Mainline® INFORMATION SYSTEMS

Construindo uma proteção de dados resiliente e segura

Dicas de armazenamento

Sumário

A atual ameaça aos negócios globais	2
Segurança cibernética e gerenciamento de riscos	4
Framework do NIST: uma base para o ciclo de vida de resiliência cibernética	5
O papel da infraestrutura de armazenamento	6
Soluções de infraestrutura de armazenamento	9
Alcançando o equilíbrio ideal de segurança	12

A atual ameaça aos negócios globais

Seja por erro humano, falhas no sistema ou atos criminosos maliciosos, as violações de dados estão entre as ameaças mais graves e mais caras para as empresas atualmente.

Um relatório recente do Ponemon Institute descobriu que **o custo médio mundial de uma violação de dados nos 12 meses anteriores era de US$ 3,86 milhões**. **Para as empresas brasileiras, o custo foi de R$ 5milhões em média**[1]. As organizações afetadas por uma violação também correm o risco de interromper suas operações comerciais normais, além de perder dados valiosos, clientes e reputação dentro de sua indústria.

Há também um impacto correspondente nas pessoas. **O Relatório de Riscos Globais de 2019 do Fórum Econômico Mundial (WEF) classificou os ciberataques como um dos principais riscos ao bem-estar humano**. 82% dos pesquisados pelo WEF disseram esperar que o risco do roubo de dados ou dinheiro pelos ataques cibernéticos aumente, enquanto 80% também viram um aumento no risco de interrupção das operações e infraestrutura.[2]

As áreas de TI precisam adotar uma abordagem sistemática da segurança, para enfrentar os novos desafios impostos pelas ameaças generalizadas à segurança.

Custo médio total de uma violação

Fonte: Ponemon Institute

A atual ameaça aos negócios globais

As empresas líderes estão adotando tecnologias inovadoras de armazenamento, como cópias protegidas. Também estão utilizando métodos existentes e altamente eficazes de *physical air gap*, uma medida de segurança de rede empregada em um ou mais computadores, para garantir que uma rede segura de computadores esteja fisicamente isolada de redes não seguras, visando impedir ameaças e atender às expectativas de negócios da organização. **A chave para executar essas abordagens está em um gerenciamento bem-sucedido de riscos**.

As áreas de TI precisam adotar uma abordagem sistemática da segurança, para enfrentar os desafios impostos pelas ameaças generalizadas.

Segurança cibernética e gerenciamento de riscos

Existem vários métodos disponíveis para as organizações se protegerem de interrupções ou ajudar a minimizar seus custos.

O Ponemon Institute sugere as quatro estratégias a seguir, para reduzir o custo de uma violação de dados[1]:

Criar uma equipe de resposta a incidentes

Empregar gerenciamento de continuidade de negócios

Usar criptografia em larga escala

Melhorar o treinamento dos funcionários

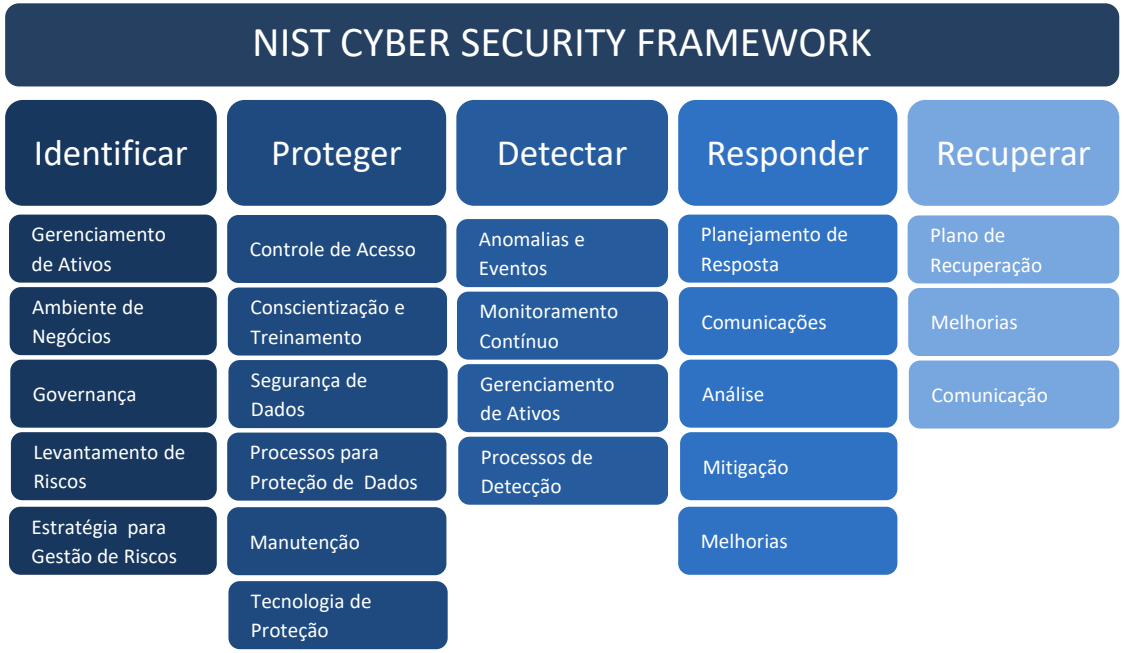
Para estabelecer e manter uma estratégia robusta de segurança cibernética, deve ser empregada uma **abordagem baseada em processos**, para entender quais dados e ativos do sistema você possui, qual é o valor deles e a quais riscos estão expostos.

A adoção de **princípios de gerenciamento de riscos** para identificar o estado atual e o estado desejado de segurança da sua organização permite considerar uma variedade de possíveis níveis de implementação. Esse passo é fundamental para avaliar e executar uma estratégia de resiliência cibernética e facilitará a definição de uma plataforma sólida de proteção.

Framework do NIST: uma base para o ciclo de vida de resiliência cibernética

Em 2018, o National Institute of Standards and Technology (NIST) publicou nos Estados Unidos o "Framework for Improving Critical Infrastructure Cybersecurity" (Bases para Melhorar a Segurança Cibernética da Infraestrutura Crítica). O documento apresenta três partes: Núcleo da Estrutura, Níveis de Implementação da Estrutura e Perfis da Estrutura.[3] No Núcleo da Estrutura, existe uma série de objetivos da segurança cibernética.

Trabalhando juntas, essas funções fornecem maior visibilidade ao gerenciamento dos riscos de segurança cibernética de uma organização. Com um entendimento mais claro, a organização pode se concentrar nas soluções mais apropriadas de armazenamento. Todas as organizações podem adotar essas etapas necessárias e factíveis, se ainda não tiverem feito:



Identificar: promover um entendimento organizacional dos riscos que as ameaças à cibersegurança representam para sistemas, pessoas, ativos, dados e recursos.

Proteger: garantir a entrega de serviços críticos com as salvaguardas apropriadas.

