Mögliches Szenario

Swiss Conference Center Hackerangriff auf AV-Anlage hätte mit HP PC Sicherheits-funktionen verhindert werden können

Offizieller Abschlussbericht über das Datenleck

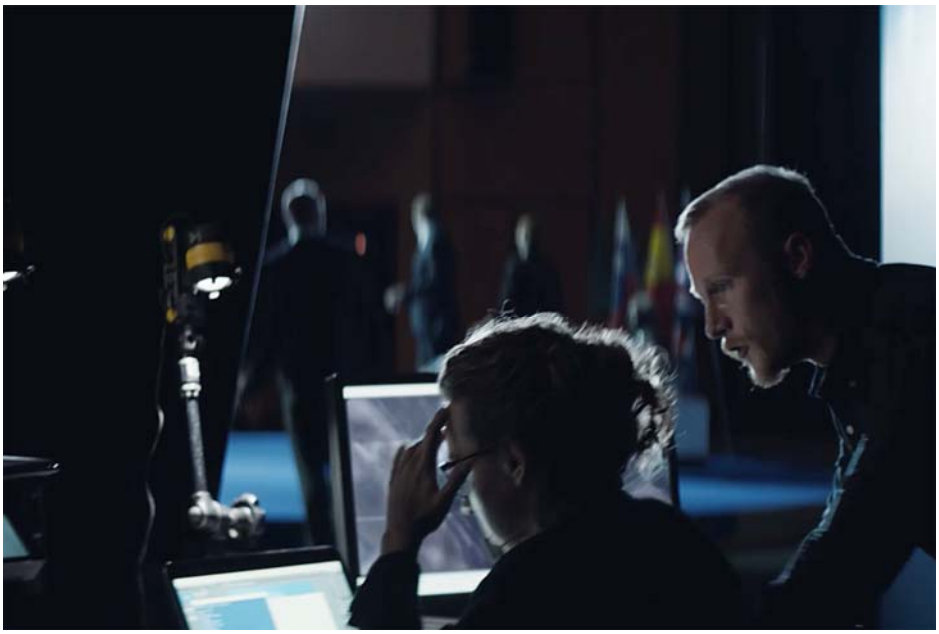
Branche
Konferenzräume

Ziel
Überprüfung der Sicherheitspraktiken zum besseren Schutz des Konferenzzentrums und sensibler Kundendaten

Vorgehensweise
Zusammenarbeit mit ihrem Sicherheitsberater zur Analyse der Sicherheitspraktiken und Erkennung von Problemfeldern

IT-Aspekte
- Upgrade der IT auf HP Elite PCs mit integrierten Schutzfunktionen gegen Malware
- Schließung ungenutzter Ports, um unbefugte Nutzung zu verhindern
- Integration des HP Manageability Integration Kit Plug-ins in den Microsoft System Center Configuration Manager (SCCM) zur Remote-Steuerung sämtlicher Netzwerk-PCs

Geschäftliche Aspekte
Aktualisierung der Maßnahmen zur Cybersicherheit für einen besseren Schutz der Anlagen gegen ausgeklügelte Angriffe und um Kundenvertrauen zurückzugewinnen



Überblick

Das Swiss Conference Center* in der Nähe von Genf veranstaltet jedes Jahr über 230 Events. Das Center gilt als Top-Adresse in Europa für Wirtschaftskonferenzen und große Produkt-Launches und richtet sich an Spitzenunternehmer und Branchenführer weltweit.

Das Gebäudemanagement hat umfangreiche Investitionen in die Technologieinfrastruktur getätigt, um seinen Kunden das Konferenzerlebnis nach ihren Wünschen an einem einzigartig schönen Ort zu bieten. Leider wurden die entsprechenden Sicherheits-Upgrades nicht für die PCs im Netzwerk durchgeführt.

Am 23. April 2018 infiltrierte ein Hacker, der sich „The Wolf“ nennt, einen PC im Tagungszentrum, um eine hochrangige Präsentation vor internationalem Publikum zu stören. Nach dem Vorfall wandte sich das Swiss Conference Center an seinen Sicherheitsberater, um Schwachstellen in der Cybersicherheit aufzuspüren und zu reparieren.

Was ist passiert?

