Étude de cas

Les tests d'intrusion démontrent que la brèche dans la cybersécurité de Torvik Industries par aurait pu être stoppée par les imprimantes HP

Rapport de synthèse officiel sur la violation des données

Secteur d'activité
Logistique

Objectif
Analyser et supprimer les zones de vulnérabilité du réseau

Approche
Tests d'intrusion pour trouver les failles qui ont mené à l'attaque

Constatations et recommandations
- Inciter les utilisateurs à la méfiance vis-à-vis des courriers électroniques suspects et de l'impression de pièces jointes
- Déployer des imprimantes HP avec détection des menaces
- Configurer la sécurité de tous les terminaux, y compris l'infrastructure qui a été déplacée ou qui se trouve dans des emplacements temporaires

Enjeux commerciaux
Appliquer des mesures de sécurité renforcées pour éviter l'arrêt des opérations et améliorer l'image de marque. Améliorer les politiques de surveillance des terminaux sur le réseau dans les emplacements temporaires

Aperçu

Torvik Industries* expédie 8 millions de conteneurs chaque année. Pour 22 000 fabricants et grossistes, Torvik est le lien vital entre les produits et les gens du monde entier. Les actifs de l'entreprise comprennent des chantiers maritimes, des navires, des entrepôts et toute la technologie qui soutient le vaste réseau de Torvik.

L'infrastructure technologique a eu du mal à s'adapter au développement continu de l'entreprise. Bien que le service de sécurité informatique ait configuré les serveurs de l'entreprise, la sécurité de certaines imprimantes des bureaux satellites ou des emplacements temporaires n'est pas gérée.

Le 23 avril 2018, le cyberterroriste connu sous le nom de The Wolf a utilisé une imprimante non sécurisée pour saboter les opérations de Torvik Industries, des ordinateurs aux grues, en passant par les porte-conteneurs. Leur conseiller en sécurité a utilisé des tests d'intrusion pour analyser l'événement et a formulé des recommandations pour accroître la sécurité et la formation du personnel.

Ce qui s'est passé

Les dirigeants de Torvik Industries avaient l'habitude de faire la pluie et le beau temps dans les transactions à enjeux élevés, ils ne s'attendaient donc pas à ce que des hackers infiltrent leur réseau si profondément au point de fermer les portiques de l'entreprise et rediriger les navires vers le large.

Il suffisait à The Wolf de compromettre une imprimante grand format sur un chantier de construction. Ensuite, il pouvait se déplacer latéralement à travers le réseau de l'entreprise vers les grandes cibles dans les opérations de l'entreprise. Très rapidement, cette société de transport maritime de premier plan a dû faire face à des perturbations opérationnelles massives, à une surveillance internationale intense et à des milliers de clients insatisfaits.

Comment c'est arrivé

Le service de sécurité informatique de l'entreprise pensait être protégé. Leurs équipes techniques et logistiques surveillaient constamment les opérations mondiales à la recherche de problèmes de sécurité potentiels. Ils avaient même mis en place des procédures de sécurité pour des terminaux tels que les imprimantes. Mais ils ont négligé quelque chose : la configuration de la sécurité d'une imprimante grand format stationnée temporairement dans une remorque de chantier.

Le pirate n'avait même pas besoin d'accéder directement à l'imprimante - il lui suffisait d'envoyer un courrier électronique avec une pièce jointe PDF à l'employé de Torvik chargé de l'impression des documents grand format. Ce PDF contenait un fichier Postscript caché, qui pouvait s'ouvrir et s'exécuter tout seul lorsque le fichier PDF était envoyé à l'imprimante. Une fois que l'employé a envoyé le travail d'impression, le logiciel malveillant s'est introduit dans l'imprimante, puis s'est répandu dans le réseau. En copiant un logiciel malveillant dans une pièce jointe d'apparence innocente, le hacker a contourné les outils de lutte contre les logiciels malveillants des ordinateurs de l'entreprise.

L'intrusion a été possible parce que l'imprimante grand format n'était pas dotée d'une sécurité intégrée, telle que la détection des menaces. De plus, l'entreprise n'a pas réussi à surveiller et à gérer la configuration de chaque imprimante de son parc, comme celles placées temporairement dans des bureaux satellites.

Réparation de la faille

Torvik Industries a retenu les services d'une société de tests d'intrusion de premier plan pour effectuer une analyse approfondie de la cybersécurité de l'organisation.

L'équipe des tests d'intrusion a recommandé l'installation d'imprimantes HP avec des fonctions de sécurité intégrées, y compris la série HP DesignJet avec démarrage sécurisé et la liste blanche des micrologiciels. Ces fonctions aident l'imprimante à détecter les codes malveillants et à s'éteindre, puis à alerter le service informatique de la nécessité de réinstaller les micrologiciels légitimes HP.

Ils ont également recommandé d'utiliser la fonction Instant-On Security de HP JetAdvantage Security Manager, un logiciel de gestion de la sécurité pour l'ensemble du parc, pour appliquer automatiquement les politiques de sécurité dès que des périphériques sont ajoutés au réseau. HP Security Manager peut également créer des rapports de conformité qui affichent chaque Imprimante HP, même dans des endroits éloignés ou temporaires. Cela permet de démontrer que les configurations de sécurité du parc ont été maintenues.

En outre, le conseiller en sécurité a proposé un programme de formation pour aider les employés à reconnaître les courriers électroniques malveillants, et sensibiliser au sujet de l'impression de pièces jointes inconnues.

Conclusion

Torvik Industries est toujours sous le choc de l'impact causé par cette violation de la cybersécurité dans ses opérations, ainsi que par la divulgation des pratiques illégales de leur président. Alors que l'organisation cherche à prendre une nouvelle direction, l'orientation de la cybersécurité est claire : se tourner vers les imprimantes et les solutions HP aidera à déjouer l'attaque du prochain pirate.

**Torvik Industries est une société 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 :
HP DesignJet : hp.com/go/designjetsecurity
Sécurité d'impression : hp.com/go/reinventsecurity
Pour visionner les films « The Wolf », rendez-vous sur : hp.com/thewolf

Abonnez-vous sur
hp.com/go/getupdated

Partagez ce document avec des collègues

4AA7-3562FRE, septembre 2018