Ihre Daten werden gestohlen !

(Experten für Cybersicherheit von Affirm)

Von **Julian Murguia** , CTO
Omega Krypto
16. März 2026

Die weltweit führenden Cybersicherheitsexperten sind sich einig, dass Sicherheitslücken unvermeidlich sind und bestätigen, dass es nicht mehr die Frage ist, **ob** Ihr Unternehmen angegriffen wird, sondern **wann** und **wie oft** .

Hinzu kommt, dass im Microsoft Digital Defense Report 2025 klar angegeben wird, dass die Datenerfassung bei 80 % aller Cyberangriffe im Jahr 2025 das Hauptziel war; und Ihr schlimmster Albtraum wird wahr, wenn Sie feststellen, dass auch Datendiebstahl unvermeidlich ist.

Der IBM-Bericht „Kosten von Datenschutzverletzungen 2025“ bestätigt, dass *Datenschutzverletzungen trotz strenger Präventionsmaßnahmen vorkommen* . Mit zunehmender digitaler Abhängigkeit werden Angriffe häufiger, ausgefeilter und kostspieliger. Der Einsatz von Künstlicher Intelligenz durch die Angreifer verschärft die Situation zusätzlich.

Laut TotalAssure betrug die *durchschnittliche Zeit bis zur Entdeckung eines Sicherheitsvorfalls im Jahr 2025 181 Tage* , während Angreifer laut dem „Unit

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

42 Global Incident Response Report 2025“ von Palo Alto Networks teilweise *nur 72 Minuten benötigten, um Daten zu exfiltrieren* .

Das Gefühl, dass Ihre Organisation bereits im Todestrakt liegt und auf den unvermeidlichen Tag wartet, an dem sie gehackt und Ihre sensiblen Daten gestohlen werden, nagt an Ihrem Herzen und Verstand, aus Angst, dass dies zum Zusammenbruch Ihrer Organisation und zum Ende ihrer Existenz führen könnte.

Mit dieser Denkweise wird der durch Datendiebstahl verursachte Schaden niemals behoben werden – denn die Niederlage wurde bereits akzeptiert.

Was anderes als ein Eingeständnis der Niederlage ist es, wenn man Ihnen sagt, dass Sicherheitslücken (und Datendiebstahl) unvermeidlich sind?

Infolgedessen hat sich die Cybersicherheitsstrategie von reiner Prävention hin zu Resilienz verlagert: schneller erkennen, schneller reagieren, schneller wiederherstellen, so viel Schaden wie möglich abmildern.

Doch Resilienz hat einen entscheidenden blinden Fleck:

Manche Schäden lassen sich einfach nicht mindern!

Wenn ein Cyberangriff kritische medizinische Geräte in einem Krankenhaus lahmlegt und Patienten infolgedessen sterben, kann keine Schadensbegrenzungsstrategie diesen Verlust ungeschehen machen.

Der Tod ist unumkehrbar, und Datendiebstahl ebenso.

Sobald Außenstehende Ihre sensiblen Daten besitzen, ist der Schaden bereits angerichtet. Die Daten werden kopiert, gespeichert und können unbegrenzt missbraucht werden.

Es spielt keine Rolle, wie schnell ein Sicherheitsverstoß entdeckt wird; wenn die Entdeckung erst nach der Datenexfiltration erfolgt, ist es bereits zu spät.

Die Wiederherstellung kann Systeme wiederherstellen – aber sie kann gestohlene Informationen nicht aus dem Besitz des Angreifers löschen.

Systeme können wiederhergestellt, der Betrieb kann wiederaufgenommen werden, Ransomware kann manchmal vermieden werden, aber gestohlene Daten behalten 100% ihres Wertes und bleiben voll nutzbar.

Selbst wenn ein Lösegeld gezahlt und die Systeme wiederhergestellt werden, behalten die Angreifer die gestohlenen Daten. Die langfristigen Kosten von Datenlecks halten oft jahrelang an und können Unternehmen schwer schädigen oder sogar zum Konkurs zwingen.

