Güvenlik Yazılımlarını “Gagalıyorlar”

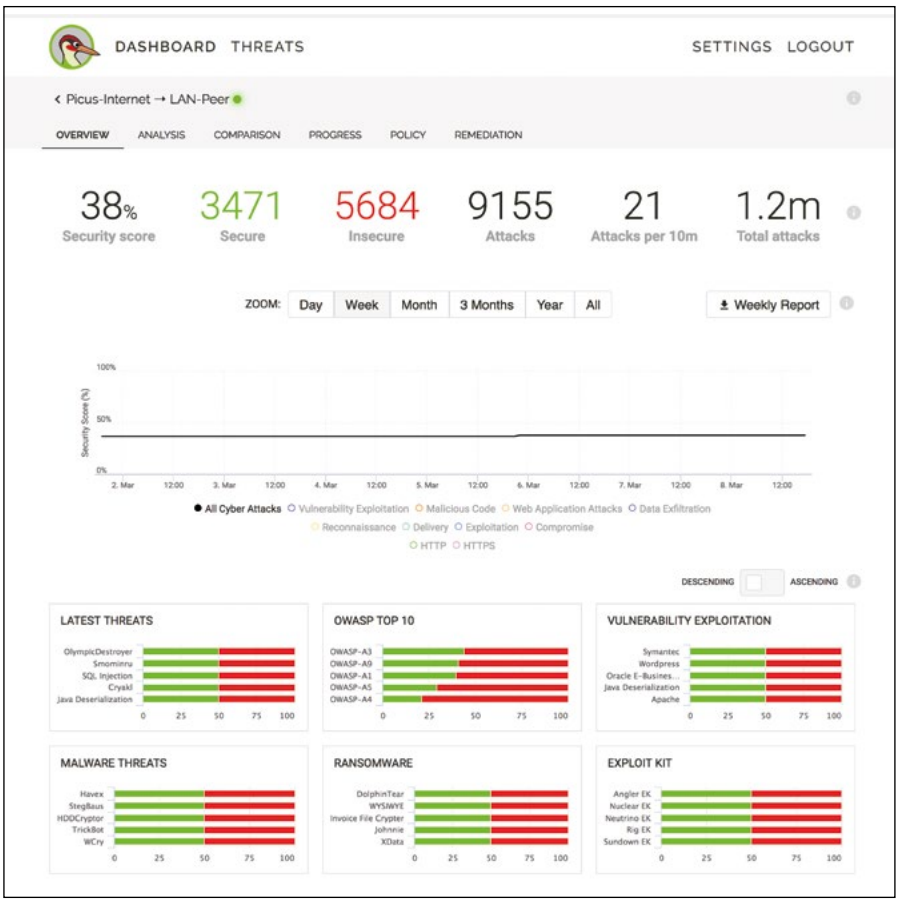
Pınar Dündar [*TÜBİTAK Bilim ve Teknik Dergisi*

Cep telefonlarımızın neredeyse tüm kişisel bilgilerimizi içermesi, bu bilgilerin bir başkasının eline geçme ihtimalinin yarattığı tedirginliği de beraberinde getirdi. Üstelik bilgilerin yayılması için illa telefonumuzun çalınması gerekmiyor. Zararlı yazılımlar yoluyla, internet üzerinden, kilometrelerce uzaktan dahi bilgilerimiz erişime açık hale gelebiliyor.

