veeam Insights

Do risco à resiliência

2025 Tendências de ransomware e estratégias proativas

Sumário executivo:

Avaliando ameaças e defesas contra ransomware em 2025

Os ataques de ransomware estão evoluindo, crescendo mais rápido e mais sofisticados do que nunca. Uma coisa é certa: **A ameaça do ransomware continuará a impactar as organizações de forma generalizada em 2025 e nos anos seguintes.** Seja originados por grupos já consolidados ou por um número crescente de agentes de ameaça individuais, a falta de preparação adequada pode resultar em perdas consideráveis de tempo e dinheiro para a organização, além de preiudicar a confiança entre as partes interessadas.

Para ai udar a lidar com essas ameaças cibernéticas persistentes, nosso Relatório de Risco à Resiliência em 2025 mostra várias medidas acionáveis que as empresas podem tomar para mitigar o risco e se recuperar mais rapidamente de um ataque. **Entrevistamos 1.300 organizações em todo o mundo** para avaliar como os CISOs (Chief Information Security Officers), profissionais de segurança e líderes de TI estão se recuperando de ameaças cibernéticas.

As estratégias adotadas pelas empresas que se recuperaram mais rapidamente dos ataques refletem um conjunto de melhores práticas em resiliência cibernética, as quais todas as organizações deveriam considerar implementar.

Há boas notícias. Em comparação com nossa pesquisa de 2024,[1] **a porcentagem de empresas impactadas por pelo menos um ataque de ransomware que resultou em criptografia ou exfiltração de dados diminuiu ligeiramente, de 75% para 69%.** Essa redução provavelmente decorre da continuidade das organizações em melhorar suas práticas de preparação e resiliência, além do aumento da colaboração entre as equipes de TI e segurança. Os governos também se uniram para desmantelar os principais grupos de ransomware, forçando os agentes de ameaça a se adaptarem e alterarem suas estratégias de ataque de forma mais abrangente.

Nossa análise revela **seis tendências principais que moldam o cenário de ameaças de ransomware em 2025** e os insights baseados em dados que podem ajudar as empresas a aumentar a resiliência. Desde as táticas de gato e rato e o aumento da exfiltração de dados até a queda nos pagamentos de resgate e o crescimento da colaboração entre as partes interessadas, analisamos o cenário de ameaças persistentes e como as organizações bem-sucedidas conseguem minimizar os riscos e impactos do ransomware.

1.300

Organizações em todo o mundo foram entrevistadas pela Veeam

6%

Menos empresas impactadas por pelo menos um ataque de ransomware

As organizações precisam fazer a transição da segurança reativa para **estratégias proativas de resiliência cibernética** para enfrentar os desafios do ransomware, utilizando a preparação, a resposta ágil e as medidas de recuperação seguras para mitigar os riscos.

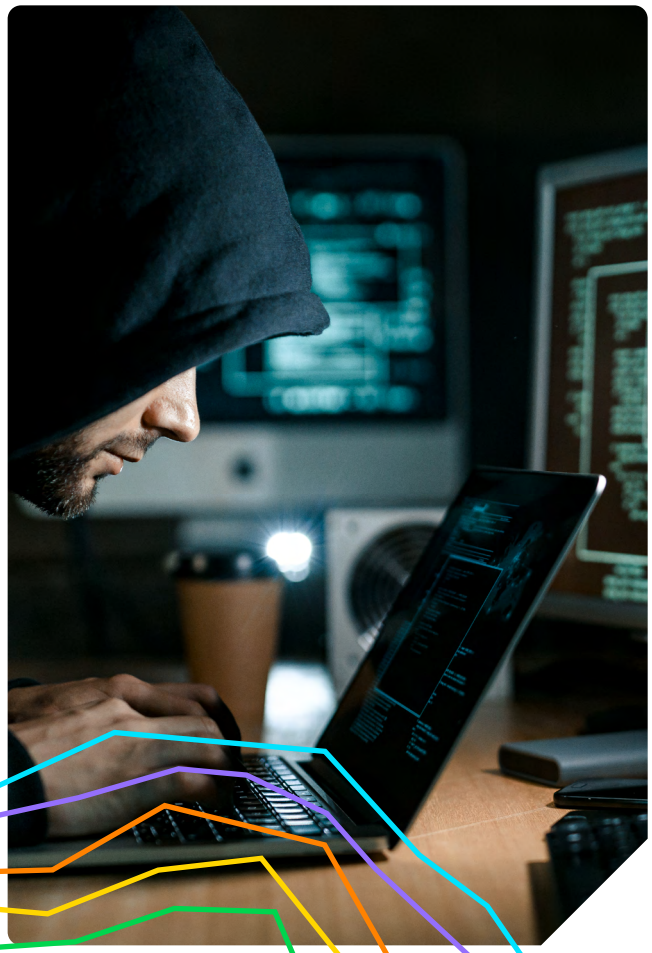
6 principais tendências de ransomware para observar em 2025

