Vos données seront volées !

(Affirm, experts en cybersécurité)

Par **Julian Murguia** , directeur technique
Omega Krypto
16 mars 2026

Les plus grands experts mondiaux en cybersécurité s'accordent à dire que les violations de données sont inévitables et affirment qu'il ne s'agit plus de savoir **si** votre organisation sera victime d'une violation de données, mais **quand** cela se produira et **à quelle fréquence** .

Ajoutez à cela que le rapport Microsoft Digital Defense Report 2025 indique clairement que la collecte de données était l'objectif principal de 80 % des cyberattaques de 2025 ; et votre pire cauchemar devient réalité lorsque vous réalisez que le vol de données est également inévitable.

Le rapport IBM sur le coût des violations de données en 2025 confirme que *des violations surviennent malgré des mesures de prévention robustes* . À mesure que la dépendance numérique s'accroît, les attaques deviennent plus fréquentes, plus sophistiquées et plus coûteuses. Et le recours à l'intelligence artificielle par les attaquants ne fait qu'aggraver la situation !

Selon TotalAssure , le *temps moyen de détection d'une violation de données en 2025 était de 181 jours* , tandis que selon le rapport 2025 de l'unité 42 de

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

Palo Alto Networks sur la réponse aux incidents dans le monde, *il ne fallait aux attaquants que 72 minutes pour exfiltrer des données* .

Le sentiment que votre organisation est déjà condamnée à mort, attendant l'inévitable jour où elle sera piratée et vos données sensibles volées, vous ronge le cœur et l'esprit, vous faisant craindre que cela n'entraîne l'effondrement et la disparition de votre organisation.

Avec cet état d'esprit, les dommages causés par le vol de données ne seront jamais réparés, car la défaite est déjà acceptée.

Que penser, sinon d'un aveu de défaite, lorsqu'on vous dit que les violations de données (et les vols de données) sont inévitables ?

De ce fait, la stratégie de cybersécurité est passée de la simple prévention à la résilience : détecter plus vite, réagir plus rapidement, récupérer plus vite, atténuer autant que possible.

Mais la résilience a un angle mort critique :

Certains dommages sont tout simplement irrémédiables !

Si une cyberattaque met hors service des dispositifs médicaux essentiels dans un hôpital et que des patients en meurent, aucune stratégie d'atténuation ne peut réparer ces pertes.

La mort est irréversible, tout comme le vol de données.

Une fois que des tiers ont mis la main sur vos données sensibles, le mal est fait. Les données sont copiées, conservées et exploitables indéfiniment.

Peu importe la rapidité avec laquelle une brèche est détectée, si la détection intervient après l'exfiltration des données, il est déjà trop tard.

La récupération peut restaurer les systèmes, mais elle ne peut pas effacer les informations volées en possession de l'attaquant.

Les systèmes peuvent être reconstruits, les opérations peuvent reprendre, les ransomwares peuvent parfois être évités, mais les données volées conservent 100 % de leur valeur et restent pleinement utilisables.

Même si une rançon est versée et que les systèmes sont restaurés, les pirates conservent les données volées. Les conséquences à long terme des violations de données se font souvent sentir pendant des années, paralysant les organisations, voire les contraignant à cesser leurs activités.

La cybersécurité se déroule sur un champ de bataille asymétrique. Les attaquants n'ont besoin que d'une seule faille : erreur humaine, vol d'identifiants, accès non autorisé, compromission de la chaîne

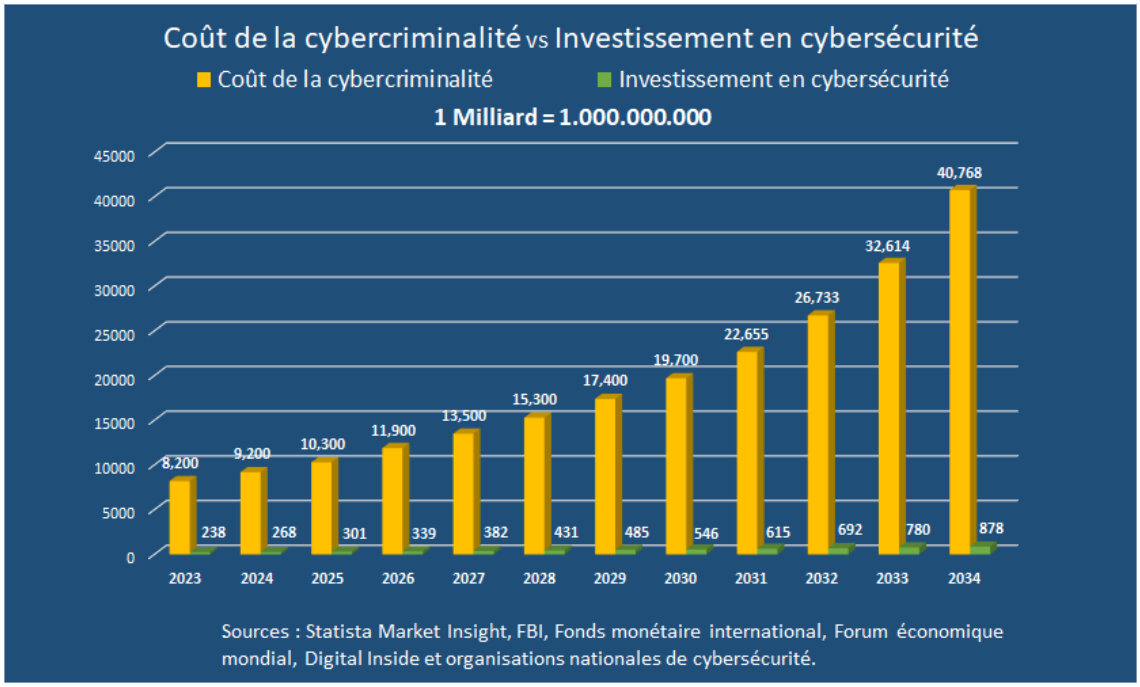
Julian Murguía, directeur technique
julian.murguia@omegakrypto.com
https://omegakrypto.com

