UNIVERSIDADE SÃO JUDAS TADEU

GESTÃO DA TECNOLOGIA DA INFORMAÇÃO

NATASHA MELO E YASMIN VICTÓRIA

**IMPACTO E PREVENÇÃO: O ATAQUE AO MOVEIT E MEDIDAS DE SEGURANÇA**

SÃO PAULO – SP

2024

NATASHA MELO E YASMIN VICTÓRIA

RA:82429222 E 824210011

**IMPACTO E PREVENÇÃO: O ATAQUE AO MOVEIT E MEDIDAS DE SEGURANÇA**

Este trabalho aborda dois temas principais. Primeiro, examina o ataque cibernético ao software MOVEit em maio de 2023 pelo grupo Clop, destacando os impactos e propondo medidas para melhorar a segurança, como aplicação de patches e sistemas de monitoramento. Em segundo lugar, analisa as invasões no sistema do Tribunal Federal entre novembro de 2020 e abril de 2022, explorando os métodos dos hackers, os danos causados e as respostas adotadas para a proteção do sistema.

Orientador: Robson Calvetti

SÃO PAULO – SP

# **IMPACTO E PREVENÇÃO: O ATAQUE AO MOVEIT E MEDIDAS DE SEGURANÇA**

# **Prática 3:**

Em maio de 2023, o MOVEit, um software amplamente utilizado para a transferência segura de arquivos, foi alvo de um ataque cibernético significativo. O grupo de hackers Clop, conhecido por suas operações de ransomware, foi responsável pelo incidente. Aproveitando uma vulnerabilidade crítica no software, classificada como CVE-2023-34362. A vulnerabilidade CVE-2023-34362 é uma falha de segurança zero-day, os invasores exploraram essa falha para carregar uma web shell e acessar dados confidenciais, resultando na exfiltração de informações e assim dessa forma os atacantes conseguiram comprometer o sistema MOVEit. Esta falha de execução remota de código permitiu que eles acessassem e criptografassem dados sensíveis, exigindo resgates das organizações afetadas para a liberação dos arquivos.

O ataque teve um impacto profundo, afetando uma variedade de empresas e organizações que dependiam do MOVEit para transferências de dados seguras. A estimativa dos prejuízos é de milhões de dólares, considerando os custos associados à resposta ao incidente, à recuperação dos dados criptografados e à interrupção das operações. Além disso, a exposição de informações sensíveis trouxe um risco adicional à reputação das organizações envolvidas.

Para evitar tais incidentes, as organizações devem adotar uma abordagem abrangente de segurança cibernética. Manter o software atualizado com os últimos patches de segurança é crucial para proteger contra vulnerabilidades conhecidas, como a que foi explorada no ataque ao MOVEit. Implementar sistemas avançados de monitoramento e detecção de intrusões é fundamental para identificar e reagir rapidamente a atividades suspeitas. Medidas de segurança de rede, como firewalls e segmentação de rede, também desempenham um papel essencial na proteção dos sistemas contra invasões e restrição do impacto de ataques.

Além dessas práticas, a adoção de soluções de segurança mais diretas pode fazer uma grande diferença. Ferramentas de prevenção de perda de dados (DLP) podem ajudar a proteger informações sensíveis contra acesso não autorizado e exfiltração. Sistemas de backup e recuperação são igualmente importantes, pois garantem que dados críticos possam ser restaurados em caso de criptografia por ransomware. Além disso, a capacitação constante dos funcionários é essencial. Para reconhecer e responder a tentativas de phishing e outras formas de engenharia social é vital para reduzir o risco de comprometimento inicial e fortalecer a segurança da organização como um todo.

**Fonte de Referência**

Para mais detalhes sobre a vulnerabilidade CVE-2023-34362, consulte a <https://www.danresa.com.br/>

# **Prática 3:**

Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias

Um outro caso de ataque cibernético foi no período de novembro de 2020 até abril de 2022, nos tribunais brasileiros. Com hackers se infiltrando nos sistemas de dados, de vários estados do país, mais tendo como foco os pontos superiores dos Governos e Estados.

O caso foi algo muito alarmante tanto para os processos jurídicos dos tribunais quanto para os problemas da população, atrasando os processos judiciais.

Os ataques ocorriam a cada 41 dias, não sendo tão frequente, porém era de se preocupar, pois geralmente era sempre visado o ambiente de tecnologia dos tribunais. Fazendo com que, os membros dos órgãos judiciais se precavessem no sistema de segurança digital, contra qualquer ameaça.

Os objetivos dos hackers não eram apenas financeiros, mas também o intuito era violar os dados e destruir as informações contidas nos sistemas. E em sua maiorias das vezes, quando paralisavam os sistemas, pediam o resgate dos dados, em criptomoedas.

Segundo o ponto de vista, do especialista em Direito Informático e internet, Omar Kaminski “o que tem prevalecido no Brasil, na esfera pública, é a chamada segurança por obscuridade — em que se acredita que, sem transparência, sem publicidade e sem detalhamento há uma menor expectativa de prejuízos e danos. Temo que esse número (13 ataques em 18 meses) possa ser ainda maior, a depender da competência e interesse dos hackers envolvidos".

E não para por aí, os dados pessoais e identidade das pessoas contidas no meio dos procedimentos, são violados para serem vendidos na dark web.

Por isso é fundamental adotar a aplicação (LGPD), investindo em medidas de proteção e segurança.

**Fonte de Referência**

Para mais detalhes sobre a onda de invasões de *hackers* sobre o sistema do Tribunal Federal, consulte a <https://www.conjur.com.br/>