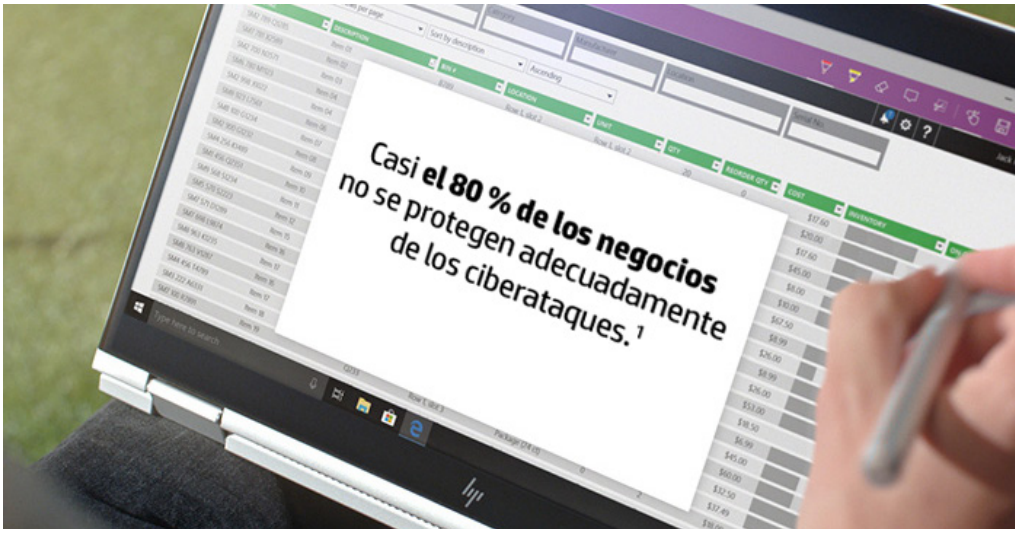
Cómo una defensa automática puede salvar los dispositivos de tu empresa

Más información



¿Cómo te puedes enfrentar a una amenaza oculta tras tus defensas? Apostando por la automatización.

600 000 millones de USD al año. Ese fue el coste de los delitos cibernéticos en todo el mundo en 2017[2]. Un número que sigue aumentando al tiempo que los hackers se vuelven cada vez más sofisticados y habilidosos. Recientemente se ha sabido que el 20 % de pymes tuvo que detener sus operaciones empresariales de manera inmediata y un 12 % perdió ingresos después de un ciberataque[3]. Uno de los últimos ataques por sorpresa que se ha convertido en la pesadilla de los directores de IT es el que ataca el firmware durante el arranque del ordenador: los ataques a la BIOS.

Millones de máquinas poseen una BIOS vulnerable, lo que significa que podrían ser hackeadas incluso por alguien con habilidades de pirateo moderadas. Los investigadores Xeno Kovah y Corey Kallenberg presentaron hace unos años un nuevo tipo de ataque en una conferencia y desvelaron que en unas pocas horas podían hackear e infectar de manera remota la BIOS de varios sistemas[4]. Debido a que la mayoría de las BIOS comparten el mismo código, una vez que se penetraba en la primera, solo era cuestión de tiempo que las defensas de muchas otras máquinas fueran derribadas.

El peligro de este tipo de ataque se debe a que se centra en un lugar que no ha sido protegido. Existe un espacio oculto entre el sistema operativo y el hardware que solía ignorarse. Y, aunque tu red pueda parecer hermética y tu dispositivo esté protegido por el mejor software antivirus del mundo, sigue habiendo un breve momento entre el arranque y el encendido de las defensas en el que un ataque a la BIOS puede sembrar el caos.

La mayoría de software de ciberseguridad se encuentra al mismo nivel que el sistema operativo, por lo que el software malintencionado o malware inyectado en la BIOS (antes del arranque e introducido en el Modo de Gerencia de Sistema) será indetectable para el software de ciberseguridad del terminal. Una vez ahí, los hackers obtienen un control total sobre tu sistema. Podrán robar tus datos, hacerlos ilegibles o propagar nuevo malware por toda la red de tu empresa. Y lo que es peor, es casi imposible descubrir si se ha producido una vulneración o una infección.

