

# O ataque ao Swiss Conference Center poderia ter sido evitado através das funcionalidades de segurança informática da HP



## Relatório resumido oficial sobre o ataque

### Setor de atividade

Locais de eventos

### Objetivo

Realizar uma auditoria às práticas de segurança para melhor proteger o centro de conferências e dados sensíveis de clientes

### Abordagem

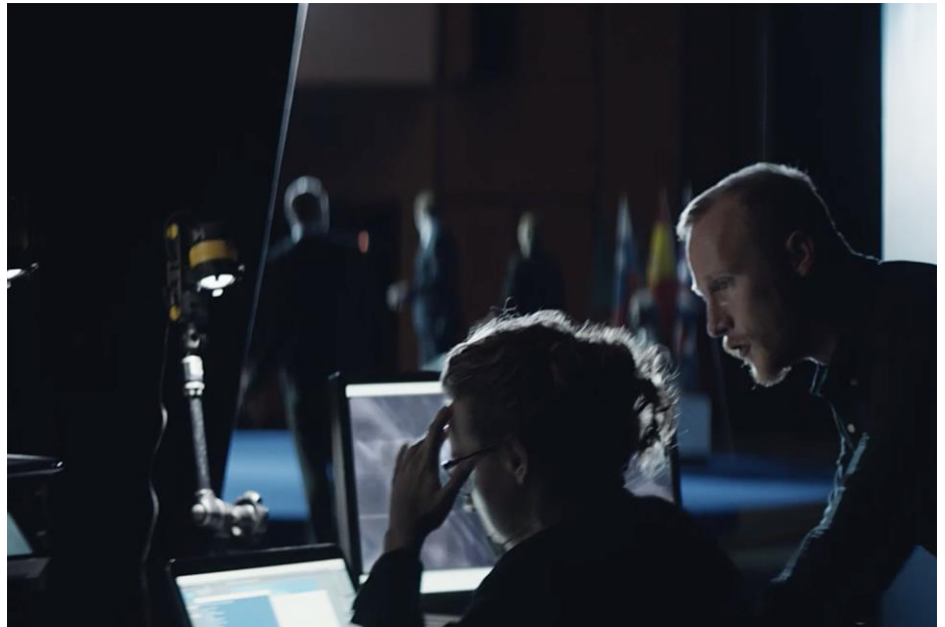
Cooperação com o seu consultor de segurança para analisar práticas de segurança e identificar áreas de preocupação

### As TI são fundamentais

- Atualização do parque para computadores HP Elite com proteção incorporada contra malware
- Desativação de portas desnecessárias para evitar a utilização não autorizada
- Integração do plug-in HP Manageability Integration Kit no Microsoft® System Center Configuration Manager (SCCM) para gerir remotamente o parque de computadores

### A segurança é fundamental

Atualização das medidas de cibersegurança para melhor proteger as instalações contra ataques sofisticados e reconquistar a confiança dos clientes



## Descrição geral

O Swiss Conference Center\*, localizado próximo de Genebra (Suíça), acolhe mais de 230 eventos por ano. Como o local de eleição europeu para conferências de negócios e grandes eventos de lançamento de produtos, o Swiss Conference Center responde às necessidades dos líderes da indústria a nível mundial.

A administração do Swiss Conference Center fez grandes investimentos em infraestruturas de tecnologia para proporcionar aos clientes uma experiência de conferência altamente personalizável num espaço incrivelmente bem construído. Infelizmente, não foram feitas atualizações de segurança ao parque de computadores.

A 23 de abril de 2018, um hacker que se autodenomina "The Wolf" acedeu a um computador no Swiss Conference Center por forma a manipular uma apresentação de alto nível perante uma audiência internacional. No seguimento do ataque, o Swiss Conference Center recorreu ao seu consultor de segurança para identificar e reparar as vulnerabilidades de cibersegurança.

## O que aconteceu?

Sendo um dos mais consagrados locais de eventos empresariais do mundo, o Swiss Conference Center teve um desempenho excepcional na criação de experiências extraordinárias para os visitantes. Infelizmente, no que toca à questão da cibersegurança, o seu desempenho deixou algo a desejar. The Wolf transferiu malware para um dos computadores do Swiss Conference Center e, em seguida, substituiu a apresentação de um orador por uma sua. O pessoal de segurança de TI envidou todos os esforços para recuperar o controlo da sua rede entre o caos instalado na sala de conferências.

