PESQUISA ATAQUES CIBERNÉTICOS

Lucas Augusto de Oliveira Barbosa RA: 824126373

Denis Lucas Ribeiro Vaz RA: 824216428

ATAQUE AO SISTEMA DE SAÚDE DA PREFEITURA DO RIO DE JANEIRO

- O ataque ocorreu em junho de 2021.

TIPO DO ATAQUE:

Foi um ataque de ransomware. Esse tipo de ataque se caracteriza por criptografar dados e exigir um resgate em troca da chave de descriptografia.

DESCRIÇÃO DO ATAQUE

Os atacantes atingiram os sistemas de TI da Prefeitura do Rio de Janeiro, bem como vários setores do sistema de saúde. O ransomware bloqueou os agendamentos, registros de pacientes e até mesmo informações sobre campanhas de vacinação. Para manter o funcionamento básico dos serviços de saúde, a prefeitura foi obrigada a interromper vários serviços e recorrer a processos manuais.

VULNERABILIDADES EXPLORADAS:

O ataque buscou uma falha em sistemas de segurança desatualizados e técnicas de segurança cibernética inadequadas. Muitos dos sistemas afetados não estavam atualizados com os patches de segurança mais recentes, o que permitiu a exploração. Além disso, os atacantes foram mais fáceis de obter acesso devido às práticas inadequadas de controle de acesso e gerenciamento de senhas.

IMPACTOS E PREJUIZOS:

Interrupção de serviços: A operação dos serviços de saúde foi gravemente impactada, com consequências diretas na capacidade de atendimento a pacientes e na organização de campanhas de vacinação.

Costos financeiros: A adoção de medidas de segurança emergenciais e recuperação de dados representaram custos significativos para a prefeitura. Além disso, a perda de produtividade e os resgates eram preocupações potenciais.

Reputação: A confiança pública foi abalada, o que prejudicou a percepção da eficácia e segurança dos serviços da prefeitura.

O QUE PODERIA SER FEITO PARA EVITAR:

Atualização de Sistemas e Patches: É fundamental que todos os sistemas estejam atualizados com os patches de segurança mais recentes. Os atacantes frequentemente exploram vulnerabilidades conhecidas que poderiam ter sido corrigidas por atualizações.

Educação e treinamento: Os ataques cibernéticos podem ser menos eficazes se os funcionários forem treinados em práticas seguras de uso de sistemas.

Implementação de Medidas de Segurança: Proteger-se contra ataques pode ser facilitado por meio do uso de medidas de segurança robustas, como autenticação multifatorial, criptografia de dados e sistemas de detecção de intrusões.

Backups Regulares: Fazer backups regulares e testá-los regularmente garante que os dados possam ser restaurados sem gastar dinheiro em resgates em caso de ataques.

Monitoramento e Resposta a Incidentes: Criar um plano de resposta a incidentes e ter uma equipe comprometida. O monitoramento da segurança cibernética pode ajudar a detectar e mitigar ataques antes que causem danos significativos.

Para proteger empresas e serviços essenciais contra ataques futuros, é necessário investir em práticas preventivas e segurança cibernética.

- ATAQUE DoS e DDoS

A AWS divulgou que mitigou um gigantesco ataque de DDoS em fevereiro de 2020. No seu ápice, o ataque disparou um tráfego de entrada a uma taxa de 2,3 terabits por segundo (Tbps). A AWS não divulgou a qual cliente o ataque foi direcionado.

Os ataques de DDoS são bem-sucedidos graças ao uso de vários sistemas de computadores comprometidos como fontes de tráfego do ataque. As máquinas usadas indevidamente podem ser computadores e outros recursos de rede, como dispositivos de IoT.

Os invasores responsáveis usaram servidores web sequestrados com Protocolo de Acesso Leve a Diretórios sem Conexão (CLDAP). O CLDAP é um protocolo para diretórios de usuários. Trata-se de uma alternativa ao LDAP, uma versão mais antiga do protocolo. O CLDAP tem sido usado em diversos ataques DDoS nos últimos anos.

O relatório não identificou o cliente visado da AWS, mas disse que o ataque foi realizado usando servidores web CLDAP sequestrados e causou três dias de "ameaça elevada" para sua equipe do AWS Shield.

Como funciona um anti-DDoS? É um serviço de monitoramento que detecta ataques volumétricos na sua rede, separando o tráfego legítimo do ilícito.

Com ele, você também recebe relatórios que mostram como o tráfego da sua operadora se comportou nos últimos meses.