İŞ HAYATINDA BİLGİ GÜVENLİĞİ

Konferans Raporu

15 Aralık 2017, İstanbul

İstanbul 2018
Yayın No: TÜSİAD-T/2018, 03 – 590

Meşrutiyet Caddesi. No. 46 34420 Tepebaşı/İstanbul
Telefon: (0 212) 249 07 23 •Telefaks: (0 212) 249 13 50
www.tusiad.org

© 2018, TÜSİAD

Tüm hakları saklıdır. Bu eserin tamamı ya da bir bölümü,
4110 sayılı Yasa ile değişik 5846 sayılı FSEK uyarınca,
kullanılmazdan önce hak sahibinden 52. Maddeye uygun
yazılı izin alınmadıkça, hiçbir şekil ve yöntemle işlenmek, çoğaltılmak,
çoğaltılmış nüshaları yayılmak, satılmak,
kiralamak, ödünç verilmek, temsil edilmek, sunulmak,
telli/telsiz ya da başka teknik, sayısal ve/veya elektronik
yöntemlerle iletilmek suretiyle kullanılamaz.

ISBN: 978-605-165-025-8

Editör: H. Altay Güvenir

Dizgi ve Sayfa Uygulama: Ceren Yazıcı

ÖNSÖZ

TÜSİAD Türkiye'nin önde gelen girişimcileri ve iş dünyası yöneticileri tarafından 1971 yılında, Anayasamızın ve Dernekler Kanunu'nun ilgili hükümlerine uygun olarak kurulmuş, kamu yararına çalışan bir dernek olup gönüllü bir sivil toplum örgütüdür.

TÜSİAD, insan hakları evrensel ilkelerinin, düşünce, inanç ve girişim özgürlüklerinin, laik hukuk devletinin, katılımcı demokrasi anlayışının liberal ekonominin, rekabetçi piyasa ekonomisinin kurum ve kurallarının ve sürdürülebilir çevre dengesinin benimsendiği bir toplumsal düzenin oluşmasına ve gelişmesine katkı sağlamayı amaçlar.

TÜSİAD, Atatürk'ün öngördüğü hedef ve ilkeler doğrultusunda, Türkiye'nin çağdaş uygarlık düzeyini yakalama ve aşma anlayışı içinde, kadın-erkek eşitliğini, siyaset, ekonomi ve eğitim açısından gözeten iş insanlarının toplumun öncü ve girişimci bir grubu olduğu inancıyla, yukarıda sunulan ana gayenin gerçekleştirilmesini sağlamak amacıyla çalışmalar gerçekleştirir.

TÜSİAD, kamu yararına çalışan Türk iş dünyasının temsil örgütü olarak, girişimcilerin evrensel iş ahlakı ilkelerine uygun faaliyet göstermesi yönünde çaba sarf eder; küreselleşme sürecinde Türk rekabet gücünün ve toplumsal refahın, istihdamın, verimliliğin, yenilikçilik kapasitesinin ve eğitimin kapsam ve kalitesinin sürekli artırılması yoluyla yükseltilmesini esas alır.

TÜSİAD, toplumsal barış ve uzlaşmanın sürdürüldüğü bir ortamda, ülkemizin ekonomik ve sosyal kalkınmasında bölgesel ve sektörel potansiyelleri en iyi şekilde değerlendirerek ulusal ekonomik politikaların oluşturulmasına katkıda bulunur. Türkiye'nin küresel rekabet düzeyinde tanıtımına katkıda bulunur, Avrupa Birliği (AB) üyeliği sürecini desteklemek üzere uluslararası siyasal, ekonomik, sosyal ve kültürel ilişki, iletişim, temsil ve işbirliği ağlarının geliştirilmesi için çalışmalar yapar. Uluslararası entegrasyonu ve etkileşimi, bölgesel ve yerel gelişmeyi hızlandırmak için araştırma yapar, görüş oluşturur, projeler geliştirir ve bu kapsamda etkinlikler düzenler.

TÜSİAD, Türk iş dünyası adına, bu çerçevede oluşan görüş ve önerilerini Türkiye Büyük Millet Meclisi (TBMM)'ne, hükümete, diğer devletlere, uluslararası kuruluşlara ve kamuoyuna doğrudan ya da dolaylı olarak basın ve diğer araçlar aracılığı ile ileterek, yukarıdaki amaçlar doğrultusunda düşünce ve hareket birliği oluşturmayı hedefler.

TÜSİAD, misyonu doğrultusunda ve faaliyetleri çerçevesinde, ülke gündeminde bulunan konularla ilgili görüşlerini bilimsel çalışmalarla destekleyerek kamuoyuna duyurur ve bu görüşlerden hareketle kamuoyunda tartışma platformlarının oluşmasını sağlar.

"İş Hayatında Bilgi Güvenliği Konferans Raporu" Bilkent Üniversitesi - TÜSİAD Bilgi Toplumu Forumu'nun bir etkinliği olarak 15 Aralık 2018 günü Çırağan Palace Kempinski İstanbul adlı otelde gerçekleştirilen "İş Hayatında Bilgi Güvenliği" adlı konferansta yapılan konuşmaları içermekte olup Forumun direktörü Prof. Dr. H. Altay Güvenir tarafından hazırlanmıştır.

Şubat 2018

Şekil Listesi:

KISALTMALAR

BT	: Bilgi Teknolojileri
BTF	: Bilkent Üniversitesi-TÜSİAD Bilgi Toplumu Forumu
CDO	: Chief Data Officer
CEO	: Chief Executive Officer
CFO	: Chief Financial Officer
CIO	: Chief Information Officer
CISO	: Chief Information Security Officer
CISO	: Chief Information Security Officer
CPU	: Central processşng Unit
CRM	: Customer Relationship Management
CRM	: Customer Relationship Management
ERP	: Enterprice Resource Planning
GDPR	: General Data Protection Regulation
IoT	: Internet of Things
KOBİ	: Küçük ve Orta Büyüklükteki İşletmeler
KVKK	: Kişisel Verileri Koruma Kanunu
PDKS	: Personel Devam Kontrol Sistemleri
TCP	: Transmission Control Protocol
VP	: Vice President

SUNUŞ

Bilkent Üniversitesi – TÜSİAD Bilgi Toplumu Forumu (BTF) 21 Ocak 2015 tarihinde imzalanan bir protokol ile kuruldu. Türkiye'nin dijital dönüşümüne katkı sağlamayı amaçlayan Forum, iş dünyasının ve kamu sektörünün bu dönüşümü hızlandırmasına destek olacak nitelikte çalışmalar yapacaktır.

Bilgi güvenliği forumun çalışmalarında öncelik verdiği alanlardan biridir. Zira tüm dünyada ve ülkemizde dijital dönüşümün yaşandığı şu günlerde, yine bu dönüşümün bir parçası olarak akıllı şehirler, sürücüsüz araçlar, fabrikalarda kullanılan otomasyon sistemleri, bilgisayarlar, telefonlar sayesinde teknolojiye olan bağımlılığımız günden güne ve hızlı bir şekilde artmakta. Bu teknolojik dünyanın avantajları günden güne artarken, beraberinde şirketlerimiz ve hatta kişisel olarak bizler için, bireyler olarak bizler için tehlikeler oluşturabiliyor. Maalesef siber saldırılar çok yaygın hale geldi. Yanlış bilgi, yanlış ellere geçtiğinde bir firmayı mahvedebilir ve hatta müşterilerine önemli zararlar verebilir. Bilgi Toplumu Forumu bu nedenle olası riskler konusunda tüm toplumu ve özellikle de iş dünyasını uyarmayı hedeflemektedir.

İşte bu öncelikler ve hedefler doğrultusunda BTF'nin bilgi güvenliği alanındaki ilk etkinliği "İş Hayatında Bilgi Güvenliği" adlı konferans organizasyonu oldu. Konferansın açılış konuşmalarını Sayın Filiz Akdede ve Sayın Erol Bilecek yaptılar. Konferansta Sayın Prof. Dr. Engin Kırda yapay Zeka alanındaki çalışmaların siber güvenlik konusunda uygulamalarını konusunda örnekler verdi. Sayın Engin Özbay firmaları bekleyen siber saldırı riskleri konusunda dinleyicileri uyardı. Sayın Berna Kulaksız bir mobil iletişim firması için bilgi güvenliğinin önemini ve yeni nesil siber güvenlik yaklaşımlarını ele aldı. Konferansa katılamayan Onur Koç yerine konuşmayı iş arkadaşı Ozan Öncel yaptı. Sayın Öncel büyük yazılım firmalrının bilgi güvenlik konusunda yapmakta olduğu çalışmalar hakkında bilgi verdi. Son olarak Sayın Fatih Emiral bir birine İnternet üzerinden bağlı iki bilgisayarın birinden diğerine bir saldırı senaryosunu adım adım icra ederek katılımcılara bir tür saldırının nasıl olacağını gösterdi.

Prof. Dr. H. Altay Güvenir
BTF Direktörü

BİLKENT ÜNİVERSİTESİ – TÜSİAD BİLGİ TOPLUMU FORUMU

İŞ HAYATINDA BİLGİ GÜVENLİĞİ

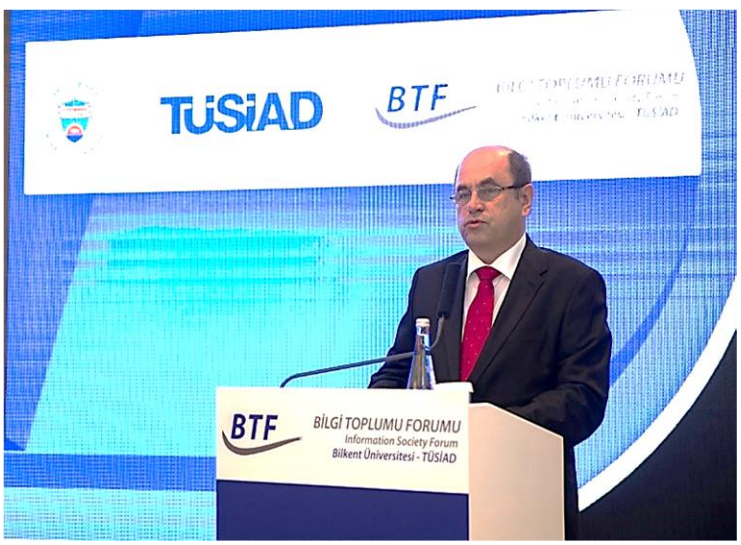
Sunucu

Sayın TÜSİAD başkanım, Sayın TÜSİAD Yönetim Kurulu Üyeleri, Sayın Bilgi Toplumu Forumu üst kurul üyelerim, iş ve teknoloji dünyasının değerli temsilcileri, sayın basın mensupları ve çok değerli konuklar, Bilkent Üniversitesi TÜSİAD Bilgi Toplumu Forumu tarafından düzenlenen, "İş Hayatında Bilgi Güvenliği" konferansına hepiniz hoş geldiniz. Konferansımız, açılış konuşmalarının ardından Sayın Prof. Dr. Engin Kırda ve Sayın Engin Özbay'ın konuşmaları ile devam edecek. Kahve arasından sonra ise Sayın Berna Kulaksız ve Sayın Ozan Öncel'in konuşmalarının ardından, Sayın Fatih Emiral'ın uygulayacağı siber saldırı senaryosunda, zararlı bir yazılımın kullanıldığı uygulama sayesinde, saldırgan cephesini daha yakından gözlemleme imkânı bulacağız.

Saygıdeğer konuklar, ilk olarak Bilkent Üniversitesi TÜSİAD Bilgi Toplumu Forumu Direktörü Sayın Prof. Dr. Halil Altay Güvenir'i, açılış konuşmalarını yapmak üzere kürsüye davet ediyoruz.

Prof. Dr. Halil Altay Güvenir

Teşekkür ederim. Sayın TÜSİAD yönetim kurulu başkanım, Sayın TÜSİAD yönetim kurulu üyeleri, Sayın konuklar, Bilkent Üniversitesi TÜSİAD Bilgi Toplumu Forumu tarafından düzenlenen, "İş Hayatında Bilgi Güvenliği" konferansımıza hoş geldiniz.



Prof. Dr. H. Altay Güvenir (Bilkent Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı, Bilkent Üniversitesi-TÜSİAD BTF Direktörü)

Bilgi toplumu forumumuzun amacı, Türkiye'nin bilgi toplumuna dönüşümü için gereken orta ve uzun vadeli politikalar hakkında araştırmalar ve faaliyetler gerçekleştirmek ve bilgi toplumu kavramının ülke gündemindeki yerinin sürekliliğini ve Türkiye'nin bilgi toplumu dönüşümü politikalarına katkı sağlamaktır.

Tüm dünyada ve ülkemizde dijital dönüşümün yaşandığı şu günlerde, yine bu dönüşümün bir parçası olarak akıllı şehirler, sürücüsüz araçlar, fabrikalarda kullanılan otomasyon sistemleri, bilgisayarlar, telefonlar sayesinde teknolojiye olan bağımlılığımız günden güne ve hızlı bir şekilde artıyor. Bu teknolojik dünyanın avantajları günden güne artarken, beraberinde şirketlerimiz ve hatta kişisel olarak bizler için, bireyler olarak bizler için tehlikeler oluşturabiliyor. Maalesef bilgi sızıntıları çok yaygın hale geldi. Yanlış bilgi, yanlış ellere geçtiğinde işinizi mahvedebilir ve hatta müşterilerinizin hayatını da mahvedebilir. Biraz önce izlediğimiz giriş videosunda durumun vahameti hakkında ürkütücü rakamlar izledik.

Cyber Security Business Report'a göre siber suçların oluşturduğu zarar 2015 yılında 3 trilyon dolar civarındayken, 2021'de bu rakamın yaklaşık 6 trilyon dolara ulaşması bekleniyor. Gartner tarafından 2017'de, içinde bulunduğumuz yıl Ağustos ayında yayınlanan bir rapora göre, 2017 yılında 86 milyar dolar olan siber güvenlik harcamalarının önümüzdeki 5 yıl içinde 1 trilyon doları aşması bekleniyor, yaklaşması bekleniyor. Buradan da görüldüğü üzere, bilgi güvenliğinin önemi her geçen gün artıyor. Kişisel verilerimiz, şirket bilgilerimiz, müşteri bilgilerimiz, hepsi uğrayabileceğimiz bir siber saldırı sonrasında tehlikeye girebilir ve hatta telafi edilemeyecek şekilde bize ve şirketimize zarar verebilir.

Her geçen gün daha da bağımlı hale geldiğimiz bilgi teknolojilerinin güvenlik riskleri taşıması, dijital dönüşümden kaçmamıza neden olmamalı. Bunun yerine, bu risklerin bilincinde olup önlemlerimizi almamız gerekiyor. Bilkent Üniversitesi TÜSİAD Bilgi Toplumu Forumu olarak bu konferansı düzenlememizin amacı işte bu. Bilgi güvenliği konusunda şu anki durumu tespit etmek, gelecekte olası ortaya çıkabilecek riskleri ön görmek ve onlara karşı kendimizi ve şirketimizi hazırlamak için neler yapabileceğimiz hakkında bilgi alışverişinde bulunmak.

Bugün çok önemli konuklarımız var. Lastline Inc. kurucu ortağı ve Northeastern Üniversitesi öğretim üyelerinden Sayın Prof. Dr. Engin Kırda, Amerika'dan bu konferansa katılmak için aramıza geldi. Kendisine teşekkür ediyorum. İş dünyamızdan alanının uzmanları, konferansımıza konuşmacı olarak katılıyorlar. IBM Türk Güvenlik Ülke Lideri Sayın Engin Özbay'a, Vodafone Kurumsal Çözümler Direktörü Sayın Berna Kulaksız'a, Microsoft Türkiye Kurumsal İş, Üretkenlik ve Güvenlik Uygulamaları Satış Direktörü Sayın Ozan Öncel'e, yapacakları konuşmaları için şimdiden teşekkür ediyorum. Konuşmaları takip eden BT Risk adlı firmanın kurucu ortağı Sayın Fatih Emiral, uygulayacağı bir siber saldırı senaryosu yapacak, çok ilginç olacağını düşünüyorum, ona da şimdiden teşekkür ediyorum. Bilgi Toplumu Forumunu kuran ve desteğini esirgemeyen Sayın Erol Bilecik, Sayın Esin Güral Argat, Sayın Filiz Akdede'ye ve Bilkent tarafında rektörüm Sayın Abdullah Atalar'a çok teşekkür ediyorum. Bugün gerçekleştireceğimiz konferansın tüm katılımcılar için yararlı olmasını diliyorum, herkese katılımı için teşekkür ediyorum.

Sunucu

Sayın Halil Altay Güvenir'e konuşmaları için teşekkürlerimizi sunuyoruz.

Çok değerli konuklar, şimdi ise TÜSİAD Bilgi ve İletişim Teknolojileri Çalışma Grubu Başkanı Sayın Filiz Akdede'yi, konuşmalarını yapmak üzere kürsüye davet ediyoruz.

Filiz Akdede

Sevgili konuklar, günaydın. İş Hayatında Bilgi Güvenliği konferansına hoş geldiniz. Umarım hepimiz için güzel verimli bir gün olur.

Filiz Akdede (TÜSİAD Bilgi ve İletişim Teknolojileri Çalışma Grubu Başkanı)

Küresel rekabette öne geçmenin yolu, bilimsel ve teknolojik gelişmeleri yakından takip edebilmek. İnsana, bilime, teknolojiye yatırım yapan firmalar ve ülkeler, ekonomik büyümelerini devam ettiriyorlar. Biz de TÜSİAD olarak yıllardır makro düzeyde inovasyona yönelik yatırımların artırılmasıyla ilgili çalışmalarımızı sürdürüyoruz.

Eğitimli, nitelikli insan gücünün artırılmasından, bilişim alanındaki teknolojilerle ilgili yatırımların, reformların yapılmasına kadar atılacak yüzlerce adım var. Bunlardan bir tanesi de bilgi güvenliği. Dünyada veri artık inanılmaz bir hızla artıyor, veriyi doğru kullanan firmalar, bununla ilgili yatırımlarını yapan firmalar, ilerleme kaydediyorlar ama aynı zamanda bilgi güvenliği bir risk de oluşturuyor, özellikle siber güvenlik alanında geçtiğimiz yıllarda birçok örneğini, milyarlarca dolarlık zararları gördük. Bu tarafta yatırımlar yapan firmalarsa ilerlemeye devam edebiliyorlar. Ülkemizde bilgi güvenliği konusunda hem bilinç yaratılması hem de aynı zamanda kamu, özel sektör, üniversitelerin birlikte çalışması gerekiyor. Son dönemde gördüğümüzse, büyük firmaların bu konuda bilincinin arttığı, yatırımlarını artırdığı, KOBİ'ler tarafında belli bir aydınlanma aslında bu konuda bir anlayış bilinç var, biraz daha üzerinde çalışılması ve bu konuda danışmanlıkların artırılması, bilgi güvenliği konusunun hepimiz için stratejik önemde olduğunun vurgulanması gerekiyor. Ülkelere, gelişmiş ülkelere de baktığımızda, ayrı bir stratejiyle siber güvenliğin, bilgi güvenliğinin özellikle vurgulandığı, takip edildiği görülüyor. Ülkeler için de önemli çünkü dediğim gibi ciddi anlamda geride kalma, geride bırakma riski olabiliyor. Artık üretim tarafında tasarımdan üretime, lojistikten satış sonrası servislere kadar uçtan uca güvenliğe hepimizin dikkat etmesi, önem vermesi ve ekiplerimizi bu konuda bilgilendirmemiz gerekiyor.

Biz de TÜSİAD olarak dijital dönüşüm yolculuğunda sadece ekonomik ve sektörel bazda değil, toplumsal perspektiften de bakmaya çalışıyoruz. Eğitim gücünün bu anlamda geliştirilmesine inanıyoruz, üniversitelerde özellikle doktora, yüksek lisans alanında bu konuların özellikle vurgulandığını görmek de sevindirici.

Bugün Bilkent Üniversitesiyle iş birliğiyle yaptığımız bu toplantıda çok kıymetli konuşmacılar var. Ben hem Bilkent Üniversitesine hem değerli konuşmacılarımıza hem de geldiğiniz için sizlere çok teşekkür ederim, keyifli bir gün geçirmenizi diliyorum. Teşekkürler.

Sunucu

Sayın Filiz Akdede'ye konuşmaları için teşekkür ediyoruz.

Değerli konuklar, şimdi ise TÜSİAD Yönetim Kurulu Başkanı Sayın Erol Bilecik'i, konuşmalarını yapmak üzere kürsüye davet ediyoruz.

Erol Bilecik

Erol Bilecik (TÜSİAD Yönetim Kurulu Başkanı)

Çok değerli konuklar, çok değerli basın mensupları, hatta izin verirseniz çok sevgili dostlar diyerek sizlerle olan bu keyifli muhabbetin içerisinde veya sohbetin içerisinde bulunmaktan duyduğum ben de memnuniyeti paylaşmak istiyorum. Ve sizleri gerçekten öncelikle şahsım ve TÜSİAD yönetim kurulu adına sevgi ve saygıyla selamlıyorum.

Neredeyse doğumundan bu yana, sevgili Altay Hocamla çok vakit geçirdiğimiz, çok hakikaten zaman zaman tartıştığımız, zaman zaman da gerçekten çok böyle sonuç odaklı bir şekilde neticeyi aldığımız BTF'nin bu noktalara gelmesini görmekten de hakikaten ekstradan çok mutlu oluyorum. Emeği geçen Altay Hocam başta olmak üzere, bütün gerçekten ekibi canı gönülden ben de bu vesileyle teşekkürlerimi paylaşmak istiyorum.

Çok değerli konuklar, yılın son günlerine, yani neredeyse günler hatta saatler kalmaya başlarcasına, yani çok az bir vakit kaldı. Şüphesiz ki iş dünyasında 2017'nin en fazla konuşulan konusu istisnasız değişim kelimesi oldu. Biz de konuşmalarımızda ve hatta sizler de sohbetlerinizde, konuşmalarınızda hep andığınız kelime hep değişim üzerine oldu. Dijital

dönüşüm hem ülkemizde hem de bütün dünyada şirketlerin şu an en popüler ve bir o kadar da ama kritik gündemi. Teknoloji merkezli dijital dönüşümde her konudaki iş yapış şekilleri de zaten kendi şirketlerimizde bulunduğumuz bütün auralarda çok hızlı bir şekilde değişmeye zaten başladı. Aslında değişen gerçekten hayatımızın ta kendisi. Dolayısıyla her şeye olduğu gibi işte de bakışımız değişiyor. Yılın özetini değişen birey, dönüşen toplum diye ifade edersek, tahmin ediyorum yanlış bir ifade kullanmamış oluruz. Değişen bireyler ve dönüşen toplumlar.

Çok değerli konuklar, dijital dönüşümün etkisiyle insanlık tarihinin her zaman söylediğimiz gibi hakikaten olağanüstü bir döneminde yaşıyoruz. Bu öyle bir değişim ki etkileri tüm dünyaya ve hayatın her alanına dokunuyor. Dünya, yeni bir sanki Rönesans yaşıyor. Düşünürseniz gerçekten bunun ne kadar anlamlı olabileceğini hep beraber tahmin ediyorum hemfikir oluruz. Rönesans bildiğiniz gibi sözlük anlamı itibariyle yeniden doğuş anlamına geliyor. Bugün ayakta kalmak için tüm değerlerin gerçekten yeniden doğması gerekiyor, bu değişim içerisinde çok harika bir şekilde yolculuğuna devam edebilmesi için. Bir başka deyişle de her insan, her şirket, hatta her ülke kendi Rönesans'ını da yaşamak zorunda. İnternet ve bilişim teknolojileri, otomasyon, yapay zekâ, nesnelerin interneti ve yeni iş modelleri, değerli Altay Hocamızın söylediği gibi hayatımızın her alanını etkiliyor dedik. Evet, teknolojiyle birlikte müthiş fırsatlarla karşılaşıyoruz. Bu fırsatlarda hem üretim metotlarında ve ürün geliştirmelerde hem de hizmet sunum süreçlerinde yepyeni bildiğimiz gibi dinamikler gelişiyor.

Bakın bu çağ şirketler için aslında en şanslı yüzyıl olabilir. Belki de en şanssız yüzyıl. Bunun hakikaten arası olmayan bence bir çağda yaşıyoruz veyahut da yüzyılı bu şekilde tanımlarsak ya çok şanslı olacak şirketler ya da en şanssız. Sonucu, değişime olan tamamıyla uyumumuz belirleyecek inanın. Yani değişime direnenler ve değişimi gerçekten ilk başlangıçta kabul edip bu değişimin önemli aktörü olanlar. Yüzyıl böyle bir yüzyıl. Teknolojinin getirdiği avantajlar şüphesiz hayatımızı fevkalade kolaylaştırdı. Eksikliğini hissettiğimiz en büyük avantajlardan biri de bildiğiniz gibi Vikipedia'ydı ama. Daha önce de birçok çağrılarda bulunduk ama çok olumlu gelişmelerin olduğunu da takip ediyoruz. Bu bakımdan diliyorum bu Vikipedia'yla sizlerin bizlerin arasındaki hasret tahmin ediyorum inşallah önümüzdeki günlerde sonlanmış olur, bunu da buradan tekrardan çağrımızı ben de yenilemek istedim. Bununla birlikte tekrardan dönersek, teknolojinin getirdiği avantajlara, bu yenilikler beraberinde yeni riskleri de ortaya çıkardı ve sonuçta günümüzün de esas konusu olan bilgi güvenliği kavramı dünya gündemine A'dan Z'ye yetişmiş vaziyette ve yerleşmiş vaziyette. Dünya dijitalleşmeyle birlikte pazarlama, satış, üretim, vergi gibi kavramları yeniden tanımlarken bugün artık risk ve tehditleri de yeniden tanımlama gereğini hissediyor ki ilk başta izlemiş olduğumuz videoda bunun nümerik değerlerini de son derece ilginç bir şekilde izlemiş olduk. Eskiden nereden ve hangi amaçla geleceğini tahmin edebildiğimiz risk ve tehditleri konuşurduk. Ama o dönemler bildiğiniz gibi artık geride kaldı. Yani nereden ve hangi amaçla gelen tehditleri artık konuşabilmek bir miktar gerçekten çok geçmişte kaldı. Artık tehdidin açık bir gönderici adresi yok sevgili dostlar. Bugün siber saldırılar bireylere, şirketlere, bankalara

ve hatta kamu kurumlarına fevkalade zarar vermekle yetinmiyorlar, ülkelerin güvenliklerini de tehdit ediyorlar. Hatırlarsınız tahmin ediyorum, siber saldırıların boyutunun ne kadar büyük olabileceğini, dünya ilk kez 2007 yılında Estonya örneğiyle görmüş oldu. Ülkedeki, Estonya'daki hatırlarsınız, yıl 2007, bankacılık sistemleri, devlete ait internet siteleri ve haber portallari gibi başlıca internet hizmetleri kullanılamaz hâle gelmişti. Bu enteresan bir örnek. Fakat aynı Estonya'yı tahmin ediyorum yine aynı şekilde izliyorsunuz, her ne kadar fevkalade küçük bir ülke olmasına rağmen dönemin bildiğiniz gibi Avrupa Birliği başkanlığını yapan bir ülke. Business Europe dediğimiz yani bütün Avrupa Birliği ülkelerinin iş dünyası örgütleri, TÜSİAD gibi hemen hemen 28 ülkenin beraberinde oluşturdukları Business Europe toplantısı hemen geçtiğimiz yakın günlerde 30 Kasım'da, 1 Aralık'ta Estonya'daydı arkadaşlar. Gerçekten buradan küçük bir anekdot paylaşmak istedim. Dönem başkanlığını da Avrupa Birliği'nin Estonya yaptığı için. Bu 2007'de saldırıya uğrayan, siber güvenlik problemlerinden dolayı bir hayli zor durumlar yaşayan o Estonya, bugün gördüğünüz gibi dünyada digital country veya dijital ülkeler noktasında ne yapılması gerektiği konusunda tamamen rol model olmuş vaziyette. Bunu da bu anekdotla paylaşmak istedim, ben de bilfiil çıplak gözlerle izleme şansım olan çok örnekler vardı, çok da hoş sunumlar izledik.

