CINCO ETAPAS ESSENCIAIS

PARA MELHORAR A RESILIÊNCIA CIBERNÉTICA DA SUA ORGANIZAÇÃO

COHESITY

RESILÊNCIA EM QUALQUER LUGAR

INTRODUÇÃO

O aumento dos ataques de ransomware e seus impactos cada vez mais graves revelam uma verdade desconfortável. Mesmo com investimentos substanciais em prevenção, essas medidas sozinhas não são suficientes para combater as ameaças de hoje.

Gostemos ou não (e não gostamos), os ataques cibernéticos não vão desaparecer. E eles nunca permanecerão os mesmos, seja em frequência, gravidade ou escala.

Essa é a má notícia.

Agora as boas notícias. Há um método comprovado para melhorar a resiliência cibernética, e ele está sendo adotado por organizações como a sua para repensar a abordagem e desfrutar de melhores resultados.

Neste eBook, apresentamos este manual como uma progressão de cinco etapas para alcançar a resiliência cibernética. Ao tomar medidas concretas em todas as cinco etapas, você estará alinhado com as melhores práticas em resposta e recuperação cibernética. Você também verá benefícios substanciais em termos de segurança, economia de custos e risco reduzido.

ALGUMAS INFORMAÇÕES rÁPIDAS DE CONTEXTO

Apesar de maior conscientização sobre ameaças cibernéticas como ransomware, os ataques cibernéticos continuam a causar enormes danos operacionais, financeiros e à reputação. Na verdade, eles são a ameaça número um para as empresas em todo o mundo.

O custo financeiro é real:

US$ 540.000
perdidos para cada hora de inatividade[1]

Mais de US$ 1 bilhão
em pagamentos de ransomware anualmente[2]

The State of Ransomware 2024 da Sophos[3] inclui estatísticas igualmente preocupantes:

Das 59% das organizações pesquisadas que foram atingidas por ransomware no ano passado, **94% disseram que os invasores visaram seus backups,** e **57% dessas tentativas de comprometimento de backup foram bem-sucedidas.**

E mais:

- **70% dos ataques resultaram em criptografia de dados**
- **US$ 2 milhões em média foram exigidos em resgate**
- **34% das organizações levaram mais de um mês para se recuperar**

Chegou a hora de estratégias, capacidades e soluções novas e mais eficazes.

[1] Splunk, The Hidden Costs of Downtime: The $400B problem facing the Global 2000: https://www.splunk.com/en_us/pdfs/gated/ebooks/the-hidden-costs-of-downtime.pdf

[2] Chainalysis, Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline, 07/02/24: https://www.chainalysis.com/blog/ransomware-2024/

[3] Sophos, The State of Ransomware 2024: https://www.sophos.com/en-us/content/state-of-ransomware

DUAS RAZÕES PELAS QUAIS A RESILIÊNCIA CIBERNÉTICA PODE SER ESPECIALMENTE DESAFIADORA:

1. Recuperação cibernética não é como recuperação de desastres.

Mesmo que sua organização tenha processos sólidos de recuperação de desastres em vigor, você não pode confiar neles para se recuperar de ataques cibernéticos.

Em um desastre, seja um incêndio, inundação, falta de energia ou até mesmo uma configuração incorreta, você pode fazer rapidamente uma análise da causa raiz para descobrir o que deu errado. Em um ataque cibernético, centenas de coisas podem ter acontecido, o que exigirá investigação e correção minuciosas. Além disso, você tem um criminoso atuando ativamente para minar seus esforços de recuperação e pressionando você a pagar o resgate.

2. Até mesmo organizações e especialistas experientes podem subestimar o quanto um ataque de ransomware pode ser destrutivo.

Você pode presumir que sistemas confiáveis podem ajudá-lo a voltar a ficar on-line ou contar com dados e evidências para a saber o que aconteceu.

Mas em um ataque cibernético, os próprios sistemas nos quais você confia para investigar o incidente podem estar inativos ou mesmo terem sido burlados ou comprometidos. Quando dados bons se misturam com dados ruins, o caminho para a recuperação será mais longo e difícil. É por isso que vemos muitas organizações inteligentes ainda enfrentando dificuldades para executar uma recuperação rápida, limpa e confiante.

VAMOS VER AS **CINCO ETAPAS CRÍTICAS** PARA MELHORAR A RESILIÊNCIA CIBERNÉTICA

Pense nisso como um modelo prático em que cada passo que você der faz você avançar ao longo da progressão.

ETAPA UM

PROTEJA TODOS OS DADOS.

Pode parecer simples, mas muitas organizações ainda não dão esse primeiro passo crucial – e a disseminação de dados provavelmente é a culpada.

