2024

POR QUE A SEGURANÇA CIBERNÉTICA É IMPORTANTE PARA O SETOR DA SAÚDE?

A chave para proteger instituições de saúde na Era da Cibersegurança

WWW.LATUSEGUROS.COM

latú Seguros

POR QUE A SEGURANÇA CIBERNÉTICA É IMPORTANTE PARA O SETOR DA SAÚDE?

Instituições de saúde lidam com dados sensíveis de pacientes, o que as torna alvos atrativos para cibercriminosos. **A exposição de dados médicos pode causar danos irreparáveis à reputação e trazer altos custos regulatórios.**

Conheça os aspectos mais importantes para proteger instituições de saúde na era da cibersegurança.

Vazamentos de informações, interrupção de serviços críticos e danos à reputação são apenas alguns dos riscos envolvidos. Este e-book explora as principais vulnerabilidades tecnológicas e **como o Seguro Cyber pode ajudar a mitigar esses riscos, garantindo a proteção de pacientes e a continuidade dos serviços**.

Principais fatores de risco para instituições de saúde:

Quantidade de dados.

Vazamentos de dados de saúde afetam a privacidade dos pacientes, gerando desconfiança e possíveis ações legais.

Sensibilidade dos dados.

Um incidente pode destruir a confiança na instituição, afastando pacientes e parceiros.

Riscos operacionais.

Ataques cibernéticos podem interromper serviços críticos, colocando a vida dos pacientes em risco.

Exposições tecnológicas únicas e seus riscos.

As tecnologias essenciais no setor de saúde criam **riscos cibernéticos específicos**:

01 Sistemas de ERP para clínicas.

O software ERP pode conter vulnerabilidades de segurança que podem ser exploradas por cibercriminosos para obter acesso não autorizado aos sistemas da clínica.A segurança dos dados da clínica depende das práticas de segurança do fornecedor do ERP.

02 Plataforma de comunicação como e-mail ou whatsapp

Fluxo de informaçoes sensiveis por esses canais sem uma proteção adequada, pode ser uma porta de entrada para cibercriminosos.

03 Dispositivos médicos.

Equipamentos desatualizados são vulneráveis a ataques, afetando a segurança do paciente.

04 Telemedicina.

Plataformas vulneráveis expõem organizações de saúde a ataques de phishing e malware.

Exemplos reais de vazamento de dados:

Ministério da Saúde - 2020

Dados de 243 milhões de brasileiros foram expostos na internet devido a falhas de segurança no SUS, comprometendo informações pessoais como nome, CPF e endereço.

CLIQUE AQUI PARA LER

Clínicas brasileiras sofrem vazamento

Os hackers publicaram imagens íntimas e dados financeiros dos pacientes de consultórios de cirurgia plástica do Rio Grande do Sul e do Paraná.

CLIQUE AQUI PARA LER

Esses incidentes ressaltam a necessidade de proteger dados sensíveis e de adotar seguros cibernéticos que cubram custos de recuperação e mitiguem danos reputacionais.

> *Empresas de RaaS (Ransomware as a service) comprometeram entidades de saúde e destacaram que conseguiram acessar - e forneceram visualizações de - dados e registros confidenciais, incluindo fotos de pacientes, em postagens do DLS.*
>
> **FONTE: GLOBALTHREATREPORT2024- CROWDSTRIKE**

Mitigação de riscos com **medidas de cibersegurança para instituições de saúde**:

01 Proteção de dados de pacientes.

Uso de criptografia e controles rigorosos de acesso para proteger informações sensíveis, como registros médicos e dados pessoais.

02 Treinamento de equipe clínica e administrativa.

Capacitação contínua para reconhecer ameaças como phishing e ransomware, reduzindo erros humanos que possam comprometer a segurança.

03 Soluções tecnológicas especializadas.

Implementação de firewalls, antivírus e monitoramento constante para detectar vulnerabilidades e proteger sistemas de ERP e prontuários eletrônicos.

A importância do **Seguro Cyber**:

Instituições de saúde lidam com grandes volumes de dados sensíveis e são alvos frequentes de ataques como ransomware e phishing. Com o aumento das ameaças cibernéticas e a complexidade dos dados gerenciados, o seguro cibernético é essencial para mitigar riscos financeiros, garantir continuidade dos serviços, cumprir regulamentações como a LGPD e **acessar especialistas para resposta rápida a incidentes, protegendo a instituição e seus pacientes**.

Como atuar no caso de sofrer um ataque cibernético:

Em caso de ataque cibernético, **siga as etapas a seguir para minimizar os danos**:

01 Se sua empresa já tiver Seguro Cyber: **notificar a seguradora**.

Imediatamente reportar o incidente à seguradora. Isso permite que as coberturas como resposta incidentes e custos forenses sejam ativadas, proporcionando suporte financeiro e acesso a equipes especializadas que auxiliarão na gestão e mitigação do incidente.

02 Identificar e conter o incidente.

Após notificar a seguradora, **é crucial identificar a origem e a extensão do incidente**. Isolar os sistemas afetados impede a propagação do ataque. Desconecte dispositivos comprometidos e preserve evidências para análises futuras, garantindo uma resposta eficaz e informada.

03 Avaliar o impacto e documentar tudo.

Compreenda quais dados ou sistemas foram comprometidos e como isso afeta clientes e operações. **Documente detalhadamente todas as ações tomadas durante e após o incidente.** Essa documentação é vital para questões legais, auditorias e para aprimorar futuras respostas a incidentes.

04 Notificar partes **interessadas** e cumprir obrigações legais.

Comunique o incidente de forma transparente à clientes afetados, parceiros comerciais e autoridades regulatórias, conforme exigido por lei. Cumprir obrigações legais e regulatórias é essencial para evitar penalidades e manter a confiança das partes envolvidas.

05 Remediar sistemas e fortalecer a segurança.

Corrija as vulnerabilidades exploradas pelo ataque atualizando softwares, reforçando medidas de segurança e aplicando patches necessários. Engaje equipes especializadas internas e externas, incluindo suporte oferecido pela seguradora, para gerenciar a crise de forma eficaz.

Conclusão.

Em um setor onde a confiança é primordial e a proteção de dados é vital, a cibersegurança se torna essencial para a continuidade das operações nas instituições de saúde. Com o crescimento exponencial dos ataques cibernéticos e o manuseio de informações sensíveis de pacientes, proteger esses dados é mais do que uma questão de conformidade — é uma responsabilidade ética.

A adoção de medidas de segurança robustas, combinadas com o Seguro Cyber, proporciona uma defesa sólida contra as ameaças digitais que podem comprometer tanto a reputação quanto a operação das instituições de saúde. Ao implementar soluções tecnológicas avançadas e investir em treinamento contínuo dos funcionários, é possível mitigar os riscos e responder de forma eficiente a incidentes, protegendo a integridade dos serviços médicos.

Com o apoio de um Seguro Cyber, as instituições de saúde conseguem não apenas cobrir os custos de recuperação e cumprir as regulamentações de privacidade, como também fortalecer a confiança de seus pacientes e parceiros, garantindo a segurança de dados sensíveis e a continuidade de um atendimento de qualidade.

Conte conosco!

Fontes:

- CSI Web: Cyber Insurance 101.
- TCS: Cyber Risk Insurance for Financial Services
- Insureon: Cyber Liability for Finance and Accounting Businesses
- https://www.microserviceit.com.br/ataque-hacker/