Étude de cas

Le piratage de l'antivirus du Centre de conférences suisse aurait pu être empêché par les fonctionnalités de sécurité des ordinateurs de HP

Rapport de clôture officiel sur la violation de données

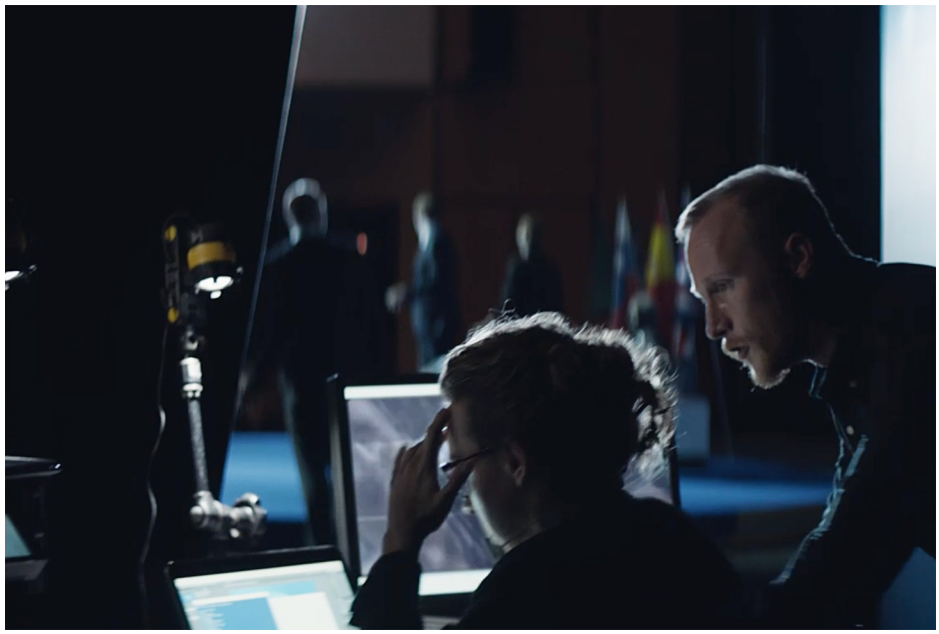
Industrie
Sites d'événements

Objectif
Vérifier les pratiques de sécurité afin de mieux protéger le Centre de conférences et les données sensibles du client

Approche
Travailler avec leur conseiller en sécurité pour analyser les pratiques de sécurité et identifier les domaines de préoccupation

Questions liées aux TI
- Mise à niveau du parc vers les ordinateurs HP Elite avec protections intégrées contre les logiciels malveillants
- Fermeture des ports non utilisés pour empêcher toute utilisation non autorisée
- Intégration du module complémentaire HP Manageability Integration Kit dans le Microsoft® System Center Configuration Manager (SCCM) pour gérer le parc d'ordinateurs à distance

Questions liées aux affaires
Mise à jour des mesures de cybersécurité pour mieux protéger les installations contre les attaques sophistiquées et regagner la confiance du client



Aperçu

Le Centre de conférences suisse*, situé près de Genève, accueille plus de 230 événements chaque année. En tant que site européen de choix pour les conférences d'affaires et les principaux événements de lancement de produits, il attire les leaders de l'industrie de partout dans le monde.

Le gestionnaire des installations a fait des investissements importants dans l'infrastructure technologique pour offrir aux clients une expérience de conférence hautement personnalisable dans un espace magnifiquement aménagé. Malheureusement, des mises à niveau de la sécurité d'une même ampleur n'ont jamais été entreprises pour le parc d'ordinateurs.

Le 23 avril 2018, un pirate informatique qui s'est fait connaître sous le nom de « The Wolf » a infiltré un ordinateur du Centre de conférences pour perturber une présentation de haut profil destiné à un public international. Après la violation de sécurité, le Centre de conférences suisse s'est tourné vers son consultant en sécurité pour trouver et réparer les vulnérabilités de cybersécurité.

