18 TEMMUZ'DAKİ YAZILIM KRİZİNDEN ÇIKAN DERS

Veri güvenliğinin kilidi sağlam olmalı

18 Temmuz Cuma, dünya için tarihi bir gün olarak kayıtlara geçti. O gün yaşanan tarihin en yaygın yazılım krizi, havacılıktan sağlığa, perakendeye kadar farklı alanlarda hizmet alan yüz milyonlarca insanı, ABD'den Avustralya'ya uzanan geniş coğrafyada etkisi altına aldı. Verinin üçte ikisinin birkaç büyük şirketin elinde bulunması, şirketler açısından dijitalleşmenin temel konusu güvenliği, en kilit noktaya taşıyor.

Gelecek 5 yıl içerisinde 5G teknolojilerinin tam anlamıyla devrede olması, blokzinciri, kuantum bilgisayarlar gibi erişkin cihazların yaygın şekilde kullanılması, bulut sistemler ve IOT cihazların daha da yaygınlaşması ile birlikte veri üreten ve barındıran tüm sektörler uçtan uca bilgi teknolojileri ile entegre hale gelecek. Bugüne göre çok daha fazla veri üretilecek, işlenecek ve depolanarak, korunmaya çalışılacak.

Siber güvenlik, 4 yılda iki kattan fazla büyüyen ve gelecek 4 yılda da 2,27 kat daha büyümesi öngörülen veri miktarı düşünüldüğünde, en temel gündem olarak karşımızda duruyor. Dünya genelinde veri miktarı, 2024 yılı başında sadece 4 yıllık bir sürede benzersiz verilerin 7.51 Zettabayt artışı ile 13.41 Zettabayt seviyesine ulaştı. Yani çeşitli büyük veri ve yapay zeka uygulamalarında kullanmak üzere 4 yıllık süre içerisinde 2.27 kat daha fazla veri saklanacak ve bir o kadar daha fazla verinin saldırıya uğramaması için gerekli tedbirlerin alınması gerekecek.

Veri güvenliği, dünyada ulusal güvenlik sorunu ile bir tutuluyor. İşin özel sektör yanı olduğu kadar, kamu kurum ve kuruluşlarına yönelik tehditler de doğal olarak bir o kadar kritik görülüyor. Tüm bunların yanı sıra kişi güvenliği de bu noktada devreye giriyor. Başkalarının elinde bulunan kişisel veriler, korunmaya muhtaç alanların başında geliyor.

Gerek kamu kurumları ve gerekse özel sektör kuruluşları, artan veri miktarı ile birlikte güvenliğin sağlanması

adına eğitim ve yetkinliklerini ne kadar artırırsa artırsın, artan veri miktarı kötü niyetli bakışların açık saldırı alanını oluşturuyor. Yapılan hesaplamalar gösteriyor ki dünya genelinde dakikada dört şirket siber saldırılara maruz kalıyor. Her geçen gün güvenlik birimleri kötü amaçlı yazılımlara karşı antivirüs uygulamaları ve koruma araçları geliştirse de saldırganlar tarafından günde ortalama 560.000 yeni kötü amaçlı yazılım piyasaya sürülüyor.

Türkiye de birden fazla nedenden ötürü bu sorundan yüksek oranda nasibini alıyor. Ülkemizin dünya coğrafyasındaki kritik yeri, diğer yandan teknoloji alanındaki performansı, saldırıların açık hedefi olmasında en önemli iki unsur. Türkiye'de de kurumlar ya da şahıslar, her 6,24 dakikada bir siber saldırıya uğruyor. Bu dünya ortalamasının altında kalıyor gibi görünse de yine de yüksek bir oran.

Ulaştırma ve Altyapı Bakanlığı tarafından yapılan açıklamaya göre 2020 yılında 118 bin 470 siber saldırı gerçekleşirken, bu sayı 2021'de 84 bin 113'e geriledi. Ülkemizde, bu konuyu son derece ciddiye alan kamu kurumlarının varlığı, saldırı oranının düşürülmesinde en önemli önleyici ve caydırıcı güç olarak hizmet üretiyor. Yapılan yatırımlar ve gelişen altyapı sayesinde her yıl düzenli olarak yapılan Global Siber Güvenlik İndeksi çalışmasında Türkiye yakaladığı ivme ile dünya sıralamasında 11. sıraya kadar yükseldi.

Her şirket, siber güvenlik stratejisi oluşturmalı

Türkiye'de kurumların en çok maruz kaldığı siber saldırı türü fidye yazılımları. Dark Web forumlarında Türk kurumlarından sızan verileri içeren 40'tan fazla liste bulunuyor. Bu listelerin yüzde 30'u müşteri veri tabanı, yüzde 11'i ise yetkisiz ağ erişimi verilerinden oluşuyor. Eset Türkiye COO'su Erkan Tuğral, "Yine Dark web forumları ve pazar yerlerinde Türk kullanıcılara ait 1 milyardan fazla açık, şifrelenmemiş oturum açma bilgisi görülüyor. Sorun bu kadar büyükken ilk yapılması gereken şirketlerin bir siber güvenlik stratejileri geliştirmesinden geçiyor" diyor.

