişim sistemlerinden ve onları birbirine bağlayan ağlardan ve/veya bilgi sistemlerinden oluşan bir sayısal ortam olarak tanımlanmaktadır. Genel yapı itibarıyla baktığımızda; siber uzay bizim için şu anda bir çalışma uzayı, bir çalışma alanı olarak tanımlanabilir. Çünkü bilişim dünyasının gelişimine ve geçmişine baktığımızda elektronik sistemler, enformasyon sistemleri vardır. İletişim sistemlerinden bahsettik, sonra internet ve web karşımıza çıktı. Bunların hepsini birlikte değerlendirdiğimizde şu anda oluşan dijital dünyayı bu terimlerle tanımlayamıyoruz. Diğer taraftan geçmişte geliştirilmiş olan telefon, faks sistemleri, televizyon sistemleri, elektrik ve enerji sistemleri gibi sistemler var. Bu sistemler biraz önce saydığım sistemlerle entegre bir şekilde çalışmaktadır. Doğrudan ve dolaylı bir ilişkisi söz konusu ama tehdit açısından baktığımızda, bu sistemlerin hepsi aslında bir siber tehdit içindedir. Bu nedenle siber uzay, burada hızır gibi karşımıza çıkan bir terim olarak değerlendirilebilir. Siber uzayı birçok sistemi içine alan ve çok yönlü bir kavram olarak değerlendirebiliriz.

Siber uzayı yeni bir çalışma alanı olarak değerlendirdiğimizde; beraberinde siber saldırı, siber savunma, siber caydırıcılık, siber dayanıklılık, siber güç, siber savaş gibi birçok terim de

> "Siber uzayda bir siber saldırı yapmak için geliştirilecek olan siber silahların askeri sistemlerde geliştirilen tank, füze, helikopter, uçak gibi bileşenlere göre çok daha ucuz bir şekilde geliştirildiğini görebiliyoruz."

karşımıza çıkmaktadır. Tehdidi artık siber tehdit olarak tanımlıyoruz. Siber güvenlik çok basit olarak, siber uzaydaki her türlü bilişim sistemini savunmak anlamında değerlendirilebilir. Böyle birçok sistem söz konusu, bizim bunları bir noktada savunmamız gerekiyor. Ülkeler de bu savunmayı gerçekleştirebilmek için siber güvenliği ulusal güvenliğin vazgeçilmez ve kritik bir parçası olarak görüyor. Dolayısıyla güvenlik politikalarının oluşturulması gerekiyor ama bu güvenlik politikalarının oluşturulabilmesi için siber uzayın birtakım karakteristik özelliklerine de dikkat etmek gerekiyor. Mesela ilk dikkat çekilmesi gereken konulardan bir tanesi, siber uzayın fiziksel bir sınırının ya da özel bir çalışma saatinin olmamasıdır. Sadece kara olarak komşularınızla ilişkili değilsiniz. Dolayısıyla herhangi bir fiziksel lokasyonda ya da herhangi bir saatte tehdit altında olabilirsiniz. Bu savunma açısından ve politika noktasında dikkat edilmesi gereken bir konu. Zira NATO'nun kara, deniz, hava ve uzaydan sonra siber uzayı da beşinci boyut ve savaş alanı olarak tanımlamasının önemi buradan geliyor.

İkinci dikkat çekmek istediğim konu; siber uzayda bir siber saldırı yapmak için geliştirilen siber silahların, askeri sistemlerde geliştirilen tank, füze, helikopter, uçak gibi bileşenlere göre çok daha ucuz bir şekilde geliştirilmesidir. Bir internet ve bir bilgisayara sahip olmak hatta taşeron kullanılmak istendiğinde 100 dolarla siber askerleri, yani botnet'leri kiralamak çok mümkün. Siber uzay açısından bu durum, tehdidin oldukça büyük bir boyutta olduğu anlamına geliyor. Politikalar geliştirilirken siber uzayda kurumları ve özellikle son kullanıcıları etkileyen birçok veri hırsızlığı ve dolandırıcılığın olduğunu görmekteyiz. O nedenle geliştirilecek politikaların içine bu tür vakaları önleyici ya da mağduriyetleri giderici çözümlerin alınması gerekmektedir. Çok yakın zamanda Squid Game oyunuyla ilgili yaşanmış bir dolandırıcılık vakası oldu ve ciddi mağduriyetler doğdu. Dolayısıyla bunlarla ilgili bazı yaptırım ya da hukuki süreçlerin dikkate alınması gerekiyor. Diğer taraftan, siber uzayda gerçekleştirilen dolandırıcılık ya da bu tür suçların tespit edilmesinin çok kolay olmadığı da aşikâr. Bu da tamamen ayrı bir çalışma alanı olarak değerlendirilebilir.

Siber uzayda önemli konulardan bir diğeri de sosyalleşme kısmıdır. Sosyal medya uygulamalarıyla artık ülkelerin birbirleri arasındaki fiziksel sınırlar ortadan kalkıyor, benzer yaşam modelleri ortaya çıkıyor, inanışlar ortaklaşmaya başlıyor. Bu durum sosyal medyanın siber uzaydan uzak kalmasının çok mümkün olmadığını gösteriyor, zira sosyal medya üzerinden birçok saldırı alıyoruz.

70'in Üzerinde Ülkenin Siber Güvenlik Politikası Var

Tüm bunları bir bütün olarak politika ekseninde değerlendirdiğimizde; ülkelerin hem ulusal güvenlik açısından, hem de kendi kurumlarını ve vatandaşlarını koruma noktasında siber güvenlik politikalarını icra etmeleri gerekiyor. Uluslararası Telekomünikasyon Birliğinin 2020

yılında yayınladığı rapora göre, 70'in üzerinde ülkenin siber güvenlik politikası bulunuyor. Türkiye bu raporda yanlış hatırlamıyorsam 14'üncü sıradaydı. ABD, Rusya ve Çin'in bu raporda ilk 10'a giremediği görülüyor ama bu üç ülkenin siber güvenlik dünyasına geçmişte olduğu gibi gelecekte de yön vermeye devam edeceğini çok net bir şekilde biliyoruz. Bu ülkeler siber güvenlik politikaları uygulamaya 2000'li yıllarda başladı. Yani Soğuk Savaş'ın bitişi, diğer taraftan internetin doğuşu ve ona bağlı olarak ortaya çıkan birtakım vakalar, ülkeleri bu konuya dikkat etmeye zorladı. 2000'li yıllardan itibaren bu büyük ülkeler birçok siber güvenlik politikası yayınladı. İlk ana bakışları savunma eksenliydi fakat zamanla ortaya çıkan siber olaylar ve vakalar sonucunda ülkeler birbirlerini artık siber uzayda tehdit olarak görmeye başlayıp saldırıya karşı saldırı, tehdide karşı tehdit gibi belli içerikleri politikalarına dahil ederek bütün dünyaya ilan ettiler.

Endüstriyel Kontrol Sistemlerinde Siber Güvenlik

Siber saldırılarda ortak nokta, toplum ve devlet düzeninin bozulmasıdır. Toplum ve devlet düzeninin bozulması, can ve mal kayıplarının oluşması söz konusu olduğunda, bunun tanımı kritik altyapıların güvenliğine giriyor. Kendi ülkemizde de 2013'te başlayan Ulusal Siber Güvenlik Strateji Eylem Planlarında kritik altyapıların korunması ve mukavemetin artırılması birinci stratejik amaç olarak ele alınıyor. Çünkü oluşan zararların boyutları çok yüksek. Bunun EKS, yani "Endüstriyel Kontrol Sistemleri" tarafı var. Burada kontrol sistemleri kullanılıyor, SCADA sistemleri kullanılıyor. Dolayısıyla bu tür sistemlerde siber saldırıları tespit etmek için proses merkezli hareket etmek gerekiyor. Belirli IT sistemleri mevcut ama işin arka planına baktığımızda kontrol cihazları, yani PLC, RTU, SCADA ya da IED diye tanımladığımız kontrol cihazları var. Ama onun da ötesinde, enerji prosesi ya da su yönetimi başlı başına önem taşıyan konular. Öyle ki enerjinin içinde sadece elektrik de yok; petrol, doğalgaz gibi alanlar da enerjinin kendi içerisinde değerlendiriliyor. Ulaştırma yine ayrı bir konu. Bu tür alanlarla alakalı tehditleri, saldırıları tespit etmek için proses üzerinde çalışmaların yapılması ve bu konuyla ilgili bilgi birikimlerinin elde edilmesi gerekiyor. ABD'de, Singapur'da, Japonya'da, Hollanda'da Kritik Altyapılar Ulusal Test Yatağı Merkezleri kurulmuştur. Ülkemizde siber güvenlikle ilgili 200'e yakın firma var ama EKS ile ilgili, bu sistemlerin siber güvenliğini sağlayacak yerli bir ürünümüz henüz yok. Yani donanımlar ve bunların üzerinde çalışan yazılımlar yabancı. Bu sistemlerin güvenliğini sağlayacak siber güvenlik yazılımlarımız da yabancı. Dolayısıyla neyin siber güvenliğinden bahsettiğimiz burada büyük bir soru işareti hâline geliyor. Biz de Sakarya Üniversitesi olarak, Türkiye'de ihtiyaç olan bu konuyla ilgili, T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı'na (SSB) bir proje teklifiyle gittik. SSB teklifi kabul etti ve STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) işbirliğiyle projeyi hayata geçirdik. Şubat 2021'de "Kritik Altyapılar Ulusal Test Yatağı Merkezi" hayata geçmiş oldu.

EKS güvenliği ile ilgili olarak belli birikimlerimiz söz konusu ama APT (Advanced Persistent Threat) tabanlı siber tehdit aktörleri çok sofistike saldırılar gerçekleştiriyor. Hedef odaklı ve belli bir motivasyon doğrultusunda saldırılar düzenliyor ve saldırı vektörlerini sürekli değiştiriyorlar. Daha önce ifşa olmuş tehditlere karşı tespit açısından birtakım güvenlik önlemleri alınmış olabilir. O zaman yeni savunma çözümlerini atlatmak için saldırı vektörlerini değiştirmek gerekiyor. Diğer taraftan, EKS'lerin siber savunması için prosesle ilgili bazı bilgilere de

sahip olmamız gerekiyor. Olayı sadece tek bir uzlaşma göstergesi (indicator of compromise) ile, tek bir imza tabanlı yapıyla tespit etmemiz mümkün olmuyor. Mümkün olsaydı, bir zararlı yazılım bulaştıktan sonra domain admin'in iki saat içinde elde edilebileceğini biliyoruz. Bu çok hızlı bir süre ve APT grupları saatler ve günler mertebesinde hedefe çok rahatlıkla sızabiliyor. Bu işin bir tarafı. Bir diğer tarafı ise, sızıldıktan sonra bizim onu algılamamız ve tespit etmemiz günler sürüyor. Literatürde bununla ilgili 100, 150 gün gibi değerler var ki Solarwind siber saldırısında Mart'ta başlayıp Aralık'ta ilan edilen bir süreçten bahsediyoruz. Böyle olunca, bu tür EKS ya da kritik altyapılarla ilgili prosesler üzerinde özel çalışmaların yapılması, bu sistemlerden verilerin toplanması, bu alanda ortaya çıkmış APT gruplarının özellikle kullandığı teknik ve taktiklerin incelenmesi, izlenmesi gerekiyor. Örneğin, MITRE APT gruplarını sıralıyor, kullandığı teknikleri gösteriyor. Teknikler olarak sayfası güncel fakat şu anda MITRE'nin sunduğu üç matris var. Kurumsal bir matris, mobil ile alakalı bir matris ve ICS ile ilgili bir matris var. MITRE ICS matris sayfasına tıklayıp APT gruplarına baktığınızda, 10'a yakın APT grubu görüyorsunuz. Diğer yandan, Dragos adlı firmanın sayfasına baktığınızda, firma proses merkezli çalıştığı için ilgili APT gruplarından topladığı sadece 15 grup var. MITRE'nin sayfasında bu grupların sadece üç tanesi görünüyor ve bu gruplar 2014 yılından itibaren ortaya çıkan gruplar.

Özellikle enerji birçok alanın merkezinde duruyor; suyu, petrolü, ulaştırmayı, ve telekomünikasyonu besliyor. Bir kritik altyapının siber saldırıya uğraması sonucunda ortaya çıkabilecek hasar ve bir problemin, diğer kritik altyapıları ne kadar etkileyebileceğiyle ilgili ülkemizde çalışmalar yapılması gerekiyor. Bizim de kendi kritik altyapılarımız var. Dolayısıyla bu kritik altyapılara gelebilecek saldırıları tespit etmek amacıyla siber güvenlik farkındalıklarımızı artırmakla birlikte aynı zamanda prosesi de bilerek, EKS dünyasına ait siber savunma çözümlerinin geliştirilmesinin önemli olduğunu düşünüyoruz. Bu konu test yatağı merkezimizin mottosu ve amaçlarından biriydi. Yerli ve milli ürünlerin ortaya çıkarılması için belli hedefler

belirlemiştik. İki ayrı firmayla sözleşme imzalandı, ürün geliştirme ve bu firmalar test süreçlerini bizim test yatağı merkezimizde gerçekleştiriyorlar. Yine SSB'de bir başka projede değerli kurumlarla birlikte bu tür APT saldırılarının hem gerçekleştirilmesi hem de savunması noktasında belli çalışmalar yapabileceğimiz bir projemiz de söz konusu.

Türkiye'de biz bir strateji olarak, test yatağı merkezimizde sadece elektrik ve su yönetimini hedefledik ancak petrol, doğalgaz, ulaştırma gibi diğer kritik altyapılarla ilgili ülkemizde böyle bir test yatağı merkezi bulunmuyor. Bunların ya üniversitemizde ya da başka üniversitelerde genişlemesi ve yatırımların yapılması gerekiyor. Bizim test yatağı merkezimizin projesinin desteği de SİSAMER (Siber Savunma Merkezi) projesinin Kategori C'si üzerinden desteklendi.

Enterkonnekte sistemin içerisinde özellikle enerji sistemlerinde herhangi bir kırılım merkezinin çökmesi, ondan beslenen diğer sistemin de çökmesi anlamına geliyor. Bu konuda TEİAŞ'ın, proses tarafında çalışan kişi ve kurumların, üniversitelerin ve sektördeki firmaların birlikte çalışarak, bu tür siber saldırılarda geri dönüşü nasıl yapabileceklerini ortaya koymaları gerekiyor. Bu çok önemli bir eksiklik. IT sistemlerinde belki bu konularla ilgili bazı eksikler söz konusu olabilir ama özellikle kritik altyapılar ekseninde hem siber olaylara müdahale boyutuyla hem de geri dönüşüm boyutuyla EKS tarafında çok net tanımlamalar söz konusu değil. Çözümler de çok yok gibi. Bu konu üzerinde özel çalışmaların olması gerekiyor.

2022 Yılında Öne Çıkabilecek Siber Tehditler

Üniversitelerimizde yaklaşık 20-25 yıllık bir yapay zekâ geçmişimiz var ama şu anda sektörün ihtiyacı olan konular henüz üç, beş yıllık bir zaman dilimi içinde popülerleşmeye başladı. Yapay zekâ tabanlı savunma sistemleri varken, saldırı tarafında da yapay zekânın çok yaygın bir şekilde kullanılacağı bir döneme giriş yaptığımızı düşünüyorum. Bu konuda sektörün hem saldırı tarafında, siber silah ya da siber taarruz konusunda hem de siber savunma tarafında üniversiteler ve akademisyenlerle çok yoğun bir mesai içinde çalışmasının önemli olduğunu düşünüyorum. Özellikle zararlı yazılımlarla ilgili süreçlerde; yani APT tabanlı grupların sisteme ilk sızarken zararlı yazılımlar üzerinden sızmaları haricinde, genetik algoritmalarla mutasyona uğramış zararlı yazılımların geliştirilme durumları da söz konusu. Bu apayrı bir boyut. Yine saldırı kısmında insan ve makinelerin birlikte çalışabileceği yeni saldırı türleri ortaya çıkabiliyor. Bunlar tamamen yapay zekâ ekseni içinde ilişkili teknolojilerle birlikte yapılabilecek saldırı çeşitleri olarak düşünülebilir.

"Türkiye'de biz bir strateji olarak, test yatağı merkezimizde sadece elektrik ve su yönetimini hedefledik ancak petrol, doğalgaz, ulaştırma gibi diğer kritik altyapılarla ilgili ülkemizde böyle bir test yatağı merkezi bulunmuyor. Bunların ya üniversitemizde ya da başka üniversitelerde genişlemesi ve yatırımların yapılması gerekiyor."

PEW Araştırma Merkezince yapılan bir akademik çalışmada, görüşlerine başvurulan 1.600 teknoloji uzmanının üçte ikisi 2025 yılına kadar büyük maddi hasar ve can kaybı da yaşanabilecek bir siber savaşın olabileceğini beyan etti. Bunların ağırlıklı olarak kritik altyapılara yapılacak siber saldırılarla ortaya çıkabileceğini düşünüyorum.

Maddi ve finansal kazançların çok yüksek olması sebebiyle 2022'de ve sonraki yıllarda fidye siber saldırılarının sürekli olacağını düşünüyorum. Ülkemizin ya da farklı ülkelerin seçim sistemlerine müdahaleler söz konusu olabilir. Bu fiziksel olarak da, sosyal mühendislik saldırıları üzerinden insanları farklı kanallara yönlendirme biçiminde de olabilir.

Sektörün Yetişmiş Uzman İnsan Kaynağına İhtiyacı Var

Daha önceki Ulusal Siber Güvenlik Eylem Stratejisi kapsamı içerisinde YÖK'de Siber Güvenlik Kurulu oluşturulmuştu. Burada bir siber güvenlik lisans programının açılması konusunda bir çalışma yapıldı ancak bir sonuca varılmadı. Fakat Siber Güvenlik Kurulunda yapılan değerlendirmelerde, uluslararası arenada ağırlıklı olarak bu tür çözümler ve programlar olmadığı için kabul görmedi. Özel alanların yüksek lisans programı ya da doktora programı şeklinde açılması gibi görüşler dile getirildi. Ancak öte yandan, farklı farklı firmalardan gelen yetenekli çalışan talebi de söz konusu. Sektörün şu anda siber güvenlikle ilgili çok ciddi yetişmiş uzman insan kaynağına ihtiyacı var. Ulusal Siber Güvenlik Eylem Planları -eğer buna önem veriyorsa- ile bu programlar çok rahat açılabilir. Bunun adı siber güvenlik mühendisliği olmayabilir, bilgi güvenliği mühendisliği olabilir. Eğer böyle bir program söz konusu olmazsa da, şu anda SSB'nin siber güvenlik kümelenmesi Türkiye'de otorite olarak üstte görünüyor. Dolayısıyla üniversitelerle özel sektör bir araya getirilerek sübvanse edilip sertifika programları şeklinde değil de bu tür eğitim programları açılabilir ve sektörün ihtiyacı olan uzman insan kaynağı yetiştirilebilir.

Diğer yandan, bilgi güvenliği ile siber güvenlik her zaman birbirlerine göre nerede konumlandırılması gerektiği konusunda tartışma yaşanan iki kavram olageldi. Sektörel olarak bilgi güvenliği daha erken geliştiği için otoriteler siber güvenliği bilgi güvenliği konsepti içinde tanımlamıştır. Örneğin TÜBİTAK'ta siber güvenlik, akademik olarak ARBİS'te tanımlanamıyor, bilgi güvenliği konsepti içinde anahtar kelime geçmek zorundasınız. Akademik performansa bakmak istediğiniz zaman her şeyi bilgi güvenliği olarak tanımlıyorsunuz. Dolayısıyla Türkiye'de bilgi güvenliğinin ayrı bir anahtar kelime, siber güvenliğin ayrı bir anahtar kelime olması kabul edilmelidir -ki TÜBİTAK, üniversiteleri her bir iki yılda bir yetkinlik analizine göre sınıflandırıyor. Siber güvenliği bilgi güvenliğinin altına alarak üniversiteleri böyle değerlendiriyor mesela. Bunun bir şekilde aşılması gerektiğini düşünüyorum.

Abdurrahman Emre ÖZKÖK
TÜBİTAK BİLGEM Siber Güvenlik Hizmetleri
Birim Yöneticisi

SİBER TAARRUZ POLİTİKAMIZ OLMALI

Etrafı uzun yıllardır terör örgütleriyle yoğun olarak sarılmış bir ülkede yaşıyoruz. Dolayısıyla savunma politikalarından asla vazgeçmeden siber taarruz politikamız olmalı ve buna yönelik ekipler oluşturulmalı. Ayrıca fidye saldırılarının önümüzdeki yıllarda da artacağını düşünüyorum. Bu saldırı türünde kayıplar yüksek seviyede, bu nedenle uç kullanıcıya ve organizasyonlara konuyla ilgili destek verebilecek bir merkezin kurulmasında fayda görüyorum.

Siber uzay dediğimizde, William Gibson'un *Matrix Avcısı* adlı kitabındaki sibernetix kavramından bir siber kavramı dünyamıza geliyor. Dijital uzay kavramına buradan ulaşabiliriz. "Uzay" tabirini kullanma sebebimiz bir yıldız sistemine benzerliğinden kaynaklanması. Yıldız sisteminin her bir parçasında dijital bir parça var. Siber uzayın bir parçası da insanlar. Sektörel düşündüğümüzde, yani bir yazılım sektörü dediğimiz zaman ya da bir kritik altyapı dediğimiz zaman daha dar kapsamlı konular gündeme geliyor ama siber uzay denildiğinde artık işin içine çocuklarımız, bilgi işlem personelimiz, idari çalışanlarımız veya teknoloji bileşenlerimiz dahil oluyor. Yaş ayrımı, bilgi birikimi, eğitim ayrımı olmadan bir alana girmiş oluyoruz. Dolayısıyla etki alanımız çok geniş. Bu nedenle yıldız sistemi ve uzay ifadesi gündeme gelmiştir.

