

Napad na Švicarski konferenčni center bi bilo mogoče preprečiti z varnostnimi funkcijami računalnikov HP



Uradno zaključeno poročilo o varnostni kršitvi

Panoga

Prireditve

Cilj

Nadzor nad varnostnimi praksami za boljšo zaščito konferenčnega centra in občutljivih podatkov o strankah

Pristop

Sodelovanje s svetovalcem za varnost, s katerim se analizira varnostne prakse in prepoznajo področja, ki zbujejo skrb

Zadeve na področju informacijske tehnologije

- Nadgradnja skupine naprav na računalnike HP Elite z vgrajeno zaščito pred zlonamerno programsko opremo
- Zapiranje nepotrebnih vrat, da se prepreči nepooblaščen uporaba
- Vgraditev vtičnika HP Manageability Integration Kit v orodje Microsoft® System Center Configuration Manager (SCCM) za upravljanje skupine računalnikov na daljavo

Zadeve na področju poslovanja

Posodobljeni ukrepi na področju spletne varnosti, ki zagotavljajo boljšo zaščito objektov pred prefinjenimi napadi in vnovično pridobitev zaupanja strank



Pregled

Švicarski konferenčni center* v bližini Ženeve v Švici gosti več kot 230 dogodkov vsako leto. Kot evropsko prizorišče za poslovne konference in velike dogodke, na katerih se predstavijo izdelki, center oskrbuje vodilna podjetja z vsega sveta.

Uprava objekta je veliko vložila v tehnološko infrastrukturo, da lahko strankam zagotavlja prilagodljivo konferenčno izkušnjo in čudovito opremljen prostor. Žal v skupini računalnikov niso bile izvedene ustrezne varnostne nadgradnje.

23. aprila 2018 je napadalec, ki samega sebe imenuje »The Wolf«, vdrl v računalnik konferenčnega centra in prekinil visoko odmevno predstavitev za mednarodno občinstvo. Po kršitvi se je Švicarski konferenčni center obrnil na svojega svetovalca za varnost, da bo odkril in odpravil ranljivosti v spletni zaščiti.

Kaj se je zgodilo

Kot eno od glavnih prizorišč na svetu za prireditve podjetij je Švicarski konferenčni center slovel po ustvarjanju osupljivih izkušenj za stranke, toda njihova spletna varnost ni naredila vtisa. »The Wolf« je na enega od računalnikov v centru naložil zlonamerno programsko opremo, potem pa prevzel nadzor nad predstavitvijo govorca. Osebe, zadolžene za varnost informacijske tehnologije v objektu, je sredi zmede v predavalnici poskušalo vzpostaviti nadzor nad omrežjem.

Škoda se ni končala pri uničeni predstavitvi. Izgubljen prihodek zaradi preklicanih rezervacij je trenutno ocenjen na 3,2 milijona evrov.

Kako se je to lahko zgodilo

Vse, kar je moral narediti »The Wolf«, je bilo vdreti v enega od nezaščitenih računalnikov, tako da je uslužbenca prepričal, da je kliknil zlonamerno povezavo v e-pošti ali prenesel navidez neškodljivo prilogo. Ali ker je bil v fizični bližini računalnika, je lahko v nenadzorovana vrata USB vstavil ključek.

Skupini računalnikov v Švicarskem konferenčnem centru je manjkala ključna zaščita, ki bi izolirala zlonamerno programsko opremo in zaustavila ta poskus vdora. Čeprav so namestili protivirusno programsko opremo, nobeden od njihovih računalnikov ni imel vgrajenih varnostnih funkcij, temelječih na strojni opremi.

Okrepitev varnosti

Švicarski konferenčni center je skupaj s svojim svetovalcem za zaščito izvedel natančen pregled obstoječih ukrepov za spletno varnost. Ta pregled je vodil do nadgradnje celotne skupine naprav na računalnike HP Elite z vgrajeno zaščito pred zlonamerno programsko opremo, vključno s HP Sure Start četrte generacije, ki lahko samodejno odkrije in zaustavi napad na sistemski BIOS ali okvaro v času zagona ali med izvajanjem ter izvede obnovitev po njih.¹

Novi računalniki HP Elite vključujejo tudi funkcijo HP Sure Click, ki s fizično izolacijo vsakega zavihka brskalnika ali prenesene datoteke PDF ali dokumenta Microsoft Office na mikro navidezni računalnik (VM) zagotavlja boljšo zaščito, saj prepreči razširjanje na spletu temelječe zlonamerne programske opreme ali e-poštnih prilog na druge povezane naprave v omrežju.²

Ekipa za informacijsko tehnologijo zdaj za upravljanje vrat in izmenljivih medijev uporablja orodje HP Device Access Manager, za poenostavitev zaščite in upravljanje systemskega BIOS-a v celotni skupini naprav pa HP Manageability Integration Kit za Microsoft SCCM.³

Sklep

Švicarski konferenčni center je utrpel izgubo prihodkov in zmanjšano zaupanje v znamko svojih najpomembnejših strank. Toda z uvedbo računalnikov HP z obsežnimi varnostnimi ukrepi in učinkovitim upravljanjem rešitev se lahko center zdaj pohvali z globljo zavezo na področju spletne varnosti.

**Švicarski konferenčni center je izmišljeno podjetje, ki je cilj spletnega napada v filmu HP Studio »THE WOLF: PRAVI ALFA«.*

Več informacij o HP-jevih rešitvah:

Varnost računalnikov: hp.com/go/computersecurity

Varnost tiskanja: hp.com/go/reinventsecurity

Za ogled filmov »The Wolf« obiščite spletno mesto

hp.com/thewolf

¹ HP Sure Start četrte generacije je na voljo v izdelkih HP Elite in HP Pro 600, ki so opremljeni s procesorji Intel® ali AMD osme generacije.

² HP Sure Click je na voljo na večini računalnikov HP in zagotavlja podporo za Microsoft® Internet Explorer in Chromium™. Podprte priloge vključujejo datoteke Microsoft Office (Word, Excel, PowerPoint) in PDF v načinu samo za branje, če imate nameščen program Microsoft Office ali Adobe Acrobat.

³ Komplet HP Manageability Integration ni prednameščen, na voljo pa je na spletnem mestu hp.com/go/clientmanagement.

Prijavite se za posodobitve
hp.com/go/getupdated



Delite s kolegi

© Copyright 2014 Hewlett-Packard Development Company, L.P. Informacije v tem dokumentu se lahko spremenijo brez predhodnega obvestila. Edina jamstva za HP-jeve izdelke in storitve so navedena v izrecnih garancijskih izjavah, ki so priložene takšnim izdelkom in storitvam. Noben del tega dokumenta se ne sme razlagati kot dodatna garancija. HP ne odgovarja za tehnične ali uredniške napake oziroma pomanjkljivosti v tem dokumentu.

AirPrint in logotip AirPrint sta blagovni znamki družbe Apple Inc. iPad, iPhone, in iPod touch so blagovne znamke družbe Apple Inc., registrirane v ZDA in drugih državah. ENERGY STAR in oznaka ENERGY STAR sta znamki, registrirani v ZDA. Microsoft, Windows, Windows XP in Windows Vista so registrirane blagovne znamke družbe Microsoft Corporation. UNIX je registrirana blagovna znamka družbe The Open Group.

4AA7-3561SLE, mesec 2014