Siber saldırı teknikleri, bildiğiniz gibi teknolojinin gelişimine paralel bir hızla ilerliyor. Bunun sonucunda da operasyonların zarar görmesi, finansal kayıplar, rekabet gücünde geriye gidiş derken ciddi bir itibar ve güven kaybına uğramak, açıkçası tahammülü zor riskler ortaya çıkıyor. Şuna emin olunuz ki ben sizlere karanlık bir tablo çizmeye kati suretle çalışmıyorum. Bakın konu ne olursa olsun, bir sorunla mücadele edebilmek için önce tehdidin gerçekten adını koymamız gerekir. Bugün kazanılması gereken zafer veya sonuç şu; dijital dönüşümün sunduğu fırsatlardan hız kesmeden yararlanmak ve bu süreçlere, risklere karşı her an hazır ve korunaklı olmak zorundayız. Bilgi güvenliği sağlamadan sanayide dijital dönüşüm hedefini gerçekleştirmemiz zaten söz konusu olamaz. Konu ne olursa olsun, stratejisi olmayanları sadece yenilgiler bekler. Bunu bir tarafımızda her zaman kulağımıza küpe olarak almamız gerekir. Bu nedenle bilgi güvenliği konusunda ulusal düzeyde mutlaka bir strateji geliştirmemiz gerektiği de çok net ve açık. Stratejileri olmayanların hakikaten yenilgiyle buluşmalarından başka bir netice olmaz sevgili dostlar.

Çok değerli konuklar, dünya hızla değiştiği zaman her şeyi biraz daha hatta daha hızlı bir şekilde değiştiriyor. Her zaman söylüyoruz, dijital dönüşüme ayak uydurma kapasitemiz hem yeniliklerin getirdiği fırsatları hem de riskleri değerlendirecek bilgi ve öngörüye, gerekli adımları atabilecek çeviklik ve esnekliğe ne kadar sahip olduğumuza bağlı. Gelişen teknolojilerle birlikte sanal ortamda depolanan bilgi yoğunluğu ve bu bilgi yoğunluğunun taşıdığı önem, her geçen gün şüphesiz artıyor. Ülkede, ülkece bu konuda karnemiz maalesef bir miktar zayıf. Sadece kanuni düzenlemeler değil, bu konudaki kişisel bilinç de hâlâ geliştirilmeye çok açık bir şekilde ama duruyor orada. Oysa kişisel güvenliği, bilgi güvenliği konusu, diğer sorunların da en önemli tetikleyicilerinden bir tanesi. Bu konu, toplumumuzu oluşturan

yediden yetmişe herkesi zorunlu bir biçimde ilgilendiren bir konudur. Kişisel veri ifadesi, kulağa biraz teknik gelebilir arkadaşlar, uzun dönemlerdir kullanıyoruz. Tabi ki siz profesyonellerin son derece iç içe olduğu ama kamuoyuna baktığınız zaman kişisel veri meselesi biraz daha kulağa hakikaten teknik geliyor. İzninizle ben terimi biraz gündelik hayata tercüme etmek isterim. Buna çok kısaca tek kelimeyle biraz mahremiyet diyebiliriz belki de. Kişisel verilerin izinsiz erişimi, değiştirilmesi ve kullanımı gerçekleştiğinde, bireysel mahremiyet de ortadan kalkıyor. Mahremiyete yönelik tehditle ilgili çok sevdiğim ben de bir sözü, eminim birçoğunuz biliyorsunuzdur, sizinle de paylaşmak isterim. İnsan nüfusu, 18 ayda bir ikiye katlanmayabilir ama bilgisayarların bizi izleme yeteneği, 18 ayda bir ikiye katlanmaktadır sevgili dostlar. Yani tehdidin boyutu bu kadar net. Dolayısıyla günümüzde dijital verilerin önem kazanmasıyla birlikte bu verilerin güvenli bir şekilde saklanması ve kişilik haklarının korunması, aslında artık tamamen bir gereklilik haline gelmiştir. Bu noktada bireysel farkındalığın da fevkalade önemli olduğunu tekrardan paylaşmak isterim sizlerle. Ancak biliyoruz ki toplumumuzun çok büyük bir kesimi, çok büyük bir bölümü, veri güvenliği konusunda hakikaten yeterli farkındalıkta maalesef değil. İnsanların sosyal medya ortamlarında fark etmeden verebilecekleri güvenlik açıklarının nasıl mahremiyet sorunlarına yol açabileceğini gösteren popüler örnekleri her zaman her gün ve her daim birlikte gözlemliyoruz. Şifrelerini kolay tahmin edilebilir şekilde oluşturanlar, anti virüs yazılımlarından haberdar olmayanlar veya bunlara yapacağı yatırımı gereksiz bulan kurumlar var. Sonuçta dolandırıcılık amaçlı tuzaklara düşenlerin hikâyelerinde maalesef zaman zaman üzülerek okuyoruz veyahut da dinliyoruz. Bu durum, tabi ki bireyden, firmalara ve daha geniş çaplı olarak kamu kurumlarına, devletlere kadar halka halka da büyüdüğünü görüyoruz. Şirketler açısından bakıldığı zaman, koruyucu teknolojilere yatırım ve kurumsal farkındalık kritik gerçekten bir önemde. Siber saldırılar karşısında güvenlik çözümlerinin de mutlaka ve mutlaka kuvvetlendirilmesi gerekiyor.

En başta belki de fabrika yönetim sistemleri, fabrikadaki makineleri yöneten yazılımların güvenli olması gerekiyor sevgili dostlar. Bunun için kullanılan işletim sisteminin güvenliği de fevkalade elzem. Birçok üretim yapılan alanlarda, fabrikalarda üretim sahasını ve siber fiziksel sistemleri kontrol eden bilişim ekipmanları şüphesiz var ancak bizim bu ekipmanlardaki sistemlerin siber ataklardan korunmasını da mutlak sağlamamız gerekiyor. Bakın bu nedenle siber güvenliğin ihtiyaç duyduğu altyapı, sanayide kullanılan siber fiziksel sistemler için de büyük bir önem taşıyor. Milli güvenli işletim sisteminin donanım ve siber güvenlikli yazılımların buradaki rolü gerçekten son derece önemli. Böyle bir sistem, dijital dönüşüm sürecinde üretim altyapısının korunması, üretimin sürekliliğinin sağlanması ve kalitesinin standartlaşmasında da fevkalade önemli roller oynamakta.

Çok değerli konuklar, bugün artık siber saldırıya uğrar mıyım, geçerli soru değil. Bugün bizim çözümü için kafa yorduğumuz bütün sorular, siber saldırıya uğramamak için neler yapmalıyım olmalı ve böyle bir saldırıya uğradığımda ne yapacağım, daha fazla olmalı hatta.

Bugün etkinlik boyunca ele alınacak birçok konu, belki bazılarımızı tedirgin edebilir sevgili dostlar, profesyoneller olmasına rağmen. Ancak unutmamamız gerekir ki bugün günlük hayatımızın vazgeçilmezi olan birçok teknoloji de çok değil bundan 10 yıl önce birçoğumuz için sanki bir bilimkurgu masalı gibiydi veya filmi gibiydi. Evet dünya yepyeni bir Rönesans yaşıyor, böyle bir çağda Türkiye'nin en büyük avantajı şüphesiz yenilikçi ve Türk iş dünyasının genç dinamik ve değişime açık, Türk toplumunun yeni teknolojilere ve değişime uyum sağlama iştahı ve gücüdür.

Bu değerli etkinlikte emeği geçen herkese ben de tekrardan canı gönülden teşekkürlerimi paylaşıyorum. Konferansın, toplumumuzun bilgi güvenliği konusundaki farkındalık süreçleri başta olmak üzere, bütün katkıları sağlaması temennisiyle, hepinizi bir kez daha TÜSİAD yönetim kurulu adına sevgi ve saygıyla selamlıyorum. Tekrardan çok çok teşekkürler.

Sunucu

Sayın Erol Bilecik'e konuşmaları için teşekkürlerimizi sunuyoruz. Sayın konuklar, açılış konuşmalarının ardından "Yapay zekâ ve siber güvenlik, gerçek mi yoksa abartı mı?" başlıklı konuşmasını yapmak üzere, Lastline Kurucu Ortağı ve Northeastern Üniversitesi Öğretim Üyesi Sayın Prof. Dr. Engin Kırda'yı sahneye davet ediyoruz.

Prof. Dr. Engin Kırda

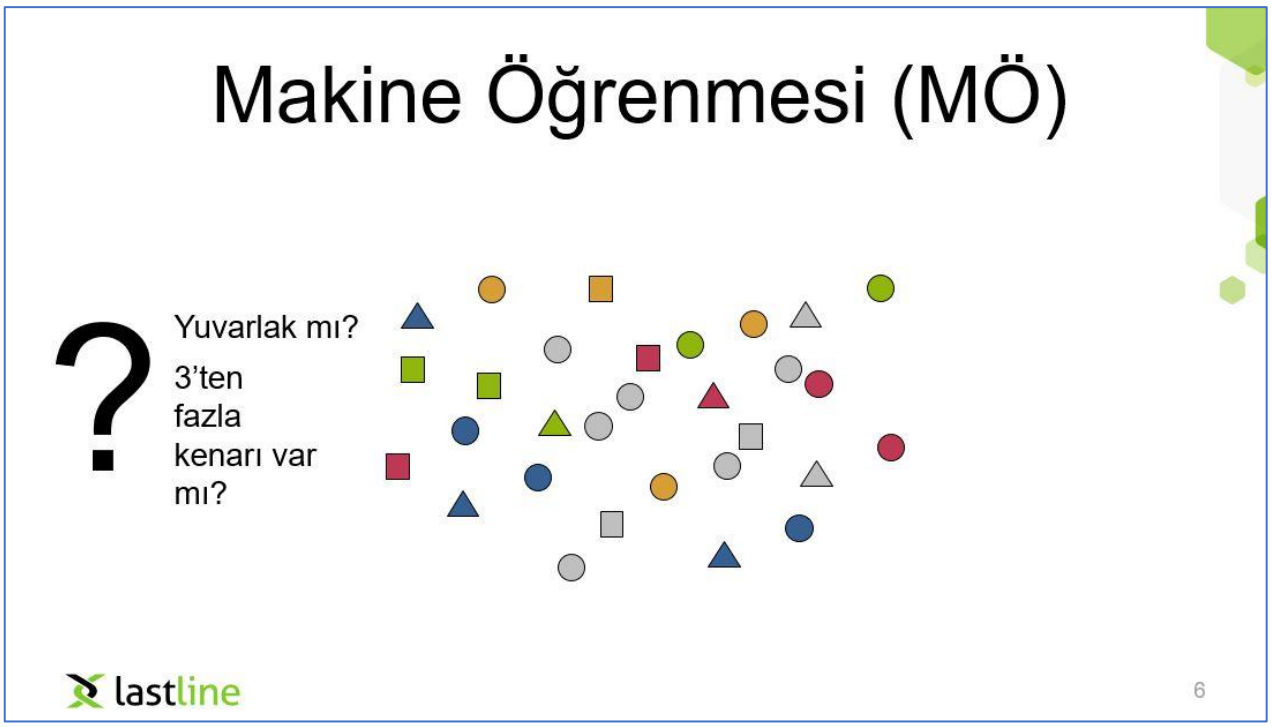
Prof. Dr. Engin Kırda (Lastline Kurucu Ortağı ve Northeastern Üniversitesi Öğretim Üyesi)

Herkese iyi günler, ilk önce TÜSİAD'a ve Bilkent'e bu davet için teşekkür etmek istiyorum. Benim sunumum yapay zekâ konusunda olacak. Son zamanlarda çok sık duyduğumuz bir konu bu, herkes yapay zekâ hakkında konuşuyor. Dünyayı değiştireceğinden bahsediyor. Biraz daha detaya girip, yapay zekanın aslında genelde ürünlerde veya siber güvenlikte ne olduğu konusunda biraz konuşmak istiyorum. Ve aslında bu alandaki biraz sorunlara değinmek istiyorum. Maalesef siber güvenlikte her derde deva olan çözümler yok, çözümler kolay değil her zaman. Burada sorunlar nelerdir, biraz o konulara girmek istiyorum. İlk önce biraz ön bilgi vereyim kendim hakkında. Ben Northeastern Üniversitesinde öğretim üyesiyim,

yaklaşık 10 yıldır zararlı yazılımlar konusunda araştırmalar yapıyorum. Benim çok ilgi duyduğum alanlardan bir tanesi ama genel olarak sistem güvenlikçiyim, yani pratik olan her türlü güvenlik sorununa aslında ilgi duyuyorum. Bu yaptığımız üniversite araştırmamızın sonucu olarak, Anubis ve Wepawet gibi bazı sistemler yaptık. Zararlı yazılım konusunda çalışanlarınızın belki duymuş olacağı sistemlerdir. Bunlar popüler olduktan sonra bize birçok şirketten talep gelmeye başladı, biz bunları kullanmak istiyoruz, bize verebilir misiniz diye. Biz de üç arkadaş; diğer iki arkadaşım Kaliforniya Üniversitesinde, Santa Barbara'da öğretim üyeleri, Lastline'ı kurduk. Şu anda sıfır gün zararlı yazılım saldırılarına çözüm sunan bir şirketiz. Yani kompleks, önceden görülmemiş tarzda zararlı yazılımları nasıl bulabiliriz, bunları daha etkin bir şekilde nasıl engelleyebiliriz, genelde bu alanlarda çalışıyoruz. Ve aslında uzun yıllar üniversitede yaptığımız araştırmalar üzerine kuruldu Amerika'da. Ve kanımca üniversitede yapılan işlerin de normalde pratikte endüstride ve özel şirketler için de işe yarayabileceğinin güzel bir göstergesi.

Bugün yapay zekâ dendiği zaman, aslında çoğunlukla insanlar makine öğrenmesi konusundan konuşuyorlar. Yapay zekâ konu olarak çok eski bir konu. Son 30 yıldır, son 40 yıldır insanların araştırmalar yaptığı bir konu, yani yeni bir şey değil. Ama son zamanlarda özellikle makine öğrenme konusunda, yani bazı algoritmalarda gelişmeler oldu. Şu anda daha çok bilgi toplamaya başladık, elimizdeki donanımlar daha iyi olmaya başladı, yani bu bilgileri daha iyi analiz edebiliyoruz. Bunun sonucu olarak birçok algoritma çıkmaya başladı ve özellikle derin öğrenme gibi yeni algoritmalar daha çok ve yeni teknikler ilgi çekmeye başladı. Onun için bugün birisi size ürününde aslında yapay zekâ falan kullandığını söylüyorsa, büyük ihtimalle makine öğrenmesinden bahsediyor ve bilgisayarların düşünmeye başlayıp da bir şeyler hissetmeye başladığı günler falan aslında bana sorarsanız hiç de yakın değil, bayağı uzakta. Ama makine öğrenmesi, pratikte bayağı ilginç sonuçlar doğurmaya başladı. Makine öğrenmesi peki nedir? Matematiksel ve istatistiksel yöntemler kullanılarak aslında verilere bakıp, bu veriler konusunda bazı kararlar vermek oluyor. Yani bazı tahminlerde bulunabiliyoruz. Önceden gördüğümüz şeylerden öğrenerek, görmediğim, yeni gördüğüm şeyler hakkında bazı kararları otomatik olarak verebiliyorum. İngilizcede machine learning deniyor tabi. Ve aslında bunlar algoritmalar ve hüristikler, yani sezgisel teknikler. Ve aslında burada bilimden bahsediyoruz, matematikten bahsediyoruz, yani yapay zekayla, zekayla falan pek bir ilgisi yok bunun.

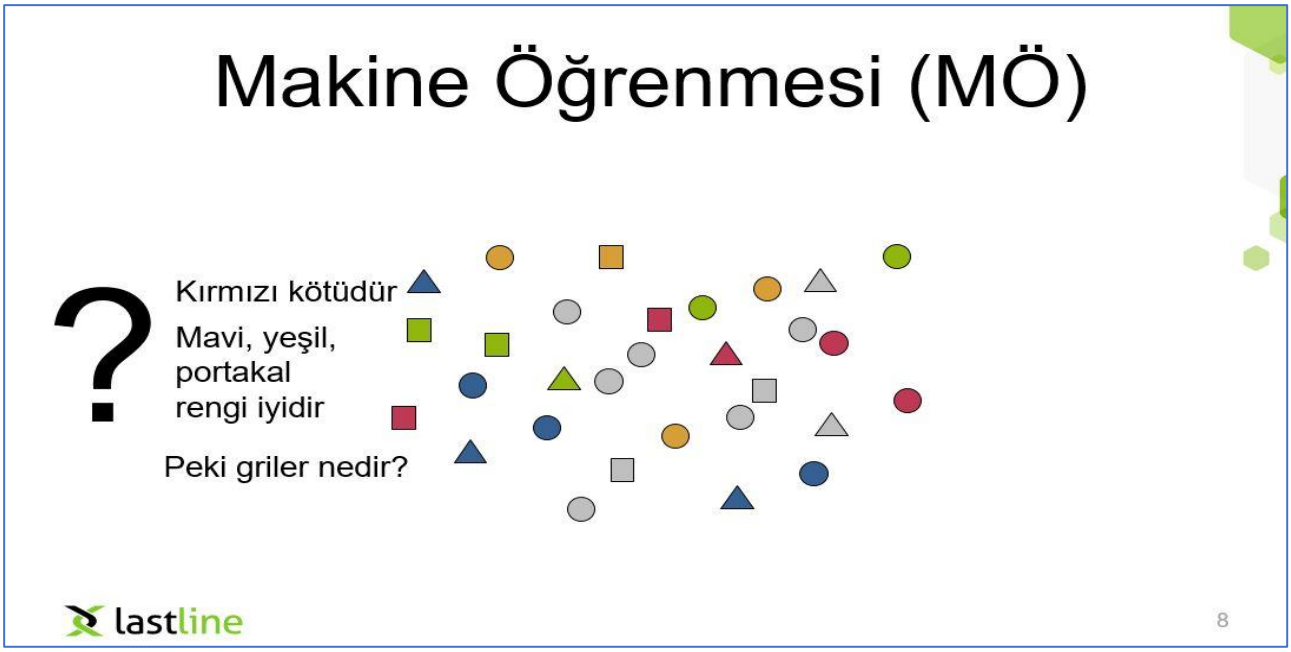
Peki makine öğrenmesi ne aslında, yapay zekâ dediğimiz şeyi niye çok duyuyoruz? Çünkü bu veri analizini destekliyor ve günümüzde herkes çok fazla veri toplamaya başladı ve makine öğrenme teknikleri, bu verileri analiz etmede, bunları gruplamada, kümelemede çok çok etkili ve aynı zamanda sınıflandırmayı destekliyor. Yani ben önceden gördüğüm şeylerden öğrenip de yeni gördüğüm şeyler hakkında bazı kararlar verebiliyorum, bunları bazı gruplara koyabiliyorum. Tabi bu da bilgisayar açısından, programlar açısından, ürünler açısından ilginç olmaya başlıyor. Peki makine öğrenmesi aslında nedir?



Şekil 1 Makine öğrenmesi-1

Şöyle bir örnek vereyim size; (Şekil 1) farz edelim ki bütün bu verileri bir şekilde gruplandırmam gerekiyor, makine öğrenmesi teknikleri kullanarak ilk önce bazı özellikler tanımlamak zorundayım. Mesela şöyle bir soru sorabilirim, derim ki yuvarlak mı, eğer yuvarlaksa o zaman elimdeki veri daire olur. Başka soruları da şöyle sorabilirim, üçten fazla kenarı var mı, yok mu diye. Aslında şurada yaptığım bu algoritmaya bazı özellikler öğreterek, sonra benim için otomatik olarak bazı şeylere karar vermesini sağlamak. Yani algoritmamı çalıştırdığım zaman, bu verileri verdiğim zaman bu özellikleri kullanarak algoritma otomatik olarak üçgenleri belli bir yere koyacak, kareleri belli bir yere koyacak ve daireleri belli bir yere koyacak. Ve buradaki avantaj da bunu elle yapmak zorunda değilim, burada insana ihtiyacımız yok. Bunu algoritmama veriyorum, çok fazla veri veriyorum, önceden öğrettiğim özelliklerle bunu benim için otomatik olarak hallediyor.

Bir başka yapabileceğimiz bir şey makine öğrenmesiyle, sınıflandırmak. Biraz önce yaptığım kümelemeydi, otomatik olarak bu elimdeki verileri belli gruplara ayırdım ve makine öğrenmesi bu tür şeyler için çok çok ideal bir şey. Başka yapabileceğim şey şöyle olabilir; mesela sorarım, derim ki veya tanımlarım (Şekil 2), kırmızılar kötüdür derim, kötü ne demekse, bunu bir güvenlik aplikasyonu olarak düşünün, kırmızıların kötü olduğuna karar verdik. Ve kırmızı örnekler var elimde. Aynı zamanda mavi, yeşil, portakal rengi iyidir diyorum. Bunlar da elimdeki örneklerden karar verdiğim bir şey.



Şekil 2 Makine öğrenmesi-2

Bunu makine öğrenme tekniğimize öğretiyoruz ve şimdi algoritmamı çalıştırdığım zaman, verilere, bunları git de görmediğim şeyler hakkında karar ver dediğim zaman, ilk önce bir öğrenme aşaması var ve griler hakkında bir şekilde karar vermek istiyorum ama otomatik karar vermek istiyorum. O zaman başlangıçta diyoruz ki kırmızıların hepsi kötüdür, yani bunu öğretiyoruz algoritmaya. Sonra diyoruz ki maviler, portakal rengi ve yeşiller iyidir, bunu da algoritmamız öğrendi. Şimdi teker teker, önceden görmediğim bir şeyler karşıma çıkarsa, veriler karşıma çıkarsa, şimdi algoritmaya soru sorabiliyorum. Diyorum ki bu nedir, özelliklerine bakarak bunu kırmızıyla daha yakın bulduğu için algoritma diyor ki bu kötüdür diyor. Bir başkasına bakıyoruz, bunun iyi olduğuna karar veriyor otomatik olarak, sırf özellikler ve önceden öğrettiğimiz şeyleri kullanarak. Yani teker teker önceden görmediğimiz şeyleri bir şekilde sınıflandırma bize kapasitesini vermiş oluyor. Ve tabi bunu güvenlik açısından düşünürseniz bu ilginç bir şey çünkü bir şeyin iyi veya kötü olduğunu otomatik olarak görebiliyorsam, önceden öğrendiğim örneklere dayanarak, bu avantajlı bir şey olabilir çünkü bu tür şeyleri günümüzde veya daha çok geçmişte insanlar yapıyordu. Bir şeye bakıp da bu kötü mü iyi mi diye insanlar karar vermek zorundaydı ama biz bunu otomatik hale getirmek istiyoruz ve makine öğrenmesi için bu tür şeyler için aslında bayağı ideal bir şey. Yani son zamanlarda kullanılmasının sebeplerinden bir tanesi de bu.

Şimdi siber güvenlik konusunda nesne ve olaylar çok oluyor, değil mi, kurumlarda bilgileri topluyoruz, bilgilere giden insanlar nereye bağlanıyor, hangi web sitelerine bağlanıyorlar, neler yapıyorlar, bunlar elimizdeki bilgiler. Bunları gruplandırabilmek, bunlar hakkında bir karar vermek avantajlı bir şey, onun için siber güvenlik için makine öğrenmesi popüler olmaya başladı.

Gözlemlere dayanarak otomatik sınıflandırıcı yaratabiliriz ve önceden gördüğüm saldırıları mesela öğreterek, yeni gördüğüm şeylerin saldırı olup olmadığına belki otomatik olarak karar veriyor derim ki bu da avantajlı bir şey olur. Yani makine öğrenmesini kullanırsak siber güvenlikte, o zaman insanın analiz ve karar yeteneğine duyulan ihtiyacı azalır. Önceden duyduğunuz gibi bu alanda çok yeterli, kalifiye eleman olmadığı için, birçok şeyi otomatize edebilirsek, bu büyük bir avantaj. Onun için makine öğrenmesine duyulan ilgi arttı ve bu alanda çok daha fazla çalışmalar yapılmaya başladı. Ama şunu da söyleyeyim, bunlar yeni çalışmalar da değil, son 15-20 yıldır makine öğrenmesi aslında siber güvenlikte çok kullanılan bir şeydi ama son zamanlarda ürünlerde de görmeye başladığımız için ve pazarlama da çok sık duyduğumuz için yapay zekâ makine öğrenmesini artık herkes neredeyse duymaya başladı. Oysa o kadar da yeni bir şey değil.

Peki makine öğrenmede zorluklar var mı, yoksa makine öğrenmesi yapıyorum dediğim zaman bütün bu sorunları otomatik olarak çözebiliyor muyum? Özellikle pazarlama şirketlerinin çok çok sık yaptığı bir şey, makine öğrenmesi var, onun için biz sizi çok güzel koruyoruz gibi şeyler söylemeleri. Ya da bizim çözüm başka çözümlerden daha iyi çünkü biz yapay zekâ kullanıyoruz demeleri. Peki bu doğru mu? Burada bazı sormanız gereken sorular var. Birincisi, elinizdeki veriler ne kadar iyi? Sonuçta bir şeyi öğretmeniz gerekiyor algoritmalara, onun için ne öğrettiğinizin, nasıl öğrettiğinizin çok büyük bir önemi var burada. İkincisi, kullandığınız veri özellikleri ne derece kaliteli? Bir şeyi öğretmek için bu tekniğe, bir özellikler öğretmeniz lazım, yanlış özellikleri öğretiyorsanız o zaman etkili olmayabilir ya da yanlış şeyleri bulmaya başlayabilir sizin için. Mesela zararlı yazılımlar bugün çok hızlı bir şekilde değişiyorlar, siz sırf görünüme göre bir şey öğretirseniz o zaman aslında bu pek efektif, iyi bir çözüm olmuyor. Kullandığınız algoritmalar ne derece iyi? Çok değişik teknikler var burada. Bir kullandığınız teknik başka bir alanda o kadar işinize yaramayabilir ya da o kadar iyi sonuç vermeyebilir. Ve kullandığınız makine öğretim yaklaşımı, değişime ne kadar dirençli? Bugün yaptığınız bir şey bir yıl sonra aslında bugün kadar iyi çalışmayabilir. O da bir sorun ve bunu da düşünmek zorundasınız.

Makine öğrenmesinde bazı sihirler var tabi, bunlar bir şekilde bu verileri veriyorsunuz, makine öğrenme tekniği bunları öğreniyor, sizin için bazı kararlar veriyor. Peki bu nasıl çalışıyor? Şöyle bir örneğe bakalım. Hepinizin bildiği Google, Facebook gibi sitelerde bazen resimleri aratabiliyorsunuz değil mi, otomatik olarak aradığınız resimleri size çok güzel bunlar sunuyorlar. Bunlar nasıl çalışıyor?

