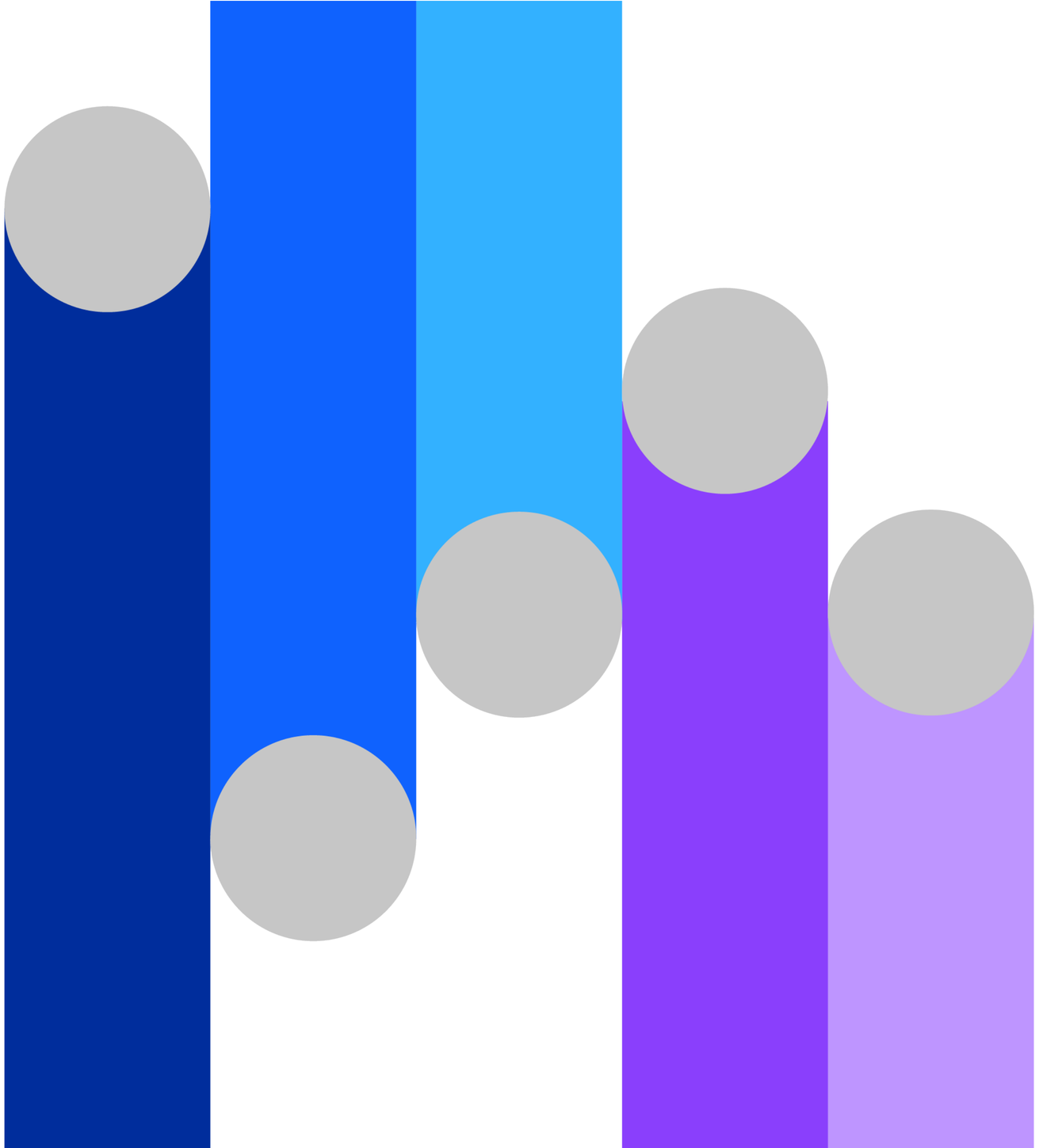
IBM **Security**

Cinco armadilhas comuns para evitar na segurança de dados

Aprenda a melhorar a segurança e a conformidade dos seus dados



Índice

00

Introdução

A segurança de dados deve ser prioridade nas empresas, e por um bom motivo

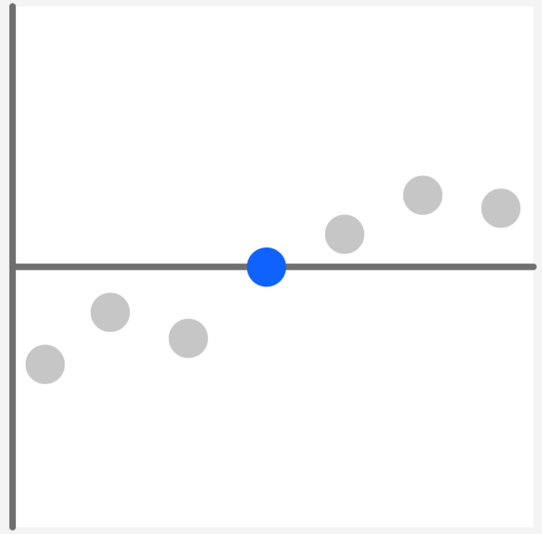
Mesmo com a TI cada vez mais descentralizada e complexa, é importante saber que muitas violações dos dados podem ser evitadas. Cada empresa tem desafios e metas específicos para a cibersegurança, mas é normal que as organizações cometam os mesmos erros no geral quando começam a abordar a segurança de dados. Além disso, vários líderes corporativos aceitam esses erros como prática normal nos negócios.

Vários fatores internos e externos podem levar a que os ciberataques tenham sucesso:

- Erosão dos perímetros da rede
- Maior superfície de ataque nos ambientes mais complexos de TI
- Uma demanda crescente do serviço de nuvem nas práticas de cibersegurança
- A natureza cada vez mais sofisticada dos cibercrimes
- Uma escassez persistente das competências em cibersegurança
- Falta de conscientização dos funcionários sobre os riscos na segurança de dados

US$ 4,45 mi

O custo global médio de uma violação dos dados aumentou em 2023 — 15% em três anos.[1]



Próximo capítulo

01

Armadilha 1: incapacidade de ir além da conformidade

Armadilha 1: incapacidade de ir além da conformidade

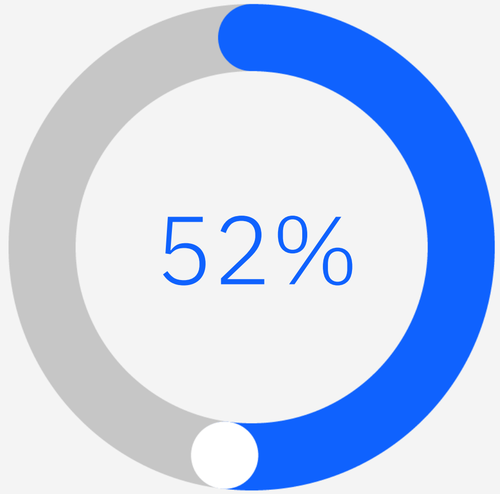
