I tuoi dati verranno rubati !

(Affermano gli esperti di sicurezza informatica)

Di **Julian Murguia** , CTO
Omega Krypto
16 marzo 2026

I maggiori esperti mondiali di sicurezza informatica concordano sul fatto che le violazioni siano inevitabili e affermano che non si tratta più di chiedersi **se** la propria organizzazione subirà una violazione, ma **quando** accadrà e **con quale frequenza** .

A tutto ciò si aggiunge il fatto che il Microsoft Digital Defense Report 2025 afferma chiaramente che la raccolta di dati è stata l'obiettivo principale nell'80% di tutti gli attacchi informatici del 2025; e il vostro peggior incubo diventa realtà quando vi rendete conto che anche il furto di dati è inevitabile.

Il rapporto IBM "Cost of a Data Breach Report 2025" conferma che *le violazioni dei dati si verificano nonostante l'adozione di solidi controlli preventivi* . Con la crescente dipendenza dal digitale, gli attacchi diventano più frequenti, più sofisticati e più costosi. E l'utilizzo dell'intelligenza artificiale da parte degli aggressori non fa che peggiorare ulteriormente la situazione!

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

Secondo TotalAssure , *nel 2025 il tempo medio necessario per rilevare una violazione era di 181 giorni* , mentre secondo il Global Incident Response Report 2025 di Unit 42 di Palo Alto Networks , *agli aggressori bastavano appena 72 minuti per esfiltrare i dati* .

La sensazione che la tua organizzazione sia già nel braccio della morte, in attesa dell'inevitabile giorno in cui verrà violata e i tuoi dati sensibili rubati, ti rode il cuore e la mente, temendo che ciò possa portare al collasso e alla cessazione dell'esistenza dell'azienda.

Con questa mentalità, i danni causati dal furto di dati non saranno mai riparati, perché la sconfitta è già stata accettata.

Che cosa è, se non un'ammissione di sconfitta, quando ti dicono che le violazioni (e il furto di dati) sono inevitabili?

Di conseguenza, la strategia di sicurezza informatica si è spostata dalla pura prevenzione alla resilienza: rilevare più velocemente, rispondere più rapidamente, ripristinare più velocemente, mitigare il più possibile.

Ma la resilienza ha un punto cieco cruciale:

Alcuni danni non possono essere mitigati in alcun modo!

Se un attacco informatico mette fuori uso apparecchiature mediche critiche in un ospedale e i pazienti muoiono di conseguenza, nessuna strategia di mitigazione può rimediare a tale perdita.

La morte è irreversibile, così come il furto di dati.

Una volta che terzi entrano in possesso dei tuoi dati sensibili, il danno è già fatto. I dati vengono copiati, conservati e possono essere sfruttati a tempo indeterminato.

Non importa quanto velocemente venga rilevata una violazione, se il rilevamento avviene dopo l'esfiltrazione dei dati, è già troppo tardi.

Il ripristino può rimettere a posto i sistemi, ma non può cancellare le informazioni rubate in possesso dell'attaccante.

I sistemi possono essere ricostruiti, le operazioni possono riprendere, a volte è possibile evitare gli attacchi ransomware, ma i dati rubati mantengono il 100% del loro valore e rimangono pienamente utilizzabili.

Anche se viene pagato un riscatto e i sistemi vengono ripristinati, gli aggressori conservano comunque i dati rubati. Il costo a lungo termine delle violazioni spesso persiste per anni, paralizzando le organizzazioni o costringendole a chiudere definitivamente.

