

Invasão de hacker no Centro Suíço de Convenções poderia ter sido evitada com recursos de segurança da HP no PC



Relatório oficial resumido sobre a violação de dados

Setor

Locais para eventos

Objetivo

Auditar práticas de segurança para proteger melhor o centro de conferências e os dados confidenciais do cliente

Abordagem

Trabalho com o consultor de segurança deles para analisar as práticas de segurança e identificar áreas de preocupação

Questões de TI

- Atualização do conjunto de dispositivos para PCs HP Elite com proteção integrada contra malware
- Fechamento de portas desnecessárias para evitar uso não autorizado
- Plug-in do HP Manageability Integration Kit integrado ao Microsoft® System Center Configuration Manager (SCCM) para gerenciar remotamente o conjunto de PCs

Questões de negócios

Medidas atualizadas de cibersegurança para proteger melhor as instalações contra ataques sofisticados e reconquistar a confiança do cliente



Visão geral

O Centro Suíço de Convenções* próximo a Genebra, na Suíça, recebe mais de 230 eventos por ano. Como o local europeu preferido para conferências de negócios e grandes lançamentos de produtos, o Centro atende os líderes do setor no mundo inteiro.

A gerência das instalações fez grandes investimentos em infraestrutura de tecnologia para oferecer aos clientes uma experiência de conferência altamente personalizada em um espaço lindamente decorado. Infelizmente, as respectivas atualizações de segurança não foram feitas no conjunto de PCs.

No dia 23 de abril de 2018, um hacker que se autointitula “The Wolf” (O Lobo) invadiu um PC no centro de conferências para interromper uma apresentação de alto nível para um público internacional. Após a violação, o Centro Suíço de Conferências recorreu ao seu consultor de segurança para localizar e reparar as vulnerabilidades de cibersegurança.

O que aconteceu

Como um dos principais locais corporativos do mundo, o Centro Suiço de Conferências dominou a arte de oferecer experiências incríveis aos convidados — já a cibersegurança deles causou uma impressão não tão positiva. O hacker The Wolf infiltrou malware em um dos PCs do Centro, depois substituiu a apresentação de um palestrante por outra de sua autoria. A equipe de segurança de TI das instalações se debateu para retomar o controle da rede diante do caos estabelecido na sala da palestra.

Os danos não se limitaram a uma apresentação arruinada. A perda de faturamento com o cancelamento de reservas está estimada em € 3,2 milhões.

Como aconteceu

Bastou que o hacker The Wolf invadisse um PC desprotegido, conseguindo com que um funcionário clicasse em um link mal-intencionado em um e-mail ou baixasse um anexo com aparência inocente. Ou, como ele estava fisicamente próximo ao PC, ele pode ter inserido um pen drive em uma porta USB sem supervisão.

O conjunto de dispositivos do Centro Suiço de Conferências não contava com proteções importantes que poderiam ter colocado o malware de quarentena e interrompido essa tentativa de infiltração. Embora eles *tivessem* um antivírus instalado, nenhum dos PCs tinha recursos de segurança integrados reforçados por hardware.

Reforço da segurança

Com o consultor de segurança, o Centro Suiço de Convenções conduziu uma auditoria completa das medidas de cibersegurança já existentes. Essa revisão levou a uma atualização de todo o conjunto de dispositivos para PCs HP Elite com proteção integrada contra malware, incluindo o HP Sure Start Gen4, que é capaz de automaticamente detectar, interromper e se recuperar de um ataque ou corrupção no BIOS durante a inicialização e o tempo de execução.¹

Os novos PCs HP Elite também incluem HP Sure Click, que oferece maior proteção, isolando fisicamente cada guia do navegador, PDF baixado ou documento do Microsoft Office em uma micromáquina virtual (VM) para evitar que malware baseado na web ou anexos de e-mail se espalhem para outros dispositivos conectados na rede.²

Agora a equipe de TI usa o HP Device Access Manager para gerenciar portas e mídias removíveis e o HP Manageability Integration Kit para Microsoft SCCM para aperfeiçoar a segurança e a administração do BIOS no conjunto de dispositivos.³

Conclusão

O Centro Suiço de Conferências sofreu perda de faturamento e redução de confiança na marca por parte de clientes importantes. Porém, com a implantação de PCs da HP com medidas abrangentes de segurança, agora o Centro consegue demonstrar um compromisso mais forte com a cibersegurança.

**O Centro Suiço de Convenções é uma organização fictícia alvo de um ciberataque no filme da HP Studio "THE WOLF: TRUE ALPHA."*

Para obter mais informações, consulte:

Segurança de PC:

hp.com/go/computersecurity

Segurança da impressão:

hp.com/go/reinventsecurity

Para assistir aos filmes "The Wolf", acesse:

hp.com/thewolf

¹ O HP Sure Start Gen4 está disponível nos produtos HP Elite e HP Pro 600 equipados com processadores Intel® ou AMD de oitava geração.

² O HP Sure Click está disponível na maioria dos PCs da HP e é compatível com o Microsoft® Internet Explorer e Chromium™. Os anexos compatíveis incluem arquivos do Microsoft Office (Word, Excel, PowerPoint) e PDF no modo apenas leitura, quando o Microsoft Office ou Adobe Acrobat estão instalados.

³ O HP Manageability Integration Kit não vem pré-instalado; disponível em hp.com/go/clientmanagement.

Inscreva-se para obter atualizações
hp.com/go/getupdated



Compartilhe com colegas

© Copyright 2018 HP Development Company, L.P. As informações aqui contidas estão sujeitas a alterações sem aviso. As únicas garantias para produtos e serviços HP estão definidas nas declarações de garantia expressa que acompanham tais produtos e serviços. Nenhuma parte deste documento deve ser interpretada como garantia adicional. A HP não se responsabiliza por omissões, erros técnicos ou erros editoriais contidos neste documento.

Microsoft é uma marca comercial registrada nos EUA do grupo de empresas Microsoft. Intel é marca comercial da Intel Corporation ou suas subsidiárias nos EUA e em outros países.

4AA7-3561PTL, novembro de 2018

