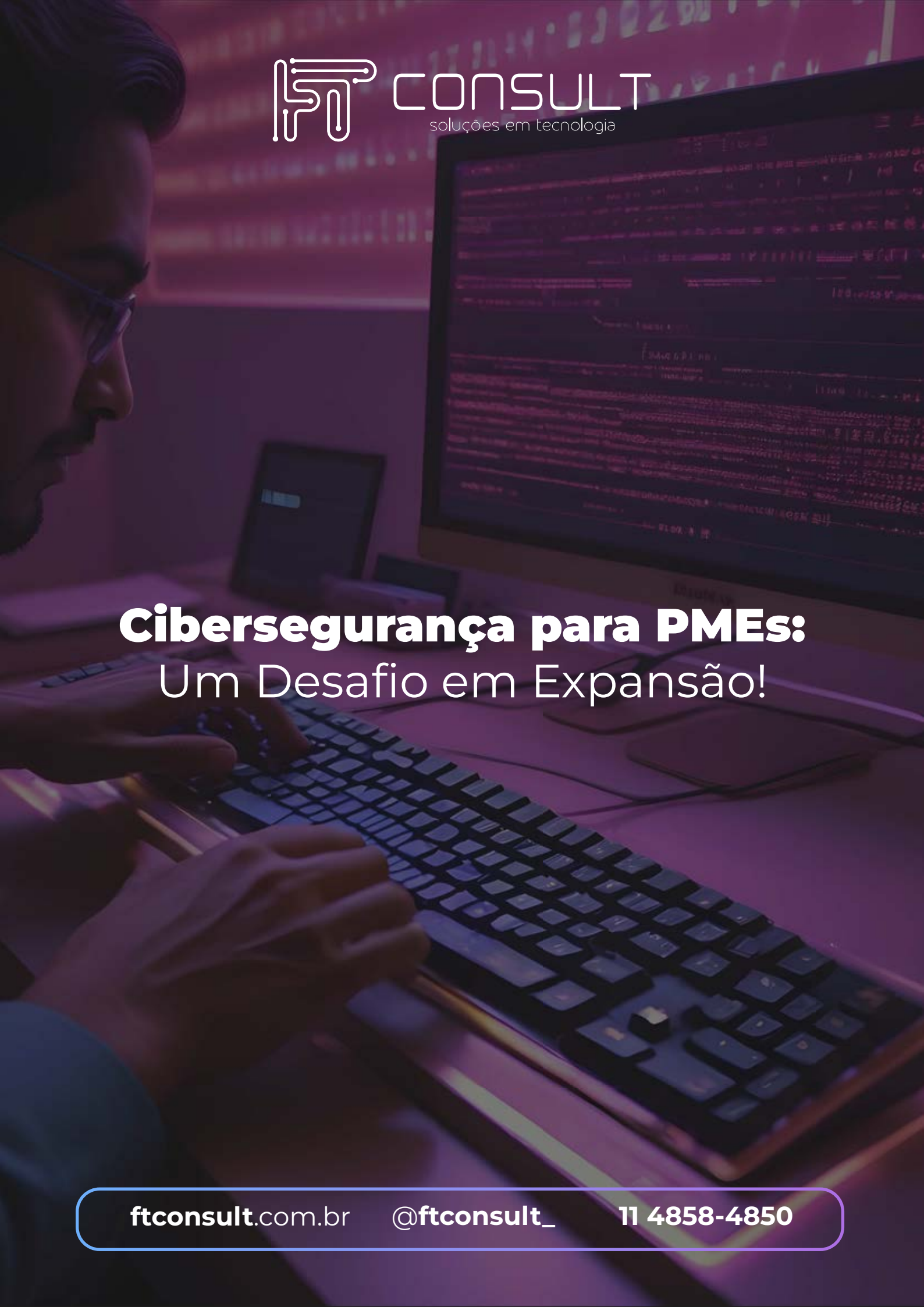

CONSULT
soluções em tecnologia
Cibersegurança para PMEs:
Um Desafio em Expansão!
ftconsult.com.br
@ftconsult_
11 4858-4850

Sumário

Introdução

Com mais de uma década de experiência no mercado, aqui na **FT Consult** já lidamos com inúmeros desafios relacionados à cibersegurança das empresas. Acompanhamos de perto todas as mudanças e desafios que surgiram nos últimos anos no mundo **cibernético!**

É cada vez mais **indispensável** a adoção de medidas para a **proteção dos dados** das empresas. Existe uma concepção equivocada em torno de qual é o perfil das empresas que devem investir em **cibersegurança,** muitas pessoas ainda acreditam que essa questão diz respeito apenas a empresas de grande porte, com operações complexas e que possuem **centenas de milhares** de funcionários.