O crescimento orgânico de dados levou à fragmentação e silos, ampliando significativamente a superfície de ataque e deixando as organizações mais expostas do que nunca. Ao mesmo tempo, gerenciar e proteger dados em escala exerce uma pressão crescente sobre a eficiência operacional.

Essa combinação – mais dados em mais lugares, com menos capacidade de gerenciá-los com eficiência – criou as condições perfeitas para que os invasores causem estragos.

BENEFÍCIOS NOTÁVEIS DA ETAPA UM

- ☑ **Segurança aprimorada**
- ☑ **Risco reduzido**
- ☑ **Melhor conformidade e governança**
- ☑ **Custos mais baixos e melhor ROI**
- ☑ **Maior eficiência de TI**

PRINCIPAIS AÇÕES PARA IMPLEMENTAR A ETAPA UM

1. Adote uma plataforma de dados moderna que suporte mais de 1.000 fontes de dados, incluindo:

- Máquinas virtuais (VMs)
- Aplicativos SaaS
- Bancos de dados
- Ambientes NAS (dados não estruturados)

2. Garanta que sua plataforma seja executada em ambientes locais, na nuvem e em SaaS.

Como você tem dados dispersos em vários locais, sua plataforma deve ter modelos de implantação flexíveis unificados por uma interface do usuário e APIs comuns.

3. Simplifique as operações com uma interface do usuário intuitiva.

Quando sua interface do usuário é fácil de usar, você pode ter uma equipe relativamente pequena gerenciando um grande patrimônio – e gerenciando-o bem. Nossos clientes desfrutam de eficiências operacionais superiores com uma única interface do usuário e um conjunto de APIs para automatizar fluxos de trabalho em nossa plataforma.

4. Obtenha uma forte compressão de armazenamento.

Você vai querer usar uma plataforma com forte compactação de dados. Isso gerará economias substanciais ao executar em escala de petabytes. Temos um sistema de arquivos exclusivo que é o padrão do setor. Uma compactação realmente forte do armazenamento reduz o TCO.

ETAPA DOIS

GARANTA QUE OS DADOS SEJAM SEMPRE RECUPERÁVEIS.

Os invasores têm como alvo os backups. Eles sabem que, se puderem afetar essa última linha de defesa, você terá muito mais probabilidade de pagar o resgate, pois sua organização não terá nenhum outro recurso.

E embora possa ser bom supor que uma plataforma de dados moderna garanta backups recuperáveis prontos para uso, isso não é verdade.

Você precisa tomar várias medidas para dificultar o acesso dos invasores e para que sua organização recupere backups limpos, se isso acontecer.

BENEFÍCIOS NOTÁVEIS DA ETAPA DOIS

- ☑ **Recuperação mais rápida e segura**
- ☑ **Proteção mais forte contra ataques**
- ☑ **Prontidão para auditoria**
- ☑ **Alinhamento de confiança zero**

PRINCIPAIS AÇÕES PARA IMPLEMENTAR A ETAPA DOIS

1. **Fortaleça sua plataforma configurando recursos avançados, como:**

- Autenticação multifatorial (MFA)
- Imutabilidade (para que os dados não possam ser alterados ou excluídos)
- Controle de acesso baseado em função (RBAC)
- Separação de tarefas (dividindo tarefas críticas entre diferentes indivíduos)

2. **Implementar um cofre cibernético**

Com uma cópia isolada de seus dados mais importantes e a adesão à **regra de backup 3-2-1-1** (três cópias de dados, duas mídias diferentes, uma externa e uma imutável), você sempre terá uma cópia de seus dados disponível em caso de emergência.

Nós da Cohesity também fornecemos um sistema avançado de gerenciamento de chaves, para que ainda possamos garantir aos nossos clientes acesso aos seus dados em caso de um ataque.

Esse acesso garante que os backups sejam sempre recuperáveis.

