Casestudie

AV-hacking af Swiss Conference Center kunne have været undgået med HP's pc-sikkerhedsfunktioner

Officiel sammendragsrapport om databruddet

Industri
Konferencecentre

Mål
Gennemgang af sikkerhedspraksisser til forbedret beskyttelse af konferencecenteret og følsomme kundeoplysninger

Fremgangsmåde
Samarbejdede med deres sikkerhedsrådgiver om analyse af sikkerhedspraksisser og identificering af mulige problemområder

IT-anliggender
- Opgradering af flåde til HP Elite-pc'er med indbygget malwarebeskyttelse
- Lukning af unødvendige porte til forebyggelse af uautoriseret brug
- Integrering af HP Manageability Integration Kit-plug-in i Microsoft® System Center Configuration Manager (SCCM) til fjernstyring af pc-flåden

Virksomhedsanliggender
Opdatering af cybersikkerhed til forbedret beskyttelse af faciliteter imod avancerede angreb og genoprettelse af kundetillid

Oversigt

Swiss Conference Center* i nærheden af Genève i Schweiz afholder mere end 230 begivenheder årligt. Som det europæiske mødested for erhvervskonferencer og større produktlanceringsbegivenheder imødekommer centeret brancheledere fra hele verden.

Facilitetsledelsen har investeret kraftigt i teknologisk infrastruktur, så kunder kan tilbydes en højt tilpasset konferenceoplevelse i flotte og veludstyrede omgivelser. Desværre blev lignende sikkerhedsopgraderinger ikke foretaget for pc-flåden.

D. 23. april 2018 infiltrerede en hacker under navnet "The Wolf" en pc i konferencecenteret for at afbryde en højt profileret persons præsentation til et internationalt publikum. Efter bruddet henvendte Swiss Conference Center sig til deres sikkerhedsrådgiver for at identificere og reparere sårbarheder i forbindelse med cybersikkerhed.

Hvad skete der?

Som et af verdens førende steder for afholdelse af erhvervsbegivenheder udmærkede Swiss Conference Center sig i at skabe utrolige oplevelser for deres gæster – men deres cybersikkerhed var knap så imponerende. The Wolf uploadede malware til én af centerets pc'er og erstattede derefter en talers præsentation med sin egen. Centerets it-sikkerhedspersonale kæmpede med at genvinde kontrollen over deres netværk midt i kaosset.

Resultatet var ikke blot en ødelagt præsentation. Tabte indtægter fra annullerede reservationer er på nuværende tidspunkt estimeret til at være 3,2 mio. EUR.

Hvordan skete det?

Alt, hvad The Wolf behøvede at gøre, var at udnytte en ubeskyttet pc ved at få en ansat til at klikke på et dårligt link i en e-mail eller downloade en uskyldigt udseende vedhæftet fil. Eller da han var fysisk tilstede nær pc'en, kunne han have indsat en usb-nøgle i en usb-port uden opsyn.

Swiss Conference Centers pc-flåde manglede vitale beskyttelsesfunktioner, der ville have sat malwaren i karantæne og stoppet indtrængningsforsøget. Selvom de *havde* installeret antivirussoftware, havde ingen af deres pc'er indbygget hardwareforstærkede sikkerhedsfunktioner.

Forbedring af sikkerheden

Swiss Conference Center udførte i samarbejde med deres sikkerhedsrådgiver en omfattende analyse af deres eksisterende cybersikkerhedsforanstaltninger. Den analyse førte til en opgradering af hele deres flåde til HP Elite-pc'er med indbygget malwarebeskyttelse, inklusive HP Sure Start Gen4, der automatisk registrerer, stopper og repareres fra et BIOS-angreb eller beskadigelse ved opstart og under run-time.[1]

De nye HP Elite-pc'er inkluderer også HP Sure Click, der giver forbedret beskyttelse via fysisk isolation af hver browserfane eller downloadet pdf- eller Microsoft Office-dokument i en mikrovirtuel maskine (VM) til forebyggelse af spredning af webbaseret malware eller vedhæftede filer på e-mails til andre forbundne enheder på netværket.[2]

It-teamet bruger nu HP Device Access Manager til at administrere porte og udtagelige medier samt HP Manageability Integration Kit til Microsoft SCCM til effektivisering af sikkerheden og BIOS-styring på tværs af flåden.[3]

Konklusion

Swiss Conference Center mistede indtægter og brandtillid fra sine højprofilkunder. Ved implementering af HP-pc'er med omfattende sikkerhedsforanstaltninger og effektive styringsløsninger er centeret nu i stand til at udvise en større forpligtelse i forbindelse med cybersikkerhed.

** Swiss Conference Center er en fiktiv virksomhed, der blev målrettet i et stort cyberangreb i HP Studios film, "THE WOLF: TRUE ALPHA".*

Få flere oplysninger om HP's løsninger:
PC-sikkerhed: hp.com/go/computersecurity
Printersikkerhed: hp.com/go/reinventsecurity

Se "The Wolf"-filmene på:
hp.com/thewolf

[1] HP Sure Start Gen4 fås til HP Elite- og HP Pro 600-produkter med 8. generations Intel®- eller AMD-processorer.
[2] HP Sure Click fås til udvalgte HP-pc'er og understøtter Microsoft® Internet Explorer og Chromium™. Understøttede vedhæftede filer inkluderer Microsoft Office- (Word, Excel, PowerPoint) og pdf-filer i skrivebeskyttet tilstand, når Microsoft Office eller Adobe Acrobat er installeret.
[3] HP Manageability Integration Kit er ikke forudinstalleret, men kan tilkøbes på hp.com/go/clientmanagement.

Tilmeld dig for at få opdateringer
hp.com/go/getupdated

Del med kolleger

4AA7-3561DAE, august 2018