Caso prático

Teste de intrusão revela que o ataque de "The Wolf" à cibersegurança da Torvik Industries poderia ter sido impedido pelas impressoras HP

Relatório resumido oficial sobre o ataque

Setor de atividade
Transporte/Logística

Objetivo
Analisar e eliminar áreas de vulnerabilidade na rede

Abordagem
Realização de testes de intrusão para identificar as vulnerabilidades que permitiram a execução do ataque

Conclusões e recomendações
- Ensinar os utilizadores a desconfiar de e-mails e anexos de impressão suspeitos
- Implementar impressoras HP capazes de detetar ameaças
- Configurar todos os pontos finais relativamente a segurança, incluindo infraestruturas em localizações temporárias ou que tenham sido transferidas

A segurança é fundamental
Aplicação de medidas de segurança mais eficazes para evitar períodos de inatividade e melhorar a confiança na empresa. Melhoramento de políticas para monitorizar os pontos finais da rede em localizações temporárias.

Descrição geral

A Torvik Industries* transporta mais de 8 milhões de contentores por ano. Para 22 000 fabricantes e revendedores, a Torvik é a ponte de ligação vital entre os produtos e as pessoas em todo o mundo. Os ativos da empresa incluem, estaleiros de envio, navios, armazéns e toda a tecnologia que suporta a vasta rede da Torvik.

A empresa começou a sentir dificuldades em adaptar a sua infraestrutura tecnológica à medida que ia crescendo. Apesar de o pessoal de segurança de TI ter configurado os servidores da empresa, algumas impressoras em escritórios "satélite" ou localizações temporárias não são geridas em termos de segurança.

A 23 de abril de 2018, o ciberterrorista conhecido como "The Wolf" utilizou uma impressora desprotegida para sabotar as operações da Torvik Industries – desde computadores e gruas a navios de contentores. O seu consultor de segurança recorreu a testes de intrusão para analisar o evento e apresentou recomendações para reforçar a segurança e aprofundar a formação do pessoal.

O que aconteceu?

A administração da Torvik Industries estava habituada a ditar as regras em jogos de alto risco e, por isso, não estava à espera que os hackers se infiltrassem tão profundamente na sua rede a ponto de conseguirem desativar e encerrar os guindastes de pórtico da empresa e direcionar os navios para mar aberto.

Tudo o que The Wolf teve de fazer foi comprometer uma impressora para grandes formatos localizada num estaleiro de construção. Depois, conseguiu mover-se pela rede da empresa até chegar aos grandes alvos da empresa. Num instante, esta empresa de transportes líder a nível mundial sofreu graves consequências: fortes perturbações nas suas operações, escrutínio internacional intenso e milhares de clientes insatisfeitos e furiosos.

Como aconteceu?

O pessoal de segurança de TI da empresa pensava que estavam devidamente protegidos. As suas equipas técnicas e de logística monitorizavam constantemente operações globais quanto a potenciais problemas de segurança. Dispunham, inclusive, de procedimentos de segurança para pontos finais como impressoras. Mas esqueceram-se de algo: a configuração de segurança de uma impressora para grandes formatos temporariamente instalada num atrelado de construção.

O hacker nem sequer teve de aceder diretamente à impressora. Bastou-lhe enviar um e-mail com um anexo PDF para o funcionário da Torvik responsável pela impressão de documentos de grande formato. Esse PDF continha um ficheiro PostScript armadilhado que era capaz de se abrir e executar automaticamente quando o PDF foi enviado para a impressora. Assim que o funcionário enviou o trabalho de impressão, o malware incorporou-se na impressora e, em seguida, propagou-se pela rede. Ao carregar o malware num anexo de e-mail aparentemente inofensivo, o hacker contornou o software antimalware dos computadores da empresa.

O ataque foi possível porque a impressora para grandes formatos não incorporava segurança reforçada, como deteção de ameaças. Além disso,, a empresa falhou na monitorização e gestão da configuração de cada impressora em todo o parque, tais como aquelas temporariamente localizadas em escritórios "satélite".

Recuperação após a o ataque

A Torvik Industries solicitou a uma empresa líder especializada em testes de intrusão que realizasse uma análise exaustiva à cibersegurança da empresa.

A equipa especializada em testes de intrusão recomendou a instalação de impressoras HP com funcionalidades de segurança incorporadas, incluindo impressoras HP DesignJet com arranque seguro e whitelisting de firmware. Estas funcionalidades permitem à impressora detetar código malicioso e encerrar e, subsequentemente, alertar a equipa de TI para a necessidade de reinstalar firmware HP legítimo.

Também recomendaram a utilização de uma funcionalidade de segurança Instant-On do HP JetAdvantage Security Manager, um software de gestão de segurança em todo o parque, para aplicar automaticamente políticas de segurança assim que dispositivos são adicionados à rede. O HP Security Manager consegue também gerar relatórios de conformidade que revelam cada impressora HP, mesmo em localizações remotas ou temporárias. Isto ajuda a demonstrar que as configurações de segurança do parque foram devidamente mantidas.

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

Conclusão

A Torvik Industries ainda está a sofrer os impactos do ataque à cibersegurança nas suas operações, bem como críticas negativas relativas a abordagens polémicas e a atos criminosos do seu presidente. Enquanto a organização procura definir um novo rumo em termos de administração e liderança, o rumo em termos de cibersegurança é claro: recorrer a impressoras e soluções da HP ajuda a caçar o próximo Lobo.

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

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

Para ver os filmes "The Wolf":
hp.com/thewolf

Registe-se para receber atualizações
hp.com/go/getupdated

Partilhar com colegas

4AA7-3562PTE. Agosto de 2018.