MILVUS CECyber

Webinar Milvus & CECYBER:

Sua Segurança em Rede

Milvus + CECyber

Sua Segurança em Rede

Este eBook é uma iniciativa do **Milvus** em parceria com a **CECYBER**, como parte da campanha **Sua Segurança em Rede**. Ele reúne os principais insights do webinar exclusivo apresentado por **Almir Meira Alves**, especialista em cibersegurança, para ajudar você a proteger ainda mais o seu negócio.

SUMÁRIO

SUMÁRIO

1. INTRODUÇÃO

O IMPACTO DA CIBERSEGURANÇA NO MUNDO DIGITAL

Vivemos em uma era digital onde a conectividade é essencial para o funcionamento de empresas, governos e indivíduos. Com o avanço da tecnologia, nossa dependência da internet e de sistemas digitais cresceu exponencialmente, tornando a cibersegurança um fator crítico para a proteção de dados e continuidade dos negócios.

Todos os dias, bilhões de dados são gerados, compartilhados e armazenados em redes e servidores ao redor do mundo. Desde informações bancárias e registros médicos até dados estratégicos de grandes corporações, **tudo está sujeito a ameaças cibernéticas que se tornam cada vez mais sofisticadas.**

Ataques como **ransomware, phishing, vazamento de dados e invasões de sistemas podem causar prejuízos financeiros milionários** e danos irreversíveis à reputação de empresas e indivíduos.

Para se ter uma ideia da gravidade do cenário, estudos apontam que os crimes cibernéticos causarão prejuízos globais superiores a 10 trilhões de dólares anuais até 2025.

Isso faz com que a segurança digital não seja apenas uma necessidade técnica, mas um **pilar essencial da proteção empresarial e da privacidade pessoal.**

Além dos riscos financeiros, ataques cibernéticos podem comprometer **infraestruturas críticas** — como sistemas de saúde, transportes e energia — impactando diretamente a sociedade.

Governos e organizações têm investido cada vez mais na proteção de redes e dados, mas, mesmo assim, a vulnerabilidade permanece, especialmente quando as boas práticas não são adotadas por todos os usuários.

Diante desse cenário, este eBook, uma **parceria entre Milvus e CECyber**, surge como um **guia prático para fortalecer a segurança digital**, ajudando empresas e profissionais a se protegerem de ameaças e adotarem estratégias eficazes de defesa.

Ao longo dos próximos capítulos, exploraremos as principais vulnerabilidades, tipos de ataques e as melhores práticas para garantir um ambiente digital mais seguro e confiável.

A IMPORTÂNCIA DE ADOTAR BOAS PRÁTICAS DE SEGURANÇA

A segurança digital não é exclusiva de grandes corporações – **qualquer empresa ou indivíduo conectado à internet pode ser alvo de ataques cibernéticos.**

Muitas violações ocorrem não por falhas tecnológicas, mas por erros humanos, como senhas fracas, acessos desprotegidos e softwares desatualizados.

Adotar boas práticas de segurança reduz riscos e evita prejuízos.

Conheça algumas das medidas essenciais:

- ☑ Manter sistemas e softwares atualizados para corrigir vulnerabilidades.
- ☑ Usar autenticação multifator (MFA) para impedir acessos indevidos.
- ☑ Criar senhas fortes e únicas para cada conta.
- ☑ Treinar usuários e funcionários contra golpes e engenharia social.
- ☑ Realizar backups frequentes para evitar perda de dados.

A segurança digital deve ser um hábito contínuo. Nos próximos capítulos, exploraremos como implementar essas práticas para proteger dados e reduzir ameaças.

COMO ATAQUES CIBERNÉTICOS PODEM AFETAR EMPRESAS E INDIVÍDUOS

Os ataques cibernéticos podem gerar prejuízos financeiros, interrupção de serviços e danos à reputação. Empresas e indivíduos são alvos frequentes, e as consequências vão muito além da perda de dados.

Para as empresas, os principais impactos incluem:

- **Perda de dados críticos** – Informações estratégicas podem ser sequestradas ou apagadas.
- **Prejuízo financeiro** – Custos elevados com recuperação de sistemas e pagamento de resgates em ataques de ransomware.
- **Danos à reputação** – Clientes e parceiros podem perder a confiança na empresa.
- **Multas e penalizações** – Vazamentos de dados podem resultar em sanções da LGPD e outras legislações.

Para indivíduos, os riscos podem ser diferentes:

- **Roubo de identidade** – Dados pessoais podem ser usados para fraudes bancárias e criação de contas falsas.
- **Perda de acesso a contas** – Phishing e clonagem de aplicativos como WhatsApp comprometem a privacidade.
- **Exposição de informações pessoais** – CPF, endereço e dados bancários podem ser vazados e utilizados indevidamente.

Além dos impactos financeiros e legais, os ataques afetam o aspecto emocional das vítimas, causando medo, ansiedade e insegurança.

A prevenção é a melhor defesa, e ao longo deste eBook exploraremos medidas eficazes para reduzir esses riscos.

O QUE VOCÊ VAI APRENDER NESTE EBOOK

Este eBook foi criado para ajudar empresas e profissionais a entenderem os riscos cibernéticos e adotarem estratégias eficazes de proteção digital. Você aprenderá desde conceitos básicos até técnicas avançadas, garantindo mais segurança para seus dados e sistemas.

Nos próximos capítulos, você descobrirá:

- Como cibercriminosos exploram vulnerabilidades para roubo de dados e invasões.
- Principais ameaças atuais, como ransomware, phishing e engenharia social.
- Boas práticas de segurança, incluindo autenticação multifator e backups regulares.
- Como proteger o home office e minimizar riscos em ambientes híbridos.
- Segurança em camadas como modelo eficaz de proteção digital.
- O impacto da LGPD e como garantir conformidade legal.
- Como criar uma cultura de segurança para reduzir falhas humanas.
- E muito mais!

Ao final, você terá conhecimento prático para implementar medidas de proteção digital eficazes.

2. O ELO MAIS FRACO: COMO SOMOS ENGANADOS ONLINE

A EXPOSIÇÃO EXCESSIVA DE DADOS NAS REDES SOCIAIS

As redes sociais fazem parte do cotidiano, mas **compartilhar informações demais pode facilitar golpes e ataques cibernéticos.**

Detalhes como localização, rotina, nome de familiares e informações financeiras podem ser usados por criminosos para engenharia social. Aprender a controlar seus dados digitais é essencial para evitar fraudes.

