Fallstudie

Sabotaget av en presentation på Swiss Conference Center kunde ha förhindrats med säkerhetsfunktionerna hos HP-datorer

Officiell sammanfattningsrapport över dataintrånget

Bransch
Evenemangsplatser

Målsättning
Granska säkerhetsrutinerna för att bättre skydda konferenscentret och känsliga klientdata.

Metod
Arbetade med säkerhetskonsulter för att analysera säkerhetsrutiner och identifiera problematiska områden.

IT-frågor
- Uppgraderade sin datorpark till HP Elite-datorer med inbyggt skydd mot malware.
- Stängde portar som inte används för att förhindra obehörig användning.
- Integrerade insticksprogrammet HP Manageability Integration Kit i Microsoft® System Center Configuration Manager (SCCM) för att managera datorparken på distans.

Verksamhetsfrågor
Uppdaterade cybersäkerhetsåtgärder för att bättre skydda anläggningar mot avancerade attacker, samt för att återfå klienternas förtroende.

Översikt

Konferenscentret Swiss Conference Center* nära Genève i Schweiz är värdplats för fler än 230 evenemang varje år. För många är Swiss Conference Center förstahandsvalet i Europa när det gäller affärskonferenser eller evenemang för stora produktlanseringar, och centret tar emot branschledare från hela världen.

Anläggningens ledning har gjort stora investeringar i den tekniska infrastrukturen för att kunna erbjuda sina klienter en högst anpassningsbar konferensupplevelse i den vackra miljön. Olyckligtvis gjorde de inte motsvarande säkerhetsuppgraderingar i sin datorpark.

Den 23 april 2018 infiltrerades en dator på konferenscentret av en hackare som kallar sig "The Wolf". Hackaren störde sedan en stor presentation inför en internationell publik. Efter det dataintrånget vände sig Swiss Conference Center till sina säkerhetskonsulter för att hitta och åtgärda sårbarheter i sin cybersäkerhet.

Vad hände?

Swiss Conference Center är en av världens främsta konferensplatser för företag, och de har varit mycket bra på att skapa fantastiska gästupplevelser. Tyvärr var deras cybersäkerhet inte lika imponerande. The Wolf laddade upp malware i ett av centrets datorer, och bytte sedan ut en talares presentation mot sin egen presentation. Anläggningens IT-säkerhetspersonal kämpade för att återfå kontrollen över sitt nätverk medan kaos utbröt i föreläsningssalen.

Den saboterade presentationen var inte den enda skada som uppstod. Centret har hittills förlorat uppskattningsvis 3,2 miljoner euro i avbeställda bokningar.

Hur gick det till?

Allt The Wolf behövde göra var att koppla upp sig mot en oskyddad dator genom att lura en medarbetare att klicka på en skadlig länk eller ladda ned en skenbart ofarlig bilaga. Eftersom The Wolf befann sig fysiskt nära datorn kan hackaren även ha satt i ett USB-minne i en obevakad USB-port.

Swiss Conference Centers datorpark saknade viktigt skydd som kunde ha satt den malware-koden i karantän och stoppat infiltrationsförsöket. Man hade installerat antivirusprogram, men ingen av datorerna hade inbyggda säkerhetsfunktioner med stöd från hårdvaran.

Stärka säkerheten

I samarbete med sina säkerhetskonsulter utförde Swiss Conference Center en noggrann granskning av sina befintliga cybersäkerhetsåtgärder. Granskningen ledde till att hela datorparken uppgraderades till HP Elite-datorer med inbyggt skydd mot malware, inklusive skyddsfunktionen HP Sure Start Gen4, som automatiskt kan upptäcka, stoppa och återställa från BIOS-attacker eller skador vid uppstart och under körtid.[1]

De nya HP Elite-datorerna är även utrustade med HP Sure Click, som ger starkare skydd genom att fysiskt isolera varje webbläsarfönster eller hämtat PDF- eller Microsoft Office-dokument i en virtuell mikromaskin (VM), för att hindra att malware från webbplatser eller e-postbilagor sprids till andra enheter som är anslutna i nätverket.[2]

IT-teamet använder nu programvaran HP Device Access Manager för att hantera portar och flyttbara medier, och HP Manageability Integration Kit för Microsoft SCCM för att effektivisera hanteringen av säkerheten och BIOS i hela enhetsparken.[3]

Sammanfattning

Swiss Conference Center drabbades av minskade intäkter och minskat förtroende för sitt varumärke från sina högprofilerade klienter. Men genom att driftsätta HP-datorer med omfattande säkerhetsfunktioner och effektiva manageringslösningar kan centret nu uppvisa ett starkare engagemang i cybersäkerhet.

** Swiss Conference Center är en fiktiv organisation som utsätts för en cyberattack i HP Studios film "THE WOLF: TRUE ALPHA."*

Mer information om HPs lösningar finns på:
Datorsäkerhet: hp.com/go/computersecurity
Skrivarsäkerhet: hp.com/go/reinventsecurity

Du kan se filmerna om "The Wolf" genom att besöka: hp.com/thewolf

[1] HP Sure Start Gen4 är tillgängligt på HP Elite- och HP Pro 600-produkter som är utrustade med 8:e generationens Intel®- eller AMD-processorer.
[2] HP Sure Click är tillgängligt på de flesta HP-datorer och stödjer Microsoft® Internet Explorer och Chromium™. Bilagor som stöds är Microsoft Office (Word, Excel, PowerPoint) och PDF-filer i skrivskyddat läge, när Microsoft Office eller Adobe Acrobat är installerat.
[3] HP Manageability Integration Kit är inte förinstallerat. Det finns tillgängligt på hp.com/go/clientmanagement.

Registrera dig för att få uppdateringar
hp.com/go/getupdated

Dela med kollegor

4AA7-3561SVE, månad 2014