Insights

Sumário executivo

Tendências de Ransomware 2024

Edição LATAM

De acordo com o Relatório sobre Tendências em Proteção de Dados 2024, que entrevistou líderes e implementadores de TI em 10 países ao redor do mundo:

- Apenas 25% das organizações acreditam que não foram atacadas por ransomware em 2023
- 49% afirmaram que foram atingidas entre uma e três vezes naquele ano
- 26% das organizações declararam que foram atacadas quatro vezes ou mais

Devido às altas taxas de ataques mostradas neste relatório imparcial a cada ano, o Relatório sobre Tendências de Ransomware foi encomendado para entender melhor os ataques, as recuperações e as lições aprendidas por meio uma pesquisa anônima duplo-cega com líderes de TI comprovados e com experiência em primeira mão com esses ataques virtuais para se aprofundar em um estudo adicional: O Relatório sobre Tendências de Ransomware 2024.

Por dentro das tendências de ransomware em 2024

O Relatório sobre Tendências de Ransomware 2024 é a terceira publicação anual de uma pesquisa imparcial conduzida por uma equipe de analistas independentes que entrevistaram organizações anônimas, mas comprovadas, que sofreram pelo menos um ataque virtual bem-sucedido nos últimos 12 meses. A cada ano, esse relatório seleciona 1.200 respostas, com uma divisão intencional de cerca de 400 indivíduos em três funções-chave que são responsáveis por parte da estratégia de resiliência virtual de uma organização:

- **CISO ou executivo sênior:** Responsável pela estratégia de resiliência virtual de uma organização
- **Profissional de segurança da informação:** Responsável pela prevenção e detecção de eventos virtuais
- **Administrador de backup:** Responsável pela proteção e recuperação contínuas de dados de TI

O ransomware continua a ser uma preocupação crescente para todos no setor de TI. A Gartner prevê globalmente um aumento planejado de 3,5% nos orçamentos gerais de TI para 2024. Os entrevistados da LATAM nesta pesquisa esperam aumentos de orçamento de:

6.2%

de aumento no orçamento para tecnologias de prevenção e detecção cibernéticas

5.9%

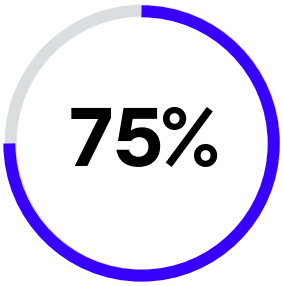
de aumento no orçamento para tecnologias de recuperação, como backup e continuidade dos negócios/recuperação de desastres (BCDR)

Os gastos geral de TI estão em alta, aumentando os orçamentos de resiliência virtual para quase o dobro do aumento geral nos gastos com TI. Assim, os investimentos em backup e segurança virtual estão consumindo "mais do que sua parte" do aumento dos investimentos em TI, enquanto outras áreas estão sendo despriorizadas para lidar com ameaças virtuais. Cópias de backup limpas, em que se presume que os dados tenham sobrevivido contra ataques e não incluam código malicioso.

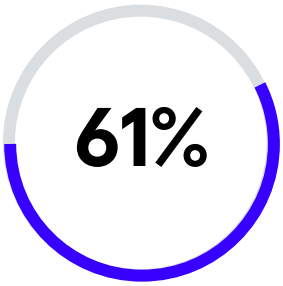
63% das organizações não estão alinhadas

Pelo terceiro ano consecutivo, mais da metade das organizações – 69% na LATAM – acreditam que uma "melhoria significativa" ou uma "reformulação completa" seja necessária para que as equipes de backup e cibernética das organizações estejam alinhadas.