Como suas informações podem ser usadas contra você

- **Phishing personalizado** – Hackers criam e-mails falsos com base na sua rotina, simulando bancos ou serviços que você usa.
- **Sequestro de identidade** – Com CPF e outros dados, criminosos podem abrir contas e realizar compras em seu nome.
- **Golpes do WhatsApp** – Falsificação de identidade para pedir dinheiro a amigos e familiares.
- **Ataques corporativos** – Informações sobre sua empresa podem ser usadas para planejar invasões.

Como reduzir sua exposição e se proteger

- Evite check-ins e localização em tempo real.
- Ajuste a privacidade do seu perfil, limitando o acesso a desconhecidos.
- Tome cuidado com quizzes e desafios que coletam informações.
- Não compartilhe dados sensíveis publicamente.
- Monitore suas informações na internet regularmente.

COMO CIBERCRIMINOSOS EXPLORAM INFORMAÇÕES PÚBLICAS

No mundo digital, tudo o que compartilhamos online pode ser usado contra nós. Hackers utilizam informações disponíveis em redes sociais, fóruns e vazamentos de dados para criar golpes altamente personalizados.

Táticas utilizadas pelos criminosos

- **Open-Source Intelligence (OSINT)** – Coleta de dados em fontes abertas, como redes sociais e sites governamentais.
- **Scraping de redes sociais** – Programas automatizados extraem informações como e-mails, localização e hábitos de navegação.
- **Vazamentos de dados** – Informações roubadas são vendidas na dark web para ataques futuros.

Exemplos de golpes baseados em informações públicas

- **Fraudes bancárias personalizadas** – Criminosos se passam por seu banco usando dados vazados.
- **Roubo de identidade** – Dados do LinkedIn podem ser usados para criar perfis falsos e aplicar golpes.
- **Spear phishing** – Hackers enviam e-mails fraudulentos com base em sua participação em eventos ou serviços online.
- **Golpe do WhatsApp** – Com dados familiares, criminosos se passam por parentes pedindo dinheiro.

Como se proteger

- Ajuste a privacidade das redes e limite quem vê suas postagens.
- Monitore vazamentos de dados em sites como Have I Been Pwned.
- Evite expor dados sensíveis como documentos, endereço e telefone.
- Desconfie de contatos suspeitos pedindo informações pessoais.
- Utilize novas senhas para cada serviço e ative autenticação multifator.

Quanto menos dados você expuser publicamente, mais difícil será para hackers explorarem sua identidade e aplicarem golpes.

GOLPES COMUNS VIA APLICATIVOS DE MENSAGENS

Aplicativos como WhatsApp, Telegram e e-mail são alvos frequentes de cibercriminosos.

Veja os golpes mais comuns e como se proteger:

- Clonagem de WhatsApp – Golpistas fingem ser suporte e pedem o código de verificação por SMS para roubar a conta.
- Como evitar: Ative a verificação em duas etapas e nunca compartilhe códigos de segurança.
- Falso suporte técnico – Golpistas se passam por atendentes de bancos ou operadoras para roubar senhas e dados.
- Como evitar: Empresas legítimas nunca pedem senhas por mensagem ou ligação.

Phishing por e-mail – Mensagens falsas imitam bancos e empresas, induzindo a vítima a clicar em links maliciosos.

Como evitar: Verifique o remetente e desconfie de pedidos urgentes.

Golpe do amigo ou familiar pedindo dinheiro – Perfis clonados solicitam transferências alegando emergências.

Como evitar: Sempre ligue para a pessoa antes de transferir dinheiro.

Falsa promoção ou sorteio – Ofertas enganosas pedem dados ou taxas para liberação de prêmios inexistentes.

Como evitar: Empresas não cobram taxas para entrega de prêmios.

Como se proteger

- Ative a verificação em duas etapas para bloquear invasores.
- Desconfie de mensagens urgentes pedindo ação imediata.
- Nunca clique em links suspeitos — acesse o site oficial.
- Confirme solicitações por outro canal antes de compartilhar dados.

A informação é sua melhor defesa. Fique atento, adote boas práticas e evite cair em golpes digitais.

ENGENHARIA SOCIAL: O PERIGO DA MANIPULAÇÃO PSICOLÓGICA

Ataques cibernéticos nem sempre exploram falhas tecnológicas — muitas vezes, exploram o fator humano.

A engenharia social explora fraquezas emocionais, como medo, urgência, curiosidade e confiança, para enganar vítimas e levá-las a revelar senhas, dados bancários ou instalar malwares sem perceber.

Como os criminosos manipulam as vítimas com engenharia social

- Criação de senso de urgência: Golpistas pressionam a vítima com avisos falsos de bloqueio de conta para obter dados rapidamente.
- Como evitar: Desconfie de solicitações urgentes. Empresas legítimas não pressionam clientes para agir rapidamente.
- Uso de autoridade falsa: Golpistas fingem ser bancos, empresas ou órgãos oficiais para obter dados sigilosos.
- Como evitar: Nunca forneça senhas ou códigos por telefone ou e-mail. Se tiver dúvidas, contate a instituição diretamente.

- Exploração da confiança: Hackers fingem ser amigos, colegas ou familiares e pedem senhas, acessos ou transferências bancárias.
- Como evitar: Confirme a identidade por outro canal antes de atender qualquer solicitação suspeita.

- Indução à curiosidade: Mensagens falsas com títulos chamativos, como “Você ganhou um prêmio!” ou “Confirmação de pagamento”.
- Como evitar: Evite clicar em links ou abrir anexos desconhecidos, mesmo que pareçam legítimos.

- Ataque na distração: Criminosos agem quando a vítima está ocupada ou cansada, aumentando a chance de erro.
- Como evitar: Sempre valide informações antes de compartilhar dados, mesmo sob pressão.

A engenharia social explora confiança e distração. **Informação e cautela são suas melhores defesas.**

EXEMPLO REAL: GOLPISTAS USAM IA PARA FALSIFICAR REUNIÕES CORPORATIVAS

Cibercriminosos estão explorando a inteligência artificial (IA) para aplicar golpes sofisticados. Em Hong Kong, deepfakes foram usados para simular uma reunião corporativa e desviar US$ 25 milhões de uma multinacional.

O que são deepfakes? São vídeos ou áudios gerados por IA que imitam pessoas reais, permitindo fraudes como reuniões falsas para enganar funcionários.