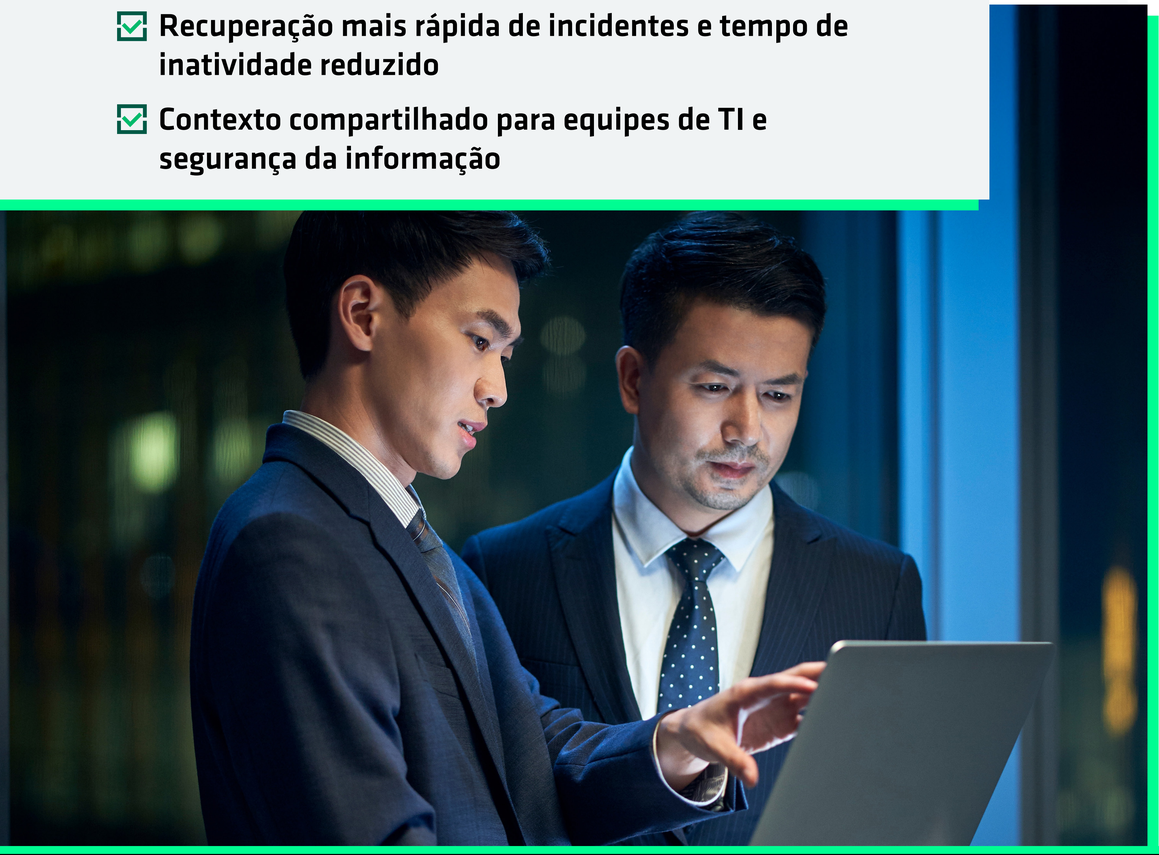
ETAPA TRÊS

DETECTE E INVESTIGUE AMEAÇAS.

Esta etapa está relacionada ao poder combinado das capacidades de varredura e caça a ameaças.

BENEFÍCIOS NOTÁVEIS DA ETAPA TRÊS

- ☑ **Detecção e mitigação precoces de ameaças**
- ☑ **Garantia de integridade de backup**
- ☑ **Recuperação mais rápida de incidentes e tempo de inatividade reduzido**
- ☑ **Contexto compartilhado para equipes de TI e segurança da informação**



PRINCIPAIS AÇÕES PARA IMPLEMENTAR A ETAPA TRÊS

1. Seja proativo verificando regularmente se há ameaças em seus backups. Pense nesta varredura proativa de **ameaças** como praticar a higiene de forma consistente. Isso ajudará você a:

- Eliminar todas as alterações o mais rápido possível
- Identificar malware ou outras vulnerabilidades

2. Inicie as capacidades de **caça a ameaças** ao buscar ameaças específicas. Nossos feeds de ameaças selecionados e as integrações com os fornecedores do ecossistema de segurança em nossa Data Security Alliance, incluindo CrowdStrike, Palo Alto Networks, Cisco e muito mais, significam que você obtém o benefício combinado da sua sabedoria coletiva com os dados que podemos trazer para esses sistemas.

Suas equipes de segurança da informação e TI também operarão com o mesmo conjunto de informações.

Como ajudamos os clientes a se recuperarem de ataques cibernéticos ao longo dos anos, as capacidades nativas de varredura e caça a ameaças devem fazer parte da sua plataforma de dados.

Por quê? Porque outros sistemas de segurança podem estar desativados ou off-line quando você está sob ataque.

ETAPA QUATRO

PRATIQUE A RESILIÊNCIA DE APLICAÇÃO.

Quando se trata de "prática", você está em boa forma se já tiver executado as etapas 1 a 3 acima. Você conseguiu que sua plataforma se levantasse, endurecesse e estendesse sua implantação com um cofre cibernético.

Você também teve uma boa experiência com varredura regular de ameaças e caça a ameaças. Muito bem!

Na etapa quatro, você aprimora sua preparação praticando seus processos de resposta e recuperação para infraestrutura, dados e aplicativos. Afinal, você não quer fazer isso pela primeira vez durante um ataque real quando seus sistemas foram derrubados e você está sob pressão.

