

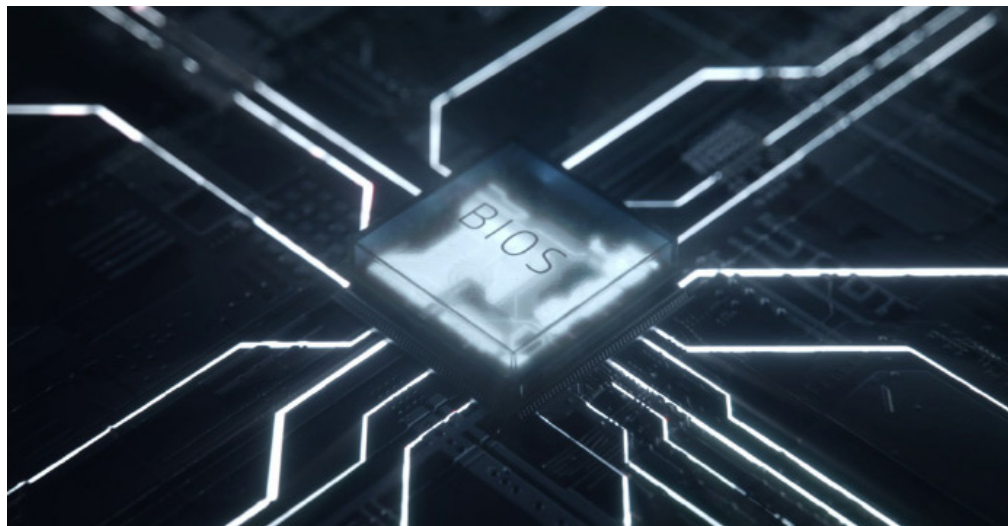


Como as defesas automáticas vão proteger os seus dispositivos

Escrito por Alexandre Silveira



Saiba mais



Como combater uma ameaça oculta? Automatize.

338 mil milhões de libras por ano. É o custo atual do cibercrime em todo o mundo¹. O número aumenta à medida que os hackers se tornam mais sofisticados e capazes. Um dos recentes ataques que mais assustam gestores de TI é o ataque à BIOS.

Milhões de máquinas têm vulnerabilidades básicas na BIOS, o que significa que podem ser hackeadas por alguém mesmo com aptidões de hacking moderadas. Os investigadores Xeno Kovah e Corey Kallenberg apresentaram um novo tipo de ataque numa conferência há uns anos, revelando que em poucas horas poderiam atacar e infetar remotamente a BIOS de diversos sistemas². Visto que a maioria das BIOS partilham o mesmo código, assim que o primeiro for decifrado, é uma questão de tempo para que as defesas de muitas outras máquinas sejam derrubadas.

Este tipo de ataque é tão perigoso porque tem como alvo algo que não está protegido. Existe um espaço oculto entre o sistema operativo e o hardware, que é normalmente ignorado. E enquanto a sua rede poderá parecer estanque e o seu dispositivo protegido com os melhores sistemas de segurança no mundo, há um breve momento durante o arranque em que as suas defesas estão em baixo. É o momento em que um ataque à BIOS pode causar o caos.

Sendo que a maioria do software de cibersegurança está ao nível do sistema operativo, o malware injetado na BIOS (antes do arranque e passando para o Modo de Gestão do Sistema) será indetetável no software de cibersegurança no endpoint. A partir daqui, os hackers substituem a sua BIOS pela sua própria versão personalizada, que pode ser gerida remota e indefinidamente. O pior é que é quase impossível descobrir que a falha e infeção ocorreram.

A melhor forma de proteger os dispositivos da sua empresa é usando segurança em várias camadas. As capacidades da sua equipa de TI não devem resumir-se a constante verificação e reparações manuais. A HP fornece uma resposta automática – como parte de uma gama de soluções de segurança – [HP Sure Start](#).

“Isto faz parte de um esforço conjunto com os HP Labs para ajudar as empresas a gerir melhor o risco e a proteger o utilizador e produtividade de TI contra ataques maliciosos, uma atualização falhada ou outras causas acidentais ou desconhecidas.”

- afirmou Vali Ali, Diretor de Tecnologia para Segurança e Privacidade da HP PC Business Unit.

Como as defesas automáticas vão proteger os seus dispositivos

HP Sure Start é uma proteção de auto-recuperação ao nível da BIOS. Chamamos a esta abordagem ciber-resiliente. O sistema funciona criando um “gold master” da BIOS, que é diretamente codificado no dispositivo. Desta forma, se alguém tentar atacar a BIOS, automaticamente reinicia e carrega o “gold master”, limpa o ficheiro infetado e informa-o a si e à sua equipa sobre o ataque. Basicamente, a máquina regenera-se a ela própria.

Significando uma produtividade sem interrupções. Significa menos custos, e mais dispositivos em conformidade. Acima de tudo, uma forma mais fácil de trabalhar.

Se quer saber qual a forma mais fácil de ativar o HP Sure Start nos seus dispositivos para todos os seus utilizadores, considere o **HP Device as a Service**. É um modelo de consumo de PC moderno que simplifica a forma como as empresas equipam os seus colaboradores com o hardware e acessórios adequados, gerem as frotas de dispositivos com diversos SO's e obtêm serviços de vida útil adicional. O HP DaaS oferece planos simples e flexíveis, com um preço por dispositivo para manter o funcionamento simples e eficiente.

Os endpoints e pontos de acesso devem ser monitorizados a todos os níveis. Este é o momento de evitar as partes ocultas nos nossos dispositivos. Todas as pessoas, empresas e organizações em todo o mundo podem tornar-se mais seguras e resilientes com o portfólio da HP em termos de produtos, incluindo a série **HP EliteBook 800**, com processadores opcionais de 8ª geração Intel® Core™. Como parte da família HP Elite, este dispositivo oferece tecnologia de segurança graças às suas funcionalidades de segurança integradas, como o HP Sure Start.

Para saber mais sobre como proteger os dispositivos da sua empresa, [leia o mais recente Artigo HP Sure Start](#), e descubra as vantagens das [soluções de segurança HP](#) para a sua empresa.

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. Estão disponíveis diversas gerações de HP Sure Start em configurações selecionadas dos sistemas HP Elite e HP Pro.

© Copyright 2018 HP Development Company, L.P. As informações apresentadas estão sujeitas a alteração sem aviso prévio.

4AA7-3219PTE, Maio de 2018

