MILVUS

RANSOMWARE

COMO PROTEGER AS INFORMAÇÕES DAS EMPRESAS DESTA AMEAÇA?

milvus.com.br

APRESENTAÇÃO

O ransomware se tornou uma das ameaças cibernéticas mais perigosas e lucrativas para criminosos digitais.

Empresas de todos os portes estão na mira desses ataques, que sequestram dados e exigem resgates milionários, causando prejuízos financeiros e operacionais devastadores.

Neste eBook **“Ransomware - Como proteger as informações das empresas desta ameaça?”**, você entenderá como o ransomware funciona, quais são as estratégias mais comuns usadas pelos hackers e, principalmente, como proteger sua empresa dessa ameaça.

Além disso, exploraremos soluções eficazes para prevenir ataques e minimizar os impactos caso sua organização seja alvo desse tipo de crime digital.

Descubra as melhores práticas de segurança da informação e veja como o Milvus pode ajudar sua empresa a manter seus dados protegidos e evitar prejuízos.

Este eBook foi originalmente escrito por Fouad Ata em 2022 e atualizado em 2025 pela equipe do Milvus, incorporando as mais recentes informações, tendências e casos relevantes do setor de cibersegurança

Fouad Ata

fouad@infomach.com.br

Engenheiro de computação com mais de 22 anos de experiência, especialista em Cibersegurança. Certificações e curso em: CCNA, CCNP | CheckPoint | ITIL V3 | MCP, MCSA, MCSE | CEH | Arquiteto AWS | CNSS | MGMT 3.0

INTRODUÇÃO

Os crimes cibernéticos estão em constante crescimento, afetando empresas e indivíduos em qualquer lugar do mundo. Ataques digitais podem ser lançados de qualquer parte do planeta, comprometendo dados e operações críticas a milhares de quilômetros de distância.

Entre as ameaças mais perigosas está o ransomware, um ataque que sequestra dados e exige resgate financeiro para sua liberação.

Essa prática tem sido **amplamente explorada por grupos criminosos internacionais.**

Com a Lei Geral de Proteção de Dados Pessoais (LGPD) em vigor, a preocupação com a segurança digital se tornou ainda maior, pois as informações passaram a ter um valor estratégico significativo — tornando-se um alvo ainda mais atrativo para os cibercriminosos.

Este eBook foi desenvolvido para explicar como funcionam os ataques de ransomware, quais os principais impactos nas empresas e, mais importante, como você pode proteger suas informações contra essa ameaça digital.

O QUE É RANSOMWARE E COMO ELE SEQUESTRA SEUS DADOS

Entre os ataques cibernéticos, o ransomware é um dos 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.

01 Infecção
O malware entra no sistema por e-mails maliciosos (phishing), downloads infectados ou falhas em softwares desatualizados.

02 Propagação
O ransomware se espalha pela rede, comprometendo múltiplos dispositivos.

03 Criptografia dos dados
Arquivos são bloqueados, impedindo o acesso.

04 Pedido de resgate
Uma mensagem exige pagamento, geralmente em criptomoedas.

05 Sem garantia de recuperação
Mesmo pagando, não há garantia de que os dados serão restaurados.

O QUE É RANSOMWARE E COMO ELE SEQUESTRA SEUS DADOS

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.

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.

CASOS NOTÁVEIS DE RANSOMWARE

Nos últimos anos, ataques de ransomware se tornaram mais sofisticados, **causando prejuízos bilionários e impactando organizações de diversos setores.**

Empresas privadas, infraestruturas críticas e até governos foram alvos desses ataques, demonstrando que ninguém está imune.

O impacto financeiro e operacional

Os ataques de **ransomware** deixaram de ser apenas um problema de TI para se tornarem uma ameaça à continuidade dos negócios e à segurança nacional.

Além dos custos diretos com resgate e recuperação de sistemas, as empresas sofrem perdas financeiras significativas com paralisações operacionais, danos à reputação e multas regulatórias.