Como deepfakes são usados para golpes?

- **Falsificação de reuniões** – Executivos falsos instruem transferências fraudulentas.
- **Engenharia social avançada** – Golpistas usam IA para enganar e obter informações sigilosas.
- **Espionagem corporativa** – Deepfakes podem ser usados para manipular mercados ou prejudicar empresas.

Como se proteger

- Verifique identidades em reuniões virtuais usando códigos de autenticação para validar participantes e evitar fraudes.
- Fique atento a sinais suspeitos: sincronização labial falha ou atrasos no áudio podem indicar deepfakes.
- Exija múltiplas aprovações para transações financeiras
- Treine funcionários para reconhecer golpes digitais.
- Utilize ferramentas de IA para detectar deepfakes.

3. VULNERABILIDADES MAIS COMUNS E COMO EVITÁ-LAS

APLICAÇÕES INTERNAS SEM REVISÃO DE SEGURANÇA

Aplicações internas são essenciais para empresas, mas sem revisões de segurança, **podem se tornar brechas para ataques.**

Falta de auditoria, códigos desatualizados e credenciais expostas tornam essas aplicações alvos fáceis para hackers.

Principais riscos

- **Roubo de dados** – Falhas podem permitir que invasores acessem informações sigilosas.
- **Ataques de ransomware** – Sistemas vulneráveis podem ser sequestrados, resultando em bloqueio de dados.
- **Execução de comandos maliciosos** – Hackers podem assumir controle remoto dos sistemas.
- **Fraudes e manipulação de informações** – Registros podem ser alterados para desviar pagamentos ou comprometer processos.

Como evitar vulnerabilidades

- Realize auditorias regulares e testes de segurança.
- Mantenha softwares e frameworks sempre atualizados.
- Evite armazenar credenciais no código, utilizando cofres de senhas.
- Implemente autenticação multifator (MFA) para restringir acessos indevidos.
- Monitore atividades suspeitas com ferramentas de detecção de intrusão.

Garantir a segurança dessas aplicações é fundamental para evitar prejuízos financeiros e danos à reputação.

EXPOSIÇÃO DE PORTAS ABERTAS EM SERVIDORES

Servidores armazenam dados e sistemas críticos, mas portas abertas sem necessidade criam brechas para ataques. Hackers varrem redes em busca de servidores vulneráveis, explorando falhas para invadir sistemas.

Principais riscos

- **Força bruta** – Tentativas repetitivas de login para invadir servidores.
- **Exploração de falhas** – Brechas em softwares permitem acessos remotos.
- **Controle total do sistema** – Hackers podem executar comandos maliciosos.
- **Ransomware** – Servidores expostos são alvos fáceis para sequestro de dados.

Como evitar ataques

- [x] Feche portas desnecessárias para reduzir pontos de vulnerabilidade.
- [x] Utilize firewalls para restringir acessos externos.
- [x] Ative autenticação multifator (MFA) para conexões remotas.
- [x] Monitore tentativas de acesso com sistemas de detecção de intrusão (IDS/IPS).
- [x] Prefira conexões via VPN para ocultar serviços expostos.
- [x] Mantenha servidores sempre atualizados com patches de segurança

A exposição de portas abertas é um dos erros mais explorados por cibercriminosos. **Revisar configurações e reforçar a segurança é essencial para evitar invasões e proteger dados corporativos.**

ATUALIZAÇÃO DE ROTEADORES, SOFTWARES E FIRMWARE: POR QUE É ESSENCIAL?

A segurança digital depende da atualização constante de dispositivos e sistemas. Roteadores, softwares e firmwares desatualizados facilitam invasões, roubo de dados e ataques de malware.

Por que atualizar?

- **Elimina vulnerabilidades** – Corrige brechas exploradas por cibercriminosos.
- **Protege contra novos ataques** – Novas ameaças surgem constantemente.
- **Melhoria no desempenho** – Além de segurança, atualizações corrigem bugs e otimizam sistemas.
- **Conformidade legal** – Regulamentações como LGPD e GDPR exigem medidas de proteção adequadas.

Principais riscos de não atualizar

- **Roteadores vulneráveis** – Hackers podem acessar sua rede e monitorar tráfego.
- **Ataques de ransomware** – Softwares desatualizados facilitam a instalação de malwares.

- **Roubo de credenciais** – Navegadores e aplicativos sem atualização podem expor senhas.
- **Exploração de dispositivos IoT** – Câmeras, smart TVs e assistentes virtuais sem atualização são alvos fáceis.

Como evitar ataques

- Ative atualizações automáticas.
- Verifique a versão atualizada do firmware do roteador regularmente no site do fabricante.
- Substitua dispositivos obsoletos que não recebem mais suporte.
- Baixe apenas de fontes oficiais para evitar arquivos infectados.
- Revise manualmente as atualizações pelo menos uma vez por mês.

PRIVILÉGIO MÍNIMO E ZERO TRUST: CONTROLE RIGOROSO DE ACESSOS

Permissões excessivas facilitam ataques cibernéticos, permitindo que invasores roubem dados e modifiquem informações críticas. Para mitigar esse risco, é essencial aplicar o Privilégio Mínimo e o modelo Zero Trust.

Privilégio Mínimo
Usuários e sistemas devem ter acesso apenas ao que precisam.

- **Restrições por função** – Funcionários não devem ter acesso a sistemas que não utilizam.
- **Contas administrativas limitadas** – Apenas usuários essenciais devem possuir permissões avançadas.
- **Controle de dados sensíveis** – Acesso a informações críticas deve ser concedido apenas por tempo determinado.

Zero Trust (Confiança Zero)
Nenhum usuário ou dispositivo deve ser confiável por padrão.

1. **Verificação contínua** – Sempre autenticar identidades e dispositivos antes de conceder acesso.
2. **Restrições de acesso** – Conceder permissões apenas quando necessário e por tempo limitado.
3. **Monitoramento ativo** – Analisar atividades em tempo real para identificar comportamentos suspeitos.

Como implementar essas práticas?

- ☑ Defina permissões por cargo e função.
- ☑ Implemente autenticação multifator (MFA).
- ☑ Utilize monitoramento contínuo para detectar acessos suspeitos.
- ☑ Segmente redes internas para evitar movimentação lateral de invasores.
- ☑ Revise permissões para eliminar acessos desnecessários com auditorias regulares.