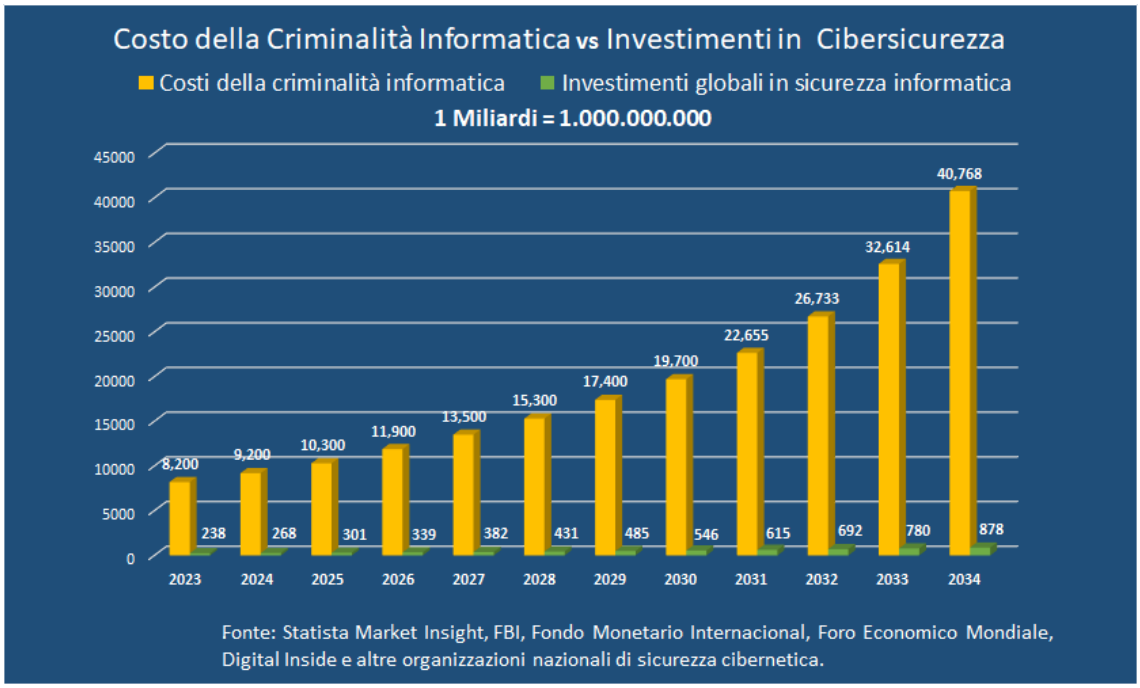
Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

La sicurezza informatica opera su un campo di battaglia asimmetrico. Agli aggressori basta una sola debolezza: errore umano, furto di credenziali, accesso non autorizzato, compromissione della catena di approvvigionamento. Chi si occupa della difesa deve proteggere tutto, in ogni momento.

Non si tratta di un fallimento della sicurezza informatica, bensì della natura stessa del panorama delle minacce.

La cruda verità: nel 2025 gli investimenti globali nella sicurezza informatica si aggiravano sui 301 miliardi di dollari, mentre il costo globale della criminalità informatica per lo stesso anno era di circa 10.300 miliardi di dollari (oltre 34 volte superiore), posizionando la criminalità informatica come la terza economia globale per importanza (dopo Stati Uniti e Cina).

E le previsioni sull'evoluzione di questa battaglia sono inquietanti:



Costo annuale globale della criminalità informatica a confronto con gli investimenti annuali globali in sicurezza informatica - Anni 2023-2034

È un dato di fatto che la sicurezza informatica non riesca a fermare il furto di dati perché si concentra sul controllo degli accessi, non sulla protezione del contenuto dei dati. Firewall, VPN, autenticazione, architetture Zero Trust: tutti questi sistemi mirano a impedire l'accesso non autorizzato. Ma una volta ottenuto l'accesso, i dati sono leggibili.

A un certo punto, ripetere le stesse tattiche difensive aspettandosi risultati diversi smette di essere ottimismo e diventa follia.

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

Se le violazioni non possono essere completamente prevenute e il furto di dati non può essere annullato, allora fermare i danni correlati alle violazioni richiede un approccio radicalmente diverso.

Invece di cambiare la domanda da se la tua organizzazione subirà o meno una violazione, e quando e con quale frequenza, ci siamo semplicemente posti una domanda completamente diversa:

E se i dati rubati non avessero alcun valore?

Gli hacker non si introducono nei sistemi per rubare i dati. E se i dati rubati non possono essere utilizzati, monetizzati o sfruttati, allora la violazione stessa perde il suo scopo.

Vi faccio un esempio:

Una banca subisce un attacco informatico e gli aggressori ottengono l'accesso a tutti i suoi sistemi e database.

Possono visualizzare il saldo di ciascun conto, ma quando tentano di ottenere le informazioni personali del titolare del conto, queste informazioni specifiche nel database sono protette in modo tale da impedirne la lettura.

Hanno appena scoperto che tutti i loro sforzi, il tempo e il denaro investiti per violare la banca sono stati vani, una perdita totale.

I dati a cui hanno avuto accesso sono inutili; hanno rapinato la banca e rubato carta igienica usata.

Per la banca, l'incidente equivale a un guasto hardware: l'apparecchiatura interessata viene sostituita, i backup vengono ripristinati e le operazioni riprendono rapidamente.

Nessun dato riservato è stato divulgato e non vi è stato alcun impatto sulla reputazione o sulle finanze della banca.

Per i clienti non è successo nulla: il loro denaro è ancora nei loro conti e le loro informazioni personali restano riservate.

Rendere i propri dati sensibili completamente inutilizzabili in caso di furto non solo previene i danni che tali dati rubati potrebbero causare, ma scoraggia anche futuri attacchi informatici volti a impossessarsene.

Come proteggere il contenuto dei propri dati e neutralizzarne il valore in caso di furto?

La crittografia è l'unico meccanismo in grado di neutralizzare il valore dei dati rubati.