Siber uzay dediğimiz zaman işler Arpanet veya internetle başlıyor diyebiliriz. Öncesinde de birtakım çalışmalar var ama aslında Arpanet'le başlayan ve bu serüvende dev üreticilerin trend hayallerle sektöre yön verdiği bir yola girmiş oluyoruz. Bu nedenle öngörülmesi zor olan bir alandan bahsediyoruz. Kısa vadede öngörülerimiz olsa da gelişiminde üreticilerin değil kullanıcıların yön verdiği bir dünyaya girmiş oluyoruz. Kullanıcıların bu denli çok olması siber uzayda siber savaş, siber saldırılar, siber caydırıcılık gibi kavramları da beraberinde getiriyor. Bu nedenle, siber savaş gibi tehditleri önlemek için bazı tedbirler almamız gerekiyor.

İşin diğer boyutuna yani stratejiler tarafına geçtiğimizde tabii ki üç büyük güç olan ABD, Rusya ve Çin -kendi politikalarında da belirttikleri gibi- birbirleriyle bu noktada çatışma hâlindeler. İplerin gerildiği noktada uzun yıllar aklımıza sadece Rusya ve ABD gelirken, işin içine Çin de dahil oldu. Bu üç ülke birbirini tehdit olarak görüyor.

ABD'nin Savunma Bakanlığı politikalarını incelediğimizde yenilikçilikten bahsettiğini görüyoruz. Siber uzayın nereye gideceğini bilmediğimiz noktada, yenilikçi bakış açısını önemli bir nokta olarak düşünüyorum. Sektör işbirliğinden çok dikkatle bahsedilmiş. ABD Savunma Bakanlığının personelinin yetkinliğinin artırılmasıyla ilgili, maliyet etkin çözümlerden ve "Caydırıcılık başarısız olursa tüm askeri kuvvetlerin kullanabileceği" doğrultusunda bir ifadeden bahsediliyor.

Rusya'nın politikalarında ise biraz daha milliyetçi bir bakış açısı var. Yerli çözümlerin gündeme gelmesiyle ilgili işbirliği, uluslararası işbirliği vurgusu ve daha çok savunma bakış açısı mevcut ama onların da son zamanlarda siber taarruz tarafına yönelen bir politikalarının olduğunu görüyoruz.

Çin tarafında ise olay siber uzay kültürünün daha da artırılmasının önemli olduğu yönünde. Diğer yandan, siber terör kavramı da Çin'in politikalarında geçiyor, uluslararası işbirliği hakeza aynı şekilde.

Sektör İşbirliği ve Siber Taarruz

Siber saldırıların dünyadaki ekonomik etkileri çok büyük. Bunların azaltılmasına yönelik bazı tedbirler var. Benim özellikle odaklanmak istediğim ve çokça bahsedildiğini düşündüğüm konu sektör işbirliği ve siber taarruz konuları. Türkiye'de sektör işbirliğinde TÜBİTAK BİLGEM'in kuruluş sürecinde rol aldığı, SSB'nin uçtan uca yönetimini sürdürdüğü siber küme yapısı oluşturuldu. Burada ciddi tedbirler ve aksiyonlar alındı ama buna katkı olarak şöyle bir öneri olabilir: TÜBİTAK'ın veya benzer kurumların teşvik yöntemleri var. Bu noktada belki biz bazı firmaların olgunlaşmasını beklemeden, henüz teşvik aşamasında, mutualist bakış açısıyla, firmaların uçtan uca gelişmesi sürecini takip edebiliriz. Bununla ilgili bir politika oluşturulabilir. TÜBİTAK projelere destek verdiği gibi projelerin firmalarına da destek veriyor. Siber kümelenmede biz firmalara ve firmaların geliştirdiği teknolojilere odaklanıyoruz ve onlardan bir olgunlaşma bekliyoruz. Benim önerim, bu olgunlaşmayı beklemeyelim, biz de başlangıcında katkılar sunalım, teşvikten sonraki denetimleri çoğaltarak onlara yön verelim. Denetim sürecinde firmaların çıktılarının takibiyle birlikte işleyiş süreçleri, standartlara uygunluk gibi hususlara dikkat edilebilir. Burada mutualist ifadesini kullanmamın sebebi, firmaların yön verme sürecinde gerek maddi gerek iyileşme anlamında kazanç sağlamalarıdır. Bu işlemde iki tarafın da mutlu olduğu bir model çizebilirsek meyvelerini çok daha hızlı alabiliriz. Bu konuyla ilgili farklı ülkelerde benzer modeller işletilerek büyük siber güvenlik firmaları veya ürünleri olgunlaştırılabilmiştir. Dolayısıyla biz de böyle modelleri örnek alabilir ve verimli bir şekilde değerlendirebiliriz.

Taarruz konusuna gelecek olursak; ülkelerin artık siber taarruzu tehdit olarak görerek bununla

ilgili aksiyonları almaya başladığını biliyoruz. Etrafı uzun yıllardır terör örgütleriyle yoğun olarak sarılmış bir ülkede yaşıyoruz. Dolayısıyla savunma politikalarından asla vazgeçmeden siber taarruz politikamız olmalı ve buna yönelik ekipler oluşturulmalı.

Verinin paylaşımı noktasında, kriptoloji çok kıymetli bir yerde ve minimum bilmesi gerekenler prensibine göre, aradaki sistem yöneticisinin dahi veriye ulaşamaması gerekiyor. Kullanıcı tarafında verinin şifrelenmesi, anahtarının iki parçaya bölünerek belirli bir algoritma ile güvenliğinin sağlanması hususunda araştırma ve çalışmalarımız mevcut. TÜBİTAK BİLGEM'in geliştirdiği Safir Depo çözümünü birçoğumuz veri depolama ve paylaşım için kullanıyoruz. Safir Depo içerisinde geliştirdiğimiz güvenli depolama seçeneğinde de bu bahsettiğim güvenlik tedbirlerini almaya çalıştık.

2022'de Karşılaşabileceğimiz Tehdit Türleri

Deep Fake bir yapay zekâ teknolojisi. Saldırıları ben ikiye ayırıyorum. Akış temelli DDOS gibi kas gücü gerektiren ama arkasında çok fazla bilimin olmadığı bir saldırı türüyle bu tarz saldırılar biraz farklı. Burada altyapısında biraz daha teknoloji var. Bir yapay zekâdan bahsediyoruz. Yüz hatlarımız belli. Yüz hatlarımızın da özelleşmiş noktaları var. Bunu irisle tanımada, parmak izi tanımada, sesle tanımada kullanabiliyoruz. Herkese özgü, benzer ama kişisel olarak farklılaşan noktalar olduğu zaman bu eğitilebilir bir data hâline geliyor. Deep Fake, görüntüyü simüle edip, üstüne video konferans yapıp, kişiyi görüntüye ekleyip arka tarafta bilinmeyen bir makine ile görüştürebiliyor. Bu teknoloji sizi yapay zekâ özelliklerini

> "2022'de belki Deep Fake kullanılarak iris tanıma veya yüz tanıma sistemlerinin aldatılması mümkün hâle gelebilecek. Çünkü üç boyutlu versiyonları gelişebilir."

kullanarak ikna edebiliyor. Olay buralara kadar geldi ve bence daha henüz başlangıç döneminde. Dolayısıyla 2022'de belki Deep Fake kullanılarak iris tanıma veya yüz tanıma sistemlerinin aldatılması mümkün hâle gelebilecek. Çünkü üç boyutlu versiyonları gelişebilir diye düşünüyorum. Olaylara bakarsak, 2019 yılında bir CEO'nun sesi taklit edilerek yüksek meblağda para dolandırıcılar tarafından ele geçirilmiştir. Yine İsrailli üç korsan Fransa Dışişleri Bakanını taklit ederek 800 milyon dolar gibi bir para elde etmiştir. Başka bir olayda ise Barrack Obama'nın görüntüsü başka bir aktörün görüntüsüyle değiştirilerek Trump hakkında olumsuz sözler sarf eder gibi gösterilmiştir.

Tehdit artı zafiyetler eşittir risk diyoruz. Saldırı motivasyonunu buna eklersek -ki saldırı motivasyonu kaynak kazanımı olabilir, bir ideoloji olabilir, itibarsızlaştırma olabilir veya kendini ispat etme olabilir- gelecekte ne yönde saldırılar olacağını biraz tahmin edebiliriz. Orada da karşıda kazanım elde edilecek alanı şöyle değerlendiririz: Dünya nereye gidiyor, trend hayaller dediğimiz şey nelerdir diye düşünebiliriz. IoT'ler olabilir, bulut bilişim çok ciddi şekilde olabilir. Geleceğimizin bu noktalarda olması kuvvetle muhtemel. Sosyal medya haberin doğruluğuna bakılmayan bir platform hâline geldi. Fidye saldırılarının önümüzdeki yıllarda artacağını düşünüyorum. Bu saldırı türünde kayıplar yüksek seviyede, bu nedenle uç kullanıcıya ve organizasyonlara konuyla ilgili destek verebilecek bir merkezin kurulmasında fayda görüyorum.

Bulut bilişim alanına baktığımızda ise mikro servise yönelik exploit'ler yazılmaya başlandı; onları 2022, 2023 yıllarında görebiliriz. Kripto cüzdanlarının çalındığına yönelik haberler var. Kripto para sektörünün geliştiğini görüyoruz, bu alanda yeni saldırı türlerinin oluşacağını düşünüyorum. IoT endüstriyel alanda çok daha hızlı yayılıyor ve normal ağlarımıza yayılım gösteriyor. Akıllı cihazların mahremiyete ve kişisel bilgilere yönelik etkilerini göz önünde bulundurursak, IoT alanında son kullanıcıyı etkileyecek saldırıları görmek mümkün. Siber alanda soğuk savaş çok ciddi şekilde gündeme geliyor. Çok dillendirilmese de aslında arka planda Suriye'de, Gürcistan'da, Ukrayna'da, Estonya'da bazı saldırılar görüyoruz. Bunların devamı gelebilir. Dolayısıyla elektronik harp ile siberin birleşimi bir versiyonu çıkabilir. Bizim de oralara hazırlık yapmamız gerekebilir diye düşünüyorum.

Eğitici Bir Uygulama Yapılabilir

Sosyal mühendislikle ilgili sızma testleri yapıyoruz. Maalesef çoğunlukla yüksek başarı oranında sonuçlarla karşılaşıyoruz. Bu çalışma sonucunda kurumun bir farkındalığı oluşuyor. Sonrasında farkındalık eğitimleri, videolar, broşürler yayınlıyoruz ama ben hiçbirinin yeterli olduğunu düşünmüyorum. İnsanlar maalesef bir şeyleri yaşamadan tam olarak

öğrenemiyorlar. Dolayısıyla yaşayarak nasıl öğrenebileceğimiz ve sosyal mühendislik testlerini kurumlarda nasıl uygulayabileceğimiz konularında normal sosyal mühendislik testlerinden farklı bir proje önerisi geliştirdim. Kullanıcıya o linke tıkladığında ve önüne bir pop-up veya bir video çıktığında nerede hata yaptığını, örneğin kaynak adresi kontrol edebileceğini veya IP adresine bakabileceğini göstereceğiz ve eğitici öneriler sunacağız. Bunu yaptıktan sonra, bu gerçek bir olay olsaydı karşılaşabileceği durumları, örneğin dosyalarının şifreleneceğini ya da cihazın ele geçirilmesiyle sonuçlanan diğer problemleri göstereceğiz. Yani alabileceği önlemleri, nasıl yedeklemeler yapabileceğini, şifreyi çözmek için hangi yöntemlere başvurabileceğini anlatan içerikleri olan eğitici bir uygulamadan bahsediyorum. Kamu kurumlarında veya sivil noktalarda kanuni sınırlara da dikkat edilerek böyle bir yöntem uygulanabilir, etkisi de yüksek olabilir.

Enis Müçteba MEMİŞ
STM Teknoloji Genel Müdür Yardımcısı

KRİTİK ALTYAPILARI YEDEKLEMELİYİZ

Yoğun bir şekilde doğa olaylarının farklılaştığı ve kamu düzenini tehdit edecek şekilde çeşitli altyapıların devreden çıktığı bazı vakalarla zaman içerisinde karşılaşmaya başladık ve bu riskler artarak devam edecek gibi görünüyor. Bununla ilgili belki bir merkezi koordinasyonla bir savaş ya da felaket durumuna karşı ya da küresel ısınma gibi negatif etkilerden en az etkilenmek için önlemlerin toparlanıp bir politikaya dönüştürülmesi ve bunlarla ilgili çeşitli altyapı projelerinin ortaya çıkartılması gerekiyor.

Kamu düzeni, verilen hizmetlerin devamlılığıyla mümkün olabiliyor. Bu anlamda özel, kamu fark etmeksizin düzenli bir iş hayatı şu anda devam ediyor. Dolayısıyla işlerin devamlılığı bizim için kritik. Diğer yönüyle, çeşitli hizmetler veren kurum, kuruluş, banka, internet sağlayıcısı, marketler; artık bunların tamamı şu anda siber dünyanın bir parçası. Dolayısıyla hizmet verenle hizmet alanların alım satım işlemlerinin devamlılığı burada esastır. Bir yandan güvenlik birimlerimiz, Türk Silahlı Kuvvetleri (TSK), Emniyet, İstihbarat birimleri ve savunma sanayii gibi bizlerin hinterlandını oluşturduğu bir güvenlik ağı var ve bu ağda da güvenliğin devamı bizim için esas.

Hatırlanacak olursa, 2021 yılında Maden Tetkik ve Arama Genel Müdürlüğünde (MTA) büyük bir patlama meydana geldi. Patlama doğalgaz hattında meydana gelmiş ancak aynı hattın devamındaki çeşitli elektrik hatları, network kabloları ve çeşitli bakır kablolar da imha olmuştu. O bölgede yoğun bir şekilde bir telefon trafiği meydana geldi. Şehirde sesi duyan herkes telefonlarına sarıldı ve o anda cep telefonu operatörleri kısa süre de olsa hizmet dışı kaldı. Aynı şekilde o bölgedeki belli mahallelerde elektrik, gaz kesintisi gibi sorunlar yaşandı. Akşama doğru hizmetler tekrar stabil hâle geldi ama o olayı örnek vaka olarak ele aldığımızda, bir bölgenin tamamen devreden çıkmasıyla iletişim, elektrik ve kamu hizmetleri ile iş devamlılığı bakımından ciddi bir sıkıntı yaşandığını gözlemledik.

Temel olarak işlerimizin devamlılığı için bizler siber güvenlik için nasıl verileri yedekliyorsak, altyapıların da yedeklenmesi ihtiyacı burada net bir şekilde ortaya çıkmış oldu. Enerji nakil hatları bunun için önemli bir örnek. Şehir sularının çeşitli barajlardan akışının devamlılığı yine toplum ve kamu düzeninin devamlılığı için esas teşkil ediyor. Bu anlamda altyapıların da yedeklenme ihtiyacı burada ortaya çıkıyor. Siber güvenlikle yine birbirlerine teğet durumdalar. Kimisi çeşitli sabotaj ya da kazalarla meydana gelebilirken, kimisi çeşitli siber olaylarla ortaya çıkıyor.

İran'da bir nükleer santralde ortaya çıkan Stuxnet zararlısı, o dönem İran'daki nükleer çalışmaları aksatmıştı ama o sıradan ve kamuyu ilgilendirmeyen bir vakaydı. Yine dört, beş sene önce Türkiye genelinde yoğun bir elektrik kesintisi olmuş, Batı bölgesi tamamen enerjiden mahrum kalmıştı. Burada da PLC, SCADA gibi çeşitli kontrol sistemlerinin güvenliği, bunların yedekliliği, işletilmesine yönelik çeşitli güvenlik kural ve politikalarının oluşturulması gibi konular bizim için oldukça önemli gözüküyor. İçinden geçtiğimiz küresel ısınma sürecinde doğa olaylarının farklılaştığı ve altyapıların kamu düzenini tehdit edecek şekilde devreden çıktığı çeşitli vakalarla karşılaşmaya başladık ve bu riskler artarak devam edecek gibi görünüyor. Benzer bir başka olayı 2021'in yaz aylarında Muğla Milas bölgesinde bir enerji santraline kadar yaklaşan orman yangınıyla yaşadık. Dolayısıyla temel altyapılarımızla ilgili güvenlik odaklı bir yedekliliği kamu otoritelerinin, ilgili hizmeti veren kurum ve kuruluşların belli bir politika çerçevesinde oluşturması gerekiyor. Bununla ilgili belki bir merkezi koordinasyonla bir savaş ya da felaket durumuna karşı ya da küresel ısınma gibi negatif etkilerden en az etkilenmek için önlemlerin toparlanıp bir politikaya dönüştürülmesi ve bunlarla ilgili çeşitli altyapı projelerinin ortaya çıkartılması gerekiyor.

Platformlarda Alınan Siber Güvenlik Tedbirleri

Son 15 yıldır savunma sektöründe artık platform seviyesinde ürünler olgunlaşmaktadır. 1974'teki Kıbrıs Harekâtı'ndan itibaren, Kara Kuvvetleri Güçlendirme Vakfı, Hava Kuvvetleri Güçlendirme Vakfı, Deniz Kuvvetleri Güçlendirme Vakfı gibi vakıflar kuruldu. Ardından tüm bu vakıflar birleştirilerek Türk Silahlı Kuvvetlerini Güçlendirme Vakfı tepede bir çatı organizasyon olarak oluşturuldu. Bu vakfın altında ASELSAN, HAVELSAN, ROKETSAN, İŞBİR gibi şirketler var. STM Savunma Teknolojileri, Mühendislik ve Ticaret A.Ş. (STM) de kısmi olarak o grubun içinde. Bizde de Vakfın yüzde 33 hissesi var. Toplanan fonun yönetimi ile projelerin önceliklendirmesini yapmak üzere o dönemde Savunma Sanayii Müsteşarlığı kuruldu. 80'li yılların başlarında da Savunma Sanayii Destekleme Fonu adı altında bir fon oluşturuldu. Çeşitli platform projeleri, çeşitli vergilerden elde edilen gelirlerle bu fondan, merkezi bütçeden bağımsız olarak Genelkurmay'ın önceliklendirme sırasına göre başlatıldı.

Akabinde hazır alımlar, sonrasında montaj gibi çeşitli emekleme süreçleri geçildikten sonra aşağı yukarı 2000'li yıllarla beraber özgün tasarımlar, özgün üretimler başladı. Böylece hava, kara, deniz ve uzay alanlarında çalışmalar başlatılmış durumda. Bu çalışmalar neticesinde çok sayıda platform devreye alındı. Hava tarafında F-16'ların millileşmesi için Özgür Projesi yürütüldü. C-130 nakliye uçaklarımızın modernizasyonu kapsamında bir aviyonik

modernizasyon paketi Türkiye'de ilk defa geliştirildi. Oradaki görev bilgisayarı, görev yazılımları TUSAŞ'ta o dönemde geliştirildi. Ülkemizdeki kurum ve kuruluşlar, emniyet ve güvenlik tarafıyla ilgili harekât uçuş yazılımlarındaki temel tecrübeyi o dönemde edindiler. Yani TUSAŞ'ın, ASELSAN'ın mühendisleri, SSB ve Hava Kuvvetleri Komutanlığının bu dönemde edindiği tecrübeler, temel olarak Erciyes Projesi, C-130 ve F-16'nın özgürleştirilmesiyle ilgili olan Özgür Projesi ile başladı.

Bunlar envanterdeki uçaklardı, onlarda bir modernizasyon gerçekleştirildi. Ardından biz kendi özgün uçaklarımızı geliştirmeye başladık. Hürkuş bunlardan bir tanesi. Hürkuş'un A varyantı, B varyantı, C varyantı çeşitli görevlere yönelik geliştirildi. Akabinde bir Hafif Taarruz Helikopteri projesi olan Atak Projesi başlatıldı. Atak Projesi de bizim için önemli kilometre taşlarından bir tanesiydi. Atak; ASELSAN'ın temel görev sistemlerini, görev yazılımlarını, çeşitli sensörlerini millileştirdiği, ROKETSAN'ın da çeşitli mühimmatlarını bu platforma entegre ettiği döner kanattaki ilk proje oldu.

Akabinde Hürjet Projesi, Milli Muharip Uçak Projesi gibi artık dünyada birinci sınıf ülkelerin giriştiği bir iş alanına Türkiye giriş yaptı. Milli Muharip tarafı zaten bu işin zirvesi. Şu an dünyada beşinci jenerasyon dediğimiz, ABD'nin F-22 ve F-35 uçakları dışında henüz envantere alınmış ve kabiliyetini kanıtlamış, harp sahasında da combat proven olmuş bir platform yok. Biz başladık. İngilizler başladılar. Almanya-Fransa ortaklığı bir projeye başladı. Rusların SU-57 projesi var. Onun dışında da Çin'in J-20 serisi uçağı var. Bu platformlarda temel olarak yoğun bir şekilde teknoloji kullanılıyor. Hemen hemen o platformun ortaya çıkmasında

harcanan adam saatinin minimum yüzde 60'ı teknoloji alanında çalışan elektronik ve bilgisayar mühendisleri tarafından gerçekleştiriliyor. Yani uçağın yapısal kısımları, alt kısımları, hidrolik sistemleri, makine dünyasına, metalurji dünyasına ait olan kısmı teknoloji alanına kıyasla adam-saat olarak daha azalmış durumda. Burada kullanılan teknolojiler içinde kripto teknolojileri; çeşitli askeri ağ yapıları; 1553 gibi, 429 gibi BUS yapıları var. Artık fiber optik haberleşme BUS'ları uçaklarımızın içine girmiş durumda. Kırmızı ağ, siyah ağ uçağın içini ayrıştırmış durumda.

