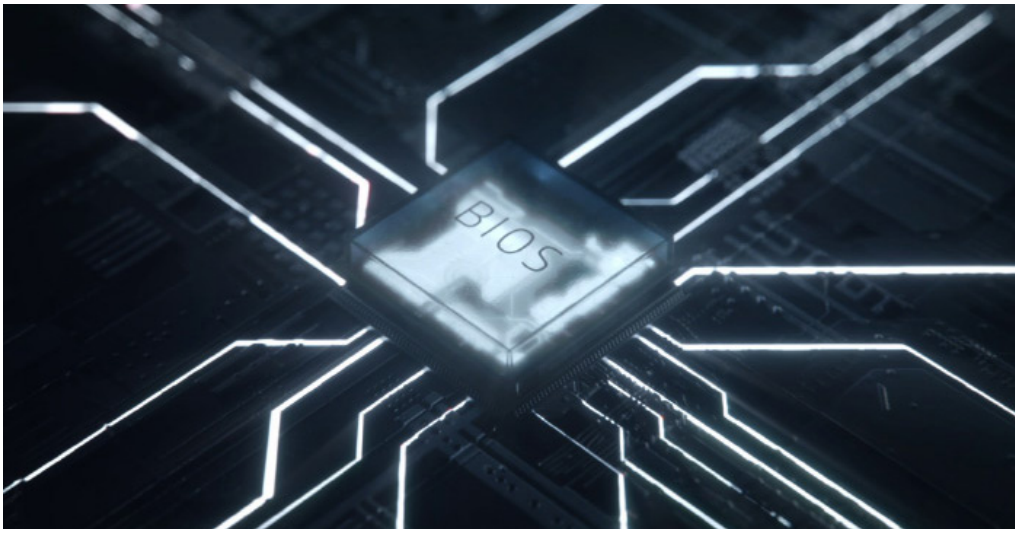
Dlaczego zabezpieczenia automatyczne ochronią urządzenia w Twojej firmie

Napisane przez Luizę Dzienkiewicz-Kobus

Dowiedz się więcej



Jak walczysz z zagrożeniami ukrywającymi się pod Twoimi zabezpieczeniami? Dzięki automatyzacji.

£338 mld GBP rocznie. To aktualny koszt cyberprzestępstw, do których dochodzi na świecie[1]. Kwota ta cały czas rośnie, ponieważ hakerzy stosują coraz to nowsze i bardziej skomplikowane metody. Jednym z najnowszych i potajemnych ataków, które stają się zmorą menedżerów IT, są ataki na BIOS.

Miliony urządzeń posiadają podstawowe luki w BIOS-ie, przez które urządzenia te mogą paść ofiarą hakerów o nawet przeciętnych umiejętnościach. Podczas konferencji, która odbyła się kilka lat temu, badacze Xeno Kovah i Corey Kallenberg przedstawili nowy rodzaj ataku, ujawniając, że w ciągu kilku godzin byliby w stanie włamać się zdalnie i zainfekować BIOS w wielu systemach[2]. Ponieważ w przypadku większości wersji BIOS-u stosowany jest ten sam kod, po złamaniu go po raz pierwszy pokonanie zabezpieczeń tak wielu kolejnych urządzeń było tylko kwestią czasu.

Ten rodzaj ataku jest tak niebezpieczny, ponieważ jego celem jest miejsce, które nie było chronione. Pomiędzy systemem operacyjnym a sprzętem jest ukryte miejsce, które było ignorowane. Mimo że Twoja sieć może wydawać się szczelna, a Twoje urządzenie jest chronione przez najlepsze na świecie systemy zabezpieczające, podczas uruchamiania systemu występuje krótka chwila, w trakcie której Twoje zabezpieczenia mogą zostać pokonane. Właśnie w tym momencie wrogi atak na BIOS może dokonać spustoszenia.