Mas os danos não se ficaram por uma apresentação arruinada. As perdas de receitas devido a reservas canceladas estão atualmente avaliadas em cerca de 3,2 milhões de euros.

## Como aconteceu?

Tudo o que The Wolf teve de fazer foi aceder a um computador desprotegido, fazendo com que um funcionário clicasse numa hiperligação maliciosa num e-mail ou descarregasse um anexo aparentemente inofensivo. Ou, uma vez que estava fisicamente perto do computador, poderia ter inserido uma unidade flash numa porta USB não monitorizada.

O parque de computadores do Swiss Conference Center não dispunha de proteções cruciais que teriam colocado o malware em quarentena e parado esta tentativa de intrusão. Apesar de terem de facto instalado um software antivírus, nenhum dos seus computadores integrava funcionalidades de segurança imposta por hardware.

## Reforço da segurança

Em conjunto com o seu consultor de segurança, o Swiss Conference Center realizou uma auditoria completa às suas medidas de cibersegurança existentes. Essa análise resultou numa atualização de todo o parque para os computadores HP Elite com proteção contra malware, incluindo HP Sure Start Gen 4, capaz de detetar, parar e recuperar automaticamente de um ataque ao BIOS ou corrupção no arranque e durante o tempo de execução.<sup>1</sup>

Os novos computadores HP Elite incluem também o HP Sure Click, que oferece proteção reforçada isolando fisicamente cada separador do browser ou documento PDF ou do Microsoft Office descarregado numa máquina microvirtual (VM) para evitar que malware baseado na Internet ou em anexos de e-mail se propague para outros dispositivos ligados na rede.<sup>2</sup>

A equipa de TI utiliza agora o HP Device Access Manager para gerir portas e unidades de armazenamento de dados amovíveis, bem como o HP Manageability Integration Kit para Microsoft SCCM para agilizar a segurança e a administração do BIOS em todo o parque.<sup>3</sup>

## Conclusão

O Swiss Conference Center sofreu perdas de receitas, e os seus clientes de alto perfil perderam a confiança no centro. Contudo, ao instalar computadores HP com medidas de segurança abrangentes e soluções de gestão eficazes, o Swiss Conference Center consegue agora demonstrar um maior compromisso quanto à cibersegurança.

*\*O Swiss Conference Center é uma organização fictícia alvo de um ciberataque no filme da HP Studios, "THE WOLF: TRUE ALPHA."*

### Para saber mais informações sobre as soluções da HP:

Segurança informática:  
[hp.com/go/computersecurity](http://hp.com/go/computersecurity)  
Segurança de impressão:  
[hp.com/go/reinventsecurity](http://hp.com/go/reinventsecurity)

### Para ver os filmes "The Wolf":

[hp.com/thewolf](http://hp.com/thewolf)

<sup>1</sup> O HP Sure Start Gen 4 está disponível em dispositivos HP Elite e HP Pro 600 equipados com processadores Intel® ou AMD de 8.ª geração.

<sup>2</sup> O HP Sure Click está disponível na maioria dos computadores HP e suporta Microsoft® Internet Explorer e Chromium™. Os anexos suportados incluem ficheiros do Microsoft Office (Word, Excel, PowerPoint) e ficheiros PDF no modo só de leitura, quando o Microsoft Office ou Adobe Acrobat estão instalados.

<sup>3</sup> O HP Manageability Integration Kit não está pré-instalado. Está disponível em [hp.com/go/clientmanagement](http://hp.com/go/clientmanagement).

Registe-se para receber atualizações  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Partilhar com colegas

© Copyright 2018 HP Development Company, L.P. As informações apresentadas estão sujeitas a alteração sem aviso prévio. As únicas garantias para os produtos e serviços da HP estão definidas nas declarações de garantia expressas que acompanham os respetivos produtos e serviços. Nada do aqui apresentado deverá ser interpretado como constituição de garantia adicional. A HP não é responsável por omissões nem erros técnicos ou editoriais aqui apresentados.

Microsoft é uma marca comercial do grupo de empresas Microsoft, registada nos E.U.A. Intel é uma marca comercial da Intel Corporation ou das suas subsidiárias nos E.U.A. e/ou noutros países.

4AA7-3561PTE. Agosto de 2018.

