ATAQUE DA PROSPECT MEDICAL HOLDINGS

A rede de saúde norte americana, *Prospect Medical Holdings* foi vítima de um ataque cibernético em agosto de 2023, onde os cibercrimionosos coletaram e bloquearam os dados confidenciais de pacientes, que são de extrema importância, e alegaram só desbloquearem mediante resgate.

1. Tipo de ataque: Foi um ataque do tipo *RANSOMWARE* (um tipo de *malware)* que hackers instalam na sua rede ou computador que coletam os dados do dispositivo de uma vítima, ameaçando mantê-los bloqueados a menos que a vítima pague um resgate ao invasor-hacker);
2. Impactos: Os hospitais e instalações foram obrigados a ficar off-line, desmarcar procedimentos cirúrgicos, transferir pacientes e adotar um sistema de controle manual, até a volta do digital. Ao total 16 hospitais e mais de 165 clínicas e ambulatórios foram afetados.
3. Vulnerabilidade: Ocorreu devido à falta de treinamento em segurança digital para os funcionários da saúde e uso de software obsoletos.
4. Tipos de proteção: Manter sempre programas e sistemas operacionais atualizados, não conectar dispositivos USB desconhecidos, não abrir e-mail suspeito.

ATAQUE AO PARLAMENTO FINLANDÊS

Ocorreu em agosto de 2022, enquanto o parlamento estava em sessão para ingressar na OTAN (Organização do Tratado do Atlântico Norte – NATO, *North Atlantic Treaty Organization*).

O intuito do ataque foi afirmado por uma retaliação pela entrada da Finlândia na OTAN, parte de uma campanha coordenada por hackers (NoName057- especializados em DDoS), patrocinados pelo estado russo para interromper os sites do governo finlandês, desativando funções e publicando informações falsas.

1. Tipo de Ataque: O ataque foi em DDoS (*Distribuited Denial of Service* – Ataque de negação de serviço distribuído), bloqueia temporariamente o acesso a um site, mas não causa destruição permanente - é maior em escala. Ele utiliza milhares (até milhões) de dispositivos conectados para atingir sua meta. O grande volume dos dispositivos usados torna a DDoS muito mais difícil de lutar.

2. Vulnerabilidade explorada (CVE e Código):

- Avaliação de risco: realizar regularmente avaliações de risco e auditorias em seus dispositivos, servidores e rede;

- Diferenciação de tráfego: saber como é o tráfego normal da rede, tais como desempenho de rede inexplicavelmente lento, conectividade com pontos, falhas intermitentes na web, fontes de tráfego incomuns, ou uma onda de spam; Fazer um Plano de Resposta de Negação de Serviço; Garantir uma infraestrutura resistente; Refúgio na Nuvem; Implantar Soluções de Proteção DDoS e Threat Intelligenc.

3. Impactos e Prejuízos (estimado): A função deste ataque é sobrecarregar os dispositivos, serviços e a rede de seu alvo pretendido com tráfego de internet falso, tornando-os inacessíveis ou inúteis para usuários legítimos.

4. Tipo de Proteção que poderia ter sido aplicado para evita-lo: Firewall de Aplicativos Web (WAF), Mitigação de DDoS sempre ativada.

Sites de pesquisas:

Site da Fortinet - Ataques cibernéticos recentes: 2023 e 2022:

https://www.fortinet.com/br/resources/cyberglossary/recent-cyber-attacks

Notícias:

https://www.dn.pt/internacional/nato-parlamento-finlandes-alvo-de-ataque-informatico-por-hackers-pro-russos-16121292.html/

O que é DDoS:

https://www.fortinet.com/br/resources/cyberglossary/ddos-attack

Prevenção:

https://securityleaders.com.br/5-melhores-praticas-para-a-prevencao-de-ataques-ddos/

https://www.cloudflare.com/pt-br/learning/ddos/how-to-prevent-ddos-attacks/

https://securelist.com/ddos-attacks-in-q2-2020/98077/

Vulnerabilidade:

https://www.fortinet.com/br/resources/cyberglossary/cve

https://www.redhat.com/pt-br/topics/security/what-is-cve

Informações sobre a empresa, ataque, impactos e vulnerabilidade:
https://www.fortinet.com/br/resources/cyberglossary/recent-cyber-attacks

https://www.welivesecurity.com/pt/ameacas-digitais/ataque-de-ransomware-afeta-a-operacao-de-16-hospitais-nos-eua/

Tipos de proteção contra um ransomware:
https://www.kaspersky.com.br/resource-center/threats/how-to-prevent-ransomware