COMO IDENTIFICAR E CORRIGIR VULNERABILIDADES ANTES QUE OS HACKERS AS EXPLOREM

Hackers buscam falhas o tempo todo, e muitas empresas só percebem após um ataque. Identificar e corrigir vulnerabilidades com antecedência é essencial para evitar riscos.

Principais formas de identificar vulnerabilidades

- 🔍 **Pentest (Testes de invasão)** – Contrate especialistas ou use ferramentas de automação para simular ataques e encontrar falhas antes dos criminosos.

- **Varredura de vulnerabilidades** – Ferramentas como Nmap e Nessus detectam portas abertas e softwares desatualizados.
- **Monitoramento de logs** – Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS) alertam sobre acessos indevidos em tempo real.
- **Atualizações e patches de segurança** – Mantenha atualizações automáticas ativadas e monitore alertas dos fabricantes para corrigir falhas rapidamente.
- **Auditorias regulares** – Revise permissões e políticas de segurança para eliminar brechas.

Como corrigir vulnerabilidades antes que os hackers explorem?

- **Ação imediata** – Resolva falhas assim que forem detectadas.
- **Reduza a superfície de ataque** – Feche portas desnecessárias, restrinja acessos e desative serviços que não são utilizados.
- **Implemente autenticação forte** – Utilize autenticação multifator (MFA) e exija senhas longas e complexas.
- **Treine colaboradores** – Erros humanos são sempre a principal causa. Conscientização sobre phishing e engenharia social reduz riscos.
- **Plano de resposta a incidentes** – Defina procedimentos claros de contenção e recuperação para minimizar danos em caso de ataque.

4. ATAQUES CIBERNÉTICOS NA PRÁTICA

O QUE É RANSOMWARE E COMO ELE SEQUESTRA SEUS DADOS

O ransomware é um dos ataques cibernéticos mais destrutivos, bloqueando o acesso a arquivos por meio de criptografia e exigindo pagamento para sua liberação. **Empresas, governos e indivíduos já sofreram prejuízos milionários com esse tipo de ameaça.**

Como funciona um ataque de ransomware?

1. **Infecção** – O malware entra no sistema por e-mails maliciosos (phishing), downloads infectados ou falhas em softwares desatualizados.
2. **Propagação** – O ransomware se espalha pela rede, comprometendo múltiplos dispositivos.
3. **Criptografia dos dados** – Arquivos são bloqueados, impedindo o acesso.
4. **Pedido de resgate** – Uma mensagem exige pagamento, geralmente em criptomoedas.
5. **Sem garantia de recuperação** – Mesmo pagando, não há garantia de que os dados serão restaurados.

Principais tipos de ransomware

- **Crypto ransomware** – Criptografa arquivos e exige pagamento de resgate em criptomoedas
- **Locker ransomware** – Bloqueia o sistema inteiro, impedindo seu uso.
- **Ransomware como serviço (RaaS)** – Hackers vendem ou alugam kits de ataque para terceiros.

Como se proteger?

- **Backups atualizados** – Guarde cópias seguras e offline.
- **Sistemas atualizados** – Corrija falhas exploradas por hackers.
- **Autenticação multifator (MFA)** – Proteja acessos críticos com camadas extras de segurança.
- **Treine funcionários** – Reduza erros humanos que podem levar a infecções via phishing.
- **Implemente soluções de segurança** – Firewalls, antivírus e sistemas de detecção e prevenção de intrusão ajudam a prevenir ataques.

Ataques de ransomware já causaram prejuízos bilionários ao redor do mundo, tornando essencial a adoção de medidas preventivas. **Proteger seus dados é a melhor estratégia** para evitar perdas e manter a continuidade dos negócios.

Confira alguns dos casos mais marcantes e, se quiser se aprofundar, pesquise mais sobre eles:

- **WannaCry (2017)** – Infectou mais de 200 mil computadores em 150 países, explorando falhas no Windows.
- **NotPetya (2017)** – Disfarçado de ransomware, causou bilhões em prejuízos sem intenção de restaurar dados.
- **Colonial Pipeline (2021)** – Paralisou um grande oleoduto nos EUA, resultando no pagamento de US$ 4,4 milhões.

DEMONSTRAÇÃO REAL DE UM ATAQUE: COMO UM SIMPLES ERRO PODE GERAR UMA CRISE CIBERNÉTICA

Muitas empresas subestimam os riscos cibernéticos até sofrerem um ataque. O caso da Travelex, gigante do câmbio, ilustra como uma falha ignorada resultou em uma crise milionária.

O caso Travelex: um ataque devastador

- **Sequestro dos sistemas** – Em janeiro de 2020, um ransomware criptografou todos os arquivos da empresa, paralisando suas operações.
- **Infecção silenciosa** – Hackers acessaram a rede seis meses antes do ataque, explorando uma vulnerabilidade não corrigida e roubando 5 GB de dados.

Pedido de resgate – Os criminosos exigiram US$ 6 milhões, e a empresa, sem alternativas, pagou US$ 2,3 milhões para recuperar os dados.

Impactos do ataque

Prejuízo financeiro

Perda de receita e altos custos de recuperação.

Danos à reputação

Clientes e parceiros perderam a confiança.

Longo tempo de recuperação

Mesmo após o pagamento, a normalização levou meses.

Mudança forçada na segurança

A empresa precisou revisar toda sua estratégia digital.

O que poderia ter evitado esse ataque?

- **Correção de vulnerabilidades** – A falha explorada já era conhecida, e uma simples atualização poderia ter evitado o ataque.
- **Monitoramento proativo** – Detectar acessos não autorizados poderia ter interrompido a ameaça antes do sequestro dos sistemas.
- **Backups isolados e atualizados** – Um plano de recuperação bem estruturado evitaria o pagamento do resgate.
- **Treinamento contínuo de funcionários** – A conscientização reduz riscos e ajuda a detectar sinais de invasão antes que o dano ocorra.

⚠ Lição aprendida: a segurança está nos detalhes ⚠

BUSINESS EMAIL COMPROMISE (BEC): COMO ATAQUES VIA E-MAIL ROUBAM MILHÕES DE DÓLARES

O Business Email Compromise (BEC) é um dos golpes mais lucrativos para cibercriminosos. Sem precisar de malwares, hackers exploram a confiança humana para enganar funcionários e induzi-los a transferir dinheiro para contas fraudulentas.

Como funciona um ataque BEC?

