RCG
Risk Consulting Group
HERCO

Cyber SECURITY SERVICE

Este é um guia básico de informações desenvolvido por nossos especialistas, para trazer um pouco mais de conhecimento sobre esse mercado em expansão.

GUIA BÁSICO

Para mais informações
rcgherco.com

A RCG

Com mais de 50 anos de experiência, a RCG| Powered by Herco é hoje conhecida como modelo de excelência na análise de risco, controle de perdas e implantação de programas de gestão de riscos.
A empresa fornece serviços em nível mundial para diversos segmentos da indústria com equipe técnica multidisciplinar composta por engenheiros, técnicos e especialistas.
Apoiamos as organizações a melhor compreender o impacto dos riscos a que estão expostas e a implementar um framework de Gestão de Risco ajustada a cada empresa e que responda às necessidades da correta identificação, análise, mitigação e financiamento dos riscos.
Temos uma equipe altamente qualificada com uma vasta experiência na gestão de risco em diversas áreas.
Avaliamos os riscos das suas operações em qualquer parte do mundo para potenciar a segurança dos seus investimentos, otimizando a redução de risco de prejuízos patrimoniais e a adequação dos programas de seguros.

Nosso impacto no globo

INTRODUÇÃO

No mundo altamente conectado de hoje, a segurança cibernética tornou-se uma preocupação central para muitas empresas e governos. Com a crescente dependência de tecnologias para o desenvolvimento das corporações, **proteger informações e sistemas contra ameaças cibernéticas é mais crítico do que nunca**. Este ebook foi desenvolvido para fornecer uma compreensão abrangente do ambiente cibernético, destacar as ameaças que enfrentamos e oferecer estratégias eficazes para mitigar riscos.

Exploraremos a importância do ciberespaço em nosso mundo globalizado. Discutiremos as diversas formas de ameaças cibernéticas, desde ransomware e phishing até malware e ataques de negação de serviço, examinando como essas ameaças podem impactar financeiramente e operacionalmente tanto indivíduos quanto organizações.

O AMBIENTE CIBERNÉTICO E OS PERIGOS

O que é um ambiente cibernético?

O ambiente cibernético, ou ciberespaço, refere-se à rede interconectada de sistemas de informação, dispositivos de comunicação, infraestruturas digitais e serviços baseados na internet. Ele engloba tudo, desde redes privadas e públicas até a nuvem. Desde a criação da ARPANET, o ciberespaço evoluiu significativamente, transformando-se em uma infraestrutura global essencial para a comunicação, comércio, entretenimento e governança.

A importância do ambiente cibernético no mundo globalizado não pode ser subestimada. No comércio eletrônico, ele facilitou transações comerciais rápidas e eficientes, permitindo o crescimento de mercados globais.

Ameaças cibernéticas

Ameaças cibernéticas são **ações maliciosas** que visam comprometer a integridade, confidencialidade e disponibilidade dos sistemas de informação. Essas ameaças podem ser originadas por hackers, insiders maliciosos, grupos hacktivistas ou até mesmo estados-nação.

- **Ransomware:** É uma espécie de Malware que criptografa dados e exige resgate para desbloqueá-los.
- **Phishing:** São técnicas fraudulentas para obter informações sensíveis, como senhas e dados de cartão de crédito.
- **Malware:** É um software malicioso projetado para causar danos a sistemas ou roubar informações.
- **Ataques de negação de serviço (DDoS):** São tentativas de tornar um serviço online indisponível sobrecarregando-o com tráfego.

ASSESMENT CYBER

A avaliação de risco cibernético atualmente se mostra como uma análise de suma importância para a segurança digital de qualquer organização. Essa metodologia permite identificar, quantificar e priorizar os riscos associados às ameaças cibernéticas a que a empresa está vulnerável. Com a crescente dependência da tecnologia, essas ameaças tornaram-se uma realidade constante. Sem uma avaliação adequada, as organizações podem ser vulneráveis a ataques que podem resultar em perdas financeiras significativas e danos à reputação.

COM UM ESPECIALISTA É MAIS RÁPIDO E PODE SER FEITO EM POUCOS PASSOS

1

Iniciaremos com uma reunião estratégica com os líderes do processo de gestão de cibersegurança da empresa a ser analisada, esta etapa dura em torno de 4 horas, podendo essa ser fracionada em reuniões menores, conforme a agenda dos envolvidos. Nessa reunião serão coletadas as informações necessárias para mapear e projetar o estado de segurança da empresa, sendo os essas obtidas através de um questionário específico desenvolvido pelos time da RCG. Após esta fase ainda podem ser solicitadas informações adicionais por outros meios.