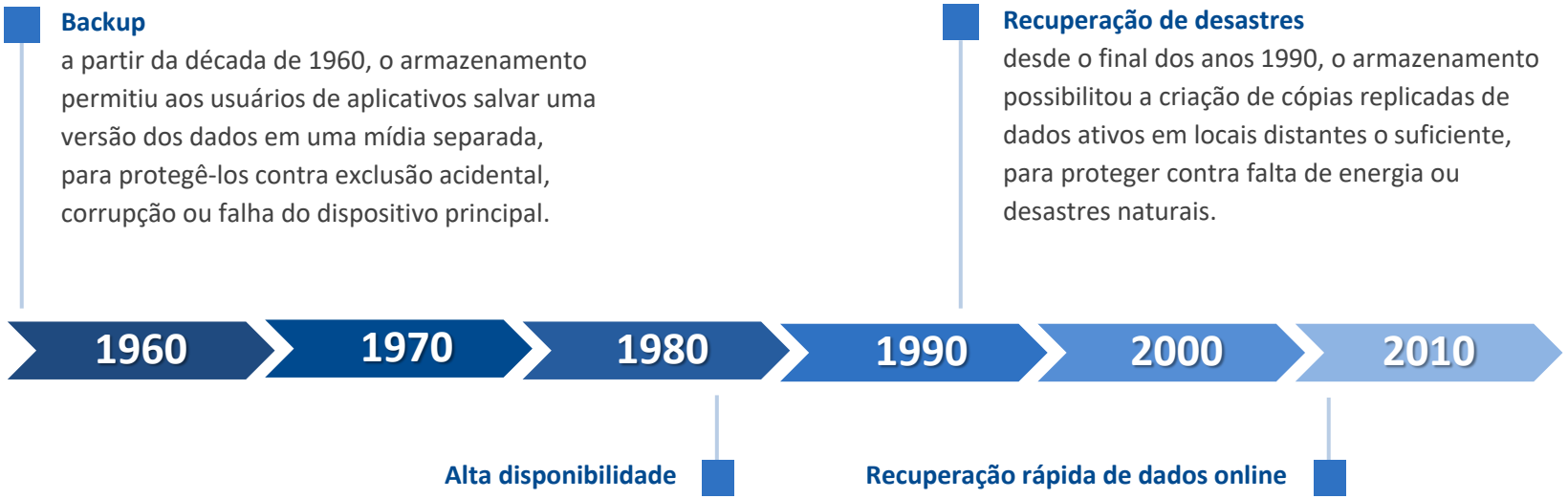
Detectar: identificar um evento de segurança cibernética na hora em que ele ocorre.

Responder: tomar medidas em relação a um incidente de segurança cibernética.

Recuperar: restaurar quaisquer recursos ou serviços prejudicados por um incidente de segurança cibernética.

O papel da infraestrutura de armazenamento

O armazenamento há muito tempo desempenha o papel de "guardião dos dados" nas operações corporativas. Além de fornecer espaço aonde os dados são alocados quando não estão na memória principal, tradicionalmente a camada de armazenamento dos sistemas fornece funções de proteção, que ajudam as organizações a se recuperarem de eventos não desejados. Com o tempo, o alcance dessas funções aumentou:



O papel da infraestrutura de armazenamento

Em cada um desses casos, a nova função foi introduzida nos sistemas de armazenamento, softwares de gerenciamento e processos operacionais, para abordar as especificidades de cada caso de risco.

Mudando das funções gerais de armazenamento para as relacionadas à resiliência cibernética, existem quatro recursos-chave, que atuam em blocos, arquivos, objetos, fitas, armazenamento definido por software e nuvem:

Isolamento é o grau de separação dos dados de captura instantânea ou de *backup* do restante da rede. O isolamento pode ser alcançado por meios lógicos utilizando cópias protegidas, armazenamento de objetos na nuvem ou através de isolamento físico.

Imutabilidade ou armazenamento inviolável impede que qualquer invasor, externo ou interno, altere ou exclua dados.

Performance é uma funcionalidade importante da estrutura de resiliência cibernética e tem relação com a rapidez que a sua organização pode se recuperar de um ataque cibernético. Embora a fita se destaque no isolamento e na imutabilidade dos dados de *backup*, uma recuperação por fita pode levar várias horas para ser efetivada.

Facilidade de reutilização ou facilidade de acesso aos dados de *backup* é uma função importante para testar os procedimentos de recuperação, validar *backups* e restaurar dados em um ambiente de *sandbox* e para encontrar um ponto de recuperação válido no caso de um incidente de *ransomware*.

A ameaça de corrupção de dados lógicos (Logical Data Corruption ou LDC) por meio de um ataque cibernético, especificamente um ataque de *ransomware* ou *wiper*, apresenta um novo conjunto de preocupações sobre proteção.

O papel da infraestrutura de armazenamento

Para alcançar o nível necessário de resiliência para o armazenamento, as empresas podem se valer de algumas das ferramentas existentes para *backup* e recuperação de desastres. Entretanto, novas funções de armazenamento também são necessárias para lidar com as novas ameaças.

É necessário um mecanismo que combine as funções de armazenamento e processos operacionais, para preservar as cópias de recuperação dos dados atuais, mesmo diante de um sofisticado ataque de *malware*. Uma vez que um ataque foi detectado e foi articulada uma resposta, essas cópias reservadas podem ser usadas para reiniciar os aplicativos e retomar o serviço normal.

