thinktech
STM Teknolojik Düşünce Merkezi

Siber Saldırılardan Korunma Yöntemleri

2017'nin Ekim ayında Japonya'da, Tokyo Keio Üniversitesinde düzenlenen Cyber3 Konferansı büyük ölçekte bir siber saldırı tatbikatına ev sahipliği yaptı. "2020 ve Ötesi" temasıyla üçüncü kez düzenlenen ve sanal saldırıların gerçek etkilerini tartışmak için önemli bir platform oluşturan bu konferansta devletler, istihbarat ajansları ve özel sektörden yetkililer bir araya gelerek her gün artan siber saldırılara karşı alınabilecek güvenlik tedbirlerini masaya yatırdılar.

Etkinliğe ev sahipliği yapan Keio Üniversitesi rastgele seçilmiş bir adres değil. 2015 yılından bu yana kendi bünyesinde bir "Siber Güvenlik Araştırma Merkezi" barındıran bir kurum. O tarihten itibaren siber güvenlik alanında düzenlenen sempozyum ve toplantılara ev sahipliği yapmanın yanı sıra siber saldırıları önlemede istihbarat örgütleriyle birlikte çalışarak uluslararası arenada faaliyet gösteren bir üs vazifesi de görüyor.

Japonya Bilgi Teknolojileri Ajans Başkanı Tatsuo Tomita'nın konferansın açılış konuşmasında altını çizdiği önemli başlıklardan biri siber saldırılara karşı uluslararası işbirliğinden doğacak gücün önemiydi. Tomita, katılımcılara 2015 yılında Ukrayna elektrik dağıtım şirketlerine yapılan saldırıyı anımsatarak siber saldırıların fiziksel dünyada yarattığı gerçek sonuçlara dikkat çekti ve bu meselenin şirketlerin IT departmanlarının sorunu değil üst düzey bir tartışma konusu olduğunu belirtti. ABD'nin eski Savunma Bakan Yardımcısı Linton Wells II de "Siber güvenlik sorunu sunucu odasında değil yönetim kurulu salonunda başlıyor" diyerek siber güvenliğin şirketlerin, hatta devletlerin bütün birimlerini etkileyecek bir mesele olduğunu dile getirdi.

Aralarında Keio's Medya Enstitüsü Dekanı Jun Murai, İletişim Bakanlığı'ndan Seiko Noda ve ABD Japonya Büyükelçisi William Haggerty IV gibi önemli isimlerin de yer aldığı diğer konuşmacılar da siber riskle mücadelede grupların bireysel çabalarının yetersiz olacağına dikkat çekti. İş dünyası, devletler ve akademik çevrelerin ele ele vererek aşabileceği bu saldırılarda ulusal, bölgesel ve global ittifakların gerekliliği de konferans boyunca sıklıkla vurgulandı. Bu itifaklardan doğan güçle, siber saldırılara karşı daha korunmasız olan küçük ve orta ölçekteki işletmelere de yardımcı olacak araç ve kaynakların sağlanması gerektiğine değinildi.

Konferansta, Japonya'nın 2020 siber güvenlik hedefleri de masaya yatırıldı. Malum, Japonya 2020 yılında Tokyo Olimpiyatları'na ev sahipliği yapacak ve bu tür dünya çapında organizasyonlar, yaratacağı etkinin büyüklüğü sebebiyle siber saldırıların hedefi olarak seçilebiliyor.

Benzer bir saldırıda yaşanabilecekleri prova etmek için 2019 yılında yine Japonya'da yapılması planlanan Dünya Rugby Şampiyonası'na yönelik bir siber saldırı simülasyonu yapıldı. "Rugby Daemon" adı verilen bu simülasyon, belli bir tarih aralığında yapılacak farklı tip siber saldırıları içeriyordu; şehrin elektrik şebekesini devre dışı bırakmak, e-posta dolandırıcılığı, şampiyonanın web sitesine erişim engeli gibi farklı alanlardan gelen saldırılara karşı geliştirilen çözüm önerileri siber güvenlik altyapılarını geliştirmek için önemli bilgiler üretti.

8 ila 10 kişilik dört gruba ayrılan katılımcılar gerçek zamanlı bu simülasyonda zamana karşı yarıştılar. Yanlış bir adım atarlarsa, Yokohoma Stadyumu final maçı esnasında karanlığa bürünecek, DDoS saldırılarının önüne geçilemezse sadece şampiyonanın değil birçok kamu kuruluşunun web sitesine erişim engellenecekti. Takımlar koordineli ve hızlı çalışmaya teşvik edildi. Rugby Daemon Projesi, kâğıt üstünde bir tehlikeydi ve gerçek olsa ne tür krizler yaşanabileceğini katılımcılara gösterdi.

