Enterprise Strategy Group | Getting to the bigger truth. ™

RELATÓRIO ESG

O papel do armazenamento no enfrentamento dos desafios para garantir a resiliência cibernética

Por Scott Sinclair, ESG Diretor de Prática e Analista Sênior
e Monya Keane, ESG Analista Sênior de Pesquisa

Janeiro 2022

Este documento da ESG foi encomendado pela IBM
e é distribuído sob licença da TechTarget, Inc.

Índice

Sumário executivo

O papel dos dados como ativo de negócios transformador continua a crescer. Graças ao aumento dos investimentos no desenvolvimento de aplicativos; práticas modernas de DevOps; e aumento das demandas de inteligência de negócios, análise e aprendizado de máquina, quase todas as empresas estão acelerando a criação e o uso de dados. Elas também estão dimensionando o número de locais que utilizam estes dados. Essa proliferação de dados combinada com a pressão crescente para acelerar as operações levou a um aumento na complexidade tanto da infraestrutura de TI quanto das operações de TI.

Tais fatores colocaram as organizações e suas infraestruturas sob um grande risco de sofrer ataques maliciosos, erros humanos e comportamento negligente. Infelizmente, as estratégias legadas não bastam para garantir adequadamente que as operações de negócios continuem durante e após esses tipos de incidentes. As empresas podem tentar integrar capacidades distintas em uma tentativa de prevenir ataques e outras violações, mas lacunas funcionais, má integração e complexidade de gerenciamento tornam o cumprimento de objetivos de segurança demorados e difíceis.

Mudar a mentalidade organizacional da prevenção à preparação contra incidentes — por exemplo, implementar soluções de armazenamento com resiliência cibernética incorporada — é fundamental para proteger ativos de dados críticos e ser capaz de responder e se recuperar rapidamente de ransomware e outros ataques cibernéticos.

Introdução

A TI enfrenta novos desafios. Quase metade (46%) dos entrevistados da pesquisa ESG dizem que a TI é mais complexa hoje do que era há dois anos. Esse aumento da complexidade pode ser resultado de iniciativas de transformação digital em andamento (citadas por 29%), volumes maiores de dados (35%), a rápida evolução do cenário de cibersegurança (37%) e/ou esforços para aderir a novas regulamentações de segurança e privacidade de dados (32%).

Simultaneamente, as organizações estão lutando para enfrentar uma escassez problemática de habilidades críticas de TI. De fato, 48% das organizações pesquisadas relatam não ter especialistas em segurança cibernética suficientes — foi a área de escassez mais citada. Além disso, essas organizações estão lidando com a dispersão de aplicativos, dispositivos e trabalhadores remotos/móveis, que estão aumentando o tamanho e o escopo do perímetro de segurança que a TI é encarregada de proteger.

Dada a complexidade da TI moderna, a proliferação de dados e as ameaças de ataque cibernético cada vez maiores, as equipes de TI muitas vezes se veem lutando para manter o ritmo. Tentar lidar com a complexidade apenas com pessoal interno é uma batalha perdida. O sucesso requer a modernização da própria infraestrutura subjacente. No entanto, ao fazê-lo, os tomadores de decisão de TI devem buscar por tecnologias que atendam não apenas às necessidades do aplicativo ou simplifiquem as operações. Alcançar o verdadeiro sucesso significa encontrar tecnologia que possa atingir esses objetivos e melhorar a postura de resiliência cibernética do ambiente de aplicativos também.