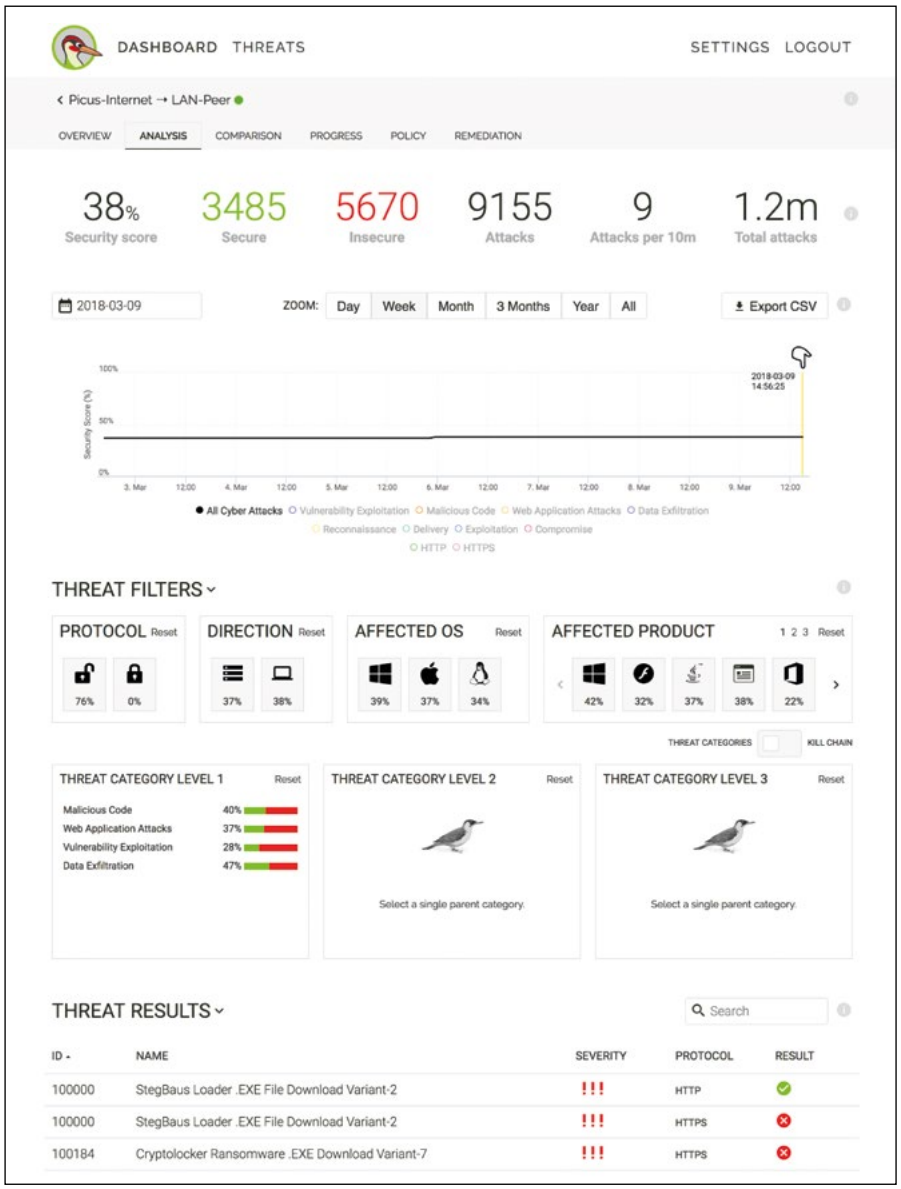
Diğer yandan internet ortamında kişisel veriler için geçerli olan tehditler kurumlar için de geçerli. Kurumsal yapılar söz konusu olduğunda da verileri korumak için çok geniş kapsamlı çözümler gerekiyor.

Her şey sayısal veriye dönüştükçe firmalar ve kamu kurumları verilerini koruma konusunda daha titiz ve dikkatli davranıyor, bunun için güvenlik yazılımlarına büyük miktarlarda para harcıyor. Çünkü güvenlik açıklarının yarattığı sorunlar verilerin çalınmasından kurumların veri tabanının çökertilmesine kadar gidebiliyor. Buradaki sorun kurumların, satın aldıkları güvenlik yazılımlarının ne kadar işe yaradığını bilmemesi. Projesi, TEYDEB'in 2016 yılı başarı hikâyeleri arasında yer alan Picus Security adlı firma da işte burada devreye giriyor ve "kurumların yurtdışından satın aldıkları güvenlik yazılımları onları ne kadar etkin koruyor" sorusuna yanıt veriyor. Bu sayede kurum yöneticileri bilişim güvenliği (kurumsal ağ güvenliği ve veri güvenliği) kapsamında kullanılan ürünlere yaptıkları yatırımın onları ne kadar geliştirdiğini ve yeni siber ataklara karşı ne kadar hazırlıklı olduklarını öğrenip gerekli önlemleri alabiliyor.

Firmanın kurucu ortaklarından Volkan Ertürk, işe başladıklarında dünya piyasasında söz konusu soruya cevap veren bir ürün olmadığını belirtiyor. 2013'te TEYDEB'in 1512 kodlu Girişimcilik Aşamalı Destek Programı'ndan yararlanarak ODTÜ Teknokent bünyesinde kurulan ve şu an Hacettepe Üniversitesi Teknokent bünyesinde faaliyet gösteren firma, karşılık beklemeyen bir yatırımcıdan alınan destekle aynı yıl içinde ürünün prototipini geliştirmiş. Ardından TEYDEB'in 1507 kodlu TÜBİTAK KOBİ Ar-Ge Başlangıç Destek Programı ile prototipi ürün haline getirmiş. 2014'te Ankara'da ilk satışlarını kamu kurumlarına gerçekleştiren firma, 2015'te İstanbul'da bankalara ve özel sektöre satışlar yapmış. Ürünün yurtdışına ilk satışı ise 2016'da Singapur'a gerçekleştirilmiş. Firmanın şu anda Türkiye'de elliden fazla müşterisi var. Türkiye'deki büyük on bankanın sekizi Picus Security'nin geliştirdiği yazılımı kullanıyor.