Bu yazılımların geliştirilmesi sırasında, bizim temel emniyet seviyesinde kullandığımız standartların yanında artık güvenlik standartları da işin içine girmiş durumda. Dolayısıyla artık yazılımı geliştirirken bizim tüm süreçlerimizi güvenli yazılım geliştirme yönünde bir dönüşüme uğratmamız gerekiyor. O çalışma çok yeni. Şu anda TUSAŞ, STM ve HAVELSAN üçlüsü, beşinci jenerasyon bir uçak tarafında siber güvenlik kurallarına uygun bir şekilde bu işin nasıl yapılabileceğini çalışmaktalar. Çeşitli çalıştaylar devam ediyor. Tabii ki TÜBİTAK da bu işin içinde var. Görev bilgisayarı kısmı, şu anda donanım geliştirme yönüyle TÜBİTAK tarafından geliştiriliyor. Çok büyük ekipler, multi-disipliner ekipler çalışıyor. Uçağın radar yazılımı farklı bir disiplinin ürünü; elektronik harp sistemindeki yazılımlar farklı bir disiplindeki arkadaşların ürünü. Uçağın temel görevlerini icra etmesini sağlayacak, silahlarını yönetecek, elektronik harbini yönetecek, radarını yönetecek, diğer uçaklarla bir network'e girecek, Network Centeric Warfare'i sağlayacak, mühimmatlar dahil olmak üzere havada ağ oluşturacak sistemleri de yöneten merkezde bir görev yazılımı var. Buna biz genel olarak harekât uçuş yazılımı diyoruz. Yaklaşık 400-500 kişilik bir ekip yalnızca Milli Muharip Uçak tarafında yazılım mühendisi olarak görev alacak. Dolayısıyla bu kuralların çok ciddi manada oluşturulup, farkındalığın artırılıp, sürekli ve bitmeyecek şekilde eğitimlerin tekrar tekrar hatırlatma şeklinde verileceği bir sürece şu anda girmiş durumdayız.

Güvenliğimiz Çip Seviyesinden Başlıyor

Yalnızca Milli Muharip Uçak tarafında değil deniz tarafında da çok değişik projeler yürüyor. Deniz Kuvvetlerimiz için geliştirilen MİLGEM projesi STM'nin ana yükleniciliğinde yürüyor. Burada büyük bir komuta kontrol yazılımı var. Bu komuta kontrol yazılımıyla geminin radarını; hava savunmasına yönelik farkındalığını; sualtındaki sonarlarıyla ilgili olan haberleşmesini; durumsal farkındalığını; havada, suyun altında, satıhta ne olduğunu sizin takip etmeniz gerekiyor. Ayrıca sizinle dost kuvvet olan ya da sizin filonuzda bulunan gemilerle güvenli bir şekilde veri haberleşmesini, sesli haberleşmeyi, gerekiyorsa görüntülü haberleşmeyi de sağlamanız gerekiyor. Burada herhangi bir hasmın bu network'te araya girip sizi dinlemesi, kriptoları kırması gibi durumlar yaşanabilir. Bunların tamamı kriptolu ağlar. Link 11, Link 22 dediğimiz ağlar ağırlıklı olarak deniz tarafında kullanılıyor. Link 16 ağı ise çoğunlukla hava ve deniz platformlarında ve akıllı mühimmatlarda ortak kullanılıyor. Bu ağlardan yalnızca platformların kendisi faydalanmıyor, platformlardan atılan ve uzun erimli mühimmatlar bulunuyor. Hem gemiyle iletişimini hem uyduyla olan iletişimini sizin bu ağlar üzerinden güvenli bir şekilde devam ettirmeniz gerekiyor. Dolayısıyla ağ tarafındaki güvenlik bizim için platformdan attığımız mühimmatları da takip etmek bakımından oldukça önemli. Platformun içine

> "Türkiye'de henüz bir çip fabrikası, ona yönelik bir yatırım yok. Dolayısıyla kullandığımız ürünler, mikroişlemciler, micro-controller'ların tamamı dünyadaki belirli üreticilerden geliyor. Hâliyle bu çiplerin içinde bizim gerçek zamanlı kullandığımız işletim sistemleri, çeşitli kriptolama algoritmaları, görüntü işleme algoritmaları ya da veri kayıt algoritmalarının pek çoğuyla ilgili bizim IP core dediğimiz ve diğer üçüncü parti olarak aldığımız ürünler de henüz yurtdışından geliyor. Dolayısıyla çip seviyesi bizim için ciddi tehditlerden biri olmaya devam ediyor. Bununla ilgili yapılacak en önemli girişim Türkiye'de bir çip yatırımının başlatılması."

döndüğümüz zaman; aslında bizim güvenliğimiz çip seviyesinden yani en alt seviyeden başlıyor. Maalesef Türkiye'de henüz bir çip fabrikası, ona yönelik bir yatırım yok. Dolayısıyla kullandığımız ürünler, mikroişlemciler, micro-controller'lar, FPGA'ler (Field Programmable Gate Array/Alanda Progranlanabilir Kapı Dizisi); bunların tamamı dünyadaki belirli üreticilerden geliyor. Hâliyle bu çiplerin içinde bizim gerçek zamanlı kullandığımız işletim sistemleri, çeşitli kriptolama algoritmaları, görüntü işleme algoritmaları ya da veri kayıt algoritmalarının pek çoğuyla ilgili IP core dediğimiz, temel FPGA kodları ve diğer üçüncü parti olarak aldığımız ürünler de yurtdışından geliyor. Dolayısıyla şu anda, bu kapalı kutu şeklinde işlemcilerimizin içine gömdüğümüz ürünlerin güvenliğine dair pek çok bilinmeyen var. Çip seviyesi bizim için ciddi tehditlerden biri. Bununla ilgili yapılacak en önemli girişim Türkiye'de bir çip yatırımının başlatılması. Minimum bir milyar dolar yatırımla bu işe başlanabilir, devamında temel ihtiyaçlarımızı karşılamak üzere 10 milyar dolara kadar giden bir yatırım gerekiyor. Çin yaklaşık 20 yıldır bu alana yatırım yapıyor. Savunma sektörü öncelikli başladılar, sonrasında haberleşme ve network tarafına doğru yayıldılar ama ilk başlangıç noktaları tamamen savunma sanayii üzerineydi. Şu ana kadar 100 milyar doların üzerinde bir çip yatırımı gerçekleştirmiş durumdalar. Çip seviyesinden sonra kart seviyesine geçiyoruz, kart seviyesinden kutu seviyesine, kutu seviyesinden o kutuların bir araya geldiği bir sistem network'üne erişiyoruz. En tepede ise sistemler sistemi, yani platformun kendisi. Artık pek çok sistemin beraber, belli haberleşme kuralları içinde eşgüdümle çalıştığı bir platform meydana geliyor. Bunların tamamında bizim siber dünyadaki, sivil dünyadaki pek çok önlemleri, kuralları bu tarafa aktarmamız, gerekiyorsa askeri tarafta yeni kural setlerini oluşturmamız gerekiyor. Örnek vermek gerekirse, askeri anlamda Hava Kuvvetleri ile SSB'nin oluşturduğu bir uçuşa elverişlilik sertifikasyon otoritemiz var. Sertifikasyon Kurulu ile uçağımızın elektriksel, çevresel, EMI/EMC'ye dayanımı, nükleer, biyolojik, kimyasal saldırılara dayanıklığı vb. gibi çeşitli alt dallarda sertifikasyonunu sağlıyoruz. Siber tarafla ilgili alan şu anda boş. Siber sertifikasyona yönelik hem SSB'de hem Hava Kuvvetleri ve diğer kuvvetler içinde temel kuralları koyacak, bu kuralları uygulayacak ve projelerin tüm süreçleri boyunca temel denetimleri gerçekleştirecek bir yapıya ihtiyacımız var. Yani siber dünyanın platform ayağında pek çok eksiğimiz var. Şu ana kadar hep emniyet odaklı gittik. Bundan sonra güvenlik tarafını da işin içine dahil edecek çalışmaları genişletmemiz gerekiyor.

> Siber sertifikasyona yönelik hem SSB'de hem Hava Kuvvetleri ve diğer kuvvetler için de temel kuralları koyacak, bu kuralları uygulayacak ve projelerin tüm süreçleri boyunca temel denetimleri gerçekleştirecek bir yapıya ihtiyacımız var. Yani siber dünyanın platform ayağında pek çok eksiğimiz var. Şu ana kadar hep emniyet odaklı gittik. Bundan sonra güvenlik tarafını da işin içine dahil edecek çalışmaları genişletmemiz gerekiyor.

Ortak Operasyon Merkezi Kurulmalı

Kamu tarafında belki sivil kurum ve kuruluşlar için bir ortak operasyon merkezi; bir de güvenlik kurumlarına yönelik ortak operasyon merkezi kurulabilir. ABD'de NSA'in, CIA'in, FBI'ın ortak işlettikleri, her birinin kendi siber operasyon merkezinde topladığı, zafiyet analiz laboratuvarlarında üzerinde çalıştığı ama bu ortak operasyon merkezinde bunları işleyip ilgili kurumun kılcallarına kadar bilgilendirdiği bir operasyon merkezi konsepti zaten hâlihazırda var. Böyle bir ortak operasyon merkezi ihtiyacı sivil dünyada da gözüküyor.

Başka önemli bir konu ise, bu alanda bizim en büyük sıkıntımız nitelikli personel bulmak. Sızma testi yapacak bir arkadaştan tutun da bir SIEM ürünü geliştirecek developer'a kadar pek çok alanda açığımız var. Bilgisayar mühendisliği, elektronik mühendisliği, yazılım mühendisliği bölümlerinden mezun arkadaşları, bir miktar network tecrübesi olduysa, Telco operatörlerinde ya da kurumların bilgi sistemleri bölümlerinde bir network grubunda çalıştılarsa, çoğunlukla kısıtlı personeli bir araya getirip bu projeleri yürütmeye çalışıyoruz. Bir yandan da personelin eksik yönlerini tamamlamak üzere sürekli eğitim programları düzenliyoruz. Verdiğimiz eğitimler de pahalı eğitimler. Bir müddet sonra bir bakıyoruz Dubai'den, Almanya'dan bir iş teklifi alınmış, herkes yurtdışına geçiyor. Ülkemizde alan uzmanlarını büyük zorluklarla yetiştiriyoruz, yetiştirdiklerimizi de yurtdışına kaybediyoruz. Dolayısıyla yetişmiş personel arzını artırmamız gerekiyor. O bakımdan üniversitelerimizdeki akademik eğitimlerimizi çeşitlendirmemiz gerekiyor.

Güray YILDIZ
TUSAŞ Yazılım Mühendisliği Direktörü

SİBER GÜVENLİK KURULUNA İHTİYACIMIZ VAR

TUSAŞ başta, vakıf firmalarımızın, platform üreticilerimizin siber güvenlik tehdidinin kesinlikle çok farkında olması gerekiyor. Siber güvenlik doğrudan emniyetle bire bir ilişkilidir. Bir şey emniyet kritikse, siber güvenlik anlamında da kesinlikle kritiktir. Bizim siber güvenlik anlamında da bir Siber Güvenlik Kuruluna ihtiyacımız var. Bu kurul, ama proje bazlı ama daha üst seviyede, hava aracı platformuna uçuş izni verirken, sistemi siber güvenlik açısından değerlendirip izin vermelidir.

Emniyet (safety) ve güvenlik (security) hep karıştırılır. Yanlış çalışması sonucunda ölümcül bir sonuca yol açan bir sistemin parçası olan yazılımlar emniyet kritiktir. Örneğin, bir uçağın otokontrol yazılımıyla ilgili olarak beta sürümünü çıkartayım, yayınlayayım, kullanıcılar kullansın, bana geribildirim yapsınlar, düzelteyim demek gibi bir şansınız yoktur. İlk yapışınızda doğru yapmak zorundasınız. Emniyet olarak baktığımızda, dünyadaki havacılık yazılımları, kullanılan teknoloji anlamında 15 yıl kadar sektörün gerisindedir çünkü teknolojilerin kendini kanıtlamasını bekleriz. Herkes Java kullanırken biz C kullanırız, hatta Ada kullanırdık. Keza şu an safety olarak baktığımda emniyette sektör, otorite, uçuşa elverişlilik standartları oturmuştur. 1990'lı yıllardan gelen, en son standart güncellemesi 2011'de olan, DO 178 denen bir standart vardır. Eğer ki siz yazılımınızı hem süreç hem ürün anlamında belirtilen standarttaki kriterlere uyumlu geliştirirseniz, bu yazılım uçuş emniyetini sağlar ve hem SSB'de hem de Sivil Havacılık Genel Müdürlüğü kapsamında bu mekanizmalar kurulmuştur.

İşin emniyet tarafında ise ilgili standart 2020'de yayınlandı. 2020'de yayınlanan Advisory Circular ile DO 326 ve 356 denen, Airworthiness Security Method Specifation Guideline'ları ile uyum, zorunlu hâle geldi. Milli Muharip Uçak öncesindeki projelerimizde, siber güvenlik ile ilgili isterlere, çok rahat "not applicable", air gap var deyip geçiyordum. Ama şu an öyle değil. Hatta daha önce de öyle olmaması gerektiğini şu an anlıyorum. Örneğin, yer görev planlama var, uçuş planlarını bir RMM (Removable Media) card ile uçağa aktaracaksınız. Air gap zaten

var ama ben şu an siber güvenlikle ilgili standartları incelediğimde bakıyorum ki bir insider, bir casus ya da bilinçsiz bir kullanıcı o RMM safe kartı alıp dışarıya yayınlayabilir. Buradaki tehdit siber değil insan. Ama tehdide uğrayan sizin dijital varlığınız. Dolayısıyla bu bir örnek.

TUSAŞ başta olmak üzere, vakıf firmalarımızın, platform üreticilerimizin siber güvenlik tehdidinin kesinlikle çok farkında olması gerekiyor. Siber güvenlik doğrudan emniyetle bire bir ilişkilidir. Bir şey emniyet kritikse, siber güvenlik anlamında da kesinlikle kritiktir.

En Zayıf Halka Kadar Güçlüsünüz

Önemli konuların başında eğitim ve farkındalık geliyor. Siz ne kadar güçlü bir sistem oluşturursanız oluşturun en zayıf halka kadar güçlüsünüz. Bu en zayıf halka da son kullanıcıdır. Dolayısıyla eğitim bilinçlendirme seviyesini artırmamız gerekiyor. Bu anlamda anket, oyunlama yöntemleri gibi interaktif yöntemlerle bilinç artırılabilir. Genelde yüksek lisans programlarımız var ancak lisans seviyesinde de olmalı. Bu kapsamda STM'nin de ortağı olduğu İstanbul Teknopark tarafından İstanbul'da açılan Siber Güvenlik Mesleki ve Teknik Anadolu Lisesi'nin iyi bir örnek olduğunu düşünüyorum.

İkinci önemli husus, hem yazılım hem donanım anlamında yerli ürünlerimizi kullanmaktır. Yerli yazılım ve donanım kullanımında Milli Muharip Uçak'tan örnek vermek istiyorum. İşletim sistemi ve donanımın yerli, milli olması hem maliyet etkinlik hem de emniyet ve güvenilirlik anlamında çok çok önemli. Bir uçağa bir yazılım yaptığımız zaman COTS (Hazır Ürün -Commercial Off The Shelf) diye bir şey kabul etmeyiz çünkü arkada ne çalıştığını bilmeyiz. Ama siz bir emniyet kritik yazılım yazdığınızda, yazdığınız her kod satırının tek tek test edildiğini ve sonuca etkisini görmek zorundasınız. Çünkü "uçtuğunu test et, test ettiğini uç" kuralımız var. Bunu hem donanıma hem işletim sistemine uyarlamak durumundasınız. Windows işletim sistemini 100 dolara alırsınız ya da bilgisayarın içinde parasız alırsınız. Ama gerçek zamanlı bir işletim sistemi alalım dediğiniz zaman (kaynak kodu olmadan sadece executable/uygulama olarak), 300 bin dolar civarındadır. "Sertifikasyon paketini/kanıt dosyalarını göster" dediğiniz zaman 4-5 milyon dolar ödemeniz gerekiyor. Ayrıca paradan ziyade esas problem, kendi geliştirdiğiniz bilgisayarı yurtdışına göndermeniz. Böylece sizin tüm know how'ınız, tasarımınız gidiyor. Üstelik gönderdikten sonra karşı taraf belki içine bir şey katacak; yani sisteminizi de tamamen zafiyete açık hâle getiriyorsunuz. Dolayısıyla bizim en başta işletim sistemi, sonra donanım tasarımı ve kendi yazılımlarımızı geliştirmemiz lazım. Biz bu bilinçle projemizi kurguladık, işletim sistemi ve donanım anlamında TÜBİTAK BİLGEM'le beraber çalışıyoruz.

Burada eksik olduğunu düşündüğüm şey şu: Ben bir dokümanı ürettim, risk analizi yaptım, tehdit faktörlerini değerlendirdim, onaya gönderdim, bu doküman doğru ise ben denetimi geçtim olmamalı. Emniyette şu vardır: Aktif involment, stage of involment denen SOI denetimleriyle SSB, Sivil Havacılık, STM'nin sağladığı danışmanlar bizleri denetler. Denetlemek de sadece gelip anlık resim çekme şeklinde değil sürece ve ürüne sürekli katkı şeklinde olur. Dolayısıyla bizim siber güvenlik anlamında da bir Siber Güvenlik Kuruluna ihtiyacımız var. Bu kurul, ama proje bazlı ama daha üst seviyede, hava aracı platformuna uçuş izni verirken sistemi

> "Uçuşa elverişlilik, DO-326/55'e uyumumuz anlamında, sektörü denetleyecek, özellikle devletimizle ilişkili olacak bir kuruluşa, SSB'nin önderlik edeceği bir mekanizmaya ihtiyaç olduğunu değerlendiriyorum."

siber güvenlik açısından değerlendirip izin vermeli. Uçuşa elverişlilik, DO-326/55'e uyumumuz anlamında, sektörü denetleyecek, özellikle devletimizle ilişkili olacak bir kuruluşa, SSB'nin önderlik edeceği bir mekanizmaya ihtiyaç olduğunu değerlendiriyorum.

Bunun yanı sıra şirketler, CMM (Capabilitiy Mature Model -Olgunluk Değerlendirme Modeli) denilen değerlendirme yöntemini de uyguluyor. Sen ürün anlamında, tasarım organizasyonu anlamında ne kadar olgunsun (seviye 1 misin, 2 misin, 3 müsün); bunların denetlenmesi anlamında ben devletimizden bu kurulların oluşmasında destek bekliyorum.

Üçüncü konu ise özel sektörden ne beklediğimizdir. STM, HAVELSAN gibi bu konuya özel olarak adanmış, başta vakıf firmalarımızdan özel sektörün de bilgi birikimini, yetkinliklerini, ürünlerini alarak Milli Muharip Uçak projemize katkıda bulunmasını istiyoruz.

Platformlarda Siber Güvenliğe Yönelik Tedbirler

Yazılım olarak şu an Milli Muharip Uçak'ta projenin en başındayız. Mesela ağırlık konusu konuşuluyor. SWAP (Size Weight and Power) denilen kısaltmalar var. Ağırlık olarak yazılımın hiçbir etkisi yok ama fonksiyon olarak çok büyük bir etkimiz var. Bir uçağın gerçekleştirdiği görevlerin -ama görev ama seyrüsefer- yüzde 60-66'sını yazılım ağırlıklı sistemler gerçekleştiriyor. Bu da yazılımın karmaşıklığına direkt yansıyor. Wright Kardeşler ile 1900'lü yıllarda uçuş başladı, sıfır satır kod. F-16'da iki milyon satır kod, Erciyes'te iki milyon satır kod, F-35'te 15 milyon satır kod. Biz de F-35'i baz aldığımızda yine 15 milyon satırlık bir kod hacmiyle karşı karşıyayız. Ben emniyet/güvenilirlik ilişkisine çok meraklıyım. Örneğin bir aviyonik cihaz aldığınızda İngilizce'de şu denir: "No single point of failure should result in a catastrophic event". Yani, hiçbir tek kaynaktan hatanın sonucu ölümcül olmamalıdır. Örneğin, irtifa ölçer. Gece şartlarında, Instrumented Flight Rules (IFR) rejiminde siz o irtifaya güvenerek uçarsınız. Eğer tespit edemediğiniz bir hata varsa dağa çarparsınız ve ölüme yol açar. Ve burada şu söylenir. Bunun güvenilirliğinde, hata oranının küçük olması gereken, 10-9 diye bir rakam vardır. Sağlaması yetmez. En az iki tane olması lazım. Yedekliliği sağlamanız gerekir. Çünkü sistematik olarak hata olmaz, random bir hata olur, tek cihazdaki hata sizi öldürür. Yazılımda bu Süreç Teminatı (Process Assurance) ile sağlanır. Yani confidence level denilen; ekibiniz, ortamınız, bu işe ayırdığınız vakit ile sizin gerçekten emniyetli bir yazılım geliştirebileceğinize dair güvenilirliğinizden emin olmanız gerekir. Otorite bunu her defasında denetler. Bir firmayı bir kez denetlediyse, ikincisinde daha az denetler çünkü size güven duyar. Güvenli yazılım geliştirme için de benim kendi adıma direktör olarak, ekip olarak farkındalığım arttı, iyi doküman çıkardım demek yetmez. SSB'nin, Kuvvetin, Devletimizin, otorite olarak en başından en sonuna aktif olarak içimizde yer alarak bunu sağlaması gerekir.

