

Atacul AV de la Swiss Conference Center ar fi putut fi prevenit de caracteristicile de securitate ale PC-urilor HP



Raportul oficial privind breșa de date

Industrie

Locuri de întâlnire pentru evenimente

Obiectiv

Verificarea practicilor de securitate pentru mai buna protecție a centrului de conferințe și a datelor sensibile ale clienților

Abordare

S-a lucrat cu consultantul lor pe probleme de securitate pentru analiza practicilor de securitate și identificarea zonelor de preocupare

IT contează

- S-a îmbunătățit flota de dispozitive cu PC-uri HP Elite cu protecții încorporate împotriva malware-ului
- S-au închis porturile inutile, pentru a preveni utilizarea neautorizată
- S-a integrat plug-inul Kit HP de integrare și manevrabilitate în Microsoft® System Center Configuration Manager (SCCM), pentru gestionarea de la distanță a flotei de PC-uri

Afacerea contează

S-au actualizat măsurile de securitate cibernetică, pentru a se asigura o mai bună protecție a instalațiilor împotriva atacurilor sofisticate și pentru a recâștiga încrederea clienților



Prezentare generală

Swiss Conference Center* de lângă Geneva, Elveția, găzduiește peste 230 de evenimente în fiecare an. Fiind centrul european preferat pentru conferințele de afaceri și evenimentele importante de lansare a produselor, Centrul oferă servicii liderilor în industrie din întreaga lume.

Conducerea centrului a făcut investiții mari în infrastructura tehnologică, pentru a oferi clienților o experiență de conferințe cu un înalt nivel de particularizare, într-un spațiu frumos amenajat. Din nefericire, pentru flota de PC-uri nu s-au efectuat actualizările de securitate corespunzătoare.

Pe 23 aprilie 2018, un hacker care se autointitulează „The Wolf” a accesat în mod neautorizat un PC de la centrul de conferințe, pentru a întrerupe o prezentare foarte așteptată de auditoriul internațional. După breșă, Swiss Conference Center a apelat la consultantul în securitate pentru a găsi și a repara vulnerabilitățile securității cibernetică.

Ce s-a întâmplat

Fiind unul dintre principalele locuri de organizare a evenimentelor corporative din lume, Swiss Conference Center a excelat la capitolul experiențe remarcabile pentru invitați, dar securitatea lor cibernetică a fost mai puțin impresionantă. The Wolf a încărcat malware în unul dintre PC-urile Centrului, apoi a înlocuit o prezentare a vorbitorului cu una proprie. Personalul de securitate IT al centrului a încercat cu disperare să recapete controlul asupra rețelei, în haosul creat în sala de conferință.

Pagubele nu s-au limitat la distrugerea unei prezentări. Pierderile de venituri din cauza rezervărilor anulate sunt estimate la 3,2 milioane de euro.

Cum s-a întâmplat

A fost suficient ca The Wolf să pătrundă într-un PC neprotejat, așteptând ca un angajat să facă clic pe o legătură greșită dintr-un e-mail sau să descarce o atașare aparent inofensivă. Sau, dacă se afla fizic lângă PC, să fi introdus o unitate flash într-un port USB nesupravegheat.

Flota de PC-uri de la Swiss Conference Center nu era prevăzută cu protecții cruciale, care ar fi pus malware-ul în carantină și ar fi oprit această încercare de infiltrare. Cu toate că acestea aveau instalat software antivirus, niciunul dintre PC-uri nu avea caracteristici de securitate încorporate, implementate în hardware.

Fortificarea securității

Împreună cu consultantul pe probleme de securitate, Swiss Conference Center a efectuat o verificare minuțioasă a măsurilor de securitate cibernetică existente. Rezultatele verificării au dus la un upgrade al întregii flote cu PC-uri HP Elite cu protecție încorporată împotriva malware-ului, inclusiv HP Sure Start Gen4, care poate să detecteze și să oprească un atac sau o acțiune de corupere a BIOS-ului la pornire și în timpul funcționării, pentru ca apoi să recupereze sistemul, toate în mod automat.¹

Noile PC-uri HP Elite includ, de asemenea, HP Sure Click, care asigură o protecție fortificată prin izolarea fizică a fiecărei file de browser sau a fiecărui document PDF sau Microsoft Office descărcat, într-o micro-mașină virtuală (VM), pentru a preveni răspândirea malware-ului de pe web sau a atașărilor de e-mail spre alte dispozitive conectate în rețea.²

Echipa IT utilizează acum HP Device Access Manager pentru a gestiona porturile și suporturile amovibile, precum și Kitul HP de integrare și manevrabilitate pentru Microsoft SCCM, pentru a eficientiza securitatea și administrarea BIOS-ului în întreaga flotă de dispozitive.³

Concluzie

Swiss Conference Center a suferit pierderi de venituri, iar încrederea principalilor clienți în acest brand a scăzut. Totuși, prin instalarea PC-urilor de la HP, prevăzute cu măsuri de securitate cuprinzătoare și cu soluții de gestionare eficiente, Centrul este acum capabil să demonstreze un angajament mai puternic față de securitatea cibernetică.

**Swiss Conference Center este o organizație fictivă, supusă unui atac cibernetic, în filmul realizat de Studiourile HP, „THE WOLF: TRUE ALPHA”.*

Pentru mai multe informații despre soluțiile HP:

Securitatea PC-urilor: hp.com/go/computersecurity
Securitatea imprimării: hp.com/go/reinventsecurity

Pentru a vedea filmele „The Wolf”, vizitați: hp.com/thewolf

¹ Instrumentul HP Sure Start Gen4 este disponibil la produsele HP Elite și HP Pro 600 care sunt echipate cu procesoare Intel® sau AMD din a 8-a generație.

² Tehnologia HP Sure Click este disponibilă pe majoritatea PC-urilor HP și acceptă Microsoft® Internet Explorer și Chromium™. Atașările acceptate includ fișiere Microsoft Office (Word, Excel, PowerPoint) și PDF în mod de citire exclusivă, când este instalat Microsoft Office sau Adobe Acrobat.

³ Kitul HP de integrare și manevrabilitate nu este preinstalat și este disponibil la hp.com/go/clientmanagement.

Înregistrați-vă pentru actualizări

hp.com/go/getupdated



Partajați cu colegii

© Copyright 2014 Hewlett-Packard Development Company, L.P. Informațiile din documentul de față pot fi modificate fără notificare prealabilă. Singurele garanții pentru produsele și serviciile HP sunt cele specificate în declarațiile speciale de garanție care însoțesc respectivele produse și servicii. Nimic din documentul de față nu trebuie interpretat ca reprezentând o garanție suplimentară. Compania HP nu va fi răspunzătoare pentru erorile tehnice sau editoriale ori pentru omisiunile din documentul de față.

AirPrint și sigla AirPrint sunt mărci comerciale ale Apple Inc. iPad, iPhone și iPod touch sunt mărci comerciale ale Apple Inc., înregistrate în S.U.A. și în alte țări/regiuni. ENERGY STAR și simbolul ENERGY STAR sunt mărci înregistrate în S.U.A. Microsoft, Windows, Windows XP și Windows Vista sunt mărci comerciale înregistrate în S.U.A. ale Microsoft Corporation. UNIX este marcă comercială înregistrată a The Open Group.

