Siber Güvenlik[(*)]

Ali Akurgal

Bu sayıda, Pentagon'u en çabuk ve en derin "hack"leyen
Can Yıldızlı'yı konuk ediyor ve sözü ona bırakıyorum.

Siber Güvenlik; bir kaç yıl öncesine kadar ülkemizde insanların önemini kabul ettiği ancak gündelik hayat ile bağdaştıramadığı hayali bir savaş alanı olarak algılanıyordu. Haber kaynaklarında, siber saldırılarla devletler, kurumlar veya şahıslar arası casusluk, sabotaj ve bilgi kaçırma girişimleri yer alıyordu. Ama siber güvenlik konusunda kararlı adımlar atılması gerekliliği, ne toplumda ne de kamu kurumları ve günlük yaşamın sürdürülmesinde etkin sektörlerde bir öncelik olarak kendine yer bulamıyordu. Ülkemizde yavaş yavaş da olsa, farkındalığı yüksek olan bankacılık sektörü dışındaki endüstrilerin de tehditlerin gerçekliği ve nelere mal olabileceği hakkında fikirleri oluşmaya başladı.

Halen politika geliştirmekte, eylem planları oluşturmakta dünya genelinden geride olsak da; en azından siber güvenliğin, genel adı ile bilgi güvenliği'nin, doğrudan bir ülkedeki tüm ulusal kaynakları hedef alabilecek, gündelik yaşamı baltalayacak veya saldıran tarafın istekleri doğrultusunda kısıtlayabilecek kadar kuvvetli bir silah olduğunun farkındayız. Ama, "**Kritik Altyapı**" olarak kabul edilen alanlar için yapılması gerekenden çok geride olduğumuzu söylemeliyiz.

ABD *"**Department of Homeland Security**"* kurumunun 17 maddelik "**Kritik Sektörler**" listesinde Savunma, Kimya, Finans, Telekomünikasyon, Enerji, Sağlık, Ulaştırma, Güvenlik, Gıda ve Tarım başta olmak üzere, yara alması durumunda bir ulusun kaderini değiştirebilecek düzeyde önem sahibi alanlar yer alır. Devletlerarası stratejik siber savaş senaryolarının tümünde de bu sektörler hedeftedir. Bunlara, gerçek ARGE çalışmalarının tümünü de ekleyebiliriz.

Akurgal'ın **"patron, fabrikayı hacklemişler..."** yakıştırması abartılıysa da buna işaret etmekte... Bu bir **"sabotaj" senaryosu**... Başta ARGE çalışmaları yürüten birimle, şirketlerin yalnızca sistemsel değil, fiziksel olarak da, dış dünya ile bağının tamamen ayrılması gerektiğinin pek farkına değiliz. Reel sektörde gizliliğe hiç önem vermiyoruz. Hâlbuki, işe alınacak insanların niteliklerine bakarak bile o birimde ne gibi bir ürün tasarlandığını kestirmek hiç de zor değil.

Kuruluşlarımız, giderek daha çok işlevlerini **ERP yazılımları** ile yönetiyorlar. Bunlar, ne yazık ki, herhangi bir **sızma testi** uygulanmadan, çoğunlukla yalnızca "işlevsel" testlerle devreye alınıyor. Bir sektörde bir firma bir yönetim yazılımını uygulamaya koymuşsa diğerleri de onun kullandığına yöneliyorlar. Böylece, kötü niyetliler, tek bir yazılımı ele geçirmekle tüm sektörü çökertmek olanağına kavuşuyor. Sanayimiz en kısa sürede, "tak-kullan-kurtul" mantığından öteye geçmeli.

Firmaların sığındıkları güvenlik çözümleri, genelde yabancı... Bunların **milli**leştirilmesi ulusal güvenlik açısından yaşamsal önem taşıyor. Egemen devletler öyle yapıyorlar. Yabancı bir ürün aldığınızda, çoğu kez okumadan kabul ettiğiniz "kullanıcı sözleşmesi"nde, nelere izin verdiğinize şaşarsınız! "ISO 27001" sertifikası ile "Siber Güvenlik" arasındaki **uçurum**u algılamakta ise, çoğu kuruluş "sağır"!

Firmaların, düzenli olarak "penetrasyon testi" ile, kendilerini sızmalara karşı sınamaları gerekiyor.

(*) herkese bilim teknoloji dergisinin 20 Mayıs 2016 tarihli 8. sayısında yayımlanmıştır.

Her güvenlik sisteminin **en zayıf halka**sı olarak kabul edilen **insan faktörü riski**ni en aza indirmek için ise, siber güvenlikten sorumlu personelin güncel tehditlere karşı eğitimi yaşamsal önem taşıyor. Özetle; hem sürekli siber güvenlikçi istihdam etmek, hem de **yerli ve milli** güvenlik firmalarından hizmet ve ürün almak gerekli.

Bu alanda yapılanma bir devlet politikası ile düzenleyici-denetleyici bir kurumun mecbur tutması ve gerekli teşvik sağlanması ile mümkün. Önümüzde, BDDK'nın bankalar için uyguladığı olumlu bir örnek var. Yavaş yavaş bir şeyler yapmak yerine hemen ciddi önlemler alınmalı. Gelişmiş ülkelerin yaklaşımı, siber tehditlerin tek bir bağımsız merkezde analiz edilerek değerlendirilmeleri; ilgili kuruluşlara alınması gereken eylemlerin bildirilmesi şeklinde. Firmaların bünyelerinde bir Güvenlik Operasyon Merkezi ("SOC") oluşturması veya dışarıdaki bir uzman kuruluştan hizmet alarak bildirilen eylemleri uygulaması yeterli. Ülkemizde, 2012 yılından bu yana PRODAFT ve INVICTUS ortaklığı ile geliştirilen **Ulusal Siber Tehdit Ağı** projesi, böyle çalışmakta ve ağırlıklı olarak Finans ve Telekomünikasyon firmaları tarafından kullanılmakta. Bu platformdan, 2015'in ilk çeyreği itibarı ile toplam 55.000 farklı siber tehdit hakkında bildirimde bulunulmuş.