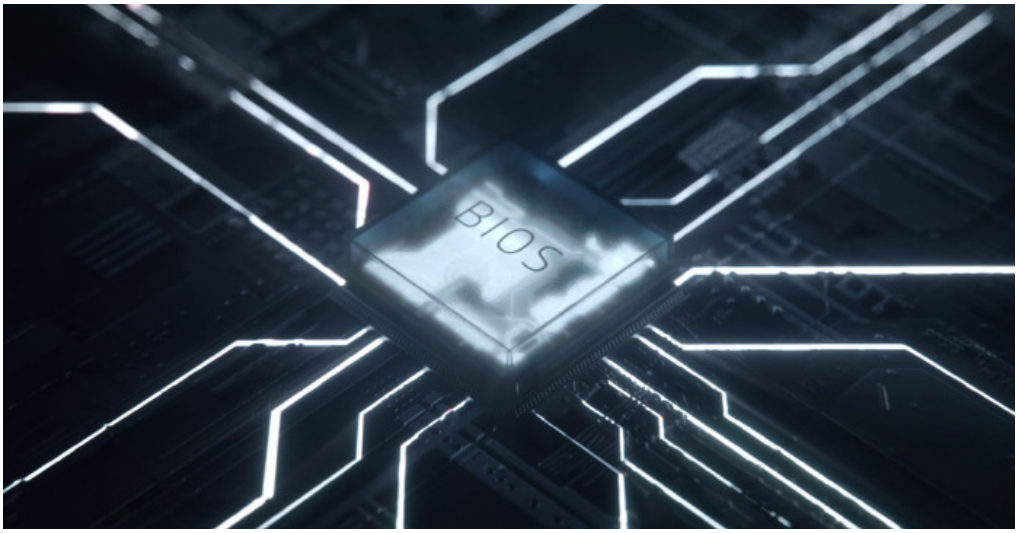
# Warum automatische Abwehrsysteme Ihre Firmengeräte schützent

Mehr erfahren




**Wie aber gehen Sie gegen eine Sicherheitsbedrohung im Deckmantel Ihrer Abwehrmassnahmen vor? Durch Automatisierung.**

338 Mrd. GBP pro Jahr. Das sind die aktuellen durch Cyberkriminalität verursachten Kosten weltweit[1]. Diese Zahl steigt, da Hacker immer scharfsinniger und kompetenter werden. Einer der aktuellsten Angriffe durch Hintertüren, die das Leben von IT-Fachkräften schwer machen, ist der BIOS-Angriff.

Millionen von Rechnern haben grundlegende BIOS-Schwachstellen, d. h., dass sie von jemanden mit lediglich mittelmässigen Hackerfähigkeiten gehackt werden können. Die Branchenexperten Xeno Kovah und Corey Kallenberg stellten vor ein paar Jahren auf einer Konferenz eine neue Art von Angriffen vor, wobei sie enthüllten, dass sie innerhalb von ein paar Stunden das BIOS von vielfältigen Systemen ferngesteuert hacken und infizieren können[2]. Da die meisten BIOS sich denselben Code teilen, war es nur eine Frage der Zeit, bis dieselben Hackerfähigkeiten die Abwehrmassnahmen von vielen weiteren Rechnern zu Fall bringen konnten, sobald der erste geknackt war.

Diese Art von Angriffen ist deshalb so gefährlich, weil sie einen Ort bedrohen, der nicht geschützt ist. Zwischen dem Betriebssystem und der Hardware befindet sich ein verborgener Raum, der bisher ignoriert wurde. Und obwohl Ihr Netzwerk hieb- und stichfest zu sein scheint und Ihr Gerät durch die besten Sicherheitssysteme der Welt geschützt ist, gibt es dennoch einen kurzen Moment, während dem Ihr Rechner hochfährt und sich Ihre Sicherheitsvorkehrungen positionieren. Und genau zu diesem Zeitpunkt kann ein feindlicher BIOS-Angriff verheerenden Schaden anrichten.

