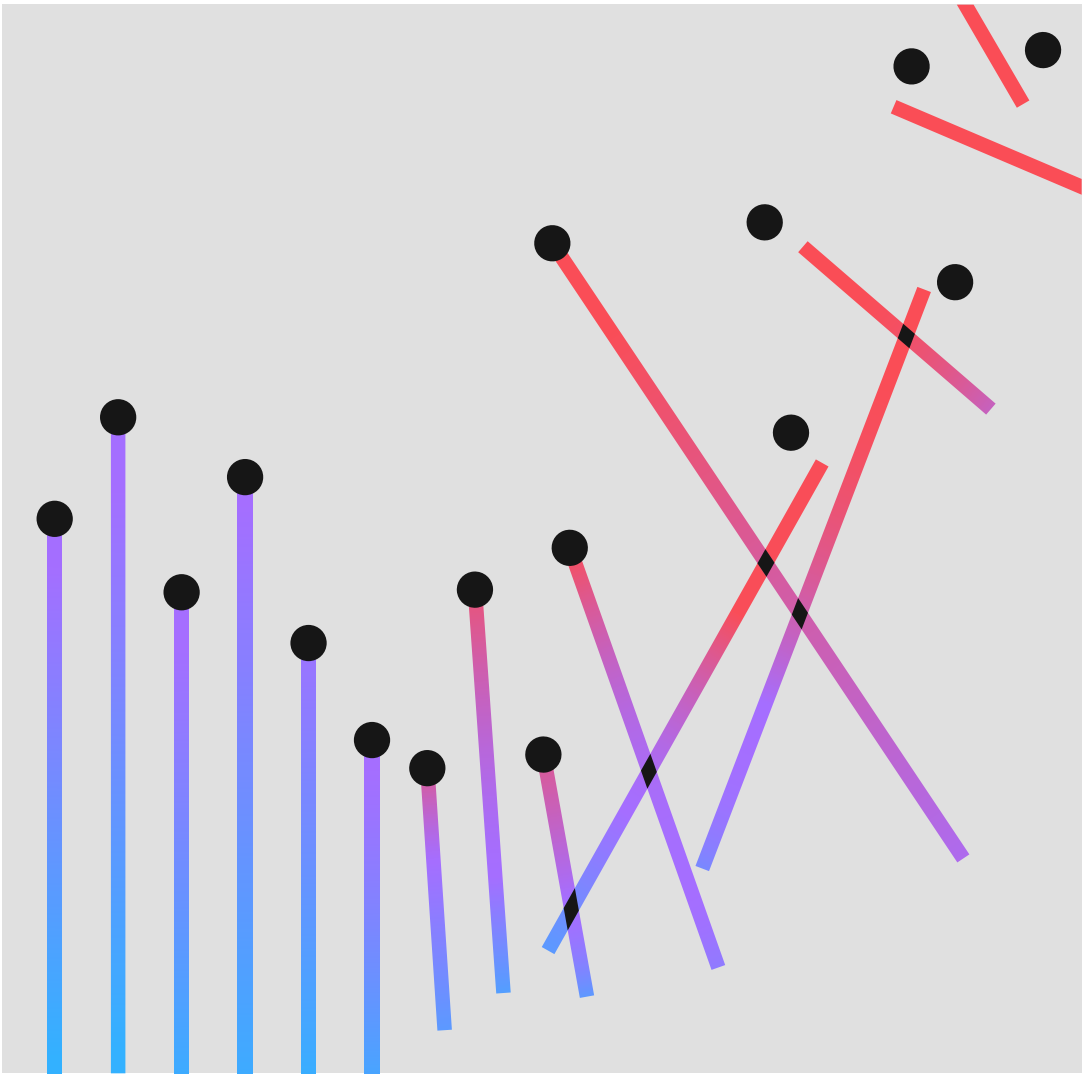
IBM **Security**

Relatório do custo de uma violação de dados de 2022: Resumo executivo



Conteúdo

03 Resumo executivo

07 Recomendações de segurança

09 Sobre o Ponemon Institute
e a IBM Security

10 Dê os próximos passos

Resumo executivo

O Relatório do custo de uma violação de dados ajuda os líderes de TI, gerenciamento de risco e segurança a entender os fatores que podem aumentar ou reduzir o custo crescente das violações de dados.