A crescente ameaça de ataques cibernéticos e ransomware

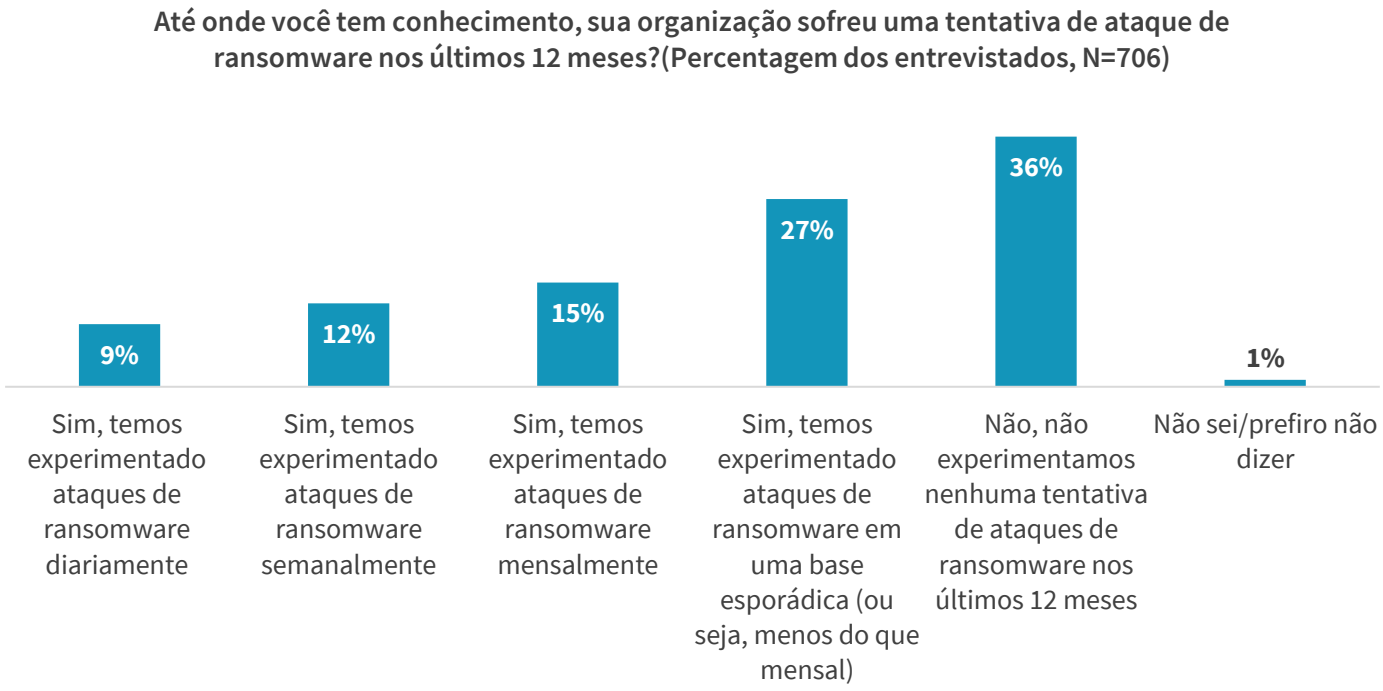
As organizações enfrentam ameaças crescentes de segurança cibernética, alimentadas provavelmente pelo aumento dos incentivos financeiros para cibercriminosos. Por exemplo, as queixas do público americano em 2020 ao Centro de Queixas de Crimes na Internet (IC3) do FBI aumentaram 69% em relação a 2019, com perdas reportadas superiores a US$ 4,1 bilhões. Além disso, nos últimos cinco anos, o IC3 reportou um total combinado de US$ 13,3 bilhões em perdas totais. A partir do quarto trimestre de 2020 nos EUA, o tempo médio de interrupção após ataques de ransomware a empresas foi de 21 dias. Claramente, o impacto negativo do ransomware nas operações de negócios é substancial.

Existe uma forte correlação entre a complexidade de TI e a vulnerabilidade de ataques cibernéticos. À medida que a TI se torna mais complexa, os ataques cibernéticos aumentarão em frequência e terão um custo mais alto.

Ransomware é um tipo de ameaça generalizada e que ataca o ativo mais valioso de uma empresa — seus dados. O IC3 identificou 2.474 incidentes de ransomware relatados em 2020, e o ESG descobriu que 63% das organizações pesquisadas sofreram ataques de ransomware no último ano. De fato, 9% experimentaram ataques de ransomware diariamente (ver Figura 1).[1]

A proteção contra ransomware requer uma estratégia tecnológica que se expanda além do domínio da segurança cibernética tradicional — ela deve aproveitar os avanços no armazenamento de dados e na proteção de dados também.