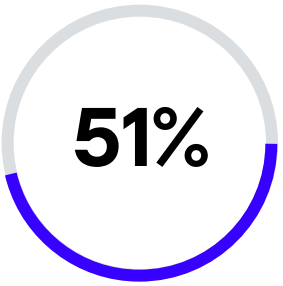
Globalmente, das três funções pesquisadas, os administradores de backup foram os menos satisfeitos com o alinhamento de suas equipes.



dos administradores de backup acreditam que uma reformulação completa de seu sistema é necessária



dos profissionais de segurança estão procurando mudanças em sua organização



dos CISOs ou outros executivos equivalentes têm preocupações relacionadas ao alinhamento organizacional

A recuperação não será simples

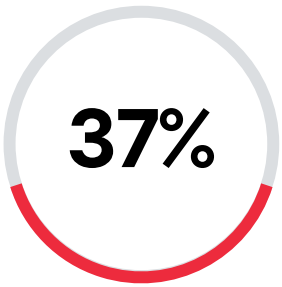
De acordo com os participantes da pesquisa, as duas equipes mais notificadas para iniciar esforços de correção são os executivos responsáveis pela prevenção e correção e a equipe de backup de TI. Isso é seguido rapidamente por especialistas em segurança cibernética e pela equipe geral de gerenciamento de riscos da organização.

89% das organizações pesquisadas afirmaram que também utilizaram terceiros durante seu processo de recuperação, sendo estes os quatro tipos de especialistas os mais utilizados:

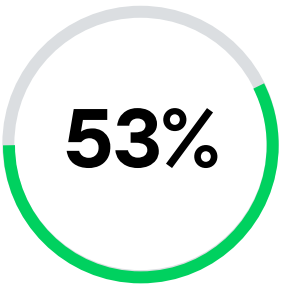
- **Fornecedores de software de segurança**
- **Fornecedores de software de backup**
- **Especialistas em segurança para análise forense**
- **Revendedores, parceiros ou provedores de serviços**

Espere perder 18% dos seus dados em caso de ataque cibernético

Duas das estatísticas mais impactantes das 1.200 lições globais que aprendemos em 2023 são:



dos dados de produção foram criptografados com sucesso por agentes maliciosos em ataques do ano passado



dos dados afetados eram recuperáveis após serem criptografados em um ataque de ransomware

Infelizmente, se apenas 53% dos seus dados eram recuperáveis, isso significa que 47% não eram. Portanto, 17% dos seus dados de produção eram irrecuperáveis. Organizações de todos os tamanhos participaram desta pesquisa e, surpreendentemente, revelaram que nem o tamanho da organização, nem a localidade tiveram um efeito significativo em suas taxas de ataque ou recuperabilidade. Todas as organizações foram atingidas aproximadamente na mesma quantidade em todo o mundo e enfrentaram uma quantidade semelhante de danos.

As organizações também podem se surpreender ao descobrir que não houve uma variação significativa entre os efeitos de data center encontrados em escritórios remotos vs. filiais, ou mesmo em dados hospedados em uma nuvem pública vs. privada.

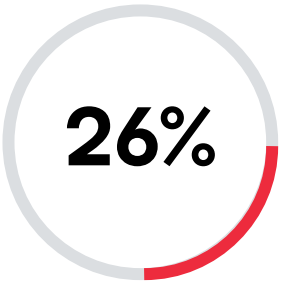
Vocês pagaram? Deu certo?

Duas perguntas fundamentais feitas a cada ano nesta pesquisa são:

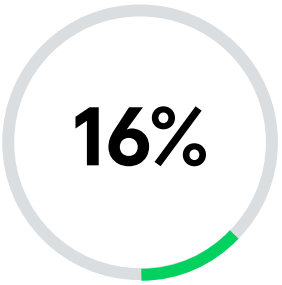
- **Vocês pagaram o resgate?**
- **Vocês conseguiram recuperar os dados?**

Em 2023 dentro da LATAM:

Pagaram e conseguiram recuperar seus dados após o ataque



Pagaram, mas não conseguiram recuperar os dados perdidos no ataque



Conseguiram recuperar os dados *sem pagar* o resgate exigido

Os resultados globais foram semelhantes:

- 54% pagaram e conseguiram recuperar seus dados após o ataque
- 27% pagaram, mas não conseguiram recuperar os dados perdidos no ataque
- 15% conseguiram recuperar os dados sem pagar o resgate exigido

Para os 4% restantes, nenhum resgate foi pedido. Essas estatísticas são notáveis, principalmente porque mostram que **uma em cada quatro organizações que pagaram o resgate não conseguiram recuperar os dados *mesmo após pagarem***.

