Siber Risk ve Dijital Finans Konusunda Derleme
(07.02.2022)

Pandemi, çalışma şeklimizi, iş yapma şeklimizi ve hatta nasıl yaşadığımızı ve birbirimizle nasıl etkileşim kurduğumuzu temelden değiştiriyor. Mal ve hizmetler için nasıl ödeme yaptığımızı etkiliyor, nakitsiz ve temassız ödemelere yönelik eğilimi hızlandırıyor.

Pandemi boyunca, finansal piyasa altyapıları ve bunlarla ilgili ekosistem, ekonominin direncini destekledi ve yeni ihtiyaçlara uyum sağladı. Dijital dönüşüme eşlik ettiler. Bu süreç pandemi sonrasında da devam edecek.

Merkez bankaları bu değişimde aktif rol oynamaktadır. Avrupa Merkez Bankası (ECB), anında ödemeleri teşvik ediyor ve sunuyor, dijital bir euro başlatma olasılığını araştırıyor ve G20'nin güvenlik ve güvenliklerini korurken sınır ötesi ödemeleri daha hızlı, daha ucuz, daha şeffaf ve daha kapsayıcı hale getirme çalışmalarını destekliyor.

Ancak dijitalleşme aynı zamanda ödeme sistemi, parasal egemenlik ve bir bütün olarak finansal sistem için riskleri de beraberinde getiriyor. Bu gelişmelere yanıt olarak ECB, gözetim çerçevesini uyarlıyor. Avrupa Komisyonu ise kripto varlıklar ve dijital operasyonel esneklik konusunda düzenleyici girişimler başlattı.

Ancak siber riske karşı koruma olmadan dijital finans ve ödemelerin bütünlüğü olmayacaktır. Bugün siber risklerin nasıl geliştiğini ve Euro Siber Esneklik Kurulu'nun (ECRB) bunları ele almadaki rolü önem taşımaktadır.

Daha Karmaşık Siber Tehdit Alanları

Dijital hizmetlerin artan kullanımı ve teknolojiye olan yaygın güven, üçüncü taraf ürün ve hizmetlerin artan kullanımı ve birbirine bağlılığı ile birlikte, finansal piyasa altyapılarının siber saldırılara karşı savunmasızlığını artırıyor. Finans uzmanları, siber saldırıları küresel finans sistemi için bir numaralı risk olarak görüyor.

Siber tehdit ortamı karmaşık (Şekil 1) ve sürekli olarak gelişmektedir. Örneğin saldırganlar, koronavirüs temalı kimlik avı e-postalarıyla kurbanları cezbetmek ve uzaktan çalışmayla ilgili zayıflıklardan yararlanmak için pandemiden yararlanmakta.

Şekil 1

Avrupa'daki finansal piyasa altyapıları için siber tehdit

Aktörler	Devlet Aktörleri Organize suç grupları İç tehditler Korsanlar	**Motivasyon**	Yıkıcı Zarar verici Kurumsal bilgi hırsızlığı	**Tehditler**	Tedarik zinciri/servis sağlayıcı Yama uygulanmamış açıklar İşyeri e-postaları Kimlik avı (Phishing)/Yemleme Fidye yazılımlar

					Yanlış konfigürasyonlar Trojan – Truva atı Yükseltme ayrıcalığı – yetkili kullanıcılar Dağıtık ağlardan gelen istenmeyen ataklar (DDOS) Web uygulamaları Mobil uygulamalar

Not: Tehditler (sağdaki sütun), önem derecesine göre sıralanmıştır (en ciddi tehditler en üstte).

Siber suçlular, hedeflerinden para çalmanın kazançlı yollarını bulma konusunda da yenilikçi olmuştur. Fidye yazılımı saldırıları genellikle kripto varlıkları biçimindeki fidye ödeme talepleriyle birleşmektedir. Saldırganlar, verileri tehlikeye atmak veya çalmak, hizmetleri kesintiye uğratmak veya fidye ödemeleri talep etmek amacıyla tedarik zincirindeki ve üçüncü taraf sağlayıcılardaki güvenlik açıklarından giderek daha fazla yararlanmaktadır.

