



Artık dijital cihaz veya yazılım kullanılmadan yapılan iş kalmadı. Aynı zamanda dijital dünyadaki zararlı yazılım sayısı da 850 milyon adeti geçti ve bunların pek çoğu şirketleri hedef alıyor. Peki kurumları, siber saldırıdan uzak tutmak artık mümkün mü? ESET Türkiye Satış Müdürü Asım Akbal'a göre, bu kadar çok tehditle her şirketin dijital saldırıya uğrayacağı kesin. Ama önlem alarak bunları püskürtmek mümkün. Akbal, siber sızıntı ve saldırıları önlemek için kurumların dikkat etmesi gereken 10 konuyu sıraladı.

► Tam yapılmış güncellemeler: Yazılım şir-

ketleri düzenli güncellemelerle hem yeniliklerini kullanıcılarına yansıtır hem de yazılımlarındaki güvenlik seviyesini yükseltir. Hackerlar ise siber saldırı yapmak için sistem açıklarını kollarlar. Bu nedenle ilk kural, maliyeti de olsa yazılımları güncel tutmak, program yamalarını düzenli olarak yapmaktır.

► Kurtarma değil koruma: Düzenli olarak lisanslı ve güncel yazılım kullanmanın maliyeti var. Ama sisteminize sızıntı olduktan, bilgileriniz çalıdıktan veya verileriniz şifreledikten sonra yaşadığınız iş kaybı ve yapacağınız pişmanlık dolu harcamanın maliyeti ne yazık ki daha yüksek olacaktır.

► Güçlü şifreler: Sistemlerde zayıf şifreler kullanılmamalı, alfa numerik, karmaşık şifreler belirlenmeli, sık aralıklarla değiştirilmeli ve benzer şifrelerin tekrar kullanılması engellenmelidir.

► Yedekleme: Hangi sektörde olursa olsun, fidye saldırısı sonucu şirket verilerinin

ulaşılması hale gelmesi; güven, itibar, bilgi, iş ve para kaybı anlamına gelir. Olabilecek her tür siber saldırı veya meydana gelebilecek her tür fiziksel felaket için şirket verileri mutlaka yedeklenmeli. Üstelik mümkünse başka bir lokasyona kopyalanmalıdır.

► Kurumlara yönelik uç nokta (Endpoint) güvenlik yazılımı: Bu yazılımlar, çok kullanıcı sistemlere yönelik birden fazla koruma katmanı sağlar. Ayrıca merkezi bir yönetim konsolu üzerinden denetim ve raporlama imkânı sunar. Örneğin ESET Endpoint Security yazılımları, ağ saldırısı koruması, davranışsal algılama (HIPS) veya fidye yazılımı kalkını gibi katmanlarla şirketleri hedefleyen karmaşık saldırıları engeller.

► Çift faktörlü koruma (2FA): Kurumun yapısı gereği şirket verilerine uzaktan erişim gerekiyorsa, mutlaka çift kimlikli doğrulama sistemi kullanılmalıdır (Two-factor authentication). Tıpkı online banka girişlerinde olduğu gibi, sistem girişi için ilgili kişiye telefon üzerinden ikinci bir giriş şifresi iletilir. Sisteme ancak böyle giriş sağlanabilir.

► Veri Sızıntısı Önleme Çözümü (DLP): Tehdit çok uzaktan değil, çok yakından da gelebilir. DLP yani Data Loss Prevention yazılımları, kurum içinden oluşabilecek veri sızıntılarını engellemeye yöneliktir. Çalışanlar, önemli verileri şirket dışında bir oluşuma taşıyamaz. ESET'in DLP çözümü Safetica, veri sızıntısı sonucu oluşacak maddi zararlardan ve itibar kaybından korur. Ayrıca şirket verilerini çalışanlara ait cihazlara karşı da denetim altında tutar.

► Mail Security ve Antispam çözümleri: Kurumlara ulaşan virüslerin çoğu, özellikle de fidye yazılımları, çalışanlara gelen e-posta ve spam mesajlar yoluyla ulaşır. Şirket sunucularına odaklanan Mail Security yazılımları, ek güvenlik katmanı sağlar. Gelişmiş antispam filtreleriyle zararlı mesaj ve eklentilerini kullanıcıya ulaşmadan durdurur. ESET Mail Security, potansiyel tehditleri bile ekstra bir güvenlik katmanı olan sandbox çözümünde inceler.

► Kurum içi güvenlik politikası: Herkes her dosyaya ulaşamamalı. Şirket içinde bir güvenlik ve gizlilik politikası oluşturulmalı. Erişim kuralları belirlenmeli, duyurulmalı. Güvenlikle ilgili personele yüklenecek rol ve sorumluluklar tanımlanmalı.

► Eğitim şart: Güvenlik konusunda belirlenen rol ve sorumluluklara ilişkin çalışanlara mutlaka bilgi ve eğitim verilmeli. Böylece kurum, hatalı kullanım ve kurumlara maruz kalmayacaktır.

