Estudo de caso

Quando o aeroporto de Londres foi alvo de um ciberataque destrutivo, as impressoras da HP detectaram a ameaça

Relatório oficial resumido sobre a violação de dados

Setor
Aviação

Objetivo
Identificar elos fracos em práticas de cibersegurança e cuidar deles

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

Questões de TI
- Aplicação de medidas de segurança em pontos de extremidade IoT
- Ativação de recursos de segurança embutidos em impressoras HP
- Maior monitoramento da segurança em toda a rede

Questões de negócios
Melhora na cibersegurança para proteger infraestrutura internacional importante e manter a segurança dos passageiros

Visão geral

Todos os dias, o aeroporto de Londres* atende a mais de 300.000 passageiros, que viajam para 94 países do mundo inteiro. Quase 50.000 pessoas de 300 empresas trabalham no aeroporto, o que faz com que ele seja praticamente uma cidade compacta.

Conforme o aeroporto foi crescendo, a infraestrutura foi ficando cada vez mais conectada e automatizada. Sistemas internos, desde refrigeração/aquecimento até iluminação e impressoras estão agora na rede do aeroporto. A impressão, a digitalização e a cópia são feitas por um conjunto de mais de 60 multifuncionais HP distribuídas por toda a área.

No dia 23 de abril de 2018, um ciberterrorista conhecido como “The Wolf” (O Lobo) usou os sistemas de iluminação conectados do aeroporto para acessar e infectar o malware pela rede. Como ele é conhecido por explorar pontos de extremidade desprotegidos, os especialistas em segurança de TI buscaram imediatamente os registros de ameaça das impressoras HP Enterprise como parte da investigação para isolar e interromper o ataque. Surpreendentemente, os logs traziam pistas do The Wolf sobre o local de origem da invasão. Em seguida, o aeroporto de Londres recorreu à HP para reforçar a segurança de pontos de extremidade.

O que aconteceu

Quando o The Wolf encontrou uma vulnerabilidade, provavelmente por meio de phishing em e-mails de usuários da rede, ele conseguiu infectar o sistema de iluminação IoT com malware. Depois ele conseguiu espalhar o malware pela rede, criando pontos de apoio em outros dispositivos de ponto de extremidade não monitorados.

Ao ocultar a própria presença em dispositivos IoT não monitorados, a equipe do The Wolf conseguiu passar despercebida pelos sistemas de monitoramento da rede enquanto desenvolvia diversos pontos de lançamento para um ataque maciço destrutivo.

A administração do aeroporto ficou desesperada tentando desligar vários sistemas, ao mesmo tempo mantendo a infraestrutura crítica, como aeronaves e passageiros, em movimento.

Resposta ao ataque

O hacker The Wolf tinha sido contratado para atacar a rede do aeroporto. A equipe de segurança de TI do aeroporto *pensava* que a rede do aeroporto estava bem protegida contra hackers, mas faltava visibilidade para ameaças ocultas em dispositivos IoT.

Felizmente, as impressoras HP Enterprise do aeroporto incluíam o HP Connection Inspector, que interrompeu o malware quando ele fez tentativas suspeitas com uso de recursos "call home" para os servidores de controle e comandos dos hackers.

As ações foram registradas nos syslogs da impressora. Quando a equipe de TI percebeu que havia algo errado, procurou nos syslogs detalhes sobre o ataque. Mas o tempo é de suma importância quando o malware está se espalhando pela rede. Se a equipe de segurança de TI tivesse conectado os syslogs de detecção de ameaças da impressora ao sistema de monitoramento de eventos e informações de segurança (SIEM), teria sido imediatamente alertada sobre a ocorrência da invasão.

Segurança mais forte que nunca

Após a violação, a equipe de TI revisou as práticas de segurança junto aos prestadores de serviço de impressão gerenciada e aos consultores de segurança da HP.

Ao instalar as impressoras HP Enterprise, o aeroporto de Londres já estava no caminho certo. Só as impressoras e multifuncionais HP Enterprise oferecem detecção de invasão em tempo de execução e o HP Connection Inspector para detectar e interromper malware durante as operações e forçar uma reinicialização. Durante a reinicialização, o HP Sure Start verifica o BIOS e pode fazer o reparo automático se o código estiver comprometido, enquanto a lista de permissões verifica o firmware.

O prestador de serviços de impressão gerenciados implantou o HP JetAdvantage Security Manager para verificar automaticamente as configurações de segurança todas as vezes em que a impressora é reinicializada e restaurou todas as configurações alteradas.

A equipe de segurança de TI do aeroporto também conectou os syslogs da impressora à ferramenta SIEM. Diferente de impressoras de outros fabricantes, os dispositivos HP podem fornecer logs de ameaças específicas a muitas ferramentas SIEM para que a equipe de TI possa receber alertas em tempo real sobre possíveis incidentes de segurança. Isso faz com que as impressoras HP sejam "olhos" de valor inestimável para a rede.

Conclusão

Por causa das impressoras HP Enterprise no aeroporto e das pistas deixadas pelo hacker The Wolf, a equipe de segurança conseguiu isolar o ataque com rapidez suficiente para evitar a interrupção das operações, publicidade negativa, multas pela falta de conformidade e danos à marca.

Ao empregar práticas de segurança mais fortes e tirar o máximo proveito dos recursos de segurança integrados das impressoras HP, o aeroporto reforçou 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 Studio "THE WOLF: TRUE ALPHA."*

Para obter mais informações sobre as soluções da HP:
Segurança da impressão:
hp.com/go/reinventsecurity
Segurança de PCs:
hp.com/go/ComputerSecurity

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

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

Compartilhe com colegas

4AA7-3560PTL, novembro de 2018