Cybersicherheit findet auf einem asymmetrischen Schlachtfeld statt. Angreifer benötigen nur eine Schwachstelle – menschliches Versagen,

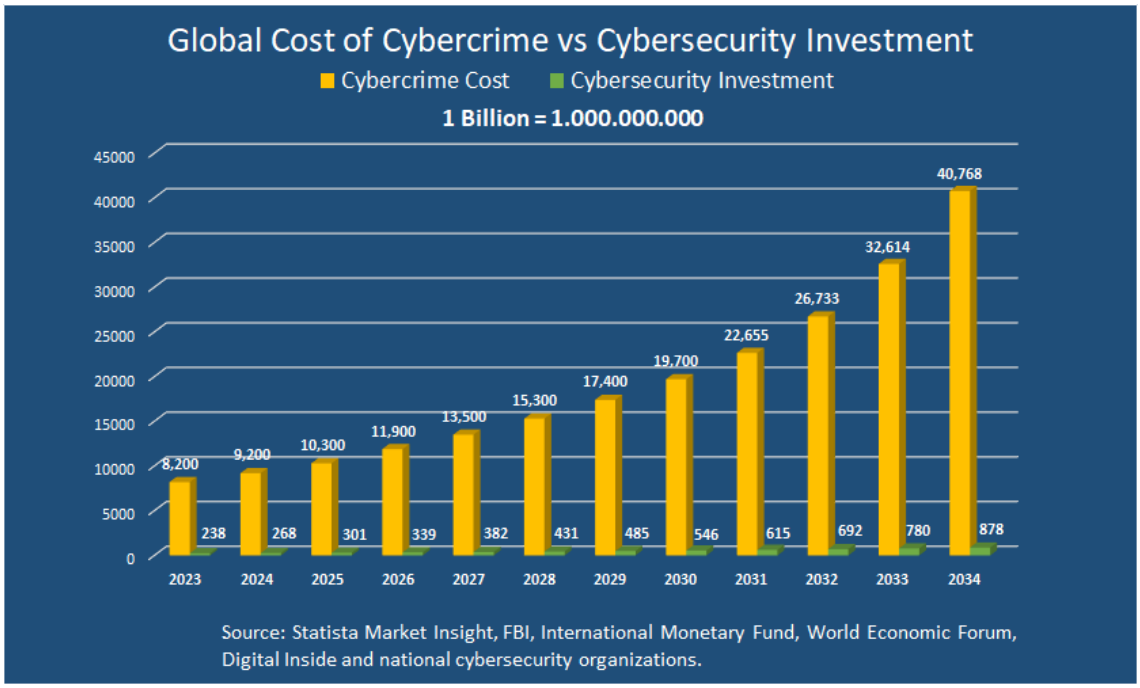
Julian Murguía, CTO
julian.murguia@omegakrypto.com
https://omegakrypto.com

Diebstahl von Zugangsdaten, Insiderzugriff oder Kompromittierung der Lieferkette. Verteidiger müssen daher jederzeit alles absichern.

Dies ist kein Versagen der Cybersicherheit, sondern liegt in der Natur der Bedrohungslandschaft.

Die bittere Wahrheit: Die weltweiten Investitionen in Cybersicherheit beliefen sich im Jahr 2025 auf rund 301 Milliarden US-Dollar, während die globalen Kosten der Cyberkriminalität im selben Jahr rund 10,3 Billionen US-Dollar betrugen (mehr als 34 Mal so hoch), wodurch die Cyberkriminalität zur drittgrößten globalen Volkswirtschaft wurde (nach den Vereinigten Staaten und China).

Und die Prognosen für den weiteren Verlauf dieser Schlacht sind beunruhigend:



Jährliche Kosten globaler Cyberkriminalität im Vergleich zu jährlichen Investitionen in globale Cybersicherheit – Jahre 2023 bis 2034

Es ist eine Tatsache, dass Cybersicherheit Datendiebstahl nicht verhindern kann, weil sie sich auf die Zugriffskontrolle und nicht auf den Schutz der Dateninhalte konzentriert. Firewalls, VPNs, Authentifizierung, Zero-Trust-Architekturen – sie alle zielen darauf ab, unberechtigten Zugriff zu verhindern. Doch sobald der Zugriff erlangt ist, sind die Daten lesbar.