- **Custos com resgate**
Algumas empresas já chegaram a pagar milhões de dólares para recuperar seus dados.

- **Paralisação das operações**
Setores como energia, transporte e saúde foram gravemente afetados por ataques recentes.

- **Danos à reputação**
Empresas que sofrem vazamento de dados podem perder a confiança de clientes e parceiros.

- **Multas regulatórias**
Regulamentações como a LGPD e o GDPR penalizam organizações que falham na proteção de dados.

CASOS NOTÁVEIS DE RANSOMWARE

Tendências recentes nos ataques

Grupos mais organizados e patrocinados

Ataques como o NotPetya mostraram que algumas campanhas de ransomware podem ter motivação geopolítica, indo além do objetivo financeiro.

Ransomware como serviço (RaaS)

Criminosos agora alugam kits de ransomware para outros hackers, tornando os ataques mais acessíveis.

Ataques duplos e triplos

Além da criptografia dos arquivos, grupos de ransomware passaram a roubar dados sensíveis e ameaçar vazá-los caso o pagamento não seja feito.

Infraestruturas críticas na mira

Serviços essenciais, como energia e abastecimento de combustível, se tornaram alvos preferidos devido ao impacto gerado.

Casos recentes de grande impacto

A seguir, vamos analisar três dos casos mais marcantes dos últimos anos, explorando como ocorreram e quais foram os danos causados por essas ameaças.

- **WannaCry (2017)**
  Infectou mais de 200 mil computadores em 150 países, explorando falhas no Windows.

- **Colonial Pipeline (2021)**
  Paralisou um grande oleoduto nos EUA, resultando no pagamento de US$ 4,4 milhões.

- **Dark Angels (2024)**
  Estabeleceu o maior resgate de ransomware da história, com um pagamento recorde de US$ 75 milhões.

WANNACRY (2017)
O ATAQUE QUE PAROU O MUNDO

⚠ Como o ataque aconteceu?

O WannaCry foi um dos ataques de ransomware mais devastadores da história, afetando mais de 200 mil computadores em 150 países. O malware explorou uma vulnerabilidade do Windows chamada EternalBlue, vazada da NSA (Agência de Segurança Nacional dos EUA).

01 O WannaCry se espalhou rapidamente pela internet, explorando sistemas desatualizados.

02 Empresas, hospitais e até órgãos governamentais foram atingidos, paralisando operações.

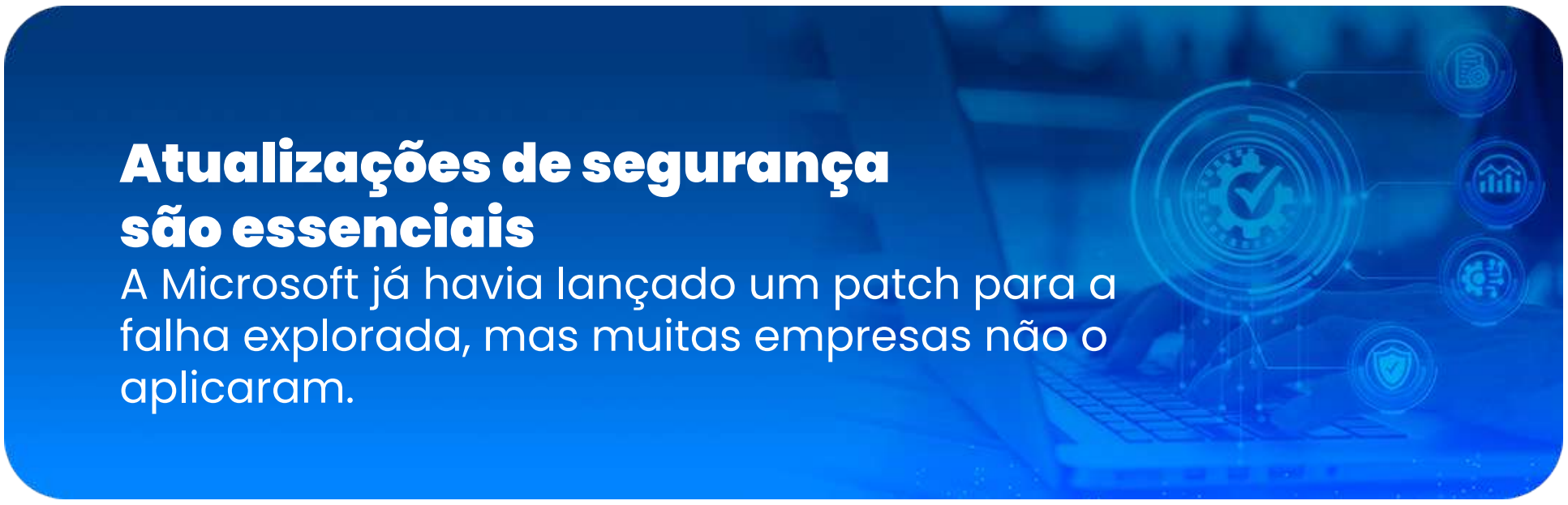
03 Os arquivos eram criptografados, e as vítimas recebiam uma exigência de pagamento em Bitcoin para restaurar o acesso.