1. **Escolha da vítima** – Criminosos analisam a empresa e selecionam gestores financeiros ou executivos com poder de decisão.
2. **Comprometimento do e-mail** – Invadem contas por phishing ou criam domínios falsos para enviar mensagens convincentes.
3. **Solicitação fraudulenta** – Fingem ser um executivo ou fornecedor e pedem pagamento urgente sob pretextos como mudança de conta bancária ou aquisição sigilosa.
4. **Desvio de dinheiro** – A vítima transfere os valores para contas de criminosos, muitas vezes em países sem regulamentação bancária.

Como evitar ataques de BEC?

- **Verificação em duas etapas para pagamentos** – Sempre valide pedidos por telefone ou pessoalmente antes de aprovar transferências.
- **Atenção ao domínio do e-mail** – Cuidado com domínios semelhantes (ex: mycompany.com > mycornpany.com).
- **Autenticação multifator (MFA)** – Proteja contas corporativas contra invasões com autenticação extra.
- **Treinamento de funcionários** – Ensine funcionários a identificar e-mails suspeitos e validar alterações bancárias com fornecedores.
- **Alertas de segurança** – Utilize soluções que detectem padrões incomuns em e-mails corporativos.

Veja alguns dos casos mais impactantes e, se quiser saber mais, explore detalhes adicionais sobre cada um:

- **Toyota (2019)** – Funcionário transferiu US$ 37 milhões após receber um e-mail falso de um fornecedor.
- **Facebook e Google (2013-2015)** – Empresas perderam US$ 100 milhões após fraudadores se passarem por fornecedores legítimos.
- **Ubiquiti Networks (2015)** – Empresa foi enganada e perdeu US$ 46,7 milhões em transferências fraudulentas.

NEGAÇÃO DE SERVIÇO (DDOS): COMO EMPRESAS SÃO DERRUBADAS ONLINE

Os ataques de Negação de Serviço Distribuído (DDoS) **sobrecarregam servidores com tráfego malicioso, tornando sites e serviços inacessíveis.** Empresas que dependem da internet, como e-commerces e bancos, podem sofrer grandes perdas financeiras e reputacionais.

Como um ataque DDoS funciona?

Hackers usam redes de computadores zumbis (botnets) para gerar um volume extremo de solicitações e derrubar sistemas.

Os principais tipos incluem:

- **Ataques de volume** – Sobrecarga de banda com tráfego massivo.
- **Ataques a protocolos** – Exploração de falhas na comunicação.
- **Ataques a aplicações** – Consumo excessivo de recursos em sistemas web.

Quanto maior a botnet envolvida, mais difícil será para a empresa se recuperar.

Consequências de um ataque DDoS

⚠ **Serviços fora do ar** – Sites e aplicativos podem ficar indisponíveis por horas.

⚠ **Prejuízo financeiro** – Empresas perdem vendas e credibilidade.

⚠ **Danos à reputação** – A confiança de clientes e parceiros é abalada.

⚠ **Invasões combinadas** – Ataques DDoS podem servir de distração para invasões mais graves.

Como se proteger?

☑ **Use serviços de mitigação DDoS** – Plataformas como Cloudflare, AWS Shield e Akamai ajudam a filtrar tráfego malicioso.

☑ **Monitore o tráfego da rede** – Ferramentas especializadas detectam padrões suspeitos e acionam respostas automáticas.

☑ **Implemente firewalls avançados** – Sistemas de segurança podem bloquear acessos suspeitos antes que o ataque tenha impacto.

☑ **Crie planos de resposta a incidentes** – Defina ações rápidas para minimizar impactos.

☑ **Distribua sua infraestrutura** – Servidores espalhados por diferentes localidades ajudam a minimizar os efeitos de um ataque direcionado.

Os ataques DDoS são uma ameaça real para qualquer empresa com presença digital. A proteção contra DDoS é essencial para garantir a continuidade dos negócios e evitar interrupções causadas por ataques cibernéticos.

O IMPACTO DE UM ATAQUE: PREJUÍZOS FINANCEIROS, DANOS REPUTACIONAIS E PROCESSOS JUDICIAIS

Ataques cibernéticos causam mais do que interrupções: podem gerar perdas milionárias, abalar a reputação da empresa e resultar em processos judiciais.

Principais impactos

- **Perdas financeiras** – Custos com recuperação, resgates e paralisações.
- **Danos à reputação** – Vazamentos reduzem a confiança de clientes e parceiros.
- **Processos e multas** – Regulamentações como LGPD e GDPR punem falhas na proteção de dados.

A segurança digital não é opcional — ignorá-la pode custar caro em todos os aspectos do negócio.

Trouxemos mais um caso real para você se aprofundar:

- **Marriott (2018)** – A rede hoteleira sofreu um vazamento de 500 milhões de registros, resultando em uma multa de US$ 23,8 milhões.

5. DICAS DE SEGURANÇA NO TRABALHO HIBRIDO E HOME OFFICE

COMO PROTEGER SUA REDE DOMÉSTICA CONTRA INVASORES

O modelo híbrido e o trabalho remoto trouxeram flexibilidade para empresas e profissionais, mas também aumentaram os desafios de segurança digital.

Uma rede doméstica mal configurada pode ser um alvo fácil para hackers, que exploram brechas para interceptar dados, acessar dispositivos e até controlar remotamente computadores e câmeras conectadas.

Para evitar riscos:

Altere credenciais padrão do roteador e crie uma senha forte.

Habilite criptografia WPA3 ou WPA2 para impedir acessos não autorizados.

Atualize o firmware do roteador regularmente para corrigir falhas.

Crie uma rede separada para o trabalho, evitando misturá-la com dispositivos pessoais.

Ative firewalls e monitore acessos suspeitos.

A segurança da rede doméstica é a base da proteção no trabalho remoto. Pequenos ajustes nas configurações do roteador e o uso de protocolos seguros garantem que seus dados e dispositivos fiquem protegidos contra ataques.

RISCOS DAS REDES WI-FI PÚBLICAS E COMO EVITÁ-LOS

Redes Wi-Fi públicas, como as de cafés, aeroportos e hoteis, são extremamente vulneráveis a ataques, pois muitas vezes não possuem criptografia ou controles de segurança. Hackers podem monitorar conexões, capturar senhas e até realizar ataques do tipo “man-in-the-middle” para interceptar dados.

Para minimizar a exposição:

- ☑ **Evite acessar e-mails corporativos e contas bancárias.**
- ☑ **Não insira credenciais** ou dados sensíveis em sites e apps.
- ☑ **Prefira redes móveis (4G/5G)** para maior segurança.
- ☑ Se precisar usar Wi-Fi público, **ative uma VPN** para criptografar sua conexão.