Firmanın geliştirdiği bilişim güvenliği ürünleri analiz ve denetim yazılımında, kurumların veri güvenliği için gereken bilgiler farklı bölümler altında, ayrıntılı olarak veriliyor. Örneğin bu resimde görülen *overview* bölümü toplam kaç atak gerçekleştiği, bunların kaçının güvenlik açığından geçtiği gibi bilgileri sunuyor. Alttaki tablolarda ise hem son çıkan tehditlere göre hem de farklı tehdit gruplarına göre kullanıcının güvenlik durumu görülebiliyor.



Analysis bölümü, kullanıcının güvenlik durumunu daha detaylı olarak inceleyebildiği bir bölüm. Kullanıcı bu bölümde filtreleme yaparak en çok kullandığı ürünleri (örneğin Office programını) seçip bunların ne durumda ne olduğuna bakabiliyor.

Picus Security'nin geliştirdiği ürün "bilişim güvenliği ürünleri analiz ve denetim yazılımı" olarak adlandırılıyor. Yazılım kurumların güncel siber ataklara karşı ne kadar hazırlıklı olduğunu test ederek, kurumları bu tehditlere karşı neler yapılması gerektiği konusunda bilgilendiriyor. Kurumlar yazılımı internet üzerinden ya da kendi sistemlerine yükleyip kullanabiliyor. Ancak tehditlerin sayısı ve niteliği sürekli değiştiğinden, yazılımın da bu tehditleri tespit etme ve bunlara karşı çözümler sunma özelliklerinin de sürekli geliştirilmesi gerekiyor. Bu nedenle kurumlara sabit bir yazılım satılmıyor, bunun yerine *software as a service* olarak bilinen yazılım bir tür hizmet olarak kiralanıyor. Düzenli olarak güncellenen ve geliştirilen yazılımın şu anki yıllık birim fiyatı yaklaşık 20 bin dolar. Bu fiyat güvenlik sistemlerinin kontrol edilmesi istenen birim sayısına göre değişiyor (e-posta güvenliği, ağ güvenliği, istemci güvenliği vs.). Bir ağ üzerinde, sunucu bilgisayarlardan hizmet alan kullanıcı bilgisayarlara istemci bilgisayar adı veriliyor.

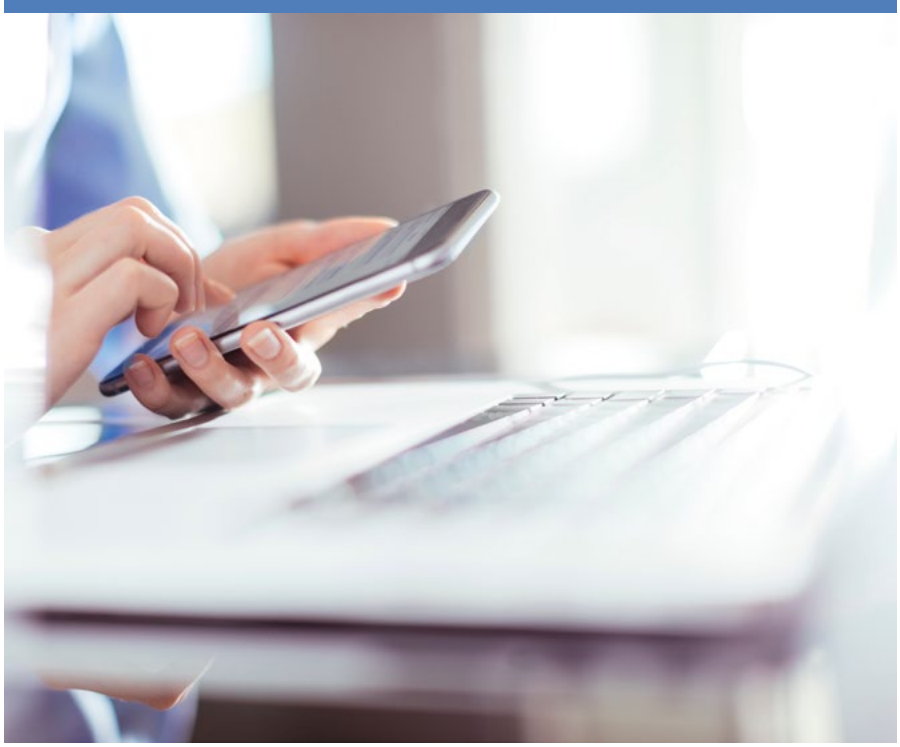
Ertürk, Latince bir sözcük olan *picus*'un ağaçkakan anlamına geldiğini, Picus Security ürününün de tıpkı bir ağaçkakan gibi güvenlik yazılımlarını "gagaladığını" söylüyor. Bunun teknik anlamdaki karşılığı ise atak simülasyonu. Geliştirilen ürün, bilgisayar korsanları tarafından bilinen atak yöntemlerini kullanarak, kurumun kullandığı güvenlik sistemlerindeki eksikleri ortaya çıkarıyor. Buna ek olarak, bu eksiklerin giderilmesi için kuruma mevcut güvenlik altyapısında yapabileceği iyileştirmeler de sunuyor. Firmanın geliştirdiği yazılımın yaptığı iş kısaca saldırgan bakış açısıyla güvenliği sağlamak olarak adlandırılıyor (*offensive security*). Güncel siber atakların geliştirildiği güvenlik laboratuvarlarında çalışan kişiler ise "beyaz şapkalı hacker" olarak biliniyor.

