

# Las funciones de seguridad para ordenadores de HP podrían haber evitado el ataque audiovisual al Centro de Conferencias Suizo



## Informe oficial final relativo a la brecha de datos

### Sector

Locales para eventos.

### Objetivo

Auditar las prácticas de seguridad para proteger mejor el centro de conferencias y los datos confidenciales de los clientes.

### Enfoque

Se trabajó con el asesor de seguridad para analizar las prácticas de seguridad e identificar las áreas de preocupación.

### La IT importa

- Flota actualizada de ordenadores HP Elite con protección de malware integrada.
- Cierre de los puertos que no se necesitan para evitar un uso no autorizado.
- Complemento del kit de integración de gestión de HP integrado en Microsoft® System Center Configuration Manager (SCCM) para gestionar remotamente la flota de ordenadores.

### Los negocios importan

Se han actualizado las medidas de ciberseguridad para mejorar la protección de las instalaciones frente a ataques sofisticados y recuperar la confianza de los clientes.



## Información general

El Centro de Conferencias Suizo\*, situado cerca de Ginebra, celebra más de 230 eventos cada año. Como el mejor centro europeo para conferencias de negocios e importantes eventos de lanzamiento de productos, el centro ofrece servicios para líderes del sector de todo el mundo.

La gestión de las instalaciones ha realizado grandes inversiones en infraestructura tecnológica con el fin de ofrecer a sus clientes experiencias de conferencias enormemente personalizables en un espacio exquisito. Lamentablemente, no se implementaron las actualizaciones de seguridad correspondientes en la flota de ordenadores.

El 23 de abril de 2018, un hacker, que se hace llamar «The Wolf», se infiltró en un ordenador del centro de conferencias para interrumpir una presentación del más alto nivel que se estaba celebrando ante un público internacional. Después de la brecha, el Centro de Conferencias Suizo recurrió a su asesor de seguridad para encontrar y reparar sus vulnerabilidades de ciberseguridad.

## ¿Qué sucedió?

Como uno de los centros para eventos corporativos más importantes del mundo, el Centro de Conferencias Suizo destacaba en la preparación de experiencias increíbles para sus invitados; sin embargo, su ciberseguridad era bastante menos impresionante. «The Wolf» consiguió cargar malware en uno de los ordenadores del centro y sustituyó la presentación de un ponente por una propia. El personal de seguridad de IT de las instalaciones hizo todo lo posible por recuperar el control de su red en medio de la confusión creada en la sala de conferencias.

Los daños no se limitaron a la presentación. Los ingresos perdidos por reservas canceladas se estiman actualmente en 3,2 millones de euros.

## Cómo ocurrió

Lo único que tuvo que hacer «The Wolf» fue conectarse a un ordenador sin protección, consiguiendo que un empleado hiciera clic en un vínculo malicioso de un mensaje de correo electrónico o que descargara un archivo adjunto de aspecto inofensivo. O bien, dado que estaba físicamente cerca del ordenador, pudo introducir una unidad flash en un puerto USB sin vigilancia.

La flota de ordenadores del centro de conferencias suizo carecía de cualquier tipo de protección crucial capaz de poner en cuarentena el malware y detener este intento de infiltración. Aunque *habían* instalado software antivirus, ninguno de sus ordenadores contaba con funciones de seguridad integradas y aplicadas mediante hardware.

## Fortalecimiento de la seguridad

El Centro de Conferencias Suizo y su asesor de seguridad llevaron a cabo una auditoría completa de las medidas de ciberseguridad existentes. Ese análisis les llevó a actualizar la flota completa a ordenadores HP Elite, con protección de malware integrada y HP Sure Start Gen4, capaz de detectar automáticamente un ataque de la BIOS o episodio de corrupción, detenerlo y realizar la recuperación posterior, tanto durante el arranque como en tiempo de ejecución.<sup>1</sup>

Los nuevos ordenadores HP Elite también incluyen HP Sure Click, que proporciona protección reforzada al aislar físicamente cada pestaña del navegador, archivo PDF descargado o documento de Microsoft Office en una micro máquina virtual para evitar que el malware basado en web o procedente de archivos adjuntos de correo electrónico se extienda a otros dispositivos conectados a la red.<sup>2</sup>

El equipo de IT utiliza ahora el gestor de acceso a dispositivos de HP para gestionar los puertos y soportes extraíbles, así como el kit de integración de gestión de HP para Microsoft SCCM, con el fin de optimizar la seguridad y la administración de la BIOS en toda la flota.<sup>3</sup>

## Conclusión

El Centro de Conferencias Suizo se enfrentó a la pérdida de ingresos y confianza por parte de sus mejores clientes. No obstante, gracias a la implementación de ordenadores HP con medidas de seguridad exhaustivas y soluciones de gestión eficaces, el centro está ahora en posición de demostrar un compromiso más profundo con la ciberseguridad.

*\*El Centro de Conferencias Suizo es una empresa ficticia que sufre un ciberataque en la película de HP Studio: «THE WOLF: TRUE ALPHA».*

### Para obtener más información sobre las soluciones de HP:

Seguridad para ordenadores:  
<https://www8.hp.com/es/es/solutions/computer-security.html>  
Seguridad de la impresión:  
[www.hp.es/seguridad-impresion](http://www.hp.es/seguridad-impresion)

### Para ver las películas de «The Wolf», visite:

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

<sup>1</sup> HP Sure Start Gen4 se encuentra disponible en los productos HP Elite y HP Pro 600 equipados con procesadores Intel® o AMD de 8.ª generación.

<sup>2</sup> HP Sure Click se encuentra disponible en la mayoría de los ordenadores HP y es compatible con Microsoft® Internet Explorer y Chromium™. Entre los archivos adjuntos compatibles, se incluyen los archivos de Microsoft Office (Word, Excel y PowerPoint) y archivos PDF en modo de solo lectura, siempre y cuando se haya instalado Microsoft Office o Adobe Acrobat.

<sup>3</sup> El kit de integración de gestión de HP no se instala de forma predeterminada y se encuentra disponible en [hp.com/go/clientmanagement](http://hp.com/go/clientmanagement).

Suscríbase para recibir novedades  
[hp.com/go/getupdated](http://hp.com/go/getupdated)



Compartir con compañeros

© Copyright 2018 HP Development Company, L.P. La información que contiene este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de HP quedan establecidas en las declaraciones de garantía expresas que acompañan a dichos productos y servicios. Nada de lo aquí indicado debe interpretarse como una garantía adicional. HP no se responsabiliza de errores u omisiones técnicos o editoriales que puedan existir en este documento.

Microsoft es una marca comercial registrada en Estados Unidos por el grupo de compañías Microsoft. Intel es una marca comercial de Intel Corporation o de sus filiales en Estados Unidos y en otros países.