La mejor forma de proteger los dispositivos de tu empresa es empleando seguridad de múltiples capas. No desperdicies las habilidades de tu equipo de IT con análisis constantes y reparaciones manuales. HP ofrece una respuesta automática como parte de una gama de soluciones de seguridad: HP Sure Start[5].

"Esto forma parte de un esfuerzo conjunto con HP Labs para hacer que los negocios gestionen mejor los riesgos y protejan la productividad de usuarios y IT frente a ataques maliciosos, actualizaciones fallidas o cualquier otra causa accidental o desconocida".

- Vali Ali, director de Tecnología de seguridad y privacidad de la unidad de negocio de ordenadores de HP.

Cómo una defensa automática puede salvar los dispositivos de tu empresa

HP Sure Start es una protección autorreparadora a nivel de la BIOS. A este enfoque lo llamamos resistencia cibernética. El sistema funciona creando una "versión final" de la BIOS, que está cifrada directamente en el dispositivo. De esta forma, si alguien intenta hackear la BIOS, esta se reinicia automáticamente y carga la "versión final", elimina el archivo infectado y te informa a ti y a tu equipo del ataque. En resumen, la máquina se autorrepara.

Esto supone una productividad ininterrumpida, menos costes y dispositivos más compatibles. Y, sobre todo, facilita mucho el trabajo.

Si estás planteándote la manera más sencilla de disponer de dispositivos innovadores con HP Sure Start para tus usuarios, ten en cuenta HP Device as a Service (HP DaaS)[6]. Es un modelo de servicio moderno de ordenadores que simplifica la forma en que las organizaciones comerciales proporcionan a sus empleados hardware y accesorios adecuados, gestionan flotas de dispositivos con múltiples sistemas operativos y obtienen servicios del ciclo de vida adicionales. HP DaaS ofrece planes sencillos a la vez que flexibles, a un precio por dispositivo para que todo funcione sin problemas y de manera eficiente.

Los terminales y los puntos de acceso deben monitorizarse a todos los niveles. Es hora de plantar cara a las partes ocultas de nuestros dispositivos. Todas y cada una de las personas, negocios y organizaciones del mundo pueden volverse más seguros y resistentes con el catálogo de productos de HP, como la serie HP EliteBook x360, con procesadores opcionales Intel® Core™ i7 de 8.ª generación. Como parte de la familia HP Elite, este dispositivo ofrece tecnología de seguridad gracias a sus características de seguridad integrada, como HP Sure Start.

Descubre las ventajas que ofrecen las soluciones de seguridad de HP a tu negocio.

Fuentes:

1. Encuesta de Statista con ID 622857, "Small and medium sized enterprises in the U.S" de Statista, octubre de 2016
2. https://www.mcafee.com/enterprise/en-gb/solutions/lp/economics-cybercrime.html
3. Informe Osterman, patrocinado por Malwarebytes "Second Annual State of Ransomware Report: US Survey Results", julio de 2017
4. https://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/
5. Varias generaciones diferentes de HP Sure Start están disponibles en configuraciones seleccionadas de los sistemas HP Elite y HP Pro.
6. Los planes y/o componentes de HP DaaS incluidos pueden variar según la región o el proveedor de servicios autorizado de HP DaaS. Contacta con tu representante local de HP o tu socio de DaaS autorizado para obtener información específica en tu ubicación. Los servicios HP se rigen por los términos y condiciones aplicables de HP que se proporcionan o indican al cliente en el momento de la compra. El cliente puede tener derechos legales adicionales según las leyes locales respectivas, los cuales no se ven afectados en modo alguno por los términos y condiciones de servicio de HP ni por la garantía limitada de tu producto HP.

4AA7-3219ESES, abril de 2019