1. A aplicação da lei obriga os atores de ameaça a se adaptarem
2. Aumentam os ataques de exfiltração de dados
3. Os pagamentos por ransomware estão diminuindo
4. Consequências legais emergentes do pagamento de resgate
5. Colaboração reforça resiliência contra ransomware
6. Os orçamentos aumentam para segurança e recuperação, mas é preciso mais

A aplicação da lei obriga os atores de ameaça a se adaptarem

TREND# 1

Em 2024, as autoridades lançaram várias operações bem-sucedidas para derrubar grupos proeminentes de ameaças cibernéticas. A remoção desses grupos maiores é, sem dúvida, um avanço positivo na defesa contra ameaças cibernéticas. No entanto, **o número de grupos menores e de atores de ameaças "lobo solitário" tem aumentado, ampliando a propagação de ataques.** Alguns grupos também mudaram seu objetivo a jusante, evitando infraestrutura crítica para reduzir o escrutínio das autoridades policiais e visando pequenas e médias empresas (PMEs) que geralmente têm defesas cibernéticas mais fracas.



Alguns dos maiores grupos que foram encerrados, desapareceram ou cessaram a operação incluem:

- **LockBit**, um grupo de ransomware como serviço (RaaS), foi desmantelado graças aos esforços das forças de segurança, liderados pela Agência Nacional do Crime do Reino Unido, em colaboração com o FBI e a Europol.[2]
- **BlackCat**, um grupo RaaS que o FBI havia interrompido em 2023,[3] encerrou suas operações em março de 2024, após realizar um ataque bem-sucedido contra a Change Healthcare, resultando em um pagamento de resgate estimado em mais de 22 milhões de dólares americanos.[4]
- **Black Basta**, que parecia encerrar suas operações em 2025, foi afetado pelo aumento do escrutínio das autoridades após a divulgação de registros de bate-papo vazados. Esse escrutínio surgiu após o grupo realizar um ataque ao US Health System Ascension, que afetou 140 hospitais em 19 estados.[5]

Aumentam os ataques de exfiltração de dados

TREND# 2

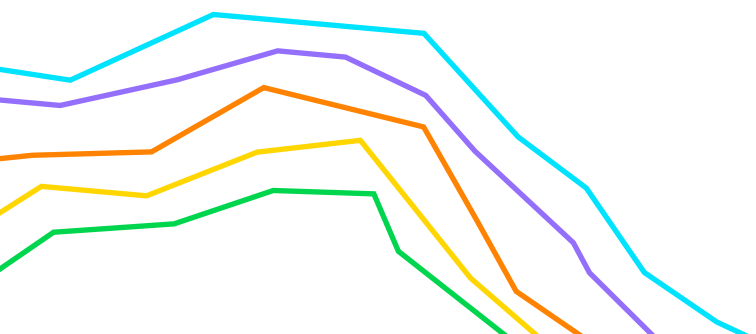
À medida que o cenário de ameaças evolui, os agentes de ameaças continuam a mudar suas táticas. Notavelmente, embora as táticas de exfiltração sejam normalmente usadas em conjunto com a criptografia de dados, o número de vítimas exclusivas de exfiltração que pagaram um resgate aumentou durante o 4º trimestre.[6]

A exfiltração reflete uma abordagem de "esmagar e agarrar" que é comum em ataques de ransomware tradicionais antes da criptografia. Isso também ocorre com aplicativos baseados em nuvem e infraestrutura de nuvem mal protegidos. Juntamente com essa mudança em direção à exfiltração de dados — e à extorsão dupla, que combina a criptografia para bloquear o acesso e a publicação de dados exfiltrados confidenciais — **também houve uma redução no tempo de permanência, ou seja, o intervalo entre o comprometimento e a execução do ataque, com muitos incidentes ocorrendo em apenas algumas horas.**

No segundo trimestre de 2024, a Coveware by Veeam observou que dois dos três principais adversários de ransomware naquele trimestre tiveram um tempo médio de permanência inferior a 24 horas.[7] Essa queda é significativa em relação aos trimestres anteriores, e a tendência se manteve até o quarto trimestre.

Quando os atores de ameaças obtêm acesso às redes das vítimas, eles tendem a usar técnicas de movimento lateral. Eles buscam facilidade de exfiltração ou um objetivo específico, como comprometer os hipervisores VMware ESXi, para coagir as vítimas a pagar o resgate. Essas estratégias eficientes e bem ensaiadas geralmente resultam em ataques mais rápidos que podem ser difíceis de detectar e conter.

Com muita frequência, asorganizações que têm uma postura de segurança cibernética fraca e arquiteturas de rede complexas são particularmente vulneráveis à exfiltração de dados e ameaças cibernéticas relacionadas.



