Seus dados serão roubados !

(Afirmam especialistas em cibersegurança)

Por **Julian Murguia** , CTO
Ômega Krypto
16 de março de 2026

Os maiores especialistas em cibersegurança do mundo concordam que as violações de segurança são inevitáveis e afirmam que a questão não é mais **se** a sua organização será violada, mas sim **quando e com que frequência** isso acontecerá .

A isso se soma o fato de que o Relatório de Defesa Digital da Microsoft de 2025 afirma claramente que a coleta de dados foi o principal objetivo em 80% de todos os ataques cibernéticos de 2025; e seu pior pesadelo se torna realidade quando você percebe que o roubo de dados também é inevitável.

O relatório da IBM sobre o custo de uma violação de dados em 2025 confirma que *as violações ocorrem apesar de fortes controles preventivos.* À medida que a dependência digital aumenta, os ataques se tornam mais frequentes, mais sofisticados e mais dispendiosos. E o uso de Inteligência Artificial pelos atacantes só piora a situação!

Segundo a TotalAssure , o *tempo médio para detectar uma violação de segurança em 2025 foi de 181 dias* , enquanto, de acordo com o Relatório

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Global de Resposta a Incidentes da Unidade 42 da Palo Alto Networks de 2025, *os invasores levaram apenas 72 minutos para exfiltrar dados* .

A sensação de que sua organização já está no corredor da morte, aguardando o inevitável dia em que será invadida e seus dados confidenciais serão roubados, corrói seu coração e sua mente, temendo que isso possa levar sua organização ao colapso e à sua extinção.

Com essa mentalidade, os danos causados pelo roubo de dados jamais serão solucionados, pois a derrota já foi aceita.

O que mais poderia ser, senão uma admissão de derrota, quando dizem que as violações de segurança (e o roubo de dados) são inevitáveis?

Como resultado, a estratégia de cibersegurança passou da pura prevenção para a resiliência: detectar mais rapidamente, responder mais rapidamente, recuperar mais cedo e mitigar o máximo possível.

Mas a resiliência tem um ponto cego crítico:

Alguns danos simplesmente não podem ser atenuados!

Se um ataque cibernético desativar equipamentos médicos essenciais em um hospital e pacientes morrerem como consequência, nenhuma estratégia de mitigação poderá reverter tal perda.

A morte é irreversível, assim como o roubo de dados.

Uma vez que terceiros tenham acesso aos seus dados sensíveis, o dano já está feito. Os dados são copiados, armazenados e podem ser explorados indefinidamente.

Não importa a rapidez com que uma violação seja detectada; se a detecção ocorrer após a exfiltração de dados, já será tarde demais.

A recuperação pode restaurar os sistemas, mas não pode apagar as informações roubadas que estão em posse do invasor.

Os sistemas podem ser reconstruídos, as operações podem ser retomadas, o ransomware pode, por vezes, ser evitado, mas os dados roubados retêm 100% do seu valor e permanecem totalmente utilizáveis.

Mesmo que o resgate seja pago e os sistemas sejam restaurados, os invasores ainda retêm os dados roubados. O custo a longo prazo das violações de segurança costuma persistir por anos, prejudicando gravemente as organizações ou levando-as à falência.

A cibersegurança opera em um campo de batalha assimétrico. Os atacantes precisam apenas de uma vulnerabilidade — erro humano, roubo

