Rubrik Zero Labs

L'état de la sécurité des données :

LA DURE REALITE

Sommaire

Sources de données

RT **TÉLÉMÉTRIE DE RUBRIK** WR **WAKEFIELD RESEARCH** ER **DONNÉES SUR LES RÉPONSES AUX INCIDENTS**

À PROPOS DES DONNÉES

Le Rubrik Zero Labs s'efforce de fournir des informations exploitables et indépendantes afin de réduire les risques liés à la sécurité des données. Nous avons intégré des résultats de différentes sources, sur la période du 1er janvier au 31 décembre 2022.

TÉLÉMÉTRIE de RUBRIK :

Nous nous appuyons sur la télémétrie de Rubrik afin de refléter au mieux la réalité sur le terrain des organisations de tous les jours, tout en apportant une bonne visibilité sur nos erreurs systématiques.

+ DE 5000
clients

3
régions

22
secteurs d'activité

57
pays

Volume total de données sécurisées

28
exaoctets (Eo)
de stockage logique

659
pétaoctets (Po)
de stockage back-end

Données sensibles disséminées dans :

+ de 8,7 milliards
de fichiers

1 fichier sur 38
renferme des
données sensibles

+ de 19 milliards
d'enregistrements de
données sensibles
contenus dans les fichiers

Tout est question d'échelle :

Selon certaines estimations, tous les mots prononcés par les êtres humains depuis le début de leur histoire représenteraient 5 Eo,soit l'équivalent de seulement 18 % des données sécurisées par Rubrik en 2022.[1,2,3,4]

28 Eo contre 659 Po de stockage back-end

Mais au fait !
Quand le commun des mortels entend le mot « données », il pense au stockage logique, autrement dit au stockage front-end. Nous qui évoluons dans le monde des données, nous préférons nous concentrer sur le stockage back-end.

Rubrik prend l'intégralité des données d'une organisation et applique différentes fonctions (notamment la déduplication et la compression) pour réduire la quantité de données stockées en back-end. Voilà pourquoi nous nous concentrerons sur le stockage back-end dans la suite du présent rapport.

Étude de cas :
Nous nous sommes également intéressés tout particulièrement à une attaque perpétrée contre l'une des organisations incluses dans les analyses de télémétrie de Rubrik. Le nom de l'organisation a été modifié pour des raisons de confidentialité.

1 https://www.space.com/18383-how-far-away-is-jupiter.html
2 https://www.sizes.com/tools/filing_cabinets.htm
3 https://www.zmescience.com/science/how-big-data-can-get/
4 https://www.backblaze.com/blog/what-is-an-exabyte/

WAKEFIELD RESEARCH :

Nous avons demandé à Wakefield Research de réaliser une étude afin de compléter notre propre télémétrie en y apportant une vision plus large du contexte de la sécurité des données.

Nous avons choisi d'y faire participer des responsables informatiques et de la cybersécurité afin d'étudier leurs différences de points de vue.

+ DE 1600
responsables informatiques et de la cybersécurité

49 %
de DSI et RSSI

3 régions
États-Unis, EMEA et APAC

16 %
Vice-présidents

38 %
Directeurs

10 pays
États-Unis, Royaume-Uni, France, Allemagne, Italie, Pays-Bas, Japon, Australie, Singapour, Inde

DONNÉES SUR LES RÉPONSES AUX INCIDENTS :

Nous avons contacté certains organismes reconnus dans le domaine de la cybersécurité afin d'obtenir une perspective plus complète sur le contexte de la sécurité des données. Nous les remercions de nous avoir autorisés à utiliser leurs résultats.

