thinktech
STM Teknolojik Düşünce Merkezi

Siber Güvenlik Yapay Zeka ve Makine Öğrenmesi ile Yeniden Şekilleniyor

Çağımızın en başarılı uygulamaları arasında görülen Uber'ın özellikle Orta Doğu'daki en büyük rakibi olan Dubai merkezli Careem'e düzenlenen siber saldırı sonrasında kişisel veri güvenliği konusu Türkiye'de tekrar gündeme geldi. 14 Ocak tarihinde yapılan ve Nisan ayı sonunda duyurulan saldırı sonucunda aralarında Türk müşterilerin de olduğu 14 milyon kişinin isimleri, mail adresleri, telefon numaralı ve yolculuk kayıtları çalındı. Careem, şifre ve kredi kartı bilgilerinin çalınmadığını belirtti ve kullanıcıların bu duyuruya riayet etmekten başka çaresi yoktu. 78 şehirde 600 bine yakın şoförle çalışan; Suudi Arabistan, Türkiye, Pakistan ve Kuzey Afrika gibi ülkelerde çok popüler olan Careem'e yapılan saldırının böyle kapsamlı bir başarıya ulaşması, her gün pek çok uygulamayla paylaştığımız verilerin aslında çok da emin ellerde olmadığının bir başka kanıtı oldu.

IEEE ve Kanadalı teknoloji danışmanlığı firması Syntegrity'nin ortaklaşa oluşturduğu "Siber Güvenlikte Yapay Zekâ ve Makine Öğrenmesi Kullanımı" başlıklı rapor da tam olarak bunu ele alıyor. Raporda, siber güvenliği bekleyen tehlikeler ve bu tehlikeler karşısında savunmaya geçmek durumunda kalacak şirketlerce alınabilecek önlemler sıralanıyor.

Siber Saldırılar Artık Eskisinden Çok Daha Güçlü

Rapor, saldırı programlarının eskiden manuel olarak oluşturulan yazılımlar olduğunu, ancak son dönemde gerçekleşen saldırıların yeterli finansmana sahip, tecrübeli gruplarca yapıldığına dikkat çekerek başlıyor. Dolayısıyla saldırının kapsamı ve hızı eskisine göre çok daha gelişmiş durumda. Eskiden manuel olarak bulunan sistem açıklarına yapılan saldırılar tek bir bilgisayarı etkilerken, bugün tek bir açık bularak dünyanın dört bir yanında internete bağlı cihazlara erişim sağlanabiliyor. Birbirine bağlı tüm bu cihazlarla saldırılar sadece dijital dünyayı değil, nesnelerin interneti ve sosyal medya aracılığıyla gerçek dünyayı da etkileyebiliyor. Dahası; kredi kartı bilgilerinizin başkalarının eline geçmesiyle birikiminizi kaybetme ihtimaliniz dahi söz konusu olabiliyor. Raporda, bugün 1 milyarlık cihaz nüfusunun sadece yüzde 1'ini etkileyecek bir açığın, 10 milyon cihaza sızılmasına neden olacağına dikkat çekiliyor.

Yapay Zekâ ve Makine Öğrenmesi Kullanımı Artık Bir Zorunluluk

Peki siber saldırı tehdidine karşı ne yapabiliriz? Daha doğrusu, şirketler bu saldırılara karşı kendilerini ve dolayısıyla bizim kişisel bilgilerimizi korumak için neler yapmalı? IEEE ve Syntegrity'nin raporunda kişisel veri güvenliğini sağlamak için yapay zekâ ve makine öğrenmesinin kullanılmasının artık bir zorunluluk haline geldiğinin altı çiziliyor. Bu teknolojiler siber güvenlik sistemlerini güçlendirerek, savunmanın çok daha kapsamlı ve hızlı olmasını sağlayabilir.

Yani yapay zekâ ve makine öğrenmesini kullanmak veri güvenliği için sınıf atlamamızı sağlayabilir. Peki veri güvenliğinin kötü aktörleri bundan haberdar değil mi dersiniz? Rapora göre, siber saldırılarda bu teknolojilerin bugün kullanılmıyorsa bile, yakın gelecekte kullanılmaya başlanacağına kesin gözüyle bakılıyor. Bu gelişmiş saldırılara, bu teknolojileri kullanmadan gerekli savunmanın yapılmasına, neredeyse imkânsız gözüyle bakılıyor.