CMMI olgunluk modelinin de denetçileri vardır. Beş aşaması söz konusudur. Bir; niyet ettim, şu işe girdim. İki; proje başına uyguluyorum. Üç; şirketteki tüm projelerde uyguluyorum. Dört; uyguladığımı ölçüyorum. Beş ise; ölçüp, sürekli iyileştirme gösteriyorum. Benzeri siber güvenlik için de var. Siber hijyen olduğunuzu veya emniyet kritik yazılım geliştirebildiğinizi, güvenli yazılım geliştirebildiğinizi göstermeniz gerekiyor. Yıldırım düşme ihtimali herhalde milyonda birdir ama bir hava aracı tasarımına baktığınız zaman kesinlikle ve kesinlikle o hava aracına yıldırım çarpacakmış gibi tasarlanması gerekir. Nasılsa çarpmaz, milyonda bir olasılık demezsiniz. Tüm o elektrik sistemlerini, uçağın yapısını, vs. elektrik çarpmasına uygun bir şekilde tasarlamanız gerekir. Yazılım da öyle. Yazılımda ben belki şunu diyebilirim: "Benim çok iyi bir ekibim var, emniyet kritik yazılım yapıyorum, yüzde 100 test ettim." Ama siber güvenlik için böyle diyemezsiniz. Kesinlikle ve kesinlikle benim sistemim saldırıya uğrayacak diye düşünmeliyiz. DO-326/56 gibi standartlar sizi bunları düşünmeye zorluyor.

Milli Muharip Uçağı beşinci nesil yapan özelliklerin çoğu ses tanıma sistemi, pilot farkındalığını kaybettiğinde bunun anlaşılıp otonom sistemler devreye alınarak üsse geri dönmesi gibi yazılımla ilgili konulardır. Onun için biz emniyetli programlama geliştirme eğitimleri almaktan başlayarak farkındalığımızı artırıyoruz. Eğitim ajandasında SQL, Injection Web Programming gibi konular var. Bu tip jenerik eğitimlerin aviyonik alanına uyarlanması çok ciddi bir ihtiyaç.

İlave olarak şunları da yapmalıyız: Normal çalışma koşullarında 1500, 429 gibi pek çok askeri veri yolu protokolü var. Bunların kapasitesi de belli. Sizin çalışmanızın, uygulamanızın normal şartlarda çalıştığında ne kadar network, veri yükü gerektirdiği de belli. Sisteme önlemleri koymanız lazım. Benim bir saldırıya uğradığımı anlayıp, daha düşük modda çalışabilir model geliştirecek şekilde önlemler almam gerekiyor. Örneğin, "Login olmak yetmez, ben bilgisayarı

açtığımda açılan imajım, gerçekten de yüklediğim imaj mı, bire bir aynı mı? Bir tane mouse taktım, herhangi bir mouse olması yetmiyor, benim mouse'um mu? Hem kripto hem identification yapmalıyım. Ben uygulamamı açtım, farklı emniyet ve güvenlik seviyesindeki uygulamaların birbirini etkilemediğine emin olacak şekilde yazılımları geliştirmem gerekiyor" gibi pek çok emniyet ve güvenlik kritik yazılımı şu an geliştirmiş olmamız gerekiyor.

Ahmet Gökhan YALÇIN
Yapı Kredi Teknoloji Bilgi Sistemleri Güvenlik Yönetimi
Genel Müdür Yardımcısı

ULUSAL TEHDİT İSTİHBARAT AĞI OLUŞTURMAMIZ GEREKİYOR

Siber güvenlik konusunda ulusal çapta farkındalık yaratmamız ve ulusal tehdit istihbarat ağı oluşturmamız gerekiyor. Sektör bağımsız olarak ülkemizdeki kamu ve özel bütün kurumları etkileyen herhangi bir saldırının istihbaratının, ülke çapında güvenli bir şekilde paylaşılacağı bir ortam oluşturulması ve paylaşılması gerekiyor.

Ekim 2021'de İran'da benzin dağıtım sisteminde meydana gelen teknik arıza sonucu benzinliklerin önünde uzun kuyruklar oluşurken bunun siber saldırı kaynaklı olduğu Yüksek Ulusal Güvenlik Konseyi tarafından da teyit edilmişti. Bu ve benzeri olaylar bizi şuraya vardırıyor: Siber vakalar artık sadece bizim dijital dünyamızı, verilerimizi, veri güvenliğimizi etkileyen bir konu olmanın ötesine geçti ve siber saldırılar insanların fiziki hayatlarında ciddi etkiler yaratan bir noktaya ulaştı. İran'da yaşanan vaka da bunu destekliyor. Yine 2021'in Temmuz ayında İran'da bir demiryoluna yapılan siber saldırıda insanların demiryolu seyahatleri etkilenmişti. Mayıs 2021'de ABD'nin Colonial boru hattında yaşanan bir fidye zararlısı konusu vardı. Bu nedenle Doğu Yakası'nda uzun süre insanlara petrol verilemedi ve petrol fiyatları dahi bundan etkilendi. İsrail'in su dağıtım sistemine de benzer bir saldırı oldu. ABD'de bu saldırının Rusya kaynaklı olduğu söylendi. Şirket burada her ne kadar fidyeyi saldırganlara verse de, o fidyenin çözülmesi için bile birkaç gün geçti. Yani hızlı bir şekilde geri getiremediler. O şifreyi de çözemediler, orada da bir vakit kaybı oldu. 2021'in Eylül ayında ilk defa siber saldırı kaynaklı bir insan hayatının kaybedilmesi vakası yaşandı. Acil durumda olan bir kadın Almanya'da en yakın hastaneye yetiştirilmek istendi. Ancak o hastanede bir fidye zararlısından -ransomware- dolayı acil ünitesinin kapalı kalması nedeniyle daha uzaktaki bir hastaneye götürülmek zorunda kaldı ve bir saatlik zaman kaybı nedeniyle hasta yolda vefat etti. Bu durum siber saldırı kaynaklı ilk ölüm olarak kayıtlara geçti.

Özetle, siber saldırılar artık sadece kurumları etkileyen ya da dijitalde kalan bir durumda değil. Bunun yanında, hedefli, sofistike ve kompleks diye tabir ettiğimiz siber vakalar oluyor ve genel olarak APT grupları dediğimiz siber saldırgan grupları tarafından icra ediliyor. Ayrıca bu tip saldırıları yapmanın maliyeti çok yüksek. Ekipler hâlinde çalıştıkları için, doğru araçları temin etmek, bunları yazmak, bunları temin etmek maliyetli olduğundan genelde APT gruplarının devlet destekli gruplar olduğunu da görüyoruz. Bu da işin gerçekten devlet seviyesinde bir siber savaş noktasına gittiğini gösteren faktörlerden biri.

Bu saldırıların kaynağını tespit etmek için yapılabilecek birkaç şey var. Örneğin uzmanlar, İran'da yaşanan benzin vakası ile, yine Temmuz'da yaşanan demiryolu vakasını birbiriyle ilişkilendiriyor ve benzer saldırgan grubunun benzer motivasyonla yaptığını söylüyorlar. Biz de şunu görüyoruz: Bu saldırgan grupları daha önceki saldırılarda işe yaramış teknik ve araçları tekrar kullanma eğiliminde oluyorlar. Bu sebeple biz daha önce yaşanmış vakalara, belirli saldırı araçlarına ya da atak göstergelerine bakarak bir saldırının hangi gruplardan ya da hangi ülkeden gelebildiğini az çok tahmin edebiliyoruz. Bunu destekleyecek bir büyük veri de OSINT dediğimiz açık kaynak kodlu istihbarat verisi. Bu veri temelde genel kullanıma açık, aksiyon alınabilir bir istihbarat verisi. Açık kaynak kodlu verilerin içinde; meta data'lar, sosyal medya verileri, arama motorlarından gelen veriler, daha önceki veri sızıntısında ifşa olmuş verilerin kullanımı gibi birçok kaynak var.

Biz kurumlar ve ülke olarak bu tip verileri kullanarak saldırganların araçlarını tespit edebiliriz. Hatta APT grupları ya da saldırganların, bazen atağın ilk giriş noktası olarak kullandıkları oltalama saldırılarını, daha önce başka yerde kullandıkları domain ve IP adreslerini aynen kullanarak yaptığını da görüyoruz. Bu sebeple, bütün bu açık kaynak kodlu istihbarat verisinden faydalanarak, geçmiş vakaları da tarayarak hâlihazırda güncel olan vakaların kimler tarafından yapıldığı kısmen eşleştirilebilir. Kurumlar olarak, ücretli ücretsiz bütün bu kaynakları kullanmamız lazım. Ama ben -bunu sektör bağımsız söylüyorum- ülkemize özel istihbarat verisini ülke çapında paylaşabileceğimiz ve aktif olarak sistemlerimizde kullanabileceğimiz bir yapının eksik olduğunu düşünüyorum. Örneğin, biz özel bir bankayız ama ülke dışından birileri bize bir saldırı yaptığında, bakıyoruz ki üç beş bankaya aynı anda yapıyorlar. Yani Türkiye'de bankacılık sektörünü hedef alıp zafiyet buldukları üzerinden ilerliyorlar. Belki ilk bende başlıyor. Ben engelliyorum ama benden sonra üç dört tane daha banka kurban olabilir. Hem tespit sistemlerimizde hem dönmeli sistemlerimizde, saldırıları anlık işleyebildiğimiz böyle bir platformun, ülke çapında sektör bağımsız bir şekilde oluşturulması ve bu platformda hızlıca o istihbaratı paylaşabilmemiz gerekiyor.

Bir de saldırganların her attack chain'indeki hareketlerini, taktik ve tekniklerini temelde birbirine eşleştiren bir matris gibi düşünebileceğimiz MITRE ATT&CK framework var. Bu matris üzerinden belirli devlet destekli saldırganların temelde hangi hareketleri, hangi teknik ve taktikleri kullandığını izleyerek çok daha nokta atış tespitler yapmak mümkün. Bizim genelde yaşadığımız siber saldırı olaylarında ya da içeride kullandığımız yerli ürünlerde ya da diğer yabancı ticari ürünlerde bu attack framework'ünü eşleştirmeyi, hem CM gibi tespit sistemlerinde hem de bilfiil önleme yapan diğer analitik sistemlerde mutlaka yapmamız lazım. Temel olarak MITRE ATT&CK dediğimiz matriste saldırganların hangi adımları hangi sırayla

izlediklerine dair bir eşleştirme yapabilirsek, kimler tarafından saldırıya maruz kaldığımızı tespit etmemizin bir yolu daha olmuş olur.

Siber Olayların Tanımlanması

Finansal servislerle bankacılık sektörü, uzun yıllardır siber saldırganların hedefindeki öncelikli sektörler arasında yer alıyor. Bunun bir sebebi doğrudan finansal gelir elde etmek umudu ama son zamanlarda finans kurumlarından siber olay bağlantısı olan ya da olmayan farklı vakalar da duyuyoruz. Artık bir bankanın mobil uygulamasının veya herhangi bir servisinin kısa süreli de olsa hizmet verememesi itibari anlamda büyük bir sorun teşkil ediyor ve yarattığı sansasyon da çok büyük oluyor. Sadece bankalar için de geçerli değil. Online hizmet veren tüm kurumlar için geçerli olan bu faktör, siber saldırganların iştahını biraz daha kabartıyor. Önümüzdeki dönemde finans sektörünün aynı şekilde yine saldırganların öncelikli hedeflerinden biri olmaya devam edeceğini öngörüyorum.

Aktif Veri Merkezlerinin İşlerliği Sağlanmalı

Siber olay ve siber saldırı kavramları birbiriyle aynı olmayan kavramlar. Siber saldırıyı, siber olayların bir alt başlığı olarak değerlendirebiliriz. Siber saldırı sebepli olmayan siber vakalar genelde sistemlerdeki hatalar ya da kullanıcıların art niyetli, sehven veya yetkileri dışında yaptıkları hareketler olabiliyor. Kurumlar olarak buradaki sistem hatalarını minimuma indirmek için neler yapılabilir diye baktığımızda, öncelikle kurum içerisinde doğru bir değişiklik yönetim süreci tasarlamak gerekiyor. Bu değişiklik sürecinin -bir konfigürasyon

değişikliği olabilir, bir sistem update'i olabilir- gerçekten geri dönüş planlarının ve testlerinin doğru bir şekilde yapıldığının teyidi üzerine işletilmesi lazım. İkincisi, özellikle bankalardaki Olağanüstü Durum Merkezlerinin (ODM) de gerçekten doğru çalıştığından emin olmak lazım. Genelde kurumlar nispeten çok daha küçük ölçekte ODM kuruyorlar ve bunlar gerçek bir felaket senaryosunda erişilemez oluyor. ODM, yedeklilik sağlıyor. Örneğin İstanbul'da bizim ana veri merkezlerimiz var ama Ankara'da da bankanın ODM'si var. Ankara'daki ODM; İstanbul'da herhangi bir felaket olması ve oradaki veri merkezinin çalışamaması senaryosunda, uygulamalarımızı müşterilerimize hizmet verir hâle getirmek için yaptığımız bir çalışma. Bunun regülasyon olarak da bir zorunluluğu var ama bir yandan iş sürekliliği açısından da kritik. Fakat görüyoruz ki çok büyük yapılar kurguladığımız için ODM'lerimizde benzer yapıları kurgulamak bütçesel olarak da yapı olarak da maliyetli. Sektör olarak da genel olarak da kritik altyapılar için o noktaya biraz daha çalışmamız lazım. Aktif veri merkezlerinin gerçekten işlerliğini sağlamak gerekiyor. ODM'lerin sadece test yapmaktan öteye geçmesi lazım.

Ayrıca biraz daha mikro servis mimarileri ve modüler uygulama geliştirmeden bahsediyoruz. Biz de bankacılık uygulamalarımızı özel bulut altyapılarında, bu tip mimarilerde geliştirmeye başladık. Burada zamanla uygulamaların daha modüler ve bölünebilir hâle geleceği ve herhangi bir sorunun tüm uygulamayı değil de mobil uygulamadaki sadece para transferi fonksiyonunu etkileyeceği bir noktaya gideceğimizi düşünüyoruz. O yüzden mikro servis ve modüler uygulama geliştirmeyi önemli buluyorum.

Bir de işin kullanıcı bacağı var. Kullanıcı kaynaklı siber olay olmasının önüne geçmek için, birincisi görevler ayrılığı prensibini uygulamamız lazım. Yani bir talebi değerlendiren ve onaylayan kişiyle, yapan kişinin farklı olması lazım. İkincisi de minimum yetki prensibi. Yani herhangi bir çalışanımıza gerçekten minimum seviyede, işini yapacak kadar yetki vermek lazım. Böylelikle kullanıcı hatasından oluşabilecek sistem arızalarını da minimum seviyeye indirmiş oluyoruz.

Ulusal Çapta Bilgi Güvenliği Farkındalığı Sağlanmalı

İşin siber saldırı boyutunda neler gördüğümüzden bahsetmek gerekirse, özellikle pandemiyle birlikte bankacılık sektöründe oltalama saldırıları, fidye zararlıları ve DDOS saldırılarında, hem saldırı sayılarında hem de saldırıların etkilerinin büyüklüğü anlamında muazzam bir artış görüyoruz. Oltalama tarafında kurumlar olarak biz gerekli e-posta güvenlik sistemlerini kurguladık, bunu send box'larla entegre ettik. Bu zararlıların uç noktadaki cihaza kadar gelmesi durumunda da teknik anlamda gerekli önlemleri alıyoruz ama iş hep insana kalıyor. Milyon dolarlık yatırımlar yapsak da bir çalışanımızın bir linke tıklaması her şeyi bitirebiliyor. Bunun için farkındalık tarafına dikkat çekmek istiyorum. Biz kurum olarak çalışanlarımızın bilgi güvenliği farkındalığının artırılması için çok sayıda çalışma yapıyoruz. Bültenler yayınlıyoruz, testler, tatbikatlar yapıyoruz, eğitimler veriyoruz, yarışmalar düzenliyoruz. Fakat bunu ulusal çapta bir noktaya getirmemiz lazım. Biz kurum olarak çalışanlarımıza yapıyoruz ama ulusal çapta her vatandaşımızın bilgi güvenliği farkındalığını artıracak şekilde ulusal hareket başlatmamız gerekiyor. Dolandırıcılık vakalarının da bu sayede önüne geçebileceğimizi düşünüyorum.

> "Kullanıcı kaynaklı siber olayların önüne geçmek için, birincisi görevler ayrılığı prensibini uygulamamız lazım. Yani bir talebi değerlendiren ve onaylayan kişiyle, yapan kişinin farklı olması lazım. İkincisi de minimum yetki prensibi. Yani herhangi bir çalışanımıza gerçekten minimum seviyede, işini yapacak kadar yetki vermek lazım. Böylelikle kullanıcı hatasından oluşabilecek sistem arızalarını da minimum seviyeye indirmiş oluyoruz."

Fidye zararlılarında da yine teknik önlemleri ya da başka kurumların yaşadığı bir fidye saldırısında elde ettiğimiz zararlı IP'leri istihbarattan alıp sistemlerimize koyuyor ve engelliyoruz. Ancak bence asıl yapılması gereken şudur: Böyle bir zararlıya maruz kaldığımızda üst kurum olarak sonrasına hazır mıyız? Yani bunun tatbikatına, iletişimine hazır mıyız, test etmemiz lazım. O anlamda da fidye zararlısı denetim ve değerlendirme servislerini, danışmanlık hizmetlerini de çokça görmeye başladık. Burada bir de önemli olan bizim yedeklememiz doğru mu, erişilebilir mi, gerektiğinde yedekten dönebilir miyiz, buna özellikle çalışmamız lazım.

DDOS saldırılarına gelecek olursak, biz de çok fazla sayıda DDOS saldırısına maruz kalıyoruz. Çoğunluğu yurtdışı kaynaklı olmak üzere bu saldırılar bazen çok ciddi boyutlara ulaşıyor. Burada üç katmanlı bir koruma sisteminin faydalı olacağını düşünüyorum. Üç katmanlı bir yapının artık günümüzde mecburiyet ve zorunluluk olduğunu görebiliyoruz:

- Kendi veri merkezlerimizde lokal DDOS koruma çözümleri,
- Daha yüksek seviyeli saldırılar için ISP seviyesinde aldığımız korumalar,
- Yurtdışından gelecek saldırıları kaynağında kesmek için global seviyede, sadece yurtdışı tarafında bir koruma sağlayan global DDOS.

Bir yandan da bazı DDOS saldırılarının arasında, yurtiçindeki zombi makinelerin sıklıkla kullanıldığını görüyorum. Bu sebeple ulusal çapta hakikaten zombi bilgisayarlar, zombi IoT cihazları olup olmadığının sürekli taranması, tespit edilip giderilmesi ve ülkemizin bu saldırılara alet olmasının önüne geçmemiz lazım.

Siber Hijyen

Bankamızda çok fazla ürün yönetiyor, çok fazla saldırı karşılıyor ve alarm tespit ediyoruz. Ama bir yandan da denetim ve iş kontrol ekipleri bizim süreçlerimizde, iş yapışlarımızda eksiklik görebiliyorlar. Biz kendi bünyemizde bazı güvenlik uzmanlarımızı iç kontrol, iç denetçi rolüyle görevlendirip, denetimi beklemeden iş yapışlarımızda, süreçlerimizde, kontrollerimizde eksiklikler, iyileştirilebilecek noktalar olup olmadığına bakıp bir temizlik yapıyoruz. Ben siber hijyeni biraz da böyle yorumluyorum.

Bunlara ilave olarak, yönetim kurulu çalışanları, genel müdür, genel müdür yardımcıları gibi VIP dediğimiz bankada en üst düzeyde çalışan kişilerin güvenliğinin de çok kritik olduğunu

düşünüyorum. Çünkü bazen hedefli saldırılarda doğrudan hedef konumunda olabiliyorlar. Ya da o kişilerin e-posta hesapları, bilgisayarları ele geçirildiğinde kurum için daha büyük bir risk oluşturabiliyor. O açıdan da biz özellikle bu seviyedeki kişiler için bir VIP güvenliği çalışması da yapıyoruz. Kurumlar, özellikle de bankalar özelinde bu konuya dikkat çekilmesi gerekiyor.

Veri Güvenliği Uygulamaları

Finans sektörü olarak ciddi regülasyonlara tabiyiz. Hem BDDK'nin 2021'de çıkan bankaların elektronik bankacılık hizmetleri hakkındaki yönetmeliği hem de Kişisel Verilerin Korunması Kanunu sebebiyle veri güvenliği çok önemli bir noktaya geldi. Veri ve veri güvenliği ihlallerinde artık maddi cezalar dahil olmak üzere çok ciddi yaptırımlara tabiyiz. Temelde korumaya çalıştığımız şey veri olduğu için, artık veri güvenliği siber güvenliğe eşit oldu. Bütün güvenlik süreçlerimiz ve programlarımız veri güvenliği anlamına geldi. Korumamız gereken çok farklı veriler var. Kişisel veriler, ticari bilgilerimiz, bankacılık için bakarsak banka sırları var. Farklı tipte verileri farklı şekilde korumamız lazım. İhlal olduğunda hepsi için çok farklı yaptırımlar var. Veri yönetişim kavramıyla veri güvenliği kavramını önce birbirinden ayırmak gerekiyor. Veri güvenliği toplam veri yönetişimi kuramının bir alt başlığı olabilir. O yüzden bir kurumun doğru bir veri yönetişim stratejisi yoksa üstüne bir veri güvenliği programı inşa etmek mümkün değil. Önce bizim yapısal ve yapısal olmayan ortamlarda ne gibi verilerimizin olduğunun resmini doğru çıkarmamız ve bu veriyi doğru yönetmemiz lazım. Programı tamamladıktan sonra verilerimizi doğru bir şekilde sınıflandırarak o noktada veri güvenliği aksiyonlarımız başlıyor. Sınıflandırılan verinin tipine ve sınıfına göre de farklı güvenlik aksiyonları almak durumundayız.

