Esimerkkitapaus

Swiss Conference Centerin AV-järjestelmän hakkerointi olisi voitu estää HP:n tietokoneiden tietoturvatoiminnoilla

Tietomurron virallinen kokoomaraportti

Ala
Tapahtumatuotanto

Tehtävä
Selvittää toimia konferenssikeskuksen ja asiakkaiden arkaluontoisten tietojen suojauksen parantamiseksi

Lähestymistapa
Tietoturvakäytäntöjä analysoitiin ja riskialueita tunnistettiin yhteistyössä yrityksen tietoturvakonsultin kanssa

Tietotekniikkaan liittyvät toimet

- Laitteisto päivitettiin HP Elite -tietokoneisiin, joissa on sisäinen haittaohjelmasuojaus
- Luvaton pääsy estettiin sulkemalla tarpeettomia portteja
- HP Manageability Integration Kit -lisäosa integroitiin Microsoft® System Center Configuration Manageriin (SCCM), mikä mahdollisti PC-laitteiston etähallinnan

Yritystoimintaan liittyvät toimet
Kyberturvallisuustoimet päivitettiin niin, että suojautuminen monimutkaisilta hyökkäyksiltä on helpompaa ja asiakasluottamus voidaan ansaita takaisin

Katsaus

Sveitsissä Geneven lähellä sijaitseva Swiss Conference Center* järjestää yli 230 tapahtumaa joka vuosi. Se on suosittu eurooppalaiskohde yrityskonferenssien ja suurten tuotejulkistusten järjestämiseen ja palvelee eri alojen suuria maailmanlaajuisia toimijoita.

Keskuksen hallinto on investoinut runsaasti tekniseen infrastruktuuriin, joka tarjoaa asiakkaille laajasti mukautettavan konferenssikokemuksen näyttävässä ympäristössä. Valitettavasti tietokonelaitteiston turvallisuuteen ei ole panostettu vastaavalla tavalla.

23. huhtikuuta 2018 itseään nimellä ”The Wolf” kutsuva hakkeri murtautui konferenssikeskuksen tietokoneeseen ja keskeytti laajalle kansainväliselle yleisölle pidetyn esityksen. Murron jälkeen Swiss Conference Center kääntyi tietoturvakonsulttinsa puoleen kyberturvallisuuden haavoittuvuuksien paikantamista ja korjaamista varten.

Mitä tapahtui

Yhtenä maailman suosituimmista yritystapahtumien järjestämispaikoista Swiss Conference Center loisti asiakaskokemusten tarjoamisessa, mutta heidän kyberturvallisuutensa taso ei ollut kovinkaan vakuuttava. The Wolf latasi haittaohjelman keskuksen yhdelle tietokoneelle ja korvasi puhujan esityksen omallaan. Keskuksen tietoturvahenkilöstö yritti saada verkkoa omaan hallintaansa kaaoksen keskellä.

Vahingot eivät rajoittuneet yhteen epäonnistuneeseen esitykseen. Peruttujen varausten myötä menetettyjen tuottojen arvioitu määrä nousi 3,2 miljoonaan euroon.

Syy tapahtuneeseen

Suojaamattoman tietokoneen kaappaaminen edellytti The Wolfilta ainoastaan haittaohjelman lähettävän linkin tai vaarattomalta vaikuttavan liitteen lähettämistä työntekijälle. Hän oli myös fyysisesti lähellä tietokonetta, joten hän olisi voinut asettaa flash-aseman valvomattomaan USB-porttiin.

Swiss Conference Centerin tietokonelaitteistoa ei ollut suojattu ohjelmistolla, joka olisi asettanut haittaohjelman karanteeniin ja estänyt hyökkäyksen. Vaikka tietokoneille *oli* asennettu virustentorjuntaohjelmisto, niistä yhdessäkään ei ollut laitteistotason tietoturvatoimintoja.

Tietoturvan vahvistaminen

Swiss Conference Center teki kattavan selvityksen käytössä olevista kyberturvallisuustoimista yhdessä tietoturvakonsultin kanssa. Selvityksen myötä keskus päätti päivittää koko tietokonelaitteistonsa HP Elite -malleihin. Laitteet on varustettu sisäisellä haittaohjelmasuojauksella, kuten 4. sukupolven HP Sure Startilla, joka pystyy automaattisesti havaitsemaan, pysäyttämään ja korjaamaan BIOS-hyökkäyksen tai tiedostojen vioittumisen käynnistyksen ja käytön aikana.[1]

Uusissa HP Elite -tietokoneissa on myös HP Sure Click -toiminto, joka tarjoaa parannetun suojauksen. Se pystyy eristämään jokaisen selaimen välilehden tai ladatun PDF:n tai Microsoft Office -asiakirjan mikrotason virtuaalikoneeseen (VM) ja näin estämään verkkosivun tai liitteen sisältämän haittaohjelman leviämisen muihin samaan verkkoon liitettyihin laitteisiin.[2]

IT-tiimi käyttää nyt HP Device Access Manageria porttien ja siirrettävien laitteiden hallintaan sekä Microsoft SCCM:ään asennettavaa HP Manageability Integration Kitiä, joka helpottaa koko laitteiston laajuista tietoturva- ja BIOS-hallintaa.[3]

Lopuksi

Swiss Conference Center menetti paitsi voittoja myös korkean profiilin asiakkaidensa luottamuksen. Kattavilla tietoturvaominaisuuksilla varustettujen HP-tietokoneiden sekä tehokkaiden valvontaratkaisujen käyttöönoton myötä keskus voi kuitenkin osoittaa sitoutuneensa kyberturvallisuuteen.

**Swiss Conference Center on fiktiivinen yritys, joka joutuu kyberhyökkäyksen kohteeksi HP Studion elokuvassa "THE WOLF: TRUE ALPHA".*

Lisätietoja HP:n ratkaisuista:

Tietokoneiden tietoturva:
hp.com/go/computersecurity
Tulostimien ja monitoimilaitteiden tietoturva:
hp.com/go/reinventsecurity

Katso "The Wolf" -elokuvat osoitteessa

hp.com/thewolf

[1] 4. sukupolven HP Sure Start on käytettävissä 8. sukupolven Intel®- ja AMD-prosessoreilla varustetuissa HP Elite- ja HP Pro 600 -laitteissa.
[2] HP Sure Click on saatavana useimpiin HP:n PC-laitteisiin. Se tukee Microsoft® Internet Exploreria ja Chromiumia™. Tuettuihin liitteisiin kuuluvat Microsoft Office-tiedostot (Word, Excel, PowerPoint) ja PDF-tiedostot vain luku -tilassa, kun Microsoft Office tai Adobe Acrobat on asennettu.
[3] HP Manageability Integration Kitiä ei ole esiasennettu, vaan se on ladattavissa osoitteesta hp.com/go/clientmanagement.

Tilaa päivitysilmoitukset

hp.com/go/getupdated

Jaa kollegoiden kanssa

4AA7-3561FIE, heinäkuu 2014