6 Maddede Siber Güvenliğe Teknolojik Dokunuş

Raporda, yapay zekâ ve makine öğrenmesinin siber güvenlikte kullanımı altı farklı boyutta ele alınıyor. Bunlar:

1. Yasal ve politik konular
2. İnsan faktörü
3. Veri
4. Donanım
5. Yazılım ve algoritmalar
6. Operasyonelleşme

Şimdi bu boyutlara biraz daha detaylı bakalım:

1) YASAL DÜZENLEMELER GELİŞMELERİN HIZINA UYAMIYOR

Raporda endüstri, akademi, standardizasyon kuruluşlarına ve hükümetlere yönelik öneriler sıralanıyor. Raporda, gelişmiş yapay zekâ ve makine öğrenmesi teknolojilerinin ulusal güvenlik, ekonomik stabilite ve sosyal yapılara geri dönülemez zararlar verebileceğine dikkat çekiliyor. Bu sebeple raporda, yasal ve etik kısıtlamaların gerekli olduğu vurgulanıyor.

En Basit Yapay Zekâ, Gelişmiş Savunma Sistemlerini Yenebilir

Yapay zekâ ve makine öğrenmesi üzerine çalışan bireylerin, kapsamlı bir analiz ve testten geçirmedikleri sürece bu kodları paylaşması sorun olabilir. Yapay zekâda sonradan yapılacak güncellemelerde kusurların giderilmesi hem zor, hem de bu süreçte çok ciddi sorunlar yaşanabilir. Yapay zekânın sınırlarına dair şu örneği verebiliriz: 2016 yılında Mirai botnet, DDOS saldırılarına yeni bir soluk getirdi. Zira bu saldırılar IOT cihazlarındaki bir açıklığı istismar edilerek oluşturulan botnetler ile yapılıyordu. Oldukça düşük işlemci gücüne sahip bu botnetler internetin en iyi savunma sistemlerine sahip sitelerini devre dışı bırakabildi. Kısıtlı teknolojiyle bu olabiliyorsa, çok daha gelişmiş ve finansal olarak desteklenen bir yapay zekâ ve makine öğrenmesi programıyla yapılabileceklerin sınırı yok gibi görünüyor.

Yapay zekâ ve makine öğrenmesi teknolojilerinin bilinçsizce gelişmesinin korkutucu sonuçlarından biri de kamuoyunun bu teknolojilere olan güveninin sarsılma ihtimali. Özellikle de geliştirici ve operatörlerin yapay zekâ ve makine öğrenmesi programlarının kontrolünü kaybetmesi sonucu yaşanabilecek felaket sonuçlar, bu teknolojilere olan desteğin kesilmesine sebep olabilir. Raporda şu ana kadar gerekli yasal düzenlemelerin, çoğu ülkede gerekli hızda yapılmadığına ve bunun değişmesi gerektiğine dikkat çekiliyor.

Yasal Düzenlemeler İçin 10 Adım

Rapora göre bu konuda yasal ve politik çerçevede atılabilecek 10 adım var:

- Kapsamlı bir mevzuatın geliştirilmesi için gerekli destek verilmeli,
- Ulusal yasama ve yürütme kuruluşlarınca gerekli geribildirim sağlanmalı, Güvenlik araştırmaları daha iyi korunmalı,
- Yasa ve mevzuatın birlikteliğinden doğacak sorunlar baştan kabullenilmeli, Yetkili mercilere bu teknolojilerdeki usulsüzlüğü duyuranlar korunmalı,

- Bu teknolojilerin kullanımının insan haklarını zedeleyebileceği göz önünde tutulmalı,
- Teknik standartlar yasal çerçevede belirlenmeli, Önlemler baştan alınmalı,
- Güvensiz ürünler piyasadan kaldırılmalı,
- Bu konuda gerekli tartışmalar yapılmalı.

Raporda özellikle telif hakkı ve ihracat kontrolü standartlarının değiştirilerek, güvenlik araştırmacılarının yasalara ters düşme kaygısı olmadan çalışmasının sağlanması gerektiği belirtiliyor.

2) İNSAN FAKTÖRÜ SİSTEMİN BİR PARÇASI OLMALI

İkinci boyut olan insan faktöründe ise özellikle teknik ve insani güvenin sağlanmasının önemine değiniliyor. Bunun için şeffaf ve risklerin öngörüldüğü bir ilerleyişin tercih edilmesi gerektiğinin altı çiziliyor. Risk yönetiminde insan faktörü bir "bug" değil, sistemin bir parçası olarak ele alınmalı ve gelişmeler, saldırıyı yapan tarafın gözünden ilerletilmeli.