É possível evitar que os dados sejam modificados ou excluídos devido a erros do usuário, destruição maliciosa, ataques de *malware* ou *ransomware* por meio de cópias imutáveis e pontuais dos dados de produção e controle duplo de segurança.

Três novos recursos são necessários para a criação de cópias preservadas:

Granularidade: as organizações devem poder criar várias cópias de proteção, para minimizar a perda de dados em caso de um incidente de corrupção.

Isolamento: as cópias de proteção devem ser isoladas dos dados de produção ativos, para que não possam ser corrompidas por um sistema *host* comprometido.

Imutabilidade: as cópias devem ser protegidas contra manipulação não autorizada[4].

No documento “Five Key Technologies for Enabling a Cyber-Resilience Framework”[3], a IDC acrescentou duas considerações:

Automação e orquestração.

Relatórios e garantias regulatórias.

Embora não sejam itens exclusivos de resiliência a ataques de corrupção de dados, esses dois tópicos são válidos para integrar uma lista de boas práticas.

Soluções de infraestrutura de armazenamento

Uma boa solução de armazenamento deve entregar um amplo espectro de recursos para desenvolver operações de TI que são resilientes diante de ataques cibernéticos ou interrupções acidentais. **Soluções abrangentes combinam funcionalidade de armazenamento, configuração de rede, controles administrativos e segurança física.**

Vamos dar uma olhada em algumas das principais soluções e tecnologias de resiliência cibernética disponíveis atualmente, incluindo *snapshots*, *backups* protegidos com mídia WORM (Write Once, Read Many), proteção de *air gap* por fita e armazenamento de objetos na nuvem.

Figura - O IBM® DS8880 é um sistema de armazenamento corporativo, projetado para incorporar à sua infraestrutura um armazenamento seguro de alto desempenho e alta capacidade, para ambientes de missão crítica exigentes.

Backup e recuperação tradicionais baseados em snapshots

Os *snapshots*, ou capturas instantâneas, se tornaram um dos métodos com melhor desempenho e menor custo para atender aos requisitos de *backup* tradicional. Cópias de dados somente para leitura, com eficiência na utilização de espaço, fornecem pontos de recuperação econômicos, que podem ser usados para restaurações rápidas de versões anteriores dos dados. O uso de *snapshots* para recuperar uma exclusão ou corrupção acidental se tornou uma prática generalizada.

Snapshots protegidos

Qual é a melhor maneira de proteger *snapshots*? Uma boa abordagem é replicar volumes de armazenamento do sistema de produção para um sistema de armazenamento secundário do mesmo tipo. *Snapshots* periódicos podem ser usados como cópias de recuperação na matriz secundária.

A função de replicação e captura instantânea deve ser automatizada por meio de software. O sistema de armazenamento que não é de produção não deve ser conectado diretamente a nenhum servidor de aplicativos e a única conexão de dados de armazenamento ativa deve ser a porta ou portas pelas quais as cópias de *backup* chegam.

Soluções de infraestrutura de armazenamento

No caso de um ataque de *malware* ou um teste de uma ação de recuperação, as cópias de dados armazenadas no sistema que não está em produção devem ser usadas como a fonte das cópias de recuperação, que podem ser movidas de volta ao sistema de armazenamento de produção.

O uso de um sistema de armazenamento que não seja de produção pode oferecer um *air gap* lógico entre a produção e as cópias protegidas. A separação física entre os sistemas é uma questão de estrutura de implementação. A proximidade, mesmo que seja no mesmo *data center*, oferece melhor desempenho e custos de rede mais baixos, e a solução de armazenamento que não é de produção pode ser incluída em um local diferente, usado para recuperação de desastres.

Backups protegidos por mídia WORM

Um sistema funcional de software de backup e arquivamento pode mover cópias completas de dados para um espaço de armazenamento gerenciado e manter versões de *backup*, armazenando os dados alterados. **Uma mídia WORM (Write Once, Read Many) pode ser útil para a proteção das cópias de recuperação.** Cartuchos de fita podem ser configurados como WORM e usados para gravar cópias de recuperação protegidas contra substituição pela unidade de fita.