Peki, yapılması gerekenler neler? Erkan Tuğral, bu noktada şu değerlendirmelerde bulunuyor:

"Büyük şirketlerde, şirketin siber güvenliğini denetleyen ve etkin stratejiler oluşturan departmanlar genellikle var. KOBİ'lerin ise birçoğunda, çalışanlar arasında dijital güvenlik stratejisinden sorumlu az sayıda personel bulunuyor. Kurumlar öncelikle "En önemli güvenlik açıklarını belirlemeyi içeren risk tabanlı bir yaklaşım benimsemeliler."

Siber güvenlik stratejisini oluşturacak beş ana başlık:

- Verilerin korunması ve şifrelenmesi
- Kullanıcılar için kısıtlı erişim kurallarının oluşturulması
- Çok katmanlı uç nokta güvenliği sağlanması
- Tüm cihazlarda çok faktörlü kimlik doğrulamasının (MFA) bulunması
- Tüm işletim sistemlerinin en son sürümlerinin kullanılması

Siber güvenliğe yapay zekâ uygulamaları yön verecek

Yapay zekâ, her sektöre yeni bir bakış açısı kazandırmaya başladı. Bu gerçeklik, siber güvenlik uygulamaları için de geçerli. Öyle ki yapay zekâdaki gelişmeleri hem güvenlik birimleri, hem de tehdit aktörleri yakından takip ediyor. Dijital yatırımlar yıllar içinde artıkça sürdürülebilir büyümeyi ve rekabet avantajını desteklemek için BT sistemlerine olan güven de arttı. Ağ savunucuları, siber tehditleri önleyemez ya da hızla tespit edip kontrol altına alamazlarsa kurumlarının büyük mali ve itibar kaybına uğrayabileceğini biliyor. Günümüzde bir veri ihlalinin maliyeti ortalama 4,45 milyon dolar. Ancak hizmet kesintisi ve veri hırsızlığı içeren ciddi bir fidye yazılımı ihlali bunun çok daha fazlasına mal olabilir. Bir tahmine göre sadece finans kurumları 2018'den bu yana hizmet kesintisi nedeniyle 32 milyar dolar kaybetti.

Yapay zekâ siber saldırılarda nasıl kullanılıyor?

- **Sosyal mühendislik:** GenAI'ın en belirgin kullanım alanlarından biri, tehdit aktörlerinin büyük ölçekte son derece ikna edici ve neredeyse gramatik olarak mükemmel kimlik avı kampanyaları oluşturmasına yardımcı olmak.
- **BEC ve diğer dolandırıcılıklar:** GenAI teknolojisi bir kez daha, belirli bir kişi ya da kurumsal kişiliğin yazı stilini taklit etmek, kurbanı kandırarak para havalesi yaptırmak ya da hassas verileri teslim etmesini sağlamak için kullanılabilir. Deepfake ses ve video da aynı amaçla kullanılabilir.
- **Dezenformasyon:** GenAI, etki operasyonları için içerik yaratma işinin ağır yükünü de ortadan kaldırabilir. Yakın tarihli bir rapor, Rusya'nın bu tür taktikleri halihazırda kullandığı konusunda uyarıda bulundu ki bu taktikler başarılı bulunursa geniş çapta tekrarlanabilir.

Yapay zekâ güvenlik ekipleri tarafından gelecekte nasıl kullanılabilir?

- **Tehdit istihbaratı:** LLM destekli GenAI asistanları, analistler için temel noktaları ve eyleme geçirilebilir, çıkarımları sade bir İngilizce ile özetlemek için yoğun teknik raporları analiz ederek karmaşık olanı basitleştirebilir.
- **Yapay zekâ asistanları:** BT sistemlerine yapay zekâ "yardımcı pilotları" yerleştirmek, kuruluşları saldırıya maruz bırakacak tehlikeli yanlış yapılandırmaları ortadan kaldırmaya yardımcı olabilir. BÖrneğin, bulut platformları gibi genel BT sistemleri içerisinde yer alan ve güvenlik duvarları gibi karmaşık ayarların güncellenmesinde kullanılacak güvenlik araçları için de işe yarayabilir.
- **SOC üretkenliğini güçlendirmek:** Günümüzün Güvenlik Operasyon Merkezi (SOC) analistleri, gelen tehditleri hızla tespit etmek, yanıtlamak ve kontrol altına almak için büyük bir baskı altında. Saldırı yüzeyinin büyüklüğü ve uyarı üreten araçların sayısı çoğu zaman bunaltıcı olabiliyor. Bu, analistler zamanlarını yanlış pozitiflerle harcarken meşru tehditlerin radara yakalanmadığı anlamına gelir. Yapay zekâ, bu tür uyarıları bağlamsallaştırarak ve önceliklendirerek ve hatta muhtemelen küçük uyarıları çözerek yükü hafifletebilir.
- **Yeni tespitler:** Tehdit aktörleri taktiklerini, tekniklerini ve prosedürlerini (TTP'ler) sürekli olarak geliştirmektedir. Ancak yapay zekâ araçları, risk göstergelerini (IoC'ler) kamuya açık bilgiler ve tehdit yayınlarıyla birleştirme yaparak en yeni tehditleri tarayabilir.

