2024

ATAQUES CIBERNÉTICOS À EMPRESAS BRASILEIRAS

Lições de Segurança
e Conformidade para Empresas

WWW.LATUSEGUROS.COM

latú Seguros

OPPOnet

ATAQUES CIBERNÉTICOS À EMPRESAS BRASILEIRAS

Casos Vivara e EstrelaBet e a necessidade de proteção.

Nos últimos tempos, **grandes empresas brasileiras têm sido alvo de ataques cibernéticos devastadores**, destacando a crescente ameaça que essas invasões representam para a segurança corporativa. **Recentemente, a joalheria Vivara e a casa de apostas EstrelaBet enfrentaram incidentes graves**, com consequências potencialmente catastróficas para suas operações e reputação.

O que você vai encontrar **NESSE E-BOOK**?

01

O que aconteceu?

Vivara e EstrelaBet sofreram ataques cibernéticos com vazamento de dados sensíveis, impactando milhões de usuários.

02

O que são esse tipo de ataques?

Ransomware criptografa dados e exige resgate. Vazamentos expõem informações, causando perda de confiança e penalidades legais.

03

Pilares de proteção contra ataques cibernéticos.

A conformidade com a LGPD e o Seguro Cyber são essenciais para mitigar danos de ataques cibernéticos e evitar perdas graves.

04

Dê o primeiro passo para proteger sua empresa

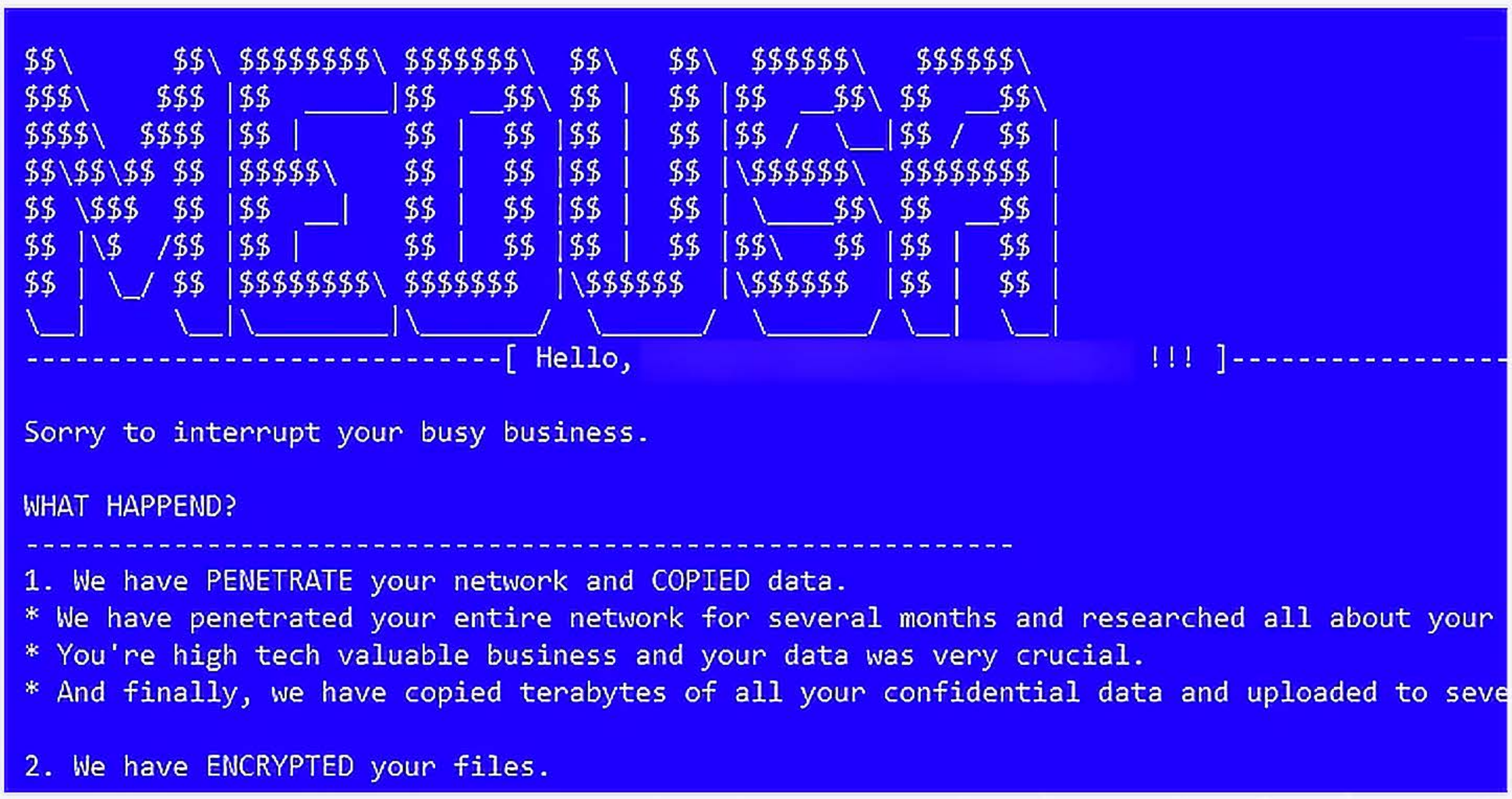
Ataques cibernéticos ressaltam riscos digitais. Oferecemos avaliação de risco cibernético com a Latú Seguros para proteção.