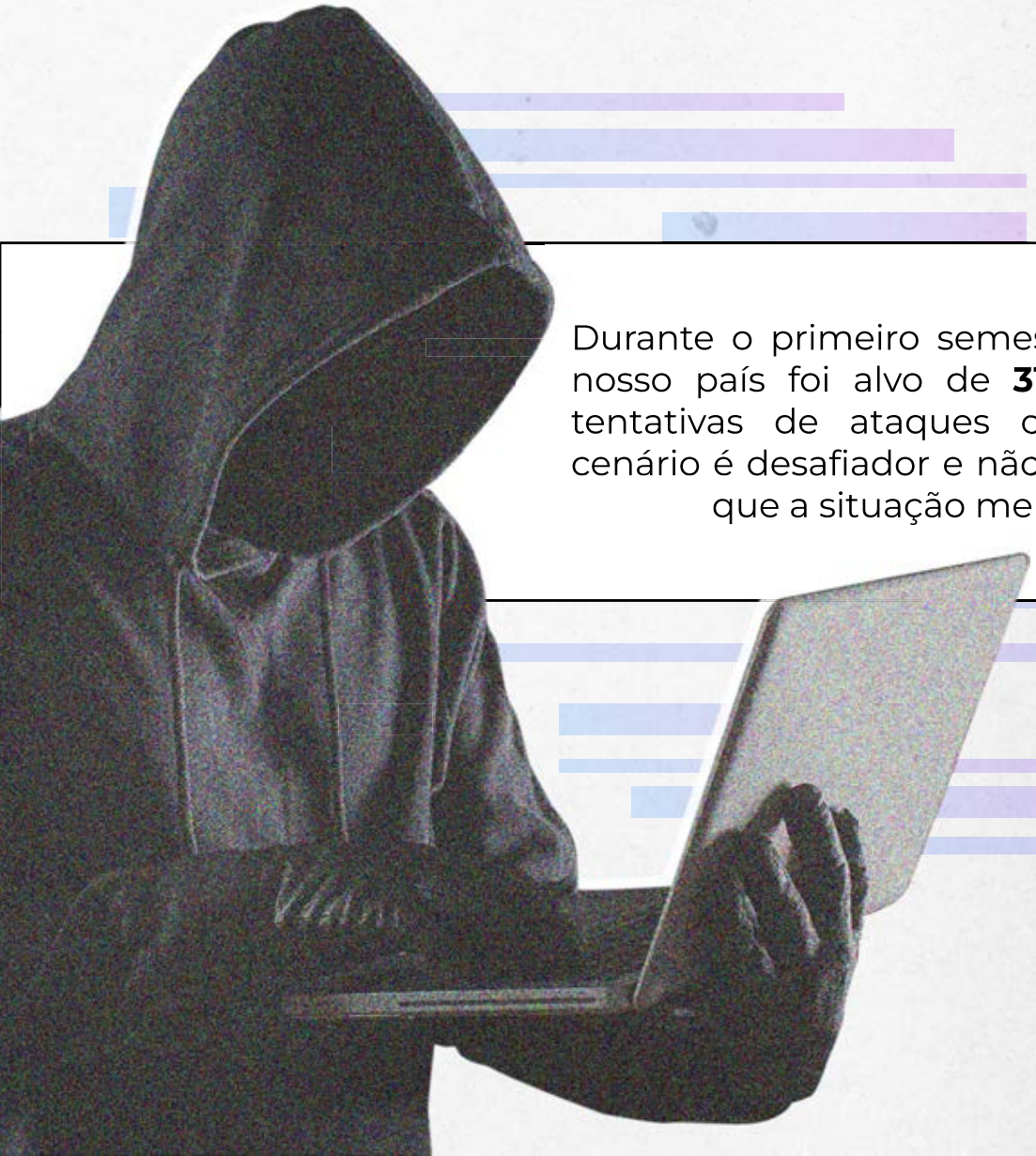
Neste **e-book** esperamos quebrar essa percepção e demonstrar, principalmente aos **pequenos** e **médios empresários,** que a cibersegurança deve ser uma prioridade para negócios de todos os portes!

A **cibersegurança,** portanto, é vital para garantir não só a proteção dos dados, mas também a continuidade das operações empresariais. Para as **PMEs,** a falta de proteção pode significar a **perda** de dados valiosos, interrupção de negócios e **danos irreparáveis** à reputação.

O Cenário da Cibersegurança no Brasil

O avanço da tecnologia trouxe inúmeras facilidades e oportunidades para as empresas. No entanto, esse progresso também abriu caminho para ameaças digitais cada vez mais sofisticadas.

De acordo com dados coletados pela **Kaspersky** (uma empresa russa que atua no ramo de desenvolvimento de softwares de segurança cibernética), entre Outubro de 2022 e Outubro de 2023, houve **192 milhões de tentativas** de ataques cibernéticos bloqueados contra **pequenas e médias empresas** no Brasil, isso equivale a 365 ataques por minuto! A maior incidência de ataques cibernéticos contra pequenas e médias empresas, comparadas a empresas de maior porte, se dá devido à percepção de que elas possuem **defesas mais fracas.**



Durante o primeiro semestre de 2024 o nosso país foi alvo de **31,5 bilhões** de tentativas de ataques cibernéticos. O cenário é desafiador e não há indícios de que a situação melhore no futuro.

O Cenário da Cibersegurança no Brasil

Ao realizarmos uma análise de uma pesquisa feita pela **AX4B** em 2023 (organização especializada em soluções de tecnologia), nos deparamos com uma realidade preocupante das **PMEs** quanto aos ciberataques. Mais da metade das empresas (**61,5%**) que foram vítimas de ataques, optaram por pagar os resgates exigidos pelos criminosos na tentativa de reaver os seus dados.

Dentre as empresas afetadas, 45,7% tiveram que arcar com valores superiores a **R$100 mil reais.** Diante dessas informações podemos concluir que nenhuma empresa está imune a esse tipo de ataque. Aqui na **FT Consult,** temos o compromisso em conscientizar e auxiliar as PMEs na adoção de melhores práticas de segurança cibernética.

Gustavo Oliveira, Head de Segurança da AX4B, alertou sobre a gravidade da situação: "Os números revelam uma realidade alarmante. Independentemente do porte, setor ou modelo de trabalho, nenhuma empresa estará imune aos ataques cibernéticos em 2024. É crucial que as organizações priorizem a segurança digital e adotem medidas preventivas robustas, como soluções de antivírus para empresas, proteção anti-ransomware e firewall." Comenta.

* * * *

Os Desafios das PMEs para Protegerem os seus Dados

As **PMEs** são frequentemente vistas como alvos fáceis pelos ataques cibernéticos sofisticados. Isso ocorre porque muitas vezes elas não possuem os mesmos recursos de segurança do que grandes corporações.

São muitos os desafios que as PMEs enfrentam em relação à **cibersegurança.** Desde a falta de recursos dedicados a essa área, equipes de TI pequenas e despreparadas, serviços terceirizados que não realizam o acompanhamento contínuo e que não adotam medidas eficazes.

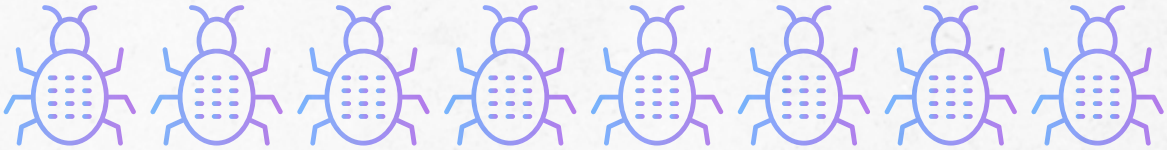
O baixo nível de **conscientização** dos colaboradores e gestores sobre as ameaças cibernéticas também é um obstáculo para as **PMEs.**

Muitos gestores subestimam a vulnerabilidade da empresa, pois, como já abordado anteriormente, existe a percepção errônea de que os cibercriminosos só se interessam por empresas de grande porte.