Impacto e prejuízos

- Empresas perderam **milhões de dólares** em paralisações e recuperação de dados.
- O **Sistema Nacional de Saúde do Reino Unido (NHS)** teve hospitais e clínicas afetados, cancelando atendimentos médicos.
- Grandes corporações, como a **Renault e a FedEx**, sofreram interrupções significativas.

WANNACRY (2017)
O ATAQUE QUE PAROU O MUNDO

O que aprendemos com o WannaCry?



Atualizações de segurança são essenciais
A Microsoft já havia lançado um patch para a falha explorada, mas muitas empresas não o aplicaram.

Backups são indispensáveis
Organizações sem cópias de segurança sofreram perdas irreversíveis.

A segurança digital deve ser prioridade
O ataque mostrou como redes desatualizadas e sem proteção são vulneráveis.

O WannaCry serviu de **alerta global** sobre a importância da cibersegurança, levando empresas e governos a reforçarem suas defesas contra ransomware.

COLONIAL PIPELINE (2021)
O CIBERATAQUE QUE PAROU O ABASTECIMENTO DE COMBUSTÍVEL NOS EUA

⚠ Como o ataque aconteceu?

Em maio de 2021, a Colonial Pipeline, uma das maiores operadoras de oleodutos dos Estados Unidos, sofreu um ataque de ransomware, levando à paralisação de suas operações e afetando o fornecimento de combustível em várias regiões do país.

01 O grupo de hackers DarkSide invadiu os sistemas da empresa e criptografou dados críticos.

02 Como medida de precaução, a Colonial Pipeline suspendeu todas as operações, afetando o transporte de gasolina, diesel e querosene de aviação.