WWW.**LATUSEGUROS**.COM

O que aconteceu?

A joalheria Vivara foi atacada pelo ransomware Medusa, com hackers exigindo um resgate de US$ 600 mil para não divulgarem 1,18 TB de dados roubados, incluindo informações sensíveis de executivos, clientes e até do CEO da empresa. Entre os dados comprometidos estavam documentos financeiros, fotos pessoais, planilhas e e-mails. Foi dado à Vivara o prazo de oito dias para pagar o resgate, sob a ameaça de divulgação pública dos dados.

Outro incidente preocupante foi o vazamento de dados sofrido pela EstrelaBet, uma popular casa de apostas no Brasil. De acordo com informações recentes, uma falha de segurança resultou na exposição de 3 milhões de registros de usuários, incluindo informações pessoais e financeiras. Este vazamento coloca em risco a privacidade dos usuários e expõe a empresa a possíveis sanções e perda de confiança.



O que são esses tipos de ataque?

Um ataque de ransomware é uma forma de crime cibernético em que hackers infectam os sistemas de uma empresa com um software malicioso que criptografa os dados, tornando-os inacessíveis. Os criminosos então exigem um pagamento, geralmente em criptomoedas, para fornecer a chave de descriptografia que restaura o acesso aos dados. Esses ataques são especialmente perigosos porque podem paralisar as operações de uma empresa e resultar em perdas financeiras significativas.

> *Medusa, que não deve ser confundido com Medusa Locker, se refere a uma família de ransomware que surgiu no final de 2022, ganhando destaque em 2023.*
> *É **conhecida por atacar oportunisticamente uma ampla gama de indústrias, como alta tecnologia, educação, manufatura, saúde e varejo**.*
>
> **FONTE:** THEHACKERNEWS.COM

Um vazamento de dados ocorre quando informações sensíveis de uma empresa ou de seus clientes são expostas sem autorização. Isso pode acontecer por meio de ataques cibernéticos, falhas de segurança ou até mesmo erros humanos.

As consequências de um vazamento de dados incluem perda de confiança dos clientes, danos à reputação da empresa e possíveis penalidades legais, especialmente se a empresa não estiver em conformidade com regulamentos como a Lei Geral de Proteção de Dados (LGPD). Da mesma forma, a empresa é obrigada a comunicar a todos os seus clientes ou aliados que seus dados foram roubados, o que implica uma exposição muito grande a serem processados judicialmente.

> *A Lei Geral de Proteção de Dados Pessoais (LGPD) determina que "o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares".*
>
> **FONTE:** GOV.BR

Pilares de proteção contra ataques cibernéticos.

É importante estar sempre preparado para situações como essas, mitigando os riscos que estão ao seu alcance e transferindo a outra parte dos riscos para que a empresa não sofra consequências catastróficas caso isso ocorra.

Estar em conformidade com a LGPD é fundamental para mitigar os danos de um ataque cibernético. A LGPD exige que as empresas adotem medidas de segurança rigorosas para proteger os dados pessoais que coletam e processam. Em caso de falha em proteger essas informações, as empresas podem enfrentar multas que podem chegar a até 2% do faturamento anual, até R$ 50 milhões por infração.

No caso de um ataque como o sofrido pela Vivara, **a conformidade com a LGPD não apenas minimiza o risco de multas adicionais, mas também demonstra um compromisso com a privacidade e a segurança dos dados dos clientes**. Empresas que não se alinham às exigências da LGPD correm o risco de sofrer danos reputacionais severos, além de perdas financeiras significativas.