Há mais em um ataque do que o resgate

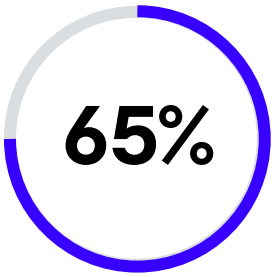
73% das organizações acreditam que têm seguro, embora 21% dessas apólices de seguro excluam especificamente o ransomware. No entanto, os custos de serviços de prevenção, detecção, recuperação e o próprio resgate estão longe de ser os únicos fatores financeiros que podem impactar a sua organização em caso de ataque de ransomware. Na verdade, de todas as respostas à pesquisa deste ano, apenas 1 em cada 9 organizações (11%) declarou que o pagamento do resgate representou a parte mais significativa do impacto financeiro geral na organização. Para o resto das vítimas virtuais, o impacto financeiro geral foi substancialmente maior do que "apenas" o resgate em si.

65% das organizações pagaram o resgate com o seguro

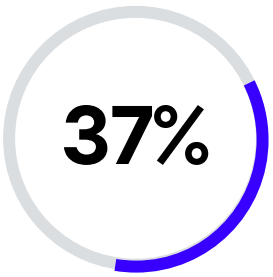
Em relação às políticas internas das empresas em 2023, apenas algumas organizações (14%) não tinham uma política de pagamento ou não. Embora a maioria das organizações tivesse uma política, havia ***sentimentos quase iguais em relação a pagar (49%) versus não pagar (38%)***.

Independentemente de terem ou não uma política, não chega a surpreender que, enquanto apenas uma minoria das organizações tinha uma política para pagar, 76% acabaram pagando. Dito isso, 66% pagaram com o seguro e outros 17% tinham seguro, mas optaram por pagar sem abrir um sinistro. Isso significa que, em 2023, 83% das organizações tinham um seguro que poderiam ter usado em caso de evento virtual.

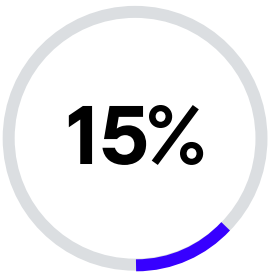
Essas opções diminuirão à medida que o seguro cibernético continuar a mudar em resposta a sinistros cada vez maiores. Na última renovação:



das empresas sofreram aumento no prêmio em resposta à mudança do panorama de TI



tiveram a franquia aumentada devido a ataques virtuais e ransomware se tornarem cada vez mais comuns



viram seus benefícios de cobertura reduzidos à medida que as seguradoras tentavam se proteger da ameaça crescente representada pelo ransomware

Os vilões virtuais querem seus backups

Da mesma forma que o manual da sua equipe de prevenção espera um backup limpo e recuperável, o manual do vilão virtual pretende desabilitar sua capacidade de recuperar seus próprios dados. Infelizmente, em muitos ataques, os invasores conseguem desabilitar sua capacidade de reagir. Assim, os dados mostram que apenas 16% das empresas conseguiram se recuperar sem pagar. Em média, 36% dos repositórios de backup foram afetados por um ataque bem-sucedido.

72% não têm um plano de recuperação

Em 95% das organizações — que tinham uma equipe com um plano —, os dois aspectos mais comuns de seus manuais de resposta a incidentes eram a garantia de dados ***limpos*** e ***recuperáveis***.

Isso explica por que 28% das organizações na LATAM têm uma infraestrutura alternativa em seus planos, o que infelizmente significa que os outros 72% não têm um plano para o destino da recuperação após uma crise em nível de site.