Irgendwann hört es auf, Optimismus zu sein, wenn man immer wieder dieselben Abwehrmechanismen anwendet und andere Ergebnisse erwartet – und wird dann zum Wahnsinn.

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

Wenn sich Sicherheitslücken nicht vollständig verhindern lassen und Datendiebstahl nicht rückgängig gemacht werden kann, dann erfordert die Verhinderung von Schäden im Zusammenhang mit Sicherheitslücken einen grundlegend anderen Ansatz.

Anstatt die Frage zu ändern, ob Ihre Organisation gehackt wird und wann und wie oft, haben wir uns einfach eine ganz andere Frage gestellt:

Was wäre, wenn gestohlene Daten wertlos wären?

Angreifer dringen nicht in Systeme ein, sondern in Daten. Und wenn gestohlene Daten nicht genutzt, monetarisiert oder anderweitig missbraucht werden können, verliert der Angriff seinen Zweck.

Ich gebe Ihnen ein Beispiel:

Eine Bank wird gehackt und die Angreifer erlangen Zugriff auf alle Systeme und Datenbanken.

Sie können den Kontostand jedes Kontos einsehen, aber wenn sie versuchen, die persönlichen Daten des Kontoinhabers zu erhalten, sind diese spezifischen Informationen in der Datenbank so geschützt, dass sie sie nicht lesen können.

Sie haben gerade erst festgestellt, dass all ihre Mühe, Zeit und ihr Geld, die sie in den Bankeinbruch investiert haben, vergeblich waren – ein totaler Verlust.

Die erbeuteten Daten sind nutzlos; sie haben die Bank ausgeraubt und gebrauchtes Toilettenpapier gestohlen.

Für die Bank ist der Vorfall mit einem Hardwareausfall vergleichbar: Die betroffenen Geräte werden ersetzt, Backups wiederhergestellt und der Betrieb wird schnell wieder aufgenommen.

Es wurden keine vertraulichen Daten offengelegt, und es gab keine Auswirkungen auf den Ruf oder die Finanzen der Bank.

Für die Kunden hat sich nichts geändert: Ihr Geld befindet sich weiterhin auf ihren Konten und ihre persönlichen Daten bleiben vertraulich.

Indem Sie Ihre sensiblen Daten im Falle eines Diebstahls absolut unbrauchbar machen, verhindern Sie nicht nur jeglichen Schaden, den solche gestohlenen Daten anrichten könnten, sondern schrecken auch zukünftige Cyberangriffe ab, die versuchen, diese Daten zu stehlen.

Wie schützen Sie den Inhalt Ihrer Daten und neutralisieren deren Wert im Falle eines Diebstahls?

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

Verschlüsselung ist der einzige Mechanismus, der den Wert gestohlener Daten neutralisieren kann.

Aber nicht jede Verschlüsselung. Moderne Verschlüsselungsalgorithmen – ob symmetrisch oder asymmetrisch – sind nicht unknackbar. Sie sind lediglich rechenintensiv. Mit genügend Zeit und Rechenleistung versagen sie. Gestohlene verschlüsselte Daten werden irgendwann lesbar sein.

Dies ist keine Theorie. Die von Palo Alto Networks dokumentierte Bedrohung „ Ernten jetzt, Entschlüsseln später “ bedeutet, dass Angreifer bereits verschlüsselte Daten sammeln und auf Quantentechnologie warten, um diese zu entschlüsseln.

Wenn Verschlüsselung die Lösung sein soll, muss sie anders sein, eine alternative Verschlüsselungsmethode ist erforderlich.