Figura 1. 69% dos entrevistados sofreram ataques de ransomware nos últimos 12 meses



Fonte: ESG, uma divisão de TechTarget, Inc.

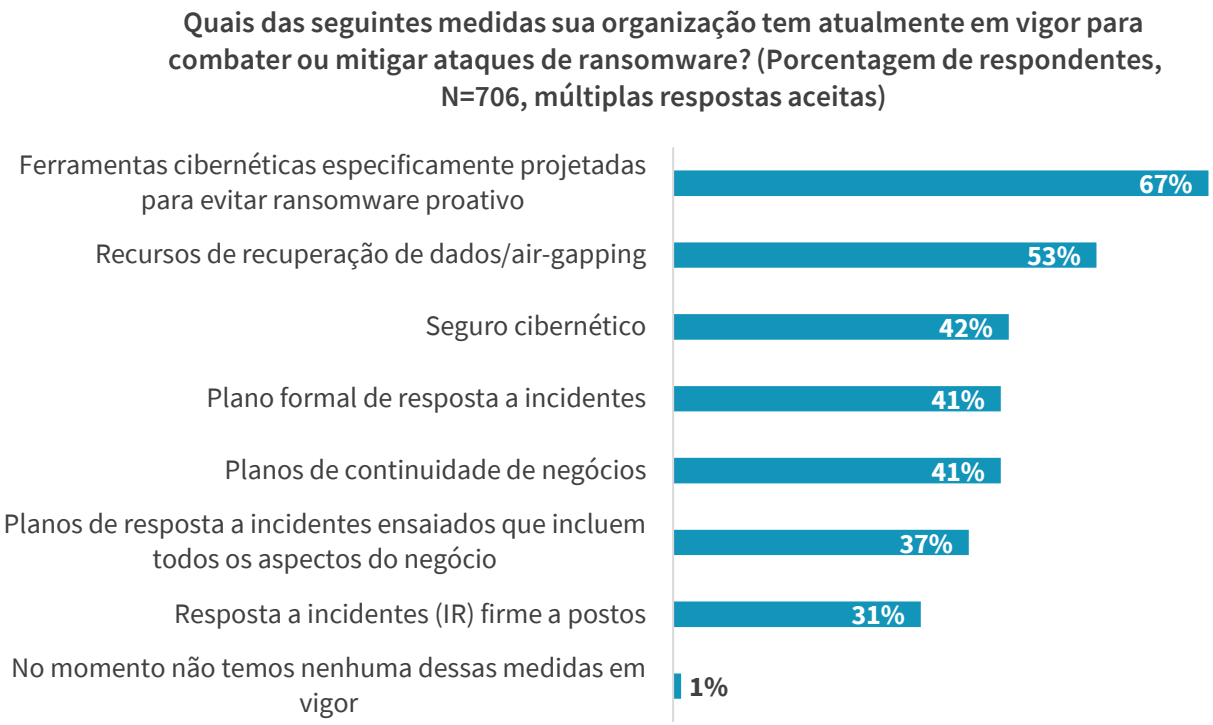
O papel do armazenamento de dados na resiliência cibernética

Os sistemas de armazenamento e os administradores de armazenamento desempenham ambos um grande papel na proteção contra ransomware. Quando o ESG perguntou aos tomadores de decisão de TI quais medidas suas organizações têm em vigor para combater ou mitigar ataques de ransomware, 67% dos entrevistados relataram usar ferramentas cibernéticas para evitar ransomware de forma proativa e 53% identificaram recursos de recuperação de dados, como o air-gapping (ver Figura 2). [2] Essas duas respostas comumente identificadas destacam a importância de não apenas implementar medidas para evitar um ataque, mas também investir em soluções para garantir que o negócio esteja preparado para se recuperar quando um ataque inevitavelmente ocorrer. É importante evitar simplesmente configurar políticas para combater ou mitigar ransomware e, em seguida, parar. Essa abordagem "parcial" cria uma falsa sensação de

[1] Fonte: ESG Resultados completos da pesquisa, *Pesquisa de Intenções de Gastos Tecnológicos 2022*, novembro de 2021.
[2] Ibid.

segurança porque, embora tenha sido feito um esforço para mitigar ataques, pouco ou nenhum esforço é feito para estabelecer um plano eficaz de recuperação de dados *antes* que seja necessário.