Genel olarak birçok resim üzerinde bazı şeyler, bazı özellikler öğrenilerek çalışıyor. Mesela algoritmama ben bu kedidir diyorum (Şekil 3), şu kedidir diyorum, bu kedidir ve bu kedidir diye öğretiyorum.

Şekil 3 Makine öğrenmesindeki sihir-1

Binlerce, milyonlarca kedi resmini öğrettikten sonra algoritma bazı özellikleri anlamaya başlıyor, yani öğrenmeye başlıyor. Ve bilmediğim bir resim geldiği zaman, bu nedir dediğim zaman, algoritma otomatik olarak bu kedidir diyor bana. Şu anda burada bir sorun yok, bu Google, Facebook örneği. Ve burada bir saldırgan yok, yani burada pek bir sıkıntı yaşamıyoruz genelde. Ama siber güvenlik durumuna, öyle bir aplikasyon uygulamanız varsa şöyle bir sorun ortaya çıkabilir; dersiniz ki bu kedi ve saldırgan bir resim koyar oraya, bu aslında kedi değil ama kediye benzeyen bir insan, bu da kedi, yine kediye benzeyen bir insan var. Yani veriyi kirletmeye başlarsınız saldırgan olarak. Ve sizin makine öğrenme tekniğinize sorduğu zaman, bu nedir dediği zaman, çocuk olmasına rağmen bu da kedi diyebilir size. Yani makine öğrenme tekniklerinin de tabi ki sınırları var ve herkesin belki söylediği kadar da dünyayı tamamen değiştirecek şeyler olmayabilirler, bazı sıkıntılar var (Şekil 5).

Bir başka örnek de bu kedi diye öğretirsiniz, bu kedi dersiniz, bu kedi bu kedi, yani gördüğünüz gibi buradaki verilerde hepsi kedi, burada bir sıkıntı olmaması lazım, değil mi? Ama şu resmi sorduğunuz zaman algoritma size bu da kedi diyebilir. Peki bu niye oluyor çünkü bu resimde saldırgan bütün kedi özelliklerini almış, yani burnu kediye benziyor, kulaklar kediye benziyor, kuyruğu var ve algoritma bunları öğreniyorsa ki zaten buna benzer şeyler öğreniyor, o zaman bunun da kedi olduğunu düşünebilir. Yani bir saldırgan makine öğrenme teknikleriyle oynayarak ya da bazı şeyleri sizin öğrendiğiniz şeylere benzeterek saldırıları yine aktif hale getirme imkânı doğurabilir (Şekil 4).

Şekil 5 Makine öğrenmesindeki sihir-2

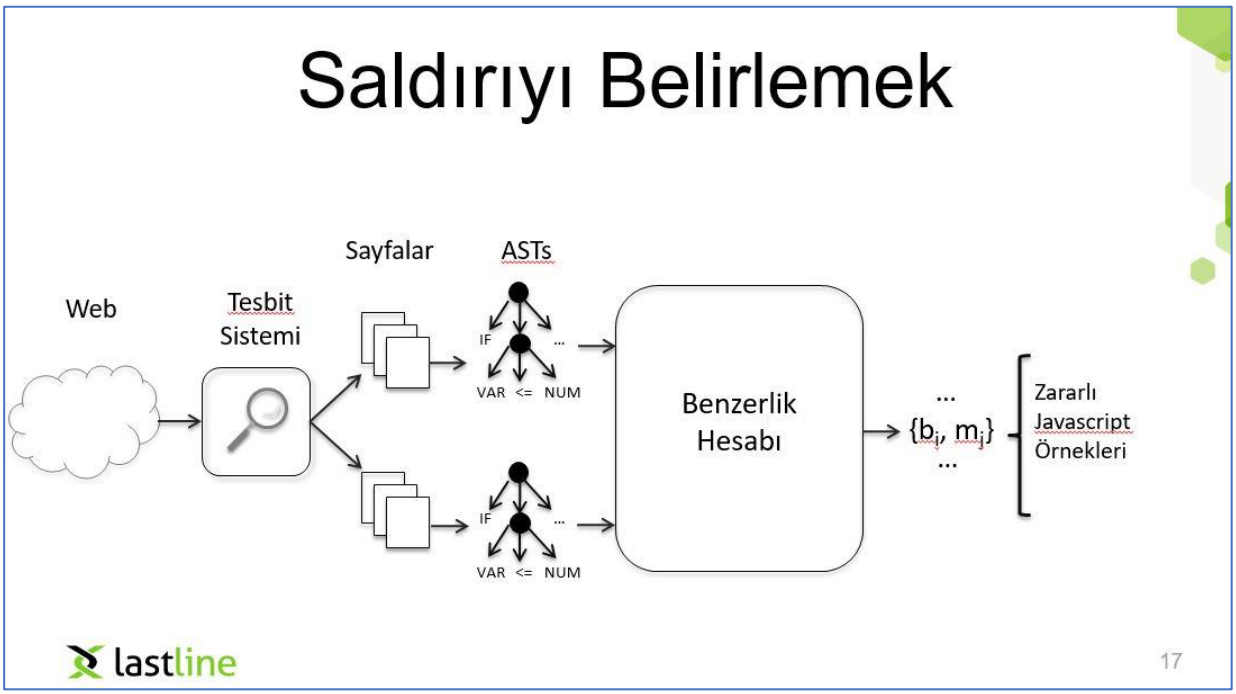
Şekil 4 Makine öğrenmesindeki sihir-3

Son zamanlarda, henüz herkesin çok konuşmadığı yeni yeni araştırma alanları ortaya çıkmaya başladı. Bir tanesi, saldırgana rağmen makine öğrenmesi. İngilizcede "aggressive machine learning" denilen bir alan. Çok çok yayınlar çıkmaya başladı. Bunu henüz ürünlerde falan görmüyoruz, insanlar çok klasik makine öğrenmesi yapıyorlar. Saldırganların ne

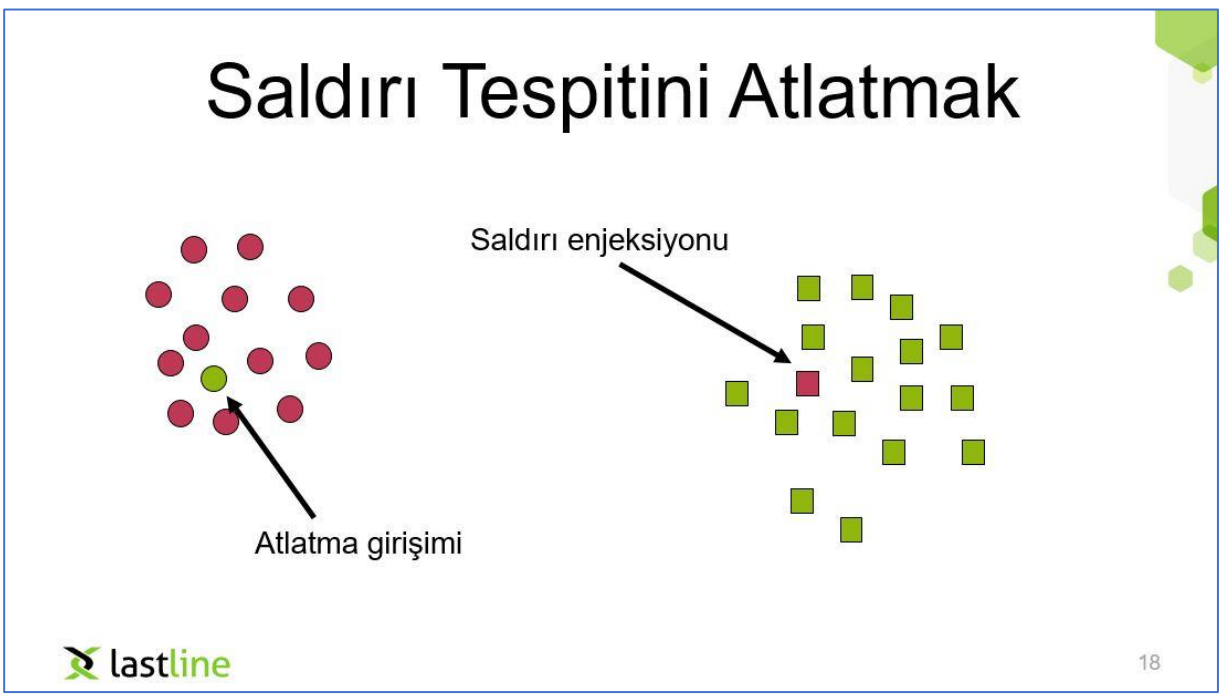
yapacağını şu anda pek düşünmüyorlar. Ama burada olay, saldırganın verinin bir kısmıyla oynayabilmesine rağmen, bir şekilde öğrenme yapmak, etiketleme, sınıflandırma yapabilmek. Yani buna rağmen makine öğrenme nasıl yapılır, bu konuda yapılan çalışmalar var. Yani saldırgan verinizi kirletebilir, ürettiğiniz modelleri çalabilir, saldırıyı ürettiğiniz sınıflandırma modellerine göre her şeyi değiştirebilir, biraz önce verdiğim örnekler gibi. Yani çok ileride önemli olacak alanlardan bir tanesi ve ürünlerin, özellikle siber güvenlik ürünlerinin bunu düşünmesi gerekiyor. Bildiğiniz, her zaman duyduğunuz klasik makine öğrenmesi olmuyor. Bir örnek, sürücüsüz arabalardan bahsedildi. Şu anda bunların en büyük sıkıntılarından bir tanesi, araba kendi kendine giderken makine öğrenmesiyle çevresindeki nesneleri tanımaya çalışıyor. Ve son çıkan yayınlarda, makineye yanlış fikir verilebiliyor. Mesela size göre ışık kırmızı gibi görünüyor ama modelleri ona göre yapabilirseniz alet veya araba ışığın yeşil olduğunu zannediyor ve devam ediyor ve böyle tehlikeli tarzda saldırılar ileride büyük ihtimalle daha çok ortaya çıkacak.

Peki biz ne yapabiliriz, makine öğrenmesinin böyle sınırları varsa? Veri kirliliğini önlemek için veriyi filtrelemek gerekiyor, yani bir şeyi öğrenirken o veri ne derece kaliteli, bunu bir şekilde yapmanız lazım. Saldırının gerçek özelliklerini açığa vuran davranışları ortaya çıkarmanız lazım. Yani saldırıda ben bir şeyi buluyorum ama hangi özelliklere bakıyorum, burada zararlı koda mı bakıyorum, belli davranışlara mı bakıyorum, birisinin bir yerden bir yere nasıl bağlandığına mı bakıyorum. Bunları bir şekilde bilmem lazım ve iyi özellikler bulmam lazım. Ve analiz atlatan saldırıları tanımlamak için çoklu sınıflandırma ve kümeleme kullanmam gerekiyor, yani saldırgan benim analiz yaptığımı bilebiliyor ki son zamanlarda görülen saldırılarda, saldırganların hiç de aptal olmadığını görüyoruz. Bu tür sistemlerin kullanıldığını biliyorlar ve saldırılar daha komplike hale gelmeye başladı. Yani bir makine öğrenme tekniği kullanacağıma belki birçok makine öğrenme tekniği kullanmam gerekiyor ve bir tek makine öğrenme değil, başka şeyler de kullanıp bunları birleştirmem gerekiyor.

Bir örnek olarak size bizim son zamanlarda uğraştığımız bir şeyden bahsedeyim. Mesela ilk videoda “drive by” tarzı saldırılardan bahsedildi. Bir web sitesine gittiğiniz zaman orada zararlı kod olabiliyor, javascript, çalıştığı zaman sizin tarayıcınız içinde size bir şey yüklenmesi sağlanıyor. Bu tür saldırıları tanımak için elimizdeki örneklerden yola çıkarak, benzer kodları arıyoruz. Bir kod eğer zararlıysa ona benzer zararlı kodları görüyoruz, yani benzerlik hesabı (Şekil 7) denilen tarzda analizler yapmamız mümkün. Eğer gördüğüm bir şey kötüyse, ona benzer bir kod varsa, büyük ihtimalle o da kötüdür.



Şekil 7 Saldırıyı belirlemek



Şekil 6 Saldırı tespitini atlatmak

Ama biz son zamanlarda bu tür şeyleri makine öğrenmesiyle kombine etmeye başladık. Mesela ben bu kodlara bakıp (Şekil 6) da bunları makine öğrenmesiyle kötü iyi diye değişik gruplara ayırmış olabilirim. Ama iyi dediğim kodlardan bir tanesi kötü kodlara benziyorsa,

demek ki orada makine öğrenmemde bir sorun var ve beni atlatmış demek oluyor. Yani benzerlik hesabıyla makine öğrenimini kombine edip de daha iyi sonuçlar almamız mümkün ve aynı şekilde eğer kötü olarak tanıdığım bir şey iyi koda benziyorsa, belki iyi bir kod alınıp da onun içine saldırı enjekte edilmiş de anlamına gelebilir. Yani makine öğrenmesinin iyi olmadığından yola çıkarak, bazı şeyleri kombine ederek daha iyi sonuçlar almaya çalışıyoruz.

Lastline'da makine öğrenimini son zamanlarda çok çok kullanmaya başladık. Bunu kara listelerin otomatik üretiminde yapıyoruz, trafik tanıma sistemlerinin otomatik üretiminde yapıyoruz. Yani bilgisayar ağında ne olup bittiğini tanımlayabilmek için otomatik olarak, önceden öğrendiğimiz şeylerden yola çıkarak bazı kararlara varabiliyoruz otomatik olarak. Trafik modellerini otomatik üretebiliyoruz. Yani saldırıya benzeyen bir şeyi önceden gördüysek, bundan öğrenip yeni görmediğimiz şeyleri bulmaya çalışıyoruz. Ve zararlı yazılım sınıflandırmasını yapıyoruz. Bugün herhangi bir güvenlik şirketinin eline günde belki 200 bin tane, şimdiye kadar görmediği zararlı yazılım geçiyor. Bunların otomatik olarak analiz edilmesi şart çünkü bunu elle yapmak istediğiniz zaman maalesef bu yeterli olmuyor, yeterli insan kapasiteniz yok, yeterli zamanınız yok. Yani bu zararlı yazılımları makine öğrenmesiyle otomatik olarak değişik gruplara koymaya çalışıyoruz. Hangi aileye benziyor, bir önceki gördüğümüz şeye benziyor mu, bu tür şeyleri sınıflandırıp gruplar oluşturmaya çalışıyoruz. Ve bilgi tabanında kullanıcılarımız, özellikle daha teknik olanlar bu tür bilgileri arayabiliyorlar ve benzer örneklerin ve saldırıların özelliklerini görebiliyorlar. Belli kurumlarda görülen saldırı örneklerini başka kurumlarda görülmüş mü, o tür testler yapmaları mümkün. Yani bu bilgi tabanına her şeyi makine öğrenimi kullanarak da aktarmak ve burada ilginç analizler yapmak da mümkün oluyor. Bir başka alan da çok ilgi duyulan ve ileride daha önemli olacak alanlardan bir tanesi, otomatik ağ analizi.

Makine öğrenimi aynı zamanda bilgisayar ağlarında anormallik tespiti dediğimiz teknikler için de çok verimli ve yararlı. Anormallik tespiti, İngilizcede "anomaly detection" dediğimiz fikir de aslında çok eski bir fikirdir, son 20-30 yıla dayanan bir fikirdir. Ama son yıllarda tekrar ürünlerde bunu görmeye başladık. Çünkü kullandığımız klasik anti virüs teknikleri işe yaramıyor çünkü onların genel olarak yaptığı, bildiğimiz saldırıları tespit etmek ama bugünlerde şimdiye kadar hiç görmediğimiz saldırıları görüyoruz ve bu saldırıların neye benzediğini de görmediğimiz için tespit etmemiz mümkün olmuyor. Onun için anormallik tespiti daha çok ilgi çekmeye başladı.

Burada iki tane kullanabileceğiniz yöntem var. Birisi yanlış kullanım yöntemi, diğeri de anormallik tespiti. Yani yapabileceğiniz şey, kötü olanı modellemek olabilir. Bu çok eski bir fikir ve çoğu çözüm zaten bununla çalışıyor. Kötü olan şeyleri modelleyip, eğer sizin kurumda bu kötü aktiviteleri görüyorsanız bu kötüdür diye tespit etmeniz mümkün olabiliyor.

Şekil 8 Yanlış kullanıma karşı anormallik tespiti

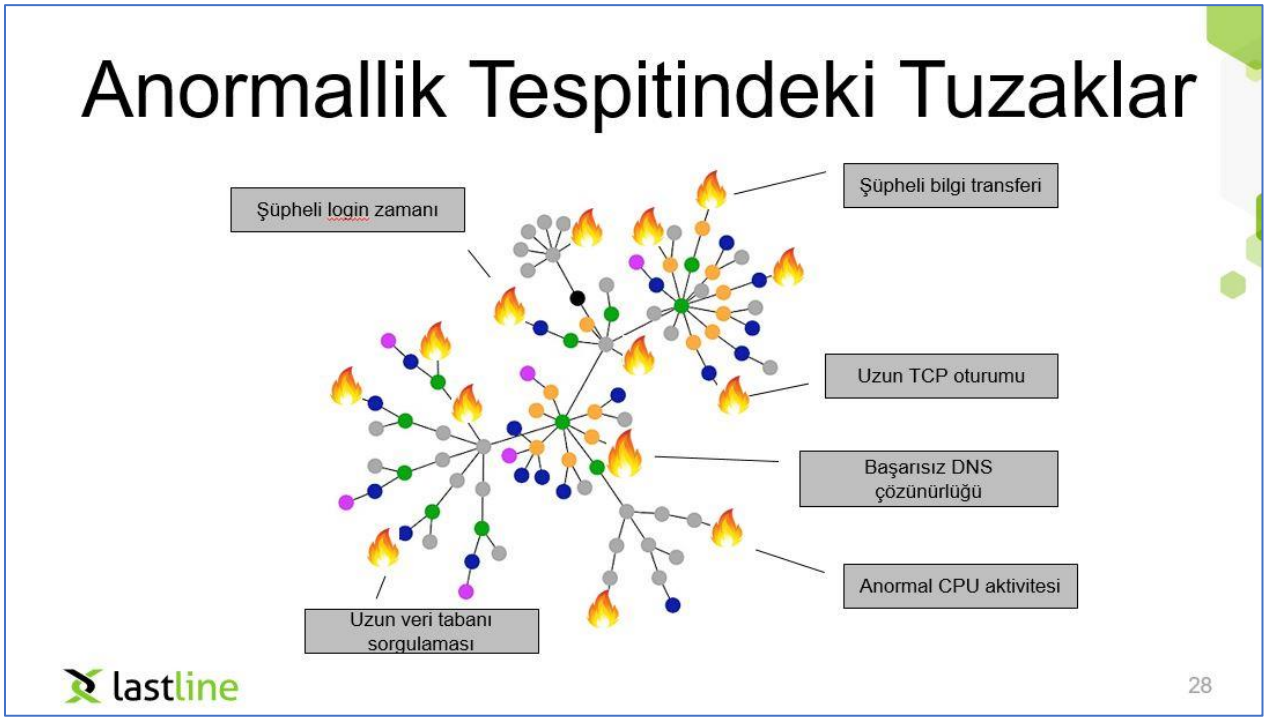
Bir başka fikir, biraz daha yeni olan fikir de anormallik tespiti. Burada iyi olanı modellemek amacınız. Yani ben iyi olan her şeyi modelleyeyim, bunun dışına çıkış olursa anormallik görürsem demek ki bir şekilde bir saldırı oluyor anlamına gelebilir (Şekil 8). Yani iyi olanı modellemek hedef. İyi davranışları modellemek fikir olarak güzel bir fikir ama zaman alan bir şey çünkü bütün iyi davranışlarınızı belki bir gün içinde göstermezsiniz. Ben sizi izliyorsam, yapacağınız her şeyi belki bir hafta içinde yapabilirsiniz. Kesinlikle uzman bilgisi gerektirir çünkü sizin işinizi bilmeyebilirim.

Bir model yaratmak için nasıl çalıştığınızı öğrenmem lazım. Her zaman eksik olur, belki o bir hafta içinde, sizi gözlemlediğim bir hafta içinde yapacağınız her şeyi yapmazsınız, yani hiçbir zaman tamamen bitmiş bir model yakalamam mümkün değil, bu sıkıntılardan bir tanesi. Ve geçerliliği her zaman sınırlıdır. Bugün yaptığınız işi yarın farklı yapmaya karar verebilirsiniz, farklı yapmak zorunda kalabilirsiniz. Onun için bugün yaptığım model yarın geçerli olmayabilir. Ve bu da anormallik tespiti sistemlerinin yaşadığı büyük sorunlar. Her ihtimalde eğer iyi davranışı öğrenmek istiyorsam, bu otomatik olmalı, sürekli yapılmalı, kapsamlı olmalı, yani yapacağınız her türlü iyi davranışı görmek zorundayım. Ve bu da tahmin edeceğiniz gibi zor bir şey. Güvenlikte maalesef yüzde yüzlük çözümler yok. Birisi gelip de size her şeyi çözen bir çözüm buldum diyorsa bu büyük ihtimalle doğru da değildir. Anormallik tespitinde bazı tuzaklar var. Mesela kötü olan anormal görünür düşüncesi. Kaçınız bu adamı tanıdınız bilmiyorum ama Jeffrey Damer (Şekil 9), seri katillerden bir tanesi. Kurbanlarını zaten kandırmasının sebeplerinden bir tanesi de anormal görünüşü olmaması ve kimseyi

Şekil 9 Anormallik tespitindeki tuzaklar- 1

korkutmaması, iyi bir insan gibi görünmesi. Yani bu davranıştan yola çıkarsanız, kötü olan her şey anormal görünür derseniz, bu maalesef siber güvenlikte doğru olmuyor. İkincisi de anormal görünen kötüdür diye. Bu canavar, anormal görünüyor, kötü gibi görünüyor ama aslında "The Goonies" filmindeki iyi kalpli canavar.

Normal bir kurumda anormallik tespiti yaptığınız zaman, birçok bilgi görüyorsunuz, yani sürekli anormal bir şeyler görme ihtimaliniz var. Özellikle büyük kurumlarda bu oluyor. Anormallik tespitini tek başına kullandığınız zaman, mesela şüpheli bilgi transferleri görürsünüz, belki şüpheli CPU kullanımı olabilir, TCP session'ları uzun olabilir, yani bir sürü alarmlar, bir sürü yangınlar görürsünüz kurumda (Şekil 10). Tek başına onun için çok efektif, çok işe yarayan bir teknik değil. Buradaki sorun şu; bu çıkan yangınların her birini ciddiye almazsanız, o zaman eviniz yanabilir. Hepsini ciddiye alırsanız kediyi kurtarırsınız ama çok da vakit harcamış olursunuz. Yani burada bir dilemma var aslında, yani anormallik tespit sistemlerinin en büyük sorunları da bu zaten. Burada da birebir her şeyi çözen, her derde deva bir çözüm aslında yok.



Şekil 10 Anormallik tespitindeki tuzaklar- 2

Peki makine öğrenimini nasıl doğru kullanabiliriz, yani bunu başka şeylerle kombine edebilir miyiz? Son zamanlarda bu alanlarda bazı gelişmeler var. Tespit ettiğimiz saldırılardan modeller çıkarabiliriz, bilinmeyen yeni saldırıları ve davranışları öğrenmeye çalışabiliriz. Yani yapmaya çalıştığımız aslında bu. Makine öğrenimi, yapay zekâ denilen şey her şeyi çözmüyor, anormallik tespiti işe yarayan bir şey ama her şeyi çözmüyor. Bunları kombine edip de daha iyi sonuçlar alabilir miyiz? Her ihtimalde bir saldırı bulduğumuz zaman, amacımız benzer saldırıları bulmaya çalışmak. Yani nasıl olabilir, şu anda uğraştığımız, yaptığımız çözümlerde; siz eğer bir şey bulduysanız, birisi sizin sistemlerden bir tanesini hack ettiyse, bu sisteme günümüzdeki çoğu çözüm ne yapıyor, burada bir sorun var deyip sizi uyarıyor ve işini bitirmiş oluyor.

Bizim şu anda çalıştığımız alanda, araştırma olsun, daha çok ürün olsun, yapmaya çalıştığımız şey, böyle bir saldırı bulduğumuz zaman, bu saldırının neye benzediğini öğrenip de benzer saldırıları kurumda görebilir miyiz? Çünkü böyle bir saldırı olduysa, kurumda büyük ihtimalle ona benzer saldırılar da olmuş demektir. Yani bir saldırıdan yola çıkarak benzer saldırıları otomatik olarak bulabiliyor muyuz? Bugün bu yapılan bir şey değil ama aslında yapmamız gereken bir şey. Bugün çözümlerin çoğu bir şey olduğu zaman sizi uyarıyor ama başka bir şey olana kadar da bir şeyden haberiniz olmuyor. Burada amaç, bir şeyi bulduktan sonra reaktif olmaktansa proaktif olmak. Böyle bir şey buldum, buna benzer başka şeyler var mı demek. Yani bir saldırıdan yola çıkarak birçok saldırı bulmak.

Sonuç olarak, makine öğrenimi ve anormallik tespiti, siber saldırı bulmak için önemli araçlar. Son zamanlarda, eğer konferanslara giderseniz; mesela Black Hat, RSA, bizim alanda bilinen konferanslar, birçok ürünün satıldığı konferanslar. Burada birisine gittiğiniz zaman, ürününüz nasıl çalışıyor diye sorduğunuz zaman, biz yapay zekâ kullanıyoruz, biz makine öğrenimi yapıyoruz, bize güvenin, onun için çok iyi çalışıyor diyorlarsa veya başka alanlarda yine bunu pazarlama aracı olarak kullanıyorlarsa, burada benim tavsiyem biraz dikkatli olmanız. Çünkü yüzde yüzlük bir sistem, yüzde yüzlük fikirler maalesef bilgisayar biliminde yok. Her şeyin çözümü değil, gördüğünüz gibi bazı zorlukları aşmak zorundayız, bunu nasıl yaptığımız önemli. Bu, sorunları aşamayacağımız anlamına gelmiyor ama her şey çözülmüş anlamına da gelmiyor.

Anormallik tespitinin iyi çalışması için makine öğrenimi ile birleştirmek, kanımca mantıklı ve verimli, onun için bu alanda daha çok araştırma yapmaya başladık. Önümüzdeki yıllarda da ilginç sorunlar ve çözümler göreceğiz, özellikle makine öğrenim sistemlerinin de saldırı altında kaldığını göreceğiz. Siz yapay zekâ kullanacaksınız bir nevi, makine öğrenimi kullanacaksınız ama birisi o modellerinizi öğrenip yine başarılı saldırı yapabilecek. Onun için bu sistemlerin gerçekten iyi olup da iyi tasarlanması gerekiyor. Umarım amaç, tuzak kurup da bir şeyleri yakalamaktan, avlanmaya doğru geçecek, bizim de hedefimiz bu. Şu anda önümüzdeki birkaç yılda bu alanda daha çok işler yapabileceğimizi umuyoruz. Teşekkür ederim. Sorularınız varsa buralardayım.