Conformidade não significa necessariamente segurança de dados. As organizações que dedicam os limitados recursos de segurança de dados para cumprirem uma auditoria ou certificação podem ficam complacentes. Já ocorreram várias violações dos dados em organizações que, no papel, estavam totalmente em conformidade. Os exemplos a seguir mostram que focar apenas a conformidade pode diminuir a segurança efetiva.

Cobertura incompleta
As empresas muitas vezes sofrem ao lidarem com a configuração incorreta dos bancos de dados e das políticas de acesso desatualizadas antes da auditoria anual. A avaliação da vulnerabilidade e dos riscos deve ser uma atividade contínua.

Mínimo esforço
Muitas empresas adotam soluções em segurança de dados apenas para cumprir requisitos legais ou dos parceiros de negócios. A mentalidade de “vamos implementar um padrão mínimo e voltar para o trabalho” pode ir em contra das boas práticas de cibersegurança. A segurança eficaz dos dados é uma maratona, não um sprint.

Diminuição da urgência
As empresas podem ficar complacentes em relação à gestão dos controles quando as regulamentações amadurecem, como no caso da Lei Sarbanes-Oxley (SOX), do Regulamento Geral de Proteção de Dados (GDPR), do Padrão de Segurança de Dados de Cartões de Pagamento (PCI DSS) e da Lei de Direitos de Privacidade da Califórnia (CPRA), antiga CCPA. Embora, com o tempo, os líderes possam se preocupar menos com a privacidade, a segurança e a proteção dos dados regulamentados, os riscos e custos associados ao descumprimento continuam.