Mandiant :
Données sur les temps de séjour médians et sur les rapports d'enquête sur le ransomware dans le monde, d'après le rapport M-Trends 2023

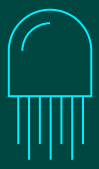
Palo Alto Networks Unit 42 :
Demandes de rançons en 2022, d'après le rapport 2023 Unit 42 Ransomware and Extortion Report

Expel :
Signes précurseurs du ransomware et augmentation du taux d'intrusion dans les clouds publics, d'après le rapport Great Expectations 2022

Permiso :
Données sur l'utilisation illicite d'informations d'identification pour les intrusions dans le cloud et sur les niveaux de privilège des informations d'identification, d'après le rapport Permiso 2022 - End of Year Observations

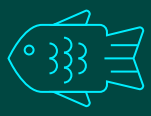
UN OCÉAN DE DONNÉES

Les organisations naviguent sur un océan de données. En surface, cet océan semble vaste mais stable.



Mais toute personne qui plonge dans ses profondeurs sait qu'elle y trouvera de la vie.

La visibilité est mauvaise mais les données se révèleront peu à peu – dans des grottes, sous des rochers, où que vous regardiez ! Les courants sont puissants. Vous ne serez jamais témoin deux fois de la même scène.



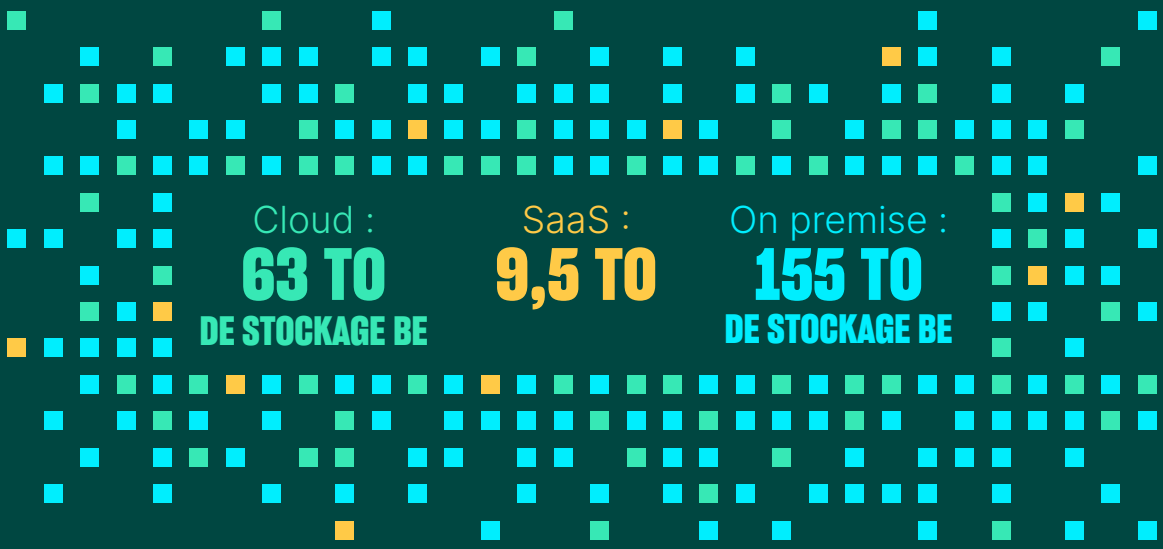
Mais une question vous taraude :

Y A-T-IL DES PRÉDATEURS TAPIS DANS L'OMBRE, ATTENDANT LE MOMENT PROPICE POUR ATTAQUER ?

Les données prolifèrent plus rapidement et s'étendent géographiquement bien plus largement que nous ne l'imaginons ®

Données sécurisées dans un environnement type :

TOTAL : 227 TO DE STOCKAGE BE



Croissance moyenne des données sécurisées au cours de l'année 2022 :

Total :	Cloud :	SaaS :	On premise :
25 %	**61 %**	**236 %**	**19 %**

Le volume de données d'une organisation type triplera au cours des cinq prochaines années. Cela représentera

545 TO DE DONNÉES DE STOCKAGE BACK-END

à sécuriser, si les taux de croissance restent stables.

45 %

des entreprises mondiales sécurisent leurs données dans un environnement mixte (on-premise, cloud et SaaS).

36 %

des entreprises mondiales font appel à plusieurs fournisseurs de clouds simultanément.

