Étude de cas

Quand l'aéroport de Londres a été pris pour cible par une cyberattaque destructrice, les imprimantes HP ont détecté la menace

Rapport de synthèse officiel sur la violation des données

Secteur d'activité
Aviation

Objectif
Identifier les failles dans les pratiques de cybersécurité et les combler

Approche
Élaboration d'un plan de sécurité complet en partenariat avec les experts en sécurité HP

Enjeux informatiques
- Mesures de sécurité appliquées aux terminaux de l'IdO
- Fonctionnalités de sécurité intégrées aux Imprimantes HP
- Amélioration de la surveillance de la sécurité à l'échelle du réseau

Enjeux commerciaux
Amélioration de la cybersécurité pour protéger les infrastructures internationales critiques et assurer la sécurité des voyageurs

Aperçu

L'aéroport de Londres* dessert plus de 300 000 passagers chaque jour qui voyagent vers 94 pays à travers le monde. Près de 50 000 personnes de 300 compagnies travaillent à l'aéroport, ce qui en fait une ville particulièrement dense.

Au fur et à mesure du développement de l'aéroport, son infrastructure est devenue de plus en plus connectée et automatisée. Les systèmes internes, du chauffage à l'éclairage, en passant par les imprimantes, sont maintenant sur le réseau de l'aéroport. L'impression, la numérisation et la copie sont effectuées par un parc de plus de 60 multifonctions HP réparties sur le site.

Le 23 avril 2018, le cyberterroriste connu uniquement sous le nom de « The Wolf » a utilisé les systèmes d'éclairage connectés de l'aéroport pour accéder au réseau et y diffuser des logiciels malveillants. Étant connu pour ses exploits dans l'utilisation de terminaux sous-sécurisés, les experts en sécurité informatique se sont immédiatement tournés vers les registres de menaces de leurs imprimantes HP Enterprise dans le cadre de l'enquête pour isoler et arrêter l'attaque. Étonnamment,
ces journaux contenaient des indices sur The Wolf quant à l'origine de l'intrusion. Par la suite, l'aéroport de Londres s'est tourné vers HP pour renforcer sécurité de ses terminaux.

Ce qui s'est passé

Une fois que The Wolf a découvert une faille, probablement en piégeant les courriers électroniques envoyés aux utilisateurs du réseau, il pouvait infecter le système d'éclairage de l'IdO avec des logiciels malveillants. Il pouvait alors étendre ses logiciels malveillants à travers le réseau, créant ainsi des points d'ancrage dans d'autres périphériques de terminaison non surveillés.

En cachant leur présence dans des dispositifs d'IdO non surveillés, l'équipe de The Wolf pouvait ne pas être découverte par les systèmes de surveillance du réseau pendant qu'ils développaient de multiples points de lancement pour une attaque de destruction massive.

La direction de l'aéroport a désespérément essayé de fermer de multiples systèmes tout en maintenant les infrastructures essentielles comme les avions et les passagers en mouvement.

Répondre à l'attaque

The Wolf avait été engagé pour attaquer le réseau de l'aéroport. Le personnel de sécurité informatique de l'aéroport *pensait que* le réseau de l'aéroport était bien protégé contre les pirates informatiques, mais il manquait de visibilité sur les menaces se cachant dans les dispositifs IdO.

Fort heureusement, les imprimantes HP Enterprise de l'aéroport comprenaient HP Connection qui a arrêté le logiciel malveillant lors d'une tentative suspecte de rabattage des serveurs de commande et de contrôle des pirates.

Ces opérations ont été capturées dans les registres des imprimantes. Une fois que le personnel informatique s'est rendu compte du problème, il a consulté les registres pour examiner les détails de l'attaque. Mais le temps presse lorsque des logiciels malveillants se propagent sur le réseau. Si le service de sécurité informatique avait relié les registres de détection des menaces des imprimantes à leur système de gestion des événements et informations de sécurité (SIEM), il aurait été alerté immédiatement lors de l'intrusion.

Une sécurité plus forte que jamais

Après la faille, le personnel informatique a passé en revue les pratiques de sécurité avec leur fournisseur de services d'impression gérés et les conseillers en sécurité HP.

En installant des imprimantes HP Enterprise, l'aéroport de Londres était déjà sur la bonne voie. Seules les imprimantes et multifonctions HP Enterprise offrent la détection d'intrusion en temps réel et HP Connection Inspector pour détecter et arrêter les logiciels malveillants pendant les opérations et forcer un redémarrage. Au démarrage, HP Sure Start vérifie le BIOS et peut s'autorétablir si le code a été compromis, tandis que la liste blanche vérifie le micrologiciel.

Le fournisseur de services d'impression gérés a déployé HP JetAdvantage Security Manager pour vérifier automatiquement les paramètres de sécurité à chaque fois qu'une imprimante est redémarrée, et réinitialise tout paramètre modifié. Le personnel de sécurité informatique de l'aéroport a également pris l'initiative de connecter les registres des imprimantes à leur outil SIEM. Contrairement aux imprimantes d'autres fabricants, les périphériques HP peuvent fournir des registres spécifiques aux menaces à de nombreux outils SIEM afin que le personnel informatique puisse recevoir des alertes en temps réel sur les éventuels incidents de sécurité. Les imprimantes HP deviennent ainsi des « yeux » inestimables sur leur réseau.

Conclusion

Grâce aux imprimantes HP Enterprise de l'aéroport et aux indices laissés par The Wolf, l'équipe de sécurité a pu isoler l'attaque assez rapidement pour éviter de perturber les opérations, de ternir l'image de marque et de payer des amendes pour non-conformité.

En employant des pratiques de sécurité renforcées et en tirant pleinement parti des fonctions de sécurité intégrées de ses imprimantes HP, l'aéroport a renforcé la sécurité dans l'ensemble du réseau.

**L'aéroport de Londres est une organisation fictive prise pour cible dans une grande attaque informatique dans le film de HP Studio, « The Wolf : TRUE ALPHA ».*

Pour plus d'informations sur les solutions HP :
Sécurité d'impression : hp.com/go/reinventsecurity
Sécurité des ordinateurs : hp.com/go/ComputerSecurity
Pour visionner les films « The Wolf », rendez-vous sur : hp.com/thewolf

Abonnez-vous
hp.com/go/getupdated

Partagez ce document avec des collègues

4AA7-3560FRE, septembre 2018