Případová studie

Swiss Conference Center AV hack bylo možné odvrátit použitím bezpečnostních funkcí počítačů HP

Oficiální závěr k neoprávněnému přístupu k datům

Odvětví
Místa konání

Cíl
Auditování zabezpečení s cílem lépe ochránit konferenční střediska a citlivá data klientů

Přístup
Spolupráce s poradcem pro zabezpečení s cílem analyzovat bezpečnostní postupy a určit oblasti vyžadující zlepšení

IT záležitosti
- Přechod na používání počítačů HP Elite s integrovanou ochranou proti malwaru
- Zamykání nepoužívaných otevřených portů jako prevence před neoprávněným přístupem
- Doplněk HP Manageability Integration Kit integrovaný v nástroji Microsoft® System Center Configuration Manager (SCCM), který umožňuje vzdáleně spravovat firemní počítače

Obchodní záležitosti
Aktualizovaná opatření chránící pracoviště před sofistikovanými kybernetickými útoky a důvěru klientů ve váš podnik

Přehled

Středisko Swiss Conference Center* v blízkosti Ženevy ve Švýcarsku pořádá každoročně více než 230 událostí. Toto Evropské středisko je oblíbeným místem pro konání firemních konferencí a představení produktů těch nejvýznamnějších světových firem.

Vedení střediska investovalo velké částky do technologické infrastruktury, aby tak mohlo nabídnout svým klientům prostředí pro vedení na míru přizpůsobených konferencí v krásném prostředí. Zabezpečení počítačů ve středisku však bohužel nebylo v této investici zahrnuto.

23. dubna 2018 se podařilo hackerovi známému pouze pod přezdívkou „The Wolf“ (Vlk) získat přístup do počítače v konferenčním středisku a přerušit významnou prezentaci, které se účastnily důležité osoby z celého světa. Po tomto útoku se Swiss Conference Center obrátilo na svého bezpečnostního poradce ve snaze najít a odstranit slabá místa v kybernetickém zabezpečení.

Co se stalo

Swiss Conference Center je vyhlášeným světovým střediskem, které je známo zajišťováním úžasného prostředí pro své hosty. Jejich ochrana před kybernetickými útoky je však již o něco méně úžasná. Vlkovi se podařilo odeslat malware do jednoho z počítačů střediska, který mu umožnil nahradit prezentaci řečníka svou vlastní. Zatímco v konferenčním sále panoval chaos, pracovníkům IT se jen velmi pomalu dařilo získat zpět kontrolu nad svojí sítí.

Škody se neomezily jen na jednu zmařenou prezentaci. Ušlý zisk ze zrušených rezervací je odhadován přibližně na 3,2 milionu eur.

Jak se to stalo?

Jediné, co Vlk musel udělat, bylo proniknout do jednoho nechráněného počítače tím, že přiměl zaměstnance kliknout na nebezpečný odkaz v e-mailu nebo stáhnout neškodně se tvářící přílohu. Stejně tak pokud se mu podařilo dostat se do blízkosti počítače, stačilo mu vložit jednotku flash do nechráněného portu USB.

Počítačům střediska Swiss Conference Center scházela potřebná ochrana, která by dokázala malware uložit do karantény a zastavila tak útok ještě v jeho začátku. I když v rámci celého střediska *byly* nainstalovány antivirové programy, žádný z počítačů nenabízel integrované funkce pro ochranu hardwaru.

Posílení zabezpečení

Společně s bezpečnostním poradcem provedlo středisko Swiss Conference Center důkladný audit stávajících zabezpečení před kybernetickým útokem. Výsledkem bylo nahrazení všech počítačů za počítače HP Elite s integrovanou ochranou proti malwaru a firmwarem HP Sure Start Gen4, který dokáže automaticky detekovat a zastavit útok na systém BIOS nebo škodlivý kód aktivní při spuštění nebo inicializaci počítače a počítač z tohoto útoku automaticky obnovit.[1]

Nové počítače HP Elite současně nabízí funkci HP Sure Click, která zajišťuje ochranu hardwaru fyzickým izolováním jednotlivých záložek prohlížeče nebo stažených souborů PDF / dokumentů Microsoft Office do prostředí mikroVM a dokáže tak zabránit šíření webového malwaru či škodlivých e-mailových příloh do ostatních zařízení připojených v síti.[2]

Tým IT nyní používá nástroj HP Device Access Manager, s jehož pomocí může spravovat porty a vyjímatelná média, stejně jako doplněk HP Manageability Integration Kit pro nástroj Microsoft SCCM, se kterým má možnost zjednodušit zabezpečení a správu systému BIOS ve všech firemních počítačích.[3]

Závěr

Středisko Swiss Conference Center utrpělo ušlý zisk a pokles důvěryhodnosti mezi důležitými klienty. Díky nasazení počítačů HP s ucelenými bezpečnostními funkcemi a použitím kvalitních řešení pro správu je vidět, že středisko je na další případný kybernetický útok důkladně připraveno.

**Swiss Conference Center je fiktivní společností, která se stala cílem kybernetického útoku v krátkém filmu společnosti HP Studio: „THE WOLF: TRUE ALPHA".*

Další informace o řešení HP:
Zabezpečení PC: hp.com/go/computersecurity
Zabezpečení tisku: hp.com/go/reinventsecurity

Film „The Wolf" můžete vidět zde:
hp.com/thewolf

[1]HP Sure Start Gen4 je k dispozici pro zařízení HP Elite a HP Pro 600 s procesory Intel® nebo AMD 8. generace.
[2] HP Sure Click je k dispozici na většině počítačů HP a podporuje prohlížeče Microsoft® Internet Explorer a Chromium™. Mezi podporované přílohy patří Microsoft Office (Word, Excel, PowerPoint) a soubory PDF v režimu jen pro čtení, pokud je nainstalována sada Microsoft Office nebo Adobe Acrobat.
[3] Doplněk HP Manageability Integration Kit není předem nainstalován a je k dispozici na adrese hp.com/go/clientmanagement.

Přihlásit se k odběru novinek
hp.com/go/getupdated

Sdílet dokument s kolegy

4AA7-3561CSE, měsíc 2014