Ce qui est arrivé

En tant que l'un des meilleurs sites pour événements d'entreprise du monde, le Centre de conférences suisse excellait dans la création d'expériences mémorables pour les invités, mais sa cybersécurité était moins impressionnante. The Wolf a téléversé un logiciel malveillant vers l'un des ordinateurs du Centre, puis a remplacé la présentation d'un orateur par la sienne. Le personnel de la sécurité informatique de l'établissement s'est dépêché pour reprendre le contrôle de son réseau au milieu du chaos dans la salle de conférence.

Les dommages ne se sont pas limités à une présentation ruinée. Les revenus perdus associés aux réservations annulées sont actuellement estimés à 3,2 M€.

Comment c'est arrivé

Tout ce que The Wolf a eu à faire était de s'immiscer dans un ordinateur non protégé en faisant cliquer un employé sur un lien malveillant dans un courriel ou en lui faisant télécharger une pièce jointe à l'air inoffensif. Ou, comme il était physiquement près de l'ordinateur, il aurait pu insérer une clé USB dans un port USB non surveillé.

Le parc d'ordinateurs du Centre de conférences suisse n'avait pas les protections essentielles qui auraient mis en quarantaine le code malveillant et qui auraient arrêté cette tentative d'infiltration. Alors qu'ils *avaient* un logiciel antivirus installé, aucun de leurs ordinateurs n'avait de fonctionnalités intégrées de sécurité de matériel renforcée.

Renforcement de la sécurité

Avec leur consultant en sécurité, le Centre de conférences suisse a mené une vérification approfondie de ses mesures de cybersécurité existantes. Cet examen a conduit à une mise à niveau du parc entier vers des ordinateurs HP Elite avec une protection intégrée contre les logiciels malveillants, y compris HP Sure Start Gen4, qui peut détecter, arrêter et récupérer automatiquement lors d'une attaque ou de la corruption du BIOS au démarrage et pendant l'exécution[1].

Les nouveaux ordinateurs HP Elite comprennent également HP Sure Click, qui fournit une protection renforcée en isolant physiquement chaque onglet du navigateur ou chaque fichier PDF ou Microsoft Office téléchargé dans une micromachine virtuelle (MV) pour empêcher des logiciels malveillants sur Internet ou des pièces jointes dans le courriel de se répandre vers d'autres périphériques connectés au réseau[2].

L'équipe informatique utilise maintenant HP Device Access Manager pour gérer les ports et les supports amovibles et la trousse HP Manageability Integration Kit pour SCCM de Microsoft pour simplifier la sécurité et l'administration du BIOS dans tout le parc d'appareils[3].

Conclusion

Le Centre de conférences suisse a subi des pertes de revenus et une diminution de la confiance de ses clients de haut profil envers la marque. Cependant, par le déploiement d'ordinateurs HP avec des mesures de sécurité complètes et des solutions de gestion efficaces, le Centre est maintenant en mesure de démontrer son engagement plus profond envers la cybersécurité.

** Le Centre de conférences suisse est une entreprise fictive ciblée par une cyberattaque dans le film de HP Studios : « THE WOLF: TRUE ALPHA. »*

Pour en savoir plus sur les solutions HP :
Sécurité des ordinateurs :
hp.com/go/computersecurity
Sécurité d'impression :
hp.com/go/reinventsecurity

Pour voir les films « The Wolf », visitez la page :
hp.com/thewolf

[1] HP Sure Start Gen4 est disponible sur les produits HP Elite et HP Pro 600 dotés de processeurs Intel® de 8e génération ou AMD.
[2] HP Sure Click est offert sur la plupart des ordinateurs HP et prend en charge Microsoft® Internet Explorer et Chromium™. Les pièces jointes prises en charge comprennent Microsoft Office (Word, Excel, PowerPoint) et les fichiers PDF en mode lecture seule, lorsque Microsoft Office ou Adobe Acrobat sont installés.
[3] La trousse HP Manageability Integration Kit n'est pas préinstallée, disponible à hp.com/go/clientmanagement.

Inscrivez-vous aux mises à jour
hp.com/go/getupdated

Partager avec des collègues

4AA7-3561FCCA, octobre 2018