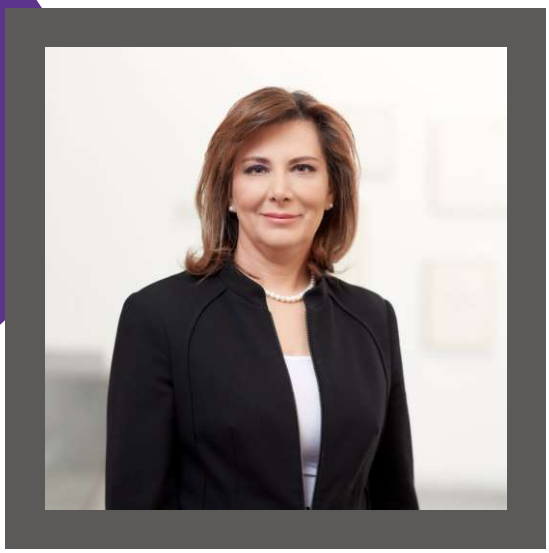
Milli Reasürans olarak yaptığımız değerlendirmeler sonucunda "sıfırıncı gün atakları"nda yüksek bir başarı oranına sahip olan Checkpoint EDR uygulamasına geçilmesi kararı verilmiştir. Checkpoint EDR ürünü, son kullanıcılarının VPN bağlantılarını gerçekleştirebildikleri, içerisinde antivirüs çözümlerinin yanında sıfırıncı gün ataklarına karşı korumalı alanların çalışabildiği bütünleşik bir sistem sunmaktadır.



Şebnem KURHAN ÜNLÜ
Genel Müdür Yardımcısı
Milli Reasürans T.A.Ş

2020 yılının başından itibaren tüm dünyada olduğu gibi ülkemizi de etkisi altına alan Covid 19, birçok şirketin iş modellerinde değişikliğe neden oldu. Biz de Milli Reasürans olarak ülkemizde görülen vaka sayılarındaki artış paralelinde, çalışanlar ve aile bireylerine yönelik risklerin asgariye indirilmesi ve iş sürekliliğinin sağlanması amacıyla Mart ayından itibaren uzaktan çalışma sistemine geçmiş bulunmaktayız.

Şirketimizin çalışanlarımıza sunduğu teknolojik güvenliğe yönelik yapmış olduğu yatırımlar, faaliyetlerimizin kesintisiz olarak yürütülmesini sağlamıştır. Çalışanlarımız iki aşamalı koruma ile desteklenen sanal özel ad (VPN) aracılığıyla, Şirket sunucularına güvenli bir şekilde bağlanabilmiş ve süreçlerini ofis ortamındaki gibi sorunsuz yürütebilmişlerdir.

Öte yandan, Şirketimizin Bilgi Teknolojileri Servisi yaşanan bu özel dönemde yeni saldırı veya atakların olması ihtimaline karşı, son kullanıcılar tarafından kullanılan donanımlardaki güvenlik standartlarının üst bir seviyeye taşınmasını oldukça önemsemiş, "sıfırıncı gün atakları"na karşı çeşitli ürün ve uygulamaları araştırmıştır. Böylelikle genel sistemlerimize uyumlu olarak entegre olan uygulama performans değerlerimizdeki optimizasyonu desteklemiştir.

Son kullanıcıların internet üzerinden indirdikleri dosya veya uygulamalar öncelikle Checkpoint EDR çözümü ile Checkpoint'in sürekli güncellenen veritabanlarında taratılmaktadır. Ancak indirilen dosya veya uygulamalar güvenli olarak EDR tarafından imzalanırsa, son kullanıcı ilgili dosya veya uygulamasını makinasında görüntüleyebilmektedir. Bu yöntemde güvenlik taraması, dosya veya uygulamanın indirilme aşamasında gerçekleştiğinden, süreç tamamlanmadan yaşanabilecek olası tehditler sistem tarafından engellenmektedir.

Bir şirketin sistemlerindeki veriler o şirketin en değerli varlıkları arasındadır. Bu sebeple sistemlerin güvenliğinin sağlanması son derece hassas ve önemli bir konu olarak değerlendirilmektedir. Son kullanıcılar gerek sistemler gerek veriler üzerinde farklı seviyelerde erişim yetkilerine sahip olarak tanımlanmaktadır. Bu yetkilerin kullanımı, çeşitli güvenlik araçlarıyla korunmakta olan şirket sistemlerine açılan pencereler gibi değerlendirilebilir. Güvenliğin uçtan uca sağlanması, açılan bu pencerelerin güvenlik seviyesinin, en az sistemler için oluşturulan güvenlik seviyesi kadar olduğunda söz konusu olmaktadır. Bu nedenle, son kullanıcıların bilgisayarlarında disk şifreleme uygulamaları ve güvenli bağlantı hizmetleri gibi teknolojinin sağladığı imkanlardan yararlanarak güvenli ortamlar yaratılmakta ve kurumumuzun veri güvenliğinin desteklemesi için azami özen göstermekteyiz.

Tüm dünyada teknolojinin hızla ilerlemesi ve ulaşım imkanın artması hayatımızı önemli ölçüde kolaylaştırırken artan riskleri de beraberinde getirmektedir. Pandeminin katalizör etkisiyle hemen her kesim tarafından teknolojinin yaygın bir şekilde kullanımı artarken aynı zamanda bu durum çeşitli siber saldırı veya atakların çeşitlenerek artmasına ve yaratabileceği zarar boyutlarının da üst seviyelere ulaşmasına neden olmaktadır. Şirketlerin veri ve sistem güvenliği konusunda gerçekleştirdiği yatırımlarını arttırması bu tür tehditlerin önüne geçilmesi açısından önem arz etmektedir. Bunun yanı sıra son kullanıcıların da sanal saldırılara karşı öz farkındalıklarını geliştirmeleri yaşanabilecek olumsuzluklara karşı korunma mekanizmalarını destekleyecektir. Zaman zaman en bilinçli kullanıcılarda bile zafiyetlerin oluşabileceği kaçınılmaz bir gerçektir. Bu noktada Millî Reasürans, Bilgi Güvenliği ekibi tarafından yayımlanan bültenler, e-posta bilgilendirmeleri ve çeşitli eğitimler ile son kullanıcılarımızın farkındalığının arttırılması hedeflenmiştir.

Siber saldırılar konusunda yayımlanan bültenler ve bu konuya yönelik önerilen son teknolojiler yakından takip edilerek sistemlerimize önemli ölçüde dahil edilmektedir. Küresel ürün tedarikçiklerinin ve güvenlik konusunda çalıştığımız firmaların ürettiği raporlar, geri bildirimler ve yayımlanan bültenleri oldukça değerli buluyoruz. Bu çerçevede sistemlerimizin ve son kullanıcılarımızın güvenliğini düzenli olarak artırmayı hedefliyoruz.

Son kullanıcı verileri sektörümüz gereği çok değerli bilgiler içermektedir. Bu sebeple Şirket verilerinin zararlı yazılımlardan etkilenmemesini son derece önemsiyoruz. İmza tabanlı antivirus çözümleri yanında şüpheli davranış tabanlı antivirüs çözümlerini de kullanarak zararlı yazılımlara karşı düzenli taramalar yapmaktayız.

Şirketimiz tarafından ağ trafiği içerisindeki zararlı hareketlerin veya bağlantıların tespiti ve önlenmesi için IPS sistem kullanılmaktadır. Güvenlik firmasından haftalık olarak alınan IPS raporları ve analizleri doğrultusunda gerekli bilgileri sağlayarak tüm süreçleri aktif şekilde takip etmekteyiz.