Pour chaque solution de sécurité des données, il y a un défi à relever ®

En situation de crise, le dernier rempart n'est autre que les systèmes de sauvegarde et de restauration, avec les processus associés. Mais les organisations ont compris qu'il ne suffit plus désormais de se contenter d'une simple solution de sauvegarde.

99 %

des organisations externes déclarent disposer d'une solution de sauvegarde et de restauration.

Cependant, 93 %

ont rencontré des problèmes majeurs au niveau de leur solution. Les pénuries de personnel, les limites de bande passante, les manquements au niveau de l'infrastructure et l'absence de plans ou de priorités préalablement coordonnés figurent parmi les problèmes les plus fréquemment signalés.

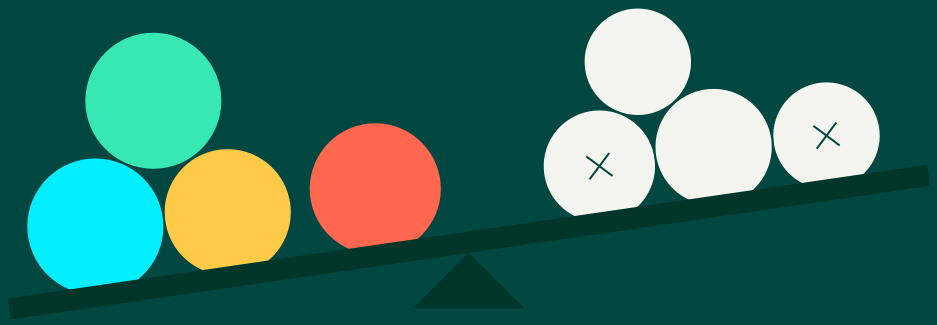
93 %

des organisations externes indiquent que des acteurs malveillants ont tenté de cibler leurs sauvegardes de données au cours d'une cyberattaque

73 %

ont signalé que les tentatives ont en partie abouti

Tout le monde « **fait** » de la sécurité des données, mais en 2022 la réalité recèle des disparités ®



56 %

des organisations ont utilisé au moins une initiative Zero Trust.

56 %

ont élaboré ou étudié un plan de réponse en cas d'incident.

54 %

ont testé des options de sauvegarde et de restauration.

52 %

ont créé ou affiné leur plan d'orchestration de la restauration de données.

L’étude de cas

2024

En 2022, un établissement universitaire américain a fait l’expérience de la dure réalité de la sécurité des données. Au travers de son histoire, nous nous demanderons à quel point ce type d’expérience est fréquent.

Les faits relatés dans cette étude de cas sont véridiques, mais le nom réel de l’organisation est anonymisé afin de protéger la confidentialité du client.

Environnement de l'Université de Stone :

2,9 Po
de stockage logique

64 To de stockage back-end
physique

Données réparties entre deux
environnements distincts

155 %
de croissance de données sur l'année 2022

CE QUE VOUS NE SAVEZ PAS

PEUT VOUS NUIRE

Les pirates ont fait intrusion dans les données de l'Université de Stone en exploitant une vulnérabilité Log4j exposant le serveur de système de tickets d'assistance de l'établissement à des risques de violation.

Log4j

Fin 2021, une vulnérabilité détectée au niveau de la bibliothèque logicielle Log4j d'Apache, l'un des composants les plus déployés parmi les logiciels open source, a massivement ébranlé l'industrie technologique. Les cybercriminels sont parvenus à exploiter cette vulnérabilité (désormais connue sous le nom de Log4Shell) en seulement 12 heures, et continuent encore à le faire[5].

5 The Guardian : Une faille logicielle récemment découverte constitue « la vulnérabilité la plus critique de la dernière décennie ».

En entrant via le serveur, les hackers ont contourné les mesures de sécurité protégeant l'infrastructure.