d'approvisionnement. Les défenseurs doivent sécuriser l'ensemble du système, en permanence.

Il ne s'agit pas d'un échec de la cybersécurité, mais de la nature même du paysage des menaces.

La triste réalité : en 2025, les investissements mondiaux en cybersécurité s'élevaient à environ 301 milliards de dollars américains, tandis que le coût mondial de la cybercriminalité pour la même année atteignait environ 10 300 milliards de dollars américains (plus de 34 fois supérieur), ce qui place la cybercriminalité au troisième rang des activités économiques mondiales (derrière les États-Unis et la Chine).

Et les projections quant à l'évolution de cette bataille sont inquiétantes :



Coût annuel mondial de la cybercriminalité vs investissement annuel mondial en cybersécurité (Années 2023 à 2034)

Il est indéniable que la cybersécurité ne parvient pas à empêcher le vol de données car elle se concentre sur le contrôle d'accès et non sur la protection du contenu des données. Pare-feu, VPN, authentification, architectures Zero Trust : tous ces dispositifs visent à empêcher les accès non autorisés. Mais une fois l'accès obtenu, les données sont lisibles.

À un certain moment, répéter les mêmes mécanismes de défense en espérant des résultats différents cesse d'être de l'optimisme et devient de la folie.

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

S'il est impossible de prévenir totalement les violations de données et d'annuler un vol de données, alors la mise fin aux dommages qui en découlent exige une approche fondamentalement différente.

Au lieu de nous demander si notre organisation sera victime d'une intrusion, quand et à quelle fréquence, nous nous sommes posé une question totalement différente :

Et si les données volées n'avaient aucune valeur ?

Les attaquants ne s'introduisent pas dans les systèmes pour s'emparer des données. Et si les données volées ne peuvent être utilisées, monétisées ou exploitées, alors l'intrusion elle-même perd tout son sens.

Permettez-moi de vous donner un exemple :

Une banque est victime d'une intrusion et les pirates informatiques obtiennent l'accès à tous ses systèmes et bases de données.

Ils peuvent consulter le solde de chaque compte, mais lorsqu'ils tentent d'obtenir les informations personnelles du titulaire du compte, ces informations spécifiques sont protégées dans la base de données de manière à ce qu'ils ne puissent pas les lire.

Ils viennent de découvrir que tous leurs efforts, leur temps et leur argent investis pour pénétrer dans la banque ont été vains, une perte totale.

Les données auxquelles ils ont accédé sont inutiles ; ils ont braqué la banque et volé du papier toilette usagé.

Pour la banque, l'incident équivaut à une panne matérielle : l'équipement concerné est remplacé, les sauvegardes sont restaurées et les opérations reprennent rapidement.

Aucune donnée confidentielle n'a été divulguée et la réputation ou les finances de la banque n'ont subi aucune incidence.

Pour les clients, rien n'a changé : leur argent est toujours sur leurs comptes et leurs informations personnelles restent confidentielles.

Rendre vos données sensibles totalement inutilisables en cas de vol permet non seulement d'éviter les dommages que de telles données volées pourraient causer, mais aussi de dissuader les futures cyberattaques de tenter de les dérober.

Comment protéger le contenu de vos données et neutraliser leur valeur en cas de vol ?

Le chiffrement est le seul mécanisme capable de neutraliser la valeur des données volées.

