Por Helder Assis (*)

Episódios de ataques cibernéticos, que ocorrem com frequência – principalmente após o início da pandemia, período que forçou a descentralização das operações e, consequentemente, ampliou a vulnerabilidade dos ambientes de TI das empresas em função das novas formas de acessar os sistemas internos, é uma ameaça para diferentes setores, entre eles o da saúde, a exemplo do caso que envolveu o Grupo Fleury recentemente.

Um levantamento realizado pela Check Point Software Technologies aponta que houve alta de 45% nos ataques a empresas do setor de saúde no mundo e hospitais são os mais visados, principalmente em função do acesso a dados pessoais e sensíveis, o que pode render duplamente ao cibercriminosos, que podem ganhar com o resgate (descriptografia) e com a promessa de não divulgação dos dados. Além disso, o segmento ampliou há poucos anos a sua maturidade de segurança, o que também contribui para ser um alvo.

Mas, quais medidas devem ser tomadas para minimizar os ataques e os danos neste setor? A começar pelo treinamento dos colaboradores no que diz respeito aos cuidados com e-mails recebidos contendo um malware em anexo ou com link para um site malicioso – o famoso phishing, que configura como uma das mais tradicionais portas de entrada para diversos tipos de ataque, há outras maneiras de conter as vulnerabilidades nas empresas de saúde a partir de práticas que são típicas deste modelo de negócio.

A gestão de acesso, por exemplo, é um problema muito comum em centros médicos. Muitas pessoas acessam as aplicações administrativas utilizando senhas fracas e uma maneira de ampliar a segurança é diminuir o volume de profissionais habilitados, além de exigir o uso de senhas fortes, o que também pode incluir a adoção de duplo fator de autenticação, por exemplo.

A segregação de redes, distribuindo por segmentos, também é uma boa dica. Separar a rede dos computadores usados por profissionais que acessam muitos dados sensíveis e/ou que possam ser mais visados por cibercriminosos, como, por exemplo, os executivos ou VIPs, assim como criar uma rede própria para os equipamentos que contemplam sistemas embarcados e que não são atualizados após a perda da garantia, é outra orientação importante.

As recomendações de segurança também valem para os sistemas nos computadores

disponibilizados nas salas de atendimento, que muitas vezes não requerem senhas justamente por serem acessados por vários profissionais que atuam em consultas e emergência. Neste caso, um eventual ataque por meio de engenharia social pode ser facilitado quando o sistema fica 100% disponível na tela, suscetível a ações que comprometam a confidencialidade, como por exemplo, o uso de câmeras fotográficas para registrar dados médicos de terceiros ou até mesmo prontuários, que podem ser posteriormente compartilhados com criminosos cibernéticos.

Do ponto de vista técnico, listo seis orientações que podem restringir as ações criminosas no setor hospitalar:

1. Estabelecer processos em paralelo ou previamente à aquisição de software, como, por exemplo, na compra de antivírus e softwares de gestão vulnerabilidades. Muitas vezes tecnologias são compradas sem a definição de processos, o que resulta em configuração e uso incorretos. Apenas comprar ferramentas não resolve o problema. É preciso estabelecer processos, fluxos e responsáveis;

2. Instalar duplo fator de autenticação nos acessos aos principais sistemas da empresa, com atenção especial aos acessos remotos via VPNs (Rede Privada Virtual);

3. Utilizar uma solução de EDR (Endpoint Detection and Response) para bloqueio de ransomwares e criptografia de arquivos nos servidores, desktops e notebooks;

4. Efetuar testes de invasão periódicos para identificar vulnerabilidades e riscos antes dos atacantes;

5. Implementar o monitoramento dos eventos de segurança por meio de um SOC (Security Operation Center);

6. Realizar um ciclo permanente de gestão de vulnerabilidades do ambiente tecnológico de forma a identificar, priorizar, remediar e retestar.

(*) **Helder Assis** é gerente de Cyber Security e de privacidade de dados na ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados

Fonte: Portal Hospitais Brasil, em 15.09.2021