Caso prático

Quando o Aeroporto de Londres foi alvo de um ciberataque destruidor, as impressoras da HP detetaram a ameaça

Relatório resumido oficial sobre o ataque

Setor de atividade
Aviação

Objetivo
Identificar elos fracos nas práticas de cibersegurança e eliminá-los

Abordagem
Desenvolvimento de um plano de segurança abrangente em parceria com especialistas em segurança da HP

As TI são fundamentais
- Aplicação de medidas de segurança a pontos finais da IdC (Internet das Coisas)
- Ativação de funcionalidades de segurança incorporadas nas impressoras HP
- Monitorização melhorada da segurança em toda a rede

A segurança é fundamental
Reforço da cibersegurança para proteger infraestruturas críticas internacionais e assegurar a segurança dos passageiros

Descrição geral

O Aeroporto de Londres* serve mais de 300 000 passageiros por dia que viajam para 94 países de todo o mundo. Aproximadamente 50 000 pessoas de 300 empresas trabalham no aeroporto, tornando-o praticamente numa cidade condensada.

À medida que o aeroporto cresceu, a sua infraestrutura tornou-se cada vez mais ligada e automatizada. Sistemas internos, desde AVC (aquecimento, ventilação e climatização) a iluminação e impressoras, integram agora a rede do aeroporto. A impressão, digitalização e cópia são efetuadas por um parque de mais de 60 multifunções HP distribuídas por todo o complexo.

A 23 de abril de 2018, o ciberterrorista conhecido apenas como "The Wolf" aproveitou-se dos sistemas de iluminação do aeroporto para aceder à rede e propagar o seu malware através da mesma. Sendo ele conhecido por explorar pontos finais indevidamente protegidos, os especialistas em segurança de TI recorreram imediatamente aos registos de ameaças das suas impressoras HP Enterprise como parte da investigação para isolar e parar o ataque. Surpreendentemente, os registos continham pistas deixadas por The Wolf quanto à origem da intrusão. Subsequentemente, o Aeroporto de Londres recorreu à HP para reforçar ainda mais a segurança dos seus pontos finais.

O que aconteceu?

Assim que The Wolf identificou uma vulnerabilidade, provavelmente através de e-mails de phishing destinados a utilizadores na rede, conseguiu infetar o sistema de iluminação da IdC com malware. A partir daí, pôde propagar o seu malware através da rede criando bases de apoio à propagação noutros dispositivos de ponto final não monitorizados.

Ocultando a sua presença em dispositivos da IdC não monitorizados, a equipa de The Wolf conseguiu contornar os sistemas de monitorização da rede enquanto desenvolvia várias bases de lançamento para um ataque de destruição maciça.
A administração do aeroporto viu-se a braços com uma tentativa desesperada de encerrar vários sistemas mantendo, em simultâneo, infraestruturas críticas como aviões em pleno voo e passageiros em pleno movimento.

A resposta ao ataque

The Wolf tinha sido contratado para atacar a rede do aeroporto. O pessoal de segurança de TI do aeroporto *pensou* que a rede do aeroporto estava devidamente protegida contra hackers, mas tinham falta de visibilidade quanto a ameaças ocultas em dispositivos da IdC.

Felizmente, as impressoras HP Enterprise do aeroporto integravam
o HP Connection Inspector, que parou o malware quando este tentava estabelecer ligação aos servidores de controlo e comando dos hackers.

As ações foram identificadas nos syslogs da impressora. Assim que o pessoal de segurança de TI se apercebeu de que algo estava errado, verificaram os syslogs para obter detalhes sobre o ataque. O tempo é crucial quando existe malware a propagar-se pela rede. Se o pessoal de segurança de TI tivesse ligado os syslogs de deteção de ameaças das impressoras ao seu sistema de SIEM (Security Information and Event Management), poderiam ter sido imediatamente notificados da ocorrência da intrusão.

A melhor segurança de sempre

Após o ataque, o pessoal de segurança de TI analisou as suas práticas de segurança junto do seu fornecedor de serviços de impressão e de HP Security Advisors.

Ao instalar impressoras HP Enterprise, o Aeroporto de Londres passou a estar no caminho certo em termos de segurança. Apenas as impressoras e multifunções HP Enterprise oferecem deteção de intrusões em tempo de execução e o HP Connection Inspector para detetar e parar malware durante operações e forçar o reinício do dispositivo. No arranque, o HP Sure Start verifica o BIOS e executa a autorrecuperação se o código tiver sido comprometido, enquanto a lista de permissões (whitelist) verifica o firmware.

O fornecedor de serviços de impressão implementou
o HP JetAdvantage Security Manager para verificar automaticamente as definições de segurança de cada vez que uma impressora é reiniciada e para repor quaisquer definições alteradas.
O pessoal de segurança de TI do aeroporto também decidiu ligar os syslogs da impressora à sua ferramenta de SIEM. Ao contrário das impressoras de outros fabricantes, os dispositivos da HP são capazes de fornecer relatórios específicos de ameaças a muitas ferramentas de SIEM por forma a que o pessoal de segurança de TI consiga receber alertas em tempo real sobre eventuais incidentes de segurança. Isto transforma as impressoras HP em "olhos" inestimáveis na sua rede.

Conclusão

Graças às impressoras HP Enterprise do aeroporto e às pistas deixadas por The Wolf, o pessoal de segurança de TI conseguiu isolar rapidamente o ataque para evitar interrupções nas operações, publicidade negativa, multas por inconformidade em termos de segurança e danos à imagem do aeroporto.

Aplicando práticas de segurança mais eficazes e tirando total partido das funcionalidades de segurança incorporadas das impressoras HP, o aeroporto reforçou significativamente a segurança em toda a rede.

**O Aeroporto de Londres é uma organização 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:
Segurança de impressão:
hp.com/go/reinventsecurity
Segurança informática:
hp.com/go/ComputerSecurity

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

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

Partilhar com colegas

4AA7-3560PTE. Agosto de 2018.