Estudo de caso

Teste de invasão mostra que violação de cibersegurança feita pelo “The Wolf” na Torvik Industries poderia ter sido impedida por impressoras da HP

Relatório oficial resumido sobre a violação de dados

Setor
Transporte/Logística

Objetivo
Analisar e eliminar áreas de vulnerabilidade na rede

Abordagem
Teste de invasão para detectar as vulnerabilidades que levaram ao ataque

Conclusões e recomendações
- Instruir os usuários para que desconfiem antes de abrir e-mails suspeitos e imprimir anexos
- Implantar impressoras da HP com detecção de ameaças
- Configurar todos os pontos de extremidade para oferecer segurança, incluindo a infraestrutura que tenha sido deslocada ou que esteja em locais temporários

Questões de negócios
Aplique medidas mais fortes de segurança para evitar tempo de paralisação operacional e aumentar a confiança na marca. Melhore as políticas de monitoramento dos pontos de extremidade da rede em locais temporários.

Visão geral

A Torvik Industries* transporta oito milhões de contêineres por ano. Para 22.000 fabricantes e atacadistas, a Torvik é a conexão vital entre os produtos e as pessoas ao redor do mundo. Os ativos da empresa incluem estaleiros, embarcações, armazéns e toda a tecnologia que respalda a ampla rede da Torvik.

Conforme a empresa foi crescendo, a infraestrutura de tecnologia teve dificuldade para se adaptar. Embora a equipe de segurança de TI tenha configurado os servidores da empresa, algumas impressoras em escritórios satélites ou em locais temporários não têm a segurança gerenciada.

No dia 23 de abril de 2018, o ciberterrorista conhecido como “The Wolf” (O Lobo) usou uma impressora desprotegida para sabotar as operações da Torvik Industries, desde PCs a guindastes e a navios com contêineres. O consultor de segurança deles usou um teste de invasão para analisar o evento e forneceu recomendações para aumentar a segurança e o treinamento da equipe.

O que aconteceu

A liderança da Torvik Industries estava acostumada a ditar as regras em jogos de apostas altas — de modo que eles não esperavam que hackers se infiltrassem na rede de forma tão profunda que conseguissem desligar os guindastes e redirecionar os navios para o mar aberto.

Tudo o que o hacker The Wolf precisou fazer foi invadir uma impressora de grandes formatos em um local em obra. Depois ele foi conseguindo se movimentar pela rede da empresa, até os grandes alvos nas operações. Em pouco tempo, essa grande empresa de transporte teve interrupções operacionais em massa, intenso escrutínio internacional e milhares de clientes furiosos.

Como aconteceu

A equipe de segurança de TI da empresa pensou que eles estivessem protegidos. As equipes técnicas e de logística monitoravam constantemente as operações globais para detectar possíveis problemas de segurança. Elas dispunham inclusive de procedimentos de segurança para pontos de extremidade como impressoras. Mas teve uma coisa que elas subestimaram: a configuração de segurança de uma impressora de grandes formatos colocada temporariamente em um trailer em uma obra.

O hacker nem precisou ter acesso direto à impressora — bastou enviar um e-mail com um anexo em PDF para o funcionário da Torvik responsável pela impressão de documentos em grandes formatos. Esse PDF carregava um arquivo oculto em Postscript infectado, capaz de se abrir e rodar sozinho quando o PDF fosse enviado para a impressora. Quando o funcionário enviou o trabalho de impressão, o malware se instalou na impressora e depois se espalhou pela rede. Fazendo com que o malware pegasse carona em um anexo de e-mail com aspecto inocente, o hacker burlou o software antimalware dos PCs da empresa.

A violação foi possível porque a impressora de grandes formatos não tinha um recurso forte de segurança integrado, como detecção de ameaças. Além disso, a empresa acabou não monitorando nem gerenciando a configuração de todas as impressoras no conjunto de dispositivos — como os colocados temporariamente em escritórios satélites.

Recuperação após a violação

A Torvik Industries contratou uma grande empresa de teste de invasão para conduzir uma análise abrangente sobre a cibersegurança da organização.

A equipe de teste de invasão recomendou a instalação de impressoras da HP com recursos integrados de segurança, incluindo a série HP DesignJet com inicialização segura e lista de permissões de firmware. Esses recursos ajudam as impressoras a detectar códigos mal-intencionados e a se desligarem, depois alertarem a TI para a necessidade de reinstalar o firmware legítimo da HP.

Eles também recomendaram usar o recurso de segurança Instant-On do HP JetAdvantage Security Manager, um software de gerenciamento de segurança em todo o conjunto de dispositivos, para aplicar automaticamente as políticas de segurança assim que os dispositivos forem adicionados à rede. O HP Security Manager também é capaz de criar relatórios de conformidade que mostram cada impressora da HP, mesmo em locais remotos ou temporários. Isso ajuda a demonstrar que as configurações de segurança do conjunto de dispositivos foram mantidas.

Além disso, o consultor de segurança sugeriu um programa de treinamento para ajudar os funcionários a reconhecer e-mails suspeitos e evitar a impressão de anexos desconhecidos.

Conclusão

A Torvik Industries ainda está sofrendo com os impactos causados pela violação de cibersegurança nas operações, bem como com a grande publicidade negativa sobre os pontos de vista não convencionais do presidente da empresa e de seus atos criminosos. Enquanto a organização procura definir um novo rumo em termos de liderança, a direção em termos de cibersegurança é clara: recorrer a impressoras e soluções da HP para ajudar a caçar o próximo Lobo que aparecer.

**A Torvik Industries é uma empresa fictícia alvo de um ciberataque em grande escala no filme da HP Studios "THE WOLF: TRUE ALPHA."*

Para obter mais informações sobre as soluções da HP:
HP DesignJet: hp.com/go/designjetsecurity
Segurança da impressão: hp.com/go/reinventsecurity

Para assistir aos filmes "The Wolf", acesse:
hp.com/thewolf

Inscreva-se para obter atualizações
hp.com/go/getupdated

Compartilhe com colegas

4AA6-3562PTL, novembro de 2018