Checklist: Proteção contra ransomware na era do trabalho híbrido

kaspersky PREPARADOS PARA O FUTURO

O ransomware continua sendo uma ameaça crescente para todas as organizações. Estima-se que 15,45% de todos os usuários da internet sofreram pelo menos um ataque baseado em malware em 2021[1]. Não é nenhuma surpresa que a cibersegurança seja uma prioridade estratégica cada vez mais importante para as empresas.

O risco de infecção por ransomware aumentou nos últimos anos, particularmente devido o aumento do trabalho remoto, acelerado em resposta às medidas de combate à pandemia. Pesquisas sugerem que a corrida para criação de ambientes remotos fez com que muitas organizações reduzissem a fiscalização ou relaxassem seus protocolos de segurança habituais.

Quando se trata de ransomware, o grande foco é restaurar o acesso a dados criptografados o mais rápido possível. No entanto, cibercriminosos muitas vezes exfiltrarão arquivos para incrementar a chantagem, exigindo pagamentos adicionais para evitar que informações confidenciais sejam vazadas.

Poucas empresas implementaram segurança de rede (menos de 5%) ou ferramentas de monitoramento de usuários finais (menos de 6%) em 2021[2]. Sem monitoramento e segurança eficazes, o risco de se tornar uma vítima de ransomware aumenta potencialmente.

Os endpoints sempre foram um ponto fraco na segurança corporativa e muitas vezes as superfícies de ataque mais fáceis disponíveis para os hackers. Mas as práticas de trabalho remoto empurraram esses endpoints **para fora** do perímetro da rede, tornando ainda mais difícil gerenciar e garantir a segurança. A proliferação de endpoints aumenta as possibilidades de criminosos em busca de alvos potenciais, criando mais chances de sucesso.

Para evitar um surto significativo de ransomware, uma estratégia eficaz de ransomware deve ser articulada em vários níveis diferentes. À medida que o trabalho remoto se torna rotina nas operações, as organizações devem refinar e fortalecer suas proteções de endpoints, especialmente a forma como detectam e bloqueiam infecções por ransomware.

Este guia funciona como um checklist prático para ajudar você a avaliar seu nível de proteção contra ransomware na borda da rede e também onde você deve melhorar suas defesas, incluindo:

- **1. Detecção de ransomware em endpoints**
- **2. Configuração de Endpoints**
- **3. Provisões de backup**
- **4. Operações de descarregamento**
- **5. Treinamento dos usuários finais**
- **6. Planejamento de resposta a incidentes**

[1]Kaspersky Security Bulletin 2021. Estatísticas – Kaspersky –https://securelist.lat/kaspersky-security-bulletin-2018-statistics/88267/

[2]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

1. Detecção de ransomware em endpoints

Deter o ransomware antes que se prolifere é extremamente importante. Quanto mais rápido uma infecção for identificada e bloqueada, menos danos e interrupções irá causar.

Geralmente, sua organização pode contrair malware enviado diretamente aos colaboradores do servidor de correio, mas isso não os impede de serem enganados a baixar executáveis externos com uma mensagem de spear phishing bem elaborada.

Você pode melhorar seus recursos de detecção de ransomware bloqueando executáveis suspeitos em endpoints:

- **Implemente um kit de ferramentas robusto contra malware para identificar e remover executáveis suspeitos antes que possam criptografar arquivos confidenciais.**
- **Use recursos de aprendizagem de máquina de ferramentas de Detecção e Resposta de Terminais (EDR) para identificar e bloquear automaticamente a atividade suspeita do sistema.**
- **Considere adotar uma solução de detecção e resposta gerenciada (MDR) para automatizar e acelerar os esforços de atenuação de ransomware.**

A implementação dessas ferramentas ajudará a conter uma infecção, impedindo que se espalhe para níveis de armazenamento de arquivos e sistemas.

Vale a pena frisar que órgãos federais e agências governamentais estão endurecendo sua postura com relação às exigências de resposta a infecções por ransomware. Em 2019, o Centro de Queixas de Crimes na Internet (IC3) do FBI solicitou às empresas que não pagassem resgates[3].