USOM ve SOME'den Kasırga sistemiyle tam güvenli koruma

Ulaştırma ve Altyapı Bakanlığı'na bağlı Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet yürüten Ulusal Siber Olaylara Müdahale Merkezi (USOM), 27 Mayıs 2013 tarihinde hizmete girdi. 2013-2014 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı çerçevesinde de kamu kurum ve kuruluşları bünyesinde Siber Olaylara Müdahale Ekipleri (SOME) oluşturuldu. Siber saldırılara ilişkin 7/24 mücadele içinde olan kurumlar, ilgilisinin farkına dahi varmadığı tehditlere ilişkin dünya çapında hizmetler sunuyor. 17 milyon IP adresi radar mantığı ile taranıyor. Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu, 2023 yılında 140 bin büyük saldırının USOM sayesinde engellendiğini kaydetti. Uraloğlu, "Her gün yaklaşık 422 büyük saldırı ve 11 milyondan fazla zararlı erişim isteği engelleniyor. USOM'un yerli ve milli imkanlarla ürettiği Kasırga sistemi, yaklaşık 40 dakikada 17 milyon IP adresini 1000'den fazla zafiyeti tüm portlarıyla tarayabiliyor" dedi.

10 adımda güvenlik

Güvenlik yalnızca siber saldırılara yönelik düşünülmemeli; arızalardan performans düşüşlerine, sistem sorunlarından kullanım hatalarına kadar bir dizi farklı sorun için de koruma yöntemi olarak planlanmalıdır.

1- Öncelikle şirketin yürüttüğü faaliyetlere, uzmanlık alanlarına, fiziki yapısına uygun gelecek şekilde bir risk haritası çıkarılmalıdır.

2- İşletme genelinde uygulanacak siber güvenlik politikaları ve şemaları oluşturulmalı, görev tanımları ve sorumluluk alanları net şekilde ortaya konmalıdır.

3- Yürütülecek önlem çalışmaları içerisinde ilk sıraya sistem güncellemelerini koymak gerekir. Bu konuda süreç çok hızlı yönetilmelidir. Tehdit unsurları, kötü niyetli teknikler veya kodlar yaratırken siber güvenlik şirketleri tespit yöntemlerini ayarlayarak bunlara yanıt verir. Bu güncellemelerin tehdit dağılımına uyacak şekilde hızla dağıtılması gerekir.

4- Siber saldırılara karşı güvenlik duvarları da önemli bariyerler oluşturur. Antivirüs yazılımlar devreye alınır. Ağ trafiği denetimi altına alınarak filtre mekanizması devreye girer, böylelikle yetkisiz erişimler ve kötü niyetli saldırılar engellenir.

5- Uç nokta koruması, siber güvenlik yatırımının en önemli parçalarından birisidir. Güvenilir ve iş sürecine müdahalede bulunmayan uç nokta koruması seçmek çok önemlidir. İşletmeler, en uygun uç nokta koruması için referans sahibi, deneyimli kuruluşlar arasından seçim yapmalıdır.

6- Verilerin düzenli olarak yedeklenmesi ve siber saldırı durumunda hızlı bir şekilde geri yüklenebilmesi için etkili bir yedekleme ve kurtarma planı oluşturulmalıdır. Verilere ve sistemlere erişim, yalnızca yetkilendirilmiş kişilerle sınırlandırılmalı, güçlü şifreleme ve iki faktörlü kimlik doğrulama yöntemleri kullanılmalıdır. Düzenli denetimler ve sızma testleri yapılmalıdır.

7- Sistemler bir sıkıntı yaşarken, her zaman sinyal veya uyarı vermez. Bu açıdan dönem dönem testler yapmak gerekir. Bağımsız test sonuçları bu konuda şirketlere en iyi rehberdir. Doğru yöntemler eşliğinde testler mutlaka yapılmalıdır.

8- Veriler düzenli olarak yedeklenmeli, siber saldırı durumunda hızlı şekilde geri yüklenebilmesi için etkili bir yedekleme ve kurtarma planı hazırda tutulmalıdır.

9- Bulut üzerinden BT güvenliği sağlamak pratik, rahat ve kolaydır. Ek bir donanım ya da yazılıma gerek duyulmadığı için bu yöntem aynı zamanda uygun maliyetlidir.

10- Şifreler sık aralıklarla değiştirilmeli, bilgi erişimleri sınırlanmalı, çalışanlara siber güvenlik ve tehdit konularında düzenli eğitimler verilmeli.

En çok etkilenen sektörler

Siber saldırılardan en çok dijital tabanlı sektörler etkileniyor

- Finans
- Telekomünikasyon
- Havacılık
- Enerji
- Sağlık