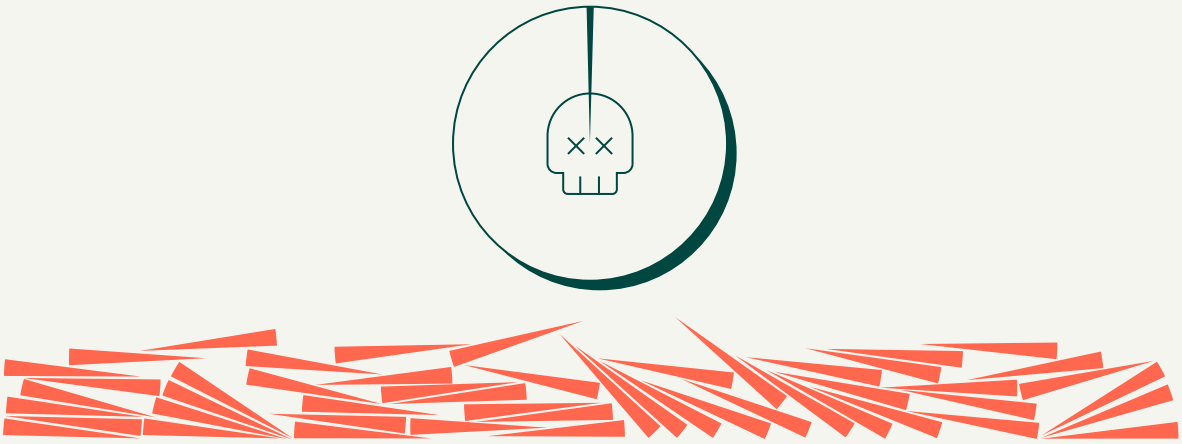
Les hackers ont utilisé tout un ensemble d'outils légitimes pour créer des identifiants illicites, élargir leur intrusion, créer de nouveaux points d'ancrage dans l'environnement et compromettre le système Active Directory.

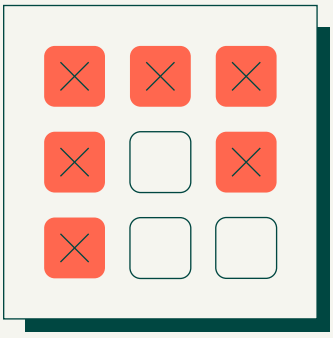
Les cybercriminels ont progressé latéralement dans l'infrastructure de l'Université de Stone pour mettre la main sur cinq ordinateurs de son environnement VMware et, ce faisant, recueillir des détails stratégiques. Et tout cela à l'insu de l'établissement.

L'expérience de l'Université de Stone, bien qu'alarmante, est étonnamment commune à en juger par ce qu'ont vécu de nombreuses organisations l'an dernier. ®

99 %

des responsables informatiques et de la cybersécurité ont eu connaissance d'au moins une attaque en 2022. En moyenne, **ils ont été confrontés à 52 attaques en 2022.**





61 %

de ces attaques ont impacté des applications SaaS, l'environnement le plus communément visé.

DANS LES PROFONDEURS DES DONNÉES :

Tous les types d'environnements ont été touchés par des activités malveillantes dans les proportions suivantes :

61 %
SaaS

62 %
Cloud

50 %
On-premise

Selon Expel, le nombre d'incidents malveillants perpétrés dans les trois principaux clouds publics a augmenté de 70 % entre 2021 et 2022.

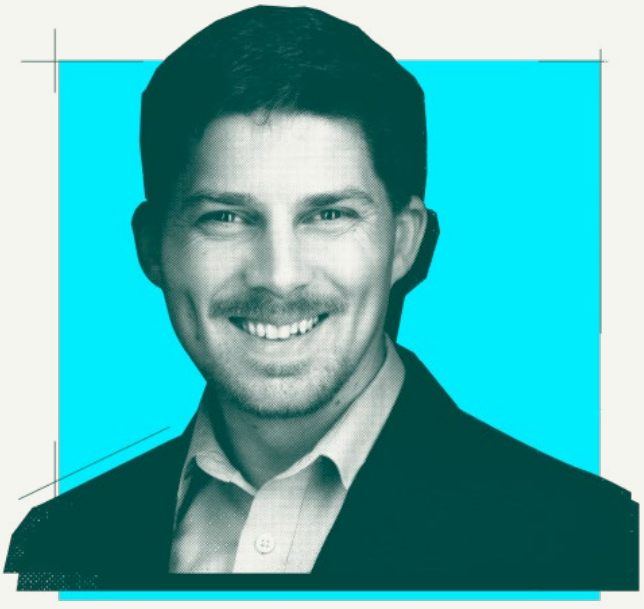
Remarque : les trois clouds publics référencés sont Amazon Web Services (AWS), Google Cloud Platform (GCP) et Microsoft Azure (Azure).[6]

