2024

POR QUE A SEGURANÇA CIBERNÉTICA É IMPORTANTE PARA INSTITUIÇÕES FINANCEIRAS?

A chave para manter instituições financeiras operando na era da cibersegurança.

WWW.LATUSEGUROS.COM

latú Seguros

A importância da segurança cibernética para instituições financeiras

Neste e-book, exploramos a crescente importância da segurança cibernética para instituições financeiras, que lidam com dados altamente sensíveis e enfrentam uma gama de ameaças. Com exemplos reais de ataques e insights sobre como mitigar riscos, **abordamos o papel do Seguro Cyber na proteção contra perdas financeiras e na recuperação rápida após incidentes**. Ao transferir esses riscos significativos para uma seguradora, as instituições financeiras protegem sua estabilidade econômica e preservam a confiança dos clientes diante de ameaças cibernéticas cada vez mais sofisticadas.

Principais fatores de risco para instituições financeiras:

Interrupção de Negócios.

Brechas cibernéticas podem introduzir malware em sistemas internos, especialmente com a conectividade heterogênea da web e de dispositivos móveis, complicando a avaliação da exposição ao risco e causando **interrupções nos serviços, o que afeta a confiança do cliente e a eficiência operacional**.

Risco reputacional.

Avaliar o impacto financeiro da exposição cibernética é complexo. **As perdas incluem não apenas o impacto imediato, mas também oportunidades de negócios perdidas e danos de longo prazo** à marca.

Riscos Regulatórios.

No setor financeiro altamente regulamentado, interrupções causadas por incidentes cibernéticos podem levar ao **roubo de identidade, transações não autorizadas e fraudes, resultando em responsabilidades legais significativas e problemas de conformidade** para CISO's ou DPO's.

A indústria financeira na América Latina é a **mais atacada por Spider Malware**, segundo o Relatório de Ameaças Globais da CrowdStrike,

> *Ataques cibernéticos geram perdas de US$ 12 bilhões ao setor financeiro global.*
>
> **FONTE: FUNDO MONETÁRIO INTERNACIONAL (FMI)**

Exemplos reais de incidentes cibernéticos:

Banco de Brasília - BRB

Alvo de ransomware, com hackers exigindo 50 bitcoins (cerca deR$ 5,17 milhões) para evitar o vazamento de dados.

CLIQUE AQUI PARA LER

Banco do Brasil

Hackers desviaram R$ 40 milhões ao instalar dispositivos em cabos de dados nas agências, realizando transferências de correntistas.

CLIQUE AQUI PARA LER

A importância do **Seguro Cyber**:

O Seguro Cyber proporciona uma rede de segurança crucial, minimizando perdas financeiras e permitindo uma recuperação mais rápida após incidentes. Com o aumento dos ataques cibernéticos, possuir Seguro Cyber, juntamente com medidas de cibersegurança robustas - como firewalls,

Coberturas Essenciais do Seguro Cyber:

01

Danos ao **próprio segurado**.

Protege contra perdas diretas, incluindo recuperação de dados, custos de notificação, perdas por interrupção de negócios e custos relacionados à extorsão cibernética ou ransomware.

02

Responsabilidade por **danos a terceiros**.

Oferece proteção contra responsabilidades decorrentes de vazamento de dados, custos legais e multas regulatórias.

Mitigação de riscos com medidas de cibersegurança:

Instituições financeiras devem adotar **práticas de segurança cibernética específicas** como:

- Implementar **Autenticação Forte do Cliente (SCA)** conforme a Resolução BACEN n.º 4.658 e a LGPD.
- Implantar **sistemas avançados de monitoramento** de transações e detecção de fraudes.
- Adotar **padrões rigorosos de conformidade e segurança** (PCI DSS, ISO 27001).
- Realizar **avaliações de risco e testes de penetração** focados em ameaças financeiras.
- Incorpore **análise de identidade** para detecção e prevenção avançadas de fraudes.

Instituições financeiras devem **exigir segurança cibernética de seus fornecedores**?

As instituições financeiras precisam garantir que seus fornecedores adotem medidas mínimas de segurança cibernética ou possuam seguro cibernético. Essas medidas protegem dados sensíveis, reduzem o risco de violações e evitam perdas financeiras e danos à reputação. **Ao impor essas exigências, as instituições ampliam o perímetro tecnológico que controlam, fortalecendo a segurança geral.** Isso também assegura a conformidade regulatória, mantém a confiança dos clientes e protege tanto a instituição quanto seus clientes contra ameaças cibernéticas.

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 tem Seguro Cyber, **notifique a seguradora**:

assim que detectar um incidente, comunique-o imediatamente à seguradora. Isso permitirá a ativação das coberturas contratadas, como a resposta a incidentes e os serviços forenses. Além disso, garante suporte financeiro e acesso a equipes especializadas que auxiliarão na mitigação do impacto.

02 **Identificar e conter** o incidente:

após notificar a seguradora, **é fundamental identificar a origem e a extensão do incidente e isolar os sistemas afetados para impedir a propagação**. Desconecte dispositivos comprometidos e preserve evidências para futuras análises, garantindo uma resposta informada e eficaz.

03 Avaliar o impacto e **documentar tudo**:

compreenda quais dados e sistemas foram comprometidos e como isso afeta clientes e operações. Documente detalhadamente todas as ações tomadas durante o incidente. **Essa documentação é essencial para auditorias, questões legais e aprimoramento de futuras respostas a incidentes.**

04 Notificar as partes interessadas e **cumprir obrigações legais**:

comunique o incidente de forma transparente a clientes afetados, parceiros comerciais e autoridades regulatórias, conforme exigido por lei. Cumprir essas obrigações é fundamental 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. Envolva equipes especializadas internas e externas, incluindo o suporte oferecido pela seguradora, para gerenciar a crise de forma eficaz.

Essas medidas não apenas ajudam a conter o impacto, mas também garantem que a organização se recupere mais rapidamente. **O Seguro Cyber é essencial para cobrir os custos associados a essas ações e mitigar as perdas financeiras e reputacionais após um ataque.**

Oferecer Seguro Cyber para instituições financeiras não só proporciona proteção, mas também fortalece todo o ecossistema financeiro, reduzindo riscos. O Seguro Cyber complementa práticas de segurança robustas, criando uma defesa resiliente contra ameaças.

Conclusão.

À medida que o panorama digital continua a evoluir, a cibersegurança se torna um pilar fundamental para garantir a continuidade das operações nas instituições financeiras. **Com a crescente sofisticação dos ataques cibernéticos, a combinação de medidas preventivas de segurança e a adoção de seguros cibernéticos se mostra essencial para proteger ativos, dados sensíveis e a reputação das organizações.**

Proteger-se contra as ameaças cibernéticas vai além de um simples protocolo de segurança. Envolve uma abordagem proativa, onde a tecnologia e o seguro caminham lado a lado, garantindo não apenas a mitigação de riscos, mas também uma rápida recuperação após incidentes. Ao adotar essas práticas, as instituições financeiras não só protegem a si mesmas, como também contribuem para a estabilidade do setor, fortalecendo a confiança de clientes e parceiros.

Portanto, **ao incorporar estratégias robustas de cibersegurança e investir em Seguro Cyber, as instituições financeiras podem enfrentar com mais segurança os desafios do ambiente digital**, garantindo um futuro mais seguro e resiliente.

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/