No entanto, os ataques cibernéticos afetam não apenas a organização e suas equipes, mas também os indivíduos. Entre os participantes deste ano, os principais efeitos pessoais incluíram o aumento da carga de trabalho, estresse e outros fatores humanos que a maioria das organizações já luta para equilibrar ou mitigar mesmo em dias "normais".

O ataque será pior do que você imagina e custará mais do que você está esperando

Com 37% dos dados afetados por um ataque virtual e somente 53% dos dados afetados sendo recuperáveis, as empresas podem esperar perder 17% dos dados por ataque virtual. Além disso, o resgate representa, em média, apenas 37% do impacto financeiro geral, enquanto apenas 68% do impacto global é, de alguma forma, recuperável por meio de seguro ou outros meios. Tudo isso se junta para sobrecarregar ainda mais o orçamento da organização.

2024 não é imutável o suficiente

Em 2024, é razoável que as empresas adotem o storage imutável em seus discos locais, complementado por repositórios de nuvem imutáveis e fitas isoladas. Infelizmente, mesmo entre aqueles que sofreram pelo menos um ataque virtual no passado, apenas 76% usam discos seguros no local e apenas 80% usam nuvens imutáveis.

Apenas 49% do storage de backup geral da organização é imutável.

Dito isso, é encorajador que as organizações estejam adotando a regra padrão do setor 3-2-1 de ter vários tipos de mídia, independentemente de esses tipos de mídia serem imutáveis ou não. Em 2024, além dos repositórios de disco locais, 45% dos dados de produção ainda são retidos em pelo menos uma fita, enquanto 52% também são replicados para uma nuvem.

Este resumo da pesquisa é baseado em 1.200 respostas de participantes, incluindo 250 da região LATAM, todos eles líderes de TI imparciais e implementadores responsáveis pelas estratégias de resiliência cibernética de suas organizações, incluindo CISOs, profissionais de segurança de TI e administradores de backup. A pesquisa foi realizada no início de 2024 e publicada em junho do mesmo ano. Os dados foram selecionados e os sentimentos foram elaborados por dois ex-analistas do setor, anteriormente da ESG e da Gartner, com 70 anos combinados em proteção de dados.

Perguntas sobre esta pesquisa e insights/ativos publicados dela derivados podem ser enviados para StrategicResearch@veeam.com

A perspectiva da Veeam

Veeam® acredita que o backup seguro é a sua melhor linha de defesa contra o ransomware. A Veeam tem o compromisso de ajudar as empresas a minimizar o tempo de inatividade e a perda de dados para que elas nunca tenham que pagar resgates caríssimos. Somente a Veeam oferece a maior quantidade de opções de recuperação do mercado e um formato de dados verdadeiramente portátil, possibilitando que você se recupere em qualquer lugar: do físico ao virtual, entre nuvens ou até da nuvem para um data center local. Não existe uma solução mágica para resolver o seu problema de ransomware, e é por isso que a Veeam adota uma abordagem multicamadas para a proteção contra ransomware e a recuperação. Para saber mais, visite https://www.veeam.com/ransomware-protection.html

Sobre a Veeam Software

Veeam®, líder global Nº 1 do mercado em proteção de dados e recuperação de ataque de ransomware, tem a missão de capacitar cada empresa não só a retornar de uma perda ou paralisação de dados, mas de retornar e avançar. Com a Veeam, as empresas alcançam a resiliência radical com segurança, recuperação e liberdade de dados para a sua nuvem híbrida. A Veeam Data Platform fornece uma solução única para ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes, que oferece tranquilidade aos líderes de TI e Segurança, mantendo suas aplicações e dados protegidos e sempre disponíveis. Com sede em Seattle, e escritórios em mais de 30 países, a Veeam protege mais de 450.000 clientes no mundo inteiro, incluindo 74% das empresas da lista Global 2.000, que confiam na Veeam para manter seus negócios em operação. A resiliência radical começa com a Veeam.

Saiba mais em http://www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e no X @veeam.