

# Swiss Conference Center AV-hack kunne ha vært unngått med sikkerhetsfunksjonene til HP-PC-er



## Offisiell avslutningsrapport for databruddet

### Bransje

Arrangementer

### Mål

Overvåke sikkerhetsrutiner for å bedre beskytte konferansesentre og sensitive klientdata

### Tilnærming

Jobbet med deres sikkerhetskonsulent for å analysere sikkerhetspraksiser og identifisere områder av bekymring

### IT-forhold

- Oppgraderte flåten til HP Elite PC-er med innebygd beskyttelse mot skadelig programvare
- Lukket unødvendige porter for å forhindre uautorisert bruk
- Integrerte HP Manageability Integration Kit-plugin i Microsoft® System Center Configuration Manager (SCCM) for ekstern administrasjon av PC-flåten

### Forretningsforhold

Oppdaterte cybersikkerhetstiltak for bedre beskyttelse av fasilitetene mot sofistikerte angrep og for å vinne tilbake klientenes tillit



## Oversikt

Swiss Conference Center\* nær Geneve i Sveits er vertskap for over 230 arrangementer hvert år. Som Europas favorittsted for forretningskonferanser og store produktlanseringer, henvender senteret seg til bransjeledere over hele verden.

Senterets ledelse har gjort store investeringer i teknologisk infrastruktur, for å tilby klientene en skreddersydd konferanseopplevelse i omgivelser av eksepsjonell kvalitet. Dessverre ble ikke tilsvarende sikkerhetsoppgraderinger gjort på PC-flåten.

23. april 2018, infiltrerte en hacker som kaller seg selv «The Wolf» en PC i konferansesenteret, for å forstyrre en profilert presentasjon til et internasjonalt publikum. Etter dette innbruddet vendte Swiss Conference Center seg til sikkerhetskonsulenten sin for å finne og reparere svakheter i cybersikkerheten.

## Hva skjedde

Som ett av verdens ledende sentre for forretningspresentasjoner, var Swiss Conference Center ledende innen å skape utrolige gjesteopplevelser, men cybersikkerheten deres var ikke fullt så imponerende. The Wolf lastet opp skadelig programvare til en av senterets PC-er, og byttet så ut en av talernes presentasjon med sin egen. Lokalets IT-sikkerhetsansatte gjorde alt for å ta tilbake kontrollen over nettverket sitt, mens foredragssalen var i kaos.

Skadene stoppet ikke ved én ødelagt presentasjon. Tapt omsetning fra avbestillinger er nå estimert til EUR 3,2 millioner.

## Slik skjedde det

Alt The Wolf trengte å gjøre, var å lure seg inn i én ubeskyttet PC ved å få en av de ansatte til å klikke på en farlig kobling i en e-post eller laste ned et vedlegg som så harmløst ut. Eller han kunne, siden han selv var i nærheten av PC-en, sette inn en flashstasjon i en uovervåket USB-port.

Swiss Conference Center hadde en PC-flåte uten viktig beskyttelse som ville ha satt den skadelige programvaren i karantene og stoppet inntrengningsforsøket. Selv om de hadde installert antivirus-programvare, hadde ingen av PC-ene deres innebygde sikkerhetsfunksjoner håndhevet av maskinvare.

## Styrking av sikkerhet

Ved hjelp av sikkerhetskonsulenten foretok Swiss Conference Center en nøye gjennomgang av sine gjeldende cybersikkerhetstiltak. Denne gjennomgangen førte til en oppgradering av hele PC-flåten til HP Elite PC-er med innebygd beskyttelse mot skadelig programvare, inkludert HP Sure Start Gen4, som automatisk gjenkjenner, stopper og gjenoppretter etter et BIOS-angrep eller skade ved oppstart og i drift.<sup>1</sup>

Nye HP Elite PC-er inkluderer også HP Sure Click, som gir herdet beskyttelse ved å isolere hver nettleserfane eller hvert nedlastet PDF- eller Microsoft Office-dokument i en mikro-virtuell maskin (VM) for å unngå at nettbasert skadelig programvare eller e-postvedlegg sprer seg til andre tilkoblede enheter på nettverket.<sup>2</sup>

IT-teamet bruker nå HP Device Access Manager for å administrere porter og flyttbare medier, og HP Manageability Integration Kit for Microsoft SCCM for å forenkle sikkerhet og BIOS-administrering over hele flåten.<sup>3</sup>

## Konklusjon

Swiss Conference Center led tap av omsetning og nedsatt tillit til merkevaren fra sine høyprofilerte klienter. Men ved å ta i bruk HP-PC-er med omfattende sikkerhetstiltak og effektive administrasjonsløsninger, kan senteret nå vise at de tar cybersikkerhet på alvor.

*\*Swiss Conference Center er en fiktiv virksomhet som var målet til et cyberangrep i HP Studios-filmen, «THE WOLF: ALFAULVEN».*

### For mer informasjon om HP-løsninger:

PC-sikkerhet: [hp.com/go/computersecurity](http://hp.com/go/computersecurity)  
Utskriftssikkerhet: [hp.com/go/reinventsecurity](http://hp.com/go/reinventsecurity)

Hvis du ønsker å se «The Wolf»-filmer, kan du gå til: [hp.com/thewolf](http://hp.com/thewolf)

<sup>1</sup> HP Sure Start Gen4 er tilgjengelig på HP Elite- og HP Pro 600-produkter utstyrt med 8. generasjons Intel®- eller AMD-prosessorer.

<sup>2</sup> HP Sure Click er tilgjengelig på de fleste HP-PC-er og støtter Microsoft® Internet Explorer og Chromium™. Støttede vedlegg inkluderer Microsoft Office (Word, Excel, PowerPoint)- og PDF-filer i skrivebeskyttet modus, når Microsoft Office eller Adobe Acrobat er installert.

<sup>3</sup> HP Manageability Integration Kit kommer ikke forhåndsinstallert, tilgjengelig fra [hp.com/go/clientmanagement](http://hp.com/go/clientmanagement).

Registrer deg for oppdateringer  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Del med kolleger

© Opphavsrett 2018 HP Development Company, L.P. Informasjonen i dette dokumentet kan endres uten varsel. De eneste garantiene for HPs produkter og tjenester er fremsatt i de uttrykkelige garantierklæringene som følger med slike produkter og tjenester. Ikke noe i dette dokumentet skal tolkes som noen form for tilleggsgaranti. HP skal ikke holdes ansvarlig for tekniske eller redaksjonelle feil eller utelatelser i dette dokumentet.

Microsoft er et registrert varemerke i USA for Microsoft-konsernet. Intel er et varemerke som tilhører Intel Corporation eller dets datterselskaper i USA og/eller andre land.

