Étude de cas

Un test de pénétration montre que la violation de la cybersécurité de Torvik Industries par « The Wolf » aurait pu être arrêtée par les imprimantes HP

Rapport de clôture officiel sur la violation de données

Industrie
Expédition

Objectif
Analyser et résoudre les domaines de la vulnérabilité du réseau

Approche
Test de pénétration pour trouver les vulnérabilités qui ont mené à l'attaque

Conclusions et recommandations
- Éduquer les utilisateurs à se méfier de l'ouverture des courriels suspects et de l'impression des pièces jointes
- Déployer des imprimantes HP avec détection des menaces
- Configurer la sécurité de tous les points terminaux, y compris les unités déplacées ou dans des emplacements temporaires

Questions liées aux affaires
Appliquer des mesures de sécurité plus rigoureuses pour éviter les interruptions opérationnelles et améliorer la confiance en la marque. Améliorer les politiques de surveillance des points terminaux du réseau dans les emplacements temporaires.

Aperçu

Torvik Industries* expédie huit millions de conteneurs chaque année. Pour 22 000 fabricants et grossistes, Torvik est le lien vital entre les produits et les gens autour du globe. Le portefeuille de la société comprend des chantiers navals, des navires, des entrepôts et toute la technologie qui soutient le réseau entier de Torvik.

Alors que la société a grandi, son infrastructure technologique a eu de la difficulté à s'adapter. Bien que le personnel de sécurité des technologies a configuré les serveurs de la société, certaines imprimantes des bureaux satellites ou d'emplacements temporaires ne font pas l'objet de gestion de la sécurité.

Le 23 avril 2018, le cyberterroriste connu uniquement sous le nom « The Wolf » a utilisé une imprimante non sécurisée pour saboter les activités de Torvik Industries, dont les ordinateurs, les grues à conteneurs et les porte-conteneurs. Le conseiller en sécurité de la société a utilisé un test de pénétration pour analyser l'événement et a fourni des recommandations pour accroître la sécurité et la formation du personnel.

Ce qui est arrivé

Les membres de l'équipe de direction de Torvik Industries avaient l'habitude de prendre les décisions dans les situations à enjeux élevés, ils ne s'attendaient donc pas à ce que des pirates informatiques infiltrent leur réseau suffisamment profondément pour arrêter les grues à portique de la société et rediriger les navires vers le large.

Tout ce que The Wolf a eu à faire était de compromettre une imprimante grand format sur un chantier de construction. Il a pu ensuite se déplacer latéralement à travers le réseau de l'entreprise pour atteindre les importantes cibles des opérations de la société. En un instant, cette grande société d'expédition a connu des perturbations opérationnelles massives, a subi une attention internationale soutenue et a rendu furieux des milliers de clients.

Comment c'est arrivé

Le personnel de sécurité des technologies de la société a pensé que celle-ci était protégée. Les équipes techniques et logistiques surveillaient constamment les opérations mondiales pour détecter des problèmes de sécurité potentiels. Elles avaient même des procédures de sécurité en place pour les points terminaux comme les imprimantes. Pourtant, ils avaient négligé quelque chose : la configuration de la sécurité d'une imprimante grand format installée temporairement dans une remorque de construction.

Le pirate informatique n'a même pas eu besoin d'accéder à l'imprimante directement, il a simplement envoyé un courriel contenant une pièce jointe en format PDF à l'employé de Torvik responsable de l'impression des documents grand format. Ce fichier PDF portait un fichier PostScript offensif caché, qui pouvait s'ouvrir et s'exécuter lors de l'envoi du fichier PDF à l'imprimante. Une fois que l'employé a envoyé la tâche d'impression à l'imprimante, le code malveillant s'est intégré à l'imprimante, puis s'est propagé dans tout le réseau. En attachant le code malveillant à la pièce jointe d'un courriel à l'apparence inoffensive, le pirate informatique a contourné le logiciel antivirus de l'ordinateur de la société.

La violation de sécurité a été possible parce que l'imprimante grand format n'avait pas de puissante mesure de sécurité intégrée, comme la détection des menaces. De plus, la société n'a pas surveillé et géré la configuration de chaque imprimante à travers le parc de périphériques, comme celles qui sont installées temporairement dans les bureaux satellites.

Réparation de la violation

Torvik Industries a engagé une grande firme de test de pénétration pour effectuer une analyse approfondie de la cybersécurité de l'organisation.

L'équipe de test de pénétration a recommandé d'installer des imprimantes HP avec des fonctionnalités de sécurité intégrées, y compris la série HP DesignJet avec Secure Boot et la fonction de liste blanche du micrologiciel. Ces fonctionnalités aident l'imprimante à détecter les codes malveillants et l'arrêtent, puis avertissent le service informatique de la nécessité de réinstaller le micrologiciel HP authentique.

Ils ont également recommandé d'utiliser la fonctionnalité Instant-On Security de HP JetAdvantage Security Manager, un logiciel de gestion de la sécurité à l'échelle du parc, afin d'appliquer automatiquement les politiques de sécurité dès que les périphériques sont ajoutés au réseau. HP Security Manager peut également créer des rapports de conformité qui montrent chaque imprimante HP, même celles des emplacements distants ou temporaires. Cela permet de démontrer que les configurations de sécurité du parc ont été maintenues.

En outre, le consultant en sécurité a suggéré un programme de formation pour aider les employés à reconnaître les courriels suspects et à éviter l'impression de pièces jointes inconnues.

Conclusion

Torvik Industries est encore en train de se remettre des impacts de la violation de la cybersécurité sur ses opérations, ainsi que de la publicité accrue sur les points de vue et les actes criminels non conventionnels de son président. Tandis que l'organisation cherche une nouvelle direction pour son leadership, l'objectif concernant la cybersécurité est clair : le passage aux imprimantes et aux solutions HP aidera à contrecarrer les plans du prochain pirate à la recherche d'une proie.

** Torvik Industries est une entreprise fictive ciblée par une importante cyberattaque dans le film de HP Studios : « THE WOLF: TRUE ALPHA. »*

Pour en savoir plus sur les solutions HP :
HP DesignJet: hp.com/go/designjetsecurity
Sécurité d'impression : hp.com/go/reinventsecurity

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

4AA7-3562FCCA, octobre 2018