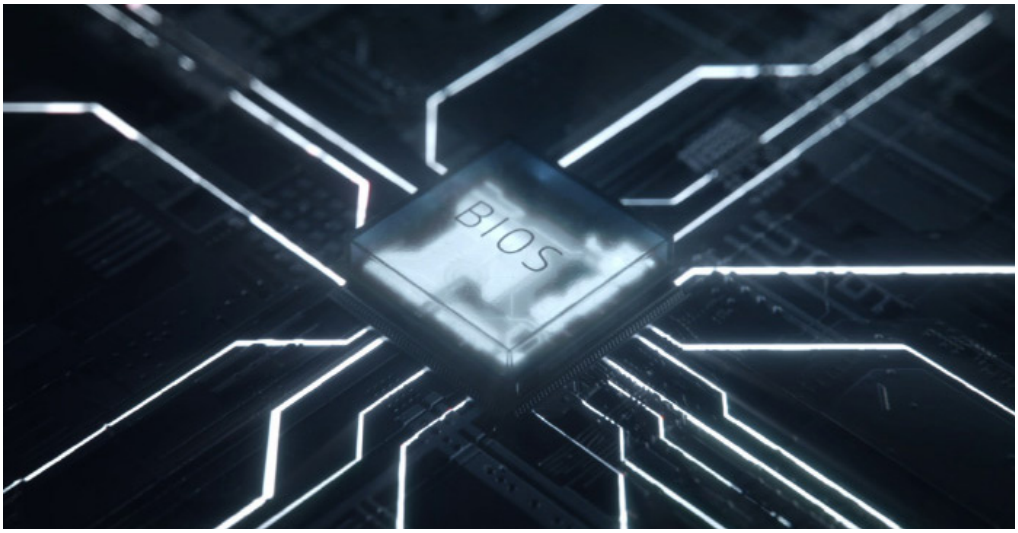
Por qué una defensa automática salvará los dispositivos de su empresa

Más información



¿Cómo se enfrenta a una amenaza oculta tras sus defensas? Apostando por la automatización.

338 mil millones de GBP al año. Ese es el coste actual de los delitos cibernéticos en todo el mundo[1]. Un número que sigue aumentando al tiempo que los hackers se vuelven cada vez más sofisticados y habilidosos. Uno de los últimos ataques por sorpresa en convertirse en la pesadilla de los directores de TI es el ataque 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, desvelando que en unas pocas horas podían hackear e infectar de manera remota la BIOS de múltiples sistemas[2]. 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 su red pueda parecer hermética y su dispositivo esté protegido por los mejores sistemas de seguridad del mundo, sigue habiendo un breve momento entre el arranque y el encendido de las defensas. Es en este momento cuando un ataque BIOS hostil puede sembrar el caos.

La mayoría de softwares de ciberseguridad se encuentran 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. En este punto, los hackers reemplazarán su BIOS con su propia versión modificada, que puede controlarse de forma remota indefinidamente. 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 su empresa es empleando seguridad de múltiples capas. No desperdicie las habilidades de su equipo de TI con análisis constantes y reparaciones manuales. HP ofrece una respuesta automática como parte de una gama de soluciones de seguridad: HP Sure Start.

"Esto es parte de un esfuerzo conjunto con HP Labs para hacer que los negocios gestionen mejor los riesgos y protejan la productividad de usuarios y TI 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 PC de HP.

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",

Por qué una defensa automática salvará los dispositivos de su empresa

elimina el archivo infectado y le informa a usted y a su 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 está planteándose la manera más sencilla de disponer de dispositivos innovadores con HP Sure Start para sus usuarios, tenga en cuenta el Dispositivo como servicio de HP. Es un modelo de consumo moderno para PC 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 800, con procesadores opcionales Intel® Core™ de octava 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.

Para obtener más información sobre cómo proteger los dispositivos de su empresa, lea nuestro último Libro blanco sobre HP Sure Start y descubra los beneficios para su negocio con las soluciones de seguridad de HP.

Fuentes:

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. Generaciones diferentes de HP Sure Start están disponibles en configuraciones seleccionadas de los sistemas HP Elite y HP Pro.

4AA7-3219ESE, Mayo de 2018