Omissão dos dados não regulamentados
Ativos como a propriedade intelectual podem colocar a sua organização em risco se forem perdidos ou repassados a pessoas não autorizadas. Ao focar apenas a conformidade, a organização pode acabar negligenciando a segurança de dados e não protegendo bem os dados valiosos.



Cerca de 52% das organizações afirmam que a complexidade resultante da mudança da carga de trabalho para a nuvem pública também dificultou a conformidade.[2]

Enxergue a conformidade como uma oportunidade para inovar e melhorar seus padrões de segurança em prol da sua empresa.

Solução: reconhecer e aceitar que a conformidade é um ponto de partida

Quanto à segurança de dados, as organizações devem estabelecer programas estratégicos que protejam consistentemente os dados críticos dos negócios, em vez de apenas responder aos requisitos de conformidade.

Os programas de conformidade e de segurança de dados devem incluir as seguintes práticas:

- Descobrir e classificar os dados sensíveis nas aplicações no local, em nuvem e no software como serviço (SaaS).
- Avaliar os riscos com insights de contextos e análise dos dados.
- Na proteção dos dados sensíveis, usar criptografia e políticas flexíveis de acesso.
- Monitorar o acesso a dados e padrões de uso para descobrir atividades suspeitas com rapidez.
- Responder às ameaças em tempo real.
- Simplificar a conformidade e os respectivos relatórios.

O elemento final pode incluir responsabilizações legais relacionadas à conformidade regulatória; possíveis perdas que a empresa venha sofrer; e os potenciais custos dessas perdas para além das multas por descumprimento.

Em última análise, você deve pensar de forma holística sobre os riscos e o valor dos dados que procura proteger.

02

Armadilha 2: incapacidade de reconhecer a necessidade de segurança centralizada dos dados

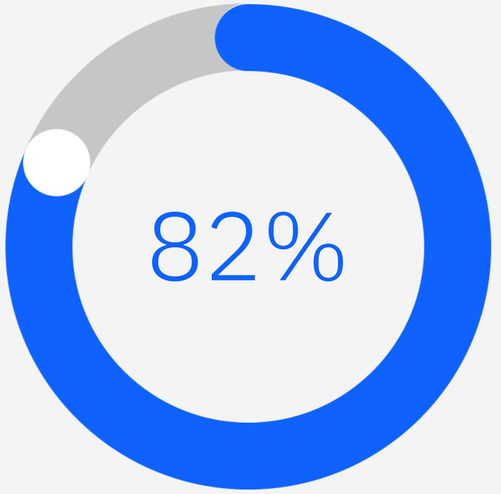
Armadilha 2: incapacidade de reconhecer a necessidade de segurança centralizada nos dados

Sem mandatos de conformidade mais amplos, que abranjam a privacidade e a segurança de dados, os líderes das organizações podem acabar negligenciando a necessidade de uma segurança de dados padronizada em toda a empresa.

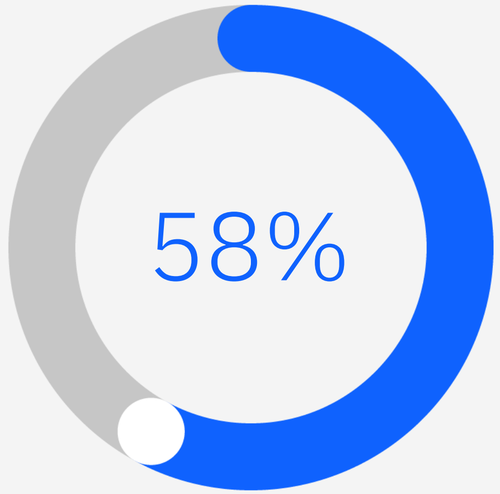
Nas empresas com ambientes multinuvem híbridos, que estão sempre mudando e crescendo, podem aparecer novos tipos de fonte de dados toda semana ou até todo dia e, com isso, dispersar bastante os dados sensíveis.

Os líderes de empresas que estão crescendo e a expandindo a infraestrutura da TI podem não reconhecer o risco que uma mudança na superfície de ataque representa. Eles podem não ter a visibilidade e o controle adequados à medida que os dados sensíveis circulam por um ambiente de TI cada vez mais complexo e díspar. O descuido de não adotar o controle completo na privacidade, segurança e proteção dos dados, principalmente em ambientes complexos, pode sair muito caro.