Os pagamentos de ransomware estão diminuindo

TREND# 3

Felizmente, o valor total dos pagamentos de ransomware diminuiu em 2024 em comparação com 2023.[8] Mais de um terço das empresas afetadas por um ataque de ransomware (36%) optaram por não pagar o resgate, e 25% conseguiram recuperar seus dados sem precisar pagar.

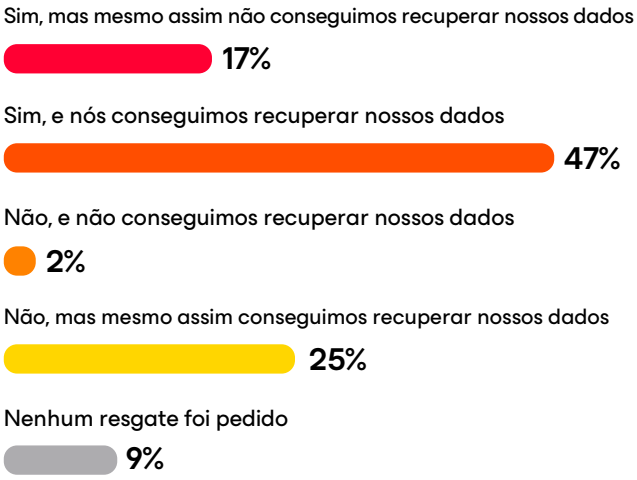
Entre os que pagaram, 82% pagaram menos do que o resgate inicial e 60% pagaram menos da metade desse valor. Esses dados também corroboram o que a Coveware by Veeam observou diretamente em seu trabalho com as empresas impactadas durante 2024. No quarto trimestre, o **pagamento médio de resgate caiu 45%**, atingindo aproximadamente US$ 110 mil, o nível mais baixo registrado até hoje.

Apenas 25% das empresas que trabalham com resposta a incidentes com especialistas da Coveware by Veeam pagaram um resgate, o que representa um "marco significativo na luta contra o ransomware".[9]

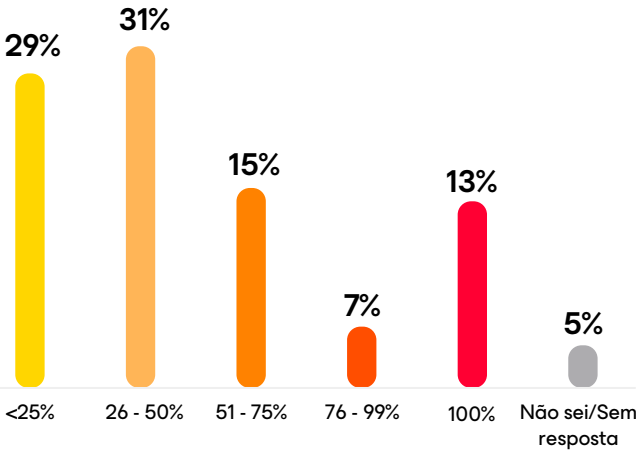
Em comparação com as empresas que utilizaram a Coveware by Veeam, outras organizações tinham 156% mais chances de pagar um resgate. Isso sugere **que trabalhar com terceiros experientes para a resposta a incidentes se correlaciona com menos pagamentos de resgate, pagamentos de resgate menores e práticas mais resilientes em geral.**

As vítimas estão se tornando cada vez mais relutantes em pagar resgates, pois não têm confiança de que os invasores realmente liberarão seus dados após o pagamento. As empresas também melhoraram proativamente seus próprios planos de resposta a incidentes, inclusive por meio do uso de backups imutáveis.

Sua empresa pagou resgate para recuperar seus dados?



Porcentagem do resgate pago



Consequências legais emergentes do pagamento de resgate

TREND#4

Pagar um resgate pode ser muito caro, pois incentiva os invasores e confirma que uma organização vulnerável está disposta a pagar. Na verdade, **entre aqueles que pagaram um resgate, 69% foram atacados mais de uma vez.** As organizações que não tomam medidas para reforçar sua capacidade de defesa e resposta ficam com menos opções quando um ataque ocorre.

69%

das organizações que pagaram resgate foram atacadas mais de uma vez

A evolução das iniciativas regulatórias e de relatórios, juntamente com a aplicação coordenada pelas autoridades em diversas jurisdições, também desempenhou um papel importante no declínio dos pagamentos de resgate. Notavelmente, a Iniciativa Internacional de Combate ao Ransomware (CRI), lançada pelo governo dos EUA em 2021, e sua força-tarefa afiliada reúnem 68 países com o objetivo de interromper o ecossistema de Ransomware e desenvolver abordagens políticas comuns.[10]

Em 2023, 40 membros do CRI assinaram um compromisso governamental conjunto para "desencorajar fortemente qualquer pessoa a pagar uma demanda de ransomware".[11] Alguns países também propuseram legislação que proíbe organizações do setor público de pagar resgates — como o Reino Unido em janeiro de 2025[12] — e dois estados dos EUA (Flórida e Carolina do Norte) aprovaram essas leis.[13]

O FBI desencoraja as organizações de pagar resgates, [14] e o Departamento do Tesouro dos EUA aconselha que pode haver riscos de sanções associados a pagamentos feitos a entidades bloqueadas pelo Escritório de Controle de Ativos Estrangeiros (OFAC).[15] As organizações globais também devem considerar outros riscos de pagamento e requisitos de conformidade.

