A Redbelt, consultoria especializada em segurança cibernética, mapeou quais são as principais informações buscadas pelos hackers ao invadir os sistemas de dados de instituições da área da Saúde e em quais pontos hospitais, clínicas e consultórios devem investir para preservar seus próprios dados e dos pacientes.

Há uma preocupação na Saúde em dar aos pacientes mais acesso à informação como parte da estratégia em melhorar a experiência. “Porém, isso deve ser feito com confidencialidade, garantindo o acesso somente por pessoas autorizadas e certificando que a informação não seja violada. Restringir o acesso com logins e senhas é uma medida, no mínimo, recomendada”, destaca Eduardo Bernuy Lopes, diretor de operações da Redbelt.

No ano passado, as áreas da tecnologia que mais receberam recursos na Saúde foram aplicações de analytics, segurança e aplicações específicas da indústria. Para a consultoria, as instituições dividem-se entre investir em tecnologias direcionadas ao paciente e em cibersegurança. “Não existe transformação digital na área da Saúde sem investimentos em cibersegurança e as instituições devem compreender que isso deve ser feito com urgência”, afirma o executivo.

“Utilização de aplicações tradicionais muitas vezes desenvolvidas por fornecedores que nem estão mais no mercado, rede wi-fi com senhas inseguras, ausência de módulos de backup, sistemas sem recursos de proteção extra. Dados de caráter médico precisam ser 100% confiáveis, pois revelam a vida inteira dos pacientes, se afetados por alguma dessas vulnerabilidades”, explica Bernuy. “Além disso, funcionários e pacientes estão utilizando canais móveis (smartphones, por exemplo) para acessos aos dados médicos, o que pode aumentar o risco de vazamento de informações, caso não haja a preocupação com a identidade nesses dispositivos”, destaca.

A Redbelt mapeou quais são os dados que os hackers buscam e algumas das ações que podem fazer com as informações levantadas. São eles:

Em relação aos pacientes:

- Informações bancárias
- Dados pessoais que podem ser vendidos no mercado negro, para fraudes de seguros, usados como insumos para identidades falsas ou ainda para a obtenção ilegal de medicamentos
- Histórico de consumo de medicamentos e doenças
- Violação de dados privados sensíveis de pessoas públicas ou políticas
- Ação direcionada de spearphishing a pacientes de alto valor

Em relação ao hospital:

- Planejamento estratégico do hospital
- Relatórios financeiros sigilosos ou movimentação bancária
- Propriedade intelectual de técnicas, metodologias, equipamentos ou sistemas
- Causar indisponibilidade dos serviços
- Bloquear o acesso às informações
- Controlar aparelhos médicos remotamente, com a ascensão da IoT (Internet das coisas), entre outras possibilidades.

Mediante um estudo das principais vulnerabilidades encontradas na TI da área da Saúde, a consultoria listou quais devem ser os pontos imediatos de investimento das instituições visando inibir a ação dos criminosos. Alguns deles são:

- Conscientização de segurança para toda a equipe, incluindo gestores, médicos, enfermeiros, administrativos e demais colaboradores;
- Testes recorrentes e avaliação de vulnerabilidades para garantir que todo o ambiente esteja

sempre com as aplicações atualizadas, evitando riscos de intrusão;
- Um time especializado e focado na rápida resposta de incidentes;
- Ataques de estresse controlados para garantir alto desempenho e funcionamento de sistemas vitais à instituição;
- *Assessment* em Políticas de Segurança para garantir conformidade com todas as normas de segurança da HIPAA e ANS;
- Controle de armazenamento, acesso e compartilhamento de dados dos pacientes com processos específicos.
- Processo de backup para evitar perda de dados ou a realização de quaisquer alterações indevidas;
- Política de *Disaster Recovery*;
- Computação em nuvem pelo baixo custo e direcionamento do foco ao tratamento de pacientes (ao invés de gerenciamento de datacenters) com proteção implementada desde *endpoints* até redes.

“À medida que a indústria de cuidados de saúde trabalha para transformar a TI com recursos digitais, também enfrenta a tarefa de proteger a segurança e a confidencialidade do paciente sob um crescente número de ataques. A falta de conhecimento para combater a essas ameaças de frente pode comprometer pacientes, prejudicar a reputação da organização e levar a severos prejuízos financeiros”, conclui Bernuy.

Fonte: Portal Hospitais Brasil, em 26.02.2018.