VPN E CRIPTOGRAFIA: PROTEÇÕES ESSENCIAIS PARA TRABALHO REMOTO

A VPN (Virtual Private Network) é uma das ferramentas mais eficazes para manter a segurança no trabalho remoto.

Ao criar um túnel criptografado entre o seu dispositivo e os servidores da empresa, ela impede que hackers ou terceiros acessem seus dados enquanto trafegam pela internet.

Para minimizar a exposição:

Use VPN corporativa para acessar sistemas da empresa com segurança.

Ative criptografia de ponta a ponta em e-mails e arquivos.

Evite armazenar dados críticos em serviços de nuvem não autorizados.

Utilize plataformas seguras para reuniões virtuais e compartilhamento de arquivos.

No trabalho remoto, adotar essas soluções reduz significativamente os riscos cibernéticos e garante que suas informações permaneçam seguras.

6. SEGURANÇA EM CAMADAS: O MODELO MAIS EFICIENTE DE PROTEÇÃO

O CONCEITO DE DEFESA EM PROFUNDIDADE: COMO FUNCIONA NA PRÁTICA

A segurança digital eficaz não se baseia em uma única solução, mas em camadas de proteção que dificultam invasões e reduzem riscos.

Esse modelo, chamado de defesa em profundidade, cria múltiplas barreiras para impedir ataques.

A defesa em profundidade segue o princípio de que nenhuma camada de proteção é infalível. **Se uma camada falhar, outra assume a proteção.**

Esse modelo se baseia em:

- **Camada externa (perímetro de rede)** – Firewalls, segmentação e monitoramento do tráfego.
- **Camada intermediária (dispositivos e sistemas)** – Proteção de endpoints e desenvolvimento seguro.
- **Camada interna (dados e acessos)** – Criptografia, controle de permissões e prevenção de vazamento.

Cada camada adiciona redundância de segurança, garantindo que mesmo em caso de falha, o impacto do ataque seja reduzido.

SEGURANÇA DO PERÍMETRO

A segurança perimetral é a primeira barreira contra invasões, bloqueando acessos não autorizados antes que alcancem sistemas internos.

Para fortalecer essa proteção:

Configure firewalls corretamente – Bloqueie tráfego suspeito e restrinja acessos indesejados.

Segmente a rede – Separe áreas críticas de ambientes menos seguros, reduzindo o impacto de invasões.

Monitore o tráfego em tempo real
Identifique padrões anormais que possam indicar ataques em andamento.

Com redes bem segmentadas, um possível invasor não consegue se movimentar livremente, reduzindo os danos.

SEGURANÇA DE DISPOSITIVOS

Dispositivos conectados à rede corporativa são alvos fáceis para ataques. **A segurança dos endpoints (computadores, celulares e tablets) é essencial para evitar brechas.**

- **Use antivírus e EDR** – Detecte e contenha ameaças antes que se espalhem.
- **Restrinja acessos e instalações** – Bloqueie softwares não autorizados e minimize riscos.
- **Ative a autenticação multifator (MFA)** – Proteja acessos, mesmo em caso de vazamento de credenciais.
- **Gerencie dispositivos móveis (MDM)** – Controle e proteja celulares e tablets usados remotamente.

Manter endpoints atualizados e monitorados reduz drasticamente os riscos de infecção por malwares e ransomware.

SEGURANÇA DE APLICAÇÕES

A segurança deve ser uma prioridade desde a fase de desenvolvimento, e não apenas após a implantação. **O conceito de Shift Left Security propõe a detecção e correção de vulnerabilidades no início do ciclo de vida do software**, reduzindo riscos antes do lançamento.

- **Revisões de código** – Identifique e corrija falhas antes da implantação.
- **Testes de segurança contínuos** – Valide sistemas e APIs regularmente.
- **Privilégio mínimo** – Garanta que aplicações tenham apenas as permissões essenciais.
- **Análises estáticas e dinâmicas** – Utilize ferramentas para detectar vulnerabilidades antes que possam ser exploradas.

Ao integrar segurança desde o desenvolvimento, as empresas reduzem falhas exploráveis e protegem seus sistemas contra ataques.

PROTEÇÃO DE DADOS

Dados são um dos ativos mais valiosos de uma empresa, e protegê-los exige camadas de segurança bem estruturadas.

Principais medidas:

- **Criptografia** – Proteja dados em trânsito e em repouso para impedir acessos não autorizados.
- **Monitoramento de logs** – Identifique acessos suspeitos e detecte vazamentos em tempo real.
- **DLP (Prevenção de Perda de Dados)** – Restrinja o compartilhamento indevido de informações sensíveis.
- **Política Zero Trust** – Controle rigorosamente os acessos, concedendo permissões mínimas e exigindo autenticação constante.

Com um plano de proteção de dados sólido, empresas evitam vazamentos e **garantem conformidade com regulamentações como LGPD** (Lei Geral de Proteção de Dados Pessoais) **e GDPR** (General Data Protection Regulation)

Nenhuma solução de segurança isolada é suficiente para proteger completamente uma empresa. A estratégia de segurança em camadas funciona como uma rede de proteção, onde cada barreira reduz os riscos e dificulta a ação de invasores.

7. PROTEÇÃO DE DADOS PESSOAIS E A LGPD

O QUE A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) EXIGE DAS EMPRESAS

A Lei Geral de Proteção de Dados (LGPD) foi criada para garantir a privacidade e segurança das informações pessoais, exigindo que empresas adotem boas práticas no tratamento de dados. O descumprimento pode resultar em multas milionárias, sanções e danos à reputação.

A LGPD estabelece regras claras sobre como as empresas devem coletar, armazenar e tratar dados pessoais.

Entre as principais exigências estão:

- ☑ **Consentimento do usuário** – Dados devem ser coletados com permissão explícita.
- ☑ **Finalidade específica** – A empresa deve informar porque os dados estão sendo coletados e como serão utilizados.
- ☑ **Acesso e transparência** – O titular dos dados tem direito de saber quais informações suas estão sendo armazenadas.
- ☑ **Segurança e proteção** – Empresas devem adotar medidas técnicas para evitar vazamentos.

Empresas que não seguem essas diretrizes podem ser responsabilizadas legalmente.