Uma vez registradas em um cartucho WORM, nenhum tipo de *malware* nos servidores de aplicativos ou gerenciamento pode destruir a cópia de *backup*.

Diferentemente dos *snapshots* com economia de espaço, cópias completas gravadas em fita requerem tempo para mover os dados. As restaurações também são muito mais lentas do que as que podem ser alcançadas com os *snapshots*.

As estruturas devem ser personalizadas de acordo com as necessidades de cada empresa, mas pode ser desejável criar uma defesa completa com uma recuperação baseada em *snapshots,* adicionada a um *backup* que coloca dados em mídia *offline*.

Figura - Cartucho e unidade de fita.

Soluções de infraestrutura de armazenamento

Proteção robusta de isolamento físico por fita

Como descrevemos anteriormente, o termo "air gap" se refere ao isolamento físico ou virtual de sistemas ou redes, para evitar corrupção generalizada de dados causada por infecção de *malware*, falhas no sistema ou erro humano.

O conceito básico em torno de um *air gap* é colocar sistemas de armazenamento secundário periodicamente *online*, para incorporar as alterações mais recentes e depois levá-las novamente para a condição *offline*. As abordagens que usam funções de *snapshot* para criar cópias podem ser montadas rapidamente para recuperar aplicativos danificados.

No entanto, a proteção total dos dados copiados tem algumas limitações. Uma abordagem de proteção mais completa, que não fornece acesso da rede ou por software às cópias protegidas, pode ser implementada usando uma biblioteca de fitas.

A natureza "*offline* por definição" da fita oferece um verdadeiro isolamento físico e fornece uma das proteções mais seguras para enfrentar o cibercrime.

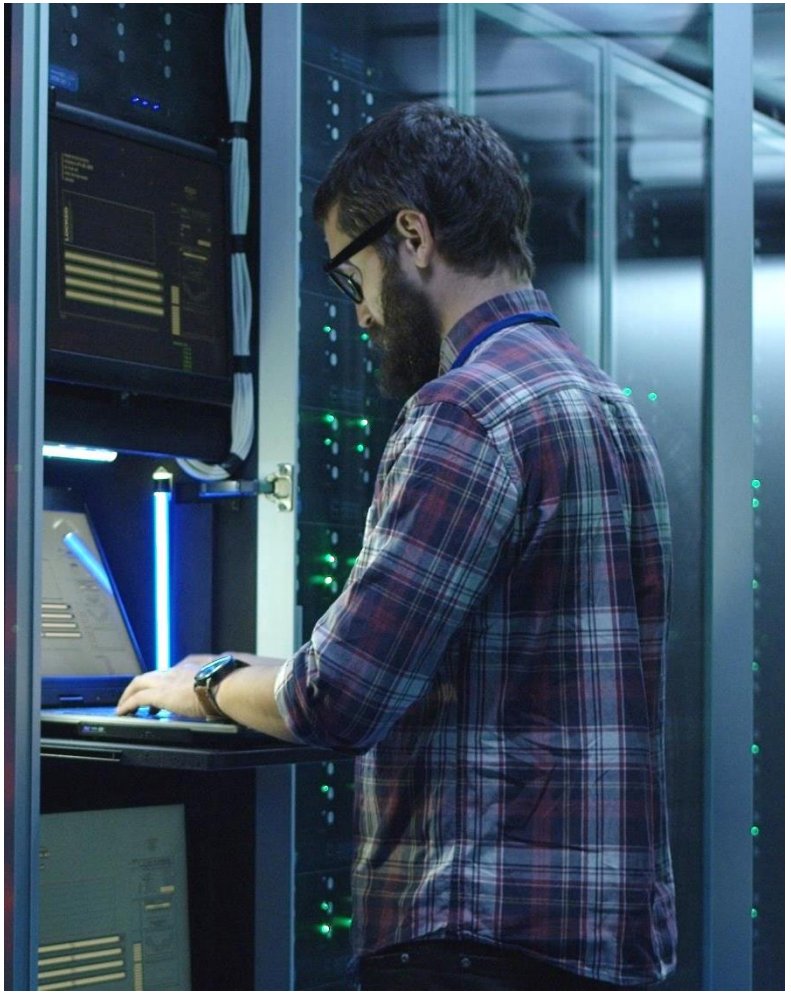
Protegendo dados com armazenamento de objetos na nuvem