Após a realização das entrevistas, os dados serão tratados e analisados com uma perspectiva técnica e voltada ao mercado segurador. Com esse tipo de verificação é possível ter uma resposta mais adequada as necessidades securitárias e uma perspectiva de um especialista no processo de adequações. Por fim os dados serão compilados e transferidos para um documento na forma de relatório.

2

3

Sendo entregue este relatório será marcada uma reunião de até uma hora para discutir pontos levantados e eventuais esclarecimentos.

QUAIS SÃO OS IMPACTOS DESSES ATAQUES?

Para responder a essa pergunta vamos entender um pouco mais sobre o Ransomware e Malware

Os ataques de ransomware e malware representam uma ameaça crescente no cenário digital atual, causando **impactos financeiros significativos** para organizações de todos os tamanhos. Essas ameaças podem resultar em perdas substanciais, tanto diretas quanto indiretas, afetando severamente as operações e a reputação das empresas.

Ransomware

Ransomware é um tipo de malware que criptografa os dados da vítima, exigindo um resgate para a liberação das informações. Os custos associados a ataques de ransomware são elevados, não apenas pelo valor do resgate, mas também pelos custos adicionais de recuperação e mitigação dos danos.

Oliveira (2023) afirma "Segundo a Forbes, o custo médio de recuperação de um ataque de ransomware é estimado em quase US$ 2 milhões, enquanto a média do custo de um trabalho forense pode ultrapassar a casa dos US$ 70.000"

Malware

O Malware é um software malicioso projetado para causar danos a sistemas e redes. Os impactos financeiros de ataques de malware podem ser devastadores. Esses ataques podem resultar na perda de dados sensíveis, interrupção de operações e custos elevados para a remediação.

Um relatório do Center for Internet Security destacou que os custos associados a ataques de malware incluem a perda de receita, os custos de mitigação e a necessidade de investimentos adicionais em segurança cibernética (CIS, 2022).

QUAIS SÃO OS POSSÍVEIS IMPACTOS FINANCEIROS E OPERACIONAIS

Os ataques cibernéticos afetam financeiramente as empresas de várias maneiras:

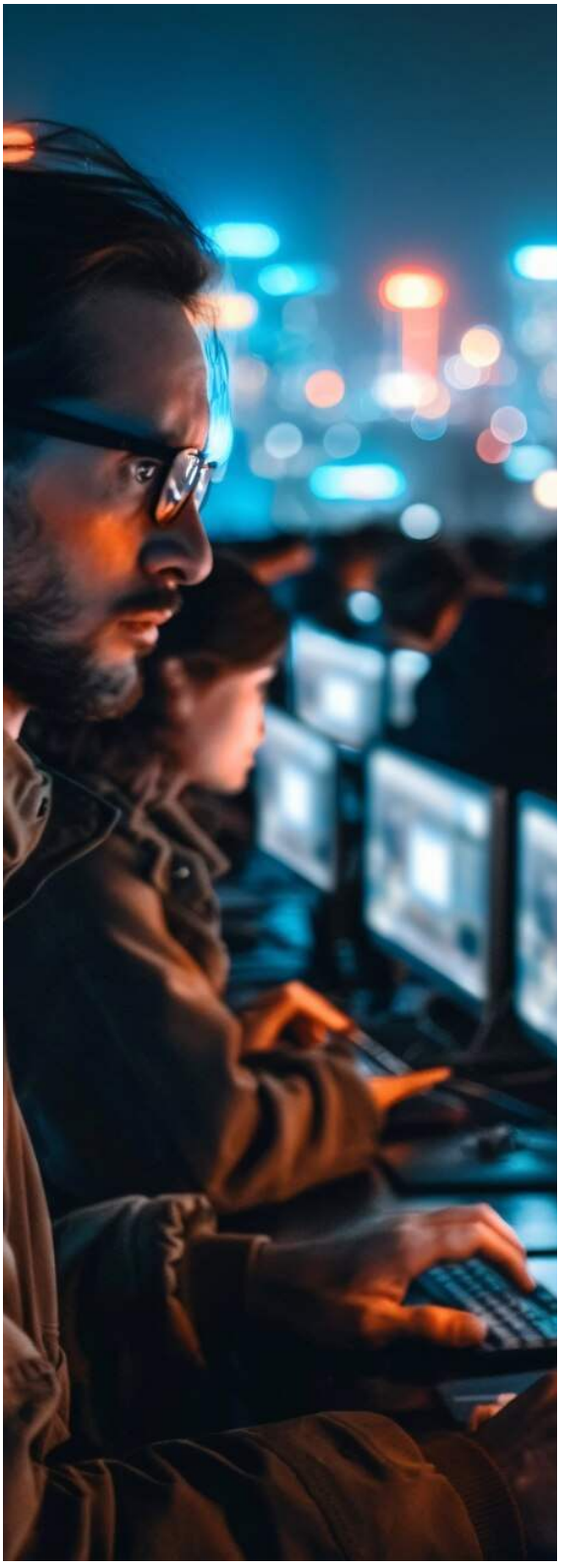
Perda de Receita: A interrupção das operações devido a ataques cibernéticos pode resultar em uma perda significativa de receita. Empresas que dependem de sistemas digitais para suas operações diárias podem enfrentar longos períodos de inatividade, afetando a produção e a entrega de serviços.