COMO A LGPD PROTEGE OS DADOS PESSOAIS DOS CLIENTES

A LGPD define que qualquer informação capaz de identificar uma pessoa – como nome, CPF, endereço e até hábitos de consumo – deve ser protegida.

Anonimização e pseudonimização

Técnicas que ocultam dados sensíveis para minimizar riscos em caso de vazamento.

Direito à portabilidade e exclusão

O titular pode solicitar a remoção ou transferência de seus dados.

Restrição ao compartilhamento

Empresas só podem compartilhar informações se houver base legal para isso.

Essas medidas aumentam a segurança e o controle que os usuários têm sobre suas informações.

MULTAS E PENALIZAÇÕES: O QUE ACONTECE EM CASO DE VAZAMENTO DE DADOS?

Empresas que violam a LGPD podem sofrer sanções severas, como:

Multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração.

Bloqueio e eliminação de dados coletados ilegalmente, afetando operações comerciais.

Danificação da reputação, levando à perda de clientes e confiança do mercado.

Processos judiciais movidos por titulares dos dados, com possibilidade de indenizações.

Manter a conformidade não é apenas uma obrigação legal, mas uma necessidade para evitar prejuízos.

COMO EMPRESAS DEVEM TRATAR, ARMAZENAR E COMPARTILHAR INFORMAÇÕES

Para estar em conformidade, as empresas devem adotar boas práticas no ciclo de vida dos dados.

Principais medidas:

- **Minimização de dados** – Coletar apenas as informações estritamente necessárias.
- **Criptografia, transporte e armazenamento seguro** – Proteger dados armazenados e em trânsito contra acessos não autorizados.
- **Controle de acesso** – Garantir que apenas funcionários autorizados tenham permissão para acessar informações sensíveis.
- **Monitoramento contínuo** – Implementar ferramentas de auditoria para identificar tentativas de violação.
- **Políticas claras de privacidade** – Explicar de forma transparente como os dados são utilizados e armazenados.

Empresas que seguem essas diretrizes reduzem os riscos de vazamento e garantem a confiança dos clientes.

DICAS PARA GARANTIR CONFORMIDADE E EVITAR PROBLEMAS LEGAIS

- Mantenha uma política de privacidade clara e acessível para os usuários.
- Implemente treinamentos de segurança para conscientizar colaboradores sobre a LGPD.
- Realize auditorias periódicas para revisar práticas de armazenamento e proteção de dados.
- Garanta canais para atendimento aos titulares que queiram acessar, corrigir ou excluir seus dados.
- Conte com um DPO (Encarregado de Proteção de Dados) para acompanhar a implementação e para supervisionar a conformidade da empresa em relação à LGPD e outros regulamentos de privacidade de dados.

A adequação à LGPD não é apenas uma exigência legal, mas uma estratégia essencial para evitar riscos e fortalecer a relação com clientes e parceiros.

8. CULTURA DE SEGURANÇA E CONSCIENTIZAÇÃO

POR QUE A SEGURANÇA DIGITAL DEVE SER UM HÁBITO DIÁRIO

A segurança digital não é apenas um conjunto de ferramentas, mas sim um hábito diário que deve ser cultivado dentro das empresas e na vida pessoal.

Muitos ataques cibernéticos ocorrem por falhas humanas, como distração, falta de atenção a detalhes e confiança excessiva em mensagens suspeitas.

Construir uma cultura de segurança significa educar colaboradores e reforçar boas práticas para evitar riscos.

PEQUENAS DISTRAÇÕES, GRANDES DESASTRES

Muitos ataques cibernéticos bem-sucedidos começam por erros simples, como clicar em um link malicioso, usar senhas fracas ou baixar arquivos infectados.

Algumas das falhas mais comuns incluem:

- **Abrir e-mails falsos** – Phishing segue sendo uma das principais ameaças, enganando funcionários para que revelem senhas ou instalem malware.
- **Uso de senhas fracas e repetidas** – Senhas previsíveis ou utilizadas em várias contas facilitam invasões.
- **Distração no home office** – Ambientes domésticos reduzem a percepção de risco, tornando mais fácil cair em golpes.
- **Compartilhamento de informações sensíveis sem verificação** – Muitas violações começam quando funcionários divulgam dados sem checar a autenticidade da solicitação.

TREINAMENTOS E POLÍTICAS INTERNAS PARA REDUZIR RISCOS

A educação contínua é essencial para criar uma mentalidade de segurança. As empresas devem implementar treinamentos periódicos para que os funcionários saibam identificar ameaças e reagir corretamente.

Boas práticas incluem:

- **Simulações de phishing** – Testes controlados ajudam a avaliar a vulnerabilidade dos colaboradores e reforçar o aprendizado.
- **Treinamentos regulares** – Funcionários devem ser atualizados constantemente sobre novas ameaças e golpes.
- **Política clara de uso de dispositivos** – Definir regras para o uso de e-mails corporativos, acesso remoto e compartilhamento de dados reduz brechas de segurança.
- **Controle de acessos e autenticação multifator (MFA)** Aplicar restrições de acesso a dados sensíveis e exigir autenticação adicional em logins críticos.

A IMPORTÂNCIA DA COMUNICAÇÃO ENTRE FUNCIONÁRIOS E EQUIPE DE TI

A segurança digital é responsabilidade de todos, não apenas do time de TI. Os funcionários devem sentir-se confortáveis para relatar incidentes ou comportamentos suspeitos, sem medo de represálias. Uma equipe confiante sempre tende a ser uma equipe mais resiliente e com maior prontidão para responder aos incidentes cibernéticos.

Algumas boas práticas incluem:

- **Canais de comunicação diretos com a equipe de TI**
  Criar um fluxo ágil para reportar atividades incomuns ou tentativas de golpe.
- **Políticas claras sobre incidentes** – Todos devem saber como agir em caso de um possível ataque.
- **Rapidez na resposta** – Quanto mais cedo uma ameaça for identificada, menor o impacto da violação.

COMO CRIAR UM AMBIENTE CORPORATIVO SEGURO PARA TODOS

A segurança deve fazer parte do dia a dia das empresas, sendo reforçada constantemente.