Este conselho é reforçado pela Kaspersky: "Não paguem. Cada pagamento de resgate representa uma contribuição para financiar desenvolvimento de malware e um sinal para os cibercriminosos de que o esquema é lucrativo. Além disso, pode não resolver, você pode não receber nada em troca, mesmo se obedecer."[4]

O Escritório Federal Alemão de Segurança da Informação (BSI) oferece algumas orientações enfáticas: "A melhor proteção contra as demandas de resgate de cibercriminosos é medidas de segurança de TI consistentemente implementadas."[5]

Medidas de TI implementadas consistentemente significa manter as mesmas proteções de endpoints **no perímetro interno e externo da rede. Neste caso, isso quer dizer ferramentas anti-malware eficazes e confiáveis e recursos EDR inteligentes que podem detectar automaticamente atividades semelhantes** a ransomware.

2. Configuração de Endpoints

A configuração de endpoints também ajudará a reduzir o efeito potencial de uma infecção por ransomware. Para dispositivos corporativos:

- Use a lista de permissões do diretório de aplicação para garantir que os colaboradores só possam executar softwares autorizados. Com a restrição correta implementada, eles não podem instalar aplicativos, reduzindo a chance de executar executáveis infectados.
- Certifique-se de que as ferramentas de segurança de endpoints, e qualquer outro software instalado, esteja definida para ser atualizada automaticamente, para bloquear novas ameaças e fechar possíveis vulnerabilidades antes que exploradas[6].

As melhores práticas de cibersegurança sugerem a aplicação de atualizações de software no intervalo de 14 dias após o lançamento. Infelizmente, apenas 43% das empresas cumprem esse objetivo[7]. Relativamente fácil de implementar, esta é uma oportunidade perdida importante para evitar a propagação de ransomware.

[3]High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations – FBI Internet Crime Complaint Center –https://www.ic3.gov/Media/Y2019/PSA191002
[4]Five tips for protecting yourself from ransomware – Kaspersky –https://www.kaspersky.com.br/blog/ransomware-five-tips/41444/
[5]Ibid.
[6]Ransomware world in 2021: who, how and why – Kaspersky –https://securelist.lat/ransomware-world-in-2021/93642/
[7]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Endpoints do tipo BYOD representam um desafio extra, pois sua organização tem controle limitado sobre o dispositivo. Neste modelo operacional você tem algumas alternativas:

- Incentive os colaboradores a instalarem uma ferramenta anti-malware aprovada em todos os seus dispositivos. Fornecer este software gratuitamente é um incentivo, pois protegerá os dados pessoais do funcionário, bem como os ativos corporativos.
- Mantenha aplicativos corporativos e dados em uma sandbox para que sejam mantidos separados de aplicativos pessoais. Se um colaborador tiver contato com malware usando seus aplicativos pessoais, a sandbox fornece alguma medida de proteção contra propagação.

Em última instância, proteger dispositivos pessoais do usuário será um processo de compromisso, concordando em implementar medidas que sejam agradáveis à empresa e aos colaboradores. Nos casos em que isso não for possível, sua empresa precisará considerar fornecer métodos alternativos de acesso ou fornecer aos colaboradores dispositivos proprietários.

