Investimentos ainda são baixos e as estruturas de proteção limitadas, apesar de o setor de saúde guardar dados sensíveis e ser alvo frequente de crimes

Na última terça-feira (19), Associação Nacional de Hospitais Privados (Anahp) realizou mais uma edição do seu tradicional Café da Manhã, dessa vez em parceria com a TOTVS, uma das principais empresas de tecnologia do país, que oferece estrutura completa para a digitalização dos negócios. O tema do evento foi “Garantindo a saúde dos dados: um encontro sobre segurança da informação e boas práticas nas instituições de saúde”.

Alexandre Chaul, diretor de Cloud Computing na TOTVS, trouxe tópicos relevantes e atuais para os hospitais, como os desafios e soluções para proteger os dados, as ameaças cibernéticas mais frequentes e as boas práticas de segurança. “O setor de saúde é o segundo mais afetado por ataques cibernéticos, com 20% de todas as ocorrências. Os criminosos preferem os alvos que guardam as informações mais sensíveis e valiosas”, informou.

O especialista explicou que os crimes mais frequentes são aqueles realizados por meio de *ransomwares*, *softwares* inseridos nos sistemas para sequestrar dados e permitir que os bandidos exijam resgate posteriormente. “Isso acontece em companhias de todos os tamanhos. Um cliente nosso de faturamento de R$ 3 bilhões, com ações em bolsa, recentemente perdeu 6 meses de dados”, contou.

Chaul alertou que os investimentos em cibersegurança ainda são muito limitados, ficando normalmente abaixo dos 10% do orçamento total de TI. “A maioria das empresas têm apenas o básico e isso é muito pouco”, avaliou. Além disso, outra dificuldade até mais séria é a falta de mão de obra especializada. “Sofremos com uma escassez severa de profissionais nessa área. Formamos pouco e grande parte do que conseguimos formar é cooptada por empresas do exterior que oferecem salários bem superiores, em dólar”, relatou.

Não bastassem todos esses problemas, continuou o especialista, ainda são comuns a falta de disciplina e erros básicos por parte dos usuários e das empresas, como senhas fracas e compartilhadas, *softwares* desatualizados e desatenção para o *phishing*, que são os e-mails e outras comunicações fraudulentas que induzem a pessoa a clicar em links ou informar dados sigilosos.

Na maioria das vezes, esse mindset só muda quando a empresa sofre um ataque, de acordo com Chaul. “Quando acontece o pior, todos ficam desesperados buscando soluções que não foram planejadas ou desenvolvidas”, ressaltou. A reação, aliás, é uma outra questão problemática. “Quase nunca existem protocolos para orientar as ações nos momentos seguintes à invasão e ninguém sabe o que fazer. Com isso, perde-se tempo valioso”, completou.

O especialista recomendou um planejamento bem elaborado de cibersegurança com a opção de transferir os dados para um *cloud* terceirizado que garanta a proteção do perímetro. “Existem alternativas com preços razoáveis, que até oferecem economia em relação à estrutura própria”, revelou. De qualquer maneira, finalizou, são indispensáveis ações como a utilização de *antimalwares* robustos e atualizados, dar o menor privilégio possível para os diversos elos do sistema, proteger o *backup* e promover treinamentos e campanhas de conscientização sobre as boas práticas para as equipes.

Fonte: Anahp, em 20.09.2023