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

Mais attention, pas n'importe quel chiffrement. Les algorithmes de chiffrement modernes, symétriques ou asymétriques, ne sont pas inviolables. Ils sont seulement difficiles à déchiffrer. Avec suffisamment de temps et de puissance de calcul, ils finissent par être compromis. Les données chiffrées volées aujourd'hui seront un jour lisibles.

Il ne s'agit pas d'une hypothèse. La menace « Récolter maintenant, déchiffrer plus tard » (documentée par Palo Alto Networks) signifie que les attaquants collectent déjà des données chiffrées, attendant les capacités de l'informatique quantique pour les déchiffrer.

Si le chiffrement doit être la solution, il doit être différent ; un chiffrement alternatif est nécessaire.

Comme l'a déclaré Arvind Krishna, PDG d'IBM, en 2018 : « *Si quelqu'un affirme vouloir protéger quelque chose pendant au moins 10 ans, il devrait sérieusement envisager de commencer dès maintenant à adopter des techniques de chiffrement alternatives* . »

Il a dit cela il y a près de 8 ans et son affirmation est plus valable que jamais. Pour stopper définitivement les dommages liés aux violations de données, le chiffrement doit répondre à des exigences auxquelles les approches actuelles ne peuvent pas répondre :

- Protéger le contenu des données, et pas seulement l'accès
- Protéger en toute sécurité les données structurées sans perturber les systèmes
- Travailler au sein de bases de données et de systèmes de stockage structurés
- Préserver le format et la longueur des données
- Rester utilisable par les applications existantes
- Être résistant à l'inversion quantique dès la conception
- Neutraliser indéfiniment les données volées

Pour y parvenir, il a fallu une technique de chiffrement entièrement nouvelle.

Pas une extension.
Pas un mode.
Ce n'est pas une solution de contournement.

Une nouvelle approche.

Nous avons créé une technologie permettant de protéger efficacement le contenu de vos données sensibles, les rendant inutilisables pour tout attaquant en cas de vol !

Après près d'une décennie de recherche et développement, nous avons créé et breveté une nouvelle technologie de chiffrement conçue spécifiquement

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

pour résoudre le problème que la cybersécurité moderne ne peut pas résoudre : prévenir et éliminer les dommages que peut causer le vol de données.

Notre technologie surpasse les exigences de sécurité les plus strictes telles que le RGPD, DORA, NIS2, HIPAA, le cadre de cybersécurité NIST, etc. ; elle présente une empreinte réduite, de faibles besoins en ressources, un impact négligeable sur les performances des systèmes et une intégration transparente dans tout système ou appareil existant.

Elle ne remplace pas la cybersécurité, elle la complète en résolvant le problème le plus coûteux – et toujours non résolu – en matière de cybersécurité : ***les dommages causés par le vol de données.***

Comme nous l'avons montré dans notre exemple, toutes les données n'ont pas besoin d'être cryptées, seulement celles qui donnent du sens à tout le reste.

En chiffrant sélectivement les champs sensibles critiques, les données restantes deviennent décontextualisées , insignifiantes et inutiles pour les attaquants.

Même en cas d'exfiltration , même en cas de tentatives de décryptage, même des années plus tard.

L'ajout de notre technologie à votre stratégie de sécurité ne garantit pas que des violations de données, des accès non autorisés à vos systèmes et des vols de données puissent toujours se produire, mais **les dégâts s'arrêtent ici !**

Car des données volées sans signification, sans structure ni valeur ne sont rien de plus que du bruit.

La question que nous vous posons est la suivante :

Accepterez-vous la défaite et attendrez-vous passivement que votre organisation soit victime d'une intrusion et que vos données confidentielles soient volées, ou agirez-vous dès maintenant pour vous assurer qu'une telle intrusion ne mette pas fin à votre organisation ?

La survie de votre organisation dépend de votre réponse !

Agissez maintenant, avant qu'il ne soit trop tard.

Nous pouvons vous aider.

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

Références :

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

Rapport IBM sur le coût d'une violation de données en 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 - Délai moyen de détection d'une cyberattaque en 2025 :
https://www.totalassure.com/blog/average-time-to-detect-cyber-attack-2025#global-detection-time-benchmarks

Rapport 2025 de l'unité 42 de Palo Alto Networks sur la réponse aux incidents à l'échelle mondiale :
https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/unit42/Unit42-Global-Incident-Response-Report.pdf#page=25

Palo Alto Networks - Récoltez maintenant, déchiffrez plus tard :
https://www.paloaltonetworks.com/cyberpedia/harvest-now-decrypt-later-hndl

Groupe Thales - Sécuriser la brèche - Webinaire :
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 confiance des clients est le meilleur indicateur de sécurité :
https://www.cloudflare.com/the-net/illuminate/security-customer-trust/

Seclore – Une violation de données est inévitable, mais pas une perte de données – Webinaire :
https://www.seclore.com/resources/videos/breach-is-inevitable-data-loss-isnt/

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