Por Thiago Fialho

A transformação digital trouxe avanços significativos na gestão hospitalar e no cuidado ao paciente. Entretanto, essa evolução tecnológica também expôs vulnerabilidades críticas, especialmente no que tange à proteção de dados sensíveis. O cenário atual é alarmante: globalmente, o custo médio de ciberataques no setor da Saúde chegou a US$ 5,3 milhões em 2023, o maior entre os segmentos pesquisados, os dados são da 26ª Global Digital Trust Insights, da PwC, lançada em setembro.

No Brasil, o contexto é ainda mais preocupante. Líder em ataques cibernéticos na América Latina e um dos cinco países mais visados no mundo, o setor de saúde brasileiro enfrenta desafios sem precedentes. Segundo pesquisa da Kaspersky, divulgada em maio, foram registrados mais de 800 bloqueios diários de ataques de ransomware em 2024, totalizando mais de 106 mil tentativas desde janeiro. As estatísticas trazem o setor da saúde como o terceiro mais atacado no ano, com 6,5 mil tentativas.

A complexidade do problema aumenta com as exigências legais. Instituições de saúde são obrigadas a armazenar dados, diagnósticos e imagens por no mínimo 20 anos, conforme a Lei nº 13.787/18. Essa necessidade de retenção prolongada de informações sensíveis torna o setor um alvo ainda mais atraente para criminosos digitais.

Os impactos dos ataques cibernéticos vão além das perdas financeiras. Estudos demonstram um aumento nas complicações médicas e até mesmo na mortalidade de pacientes durante incidentes de segurança digital. De acordo com o Relatório de Segurança Cibernética da Ponemon Healthcare 2024, 69% dos entrevistados relataram atrasos em procedimentos e testes que resultaram em desfechos adversos, enquanto 57% apontaram aumento nas complicações de procedimentos médicos. Além disso, as instituições de saúde estão sujeitas a multas substanciais previstas pela **LGPD**, que podem alcançar R$ 50 milhões em casos de vazamento de dados.

O cenário para 2025 é ainda mais desafiador, com previsões indicando o uso crescente de inteligência artificial por cibercriminosos para refinar técnicas de ataque, tornando-as mais sofisticadas e difíceis de detectar. A resposta a essa ameaça crescente deve ser multifacetada e robusta. É fundamental que as instituições de saúde invistam em infraestrutura de segurança de ponta, incluindo sistemas de monitoramento contínuo, autenticação multifator e protocolos rigorosos de proteção de dados. A capacitação das equipes também é crucial, já que colaboradores bem treinados representam a primeira linha de defesa contra ameaças cibernéticas.

O momento exige uma mudança de mentalidade no setor. A segurança digital não pode mais ser vista como um custo adicional, mas como um investimento indispensável para a continuidade dos negócios e, principalmente, para a proteção da vida dos pacientes. As instituições que não se adaptarem a essa nova realidade correm o risco não apenas de enfrentar prejuízos financeiros, mas também de comprometer a qualidade e a segurança do atendimento prestado.

A saúde brasileira está diante de uma encruzilhada digital. O caminho a seguir deve ser pautado por investimentos consistentes em tecnologia de proteção, capacitação contínua de profissionais e adoção de práticas rigorosas de segurança. Somente assim poderemos garantir que a revolução digital na saúde continue trazendo benefícios, sem comprometer a segurança e a privacidade dos pacientes.

***Thiago Fialho** é cofundador da GTPLAN.

* A opinião manifestada é de responsabilidade dos autores e não é, necessariamente, a opinião do IES

Fonte: Instituto Ética Saúde, em 20.02.2025.