Sunucu:

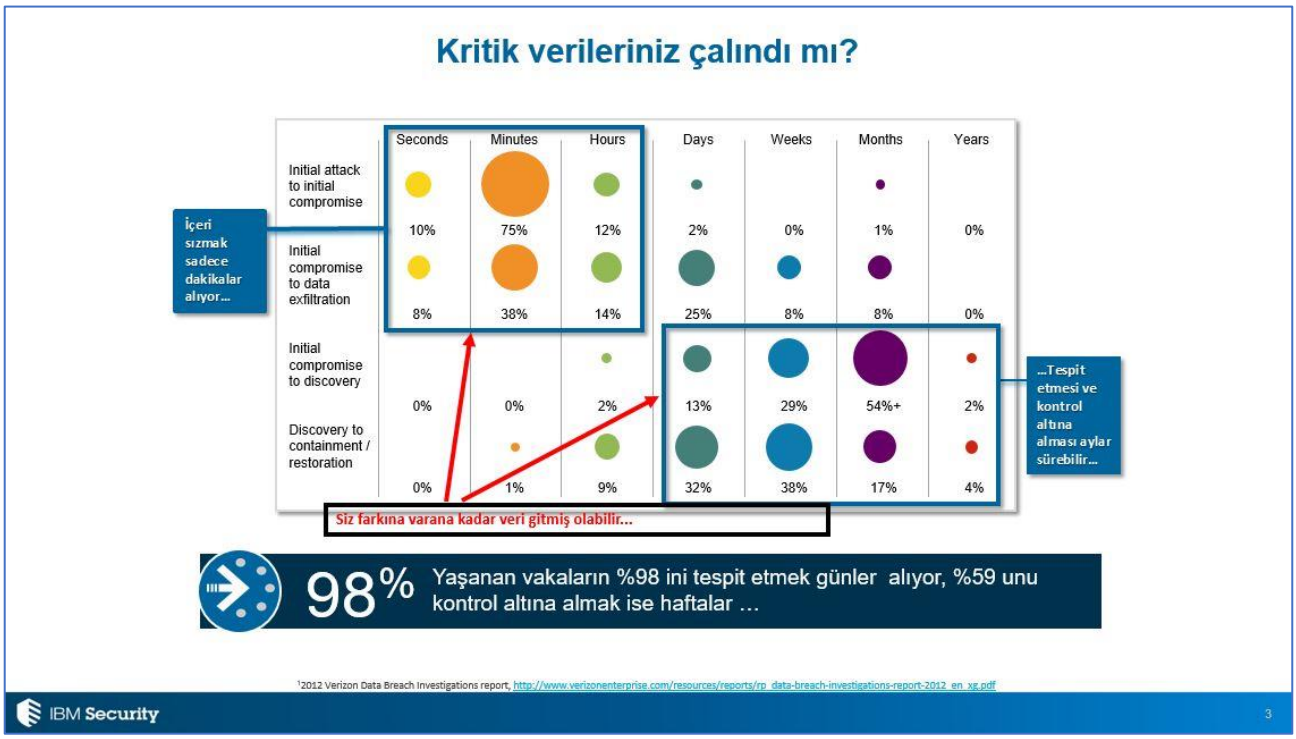
Sayın Engin Kırda'ya konuşması için teşekkürlerimizi sunuyoruz.

Sayın konuklar, şimdi ise "Gone in 60 Seconds, bir sonraki siber saldırıya hazır mısınız?" başlıklı konuşmasını yapmak üzere, IBM Türk Güvenlik Ülke Lideri Sayın Engin Özbay'ı sahneye davet ediyoruz.

Engin Özbay:

Engin Özbay (IBM Türk Güvenlik Ülke Lideri)

Evet, sunumumun başlığı, "bir sonraki siber saldırıya hazır mısınız?" Çünkü biz bu salonda otururken aslında şu anda şirketlerimiz saldırı altında. Belki bir kullanıcınız yanlış bir linke tıkladı, belki internet üzerinden saldırı alıyorsunuz ve bu devamlı olan bir şey. O yüzden şu ankine değil, bir sonrakine hazır mısınız diye başlamak istiyorum. Peki, küçük bir senaryoyla başlayalım. Bir şirketin IT bölümünde çalışan bir yönetici olduğunuzu düşünün. Sabah işe geliyorsunuz, şirketiniz büyük bir holdingin parçası. Türkiye'de çok büyük işler yapıyorsunuz, grup şirketleriniz var. Sadece Türkiye'de de değil, Avrupa'da da şirketleriniz var, satın almalar yaparak büyüyorsunuz. İşler çok iyi gidiyor, fabrikalarınız var. Sabah işe geliyorsunuz, oturuyorsunuz, kahvenizi koyuyorsunuz. Ve telefon çalıyor. Arayan kişi, şirket içinden bir çalışan ve diyor ki ekranımda bir mesaj var ve bana bitcoin denen bir şeyle para ödememi istiyor. Verilerime erişemiyorum. Bunu araştırmaya başlıyorsunuz.



Şekil 11 Kritik verileriniz çalındı mı?

Sonra ekibiniz devamlı telefon almaya başlıyor, benzer mesajları birçok kişiden alıyorsunuz. Bir müddet sonra daha önemli bir telefon alıyorsunuz. Yeni bir satın alma yapacaksınız, bir şirket birleşmesi gerçekleşecek. Bir telefon geliyor ve arayan kişi diyor ki sizin müşteri bilgileriniz şu anda dark web'de satışta. İnanamıyorsunuz, ekibinize araştırmalarını söylüyorsunuz. Girip bakıyorlar ve gerçekten sizin müşterilerinizin bilgileri dark web'de satışa sunulmuş. Ne yaparsınız? Elinizdeki senaryo bu. Böyle bir duruma hazırlıklı mıyız? Böyle bir durumda nasıl bir aksiyon alırsınız, ilk kimi ararsınız? O yüzden günümüzde artık kritik verilerin çalınması, 60 saniyeden kısa sürebiliyor. O yüzden sunumuma 2000 yılındaki "Gone in 60 Seconds" filminin mottosuyla başlamak istedim. Bugün verileri herhangi bir kurumdan çalmak, bir dakikadan kısa zaman alabiliyor (Şekil 11). Ama böyle bir veri hırsızlığını tespit edebilmek, neler olduğunu bulabilmek, belki haftalar, belki aylar alıyor. Böyle durumlara ne kadar hazırlıklıyız? Konuyu biraz daha derinleştirelim.

72 saat. Size ne ifade ediyor 72 saat? Fikri olan var mı? Şimdi önümüzdeki yılın ilk çeyreğinde Avrupa'da GDPR regülasyonu devreye girecek ve GDPR'ın, biz Türkiye'deki kişisel verileri koruma kanununun Avrupa'daki versiyonu ve GDPR'a göre eğer siz kişisel verilerle ilgili bir vaka yaşarsanız, bunu 72 saat içerisinde bildirmek durumundasınız. Yani başınıza böyle bir olay geldiğinde, bütün bu olanların nasıl olduğunu bulup, sebeplerini tespit edip, 72 saatte bunu ilgili kurumlara bildirmek zorundasınız. Yoksa şirketiniz 20 milyon dolar ya da global cironuzun yüzde 4'üne kadar ceza alabilir. İnanılmaz rakamlardan bahsediyoruz. Bu kadar şeyi 72 saat içerisinde yapabilecek miyiz? Yani böyle bir siber olay gerçekleştiğinde buna hazırlıklı olacağımız bir planımız var mı, bunu test ediyor muyuz? Şimdi diyebilirsiniz ki GDPR Avrupa'da geçerli, Türkiye'yi çok etkilemiyor. Türkiye'de de kişisel verileri koruma kanunu var. Benzer şekilde Türkiye'de de böyle bir olay yaşadığınızda, bunu kuruma bildirmek zorunda kalacaksınız ki hatta şu anda öyle bir durum da var Türkiye'de. O yüzden ülkemizde de bu verilerin korunmasıyla ilgili neler yapılması gerektiğinde daha ciddi düşünmemiz gerekiyor.

Basından duymuşsunuzdur, Amerika'daki Equifax vakasını. 143 milyondan fazla Amerikan vatandaşının kişisel verileri, sosyal güvenlik bilgileri çalındı. Bu ekranda gördüğünüz Equifax olayının duyurulduğu günkü hisse senedi verileri (Şekil 12). Bakın, veri ihlali duyurulduğu gün hisse senedindeki değer kaybını görebiliyorsunuz.

Artık bu tür veri güvenliği ihlalleri, siber saldırılardan uğrayacağınız zararlar, paralarla ölçülemeyecek duruma geliyor, çok ciddi zararlar alıyor şirketler. Sadece bununla da kalmıyoruz, bu case'de de gördük, böyle olaylar yaşadığımızda artık şirketlerin CIO'ları, CISO'ları, hatta CEO'ları görevlerini bırakmak zorunda kalıyorlar. Bu, iş dünyasının yönetim kurullarının en öncelikli konularından birisi haline geldi.

Şekil 12 Equifax veri ihlali

Neden böyle oldu, buna bir bakalım. Çünkü artık günümüzde suç boyut değiştiriyor. Suç parayı takip eder. O yüzden suç örgütleri de paranın olduğu yere doğru kayıyorlar. Suçların gelişimine bakacak olursak tarihsel olarak; eskiden atlıların yolu kesilirdi, altınlar çalınırdı, değerli varlıklar çalınırdı. Sonra tren soygunları, bu western filmlerinde seyrettik, trenlerin önü kesilirdi, bunlar soyulurdu. Böyle 80'li yıllarda telefonlar üzerinden sahtekârlıklar yapılmaya başladı. Günümüzde suç dünyası siber dünyaya kaydı. Artık suç örgütleri siber dünyada işlem yapıyorlar ve buralardan çok ciddi paralar kazanıyorlar. Hatta bugün artık uyuşturucudan kazanılan gelirler, uyuşturucu ticaretinden kazanılan gelirler, siber suçlardan kazanılan gelirlerden daha düşük bir hale geldi. Böyle bir iş yapmak çok daha kolay çünkü siber suçlular gidip de sokakta böyle bir iş yapacağına, oturup evinin rahatında, sıcağında bu işlemleri gerçekleştirebiliyorlar, çok ciddi bir ekonomiden bahsediyoruz. Tehdit ortamı değişiyor.

Bu saldırıları artık üniversite öğrencileri gerçekleştirmiyor. Karşımızda hükümetler var, kaynağını bilmediğimiz suç örgütleri var. Bunlar çok planlı, organize bütçelerle çalışıyorlar. O yüzden bizim de aynı ciddiyette, güvenlik endüstrisi olarak bunlara cevap vermemiz gerekiyor. Bunlardan birkaç örnek verelim, mesela dedik ki bazı hükümet destekli örgütler var, bunlardan bir tanesi geçtiğimiz yıllarda adını duyduğumuz mesela Suriye elektronik ordusu, duydunuz mu bilmiyorum. Web siteleri var, üye olabiliyorsunuz, atak tool'ları geliştiriyorlar, yazılımları geliştiriyorlar. Siz bunları indirip kendiniz de kullanabiliyorsunuz. Bizim bulunduğumuz coğrafyada bazı case'ler yaşıyoruz. Mesela bankaların müşterilerinin kişisel verileri çalınıyor

ve bunlar dark webde satılıyor. Bu tür her türlü veriyi satın alabiliyorsunuz, kullanabiliyorsunuz, arkasında ciddi bir ekonomi var.

Günümüzde internete bağlı her şey hack edilebilir. Bugün sabahki konuşmalarda da açılış videosunda da benzer örneklerini gördük ve artık günümüzde her şey internete bağlanıyor. Üretim sistemlerinden trafik ışıklarına, bizim kendi IT sistemlerimizden evimizdeki çocuğumuzun odasına koyduğumuz kameraya kadar her şey internete bağlı. IOT dediğimiz kavram hayatımıza girdi ve bu cihazlar internete bağlanan cihazlar artık kurumsal hayatta saldırı gerçekleştirmek için de kullanılıyor. "Denial of Service" saldırıları bu tür cihazlar kullanılarak gerçekleştirilebiliyor. Schodan (Şekil 13) mesela buna bir örneklerden bir tanesidir. İnternetteki bir arama motoru ve yaptığı şey, ücretsiz üye olabiliyorsunuz, Schodan üzerinden siz internete açık endüstriyel kontrol sistemlerini, Scada sistemlerini, trafik ışığı kontrol sistemlerini tespit edebiliyorsunuz. Ya da internet kameralarını tespit edebiliyorsunuz. Bunlara default password'leri kullanarak bağlanabiliyorsunuz. Hatta buralardan elde ettiğiniz makine ordularıyla rakip şirkete saldırı düzenleyebiliyorsunuz. Bunu servis olarak veren ve ücretsiz bir servis olarak veren bir web arama motoru.

Daha karmaşık saldırılar gördük, bu vakayı belki duymuşsunuzdur, Bangladeş merkez bankası vakası. Burada yapılmaya çalışılan şey, SWIFT sistemlerindeki zafiyetler kullanılarak, SWIFT üzerinden gerçek anlamda, yani veri sızıntısı da değil para hırsızlığı, 1 milyar dolara yakın para sızdırılmaya çalışıldı. Bunun yaklaşık 100 milyon doları aktarıldı, ikinci bir transfer

Şekil 13 Dünyanın en tehlikeli arama motoru

daha gerçekleştirilmeye çalışıldı fakat transferi yaparken ufak bir yazım hatasından dolayı son anda fark edildi ve bunlar durduruldu. İkinci transfer 800 milyon dolar civarındaydı. Ve 100 milyon dolar çeşitli ülkelerdeki sahte hesaplara aktarıldı, bunun üzerinden kumarhane hesaplarına aktırılıp bu paralar sızdırıldı. Çok ciddi, siber suçların ekonomiye verdiği zararlardan bahsediyoruz, veri hırsızlığından bahsediyoruz, bir yandan da ciddi anlamda bankalardan para da çalınabiliyor, siber dünya kullanılarak.

Ülkemizde neler oluyor? Dark web'de ufak bir araştırma yaptık, bu geçtiğimiz sene yaptığımız bir araştırmaydı. Mesela Türkiye'deki bazı sağlık kurumlarının hasta bilgileri çalındı. Şimdi bu Amerika'da da çok büyük bir olay. Bizim IBM'in XForce ekibinin her sene yayınladığı bir rapor var. Geçtiğimiz sene sağlıkla alakalı, sektörlere yönelik saldırıların daha da arttığını gördük. Sebebi de siz bir hasta kayıt bilgisini aldığınız zaman, o hastayla ilgili vatandaşlık bilgisi, sosyal güvenlik numarası, her türlü bilgiye sahip olabiliyorsunuz, sahte hesaplar, sahte kimlikler yaratıp onun adına işlemler gerçekleştirebiliyorsunuz. Ülkemizde de benzer olaylar gerçekleşti ve o hastanede tedavi görmüş, kritik hastalıkları olan, çok mahremiyet içeren bilgiler dark web'de paylaşıldı. Bunlara da herkes ulaşabilir durumdaydı. Hatta doktorların bilgileri, personel kayıtları, maaş bilgileri, her türlü bilgi halka açık bir şekilde dark web'de yayınlandı.

İşin bir sonraki boyutuna geçelim. Dedik ki karşımızda suç örgütleri var. Geçtiğimiz senelerde özellikle Rusya ve Ukrayna'daki bankaları etkileyen bir saldırı oldu, çok koordineli bir saldırı, Carbanak. Yaklaşık olarak verdiği zararın 1 milyar Euro civarında olduğu öngörülüyor. Şimdi bu suç örgütünün çalışma yöntemine bakalım, karşımızdaki kişileri daha iyi tanımak açısından. Öncelikle bu saldırıya başlamadan önce suç örgütü internet üzerinden bankalardaki bazı çalışanların bilgisayarlarına erişim bilgilerini satın alabiliyorlar. Bunu siz de yapabiliyorsunuz. 2-3 Euro, çok ucuz. Bu makinelere erişim bilgilerini alıyorsunuz. Bu bilgilerle bu suç örgütü, bankalardaki o bilgisayarlara erişim sağladı. Bunları kontrol altına aldı. Sonra içeride o kişilerin bilgisayarları üzerinden farklı sistemlere yayıldı, erişimlerini daha kalıcı hale getirdiler. Ve sonra sistemi izlemeye başladılar. Bankacılık işlemleri nasıl gerçekleşiyor, bu kişiler para transferlerini nasıl yapıyorlar, mail atarken altına saygılarımla mı yazıyor, teşekkür ederim diye mi yazıyor, bu detayda bu işleyişi öğrendiler. Kendileri bir ekip oluşturdular, bunları dokümante ettiler ve sonra da çok koordineli bir şekilde bu milyonlarca dolar parayı kendi hesaplarına aktarabildiler.

Bir başka örneği, Güney Afrika'da Standard Bank. Yaklaşık 12 milyon dolar civarında bir para hırsızlığı oldu. Bankadan çalınan kişisel verilerle sahte kredi kartları oluşturuldu ve bu kredi kartlarıyla üç saat içerisinde 100 kişilik bir örgüt, bakın ne kadar koordine çalışıyorlar; Japonya'daki ATM cihazlarından 12 milyon dolar para çekti. Şimdi banka Güney Afrika'da, çalınan bilgiler Güney Afrika vatandaşlarının bilgileri, yapılan saldırı Japonya'da yapılıyor ve Seven Eleven mağazalarının içindeki ATM'lerden bu para çekiliyor. 100 kişi üç saat içerisinde

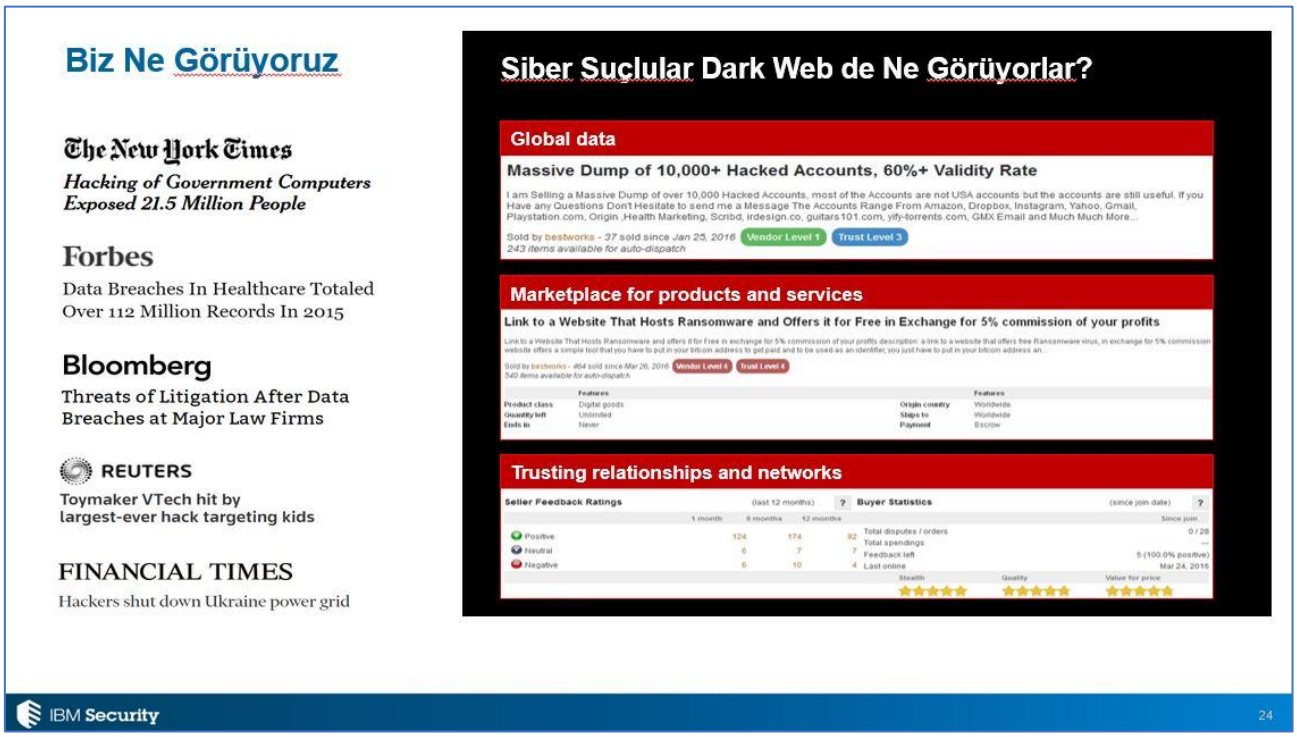
bunu tamamlıyor. Siz banka olarak daha bu olayın farkına varıp da bunu durdurmaya çalışsanız bile arada da çok ciddi bir zaman farkı var, iş işten geçmiş oluyor. Karşımızda çok koordineli çalışan suç örgütleri var.

229 gün, bugün kompleks bir zararlı yazılımı ya da bir saldırıyı bir şirketin tespit edebilmesi için geçen ortalama zaman. Yani bir saldırgan kurumunuza giriyor, içeriye yerleşiyor, 229 gün ortalama içeride kalıyor, dolaşıyor ve siz ancak bunu tespit edebiliyorsunuz. Equifax olayında da böyleydi. Bu veri sızıntısı açıklandı ama aslında Equifax olayı bundan aylar öncesinde gerçekleşmişti.

Şimdi biz iş dünyasında iş zekâsı kullanıyoruz, benzer şekilde siber suçlular da kullanıyor. Bu ekranda gördüğünüz, geçtiğimiz yıllarda internet üzerinden alabileceğiniz, hatta kiralayacağınız bir saldırı tool'uydu. Siber suçlar nasıl iş zekâsı kullandığının bir örneği. Bunu kiralayabiliyorsunuz, çok uzman olmanıza gerek yok. Siz mesela bu suç dünyasına girmek istiyorsunuz, bu alana yatırım yapmak istiyorsunuz. Böyle bir tool'u bir haftalığına kiralayıp, cuma akşamı evinize gelip evinizdeki yan odadaki ofisinize geçip, ekranını açıp hangi ülkelere hangi browser tiplerine, hangi zafiyetleri kullanarak saldırmak istediğinizi seçebiliyorsunuz. Sistemi çalıştırıyorsunuz, hafta sonunuzu eşinizle, çocuklarınızla geziyorsunuz, dolaşıyorsunuz, eğlenerek geçiriyorsunuz, pazartesi günü salonunuzdan çıkıp tekrar yan odadaki ofisinize geçip, ekranı açıyorsunuz. Ve hangi ülkede kaç tane makine ele geçirdiğinizi buradan görebiliyorsunuz ve bu sistemler üzerinden kişisel verileri çalabilirsiniz, başka sistemlere saldırıda bulunabilirsiniz, artık olay bu kadar kolay bir hale geldi. Bunun karşılığında biz ne görüyoruz? Basında yüzlerce haber görüyoruz, bu veri hırsızlığı, yapılan saldırıların verdiği zararlar konusunda. Peki, karşımızdaki siber suçlular dark web'de ne görüyor, işte bunları görüyor. (Şekil 14). Birincisi, bu hesapları satıyorlar, satın alabiliyorlar.

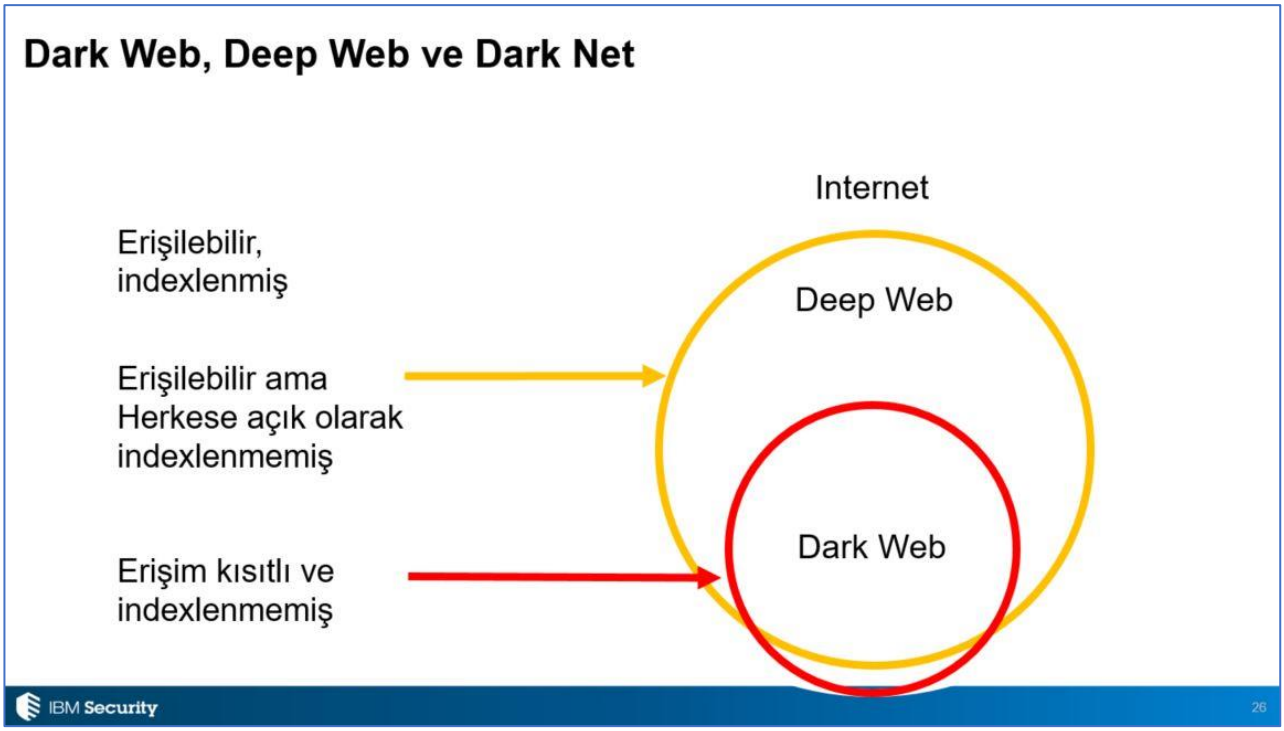
Bugün mesela Equifax olayını düşünelim. 140 milyon Amerikalının bilgileri çalındı diyelim. Bir kişisel veriyi yarım dolardan sattığını düşünün, 50 sentten. Ekonomik değerini düşünün elindeki verinin. Bunlar artık dark web'de satılıyor gerçekten, paraya çevriliyor. İkincisi, değişik iş modelleri öneriyorlar. Mesela ortadakinde okuyabiliyor musunuz bilmiyorum ama diyor ki ransomware konusunda bir fidye yazılımla saldırı yapmak istiyorsan, hiç uğraşma, ben sana ücretsiz bir yazılım veriyorum ve win-win modeliyle çalışalım. Tek istediğim, senden para istemiyorum; elde ettiğin kazancın yüzde 5'ini bana ver. Böyle paylaşımlı iş modelleri var karşımızda.

Aynı zamanda iş yaptığınız saldırganları burada değerlendirebiliyorsunuz. Yani ben bu adamdan bir hacking tool satın aldım, çok memnun kaldım. Ben buradan kredi kartı satın aldım, hepsi çalışıyordu, çok başarılı bir hacker bu, size de tavsiye ediyorum diye değerlendirme yapılıyor.