Veri güvenliğinde başımızı en fazla ağrıtabilecek iki kritik nokta var. Biri, çalışanlarımızın yetkisi dışında verilere erişimi ve aynı zamanda yetkisi dahilinde anormal erişim yapmaları. Bir banka çalışanı yetkisi dahilinde kredi sorgulaması yapıyor ama normalde işi gereği günde 10 tane sorgulayabilecekken bir gün 1.000 tane sorgulamışsa bunu inceleyebiliyoruz. Belki de birilerine satıyor. Yetki dahilindeki hareketlerde dahi bir anomali tespiti yapmak için, içeride izleme ve alarm sistemi kurduk. Sadece yetkisiz değil yetkili kişiler de bunu suistimal edebiliyor.

Tabii bu işlerin hepsinde çok ciddi etik süreçler, disiplin komite süreçleri de var. Banka içinde bu tip anormal davranışlar yapan kişiler hakkında kınamadan işten çıkarmaya kadar aksiyonlarımız var. Bankacılıkta bu zaten olmazsa olmazlardan biridir çünkü büyük bankalarda 15, 20 bin kişi çalışıyor. Kötü niyetli olabileceklerin oranı binde bir bile olsa ciddi bir sayı çıkıyor. Dışarıdan gelecek saldırılara önem verdiğimiz kadar içeriden de bu suistimalleri yakınen takip ediyoruz. Bu gizli yürüttüğümüz bir çalışma da değil çünkü amacımız kişilerin bu tip anormal davranışların doğru olmadığını bilmesi. Banka için de kendileri için de farklı sonuçları olabilir.

Bunun yanında bir de kurum dışına çıkan veri konusu kritik. Gerçekten hassas verilerin kurum dışına çıkmaması, çıkıyorsa da çok spesifik kişilerle paylaşılabilmesi noktasında kontrollerimiz var. Bu kontroller arasında veri sızıntısı önleme kontrolleri, DLP kontrolleri ve etiketleme, e-postaların etiketlenmesi, ofis dokümanlarının etiketlenmesi, hem sistem kurallarıyla otomatik olarak hem de kullanıcının kararına bırakılarak etiketlenmesi gibi uygulamalar var.

"Dışarıya olan bağımlılığın ve üçüncü parti firmalarla olan işbirliklerimizin artması günümüzde en kritik konular arasında yer alıyor. O yüzden bu entegrasyonlarla ne tip veriler paylaştığımıza, bunlar için ne gibi önlemler aldığımıza dikkat etmemiz gerekecek."

Ona göre de bizim engelleyici ya da alarm üretici kurallarımız var. Örneğin, belirli tipte dokümanlar ya da veriler dışarıyla paylaşılamaz, USB ile çıkarılamaz, print edilemez, e-posta ile gönderilemez. Bir de kurum dışına paylaşımlar bankacılık açısından çok daha önemli.

Açık Bankacılığın Getirdiği İlave Güvenlik Problemleri

Yakın zamanda dijital bankacılıkla ilgili bir taslak yönetmelik çıktı. BDDK geçen seneki yönetmelikte açık bankacılığa bir paragraf açtı. Açık bankacılık, dijital bankacılık kapsamında, bir banka artık birçok teknoloji firmasıyla, başka bankalarla, FinTech dediğimiz şirketlerle entegre olmaya başlayacak. Hatta banka uygulamaları "Super App" dediğimiz noktaya doğru gidecek. Bu da şunu doğuruyor: Daha önce bankalar belki kamu kurumlarıyla entegreydi ve kredi sorgulamaları vs. yapıyorlardı ama şimdi sizin mobil bankacılık uygulamanız bile çok çeşitli özel kurumlarla yeri geldiğinde entegre olabiliyor. O durumda uzay çok genişlediği için hangi kurumlarla nasıl veri paylaşılacağının, paylaşımın limitlerinin, oradaki tespit mekanizmalarının doğru bir şekilde ayarlanması gerekiyor.

Önümüzdeki dönemlerde fiziksel bir yansıması olmayan, sadece dijitalde yaşayan ve diğer bütün dijital kurumlarla bire bir veri paylaşımında bulunan bankacılık modelleri göreceğiz. O açıdan bu üçüncü parti firmaların devreye girmesiyle riskler gittikçe daha da artacak. Ben kendimi ne kadar korusam da arka planda anlaştığım bir kurye firmasının kendi ortamına dikkat etmemesi, limitli bile olsa benim basit bir entegrasyonum nedeniyle onun üzerinden bana bir sorgu yapılabilmesini mümkün kılıyor. Dışarıya olan bağımlılığın ve üçüncü parti firmalarla olan işbirliklerimizin artması günümüzde en kritik konular arasında yer alıyor. O yüzden bu entegrasyonlarla ne tip veriler paylaştığımıza, bunlar için ne gibi önlemler aldığımıza dikkat etmemiz gerekecek.

Sonuç olarak, kamu kurumlarıyla özel sektör, siber güvenlik anlamında daha yakın çalışmalıdır. Şu anda hiçbir çalışma içinde değiller. Tecrübelerini birbirlerine aktaracakları daha çok ortam yaratılması gerekiyor. Daha çok tecrübe paylaşımı yapmamız lazım çünkü bizler de yüzlerce siber güvenlik uzmanıyla farklı farklı başlıklarda çok kritik projeleri hayata geçiriyoruz. Belki ben bir tanesini ülkede ilk defa yapıyorum. Başka bir özel kurum, başka bir niş projeyi belki kendi içinde çıkarıyor ama neden bunun kamuya da faydası olmasın? Bunu eksiklik olarak görüyorum. Hatta devletimiz siber güvenlik stratejisinde bize de söz verilebilir. Siber taarruz planımız var mı bilmiyorum, varsa belki bizden katma değer verecek arkadaşlar olabilir. Çünkü kamuda da bizde de uzman açığı var. Kamu-özel sektör ayrımı yapmadan daha fazla çalışarak ülkeye fayda sağlayabiliriz.

Mahmut KÜÇÜK
Türk Telekom Siber Güvenlik Direktörü

SEKTÖREL OLARAK RİSK TABANLI BİR BAKIŞ AÇISI GEREKLİ

Siber güvenlik konusunda sektörel olarak bir risk kriteri koymamız gerekiyor. Hangi sektörler bilgi güvenliği anlamında riskli? Her sektörün kendine özgü riskleri var, o risklere özgü de alınması gereken önlemler var. Belli regülasyonlar çerçevesinde, o önlemleri almayan işletmelere, ruhsat iptaline kadar varan cezalar konulması gerekiyor.

Haberleşme güvenliği konusunda çok geniş bir kapsamdan bahsetmek gerekiyor. Hayatın her alanında cep telefonu ve internet geniş kitleler arasında yaygın olarak kullanıldığı için bu alanda donanım güvenliğinden donanımın üzerinde çalışan yazılımlara, B2B ve B2C servislere kadar birçok servisin güvenliği konuya dahil oluyor. Buna istinaden ilk olarak sırasıyla cihaz güvenliği, haberleşme güvenliği ve şebeke güvenliğine değineceğim.

Cihaz güvenliği dediğimizde, üreticilerin birçoğunun kullandığı ortak işletim sistemleri var. Geçmiş yıllarda Çin-ABD gerilimi sonrasında Çin kendi işletim sistemlerini geliştirmeye doğru ilerledi ve Çinli üreticiler bir yol haritası izledi. Buradaki teknolojilerin paylaşılmaması, birtakım özelliklerin kullandırılmaması, bunun rekabette birbirlerine teknolojik yaptırım olarak kullanılabildiğinin çeşitli örneklerden biri. Ülkemizde ve dünyada yaygın olarak kullanılan cep telefonuyla handset dediğimiz terminallerin yerli üretilmesi konusunda geçmişte yaşanan tecrübeler var. Maalesef o dönemde desteklense başarılı olma ihtimali çok yüksek olan bir ASELSAN 1919 varken, onun devam ettirilmemesi nedeniyle ülkemizde yerli cep telefonu üretim kabiliyetimizi, yerli ve milli savunma sanayimizi geliştirdiğimiz gibi geliştirememişiz. O dönemde üretim kabiliyeti kazanabilsek çok farklı bir noktada olabilirdik. Şimdi tekrar bu alanda çalışan özel sektör girişimleri var. Zamanında telekom operatörleri bu konuda fason üretim şeklinde bazı cihazları ürettirmeye çalıştı ancak bu tür girişimler de yerli ve milli üretime katkı sağlama amacından uzak faaliyetlerdi.

Cihaz üretimi teknolojik olarak çok hızlı ilerliyor. Dünyadaki çip krizinin temelinde yine benzer şeyler var. Pandemide bilgisayar, tablet, cep telefonu taleplerinin çok ciddi anlamda artması, üretimin bu alana kayması nedeniyle çip krizi yaşanıyor. Çip üretimi konusunda ciddi bir eksikliğimiz var. Donanım tarafını bir kenara koyacak olursak, mevcut donanımları, mevcut çip setlerini kullanıyoruz. Üzerindeki yazılım ve işletim sistemi de bizim değil. Yani bir cep telefonu için mobil işletim sistemi olarak bir Pardus mobil var mı veya bu konu üzerinde başlamış bir proje var mı, bilmiyorum. Eğer güvenlikten bahsediyorsak; en azından farklı cihazları destekleyen, her donanımla çalışacak mobil yazılım konusunda bir çalışma yapılabilir. Üzerindeki uygulamalara daha sonra başlayabileceğiz. Üzerindeki uygulamaların birçoğu kendi SDK, API ve geliştirme platformunun sağladığı imkânlarla geliştiriliyor. Kümelerden örnek verecek olursak, yazılım güvenlik ve test kalitesi dediğimiz konu fonksiyonel kümeyse, saldırganın dünyası o küme dışındaki tüm evrensel küme. Yazılım geliştirici dünyasında öncelikle fonksiyonları sağlamaya yönelik bir odak var. Saldırgan ise bütün vektör ve faktörlerle o kümeye bir şey sokmaya, enjekte etmeye ya da o kümeden bir şey çıkarmaya ya da kümeyi tamamen işlevsiz kılmaya çalışıyor.

Bu açıdan baktığımızda, cihazın üzerinde çalışan işletim sistemi ve fonksiyonlarının dışındaki uygulamaların (bankacılık uygulamaları, mobil operatörlerin online işlemler uygulamaları, e-devlet uygulamaları, birçok vatandaş ya da kurumun kendi işleri için kullandığı uygulamalar, pandemide uzaktan bağlantı amaçlı şirketlerin kendi erişimlerini sağladığı altyapı ve uygulamalar) hepsinin güvenliğine baktığımızda, kontrol alanımızın çok az olduğunu görüyoruz. Ülke olarak üretici tarafta olmanın verdiği gücü kullanamadığımız için bu tarafta ciddi çalışmalar yapılması gerektiğini düşünüyorum. Ancak çok geciktiğimiz yönündeki yaklaşımlar doğru değil. Ne zaman, nereden başlarsanız hiçbir zaman geç değildir. Bu anlamda irade konulması lazım.

Burada iletişim protokolleri konusuna da kısaca değinmek gerekiyor. Tabii ki cep telefonu dediğimizde eskiden sadece SES, SMS ve GPRS vardı. GPRS çok sonra çıktı. Cep telefonlarının 2G, 3G jenerasyonlarının kullandığı SS7 protokollerinin kendi içerdiği birtakım zafiyetler ve normal internet IP protokollerinin de benzer zafiyetler içermesi nedeniyle hem kaynağın tespiti hem haberleşmenin gizliliği tehdit altındaydı. Cep telefonları, GPS lokasyon bilgisi gibi birtakım verilerin yanı sıra, akıllı cihazlardaki yeni özelliklerle günümüzde nabzınızdan attığınız adıma kadar birçok veriyi tutan bir alete dönüştü. Dolayısıyla burada sadece ses, SMS, veri ve haberleşme güvenliğinden bahsetmediğimizi de bir kenara not edelim. Şebeke üzerinde oluşabilecek risk ve tehditler gün geçtikçe artıyor. Bunlara karşı da gerekli önlemleri şebeke seviyesinde almak mümkün ve bu önlemler alınıyor.

Tabii 2G ve 3G'deki SS7 protokolüne benzer, 4G'deki diameter protokolünde de bu tip zafiyetler bulunuyor. Sinyalleşme dediğimiz güvenliğin kendisidir. Kontrol katmanında, kullanıcı katmanında bütün verilerin korunmasına yönelik baktığınız zaman yüzde 100 uçtan uca güvenlik diye bir şey söz konusu değil. Her ne kadar şebekede encrypted da taşısanız, her ne kadar cihazların üzerinde birçok güvenli yazılım da kullansanız, çok değişik saldırı vektörleri var. Cihazın kendi içinde silent çalışan birtakım teknolojilerden kaynaklı, Silent SMS gibi yöntemler kullanılarak cihazdan bilgi toplamadan, haberleşme sırasında verinin protokol olarak ele geçirilmesine, o verinin sızdırılmasına kadar çeşitli riskler söz konusu.

Bütün bunlara karşı neler yapılıyor? Her güvenlik biriminin yaptığı gibi, risk ve tehditleri öngörebildiğiniz, bildiğiniz ve çözüm geliştirebildiğiniz kadar yapabiliyorsunuz. Teknolojiyi geliştiren üreticilerin yetkinlikleriyle sınırlısınız. Örneğin bir JAVA'nın açığından bahsediyorsak, JAVA'yı geliştirenlerle beraber buna cevap verme söz konusu. Ya da bir işletim sistemi açığından bahsediyorsak, işletim sistemi geliştirenin önce bunun yamasını geliştirmesi lazım. İşin devlet destekli şekilde, haberleşmenin kendi devletlerinin çıkarları amaçlı kullanılması gündeme geldiği zaman risk tehdit evreni de bir anda büyüyor. O yüzden üretim, üretim, üretim diyoruz. Kendi donanımımızı, yazılımımızı, işletim sistemimizi, güvenlik ürünlerimizi ve mobil uygulamalarımızı üretebilme hedefiyle ilerlememiz lazım. Kullandığımız bütün erişim araçlarında, elektronik ekipmanlarda bunları sağlamamız gerekiyor.

Sosyal Medya Dolandırıcılığı

Sosyal medya dolandırıcılığı ya da bilişim altyapıları kullanılarak yapılan dolandırıcılığın uzun bir gelişim evrimi var. Bunlara biz genel anlamda oltalama ya da sosyal mühendislik saldırıları diyoruz. Elektronik ortamlar kullanılarak yapılan suçların tespiti, hukukun birinci isteri. Ama artık o kadar iç içe geçmiş teknolojiler ve o kadar farklı altyapılar var ki suçlunun kendini gizleyebilmesi için globalde ücretsiz açık servisler ve o servisler kullanılarak yapılabilecek yöntemler de var. O nedenle tespiti zor bir konu. Oltalama ya da dolandırıcılık dediğimiz işlemlerin sosyal medya tarafından uygulanmasında en büyük sıkıntılardan biri, birtakım bilgilerin paylaşılması. ISP'lerin elinde belli şeyler var ama bunlar yeterli olmuyor. Çünkü onların altyapıları birbiriyle iç içe olduğu için, size bir dolandırıcıyı nokta atışı tespit ederek gösteremediği durumlar da çıkabiliyor. Bu tür durumların da önüne geçebilmek için kendi sosyal medya platformlarımızın yaygınlaştırılması önem taşıyor. Sosyal medya yoluyla yapılan suçlar şahısların sadece birbirine karşı işlediği suçlardan ibaret değil; sosyal medya şirketlerinin de suç işlediklerini görüyoruz. Cambridge Analytica tarzı olayları hatırlıyoruz.

Bunlar çıkıp ifşa olanlar; ifşa olmayanların boyutunu da buzdağı ölçeğinde düşünmek lazım. Bunların da şirketlerin ya da şirketlerin sattığı verileri kullanan değişik güç gruplarının, organizasyonların kendi kamu yapılarının kullandığı birtakım veriler olduğunu düşünüyorum -ki zaten sosyal medya dediğimiz olgu hayatımıza ücretsiz bir servis olarak 11 Eylül 2001sonrasında sokulmuştur.

İnsan Zihni de Hack'lenir

Sosyal medyanın arka tarafta getirdiği sorunlardan biri, sadece paraya yönelik fraud dolandırıcılığı vs. değil; zihinsel manipülasyondur. Biz hep sistemlerin hacking'inden bahsediyoruz, oysa insan zihni de hack'lenir. Sosyal medyanın insan zihnini hack'lemek için kullanılan bir platform olduğu gerçeğiyle hepimiz karşı karşıyayız. Çoluğumuz çocuğumuz orada gördüklerini doğru kabul edip daha sonra gelip anne babaya itiraz ederek, sizin 40 yıldır bildiğiniz doğruya, izlediği bir iki dakikalık videoyu göstererek itiraz ediyor. Oysa o videoda 50 doğrunun arasında bir yanlış sokuşturup onu da insanların zihnine doğru olarak yerleştirmeleri, yani bir nevi fikri injection yöntemiyle zihne yerleştirme söz konusu. Bunlara sadece teknolojik boyutta değil; sosyolog ve psikologlar dahil ne kadar akademisyenimiz varsa, bilinçli teknoloji kullanımı eğitimleriyle karşı durmamız gerekiyor.

Arka tarafta içeriğin gizliliği, haberleşmenin gizliliği boyutuyla ilgili bir sıkıntı var. Mesela hepimize, "Şunu tıklayın indirim kazanın" tarzı SMS veya mesajlar geliyor. O mesaj bir milyon kişiye gittiyse minimum yüzde 10-15'i buna gözü kapalı tıklıyor. Ya oradan zararlı indirerek ya da oraya birtakım sosyal medya, bankacılık veya uygulama şifrelerini girerek verilerini kaptırma söz konusu. Peki bunlarla nasıl mücadele edilmeli? Bunlarla mücadele ederken hukuk nerede duruyor? Bu tarz SMS'ler mesajları haberleşme olarak mı yorumluyor? Yoksa bunu haberleşme değil bir SPAM saldırısı olarak mı değerlendiriyor? Çünkü haberleşmenin gizliliği ayrı, dolandırıcılık amacıyla gönderilen mesajların tespit edilip engellenmesi ayrı bir konu. Ben bunların farklı değerlendirilmesi gerektiğini düşünüyorum. Bizim vatandaşımız, dolandırıcılara bilgisinin yanı sıra, tüm parasını da kaybediyor, bu yüzden aileler yıkılıyor ya da "Terör örgütüne para gönderdiniz" diyerek tehdit ediliyor. İnsanlar çok farklı dramlar yaşıyor. Bunları engellemek için belli önlemlerin alınması lazım. Mesela neden aynı mesaj bir milyon kişiye atılsın? Bu bir haberleşme değil artık, bir yayın. Bunu engelleyebilmenin yol ve yöntemlerini oluşturabilmemiz lazım. Hukukun da bu noktada ön açıyor olması lazım. Veya belli mecralarda içeriğinde terör ya da birtakım suçların propagandası olan birtakım reklamlar yapılıyor. Bunlarla ilgili alınacak önlemler konusunda toplumun sağlığını ve hukukunu koruyacak şekilde daha özelde birtakım geliştirmeler ve hukuksal düzenlemeler yapılması gerektiğini, bu noktada da kurumların buraya el atması gerektiğini düşünüyorum.

Siber güvenlik farkındalığı dediğiniz zaman, hedef kitlenin kim olduğunu iyi tarif etmek gerekiyor. Bahsettiğimiz farkındalık vatandaşın farkındalığıysa kamu spotlarıyla kitlelerin eğitim seviyesinin yukarıya çıkarılması gerekir.

> "Outsource yaklaşımı 90'lı yıllardan itibaren çok popüler oldu. Artık temel faaliyetler bile outsource edilmeye başlandı. Outsource edilen firmaların da alt taşeronları, onun taşeronu derken bir bakıyorsunuz -siz belki kendinizi çok güvende hissediyorsunuz ama- verileriniz ya da hizmetleriniz outsource ettiğiniz firmaların üzerinden başka birtakım risklere maruz kalabiliyor."

Her Sektörün Kendine Özgü Riskleri Var

Geniş kitleleri şartlandırırken değişik araçlar kullanılabilir. En çok kullanılması gereken mecra yine internetin ve sosyal medyanın kendisi. Burada üst seviye elit tabakanın, yöneticilerin, kamu veya özel sektör yöneticilerinin eğitiminin de ciddi anlamda gerekli olduğunu düşünüyorum. Özellikle yatırım kararı verirken siber güvenlik alanında ne kadar bütçe ve insan kaynağı ayrılıyor? Birçok firma siber güvenlik alanında personel istihdamından, altyapı yatırımına kadar çok yetersiz. Çok yakın bir zamanda ABD'nin getirdiği birtakım mücbir yaptırımlar ve belli kanunlar, kurallar konuldu. Sektörel olarak değişir değişmez, biz kendimize uyarlarız uyarlamayız ama buna bakarak siber dayanıklılığın ve duruşun güçlendirilmesi yönünde göz ardı edilen noktaların hızlıca kapatılması lazım. Örneğin kurye firmalarının elinde herhalde tüm Türkiye'nin ad soyad, TC no, telefon, iletişim bilgileri vardır. Ama hiç kimse şunu demiyor: "Kurye firması açmak için senin siber güvenlik seviyen şu olmalıdır; 1'den 10'a kadar sen top class firmasın, senin PII verisinin tamamına erişmen gerekiyor, dolayısıyla 9 ve 10'dan aşağı not alırsan senin lisansını iptale kadar cezai yaptırım uygulayabilirim, bu yönde herhangi bir aksiyon almıyorsan kapatıyorum." O kadar rahat iş yapılıyor ki sektörel olarak bir risk kriteri koymamız gerekiyor. Hangi sektörler bilgi güvenliği anlamında riskli? Sağlıkta çok ciddi kişisel veriler var. Hizmet sektörü, teknoloji sektörü, enerji sektörü, hepsinin riskleri farklı. Hepsini bir araya getirip aynı risk kriterini uygulayamazsınız. Her sektörün kendine özgü riskleri var, o risklere özgü de alınması gereken önlemler var. Belli regülasyonlar çerçevesinde, o önlemleri almayan işletmelere, ruhsat iptaline kadar varan cezalar konulması gerekiyor. Bunlar için belki süreler tanınır, yatırım yapılır, gelişimleri desteklenir.