ABD ve Japonya arasındaki ilişkileri güçlendirmek amacıyla kurulan Sasakawa ABD Vakfı da "Rugby Daemon Operasyonu"nun sonuçlarını değerlendiren bir rapor yayınladı. İngilizce ve Japonca olarak yayınlanan raporda ABD ve Japonya arasındaki ittifak gücünün önemine işaret edildi ve ülkelerin siber saldırılara hazırlıklı olmanın ötesinde birlikte çalışma becerilerinin geliştirilmesinin önemi özellikle vurgulandı.

Siber Güvenliğin Beş Temel Direği

Konferansta nesnelerin interneti (Internet of Things –IoT) teknolojilerinin yayılmasıyla çevrimiçi duruma gelen cihaz sayısının artışından ve bu durumun siber güvenlik alanında yarattığı zorluklardan da bahsedildi. IoT teknolojisinin genel sistem tasarımı ve güvenliğini yeniden dizayn etme zorunluluğu doğurduğunun da altı çizildi.

Katılımcılar etkili bir yaklaşımın beş etaplı bir sistemden oluşması gerektiği konusunda mutabık kaldı:

- Güvenlik açıklarını ele alacak yapılar oluşturmak,
- Ar-Ge'de ilerleme,
- Özel şirketler bünyesinde siber güvenlik önlemlerini teşvik etmek,
- İnsan kaynaklarını güçlendirmek,
- Uluslararası işbirliği.

Katılımcıların hemfikir olduğu bir diğer konuysa olayların üstünü örtmemekti. Çünkü bir siber saldırı yaşandığında yapılabilecek en kötü şey bunu gizlemeye çalışmak. Bu etkili bir güvenlik planının oluşmasını geciktiriyor ve bilgi paylaşımını engelleyerek gerekli işbirliğine engel oluyor. Ve malesef bu sıklıkla tekrarlanan bir durum.

Konferansta siber suçları da tartışan katılımcılar, siber suçluların kimliklerinin ve motivasyonlarının gün be gün nasıl değiştiğine dikkat çekerek adeta görünmez olan bu düşmanın "kim" olduğu kadar, bu suçları "neden ve nasıl" işlediği sorularına verilecek yanıtların da önemli olduğunu belirtti.

Girişimci, yazar, düşünce lideri, siber güvenlik uzmanı ve Japon Hükümetinin danışmanlarından biri olan William H. Saito, siber saldırıların önüne geçme konusunda yapılması ve kaçınılması gereken başlıkları şöyle sıralıyor: "Öncelikle paranoyaya kapılarak internet erişimini kesmeye çalışmamak gerekiyor. Siber endişelere kapılıp çalışanlarınızı baskı altına almak da hiç doğru bir yaklaşım sayılmaz. Kablosuz ağı yasaklamak internet çağının tabiatına ters. Güvenlik önlemlerinizin, anti virüs programlarınızın son sürümlerinin aktif olduğundan her zaman emin olun. Şüpheli bir durumla karşılaşırsanız hızlı davranıp hemen bildirin. Diyelim ki şirket telefonunu ya da laptop'unu kaybettiniz, bunu yetkililere anında bildirmek, onları bulmak için harcayacağınız zamandan çok daha kıymetli. Güvenlik sisteminizi sürekli teste tabi tutun, işletim sistemiyle entegre bir şekilde çalıştığından emin olun ve kendinize güvenin. Gerekli tedbirleri aldığınız takdirde kötü niyetli bir yazılımın sisteminize girmesi oldukça zor."

Bireysel kullanıcılar için de durum pek farklı sayılmaz aslında, görünmez bir düşmana karşı basit bir anti virüs programının sizi her saniye korumasını bekleyemezsiniz. Dikkat etmeniz gereken birtakım kurallar var. Kendinizi siber bir saldırıdan korumanın ilk koşulu işletim sisteminizi, web tarayıcınızı ve antivirüs programınızı her zaman güncel tutmak, son sürümleri indirmeyi ihmal etmemek. Bilgisayarınızın diğer aygıtlarla olan bağlantısına da dikkat etmelisiniz. Güvenlik teknolojiniz tüm ağ trafiğini ayrıntılı biçimde denetleyebiliyor mu? Özel verilerinizin ayrı bir yerde ve güvenli bir şekilde depolanması da oldukça önemli. İstenmeyen e-postaların uzantılarını açmamak, güven teşkil etmeyen sitelerden veri indirmemek, kısacası "online hijyen" sizi virüslerden uzak tutmanın olmazsa olmazlarından.

İngiliz Ulusal Siber Güvenlik Merkezinden Paul Maddinson, iki gün süren Cyber3 Konferansında konuşulanları en iyi özetleyen isimdi: "İnternet coğrafyaların ötesinde bir gerçek. Bir ülkenin füze menzili dışında kalıyor olabiliriz. Ancak o ülkenin zararlı yazılımları sizi kolaylıkla vurabilir."