İŞTE TEKNOLOJİ

Yeni nesil savunma sistemlerini kullanan firmalar saldırılardan %45 daha az etkileniyor

Makine öğrenimi ve derin öğrenmenin kullanıcı aktivitelerinin analizi, anomali tespiti, kullanıcı karakter analizi gibi önemli savunma mekanizmalarında ciddi bir verimde çalıştığını söyleyen **Siber Güvenlik Federasyonu Başkanı Batuhan Tosun**, bu kavramların entegre olduğu yeni nesil savunma sistemlerini kullanan firmaların, saldırılardan yüzde 45 oranında daha az etkilendiğini aktardı.

Siber Güvenlik Federasyonu Başkanı Batuhan Tosun, profesyonel iş hayatına Amerika'da öğrenciliği sırasında siber güvenlik ve danışmanlık şirketlerinde zafiyet araştırmaları uzmanı ve güvenlik uzmanı olarak başladı. Bu esnada gördüğü fırsatlar ile kendi şirketini kuran Tosun, "New York, Los Angeles, Londra, Berlin ve Hong-Kong başta olmak üzere birçok lokasyonda kendi firmamın baş güvenlik mimarı olarak ekibim ile finans, medya, petrokimya ve üretim sektörlerinde danışmanlık, mühendislik ve güvenlik mimarisi tasarlama üzerine hizmetler verdik." diyerek şirketin faaliyetlerini paylaşıyor. 2011 yılından bu yana, merkezi Türkiye'de olan birçok ülke ve firmaya hizmet veren şirketlerini, siber güvenliğin büyümesi ve savunma sektörüyle birleşmesinden ötürü yüksek

Yerli ve milli ürünleri öne çıkararak, uluslararası arenada firmalarımıza profesyonel rekabet edebilecek mentorluğu ve ekosistemi sağlamayı amaçlıyoruz

ivmeyle sektörde yeri olan bir yapıya dönüştürdüklerini kaydeden Batuhan Tosun, şu anda siber güvenlik, yazılım, savunma ve dijital istihbarat teknolojileri alanlarında faaliyet gösteren şirketlerden oluşan grubun yönetim kurulu başkanlığını üstleniyor. Tosun ayrıca 2010 yılından bu yana Portland, Oregon merkezli dünyanın en büyük siber güvenlik derneği ISSA'nın Türkiye başkanlığını da yürütüyor.

Batuhan Tosun ile sohbetimiz, Siber Güvenlik Federasyonu'nun daha yakından tanımakla başladı. Devamında ise siber güvenliği, dijital dönüşüm sırasındaki güvenlik unsurlarını ve yeni nesil teknolojilerin siber savunmaya katkılarını kapsamlı bir şekilde masaya yatırdık...

Siber Güvenlik Federasyonu ulusal ve uluslararası güvenlik faaliyetleri gösterme hedefinde olan bir yapı ve farklı organizasyonlarla da ortak projeler yürütüyor, eğitimler veriyor. Burada, Federasyonu'nun amaçlarını ve çalışmalarını sizden detaylıca dinlemek isteriz...

Federasyonumuzun amacı, özellikle yerli ve milli ürünleri öne çıkararak uluslararası arenada firmalarımıza profesyonel rekabet edebilecek mentorluğu ve ekosistemi sağlamak. Bu noktada, akreditasyon ve sertifikasyon süreçlerimiz başta olmak üzere birçok ülkeden temsilcilikler ile teknolojik erişebilirliği kolaylaştırmak istiyoruz. Şu ana kadar 6 farklı ülke ile temsilcilik anlaşmalarımızı tamamladık ve 11 ülke ile daha görüşmelerimiz devam ediyor. Haziran ayındaki kurul toplantımızda bunları da duyuruyor olacağız.

Amacımız; sürdürülebilir ve erişebilirliği yüksek, kaliteli ve oyun kurucu role sahip olarak Türki Cumhuriyetler başta olmak üzere Afrika, Orta Doğu, Avrupa, Orta ve Güney Amerika'nın da bir kısmını içerisine alan bir ekosistem geliştirmek. Bu bağlamda, aşağıdan gelen kişileri de bağlılığı yüksek şekilde ekosistemde tutmak amacıyla eğitimler, kamplar, yarışmalar, sertifikasyon programları ve burslar organize edeceğiz.