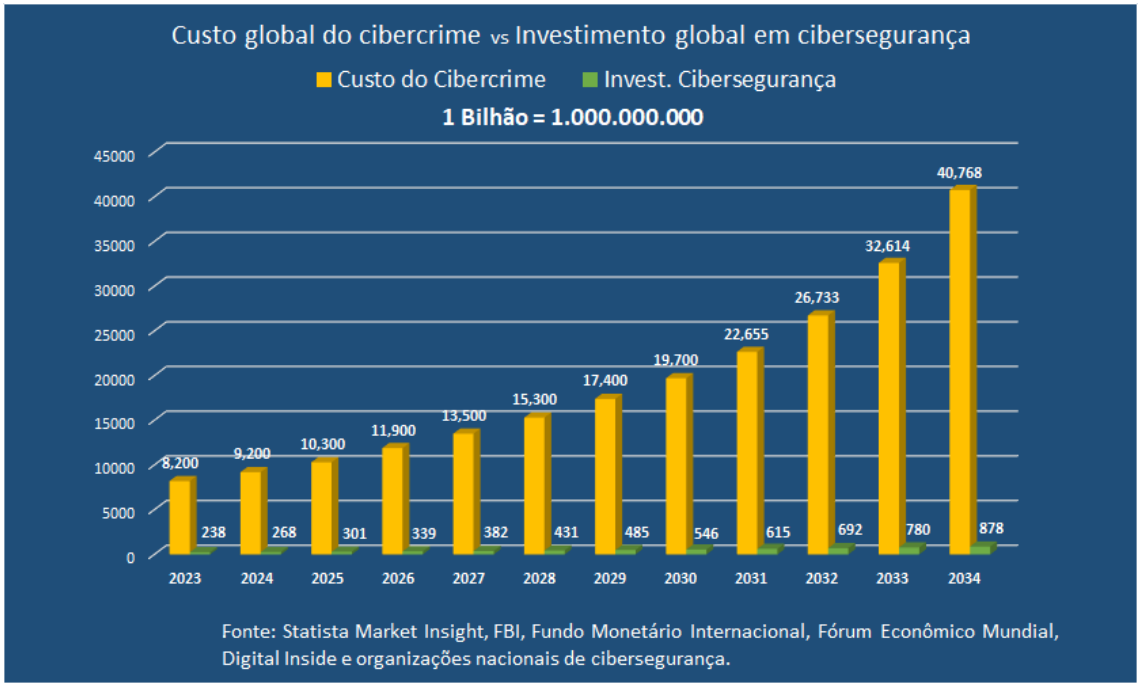
Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

de credenciais, acesso privilegiado, comprometimento da cadeia de suprimentos. Os defensores devem proteger tudo, o tempo todo.

Isso não é uma falha da segurança cibernética, é a natureza do cenário de ameaças.

A triste realidade: o investimento global em cibersegurança em 2025 foi de cerca de 301 bilhões de dólares americanos, enquanto o custo global do cibercrime no mesmo ano foi de cerca de 10,3 trilhões de dólares americanos (mais de 34 vezes maior), posicionando o cibercrime como a terceira maior economia global (atrás dos Estados Unidos e da China).

E as projeções de como essa batalha irá evoluir são preocupantes:



Custo anual global do cibercrime versus investimento anual global em cibersegurança (Anos de 2023 a 2034)

É fato que a cibersegurança falha em impedir o roubo de dados porque se concentra no controle de acesso, e não na proteção do conteúdo dos dados. Firewalls, VPNs, autenticação, arquiteturas de Confiança Zero — tudo isso visa impedir o acesso não autorizado. Mas, uma vez obtido o acesso, os dados tornam-se legíveis.

Em algum momento, repetir as mesmas estratégias de defesa esperando resultados diferentes deixa de ser otimismo e se torna insanidade.

Se as violações não puderem ser totalmente evitadas e o roubo de dados não puder ser revertido, então impedir os danos relacionados a essas violações exigirá uma abordagem fundamentalmente diferente.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Em vez de mudar a pergunta de se a sua organização será ou não alvo de uma violação de segurança, quando e com que frequência, fizemos a nós mesmos uma pergunta totalmente diferente:

E se os dados roubados não tivessem valor algum?

Os invasores não visam sistemas, mas sim dados. E se os dados roubados não puderem ser usados, monetizados ou explorados, a própria invasão perde seu propósito.

Deixe-me dar um exemplo:

Um banco é invadido e os atacantes obtêm acesso a todos os seus sistemas e bancos de dados.

Eles podem ver o saldo de cada conta, mas quando tentam obter as informações pessoais do titular da conta, essas informações específicas no banco de dados estão protegidas de forma que eles não consigam lê-las.

Eles acabaram de descobrir que todo o esforço, tempo e dinheiro investidos na tentativa de invadir o banco foram em vão, uma perda total.

Os dados acessados são inúteis; eles assaltaram o banco e roubaram papel higiênico usado.

Para o banco, o incidente equivale a uma falha de hardware: o equipamento afetado é substituído, os backups são restaurados e as operações são retomadas rapidamente.

Nenhum dado confidencial foi exposto e não houve impacto na reputação ou nas finanças do banco.

Para os clientes, nada aconteceu: o dinheiro continua nas contas e as informações pessoais permanecem confidenciais.

Tornar seus dados sensíveis absolutamente inúteis em caso de roubo não apenas evitará quaisquer danos que esses dados roubados possam causar, como também desencorajará futuros ataques cibernéticos que tentem roubá-los.

Como proteger o conteúdo dos seus dados e neutralizar o seu valor em caso de roubo?

A criptografia é o único mecanismo capaz de neutralizar o valor de dados roubados.