Algumas medidas essenciais incluem:

- **Cultura de "Zero Trust"** – Nenhum acesso ou solicitação deve ser confiado automaticamente, exigindo verificação contínua.
- **Uso exclusivo de canais corporativos** – Evitar que informações sensíveis sejam compartilhadas em e-mails pessoais ou aplicativos não monitorados.
- **Backup atualizado e redundância de dados** – Manter cópias seguras de informações críticas reduz danos em caso de ataque. A frequência do backup também é importante, pois caso haja uma perda ou roubo de dados, a sua restauração será muito próxima da totalidade dos dados da empresa.
- **Engajamento de todos os setores** – A segurança não é apenas um problema de TI; envolve RH, financeiro, marketing e qualquer área que lide com informações sensíveis. Testar e simular eventos de crise cibernética é uma atividade muito importante para envolver todas as áreas da empresa.

Construir uma cultura de segurança sólida exige consistência e comprometimento de toda a equipe. Quanto mais a conscientização for reforçada, menor será a chance de erros que possam comprometer toda a organização.

9. CONCLUSÃO E PRÓXIMOS PASSOS

O QUE FAZER AGORA PARA FORTALECER A SEGURANÇA DA SUA EMPRESA

A cibersegurança é um processo contínuo que exige vigilância constante, boas práticas e adoção de soluções tecnológicas eficazes. Ao longo deste eBook, exploramos os principais riscos, vulnerabilidades e estratégias para proteger sua empresa contra ameaças digitais.

Agora, é hora de colocar esse conhecimento em prática e fortalecer a segurança do seu ambiente digital.

Realize um diagnóstico de segurança

Identifique pontos vulneráveis na sua rede, dispositivos e práticas internas.

Implemente autenticação multifator (MFA)

Adicione camadas extras de proteção contra acessos indevidos.

Eduque e treine sua equipe

Funcionários bem treinados são a melhor defesa contra ataques de engenharia social e phishing.

Revise acessos e permissões

Utilize o princípio do privilégio mínimo para evitar acessos desnecessários a sistemas críticos.

Mantenha sistemas e dispositivos sempre atualizados

Vulnerabilidades em softwares desatualizados são uma das portas de entrada mais exploradas por hackers.

Adote uma abordagem de segurança em camadas

Combine firewall, proteção de endpoints, criptografia de dados e monitoramento contínuo para reduzir riscos.

Essas são apenas algumas das medidas essenciais para manter sua empresa protegida em um mundo digital cada vez mais complexo.

A hora de agir é agora. Quanto antes sua empresa adotar boas práticas de segurança, menores serão os riscos e maiores serão os benefícios de um ambiente digital seguro, confiável e preparado para o futuro.

COMO O MILVUS E A CECYBER PODEM AJUDAR

A cibersegurança não precisa ser um desafio enfrentado sozinho. Com soluções inteligentes e integradas, é possível automatizar a proteção digital e reduzir riscos de forma eficiente.

O Milvus oferece uma abordagem robusta para centralizar e monitorar operações de segurança, garantindo controle total sobre a infraestrutura digital da sua empresa.

MILVUS

Confira as nossas soluções

Centralize e monitore suas operações de forma segura - Com a Gestão de Canais Omnichannel do Milvus, você acompanha todas as atividades críticas da sua empresa em tempo real, detectando possíveis vulnerabilidades antes que elas se tornem problemas.

Detecte e neutralize ameaças rapidamente - Com a funcionalidade de Monitoramento de Dispositivos, o Milvus envia alertas imediatos sobre problemas de segurança, como falta de antivírus ou terminais desatualizados, permitindo que você tome medidas rápidas para garantir a proteção da sua infraestrutura.

Proteja dados sensíveis com segurança reforçada - O Cofre de Senhas e Autenticação 2FA do Milvus mantém suas informações críticas protegidas, dificultando o acesso de invasores.

Reduza a exposição de dados sensíveis - O Chatbot Milvus, integrado com o ChatGPT, fornecerá respostas automáticas e instantâneas, garantindo que informações sensíveis sejam tratadas com segurança e reduzindo a exposição a riscos.

Minimize danos financeiros e reputacionais - A Base de Conhecimento estruturada permitirá documentar e compartilhar procedimentos de segurança, garantindo respostas rápidas e minimizando danos financeiros e reputacionais em incidentes cibernéticos.

Reduza custos e garanta alta performance - O Milvus Automatiza os Processos, eliminando redundâncias, otimizando recursos e melhorando a eficiência da sua equipe.

Já a CECyber traz toda a expertise e capacitação em cibersegurança. Com uma abordagem prática e imersiva, o CECyber capacita profissionais e empresas para lidar com os desafios da segurança digital de forma eficiente. Os cursos são intensivos, aplicados aos desafios de segurança de empresas de todos os portes.

Confira as soluções CECyber

Capacitação prática e realista – Simulações em laboratórios avançados e cyber ranges replicam ambientes reais de trabalho, garantindo aprendizado aplicado.

Treinamento em segurança defensiva e ofensiva – Cursos abrangem desde proteção de infraestrutura e redes até técnicas avançadas de ataque e defesa.

Desenvolvimento seguro e DevSecOps – Treinamentos especializados para garantir segurança no ciclo devida do software.

Gestão e governança em cibersegurança – Formação estratégica para líderes e tomadores de decisão que precisam fortalecer a proteção digital de suas empresas.

Inclusão social e formação de novos talentos – Iniciativas educacionais promovem bolsas de estudo e qualificação para novas gerações de profissionais da área.

Além disso, a CECyber é parceira oficial de **certificação da Cisco e da CompTIA.** Possui também um prestigiado programa de pós-graduação, com cursos como **SEGURANÇA DA INFORMAÇÃO E INTELIGÊNCIA DEFENSIVA** e o novo **MBA CECYBER DE SEGURANÇA DA INFORMAÇÃO COM INTELIGÊNCIA ARTIFICIAL.**

Com o suporte do Milvus e da CECyber, sua empresa pode reforçar a segurança digital e também capacitar equipes para agir de forma proativa contra ameaças cibernéticas.

Com essas soluções, você ganha um ambiente digital mais protegido, eficiente e preparado para os desafios da cibersegurança moderna.

Proteja sua empresa com o Milvus e aproveite ofertas exclusivas!

Agora que você já conhece as melhores práticas para reforçar a segurança digital do seu negócio, **que tal dar o próximo passo?**

Por tempo limitado, o Milvus está oferecendo

condições especiais de até 50% OFF*

para que sua empresa se proteja contra ameaças digitais!

Saiba mais e aproveite a oferta exclusiva clicando aqui

Mas atenção! A oferta é válida

apenas até 28/02/2025!

* Confira o regulamento

milvus.com.br

MILVUS CECyber