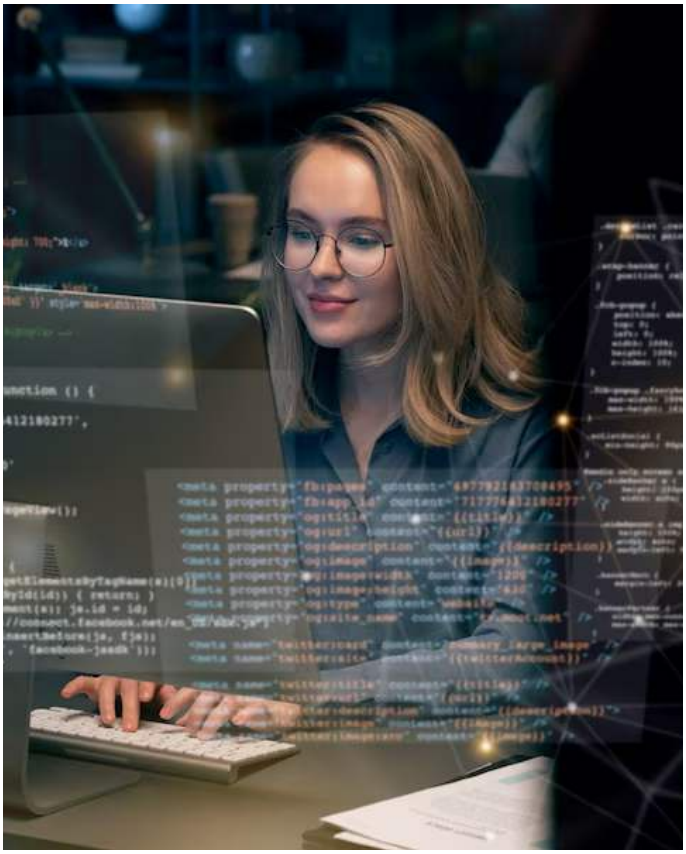
Custos de Remediação: As empresas precisam investir em especialistas de segurança cibernética para restaurar sistemas e proteger a infraestrutura contra futuras ameaças. Isso inclui a implementação de novas medidas de segurança, auditorias e testes regulares de vulnerabilidades.

Multas e Penalidades: Organizações que não cumprem regulamentos de proteção de dados podem enfrentar multas pesadas após um ataque cibernético. Regulamentações como a LGPD impõem penalidades substanciais para violações de dados.

Reputação e Confiança do Cliente: A confiança do cliente pode ser gravemente afetada após um ataque cibernético. A perda de dados sensíveis pode levar à perda de clientes e à diminuição da reputação da marca no mercado.

Em suma, os impactos financeiros de ataques de ransomware e malware são profundos e multifacetados. Além dos custos imediatos associados ao pagamento de resgates e à recuperação de sistemas, as empresas enfrentam desafios de longo prazo em termos de reputação e confiança do cliente, que podem ter repercussões duradouras.





Como podemos evitar esses ataques

Para evitar ataques cibernéticos, é crucial adotar boas práticas de segurança cibernética. Manter todos os sistemas atualizados para corrigir vulnerabilidades conhecidas é essencial. Implementar senhas complexas e autenticação multifator para proteger contas aumenta significativamente a segurança. Além disso, treinamentos regulares para identificar e evitar ameaças cibernéticas são fundamentais para educar e conscientizar os usuários.
Desenvolver políticas de segurança cibernética é outra medida importante, além da política de contingência cibernética deve abranger planos de recuperação de desastres, procedimentos para manter a continuidade dos negócios e backup e restauração de dados críticos.