2019'u güvende geçirmenin 10 yolu

Dünyadaki zararlı yazılım sayısı 850 milyon adeti geçti ve bunların pek çoğu şirketleri hedef alıyor. Ama önlem alarak bunları püskürtmek mümkün. ESET Türkiye de siber sızıntı ve saldırıları önlemek için kurumların dikkat etmesi gereken 10 konuyu sıraladı.



2 bin 750 Ar-Ge ve tasarım merkezi hedefi

Stratejik plan dönemi sonunda faaliyete geçen Ar-Ge merkezlerinin binden 2 bin 200'e ve tasarım merkezlerinin 275'ten 550'ye çıkarılması planlanıyor.

Bakanlığın temel performans göstergeleri arasında 2023'te Sanayi İşbirliği Programı uygulama sayısının 13, bölgesel girişim sermayesi modelinin uygulandığı bölge sayısının yedi, kredi desteğiyle tamamlanan OSB proje sayısının 26, yatırımcıya tahsise hazır hale getirilen endüstri bölgesi sayısının altı ve finansal destek sağlanan küme iş birliği sayısının 15 olması öngörülmüyor.

Ayrıca beş yıllık dönem sonunda, Dijital Dönüşüm Yol Haritası Eylem Planı'nı yüzde 45 gerçekleştirmek, yüksek ve orta-yüksek teknoloji yatırımların toplam yatırım tutarı içerisindeki payını yüzde 39'a çıkarmak da hedefleniyor.

Sanayide teknolojik dönüşüme 1.8 milyar lira

Sanayi ve Teknoloji Bakanlığı stratejik planına göre, sanayinin teknolojik dönüşümünü sağlamak için beş yılda 1.8 milyar lira harcama yapılacak. Bakanlık tarafından hazırlanan 2019-2023 yıllarını kapsayan stratejik planda, amaç, hedef ile bu unsurlara yönelik stratejiler ve performans göstergeleri yer aldı. Bakanlığın söz konusu döneme ilişkin planında, yedi amaç ve 32 hedef oluşturuldu ve stratejileri hayata geçirmek için tahmini maliyet toplamda 3.6 milyar lira olarak hesaplandı. Söz konusu maliyet kalemleri gelecek beş yıl için ayrı ayrı incelendiğinde 2019'da 417.1 milyon lira, 2020'de 448.5 milyon lira, 2021'de 569.5 milyon lira, 2022'de 1.2 milyar lira ve 2023'te 924.9 milyon lira harcanması gerekiyor.

Plan döneminde, söz konusu hedeflere ulaşmak ve amaçları gerçekleştirmek için en yüksek maliyetin 1.8 milyar lira ile "sanayinin teknolojik dönüşümünü sağlamak, yenilikçilik ve tasarım kapasitesini artırmak" için oluşması bekleniyor. İkinci yüksek maliyet kaleminin 1 milyar lira ile "sanayi alanında yatırım ortamının oluşumuna, sanayinin planlı gelişimine ve rekabet gücünü artırıcı iş birliklerine destek vermek" olması öngörülmüyor. Tahmini maliyetlerin beş yıllık süreçte Cumhurbaşkanlığı Yatırım Ofisi ile koordinasyon halinde iş ve yatırım ortamını iyileştirmek, yurt içinde ve yurt dışında iş birliklerini ve rekabetçi yatırımları teşvik etmek amacı için toplam 329.1 milyon lira, teknolojik gelişmeler doğrultusunda rekabetçi, yerli ve milli sanayi yapısının oluşmasını sağlamak için 190.5 milyon TL olacağı da hesaplandı. Bakanlığın kurumsal yapısı ile stratejik yönetim ve uygulama kapasitesini güçlendirmek için 158 milyon lira, güvenli, güvenilir ve kaliteli sanayi ürünlerinin yer aldığı, izlenebilir bir piyasanın oluşmasını sağlamak için 111.8 milyon lira ve merkezi ve yerel düzeyde kurumsal kapasitenin artırılması suretiyle bölge içi ve bölgeler arası gelişmişlik farkını azaltmak ve bölgelerin ulusal kalkınmaya katkısını azami düzeye çıkarmak için 2.3 milyon lira tahmini maliyet oluşacağı belirlendi.



Rolls Royce **elektrikli uçuş testini** tamamladı!

Karadan yapılan yolculuklardan sıkılan Rolls Royce uçmak için çalışmalarını sürdürüyor. Şirket şimdi de hibrit-elektrikli tahrik sistemleri sunma hedefini gerçekleştirebilmek için bir adım attı. Genellikle helikopterlerde tercih edilen sistemin testleri tamamlandı. Havacılık alanında yürütülen testler dünyanın en kapsamlı hibrit türbinli motorunu geliştirme ve entegre etme programlarının bir parçası olmasıyla önem taşıyor. Söz konusu testler 2021 yılında uçaklarla yapılacak uçuşlar için şimdiden zemin hazırlıyor. M250 gaz türbinlerinin hibrit versiyonu Seri Hibrit, Paralel Hibrit ve Turbo-Elektrik olmaz üzere üç ayrı şekilde test edildi. ABD'nin Indianapolis şehrindeki Rolls Royce tesisinde yapılan testlerden başarılı sonuçlar alındığı açıklandı.