Colaboração reforça resiliência contra ransomware

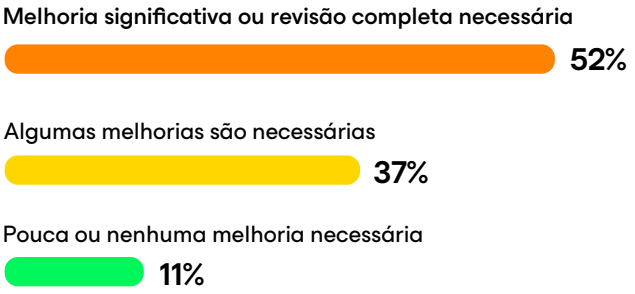
TREND# 5

Aprimorar a colaboração e a comunicação entre as equipes de operações de TI e segurança também foi fundamental para que as empresas aumentassem sua resiliência cibernética. No entanto, a maioria dos entrevistados (52%) disse que uma melhoria significativa ou uma reformulação completa é necessária para alinhar essas equipes. E apenas 11% disseram que pouca ou nenhuma melhoria é necessária.

Ao mesmo tempo, as plataformas e empresas de tecnologia estão fazendo parcerias para agregar informações sobre ransomware e fornecer serviços que ajudem as empresas a melhorar as defesas. Relatar ransomware e outros ataques virtuais às autoridades policiais e regulatórias, bem como às redes de parceiros emergentes e trocas de compartilhamento de informações do setor, fortalece as defesas coletivas.

> "Estamos em um propósito comum de segurança, e temos que fazer isso juntos. Então, não acho que haja como chegarmos a um futuro ciberseguro sem que as entidades públicas e privadas, e suas propostas de valor, se unam para encontrar algumas soluções."[16]
>
> **Sue Gordon**
>
> Ex-Diretora Adjunta Principal da Inteligência Nacional dos EUA
>
> Assista à entrevista completa com Sue Gordon e Gil Vega, CISO da Veeam, aqui

Alinhamento de Operações de TI e Equipes de Segurança



Os orçamentos aumentam para segurança e recuperação, mas é preciso mais

TREND# 6

De maneira crítica, isso permite que fornecedores e agências compartilhem indicadores de comprometimento e estratégias de mitigação com outras partes do ecossistema.

Embora muitas técnicas de defesa contra ransomware tenham mostrado sinais de melhora, **algumas empresas não estão aumentando os orçamentos de segurança e recuperação com rapidez suficiente** para acompanhar o crescimento do cenário de ameaças. As equipes de segurança também estão dispersas devido à grande variedade de ransomware e outros vetores de ataque que enfrentam.

No geral, as organizações tendem a dedicar um pouco mais de recursos à segurança (31% do orçamento de TI em média) em vez da recuperação (28% em média), o que sugere uma vulnerabilidade potencial no desenvolvimento de resiliência proativa. Chief Information Officers (CIOs) e CISOs devem encontrar o equilíbrio apropriado com base nas necessidades de sua organização ao alocar o orçamento para cada área. Os resultados da pesquisa indicam que **o subinvestimento em segurança ou recuperação pode enfraquecer a capacidade das empresas de se proteger e responder a ataques de ransomware.** A falta de foco na recuperação, em particular, pode custar tempo e recursos preciosos, especialmente quando os agentes maliciosos atacam repositórios de backup.

No lado positivo, **94% das organizações aumentaram o orçamento de recuperação para 2025, e 95% o aumentaram para prevenção,** o que indica uma prioridade crescente em fortalecer a resiliência cibernética.

Perguntas que o Conselho de Administração fará após um ataque de ransomware

Como o ataque ocorreu?

Detalhe a causa do ataque, o escopo, E impacto.

O que foi feito para eliminar a ameaça?

Descreva se um resgate foi pago (em caso afirmativo, como) e as medidas tomadas para remover a ameaça e recuperar.

Quais sistemas, dados e operações de negócios foram afetados?

Descreva os impactos do ataque, incluindo as consequências financeiras e reputacionais.

O que foi feito para melhorar a resiliência cibernética e prevenir ataques futuros?

Identificar medidas tomadas para fortalecer a segurança e a recuperação, como mudanças nas medidas de governança ou prioridades de investimento em segurança cibernética.