Operar as soluções de cibersegurança em silos pode causar outros problemas. Uma organização com um centro de operações de segurança (SOC) e uma solução em gestão de eventos e informações de segurança (SIEM), por exemplo, pode negligenciar a alimentação desses sistemas com insights obtidos da solução em segurança de dados. Da mesma forma, a falta de interoperabilidade entre equipes, processos e ferramentas de segurança pode dificultar o sucesso de um programa de cibersegurança.



82% das violações envolveram dados armazenados em nuvem.[1]



58% das organizações afirmam que cerca de 21% a 50% dos dados sensíveis em nuvem não estão suficientemente protegidos.[2]

A proteção dos dados sensíveis deve ocorrer em conjunto com esforços mais amplos de cibersegurança.

Solução: saber onde residem seus dados confidenciais, incluindo repositórios no local, hospedados em nuvem e nas aplicações de SaaS

A proteção dos dados sensíveis deve ocorrer em conjunto com esforços mais amplos de cibersegurança.Além de saber onde os dados sensíveis estão guardados, você também precisa saber quando e como eles são acessados, mesmo que essas informações mudem rapidamente. Além disso, você deve integrar as informações e políticas de segurança e proteção dos dados com seu programa geral de cibersegurança para viabilizar uma comunicação estreitamente alinhada entre as tecnologias. Uma solução em segurança de dados que opere em ambientes e plataformas díspares ajuda nesse processo.

Quando é o momento certo de integrar a segurança de dados com outros controles de cibersegurança como parte de uma prática mais abrangente de cibersegurança? Confira alguns sinais de que sua organização está pronta os próximos passos.

Risco de perder dados valiosos
O valor dos dados pessoais, sensíveis e próprios da sua organização é tanto que a perda deles causaria danos notáveis à viabilidade dos negócios.

Implicações regulatórias
Sua organização coleta e armazena dados com requisitos legais, como o número dos cartões de crédito, outros dados para pagamento e dados pessoais.

Falta de fiscalização na cibersegurança
Sua organização cresceu a tal ponto que é difícil monitorar e proteger todos os endpoints da rede, incluindo instâncias de nuvem. Por exemplo: você sabe bem onde, quando e como os dados são armazenados, compartilhados e acessados no seu depósito de dados no local, em nuvem e nas aplicações de SaaS?

Avaliação inadequada
Sua organização adotou uma abordagem fragmentada, que não mostra claramente o que é gasto em todas as suas atividades de cibersegurança. Por exemplo: você conta com processos implementados para medir, com precisão, o retorno do investimento (ROI) em termos dos recursos alocados, a fim de reduzir o risco na segurança de dados?

Se sua organização cai em alguma dessas situações, é bom você adquirir as qualificações e soluções em cibersegurança para integrar a segurança de dados na sua prática de segurança mais ampla.

Armadilha 3: incapacidade de definir o responsável pelos dados

Armadilha 3: incapacidade de definir o responsável pelos dados

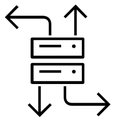
Mesmo conscientes da necessidade de segurança de dados, muitas empresas não têm ninguém especificamente responsável pela proteção dos dados sensíveis. Essa situação muitas vezes fica óbvia durante um incidente na segurança de dados ou na auditoria, quando a organização é pressionada a descobrir o responsável.

Os principais executivos podem recorrer ao diretor executivo de TI (CIO), que pode dizer: “Nosso trabalho é manter os sistemas centrais funcionando. Vá falar com alguém da minha equipe de TI.” Esses funcionários da TI podem ser responsáveis por vários bancos de dados nos quais residem dados sensíveis e, ainda assim, não terem um orçamento para cibersegurança.

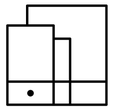
Normalmente, os subordinados ao diretor de segurança da informação (CISO) da organização não são diretamente responsáveis pelos dados que cruzam os negócios em geral. Eles podem aconselhar os diferentes gerentes na linha de negócios (LOB) dentro da corporação, mas, em muitas empresas, ninguém é explicitamente responsável pelos dados em si. Na organização, os dados são um dos ativos mais valiosos. No entanto, sem a responsabilidade de propriedade, proteger os dados sensíveis de forma adequada é um desafio.

