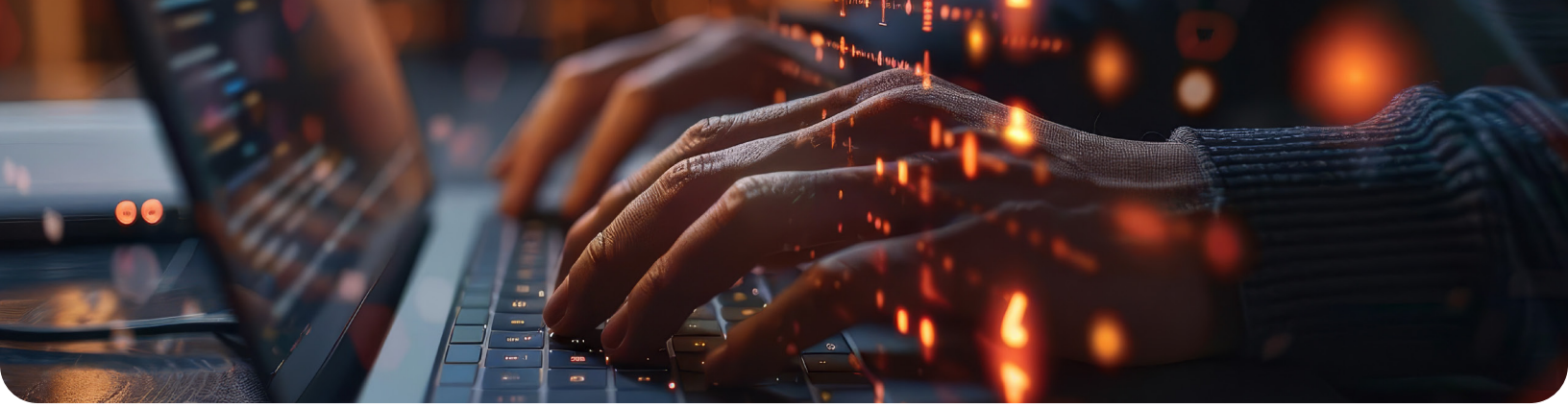


Não caia nestas ameaças cibernéticas

Um guia completo

Os cibercriminosos estão ficando mais sofisticados, e empresas de todos os portes estão em risco. Sejam e-mails de phishing enviados para roubar credenciais de login, ataques de ransomware que bloqueiam o acesso aos seus dados ou vulnerabilidades em dispositivos conectados, as ameaças cibernéticas têm consequências devastadoras. Entender essas ameaças e tomar medidas proativas para proteger sua empresa pode ajudar a evitar violações dispendiosas, tempo de inatividade e danos à reputação. Veja tudo o que você precisa saber.



1. Ataques de phishing com inteligência artificial

Os cibercriminosos utilizam inteligência artificial (IA) para criar e-mails de phishing convincentes, o que torna a identificação de mensagens fraudulentas mais difícil do que nunca. Esses ataques enganam os funcionários para que revelem informações confidenciais, como senhas ou detalhes financeiros, ou para que baixem malware em seus sistemas.

Os riscos

- Violações de dados: credenciais roubadas podem levar a acessos não autorizados a dados confidenciais da empresa.
- Prejuízo financeiro: golpes de phishing podem resultar em transações fraudulentas, fraudes por transferência bancária ou infecções por ransomware.
- Dano à reputação: uma violação de dados pode prejudicar a confiança dos clientes finais e parceiros.

Você sabia?

O phishing representou 83% de todas as ameaças por e-mail, enquanto ataques avançados corresponderam a apenas 1%.

(Fonte: Acronis Cyberthreats Report, H2 2025)

Como garantir a proteção da sua empresa

- Treine seus funcionários: instrua regularmente sua equipe para que ela saiba identificar tentativas de phishing, verificar os remetentes de e-mails e relatar mensagens suspeitas.
- Implemente filtros de segurança de e-mail: ferramentas de filtragem avançadas ajudam a detectar e bloquear e-mails de phishing antes que eles cheguem às caixas de entrada.
- Tenha um plano de resposta a incidentes: prepare uma estratégia bem definida para responder a ataques de phishing e mitigar rapidamente os danos.
- Use a autenticação multifator (MFA): adicionar uma camada de segurança extra dificulta o acesso de invasores a contas, mesmo que as senhas tenham sido comprometidas.



2.
Ataques à cadeia de suprimentos

Um ataque à cadeia de suprimentos ocorre quando cibercriminosos têm como alvo um fornecedor ou terceiro para obter acesso à sua empresa. Se um dos seus provedores de serviços for comprometido, seus dados, operações e sistemas poderão estar em risco.

Os riscos

- Violações de dados: um fornecedor comprometido pode expor dados confidenciais de clientes ou da empresa.
- Disrupção operacional: ataques cibernéticos a fornecedores podem levar a tempo de inatividade e interrupções nos negócios.
- Impacto financeiro e jurídico: as empresas podem ser multadas ou processadas judicialmente se os dados de clientes forem comprometidos devido à baixa segurança da cadeia de fornecimento.

Você sabia?