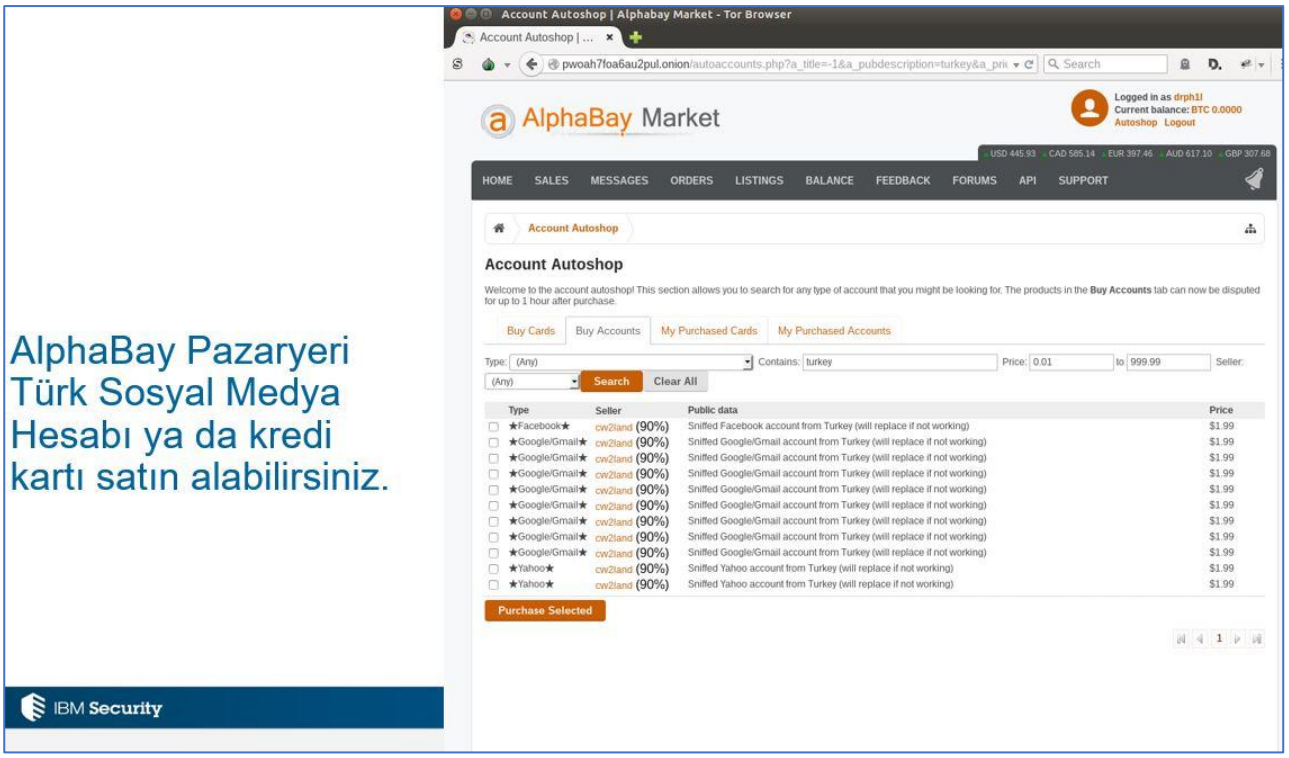
Şekil 14 Siber suçlular Dark Web'de ne görüyor?

Şimdi ülkemizde de çok yaratıcı saldırı tipleri var. Geçtiğimiz günlerde bir tanesi başıma geldi, daha doğrusu ufak bir şirket yardım istedi. Normalde çok basit bir fidye yazılım saldırısına benziyordu ama saldırgan bir sisteme girmiş, ufak bir muhasebe şirketinin bütün verilerinin bir kopyasını kendine almış, sonra bütün verileri silmiş, sistem üzerinde, backup'larını da silmiş. Çünkü backup da aynı sisteme bağlıymış, yedeklerini de ortadan kaldırmış ve şirkete bir mail atmış. Mailde de şunu söylüyor, diyor ki beni diyor bir fidye yazılımla karıştırmayın, ben fidye yazılımcısı değilim. İşlerinizi inceledim, bütün verileriniz elimde, bunlara erişemezsiniz, hiç boşuna uğraşmayın, bu şifreleri kıramazsınız, zaten sildim orijinallerini de. Sizden 2000 dolara eşdeğer bitcoin istiyorum, benimle pazarlık yapmayın, pazarlık yaptığınız her gün bu parayı artıracağım. Yani söyleyeceğiniz hiçbir şey yok. Ve arkasından da işin ilginç yanı şu; diyor ki eğer diyor parayı ödediğinizde verilerinizi kurtaracağınıza inanmıyorsanız, bakın diyor geçen gün başka bir şirketi hack etmiştim, onlar para ödediler, verilerini kurtardılar, telefon numarası bu, arayın, referans veriyor. Ve konuştuğum kişi dedi ki gerçekten aradım, konuştum. Evet dedi, bize de oldu, biz parayı ödedik, verdi verilerimizi, biz gayet memnun çalışıyoruz şimdi diyor. Artık ülkemizde böyle iş modelleri görüyoruz karşımızdaki suç dünyasında.



Şekil 15 Dark Web, Deep web ve Dark Net

Şimdi biraz önce dark web'den bahsettik, bütün bu verilerin satıldığı, kullanıldığı. Dark web nedir, belki hepimiz bilmiyor olabilir. Bir bakalım. (Şekil 15)Bir hepimizin bildiği internet var. Bu internet indekslenmiş, normal Google'a girip search ettiğinizde erişebildiğiniz bütün veriler, internet. Bir deep web var, yine erişilebilir ama belirli yetkilerle erişebiliyorsunuz. Mesela gmail, Hotmail, bir login olmanız lazım oradaki o verilere erişmeniz için, herkese açık değil. Bir de dark web var. Dark web, özel browser'larla erişilen, belirli bir giriş noktası olan ve belirli bir çıkış noktası olan ve arada ne olup ne bittiği belli olmayan bir şifreli ağdan bahsediyoruz. O yüzden suç dünyası dark web üzerinde çalışıyor. İzlerinin takip edilmesini engelleyebilmek için. Spesifik yazılımlarla, özel yazılımlarla buraya erişebiliyorsunuz. Neler yapabiliyorsunuz dark web'de. Hacker kiralayabiliyorsunuz, malware yazacak mühendis tutabiliyorsunuz. Bir hacker kiralayıp rakip şirkete saldırtabiliyorsunuz. Zaten hackerlar değerlendirildiği için, en başarılı çalışan kimse onu kiralayabiliyorsunuz, burada fiyatların karşılaştırmasını yapabiliyorsunuz. Bütün bunları nasıl kiralıyorsunuz? Bütün bu yazışmalar şifreli oluyor, yani karşı taraftaki hackerla şifreli konuşuyorsunuz. Ödemeleri bitcoin ile yapıyorsunuz. O yüzden iziniz de takip edilmiyor. Buradan siber dünyayı bir kenara bırakalım, gerçekten birçok suçun işlendiği bir ortamdan bahsediyorsunuz. Buradan eroin satın alabiliyorsunuz, silah satın alabiliyorsunuz, sahte pasaport satın alabiliyorsunuz. Tüm bu işlemleri dark web üzerinden yapabiliyorsunuz, böyle pazar yerleri var.



Şekil 16 AlphaBay Market

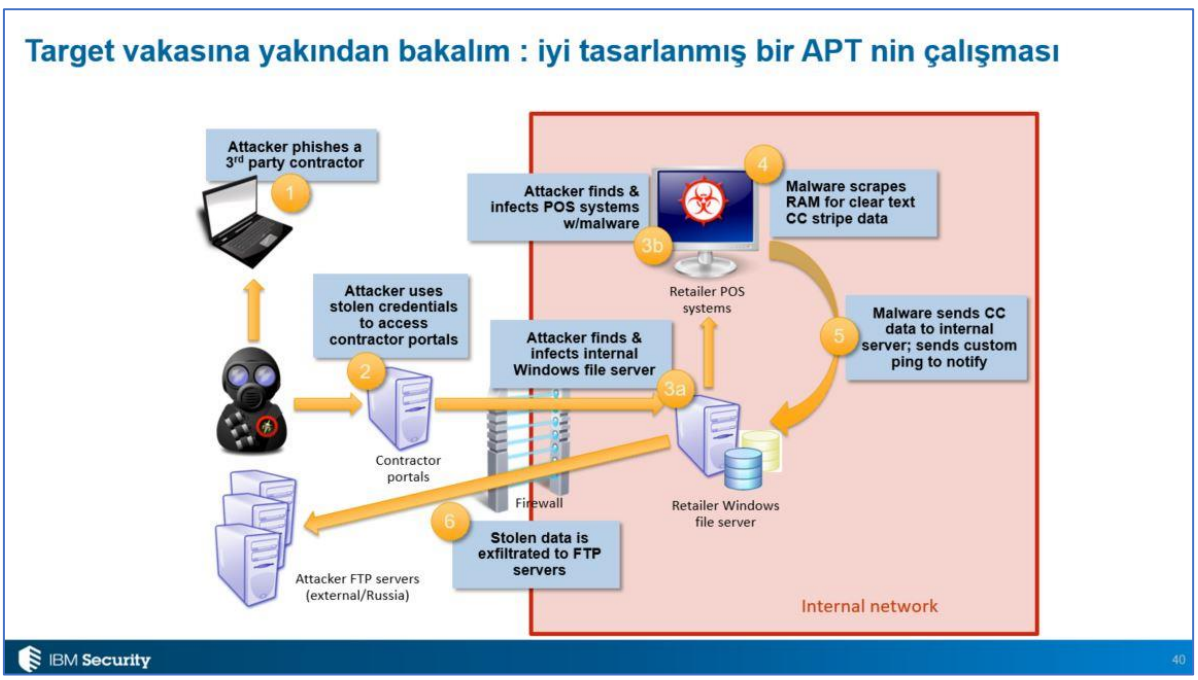
AlphaBay (Şekil 16) bunlardan bir tanesi. Mesela buradan Türk sosyal medya hesabı satın alabiliyorsunuz ya da kredi kartı bilgisi. Ve bu pazar yerlerinin işletmecileri de garanti veriyor. Diyor ki bu sosyal medya hesabıyla login olamazsan değiştiriyorum, sana yenisini vereceğim diyor, başka birisininkini vereceğim diyor. Ya da kredi kartı çalışmazsa, ben sana yeni bir kredi kartı vereceğim diyor, bunun garantisini veriyor. Bunları, bakın şurada ne kadar, 1,99 dolar, çok ucuz paralara satın alabiliyorsunuz.

İstanbul'da kopyalanan kart bilgileri, mesela burada satılıyor. Çeşitli bankaların kart bilgilerine erişmek mümkün. Türkiye vatandaşlarının kimlik bilgileri, zaten public olmuştu, burada da bir dönem satıştaydı. Başka ülkelerin de, sadece bizim ülkemizle alakalı bir konu değil bu, birçok ülkeden sızdırılan veri burada görülüyor. Finansal malware'ler var, malware'in içine spesifik banka isimlerini gömmüşler. Yani ülkemizdeki sistemlere saldırmak amacıyla da bakabilirsiniz.

Ve bir başka veri hırsızlığına bakalım. Şimdi hikâyenin başında, sunumumun başında anlattığım bir hikâye vardı. Hani bir holdingdesiniz, bir hacking yaşıyorsunuz, yeni bir satın alma yapacaksınız. Tarihteki en büyük veri sızıntısı, geçtiğimiz senelerde açıklandı, Yahoo. Üç milyar Yahoo hesabı çalındı ve bu açıklandığı zaman Yahoo, Verizon tarafından satın alınmak üzereydi. Şimdi bunun Yahoo'ya zararı ne kadar oldu, bakalım. Bu vakanın öncelikle neye zararı olabilir, 3 milyar Yahoo hesabının çalınması neye yol açabilir? Bugün günümüzde birçok insan aynı şifreyi birçok sistemde kullanıyor, o yüzden siz birisinin Yahoo şifresini bilirseniz, gidip

onu Linkedin'de de deneyebilirsiniz, sosyal medya hesaplarında da deneyebilirsiniz, böyle zararları olabilir. Gizli soruları çalındı, bu sorularla siz başka kurumsal sistemlere erişmek için bu soruları deneyebilirsiniz, cevapları. Kişisel bilgilerini kullanıp, sosyal mühendislik saldırıları gerçekleştirebilirsiniz. Finansal etkileri ne oldu? Şimdi ceza araştırma, marka değerinin düşmesi gibi konuları bir kenara bırakıyorum. İlk önce Verizon, acaba Yahoo'yu satın almaktan vazgeçecek mi diye birçok haber çıkmaya başladı basında. Ve son olarak da 4,8 milyar dolarlık satın almada Yahoo 350 milyon dolarlık bir indirim yapmak zorunda kaldı. Verizon Yahoo'yu, bu vakaların açıklanmasından dolayı 350 milyon dolar daha ucuza satın aldı. Bu işin Yahoo'ya verdiği zarar, sadece bu veri sızıntısı yüzünden 350 milyon dolarlık bir mali kayıp oldu.

Bir başka örnek geçmişte, bu da ilginç, Target vakası, Amerika'daki bir mağaza zinciri. Duymuş da olabilirsiniz. 2013 yılında açıklandı. Bilgisayar ağlarına yetkisiz erişim oldu, 110 milyon müşterinin kredi kartı bilgisi çalındı Target'ta. Bilgiler Rusya'da bir siteye aktarıldı ve buradan satışa sunuldu. Şimdi bu tabi herkesçe bilinen bir konu oldu. Target'ın VP'si ve CFO'su ifadelerinde şunu söylediler; dediler ki bizde çok katmanlı güvenlik önlemleri vardı, firewall'larımız vardı, malware detection sistemlerimiz vardı, anti virüslerimiz vardı, atak tespit sistemlerimiz, her türlü teknolojiye yatırım yaptık, aynı zamanda PCI sertifikalıydık, yani regülasyonlara da uyuyorduk. Kredi kartı bilgilerini düzgün koruduğumuza dair PCI'dan sertifikamız da vardı. Ama başlarına böyle bir vaka geldi. Ve bu vaka Target'ın havalandırma sistemleri, mağazalarındaki o havalandırma sistemlerine bakımını yapan firma için açtığı bir ara portal üzerinden, o third-party kontratların bilgileri çalınarak, bu sistem üzerinden içeri sızılarak gerçekleştirildi. Ve arkasından Target'ın CEO'su istifa etmek zorunda kaldı. Bunu sık sık görüyoruz Amerika'da da.



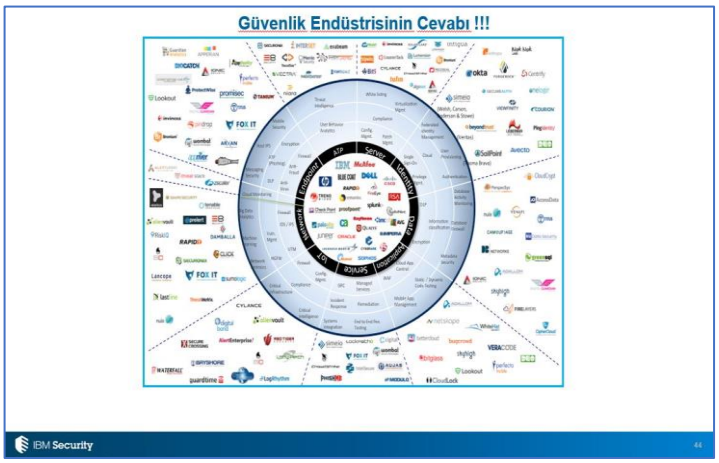
Şekil 17 Target vakası

Ne yaptı saldırganlar? (Şekil 17) Önce bu third-party kontratların bilgilerini ele geçirdiler phishing saldırısıyla. Bu çalınan saldırılarla bu üstlenici portali üzerinden içeriye sızdılar, içerideki bir sistemi enfekte ettiler, bu sistem üzerinden kredi kartı bilgilerini işleyen pos cihazlarına erişim sağladılar, buraya bir kötü amaçlı yazılım yüklediler, bu cihazlardan bu sistem üzerinden kredi kartlarını çekecek. Sonra bu kötü yazılımı test ettiler birkaç gün, sonra hataları buldular. Bakın, içeri girdiler, hataları buldular, yeni bir versiyon geliştirdiler, yüklediler. Sonra da bir anda bütün bu bilgileri alıp dışarıya sızdırdılar. Ve bu olay FBI tarafından fark edildi ve Target'a bildirildi. O yüzden Target gibi düşünürseniz, yani regülasyonlara uyumluyum, o zaman güvendeyim derseniz, bu başarısızlığın ilk adımı olur.

Şekil 18 Regulasyonlara Uymak Güvenli Olmak Anlmaına Gelmez

Günümüzde sadece regülasyonlara uymak güvenli olduğumuz anlamına gelmiyor. Bu ekranda gördüğünüz (Şekil 18) şifre paneli, görevini yapıyor mu yapıyor, tuşlara doğru girerseniz doğru kombinasyonu, kapıyı açıyor. Şu kapı da öyle, kartınızı okuttuğunuzda açılıp kapanıyor. Görevini yapıyor. Ama güvenliği sağlıyor mu, hayır. O yüzden konuya sadece regülasyon boyutunda bakmak da yanlış. Nasıl daha güvenli olabiliriz, biraz daha detaylı düşünmemiz lazım. Eğer böyle düşünmezsek, karşımıza çıkacak şeyler bunlar. Bu Amerika'daki bir şirketin girişe yazdığı yazı. Bütün networkümüz erişilmez durumdadır, bilgisayarlarınızı, laptoplarınızı bağlamayın networke. Ransomware, işte bu Wannacry'dan birisinde yaşanan olay. Ya da bu Ukrayna'daki bir markette yaşanan pos cihazlarının hepsi malware tarafından enfekte edilmiş ve iş durmuş durumda tamamen. Böyle olaylar başımıza çok kolaylıkla gelebiliyor. Ve tüm bunlara karşılık, işte güvenlik ekonomisinin cevabı da bu.

Her yıl Amerika'da RSA'in bir güvenlik konferansı yapılıyor, buraya yaklaşıak 2 bin tane üretici katılıyor. Ve bu saldırı tiplerine karşı da 2 bin tane üreticinin 2 bin farklı çözümü var, teknolojisi var. Nasıl karar vereceğiz, hangisini alacağımıza, hangisini yatırım yapacağımıza? Ya da sadece teknolojiye yatırım yapmak, siber güvenlik sorunlarını çözer mi, bu bakış açısıyla bakmamız gerekiyor.



Şekil 19 Güvenlik endüstrisinin cevabı

IBM'e her zaman sordular, dediler ki IBM sen çok büyük bir şirketsin, bir sürü ülkede iş yapıyorsun, IBM nasıl güvenliğini sağlıyor? Biz güvenliğe bakış açısını 10 tane temel başlık altında topladık. Buna "10 Security Essential Practices" diyoruz, olmazsa olmazları. Bu siber güvenlikte bir kurumsal kültürün oluşturulmasıyla başlıyor. Proaktif bir güvenlik operasyon altyapısının, operasyon sisteminin kurulması, güvenlikte hijyenin sağlanması, kimlik yönetimi, kritik veri koruması, uygulama seviyesinde güvenlik gibi birçok alanda güvenlik konseptine bakılması gerektiğini gösteren bir framework. IBM'in sayfalarından da bu framework'le ilgili daha detaylı bilgi de alabilirsiniz.

Peki, CEO'lara ne tavsiye edebiliriz? Çok beş temel anlamda, CEO'lar nelere dikkat etsinler çünkü konu biraz teknik bir konu ama biraz daha iş dünyası gözünden bakalım. Birincisi, çalışanlarımızın güvenlik IQ'sunu artırmamız lazım, çünkü en zayıf halkamız bu. Siz ne kadar güvenlik teknolojilerine yatırım yaparsanız yapın, orada bir çalışan kendisine gelen e-maildeki bir dosyayı açacak, bir linke tıklayacak. Onun zararlı bir link olduğunu, şüpheli bir bağlantı olduğunu düşünmesi lazım. O yüzden bu bilgi güvenliği farkındalığını artırıcı eğitimleri şirketlerimizde mutlaka uygulamamız gerekiyor, test etmemiz gerekiyor. Sadece eğitim vermek de yetmiyor, çalışanlarımızı test etmemiz gerekiyor.

İki, daha hızlı karşılık vermeye hazır olmamız lazım. Bugün her şirket her sene yılda bir defa yangın söndürme tatbikatı yapıyor. Peki siber güvenlikle ilgili tatbikat yapıyor muyuz? Yani yangın çıktığında nereden boşaltacağız binayı, nerede toplanacağız, kim ne yapacak, kimin görevi nedir, bunları dokümante ediyoruz, test ediyoruz, siber güvenlikte niye bunu yapmıyoruz? Her şirketin bu siber güvenlik tatbikatlarını gerçekleştirmesi gerekiyor.

"Bring your own device" konsepti konusunda dikkatli olmamız gerekiyor. Yani çalışanlarımız artık mobil dünyada yaşıyoruz, kendi cihazlarını getirip kurumsal dünyada şirket içerisinde kullanıyorlar. Tamam, kullansınlar ama "bring own your device"'a evet diyorsak, "bring your own security" 'e evet dememiz gerekmiyor. Yani sen cihazını kullanıyorsan güvenliğini de sen sağla dememiz lazım. Bizim şirketlerimizde kullanılan, çalışanlarımızın şahsi cihazları da olsa bunların güvenliğini de kurumsal olarak göz önünde bulunduruyor olmamız lazım.

Dördüncü konu, kraliyet mücevherlerinizi koruyun. Kraliyet mücevherleri dediğimiz şey, şirketinizin kritik bilgileri. Her şirkette öyle veriler var ki, bu toplam şirketin sahip olduğu verilerin yaklaşık yüzde 2'sine tekabül eder, bu verileri çaldırdığınız zaman şirket değerinizin yüzde 70'ini kaybedebilirsiniz. Öncelikle her CEO'nun, her yöneticinin düşünmesi gereken; benim kritik verilerim hangileridir, bu veriler nerededir, bu verilerin sahibi kimdir benim şirketimde, bu verilere kimler erişiyor ve kritiklik seviyesine göre koruyor muyum? Bu soruları sorduğunuzda cevabını alabiliyor musunuz? Bu gözle bakmamız gerekiyor.

Ve son olarak da güvenlik zekâsından faydalanın. Güvenlik zekâsıyla kastım, artık gelişmiş analitik teknolojilerinden faydalanmamız gerekiyor. Ne olmuşun cevabından çok ki bu ülkemizde çok yıl yapıldı, her şeyden log toplayalım, bir olay olduğunda geriye dönüp bakarız ne oldu diye. Hayır, artık proaktif olarak bütün bu kayıtları toplayıp anormallikleri tespit edip, ne olabilir, şüpheli bir aktivite var mı, bunları proaktif olarak tespit edip, takip etmemiz gerekiyor, bunun için de gelişmiş analitik tekniklerini kullanmamız gerekiyor.

Şimdi sunumumun sonuna geldim, sunumumu ufak bir videoyla bitirmek istiyorum. Siber güvenlikteki belki geçmişten beri gelen en genel konseptlerden, konulardan bir tanesi Truva atlarıdır. Hani bu siber saldırganlar nasıl sızıyor şirketlerimize, içeriye bir zararlı yazılım gönderiyorlar, bir Truva atı gönderiyorlar ve siz onun zararlı bir şey olduğunu anlamıyorsunuz, tıklıyorsunuz ve içeride yaygınlaşıyor. Gerçek hayatta tarihte Truva savaşı gibi bir örnek de varken, acaba gerçek hayatta bugün böyle bir saldırıya şirketler, kurumlar düşer miydi, bunu ufak bir videoyla seyredelim.

Video gösterimi

Evet, o yüzden biz de şirketlerin yaptığı hatalardan, bu basında okuduğumuz siber saldırılarda yapılan hatalardan ders alalım, tarihimizden ders alalım ve siber güvenliğe gereken önemi verelim. Teşekkür ederim.

Sunucu

Sayın Engin Özbay'a sunumu için çok teşekkür ediyoruz.

Sayın konuklar, şimdi programımızda 15 dakika ara vereceğiz. Aradan sonra saat 12.20'de konferansımıza, Sayın Berna Kulaksız, Sayın Ozan Öncel'in konuşmaları ve Sayın Fatih Emiral'ın hacking senaryosuyla devam edeceğiz.

Sunucu

Değerli konuklar, ikinci oturumumuza hepiniz hoş geldiniz. Yeni nesil siber güvenlik yaklaşımları başlıklı konuşmasını yapmak üzere, Vodafone Kurumsal Çözümler Direktörü Sayın Berna Kulaksız'ı sahneye davet ediyoruz.

Berna Kulaksız:

Merhabalar. Ben Berna Kulaksız, hem kendi adıma hem de Vodafone adına, Vodafone Türkiye adına bugün burada siz değerli katılımcılarla bir arada bulunmaktan dolayı son derece onur duyuyoruz. Haftanın son iş günü, son saatleri ama hep birlikte çok değerli bir kalabalık. Dolayısıyla bilgi güvenliğinin hayatımızda ne kadar önemli olduğunu, ne kadar ilgi gösterdiğinizi, bu kalabalıktan bile anlayabiliyoruz.

Berna Kulaksız (Vodafone Kurumsal Çözümler Direktörü)

Ben biraz konuşmaya şöyle başlamak istiyorum, öncelikle siber ne demek? Siber, bilişim sistemleri altyapısında çalışan soyut ve geniş bir altyapı olarak tanımlanıyor. Aslında buna kısaca siber alem de diyebiliriz. Bu peki katmanlar olarak neyi kapsıyor, aslında çok geniş bir kapsamı var, bilgi güvenliğinden, donanımların güvenliğine, aygıtların güvenliğine kadar katman katman aslında bütün bu dünyayı kapsıyor. Bizim hayatımızı niye tehdit ediyor çünkü baktığınızda artık bütün iş yapış şekilleri internete dönmüş durumda. Kullanıcılar, biz tabi mobil kullanımı hem mobil hem de fiksem kullanımı sürekli olarak ölçümlüyoruz. Ve inanın her ay kullanım biraz daha artıyor. Çünkü artık eskiden yapmadığımız çoğu şey bu internet dünyası üzerinden dönmeye başladı. Pazara baktığımızda, pazar da aslında büyük bir pazar. 75 milyar civarında bir büyüklüğe ulaştı. Üç sene sonraki rakamlar da tahmin ediliyor artık, iki katından daha fazla bir büyümeye doğru gidecek. 170 milyar civarında olacağı tahmin ediliyor. Tabi içerisinde donanım, yazılım, penetrasyon testleri gibi her türlü aslında güvenliği kapsayan servisler de bunun içerisinde.

Vodafone Grup tarafından bir araştırma yapıldı geçtiğimiz sene, ben biraz bunun sonuçlarıyla ilgili de paylaşımlar yapmak istiyorum. Burada şirketlere siber güvenlik alanında belli sorular soruluyor ve onların cevaplarına göre de bu rapor oluşuyor. Katılan şirketleri bir de gruplama yapıyorlar aslında. Bir tüm şirketlere sorulan sorular, diğeri de hızlı büyüyen, yani

verdiği büyüme tahmininin üzerine yüzde 10 daha fazla büyüyen şirketlere soruları soruyorlar ve cevapları grupluyorlar. Ve diyorlar ki siber güvenlik sizin için ne kadar önem taşıyor ve yeni iş modelleri çıkarır mı size diyor, olanakları, fırsatları çıkarır mı diyor. Yüzde 86'sı buna evet diye cevap veriyor. Arta kalan oranlamada, yani inovasyona, bana yeni iş olanakları sağlamaz diyenlerin de yüzde 57'si son üç yılda ciro kaybına uğruyor.