Örneğin biz çok kısa sürede iş sağlığı ve güvenliğiyle ilgili bir kanunla yüzleştik, yakın geçmişte bir anda iş sağlığı ve güvenliği uzmanları türedi. Bilgi güvenliğiyle ilgili böyle bir odağımız var mı? Yok. İş sağlığı ve güvenliği tabii ki çok önemli ama orada oluşan algı, kamuoyu baskısı, medya desteğini hâlâ göremiyoruz. İşin magazin boyutundan artık çıkmamız lazım.

Yapılması gerekenleri sıraladığımızda en başta sektörel olarak risk tabanlı bir bakış açısı ve orada olması gereken minimum seviyenin belirlenmesi gerekiyor. Hangi seviyede bilgi güvenliği sağlandığında bu işi yapabilir? Verilerin kontrolsüz, elden ele dolaştığı bir ortamdan bahsediyoruz. Her şey dijitalleşiyor. Artık füze göndererek, uçakla bombalayarak sizin ekonominize zarar vermiyorlar. Belki ondan çok daha risksiz ve çok daha basit bir siber saldırıda çok daha fazla zarar verebiliyorlar. Karar alıcıların önüne çok kritik istihbari bilgiler konulup, o bilgiler kullanılarak ekonominize, kurumlarınıza, imajınıza -devlet imajı çok önemli- saldırılar yapılan bir dünyada yaşıyoruz. Bunun da yolu, yöntemi ve mecrası yine teknoloji.

"Türkiye'de siber güvenliğin politik olarak derlenip toparlanması, sadece operasyon merkezi olarak değil, insan kaynağı yetiştirmesi de dahil olmak üzere sorumluluğun, kamu özel sektör demeden daha üst seviye bir organizasyon tarafından ele alınması gerekiyor."

Bu alanda belli bir karne ve not olmalı. Nasıl çevre ve sürdürülebilirlik diye bir kavram hayatımıza geliyor ve uyguluyorsak, siber güvenlikle ilgili de hayatımıza bir kavramlar bütünü gelmesi ve bunu kamuoyuna iyi anlatabilmemiz lazım.

Firma Akreditasyonu Çok Önemli

Siber güvenlik anlamında önemli noktalardan biri de firma akreditasyonu. Outsource yaklaşımı 90'lı yıllardan itibaren çok popüler oldu. Artık temel faaliyetler bile outsource edilmeye başlandı. Outsource edilen firmaların da alt taşeronları, onun taşeronu derken bir bakıyorsunuz -siz belki kendinizi çok güvende hissediyorsunuz ama- verileriniz ya da hizmetleriniz outsource ettiğiniz firmaların üzerinden başka birtakım risklere maruz kalabiliyor. Bu anlamda özellikle kamuda ihaleyi kazanan firma sağlam olabilir ama onun taşere ettiğini kontrol etmiyorsunuz. O alıp ikinci taşerona verdiği zaman, örneğin çok gizli bir silah planının başka yere gitmesi, geliştirme projelerinin ya da önemli teknolojilerin başka yerlere gitmesi söz konusu olabiliyor.

Türkiye'de siber güvenliğin politik olarak derlenip toparlanması, sadece operasyon merkezi olarak değil, insan kaynağı yetiştirmesi de dahil olmak üzere sorumluluğun, kamu özel sektör demeden daha üst seviye bir organizasyon tarafından ele alınması gerekiyor. Bütünsel bir yaklaşımla eksikliklerin tamamlanması ve bir saldırı ya da problemle karşı karşıya kalındığı zaman mukavemet anlamında neler yapılacağının planlarının hazırlanması gerekiyor. Ayrıca bu alanda kamudaki kurumlar arası rekabet yerine işbirliği sağlanması gerektiğinin, kurumlar arası yetki karmaşasının ortadan kaldırılması ve güvenlik söz konusu olduğunda ortak hareket edebilme yeteneğinin sağlanması için bir üst koordinasyon sağlanması gerektiğinin altını çizmek isterim.

Av. Ceyda CİMİLLİ AKAYDIN
Türkiye Bilişim Derneği İstanbul Şubesi Yönetim Kurulu Üyesi

HUKUKÇULARLA BİLİŞİMCİLERİN ORTAK ÇALIŞMA YAPMASI GEREKİYOR

Hukukçulara yol gösterilmesi, yani ortak çalışma yapılması lazım. Çok kıymetli hukukçularımız var. Birinin onlara ceza ve kamu alanında bilişimle ilgili düzenlemeyi yönlendirebilmeleri için bilişimin ne olduğunu tane tane anlatması lazım.

Sıkça kullanılan saldırı tekniklerinden biri olan sosyal mühendisliği engellemeye yönelik yaklaşımların gerçekten efektif olup olmadığını değerlendirmek önem taşıyor. Sosyal mühendislik açısından kendimden örnek verebilirim. Biz 12 kişilik bir büroyuz. Güvenlik yazılımlarının ücretleri bir yana, 12 kişinin başına bir bilgi güvenliği müdürü atamaya kalkmam mümkün değil. Ve çoğu danışmanlık şirketi de bu durumda. Çok büyük hukuk büroları var ama icra işi ya da seri dava yapıyorlar. Danışmanın bir konuda çok uzun yıllar uzmanlaşmış birisi olması gerektiği için büyük bir danışmanlık bürosu işin mantığına ters oluyor. Zaten danışman bağımlı çalışmak istemez, ağırlıklı olarak akademiden gelir. Dolayısıyla çok küçük yerler. Ama bizde bile çok mahrem veri var. Çoğu özel veridir ama kamudan da gelebiliyor. Özellikle bilişim ve telifle ilgiliyse bolca geliyor. Geldiğinde hem sosyal mühendislik hem son kullanıcı açısından bakarsanız ne kadar korunabiliyor? Her şeyden önce fiziksel güvenlik de çok kötü bir seviyede.

Biz çok uzun süredir KVK çalışmaları da yapıyoruz. Bütün KVK çalışmalarını yüz yüze görüşerek, yani süreç analizi sonucunda yaptık. Özellikle üst seviyede kesinlikle ve kesinlikle WhatsApp çok kullanılıyor. Şirketin genel müdür sekreterinin gelen evrağın fotoğrafını genel müdürüne WhatsApp'tan çekip göndermediği bir tane şirket bulamazsınız. Şimdiye kadar 60 civarında proje yaptık, bunların arasında çok büyükler de var. Bizimkilerin içinden hiç çıkmadı. Burada sorun şu: Sosyal mühendislik konusunda eğitimimiz de yok. Benim tek şansım, bilişimcilerin arasında çok yer aldığım ve herkes bana sürekli bir şeyler anlattığı için biraz daha okuryazarlığımın gelişmiş olması.

Biz son kullanıcı, özellikle de danışmanlar olarak riske çok açığız. Ben kamunun arabulucular için özel bir bulut geliştirmesini beklerdim. Savunma teknolojisi şirketlerinin kümelenmesinin bulutu gibi, bir arabulucu bulutu olsaydı keşke de orayı kullansaydık. Dolayısıyla yerli ve milli doğru ama yerlinin ötesinde milli olması gerekiyor. Ben avukatım ve benim ofisimde gerçekten mahrem veri var, dolayısıyla bunları yedeklemek zorundayım. İçeriye yatırım yapayım, sunucu kurayım desem güvenliğini sağlayamam. Kendi sunucumun yangınından tutun hırsızlığına kadar ne fiziksel güvenliğini sağlayabilirim ne de diğer güvenliğini. Öyle bir yatırım yapamam. Dolayısıyla bulut kullanacağım, başka şansım yok. Ne kalıyor; Amazon'la Google arasında gidip geliyorum. Yerlileri düşünecek olursak, Barikat'a gidip benim güvenliğimi sağlayın desem, ben de InterProbe'un da Innova'nın da verisi var. Innova'ya gitsem, Barikat ve InterProbe'u görecek. Bir kısırdöngü içerisindeyim. Dolayısıyla bana bunu kamunun sağlaması lazım. Keşke TÜBİTAK böyle bir şey yapsa; güvensem ve herkesten bağımsız desem.

Yasanın Kamuya Mal Edilmesi Lazım

Sosyal mühendislikte şöyle bir sorun var; bir şeyleri yasallaştırmak çok kolay, meşrulaştırmak zor. Nedir yasalla meşrunun farkı? Bazı şeyler yasal olabilir. Günlük yasa TBMM'de kabul edilir, Resmi Gazete'de yayınlanır ve artık yasaldır. Ama meşruiyet biraz da bireysel bir şeydir. Vatandaşın ve kamunun genel anlamda gözündeki bireyselliktir. Örneğin çok klasik olarak, "U dönüşü yasaktır" tabelası vardır ama bazı yerlerde herkes bilir ki oradan U dönüşü yapmak meşrudur. O semtte herkes döner orayı. Meşrudur, kimse yasak olarak görmez o işi. Burada belki biraz Amerikan film endüstrisinin de yönlendirmesiyle oluşan bir başka unsur da insanlara hacker tiplemesinin çok değişik gelmesi. Sanki bu bir hırsızlık ya da saldırganlık değilmiş gibi empoze edilmeye çalışılıyor. Böyle olunca da meşruiyeti artmaya başlıyor. Kimse kalkıp

> "Benim şimdiye kadarki hareketlerimi izleyip bundan sonrasıyla ilgili çıkarım yaparak benimle ilgili veri oluşturmanız yasaklandı, ihlal kapsamına girdi. Bunu ancak ve ancak aydınlatma metnine koyarak, rıza alarak yapabiliyoruz. Orada da işçinin rızasının ne kadar geçerli olduğu hep çok tartışmalı bir konu."

"Benim oğlum hırsız oldu" demez ama "Benim oğlum hacker'lık yapıyor" diyeni gördüm. Dolayısıyla istediğiniz kadar yasa çıkartın, olmuyor. Çünkü yasanın bir de kamuya mal edilmesi lazım. Bunun için de gerçekten sosyal mühendisliğe çok açığız. Dolayısıyla bilişimcilerin bunu sosyologlarla beraber çalışması gerekiyor. Bunun suç olduğunu anlatmak lazım ki insanlar bunu yapmasın, sosyal mühendisim diye dolaşmasın. Bir, bunu yapmak lazım. İki, biz hukukçular olarak bu konulardan hiç anlamıyoruz. Hukuk çok gelenekseldir. Roma'dan bu yana var olanla devam eder. Böyle de gitmesi gerekir ama bize yol gösterilmesi, yani ortak çalışma yapılması lazım. Çok kıymetli hukukçularımız var; cezacısı var, kamucusu var. Birinin onlara ceza ve kamu alanında bilişimle ilgili düzenlemeyi yönlendirebilmeleri için bilişimin ne olduğunu tane tane anlatması lazım.

Çalışanın Sorumluluğu İle Kişilik ve İşlem Analizinde Hukuki Çerçeve

İşçi işveren ilişkisinin çok iyi analiz edilip kullanım kurallarının çok iyi belirlenmesi gerekiyor. İşçi işveren ilişkisinde özellikle uzaktan çalışmada çok fazla hata yapıldı. Bu hatanın yapılmaması için öncelikle işverenin bütün imkânı sağlamış olması lazım. Eğitimi vermiş olması, uyarıyı yapmış olması lazım. İşveren bunların çoğunu unutmaya başladı. Yani hatalar çalışana çıkartılıyor. O anlamda da risk analizi yapılması gerekiyor. Çalışanlara mutlaka anlaşılabilir prosedürlerin anlatılıp sadece imzalatılması değil, anladığının da kayıt altına alınması gerekiyor. Çünkü kötü niyetli olduğu hâlde "Benim bundan haberim yoktu" dediği için maalesef işe iade edilen müvekkil çalışanları da oldu.

Bir de AB'de özellikle Kişisel Verilerin Korunması (Avrupa Birliği Genel Veri Koruma Tüzüğü -GDPR) kapsamında kişilik analizi ve işlem analizi yapılması çok tartışıldı. GDPR'ye geldi, yakında bize de gelmesi bekleniyor. Kişilerin verisinin kullanılarak, kendisi hakkında üretilen data -veri diye tanımlamak istemiyorum- üzerinde kişisel hakkı olması gerektiği düşünülüyor. Yani benim şimdiye kadarki hareketlerimi izleyip bundan sonrasıyla ilgili çıkarım yaparak benimle ilgili veri oluşturmanız yasaklandı, ihlal kapsamına girdi. Bunu ancak ve ancak aydınlatma metnine koyarak, rıza alarak yapabiliyoruz. Orada da işçinin rızasının ne kadar geçerli olduğu hep çok tartışmalı bir konu. Çünkü işini kaybetmemek için veriyor. Bu anlamda bir hukukçu olarak benim belki en büyük hukuki uyarım şu olacak: Bu metinlerin bütün çalışanlara yönelik hazırlanması, mavi yaka-beyaz yaka ayırmadan anlayabilecekleri şekilde anlatılması, imzalarının da alınması ama sadece imza alınıp geçilmemesi ve bunun bütün süreçlerinin risk analizinin yapılması. Çünkü kurum geliyor, "Şunu şunu analiz edeceğiz, bunu yapacağız, bu kuralı çıkardık" diyor. Her süreçte hukukçu yer almadığı için İş Hukuku'na, anayasaya ya da Kişisel Verilerin

Korunması prosedürlerine aykırı mıdır, söylenmiyor. Sonra çalışanın birisi şikâyet ediyor. Bir müvekkilimde, sendikadan dolayı, çok ciddi emek ve para sarf edilerek yapılmış olan bütün bir süreci iptal etmek zorunda kaldık.

Suçun Bilişim Sistemi Aracılığıyla İşlenmesi Ağırlaştırıcı Neden

Sosyal medya dolandırıcılığı yedi yıldır çok karşılaştığımız bir konu. Özellikle kamuoyunda bilinen müvekkiller açısından çok sıklıkla yapılıyor. Konuya ceza açısından birkaç yönden bakılabilir. Öncelikle kendisi taklit edilen kişinin, kişilik haklarına bir saldırı söz konusu. Türk Medeni Kanunu, kişinin tam doğmasıyla beraber kişilik haklarına sahip olduğunu kabul eder. Dolayısıyla kişinin adı, fotoğrafı ve kendisini tanıtacak bilgiler üzerindeki hakları mevcuttur. Bunların kötüye kullanılması nedeniyle eğer bir zarara uğradıysa, uğradığı zararın tazminini isteyebilir.

Konuyu ceza yönünden ikiye ayırmak gerekiyor. Bilişim suçu kavramı çok yanlış anlaşılmıştır. Aslında bilişim suçu, sadece Türk Ceza Kanununda tanımlanan bilişim sistemine karşı işlenen suçtur. Yani sisteme girmek, sistemin çalışmasını engellemek, bozmak ve veriyi aktarmak. Bunun dışındakiler ise bilişim yoluyla işlenen suçlardır. Örneğin dolandırıcılık. Bizde ve tüm Roma temelli sistemlerde hesap çalınabilir bir şey değil. Çünkü çalmaktan bahsedebilmeniz için fiziksel olarak zilliyetin değil mülkiyetin el değiştirmesi gerekiyor. Bu anlamda, elektrik hırsızlığının da olmayacağı söylenir. Olsa olsa bunu dolandırıcılığa bağlayabilirsiniz. Ama burada bir zarar kastı da olmadığı için hesabı alınan kişi açısından burada hırsızlıktan çok dolandırıcılık suçu işlenir. Bunu isterseniz yolda yürürken, isterseniz internet ortamında yaparsınız; bir fark yoktur. Tüm bunlar dolandırıcılık olabilir, hırsızlık olabilir, nefret suçu olarak tanımladığımız bir suç olabilir, politik suç olabilir, hakaret olabilir. Benim kendi hesabımdan 100 takipçim vardır, hakaret ederim 100 kişi görür ama çok bilinen bir hesabı ele geçirip yaparsam binlerce kişi görür. Dolayısıyla burada bilişim sistemi aracılığıyla işlenen bir suç var. Bilişim sistemi aracılığıyla işlenebilen suçlar açısından TCK bunları ağırlaştırıcı nedenler olarak tanımlar. Çok klasik bir ağırlaştırıcı neden de yüzü kapatmaktır. Örneğin ben bir yere molotof kokteyli atarım, cezası altı aydır. Yüzümü kapatarak atarım ki yine klasik terör eylemi davranışıdır, sekiz aya çıkar diyelim. Niye, çünkü gizlemektir. Dolayısıyla burada kimliğinizi gizlediğiniz için hukuk mantığı açısından ağırlaştırıcı nedendir. Örneğin zehirleyerek adam öldürmek, normal cana kast suçundan daha ağır ceza gerektirir. Niye; çünkü 1-0 önde başlarsınız. Karşınızdakinin savunma imkânı yoktur. Burada da aynı şekilde. Dolayısıyla klasik suçlar anlamında bilişim sistemi kullanılarak işlenmesinde hep ağırlaştırıcı nedendir.

Dolayısıyla hesabı çalınan kişi açısından bakarsanız, burada onun malına zarar verme, ızrar suçu vardır; çünkü onun bir malıdır. Kamuya verilen zarar açısından bakarsanız, dolandırıcılık olabilir, hırsızlık olabilir, hakaret olabilir. Üçüncü olarak, eğer sisteme girdiyseniz ya da kırdıysanız bu da bilişim sistemine girme suçunu oluşturur, çünkü yetkisiz girmişsinizdir. Bunlar da zaten TCK'de dört başlık altında tanımlanmıştır. Girmek ve orada kalmaya başlamak bir suçtur. Hiçbir şekilde zarar oluşmasa bile suç oluşmuştur, bu bir tehlike suçudur. Sonrasında bunun bir derece ağırı, sistemdeki veriyi değiştirmek, yeni veri eklemek, veri çıkarmak, veriyi başka bir yere aktarmak, sistemin çalışmasını değiştirmek, prensibini değiştirmek, sistemi durdurmak ya

da farklı şekilde çalışır hâle getirmektir. Daha sonrasında da özel olarak banka ve kredi kartlarına ilişkin daha da ağırlaştırıcı şeyler getirilmiştir. Bütün bu skala içinde bakarsanız altı aydan başlayıp sekiz buçuk, dokuz yıla kadar giden; eğer bir banka sistemine ve kamu sistemine karşı işlenmişse, oradaki ağırlaştırıcı nedenler de mevcutsa -ki burada gelir elde edip etmemesi, kendisi ya da başkası açısından ağırlaştırıcı nedendir- yaklaşık 11 yıla kadar gidebilen cezalar söz konusudur.

Türk Hukukunda Öngörülen Bilişim Suçları Cezaları Yeterlidir

Türk Hukukunda bilişim suçları yeterince tanımlanmıştır ve bu suçlara karşılık yasalarda öngörülen cezalar da yeterlidir. İhtiyacımız olan daha ağır suç tanımı değil. Aslında burada mesele, birlikte çalışıp suçluyu yakalamak. Herkes, "Bizde bilişim cezaları yok" diyor. Hayır, aslında var. Yakalasak cezası verilecek ama yakalamakta zorlanıyoruz. Burada da teknik olarak ya servis sağlayıcılara ya da adliyelerdeki teknik görevlilere, bilirkişilere çok ciddi görev düşüyor olabilir.

Biz son kullanıcıların, yani güvenlik uzmanı olmayanların erişilebilir ve onaylanabilir kaynakları bulabilecekleri bir platform olması gerektiğini düşünüyorum. Biz her bulduğumuzu bilgisayarımıza indiriyoruz. Çünkü bunu onaylayacak bir platformumuz yok. Mesela, gördüğümüz bir uygulamanın kullanılıp kullanılmayacağına bakabileceğimiz kamunun düzenlediği bir liste çok faydalı olurdu. Bir de bizim hukukçular olarak teknik uzmanların çok fazla desteğine ihtiyacımız var, çünkü çok anlamadığımız bir alana düzenleme getirmek zorunda kaldık.

Çağlar ÇAKICI
Trendyol Güvenlik Yöneticisi

SİBER İSTİHBARAT SERVİSLERİYLE ÇALIŞMAK BÜYÜK FAYDA SAĞLIYOR

Çalıntı hesaplarla ilgili süreçlerde siber istihbarat servisleriyle çalışmak büyük fayda sağlayacaktır. Konu müşteri verisi olduğu için Türkiye'deki bütün siber istihbarat servisleriyle çalışıyoruz. Global ölçekte çeşitli servisleri denedik ancak Türkiye'de yerel dili bilen ve kültürü tanıyan firmaların bu alanda daha başarılı olduğunu düşünüyorum.

Trendyol'da 1.300 kişilik bir teknoloji ekibimiz bulunuyor. Bu çalışanların 900 kişiye yakınını developer gibi düşünebiliriz. Şirkette toplam çalışan sayısı 5.000 civarında. Birçok yönetmelik, hukuksal konular ve diğer regülatif süreçlerde daha esnek olduğumuzu söyleyebilirim. Bu konuyla ilgili verilebilecek örnekler şunlar olabilir: Trendyol Pay isminde bir ödeme şirketimiz var. Yakında yaptığımız bütün alışverişleri bu "cüzdan" sistemiyle gerçekleştirilecek hâle getirmeye çalışıyoruz. Finansal konular olduğu için daha sıkı bir denetlemeye tabi oluyoruz. Bu sebeple de aslında Türkiye'de tutulması gereken veriyi Türkiye sınırları içerisinde tutmamız gerekiyor. Eğer verdiğimiz hizmet herhangi bir denetim veya regülasyona tabi değilse, bunu bulut ortamlarda kullanmayı tercih ediyoruz. Kullanılan birçok bulut ortamının güvenlik iyileştirmeleri ve denetleme süreçleri güvenlik ekibimiz tarafından sağlanıyor.

