Fernando Porto Estevão – 823123863 | LAB03

Exemplos de Ataques Cibernéticos e Suas Consequências

Nos últimos anos, diversos ataques cibernéticos de diferentes tipos demonstraram como as falhas de segurança podem causar prejuízos severos para organizações e usuário.

---

1. Ataque de Ransomware ao Health Service Executive (HSE) – Irlanda

- **Data:** Maio de 2021
- **Tipo de Ataque:** Ransomware (variante Conti)

Em maio de 2021, o serviço público de saúde da Irlanda (HSE) foi alvo de um sofisticado ataque de ransomware. O acesso inicial ocorreu por meio de um e-mail de phishing, contendo um arquivo Excel com malware. Uma vez que o arquivo foi aberto, os atacantes conseguiram se infiltrar na rede interna, se movimentar lateralmente entre os sistemas e, por fim, criptografar dados essenciais para o funcionamento do serviço de saúde.

Embora não tenha sido divulgada uma vulnerabilidade específica com código CVE, sabe-se que o ataque se aproveitou de falhas no sistema de segurança de e-mails e na ausência de mecanismos de detecção e resposta adequados.

Impactos:

- Interrupção dos serviços de saúde em todo o país
- Exposição de dados médicos confidenciais
- Estimativas de prejuízo superiores a dezenas de milhões de euros

Proteção Recomendável:

- Uso de autenticação multifator (MFA)
- Monitoramento de rede em tempo real
- Treinamento de colaboradores para identificar tentativas de phishing
- Atualizações regulares nos sistemas de segurança

---

2. Ciberataque à Optus – Austrália

- **Data:** Setembro de 2022
- **Tipo de Ataque:** Vazamento de dados pessoais

A operadora australiana de telecomunicações Optus foi vítima de um ataque que resultou no vazamento de dados sensíveis de aproximadamente 1,2 milhão de clientes. As informações expostas incluíam nomes completos, datas de nascimento, endereços e números de documentos oficiais.

O ataque foi possível devido a falhas na configuração de uma API da empresa, que permitia o acesso a dados sem a devida autenticação. Embora não tenha sido associado a um código CVE específico, o incidente escancarou a necessidade de práticas mais rigorosas na segurança de APIs.

Impactos:

- Exposição de dados pessoais de milhares de clientes
- Danos significativos à imagem da empresa
- Estimativa de custo de cerca de 140 milhões de dólares australianos

Proteção Recomendável:

- Reforço na segurança e autenticação de APIs
- Monitoramento constante de acessos não autorizados
- Implementação de políticas rígidas de controle de dados
- Auditorias de segurança periódicas