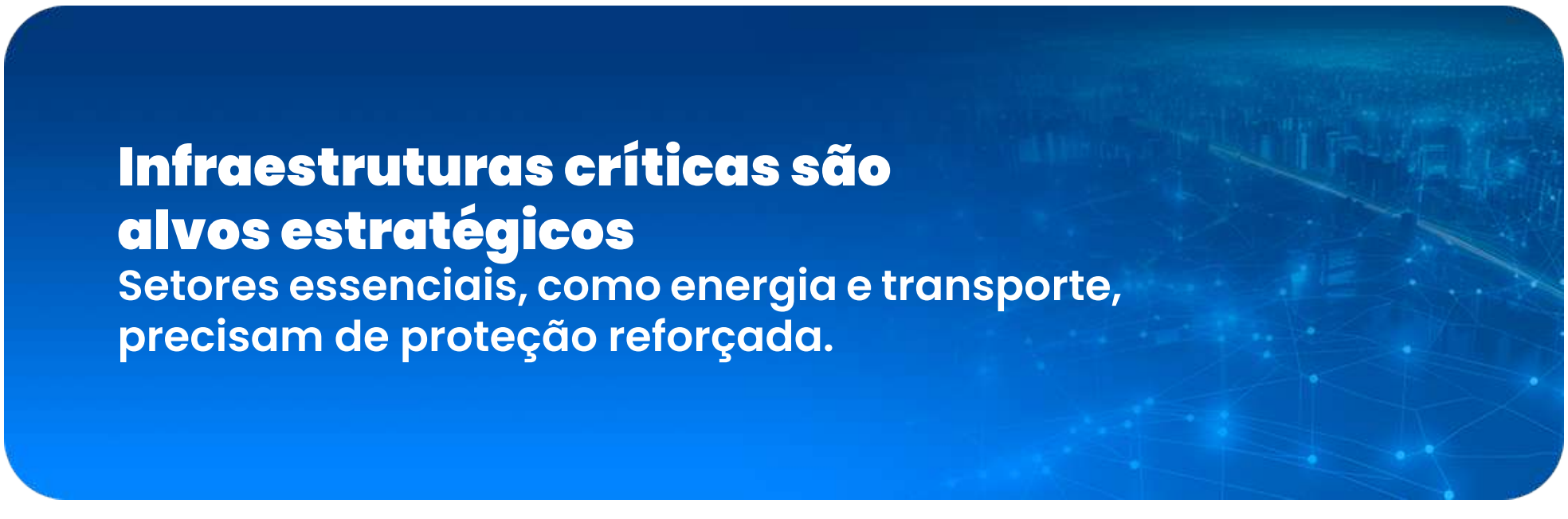
03 O ataque gerou pânico e escassez de combustível, com longas filas e preços elevados nos postos dos EUA.