O armazenamento de objetos na nuvem também é um meio robusto, seguro e econômico de arquivar e proteger dados. A definição de políticas adequadas garante a flexibilidade para especificar os períodos de retenção padrão, mínimo e máximo.

Esses períodos de preservação e retenções legais adicionais podem ser aplicados a um único objeto ou a vários objetos, à medida que os dados são alimentados na nuvem. Isso significa que os objetos não podem ser excluídos até que o período de retenção expire e todas as retenções legais sejam removidas.

Alcançando o equilíbrio ideal de segurança

Os ataques cibernéticos que impedem o acesso a dados ou os destroem estão ficando mais sofisticados. Por isso, **é essencial encontrar o equilíbrio certo entre a tecnologia que sua organização usa e a filosofia que ela adota para a proteção de dados**, para criar uma estratégia de segurança eficaz. Definir as ações necessárias para a recuperação de ataques bem-sucedidos é uma parte importante de uma postura de segurança bem planejada.



Em ambos os lados dessa balança, várias soluções de armazenamento com funcionalidades importantes de segurança podem desempenhar um papel primordial na proteção dos sistemas de uma organização, contra a variedade de ameaças cibernéticas existentes. Encontrar esse equilíbrio pode parecer uma tarefa difícil sem uma sólida compreensão do cenário atual das ameaças e das informações que você precisa proteger.

As organizações podem aproveitar abordagens como o Framework da NIST e a disciplina de gerenciamento de riscos, para ajudar a construir uma estratégia abrangente de armazenamento.

Tecnologias como *snapshots*, proteção de isolamento físico por fita e armazenamento de objetos na nuvem podem ser usadas para criar e implementar soluções de resiliência cibernética que ajudarão organizações como a sua a permanecerem seguras diante das crescentes ameaças.

Faça com que a proteção de dados seja uma prioridade

A Mainline é uma parceira de negócios da IBM e possui as soluções e o conhecimento necessários para fornecer à sua organização uma proteção holística e moderna dos dados, que oferece simplicidade, escalabilidade e gerenciamento unificado, necessários para proteger e recuperar dados em ambientes *multicloud*, enquanto ajuda a alavancar dados secundários para análises e relatórios , visando obter vantagens competitivas para seu negócio.

Não deixe sua organização ficar despreparada. Entre em contato conosco para saber mais sobre o desenvolvimento de uma estratégia de resiliência cibernética orquestrada.

Referências:

1. Data Breach Report 2019, Ponemon Institute, 2019
2. Global Risks Report 2019, 14th Edition, World Economic Forum, 2019.
3. Five key technologies for enabling a cyber resilience framework, IDC, 2018.
4. IBM FlashSystem A9000 and A9000R Business Continuity Solutions, IBM Corp., 2018.
Tricks of the storage trade: How to build an effective cyber resilience strategy, IBM Corp., 2019

www.mainlinesystems.com.br
55 (11) 3050-4400
contato@mainline.com
Rua Funchal, 411
Vila Olímpia | São Paulo, SP
04551-060

A Mainline Information Systems é uma empresa integradora de sistemas, com foco em infraestrutura de tecnologia, fundada em 1989 nos Estados Unidos e está presente no Brasil desde 2004. Ajudamos clientes de diversos segmentos, para que possam ir adiante com sua estratégia no atual cenário de transformação digital. Somos reconhecidos por sua principal parceira no Brasil como IBM Platinum Partner, título concedido a apenas 7 empresas no país, graças aos fortes investimentos em habilidades técnicas e certificações necessárias para fornecer o mais alto nível de serviços e soluções para nossos clientes em todos os produtos de hardware e software da IBM, incluindo serviços de manutenção e suporte a software.