**TRABALHO DE SEGURANÇA DA INFORMAÇÃO:** Trabalho de Incidentes de Ataques Cibernéticos.

**Alunos:** Manoel Luciano de Mesquita Neto;

Tecnologia em Analise e Desenvolvimento de Sistemas Faculdades Integradas de Três Lagoas – FITL/AEMS.

E-mail do autor: manoellmn03@gmail.com

**Professor**: Richard Vieira do Espirito Santo.

Docente das Faculdades Integradas de Três Lagoas – FITL/AEMS.

**O ataque ransomware à Ativy Digital**

A empresa Ativy Digital, especializada em hospedagem de sistemas em nuvem, sofreu um ataque ransomware no dia 28/03/2023. O ataque levou os sistemas da empresa a se desconectarem do ambiente de forma repentina, sistemas esse que são de acessos aos hosts usado pela empresa. A Ativy digital informou que não houve indícios de vazamentos de dados, já que seu sistema de criptografia afetou os arquivos operacionais de acesso às aplicações. Tiago Garbim, CEO da empresa, explicou em um vídeo lançado no canal oficial da empresa no Youtube que houve um pedido de resgate, mas a comunicação entre a empresa e os cibercriminosos foi rompida quando eles perceberam tentativas de restauração dos meios atingidos. A primeira impressão que o time de TI teve, foi estar lidando com um problema de infraestrutura, mas depois de usar todos os processos de troubleshooting, eles descobriram que o problema era muito maior. Ainda com dificuldade em lidar com o problema, eles acionaram parceiros de hardware e software para buscar pelo problema, assim descobrindo que às máquinas estavam bloqueadas devido a criptografia de ransomware que possibilitava o acesso a elas. Entendido que o ataque tinha sido na sua camada de virtualização, eles subiram uma nova camada com hosts e blades diferentes e um novo ambiente de armazenamento. Também refizeram o contato com os storages para buscar as máquinas virtuais ali armazenadas e para concluir deram continuidade ao restore dos arquivos que dão acesso às máquinas virtuais. Por ser uma empresa que hospeda e gerencia mais de 30 mil usuários em suas plataformas de nuvem tantos os negócios da própria empresa quanto dos usuários foram afetados, já que seus sistemas caíram. O executivo da empresa afirmou que as máquinas já recuperadas, começaram a voltar às atividades e o processo de restauração continuou a avançar. Para ajuda em mitigar os danos, a empresa se comprometeu em auxiliar a todos no processo de retornar as operações de seus sistemas.

Fontes:

<https://securityleaders.com.br/ativy-digital-sofre-novo-ataque-ransomware-contra-sistemas-de-hosts/>

<https://www.baguete.com.br/noticias/03/04/2023/ativy-digital-sofre-ataque-de-ransomware>