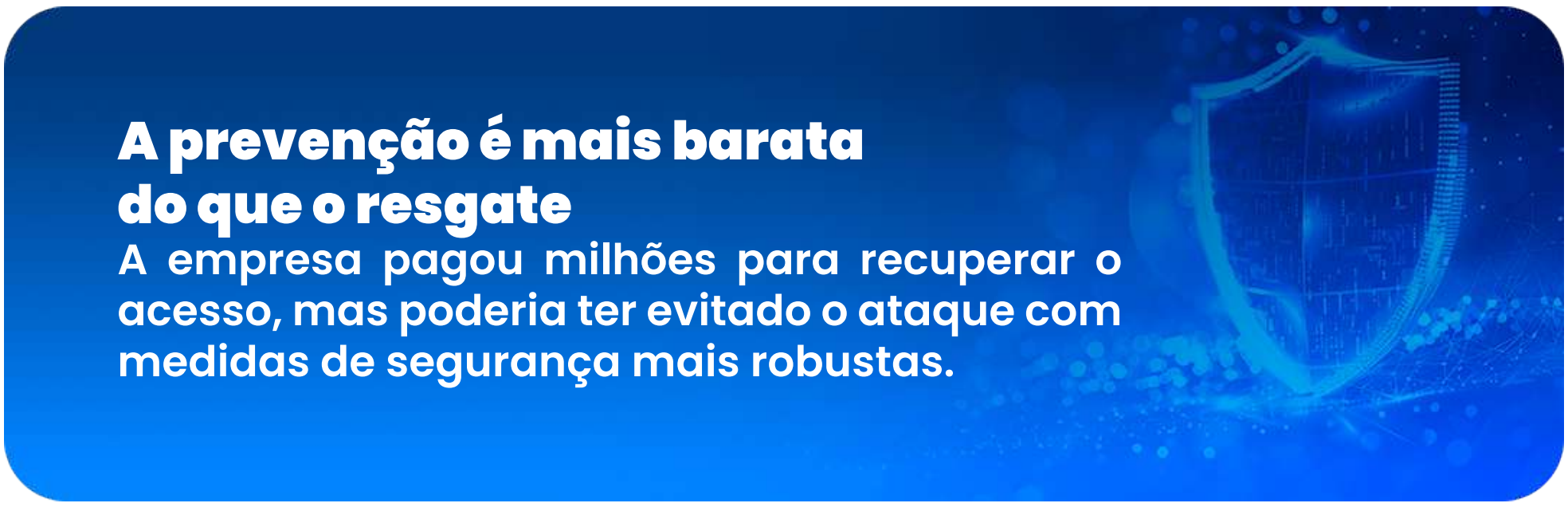
Impacto e prejuízos

- A Colonial Pipeline pagou US$ 4,4 milhões em Bitcoin para recuperar seus sistemas.
- O governo dos EUA declarou estado de emergência devido à crise no abastecimento.
- O ataque evidenciou vulnerabilidades críticas na infraestrutura de energia, colocando segurança cibernética no centro das discussões nacionais.

COLONIAL PIPELINE (2021)
O CIBERATAQUE QUE PAROU O ABASTECIMENTO DE COMBUSTÍVEL NOS EUA

O que aprendemos com o ataque à Colonial Pipeline?





O ataque à Colonial Pipeline foi um dos mais impactantes da década, evidenciando que nenhuma organização está segura sem uma estratégia eficaz de cibersegurança.

DARK ANGELS (2024)
O MAIOR RESGATE DE RANSOMWARE DA HISTÓRIA

⚠ Como o ataque aconteceu?

Em julho de 2024, o grupo cibercriminoso Dark Angels recebeu um pagamento recorde de US$ 75 milhões de uma empresa da Fortune 50, estabelecendo o maior resgate já registrado até hoje.

O caso trouxe novos desafios para a cibersegurança, evidenciando o crescimento do ransomware como uma ameaça altamente lucrativa.

01 O Dark Angels sequestrou sistemas críticos de uma grande corporação, tornando operações essenciais inacessíveis.

02 A empresa, sem alternativas imediatas, optou por pagar a maior quantia já registrada para reaver seus dados.

03 O pagamento em Bitcoin foi confirmado por análises da Chainalysis e registrado no relatório de ransomware da Zscaler.

Impacto e prejuízos

- Superou o recorde anterior de US$ 40 milhões, pago pela CNA Financial em 2021.
- Mostrou a evolução das táticas dos cibercriminosos, que agora escolhem alvos estratégicos e de alto valor.
- Reforçou a necessidade de fortalecer medidas de segurança, pois ataques direcionados estão se tornando cada vez mais sofisticados.

DARK ANGELS (2024)

O MAIOR RESGATE DE RANSOMWARE DA HISTÓRIA

O que aprendemos com o ataque do Dark Angels?

Ransomware está mais lucrativo do que nunca

O sucesso do Dark Angels pode incentivar novos ataques e grupos criminosos.

Grandes empresas continuam vulneráveis

Mesmo organizações da Fortune 50 não estão imunes a ataques sofisticados.

A prevenção é o melhor caminho

Investir em backups, autenticação multifator e monitoramento de ameaças é essencial para evitar situações semelhantes.

O Dark Angels já realizou ataques no Brasil, como no caso da Andrade Gutierrez em 2023. Seu foco em empresas estratégicas e setores essenciais mostra que nenhuma organização está totalmente segura sem uma estratégia eficaz de cibersegurança.

Fortaleça a proteção
da sua empresa
contra ataques cibernéticos
e minimize
impactos financeiros.

Teste 7 dias grátis

milvus.com.br

COMO O RANSOMWARE SE INFILTRA NO DISPOSITIVO?

Alguns tipos de ransomware podem infectar o dispositivo e acessar os arquivos sem solicitar nenhuma ação do usuário. Outros ataques funcionam por meio de infecção por malware.