Esta pesquisa anual que o Ponemon Institute conduz independentemente e que é patrocinada, analisada e publicada pela IBM Security®, já está em sua 17ª edição. Ela estudou 550 organizações atingidas por violações de dados ocorridas no período entre março de 2021 e março de 2022. As violações ocorreram em 17 países e regiões e em 17 setores diferentes.

Realizamos mais de 3.600 entrevistas com indivíduos de organizações atingidas por violações de dados. Durante as entrevistas, fizemos perguntas para determinar o custo para as organizações em diferentes atividades relacionadas diretamente tanto à resposta imediata quanto à resposta prolongada às violações de dados.

Assim como nos relatórios dos anos anteriores, os dados deste ano dão um panorama de como dezenas de fatores afetam os custos que continuam se somando depois que uma violação de dados ocorre. Além disso, o relatório examina as principais causas, as consequências a curto e longo prazo das violações de dados e os fatores e tecnologias atenuantes que permitiram às empresas limitar suas perdas.

Principais descobertas

As principais descobertas aqui descritas são baseadas na análise da IBM Security dos dados de pesquisa compilados pelo Ponemon Institute.[1]

US$ 4,35 milhões

Custo total médio de uma violação de dados

Atingindo um recorde histórico, o custo de uma violação de dados foi em média de US$ 4,35 milhões em 2022. Este valor representa um aumento de 2,6% em relação ao ano anterior, quando o custo médio de uma violação foi de US$ 4,24 milhões. O custo médio subiu 12,7% em relação aos US$ 3,86 milhões no relatório de 2020.

83%

Porcentagem de organizações que tiveram mais de uma violação

Oitenta e três por cento das organizações estudadas sofreram mais de uma violação de dados e apenas 17% disseram que esta foi sua primeira violação de dados. Sessenta por cento das organizações estudadas afirmaram que aumentaram o preço de seus serviços ou produtos por causa das violações de dados.

US$ 4,82 milhões

Custo médio de uma violação de dados de infraestrutura crítica

O custo médio de uma violação de dados nas organizações de infraestrutura crítica estudadas foi de US$ 4,82 milhões — US$ 1 milhão a mais do que o custo médio nas organizações de outros setores. Entre as organizações de infraestrutura crítica estavam as de serviços financeiros, indústrias, tecnologia, energia, transporte, comunicação, saúde, educação e setor público. Vinte e oito por cento sofreram um ataque destrutivo ou de ransomware, enquanto 17% sofreram uma violação devido ao comprometimento de um parceiro de negócios.

US$ 3,05 milhões

Economia de custos média associada a IA e automação para segurança totalmente implementadas

As violações em organizações com IA e automação para segurança totalmente implementadas custam US$ 3,05 milhões a menos do que as violações em organizações que não implementaram IA e automação para segurança. Esta diferença de 65,2% no custo médio de violação — entre US$ 3,15 milhões para implementação completa contra US$ 6,20 milhões para não implementação — representou a maior economia de custos no estudo. As empresas com IA e automação para segurança totalmente implementadas também tiveram, em média, um período 74 dias mais curto para identificar e conter a violação do que aquelas sem IA e automação para segurança. A diferença do período, conhecido como o ciclo de vida da violação, foi de 249 dias contra 323 dias. O uso de IA e automação para segurança saltou quase um quinto em dois anos, de 59% em 2020 para 70% em 2022.

1. Os valores de custo neste relatório são medidos em dólares americanos (US$).

US$ 4,54 milhões

Custo médio de um ataque de ransomware, não incluindo o custo do ransomware em si

Onze por cento das violações no estudo foram ataques de ransomware. Um aumento em relação a 2021, quando 7,8% das violações foram de ransomware, para uma taxa de crescimento de 41%. O custo médio de um ataque de ransomware caiu ligeiramente, de US$ 4,62 milhões em 2021 para US$ 4,54 milhões em 2022. Este custo foi ligeiramente superior ao custo total médio geral de uma violação de dados, US$ 4,35 milhões.

19%

Frequência de violações causadas por credenciais roubadas ou comprometidas

O uso de credenciais roubadas ou comprometidas continua sendo a causa mais comum de uma violação de dados. As credenciais roubadas ou comprometidas foram o principal vetor de ataque em 19% das violações no estudo de 2022 e também o principal vetor de ataque no estudo de 2021, tendo ocasionado 20% das violações. As violações causadas por credenciais roubadas ou comprometidas tiveram um custo médio de US$ 4,50 milhões. Estas violações tiveram o ciclo de vida mais longo: foram 243 dias para identificar a violação e outros 84 dias para conter a violação. O phishing foi a segunda causa mais comum de uma violação, com 16%, e também a mais cara, com uma média de US$ 4,91 milhões em custos de violação.