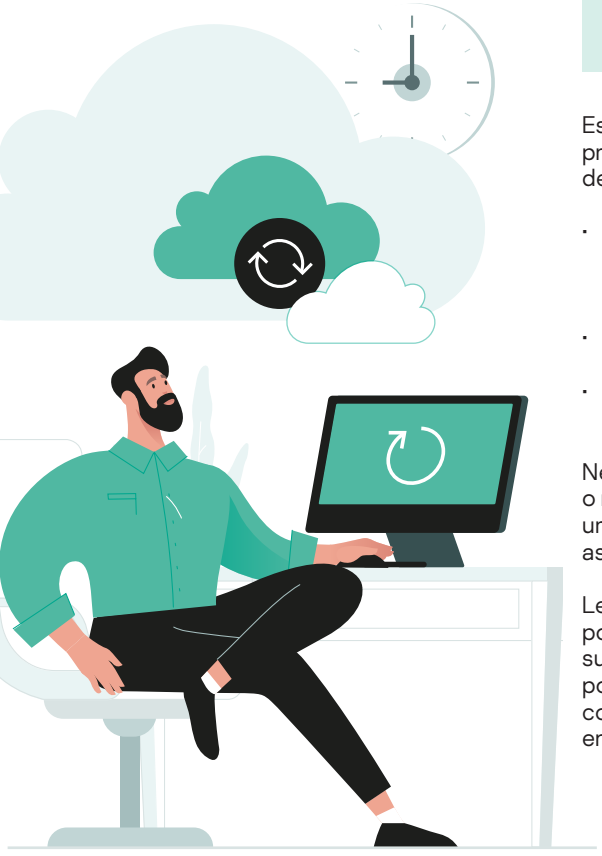
3. Provisões de backup

Depois que os arquivos são criptografados, você tem duas opções: pagar o resgate ou recuperação de cópias "limpas" dos arquivos no backup. Isso significa que é preciso ter uma rotina de backup robusta e confiável para seus dispositivos de endpoint também.

Em uma implementação ideal, os colaboradores não teriam a opção de armazenar dados corporativos localmente. Mas a realidade é que eles provavelmente salvarão documentos na unidade local, muitas vezes para a pasta do tipo Downloads ou Desktop.

Conforme sua empresa se prepara para um trabalho remoto mais seguro, você precisa considerar:

- **Qual é a probabilidade de que os dados corporativos sejam armazenados localmente?**
- **Quais dados são armazenados?**
- **Quais são os riscos se esses arquivos forem criptografados ou se tornarem inacessíveis?**
- **Como podemos fazer backup desses dados?**



Este é um desafio maior ainda fora do perímetro da rede. Como você soluciona esse problema será decidido pela sua arquitetura técnica e, até certo ponto, pelas competências de TI do usuário final. As opções a considerar incluem:

- Sincronizar dados em pastas selecionadas para armazenamento em nuvem ou outro serviço remoto, de preferência com backups imutáveis que não podem ser substituídos ou alterados.
- Fazer backup de uma unidade removível local.
- Contar com a funcionalidade incorporada ao sistema operacional para criar cópias de sombra automatizadas e pontos de reversão.

Nenhuma dessas soluções em potencial é ideal porque há sempre o risco de replicar o ransomware e arquivos criptografados no backup. No entanto, você deve identificar uma maneira de capturar dados armazenados localmente, especialmente para cumprir as obrigações de conformidade e proteção de dados.

Lembre-se: o backup de dados é sua última linha de defesa contra arquivos criptografados por ransomware. Também tenha em mente que o backup e a recuperação não protegerão sua empresa contra vazamentos de dados, ou o chamado doxxing. Os criminosos ainda podem exigir um resgate, ameaçando expor informações confidenciais. A única defesa contra esses ataques à **confidencialidade** é impedir que criminosos acessem seus endpoints.

4. Operações de descarregamento

Quanto mais dados e aplicativos mantidos em um dispositivo de endpoint, mais vulnerabilidades potenciais há para explorar. E mais atraente essa máquina se torna para os hackers. **Ao reduzir** a quantidade de aplicativos e dados mantidos localmente, menor será o impacto que uma infecção por ransomware terá.

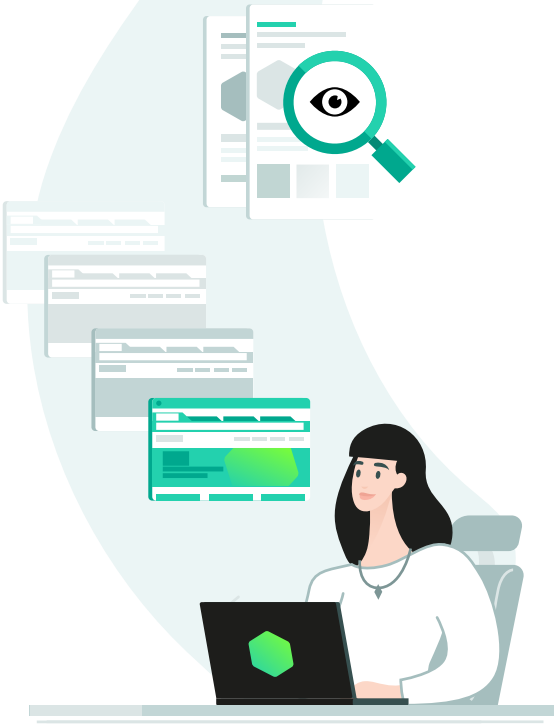
Os serviços na nuvem criaram uma maneira de descarregar aplicativos, minimizando a quantidade de dados armazenados no dispositivo local. As ferramentas de correio e produtividade agora podem ser executadas como aplicativos da web na nuvem, garantindo que quase nada seja transferido localmente. Particularmente serviços de correio, também oferecem proteção avançada contra malware para verificar, detectar e bloquear anexos suspeitos antes que seus usuários possam baixá-los.