Dünya Ekonomik Forumu'nun rakamlarına göre, pandemi döneminde Türkiye 110 binin üzerinde atakla karşılaştı. Bu siber saldırıları ve savunma mekanizmalarını nasıl değerlendirirsiniz? Siber Güvenlik Federasyonu olarak saldırıları önlemek adına kamu-özel sektör ile ne tür çalışmalarınız bulunuyor?

Son 3 ayda Türkiye'de büyük ölçekli 83 şirketin hasar etkisi yüksek siber saldırıya maruz

Artık "sibervatan" dediğimiz bir kavram mevcut. Kara, hava ya da deniz sınırlarınızı ne kadar korursanız koruyun verilerinizi ve dijital iletişim altyapınızı koruyamazsanız çok büyük zafiyetler vermiş oluyorsunuz

kaldığını biliyoruz. Dünyada ve diğer ülkelerde bu rakamlar çok daha yüksek. Pandemi süreci firmalar için de teknolojik açıdan maliyetli bir eğitim süreci oldu. Ancak bu dönemde teknolojik altyapının ve siber güvenliğin önemi, yeteri kadar olmasa da şu ana kadar hiç fark edilmediği kadar öğrenildi. Tabi bu öğrenim süreci acı bir tecrübeyle oldu ancak her ülke bu süreçlerden geçti. Özellikle Türkiye'deki özel sektör kuruluşları ve en çok da finans kuruluşları, sadece ürün satın alarak siber güvenliğin tam olarak sağlanmadığını fark etti. Diğer ülkelere kıyasla, Türkiye'de belirli hacmin üzerindeki özel sektör kuruluşları, donanım ve yazılım bazlı siber güvenlik yatırımları yapmasına karşın, siber güvenlik odaklı test, danışmanlık, mimari ve kültür entegrasyonu olmadan bu yatırımların çok da etkili olmadığını görmüş oldu.

Federasyon olarak bu süreçte, proaktif güvenlik olarak değerlendirdiğimiz siber istihbarat faaliyetlerimiz ile başta kamu kurumlarımız olmak üzere birçok kuruma destek olduk ve destek olmaya da devam ediyoruz. Bu vesile ile buradan da bir çağrıda bulunmak isterim: Kurum ve kuruluşlar 7/24, 365 gün telefon ve e-mail yoluyla tarafımıza ulaşabilir ve bizlerden anlık olarak destek alabilirler. Özellikle siber istihbarat anlamında, saldırının önceden bilgilendirilmesi noktasında kurumlar bizimle iletişime geçtikleri takdirde ücretsiz bir şekilde asli kamu görevi olarak destek oluyoruz.

Siber güvenlik artık ülke sınırları kadar mühim bir savunma alanı haline geldi. Siber güvenlik yatırımları da dijital transformasyonun ayrılmaz bir parçası oldu.

Bu dönüşüm süreci ile siber güvenlik kombinasyonu sizce nasıl ilerlemeli?

Artık "sibervatan" dediğimiz bir kavram mevcut. Kara, hava ya da deniz sınırlarınızı ne kadar korursanız koruyun verilerinizi ve dijital iletişim altyapınızı koruyamazsanız çok büyük zafiyetler vermiş oluyorsunuz. Dolayısı ile siber güvenlik, bilgi güvenliği ve dijital istihbarat noktalarının hem uygulamada hem uygulama sonuçlarının fiiliyatta kullanılmasında hem de standardizasyon anlamında geliştirilmesi gerekmekte. Ülkemizde dijital dönüşüm olarak adlandırılan süreçler şu an için büyük çoğunlukla dijital erişim, elektronik belge

> ***Yapay zekanın güvenlik süreçlerindeki kullanımı arttıkça bu alandaki verim yüzde 80'leri bulacak***

ve eşleştirme ile bilgiye kolay, hızlı ve bütünlüğü bozulmadan erişilmesi. Lakin gerekli siber güvenlik kurgusu ve mimarisi sağlanmadan bu hızlı ilerleme yaşanırsa, bu hız bizlerin de felaketi olabilir. Özellikle özel sektörün bu bağlamda kendini geliştirmesi çok önemli. Diğer ülkelere nazaran ülkemizde kamu kurumları bu konuda çok yetkin ve farkındalığı yüksek; ancak özel sektörün de aynı seviyeye gelmesi hatta diğer ülkelerdeki gibi inovatif metodlar ile kendilerini geliştiren süreçlere adapte olmaları gerekiyor.