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

Ma non una crittografia qualsiasi. Gli algoritmi di crittografia moderni, simmetrici o asimmetrici, non sono inviolabili. Sono solo computazionalmente complessi. Con tempo e potenza di calcolo sufficienti, falliscono. I dati crittografati rubati oggi, prima o poi, diventeranno leggibili.

Non si tratta di una questione teorica. La minaccia "Harvest Now, Decrypt Later" (Raccogli ora, decifra in seguito), documentata da Palo Alto Networks, significa che gli aggressori stanno già raccogliendo dati crittografati, in attesa che la tecnologia quantistica ne permetta la decrittazione.

Se la crittografia deve essere la soluzione, deve essere diversa, è necessaria una crittografia alternativa.

Come affermato dall'amministratore delegato di IBM, Arvind Krishna, nel 2018: *" Se qualcuno dice di voler proteggere qualcosa per almeno 10 anni, dovrebbe seriamente valutare se sia il caso di iniziare a passare a tecniche di crittografia alternative fin da ora"*.

Lo disse quasi 8 anni fa e la sua affermazione è più valida che mai.
Per arrestare definitivamente i danni derivanti da una violazione, la crittografia deve soddisfare requisiti che gli approcci attuali non sono in grado di garantire:

- Proteggere il contenuto dei dati, non solo l'accesso.
- Proteggere in modo sicuro i dati strutturati senza compromettere i sistemi
- Lavorare all'interno di database e sistemi di archiviazione strutturata
- Conservare il formato e la lunghezza dei dati
- Rimanere utilizzabile dalle applicazioni esistenti
- Essere resistenti ai computer quantistici fin dalla progettazione
- Neutralizzare i dati rubati in modo permanente.

Per raggiungere questo obiettivo è stata necessaria una tecnica di crittografia completamente nuova.

Non si tratta di un'estensione.
Non è una modalità.
Non è una soluzione alternativa.

Un nuovo approccio.

Abbiamo creato una tecnologia per proteggere in modo sicuro il contenuto dei tuoi dati sensibili, rendendoli inutilizzabili a qualsiasi malintenzionato in caso di furto!

Dopo quasi un decennio di ricerca e sviluppo, abbiamo creato e brevettato una nuova tecnologia di crittografia progettata specificamente per

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

risolvere il problema che la sicurezza informatica moderna non riesce a risolvere: prevenire ed eliminare i danni che il furto di dati può causare.

La nostra tecnologia supera i più severi requisiti di sicurezza, come GDPR, DORA, NIS2, HIPAA, NIST Cybersecurity Framework, ecc.; ha un ingombro ridotto, bassi requisiti di risorse, un impatto trascurabile sulle prestazioni dei sistemi e una perfetta integrazione in qualsiasi sistema o dispositivo esistente.

Non sostituisce la sicurezza informatica, bensì la integra risolvendo il problema più costoso – e tuttora irrisolto – in questo ambito: ***i danni causati dal furto di dati.***

Come abbiamo dimostrato nel nostro esempio, non tutti i dati devono essere crittografati, ma solo quelli che conferiscono significato a tutto il resto.

Crittografando selettivamente i campi sensibili critici, i dati rimanenti diventano privi di contesto , di significato e inutili per gli aggressori.

Anche se esfiltrati , anche se vengono effettuati tentativi di decrittazione, anche anni dopo.

Anche se integriamo la nostra tecnologia nella vostra strategia di sicurezza, potrebbero comunque verificarsi violazioni, accessi non autorizzati e furti di dati, ma **i danni si fermeranno qui!**

Perché i dati rubati, privi di significato, struttura o valore, non sono altro che rumore.

La domanda che vi poniamo è:

Accetterete la sconfitta e aspetterete passivamente che la vostra organizzazione venga violata e i vostri dati riservati rubati, oppure agirete ora per garantire che una violazione non distrugga la vostra organizzazione?

La sopravvivenza della vostra organizzazione dipende dalla vostra risposta!

Agisci ora, prima che sia troppo tardi.

Possiamo aiutarvi.

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

Riferimenti:

Rapporto Microsoft sulla difesa digitale 2025 :
https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=29

Rapporto IBM sui costi di una violazione dei dati nel 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 medio di rilevamento di un attacco informatico nel 2025:
https://www.totalassure.com/blog/tempo medio di rilevamento di un attacco informatico nel 2025#benchmark globali sui tempi di rilevamento

Rapporto globale sulla risposta agli incidenti dell'Unità 42 di Palo Alto Networks per il 2025:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks - Raccogli i dati ora, decifra dopo:
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Thales Group - Proteggere la violazione - 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 - La fiducia dei clienti è il miglior indicatore di sicurezza:
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – La violazione è inevitabile, la perdita di dati no - Webinar:
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

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