94%

das empresas aumentaram o orçamento de recuperação para 2025

95%

das organizações aumentaram o orçamento de recuperação como medida preventiva

Principais Fatores de Sucesso:

O que as organizações com melhores resultados têm em comum

Quando se deparam repentinamente com um ataque de ransomware, as organizações precisam agir de forma imediata e coordenada. O tempo é essencial, por isso é fundamental avaliar o escopo da violação, conter a ameaça e iniciar sua resposta a incidentes em questão de minutos.

Analisar os atributos comuns de organizações com resultados mais bem-sucedidos e menos bem-sucedidos de um ataque de ransomware pode fornecer insights para melhorar suas defesas virtuais.

Essa grande lacuna de sucesso levanta a questão:

Por que tantas organizações tiveram dificuldades para lidar com uma ameaça cibernética tão generalizada?

Examinando os resultados da pesquisa, várias áreas de deficiência se correlacionam com uma menor resiliência contra ransomware. Além disso, ao analisar quais lições as organizações disseram ter aprendido no ano passado após serem atacadas, vários padrões entram em foco e podem ser aplicados para melhorar a defesa contra ransomware e a recuperação.

Uma organização foi considerada mais bem-sucedida se cinco dos nove critérios a seguir fossem atendidos.

- ✔ A organização não pagou um resgate e conseguiu recuperar os dados.
- ✔ A organização não foi atacada várias vezes.
- ✔ A organização não sofreu impactos significativos.
- ✔ A organização não tinha dados de produção criptografados.
- ✔ A organização foi classificada como preparada ou completamente preparada pós-ataque.
- ✔ A organização recuperou a funcionalidade de mais de 80% de seus servidores.
- ✔ Mais de 90% dos dados afetados da organização foram recuperados.
- ✔ Menos de 20% das plataformas de produção da organização foram afetadas.
- ✔ Menos de 10% dos repositórios de backup foram modificados ou excluídos quando o agente malicioso tentou realizar a ação.

Roteiros de ransomware aumentam a preparação para ataques

A confiança pré-ataque nem sempre corresponde à realidade: **69% das vítimas de ransomware disseram que pensavam que estavam preparadas antes de serem atacadas, mas que a confiança caiu em mais de 20% após o ataque,** destacando lacunas críticas no planejamento.

A lacuna na percepção de preparação versus realidade também foi maior para certos papéis. Em particular, a classificação de preparação dos CIOs caiu 30% após o ataque, em comparação com um declínio de 15% para os CISOs, indicando que os CISOs têm uma compreensão mais precisa da postura de segurança de sua organização.

No geral, é fundamental promover o alinhamento organizacional em torno da resiliência cibernética, medidas de preparação e procedimentos de resposta a incidentes. Isso deve incluir treinamentos e exercícios em todos os grupos aplicáveis para apoiar uma resposta consistente e coordenada durante e após um ataque.

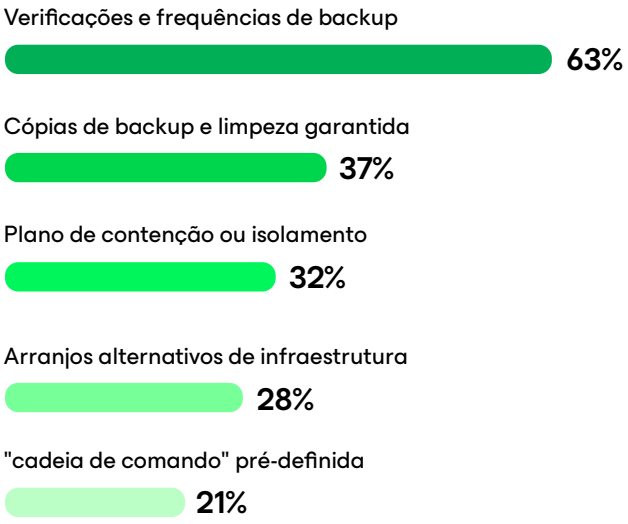
Embora 98% dos entrevistados tivessem um manual sobre ransomware, **menos da metade das empresas contava com elementos técnicos essenciais**, como verificações e frequências de backup (44%), cópias de backup e limpeza garantida (44%), arranjos de infraestrutura alternativa (37%), planos de contenção ou isolamento (32%) e uma "cadeia de comando" pré-definida (30%).

As organizações com **resultados mais bem-sucedidos apresentaram uma incidência significativamente maior de incluir esses cinco elementos-chave técnicos em seus manuais.**

estavam confiantes em seus preparativos antes de um ataque de ransomware

queda na confiança nos preparativos de sua organização após um ataque

Elementos-chave do manual para organizações mais bem-sucedidas



A recuperação de backup proativo constrói resiliência

A recuperação com backup seguro é crucial, mas é mais desafiadora do que muitos preveem. De fato, **89% das organizações tiveram seus repositórios de backup como alvo do agente da ameaça.**

E pior ainda, 34% dos repositórios de backup foram modificados ou excluídos, em média. Menos de 10% conseguiram recuperar mais de 90% dos seus servidores dentro das expectativas, e apenas 51% recuperaram a maioria dos seus servidores.