Pandemi sürecinde hackerların canı iyice sıkıldı. Her yere saldırmaya başladılar, yeni metodlar, zafiyetler geliştirdiler ve kurumlardan çok daha hızlı ve efektif çalıştıkları için bu durum bazı kuruluşlar için yıkım düzeyinde oldu. Bu noktada da şirketlerde hazırlıksız yakalanma durumu oluştu. Özellikle uzaktan çalışma altyapısı müsait olmayan ya da güvenlik açısından elverişli olmayan kurumlar sadece hackerların saldırısı değil, ciddi bir iç saldırıya yani fraud'da da maruz kaldılar. Bu noktada özellikle kayıt mekanizmaları ve iç kontrol mekanizmalarının da geliştirilmesi ciddi önem arz ediyor.

Siber saldırıları önlemek için altyapının yanında istihdamı artırmaya yönelik ne gibi teşvikler yapılmalı/ yapılıyor?

Federasyon olarak insan kaynağına çok önem veriyoruz. Bu konuda bir düşünce kuruluşu olan TÜSİDAM'ın (Türkiye Stratejik Teknoloji Dönüşümleri Araştırma Merkezi) başlattığı ve Dijital Dönüşüm Ofisi himayelerinde organize edilen, 2016 yılından bu yana devam eden 81 İlde 81 Siber Kahraman projesiyle ortaklıklar gerçekleştirdik. Şu ana kadar 150 binden fazla öğrenciye ulaştık. 1000'den fazla öğrenciyi farklı seviyelere göre mezun ettik. Uzun dönemli sertifika ve kamp programları geliştirdik ve geliştirmeye devam ediyoruz. Pandemi sürecinde de eğitimlerimize, kamplarımıza uzaktan eğitim metoduyla devam ettik. Kaliteli beyaz şapkalı hacker yetiştirmek için diğer ülkelerin izlediği gibi 13-17 yaş arasındaki gençlere ulaştık ve içlerinden çok kaliteli uzmanlar yetiştirdik. Böyle bir programı Türkiye'de ilk biz başlattık ve aynı kalite ve sürdürülebilirlikte devam ettiren tek kurumuz. Öğrencilerimizin tüm ihtiyaçları ile ilgileniyor, velileriyle de iletişimde kalıyoruz. Öğrencilerimiz hem okullarından geri kalmıyor hem de okulları bittiğinde kaliteli bir siber güvenlik uzmanı olarak mezun oluyorlar.

Son olarak, yeni nesil teknolojilerin siber savunma alanına sizce katkıları neler olacak?

Yapay zeka, güvenlik süreçlerinde özellikle ürün altyapılarında son 2 yıldır kullanılıyor. Ancak bu verim şu an için elbette yüzde 20'leri geçmiyor. Firmalar bunu biraz daha pazarlama amacıyla kullanıyor ancak uygulama alanının gelişmesiyle önümüzdeki yıllarda bu oran yüzde 80'leri bulacaktır. Lakin, özellikle makine öğrenmesi ve derin öğrenme kavramları, kullanıcı aktivitelerinin analiz edilmesi, anomali tespiti, kullanıcı karakter analizi gibi çok önemli savunma mekanizmalarında ciddi bir verimde çalışıyor. Bu kavramların entegre olduğu yeni nesil savunma sistemlerini kullanan firmalar, saldırılardan yüzde 45 oranında daha az etkileniyor ki bu oran azımsanmayacak bir oran. Blok zinciri ise bilginin bütünlüğünü korumak için çok önemli bir süreçsel güvenlik yönetimi. Örneğin; noter, bankacılık, hukuk işleri, e-devlet gibi konularda Belçika, Almanya ve İsviçre'de çok güzel örnekler mevcut. Blok zinciri verinin bozulmaya uğratılması ve değiştirilmesi gibi zararları, gelebilecek saldırılarda atak alanı yüzeyini çok minimize ettiği için çok yüksek oranda düşürüyor. Yakın zamanda ülkemizde de örneklerini görmeye başlayacağız.

Tüm bu yeni teknolojiler ile birlikte güvenlikte yeni bir döneme giriyoruz. Lakin şunu da unutmamak gerekir ki; saldırganlar da bununla birlikte yeni bir döneme giriyor ve saldırı metodlarını bunlara göre güncelliyor olacaklar. Bu nedenle %100 güvenlikten ne yazık ki hiçbir zaman bahsedemeyeceğiz.