A virtualização oferece outra possibilidade. Usando aplicativos e streaming de desktop, os usuários podem se conectar a uma sessão hospedada no data center corporativo ou na nuvem. A sessão hospedada é semelhante à área de trabalho para o usuário final, mas também todos os dados e processamentos são concluídos dentro do sistema virtualizado.

As sessões remotas de desktop (RDP) são consideradas o maior vetor de ataque para ransomware[8]. No entanto, quando configuradas corretamente, isso cria uma sandbox útil entre o dispositivo de endpoint e os sistemas corporativos, como evidenciado pelo uso extensivo de RDP dentro da rede corporativa.

É possível alcançar os mesmos benefícios para os colaboradores remotos, reforçando a segurança de endpoints, ou seja:

- **Impondo uma política de senhas robusta para evitar ataques de força bruta.**
- **Implementando autenticação multifatorial para evitar o sequestro de sessões.**
- **Usando conexões VPN para todo o tráfego entre servidores RDP e endpoints.**
- **Avaliando e reforçando as regras de firewall do perímetro de rede para evitar conexões não autorizadas.**
- **Usando ferramentas de segurança EDR para avaliar a atividade, identificar e bloquear automaticamente atividades suspeitas.**
- **Escolhendo portas de conexão RDP não padrão para evitar tentativas especulativas de hackeamento.**



Em última análise, a chave é evitar que hackers e malwares comprometam a conexão e a sessão RDP, o que resulta na proteção correta do endpoint do usuário.

5. Treinamento dos usuários finais

Os colaboradores são os ativos mais valiosos de qualquer empresa e desempenham um papel importante na prevenção da disseminação de ransomware, se souberem como agir. Todos os colaboradores, não apenas os que trabalham remotamente, devem receber treinamento regular para que estejam equipados para identificar potenciais ataques de cibersegurança, e qual o próximo passo. Diariamente, 2% dos colaboradores clicarão em um link[de phishing][9]. Estima-se números semelhantes em relação ao ransomware.

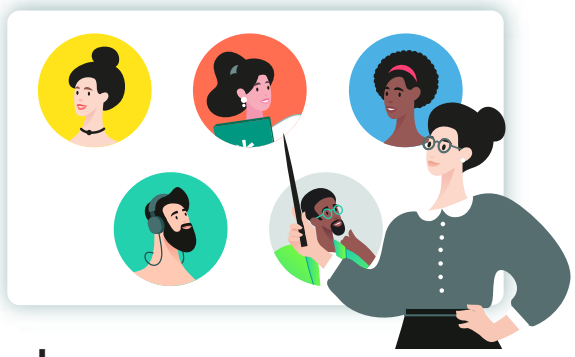
O treinamento precisa ser interativo, prático e periódico, já que as ameaças à cibersegurança estão em constante evolução. Uma apresentação única sobre a identificação de e-mails de phishing e executáveis suspeitos irá ficar desatualizada (e esquecida) rapidamente. Aqui estão alguns fatores a considerar ao elaborar um plano de treinamento de cibersegurança para os colaboradores remotos.