O planejamento da recuperação é crítico e envolve múltiplas etapas. As equipes de segurança e TI devem primeiro conter ou remover a ameaça cibernética, em seguida, remediar o acesso utilizando ferramentas como gerenciamento de identidade e acesso e outras soluções de segurança cibernética, para, por fim, restaurar os dados em um ambiente seguro.

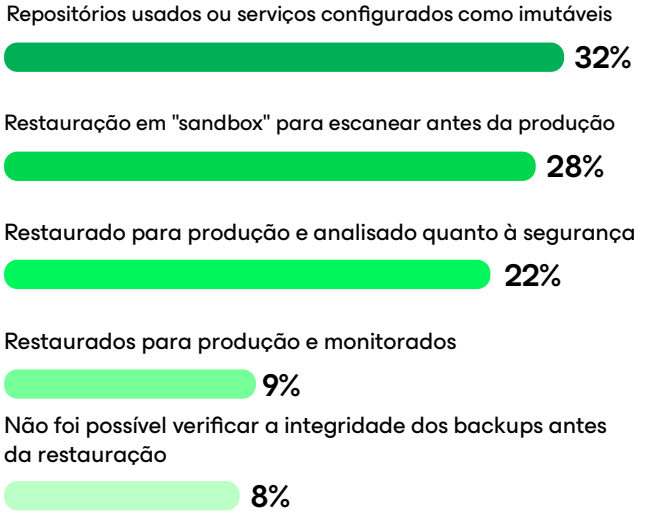
Os backups seguros também foram subutilizados como medida proativa. **Apenas 32% dos entrevistados usavam repositórios ou serviços configurados como imutáveis,** enquanto apenas 28% restauravam dados para um ambiente "sandbox" e faziam verificações de integridade. **39% dos entrevistados precisaram restaurar dados diretamente para o ambiente de produção e 8% não conseguiram verificar a integridade do backup antes da restauração.**

Os líderes de negócios e de TI devem garantir que os dados e os backups sejam verificados e estejam livres de malware antes de serem restaurados no ambiente de produção, a fim de minimizar os riscos para a empresa. Caso contrário, eles podem enfrentar uma série de consequências graves, incluindo: Reinfecção rápida, movimentação lateral, mecanismos de persistência, detonação atrasada, interrupção sustentada de negócios, violações de conformidade e muito mais.

89%

das organizações tiveram seus repositórios de backup como alvo do agente da ameaça.

Método de verificação da integridade do backup



O poder das "pessoas" na resiliência contra ransomware

Embora esses aspectos técnicos da recuperação sejam vitais, muitas empresas negligenciam os elementos cruciais de "pessoas" em seus manuais sobre ransomware.

Apenas 26% das empresas tinham um processo de decisão de pagamento de resgate para orientar uma resposta rápida às demandas de pagamento com base no impacto potencial. Muitos também não possuem procedimentos estabelecidos para informar as autoridades policiais, o que poderia ser fundamental para a recuperação e para garantir a conformidade.

Mais de um terço das organizações usou membros internos da equipe para se comunicar com os agentes de ameaças. O restante dependia de terceiros para ajudá-los, incluindo especialistas em resposta a incidentes e em negociação de resgate. Esses especialistas são indispensáveis para orientar o engajamento com base em uma compreensão detalhada do comportamento dos atores de ameaças, o que ajuda a apoiar resultados mais bem-sucedidos. Fazer com que os membros internos da equipe se comuniquem com os agentes de ameaças também pode expor inadvertidamente uma organização a riscos e ameaças adicionais.

Finalmente, apenas 30% das organizações tinham uma cadeia de comando pré-definida para lidar com ataques. A cadeia de comando ajuda a garantir as aprovações e autorizações adequadas para decisões críticas durante a resposta a incidentes, incluindo o envolvimento com agentes de ameaças ou o pagamento de um resgate.

Não importa o dia ou o horário, é sempre um mau momento para sofrer um ataque de ransomware, e é por isso que é tão importante ter um roteiro para responder a ameaças tão estressantes e sensíveis ao tempo.

26%

das organizações tinham um processo decisório de pagamento de resgate

Juntando tudo

Quando vistas em conjunto, essas medidas apontam para uma diferença fundamental de mentalidade entre as empresas que demonstraram resiliência contra ataques de ransomware no ano passado e aquelas que não demonstraram:

As organizações bem-sucedidas incorporam a resiliência cibernética como parte de sua rotina diária. Eles incorporam estratégias proativas em todas as operações diárias de TI.

