CYBER READINESS
INSTITUTE

CYBERREADINESSINSTITUTE.ORG

Manual de ransomware

Como se preparar, responder e recuperar de um ataque de ransomware

Até 2021
“a cada 11 segundos”
uma nova empresa será vítima de ransomware,
de acordo com o pesquisador de mercado Cybersecurity Ventures.[1]

Manual de ransomware

Pagar ou não pagar? Esta pergunta é frequentemente a primeira que muitas empresas consideram depois de serem alvo de um ataque de ransomware.

Infelizmente, a escolha não é simples. Muitas empresas simplesmente não sabem como se proteger contra ransomware. Este guia tem como objetivo fornecer um roteiro para que as empresas (por exemplo, pequenas e médias empresas, governos estaduais e locais) se protejam contra essa ameaça crescente.

[1] umbrella.cisco.com/blog/2019/12/17/ransomware-defense-for-dummies-2nd-edition

Todas as empresas correm o risco de ver os seus dados valiosos - sobre clientes, funcionários, operações - encriptados por um agente malicioso, de forma que a empresa perca o acesso a eles. **Um ataque de ransomware é conduzido por um agente malicioso para manter os dados de uma empresa como "reféns".** Agentes mal-intencionados podem obter acesso aos dados de uma empresa por vários meios, incluindo phishing e software sem patch. Os patches são lançados por empresas de software para vulnerabilidades encontradas nos seus programas; muitos utilizadores não conseguem descarregar os patches, o que significa que as vulnerabilidades podem ser exploradas.

Uma empresa que constrói uma cultura de prontidão cibernética pode ser resiliente contra um ataque de ransomware tomando ações preventivas (por exemplo, criando uma cópia de segurança de dados críticos e desenvolvendo e testando um plano de resposta a incidentes de ransomware. Uma empresa deve focar-se em três passos: **Preparar, Responder e Recuperar.**

PASSO 1

Preparar

PASSO 2

Responder

PASSO 3

Recuperar

Preparar

Certifique-se de que a sua empresa cria regularmente cópias de segurança dos seus dados; armazenar dados na nuvem é algo comum para cópias de segurança. Se os seus funcionários guardam informações comerciais importantes nos seus próprios computadores, a sua empresa também deve fornecer instruções claras sobre como fazer backup dos seus dados regularmente. Os principais elementos de proteção contra ransomware incluem:

- Priorize os dados que são mais críticos para a sua empresa e crie cópias de segurança dos mesmos. Certifique-se de que pode reinstalar a partir das cópias de segurança que geralmente estão na nuvem, e que as cópias de segurança são testadas com frequência.
- A deteção antecipada é importante, portanto, certifique-se de que a sua força de trabalho sabe relatar um possível incidente de ransomware ou comportamento incomum de rede.
- Contrate, se possível, um fornecedor que possa fornecer suporte de resposta se ocorrer um incidente. Estabeleça um contrato, pré-evento, para que tenha acesso ao fornecedor imediatamente.

Como os agentes mal-intencionados costumam usar phishing para infetar um sistema com ransomware, é crucial ter uma política de phishing. Realize testes de phishing de rotina para que os funcionários possam detetar um e-mail de phishing antes de clicar em qualquer ligação ou anexo perigoso e, quando possível, usar um programa de software anti-phishing.

Atualize o seu software com os patches de segurança mais recentes. Este passo preventivo tornará mais difícil para os agentes mal-intencionados comprometer o seu sistema.

Desenvolva uma política para toda a empresa em relação a ataques de ransomware. É muito mais fácil ter essas discussões quando a pressão da resposta não está a aumentar. Questões a serem consideradas: Que dados são mais críticos para a sua empresa? O seu seguro cobre ransomware? Aceita pagar um "resgate"? Em caso afirmativo, sabe como usar bitcoin e outras criptomoedas?

Discuta e concorde com uma política para toda a empresa em relação a ataques de ransomware. **É muito mais fácil ter essas discussões quando a pressão da resposta não está a aumentar.**

Os dados são **críticos para as suas operações?**

A sua empresa pré-determinou que é **normal pagar um "resgate"?**

O seu **seguro cobre ransomware?**

Responder

Se um funcionário ou a empresa for confrontado com um pedido de resgate, a sua empresa deve primeiro avaliar a legitimidade do pedido de resgate entrando em contacto com o seu gestor de TI. Se for legítimo, dois cenários possíveis são apresentados:

1 **A sua empresa tem cópias de segurança funcionais. Não precisa de se preocupar com o ransomware. Recupera os seus dados completamente e volta ao trabalho.**

2 **Os dados mantidos como "reféns" são necessários e não há cópias de segurança de trabalho.**

a. Verifique se os dados existem noutro lugar da empresa (por exemplo, arquivos de cache, e-mail) para que possa "gravar" os dados para substituir o que está a ser mantido como "refém"

b. Se não conseguir aceder aos dados noutro lugar, faça as seguintes perguntas:

- Os dados são críticos para as suas operações?
- A sua empresa pré-determinou que é normal pagar um resgate?
- O seu seguro cobre isso?