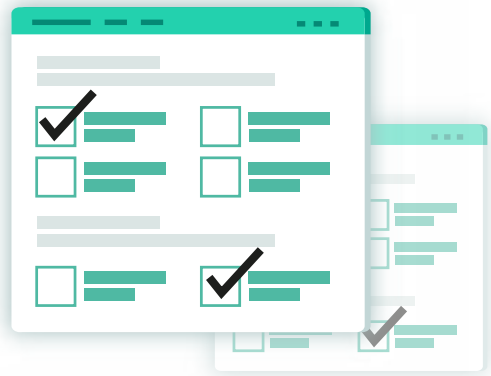
[8]How to secure RDP from ransomware attackers – Emsisoft –https://blog.emsisoft.com/en/36601/how-to-secure-rdp-from-ransomware-attackers/

[9]Mobile Security Index 2020 Report – Verizon – https://www.verizon.com/business/en-gb/resources/reports/mobile-security-index/2020/mobile-threat-landscape/user-threats/

Adapte o treinamento

Os ataques de ransomware mais eficazes são cuidadosamente direcionados a pessoas e funções específicas. Por isso, faz sentido, adaptar o treinamento da mesma forma. Finanças, marketing, RH e executivos enfrentarão ataques ligeiramente diferentes. Treiná-los em sua própria "linguagem" sobre as ameaças que eles provavelmente enfrentarão será de maior valor para eles e será mais eficaz para a empresa também.



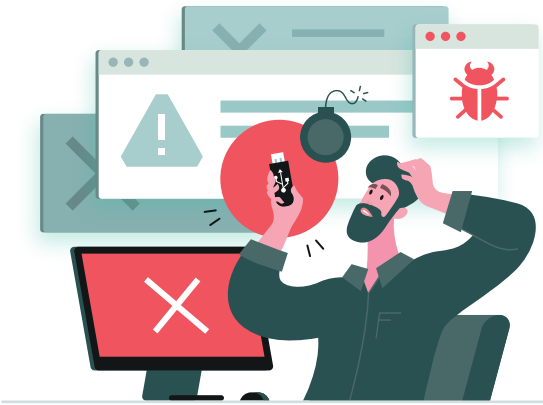


Teste seus colaboradores

O conhecimento é de pouco valor se não for colocado em ação, especialmente quando muita coisa está em jogo. Rotina e testes periódicos garantem que seus colaboradores possam colocar em prática o aprendizado, quando necessário. Avaliações de rotina também destacarão lacunas de conhecimento ou oportunidades para melhorar ainda mais suas habilidades e a postura de segurança da empresa.

Vá além do phishing

Phishing e anexos maliciosos são a fonte potencial mais óbvia de infecção por ransomware. No entanto, existem outros fatores que seus usuários finais precisam conhecer. Unidades removíveis infectadas, sites maliciosos e contaminação cruzada entre atividades profissionais e pessoais podem introduzir malware no endpoint e na rede corporativa mais ampla. Você deve garantir que os colaboradores sejam treinados para estar cientes desses problemas potenciais também.

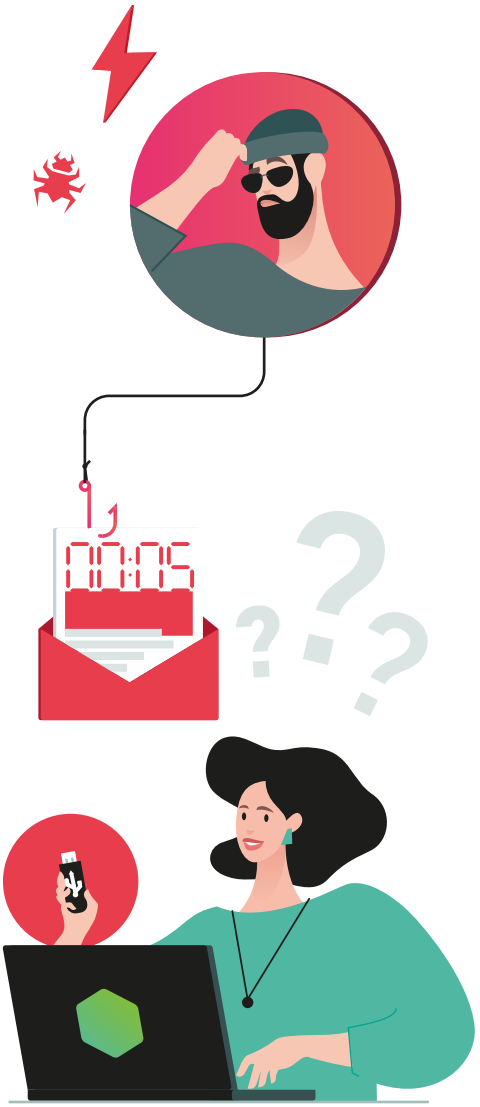


Torne o aprendizado divertido (e/ou interessante)

