Anatomia de um ataque complexo

Prof. Calvetti

Integrantes: Otavio Teles, Juliana Gomes, Maynara Olinda

Introdução:

O presente trabalho tem como objetivo analisar um caso fictício de ataque cibernético envolvendo a empresa Opticon, atuante no setor de carros autônomos. A partir do vídeo apresentado, foi possível identificar as vulnerabilidades exploradas, os tipos e técnicas de ataque utilizados, bem como a motivação do atacante. Esse estudo busca demonstrar como pequenas falhas de segurança podem resultar em grandes prejuízos corporativos.

Vulnerabilidades exploradas:

Durante o ataque, diversas vulnerabilidades de segurança foram exploradas pelo invasor. Essas falhas estavam relacionadas tanto a sistemas externos quanto à rede interna da empresa, incluindo más práticas de configuração e ausência de monitoramento adequado. Entre as principais vulnerabilidades, destacam-se:

- Site desatualizado (do boliche), com brechas que permitiram a execução de um ataque de injeção de iframe.

- Rede interna sem segmentação, configurada como uma rede plana, permitindo acesso irrestrito a diferentes setores (RH, jurídico, P&D).

- Dispositivos IoT inseguros, como o termostato conectado à rede corporativa, ainda com senha padrão de fábrica.

- Falta de monitoramento completo: embora tenha sido feita uma varredura após a detecção inicial, não houve escaneamento total da rede.

Tipos e técnicas de ataque utilizados:

O invasor utilizou uma combinação de técnicas conhecidas no campo da cibersegurança, explorando falhas já documentadas e aproveitando-se da falta de boas práticas de defesa por parte da Opticon. Os métodos identificados foram:

- Iframe Injection Attack: inserção de código malicioso em site vulnerável, permitindo a infecção de usuários que acessassem a página.

- Malware: instalação de software malicioso no laptop de um funcionário da Opticon, após este visitar o site comprometido.

- Movimento lateral na rede: exploração de dispositivos conectados, como o termostato, para ganhar acesso a toda a rede interna da empresa.

- Exfiltração de dados: cópia e transferência de documentos sigilosos, incluindo blueprints e arquivos de pesquisa.

- Ataque de destruição e limpeza: o invasor criptografou discos, apagou backups e corrompeu arquivos para dificultar a recuperação dos sistemas e ocultar rastros.

Motivação do cracker:

A motivação principal do invasor foi financeira, uma vez que ele admitiu ter recebido 75 bitcoins pela venda dos arquivos roubados. Além disso, a destruição deliberada de dados e backups indica

também uma tentativa clara de dificultar a investigação e apagar vestígios de suas ações, demonstrando preocupação em encobrir o ataque.

Conclusão:

Este caso evidencia como um conjunto de falhas aparentemente simples pode abrir espaço para ataques complexos e altamente prejudiciais. A ausência de práticas básicas de segurança, como segmentação de rede, atualização de sistemas e monitoramento adequado, possibilitou que um invasor externo tivesse acesso a informações sensíveis da empresa. Além disso, a utilização de dispositivos IoT mal configurados contribuiu para ampliar a superfície de ataque. Assim, conclui-se que a segurança da informação deve ser tratada como prioridade estratégica, exigindo investimentos contínuos em prevenção, monitoramento e conscientização dos colaboradores.