Als Premium-Adresse für Wirtschaftstagungen konnte das Swiss Conference Center seinen Gästen atemberaubende Erlebnisse bieten. Doch seine Cybersicherheit war alles andere als atemberaubend. The Wolf hatte Malware auf einen der PCs im Netzwerk des Conference Center hochgeladen und tauschte die Präsentation des Redners anschließend mit seiner eigenen aus. Die IT vor Ort versuchte verzweifelt, inmitten des Chaos im Konferenzsaal die Kontrolle über das Netzwerk zurückzugewinnen.

Der Schaden beschränkte sich nicht auf eine ruinierte Präsentation. Die Einnahmeverluste aufgrund kurzfristig stornierter Buchungen belaufen sich Schätzungen zufolge auf 3,2 Millionen Euro.

Wie konnte es passieren?

The Wolf musste lediglich einen ungeschützten PC anzapfen, indem er einen Mitarbeiter dazu brachte, einen schädlichen Link in einer E-Mail zu klicken oder einen harmlos erscheinenden Anhang zu öffnen. Da er sich vor Ort befand, hätte er sogar nur einen PC finden müssen, in den er in einem unbeobachteten Moment einen USB-Stick einsteckt.

Den Netzwerk-PCs des Swiss Conference Center fehlte es an grundlegenden Schutzmaßnahmen, die diesen Angriff einer Malware abgewendet hätten. Zwar verfügten die PCs über eine Antivirus-Software, aber auf keinem einzigen waren Hardware-basierte Sicherheitsfunktionen integriert.

Sicherheit stärken

Mithilfe seines Sicherheitsberaters führte das Swiss Conference Center eine gründliche Überprüfung der vorhandenen Maßnahmen zur Cybersicherheit durch. Nach dieser Prüfung wurden sämtliche Netzwerk-PCs auf HP Elite mit integriertem Schutz vor Malware inklusive HP Sure Start Gen4 aufgerüstet. Sie können automatisch einen Angriff auf das BIOS oder eine Störung beim Hochfahren und bei laufendem Betrieb erkennen, stoppen und das BIOS wiederherstellen.[1]

Die neuen HP Elite PCs bieten außerdem HP Sure Click. Das Programm sorgt für noch besseren Schutz, da es jede Registerkarte im Browser oder heruntergeladene PDFs oder Microsoft Office-Dokumente in einer mikro-virtuellen Maschine (VM) physisch isoliert und so webbasierte Malware oder E-Mail-Anhänge daran hindert, auf andere Geräte im Netzwerk überzugreifen.[2]

Das IT-Team verwendet jetzt HP Device Access Manager, um die Ports und Wechseldatenträger zu verwalten, und das HP Manageability Integration Kit für Microsoft SCCM, um die Sicherheit und BIOS-Verwaltung im gesamten Netzwerk zu optimieren.[3]

Zusammenfassung

Das Swiss Conference Center musste Einnahmeverluste und verlorenes Vertrauen in seine Marke vonseiten seiner hochkarätigen Kunden verkraften. Durch den Einsatz von HP PCs mit umfassenden Sicherheitsmaßnahmen und effektiven Managementlösungen kann das Center nun seinen Einsatz für bessere Cybersicherheit glaubhaft nachweisen.

**Das Swiss Conference Center ist ein fiktives Unternehmen, das im Film „THE WOLF:TRUE ALPHA" von HP Studio Ziel eines großangelegten Cyberangriffs wird. TRUE ALPHA."*

Weitere Informationen zu den Lösungen von HP siehe

PC-Sicherheitslösungen:
hp.com/go/computersecurity
Druckersicherheit.
hp.com/go/reinventsecurity

Hier können Sie die Filme über „The Wolf" sehen:

hp.com/thewolf

[1] HP Sure Start Gen4 ist auf HP Elite und HP Pro 600 Produkten mit Intel®-Prozessoren der 8. Generation oder AMD-Prozessoren verfügbar.
[2] HP Sure Click ist auf den meisten HP PCs verfügbar und unterstützt Microsoft Internet Explorer und Chromium™. Geschützte Dateiformate von Anhängen sind Microsoft Office- (Word, Excel, PowerPoint) und PDF-Dateien im schreibgeschützten Modus, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.
[3] HP Manageability Integration Kit ist nicht vorinstalliert. Es ist verfügbar unter hp.com/go/clientmanagement.

Melden Sie sich noch heute an.
hp.com/go/getupdated

An Kollegen weiterleiten

4AA3-xxxxDEE, Monat 2014