Por isso, é importante conhecer as principais formas de ataque contra o seu dispositivo e ficar atento:

Kits de exploit

Utilizam ferramentas automatizadas para explorar vulnerabilidades conhecidas nos sistemas da empresa. Esse ransomware pode infectar qualquer dispositivo conectado à rede, especialmente se houver configurações inadequadas ou softwares desatualizados.

Phishing

Se disfarça como mensagens de contatos ou organizações confiáveis para enviar e-mails com anexos ou links aparentemente legítimos. Muitas vezes, os ataques utilizam engenharia social avançada para enganar usuários e convencê-los a fornecer informações sensíveis ou baixar arquivos maliciosos.

Malvertising

Incorporam malwares a anúncios online falsos, que instalam o ransomware no dispositivo assim que a página é carregada ou após o clique na publicidade. Esses ataques podem ocorrer até mesmo em sites legítimos que hospedam anúncios comprometidos.

Downloads automáticos

Criam sites maliciosos que instalam ransomware automaticamente no dispositivo assim que a página é acessada. Navegadores desatualizados e configurações de segurança fracas tornam os dispositivos ainda mais vulneráveis a essa modalidade de ataque.

Credenciais comprometidas

Utilizam logins e senhas vazadas de ataques anteriores para tentar acessar sistemas empresariais. Muitas dessas credenciais são vendidas na dark web e podem ser usadas para acesso remoto a redes corporativas.

Força bruta

Utiliza listas de senhas comuns e algoritmos que testam milhares de combinações até encontrar a correta. Esse ataque pode ser mitigado com autenticação multifator, políticas de senha seguras e monitoramento de tentativas de login suspeitas.

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

Infecção silenciosa
Hackers acessaram a rede seis meses antes do ataque, explorando uma vulnerabilidade não corrigida e roubando 5 GB de dados.

Sequestro dos sistemas
Em janeiro de 2020, um ransomware criptografou todos os arquivos da empresa, paralisando suas operações.

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.

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

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

BOAS PRÁTICAS
CONTRA ATAQUES DE RANSOMWARE

Tenha uma visão completa do ambiente de rede

Busque uma solução que ajude a identificar cada aplicação e ativo em execução no seu ambiente de TI. Isso permite mapear rapidamente dispositivos, backups e vulnerabilidades que podem ser exploradas por ransomware

Implemente uma solução que diminua o risco de ataques

Escolha uma ferramenta capaz de detectar tentativas de movimentação lateral e atividades suspeitas na rede. A estratégia de segurança por camadas é essencial para impedir que invasores comprometam sistemas críticos.

Mantenha os softwares atualizados

Corrija falhas exploradas por hackers mantendo aplicativos e sistemas operacionais sempre atualizados. Atualizações automáticas e políticas de segurança bem definidas reduzem significativamente o risco de infecção.

Autenticação multifator (MFA)

Adicione camadas extras de segurança para evitar acessos não autorizados. Contas administrativas e sistemas críticos devem exigir MFA para impedir invasões mesmo se senhas forem comprometidas.

BOAS PRÁTICAS
CONTRA ATAQUES DE RANSOMWARE

Faça backups offline e isole-os

Realize backups automáticos e frequentes de dados essenciais. Utilize armazenamento offline e criptografado para evitar que o ransomware comprometa ou exclua as cópias de segurança.

Gestão de permissão

Aplique o conceito de Zero Trust, concedendo apenas o acesso estritamente necessário para cada usuário. Evite permissões excessivas, especialmente para funcionários com privilégios administrativos.

Use um antivírus moderno

Adote soluções que utilizam inteligência artificial e machine learning para detectar ameaças em tempo real. Além disso, implemente firewalls e sistemas de detecção e prevenção de intrusão (IDS/IPS) para bloquear ataques antes que eles cheguem à rede.