Você pode estar pensando: "A recuperação de todo o sistema online é um processo demorado. Como posso testar regularmente e ainda fazer meu trabalho diário?"

BENEFÍCIOS NOTÁVEIS DA ETAPA QUATRO

- ☑ **Recuperação mais rápida e mais segura**
- ☑ **RTO aprimorado**
- ☑ **Menor risco de reinfecção**
- ☑ **Redução de interrupções e riscos financeiros**

É aqui que a orquestração entra em jogo.

Com a orquestração, você pode automatizar fluxos de trabalho de resposta e recuperação e começar a "ensaiar" como colocar seus sistemas de volta online após um ataque. Esses ensaios ajudarão você a ser bom na resposta e recuperação, e a orquestração pode ajudá-lo a ajustar essas práticas com menos esforço manual.

Um exemplo importante de automação em ação: Nossa solução de sala limpa permite que você crie um ambiente separado onde você pode realizar análise forense e mergulhar fundo em bits de dados infectados, entender o que aconteceu e, em seguida, erradicar o artefato de ataque para ter certeza de que seus sistemas estão seguros para recuperação. Essa abordagem oferece uma combinação única de velocidade, automação e perícia poderosa para ajudar os responsáveis pela resposta a incidentes a colaborar com as equipes de TI. O resultado: resposta e recuperação cibernética mais rápidas.

Nesta etapa, você também trabalhará com o Cohesity CERT (Cyber Event Response Team). Esses especialistas ajudarão você a responder e lidar com incidentes, desde ransomware sofisticado e violações de dados até ataques direcionados. Você nunca terá que responder sozinho.

PRINCIPAIS AÇÕES PARA IMPLEMENTAR A ETAPA QUATRO

1. Pratique com orquestração e treinamentos

- Automatize seus processos de resposta e recuperação
- Realize treinamentos para refinar seus planos de resposta, incluindo como você sequencia a recuperação de infraestrutura, dados e aplicativos

2. Use uma sala limpa

- Crie um ambiente separado e seguro para análise forense
- Identifique e erradique ameaças antes de restaurar infraestrutura, fontes de dados e aplicativos

3. Obtenha suporte especializado

- Entre em contato com o Cohesity CERT quando estiver sob ataque

ETAPA CINCO

OTIMIZE A POSTURA DE RISCO DOS DADOS.

Além dos criminosos de ransomware estarem ficando mais perigosos, você simplesmente tem mais dados para gerenciar – no local, SaaS, nuvem, borda – do que nunca. Todos estão sempre pensando: "o que eu tenho naquele bucket S3 sem segurança que ninguém sabe o que é ou está acompanhando?"

Além de buckets S3 não seguros, os riscos ocultos também podem incluir bancos de dados órfãos, credenciais expostas e muito mais.

Medidas proativas, como Gestão de Postura de Segurança de Dados (DSPM) e classificação de dados, podem ajudar a reduzir esses riscos.

BENEFÍCIOS NOTÁVEIS DA ETAPA CINCO

- ☑ **Visibilidade e classificação de dados aprimoradas**
- ☑ **Identificação e mitigação proativas de riscos**

PRINCIPAIS AÇÕES PARA IMPLEMENTAR A ETAPA CINCO

1. **Descubra onde estão os dados**

- Analise seu ambiente e avalie onde estão os dados e qual nível de proteção eles possuem. Toda a classe de ferramentas com DSPM torna isso possível.
- Entenda o que pode estar em sua propriedade de backup e garanta que ela esteja protegida da maneira certa com nossas integrações completas com alguns dos melhores fornecedores do setor, incluindo Cyera e BigID.

2. **Avalie o que pode ter sido afetado em uma violação ou o que pode ter acontecido em um caso de exfiltração de dados**

- Obtenha a cobertura certa de que você precisa e reduza seu risco com a classificação de dados integrada aos nossos produtos.
- Responda rapidamente quando ocorrer um incidente e os advogados perguntarem: Quais dados foram afetados? Qual o nível de sensibilidade deles? Qual é o nosso risco? Quantos clientes foram afetados? Que tipos de registros foram afetados?

CONCLUSÃO

Agora você entende as cinco etapas críticas para melhorar a resiliência cibernética da sua organização e tem as informações práticas necessárias para implementar essas etapas no seu ambiente.

Nós da Cohesity estamos posicionados de forma única para orientá-lo ao longo dessa progressão, para que você possa ter a maior resiliência cibernética possível.

Para obter mais informações sobre como se recuperar de ransomware com segurança e rapidez, recomendamos:

"COMO FORMULAR UMA RESPOSTA EM TEMPOS DE GUERRA A ATAQUES CIBERNÉTICOS DESTRUTIVOS"

COHESITY

RESILÊNCIA EM QUALQUER LUGAR

6100028-002-EN 6-2025