Além dessas ações, **ter um Seguro Cyber pode ser a diferença entre uma recuperação rápida e a destruição financeira e reputacional de uma empresa**. Embora a Vivara ou Estrelabet não tenha divulgado se possui um Seguro Cyber, este tipo de apólice oferece coberturas cruciais em cenários de ataques cibernéticos:

01 Custos de Extorsão Cibernética.

Uma das principais coberturas é a de extorsão cibernética, que **auxilia no pagamento de resgates exigidos pelos hackers**. No caso da Vivara, essa cobertura poderia ajudar a mitigar o impacto financeiro imediato e potencialmente evitar a divulgação dos dados roubados.

02 Custos Forenses.

Após um ataque, é essencial entender a extensão da violação e como ela ocorreu. O Seguro Cyber **cobre os custos com especialistas em cibersegurança que investigam o incidente, identificam vulnerabilidades e ajudam a restaurar os sistemas comprometidos**. Essa investigação é vital para evitar futuros ataques e reforçar a segurança da empresa.

03 Responsabilidade por Danos a Terceiros.

O vazamento de dados pode levar a ações judiciais movidas por clientes, parceiros de negócios e outras partes afetadas. O Seguro Cyber **oferece cobertura para indenizações e custos legais decorrentes dessas ações, ajudando a empresa a lidar com as consequências jurídicas do ataque**.

Dê o primeiro passo para proteger a sua empresa.

Esses ataques cibernéticos são um lembrete contundente dos riscos que todas as empresas enfrentam no ambiente digital atual. **O primeiro passo para se proteger é conhecer as vulnerabilidades da superfície tecnológica da sua empresa e trabalhar para eliminá-las.**

Para isso, **a Latú Seguros oferece uma avaliação de risco cibernético para todos os seus clientes e também para os clientes DPOnet**. Essa avaliação é essencial para identificar os pontos fracos que podem ser explorados por hackers e implementar as medidas necessárias para fortalecer a segurança cibernética da sua empresa.

Clique aqui e solicite sua avaliação de risco cibernéticos agora!

QUEM É A LATÚ?

Proteção abrangente para empresas em caso de violações de dados e ameaças cibernéticas.

A Latú é uma insurtech inovadora, especializada em oferecer soluções holísticas de Seguro Cyber. Unindo tecnologia de ponta, expertise em cibersegurança e profunda experiência em seguros, estamos empenhados em ajudar organizações a avaliar, prevenir e responder prontamente a um panorama de riscos digitais em rápida transformação.

Sempre em parceria com corretores, **nossa prioridade é entregar os melhores produtos aos corretores e seus clientes**. Estamos ao lado dos corretores em todas as etapas, garantindo que tenham os recursos e o suporte necessários para apresentar soluções de excelência.

Nossa plataforma "**Latú Sonar**" avalia um conjunto abrangente de dados públicos, inteligência de ameaças e informações proprietárias de sinistros, fornecendo avaliações de risco personalizadas e um monitoramento de ameaças que ultrapassa os padrões dos seguros tradicionais. Assim, conseguimos ofereceer suporte preventivo contínuo à nossos corretores parceiros e clientes.

Com o apoio de investidores de renome tanto no Brasil quanto no Vale do Silício, nos EUA, **a Latú reforça seu compromisso e capacidade de inovação no segmento de Seguro Cyber**.

Conclusão.

Investir em seguros cibernéticos e estar em conformidade com a LGPD são passos cruciais para proteger sua empresa contra as consequências devastadoras de ataques cibernéticos. Essas medidas não apenas protegem contra as perdas financeiras imediatas, mas também ajudam a preservar a confiança dos clientes e a reputação da empresa.

Garanta que sua empresa esteja pronta para enfrentar as ameaças do mundo digital, com as ferramentas e proteções necessárias para continuar operando de forma segura e eficiente.

Conte conosco!

WWW.LATUSEGUROS.COM

latú Seguros

Aviso Legal:

Todas as informações contidas neste e-book são apenas para referência e devem ser consideradas como um guia geral. Cada caso pode variar conforme as especificidades envolvidas. Recomendamos fortemente que entre em contato conosco para obter detalhes específicos relacionados ao seu caso, bem como para acessar as condições gerais e demais informações pertinentes.

A Latú Seguros irá no mercado com um representante de seguros, um tipo de associação devidamente regulamentado pela resolução de número 431 de 11 de Novembro de 2021 do Conselho Nacional de Seguros Privados (CNSP). Um representante de seguros é autorizado a promover, ofertar e distribuir produtos de seguros em nome de uma sociedade seguradora parceira.

Este material não se destina a fornecer, e não deve ser interpretado como, aconselhamento jurídico ou profissional. A precisão, completude ou atualidade das informações não são garantidas. Não nos responsabilizamos por quaisquer erros ou omissões, nem por resultados obtidos a partir do uso destas informações.