Desconfie de links e e-mails suspeitos

Seja cético com links enviados por e-mail, redes sociais ou aplicativos de mensagens, mesmo que venham de contatos conhecidos. Ataques de phishing são uma das principais portas de entrada para ransomware.

Treine continuamente seus funcionários

Funcionários mal treinados são o elo mais fraco da segurança cibernética. Realize simulações de ataques, treinamentos regulares e campanhas de conscientização para reduzir riscos humanos.

Use bloqueadores de anúncios e proteja a navegação

Evite que malwares sejam baixados automaticamente ao acessar sites suspeitos. Bloqueadores de anúncios podem impedir ataques via malvertising e downloads drive-by.

CONCLUSÃO

Mesmo com todas as medidas preventivas, um ataque de ransomware ainda pode acontecer. Então, o que fazer quando sua empresa sofre um ataque de ransomware?

Se sua empresa for vítima dessa ameaça, siga estes passos críticos para minimizar os danos e recuperar suas operações com segurança:

01 Isolamento e contenção

- Desconecte imediatamente os dispositivos infectados da rede para evitar a propagação do malware.
- Desative conexões Wi-Fi, Bluetooth e cabos de rede em dispositivos comprometidos.

02 Identificação e avaliação do ataque

- Identifique o tipo de ransomware e analise o escopo da infecção.
- Avalie se apenas arquivos específicos foram criptografados ou se sistemas críticos foram comprometidos.
- Consulte plataformas especializadas, como No More Ransom, para verificar se já existe uma ferramenta de descriptografia disponível para esse ransomware.

CONCLUSÃO

03 Notificação e acionamento de especialistas

- Informe imediatamente a equipe de TI e de segurança cibernética.
- Caso sua empresa tenha um seguro cibernético, comunique o provedor para verificar cobertura e suporte especializado.
- Considere envolver especialistas forenses em cibersegurança para identificar a origem do ataque e evitar novas infecções.

04 Avaliação do impacto e mitigação

- Verifique se backups recentes estão disponíveis e íntegros.
- Analise o tempo de recuperação estimado e a viabilidade de restaurar dados sem negociar com os criminosos.
- Se sua empresa opera em setores críticos, determine se há riscos regulatórios e comunique as autoridades competentes.