Existe ainda o desafio de acompanhar a complexidade crescente nas regulamentações de privacidade e segurança de dados, para que as PMEs sigam de acordo com as leis vigentes como a **GDPR** e a **LGPD.**

A falta de conhecimento especializado e verba para investir em cibersegurança é uma grande pedra no sapato das pequenas e médias empresas. **Mas é exatamente por isso que a FT está aqui!**

As Principais Ameaças às PMEs



As ameaças cibernéticas estão em constante evolução, tornando cada vez mais difícil para as empresas se protegerem. Porém, existem as ameaças mais comuns que precisamos conhecer para estarmos preparados para combatê-las.

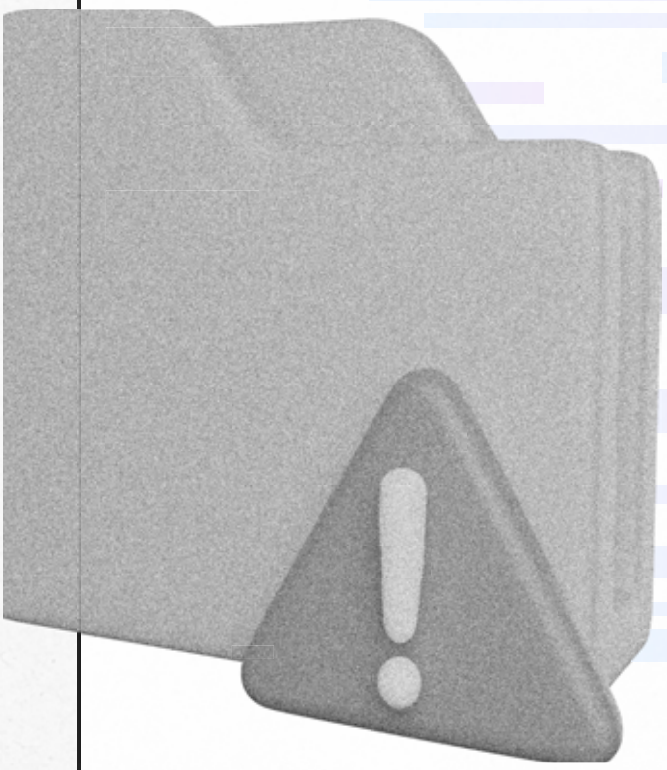
Ransomware

O **ransomware** é um tipo de malware (software malicioso) que bloqueia o acesso a dados ou sistemas da empresa, geralmente criptografando arquivos importantes.

Como funciona:
Os cibercriminosos distribuem ransomware por meio de e-mails de phishing, downloads maliciosos ou vulnerabilidades de software. Uma vez instalado no sistema, ele criptografa os dados e exibe uma mensagem exigindo o pagamento para que a chave de desbloqueio seja fornecida. Em alguns casos, os criminosos também ameaçam divulgar os dados se o resgate não for pago.

Exemplo:
Em 2017, o ataque do ransomware **WannaCry** afetou centenas de milhares de computadores ao redor do mundo, incluindo grandes corporações e sistemas de saúde. Os usuários infectados foram instruídos a pagar resgates em Bitcoin para recuperar o acesso aos seus arquivos.

Impactos:

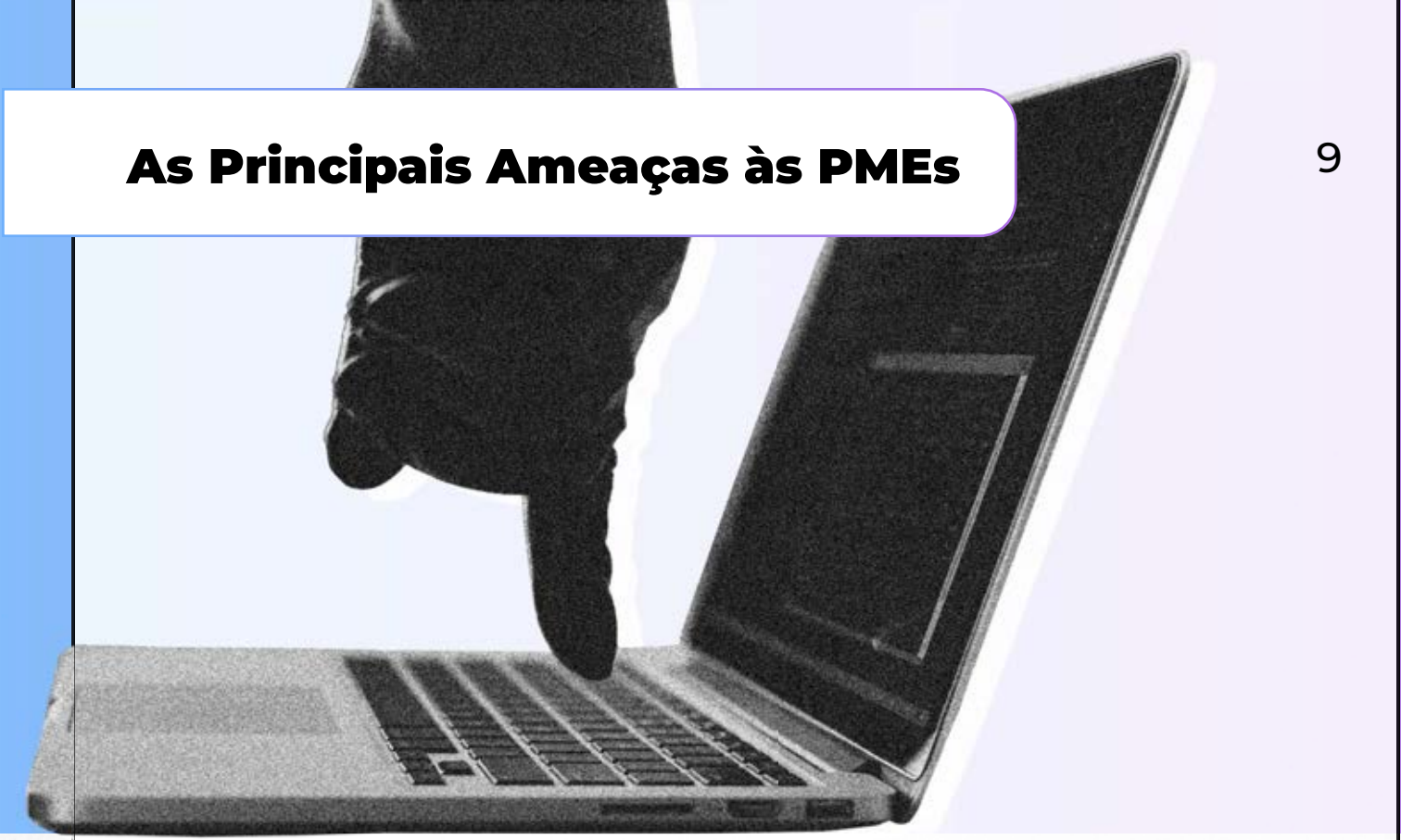


- Perda total de dados críticos, se não houver backup.
- Interrupção completa das operações da empresa.
- Potenciais danos à reputação, especialmente em casos de vazamento de dados.

Prevenção:

- Manter backups regulares de dados críticos em locais seguros e isolados da rede.
- Atualizar regularmente os sistemas operacionais e aplicativos para corrigir vulnerabilidades.
- Utilizar software antivírus e anti-ransomware.
- Treinamento constante dos funcionários sobre boas práticas de segurança

As Principais Ameaças às PMEs



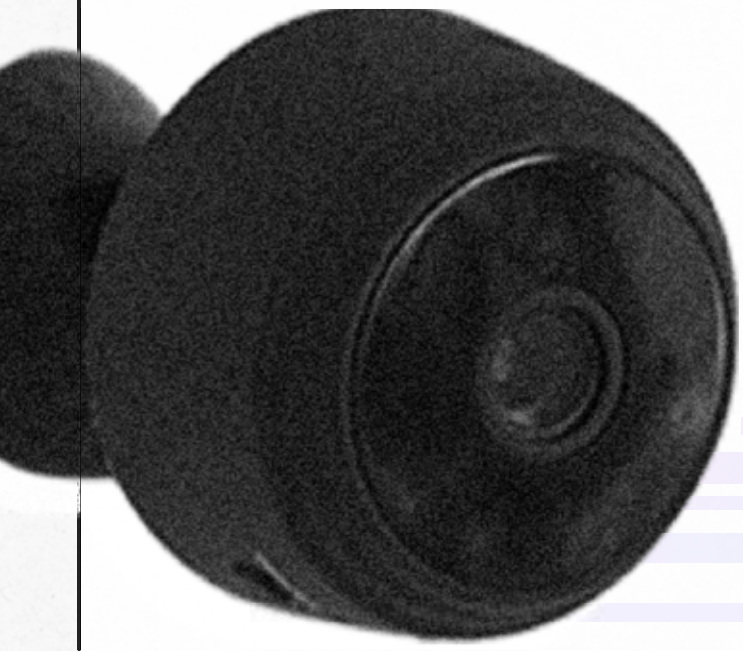
Malware

O malware (abreviação de "software malicioso") é um termo genérico para descrever qualquer programa ou código que tem como objetivo prejudicar sistemas, redes ou dispositivos. Esse tipo de software pode assumir várias formas, incluindo vírus, worms, spyware, trojans, entre outros.

Como funciona:
O malware pode ser introduzido em um sistema de várias maneiras: por e-mails infectados, downloads de software não confiável, dispositivos USB contaminados ou vulnerabilidades de segurança.

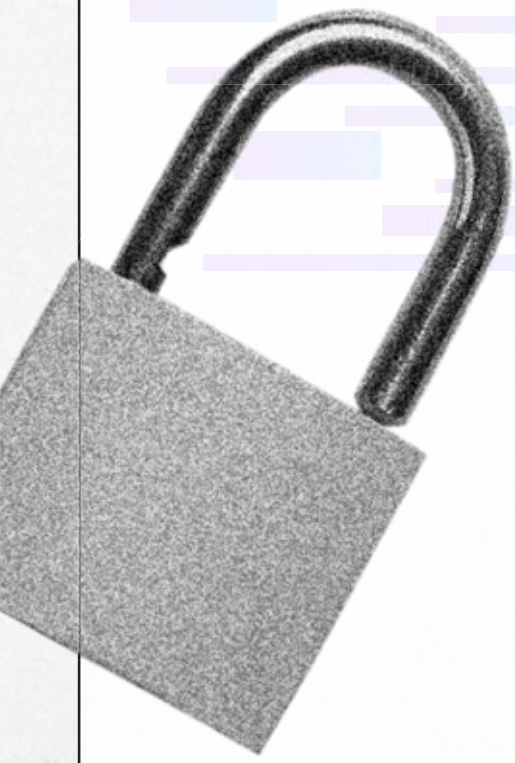
Exemplo:
Um exemplo clássico de malware é o Cavalo de Troia (Trojan), que se disfarça como um programa útil ou inofensivo, mas uma vez instalado, oferece aos criminosos controle sobre o computador da vítima. Isso pode incluir roubo de dados, espionagem ou criação de portas para futuras invasões.

Impactos:



- Comprometimento de dados confidenciais.
- Perda de controle sobre o sistema.
- Risco de espionagem corporativa.
- Dano irreparável à infraestrutura de TI.