Nos ambientes de TI mais complexos, é fundamental contabilizar os dados nos seguintes locais:

Compartilhado entre as unidades de negócios



Localizado em infraestruturas multinuvem híbridas



Armazenados em dispositivos móveis

Solução: contratar um CDO ou DPO exclusivo para o bem-estar e a segurança dos ativos com dados sensíveis e críticos

Um diretor de dados (CDO) ou diretor de proteção dos dados (DPO) pode cuidar dessas funções. Aliás, as empresas com sede na Europa ou que fazem negócios com os titulares de dados na União Europeia estão sujeitas a mandatos do GDPR que exigem que tenham um DPO. Esse pré-requisito reconhece que o valor dos dados sensíveis (neste caso, os dados pessoais) vai além do LOB que utiliza esses dados. Além disso, a exigência enfatiza que as empresas têm a função específica de serem responsáveis pelos ativos de dados.

Considere as seguintes metas e responsabilidades ao nomear um CDO ou DPO:

Conhecimento técnico e senso empresarial
Avalie os riscos e apresente um caso de negócios prático, que líderes empresariais leigos entendam, em relação aos investimentos na segurança de dados.

Implementação estratégica
Direcione um plano em nível técnico que use controles de detecção, resposta e segurança de dados para oferecer proteções.

Liderança na conformidade
Entenda os requisitos de conformidade e saiba como mapeá-los nos controles de segurança de dados, para que sua empresa garanta a conformidade.

Monitoramento e avaliação
Monitore o cenário de ameaças; e meça a eficácia do seu programa de segurança de dados.

Flexibilidade
Integre ferramentas mais avançadas para saber quando e como ajustar a estratégia da segurança de dados, como expandir o acesso aos dados e as políticas de uso em novos ambientes.

Divisão dos trabalhos
Defina expectativas com provedores de serviços de nuvem em relação aos acordos de nível de serviço (SLAs) e às responsabilidades associadas ao risco e à remediação da segurança de dados.

Plano de resposta à violação de dados
Por fim, esteja pronto para desempenhar um papel fundamental na elaboração de um plano estratégico de mitigação e resposta a violações.

Em última análise, o CDO ou DPO deve liderar a promoção da colaboração na segurança de dados entre as equipes e em toda a empresa, uma vez que todos precisam trabalhar juntos para proteger os dados corporativos. Essa colaboração pode auxiliar o CDO ou DPO a supervisionar os programas e proteções que a organização necessita para cuidar dos dados sensíveis.

04

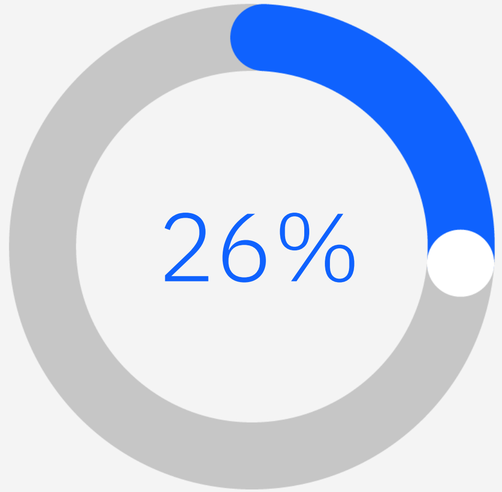
Armadilha 4: incapacidade de lidar com as vulnerabilidades conhecidas

Armadilha 4: incapacidade de lidar com as vulnerabilidades conhecidas

Nas empresas, as violações de alto perfil geralmente provêm de vulnerabilidades conhecidas que não foram corrigidas mesmo após o lançamento dos patches. A incapacidade de corrigir as vulnerabilidades conhecidas rápido coloca os dados da sua organização em risco, pois os cibercriminosos procuram ativamente esses pontos de entrada.

No entanto, muitas empresas acham complicado implementar os patches com rapidez devido ao grau necessário de coordenação entre os grupos operacionais, de TI e de segurança. Além disso, os patches geralmente exigem testes para saber se não interrompem nenhum processo nem introduzem uma nova vulnerabilidade.

Nos ambientes de nuvem, às vezes é difícil saber se um serviço terceirizado ou o componente de uma aplicação deve ser corrigido. Mesmo que se encontre uma vulnerabilidade em um serviço, os usuários muitas vezes não têm controle sobre o processo de remediação do prestador do serviço.