Bir diğer soru da yarını hazırlamak. Teknoloji sürekli gelişiyor ve şirketlere deniyor ki siber güvenlik yarınlara senin şirketini hazırlar mı? Yüzde 83 oranında evet, siber güvenlik beni yarınlara hazırlar, ben böyle düşünüyorum diyor. Yine yüksek gelir büyümesi gerçekleyen, hızlı büyüyen şirketlere sorulduğunda daha yüksek oran çıkıyor ve yüzde 88'i evet, ben teknolojiye inanıyorum ve siber güvenlik benim büyümeme etki edecek diyor. Bunun yanında toplamına sorulduğunda deniyor ki peki siber güvenlik müşteri sadakatini, müşteri bağlılığını nasıl etkiler deniyor veya artırır mı siber güvenlik servislerini entegre etmeniz diyor. Yaklaşık yüzde 90'ı, 89'u evet entegre etmeliyiz cevabını veriyor.

Biraz müşteri konuştuk, biraz büyüme konuştuk, bir de şirketin iç süreçlerine baktığımızda, artık zaten günümüzde şirketleri nasıl dijitalleştiririz, bu hemen hemen her şirketin konusu. Hatta yeni iş kolları, yeni departmanlar da kurulmaya başlandı. CDO dediğimiz dijitalleşme genel müdürlüğü yapısı, dijitalleşme organizasyonları birçok şirketin içerisinde var. Tabii bunun yanında insan kaynaklarının da gündeminde ve deniyor ki esnek çalışma saatleri, çalıştığın yerden, bulunduğun konumdan bağımsız çalışma, kendi cihazını getir, cihazınla birlikte çalış gibi çeşitli konseptler artık hayatımızda. Bunun da temeline baktığınızda iyi bir güvenlik altyapınız olmazsa bütün bunları yapamazsınız. Çünkü siz ofiste verdiğiniz güvenlik kurallarını, sistemlere bağlanılması, çeşitli hizmetlerin kullanılması, çeşitli uygulamalara erişimi eğer dijital ortamda da veremezseniz, mobil dünyada yani şirketten çıktığınız dünyada da veremezseniz, bu esnek çalışma ortamlarını sağlayamazsınız. Dolayısıyla işletmelerin de yine yüzde 99'u diyor ki ben inovasyonla ilgili planlarımda büyüme aktivitelerimi planlarken mutlaka siber güvenlik hizmetleri karar verme süreçlerimi etkiliyor.

Tabi diyoruz ki bilgi günümüzün en değerli metası çünkü teknoloji geliştikçe biz daha fazla internete bağlanıyoruz. Geçmişi düşündüğünüzde, alışveriş alışkanlıklarımız internet üzerinden değildi. Bankacılık hizmetleri, yeni nesil artık bankacılığın bankaya gidip sıra beklenip, fatura ödeme ya da işlem yapma olduğunu bilmiyor bile. Çünkü hayatımıza güvenlik katmanlarıyla birlikte bu hizmetler dijital hizmetler girmiş durumda. Hatta sosyalleşme, arkadaşlık bile sosyal ortamdan yapılıyor ve burada tabi veriler yaşamımızın her alanındaki veriler, iş, özel hayat, bütün veriler internette bulunuyor, yani açık bir paylaşımda bulunuyor, bunları da koruma altına almamız gerekiyor. Bu yüzden de güvenlik önemli.

Tabii bir de teknoloji teknolojiyi doğuruyor. Biz güvenlik diyoruz ama bunun arkasında güvenlik hizmetlerinin ön plana çıkmasına temel neden olan aslında iki tane de yeni teknoloji

var. Bir tanesi nesnelerin interneti, diğeri bulut. Bu iki hizmet, iki servisin hayatımıza girmesiyle de güvenliğin önemi daha da artıyor. Yine tüm işletmelere sorulduğunda, Vodafone'un yaptığı araştırmaya katılan tüm işletmelere sorulduğunda, deniyor ki siber güvenlik yeni fırsatlar açar mı size, yüzde 70'i evet diyor. Ve bu evet diyenlerin alt kırılımlarına da bakıldığında, yüzde 82 nesnelerin internetini iş hayatına sokmuş, iş yapış şekillerine entegre etmiş, yüzde 76'sı da servislerini buluta doğru çıkarmış durumda.

Peki günümüzde şirketler için bütün bunları biliyorlar, anlıyorlar, öğreniyorlar, bir diğer önemli sorun ne; sorun hangi hizmeti nereden alacağına, ne zaman entegre edeceğine karar verememeleri. Bu tür kafasında düşünce yaşayan firmaların sayısı da, işletmelerin sayısı da yüzde 41 oranında.

Ben biraz da trendlerden bahsetmek istiyorum. Siber güvenliğe yön veren trendlerden. Öncelikle bir videomuz var.

Video gösterimi

Evet, trendlerle ilgili aslında bir video ve Vodafone'un buradaki rolüyle ilgili bir kısa videomuzdu. Kısaca özetlemek gerekirse, bu trendleri, artık ataklar, siber tehlikeler, daha hedefli ve sofistike oluyor. Nereye doğru atak yapılması isteniyorsa, bir planlı şekilde geliyor bu ataklar. Cloud'a doğru yoğun bir göç var, IOT dünyası sürekli olarak artıyor, her gün yeni uygulama alanlarını görüyoruz ve buradaki kaç tane thing birbirine bağlanacak, her gün yeni rakamlar telaffuz ediliyor. Bu kadar büyük veri olunca regülasyonlar, yaptırımlar, hukuki yaptırımlar söz konusu, bunlara karşı nasıl çalışılmalı, aksi takdirde sonuçları çok ağır oluyor, cezalar oldukça yüksek bedelli.

İş modelleri değişiyor, biraz önce de bahsettiğim gibi, mobilite ihtiyacı kat be kat artıyor ve sonuncusu da bir hata onlarca müşteriye sirayet ediyor ve artık her yerde açık paylaşımı olduğu için güvenlikle ilgili en ufak bir tehdit hemen bilinir hale geliyor ve kulaktan kulağa kartopu etkisiyle yükseliyor.

Şimdi biraz bunları detaylandırırsak, neler. Hedefli saldırılar dedik, bir önceki sunumda da bir firmayla ilgili çarpıcı örnekler verildi. Dolayısıyla artık hedef security saldırıları, güvenlik saldırıları daha çok hedefli geliyor. Biz 2015 yılında aslında Türkiye'de yaşadık, finansal sisteme doğru bir atak yaşandı ve buradaki yaklaşık bir gün boyunca çeşitli firmalara doğru çeşitli sistemlere doğru çalışılmaz duruma geldi. Tabi bunlar daha büyük boyuta geldiğinde ülke ekonomisini de tehdit eder hale geliyor. Yine 2017'de Rusya bir saldırının hedefindeydi.

Oradaki hedef başka bir sektördü, petrol ve telekomünikasyon sektörüydü. Onunla da epey uzun uğraşlar sonucunda sistemleri geri döndürebildiler. Tabi büyük sistemleri korumak ayrı bir şey, büyük firmaların IT ekipleriyle birlikte oradaki güvenlik ekipleriyle sistemlerini koruma altına alması farklı bir boyut. Ama ülkemizde büyük orta ölçekli ve küçük işletmeler de var. Dolayısıyla bu tehdit herkes için, bu servislerin herkese erişilebilir olması önemli, paylaşımlı altyapılardan verilmesi, daha anlatılır halde nasıl faydalanacağının bilinmesi hem mobilde hem de karasal servislerde bu hizmetleri gruplamak önemli. Ve en basit anlamda firmaları korumak için atak önleyici servisler, virüs hizmetleri, networke access'lerin kontrol edilmesi için kimin hangi yetkiyle sistemlere gireceğini kontrol etmek için sistemleri kurgulamak önemli.

Bir diğer konumuz, cloud'a doğru yaşanan göç. Cloud, bulut hizmetleri aslında çok gündemde. Avantajları çok büyük çünkü sistem odanızda orta ölçekli işletmelerde küçük sistem odalarında bulundurulan sunucular, bunların yönetilmesi, bakımları derken, artık bu hizmetlerden çıkıp daha çok sanalda istediğin kadar kapasitene göre kullan, kapasite artımı yap, servis yenilemeden bakım maliyetlerinden kurtul gibi cazip seçenekler sayesinde buraya doğru bir giriş var. Ama artık veri de firmaların kendi kontrolünden çıkıp daha farklı bir kontrol dünyasına geliyor. Burada kiminle çalışıldığı önemli, kime güvenildiği önemli yoksa öbür türlü biz bir hizmeti dışarıda daha avantajlı olarak kullanalım derken sonuçları ağır olabiliyor. Bu yüzden de güvenli cloud ortamları, güvenlik sertifikalarıyla desteklenmiş cloud ortamları oldukça önemli.

Bir diğer trend de IOT. Biliyorsunuz, IOT aslında son 10 yıldır hayatımızda ama hep daha basit servislerle biliyoruz. Mobil posların içindeki IOT servisleri, araç takipler ve enerji sayaçlarının uzaktan ölçülmesi gibi. Artık ama buradan dünya daha eviriliyor, bizim hem iş hem de günlük yaşamımızdaki servislerin tam içerisine, tam ortasında yer almaya başlıyor. Yani siz işinizden çıktığınızda, evinize ne kadar sürede gideceksiniz, evde o yol üstünde nerelere uğrayacaksınız, nereden nasıl alışveriş yapıyorsunuz ya da evinize yaklaştığınızda evin sıcaklığı ne olacak gibi veriler, IOT sayesinde hizmetlere dönüştürülüp bizlere sunulmaya başlıyor. Günün sonunda bu aslında ne demek oluyor, sizi kendi ailenizden, evin içerisindekilerden daha iyi tanıyan, sizin ne istediğinizi bilen servisler yaratılmaya başlanıyor. Bu bilgi güvenli olduğunda sorun yok çünkü sizin için hizmete dönüşüyor ama olmadığı takdirde ciddi bir sorun var çünkü bunun önünün alınamaz bir fraud'a ya da tehlikelere yol açıyor. Dolayısıyla IOT'nin üzerine de yeni bir kavram geliyor, "IOT security" kavramı geliyor, IOT'lerin güvenliği. Yine burada platformların güvenli olması, güvenli lokasyonlarda tutulması da önem teşkil ediyor.

Biraz önce IOT'den bahsettim, bir diğer konumuz da regülasyon ve hukuki yaptırımlar. Bu kadar veri hayatımızda olunca veriler toplanınca, artık sadece belli lokasyon datalarının haricinde yaşam biçimleri verilerimiz de işin içerisine girince, bu veriyi regülasyona tabi olan firmalar da korumak zorunda ve güvenlik katmanlarını üzerine koymak zorunda. Aksi takdirde,

biraz önce de bahsettiğim gibi sonucu çok ağır faturalara, hatta lisansları tehdit edecek noktalara doğru geliyor. O yüzden de regülasyona uyum için güvenlik ihtiyaçları daha da artıyor.

Bir diğer konumuz değişen iş modelleri ve mobilite ihtiyacı. Bahsettim, artık istediğin yerden çalış konseptleri, çalışma saatlerini kendin belirle derken, mobilite önem kazanıyor. Burada da öne çıkan güvenlik servisleri genelde cihazın kontrol edildiği "MDM" diye bir aslında genel tabiri var, mobil cihazların uzaktan yönetilmesi, önem kazanıyor. Çünkü hangi uygulamayı kim kullanacak hem güvenlik hem de kullanım kolaylığı açısından, hangi uygulamayı kim kullanacak, kimin cihazı uzaktan silinecek ya da yeni servisler yüklenecek, bu tür güvenlik servisleriyle, bir de tabi cihazın içerisindeki güvenliği kontrol eden ayrı uygulamalar önem kazanıyor. Yine evdeki cihazlarda da artık daha cihazları biraz daha donanımın içindeki akıllı software'ler konseptinden biraz daha cihaza sonradan yüklenebilir uygulama konseptlerine doğru dönüş başlıyor. Aksi takdirde zaten bu tür uygulamaları şirketler kullanamayacak.

Son olarak da bu kadar konseptten bahsettik ama bunların en temelinde günün sonunda müşteri geliyor. Biz zaten müşterilerimiz olmazsa servisler, sistemler, bunları çalıştırmanın ve hizmetlere dönüştürmenin çok bir anlamı kalmıyor. Müşteriyi anlayıp beklentilerine göre servisler çıkarıyoruz. Sadece servisin tanımı değil, servisin ne kadar güvenli olduğu da müşterilerimiz açısından oldukça önemli. Çünkü herkesin de bildiği gibi müşterinin güveni kaybolduğunda onu geri kazanmak, yeniden kazanmak kat be kat daha fazla efor sarf ettiriyor. O yüzden de her şeyin ortasında müşteriyi koyuyoruz ve müşterilerimizin içinde ekstra güvenlik katmanlarıyla sağlamlaştırıyoruz.

Benim sunumum bu kadar. Ben herkese güvenli günler diliyorum. Teşekkür ederim.

Sunucu

Sayın Berna Kulaksız'a konuşması için teşekkürlerimizi sunuyoruz.

Çok değerli konuklar, şimdi ise "Bulut ve mobil öncelikli bir dünyada siber güvenlik ve kişisel verilerin korunması" başlıklı konuşmasını yapmak üzere, Microsoft Türkiye Kurumsal İş Üretkenlik ve Güvenlik Uygulamaları Satış Direktörü Sayın Ozan Öncel'i sahneye davet ediyoruz.

Ozan Öncel

Ozan Öncel (Microsoft Türkiye Kurumsal İş Üretkenlik ve Güvenlik Uygulamaları Satış Direktörü)

Merhabalar, çok teşekkürler. Aranızda olmaktan ben de onur duyuyorum, bu değerli toplulukta. İsmim Ozan Öncel, anons edildiği gibi Microsoft'ta iş üretkenlik ve güvenlik çözümlerinden sorumlu olarak çalışıyorum. Aradan önce değerli meslektaşım bir örnek vermişti Yahoo'yla ilgili. Bana da şeyi hatırlattı, biz Microsoft olarak Yahoo'ya bundan seneler önce 42 milyar dolar bir bedel önermiştik. O zamanki yönetim kurulu Yahoo'nun, bunu reddetmişti, beğenmemişti teklifimizi. Şimdi 4,5 milyar dolar gibi satış gerçekleşti. Şimdi düşününce aslında koca koca yöneticiler, milyarlarca dolarlık şirketleri yöneten, başarılar elde etmiş bir firmanın, mesela böyle bir öngörüde, böyle bir kararda şirketin geleceğine nasıl bir yön verebileceğine bakması da çok manidar gerçekten. 42 milyar dolarlık bir satın almadan ki o zaman hissedarlar da çok büyük problem çıkarmıştı. Bilmiyorum, tahmin ediyorum o zamanki yönetim kurulu oldukça zor zamanlar geçirmiştir diye düşünüyorum diyerek sunumuma yavaş yavaş geçmek isterim.

Şimdi bildiğiniz gibi değişik bir dönem yaşıyoruz, bizim jenerasyonumuz belki de bir geçiş döneminde. Hem ekonomik olarak hem jeopolitik olarak dünyada kartların yeniden karıldığı, rekabetin artık çok keskin olduğu, sınırları aştığı, kârlılık baskılarının yüksek olduğu, müşteri memnuniyetinin, müşterinin satın alma sürecinde güçlü tarafa geçtiği önemli bir dönemdeyiz. Hatta belki de çok kısa bir dönem sonra kaybolacak mesleklerden bahsediyoruz. Bu teknoloji tabi burada çok önemli bir rol oynuyor. Bu önemli rol içerisinde tabi teknolojiden faydalanmak istiyor bütün firmalar ve bunun ismine de aslında hatta içinde bulunduğumuz çağa da dijital dönüşüm çağı adını veriyoruz ve bu dijital dönüşüm çağında yeni para birimi olarak veri deniyor, kimisi hız diyor. Ben ikisine de katılıyorum, yani hem hız, hızlı hareket edebilmek, esnek olabilmek hem de veriye sahip olabilmek ciddi anlamda bir para birimi, yani yeni dünyanın aslında değeri anlamına geliyor. Tabi bütün bunlara sahip olabilmek, süreçlerimizi teknolojinin vermiş olduğu, sağlamış olduğu faydaları katabilmek, verimliliğimizi artırıp maliyetlerimizi düşürmek, müşterilerimize yaşattığımız deneyimi daha ileri seviyeye çıkartmak, yani satışları artırmak, maliyetleri düşürmek, kârlı bir büyüme sağlayabilmek hedefiyle bütün ticari kurumların olduğu gibi, teknolojiden faydalanmak istiyoruz ve sonuna kadar da gidiyoruz. Tabi bu neyle birlikte geliyor, her zaman olduğu gibi daha evvelki sunumlarda da bahsedildi, bir yerde bir meta varsa, bir yerde bir rant varsa, bunu almak

isteyen, yasal yolla çalışan insanlar olduğu gibi, organizmalar olduğu gibi, aynı zamanda yasa dışı organizasyonlar da tabi ki buradan faydalanmaya çalışıyorlar. Bir iş dünyası ne kadar dijital ortama taşınıyorsa, daha evvel Engin Beyin de söylediği gibi suç dünyası da çok doğal olarak dijital ortama taşınıyor. Ve biz de her geçen gün, daha evvelki sunumlarda da meslektaşlarımın gösterdiği gibi, ben oralara çok fazla girmek istemiyorum, çok güzel örnekler verildi, çok ciddi sayıda her gün çeşitli örneklerini görüyoruz. Büyük büyük firmaların yaşadığı sıkıntıları görüyoruz. Tabi güvenlik katman katman, halka halka hiçbir güvenlik önlemi aşılmaz değil, muhakkak ki bu bir denge ve bir mücadele ama bu tabi ki işi bu suçlular için kolaylaştıracağımız anlamına gelmez. Bu katmanları işimizin riskine göre, katlanmak istediğimiz maliyete göre korumak ve gerekeni yapmakla yükümlüyüz.

Birkaç örnek var, ben de onları istatistiki anlamda paylaşmak isterim. Sadece geçen senelik dönemde 2 milyarın üzerinde bir bilginin sızdığı tahmin ediliyor. Daha evvelki sunumlarda daha uzun bir gün bilgisi vardı ama bizim yaptığımız değerlendirmeler ve istatistiklere göre de bir işletme ortalama, sızıntı olduktan sonra ortalama tespit süresinin 140 günün üzerinde olduğunu biz değerlendiriyoruz. Bu gerçekten zaten felaket senaryosu, bir evinizi düşünün, bir de yabancı biri gelmiş salonunuzda oturuyor, 140 gün boyunca sizin her konuştuğunuzu, her söylediğinizi dinliyor, dolayısıyla sizinle ilgili zaten artık her şeyi öğrenmiş olacaktır, 140 gün içerisinde fazlasıyla. Bunun da ortalama olarak kişilere veya şirketlere maliyetinin de 15 milyon doları ortalama bulan bir zararı olduğunu görüyoruz. Tabi ki bu zararlar her geçen gün dijitalleşme arttıkça devam ediyor olacaktır.

Şimdi tabii eski dönemde bilgi işlem, yaşları da uygun olanlar bilir, bu mobilleşme, teknolojiden faydalanma aslında hızı 15 senelik bir döneme tekabül ediyor yaklaşık olarak. Benim de 15 seneyi aştı, birkaç sene aşmış oldu sektöre girişim. Ben ilk girdiğim zaman çalıştığım firmada bir kısım insanlarda bilgisayar yoktu, bilgisayar yaygınlaşmaya başlamıştı, yani kişisel insanların masalarına bilgisayarlar gelmeye başlamıştı. Benden bir evvelki jenerasyonda masalarda bilgisayarlar da yokmuş, ben o dönemde çalışmadım ama sunucuların bulunduğu sistem odası diyorduk, şimdi artık data center deniyor, sunucuların olduğu yerlerde ise bir tane bir mainframe makinesi vardı, AS-400'dü. IBM'in AS-400 makinesi vardı. 3-4 tane de kabinette de yeni nesil Intel tabanlı sunucu vardı. Şimdi o firmayı düşünüyorum, o büyük bir firma, artık sistemlerinin nerede olduğunu kendisi de muhtemelen bilmiyordur. Çünkü artık sistemlerimiz sadece kendi sistemlerimiz değil, tedarikçilerimiz var, iş ortaklarımız var, bayilerimiz var, kimisini kendi veri merkezimizde tutuyor, kimisi hep konuşuluyor bulut ortamında tutuyoruz. Dolayısıyla çok dağıtık, bunun da uç noktalarda tabii ki herkesin birden fazla cihazı var, tableti var, bilgisayarı var, evinde var, cep telefonu var, bunlar da hepsi akıllı hale geldi. Dolayısıyla artık yönetmemiz gereken çok farklı bir ortamdan bahsediyoruz, sizlerin de bildiği gibi. Şimdi tabii hep riskleri konuştuk, çok ciddi risk var, önlem almak zorundayız. Bu başımıza gelmez demeyin, başa gelebilecek konular.

Çok küçük KOBİ seviyesinde de biliyorsunuz hep bahsedildiği gibi dataların ele geçirilmesi ve para karşılığı satılması gibi küçük çaplı olaylardan artık günümüzde çok büyük sıkıntılar ve maliyetler yaratabilecek noktalara geldi.

Ben de bir iki örnek vermek isterim, Microsoft'un özellikle uğraştığı konularla ilgili. Bildiğiniz gibi bu malware konusu ve botlar konusu, bot networkleri konusu oldukça can yakıcı ve mücadele etmesi güç ortamlar. Burada nasıl bir işlem yapılıyor, özellikle internet ortamlarında kişilerin girdiği ve indirdiği yazılımlarda veya zararlı web sitelerine giren bilgisayarlara bulaşan, arka tarafta çalışan ve kullanıcının da bilmediği ve sürekli dinleme yapan küçük yazılımlardan, zararlı yazılımlardan bahsediyoruz. Bunların bizim tespitlerimizde yüz binleri aştığı senaryoları oldu. Düşünün dünyanın çeşitli yerlerinde bilgisayarlar var, ve bunlar açıkken sürekli bir çoban ismini verdiğimiz bir kişi tarafından komut almayı bekliyor ve bu kişiden, bu dark web'lerde gidip bu botnetworklerini satın alarak, para ödeyerek, yüzbinlerce bilgisayarı, açık olanlarını istediğiniz hedefe çeşitli ataklar yapmak için kullanabiliyorsunuz. Bunun çeşitli şeyleri var, bunu bir hükümete şantaj için de kullanabilirsiniz veya bir markanın o gün lansmanı vardır, rakibiniz o markayla ilgili lansmanı sabote etmek için de kullanılabilir. Ya da sizin dijital pazarlama yapıyorsunuzdur, bir sayfa ziyareti ya da klik bazlı anlaşmanız vardır, gidip o web sitesine sadece çok basit kliklemeler yapan ve yarım saatte sizin pazarlama bütçenizi eritebilecek şeye kadar, aklınıza gelebilecek birçok şeyi yapmak mümkün. Ama hep konuşuluyor, bu IOT senaryolarının artmasıyla birlikte, buzdolabından tutun arabaya kadar, yarın öbür gün göreceksiniz kullandığımız saatlerdeki şeylere kadar ki bunlar yarın öbür gün hastanelere de bağlı oluyor olacak çünkü artık her yeri sensörlerle donatıyoruz, buralara gidip çok çok daha büyük, sağlığa da sadece maliyet anlamında değil, sağlığa da zarar verebilecek noktalara gelebilecek bir tehditten bahsediyoruz. Herkesin tabi ki riskine göre değişebilir boyutta bir tehdit var.

Ancak ve ancak bu tabii ki bizim teknolojinin getirdiği fırsatları göz ardı edeceğimiz anlamına gelmiyor. Çünkü iyi haber, bunca tehlikenin yanı sıra iyi haber, Microsoft gibi, IBM gibi birçok değerli üretici firma bu alanda ciddi bir çalışma içerisindeler. Dolayısıyla bu sofistike, bundan yaklaşık 2000'lerin başında sadece yaramazlık yapmak için gençlerin ilgilendiği ve ufak tefek zararlar, eğlence için zarar verdiği noktadan organize, çok yüksek bütçeli organize suç şebekelerinin olduğu camiaya karşı bizler de üreticiler olarak çok yoğun çaba içerisindeyiz. Dolayısıyla bu çok sofistike, çok katmanlı, birçok noktada bizim önlem almamızı gerektiren yapıya karşı çözümler üretiyoruz. Ve bunlar da aslına bakarsanız sadece reaktif değil, şu an yaptığımız bütün çalışmalar tamamen etkin savunma şeklinde. Yani pasif bir savunmadan, yani olay başımıza geldikten sonra hareket etmekten öte, tamamıyla aktif bir savunma ki bunu da nasıl yaptığımızı biraz bu sunumda çok tekniğe girmeden bahsediyor olacağım.

Şimdi biz Microsoft olarak, biz de tabi ki bu güvenlik konsepti üzerine belli senelerdir yoğun çaba harcıyoruz ve yatırım yapıyoruz. Bizim sadece güvenliğe ayırdığımız bütçe 1 milyar doları aşkın ve bunu her sene harcadığımız bir bütçe. Ciddi oranda bir çaba içerisindeyiz ve

bunları da hem kendi çözümlerimizin içerisinde gerçekleştiriyoruz hem de müşterilerimize hizmet olarak sunuyoruz. Şu an 3500 kişi sadece Microsoft içerisinde güvenlik çözümleri üzerine çalışıyor ve 3500, yani biz 100 bin kişilik bir organizasyonuz kendi bordromuzda çalışan, 3500 kişi size böyle çok yüksek bir oran gibi gözükmeyebilir ama şunu vurgulamak için özellikle söylüyorum, bunlar sizi de ilgilendiriyor. Şimdi çoğumuzun şirketinde güvenlikten sorumlu sadece güvenlikten, bilgi güvenliğinden sorumlu görevli insanlar bulunmuyor. Genelde bilgi işlemcilerin yan görevleri ya da bilgi işleme bağlı çeşitli şeyler ya da bir veritabanı uzmanının güvenliğe de bakması gerekiyor. Ben bundan 10 küsur sene evvel çok büyük bir ERP sistemi kurarken, database'deki admin user'ların şifrelerinin boş geçtiğini defalarca gördüm. Rahatlıkla o bir ERP sistemine geçip tarumar edip çıkabilecek bir dönem yaşadık biz. Hâlâ da öyle olan var mıdır bilmiyorum ama buradaki güvenlik algısı sadece bir ana işi değil, yan iş olarak ortaya çıkıyor. Bunun iki sebebi var. Bir, bu konudaki ilgili farkındalığımızın seviyesi. İkincisi de güvenlik uzmanı bulabilmek o kadar kolay değil. Bu böyle okullarda öğretilen genel bir müfredatı olan, genel bir prensibi olan, özellikle bilgi güvenliği açısından söylüyorum ve yaygın olarak olan bir yapı olmadığı için de 3500 kişilik bir grup oluşturmak da gerçekten kolay bir yapı değil. Burada tabi ki bizim de yapmamız gereken şey, zaman içerisinde şirketimizin büyüklüğüne göre, bu konuyla ilgili yani bilgi güvenliği, siber güvenliğiyle ilgili sadece işi bu olan, burayı takip eden, sizi koruyacak ve büyük zararları önleyebilecek kişileri de şirketlerimizde istihdam ediyor olmak.