Prevenção:



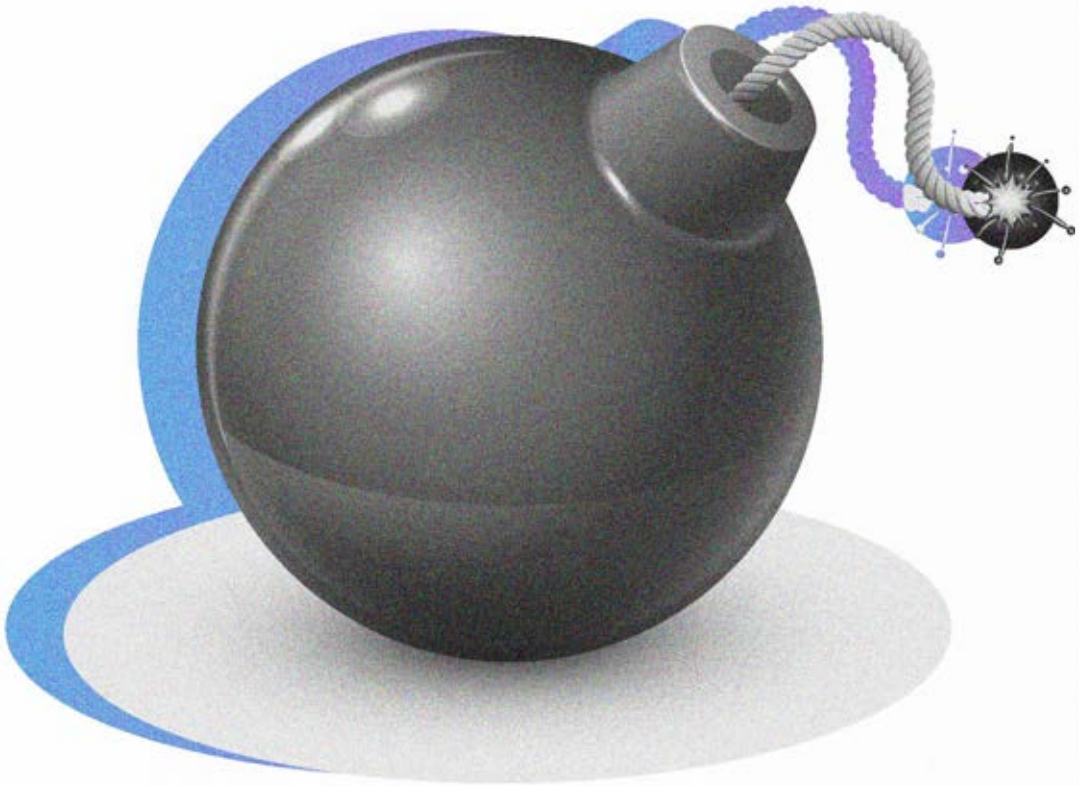
- Implementar softwares de segurança robustos e manter todos os sistemas atualizados.
- Treinamento de funcionários para reconhecer sinais de malware.
- Restringir downloads de software de fontes não verificadas.

Ataques DDoS (Distributed Denial of Service)

Um ataque DDoS (ataque distribuído de negação de serviço) sobrecarrega os sistemas de uma empresa com um grande volume de tráfego falso, tornando seus serviços e sites indisponíveis para usuários legítimos. Esses ataques geralmente envolvem o uso de uma rede de computadores infectados (também conhecida como botnet) para inundar os servidores da empresa com solicitações simultâneas.

Como funciona:
Os atacantes comprometem vários dispositivos conectados à internet, criando uma botnet que, quando ativada, sobrecarrega os servidores alvo com mais solicitações do que eles podem processar. Isso resulta em lentidão ou interrupção completa dos serviços.

Exemplo:
Em 2016, o ataque DDoS à Dyn, uma grande provedora de DNS, causou interrupções em sites populares como Twitter, Spotify, e Amazon. Milhões de dispositivos IoT foram infectados com malware e usados como uma botnet para lançar o ataque.



Impactos:

- Indisponibilidade de serviços online e interrupção das operações.
- Perda de receita em e-commerces.
- Danos à reputação por inatividade prolongada.
- Potenciais penalidades contratuais, dependendo do setor.

Prevenção:

- Implementar serviços de mitigação DDoS que detectam e bloqueiam tráfego malicioso.
- Usar balanceamento de carga e redes de entrega de conteúdo (CDN) para distribuir o tráfego.
- Monitoramento contínuo para identificar sinais de ataques antes que causem danos.