Genel siber saldırılara örnek verecek olursak; DDOS bizde en kritik konulardan bir tanesi. Trendyol erişilebilir olduğu sürece müşteriler alışveriş yapabiliyor. Geçtiğimiz yıllarda çok büyük boyutlu DDOS saldırıları aldık. Hatta bazı saldırılar İnternet Servis Sağlayıcıları (ISP) etkileyecek seviyedeydi. Bu tarz servis engelleme saldırılarını yurtdışından gelen trafiğe kapatmak, trafiğin temizlenmesini sağlamak için bulut ortamlara yönlendirmek ve ISP seviyesinde hizmet almak büyük önem taşıyor.

Ağ seviyesi güvenlik saldırılarının haricinde "hesapların ele geçirilmesi/hesap çalınmaları" bizim için çok önemli ve kritik bulduğumuz konuların başında geliyor. Örnek verecek olursak; daha az güvenlik olgunluğuna sahip kuruluşların, müşteri verilerinin sızdırılması sonucu, ele

> "Daha kolay istismar edilebilecek üçüncü parti (depo, hukuk büroları, entegratörler) firmalarını ele geçirerek, bu firmalar üzerinden saldırıyı gerçekleştirmek saldırganlar için daha çok tercih edilen bir yöntem oluyor."

geçirilen müşteri hesaplarının Trendyol üzerinde kullanılması ve bu hesapların yeraltı forumlarda satılması. Aslında hesap sahipleri aynı parola ve e-posta kombinasyonunu tüm üyelik gerektiren platformda kullanmazlarsa bu problem büyük ölçekte gideriliyor. Ayrıca iki faktörlü doğrulama özelliğinin aktif edilmesi bu tip saldırılarda önemli bir koruma sağlıyor.

Bunun haricinde sahtekârlık (fraud) tipi işlemler var. Bu saldırıyı gerçekleştirmek isteyen kişiler genelde çok teknik altyapıya sahip kişiler değil. Uygulamaların veya sürecin mantıksal hatalarından faydalanarak bu zafiyetler istismar ediliyor. Örnek verecek olursak; sahte ürün ile gerçeğinin yer değiştirilmesi, kupon kullanımına yönelik saldırılar vb. şeklinde özetleyebiliriz.

Üçüncü parti firmalar üzerinden gerçekleştirilen saldırıların sayısı gün geçtikçe artıyor. Saldırganlar genel olarak bu metodu kullanmayı tercih ediyorlar. Yine Trendyol özelinden örnek verecek olursak; 7/24 güvenlik olaylarını takip eden bir ekibimiz bulunuyor, çeşitli saldırı tekniklerini kullanarak sistemler üzerinde zafiyet tespit etmeye ve kapatmaya çalışıyoruz. Ancak daha kolay istismar edilebilecek üçüncü parti (depo, hukuk büroları, entegratörler) firmalarını ele geçirerek, bu firmalar üzerinden saldırıyı gerçekleştirmek saldırganlar için daha çok tercih edilen bir yöntem oluyor.

Çalıntı hesaplarla ilgili süreçlerde siber istihbarat servisleriyle çalışmak büyük fayda sağlayacaktır. Konu müşteri verisi olduğu için Türkiye'deki bütün siber istihbarat servisleriyle çalışıyoruz. Bu servisler bu forum ve bu işleri yapan kişilerden çok güzel veri elde edebiliyor. Global ölçekte çeşitli servisleri denedik ancak Türkiye'de yerel dili bilen ve kültürü tanıyan firmaların bu alanda daha başarılı olduğunu düşünüyorum. Dil engeli sebebiyle global firmalar genelde pazarlık sürecini iyi yönetemiyorlar.

Yakın zamanda siber sigorta konusu üzerinde bir ekiple beraber çalıştık. Bağımsız bir kuruluş tarafından güvenlik olgunluğunuz ölçülüyor ve bunun sonucunda bir rapor ve skor oluşturuluyor. Bu rapor ve skor ile beraber sigorta sürecine başlayabiliyorsunuz. Ancak çoğu sigorta firması fidye yazılımı (ransomware) ile ilgili konuları karşılamıyor.

Ticari Faaliyetlerde Kullanılan Kişisel Verilerin ve Ticari Bilgilerin Güvenliği

Ticari faaliyetlerde kullanılan kişisel verilerin ve ticari bilgilerin güvenliği konusuyla alakalı bulut güvenliğinden bahsetmek faydalı olabilir. Türkiye'de birçok kurum ve kişi için bulut çok yeni bir ortam. Çoğu kamu veya özel sektördeki çalışan arkadaşlar, regülasyonlar gereği bu alanı çok aktif kullanamıyor ve hâkimiyet sağlayamıyorlar.

İlk öncelik olarak, varlık yönetimi konusu geliyor. Varlık yönetimi dediğimiz; bulut ortamı üzerinde açılan servislerin ve ayağa kaldırılan sunucuların envanterinin tutulması demek oluyor. Güvenlikte de ilk öncelik her zaman envanteri biliyor olmanız ve sonrasında bunun güvenliğini sağlıyor olmanız. Bir diğer konu; hesap yönetimi hususu. Bu servis ve sunuculara erişen hesapların belirli aralıklarla gözden geçirilmesi ve ihtiyaç kalmaması hâlinde kapatılması.

Trendyol güvenlik ekibi olarak ayrıca bulut ortamında ayağa kaldırılan bir servis veya sunucuyu tespit etmek için çeşitli script'ler/kod blokları geliştirdik. Bu scriptler sayesinde envanteri güncel tutabiliyor ve elde ettiğimiz uç nokta bilgilerini zafiyet tarama yazılımına otomatik olarak ekleyebiliyoruz. Bazı sistem yöneticileri veya yazılımcılarda güvenlik bakış açısı henüz olgunlaşmadığı için, sadece kurulan sistemin veya yazılan kodun çalışıp/çalışmadığı ile ilgileniyorlar. Bu tarz bir senaryoda sunucuyu bazen tamamen internete açabiliyorlar veya zafiyet barındıran bir servisle hizmet vermeye başlıyor olabilirler.

ZDI örneğinden yola çıkarak bu alanda bir şeyler yapılmasını destekliyorum. Cep telefonlarında kullanıcı etkileşimi olmadan çalıştırılabilecek bir zafiyete 2,5 milyon dolar civarında bir ödeme gerçekleştiriliyor. Sunucu ve diğer çok kullanılan uygulamalarda bu ödüllendirme bir milyon dolara kadar çıkabiliyor. Türkiye'de de benzer sürecin işletilmesi, siber taaruz ve siber silahlanmada kullanabileceğimiz bir altyapının oluşmasını sağlayacaktır.

Bunların haricinde, kurumlar arası siber istihbarat paylaşılabilecek bir platformun kurulması fayda sağlayacaktır. IP, çalıntı kredi kartları veya çalıntı hesapları vb. ortak bir platform üzerinden paylaşmak tüm kurumlara fayda sağlayacaktır.

Gökhan ÖNAL
LpsChain Genel Müdürü

SİSTEMİN YEDEKLENMESİ, GÜVENLİĞİ AÇISINDAN BÜYÜK ÖNEM TAŞIYOR

Bir rüzgâr santralinin kontrol mekanizmasına yapılacak bir siber saldırıyla, santralin üretimi 1.000 MW iken aniden sıfıra düşürülebilir, bu durum sistemde kalıcı sorunlara yol açabilir. Tabii bu durumda TEİAŞ başta olmak üzere TEDAŞ ve özel firmalar da siber saldırı senaryoları yapmaktadır. Gün geçtikçe hem siber saldırıların hem de hacker'ların artmasıyla bu durum firmalar için daha büyük bir sorun hâline gelmiştir. Şu an tüm firmalar enerji sistemlerinin tasarımlarını bu tehlikeleri göze alarak yapmaktadır.

Bir ürün geliştirici olarak devlet ve özel sektör tarafından üretilen ve kullanılan verilerin güvenli bir şekilde yedeklenmesi, depolanması ve transferinde uygulanan yöntemler, bizim yıllarca mustarip olduğumuz bir konudur. Yüzlerce insanın çalıştığı ve milyarlarca doların harcandığı bir firmanın verisinin çalınması, firmanın stratejisinin bitmesine, hatta firmanın faaliyetlerinin sona ermesine bile neden olabilir. TUSAŞ'la bir projede biz de dirsek temasındayız. Veri paylaşımı o kadar sorun ki, farklı çözümler üzerinde de düşünüyoruz. Ayrıca GE'nin yaptığı şu anda dünyanın en büyüğü olan rüzgâr türbininin tasarımında da bulunuyoruz. Fakat güvenli bir şekilde verilerimizi yollayamadığımız için USB ile gidip bu verileri bizzat elden teslim ettiğimiz oluyor. Günümüzde farklı metotlar var tabii fakat bu, firmanın ya da kurumların farkındalığıyla alakalı. Bir firma eğer verisine sahip çıkıyorsa, verisinin kıymetinin farkındaysa çözümler getirmeye çalışıyor ancak sektörün çoğu maalesef herhangi bir çözüm uygulamıyor. Birçok firma kıymetli verilerini WhatsApp'tan gönderiyor ya da çok bilindik firmalar, WeTransfer ya da Dropbox gibi halka açık çözümleri kullanıyor, ancak ülkemizde ASELSAN, TUSAŞ ya da devlet kurumları gibi kıymetli kurumlarımız verinin çok önemli olduğu durumlarda farklı çözümler arıyor.

Bu konuda biz de, dünyada ilk olan, yeni bir çözüm getirdik. Firmalar genelde kendi sunucularından kapalı devre link atarak verilerini dışarıyla paylaşıyor ancak bir ürün geliştirme birçok partnerin bir arada senkron şekilde çalışmasını gerektirdiği ve bu dosyaların encryption yapılarak

karşı tarafa yollanması gerektiği için verimli bir çalışma ortamı sağlanmıyor. Günümüzde verimli çalışma ortamı problemi var: üçüncü partnere veri yollanması. Örneğin, TUSAŞ'ta kağıda yazılan veriler bile alınıp götürülmüyor, TUSAŞ'ta kalıyor. Mesela, ben de Siemens'te çalışırken bu konudan çok şikâyetçiydim; parmak izi, PTI kartlar ile Siemens'e giriş yapılıyor ve giderken aranıyorduk ama bu durumun şu an kıymetini anlıyorum. 1.000 kişinin çalıştığı, milyarlarca doların harcandığı bir ürün geliştirirken, sonunda 30, 40 milyar dolarlık bir pazarın rakibin eline geçmesi bu işi bitiriyor. Tabii bunun devlet düzeyinde ve stratejik boyutta tamamen ayrı yeri var. Blok zinciri teknolojisiyle bu konuya yeni bir çözüm getirilmeye çalışılıyor.

Ayrıca veri güvenliği ile ilgili aşırı hassasiyet, veri analitiğinde birtakım zorluklara yol açabilirken, aşırı korumacılık yerine daha esnek koruma modelleri de bulunuyor. Bu alanda tamamen defansif olup veriyi paylaşmayalım, içeride kapalı ağda kalsın gibi bir durumda projenin gelişmesinde büyük sorunlar yaşanıyor. Özellikle bazı firmalar pandemide büyük sıkıntı yaşadı çünkü evden çalışamadılar, ofise gitmek zorunda kaldılar. Bunun için de alternatif çözümler denenmelidir.

Üçüncü Paydaşlarla Güvenli Bir Ortam Sağladık

Biz enerji ve elektronik sektöründe olduğumuz için müşterilerimizle projeler üzerinde çalışırken şimdiye kadar veriyi nereden yollayacağımız konusunda bir sorun oluşuyordu. WeTransfer

yasak, Dropbox yasak. Google Drive'ı kırmak çok fazla mümkün değil ama bu uygulamada da verilerin tek bir merkezde tutuluyor olması problem. Yani merkezi bir sistemde encryption metotlarda birisinin kontrolü altında olması gerekiyor. Bizim sunduğumuz metotta dağıtık sistem olduğu için sadece yetkili kişilerin -yani birisine bırakılmıyor bu durum- kontrolü altındadır. Üçüncü paydaşlarla güvenli bir ortam sağlanması söz konusudur. Onun için de farklı bir pencere oluşuyor. Şu an Bahçeşehir Kolejleri, Uğur Kolejleri, Kızılkaya Gümrük Müşavirliğine hizmet vermekteyiz ve 300.000'in üstünde kullanıcımız var. Ayrıca, ürünümüzü yeni pazarlara da sunmaya başladık.

Bizler de farklı bir kripto tekniği kullanıyoruz. Bilindiği gibi şifrelemede Public Private Key adında bir güvenlik sistemi var. Bizde bunlara ek olarak LPS Key var. Bu key sadece kullanıcıya tanımlanır, kullanıcı bunu kaybederse kullanıcının verisine kimse ulaşamaz. Çünkü bu key, merkezi sistemde tutulmadığı için veriye ulaşma imkânı olmaz. Ayriyeten blok zinciri sisteminde verinin akışı için güvenli bir kanal oluşturuyoruz. Hatta bunu milli uçaklarda da kullanmayı planlıyorlar çünkü altıncı nesilde uçakların İHA'larla bile uçması, sürekli bir iletişim hâlinde olması planlanıyor. Veriyi binlerce chunk'lara ayırıp farklı node'larda parçalara bölüp depoluyoruz. Bu arada LpsChain, blok zinciri olarak verinin kendisini bloklayan tek yapıdır. Bu alanda da dünyada tektir. Örnek vermek gerekirse, bir binayı kum tanesine çevirip attığımızı düşünün; birisi bunu ele geçirse bile bir manaya erişemiyor çünkü dosya asimetrik olarak binlerce parçaya bölünebiliyor. Her parçaya ulaşması gerekiyor.

Bizim ilgilendiğimiz diğer bir konu, kurumsal firmalarda yaşanması muhtemel iç tehditler. Birisi firmadan çıkarken yapacağı ilk iş tüm bilgiyi alıp gitmek olabilir. Bu doğrultuda biz verileri iç yetkilendirmeyle de koruyoruz. Çünkü blok zincirine kaydedilen bilgi silinemiyor. IT yöneticisi olsa bile bir firmada kimin nereden aldığı silinemiyor. Tabii ki bir yazılım tek başına güvenlik getiremez. Kişi kötü niyetliyse yapacağını yapar ama yetkilendirmeyle zarar vereceği alan kısıtlanabilir.

Sistem tasarımında sistemin yedeklenmesi, güvenliği açısından büyük önem taşıyor. Örneğin, bir uçakta ya da bir hastanede bu yedekleme işlemi en üst düzeyde olmalıdır. Ülkemizde ve başka birçok ülkede enerji sistemlerinde projeler yapıyoruz. Contingency analiz dediğimiz bir analiz metodu vardır; n-1 kuralı. Yani bir sistem çökerse akabinde bu enerji nereden akacak ya da bu eksik rezerv nereden gelecek diye analizler, senaryolar yapılır. Enerji sisteminde en kötü sonuç black out olmasıdır. Black out olmasını sanırım 2015'te yaşamıştık; ülke için büyük bir problemdir. Milyarlarca dolar, hatta bir savaş durumu varsa, ülkenin fişinin çekilmesi söz konusudur. Bunlar çok uzak senaryolar da değildir.

"LpsChain, blok zinciri olarak verinin kendisini bloklayan tek yapıdır. Bu alanda da dünyada tektir. Örnek vermek gerekirse, bir binayı kum tanesine çevirip attığımızı düşünün; birisi bunu ele geçirse bile bir manaya erişemiyor çünkü dosya asimetrik olarak binlerce parçalara bölünebiliyor. Her parçaya ulaşması gerekiyor."

Örneğin, Türkiye'nin elektrik şebekesi Avrupa'nın elektrik şebekesi ile senkron olarak çalışmaktadır. ENTSO-E adı verilen bir şebeke operatörleri birliği bulunmaktadır ve Türkiye bu birliğin en doğudaki üyesidir. 2021 yazında Türkiye, tüm Avrupa şebekesinin çökmesini engelledi. Fransa bölgesinde bir santralin kaybolmasıyla frekansın aşırı yükselmesini Türkiye desteklemişti. Yani Türkiye bu konumda yedekti. Sistem tasarımında da yedek bir hat veya yedek bir santral hayati önem bakımından göz önünde bulundurulmalıdır. Yani; doğu bölgesinin -doğunun önemsizliğinden değil de az insan olmasından dolayı- elektriğinin gitmesi belki göz ardı edilebilir. Fakat İstanbul için bir saatlik kesintiyi göz ardı edemeyiz. Çünkü İstanbul'da n-1 kuralı değil, n-3 kuralı vardır. Yani hat bir yerden kopsa diğer taraftan beslenmesi gerekir. Ayrıca enerji sistemlerinde birincil ve ikincil rezervler bulunur. Bir sistem yük kaybettiği zaman milisaniyeler önemlidir. Beş milisaniye içinde eğer o deficit power aktarılmazsa frekans kaybolup sistem çöker. Bu durumda da birincil rezerv sayısı artırılmaktadır. Günümüzde her şeyin dijitalleşmesiyle, ülkemizde siber saldırıların sayısı artmıştır. Yani bir rüzgâr santralinin kontrol mekanizmasına yapılacak bir siber saldırıyla, santralin üretimi 1.000 MW iken aniden sıfıra düşürülebilir, bu durum sistemde kalıcı sorunlara yol açabilir. Tabii bu durumda TEİAŞ başta olmak üzere TEDAŞ ve özel firmalar da siber saldırı senaryoları yapmaktadır. Gün geçtikçe hem siber saldırıların hem de hacker'ların artmasıyla bu durum firmalar için daha büyük bir sorun hâline gelmiştir. Şu an tüm firmalar enerji sistemlerinin tasarımlarını bu tehlikeleri göze alarak yapmaktadır.

Maalesef ben siber güvenlik konusunda farkındalığın kısa sürede oluşacağını düşünmüyorum. Çünkü özel sektörde bulunan firmaların çoğunda birçok şey maliyete bağlı. Ve kimse başına bir felaket gelmedikçe maliyetini artırmak istemeyecektir. Bu doğrultuda da devletten bir regülasyon gelmedikçe bir değişim olacağını düşünmüyorum. Devlete yük bindirmek gerekmez, bu kamunun görevi değildir. Ama kamu regülasyon, akreditasyon sağlayabilir ve bu bilinci ancak bu şekilde aşabiliriz.

Serbülend ZEREN
Trend Micro Bölge Müdürü

SİBER GÜVENLİKLİ VATANDAŞLAR YETİŞTİRMELİYİZ

> Siber güvenlik demek benim için siber güvenlikli insan demektir. Siber güvenlikli insanlar, siber güvenlikli vatandaşlar yetiştirmemiz lazım. Bu alanda da gerekirse ilkokuldan itibaren siber güvenlik dersleri açılıp eğitimlerin verilmesi gerektiğini düşünüyorum.

Ben teknolojiyi genelde doktora benzetirim. Her zaman "Allah düşürmesin, Allah onsuz da bırakmasın" derim. 50'li yılların sonu, 60'lı yılların başında bilgisayarın icadı, 89 senesinde internetin hayatımıza girmesi, Web 1.0 teknolojilerinin gelişmesi ve bunun üzerine 2004 yılında Web 2.0 ile internet satış, sosyal medya gibi ortamların gelişmesi ve bugün geldiğimiz durumda da Web 3.0 blok zinciri teknolojileri ve ileriye dönük, Metaverse dediğimiz çok ayrı bir dünyaya doğru giden bir trendin içerisindeyiz. Bu teknolojinin gelişmesiyle birlikte siber saldırganlar da çok ciddi anlamda gelişmeye başladı.

Genelde yaptığım sunumlarda bunu şu şekilde özetliyorum: Halam bir tren istasyonunun çok yakınında otururdu. 6, 7 yaşlarında oraya gittiğimizde, 10, 11 yaş arası çocuklar yerden taş alırlar, geçen trenlere fırlatırlardı. Küçük küçük camlar vardı, o camları kırdıklarında 10 puan kazanırlardı. Zamanla birlikte teknolojide değişim başladıktan sonra siber saldırganlar bu çocuklar gibi büyümeye başladı. Bu çocuklar artık bu trenin önünü kesip de treni soymaya başladı. Şu an geldiğimiz noktada da artık bu trenin içerisinde seyahat ediyorlar ve bu saldırganlar devletlerin, büyük özel şirketlerin himayeleri altına girmeye başladı. Geldiğimiz bu noktada sürekli hack'lenme psikolojisinde yaşar duruma geldik. Bugün sosyal medyada, Instagram, Facebook, Twitter gibi platformlarda çok ciddi şekilde hayatlarımızı deşifre etmeye başladık. Bu konuda aramızda çok ciddi bilinçli insanlar da var fakat benim genelde hep söylediğim mavi yakalı/beyaz yakalı çalışan arkadaşlar, güvenlik çalışanları, belki bir temizlik çalışanı, yani bilgisayar erişimi olan insanlar daha bilinçsiz olmaya başladı. Dolayısıyla hack'lemek de günümüzde çok cazip hâle gelmeye başladı.

Dünyanın en büyük şirketlerinden birinin hack'lenmesi için bir hacker özel şirketi tutuluyor. Bilinçsiz vatandaşlar alıp belki sistemlere takar, oradan sızarız diye düşünerek yerlere USB disk atıyorlar. Fakat Avrupa'da, ABD'de, dünyada birçok yerdeki kurumsal şirketlerde insanlar öyle güzel yetiştirilmişler ki, yerde sahipsiz bir flash disk bulduklarında götürüp bilgi işlem yöneticisine veriyorlar ve bir sanal ortamda bu flash disk test ediliyor.

