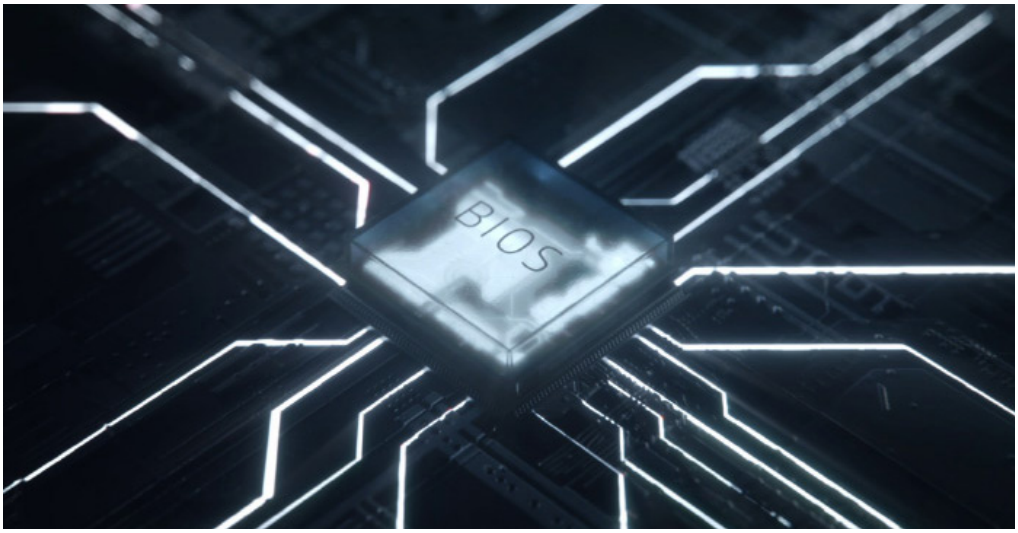
Proč automatická ochrana šetří vaše firemní zařízení

Ziskat další informace



Jak bojujete proti kybernetické hrozbě, která se před vaší ochranou skrývá? Automatizujte.

9 710 miliard Kč ročně. To jsou současné celosvětové náklady na počítačovou kriminalitu[1]. Toto číslo stále roste, protože hackeři se stávají rafinovanějšími a schopnějšími. Jedním z nejnovějších plíživých útoků, které se stávají prokletím IT manažerů, je útok na BIOS.

Miliony počítačů jsou zranitelné v systému BIOS, což znamená, že mohou být napadeny i někým, kdo má dokonce jen slabé hackerské dovednosti. Před několika lety představili výzkumníci Xeno Kovah a Corey Kallenberg na konferenci nový typ útoku a ukázali, že by mohli během několika hodin vzdáleně hackovat a infikovat BIOS mnoha systémů[2]. Většina systémů BIOS sdílí stejný kód. Proto jakmile byl prolomen první, bylo jen otázkou času, než byla stejným postupem překonána ochrana mnoha dalších počítačů.

Tento typ útoku je tak nebezpečný proto, že se zaměřuje na něco, co dosud nebylo chráněno. Mezi operačním systémem a hardwarem je skrytý prostor, který byl dříve ignorován. A zatímco se vaše síť může zdát vodotěsná a vaše zařízení je chráněno nejlepšími bezpečnostními systémy na světě, při startu systému stále ještě existuje krátký okamžik, než se spustí ochranná opatření. V této chvíli může nepřátelský útok na BIOS způsobit zmatek.

Protože se většina počítačového bezpečnostního softwaru nachází na úrovni operačního systému, malware, který je vložen do systému BIOS (před spuštěním systému a předán do režimu správy systému), nebude pro počítačový bezpečnostní software, určený ke sledování koncových bodů, detekovatelný. Zde hackeři nahradí váš BIOS vlastní verzí, která může být vzdáleně a neomezeně spravována. Nejhorší je, že je téměř nemožné zjistit, že k prolomení a infekci došlo.

Nejlepší způsob, jak chránit firemní zařízení, je použít vícevrstvé zabezpečení. Možnosti vašeho IT týmu by neměly být omezeny na neustálé skenování a ruční opravy. Společnost HP poskytuje automatickou reakci – jako součást řady bezpečnostních řešení – HP Sure Start.

„Jedná se o součást společného úsilí s HP Labs pomáhat podnikům lépe řídit rizika a chránit produktivitu uživatelů a IT před nebezpečnými útoky, neúspěšnou aktualizací nebo jakoukoli jinou náhodnou nebo neznámou záležitostí.“

– Vali Ali, vedoucí technologie pro zabezpečení a ochranu soukromí v obchodní jednotce HP PC.

Proč automatická ochrana šetří vaše firemní zařízení

HP Sure Start je samoregenerační ochrana na úrovni systému BIOS. Tomuto přístupu říkáme kybernetická odolnost. Systém funguje tak, že vytvoří „zlatou kopii“ systému BIOS, která je zakódována přímo v zařízení. Pokud se tedy někdo pokusí BIOS narušit, automaticky se sám restartuje, načte „zlatou kopii“, infikovaný soubor vymaže a vás a váš tým informuje o útoku. Počítač se vlastně sám vyléčí.

Což znamená nepřerušovanou produktivitu. To znamená nižší náklady. To znamená lépe sloužící zařízení. Především to usnadňuje práci.

Pokud přemýšlíte, jak co nejsnadněji dostat špičková zařízení s aktivovaným systémem HP Sure Start ke svým uživatelům, zvažte řešení HP Device as a Service. Jedná se o moderní model zavádění počítačů, který zjednodušuje způsob, jakým komerční organizace vybavují své zaměstnance správným hardwarem a příslušenstvím, řídí flotily zařízení s více operačními systémy a po dobu životního cyklu dostávají další služby. HP DaaS nabízí jednoduché ale flexibilní plány s jednotnou cenou za zařízení, aby vše fungovalo hladce a efektivně.

Koncové body a přístupové body je třeba monitorovat na všech úrovních. Je čas přestat se vyhýbat skrytým součástem našich zařízení. Každá osoba, firma nebo organizace po celém světě se může stát bezpečnější a odolnější díky portfoliu nabídek produktů společnosti HP, zahrnujících řadu HP EliteBook 800 s volitelnými procesory Intel® Core™ 8. generace. Jako součást rodiny HP Elite nabízí toto zařízení bezpečnostní technologie díky vestavěným bezpečnostním funkcím, jako je HP Sure Start.

Chcete-li o ochraně firemních zařízení získat další informace, přečtěte si nejnovější dokument HP Sure Start White Paper, kde objevíte výhody řešení zabezpečení od společnosti HP pro svoji firmu.

Poznámky:

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/

U vybraných konfigurací systémů HP Elite a HP Pro jsou k dispozici 3 různé generace softwaru HP Sure Start.

4AA7-3219CSCI, Smět 2018