Mas não qualquer criptografia. Os algoritmos de criptografia modernos — simétricos ou assimétricos — não são inquebráveis. São apenas computacionalmente complexos. Com tempo e poder computacional

suficientes, falham. Os dados criptografados roubados hoje eventualmente se tornarão legíveis.

Isso não é teórico. A ameaça "Colher agora, descriptografar depois" — documentada pela Palo Alto Networks — significa que os atacantes já estão coletando dados criptografados, aguardando a capacidade quântica para descriptografá-los.

Se a criptografia for a solução, ela precisa ser diferente; é necessária uma criptografia alternativa.

Como afirmou Arvind Krishna, CEO da IBM, em 2018: " *Se alguém diz que quer algo protegido por pelo menos 10 anos, deve considerar seriamente se não deveria começar a migrar para técnicas de criptografia alternativas agora* ."

Ele disse isso há quase 8 anos, e sua afirmação é mais válida do que nunca. Para impedir permanentemente os danos causados por violações de segurança, a criptografia deve atender a requisitos que as abordagens atuais não conseguem cumprir:

- Proteja o conteúdo dos dados, não apenas o acesso.
- Proteja dados estruturados com segurança sem comprometer os sistemas.
- Trabalhar dentro de bancos de dados e armazenamento estruturado
- Preservar o formato e o comprimento dos dados
- Continuar a ser utilizável por aplicações existentes
- Ser resistente à computação quântica por natureza.
- Neutralizar dados roubados indefinidamente

Para alcançar esse objetivo, foi necessária uma técnica de criptografia completamente nova.

Não é uma extensão.
Não é um modo.
Não é uma solução alternativa.

Uma nova abordagem.

Criamos uma tecnologia para proteger com segurança o conteúdo dos seus dados sensíveis, tornando-os inúteis para qualquer invasor caso sejam roubados!

Após quase uma década de pesquisa e desenvolvimento, criamos e patenteamos uma nova tecnologia de criptografia projetada especificamente para resolver o problema que a segurança cibernética moderna não consegue: prevenir e eliminar os danos que o roubo de dados pode causar.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Nossa tecnologia supera os requisitos de segurança mais rigorosos, como GDPR, DORA, NIS2, HIPAA, NIST Cybersecurity Framework, etc.; possui uma pequena pegada, baixos requisitos de recursos, impacto insignificante no desempenho dos sistemas e integração perfeita em qualquer sistema ou dispositivo existente.

Não substitui a cibersegurança, mas a complementa, resolvendo o problema mais dispendioso — e ainda não resolvido — na cibersegurança: ***os danos causados pelo roubo de dados.***

Como mostramos em nosso exemplo, nem todos os dados precisam ser criptografados, apenas os dados que dão sentido a todo o resto.

Ao criptografar seletivamente campos críticos e sensíveis, os dados restantes tornam-se sem contexto , sem significado e inúteis para os atacantes.

Mesmo que sejam exfiltrados , mesmo que sejam feitas tentativas de descriptografia, mesmo anos depois.

Como resultado da adição da nossa tecnologia à sua estratégia de segurança, violações ainda podem ocorrer, sistemas ainda podem ser acessados e dados ainda podem ser roubados, mas **os danos param por aqui!**

Porque dados roubados sem significado, estrutura ou valor não passam de ruído.

A pergunta que lhe fazemos é:

Você aceitará a derrota e esperará passivamente que sua organização seja invadida e seus dados confidenciais sejam roubados, ou agirá agora para garantir que uma violação não acabe com sua organização?

A sobrevivência da sua organização depende da sua resposta!

Aja agora, antes que seja tarde demais.

Podemos ajudar.

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Referências:

Relatório de Defesa Digital da Microsoft 2025 :
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=29

Relatório da IBM sobre o custo de uma violação de dados em 2025:
https://webobjects2.cdw.com/is/content/CDW/cdw/on-domain-cdw/brands/ibm/cost-of-a-data-breach-2025-full-report.pdf#page=27

TotalAssure - Tempo médio para detecção de um ciberataque em 2025:
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025#global-detection-time-benchmarks

Relatório de Resposta a Incidentes Globais da Unidade 42 da Palo Alto Networks 2025:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks - Colha agora, decifre depois:
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Thales Group - Protegendo a Invasão - Webinar:
https://cpl.thalesgroup.com/es/node/17376

Palo Alto Networks:
https://www.paloaltonetworks.com/perspectives/mastering-the-basics-cyber-hygiene-and-risk-management/

Cloudflare - A confiança do cliente é a melhor métrica de segurança:
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – Violação de segurança é inevitável, perda de dados não - Webinar:
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com