Figura 2. Medidas comuns adotadas para combater ou mitigar ransomware



Fonte: ESG, uma divisão de TechTarget, Inc.

É importante lembrar que combater um ataque é bem diferente da recuperação de dados tradicional. Normalmente, as organizações quase sempre querem recuperar seus dados usando a cópia mais recente. Mas com ransomware, a TI normalmente não sabe qual cópia "boa" usar; portanto, a recuperação é muitas vezes mais arriscada e pode levar muito mais tempo. Alguns ataques de ransomware não apenas visam dados, mas também visam a própria infraestrutura de backup. É por isso que os recursos avançados de armazenamento são fundamentais para uma recuperação eficaz de ransomware.

Embora a adoção das medidas identificadas na Figura 2 seja inteligente e precise ser ampliada, as organizações devem entender que nenhuma defesa única é 100% eficaz para a recuperação de ransomware. Embora seja importante considerar ferramentas especializadas em identificar e evitar ransomware, bem como recuperar dados, isso é apenas parte do esforço. Mesmo com a melhor defesa, é possível que um ataque passe. As organizações devem se preparar para essa eventualidade e avaliar como podem minimizar o impacto dos negócios, recuperando-se o mais rápido possível. Para minimizar a exposição geral de ransomware, as organizações devem procurar maneiras de acelerar a rapidez com que podem identificar ataques, quão rapidamente podem mitigar qualquer dano, e quão rápido podem se recuperar com uma cópia reconhecidamente confiável.

É aí que entram em jogo estratégias fortes de resiliência cibernética, levando em consideração *todos os componentes de manipulação de dados*, ou seja, hardware, software, pessoas e processos. Ao desenvolver uma postura de resiliência cibernética, as organizações devem mudar da questão "*Como nos protegemos*?" para "*Se somos atingidos por ransomware, quão rápido podemos nos recuperar*? *Quão rápido nosso negócio pode voltar ao normal*?"

Armazenamento de dados e proteção de dados: saiba onde focar para minimizar o risco de ransomware

A recuperação de um ataque de ransomware é uma forma de recuperação de desastres, mas os efeitos do ransomware são bem diferentes dos de um incêndio ou de uma inundação. Afinal, você geralmente pode dizer quando um incêndio é totalmente extinto. Ransomware é mais como uma faísca escondida dentro de uma parede que pode potencialmente reacender a qualquer momento. Os administradores de armazenamento precisam se concentrar em certas áreas para ajudar a reduzir os riscos associados ao ransomware. Como a velocidade é essencial, eles devem determinar a rapidez com que sua organização pode:

- Identificar um risco.
- Quantificar o tamanho do estrago que foi feito.
- Mitigar os danos identificando uma cópia confiável, recuperando-se usando essa cópia confiável e, finalmente, restaurando as operações.

Adotar uma abordagem "isso não vai acontecer conosco" é arriscado, na melhor das hipóteses. As organizações devem ser proativas e colocar em prática uma solução eficaz de armazenamento e proteção de dados — antes que realmente precisem.

Mudança da cibersegurança para a resiliência cibernética com a IBM

Com sua vasta experiência em cibersegurança e gerenciamento de riscos, a IBM é uma líder reconhecida em resiliência cibernética e oferece um conjunto abrangente de soluções avançadas de armazenamento e proteção de dados, incluindo:

1. IBM FlashSystem, IBM Cloud Object Storage e IBM Spectrum Scale, soluções de armazenamento primárias que vêm com recursos de imutabilidade de dados e criptografia.