3) VERİ

International Data Corporation'ın 2014 yılında yaptığı açıklamada dünya üzerindeki verinin her yıl katlanarak arttığını ve 2020 yılına dek 44 zetabayta ulaşmasını beklediklerini açıkladı. Bu veri bireylerden, cihazlardan, teknik ağlardan, sosyal ağlardan ve çeşitli uygulamalardan elde ediliyor. Yani güvenliği sağlamada kullanılacak yapay zekâ ve makine öğrenmesi teknolojilerinin çok büyük boyuttaki verileri işleyip korumada başarılı olması gerekiyor.

Bağımsız Bir Veri Deposu Gerekli

Bu teknolojileri test eden güvenlik algoritmaları geniş kapsamlı ve çok çeşitli denemeler gerçekleştiriyor. Ama bunun dışında bu teknolojilerin depolama, paylaşma ve verinin bütünlüğünün korunması açılarından da güvenilir olması gerekiyor. Raporda bunun için bir merkeze bağlı olmayan, standarda bağlanmamış ve kaliteli veri depolarının oluşturulması gerektiğine dikkat çekiliyor. Böyle bir gelişmenin endüstri, hükümetler ve akademi için yararlı olacağının altı çiziliyor.

4) DONANIMI YAPAY ZEKÂYA HAZIRLAMANIN 3 YOLU

Endgame'in CEO'su Nathaniel Fick, siber saldırganların her geçen gün daha da güçlendiğini, şirketlerin ise her geçen gün artan cihaz nüfusu sayesinde onlara saldırılacak yeni alanlar açtığını ifade ediyor. Raporda, ağ dediğimiz şeyin artık fiziksel dünyadaki elektronik ekipmanlarla sınırlı olmadığı, bugün bu ağa artık cihazları kullanan bireylerin yani kullanıcıların da dahil olduğu belirtiliyor. Yani siber saldırganların oyun sahası o kadar geniş ki, yapay zekâlı botların yardımı olmadan bunlara karşı savaşmak son derece güç. Öyle ki pek çok bilişim güvenliği yöneticisinin odağı bugün hacklenip hacklenmeyecekleri değil, bunun daha çok "ne zaman" olacağı. Raporda bu konuda bir diğer önemli noktanın donanım olduğu ve bu problemi çözmenin de üç yolu olduğu belirtiliyor:

- Güvenliği, donanımsal araçların tasarımlarıyla bütünleştirmek.
- Donanım ağı mimarisi oluşturarak tüm ağın güvenliğinib an be an izleyebilmek.
- Yapay zekâ ve makine öğrenmesi sistemlerine izin veren bir donanım kurarak daha karmaşık problemleri mevcut bariyerleri eleyerek çözmek.

Siber saldırılar son derece otonom bir şekilde gerçekleştiriliyor. Bunları gelişmiş yapay zekâ ve makine öğrenmesi algoritmalarıyla, üstelik insan denetimi olmadan baştan savabilmek ise hem ilgi çekici, hem de tartışmalı bir konu. Makine öğrenmesi sistemlerinin detaylı senaryolar oluşturmasını sağlamak için çalışan geliştiriciler, sistemin "normal" ve "tehdit edici" senaryoları ayırt edebilmesini kolaylıkla sağladığı belirtiliyor. Siber güvenliğe yaklaşımda raporun beşinci maddesi olan yapay zekâ ve makine öğrenmesi için yazılım ve algoritmalar konusu da burada devreye giriyor.

5) YAZILIM VE ALGORİTMALAR

Rapora göre kuruluşlar ve hükümete bağlı kurumlar yapay zekâ ve makine öğrenmesini donanım ve algoritmalarına bağlarken beş basit prensibe bağlı kalmalı.

a) Öncelikle, ikisinin de hata yapabildiği göz önünde bulundurularak hem insan hem de makinenin çıkarları dengede tutulmalı. Bu dengede kimin ne karar alacağı belirlenmeli. Zira teknik ve politik sebeplerden dolayı tehditleri saptamada tümüyle otonom bir sistem kullanılması her zaman doğru olmayabilir.

b) İkinci madde, yapay zekâ ve makine öğrenmesi teknolojileri ile siber güvenliğin hızla değiştiği göz önünde tutularak yazılımda uyarlanabilir, değiştirilebilir bir çerçeve oturtulmalı.

