UC- SISTEMAS COMPUTACIONAIS E SEGURANÇA
Maria Eduarda Medeiro Porto 824144948
ORIENTADOR: Robson Calvetti

PRÁTICA 03- Proteção de Dados e Informação I

ATIVIDADE 1

Ataque 1: Ataque WannaCry Ransomware

Data do ataque: 12 de maio de 2017
Tipo de ataque: Ransomware
Descrição do ataque: O ataque de ransomware WannaCry foi um ataque cibernético global que afetou mais de 200.000 computadores em 150 países. O ataque foi realizado explorando uma vulnerabilidade no sistema operacional Windows, especificamente no protocolo SMBv1. Os invasores usaram um worm para espalhar o malware, que criptografou arquivos em computadores infectados e exigiu resgate em bitcoin para restaurar o acesso.
Vulnerabilidade explorada: CVE-2017-0144 (exploração EternalBlue)
Impacto e/ou danos: Danos estimados em 4 mil milhões de dólares, com muitas organizações, incluindo hospitais e sistemas de saúde, afetadas.
Tipo de proteção que poderia ter sido aplicada para evitá-lo: implementar atualizações e patches regulares de software, desabilitar o protocolo SMBv1, usar software antivírus e ter um sistema de backup robusto instalado.

Ataque 2: violação de dados Capital One

Data do ataque: 22 a 23 de março de 2019
Tipo de ataque: violação de dados baseada em nuvem
Descrição do ataque: um ex-funcionário da Amazon Web Services (AWS) explorou um bucket AWS S3 mal configurado para obter acesso a dados confidenciais do Capital One, um grande banco dos EUA. O invasor usou uma técnica de falsificação

de solicitação no servidor (SSRF) para acessar os dados, que incluíam aplicativos de cartão de crédito, números de previdência social e outras informações pessoais.
Vulnerabilidade explorada: bucket AWS S3 configurado incorretamente (sem CVE específico)
Impacto e/ou danos: Estima-se que 106 milhões de pessoas sejam afectadas, com perdas potenciais na ordem das centenas de milhões de dólares.
Tipo de proteção que poderia ter sido aplicada para evitá-lo: implementação de configurações adequadas de segurança na nuvem, uso de controles de acesso e gerenciamento de identidade, monitoramento de recursos da nuvem em busca de configurações incorretas e realização de auditorias de segurança regulares.