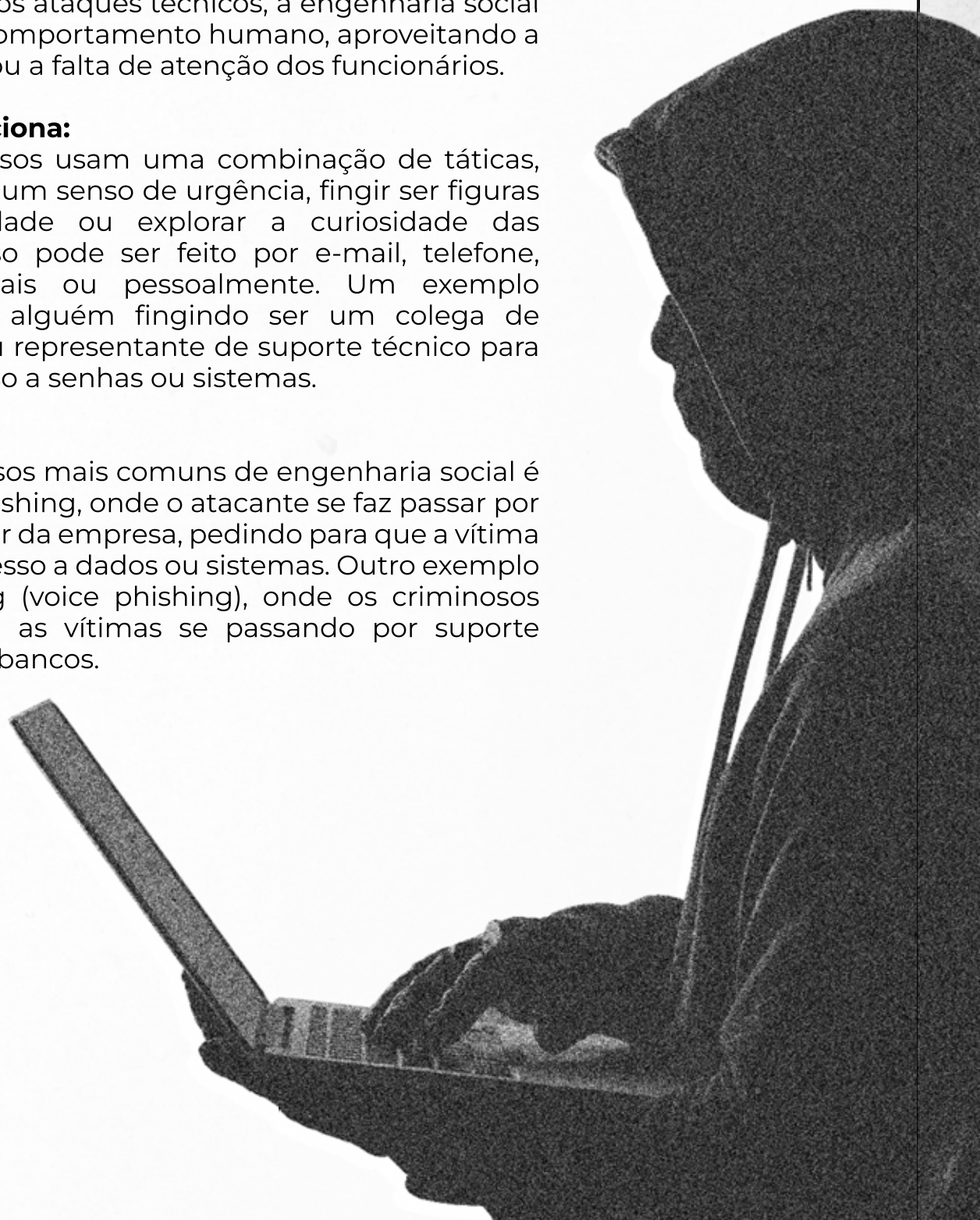
As Principais Ameaças às PMEs

Engenharia Social

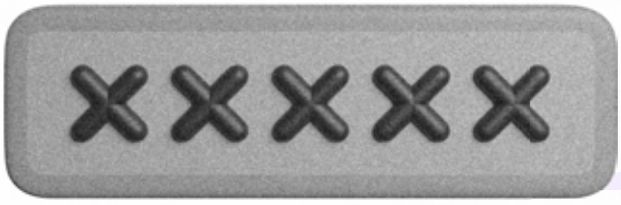
Engenharia social é uma técnica onde os cibercriminosos manipulam psicologicamente as vítimas, induzindo-as a revelar informações confidenciais ou a realizar ações que comprometem a segurança da empresa. Ao contrário dos ataques técnicos, a engenharia social explora o comportamento humano, aproveitando a confiança ou a falta de atenção dos funcionários.

Como funciona:
Os criminosos usam uma combinação de táticas, como criar um senso de urgência, fingir ser figuras de autoridade ou explorar a curiosidade das vítimas. Isso pode ser feito por e-mail, telefone, redes sociais ou pessoalmente. Um exemplo comum é alguém fingindo ser um colega de trabalho ou representante de suporte técnico para obter acesso a senhas ou sistemas.

Exemplo:
Um dos casos mais comuns de engenharia social é o Spear Phishing, onde o atacante se faz passar por um superior da empresa, pedindo para que a vítima forneça acesso a dados ou sistemas. Outro exemplo é a vishing (voice phishing), onde os criminosos ligam para as vítimas se passando por suporte técnico ou bancos.



Impactos:



- Acesso não autorizado a sistemas críticos.
- Vazamento de informações confidenciais.
- Comprometimento de senhas e credenciais.
- Fraudes financeiras e danos à reputação.

Prevenção:

- Treinar os funcionários para reconhecer tentativas de engenharia social.
- Implementar políticas de verificação rigorosas antes de fornecer informações sensíveis.
- Reforçar a conscientização sobre o perigo de compartilhar informações sem verificação adequada.

Além dos prejuízos financeiros, esses ataques têm um impacto significativo na continuidade das atividades das PMEs. De acordo com uma pesquisa realizada pela IBM (International Business Machines Corporation), realizada entre 2021 e 2022, revela que 75% das pequenas e médias empresas que sofrem ataques cibernéticos de grande escala acabam praticamente fechando as portas!

Medidas de Proteção Essenciais

Em vista dos dados apresentados, já não nos resta dúvida da importância em investir em cibersegurança para as PMEs. Portanto, adotar medidas de proteção adequadas é crucial para garantir a segurança dos dados e a continuidade dos negócios.

Vamos entender um pouco mais a fundo agora, sobre algumas medidas de proteção essenciais que as PMEs podem implementar em suas operações, para mitigar os riscos de ataques cibernéticos.

Backup Regular e Criptografia dos Dados

Uma das práticas mais importantes para evitar perdas de dados é realizar backups regulares e garantir que esses backups sejam armazenados de forma criptografada e em locais externos à rede principal da empresa, como servidores em nuvem seguros. Isso garante que, em caso de ataques como ransomware, a empresa consiga restaurar seus dados sem precisar ceder às exigências dos criminosos.

Uso de Autenticação de Dois Fatores (2FA)

A autenticação de dois fatores (2FA) adiciona uma camada extra de segurança ao exigir uma segunda forma de verificação além da senha, como um código enviado para o celular ou um aplicativo autenticador. Isso dificulta o acesso de invasores, mesmo que eles consigam descobrir a senha de um funcionário.