Por que investir em cibersegurança

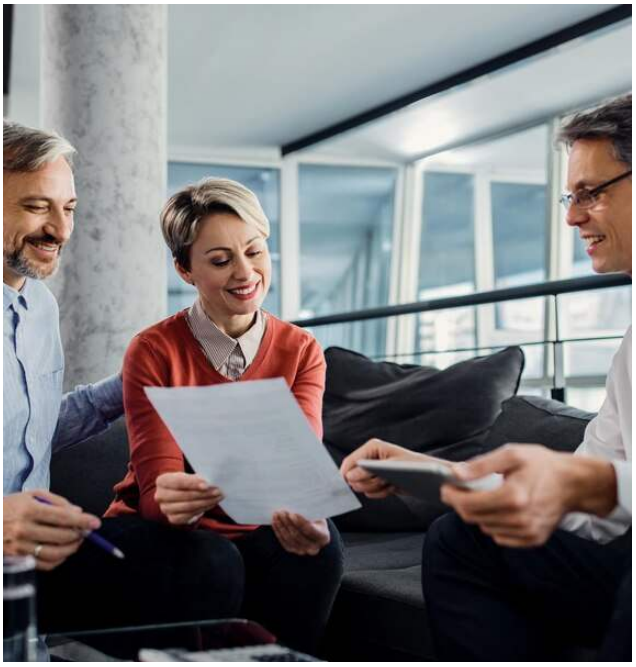
Investir em cibersegurança é uma forma de se resguardar seu patrimônio material e intelectual. Em um mundo cada vez mais digital, a proteção de informações e sistemas é essencial para prevenir interrupções, **perdas financeiras** e **danos reputacionais**. A cibersegurança protege dados sensíveis, prevenindo acessos não autorizados e garantindo a privacidade.

Os benefícios de investir em cibersegurança incluem a prevenção de perdas financeiras, como fraudes, roubos e custos de recuperação de incidentes.

Por que ter um seguro cyber?

Com a evolução tecnológica cada vez mais acelerada e a frequência dos ataques cibernéticos, o investimento em cibersegurança tornou-se essencial para a proteção das operações e da reputação das empresas. A seguir, exploramos os motivos para esse investimento e a importância de contar com uma apólice de seguro cibernético adequada.

Investir em cibersegurança não é apenas uma questão de proteção contra **perdas financeiras imediatas**, mas também uma medida preventiva contra riscos de longo prazo que podem comprometer a viabilidade e a credibilidade das organizações. A cibersegurança eficaz envolve a implementação de uma abordagem técnica qualitativa e que possa ser combinada a tecnologias avançadas, processos robustos e uma cultura organizacional consciente de segurança. Isso inclui a utilização de firewalls, sistemas de detecção de intrusão, criptografia de dados, e treinamentos regulares para funcionários.



Cobertura Financeira Ampla: Um seguro cibernético oferece proteção financeira contra diversos tipos de perdas causadas por incidentes cibernéticos, incluindo custos de resposta a incidentes, perda de receita devido à interrupção de negócios, e despesas legais e regulatórias. Algumas seguradoras podem disponibilizar de coberturas que podem incluir ainda os custos de notificação aos clientes, serviços de monitoramento de crédito, e apoio técnico especializado para mitigar e resolver o incidente.

Gerenciamento de Risco: As apólices de seguro cibernético ajudam as empresas a identificar e avaliar seus riscos cibernéticos, permitindo a implementação de medidas de mitigação específicas. Além de fornecer cobertura financeira, as seguradoras frequentemente oferecem serviços de consultoria para ajudar as empresas a melhorar suas defesas cibernéticas e reduzir a probabilidade de futuros ataques.

Resiliência Operacional: Um seguro cibernético contribui para a resiliência operativa, garantindo que as empresas possam se recuperar rapidamente após um incidente cibernético. A importância de planos de continuidade de negócios e de recuperação de desastres que são suportados por seguros cibernéticos, permitindo uma recuperação eficiente e minimizando o impacto nas operações.

RCG Risk Consulting Group POWERED BY HERCO

CONTATO

+55 47 9 9120-4402

rhuan.floriano@rcgherco.com

@rcgherco

www.rcgherco.com

Blumenau/SC e São Paulo/SP

SEGUNDA A SEXTA

Das 8:30 am to 5:00 pm