Après avoir exploité la vulnérabilité et mis la main sur l'environnement de l'Université de Stone, les cybercriminels ont rapidement utilisé les identifiants illicites à des fins malveillantes. Permiso a indiqué que la totalité des intrusions dans le cloud détectées et traitées par ses équipes étaient dues à une violation d'identifiants.[7]

Par ailleurs, 90 % des privilèges accordés à ces identifiants étaient superflus ; autrement dit, seuls 5 à 10 % des privilèges accordés étaient réellement utilisés.[8]

« La plupart des entreprises n'ont que peu de visibilité, voire aucune, sur la manière dont leurs identités sont utilisées... elles ne sont ni surveillées ni auditées...et ne sont pas si faciles à détecter lorsqu'elles sont corrompues. Avec l'essor des écosystèmes axés sur les API, on observe des fuites au niveau de ces identités, qui se propagent à un rythme ahurissant au point d'augmenter sensiblement le nombre de clés, jetons et certificats corrompus. »

Ian Ahl, VP et directeur de P0 Labs, Permiso



6 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
7 https://permiso.io/blog/s/permiso-2022-end-of-year-observations
8 https://permiso.io/blog/s/permiso-2022-end-of-year-observations

JOUR 4 :
PRÉPARATION À L'ATTAQUE DE RANSOMWARE

TOC, TOC!

En règle générale, les organisations ne s'aperçoivent qu'elles sont victimes d'une attaque que lorsque les hackers les en informent.

Toujours à l'insu de leur victime, **les cybercriminels se sont préparés à révéler leur intrusion.**

Ils ont veillé à s'emparer de plusieurs points d'accès sur les systèmes de l'Université de Stone. Résultat...

L'UNIVERSITÉ DE STONE NE POUVAIT PAS EMPÊCHER LEUR PROGRESSION EN FERMANT UNE SIMPLE PORTE.

Ils ont également créé un accès à un serveur de sauvegarde de **données traditionnel pour observer les actions de l'établissement.**

Ironie du sort : l'Université de Stone avait entrepris de changer de fournisseur et de technologie de sauvegarde, sans prendre la peine de retirer de son environnement ce serveur devenu inutile.

Au bout du compte,
les cybercriminels ont exfiltré huit gigaoctets (Go) de données de l'ensemble de l'environnement de l'Université de Stone.

La présence des cybercriminels

N'A JAMAIS ÉTÉ DÉTECTÉE

pendant ce processus.

Les attaques de ransomware sont-elles fréquentes ? ®

40 %

40 % des entreprises externes interrogées ont indiqué avoir été réellement victimes d'une attaque de ransomware.

11 %

Selon Expel, 11 % de l'ensemble des événements malveillants recensés par son SOC étaient liés à des activités de ransomware.[9]

18 %

Mandiant estime que 18 % de ses missions étaient liées à des attaques de ransomware.[10]

DANS LES PROFONDEURS DES DONNÉES :

Les cyberattaques sont-elles fréquentes ?
Types d'attaques subies par les organisations externes en 2022 :

- 59 % de violations de données
- 54 % de violations des e-mails professionnels ou de transfert frauduleux
- 41 % de menaces internes
- 40 % de ransomware

Le comportement des hackers qui ont ciblé l'Université de Stone est cohérent avec les temps de séjour médians observés par Mandiant dans le monde :