Medidas de Proteção Essenciais

Política de Senhas Fortes

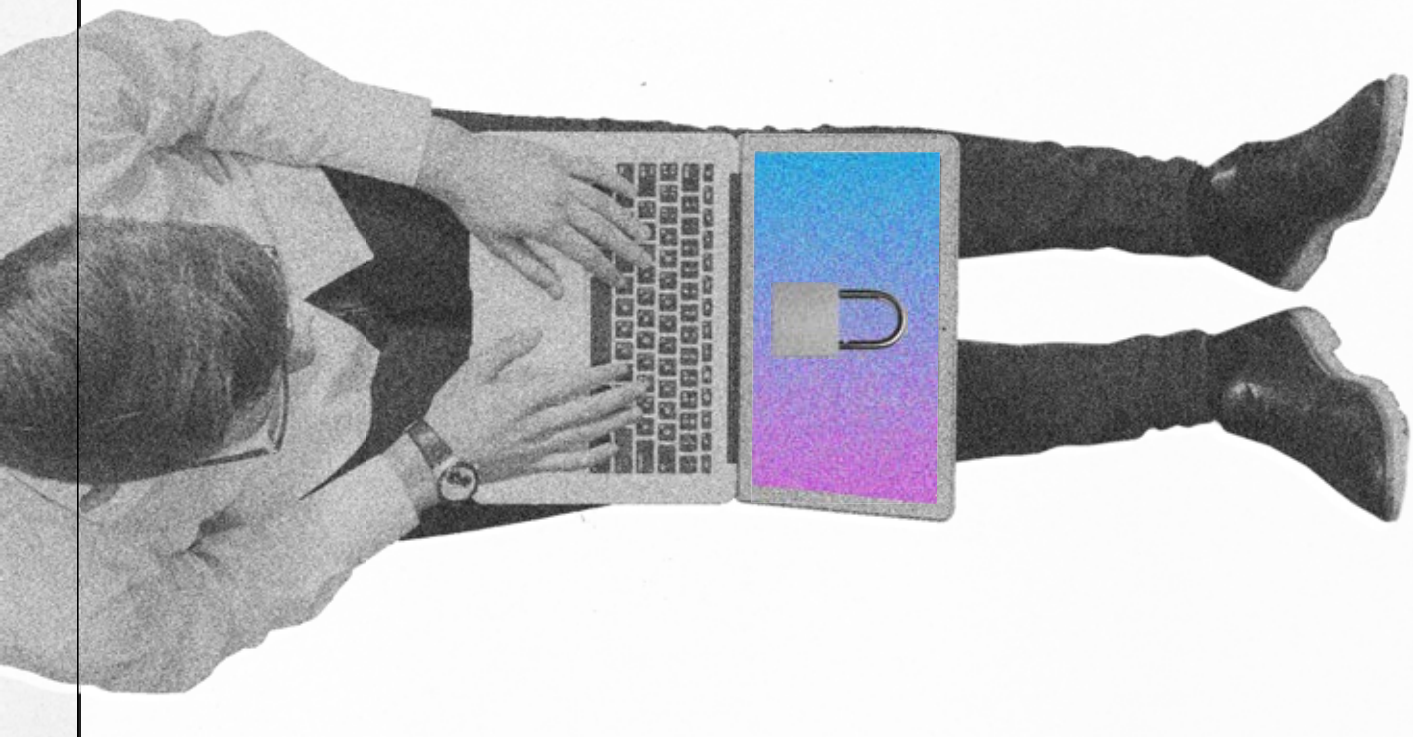
Senhas fracas são uma das portas de entrada mais comuns para ciberataques. As PMEs devem implementar políticas rigorosas de senhas, exigindo o uso de combinações complexas de letras, números e símbolos, além de troca periódica. Recomenda-se também o uso de gerenciadores de senhas, que facilitam o armazenamento e a criação de senhas seguras.

Educação e Treinamento dos Funcionários

Um dos maiores riscos para a segurança cibernética é a falta de conscientização e treinamento dos colaboradores. Engenheiros sociais e ataques de phishing costumam explorar a falta de conhecimento dos funcionários para roubar informações confidenciais. Realizar treinamentos periódicos para conscientizar os colaboradores sobre os tipos de ameaças, como identificar e-mails suspeitos e a importância de seguir boas práticas de segurança, pode reduzir consideravelmente as chances de ataques bem-sucedidos.

Uso de Softwares Antivírus e Antimalware

Manter um software de antivírus e antimalware atualizado é fundamental para proteger a infraestrutura de TI da empresa contra ataques. Essas ferramentas são capazes de identificar, isolar e eliminar ameaças como vírus, trojans, spyware e ransomwares. Além disso, elas oferecem proteção em tempo real, alertando os usuários sobre possíveis riscos.



Medidas de Proteção Essenciais

Firewall e Segmentação de Redes

Um firewall é uma barreira de segurança entre a rede interna da empresa e fontes externas de tráfego, como a internet. Ele monitora e controla o tráfego de entrada e saída, bloqueando acessos não autorizados. Além disso, segmentar a rede da empresa em diferentes partes ajuda a isolar áreas mais críticas de TI, limitando o impacto de um ataque que consiga penetrar em algum setor da rede.

Controle de Acesso Rigoroso

Nem todos os funcionários precisam ter acesso a todas as informações da empresa. Implementar um controle de acesso rigoroso, limitando os dados e sistemas aos quais cada funcionário tem acesso com base em suas funções, pode evitar que um eventual comprometimento de credenciais resulte em perda de informações críticas.

Monitoramento Contínuo e Detecção de Intrusões

Implementar ferramentas de monitoramento contínuo ajuda a identificar atividades suspeitas em tempo real. Soluções de detecção de intrusões (IDS) ou detecção e prevenção de intrusões (IDPS) monitoram o tráfego da rede em busca de sinais de ataques, notificando a equipe de TI sobre anomalias antes que causem danos maiores.

Atualizações Regulares de Software

Manter todos os softwares atualizados é uma prática essencial para evitar vulnerabilidades exploradas por cibercriminosos. Isso inclui o sistema operacional, aplicativos de terceiros e qualquer software de segurança. Muitas vezes, as atualizações trazem patches de segurança que corrigem falhas recentemente descobertas.

Diante de tantas questões, desafios e dilemas que as **PMEs** enfrentam na cibersegurança dos seus negócios, muitos gestores podem ficar completamente desencorajados e assustados.

A missão da **FT** é trazer soluções inovadoras e **revolucionárias** para suprir as necessidades das PMEs em seus departamentos de tecnologia.