A cibersegurança pode ser um assunto chato, especialmente se não for a atividade principal da pessoa. É muito pouco provável que seus usuários finais leiam (ou entendam) sumários semanais do Sistema Nacional de Conscientização Cibernética dos EUA, por exemplo. O uso da gamificação ajudará a aumentar o interesse e o engajamento, especialmente à medida que os conceitos ensinados tornam-se mais complexos. Estabelecer metas e desafios, incentivar a competição e tornar o processo divertido incentivará os colaboradores a se manterem conectados e a continuarem melhorando seus conhecimentos e habilidades.

Investir nos usuários finais é um passo importante para fortalecer a defesa de endpoints. De fato, minimizar o erro humano é talvez a forma mais eficaz de prevenção de ransomware. Isso também ajudará seus colaboradores a desempenhar um papel eficaz nas fases iniciais de uma infecção por ransomware, ajudando a minimizar a propagação e o impacto geral sobre os negócios.

6. Planejamento de resposta a incidentes



Surpreendentemente, 32% das empresas não têm um plano formal de resposta a incidentes de cibersegurança, como um surto de ransomware[10]. Essas organizações estão assumindo um alto risco injustificável porque todas irão se deparar com um incidente de malware em algum momento no futuro.

A construção de um plano de resposta a incidentes ajudará sua empresa a avaliar vulnerabilidades e tomar as medidas apropriadas para atenuá-las. O plano também ajudará a acelerar sua resposta, o que é fundamental ao lidar com ransomware onde cada segundo conta.

Mesmo que cada organização seja única, todos os planos de recuperação de desastres (DR) de endpoints devem incluir:

- **Uma estratégia de comunicação.** Você precisa ter certeza de que as informações certas estarão nas mãos dos stakeholders no momento certo. Também é preciso ter certeza de que os colaboradores remotos são capazes de se conectar a especialistas que podem ajudá-los nas fases iniciais de uma infecção.
- **Um plano para lidar com ataques.** Decida como a gravidade de um ataque é determinada e como você responderá a isso. Você quer pagar o resgate ou tentar recuperar dados do backup?
- **Documentação acessível.** Há uma grande probabilidade de que uma infecção de endpoint impedirá os colaboradores de acessarem guias de ação ou instruções contra ransomware. Você deve garantir que haverá sempre uma maneira de obter essas informações, mesmo que os sistemas estejam desligados.
- **Orientação aos colaboradores.** Assim que um problema for detectado, você deve apontar um especialista que possa auxiliar o colaborador remoto. O técnico pode ajudar nos esforços iniciais de atenuação e recuperação e também coletar informações para incluir no relatório aos reguladores, se for o caso.
- **Vigilância reforçada.** Tão logo uma infecção por ransomware seja detectada em um endpoint remoto, a segurança de TI deve aumentar os níveis de monitoramento, gerando relatórios para avaliar se os sistemas centrais também foram comprometidos. A equipe pode então acionar o plano principal de recuperação de desastres, se necessário.

Com um plano de recuperação de desastres bem traçado, sua empresa está melhor posicionada para reduzir o impacto do malware, idealmente contendo a propagação muito antes de atingir sistemas e dados críticos.

[10]Cyber Security Breaches Survey 2021 – UK Department for Digital, Culture, Media & Sport – https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021/cyber-security-breaches-survey-2021

Conclusão

Os executivos de TI têm se preocupado com o trabalho remoto há anos e com razão. No entanto, eventos recentes mudaram o jeito de operar para sempre, e o trabalho remoto agora é um aspecto padrão dos negócios.

