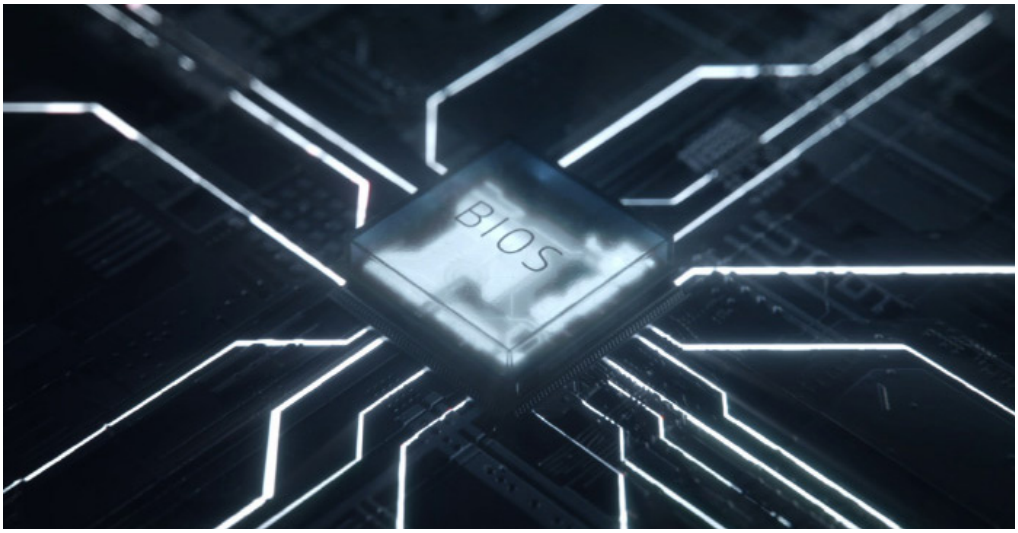
Comment améliorer la sécurité automatiquement et déjouer les plans des cybercriminels ?

En savoir plus



Comment combattre une menace qui déjoue votre protection ? Grâce à l'automatisation.

338 milliards de livres par an. C'est le coût actuel de la cybercriminalité à travers le monde[1]. Ce nombre s'accroît à mesure que les pirates perfectionnent leurs techniques et leurs compétences. L'une des dernières attaques sournoises qui est en passe de devenir le fléau des directeurs informatiques est l'attaque du BIOS.

Des millions d'ordinateurs présentent des vulnérabilités basiques au niveau du BIOS, ce qui signifie qu'ils peuvent être piratés par des personnes qui ont des compétences modestes. Il y a quelques années, les chercheurs Xeno Kovah et Corey Kallenberg ont présenté un nouveau type d'attaque lors d'une conférence, révélant ainsi qu'en quelques heures, ils pouvaient pirater à distance le BIOS de plusieurs systèmes et le contaminer[2]. Étant donné que la plupart des BIOS partagent le même code, une fois que le premier est piraté, ce n'est plus qu'une question de temps avant que les mêmes techniques ne finissent par déjouer les défenses des autres appareils.

Ce type d'attaque est extrêmement dangereux, car il vise un élément qui n'est pas protégé. Il existe un espace caché entre le système d'exploitation et le matériel informatique, qui a longtemps été ignoré. Bien que votre réseau semble étanche et que votre appareil soit protégé par les meilleurs systèmes de sécurité au monde, il existe tout de même un bref instant de vulnérabilité entre le démarrage et le lancement des protections. C'est à ce moment qu'une attaque hostile contre le BIOS peut faire des ravages.

Puisque la plupart des logiciels de sécurité informatique se trouvent au niveau du système d'exploitation, tout virus placé dans le BIOS ne pourra être détecté par le logiciel de sécurité du terminal. À partir de là, les pirates remplacent votre BIOS par leur propre version personnalisée, qui peut être gérée à distance, sans limite dans le temps. Pire encore, il est quasi impossible de détecter cette brèche et la contamination subséquente.

La meilleure façon de protéger les ordinateurs de votre entreprises est d'utiliser un système de sécurité à plusieurs volets. Les compétences de votre équipe informatique ne devraient pas se contenter des scans constants et des dépannages manuels. HP propose une réponse automatique, HP Sure Start, qui fait partie d'une gamme de solutions de sécurité.

« Ce produit est le fruit d'une collaboration avec HP Labs. Il permet aux entreprises de mieux gérer les risques et de protéger les utilisateurs ainsi que la productivité informatique contre les attaques malveillantes, les mises à jour échouées ou tout autre incident ou cause inconnue »

déclare Vali Ali, Chef de la technologie en matière de sécurité et de confidentialité au sein de l'unité commerciale PC de HP.

HP Sure Start est un moyen de protection auto-réparant au niveau du BIOS. Le système repose sur la création d'un « maître » du BIOS qui procède directement au chiffrement de l'appareil. Dès lors, si quelqu'un tente de pirater votre BIOS, votre système se réinitialisera avant de charger le « maître », qui détruira le fichier contaminé et vous

Comment les défenses automatiques vont sauver les appareils de votre entreprise

informera, vous et votre équipe, de l'attaque. En bref, la machine se répare toute seule.

Cela se traduit par une productivité ininterrompue, une réduction des coûts, des ordinateurs plus conformes, et surtout, par une façon plus simple de travailler.

Si vous vous demandez quelle est la façon la plus simple de vous procurer des ordinateurs de pointe qui intègrent la technologie HP Sure Start, pensez à HP Device as a Service. Il s'agit d'un service qui simplifie la façon dont les organisations commerciales fournissent à leur personnel le bon matériel et les bons accessoires, gèrent les divers appareils multi-OS et qui couvre toutes les étapes du cycle de vie des produits. HP DaaS propose des forfaits simples et flexibles, à un prix fixe par appareil, qui permettent à votre entreprise de fonctionner efficacement, sans accrocs.

Il est indispensable de surveiller les terminaux et les points d'accès à tous les niveaux. L'heure est venue de vous soucier des parties cachées de vos ordinateurs. Chaque personne, entreprise et organisation du monde entier gagne en sûreté et en polyvalence grâce à la gamme de produits HP, qui inclut les PC HP EliteBook 800, avec en option la 8e génération de processeurs Intel® Core™. En tant que produit de la gamme HP Elite, cet ordinateur met à votre disposition une solution de sécurité unique grâce à ses logiciels intégrés comme HP Sure Start.

Pour en savoir plus sur la façon dont vous pouvez protéger les ordinateurs de votre entreprise, lisez notre dernier Livre blanc HP Sure Start, et découvrez les avantages des solutions de sécurité HP.

Sources:

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. Générations d'HP Sure Start sont disponibles pour certaines configurations des systèmes HP Elite et HP Pro.

4AA7-3219FRFR, Mai 2018