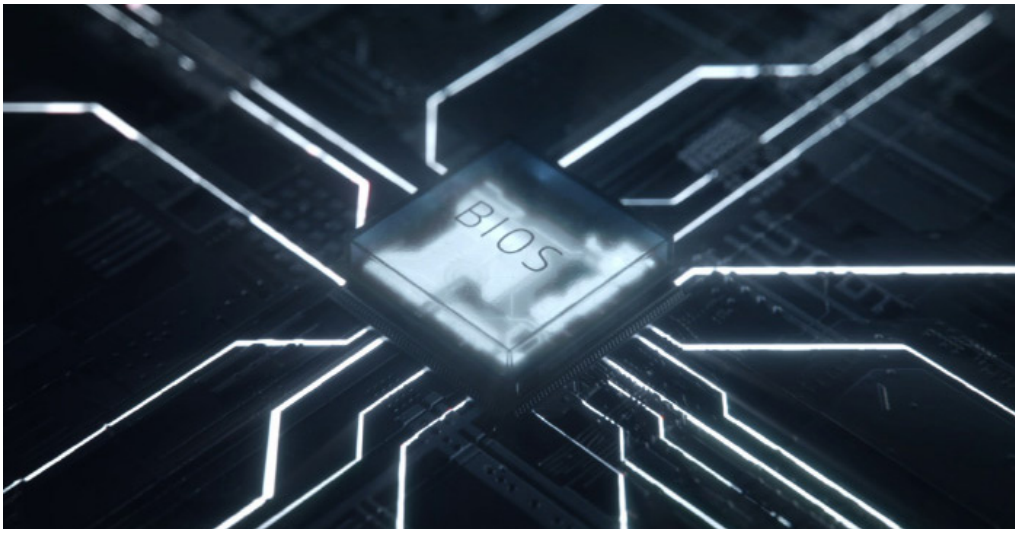
Otomatik savunmalar iş cihazlarınızı niçin koruyacak

Emre Gursoy tarafından yazıldı

Ayrintili bilgi edinin



Savunmalarınızın altında saklanan tehditle nasıl savaşırsınız? Otomatikleştirirsiniz.

Yılda 338 milyar sterlin. Bu, dünya çapında şu anda mevcut olan siber suç maliyetidir1. Bilgisayar korsanları daha yetkin ve kabiliyetli hale geldikçe, bu rakam da giderek büyüyor. BT yöneticilerinin felaketi olmak için yapılan en yeni gizli saldırılardan biri BIOS saldırısıdır.

Milyonlarca makine, BIOS konusunda savunmasız kaldıkları temel noktalara sahip. Bu da orta düzeyde bile bilgisayar korsanlığı becerisine sahip biri tarafından saldırılabilecekleri anlamına geliyor. Araştırmacılar Xeno Kovah ve Corey Kallenberg bir kaç yıl önce bir konferansta yeni tip bir saldırı sunarak birkaç saat içinde birden fazla sistemin BIOS'una uzaktan saldırıp zarar verebileceklerini gösterdiler2. Çoğu BIOS aynı kodu paylaştığı için, kod bir kez kırıldığında aynı becerileri kullanarak pek çok diğer makinenin savunmasını devirmek sadece an meselesiydi.

Korunmayan bir yeri hedeflediği için bu saldırı türü çok tehlikelidir. İşletim sistemi ve donanım arasında önceden göz ardı edilen gizli bir boşluk vardır. Ağınız hata kabul etmez görünse ve cihazınız dünyadaki en iyi güvenlik sistemlerinin arkasında korunuyor olsa da, cihazınızın çalışmaya başlaması ve savunmanızın devreye girmesi arasında yine de kısa bir süre vardır. Bu süre, düşman BIOS saldırısının cihazınızı mahvedebileceği zaman aralığıdır.