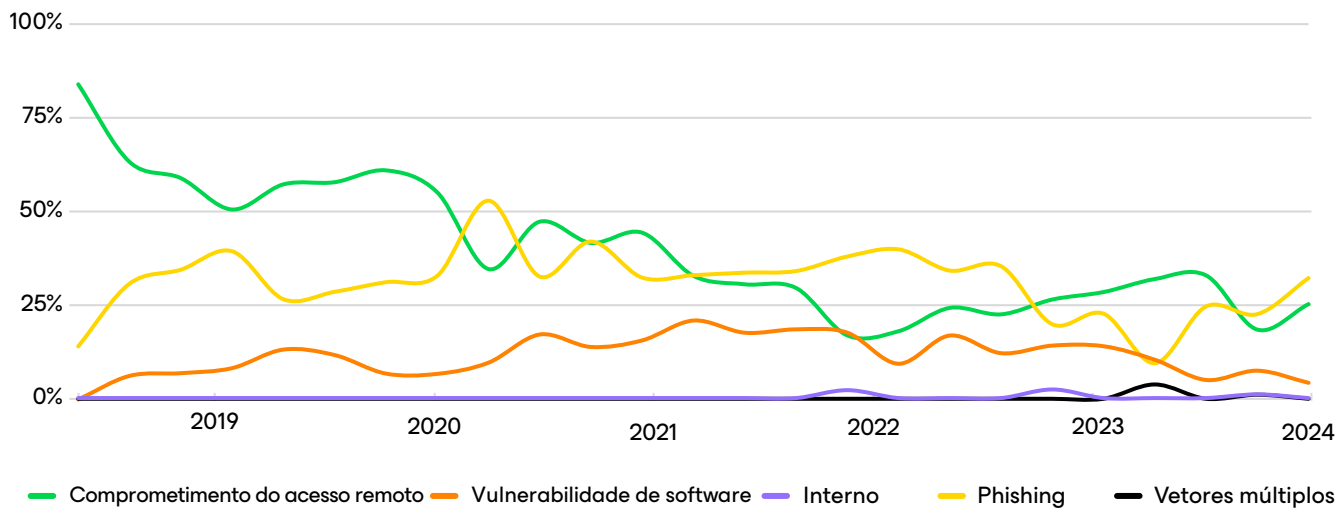
Após o ataque, as organizações mais bem-sucedidas também tiveram maior probabilidade de reforçar os programas de treinamento e conscientização dos funcionários, o que pode ajudar a mitigar ataques de engenharia social, como phishing. As políticas de atualização de software também são comumente reforçadas após o ataque para proteger contra a exploração de vulnerabilidades de software em uma base contínua. Em particular, **muitas empresas implementaram novas soluções de backup e recuperação e fizeram a transição para a nuvem ou serviços gerenciados após o ataque.** O uso dessas medidas ajuda a proteger contra vetores de ataque comuns e aumenta a resiliência.

As organizações bem-sucedidas implementaram mais elementos de recuperação proativos após o ataque do que as organizações menos bem-sucedidas.

Essas práticas proativas de defesa também são essenciais para lidar com os vetores de acesso inicial mais comuns que a Coveware by Veeam observou em seu trabalho durante o quarto trimestre, como comprometimento de acesso remoto, phishing, vulnerabilidades de software, entre outros.

Uma defesa forte contra ataques de ransomware não pode ser simplesmente criada quando um ataque ocorre. Eles devem ser uma parte fundamental das operações diárias de uma organização.

Fornecedores de soluções contra ataques de ransomware



Fonte: Coveware by Veeam, "O sucesso na aplicação da lei contra o ransomware continuará em 2025?"

Fazendo um balanço e tomando medidas

Os ataques de ransomware podem prejudicar a reputação da organização e minar a confiança entre seus clientes e usuários finais. Também pode haver graves impactos financeiros decorrentes dos custos de lidar com um ataque, incluindo tempo de inatividade operacional, perda de produtividade e possíveis multas ou ações judiciais.

Quando um ataque ocorre, as empresas devem priorizar o trabalho em equipe, a colaboração e a comunicação, mantendo a calma e a compostura enquanto implementam as estratégias de resposta definidas em seus roteiros para ataques de ransomware. Após um ataque, as organizações precisam fazer um balanço, identificar as causas principais do motivo pelo qual ele aconteceu e tomar medidas para aumentar a resiliência para evitar que isso aconteça novamente.

