ATIVIDADE 03

Docente: Robson Calvetti
UC: Sistemas Computacionais e Segurança – SCS

Marinna Pereira Carneiro da Silva
RA: 824142121
Análise e Desenvolvimento de Sistemas - ADS

Att, Marinna

ATIVIDADE 03

Escolher 2 (dois) ataques cibernéticos de tipos diferentes ocorridos nos últimos 5 anos e fazer um texto com:

- Data do ataque (pode ser aproximada);
- 2. Tipo de ataque;
- 3. Descrição do ataque ou de como aconteceu;
- 4. Vulnerabilidade explorada (verificar se está no CVE e qual o seu código);
- 5. Impactos e/ou prejuízo (pode ser estimado);
- 6. Tipo de Proteção que poderia ter sido aplicada para evitá-lo.

Att, Marinna

CASO 1 – ATAQUE CIBERNETICO

Link da Notícia - https://g1.globo.com/politica/noticia/2024/09/03/stf-anatel-e-pf-sao-alvos-de-ataque-hacker-nos-ultimos-dias.ghtml

- Data do ataque (pode ser aproximada):
  - STF: 29 de agosto de 2024
  - PF: 3 de setembro de 2024
  - Anatel: Ataques intensificados após 30 de agosto de 2024

- Tipo de ataque: Ataque de negação de serviço (DDoS), que é quando sobrecarregam o site ou sistema com muitas visitas de uma vez para tirá-lo do ar.

- Descrição do ataque ou de como aconteceu: Os ataques funcionaram basicamente mandando um monte de acessos ao mesmo tempo para os sites do STF, PF e Anatel, fazendo com que ficassem lentos ou parassem de funcionar por alguns minutos. O pessoal de tecnologia agiu rápido para normalizar tudo e reforçar a segurança.

- Vulnerabilidade explorada (verificar se está no CVE e qual o seu código): Esse tipo de ataque não explora uma falha específica do sistema, mas sim a própria capacidade dos servidores de aguentar muito acesso de uma vez só. Ele se aproveita de falhas na infraestrutura de rede, como a falta de proteção contra sobrecarga de tráfego (CVE-2021-22986).

CVE-2021-22986 - Vulnerabilidade no F5 BIG-IP que poderia permitir um ataque DDoS.

- Impactos e/ou prejuízo (pode ser estimado): Não teve um grande prejuízo ou roubo de dados. A principal consequência foi a interrupção momentânea dos serviços, o que pode ter causado alguns atrasos para quem precisava usar os sistemas.

- Tipo de Proteção que poderia ter sido aplicada para evitá-lo:
  - **Mitigação de DDoS:** Uso de sistemas de mitigação de DDoS que detectam e bloqueiam tráfegos maliciosos antes de atingir os servidores.
  - **Firewall de Aplicações Web (WAF):** Para proteger os servidores de serem sobrecarregados por tráfegos excessivos.
  - **Escalabilidade na Nuvem:** Utilização de soluções em nuvem que permitem escalar recursos automaticamente para lidar com picos de tráfego.
  - **Redundância e Distribuição de Servidores:** Distribuição dos serviços em múltiplos servidores e locais para evitar que um único ponto seja um gargalo.

Att, Marinna

Resumo da Notícia: Nos últimos dias, o STF, a Anatel e a Polícia Federal foram alvos de ataques de hackers, mas sem grandes prejuízos. O ataque na PF aconteceu em 3 de setembro e causou uma instabilidade temporária nos serviços, mas não houve comprometimento de dados. O STF sofreu um ataque no dia 29 de agosto, pouco antes de o ministro Alexandre de Moraes ordenar que a rede social X cumprisse ordens judiciais ou seria banida no Brasil. No dia 30, o X foi tirado do ar. Os sistemas do STF ficaram fora do ar por menos de 10 minutos, mas logo voltaram ao normal sem danos. Após a decisão de Moraes, a Anatel também enfrentou um aumento nos ataques hackers, causando instabilidades momentâneas. Mesmo com essas tentativas, os ataques não causaram prejuízos aos órgãos públicos.

Att, Marinna

CASO 2 – ATAQUE CIBERNETICO

Link da Notícia - https://www.baguete.com.br/noticias/11/09/2024/ponta-grossa-foi-alvo-de-ataque-de-ransomware

- Data do ataque (pode ser aproximada): 19 de agosto de 2024
- Tipo de ataque: Ransomware
- Descrição do ataque ou de como aconteceu: No dia 19 de agosto, a Prefeitura de Ponta Grossa foi atacada por ransomware. Os hackers conseguiram criptografar os arquivos nos servidores da prefeitura, tornando-os inacessíveis. Como resposta, a equipe de TI da prefeitura desligou os servidores e retirou os sistemas do ar para conter o ataque. Durante a semana seguinte, alguns serviços públicos foram afetados e os funcionários tiveram que trabalhar manualmente.
- Vulnerabilidade explorada (verificar se está no CVE e qual o seu código): O ataque de ransomware geralmente explora vulnerabilidades conhecidas no sistema, mas não há um CVE específico listado para este ataque em particular. Ransomwares podem explorar falhas em sistemas de segurança, configurações incorretas ou falta de atualizações (CVE-2019-0708).

CVE-2019-0708 - "BlueKeep", uma vulnerabilidade no Remote Desktop Protocol (RDP) do Windows que pode ser explorada para executar código remoto e espalhar ransomware.

- Impactos e/ou prejuízo (pode ser estimado): O ataque causou a paralisação de alguns serviços públicos e a necessidade de realizar tarefas manualmente durante a semana do incidente. Felizmente, registros fiscais e legais foram preservados. O impacto financeiro direto não foi especificado, mas a interrupção dos serviços pode ter causado transtornos para a população.
- Tipo de Proteção que poderia ter sido aplicada para evitá-lo:

  - **Backup Regular:** Manter backups frequentes e seguros dos dados para permitir a recuperação em caso de ataque.
  - **Atualizações de Segurança:** Manter todos os sistemas e software atualizados para proteger contra vulnerabilidades conhecidas.
  - **Treinamento de Funcionários:** Educar os funcionários sobre os riscos de phishing e outras táticas usadas para distribuir ransomware.
  - **Soluções de Segurança:** Utilizar softwares de segurança robustos e soluções de proteção contra malware e ransomware.
  - **Autenticação Multifator (MFA):** Implementar MFA para adicionar uma camada extra de segurança aos sistemas críticos.

Att, Marinna

Resumo da Notícia: A Prefeitura de Ponta Grossa sofreu um ataque de ransomware no dia 19 de agosto. Os hackers criptografaram os dados da prefeitura, fazendo com que os sistemas e servidores fossem desligados para conter o ataque. Isso causou a paralisação de alguns serviços públicos e forçou os funcionários a trabalhar manualmente por uma semana. Apesar do impacto, os registros fiscais e legais foram preservados. A prefeitura iniciou uma investigação para entender o ataque e adotou medidas de prevenção. O comunicado destacou que, apesar das medidas de proteção modernas, a segurança infalível não é possível e que tais ataques são comuns globalmente. Outras cidades também enfrentaram ataques semelhantes. O município paulista de Itu teve seus serviços paralisados por ransomware, e o Governo de Alagoas viu seu site ficar fora do ar, embora sem vazamento de dados. O sistema de administração financeira Siafi também foi invadido em abril.

Att, Marinna