Em 26% das novas vulnerabilidades, já se sabiam das explorações.[3]

Seja proativo: faça avaliações da vulnerabilidade do seu depósito de dados para mitigar os riscos.

Solução: estabelecer um programa eficaz de gestão das vulnerabilidades, com a tecnologia apropriada para viabilizar o crescimento

A gestão das vulnerabilidades normalmente envolve os seguintes níveis de atividade:

- Manter um inventário preciso e um estado básico para seus ativos de dados.
- Fazer varreduras e avaliações frequentes quanto à vulnerabilidade em toda a infraestrutura, incluindo os ativos em nuvem.
- Priorizar a remediação que considere a probabilidade de a vulnerabilidade ser explorada e o impacto que isso pode ter nos negócios.
- Incluir a gestão das vulnerabilidades e capacidade de resposta como parte do SLA junto aos prestadores de serviços terceirizados.
- Ofuscar os dados sensíveis ou pessoais sempre que possível. Criptografia, tokenização e redação são três opções para atingir esse fim.
- Empregar a gestão adequada das chaves de criptografia, garantindo que elas fiquem guardadas com segurança e tenham o ciclo adequado para manter os dados criptografados seguros.

Mesmo dentro de um programa maduro de gestão das vulnerabilidades, nenhum sistema é totalmente inviolável. Supondo que uma invasão possa ocorrer mesmo nos ambientes mais bem protegidos, seus dados requerem outro nível de proteção. O conjunto certo de técnicas e capacidades de criptografia dos dados protege os seus dados das ameaças novas e emergentes.

05

Armadilha 5: incapacidade de priorizar e usar o monitoramento moderno nas atividades dos dados

Armadilha 5: incapacidade de priorizar e usar o monitoramento moderno nas atividades dos dados

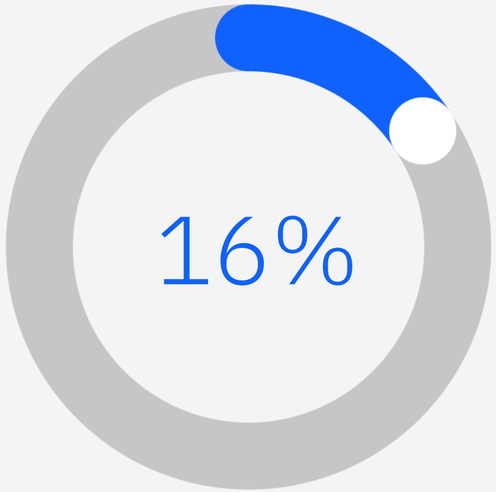
Monitorar o acesso e o uso dos dados é essencial em toda estratégia de segurança de dados. O líder da organização precisa saber quem, como e quando as pessoas têm acesso aos dados. Esse monitoramento inclui saber se essas pessoas podem ter acesso, se o nível de acesso está correto e se representa um risco elevado à empresa.

Quanto às ameaças internas, os usuários privilegiados são infratores comuns.
Um plano de proteção dos dados deve incluir monitoramento em tempo real para detectar contas de usuários privilegiados usadas em atividades suspeitas ou não autorizadas.

Para evitar possíveis atividades maliciosas, uma solução deve executar as seguintes tarefas:

- Bloquear e colocar em quarentena as atividades suspeitas com base na violação das políticas.
- Suspender ou encerrar a sessão com base no comportamento anômalo.
- Usar, nos ambientes de dados, fluxos de trabalho predefinidos de acordo com as regulamentações.
- Enviar alertas práticos aos sistemas de segurança e operações de TI.

Pode ser difícil cuidar da segurança de dados e das informações relacionadas à conformidade, além de saber quando e como responder a uma potencial ameaça. Com o acesso de usuários autorizados a diversas fontes de dados, como bancos de dados, sistemas de arquivos, ambientes de solução de aprendizado de máquina, ambientes em nuvem e aplicações de SaaS, salvar os dados de todas essas interações parece um processo complicado. O desafio está em monitorar, capturar, filtrar, processar e responder, de modo eficaz, um volume enorme de atividade de dados. Sem um plano adequado, a sua organização pode ter mais informações sobre as atividades do que pode processar; isso, por sua vez, diminui o valor do monitoramento das atividades dos dados.