Şimdi bu güvenlik konusunda birçok risk olduğundan bahsettik. Ben biraz daha nasıl bakmak gerekiyor ve neler yapmak gerekiyor, dedim ya tüm bu karşımızda duran karşı taraf, karanlık tarafa karşı bizim yaptığımız da tabi ki çok önemli işler var. Zaten şöyle düşünün, eğer bu işler yapılmıyor olsaydı, şu an ne ekonomi dönebilirdi ne bir bankacılık piyasası ayakta olabilirdi ya da herhangi bir şirketimiz hayatına devam ediyor olurdu. Dolayısıyla yüzümüzü karartmamıza neden yok, sadece gerekli önlemleri almak gerekiyor.

Şimdi bizim buradaki yaklaşımımız üç temel bacağa oturuyor. Platform, zekâ ve iş ortaklığı. Bunlar bu konseptin üç tane temel yapıtaşını oluşturuyor. Şimdi fiziksel güvenlik tabi ki çok çok önemli. Operasyonel güvenliğimiz önemli, bir de data center'lardan bahsettik. Burada fiziksel güvenlikle ilgili şu örneği vermek isterim. Yine başımdan geçen bir konu, ben askere gittiğim zaman, askere gitmek için işten ayrılmıştım, geri dönmek üzere işten ayrılmıştım ama tabi ilişkim kesilmişti. O zaman PDKS kartım yanımdaydı işten ayrılırken doğal olarak. Bir, benden o PDKS kartını almadılar işten ayrılırken. Ben 12 ay asteğmen olarak yaptım. İnanır mısınız, büyük bir şirketten bahsediyorum, 12 ay sonra şirkete ziyarete geldiğimde PDKS kartım hâlâ çalışıyordu. Bu demek oluyor ki fiziksel güvenlik anlamında ciddi bir, yani sizin PDKS sisteminiz, işte biraz sonra da bahsedeceğiz, kimlik yönetiminden bahsediyor olacağız. İşte bir kimlik var, o bir kimlik, bir yere sizin giriş yapmanızı sağlıyor. İşten ayrılmış bir kişinin tekrar bir sene sonra gelip aynı kartla işe girebilmesini sağlar bir boyuttaydı bu büyük firmada. Bu tabi benimkisi çok naif bir örnek ama biliyorsunuz bundan, hatırlayanlar hatırlar, koca bir

kulede çok değerli bir yöneticimizi de bir terör saldırısında benzer şekillerde kaybettik. Dolayısıyla bütün güvenliğin hem naif tarafı da olduğu gibi çok tabi ki tehlikeli tarafı da var.

Veri merkezleriyle ilgili şunu söylemek isterim, çok fazla tabi bunların detayına girmek istemiyorum zaman itibariyle ama şimdi biz bütün teknoloji üreticileri biliyorsunuz bulut hizmetlerine doğru kaymaya çalışıyoruz, buna çaba sarf ediyoruz. Bilgi işlemi de bir hizmet olarak sunmaya çalışıyoruz, eskiden farklı olarak. Yani bir ürün olarak satıp, sizin kurup kendinizin destek alıp yaşadığı bir şeyden farklı olarak, aynı bir elektrik gibi, bir su gibi bir hizmet olarak dönüştürmeye çalışıyoruz ve bütün ürünlerimizde bu veri merkezlerimizden, yapmış olduğumuz yatırımlardan abonelik bazında sunmaya çalışıyoruz. Tabi bu süreç içerisinde bu bir geçiş dönemi, batı buna daha hızlı geçiyor, doğu biraz daha temkinli yaklaşıyor, dünya ölçeğinde baktığınız zaman. Şöyle bir deneyim yaşadık biz, bulut hizmetlerimizi müşterilerimize anlatırken gelen ilk reaksiyon, ya benim bilgim, benim verim kendi yanımda olsun, ben güvende hissetmiyorum idi. İnanır mısınız, artık yavaş yavaş konuşmalar değişiyor. Bilginizin güvenli olması için aslında bu işin uzmanı olan ve bu işe çok büyük ölçekte yatırım yapan firmalara devretmek isteyen şirketleri de görüyoruz. Bu tabi ekseriyeti ifade etmiyor ama burada bu yönden de bir eğilim olduğunu görüyoruz. Buradaki mantık aslında çok anlaşılabilir. Şimdi bizim buluta geçmemiz ve buradaki vizyon aslında teknolojiyi demokratikleşme amacından kaynaklanıyor. Teknolojiyi demokratikleştirmek ne demek? Şimdi teknoloji her geçen gün karmaşıklaşıyor, bilgi gerektiriyor, belli bir maliyeti var, ucuz da bir maliyet değil. Şimdi bunu büyük ölçekte bütçeleri olan büyük firmaların karşılaması mümkün. Dünya ölçeğinde bir bankanın buna bütçe ayırması, sonuna kadar takip etmesi, bunlar için insanlar tutması, yetkin işgücü bulabilmesi anlaşılıyor olabilir. Ama küçük irili ufaklı ya da orta seviyedeki ölçekteki firmaların bu seviyede bir teknolojiye erişmesi, bunun maliyetine katlanması, onu yönetecek insanlar bulması, çok doğal olarak çok mümkün değil. İşte biz ne yapıyoruz, veri merkezlerimizden bunları hizmet olarak sunarak, küçük bir şirket de olsa, orta boyda bir şirket de olsa herkese aynı seviyede teknoloji hizmetini götürebiliyoruz. Aynı durum güvenlik için de geçerli. Bizim her veri merkezimizin, yani büyük ölçekteki veri merkezimizin yatırım maliyeti yarım milyar doları buluyor. Dolayısıyla hem bunun içerisinde fiziksel güvenlikten tutun, çok ileri seviyede teknolojik operasyonel güvenlikleri de içeriyor. Dolayısıyla sahip olacağınız sistemleri bulut ortamlarından güvenilir üreticilerden, güvenilir hizmet sağlayıcılarından alıyor olmanız tabi ki burada sizin güvenliğinizi de ciddi anlamda artırıyor olacak ve işi konusunda uzman, işi bu olan Microsoft gibi, IBM gibi, Vodafone gibi diğer firmalarla da sağlamanız anlamına geliyor.

Bu platformda dört tane ana şeye bakmamız gerekiyor. Biz bilgi işlemci olmayıp da bir şirketin yönetiminde olup bu işi sorgulamak isteyen ve bu işe nasıl bakmak istediğini düşünen kişiler için de dört temelde bakmak mümkün olabilir. Kimliğimiz çok önemli. Nereye girişler yapılabildiği, kimin nereye giriş yapabildiğini biliyor olmamız önemli. Tehditleri olmadan önce, olduktan sonra nasıl yöneteceğimiz çok önemli, bunları yapabilecek çözümlere sahip oluyor

olmamız çok önemli veya hizmet aldığımız firmaların böyle bir yetkinliğinin olup olmadığını değerlendirmek çok önemli. Bilgimizi korumak çok önemli. Bilgilerimizin hangisinin önemli, hangisinin kritik, hangisinin önemsiz olduğu, sadece kendi bilgilerimiz değil, birazdan mevzuat konusuna da geçeceğiz, mevzuata tabi olan veya bizim kendi müşterilerimizin bilgilerinin nerede tutulduğu. Ve aynı zamanda da sahip olduğumuz güvenlik yazılımlarının yönetimini, şeffaflığına da sahip oluyor olmamız gerekiyor. Microsoft olarak da bizim bu konularla ilgili birçok çözümümüz bulunmakta, bir kısmıyla hâlihazırda zaten birçok firmamızla, sizlerle birlikte çalıştığımızı düşünüyorum, onların detaylarına girmeden ikinci başlığa geçmek istiyorum. Burası çok kritik, burası zekâ dediğimiz kısım artık bizi geçmiş dönemdeki bilgi teknolojilerinden günümüzde ayıran ana etmen.

Şimdi hep konuşuldu, bilgi işlemciler olarak biz çoğunlukla geçmişe dönerek, geçmişteki veriyi iyi yöneterek veya daha reaktif aksiyonlar alarak ilerliyorduk. Ancak yapay zekanın gelişmesiyle, artık akademik düzeyden daha ticari bir boyuta gelmesiyle biz artık zekayı, yani yapay zekayı çeşitli algoritmalarla ve geçmiş verinin verdiği ışıkla birlikte geleceği tahminleme, öngörme imkanına sahip oluyoruz ve işin güzel tarafı daha ucuz, daha basit, diyorum ya daha pahalıydı daha akademikti, şimdi daha ticari, daha ucuz, satılabilir ve alınabilir ve aynı zamanda da daha basit, konunun çok özel uzmanı olmadan bu yapay zeka çözümlerinden faydalanabiliyoruz. Sadece güvenlik olarak görmeyin, bir ERP sisteminiz olabilir, bir CRM sisteminiz olabilir, bir perakendeciyseniz bir replenishment sisteminiz olabilir, aklınıza gelebilecek bir üretim planlama olabilir, birçok alanda artık yapay zekayı, bulut çözümlerimiz üzerinden size sunmamız mümkün durumda. Güvenlikte de bu durum söz konusu. Güvenlikte de birazdan bir miktar daha bahsediyor olacağım, artık bir hackerın ortamınıza girip yaptığı işleri sezebilen, oralarda bir şeyler oluyor, yanlış bir şeyler oluyoru hissedip size bilgi verebilen yapay zekâ sistemlerine sahibiz. Dolayısıyla kullanıcının kendisine gelen maili tıkladığı zaman açsa dahi orada arka planda çalışan ve sisteminize bulaşmaya çalışan kötü niyetli yazılımı fark edebilir bir noktaya gelmiş durumdayız şu anda.

Aynı zamanda çok değişik teknolojiler de söz konusu. Şunu da artık yapmak mümkün; kale içinde küçük kaleler, cihazlar içinde oluşturabiliyoruz. Örneğin şunu kastediyorum, konteynır adını verdiğimiz, özellikle kritik yazılımlarınızın sistemin içerisinde bağımsız bir şekilde çalışabildiği, yani bir sistemde bir şey bozulduğu zaman bulaştığı zaman o bilgisayara girmiş olması ya da o cihaza girmiş olması, o cihazda içerisindeki her yere gidebileceği anlama gelmesin diye özellikle kritik alanlarda ve sistemin çalışabilirliğini engellemeyecek çeşitli konteynırlar yaparak buralarda sistemin zarar vermesini engelleyecek uç noktadaki çalışmaları güvenlik seviyelerini müşterilerimize sağlar duruma geldik. Dolayısıyla hep katman katman ve çok sofistike bir yapıdan bahsediyorduk. Ağlardan tutun, sunuculara, sunuculardan eldeki cihazlarımıza kadar birbirinizden farklı olarak ama bütünleşik ve arka tarafta bir yapay zekâyla çalışan ciddi bir güvenlik mekanizmasını oluşturmamız mümkün ve bunu da düşük maliyetli hizmet ve abonelik bazlı bir şekilde gerçekleştirmemiz mümkün. Dolayısıyla bizim aslında

yöneticiler olarak yapmamız gereken şeylerden bir tanesi de bu konuda Microsoft gibi ve diğerleri gibi konusunda uzman, çözümleri olan firmalarla bir güvenlik tabi ki stratejisi geliştirmek ve şirketimizde de mümkünse bu konularla ilgili yetkin kişileri istihdam etmek. Aslında bu işte yapılması gereken en önemli şeylerden bir tanesi.

Bizi farklı kılan demiştim bu zekayla ilgili önemli bir avantajımız da biz tabi çok fazla sayıda müşteriye sahip olduğumuz için, şu an 1 milyarın üzerinde Windows 10 cihazı şu an müşterilerimiz de kullanıyor, bunların izin verenlerinden sürekli güvenlik verisi topluyoruz. Hotmail gibi, mail.com gibi ya da Office 365, Azure gibi çok yaygın kullanılan bulut hizmetleri üzerinden ciddi kullanım ve eğilim verisi elde ediyoruz. Bunları analiz ettiğimiz zaman, şöyle söyleyebilirim; ayda 450 milyar otantikasyonu takip ediyoruz, 1 milyarın üzerinde Windows cihazını güncelliyoruz, güvenlik güncellemelerini yapıyoruz ve 450 milyarın üzerinde e-maili de SPAM ve malware'i olup olmadığıyla ilgili denetimden geçiriyoruz. Dolayısıyla sürekli olarak müşterilerimizden, bulut ortamındaki müşterilerimizden ya da kendi ortamında bulunan müşterilerimizden izin verdikleri ölçüde sinyal toplayarak bir security graph'ı oluşturup, 3500 kişilik de güvenlik ordumuzla birlikte buralardan gereken aksiyonları çıkartarak ürünlerimize ve hizmetlerimize yerleştiriyoruz. Tabi bunu tek başımıza yapmamız mümkün değil. Bu arada, bu güvenlik ekibi içerisinde mavi ekip ve de kırmızı ekip diye iki ekibimiz var. Bu ekipler birbirleriyle yarış halinde. Bir ekip sürekli bizim sistemlerimizi korumaya çalışıyor, diğer ekip de kendi içimizdeki ekipler hack etmeye çalışıyor, dolayısıyla böyle ilginç bir mücadele içerisinde bulunan iki tane grup ekibimiz var. Ne demiştim, tabi ki bütün bu aktivitelerimizi tek başımıza yapmıyoruz. Diğer üretici firmalarla ortaklıklarımız var. Bir ürünü üretirken üzerinde çalışacağı donanım, Intel olsun, IBM olsun, diğer firmalar olsun onlarla birlikte hareket ediyoruz. Dolayısıyla güvenliği birlikte oluşturuyoruz. Regülatif çalışan firmalarla organizasyonlarla birlikte çalışıyoruz. Ve tabii ki de ülkelerin yönetimleriyle birlikte de özellikle kriz anlarında birlikte çalışıyoruz.

Bir miktar da mevzuat, hükümetlerden bahsettik, biraz da mevzuattan size hızlıca bahsetmek istiyorum. Daha evvel de GDPR'ın konusu geçmişti. Biliyorsunuz biz Avrupa Birliği uyum yasaları çerçevesinde kişisel verileri koruma kanununu Türkiye'de adapte ettik ve şu anda uygulanmasıyla ilgili de bir süreç içerisindeyiz. Bu dönem içerisinde KVKK'nın, yani kişisel verileri koruma kanununun daha da gelişmişi olduğunu söyleyebileceğimiz rahatlıkla, yeni bir mevzuat da yeni bir kurallar silsilesi de Avrupa Birliği içerisinde yasalaşmayı bekliyor. 2018 mayıs ayında devreye girecek ve Avrupa Birliği'ndeki firmalar için doğrudan bağlayıcılığı olacak, aynı zamanda Avrupa Birliği üyesi ülkelerin içerisinde yerleşik şirketlerin dışında, Avrupa Birliği içinde veya Avrupa Birliği dışındaki vatandaşlara, Avrupa Birliği vatandaşlarına hizmet veren tüm şirketleri de etkiliyor olacak. Yani biz Türkiye'deyiz, biz Türk firmasıyız, Avrupa Birliği mevzuatına, regülasyonuna tabi olarak diye de düşünmeyin, Türkiye'de yaşayan veya dünyanın herhangi bir yerinde yaşayan bir Avrupa Birliği vatandaşına bir ürün veya hizmetinizi satarsanız, bu mevzuata tabisiniz. Örneğin bir otel olduğunuzu düşünün, Antalya'da bir otel olduğunuzu düşünün. Bir Alman müşterinizle ilgili doğal olarak sizde kaldığı anda bilgilerini topluyorsunuz. O Avrupa Birliği vatandaşı kendisiyle ilgili veriler konusundan da

tasarrufta bulunma hakkına sahip ve siz de buna uymak zorundasınız. Dolayısıyla Avrupa Birliği mevzuatı olmakla birlikte Avrupa Birliği ülkeleri dışında faaliyet gösteren veya yerleşik olan şirketleri de doğrudan ilgilendiriyor.

Biz bir de bu konuya aslında iki türlü bakmayı istiyoruz. Ben şeyden çok bahsetmek istemiyorum, sebebini de açıklayacağım, bu mevzuatların çok ciddi yaptırımları var. Şimdi bir konuya yaptırımlarından doğru ele aldığımız zaman genelde, konu yaptırımlardan uzaklaşmak için yapılan aktiviteler genelde minimum seviyede oluyor. Yani oradan yırtalım, minimum şekilde bu işi kotaralım ve cezalardan yırtalım şeklinde. Aslına bakarsanız bizim burada vurgulamak istediğimiz şey, bu işin fırsat tarafı ve bunun zaman içerisinde de bir fırsat olduğu bence ortaya da çıkacaktır. Ben GDPR uyumluyum demek, ben ey müşterim senin bilgilerini bana vermiş olduğun, güvenerek vermiş olduğun bilgilerine sahip çıkıyorum, bunları koruyorum, bu benim diğer rakiplerimden farklılığım diyebilmek ve bunu ayırt edici bir özellik olarak değerlendirmek ve pozisyonlamak, bunu bu şekilde ele almak, aslında konuyu bir fırsat olarak değerlendirmek anlamına geliyor. Dolayısıyla bu konuya, ben ceza almayayım da en ufak şekilde buradan nasıl yırtarımdan ziyade, ben bu konuyu nasıl bir rakiplerime karşı bir fırsat üstünlüğü olarak değerlendiririm, bu benim müşterilerime olan saygım ve sorumluluğum gereğidir diyebilmek, aslında bu işin doğru şekilde ele alınması olarak değerlendiriyoruz. Burada yapılması gereken şeyler sadece teknolojik değil, süreçleri de ilgilendiriyor ve insanı da ilgilendiriyor birçok konuda olduğu gibi. Yani süreç, insan ve araçlar aslında birçok konuda olduğu gibi, yapılması gerekenleri içeriyor. Temelde müşterilerinizin kişisel bilgilerinin, mahremiyetlerinden sorumlusunuz.

Burada birçok oyuncu var. Bu bilgileri siz kendiniz işliyor olabilirsiniz, kendinizde duruyor olabilir ya da bir yerde hizmet aldığınız için ya da birilerine hizmet verdiğiniz için farklı bir konumu da söz konusu olabilir. Nerede olursanız olun, kim olursanız olun, bu sorumluluğu üzerinizde taşıyorsunuz. Dolayısıyla toplanılan veriler hakkındaki yaptırımlara tabiyiz. İşte kontroller, süreçler, uyarı mekanizmaları, buralarda şeffaf olmanız, şeffaflık göstermeniz ve teknolojik altyapınız ve çalışanlarınızı süreçlerle ilgili eğitmeniz gibi birçok GDPR uyumluluk için gereken faaliyeti yerine getirmeniz gerekiyor. Microsft.com/GDPR yazdığınız zaman, orada iki tane anket var, biri küçük kısa bir anket, biri daha uzun bir anket. Şirketinizin GDPR uyumluluğunu da orada çok hızlıca da böyle genel yüzeysel bir şekilde de test edebilir, değerlendirebilirsiniz. Yani bizim şirketimiz, benim şirketim bilgi güvenliğini nasıl ele alıyor, ne kadar hazır ya da GDPR uyumluluğu nedir merak ediyorsanız, oldukça çarpıcı olacağını söyleyebilirim, oradaki testi çözmenizi en azından ya da bakmanızı öneririm.

Temel olarak çok tabii yüzeysel anlatıyorum burada, çok detaylı bir mevzuat bu ama temelde şunu bekliyor mevzuat; topladığınız verileri bilmenizi, ben ne verisi topluyorum, bu verinin detayları nedir, onu biliyor olmanız önemli, bunu yönetiyor olmanız doğal olarak önemli, süreçlerinizin veriyi yönetirken ki süreçlerinizin ne olduğu önemli. Tabii ki bu veriyi koruyor olmanız çok önemli ve nasıl koruduğunuz çok önemli. Bir de bağlayıcı olan bir konu var bu mevzuat içerisinde, bir sorun olduğu zaman bunu, daha evvel de bahsedildi, 72 saat denildi, raporlayabiliyor ve ilgili yerlere aktarabiliyor olmanız gerekiyor.

Burada tabii bunları yapabilmeniz için birçok çözüm var. Şöyle düşünebilirsiniz; şimdi çok fazla yerden data topluyoruz, şimdi özellikle klasik pazarlamadan yeni modern dijital pazarlamaya geçtiğimizde artık ne yapıyor bizim pazarlamacılarımız, web sitelerinden sosyal medyadan gelen kişileri tanımaya çalışıyor, bunları lead scoring yapıyoruz, hatta belli bir skora geldiği zaman artık bu benim için bir satış fırsatıdır diyoruz, onu satış ekibine lead olarak atıyoruz, bir sürü süreçlerimiz var. Orası müşterilerimizden, hatta sosyal ortamdan topladığımız veriler var. Müşteri hizmetlerimiz var, şikâyet bildiriyor, kurulum durumu istiyor, birçok etkileşim yaşanıyor, web sitemiz ayrı bir şekilde çalışıyor, dolayısıyla bu hep çok kanallı diye bahsettiğimiz, müşteriyle olan etkileşimimiz, aslında çok kanallı devam ediyor. Çok yerden çok veri alıyoruz. Hatta birçok CRM projesinde ilk başlarken data tekilleşmesiyle uğraşıyoruz. Çünkü Ozan Öncel'den sistemde 10 tane ayrı Ozan Öncel var, ayrı yerlerden toplamışım. Dolayısıyla baktığınız zaman, verimize hiç hâkim değiliz, birçok firma için bunu söylüyorum. İlk olarak kimin ne verisine sahibiz, bu kime ait veriler, bunları biliyor olup yönetebiliyor olmamız lazım. Burada sınıflandırma gibi konular çok çok önemli. Örneğin bu hem sizin kendi kişisel verilerinizi korumak anlamında hem müşterilerinizin verilerini korumak anlamında, benim bir satış fiyat listem şifreli duruyor mu ya da bir dizayn dokümanım, ürün dokümanım, ürün spec'lerim doğru yerde encrypt bir ortamda duruyor mu, otomatik olarak şifrelenebiliyor mu, sınıflandırılabiliyor mu gibi bütün konuları takip etmeniz ve yönetmeniz gerekiyor. Bunlar için de birçok çözüm bulunmakta. Bunları monitör etmemiz, kataloglamamız, takip etmemiz gibi faaliyetler önemli. Ve doğal olarak da sistemlerin audit edilebilir, rapor verebilir ve çeşitli uyarıları sağlayabilir bir yapıda olması çok çok önemli. Ama şunu muhakkak bilin, artık günümüzde bütün bu altyapıdaki çalışmalar otomatize olmuş ve yapay zekayla desteklendiği için doğru bir kurulum yaptığınız zaman göreceksiniz ki sistem size zaten problem oluşmadan ya da oluşmaya yakın ya da oluştuktan sonra çok detaylı bilgiler vererek çok hızlı izole etmenizi ve aksiyon almanızı ve büyük zararlardan kurtulmanıza imkân sağlayacak. GDPR uyumluluğu ya da kişisel verilerin koruma kanunuyla ilgili ya da bir şekilde güvenlikle ilgili yapacağınız en hızlı kazanımlar, genelde IT tarafında yapacağınız yatırımlarla olacaktır. Çünkü süreçleri değiştirmek, uygulamak, insanları eğitmek bir zaman almakla birlikte, IT ile ilgili yapacağınız altyapısal yatırımlar buralarda çok hızlı sonuçlar almanızı ve güvenlik seviyenizi de yüksek seviyeye çekmenize olanak sağlayacaktır.

Ben son olarak bir videoyla bitiriyor olacağım. Size çok teşekkür ederim sabrınız için. Ben çok genel olarak anlatmak istedim konuya olan bakışımızı. Sabrınız için teşekkür ederim. Bu konularla ilgili Microsoft olarak veya kişisel olarak yardımcı olabileceğimiz bir konu olursa, her zaman sizinle görüşmekten mutlu oluruz. İyi günler.

Video gösterimi

Sunucu

Sayın Ozan Öncel'e, değerli katkılarından dolayı çok teşekkür ederiz, çok güzel bir sunumdu. Değerli konuklar, şimdi ise BT Risk Kurucu Ortağı Sayın Fatih Emiral'ı, hacking senaryosunu sunmak üzere sahneye davet ediyoruz.

Fatih Emiral

Fatih Emiral (BT Risk Kurucu Ortağı)

Merhaba arkadaşlar. İsmim Fatih Emiral, BT Risk firmasının ortağıyım. Şimdi riskli bir şey yapacağım, Steve Jobs'ın bile başına geliyor, biliyorsunuz bazı kazalar olabilir. Savunma tarafıyla ilgili çok vakit geçiriyoruz, daha doğrusu illegal tarafta bulunmayan taraflar genelde bir bilgi güvenliği yönetim sistemi nasıl kurulabilir, sızma testleri nasıl yapılabilir gibi konulara değiniyor. Biz her zaman saldırganın yapabildiklerini yapamadan savunmanın mümkün olmadığını düşündüğümüz için, ilk ve son defa bir malware projesi geliştirdik. Bunu sosyal mühendislik senaryosundan başlatarak anlatmaya çalışacağım. Sunum sırasında tabii bazı şeyler size transparan olarak geçecek ama teknik olarak tabii her birisinin çok ciddi derinliği olmasına rağmen, bazı konulardan bahsedilmesi gerektiğini düşünüyorum. Bu başlıklardan da kısaca bahsedeceğim. Aksi takdirde alınan güvenlik ürünlerinin, çözümlerinin veya yaptırılan sızma testlerinin, saldırıların vs. ne kadar gerçekçi olabileceğini veya istenenle tam örtüşüp örtüşmediğini anlamak mümkün değil. Bu çalışmamızda yine özellikle BT yöneticileri için bir farkındalık eğitiminin bir parçası olarak biz düşünmüştük, onun parçası olacak. Çünkü biliyorsunuz pek çok ürün tanıtılıyor, testler anlatılıyor ama gerçekte ihtiyacın ne olduğunu anlamadan, algılamadan riski ciddiye almak pek mümkün olmuyor.

Senaryomuz aslında çok basit ve çok sıklıkla yaşanan bir senaryo. Sadece şunu vurgulamak istiyorum, güvenlik veya olayın black hat tarafında bulunan kişiler tanımlanırken, hep böyle bir kapüşonlu kıyafet, ergen yaşlarına yakın çocuklar falan resmedilir. Gerçek resim bu değil. Gerçek resmi şöyle tarif edeyim ben size; yılların teknoloji deneyimine sahip bir kişi olmadan, teknolojinin nasıl çalıştığı anlaşılmadan özgün bir saldırı aracı geliştirilemez. Yani gerçekte ülkelerin desteklediği vs. ciddi saldırganlar, emin olun 40 yaşının altında değildir. Ben de değilim. Engin Hocam işin defans tarafında çalışıyor ve ben de aslında bazı şeylere vurgu yapacağım, gerçekten saldırı tespit araçları veya saldırıdan şüphelenen araçların dikkatini çekmeden nasıl bir yol alabiliriz, bizim düşünce tarzımız da böyle saldırı perspektifiyle. Şimdi

senaryo çok basit aslında, stratejimiz insanları panik moduna sokulduktan sonra bütün filtrelerini ortadan kaldırıp her şeyi yaptıracak bir kıvama getirmek. Bu tür telefonla yapılan saldırıları bolca duyuyoruz.