Ao mesmo tempo, o ransomware tornou-se uma ferramenta padrão no kit de todo cibercriminoso. Os ataques contra organizações são frequentes, eficazes e potencialmente devastadores. Com superfícies de ataque adicionais fornecidas por colaboradores remotos, é extremamente provável que todas as empresas sejam afetadas eventualmente.

Proteger endpoints contra ransomware deve, portanto, ser uma prioridade estratégica. Caso contrário, pode ser tarde demais para a sua empresa responder eficazmente quando o inevitável acontecer.

Os seis fatores descritos neste artigo ajudarão e sua empresa a se preparar melhor para quando o ransomware chegar. Abordar esses fatores melhorará imediatamente sua postura de segurança de endpoints:

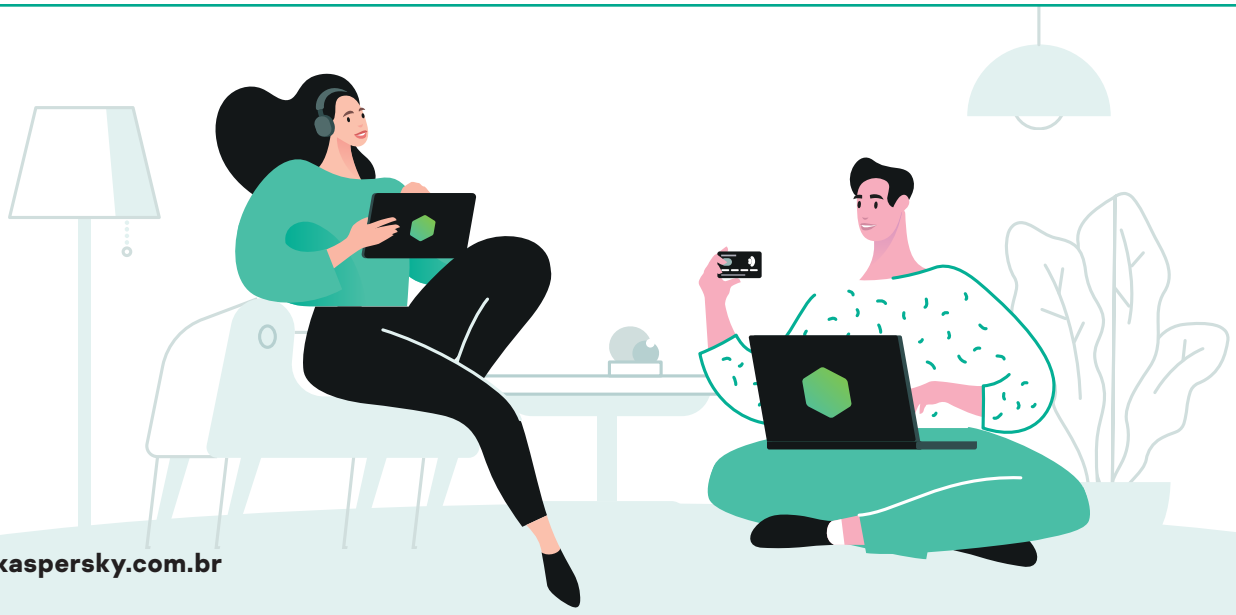
1. Detecção e remoção de malware
2. Configuração de dispositivos
3. Backup e recuperação de dados
4. Operações de descarregamento
5. Treinamento
6. Planejamento de D&R

Se quiser saber mais sobre como proteger o trabalhadores remoto e toda a sua organização contra ransomware, a Kaspersky pode ajudar. Com o Kaspersky Optimum Security habilitado para nuvem, você pode atualizar a proteção contra ameaças novas, desconhecidas e evasivas por meio de detecção e resposta eficazes de ameaças e monitoramento de segurança ininterrupto, sem custos ou complexidades limitantes. Mais visibilidade. Mais poder. Mais controle.

Saiba mais em go.kaspersky.com/pt_br_optimum

Leitura recomendada:

The story of the year: ransomware in the headlines
Como saber o nível de proteção de endpoints de que você precisa?
Guia do comprador de soluções EDR
Impulsione a cibersegurança para equipes de trabalho remoto blindando seu sistema



www.kaspersky.com.br

kaspersky PREPARADOS PARA O FUTURO