c) Teknolojiler problem odaklı geliştirilmeli. Başarılı bir yaklaşım için tek modele bağlı kalınmamalı, problemler ışığında birbirini takip eden sırayla, farklı modeller kullanılmalı.

d) Raporun öne sürdüğü dördüncü prensibe göre yapay zekâ ve makine öğrenmesi iki aşamalı olarak uygulanmalı. İlk aşamada veri ağı ve trafiğinin geçmişinin algılanması sağlanmalı. Böylece neyin tehdit, neyin bu trafiğin sıradan bir parçası olduğu sisteme gösterilmeli. İkinci aşamada ise normalin ne olduğu öğretilmeli; tehdit durumlarında insan müdahalesinin kapsamı belirlenmeli.

e) Raporun yazılıma dair son prensibi ise siber güvenlikte yapay zekâ ve makine öğrenmesi kullanımının, dolandırıcılıktakiyle aynı olması. İki durumda da muhalif bir taraf olduğundan, failler davranışları ve aksiyonlarıyla saptanıyor ve engelleniyor.

6) OPERASYONELLEŞME

Raporun siber güvenlikte yapay zekâ ve makine öğrenmesi sistemlerinin kullanılmasında ele aldığı altıncı ve belki de en önemli madde ise operasyonelleşme; yani farklı verileri, bilgileri bir araya getirme.

Belki de En Önemli Boyut: Veri Paylaşım Sistemi!

Raporun sponsor ortaklarından olan, ABD Askeri Akademisi West Point Elektrik Mühendisliği Bölümü Profesörü Barry Shoop, spectrum.ieee.org sitesine verdiği demeçte şirketlerin ellerindeki siber güvenlik verisini paylaşmakta ne kadar isteksiz olduğunu aktarıyor. Ortaya çıkan saldırılara ilişkin kimin saldırdığını, nasıl cevap verildiğini içeren verilerin dahi herkesin yararına paylaşılmadığını belirten Shoop, bunun sebebinin yasal düzenlemeler ve ekonomik kaygılar olduğunu belirtiyor ve ekliyor: "Yatırımcıları, hissedarları var. Eğer saldırıya uğradıkları ve başarısız oldukları anlaşılırsa hisse senetlerinin değeri düşer, bu da yatırımcıları kaçırır."

Yani bugün siber saldırganlar pek çok şirkete ve hatta hükümete bağlı kurumlara, saldırıya ilişkin verilerin paylaşılmayacağından emin olarak rahatlıkla saldırabiliyor. Veri paylaşımı olmadığı için kimse aynı saldırıya nasıl bir savunma yapılması gerektiğini çözemiyor. Saldırı karşısında başarısız olan şirketler bu bilgileri kendilerine saklıyor. Bu tip saldırılara karşı yapay zekâ kullanımının ideal olduğu artık kesinlik kazanmış durumda. Geçtiğimiz günlerde Capitol Hill'de ifade veren Facebook CEO'su Mark Zuckerberg de Rusya'dan gelen saldırının en iyi yapay zekâ ile savuşturulabileceğini ama bu teknolojinin olgunlaşması için 5-10 yıl gerektiğini söylemişti.

Siber Güvenlik Veri Takas Sistemi Anlık Olarak Güncellenmeli

Arizona State Üniversitesinde görevli Brian David Johnson da yaptığı açıklamada siber savunma için hem kamu hem de özel kuruluşların ortaklığında bir veri takas sistemi oluşturulması gerektiğini belirtti. Bluetooth gibi herkesin birbirine bağlı olacağı bu sistemde en azılı rakipler dahi bir araya gelerek sektörde standartları ve teknolojik rotaları oluşturmalı. Bu veri takas sisteminde küresel ve her an güncellenen bir siber saldırı ağı da olmalı, böylece herkes birlikte savunma yapmalı.

Johnson'ın önerdiği ve raporda da kendine yer bulan veri takas sistemiyle ilgili değerlendirmede bulunan Shoop ise, "Verinin nereden/hangi şirketten geldiğini bilmek zorunda değilsiniz. Ama saldırının rotasını ve verilen

yeterli ya da yetersiz cevabı görürsünüz. Böylece kendi sisteminizi, benzer saldırılara karşı hazır tutarsınız" dedi. Böylesi bir veri bankası savunmanın daha etkili yapılmasını sağlamanın ötesine geçebilir. Shoop'a göre böyle bir banka aynı zamanda algoritmaları ciddi bir veri akışı gerektiren yapay zekâ ve makine öğrenmesi teknolojilerinin de gelişimine katkıda bulunacaktır.