59%

Porcentagem de organizações que não implementam zero trust

Apenas 41% das organizações no estudo disseram que implementam arquitetura de segurança zero trust. Os outros 59% das organizações, as que não implementam zero trust, incorrem em custo médio de um milhão de dólares a mais por violação, em comparação às que implementam. Entre as organizações de infraestrutura crítica, uma porcentagem ainda mais alta, de 79%, não implementa zero trust. Estas organizações registraram em média US$ 5,40 milhões em custos de violação, mais de 1 milhão de dólares acima da média global.

US$ 1 milhão

Diferença média de custo entre onde o trabalho remoto foi fator causador da violação e quando não foi determinante

Quando o trabalho remoto esteve entre os fatores causadores da violação, os custos médios foram de quase 1 milhão de dólares a mais do que nas violações em que o trabalho remoto não foi um dos fatores — US$ 4,99 milhões contra US$ 4,02 milhões. As violações relacionadas ao trabalho remoto custam em média cerca de US$ 600.000 a mais em comparação à média global.

45%

Porcentagem de violações ocorridas na nuvem

Quarenta e cinco por cento das violações do estudo ocorreram na nuvem. No entanto, as violações que ocorreram em um ambiente de nuvem híbrida custaram em média US$ 3,80 milhões, em comparação a US$ 4,24 milhões para violações em nuvens privadas e US$ 5,02 milhões para violações em nuvens públicas. A diferença de custo foi de 27,6% entre violações em nuvens híbridas e violações em nuvens públicas. As organizações com modelo de nuvem híbrida também tiveram ciclos de vida de violação mais curtos que as organizações que adotaram apenas modelo de nuvem pública ou privada.

US$ 2,66 milhões

Economia média de custos associada à existência de uma equipe de resposta a incidentes (RI) e plano de RI regularmente testado

Quase três quartos das organizações que fizeram parte do estudo disseram ter um plano de RI, sendo que 63% dessas organizações disseram testar o plano regularmente. Ter equipe de RI e o plano de RI testado regularmente levou a uma significativa economia de custos. As empresas com uma equipe de RI que testaram seu plano de RI tiveram uma média de US$ 2,66 milhões a menos em custos de violação do que as organizações sem equipe de RI e que não testam plano de RI. A diferença de US$ 3,26 milhões contra US$ 5,92 milhões representa uma economia de custos de 58%.

29 dias

Economia no tempo de resposta nas organizações com tecnologias de detecção e resposta estendida (XDR)

Tecnologias XDR foram implementadas por 44% das organizações. As organizações com tecnologias XDR tiveram vantagens consideráveis nos tempos de resposta. As organizações com XDR implementada encurtaram o ciclo de vida da violação em cerca de um mês, em média, em comparação com as organizações que não implementaram XDR. Especificamente, as organizações levaram 275 dias para identificar e conter uma violação com XDR implementada, comparados a 304 dias, sem XDR implementada. Este número representa uma diferença de 10% nos tempos de resposta.

12 anos

Em anos consecutivos, o setor de saúde teve o maior custo médio de uma violação

Os custos da violação do setor de saúde atingiram um novo recorde. A violação média no setor da saúde aumentou em quase 1 milhão de dólares, chegando a US$ 10,10 milhões. Os custos de violação na saúde têm sido o setor mais caro por 12 anos consecutivos, aumentando 41,6% desde o relatório de 2020. As organizações financeiras tiveram o segundo maior custo — em média US$ 5,97 milhões — seguidas pelas farmacêuticas, com US$ 5,01 milhões, tecnologia, com US$ 4,97 milhões, e energia, com US$ 4,72 milhões.

US$ 9,44 milhões

Custo médio de uma violação nos Estados Unidos, o mais alto entre todos os países

Os cinco principais países e regiões com o maior custo médio por violação de dados foram: Estados Unidos, com US$ 9,44 milhões; Oriente Médio, com US$ 7,46 milhões; Canadá, com US$ 5,64 milhões; Reino Unido, com US$ 5,05 milhões e Alemanha, com US$ 4,85 milhões. Os Estados Unidos lideram a lista há 12 anos consecutivos. Enquanto isso, o país com a taxa de crescimento mais rápida em relação ao ano passado foi o Brasil, um aumento de 27,8%, de US$ 1,08 milhões para US$1,38 milhões.

