regülasyonlarla uyumlu çalışma imkânı sağlıyoruz. Biraz daha detaya inersek, proaktif ağ ve güvenlik yönetimi hizmetlerimiz sayesinde şirketlerin güncel, güvenilir ve uygulamalarını en iyi şekilde destekleyen bir yapıya sahip olmasını ve bu yapının sürekliliğini sağlamasını mümkün kılıyoruz. Ağ ve güvenlik yönetimi hizmetimizle de işletmelerin ağ cihazlarını 7/24 izliyoruz. Bu süreçte periyodik güncellemelerini ve SD-WAN yönetimini gerçekleştiriyoruz. Konfigürasyonların ve değişikliklerin de yönetimini üstleniyoruz. Aylık operasyonel raporlama ve iyileştirme önerilerimizin yanı sıra çözülemeyen sorunlarda ve donanım arızalarında işletme adına üreticiyle iletişimi kuruyoruz, süreci takip ediyoruz. Müşteriler açısından baktığımızda, onlar da ağ ve güvenlik altyapılarının operasyonel yükünden kurtuluyor ve sistemlerde oluşabilecek sorunlar daha gerçekleşmeden ortadan kalkıyor.

Veritabanını yönetmek için gerekli kaynağı bulmak, elde tutmak ve verimlilik sağlamak günümüzde oldukça zor olabiliyor. Ayrıca en son yeniliklere, regülasyonlara ve siber güvenlik tehditlerine ayak uydurmak da mümkün olmayabiliyor. Bu uygulama yoğunluğu ve karmaşası içinde tüm sistemleri çalışır durumda tutmak ve iş kesintilerinin önüne geçmek için rutin ve proaktif bakım gerekiyor. Aynı zamanda değişim sürecinde olan dinamik bir işletmede uygulamaların da her daim güncel tutularak yeni iş ihtiyaçlarını desteklemeye yardımcı olması çok önemli.


Eclit Kurucu CEO'su Egemen İnce

Dijitalleşmenin hızlanmasıyla birlikte siber saldırılarda da ciddi bir artış söz konusu. Türkiye de siber saldırıya en çok uğrayan ülkeler arasında. Bu konuda neler yapılabilir?

Ülkemizde siber saldırıların yaygın görülmesinin bir sebebi de bilgi güvenliği ve kişisel veri bilincinin henüz gelişme sürecinde olması. Kurumların ve bireylerin bu alana odaklanarak genel olarak iyileştirme sağlaması gerekiyor. Şirketlerin bu açıkları giderecek şekilde IT altyapılarını ileri taşımak için doğru uzmanlarla çalışması, "oltalama" testleri ve veri güvenliği tatbikatlarıyla da çalışanlarının bu alanda gereken bilince en kısa sürede sahip olması çok önemli. Bireylerin de kişisel verilerine gereken önemi vermesi ve birlikte çalıştıkları kurumlardan bu alanda en yüksek dikkati talep etmesi gerekiyor.

Son yıllarda siber saldırılar dünyada nasıl bir gelişim gösterdi? Ekonomik olarak getirdiği yük hangi seviyelere ulaştı?

Yeni teknolojilerin şirketlere ve bireylere sağladığı faydalar sıkça konuşuluyor. Ancak bu teknolojiler siber saldırganlara da birçok avantaj sağlıyor. Örnek vermek gerekirse, son yıllarda sıkça bahsedilen yapay zekâ ve makine öğrenmesi teknolojileri, siber saldırıların ölçeğini ve hızını görülmemiş seviyelere çıkarıyor. Gelişen teknolojilerden güç alan bu saldırganlar, birçok şirketin ve kurumun siber yapılarına aynı anda saldırı düzenleyebiliyor. Bu noktada saldırının hedefi olmak için sistemin bir internet bağlantısı olması yeterli oluyor. Saldırganlar hedef aldıkları sisteme sızabileceği bir açık bulduğunda ise hasarlar milyar dolar seviyesine ulaşabiliyor. Daha sonra buna itibar kayıpları ve yasal yaptırımlar da ekleniyor.

Sektörel olarak bakıldığında finans dışında en çok hangi alanlar risk altında?

Kimlik numarası, kredi kartı bilgileri gibi değerli veriler toplayan her sektör ve şirket siber saldırganların odağında. İlk bakışta akla finans ve bankalar gelse de sıkça hedef alınan sektörlerin başında sağlık geliyor. Çünkü bireylerin sağlık geçmişi en değerli bilgileri arasında yer alıyor ve sistemlerini kilitleyerek bir hastanenin verdiği hizmet aksatıldığında insan hayatı tehlikeye girebiliyor. Bu durum, fidye talep eden saldırganların da elini güçlendiriyor. E-ticaret ve kamu hizmetleri de finans ve sağlık sektörüyle birlikte siber saldırıya en fazla maruz kalan sektörler arasında.

