Uma invasão de hacker pode prejudicar as instituições de saúde, provocando a parada de sistemas críticos que impossibilitariam o dia a dia do hospital e resultando em prejuízos financeiros

Atualmente, computadores e smartphones são os alvos preferidos de criminosos cibernéticos. Aparelhos hospitalares, prontuários eletrônicos, histórico de consumo de medicamentos e doenças, relatórios financeiros, entre outras informações, viraram alvo dos hackers. E não é de hoje que os criminosos digitais são atraídos pelo setor da saúde.

A pesquisa divulgada pela Cyber View 2019 revela que o setor da saúde é o mais vulnerável a ataques cibernéticos, mostrando que 27% das empresas já sofreram algum tipo de ataque cibernético. São buscados desde dados pessoais e sensíveis, que individualizam uma pessoa, como informações de renda, débitos ou enfermidades, que acabam sendo visados pelos criminosos digitais para possíveis extorsões, criação de débitos em nome da pessoa e outros meios maliciosos.

Para o especialista em segurança da informação da Indyxa, empresa especializada em soluções e serviços de tecnologia, Tiago Brack Miranda, uma invasão de um hacker pode prejudicar o sistema hospitalar e trazer prejuízos diretamente e indiretamente financeiros para a instituição, como a parada de sistemas críticos que impossibilitem o dia a dia do hospital. “Além disso, pode ocasionar problemas no próprio atendimento ou consulta do prontuário do paciente, gerando prejuízos de receita ou cobrança, e indiretamente na imagem do hospital que poderá perder credibilidade e até mesmo clientes pelo descuido na proteção dos dados pessoais e sensíveis de seus pacientes”, diz.

Miranda destaca que para proteger os dados e informações de possíveis ataques cibernéticos é fundamental possuir equipamentos e ferramentas que ofereçam uma proteção tanto no perímetro, meios de acesso, quanto nos servidores, estações de trabalho e dispositivos móveis. “Com o avanço das tecnologias avançaram também os malwares e os criminosos digitais. Soluções de proteção contra malwares, vazamento de dados e ataques cibernéticos elevam a segurança da informação criando uma camada de proteção constantemente atualizada pelos próprios fabricantes de forma global”, comenta o especialista.

Além disso, é imprescindível existirem processos recorrentes para revisar a segurança da informação da instituição hospitalar. A auditoria constante sobre os controles existentes reduz eventuais riscos inerentes ao mundo conectado de hoje. “Também é importante os colaboradores possuírem consciência do tema da segurança da informação, evitando assim incidentes não intencionais, que podem ocorrer pelos próprios colaboradores ao acessarem conteúdos indevidos, por exemplo”, revela.

O que fazer quando um ataque acontecer?

Miranda revela que a resposta imediata ao incidente de segurança da informação é fundamental para evitar maiores transtornos. “É necessário identificar a origem do incidente e isolá-lo, essa ação rápida mitigará eventuais perdas e demais prejuízos. A trilha de como o evento ocorreu, identificando brechas existentes e elaborando o plano de correção ajudará o hospital ou unidade de saúde a identificar outras brechas que porventura possam existir”, expõe.

O especialista ainda revela que de acordo com a nova Lei Geral de Proteção de dados (LGPD), todo incidente de segurança da informação que gere o vazamento de dados pessoais e sensíveis, se torna obrigatória a comunicação para a Agência Nacional de Proteção de Dados (ANPD). “Ou seja, além de toda a tratativa interna que deve ser efetuada, a comunicação para a ANPD do incidente é um passo adicional para as instituições seguirem a partir de agosto de 2020”, conclui.

Sobre a Indyxa

Uma das maiores empresas de tecnologia do Sul do país, com mais de 120 colaboradores,

distribuídos em quatro sedes (Blumenau, Brusque, São Paulo e Cidade do México), a empresa possui mais de 15 anos de experiência no segmento. Integramos em nosso portfólio soluções e serviços em infraestrutura de TI com inteligência de negócios, cloud services, segurança e continuidade, ativos e projetos e serviços gerenciados.

Fonte: **Saúde Business**, em 21.11.2019