Comprometimentos de fornecedores terceirizados e da cadeia de suprimentos custam, em média, US$ 4,91 milhões.

(Fonte: IBM, julho de 2025)

Recomendações para os seus negócios

- Avalie seus fornecedores: garanta que os provedores de terceiros sigam protocolos de segurança cibernética rígidos antes de conceder a eles acesso aos seus sistemas.
- Limite o acesso: conceda aos fornecedores apenas o nível mínimo de acessibilidade necessário para que eles realizem seu trabalho e revise regularmente as permissões.
- Inclua cláusulas de segurança cibernética nos contratos: responsabilize os fornecedores pela manutenção de padrões de segurança rígidos.
- Realize auditorias de segurança regulares: avalie o procedimento de segurança da sua cadeia de suprimentos e corrija as vulnerabilidades.



3. Ransomware como serviço (RaaS)

Os ataques de ransomware estão em ascensão, e os cibercriminosos estão facilitando a vida de qualquer pessoa — mesmo aquelas com pouca experiência em TI — para realizar ataques devastadores. Esse modelo, conhecido como ransomware como serviço (RaaS), permite que os invasores aluguem ferramentas de ransomware e lucrem com os pagamentos de resgate.

Os riscos

- Perda de dados: os invasores criptografam seus arquivos e exigem pagamento para liberá-los.
- Tempo de inatividade operacional: as empresas podem ser forçadas a interromper suas operações, o que leva a perdas financeiras.
- Sem garantia de recuperação: mesmo que o resgate seja pago, não há garantia de que os dados serão restaurados.

Você sabia?

80% dos fornecedores de ransomware-as-a-service (RaaS) anunciam recursos de IA ou automação, operacionalizando a IA para escalar ataques existentes.

(Fonte: Acronis Cyberthreats Report, H2 2025)

Como garantir a proteção da sua empresa

- Faça backup dos seus dados regularmente: armazene os backups em locais seguros e fora das instalações da empresa e teste os procedimentos de recuperação.
- Instrua os funcionários: treine os funcionários para reconhecer ameaças de ransomware e evitar clicar em links ou anexos suspeitos.
- Mantenha o software atualizado: aplique patches para corrigir vulnerabilidades em sistemas operacionais, aplicativos e plug-ins.
- Use a segmentação de rede: restrinja a propagação de malware separando sistemas críticos de outras áreas da rede.



4. Vulnerabilidades da Internet das Coisas (IoT)

Dispositivos conectados, como câmeras inteligentes, termostatos e sensores industriais, melhoram a eficiência, mas também introduzem riscos de segurança. Muitos dispositivos de IoT têm configurações de segurança fracas, o que os torna destinos fáceis para hackers.

Os riscos

- Violações de dados: hackers podem explorar as vulnerabilidades do IoT para acessar seus sistemas.
- Comprometimento da rede: dispositivos comprometidos podem ser usados para realizar ataques cibernéticos em larga escala.
- Riscos de segurança física: invasores podem manipular fechaduras ou sistemas de segurança inteligentes.

Você sabia?

24% das organizações afirmam que o maior desafio para se tornarem ciber-resilientes é a falta de visibilidade nos ambientes de TI, OT e IoT.

(Fonte: World Economic Forum, janeiro de 2026)

Como garantir a proteção da sua empresa

- Segmente sua rede: mantenha os dispositivos de IoT em uma rede separada dos sistemas críticos de negócios.
- Atualize o firmware do dispositivo: instale regularmente patches e atualizações de segurança.
- Monitore as atividades: configure alertas para comportamentos incomuns em dispositivos conectados.
- Use senhas fortes: altere as credenciais padrão e use senhas exclusivas e complexas para cada dispositivo.

5.
Ameaças internas

Nem todas as ameaças cibernéticas vêm de hackers externos; algumas têm origem dentro de uma organização. Seja um funcionário descontente em busca de vingança ou um que acidentalmente clicou em um link de phishing, as ameaças internas são tão perigosas quanto os ataques externos.

Os riscos

- Vazamentos de dados: informações confidenciais da empresa podem ser expostas ou roubadas.
- Comprometimento de sistema: funcionários com acessibilidade a sistemas críticos podem causar danos intencionais ou não intencionais.
- Danos à reputação: uma violação de segurança causada por um funcionário pode prejudicar a confiança e a credibilidade da sua empresa.

Você sabia?

US$ 4,29 milhões é o custo médio de ataques maliciosos cometidos por insiders.

(Fonte: IBM, julho de 2025)

Como garantir a proteção da sua empresa

- Ofereça treinamento de segurança regular: instrua os funcionários sobre as melhores práticas de segurança cibernética.
- Limite o acesso a dados confidenciais: conceda acesso somente com base na necessidade.
- Monitore as atividades internas: use ferramentas de segurança para detectar comportamentos incomuns.



Proteja sua empresa contra ameaças cibernéticas

A segurança cibernética é um desafio crescente, mas você não precisa enfrentá-lo só. Nossos especialistas ajudam a avaliar riscos, implementar defesas robustas e fornecer proteção à sua empresa contra ameaças em evolução. Entre em contato conosco hoje mesmo para saber como podemos ajudar a proteger sua empresa: