**Ataque 1: Microsoft Exchange Server – “Hafnium” Zero-Days**

**Data do ataque:** início de 2021, com exploração ativa reportada em janeiro–março de 2021.

**Tipo de ataque:** exploração de vulnerabilidades de “zero-day” múltiplas, acesso remoto inicial + instalação de web shells + exfiltração de dados (data breach).

**Descrição de como aconteceu:**

* O grupo “Hafnium”, atribuível a um ator com apoio estatal, explorou quatro vulnerabilidades desconhecidas publicamente (zero-days) presentes em servidores Microsoft Exchange mantidos on-premises (versões 2013, 2016, 2019).
* Usando essas falhas, o atacante pôde obter acesso inicial sem autenticação (SSRF), escalar privilégios, gravar arquivos arbitrários no servidor, instalar backdoors (web shells) para persistência, e extrair conteúdos de caixas de correio, catálogos de endereços off-line (“offline address book”) etc.

**Vulnerabilidades exploradas / CVE(s):**

* **CVE-2021-26855**: SSRF (Server-Side Request Forgery), permite a execução remota de código sem autenticação inicial.
* **CVE-2021-26857**: desserialização insegura (insecure deserialization) no serviço Unified Messaging.
* **CVE-2021-26858**: escrita arbitrária de arquivos após autenticação (“post-authentication arbitrary file write”).
* **CVE-2021-27065**: similar à CVE-2021-26858, permite sobrescrever arquivos do sistema em locais arbitrários depois de obter credenciais/admin ou usar outra vulnerabilidade da cadeia.

**Impactos e prejuízos estimados:**

* Cerca de **250.000 servidores** infectados globalmente, afetando organizações variadas: ~30.000 nos Estados Unidos, 7.000 no Reino Unido, além de entidades governamentais e privadas múltiplas.
* Comprometimento de e-mails, cateóricos de endereços e outras informações internas, possibilidade de espionagem, roubo de dados sensíveis, além dos custos de resposta, mitigação, auditoria, remediação etc.
* Prejuízo financeiro direto difícil de precisar publicamente, mas inclui custos de pessoal, tempo de inatividade, perdas operacionais, possível multa ou penalidades regulatórias, danos reputacionais.

**Tipo de proteção que poderia ter sido aplicada para evitá-lo:**

1. **Gestão proativa de patches / atualizações de segurança:** aplicar correções assim que disponibilizadas, especialmente para softwares críticos de servidor com exposição externa.
2. **Segurança de perimeter (firewall, regras de acesso):** limitar ao máximo a exposição de servidores de Exchange à Internet; uso de redes de perímetro seguro, segmentação de rede.
3. **Detecção e resposta a intrusões (IDS/IPS) e monitoramento de logs:** identificar padrões de requisições maliciosas como SSRF, tentativas de registrar web shells, tráfego suspeito.
4. **Autenticação forte / controle de privilégio mínimo:** reduzir privilégios administrativos, usar autenticação multifator, limitar serviço de Unified Messaging / serviços que não forem necessários.
5. **Hardening de servidores:** desativar serviços não usados, restringir escrita de arquivos, validar entradas (deserialização) de forma segura, reforçar a configuração do IIS / software de gestão de servidor.
6. **Backups confiáveis e segregados, plano de resposta a incidentes bem praticado** para recuperação rápida caso haja comprometimento.