Recomendações para ajudar a minimizar os impactos financeiros de uma violação de dados

Nesta seção, a IBM Security descreve as medidas que as organizações podem tomar para ajudar a reduzir o custo financeiro e as consequências sobre a sua reputação decorrentes de uma violação de dados. Estas recomendações incluem abordagens de segurança bem-sucedidas adotadas pelas organizações no estudo.

Adotar um modelo de segurança zero trust para ajudar a evitar o acesso não autorizado a dados sensíveis.
Os resultados do estudo mostraram que embora apenas 41% das organizações tenham implementado uma abordagem de segurança zero trust elas tiveram uma economia potencial de custos com violação da ordem de US$ 1,5 milhão, em implementação madura. Como as organizações incorporam trabalho remoto e ambientes multinuvem híbridos, uma estratégia zero trust pode ajudar a proteger dados e recursos, limitando sua acessibilidade e exigindo contexto.

Ferramentas de segurança que podem compartilhar dados entre sistemas diferentes e centralizar as operações de segurança de dados podem ajudar as equipes de segurança a detectar incidentes em ambientes multinuvem híbridos complexos. Você pode obter insights mais profundos, mitigar riscos e acelerar a resposta com uma plataforma de segurança aberta que pode fazer avançar sua estratégia zero trust. Ao mesmo tempo, você pode usar seus investimentos existentes enquanto deixa seus dados onde eles estão, ajudando sua equipe a se tornar mais eficiente e colaborativa.

Proteger dados sensíveis em ambientes de nuvem usando políticas e criptografia.
Com o crescente volume e valor dos dados hospedados em ambientes de nuvem, as organizações devem adotar medidas para proteger os bancos de dados hospedados na nuvem. As práticas maduras de segurança em nuvem foram associadas a uma economia de custos de violação de US$ 720.000 em comparação com as práticas de segurança sem nuvem. Use o esquema de classificação de dados e programas de retenção para ajudar a trazer visibilidade e reduzir o volume de informações sensíveis que são vulneráveis a uma violação. Proteja informações sensíveis usando criptografia de dados e criptografia totalmente homomórfica. Utilizar uma estrutura interna para auditorias, avaliar os riscos em toda a empresa e rastrear a conformidade com os requisitos de controle dos dados pode ajudar a melhorar sua capacidade de detectar uma violação de dados e aumentar os esforços de contenção.

Investir em orquestração, automação e resposta de segurança (SOAR) e em XDR, para ajudar a melhorar os tempos de detecção e resposta.
Junto com IA e automação para segurança, os recursos de XDR podem ajudar a reduzir significativamente os custos médios de violação de dados e os ciclos de vida de violação. De acordo com o estudo, as organizações com XDR implementada encurtaram o ciclo de vida da violação em 29 dias em média, em comparação com as organizações que não implementaram XDR, com uma economia de custos de US$ 400.000. SOAR e informações de segurança e software de gerenciamento e eventos (SIEM), serviços de detecção e resposta gerenciadas e XDR podem ajudar sua organização a acelerar a resposta a incidentes com automação, padronização de processos e integração com suas ferramentas de segurança existentes.

Utilizar ferramentas que ajudam a proteger e monitorar os terminais e os funcionários remotos.
No estudo, as violações onde o trabalho remoto foi um fator que causou a violação custaram quase 1 milhão de dólares a mais do que as violações onde o trabalho remoto não foi um fator. O gerenciamento unificado de terminais (UEM), a detecção e resposta de terminais (EDR) e os produtos e serviços de gerenciamento de identidade e acesso (IAM) podem ajudar a fornecer às equipes de segurança uma visibilidade mais profunda de atividades suspeitas. Esta supervisão envolve trazer seus próprios dispositivos (bring your own devices, BYOD) e notebooks da empresa, desktops, tablets, dispositivos móveis e IoT, incluindo terminais aos quais a organização não tem acesso físico. UEM, EDR e IAM aceleram a investigação e o tempo de resposta para isolar e conter os danos nas violações em que o trabalho remoto foi determinante.