İnternetten indirdiğiniz dosyanın virüslü çıkması, web sunucusu üzerinden bilgisayarınıza zarar verecek bir istek gönderilmesi gibi birçok durum karşısında kişisel verileriniz tehlike altına girebiliyor.

Bilgi Güvenliği

Bilgi, fiziksel bir ortama kaydedilmiş, düzenlenebilen, saklanabilen herhangi bir iletişim aracıyla başkalarına iletilebilen anlamlı veriler topluluğu olarak tanımlanır.

Bilgi güvenliği ise sayısal ya da analog her tür bilginin silinmeye, bozulmaya ve olası saldırılara karşı korunmasını sağlayan uygulamaları kapsar. Bilgi güvenliğinin üç temel ilkesi vardır. Bu ilkeler, bilginin sürekli korunması gereken niteliklerine karşılık gelir: Gizlilik, bütünlük ve erişilebilirlik. Kurumsal açıdan düşünüldüğünde gizlilik yetkisi olmayan kişilerin kuruma özel ve gizli bilgilere erişiminin engellenmesi, bütünlük kurumsal bilgilerin yetkisiz kişilerden kaynaklanan değişmelere veya bozulmalara karşı korunması, erişilebilirlik ise kurumsal bilginin ve kaynakların ihtiyaç duyulduğunda yetkili kişilerce güvenilir bir şekilde erişilebilir olması anlamına gelir. Siber güvenlik anlamlı ya da anlamsız her tür verinin siber ortamda korunmasına karşılık gelirken, bilgi güvenliğinde ortamın bir önemi yoktur.



Günümüzde iletişimden bilgi depolamaya, alışverişten bankacılık işlemlerine kadar birçok işin bilişim teknolojileri yoluyla yapılabilmesi, dijital ortamlarda bulunan bilginin güvenliğine, diğer bir ifadeyle bilişim güvenliğine çok önem kazandırıyor. Uzmanlar kurumsal bilgi kaynaklarının hatalı kullanım, yazılım ya da donanım hırsızlığı, mevcut sistemlerle uyumsuz donanım kullanımı, lisanssız yazılım kullanımı, virüsler, istenmeyen e-postalar, bilgisayar korsanları gibi nedenlerle risk altında olabileceğini belirtiyor.

Siber güvenlik alanında yazılım geliştiren lider firmalardan olan Picus Security'nin hedefi zaman içinde hâlihazırda 33 kişiden oluşan ekibini büyütmek ve Avrupa'da ve ABD'de atak simülasyonu pazarında öne çıkmak. Yurtdışındaki rakip firmaların çok daha fazla maddi destek alması ve piyasadaki iletişim ağlarının geniş olması nedeniyle ürün geliştirme ve satış faaliyetlerinde hızlı olmaları Picus Security'nin karşılaştığı en büyük engeller. Ancak Ertürk bu alanda dünyada faaliyet gösteren ilk firma olmalarının deneyim açısından kendilerine avantaj sağladığını belirtiyor.

TÜBİTAK'ın sanayi alanında destek verdiği programlar hakkında daha fazla bilgi almak için https://www.tubitak.gov.tr/tr/destekler/sanayi/ulusal-destek-programlari internet sitesini ziyaret edebilir ya da aşağıda yer alan kare kodu akıllı cihazınıza okutabilirsiniz. Firma hakkında ayrıntılı bilgiye ise https://www.picussecurity.com/ internet sitesinden ulaşabilirsiniz. ■

Picus Security ekibinden Volkan Ertürk ve Selcen Kökcü Çetin'e teşekkür ederiz.

Kaynaklar

Öztemiz, S. ve Yılmaz, B., "Bilgi Merkezlerinde Bilgi Güvenliği Farkındalığı: Ankara'daki Üniversite Kütüphaneleri Örneği", *Bilgi Dünyası*, Cilt 14, Sayı 1, s. 87-100, 2013.

https://www.infosec.gov.hk/english/information/what.html

https://doi.org/10.6028/NIST.SP.800-12r1

http://searchcio.techtarget.com/definition/ICT-information-and-communications-technology-or-technologies