1. IBM Tape Storage, que também suporta imutabilidade de dados e criptografia, e fornece proteção através de air-gapping.

- IBM Spectrum Copy Data Management software que gerencia e protege cópias de dados.

1. IBM Spectrum Protect Suite para proteção adicional. O armazenamento definido pelo software Spectrum Protect pode gravar dados em flash, disco, armazenamento de objetos e fita física ou virtual. Em seguida, detecta a atividade de malware e ransomware, identificando desvios grandes nos padrões normais de acesso.

- Radar and Storage Insights, soluções que ajudam a acelerar a detecção de ameaças potenciais usando recursos aprimorados por IA.

Cyber Resiliência com IBM Cyber Vault

É difícil enfatizar demais o papel do armazenamento na proteção contra ransomware. O software de armazenamento está vendo as alterações feitas nos dados primários, e porque está vendo essas mudanças, está em uma ótima posição para identificar quando um ataque está começando. É a tecnologia que está pegando e protegendo cópias secundárias, também — o que torna o armazenamento criticamente importante para ajudar na recuperação. Com esses fatos em

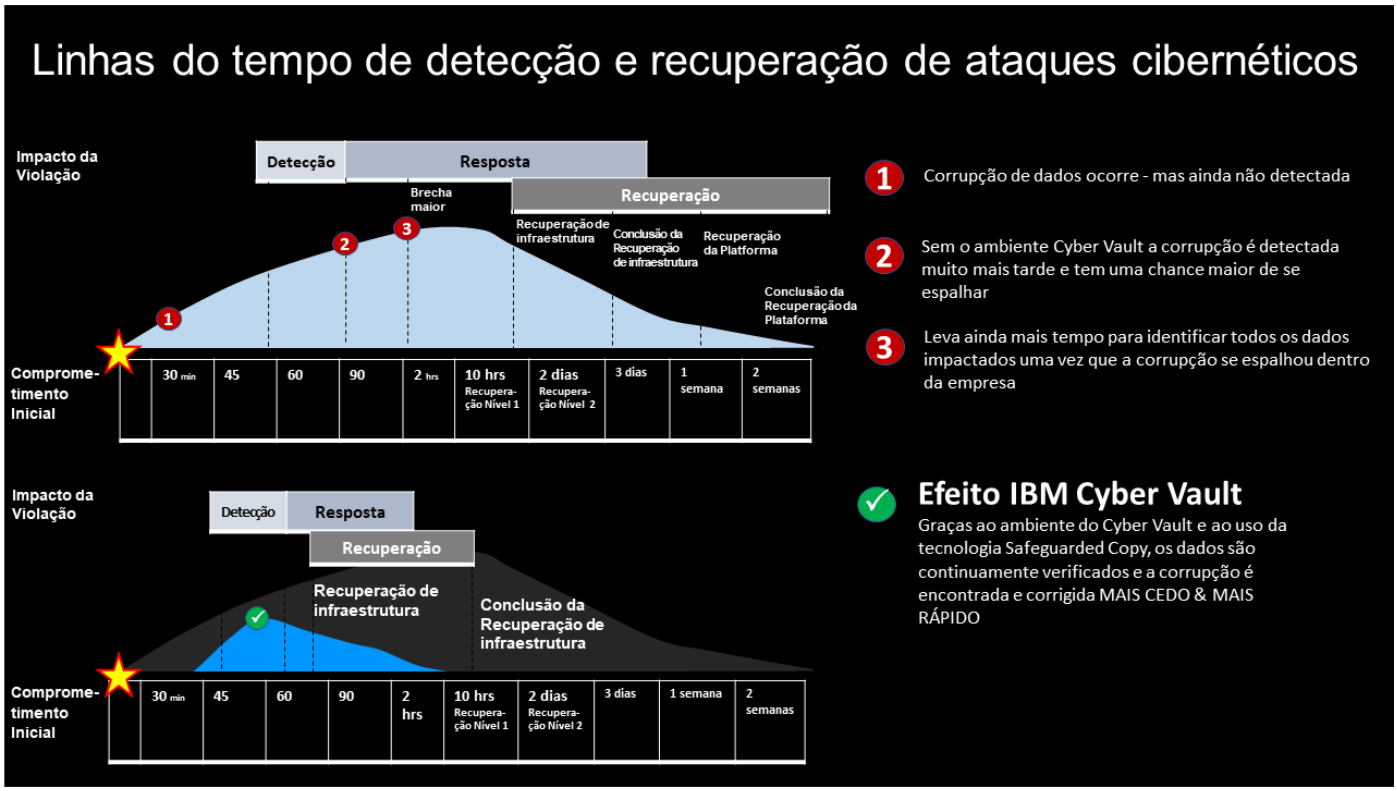
mente, talvez uma das ferramentas mais úteis de todas na caixa de ferramentas de resiliência cibernética da IBM seja o IBM Cyber Vault.

