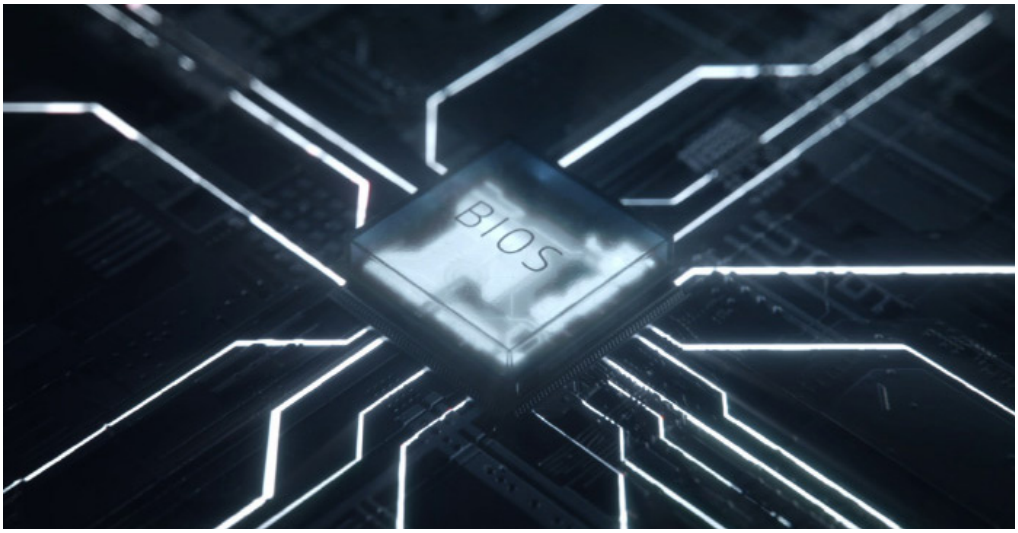
لماذا تستطيع الدفاعات التلقائية حماية أجهزة شركتك؟

بقلم: سكينة الإدريسي

Learn more



كيف يمكنك مكافحة جريمة إلكترونية متخفية تحت دفاعاتك؟ أن تضع لها آلية دفاع تلقائي.

338 مليار جنيه إسترليني في العام؛ هذه هي قيمة الخسائر الحالية بفعل الجرائم الإلكترونية في جميع أنحاء العالم[1]. وهذا الرقم يتزايد باضطراد في ظل تطور القراصنة وقدراتهم. من بين أحدث الهجمات الفتاكة التي صارت كارثة بالنسبة لمديري تكنولوجيا المعلومات هي الهجمات على نظام الإدخال والإخراج الأساسي (BIOS).

تضم ملايين الأجهزة ثغرات أمان أساسية بنظام BIOS، وهذا معناه أنّ من الممكن اختراقها بواسطة شخصٍ ما، حتى لو كانت مهاراته في القرصنة متوسطة. قام الباحثان زينو كوفا وكوري كالينبرغ بعرض نوع جديد من الهجمات في مؤتمر منذ عدّة سنوات مضت، حيث أظهرا أنّه في خلال ساعات معدودة كان بإمكانهما اختراق نظام الإدخال والإخراج الأساسي (BIOS) ونشر فيروس في العديد من الأنظمة عن بُعد[2]. ولأنّ غالبية أنظمة BIOS تتشارك نفس التعليمات البرمجية، فما إن تم اختراق النظام الأول، كانت المسألة مجرد وقت إلى أن صارت تلك المهارات نفسها قادرة على تجاوز دفاعات العديد من الأنظمة الأخرى.

هذا النوع من الهجمات خطير للغاية لأنّه يستهدف أي مكان لم تتم حمايته. هناك مكان خفي بين نظام التشغيل ومكونات الأجهزة الداخلية، عادةً ما يتم تجاهله. وبينما تظهر شبكتك بمظهر الشبكة القوية دونما ثغرة، ويظهر جهازك محميًا خلف أفضل أنظمة الأمان في العالم، فهناك جزء من الثانية بين بدء تشغيل الجهاز وانطلاق دفاعاتك. في هذه اللحظة يمكن أن يؤدي الهجوم العدائي على BIOS إلى إحداث فوضى عارمة.