05 Tomada de decisão sobre o pagamento do resgate

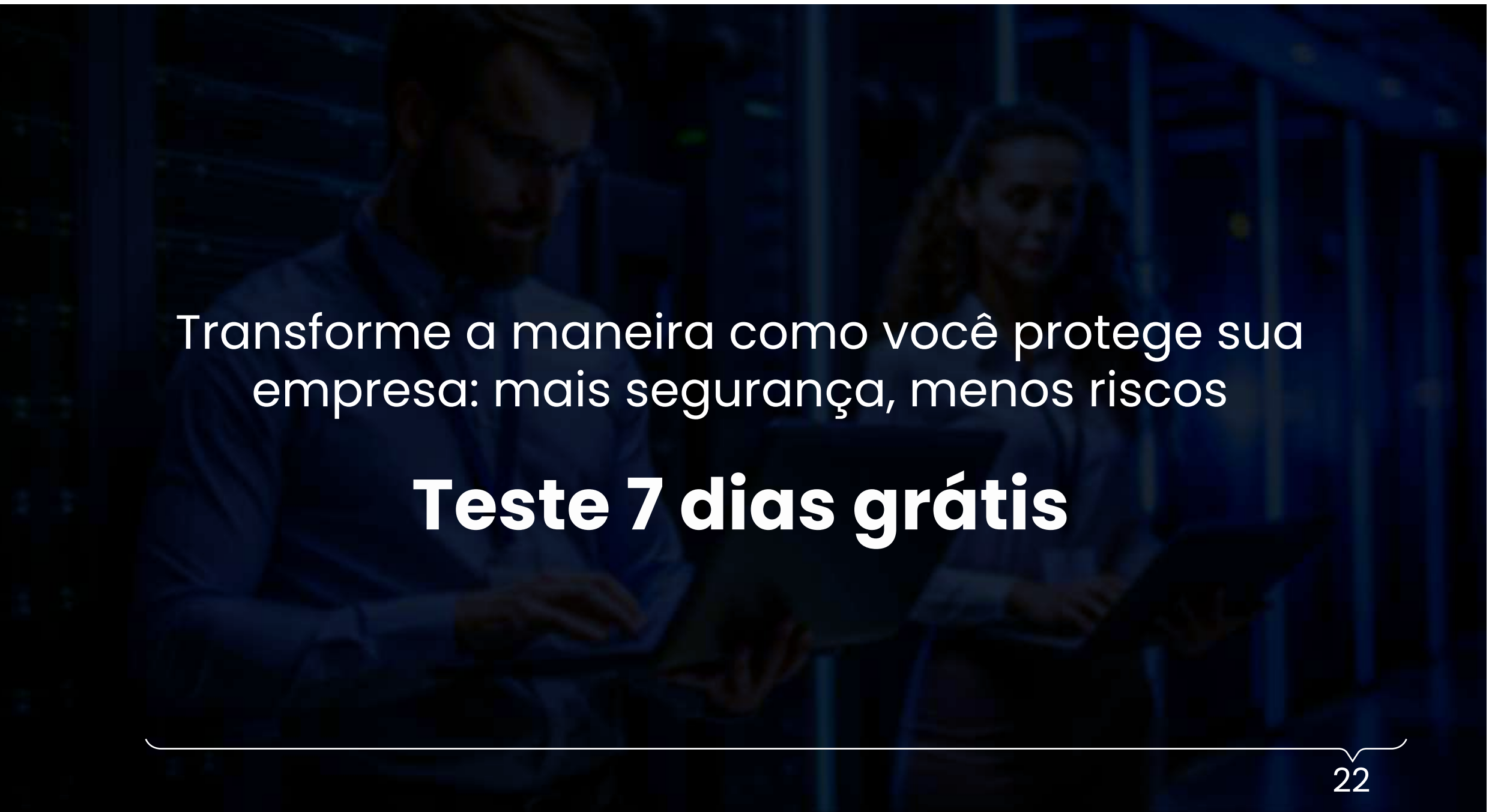
A recomendação padrão de órgãos de segurança cibernética é NÃO pagar o resgate, pois não há garantias de que os atacantes cumprirão a promessa de restaurar o acesso aos arquivos. Além disso, o pagamento pode incentivar novos ataques e financiar atividades criminosas.

No entanto, em cenários extremos, onde a continuidade do negócio está ameaçada e não há outra alternativa, a negociação pode ser considerada. Nesses casos, a recomendação é envolver um negociador especializado para avaliar as condições e minimizar riscos.

CONCLUSÃO

06 Recuperação e reforço da segurança

- Após restaurar os dados, fortaleça a segurança da empresa para evitar ataques futuros.
- Reforce backups, implemente autenticação multifator e eduque os colaboradores sobre segurança digital.
- Revise políticas de acesso, monitore atividades suspeitas e adote soluções avançadas de proteção contra ameaças.
- Nenhuma empresa está imune a ataques cibernéticos, mas com um plano de resposta estruturado e medidas preventivas robustas, é possível mitigar os impactos e reduzir significativamente os riscos.



COMO O MILVUS PODE 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.

• 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.

COMO O MILVUS PODE AJUDAR

- **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.

Com o suporte do Milvus, sua empresa fortalece a segurança digital e reduz vulnerabilidades. Com soluções inteligentes, você protege seus dados, minimiza riscos e garante um ambiente digital mais seguro, eficiente e resiliente contra ameaças como o ransomware.

Clique aqui para testar o Milvus por **7 dias grátis!**

Dúvidas?
Converse com o nosso time no **WhatsApp clicando aqui** e descubra como o **Milvus** pode ajudar sua empresa!

milvus.com.br