16% dos incidentes observados envolveram o abuso de contas válidas, no qual os adversários obtiveram e abusaram das credenciais de contas existentes como forma de obter acesso.[3]

Com uma solução de monitoramento das atividades dos dados, os analistas de segurança de dados ganham um tempo valioso.

Solução: desenvolver uma estratégia abrangente para a segurança e a conformidade dos dados

Para isso, ao iniciar uma jornada de segurança de dados, você precisa mensurar e definir o escopo dos esforços de monitoramento para lidar com os requisitos e riscos. Essa atividade geralmente envolve uma abordagem em fases para desenvolver e escalar as melhores práticas em toda a sua empresa. Além disso, é fundamental conversar com os principais stakeholders de negócios e de TI no início do processo, para saber quais são as metas no curto e no longo prazo.

Nessas conversas, também é preciso conhecer a tecnologia necessária para viabilizar as principais iniciativas. Por exemplo: ao planejar abrir filiais em uma nova zona geográfica, se sua empresa decidir usar uma combinação de repositórios de dados no local, hospedados em nuvem e em aplicações de SaaS, a estratégia para a segurança de dados deve avaliar como esse plano afetará a postura da organização quanto à segurança e a conformidade dos dados. Nesse caso, os dados de propriedade da empresa ficarão sujeitos a novos requisitos de segurança e conformidade dos dados, como GDPR, CPRA, a Lei Geral de Proteção de Dados (LGPD) do Brasil e assim por diante.

Você também deve priorizar e focar uma ou duas fontes que provavelmente tenham os dados mais sensíveis. Suas políticas de segurança de dados devem ser bem claras e detalhadas quanto a essas fontes antes de estender essas práticas ao restante da sua infraestrutura.

Procure uma solução automatizada em monitoramento das atividades com dados ou arquivos, que ofereça uma análise rica dos dados e se centre nos principais riscos e comportamentos incomuns de usuários privilegiados.

Armadilha 5: incapacidade de priorizar e usar o monitoramento moderno nas atividades dos dados

É essencial receber alertas automatizados quando uma solução em monitoramento das atividades dos dados ou arquivos detecta um comportamento anormal, mas você também precisa tomar medidas rápidas quando uma anomalia ou desvio das políticas de acesso a dados for descoberto. As ações de proteção devem incluir mascaramento ou bloqueio dinâmico dos dados.

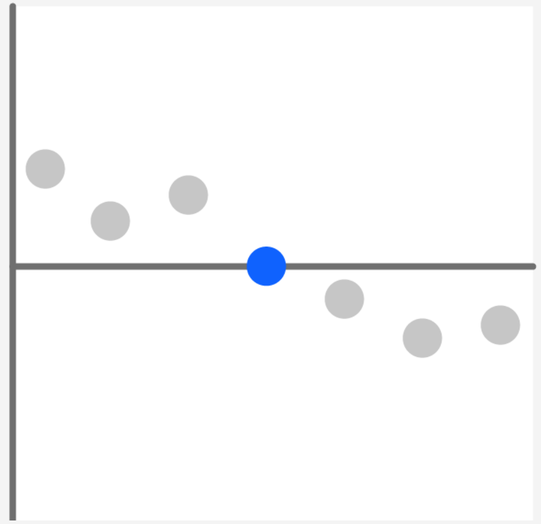
À medida que você desenvolve planos de monitoramento e proteção das atividades dos dados, é bom considerar o seguinte:

- Quais são minhas duas principais fontes de dados mais sensíveis?
- Quais fontes de dados devo priorizar em seguida (de cinco a dez fontes), com base no volume de dados sensíveis?
- Há determinados endpoints ou ativos de nuvem associados a dados em maior risco?
- Os dados sensíveis são transferidos livremente de e para ambientes locais, híbridos e em nuvem?
- A quais usuários deve ser dado o acesso à fonte de dados? E sob quais condições?
- Quais usuários ou contas privilegiadas de alto risco precisam ser desativados ou exigem um exame mais minucioso?
- Minha solução de segurança de dados faz o monitoramento das atividades em tempo real e tem recursos automatizados para a proteção dos dados?
- O monitoramento em tempo real está implementado para rastrear os dados nos arquivos em depósitos de dados, como linguagem de consulta estruturada (SQL Database, distribuições Hadoop, plataformas não SQL (NoSQL) e assim por diante?
- Minha solução de monitoramento leva em conta o armazenamento dos dados em ambientes multinuvem híbridos e gera relatórios personalizados que vão para as pessoas certas no momento certo?
- Tenho a análise de dados dos riscos e os recursos necessários para o monitoramento filtrado para priorizar, com eficácia, os riscos, vulnerabilidades e esforços de remediação?

