Universidade São Judas Tadeu

Sistemas Computacionais e Segurança

Prof. Robson Calvetti

João Luiz da Silva e Rafael Tiago Scisci Arcienega

RA: 82420546 e 824216105

Ataques cibernéticos são tentativas de acesso ilegal a uma rede de computadores. Geralmente, esses invasores podem ser indivíduos ou organizações criminosas, com objetivos bem definidos, como obter dados, dinheiro, ter intenções políticas ou simplesmente pessoais.

Um ataque divulgado no dia 8 de outubro de 2022 foi contra a emissora de televisão Rede Record. O sistema central da Record (à época, Record TV) em São Paulo sofreu um ciberataque, onde os hackers roubaram todo o acervo de reportagens pré-gravadas e quadros dos programas de auditório da emissora. Os funcionários também ficaram sem acesso ao Ibope pelos celulares da emissora, e o acesso à intranet foi cortado. Além disso, foi bloqueado o acesso aos e-mails da empresa, o que pode ter dado aos hackers acesso a todos os e-mails já enviados e recebidos pelos funcionários. A internet também foi derrubada.

Segundo informações do jornalista do Tecmundo Felipe Payão, o ataque foi realizado pelo ransomware BlackCat, que é um tipo de malware e um ransomware-as-a-service, ou seja, foi comprado pelos criminosos.

De acordo com o comunicado enviado à RecordTV, os hackers cobrariam US$ 7 milhões, mas ofereceram um desconto válido até o dia 15, reduzindo o valor para US$ 5 milhões. O pagamento deveria ser feito em Bitcoin ou Monero. Os criminosos também afirmaram que, caso o valor fosse pago, mostrariam à empresa como a invasão ocorreu e ajudariam na descriptografia dos dados. Caso contrário, realizariam um ataque DDoS e já estavam buscando possíveis compradores do conteúdo na dark web.

No dia 16, dados começaram a ser vazados na deep web, incluindo planilhas de faturamento e o passaporte de uma estrela da emissora. A Record acionou o Departamento de Crimes Cibernéticos. No dia 10, o departamento de Tecnologia e Segurança restaurou o acesso aos computadores e e-mails. Já no dia 12, o departamento de TI conseguiu fazer uma cópia dos dados sequestrados.

Inicialmente, a emissora não se pronunciou, e o ataque se tornou público no dia 8 de outubro, quando a RecordTV tirou alguns programas do ar. A emissora foi criticada por não ter backups da programação.

A vulnerabilidade explorada, identificada como CVE-2024-37085, era um desvio de autenticação no VMware ESXi, que permitia aos atacantes obter privilégios de administrador no hipervisor ao criar um grupo "ESX Admins" e adicionar usuários a ele.

Em junho de 2023, o software MOVEit (ferramenta usada para transferência de arquivos por várias organizações e empresas) sofreu um ataque cibernético do tipo Supply Chain, que ocorre quando hackers comprometem um fornecedor ou parceiro de uma organização para obter acesso aos seus sistemas ou dados. Esse ataque afetou diversas empresas, como a Shell, Boots, e o Departamento de Educação da Cidade de Nova York. O grupo explorou a vulnerabilidade CVE-2023-34362, categorizada como uma vulnerabilidade de injeção de SQL.

Com esse ataque, dados foram comprometidos e as atividades de diversas empresas de grande porte foram interrompidas. Os prejuízos financeiros não foram divulgados, mas estima-se que foram significativos.

As proteções que poderiam ter evitado esse caos incluem: a aplicação imediata de patches de segurança, a segmentação da rede em vários segmentos isolados e a adoção de monitoramento contínuo de redes. A manutenção de backups frequentes também teria ajudado na recuperação dos dados sem a necessidade de pagar o resgate.