وبما أنّ معظم برامج الأمان الإلكتروني تعمل فقط عند مستوى نظام التشغيل، فإنّ البرنامج الضار الذي تم حقنه في نظام BIOS (قبل بدء تشغيل النظام وانتقاله إلى وضع إدارة النظام «System Management Mode») سيكون غير مرئي بالنسبة لبرنامج الحماية الإلكتروني على الجهاز الطرفي. ومن هناك، سيقوم القراصنة باستبدال نظام BIOS الأصلي لديك بالإصدار المُعدّل الخاص بهم، والذي يمكن إدارته عن بُعد بلا حدود. وأسوأ ما في الأمر، أنه قد يكون شبه مستحيل اكتشاف حدوث الخرق وقرصنة النظام من الأساس.

أفضل طريقة لحماية أجهزة شركتك تتمثل في استخدام الأمان متعدد الطبقات. لا ينبغي تضييق نطاق قدرات فريق تكنولوجيا المعلومات بشركتك على الفحص الدائم والإصلاحات اليدوية للنظام. وذلك لأن HP تقدم نظام استجابة تلقائي – كجزء من مجموعة متنوعة من حلول الأمان – HP Sure Start.

«هذا جزء من جهد مشترك مع مختبرات HP لمساعدة الشركات على إدارة المخاطر بشكلٍ أفضل وحماية إنتاجية المستخدمين وفريق تكنولوجيا المعلومات من الهجمات الضارة، أو تحديث فاشل، أو أي سبب آخر عارض أو غير معروف»

– ڤالي علي، كبير متخصصي الأمان والخصوصية في وحدة أعمال أجهزة الكمبيوتر الشخصية بشركة HP.

كيف يمكنك مكافحة جريمة إلكترونية متخفية تحت دفاعاتك؟ أن تضع لها آلية دفاع تلقائي

HP Sure Start عبارة عن نظام حماية ذاتي الإصلاح على مستوى نظام BIOS. ونحن نطلق على هذا المنهج «المرونة الإلكترونية». يعمل النظام عن طريق إنشاء «نسخة أصلية (gold master)» من نظام BIOS، بحيث يتم تشفيرها مباشرةً على الجهاز. وهكذا، عندما يحاول شخصٌ ما اختراق نظام BIOS، يقوم النظام بإعادة تشغيل نفسه تلقائيًا، ثم تحميل «النسخة الأصلية»، ومحو الملف المصاب، وإبلاغك أنت وفريق عملك بحدوث الهجمة. خلاصة القول أنّ الجهاز يعالج نفسه بنفسه.

هذا يعني إنتاجية مستمرة دون انقطاع، وتكاليف أقل. كما يعني أجهزة أكثر امتثالاً للمعايير. وعلاوة على كل ذلك، فهو حل أكثر سهولة في التنفيذ.

إذا كنت تبحث عن أسهل طريقة للحصول على أجهزة فائقة التطور تشتمل على تقنية HP Sure Start مُمكّنة لدى المستخدمين، فستجد ضالتك في استخدام الأجهزة كخدمات من HP. وهو نموذج استهلاك حديث لأجهزة الكمبيوتر الشخصية يُبسّط كيفية تزويد المؤسسات التجارية موظفيها بالأجهزة والملحقات المناسبة، وإدارة أساطيل الأجهزة متعددة أنظمة التشغيل، والحصول على خدمات إضافية لإدارة دورة عمر الأجهزة. تقدم خدمة HP DaaS خططًا بسيطة مرنة، بسعر مُوحّد لكل جهاز، كي يظل كل شيء يعمل بسلاسة وكفاءة.

ينبغي مراقبة الأجهزة الطرفية المتصلة بالشبكة ونقاط الدخول على كل مستوى. لقد حان وقت التوقف عن تجاهل الأجزاء الخفية من أجهزتنا. بمقدور كل شخص، أو شركة، أو مؤسسة في جميع أنحاء العالم أن تصبح أكثر أمانًا ومرونة بفضل مجموعة منتجات HP المتنوعة، والتي من بينها سلسلة أجهزة HP EliteBook 800 Series، المزوّدة اختياريًا بمعالجات Intel® Core™ من الجيل الثامن. كجزء من عائلة HP Elite، فهذا الجهاز مزوّد بتقنيات أمان بفضل ميزات الأمان المدمجة به مثل HP Sure Start.

للتعرّف على المزيد عن كيفية حماية أجهزة شركتك، تفضَّل بقراءة المستندات الرسمية عن ميزة HP Sure Start، واستكشف مزايا حلول الأمان المقدمة من HP لشركتك.

المصادر:

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. أجيال متنوعة من HP Sure Start متاحة مع تكوينات معيّنة من أنظمة HP Elite وHP Pro.

4AA7-3219ARE, رايا 2018