**ATAQUES CIBERNÉTICOS RECENTES**

**1. Ataque à Microsoft Exchange (2021)**

**1.1 Data do ataque:** Março de 2021  
**1.2 Tipo de ataque:** Exploração de vulnerabilidades em servidores  
**1.3 Descrição:** Em março de 2021, um grupo de hackers chineses explorou falhas graves no Microsoft Exchange Server. Essas falhas permitiram que os atacantes acessassem remotamente servidores de diversas empresas e órgãos governamentais, instalando backdoors (mecanismos ocultos para manter o acesso ao sistema comprometido) e garantindo controle remoto sobre os sistemas invadidos. Esse ataque foi massivo e representou uma grande preocupação global para a segurança da informação.

**1.4 Vulnerabilidade explorada:** Foram exploradas quatro falhas de segurança, incluindo a CVE-2021-26855, que permitia a execução remota de comandos nos servidores vulneráveis.

**1.5 Impactos e prejuízos:** Centenas de milhares de servidores ao redor do mundo foram comprometidos, permitindo o roubo de dados sigilosos e a instalação de malwares (programas maliciosos) para acessos futuros. Empresas e entidades governamentais sofreram prejuízos financeiros e comprometeram a segurança de informações sensíveis.

**1.6 Tipo de proteção que poderia ter sido aplicada:** Adoção de atualizações rápidas para corrigir vulnerabilidades conhecidas, monitoramento de logs para detectar acessos não autorizados e segmentação da rede para evitar que os atacantes se movimentem entre os sistemas comprometidos.

**2. Ataque à Uber (2022)**

**2.1 Data do ataque:** Setembro de 2022  
**2.2 Tipo de ataque:** Engenharia social (phishing)  
**2.3 Descrição:** Em setembro de 2022, um hacker conseguiu obter as credenciais de um funcionário da Uber por meio de um ataque de phishing (técnica que engana a vítima para roubar informações confidenciais). O invasor utilizou um método conhecido como "MFA Fatigue", no qual envia repetidas solicitações de autenticação multifator até que a vítima, por exaustão ou distração, acabe aceitando. Com isso, o atacante obteve acesso a sistemas internos da empresa, incluindo ferramentas administrativas e códigos-fonte.

**2.4 Vulnerabilidade explorada:** Falha na autenticação multifator (MFA Fatigue), onde o atacante persuadiu um funcionário a conceder acesso involuntariamente.

**2.5 Impactos e prejuízos:** O invasor teve acesso a sistemas críticos da Uber, expondo informações confidenciais da empresa e possivelmente de seus clientes. Esse incidente gerou preocupações sobre a segurança interna da empresa e a eficácia de seus controles de acesso.

**2.6 Tipo de proteção que poderia ter sido aplicada:** Adoção de autenticação multifator mais robusta (como chaves de segurança físicas), treinamento contínuo dos funcionários para reconhecer ataques de engenharia social e monitoramento ativo de tentativas de login incomuns.

**REFERÊNCIAS**

TREND MICRO. *Ataque ao Microsoft Exchange: O que fazer se fui afetado?*. Disponível em: <https://blog.trendmicro.com.br/ataque-ao-microsoft-exchange-o-que-fazer-se-fui-afetado/>

TECHTUDO. *Uber tem sistema hackeado; entenda como aconteceu e se há riscos*. Disponível em: <https://www.techtudo.com.br/noticias/2022/09/uber-tem-sistema-hackeado-entenda-como-aconteceu-e-se-ha-riscos.ghtml>

UOL. *Invasão hacker atinge sistema interno da Uber*. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2022/09/16/uber-e-hackeado-e-funcionarios-acharam-que-aviso-do-invasor-era-piada.htm>