Quanto mais específico você for nas prioridades de monitoramento e requisitos de proteção, mais eficaz será a solução aplicável aos recursos disponíveis para detecção e resposta.

US$ 1,76 mi

Em média, as organizações que utilizam amplamente a IA e a automação da segurança economizam US$ 1,76 milhão em comparação com as organizações que não utilizam esses recursos.[1]



06

O que está por vir?

Como evitar essas armadilhas comuns na segurança de dados, principalmente agora, com mais empresas buscando ambientes multinuvem híbridos? Tudo começa reconhecendo o problema e preparando a organização para adotar uma abordagem proativa e abrangente na proteção os dados, onde quer que eles residam.

Se sua empresa tem um ambiente de TI complexo e híbrido, sua abordagem à segurança de dados não pode ser isolada. Você precisa incluir outras estratégias para a segurança e conformidade dos dados, que envolvam toda a sua infraestrutura de dados e todos os tipos de dados.

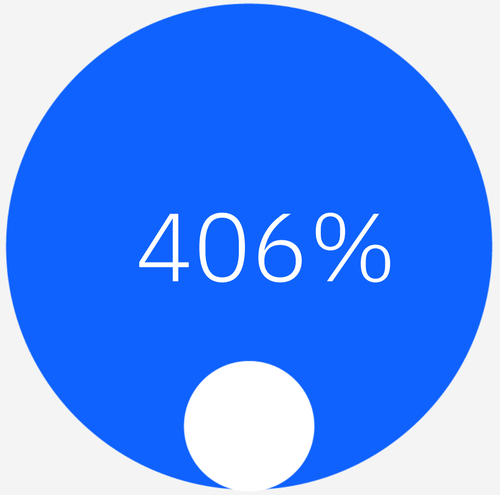
As etapas imediatas para proteger os dados valiosos da sua organização são:

- Criar um plano de conformidade e segurança de dados que viabilize as metas de negócios e de tecnologia de curto e longo prazo da sua organização
- Implementar esse plano com o pessoal, os processos e as ferramentas adequadas
- Planejar os recursos para que seu programa de segurança e conformidade dos dados se adapte de forma eficaz à medida que sua organização adota a tecnologia moderna

A plataforma IBM Security® Guardium® é uma solução de segurança e conformidade dos dados para organizações que pretendem adotar uma abordagem mais inteligente e adaptativa na proteção dos dados críticos e sensíveis, onde quer que eles estejam. Veja por que essa pode ser uma boa opção para sua organização.

Saiba mais →

Fale conosco →



Um estudo sobre a solução Guardium constatou um ROI de 406% com benefício de US$ 5,86 milhões em três anos.[4]

07

Por que o IBM Security?

O IBM Security protege as maiores empresas e governos do mundo graças ao portfólio integrado de produtos e serviços de segurança com IA de segurança dinâmica e recursos de automação. Amparado pelas pesquisas do mundialmente conhecido IBM® X-Force®, esse portfólio serve para que as organizações prevejam ameaças, protejam os dados em movimento e respondam com rapidez e precisão, sem impedir a inovação dos negócios. A IBM conta com a confiança de milhares de organizações parceiras para avaliar, definir estratégias, implementar e gerenciar as transformações na segurança.

A IBM opera uma das maiores organizações de pesquisa, desenvolvimento e entrega de segurança; monitora mais de 150 bilhões de eventos de segurança por dia, em mais de 130 países; e tem mais de 10 mil patentes em segurança em todo o mundo.

Capítulo anterior

1. Relatório do custo das violações de dados, IBM, julho de 2023.

2. The Need for Data Compliance in Today's Cloud Era, Enterprise Strategy Group by TechTarget, abril de 2023.

3. X-Force Threat Intelligence Index 2023, IBM Security, fevereiro de 2023.

4. The Total Economic Impact™ (TEI) of IBM Security Guardium Data Protection, estudo da Forrester Consulting solicitado pela IBM, junho de 2023.

IBM Brasil Ltda
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP
IBM Corporation
New Orchard Road
Armonk, NY 10504

Produzido nos Estados Unidos da América
Setembro de 2020