Siber saldırılar daha karmaşık ve daha sık hale geliyor ve potansiyel etkileri sürekli artıyor. BT hizmet sağlayıcılarına ve satıcılarına yönelik tedarik zinciri tehditleri, özel bir endişe kaynağıdır. Saldırganlar, bu hizmet sağlayıcıları ve BT satıcılarını, hizmetlerini veya yazılımlarını kullanan diğer kurumlara ulaşmak için hedefler. Tedarik zinciri saldırıları genellikle çok sayıda kurumu tehlikeye atmakta ve ardından onlardan fidye talep etmek için kullanılmaktadır.

Etkilenen kurumlar bu tür saldırıları gecikmeli olarak tespit ederse veya öğrenirse, sonuçları çok büyük olabilir. Bu nedenle BT ortamlarındaki tüm yazılım ve donanımların - ne kadar küçük olursa olsun – izlenmesi ve yalnızca en kritik üçüncü taraf sağlayıcılarına odaklanılması gerekiyor. Kritik bilgilerin değiş tokuş edilmesi ve bu tehdidin üstesinden gelinmesi gerekiyor.

Euro Siber Esneklik Kurulu'nun Katkısı

Gelişen tehdit ortamına karşı uyanık kalmamız ve sürekli olarak en yüksek düzeyde dayanıklılık sağlamamız gerekiyor. Bu odaktan taviz verilemez. Siber dayanıklılığı geliştirmenin parasal maliyeti yüksek görünse de, başarılı saldırıların maliyetleri - hem finansal hasar hem de itibar etkisi açısından - çok daha yüksektir.

Çabalarımızı daha da yoğunlaştırmamız gerekiyor. ECRB, kamu-özel diyaloğu ve ortak girişimler için benzersiz bir ortam/forum sağlar. Bu, her şeyden önce ECRB üyelerinin çıkarınadır, aynı zamanda Avrupa finans sektörünün, hane halklarının ve işletmelerin çıkarınadır. Daha önce de vurgulandığı üzere, sektörün dayanıklılığı tüm bileşenlerinin dayanıklılığına bağlıdır. Finansal sistemin bir bütün olarak güçlendirilmesi için zayıf halkaları belirlemede işbirliği içerisinde çalışmalar yapılması gereği vardır.

Siber Bilgi ve İstihbarat Paylaşım Girişimi (Cyber Information and Intelligence Sharing Initiative - CIISI-EU), tehdit istihbaratı, bilgi ve en iyi uygulamaları paylaşmak için güçlü bir araç haline geldi. Topluluk içindeki tehditler ve devam eden siber saldırılar için erken uyarı sistemi görmekte ve siber risk ortamı hakkında farkındalığı artırmaktadır. Bu bilgi havuzunu geliştirmeye çalışmalıyız.

CIISI-EU modeli İrlanda Merkez Bankası tarafından da benimsenmiş ve kritik yerel finansal kuruluşlar arasında siber bilgi paylaşımı konusunda adımlar atılmaya başlanmıştır. Gelecekte diğer ülkelerin de benzer şekilde modeli benimsediğini görebiliriz. İleriye baktığımda, diğer CIISI benzeri girişimleri belirlemenin ve tehdit ve istihbarat bilgilerini paylaşmak için ortaklıklar kurmanın değerini görüyorum**.**

Sonuç

Siber riske yönelik çalışmalarda sağlanan ilerlemeye rağmen, siber tehditlerle mücadelede proaktif olmak gerekmektedir. Artan tehdit seviyesi göz önüne alındığında siber direnci korumaya tamamen bağlı kalınması lazım.

ECRB, bu amaca ulaşmak için kritik bir platform sunmaktadır. Bilgi paylaşmamıza, yaygın siber tehditleri ve riskleri ele almamıza, kriz yönetimi ve koordinasyonunu güçlendirmemize ve kurtarma yeteneklerini desteklememize olanak tanımaktadır. Yeni iş önceliklerini belirledikçe gelişecektir. Ancak temeli aynı kalacak: ortak bir tehdide karşı güven ve işbirliği.