Bunun phishing dediğimiz oltalama saldırısıyla yapılmasına ilişkin çok basit temel bir örnek göstereceğim ama dediğim gibi olayın biraz teknik boyutlarına girmek durumundayım. SMTP protokolü, yani e-mail haberleşmesi için kullanılan protokolde belli bir e-posta sahibinin adresinden gönderiliyormuş gibi bir e-posta göndermek için herhangi bir hosting almanıza gerek yok. Yani evinizde bir SMTP gateway kurup, relay server kurup bunun üzerinden bir e-mail atabilirsiniz. Türkiye'de bunu şöyle yapamazsınız ADSL kullanıcısıysanız, ADSL hattı sağlayan operatörler TCP 25 portunu kapattığı için, sebebi de bu, çok miktarda SPAM atıldığı için bu güvenilmez IP'lerin arkasından, çünkü her gün birisi alıyor IP'yi, bu mümkün değil. Ama bunu aşmak için buluttan birkaç saatliğine bir sunucu kiralayıp böyle de yapabilirsiniz ve "kimden (from)" adresini istediğiniz adres gibi gösterebilirsiniz. Buradaki önemli olan şey şu; niye gidip bir alan adı almak gerekebilir? Anti spam çözümlerinin, bu saldırıları engellemeye çalışan çözümlerin baktığı şeylerden bir tanesi bu. From şu domainden geliyorum diyor, nereden geldiği belli, o IP'nin bir isim kaydı var, DNS kaydı, reverse look-up kaydı dediğimiz PTR kaydı var, onunla karşılaştırmayı rahatlıkla yapabiliyor bu anti SPAM çözümleri. Eğer gördükleri alan isminde from alanında gördüğü domain ismiyle ilişkili bir kayıt yoksa, bunun risk derecesini bir miktar yukarı çıkartıyor ve SPAM olma ihtimalini artırıyor. Bunun için diyelim ki biliyorsunuz EDAŞ olarak geçer hemen hemen bütün elektrik dağıtım şirketlerinin sonu, Boğaziçi Elektrik Dağıtım A.Ş., Aras Elektrik Dağıtım A.Ş. vs. gerçekçiliğe de yakın bir şey olsun diye EDAŞ Elektrik.info diye bir domain satın aldık. Domainin fiyatı 4-5 dolar bir şey, bir yıllık kullanımı. Domain satın aldığımız yerde yine gerçekçiliği artırsın diye birtakım DNS kayıtları girdik. Bunlardan bir tanesi, mail sunucumuzun DNS kaydı.

Bu gelen mailin yasallaştırma ihtimalini artırmak için gerekli olan her şeyi yapıyoruz. Yani siz de bir şirket kursanız, bu isimde bir alan adı alsanız, e-mail sistemi, e-mail gönderip almak isteseniz benzer şeyleri yapacaksınız. İnternette bir bulut sağlayıcıdan kiraladığımız bir sunucunun IP'si bu, statik IP'si. www da linkin içinde geçeceği için, orada da yine gerçekçiliği artırmak için buna da bir alan tanımladık. Şurada MX kaydı dediğimiz, bu domainin gerçekten bir mail exchange sunucusu varmış gibi bir DNS kaydı daha tanımladık. Bunları şöyle kontrol ettiğimizde, EDAŞ elektrik info domainine baktığımızda, sanki gerçek bir şirketmiş gibi bir MX kaydı var. Www sorgulamıyoruz tabi, -A'da ANY kayıtları sorguluyoruz. Nameserver kayıtları da domain hizmetini aldığımız yerin kendi DNS sunucuları. Onda bir sıkıntı yok, yani birçok yer ISP'de tutabiliyor nameserver'ını.

İkinci aşama, bir bulut sunucusu sağlayıcısından sunucuyu kiralamak. Burada da kritik olan şey şu; sunucuyu kiralarken bu sunucu bulut sağlayıcısının IP aralığında, yani bulut sağlayıcısının sahip olduğu bir IP aralığında. Dolayısıyla bir anti SPAM çözümü bu IP'yi

sorgularken, gidip bu firmanın DNS sunucusuna soracak, bu IP'nin reverse kaydı var mı diye. O yüzden sunucuyu açarken, tanımlarken, mail.edaselektrik.info host name'i vererek açıyoruz. Bu bize nasıl bir sonuç sağlıyor, şöyle baktığımda yine reverse look-up kaydına baktığımda şu IP'nin, mail.edaselektrik.info olarak görüyorum. Yine anti SPAM çözümlerinin şüphe derecesini azaltmayı amaçladığımız bir adım.

Bir tane PHP uygulaması hazırladık. Bu da yine aldatmaya yönelik bir şey. Şöyle, birazdan mail mesajını göreceksiniz, mail mesajının içinde faturanızı görüntüleyin diye verdiğimiz link, gidip de bilmem ne exe değil, uyandırmasın diye saldırılan kişiyi. Gerçekten bir web uygulaması linki, PHP linki. Ama bu PHP uygulaması ne yapıyor, yaptığı şey çok basit, satır sayısından tahmin edilebileceği gibi. Gidiyor, şu fatura alt çizgi PDF nokta SCR, buna değineceğim daha sonra, bu dosyayı anında download etmesi için bir response doğuruyor. Yani gidip de dosyaya doğrudan tıklasaydınız da benzer bir response alacaktınız, bunu ben programatik olarak yapıyorum sadece. Mailimi hazırlıyorum, şurada mailde gördüğünüz gibi tabi yaparken gösterseydim daha net olabilirdi ama şurada from alanını istediğiniz gibi bir client ile düzenleyebilirsiniz. Fatura bilgi servisi, fatura info EDAŞ elektrik info, böyle bir account yok, kendime göndermişim. Kasım 2017 elektrik faturanız 1 milyon lira. Sayın Emiral, Kasım 2017 elektrik faturanızı incelemek için tıklayınız. Bakın bu link burada da yine anti SPAM çözümlerini uyandırmamak için alan adı gerçek, linkin arkasında bazen şey olur, ismi tıklayınız der, tıklayınızın arkasında başka bir URL vardır. URL ve metin aynen birbirini tutuyor, gittiğinde o link disable olmasın diye. Şu da bahsettiğim gibi fatura PHP sanki gerçekten bir uygulamayı çağırıyormuş gibi faturaydı, bunun hiçbir önemi yok zaten. Faturanızı zamanında ödemeyi unutmayınız diye mesajı gönderiyoruz. Aldığım mail şu; kullandığımız mail hosting şirketi herkesin bildiği bir şirket, anti SPAM kabiliyetleri çok güçlü, buna rağmen bu mesaj bana ulaştı. Çünkü sanki gerçekten bir şirket kurmuşum, gerçekten bir alan adım var, her şeyim legitimate, yani herhangi bir sıkıntı yaratacak, şüpheyi artıracak hiçbir şey yok. Bu nedenle bu olabilir. Ama alan adı almak zorunda da değilsiniz, o da ayrı, yani eğer bir anti SPAM çözümünüz yoksa, yine bu relay serverdan gönderilebilir.

Bu şekilde epostayı gönderdiğimde linkim geliyor, linkim aktif, tıklıyorum. Hiçbir şey görüntülenmiyor, belki arkada bir şeyler görüntüleyebilirdim, biraz daha inandırıcı olsun diye. Hemen download menüsü açılıyor. Download ediyoruz, burada yine aldatıcı faktörlerden bir tanesi; kullandığımız client işletim sisteminde default konfigürasyonda eklentileri göstermiyor. Eklentiyi şu application type kısmında biraz ifade ediyor ama normal bir kullanıcının bunu algılamasının zor olduğunu takdir edersiniz. Dolayısıyla ikon biraz belirleyici oluyor. Herhangi bir çalıştırılabilir dosyanın ikonunu da istediğiniz bir ikon olarak belirleyebiliyorsunuz. Dolayısıyla maili alıp da file sistemine indiren bir kişinin, bunun farklı bir dosya türü olduğunu algılaması çok kolay değil. Şimdi dosyanın uzantısı olan SCR konusuna da kısaca değineyim. Biz genelde EXE ve DLL'i biliriz çalıştırılabilir dosyalar olarak.

Bunun dışında çalıştırılabilir dosya uzantıları da var, bunlardan bir tanesi de screen saver'lar. Esasında bir EXE dosyasıyla SCR dosyasının arasında file formatı olarak, portable executable file formatı olarak hiçbir fark yok. Dolayısıyla bu da işletim sistemi için gayet çalıştırılabilir bir kod. Dosyayı kısaca incelediğimizde, resource bölümünde, yine bu dosya formatının bölümlerinden bir tanesinden bahsediyorum. İçinde PDF ikonlarının gömülü olduğunu görebiliriz. Bir başka ilginç nokta da RC data diye RAW data için genellikle kullanılan bir şey, resource adı. PDF içeriğine benzer bir içerik olduğunu da görebiliyoruz. Tabi bunu normal kullanıcı göremiyor, açıp bu şekilde o formatı incelediğinizde görmek mümkün. Şimdi dosyayı indirdim artık, bilgisayarımın üzerinde var.

Şimdi saldırgan platformuna geçiyorum arkadaşlar. Şu tarafta, hazırlık aşamasına. Aldığım IP adresi 1.175, gerçi bu geçen sefer de aynıydı ama ben şüphemiz kalmaması için tekrar IP adresimizi kontrol edeyim. Bu çalışırken yine bir es vereyim. Normalde artık oturup kendi saldırı kodunuzu yazma ihtiyacınız çok fazla değil. Ama ciddi bir saldırı kampanyası yürütecekseniz, hazır tool'ları kullanmanız da doğru değil. Normalde bunca zahmete girmeyip herhangi bir malware yazmadan, herhangi bir normal legitimate bir uygulamaya bir malware'i ekleyebilirdim. Metasploit denilen framework'ün imkânlarıyla. Fakat böyle bir dosyanın algılanması anti virüs çözümleri tarafından çok kolay, anti virüs çözümleri tarafından bilinen bir payloadlarçünkü bunlar. Fakat ben yine de şöyle bir özellik kullanıyorum malware'de, biraz sonra bastığımda çalışacak olan kod şunu yapacak; biraz önce resource bölümünde gösterdiğim o PDF dosyasını file sistemde bir yere drop edecek ve PDF reader bir uygulamayı başlatarak onu görüntüleyecek, dolayısıyla kullanıcı aslında gerçekten faturaymış diye onu görecek ve kapatacak. Ama bundan sonra ayrıca içinde barındırmadığı bir payload'u gidip başka bir sunucudan çekecek. Çekeceği sunucunun alan adı da şu, tabi bu sunucunun DNS kaydının olduğunu varsayın. Burada bilgisayar üzerinde bu aldatmacayı ben yapıyorum. Şurada IP'miz doğru, şu taraftaki IP ile aynı bakın buradaki IP. Btr-mlvsunucu.com'dan gidip bir payload çekecek. Bu payload kendi içinde olsaydı, anti virüsün onu tarayıp bu payload'u tanıması ihtimali vardı ki yüzde 99 tanırdı. Çünkü çok bilinen bir metasploit payload'unu kullanacağım. Metasploit payload'unu şu yüzden kullanıyorum, HD Moore diye birisinin geliştirdiği bir framework bu, başlattığı bir framework ve içinde gerçekten hackerların işlerini çok çok kolaylaştıran, bütün hacker dizilerinde filmlerinde göreceğiniz bir framework'ten bahsediyorum. Burada ürettiğimiz payload, bir meterpreter payload'u. Meterpreter payload'unun çok fazla fonksiyonu var, birazdan kullanacağız. Bu fonksiyonaliteyi geliştirmek mümkün olabilir miydi, olurdu ama çok zaman alırdı. Malware'in iskeletini biz oluşturduk ama gerçekte payload'u ben buradan çekeceğim. Bunun yerine benim yazacağım herhangi bir binary shell kod da çalışabilirdi. Gidip o sistem üzerinde bir user da yaratabilirdim. Meterpreter payload'unun yeteneklerini birazdan göreceksiniz, tabi bu söylediğim şeyler biraz havada kalabiliyor olabilir ama bahsetmeye değer yine de.

Zararlı yazılım, internet explorer'ın kendi bileşenlerini kullanarak bu HTTP erişimini sağlayacak. Bu ne demek, kullanıcının bilgisayarı bir proxy'nin arkasında olsa bile ve HTTP erişimi firewall'dan kısıtlanmış olsa bile proxy'in içinden gidip bu isteği yapacak ve payload'u alacak. Eğer web gateway mi diyelim ona artık, Proxy sunucunuzun bir anti malware özelliği yoksa, bu gayet legitimate bir istek, gider ve alır. Ama o gelen yanıtları inceleyen bir anti malware çözümünüz varsa web proxy'de, o zaman bunu yakalama ihtimaliniz artıyor. Bu da bir başka vektör. Şimdi burada payload'umu oluşturdum. Payload'umun sunulabilmesi için de basit hacker tool'larından bir tanesi, bir tane phyton modülünü kullanacağım. Tabi bu internette olsaydı, bunu bir apache web server'a koymuş olabilirdim mesela. Şu anda bu dizinin altındaki tüm dosyalara rahatlıkla ulaşılabilecek. Yapacağım şey şu; bu payload çalıştığında ne yapacak, kabaca anlatmaya çalışayım. Bu bir meterpreter payload'u ve reverse HTTP bağlantısı kuracak. Yani payload'u göndereceğim, saldırılan bilgisayarda çalışacak, tekrar bana bir tünel açacak geriye. Bu defa çok daha yetenekli bir tünelden bahsediyorum. Birincisi sadece payload'u almak için gelmişti, ikincisi bana bilgisayarın tüm kapılarını açacak bir tünel açacak. LVOS dediğim şey saldırganın sahip olduğu IP, şu porttan dinleyeceğim, yine açık olması ihtimali yüksek olan portlardan bir tanesi. HTTPS de olabilirdi ama bu HTTP içinden gelecek bağlantı. Şimdi asıl meterpreter payload'umu karşılayacak olan handler'ı çalıştıracağım. Gördüğünüz gibi tık tık tık bir şeyden bahsetmiyoruz, epey ön araştırması, çalışması yapılması gereken bir şey bu çalışma.

O yüzden ben genellikle şunu söylerim, bazen büyük holdinglerde IT denetim çalışmaları da yapıyoruz, tabi bunlara sebep olan şeyler genellikle IT süreçlerindeki eksikler, onu vurguladıktan sonra şunu da anlatmaya çalışıyorum. Güvenlik bilgisi aslında teknolojik inovasyon yapabilme kabiliyetini çok fazla artırıyor çünkü bütün bunları anlayabilmek ve yapabilmek için aslında teknolojinin nasıl çalıştığını çok iyi anlamak durumunda kalıyorsunuz. Teknolojinin nasıl çalıştığını anladıktan sonra da onu istediğiniz gibi eğip büküp yeni çözümler geliştirebiliyorsunuz. Şimdi metasploit framework'ün console arayüzünü açtım ve handler'ımı başlatıyorum. Şimdi göreceğiniz şeyler şunlar arkadaşlar, eğer bir terslik yaşamazsak; birinci olarak şu fatura PDF dosyasına çift tıkladığımda bir PDF dosyası açılacak. Hemen ardından şurada simple HTTP servera payload'u almak üzere bir istek gelecek. O payload alınacak, yine zararlı yazılımın gizlenme yöntemlerinden bir tanesi ama bir taraftan da kendini çok aşikâr eden bir özelliği. Ayrı bir proses olarak başlamayacak payload. Gidecek mevcut proseslerden bir tanesinin adres space'ine kendini inject edecek ve orada ayrı bir thread olarak başlatacak.

Özetle şunu söylemeye çalışıyorum; şu bilgisayarda task manager'ı açtığınızda, göreceğiniz proses isimleri arasında malware'in prosesi olmayacak çünkü var olan bir prosesin adres space'inde yaşamaya başlayacak. Evet, şimdi inşallah bir sıkıntı olmaz. Evet, faturamızı gördük, şu anda gördüm ve kapattım. Kullanıcı açısından bakın burada başka bir şey yok. Tabi malware tespitinde en önemli şeylerden bir tanesi, malware de bir yazılım ve çok hataya açık bir yazılım. Dolayısıyla kullanıcılar eğer şu proses sonlandı, şurada şöyle bir hata aldınız, şu

driver'ınız bilmem ne oldu gibi şeyler gördüğünüzde, büyük ihtimalle cihazınıza integrity'si düşük bir yazılım girmiş ve sisteminizi bozmaya başlamış. Saldırgan bunu bilerek yapmıyor olabilir ama kullanılan teknikler çok kompleks olduğu için hataya açık. Dolayısıyla bu gibi uyarıları çok dikkate almak gerekiyor. Eğer böyle bir şey olmaya başlıyorsa birinin bilgisayarında, orada bir anormallik var diyebiliriz. Şimdi takip edebildiyseniz eğer arkadaşlar, şurada HTTP isteğimiz geldi, 1.109'dan paket.bin isteği geldi ve gönderdik. Şurada da bir session açıldı, bu şu anlama geliyor, gerçekten çektiğimiz payload çalıştı ve bana geri tüneli açtı. Şimdi tünelle biraz çalışalım. Bu handler multi handler, istediğimiz kadar makineden buraya bağlantıyı karşılayabiliriz, session'lar arasında geçiş yapabiliriz. Bu ilk session'ımız olduğu için session 1'e geçiyorum. Şimdi şu anda neyle karşı karşıyayız, onu göstermek için biraz şunu yaptığımda herhalde daha rahat algılanabilir; bu taraf kurban, bu taraf saldırgan, şu anda kurbanın bilgisayarında bir Shell açtım, yani onun konsolunda komut satırında erişmişim gibi oraya eriştim. Mesela şu user'ın BTRT-1 olduğunu biliyorum ben, onun desktop'ına ulaşayım. Şuradaki dosyaları şu ana görebiliyorum. Mesela burada bir küçük bir dosya oluşturalım. Sağ tarafta ABC.txt diye bir dosyanın oluşması lazım. Şurada oluştu. Yani karşı taraftaki bilgisayardan, onun file sistemindeyim şu anda. Oradaki bir dosyayı download edebilirim, yine meterpreter payload'unun nimetlerinden faydalanarak. Burada çift ters slash karakteri kullanıyorum çünkü Linux için ters slash karakteri escape karakter demek. Ters slash'ı escape etmem lazım ki komut karşıya gitsin. Ticari sır diye bir dosyamız vardı. Tabi geri tuşuna bastım, burada şey karakter bozulmuş olabilir. Geldi. Bunu aldığım yer, şeyin altı olması lazım, direk root'un altı. Şu da ticarisir.txt mesela download ettim.

Daha ilgi çekebilecek şeylerden bir tanesi, bu bilgisayardaki kameradan görüntü alabilir miyim? Meterpreter payload'unu tercih etmemin sebeplerinden bir tanesi, bir sürü fonksiyonundan biri de bu. Bakalım o da çalışacak mı? Bu bilgisayar olduğunu görmeniz açısından şöyle çevireyim. Tabi burada aklınıza kamera ışığı yanıyor mu sorusu gelecek, yanıyor. Söndürebilir misiniz, eğer devlet seviyesinde bir saldırı yapıyorsanız söndürürsünüz. Nasıl söndürürsünüz, bu driver'ı inceleyecek yeterli zamanınız ve kaynağınız olur, driver'ı update edersiniz, driver da bu ışığı yakmayacak şekilde çalışabilir. Teorik olarak mümkün, pratikte böyle bir araç Windows için hazırda yok ama eğer kameranın bir kontrol uygulaması varsa onu kullanabilirsiniz. Olabilecekleri göstermek açısından bir örnek olarak gösteriyorum.

Yapabileceğimiz şeylerden bir başkası, parola hash'lerini mesela karşı taraftaki bilgisayarın parola hash'lerini elde etmeye çalışacağım. Benim kullandığım payload x86 32 bitlik bir payload, karşıdaki bilgisayar x64, 64 bitlik bir işletim sistemi. Hash'leri dump edebilmek için 64 bitlik bir prosese atlamam lazım. Şimdi öyle bir hedef proses bulacağım. Burada tabi kullanıcılara baktığımızda, şöyle getuid diyeyim, şu anda sisteme erişim için kullandığım user, BTRISK bilgisayarın ismi, BTR1 user'ıyla erişiyorum. Administrators grubunda bu user, bunu da kontrol edebiliriz çeşitli komutlarla. Ama biliyorsunuz, Windows'da belli bir noktadan sonra administrator grubunda olsanız bile sistem haklarını, yani nihai en

yüksek haklara erişemiyorsunuz. Burada tabi ben user access control'ü demo amaçlı bir miktar aşağı indirdiğim için bu geçiş mümkün olacak. Normalde default konfigürasyonda böyle bir şey söz konusu değil ama hash'leri dump edebilmek için bu geçişi yapmam lazım. Şimdi x64 olacak ve sistem user'ının sahip olduğu bir proses olacak. Ben bu prosesin address space'ine geçeceğim şimdi. Bu geçişler nasıl oluyor, arkada nasıl çalışıyor, bunlar işletim sisteminin zaten verdiği, sağladığı API'ler sayesinde oluyor. Yani burada hacker'ın yaptığı, olmamış bir yöntemi keşfetmiyor. İşletim sistemi bunu hot patching gibi çeşitli kompleks ihtiyaçlar dolayısıyla desteklemiş. Aslında fonksiyonalite destekleri bunlar, bunu saldırgan olarak ben kötüye kullanıyorum. Proses numarası 5444, şu SVCHOST'a geçeceğim bir sıkıntı olmazsa. Olmadı. Başka proses deneyeyim, olmaya da bilir bu arada. 7152'ye geçeyim. Sanırım session'ı kaybettim burada. Bir tane daha çalıştırıp deneyeceğim. Bu defa şu 5888'i hedef alayım. Tamam. Şu anda kimim, şu anda SYSTEM'im, SYSTEM kullanıcısı Windows sistemler için en yüksek seviyeye sahip kullanıcı. Şu post exploitation script'ini çalıştıracağım, yani tünelin içinden karşı tarafa başka şeyler yaptırmaya çalışıyorum artık. Normalde alabilmem lazım hash'leri. Hash dediğimiz şey, normalde plain text olarak tutmuyor sistemler parolaları. Parolaları hash'leyerek, yani irreversible bir algoritmayla başka bir şekle çeviriyor. Kontrol ederken de sizin girdiğiniz parola aynı algoritmadan geçirilip, saklananla tutuyor mu diye bakılıyor. Ama hash'lerde eğer salt dediğimiz ekstra bir faktör kullanılmıyorsa, bunların önceden bruteforce ile hesaplanmış hash'ler çok büyük database'lerde saklanabiliyor, bunlara rainbow table diyoruz.

Dolayısıyla şurada bilgisayarın administrator kullanıcı password'ünü, hash'ini, niye diğerini almıyorsunuz diyebilirsiniz. Birincisi hash LM hash'i, ikinci hash NTLM hash'i. Yine Windows belli bir seviyeden sonra LM hash'ten hesaplamayı bıraktı çünkü kırılması çok kolaydı, algoritması yöntemi günümüz işlem teknolojisine göre çok sağlam olmadığı için NTLM hash'leri kullanılıyor. Şuna baksaydık boş görecektik. Bunu da internetteki herhangi bir rainbow table sağlayıcısını kullanarak kırmaya çalışacağım. Eğer bu parola daha önceden kırılmışsa veya bu database'de varsa anında göreceğiz. Anladığımız kadarıyla bu NTLM şifresi, parola, işte A işaretleri @ ile çevrilmiş, O sıfır, L 1 ile çevrilmiş, bu da sistem adminlerinin çok kullandığı yöntemlerden bir tanesidir. Tabi kısa bir parola bu. Ama bir ihtimal bunu elde edebilirsiniz. Şunları unutmamak lazım, bunlar hep sanki hackerların müthiş başarılarıymış gibi algılanabiliyor. Aslında olay şuna dayanıyor, mesela Microsoft bu hash'lerin başına salt koymayı yapamaz mıydı, yapabilirdi. Ama neden feragat ederdi, Kerberos gibi single sign on'u destekleyen bir imkândan, tamamen bu hash'lerin salt'suz tutulmasına bağlı yani hem client'ın hem serverın aynı hash'i biliyor olması lazım. Eğer server salt'lu bir hash tutuyor olsaydı, bu başka bir değer olacaktı ve single sign on çalışmayacaktı.

Yani saldırganların yaptığı şey, altyapının dizaynını çok iyi anlayıp, öğrenip, bunu ben nasıl kendi avantajıma kullanabilirim, bunu incelemekten ibaret. Yani hackerların yaptığı şey aslında en temelde bilim adamlığı, öyle söyleyeyim. Bir sihirbazlık falan değil. Teknolojinin nasıl

çalıştığını anlıyor, hatta belki o kum havuzlarının üzerinde oynayan sistem admin'lerden, developer'lerden daha iyi anlıyor, anlamak zorunda. Arkada bunun nasıl çalıştığını anlamak zorunda, işte bu yüzden teknolojiyi geliştirmeyen bir ülkede bunları anlayan birilerinin çıkması ve bu tool'ları yazabilmesi çok mümkün değil. Biz de böyle işte meterpreter, metasploit vs. bunlara bakıp, dünyada neler oluyor diye ancak titriyoruz yerimizde, olan bu. Benim söyleyeceklerim bunlar. Çok heyecanlı bir şey gibi geldi mi size bilmiyorum ama bana sorarsanız bu sıkı çalışma ve kan ve gözyaşı. Çok teşekkür ederim.

Sunucu:

Sayın Fatih Emiral'a çok teşekkür ediyoruz. Gerçekten senaryo için.

Tüm konuşmacılarımıza da ayrıca teşekkür ediyoruz. Değerli konuklar, konferansımızın tüm katılımcılarımız için yararlı olduğunu umuyoruz. Programımız burada sona ermiştir. Katılımınız için hepinize çok teşekkür ederiz.

Teşekkürler:

"İş Hayatında Bilgi Güvenliği" konferansının açılış konuşmalarını gerçekleştiren Sayın Filiz Akdede ve Sayın Erol Bilecik'e, konuşmacılarımız Sayın Prof. Dr. Engin Kırda, Engin Özbay, Berna Kulaksız, ve Ozan Öncel'e çok teşekkür ederim. Ayrıca konfransın sonunda gerçekleştirdiği sızma senaryosu için Fatih Emiral'a çok teşekkür edrim.

Ayrıca konferansın hazırlanmasındaki desteklerinden dolayı TÜSİAD Yönetim Kurulu Üyesi ve Bilgi Toplumu, BİT ve İnovasyon Komisyonu Başkanı Esin Güral Argat'a, TÜSİAD Bilgi Teknolojileri Ve Telekomünikasyon Çalışma Grubu Başkanı Sayın Filiz Akdede'ye, TÜSİAD Genel Sekreter Yardımcısı Sayın Ebru Dicle'ye, TÜSİAD Bilgi Toplumu ve İnovasyon Bölümü Sorumlusu Sayın Yasemin Avcı'ya ve Uzman Yardımcısı Sayın Merve Uzunosman'a çok teşekkür ederim.

Konferansın organizasyonunu üstlenen Elektrooptik firmasına ve çalışanlarına çok teşekkür ederim.

Tüm Konferansın organizasyonu üstlenen ve bu raporun hazırlanmasında çok büyük katkıları bulanan BTF Uzmanı Sayın Ceren Yazıcı'ya çok teşekkür ederim.

Prof. Dr. H. Altay Güvenir
Bilkent Üniversitesi – TÜSİAD Bilgi Toplumu Forumu Direktörü