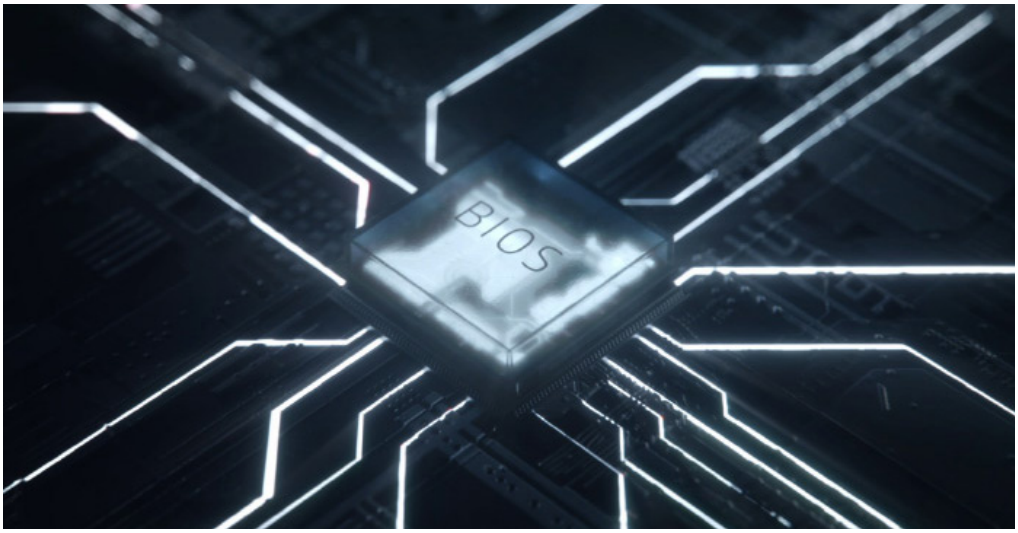
Comment les défenses automatiques vont sauver les appareils de votre entreprise

En savoir plus



Comment combattre une cybermenace cachée sous vos défenses? Grâce à l'automatisation.

338 milliards de livres par an. Voilà le coût actuel du cybercrime à travers le monde[1]. Et ce nombre continue à augmenter à mesure que les capacités des pirates deviennent plus habiles et perfectionnées. L'une des dernières attaques sournoises devenues le cauchemar des responsables informatique: l'attaque du BIOS.

Des millions de machines présentent des failles élémentaires dans leur BIOS. Or, cela signifie qu'elles peuvent être piratées par des personnes présentant des compétences, même modérées, en matière de piratage. Les chercheurs Xeno Kovah et Corey Kallenberg ont présenté un nouveau type d'attaque lors d'une conférence qui s'est tenue il y a plusieurs années de cela. Pour ce faire, ils ont montré qu'ils étaient en mesure de pirater à distance et d'infecter le BIOS de plusieurs systèmes en quelques heures[2]. Étant donné que la plupart des BIOS partagent un code commun, une fois le premier trouvé, ce n'était qu'une question de temps avant qu'il ne soit possible de renverser les défenses d'un nombre de machines bien plus conséquent.

Ce type d'attaque est dangereux car il cible des endroits qui ne sont pas protégés. Il existe un espace caché entre le système d'exploitation et le matériel, qui était jusqu'à présent ignoré. Et même si votre réseau paraît inattaquable et vos appareils protégés par les meilleurs systèmes de sécurité au monde, il reste toujours un bref moment de latence lors du démarrage et pendant le lancement de vos défenses. C'est à ce moment précis qu'une attaque agressive contre le BIOS peut causer des ravages.

Dans la mesure où la plupart des logiciels de cybersécurité se trouvent au niveau du système d'exploitation, les malwares injectés dans le BIOS (avant le démarrage et exécutés dans le mode de gestion de système) seront indétectables pour le logiciel de cybersécurité du point d'extrémité. De là, les pirates pourront remplacer votre BIOS par leur propre version personnalisée, contrôlable à distance aussi longtemps qu'ils le souhaitent. Pire encore, il peut s'avérer presque impossible de détecter la faille et l'infection.

Le meilleur moyen pour protéger les appareils de votre entreprise consiste à utiliser une sécurité sur plusieurs couches. Les capacités de votre équipe informatique ne doivent pas se résumer à un scan permanent et des correctifs manuels. HP propose une réponse automatique, HP Sure Start, dans le cadre de sa gamme de solutions de sécurité.

«Il s'agit d'un effort conjoint avec HP Labs en vue d'aider les entreprises à mieux gérer les risques et à protéger les utilisateurs et la productivité contre les attaques malveillantes, l'échec d'une mise à jour ou toute autre cause fortuite ou inconnue»

-Vali Ali, expert en technologie pour la sécurité et la confidentialité dans l'unité HP PC.

HP Sure Start offre une protection dans laquelle le BIOS est auto-réparant. Nous appelons cette approche la cyber-résilience. Le système fonctionne en créant un «original de référence» du BIOS, directement chiffré sur l'appareil. Ainsi, si une personne tente de pirater le BIOS, celui-

Comment les défenses automatiques vont sauver les appareils de votre entreprise

ci redémarre de lui-même et charge ensuite l'«original de référence», nettoie le fichier infecté et vous informe, ainsi que votre équipe, de l'attaque. La machine se répare de façon autonome.

Vous bénéficiez ainsi d'une productivité ininterrompue, avec des coûts inférieurs et des appareils plus conformes. Mais il s'agit surtout d'une manière plus simple de travailler.

Si vous vous demandez quel serait le moyen le plus simple pour proposer à vos utilisateurs des appareils à la pointe de la technologie équipés de HP Sure Start, pensez à HP Device as a Service. Ce modèle de consommation moderne simplifie la manière dont les organisations commerciales équipent leurs employés avec le matériel et les accessoires adéquats, gèrent des flottes d'appareils aux systèmes d'exploitation variés et obtiennent des services supplémentaires en termes de cycle de vie. HP DaaS propose des programmes simples et flexibles, avec un tarif par appareil, pour garantir un fonctionnement harmonieux et efficace.

Les points d'extrémité et d'accès doivent être surveillés à tous les niveaux. Il est temps d'arrêter de négliger les parties cachées de nos appareils. Chaque personne, entreprise et organisation dans le monde entier peut améliorer sa sécurité et sa résilience avec la gamme de produits HP, comprenant le HP EliteBook série 800. Cet appareil, qui fait partie de la famille HP Elite, offre une technologie sûre grâce à ses fonctionnalités intégrées telles que 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. Différentes générations de HP Sure Start sont disponibles sur les configurations sélectionnées des systèmes HP Elite et HP Pro.

4AA7-3219FRCH, Mai 2018