Étude de cas

Lorsque l'aéroport de Londres a été la cible d'une cyberattaque destructrice, les imprimantes HP ont détecté la menace

Rapport de clôture officiel sur la violation de données

Industrie
Aviation

Objectif
Identifier les maillons faibles dans les pratiques de cybersécurité et les corriger

Approche
Élaborer un plan de sécurité complet en partenariat avec des experts de la sécurité HP

Questions liées aux TI
- Mesures de sécurité installées aux points terminaux de l'IdO
- Fonctions de sécurité intégrées dans les imprimantes HP
- Amélioration de la surveillance de la sécurité dans tout le réseau

Questions liées aux affaires
Amélioration de la cybersécurité pour protéger l'infrastructure internationale essentielle et assurer la sécurité des passagers

Aperçu

Chaque jour, l'aéroport de Londres* sert plus de 300 000 passagers qui voyagent dans 94 pays autour du globe. Près de 50 000 personnes de près de 300 entreprises travaillent à l'aéroport, ce qui en fait pratiquement une ville en version condensée.

Alors que l'aéroport a grandi, son infrastructure est devenue de plus en plus connectée et automatisée. Les systèmes internes, comme le système de CVC, l'éclairage et les imprimantes sont maintenant connectés au réseau de l'aéroport. L'impression, la numérisation et la copie sont effectuées par un parc de plus de 60 imprimantes multifonctions de 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 diffuser son code malveillant sur celui-ci. Comme il est connu pour ses méfaits tirant profit des points terminaux insuffisamment sécurisés, les experts en sécurité des TI se sont immédiatement tournés vers les journaux de menaces de leurs imprimantes HP Enterprise dans le cadre de l'enquête visant à isoler et à arrêter l'attaque. Étonnamment, les journaux contenaient des indices du malfaiteur indiquant l'origine de l'intrusion. Ensuite, l'aéroport de Londres s'est tourné vers HP pour améliorer davantage la sécurité de ses points terminaux.

Ce qui est arrivé

Une fois que The Wolf a trouvé une vulnérabilité, probablement en envoyant des courriels d'hameçonnage aux utilisateurs sur le réseau, il a pu infecter le système d'éclairage de l'IdO avec un code malveillant. Ensuite, il a pu répandre son code malveillant à travers le réseau, pouvant alors s'implanter dans d'autres périphériques de points terminaux non surveillés.

En cachant leur présence dans les appareils de l'IdO non surveillés, les membres de l'équipe du Wolf pouvaient passer inaperçus des systèmes de surveillance du réseau pendant qu'ils mettaient en place de multiples points de lancement pour une attaque destructive de grande envergure.

La gestion de l'aéroport a désespérément tenté d'arrêter de multiples systèmes tout en gardant l'infrastructure essentielle en fonction, comme la circulation des avions et des passagers.

Réponse à l'attaque

The Wolf avait été embauché pour attaquer le réseau de l'aéroport. Le personnel de sécurité de l'aéroport *croyait* 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 périphériques de l'IdO.

Heureusement, les imprimantes HP Enterprise de l'aéroport étaient dotées de HP Connection Inspector, qui a arrêté le code malveillant lorsqu'il a effectué des tentatives suspectes de communication avec le serveur de commande et de contrôle des pirates.

Les actions ont été enregistrées dans les journaux syslog de l'imprimante. Une fois que les employés du service informatique ont réalisé que quelque chose ne tournait pas rond, ils ont vérifié les fichiers syslog pour obtenir plus de détails sur l'attaque. Toutefois, le temps est de la première importance lorsqu'un code malveillant se répand dans le réseau. Si le personnel de sécurité informatique avait connecté les journaux syslog de détection de menaces des imprimantes au système de gestion d'information et d'événements de sécurité (SIEM), l'alerte aurait été donnée immédiatement lorsque l'intrusion s'est produite.

Une sécurité plus solide que jamais

Après la violation de sécurité, le personnel informatique a revu les pratiques de sécurité avec le 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 les imprimantes multifonctions HP Enterprise offrent la détection des intrusions pendant le fonctionnement et HP Connection Inspector pour détecter et arrêter les logiciels malveillants pendant le fonctionnement et forcer un redémarrage. Au démarrage, HP Sure Start vérifie le BIOS, qui peut s'autoguérir 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 chaque fois qu'une imprimante est redémarrée, et réinitialise tout paramètre ayant été modifié.

Le personnel de sécurité de l'aéroport a également connecté les syslog d'imprimante à l'outil SIEM. Contrairement aux imprimantes d'autres fabricants, les périphériques HP peuvent fournir des journaux spécifiques aux menaces à de nombreux outils SIEM pour que le personnel puisse obtenir des alertes en temps réel lors des incidents de sécurité. Cela donne le rôle de « sentinelle » inestimable aux imprimantes HP sur leur réseau.

Conclusion

Grâce aux imprimantes HP Enterprise de l'aéroport et aux indices laissés par The Wolf, l'équipe de sécurité a été en mesure d'isoler l'attaque assez rapidement pour éviter de perturber les opérations, la publicité négative, les amendes pour non-conformité et l'endommagement de la marque.

En employant des pratiques de sécurité plus robustes et en tirant pleinement parti des caractéristiques de sécurité intégrées de leurs imprimantes HP, l'aéroport a renforcé la sécurité dans tout le réseau.

** L'aéroport de Londres est une organisation fictive ciblée par une importante cyberattaque dans le film de HP Studios : « THE WOLF: TRUE ALPHA ».*

Pour en savoir plus sur les solutions HP :

Sécurité d'impression :
hp.com/go/reinventsecurity
Sécurité des ordinateurs :
hp.com/go/ComputerSecurity

Pour voir les films « The Wolf », visitez la page :

hp.com/thewolf

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

Partager avec des collègues

4AA7-3560FCCA, octobre 2018