Ponieważ większość oprogramowania do zapewniania bezpieczeństwa w cyberprzestrzeni działa na poziomie systemu operacyjnego, zainfekowanie BIOS-u złośliwym oprogramowaniem (przed uruchomieniem systemu i przejściem do trybu zarządzania systemem) nie zostanie wykryte przez to końcowe oprogramowanie. Pozwoli to hakerom na zastąpienie BIOS-u własną, niestandardową wersją, którą będą oni mogli zarządzać zdalnie i w nieskończoność. A co najgorsze, wykrycie, że doszło do infekcji i naruszenia bezpieczeństwa będzie prawie niemożliwe.

Najlepszym sposobem na zabezpieczenie urządzeń swojej firmy jest korzystanie z ochrony wielowarstwowej. Zespół IT nie może poświęcać całego czasu na ciągłe skanowanie urządzeń i ręczne naprawianie błędów. Firma HP zapewnia automatyczną odpowiedź – w ramach gamy naszych rozwiązań zabezpieczających – HP Sure Start.

„W ramach współpracy z laboratoriami firmy HP pomagamy firmom w lepszym zarządzaniu ryzykiem i ochronie wydajności użytkowników i działów IT przed złośliwym oprogramowaniem, nieudanymi aktualizacjami i wszelkimi innymi przypadkowymi lub nieznanymi przyczynami problemów."

- Vali Ali, Główny Technolog ds. Bezpieczeństwa i Prywatności w jednostce biznesowej firmy HP zajmującej się komputerami.

Dlaczego zabezpieczenia automatyczne ochronią urządzenia w Twojej firmie

HP Sure Start to samouzdrawiające się zabezpieczenie, które działa na poziomie BIOS-u. Nazywamy ten sposób podejścia cyberodpornością. Praca systemu polega na tworzeniu „złotej wersji próbnej" BIOS-u, która jest szyfrowana bezpośrednio na urządzeniu. Więc gdy ktoś spróbuje włamać się do BIOS-u, nastąpi jego automatyczne, ponowne uruchomienie, a następnie wczytana zostanie „złota wersja główna", a zainfekowany plik zostanie usunięty, dzięki czemu Ty i Twój zespół dowiecie się o ataku. Urządzenie zasadniczo samo się uzdrawia.

Przekłada się to na niezachwianą produktywność. Oznacza to niższe koszty. Oznacza to więcej zgodnych urządzeń. Przede wszystkim upraszcza to pracę.

Jeżeli zastanawiasz się, jak najłatwiej możesz wyposażyć swoich użytkowników w najnowocześniejsze urządzenia z rozwiązaniem HP Sure Start, rozważ możliwość wykorzystania HP Device as a Service. Jest to nowoczesny model korzystania z komputerów, który upraszcza sposób, w jaki organizacje komercyjne wyposażają swoich pracowników w odpowiedni sprzęt i akcesoria, zarządzają flotami urządzeń z różnymi systemami operacyjnymi i korzystają z dodatkowych usług w ramach cyklu życia tych urządzeń. W ramach HP DaaS dostępne są proste, a zarazem elastyczne plany obejmujące jedną cenę dla każdego urządzenia, dzięki czemu wszystko będzie działać płynnie oraz wydajnie.

Punkty końcowe i punkty dostępu wymagają monitorowania na każdym poziomie. Nadszedł czas, aby przestać pomijać ukryte części naszych urządzeń. Każda osoba, firma i organizacja na świecie może zwiększyć swoje bezpieczeństwo i stać się bardziej odporna dzięki portfolio produktów firmy HP, w tym komputerom HP EliteBook 800 Series z opcjonalnym procesorem Intel® Core™ 8. generacji. Urządzenie to należy do rodziny HP Elite i posiada technologię zabezpieczającą dzięki wbudowanym funkcjom ochrony, takim jak HP Sure Start.

Aby dowiedzieć się więcej na temat tego, jak chronić urządzenia w swojej firmie, przeczytaj nasze najnowsze opracowanie dotyczące rozwiązania HP Sure Start i odkryj korzyści, jakie rozwiązania zabezpieczające firmy HP mogą zapewnić Twojej firmie.

Źródła:

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/

Dla wybranych konfiguracji systemów HP Elite i HP Pro dostępne są 3 różne generacje rozwiązania HP Sure Start.

4AA7-3219PLE, Może 2018 r.