Por Marcelo Ferreira de Souza (*)



Hospitais e instituições de saúde estão hoje entre os principais alvos do cibercrime global. Segundo o último levantamento da Check Point Research (CPR), divisão de inteligência de ameaças da Check Point Software, o setor sofreu, em média, 3.167 tentativas de ataques cibernéticos por semana em 2025, um índice 37% superior à média registrada nos demais segmentos econômicos.

Um levantamento da ISH Tecnologia identificou 11.426 violações de segurança em organizações de saúde brasileiras apenas no primeiro semestre de 2025. Destas, 97% foram confirmadas como incidentes reais, evidenciando que o setor convive diariamente com um cenário de exposição permanente.

Essa exposição não acontece por acaso, pois poucos setores concentram um volume tão grande de informações críticas quanto um hospital. Um único ambiente reúne prontuários eletrônicos, exames laboratoriais, imagens médicas, prescrições, dados financeiros, informações pessoais, contratos com operadoras, pesquisas clínicas e sistemas que funcionam 24 horas por dia.

Além dos sistemas financeiros e administrativos, há dispositivos IoT, aplicações em nuvem, integrações com laboratórios, plataformas SaaS, equipamentos médicos conectados e parceiros acessando informações críticas.

Cada nova conexão amplia a superfície de ataque e exige uma estratégia integrada de infraestrutura, gestão de identidades, monitoramento contínuo e proteção dos ambientes.

Na saúde, um incidente não significa apenas indisponibilidade de sistemas. Significa um médico sem acesso ao histórico clínico do paciente, um centro cirúrgico trabalhando com informações incompletas, um laboratório impossibilitado de liberar exames e uma farmácia hospitalar sem conseguir validar prescrições. Em outras palavras, significa colocar em risco a continuidade da assistência e a vida dos pacientes.

Por isso, costumo dizer que, nos hospitais, proteger a infraestrutura digital é, acima de tudo, proteger pessoas.

Muita gente ainda acredita que bancos continuam sendo o principal alvo dos criminosos digitais. Enquanto um cartão de crédito roubado pode ser bloqueado em minutos, um histórico médico nunca poderá ser substituído.

Esse dado tem enorme valor para o mercado ilegal. Segundo o IBM Cost of a Data Breach Report 2025, o custo médio de uma violação de dados no Brasil atingiu R$ 7,19 milhões. O aspecto mais preocupante é que boa parte desse prejuízo decorre da interrupção dos serviços assistenciais, e não apenas do vazamento das informações.

O principal modelo de ameaça para empresas de praticamente todos os setores continua sendo o ransomware. Segundo o 2026 Data Breach Investigations Report (DBIR), da Verizon, 48% de todos os incidentes analisados no mundo envolveram esse tipo de ataque.

Um exemplo desse tipo de incidente é o episódio que envolveu a Change Healthcare, empresa responsável pelo processamento de aproximadamente metade das transações médicas dos Estados Unidos. Ela sofreu um ataque de ransomware que paralisou grande parte do sistema de saúde americano.

Farmácias deixaram de validar receitas, os hospitais não conseguiam faturar procedimentos, laboratórios interromperam processos, consultórios ficaram semanas sem receber pagamentos e milhões de pacientes encontraram dificuldades para retirar medicamentos porque autorizações simplesmente deixaram de funcionar.

Posteriormente, descobriu-se que os invasores acessaram o ambiente utilizando credenciais comprometidas em um portal remoto que não possuía autenticação multifator (MFA). Permaneceram nove dias movimentando-se internamente, infiltraram aproximadamente seis terabytes de dados e só então criptografaram os sistemas. Mais de 190 milhões de pessoas tiveram informações potencialmente comprometidas, tornando-se essa a maior violação da história do setor de saúde.

O caso mostra que, muitas vezes, um ataque de grandes proporções começa pela ausência de um controle básico.

Sempre que um ataque ganha repercussão, toda a atenção recai sobre o ransomware, mas, na minha visão, ele é apenas a etapa final.

O relatório da Verizon também mostra que o uso de inteligência artificial pelos grupos criminosos tornou os ataques mais rápidos, personalizados e difíceis de identificar, especialmente nas campanhas de engenharia social. Hoje, e-mails falsos reproduzem com precisão a linguagem, a identidade visual e até o padrão de escrita de empresas e executivos.

Toda essa realidade mudou a forma como os gestores enxergam a cibersegurança, que exige processos, governança, monitoramento contínuo e pessoas preparadas.

Para mim, esse é o verdadeiro conceito de resiliência. Enquanto algumas empresas ainda concentram seus esforços na tentativa de bloquear todos os ataques, as mais maduras investem em antecipação, prontidão operacional e preparação contínua para reduzir impactos e manter a continuidade do negócio.

Isso significa desenvolver planos de continuidade, realizar exercícios de crise, segmentar ambientes, manter backups imutáveis, monitorar eventos em tempo real, adotar autenticação multifator, gestão de identidades, arquitetura Zero Trust, inteligência contra ameaças e processos bem definidos para lidar com incidentes.

Mais importante ainda: fazem da Segurança da Informação uma pauta permanente da alta gestão, e não apenas da equipe técnica. É exatamente essa mudança cultural que vejo acontecer nas organizações mais maduras.

Referências:

https://ish.com.br/wp-content/uploads/2025/09/Ameacas-Ciberneticas-ao-setor-de-Saude_Brasil.pdf

https://brasil.newsroom.ibm.com/2025-07-30-Relatorio-da-IBM-Custo-medio-de-uma-violacao-de-dados-no-Brasil-atinge-R-7,19-milhoes

https://www.verizon.com/business/resources/reports/dbir/

https://www.aha.org/change-healthcare-cyberattack-underscores-urgent-need-strengthen-cyber-preparedness-individual-health-care-organizations-and

https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in-cyber-threats-worldwide-with-a-rise-of-126-in-ransomware-attacks/amp

(*) **Marcelo Ferreira de Souza** é CTO de Infraestrutura e Segurança da Weega Technologies.

**Fonte**: Engenharia de Comunicação, em 21.10.2026