Criar e testar playbooks de resposta a incidentes para aumentar a resiliência cibernética.
Duas das formas mais eficazes de mitigar o custo de uma violação de dados são a formação de uma equipe de resposta a incidentes (RI) e testes contínuos do plano de RI. As violações em organizações com equipes de RI que testam regularmente seu plano geraram uma economia de US$ 2,66 milhões em comparação com as violações em organizações sem equipe de RI ou que não testam seu plano de RI. As organizações podem responder rapidamente para conter as consequências de uma violação, estabelecendo um playbook detalhado sobre incidentes cibernéticos. Teste rotineiramente esse plano por meio de exercícios de simulação ou execute um cenário de violação em um ambiente simulado, como um cyber range.

Exercícios de simulação de adversários, também conhecidos como exercícios de equipe vermelha (red team exercises), podem aumentar a eficácia das equipes de RI descobrindo caminhos de ataque e técnicas que podem falhar e identificando lacunas em suas capacidades de detecção e resposta. Uma solução de gerenciamento de superfície de ataque pode ajudar as organizações a melhorar sua postura de segurança ao localizar pontos de exposição previamente desconhecidos por meio de simulações de uma autêntica experiência de ataque.

As recomendações de práticas de segurança são para fins educativos e não garantem resultados.

Sobre o Ponemon Institute e a IBM Security

Ponemon Institute

O Ponemon Institute se dedica à pesquisa e educação independentes que promovem práticas responsáveis de gerenciamento de informações e privacidade dentro das empresas e do governo. Nossa missão é conduzir estudos empíricos de alta qualidade sobre questões críticas que afetam a gestão e a segurança de informações sensíveis sobre pessoas e organizações.

O Ponemon Institute mantém rígidos padrões de confidencialidade de dados, privacidade e pesquisa ética, e não coleta nenhuma informação pessoalmente identificável de indivíduos ou informações identificáveis da empresa em pesquisas comerciais. Além disso, padrões de qualidade rigorosos garantem que não sejam feitas aos participantes perguntas irrelevantes, impróprias ou que fujam do tema do estudo.

IBM Security

A IBM Security oferece um dos portfólios mais avançados e integrados de segurança empresarial: produtos e serviços. O portfólio, respaldado pela renomada pesquisa do IBM Security X-Force®, fornece soluções de segurança para ajudar as organizações a fomentar a segurança em todos os seus negócios para que possam prosperar frente às incertezas.

A IBM opera uma das mais amplas e profundas organizações de pesquisa, desenvolvimento e entrega de segurança. Monitorando mais de 4,7 trilhões de eventos por mês em mais de 130 países, a IBM detém mais de 10.000 patentes de segurança. Para saber mais, visite ibm.com/br-pt/security. Participe da conversa na IBM Security Community.

Se você tiver dúvidas ou comentários sobre este relatório de pesquisa, inclusive para obter permissão para citar ou reproduzir o relatório, entre em contato por carta, telefone ou e-mail:

Ponemon Institute LLC
Att.: Research Department
2308 US 31 North
Traverse City
Michigan 49686 USA

1-800-887-3118 (EUA)
research@ponemon.org

Dê os próximos passos

Soluções de segurança zero trust
Garanta a segurança de cada usuário, dispositivo e conexão.
Saiba mais

Gerenciamento de identidade e acesso
Conecte cada usuário, API e dispositivo a cada aplicativo com segurança.
Saiba mais

Segurança dos dados
Descubra, classifique e proteja dados empresariais sigilosos.
Saiba mais

Orquestração de segurança, automação e resposta a ameaças
Agilize a resposta a incidentes com orquestração e automação.
Saiba mais

Informações de segurança e gerenciamento de eventos
Adquira visibilidade para detectar, investigar e responder a ameaças.
Saiba mais

Segurança na nuvem
Integre segurança na sua jornada para a multinuvem híbrida.
Saiba mais

Segurança de terminais
Proteja dispositivos, usuários e organizações contra ataques sofisticados.
Saiba mais

Serviços de segurança cibernética
Reduza o risco com serviços de consultoria, nuvem e segurança gerenciada.
Saiba mais

Resposta a incidentes e inteligência de ameaças
Gerencie e responda proativamente às ameaças à segurança.
Saiba mais

Agende consultoria particular com um especialista do IBM Security X-Force
Agendar agora

IBM Brasil Ltda.
Rua Tutóia, 1157
CEP 04007-900
São Paulo, SP

Produzido nos
Estados Unidos da América
julho de 2022