Wie IBM-Chef Arvind Krishna im Jahr 2018 erklärte: „ *Wenn jemand sagt, er wolle etwas mindestens 10 Jahre lang schützen lassen, sollte er ernsthaft darüber nachdenken, ob er jetzt schon auf alternative Verschlüsselungstechniken umsteigen sollte* .“

Das sagte er vor fast acht Jahren, und seine Aussage ist heute aktueller denn je.
Um Schäden durch Sicherheitsverletzungen dauerhaft zu verhindern, muss die Verschlüsselung Anforderungen erfüllen, die aktuelle Ansätze nicht erfüllen können:

- Schützen Sie nicht nur den Zugriff auf Dateninhalte, sondern auch den Dateninhalt.
- Strukturierte Daten sicher schützen, ohne Systeme zu beeinträchtigen
- Arbeiten innerhalb von Datenbanken und strukturierten Speichern
- Datenformat und -länge beibehalten
- Bleibt von bestehenden Anwendungen nutzbar
- Von Grund auf quantenresistent sein
- Gestohlene Daten dauerhaft neutralisieren

Um dies zu erreichen, war eine völlig neue Verschlüsselungstechnik erforderlich.

Keine Erweiterung.
Kein Modus.
Keine Umgehungslösung.

Ein neuer Ansatz.

Wir haben eine Technologie entwickelt, die den Inhalt Ihrer sensiblen Daten sicher schützt und diese im Falle eines Diebstahls für jeden Angreifer unbrauchbar macht!

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

Nach fast einem Jahrzehnt Forschung und Entwicklung haben wir eine neuartige Verschlüsselungstechnologie entwickelt und patentiert, die speziell dafür konzipiert wurde, das Problem zu lösen, das die moderne Cybersicherheit nicht lösen kann: den Schaden, den Datendiebstahl verursachen kann, zu verhindern und zu beseitigen.

Unsere Technologie übertrifft die strengsten Sicherheitsanforderungen wie DSGVO, DORA, NIS2, HIPAA, NIST Cybersecurity Framework usw.; sie ist ressourcenschonend, hat einen geringen Ressourcenbedarf, kaum Auswirkungen auf die Systemleistung und lässt sich nahtlos in jedes bestehende System oder Gerät integrieren.

Sie ersetzt nicht die Cybersicherheit, sondern ergänzt sie, indem sie das kostspieligste – und immer noch ungelöste – Problem der Cybersicherheit löst: ***den Schaden, der durch Datendiebstahl verursacht wird.***

Wie wir in unserem Beispiel gezeigt haben, müssen nicht alle Daten verschlüsselt werden, sondern nur die Daten, die allem anderen Bedeutung verleihen.

Durch die selektive Verschlüsselung kritischer sensibler Felder werden die verbleibenden Daten kontextlos , bedeutungslos und für Angreifer nutzlos.

Selbst wenn die Daten exfiltriert werden , selbst wenn Entschlüsselungsversuche unternommen werden, selbst Jahre später.

Auch wenn Sie unsere Technologie in Ihre Sicherheitsstrategie integrieren, können Sicherheitslücken weiterhin auftreten, Systeme können weiterhin aufgerufen und Daten gestohlen werden – aber **der Schaden hört hier auf!**

Denn gestohlene Daten ohne Bedeutung, Struktur oder Wert sind nichts weiter als Rauschen.

Die Frage, die wir Ihnen stellen, lautet:

Werden Sie sich geschlagen geben und passiv darauf warten, dass Ihr Unternehmen gehackt und Ihre vertraulichen Daten gestohlen werden, oder werden Sie jetzt handeln, um sicherzustellen, dass ein Datenleck nicht das Ende Ihres Unternehmens bedeutet?

Das Überleben Ihrer Organisation hängt von Ihrer Antwort ab!

Handeln Sie jetzt, bevor es zu spät ist.

Wir können helfen.

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

Referenzen:

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

IBM-Bericht zu den Kosten eines Datenlecks 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 – Durchschnittliche Zeit zur Erkennung eines Cyberangriffs 2025:
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025#global-detection-time-benchmarks

Globaler Incident Response Report 2025 der Einheit 42 von Palo Alto Networks:
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks – Jetzt ernten, später entschlüsseln:
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Thales Group – Sicherheitslücken schließen – 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 – Kundenvertrauen ist die beste Sicherheitskennzahl:
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – Sicherheitslücken sind unvermeidbar, Datenverlust nicht – Webinar:
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

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