As organizações que tiveram recuperações mais bem-sucedidas seguiram estas melhores práticas:

- ✔ Desenvolva planos robustos de resposta a incidentes, com funções e responsabilidades claras.
- ✔ Crie uma estratégia de backup e recuperação. Siga a regra de resiliência de dados 3-2-1-1-0 para configurar os repositórios como imutáveis ou protegidos de outra forma, garantindo que os backups estejam livres de malware antes de serem restaurados.[17]
- ✔ Implemente medidas e processos de segurança proativos, como a arquitetura Zero Trust, gerenciamento de identidade e acesso (Identity and Access Management), políticas de atualização de software, soluções avançadas de detecção e resposta, além de serviços gerenciados ou em nuvem.
- ✔ Aumente o gasto em ferramentas de detecção de ameaças para prevenção e soluções de backup para recuperação. As plataformas para resiliência de dados que são integradas com ferramentas de segurança e têm recursos para prevenir ou detectar ameaças, como a Veeam Data Platform[18], ajudam muito a aprimorar a cibersegurança e a resiliência.
- ✔ Organize programas de treinamento de segurança e conscientizar todos os funcionários.

Sobre o Relatório

O relatório de ransomware deste ano pesquisou 1.300 organizações, das quais 900 sofreram pelo menos um ataque de ransomware nos últimos 12 meses, resultando em criptografia ou exfiltração de dados. Os entrevistados eram compostos por CISOs (Chief Information Security Officers) ou executivos com responsabilidades semelhantes, além de profissionais de segurança e líderes de TI das Américas, Europa e Austrália.

Acesse a nossa página inicial para saber mais sobre as soluções de segurança que podem aprimorar sua postura de cibersegurança e acelerar a recuperação, ou para conversar com um dos nossos especialistas da Veeam.

As estratégias de defesa cibernética são um problema de nível de conselho. Não espere que um ataque cibernético aconteça. Tome as medidas necessárias para minimizar os riscos e manter a resiliência.

Endnotes

1 https://go.veeam.com/ransomware-trends-executive-summary-2024-us

2 https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

3 https://www.justice.gov/archives/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

4 https://www.healthcareinfosecurity.com/blackcat-ransomware-group-seizure-appears-to-be-exit-scam-a-24521

5 https://www.databreachtoday.com/blogs/leaked-chat-logs-reveal-black-bastas-dark-night-soul-p-3828

6 https://www.veeam.com/blog/will-law-enforcement-success-against-ransomware-continue-in-2025.html

7 https://www.coveware.com/blog/2024/7/29/ransomware-actors-pivot-away-from-major-brands-in-q2-2024

8 https://www.chainalysis.com/blog/crypto-crime-ransomware-victim-extortion-2025/

9 https://www.coveware.com/blog/2025/1/31/q4-report

10 https://counter-ransomware.org/aboutus

11 https://www.centerforcybersecuritypolicy.org/insights-and-research/the-international-counter-ransomware-initiative-from-forming-and-norming-to-performing

12 https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

13 https://www.databreachtoday.com/blogs/as-states-ban-ransom-payments-what-could-possibly-go-wrong-p-3273

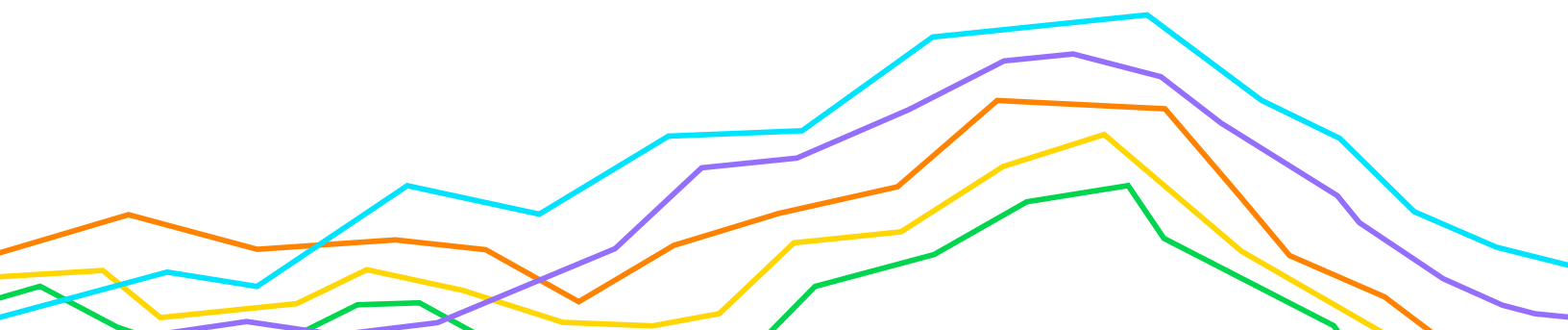
14 https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

15 https://ofac.treasury.gov/media/912981/download?inline

16 https://www.youtube.com/watch?v=Fs2xq0pb7YQ

17 https://www.veeam.com/blog/321-backup-rule.html

18 https://www.veeam.com/pt-br/products/veeam-data-platform.html



veeam Insights