Da die Cyber-Sicherheitssoftware meistens auf der Ebene des Betriebssystems angesiedelt ist, bleibt die in das BIOS eingeschleuste Malware (vor dem Hochfahren und der Einbettung im System Management Mode) für die Cyber-Sicherheitssoftware am Endpunkt unentdeckt. Von hier aus ersetzen Hacker Ihr BIOS mit ihrer selbst gebastelten Version, die von einem entfernten Ort und auf unbestimmte Zeit verwaltet werden kann. Das Schlimme ist, dass es beinahe unmöglich ist zu erkennen, dass ein Angriff und eine Infizierung stattgefunden haben.

Die beste Möglichkeit, Ihre Firmengeräte zu schützen, ist die Verwendung eines mehrstufigen Sicherheitssystems. Die Fähigkeiten Ihres IT-Teams sollten nicht durch ständige Überwachung und manuelle Behebungen überstrapaziert werden. HP bietet unter anderem eine Reihe von Sicherheitslösungen mit automatischer Reaktion an: HP Sure Start.

«Dies ist das Ergebnis aus der Zusammenarbeit mit HP Labs, um Unternehmen das Risikomanagement zu erleichtern sowie die Produktivität von Nutzern und IT-Fachkräften vor bösartigen Angriffen, einem fehlgeschlagenen Update oder anderen versehentlichen oder unbekannten Ursachen zu schützen»,

**so Vali Ali, Cheftechnologe für Sicherheit und Datenschutz bei der Geschäftseinheit HP PC.**

## Warum automatische Abwehrsysteme Ihre Firmengeräte schützen

Bei HP Sure Start handelt es sich um einen selbstheilenden Schutz auf BIOS-Ebene. Diese Herangehensweise nennen wir Cyber-Robustheit. Das System funktioniert über die «Goldmaster»-Konfiguration des BIOS, die direkt am Gerät verschlüsselt wird. Wenn also jemand das BIOS hacken will, fährt es automatisch neu hoch und lädt anschliessend die «Goldmaster»-Konfiguration, löscht die infizierte Datei und informiert Sie und Ihr Team über den Angriff. Im Wesentlichen heilt sich der Rechner selbst.

Dies bedeutet eine unterbrechungsfreie Produktivität. Es bedeutet niedrigere Kosten. Es bedeutet nachgiebigere Geräte. Vor allem erleichtert es die Arbeit.

Wenn Sie für Ihre Nutzer ein zukunftsweisendes Gerät mit aktiviertem HP Sure Start in Erwägung ziehen, dann ist HP Device as a Service (DaaS) das Richtige für Sie. Hier handelt es sich um ein modernes PC-Verbrauchsmodell, das es Unternehmen erleichtert, ihre Mitarbeiter mit der richtigen Hardware und dem richtigen Zubehör auszustatten, mehrere OS-Geräte zu verwalten und zusätzlich einen Lebenszyklusservice zu bieten. HP DaaS überzeugt mit einfachen, dennoch flexiblen Plänen mit einem festen Preis pro Gerät, sodass ein reibungsloser und effizienter Betrieb garantiert ist.

End- und Zugangspunkte müssen auf jeder Ebene überwacht werden. Es ist an der Zeit, die unsichtbaren Bereiche unserer Geräte nicht länger zu ignorieren. Jede Person, jedes Unternehmen und jeder Konzern weltweit kann mit dem HP-Produktportfolio, darunter das HP EliteBook der 800er Serie, sein System sicherer und widerstandfähiger machen. Dieses Gerät aus der HP Elite-Gerätereihe garantiert durch die eingebauten Sicherheitsfunktionen wie HP Sure Start eine zuverlässige Sicherheitstechnologie.

**Mehr Informationen zum Schutz Ihrer Firmengeräte finden Sie in unseren aktuellen HP Sure Start Produktinformationen. Entdecken Sie, welche Vorteile HP Sicherheitslösungen für Ihr Unternehmen haben.**

---

**Quellen:**


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/


Drei verschiedene Generationen von HP Sure Start sind für ausgewählte Konfigurationen von HP Elite- und HP Pro-Systeme erhältlich.



4AA7-3219DECH, Mai 2018