O IBM Cyber Vault é uma metodologia de segurança para recuperação rápida de um ataque cibernético. Ele é construído em cima do IBM Safeguarded Copy, uma tecnologia para criar instantâneos isolados e imutáveis regularmente. O Cyber Vault analisa esses instantâneos em busca de alterações potencialmente maliciosas, o que pode indicar a presença de ransomware. O IBM Cyber Vault também se integra com o IBM QRadar e o IBM Storage Insights para detecção ainda mais rápida. Sua validação de cópias imutáveis permite que os administradores identifiquem rapidamente uma boa cópia, testem e restaurem a partir dela.

Em termos de aumentar a velocidade em particular, o IBM Cyber Vault ajuda os administradores de armazenamento a acelerar:

- Identificação — A integração do QRadar e do Storage Insights oferece detecção e monitoramento aprimorados.
- Mitigação e quantificação de danos — Este é um processo automatizado. A detecção automática precoce de ataques obviamente permite uma recuperação mais rápida deles.
- Identificação de uma cópia confiável — A automação de cópias imutáveis de dados ocorre se uma ameaça for detectada.
- Restauração das operações — Uma recuperação rápida é possível em poucas horas, em vez de dias ou semanas (ver Figura 3).

Figura 3. Como o IBM Cyber Vault acelera a recuperação cibernética



Fonte: IBM

A Verdade Maior

As infraestruturas de TI continuam a se tornar mais complexas, aumentando a oportunidade de erros humanos, falhas no sistema ou negligência. Simultaneamente, atores maliciosos — dentro e fora da organização — são implacáveis em seus esforços para procurar e explorar elos fracos.

Sem dúvida, incidentes de segurança acontecerão. Esse fato deveria compelir uma mudança na mentalidade organizacional de reativa para proativa — de tentar fervorosamente impedir um ataque para se preparar e responder a falhas de segurança *quando* elas acontecem. Esta é a transformação que as organizações devem empreender à medida que viajam da cibersegurança à resiliência cibernética.

Várias organizações estão modelando suas estratégias de resiliência cibernética após a orientação fornecida pelo NIST Cybersecurity Framework, que recomenda que as organizações identifiquem recursos críticos, protejam esses recursos, detectem falhas e violações e planejem resposta e recuperação de incidentes cibernéticos. As principais organizações estão prestando atenção especial aos recursos de infraestrutura de TI que podem melhorar sua resiliência cibernética através de recursos como detecção de dados, gerenciamento de cópias, criptografia, controle de acesso e armazenamento imutável, mantendo várias opções de recuperação de dados.

Para os líderes de TI e de negócios, a resiliência cibernética é sobre tomar as decisões certas de tecnologia e as decisões certas de negócios— com o objetivo de manter o negócio operacional.

Enterprise Strategy Group é uma empresa integrada de análise, pesquisa e estratégia de tecnologia que fornece inteligência de mercado, insights acionáveis e serviços de conteúdo de mercado para a comunidade global de TI.

www.esg-global.com contact@esg-global.com 508.482.0188