Siber güvenlik hizmeti veren şirketler bu değişime karşı ne gibi hazırlıklar yapıyor? Eclit olarak yeni ürün ve çözümler geliştiriyor musunuz?

Günümüzde verilerin saklanması ve güvenliği her zamankinden çok daha önemli. Sadece şirketlerin yasal sorumlulukları açısından değil, hizmet sundukları müşterilerle güven ilişkisi kurabilmeleri için de çok kritik öneme sahip. Veriyi daha iyi kullanarak daha verimli ve iyi iş sonuçları yaratmak da her an gündemde. Dolayısıyla siber güvenlik alanındaki gelişmeleri anlık takip ediyor, bunları ürün ve sistemlerimize anlık olarak yansıtıyoruz. Birlikte çalıştığımız şirketler için tüm hizmetlerimizde olduğu gibi onların yerine araştırıp, tasarlayıp yönetiyoruz.

Araştırma sonuçlarına göre, olumsuz deneyim yaşamamış şirketlerin yüzde 61'i gelecekte olumsuz bir durum yaşamamak adına herhangi bir önlem almadığı gözleniyor. Gülen'in bu konudaki değerlendirmesi de şöyle: "Dijitalleşmedeki sevindirici hız ne yazık ki riskleri de beraberinde getiriyor. Ancak bu konuda toplumsal risk bilincimiz oldukça düşük. Gözle görülmeyen riskleri yok sayamayız. Dijital güvenlik, Aksigorta olarak sahiplendiğimiz bir alan. 2020 yılında hayata geçirdiğimiz 'Dijital Güvenlik Platformu' risk bilincini topluma aşılamak üzerine kurulmuş bir sosyal sorumluluk projesi. Bu platformla hem KOBİ'lerin hem de bireylerin karşılaşabileceği dijital riskleri ve alabilecekleri önlemleri eğitimlerle aktarıyoruz. Kurum olarak kendimizi müşterilerimizin 'risk yoldaşı' olarak tanımlıyor, dijitalleşen yeni dünyada onların kendilerini daha güvende hissetmeleri için çalışmalarımızı sürdürüyoruz."

DİJİTAL GÜVENLİK PLATFORMU
AKSigorta

BİREYLERİN YÜZDE 54'Ü HERHANGİ BİR ÖNLEM ALMIYOR

Bireysel tüketicilerin risk algısına bakıldığında ise olumsuz bir deneyim yaşamamış yüzde 54'lük kesimin, gelecekte olumsuz bir durum yaşamamak adına herhangi bir önlem almadığı görülüyor. Önlem alan grup içinde ise antivirüs programı kullanımı, tanınmayan sitelerden alışveriş yapmama, kart bilgilerini vermeme gibi konular öne çıkıyor.

Araştırmaya katılan bireysel tüketicilerin yüzde 69'u, dijital güvenlik konusunda alınacak eğitimin risklerin önlenmesi için katkı sağlayacağına inanıyor. Gülen, "2020 yılında toplumsal sorumluluk anlayışıyla hayata geçirdiğimiz Dijital Güvenlik Platformu tam da bu alandaki bilinç eksikliğini gidermek amacıyla ortaya çıktı. Boğaziçi Üniversitesi iş birliğiyle doğan bu proje, bireyler ve KOBİ'ler için ücretsiz eğitimlerin yanı sıra konuya ilişkin güncel haber ve podcast'lerle referans bir bilgi kaynağı niteliğinde. Kuruluşundan bu yana 1 milyonun üzerinde ziyaretçi sayısına ulaşan platform, gerek bireyler gerekse KOBİ'lerin dijital dünyada çok daha güvenle var olabilmesi için destek oluyor" diyor.

ECLIT

Siber saldırganların yeni hedefi sağlık kurumları

Eclit, bilişim dünyasının iki oyuncusu Clonera ve Pukta'nın Turkven ile 2021 yılında güçlerini birleştirmesiyle kuruldu. Şirket, her ölçekteki işletmenin bozuk mouse'lardan buluta kadar en temel ve en karmaşık bilişim-teknoloji ihtiyaçları için uçtan uca hizmetler sunmak amacıyla faaliyet gösteriyor. Çoğu teknik düzeyde olmak üzere 120 çalışanıyla Türkiye'nin e-fatura arşivinin yüzde 56'sının, sigorta poliçelerinin yüzde 45'inin ve perakende e-ticaretin de yüzde 40'ının bilgi teknoloji hizmetlerini yöneten Eclit, siber güvenlik alanındaki çözümleriyle de dikkat çekiyor.
Eclit Kurucu CEO'su Egemen İnce ile şirketin bu alandaki hizmet ve çözümlerini konuştuk...

Siber güvenlik sektörüne yönelik ürün ve çözümleriniz hakkında ayrıntılı bilgi verir misiniz?
IT hizmetlerimizle şirketlere güvenlik seviyesi yüksek, uluslararası standartlarda bir altyapıya sahip olma ve