Bir çok siber güvenlik yazılımı işletim seviyesinde/seviyesinin üzerinde olsa da BIOS' a sızmış olan (cihaz çalışıp Sistem Yönetim moduna geçmeden önce) kötü amaçlı yazılım, uç nokta siber güvenlik yazılımında tespit edilemez olacaktır. Buradan harekete geçerek, bilgisayar korsanları sizin BIOS'unuzu uzaktan ve süresiz olarak yönetilebilen kendi kişisel sürümleri ile değiştirecektir. En kötüsü, ihlal ve bulaşma meydana geldiğinin fark edilmesi neredeyse imkânsızdır.

Şirket cihazlarınızı korumanın en iyi yolu çok katmanlı güvenlik kullanmaktır. BT ekibinizin yetenekleri, sürekli tarama ve manuel düzeltmelerle kuşatılmamalıdır. HP, güvenlik çözümleri yelpazesinin bir parçası olarak, otomatik bir müdahale olan HP Sure Start'ı sunmaktadır.

"Bu uygulama, şirketlerin riskleri daha iyi yönetmeleri ve kullanıcı ile BT verimliliğini kötü niyetli saldırılara, başarısız bir güncellemeye ya da kazai veya bilinmeyen başka herhangi bir nedenden korumalarına yardımcı olmak için HP Labs ile gösterdiğimiz ortak çabanın parçasıdır,"

- Vali Ali, HP PC İşletme Birimi Güvenlik ve Gizlilik Baş Teknoloji Uzmanı.

Otomatik savunmalar iş cihazlarınızı niçin koruyacak

HP Sure Start kendi kendini onaran, BIOS seviyesinde bir korumadır. Bu yaklaşımı siber direnç olarak adlandırıyoruz. Bu sistem, BIOS için bir üst düzey koruma katmanı (gold master) oluşturarak çalışır ve bu katman, doğrudan cihaza şifrelenir. Böylece, birisi BIOS'a saldırmaya çalışırsa, otomatik olarak kendisini çalıştırıp ardından "gold master"ı yükler ve etkilenen dosyayı temizleyerek sizi ve ekibinizi saldırı konusunda bilgilendirir. Temel olarak makine kendi kendini iyileştirir.

Bu da kesintisiz verimlilik anlamına gelir. Kesintisiz verimlilik ise daha düşük masraflar anlamına gelir. Bu durum daha uyumlu cihazları beraberinde getirir. Bütün bunların ötesinde, daha kolay bir çalışma şeklidir.

HP Sure Start'a sahip en son teknoloji ürünü cihazları kullanıcılarınızın önüne getirmenin en kolay yolunun ne olduğunu merak ediyorsanız, HP Hizmet Olarak Cihaz'ı değerlendirin. Ticari kuruluşların çalışanlarını doğru donanım ve aksesuarlarla donatma, çoklu işletim sistemi filolarını yönetme ve ek yaşam döngüsü hizmetlerini sağlama yollarını basitleştiren modern bir PC tüketim modelidir. HP DaaS, her şeyin sorunsuz ve etkili şekilde çalışması için basit fakat esnek planları cihaz başına tek fiyatla sunar.

Uç noktaların ve erişim noktalarının her seviyede izlenmesi gerekir. Cihazlarımızın gizli parçalarından kaçmayı bırakmanın zamanı geldi. Dünyadaki her kişi, iş ve kuruluş HP EliteBook 800 Serisi (isteğebağlı 8. Nesil Intel® Core™ İşlemcileri ile birlikte) dâhil olmak üzere HP portföyünün ürün teklifleri ile daha güvenli ve daha dirençli hale gelebilir. HP Elite ailesinin parçası olan bu cihaz, HP Sure Start gibi yerleşik güvenlik özellikleri sayesinde güvenli teknoloji sunar.

Şirket cihazlarınızı nasıl koruyacağınız konusunda daha fazla bilgi edinmek için, en yeni HP Sure Start İş Raporunu okuyun ve HP güvenlik çözümlerinin işinize faydalarını keşfedin.

Fontes:

1. https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
2. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
3. Çeşitli HP Sure Start nesilleri, HP Elite ve HP Pro sistemlerinin seçili yapılandırmalarında bulunmaktadır.

4AA7-3219TRE, Mayıs 2018