

***Ciberataque no Grupo Fleury coloca em evidência a necessidade de ampliação da proteção do ambiente de TI do setor de saúde, que é um dos principais alvos por contemplar dados pessoais e sensíveis***

O incidente divulgado nesta última terça-feira, dia 22 de junho, no Grupo Fleury, que sofreu um ataque cibernético indisponibilizando o acesso a seus sistemas, mostra que o setor de saúde virou um dos principais alvos em função do acesso a dados pessoais sensíveis, podendo render duplamente aos cibercriminosos, que exigem valores de resgates para descriptografarem os dados e para não divulgarem as informações.

Esse tipo de incidente normalmente ocorre por meio de ataques de ransomwares, que começam com um e-mail recebido contendo um malware em anexo ou com link para um site malicioso, o famoso phishing. Tal modelo de ataque foi ampliado após o início da pandemia da Covid-19 devido à descentralização das operações e, no caso específico da área de saúde, a situação se agrava com a Lei Geral de Proteção de Dados (LGPD), que ainda pode render penalizações às empresas.

**[Leia aqui na íntegra.](#)**

**Fonte:** Saúde Business, em 23.06.2021