Pensando bem, a maioria das PMEs, analisando o cenário que apresentamos ao longo do e-book, não possuem um departamento de TI realmente preparado para lidar com a **cibersegurança.**

Descomplicada, acessível, simples, essas são as palavras que você vai usar para descrever a tecnologia quando você conhecer o que a **FT** pode fazer pela **sua empresa.**

Ao invés de se preocupar em manter uma **equipe de TI** no seu negócio, colocar funcionários despreparados para lidar com os problemas ou contratar serviços terceirizados que apenas apagam incêndios localizados, com a **FT,** a realidade será bem diferente.

Diante de tantas questões, desafios e dilemas que as **PMEs** enfrentam na cibersegurança dos seus negócios, muitos gestores podem ficar completamente desencorajados e assustados.

A missão da **FT** é trazer soluções inovadoras e **revolucionárias** para suprir as necessidades das PMEs em seus departamentos de tecnologia.

Pensando bem, a maioria das PMEs, analisando o cenário que apresentamos ao longo do e-book, não possuem um departamento de TI realmente preparado para lidar com a **cibersegurança.**

Descomplicada, acessível, simples, essas são as palavras que você vai usar para descrever a tecnologia quando você conhecer o que a **FT** pode fazer pela **sua empresa.**

Ao invés de se preocupar em manter uma **equipe de TI** no seu negócio, colocar funcionários despreparados para lidar com os problemas ou contratar serviços terceirizados que apenas apagam incêndios localizados, com a **FT,** a realidade será bem diferente.

Conclusão

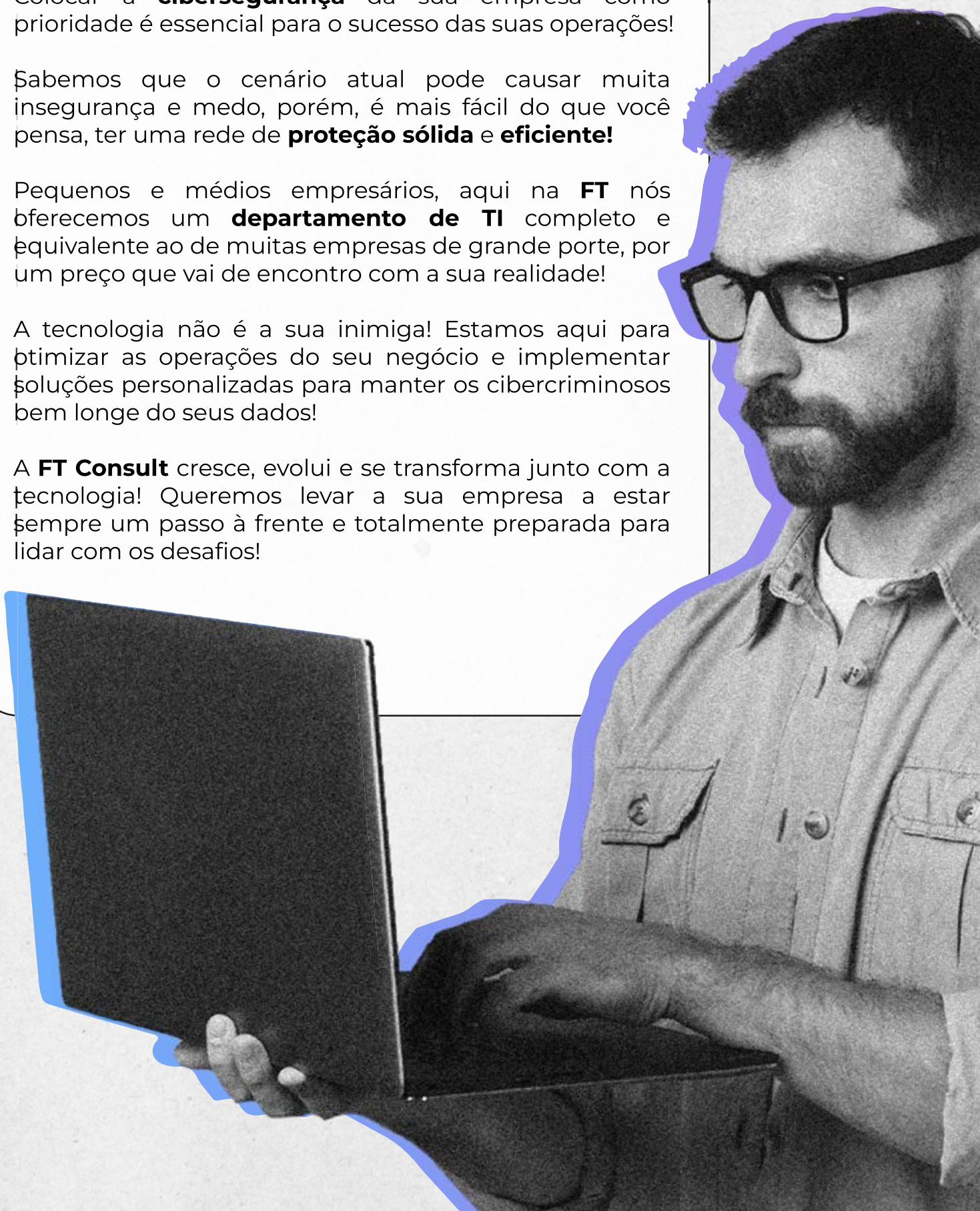
Colocar a **cibersegurança** da sua empresa como prioridade é essencial para o sucesso das suas operações!

Sabemos que o cenário atual pode causar muita insegurança e medo, porém, é mais fácil do que você pensa, ter uma rede de **proteção sólida** e **eficiente!**

Pequenos e médios empresários, aqui na **FT** nós oferecemos um **departamento de TI** completo e equivalente ao de muitas empresas de grande porte, por um preço que vai de encontro com a sua realidade!

A tecnologia não é a sua inimiga! Estamos aqui para otimizar as operações do seu negócio e implementar soluções personalizadas para manter os cibercriminosos bem longe do seus dados!

A **FT Consult** cresce, evolui e se transforma junto com a tecnologia! Queremos levar a sua empresa a estar sempre um passo à frente e totalmente preparada para lidar com os desafios!




FT CONSULT
soluções em tecnologia
Descubra a **tecnologia descomplicada** com a **FT Consult!**
ftconsult.com.br
@**ftconsult_**
11 4858-4850