Recuperar

O fogo está extinto e é hora de voltar aos negócios como de costume. O âmbito do ataque de ransomware e a gravidade do seu impacto nas suas operações diárias determinarão quanto tempo e esforço serão necessários para a recuperação. Use o incidente como uma experiência de aprendizagem para reforçar a importância dos princípios de preparação cibernética, como correção e reconhecimento de phishing.

Garantir que o seu software está sempre atualizado com os patches de segurança mais recentes tornará mais difícil penetrar no seu sistema. Da mesma forma, aplicar o treino de phishing minimiza o erro humano e os pontos de entrada potenciais no seu sistema. Como acontece com qualquer violação de segurança, notifique todas as partes afetadas, redefina os IDs de utilizador e palavras-passe de todos os dispositivos comprometidos, atualize o software em todos os dispositivos e reinstale os seus dados de backups assim que a ameaça de ransomware for neutralizada.

É especialmente importante garantir que os patches são atualizados após o ataque. Se os dados foram restaurados, às vezes as vulnerabilidades que foram corrigidas, pré-ransomware, podem reaparecer.

O programa de preparação cibernética inclui instruções detalhadas e modelos para ajudá-lo a criar as suas próprias políticas e plano de resposta a incidentes para se preparar, responder e se recuperar de um ataque de ransomware. Inscreva-se gratuitamente em **BeCyberReady.com**.

Para ler sobre exemplos reais de como empresas e municípios responderam a um ataque de ransomware, visite **Cyber Readiness News.**

O programa de preparação cibernética inclui instruções detalhadas e modelos para ajudá-lo a criar as suas próprias políticas e plano de resposta a incidentes para **se preparar, responder e recuperar de um ataque de ransomware.**

Guia de decisão de ransomware

PREPARAR

Priorizou os seus dados e sistemas para saber o que é mais crítico para as suas operações de negócios?

- 👍 Tem um plano de resposta a incidentes que cubra o ransomware?
  - 👍 Atualmente tem cópias de segurança?
    - 👍 Testou as suas cópias de segurança no último mês?
      - 👍 Parabéns. **Está preparado.**
      - 👎 Teste a sua cópia de segurança para ter a certeza de que pode recuperar os seus dados - especialmente os mais críticos para as suas operações de negócios.
    - 👎 Crie uma cópia de segurança do seu sistema e de todos os dados.
  - 👎 Desenvolva um plano de resposta a incidentes que cubra o ransomware. Visite **BeCyberReady.com** para aceder a um modelo de plano de resposta a incidentes.
- 👎 Identifique o que é mais valioso. Visite **BeCyberReady.com** para aceder a uma lista de verificação de priorização.

Confia que não irá ser vítima de um ataque de ransomware. **Não está NADA preparado.**

⚠ Ocorre um incidente de ransomware ⚠

RESPONDER

Isole o incidente e remova o(s) computador(es) infetado(s) da rede. Em seguida, prossiga.

- 👍 Bom trabalho. **Vá diretamente para Recuperar!**
- 👎 Tem um suporte de TI para entrar em contacto?
  - 👍 Uma cópia de segurança pode ser criada por si ou pelo seu suporte de TI em tempo real?
  - 👎 Os dados mantidos como "reféns" são valiosos para o seu negócio?
    - 👍 Tem seguro cibernético?
      - 👍 A sua apólice cobre eventos de "resgate"?
        - 👍 Os seus dados não são recuperáveis... **decida se quer pagar ou não.**
        - 👎
      - 👎
    - 👎

RECUPERAR

Vá para a cópia de segurança em tempo real e limpe o malware.

Redefina IDs de utilizador e altere palavras-passe

Faça uma instalação limpa a partir da sua cópia de segurança

Atualize o seu software

Reinstale os dados seletivamente

Está de volta ao trabalho!! Inscreva-se no programa de prontidão cibernética gratuito em **BeCyberReady.com** para prevenir mais ataques de ransomware no futuro.