Buradan giremeyeceklerini anlayınca fishing dediğimiz oltalama yöntemini yapmaya karar veriyorlar. Şirket CEO'sundan gelmiş gibi görünen, "Maaş Zam Artışları" konulu bir oltalama e-postası gönderiyorlar. Global bir şirket olduğu için yaklaşık 500 bin çalışan var. Fakat ne ilginç ki, e-postayı genel müdür açıyor ve hacker'lar tam umudu kesmişken birdenbire bir ışık beliriyor ekranlarda, buradan bir arka kapı açılıyor. Arka kapıdan girilip istenen bütün veriler alınıyor.

Kamu kurumlarında bu tip durumlarda genelde markamla birlikte biz arkada ciddi anlamda varlık gösteriyoruz. Gerek yerli milli alanda destekler olarak, gerekse kurumlardaki farkındalıkları artırmak açısından çok çeşitli çalışmalar yapıyoruz. Bunlardan başlıcası kurumların bilgisi dahilinde, kimseye haber vermeden kullanıcılara oltalama e-postaları atıyoruz ve bu tuzağa düşenlere neden düştüklerini anlatıyoruz. Arka tarafta düşmeyenler, e-postayı hiç görmemiş insanlar var. Bir de bu kurumlarda özellikle kamu sektöründe toplu bir şekilde ayda bir farkındalık eğitimleri veriyoruz.

Yapmamamız gerekenlere gelecek olursak, sosyal hayatımızı deşifre etmememiz, zayıflıklarımızı göstermememiz gerekiyor çünkü sosyal mühendisliğin kaynağında korku ve acı hissi yatar. Hacker'lar bunları sosyal medyada yaptığınız paylaşımlardan edinir. Bugün nereye tatile gitmiş, nerede kiminle yemek yemiş, arkadaş çevresinde kimler var; yani sizin çok zayıf, çok hassas olduğunuz noktaları çok rahat bulabilir bir duruma geldiler. Bununla ilgili farkındalık

> "Bugün hemen hemen herkesin dile getirdiği şey siber güvenlik kavramının vatandaş düzeyinde ufak yaştan itibaren insanlara aşılanması. Ben televizyon kanallarında kamu spotlarının daha çok yaygınlaştırılması gerektiğini düşünüyorum."

eğitimlerinin yapılması gerekiyor. Siber güvenlik demek benim için siber güvenlikli insan demektir. Siber güvenlikli insanlar, siber güvenlikli vatandaşlar yetiştirmemiz lazım. Bu alanda da gerekirse ilkokuldan itibaren siber güvenlik dersleri açılıp eğitimlerin verilmesi gerektiğini düşünüyorum.

Sistemlere istediğiniz kadar gerekli güvenlik önlemlerini alın ama bazen bir kullanıcının telefonundan ciddi anlamda tehditler alabiliyorsunuz. Burada bizim şöyle bir çözümümüz var, biz cep telefonlarını genelde sanallaştırıyoruz ve kullanıcılar da cep telefonlarında eğer şirket sistemli gideceklerse ya da kurum sistemine dahil olacaklarsa telefon üzerinde bir aplikasyon ile sistemlere dahil oluyorlar. Buradaki amacımız kullanıcının kendi kişisel telefonunu kullanmasını ve sistemin network'üne güvenli bir şekilde bağlanmasını sağlamak. Her iki tarafı da izole ediyoruz ve biz bunun çözümünü birçok kamu kurumunda bu şekilde sağladık. 2021'in Ağustos ayında yayınladığımız bir güvenlik raporu var. Bu güvenlik raporu diğer yıllara göre biraz farklılık gösteriyor. Şöyle ki, önceden cep telefonlarındaki zararlı dosyaların daha fazla olduğunu görüyorduk. Fakat bu 2021 Trend Micro Güvenlik Raporu bize cep telefonlarında zararlı dosyaların çok azaldığını ama zararlı uygulamaların ciddi şekilde artış gösterdiğini işaret ediyor.

Trend Micro olarak hem Apple Store hem Google Store gibi GSM kullanıcılarını ilgilendiren yerlerdeki aplikasyonları sürekli test ediyoruz. Örneğin yakın bir tarihte kripto madenciliğiyle ilgili yedi uygulamanın Google Store'da tespitini yapıp, Google Store'a uyarı göndererek bu uygulamaların kaldırılmasını sağladık. Dünyadaki bütün hacker'lar önceden "Apple'da bir açık buldum" diyerek bu açığı Apple'a gönderir, Apple'dan bir hediye almayı beklerdi. Sonradan Zero Day Initiative (ZDI) diye bir oluşum kuruldu ve bu dünyanın çeşitli yerlerindeki hacker'lar bu dataları ZDI'a gönderdi. Örneğin Microsoft'ta bir açık buldunuz, ZDI sizin yerinize Microsoft'taki tarafı kontrol edip sizin oradan para kazanmanızı sağladı. Yaklaşık dört sene kadar önce ZDI, Trend Micro'nun bünyesine katıldı. Finansör olarak ZDI'ı satın aldık. Böylece dünyadaki yeni çıkan malware'lerin yüzde 66,4'ünü Trend Micro olarak tek başımıza tespit eder duruma geldik. Aramızda Deep Security kullanıcıları da var, onlar da bileceklerdir. Bu da bize sanal yama, patch gibi çok ciddi artılar getirmeye başladı. Bunları mobil cihazlara da tatbik etmeye başladık.

Bugün hemen hemen herkesin dile getirdiği şey, siber güvenlik kavramının vatandaş düzeyinde ufak yaştan itibaren insanlara aşılanması. Ben televizyon kanallarında kamu spotlarının daha çok yaygınlaştırılması gerektiğini düşünüyorum. Bir de artık Türkiye'de siber güvenlik bakanlığının kurulması gerektiğini düşünüyorum.

THINKTECH ODAK TOPLANTISI KONUŞMACILARI ÖZGEÇMİŞLERİ

(E) KORGENERAL ALPASLAN ERDOĞAN

(E) Korgeneral Alpaslan Erdoğan, Kara Harp Okulu İşletme Bölümünü müteakip Kara Harp Akademisi, Türk Silahlı Kuvvetler Akademisi ve Türkiye Orta Doğu Amme İdaresi Enstitüsünde yüksek lisans eğitimlerini tamamladı. Bosna Hersek ve Napoli-İtalya'da NATO görevlerinde bulundu. 2004 yılında Tuğgeneral rütbesine terfi ederek İç Güvenlik Piyade Tugay Komutanı olarak atandı. Sonraki yıllarda Genelkurmay Başkanlığı Genel Plan ve Prensipler Başkanlığı Savunma Planlama ve Kaynak Yönetim Daire Başkan Yardımcılığı ve Daire Başkanlığı ile 52'nci Taktik Zırhlı Tümen Komutanlığı görevlerinde bulundu. 2012 yılında Korgeneralliğe terfi eden ve üç yıl boyunca Genelkurmay Genel Plan ve Prensipler Başkanı olarak görev yapan Erdoğan, 2016 yılında 5'inci Kolordu Komutanlığından Korgeneral Rütbesi ile emekliye ayrıldı. Nisan 2018'den bu yana STM ThinkTech Teknolojik Düşünce Merkezi Koordinatörlüğünü icra etmektedir.

MUHAMMET SAMİ ULUKAVAK

Muhammet Sami Ulukavak, 2007 yılında Orta Doğu Teknik Üniversitesi (ODTÜ) Elektrik ve Elektronik Mühendisliği Bölümünden lisans derecesini aldı. T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığındaki görevine 2008 yılında Elektronik Harp ve Algılayıcılar Daire Başkanlığında başladı. 2011 yılında El Yapımı Patlayıcılar ile Mücadelede Yeni Nesil Teknolojiler konulu teziyle Savunma Sanayii Uzmanı oldu. El Yapımı Patlayıcılar (EYP) ile mücadele, elektronik harp, kritik tesislerin korunması başta olmak üzere önemli projelerde görev aldı. EYP ile mücadele koordinasyon grubu faaliyetlerinde yer aldı. 2013 yılında ODTÜ Bilim ve Teknoloji Politikaları bölümünden yüksek lisans derecesi alan Ulukavak, savunma sanayiinde Ar-Ge ve teknoloji yaklaşımı konusunda çalışmalar yaptı. 2014 yılında öğrenim için ABD'ye gitti. 2016 yılında Harvard Üniversitesinden Kamu Yönetimi yüksek lisans derecesini aldı. Buradaki eğitimi sırasında Yönetim, Liderlik ve Karar Bilimleri konusunda çalışmalarda bulundu. Haziran 2016'da Koruma ve Güvenlik Projeleri Grup Müdürü olarak görevlendirilen Ulukavak, 2016'nın Eylül ayından 2018'in Mart ayına kadar Siber Güvenlik ve Elektronik Harp Sistemleri Daire Başkanı, Mart 2018'den Şubat 2021'e kadar ise Elektronik Harp ve Radar Sistemleri Daire Başkanı olarak görev yaptı. Şubat 2021 itibarıyla Siber Güvenlik ve Bilişim Sistemleri Daire Başkanı olarak görevlendirilen Ulukavak hâlen bu görevini yürütmektedir. Terörle mücadele, mayın ve EYP ile mücadele, elektronik ve sinyal istihbaratı, elektronik harp, radar, kritik tesislerin güvenliği, siber güvenlik, kurumsal kaynak yönetimi, yazılım, bilişim teknolojileri ve dijital dönüşüm alanlarında toplamda 200'den fazla yurtiçi geliştirme projesinde yer almıştır. Yarı iletken ve Mikroelektronik alanında faaliyetlerde bulunmuştur. Hâlihazırda 40'tan fazla projeyi yönetmekte olup, kurumsal dijital dönüşüm faaliyetlerine liderlik etmektedir.

PROF. DR. İBRAHİM ÖZÇELİK

Prof. Dr. İbrahim Özçelik, Sakarya Üniversitesi Bilgisayar Mühendisliği bölümünde öğretim üyesi ve Kritik Altyapılar Ulusal Test Yatağı Merkezi (CENTER SAU) koordinatörüdür. Bilgisayar Ağları, Araçsal Ağlar (VANET), Operasyonel Teknolojiler (OT), Endüstriyel İletişim Protokolleri, Bilgi Güvenliği, Siber Güvenlik ve Kritik Altyapıların Güvenliği gibi konularda araştırma çalışmaları yapmaktadır. Araştırma alanı ile alakalı olarak ulusal ve uluslararası saygın konferans ve dergilerde birçok bildiri ve makale yayınladı, TÜBİTAK ARDEB ve TEYDEB destekli projelerde yürütücülük ve danışmanlık yaptı ve 2012 yılında da ABD'de ziyaretçi öğretim üyesi olarak bulundu. Üniversitesinde "Siber Güvenlik Eğitim, Araştırma ve Uygulama Laboratuvarı" ve "Kritik Altyapılar Ulusal Test Yatağı Merkezi" kurulum süreçlerini yöneten Özçelik, 2014 yılından bu yana Sakarya Üniversitesi Siber Güvenlik Yüksek Lisans Program koordinatörlüğü ve Siber Güvenlik Öğrenci Topluluğu akademi başkanlığı görevlerini de yürütmektedir.

ABDURRAHMAN EMRE ÖZKÖK

Abdurrahman Emre Özkök, 2009 yılında Sakarya Üniversitesi Elektrik-Elektronik Mühendisliği bölümünden mezun olmuştur. MBA yüksek lisansını tamamladıktan sonra şu anda tez döneminde bulunduğu Gazi Üniversitesi Bilgi Güvenliği Mühendisliği yüksek lisans programına başlamıştır. İş hayatına 2010 yılında Türk Telekom Network Direktörlüğü bünyesinde network uzmanı olarak başlamıştır. 2015 yılında Kamu İhale Kurumu bünyesinde network güvenliği ve güvenlik cihazları yönetimi konularında çalışmaya başlamıştır. 2016 yılında TÜBİTAK Bilgem Siber Güvenlik Enstitüsü altında Siber Güvenlik Hizmetleri ekibinde uzman araştırmacı olarak göreve başlamıştır. Hâlen çalışmaya devam ettiği TÜBİTAK'ta sızma testi, sıkılaştırma uzmanı, güvenlik mühendisi ve siber güvenlik çözüm yöneticisi olarak çalışmalar yapmaktadır. Ayrıca Siber Güvenlik Strateji Eylem Planı, Bilgi ve İletişim Güvenliği Rehberi, Siber Güvenlik Yol Haritası Oluşturma ve Savunma Sanayii Odak Grupları gibi stratejik organizasyonlarda görev almaktadır. Siber Güvenlik Enstitüsü içerisinde asaleten yaptığı Siber Güvenlik Hizmetleri birim yöneticiliğinin yanında Siber Güvenlik Çözümleri Birimi için de eşzamanlı vekâleten birim yöneticiliği görevini sürdürmektedir.

ENİS MÜÇTEBA MEMİŞ

1995 yılında Ankara Üniversitesi Elektronik Mühendisliği bölümünden mezun olan Enis Müçteba Memiş, kariyeri boyunca üretim, tasarım, yazılım geliştirme ve program yönetimi faaliyetlerinde 27 yıllık bir deneyime sahip bulunmaktadır. STM'den önce savunma sanayiinde F-16 Aviyonik Görev Sistemleri, F-16 Elektronik Harp Kendini Koruma Sistemleri, çeşitli havacılık ve teknoloji geliştirme projelerinde ülkemizin önde gelen ulusal firmaları bünyesinde mühendis, orta kademe yönetici ve üst düzey yönetici pozisyonlarında görev almıştır. Son olarak TUSAŞ' ta Milli Muharip Uçak Program Müdürü olarak görev yapmış olan Enis Müçteba Memiş, Ağustos 2021 tarihinden itibaren STM'de taktik mini İHA sistemleri, yapay görü, otonom sistemler, siber güvenlik ve bilişim, uydu ve uzay, komuta kontrol ile radar sistemlerinden sorumlu Teknoloji Genel Müdür Yardımcısı olarak görevine devam etmektedir.

GÜRAY YILDIZ

Güray Yıldız, lisansını Bilkent Bilgisayar Mühendisliği ve yüksek lisansını ise ODTÜ Yöneylem Araştırması bölümünde tamamladı. Son 13 yılı TUSAŞ olmak üzere, savunma ve havacılık sektörü firmalarında 24 yıllık tecrübesi var. Komuta kontrol sistemleri, karar destek uygulamaları ve aviyonik yazılım geliştirme ve sertifikasyon süreci uzmanlık alanları. TUSAŞ kariyerinde, C-130 modernizasyon projesinde FMS (Flight Management System -Uçuş Yönetim Sistemi) yazılım ekibi teknik yöneticiliği, Yazılım Mühendisliği Müdürlüğü görevlerini üstlendi. Güncel olarak; TUSAŞ tarafından geliştirilmekte olan özgün hava platformlarının aviyonik yazılımlarını geliştiren, Milli Muharip Uçak Genel Müdür Yardımcılığına bağlı, Yazılım Tasarım, Yazılım Doğrulama ve Yapay Zekâ Müdürlüklerini içeren Yazılım Mühendisliği Direktörlüğü görevini yerine getirmektedir.

AHMET GÖKHAN YALÇIN

Ahmet Gökhan Yalçın, Boğaziçi Üniversitesi Elektrik-Elektronik Mühendisliği bölümünden mezun olduktan sonra kariyerine Garanti Teknoloji'de güvenlik ekibinde başladı. Garanti Teknoloji'de Network Güvenlik Yöneticisi olarak çalıştıktan sonra Yapı Kredi Bankasında Siber Güvenlik Operasyon Merkezi Müdürü olarak görev aldı. Yapı Kredi Bankasının 7/24 çalışan SOC merkezi kurulumunu ve işler hâle gelmesini başarılı bir şekilde yürüttükten sonra kariyerine alanlarında lider iki farklı küresel güvenlik üreticisinde bölgesel danışman rollerinde devam etti. Bu deneyimlerinin ardından şu an Yapı Kredi Teknoloji firmasında Bilgi Sistemleri Güvenlik Yönetimi Genel Müdür Yardımcısı olarak ve aynı zamanda Yapı Kredi Bankasında CISO olarak görev yapmaktadır.

MAHMUT KÜÇÜK

Mahmut Küçük, siber güvenlik alanında finans ve telekomünikasyon sektöründe uzmanlık ve yöneticilik görevlerinde bulunmuştur. Hâlen Türk Telekom'da Siber Güvenlik Direktörü olarak yerli ve milli siber güvenlik ekosisteminin geliştirilmesi hedefine yönelik proje ve ürünleşme çalışmalarına katkı sağlamaktadır.

AV. CEYDA CİMİLLİ AKAYDIN

Ceyda Cimilli Akaydın, 1998 yılında Marmara Üniversitesi Hukuk Fakültesinde lisans, 2004 yılında İstanbul Üniversitesi Özel Hukuk Anabilim Dalında Yüksek Lisans eğitimlerini tamamladı. Hâlen İstanbul Üniversitesi Özel Hukuk Anabilim Dalında hizmet olarak yazılım sözleşmeleri (SAS) konusunda doktora tezi çalışmalarını sürdürmektedir. 1999-2000 yılları arasında İstanbul Hukuk Bürosunda Stajyer Avukat, 2000-2001 yılları arasında Öngören Mutlu Hukuk Bürosunda Stajyer Avukat ve de büroya bağlı avukat olarak MU-YAP'ta (Müzik Yapımcıları Meslek Birliği) çalıştı. 2001 yılında İstanbul Üniversitesi Enformatik bölümünde Araştırma Görevlisi olarak akademik kariyerine başlayan Ceyda Cimilli Akaydın, bu görevinden 2008 yılında ayrıldı. Halen Yeditepe Üniversitesinde yarı zamanlı olarak özel hukuk ve bilişim hukuku dersleri vermektedir. 2008 yılından bu yana ailesinin kurmuş olduğu Cimilli Akaydın Hukuk Bürosunda çalışmakta olan Ceyda Cimilli Akaydın, müvekkillerine hukuki açıdan iş süreçlerini sorunsuz yürütebilmelerini sağlamak için hukuki risk analizi, sözleşme danışmanlığı ve genel hukuk danışmanlığı hizmetlerini sunmakta , ağırlıklı olarak bilişim hukuku, marka ve telif hakları, alan adlarından kaynaklanan uyuşmazlıklar, bayi ilişkileri hukuku konularında olmak üzere her alanda dava takibi yapmaktadır. Türkiye Bilişim Derneği İstanbul Şubesi Yönetim Kurulu Üyesi Ve Hukuk Çalışma Grubu Başkanı, İstanbul Barosu Bilişim Merkezi Kurucu Üyesi ve İnternet Kurulu Alan Adları (DNS) Çalışma Grubu Üyesidir.

ÇAĞLAR ÇAKICI

Siber güvenlik kariyerine 2006 yılında başlayan Çağlar Çakıcı, 300'ün üzerinde ağ ve uygulamaya yönelik sızma testi gerçekleştirmiş olup; içlerinde Checkpoint, Mcafee, 3Com, Tippingpoint gibi birçok üreticiye ait saldırı tespit ve saldırı önleme sistemlerinde kritik seviyede zafiyet bildirimlerinde bulunmuştur. Kariyerinin son yedi yılında ağ güvenliği yöneticiliği, güvenli yazılım geliştirme danışmanlığı, bilgi güvenliği denetimleri ve e-ticaret sistemleri güvenliği konusunda defensive tarafta çalışmalarına ağırlık vermiştir. Açık kaynak kodlu birçok projeyi geniş ölçekli yapılarda aktif olarak işletmekte ve gelişimine katkıda bulunmaktadır. 2016 yılında Türkiye'nin en büyük e-ticaret platformlarından biri olan Trendyol'da siber güvenlik uzmanı olarak çalışmaya başlamıştır. Hızla büyüyen bu e-ticaret platformunda güvenlik yöneticisi olarak görevine devam etmektedir. Profesyonel iş yaşamından geriye kalan zamanlarda da aktif olarak bug bounty programlarında zafiyet aramaktadır.

GÖKHAN ÖNAL

2008 yılında Bahçeşehir Üniversitesi Elektrik-Elektronik bölümünden mezun olan Önal, Almanya'da RWTH Aachen Üniversitesinde Elektrical Power Engineering alanında yüksek lisans eğitimini 2010 yılında tamamlamıştır. 2010 yılı itibarıyla Siemens AG'de HVDC & FACTS sistemlerinin geliştirilmesi üzerine çalışmaya başlamış, 2016 yılına dek buradaki görevini sürdürmüştür. 2016 yılında Lean Power Solutions firmasını kuran Önal, enerji alanında üreticilere, ağ operatörlerine ve danışman firmalara çözüm odaklı hizmet vermektedir. Bu zamana kadar, birçok rüzgâr türbini, HVDC, STATCOM ve benzer teknolojilerin geliştirilmesi süreçlerine dahil olmuştur. 2020 yılında bilişim alanına faaliyetlerini taşıyarak, blockchain tabanlı veri depolama, transferi ve yönetimi hizmeti sunan LPS Chain Ltd adlı firmayı kurmuştur. Hâlihazırda, Gökhan Önal, Lean Power Solutions ve LPS Chain Ltd firmalarının Genel Müdürlük görevlerini devam ettirmektedir.

SERBÜLEND ZEREN

Serbülend ZEREN, 2003 yılında Trakya Üniversitesi Bilgisayar Mühendisliği bölümünden mezun oldu. Xerox The Document Company firmasında Salt Engineer olarak üç sene çalıştı. Servus Bilgisayar A.Ş. de KKTC Bölge Müdürlüğü ve hemen ardından Turcom Teknoloji Ankara Bölge Müdürlüğü görevini üstlendi. Son yedi sene Trend Micro şirketinde Ankara Bölge Müdürü olarak görevine devam etmektedir.

@STMThinkTech

STM

www.stm.com.tr

/ @STMDefence

thinktech

STM Teknolojik Düşünce Merkezi

thinktech.stm.com.tr

/ @STMThinkTech