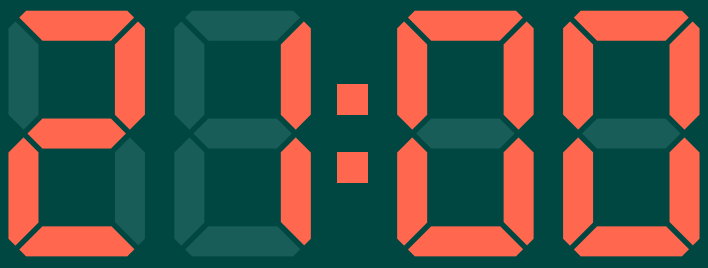
- Temps de séjour médian (échelle mondiale)
- 16 jours - Totalité des enquêtes (espionnage, gain financier, issue inconnue, etc.)
- 9 jours - Enquêtes sur le ransomware uniquement (18 % de la totalité des enquêtes réalisées par Mandiant)
- Les temps de séjour observés lors des enquêtes sur le ransomware sont généralement plus courts, car le hacker signale lui-même sa présence en envoyant la lettre de rançon ou en chiffrant un environnement.[11]

9 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/
10 https://www.mandiant.com/m-trends
11 https://www.mandiant.com/m-trends

JOUR 5 :
DÉPLOIEMENT DU RANSOMWARE

OH NON

Les hackers de l'Université de Stone ont amorcé les phases de demande de rançon le dimanche soir à environ 21 h.



Ils se sont servi d'AvosLocker pour chiffrer les fichiers de l'environnement VMware ESXi sur 150 machines virtuelles, dont les cinq initialement chiffrées au moment de leur intrusion.

AvosLocker a également déclenché l'arrêt des outils de gestion des machines virtuelles peu avant le début du chiffrement des fichiers afin d'empêcher l'Université de Stone de réagir de manière efficace.

AvosLocker

Le terme AvosLocker est employé pour décrire à la fois une famille de logiciels malveillants et un groupe de cybercriminels. Il fonctionne selon le principe du « ransomware as a Service », où les adhérents s'abonnent à un service pour exécuter des déploiements de ransomware et collecter des rançons. Dans le cas d'AvosLocker, l'abonnement couvre la gestion directe des négociations de rançons, la publication et l'hébergement des données exfiltrées des victimes, ainsi que l'utilisation proprement dite d'un outil de ransomware spécifique[12].

12 https://www.cisa.gov/news-events/alerts/2022/03/22/fbi-and-fincen-release-advisory-avoslocker-ransomware

C'est alors que les hackers ont publié leurs demandes de rançon

Le ransomware entre en scène au **MILIEU** du parcours ; ni au début, ni à la fin.

D’aucuns pensent que le chiffrement intervient à la fin de l’événement de ransomware, mais cela n’est pratiquement jamais le cas. Ainsi, dans le cas qui nous intéresse, les cybercriminels disposaient depuis des jours, à l’insu de l’université, d’un accès illimité à ses systèmes. Et il a fallu encore plusieurs jours avant que son attaque de ransomware ne trouve une issue.

DANS LES PROFONDEURS DES DONNÉES :

Le ransomware est un type de menace par déni de données.

Le déni de données peut impliquer du ransomware, des wipers, la suppression de données à l'aide d'accès valides et des efforts de déni de service. Qui plus est, les cybercriminels ont pour habitude d'exfiltrer des données à diverses fins avant de procéder au chiffrement proprement dit.

En 2022, l'équipe de réponse au ransomware de Rubrik a aidé des dizaines d'organisations à restaurer leurs données.

Voici les familles de ransomware
qui ont été les plus couramment rencontrées :

- LOCKBIT2.0
- BLACKCAT/ALPHV
- AVOSLOCKER
- META
- PLAY
- HIVE
- SPARTA
- BLACK BASTA
- SPIDER
- VICE Society

REPRENEZ LE CONTRÔLE

Votre capacité à combattre les hackers dépend de votre degré de préparation

Les services de l'Université de Stone ont rapidement commencé à travailler sur l'incident, mais ils étaient limité par l'ampleur du chiffrement.

Pour surmonter ce problème, ils ont décidé de restaurer les données dans des environnements d'analyse et de test afin d'entreprendre leur travail d'enquête et de prioriser leurs prochaines actions.

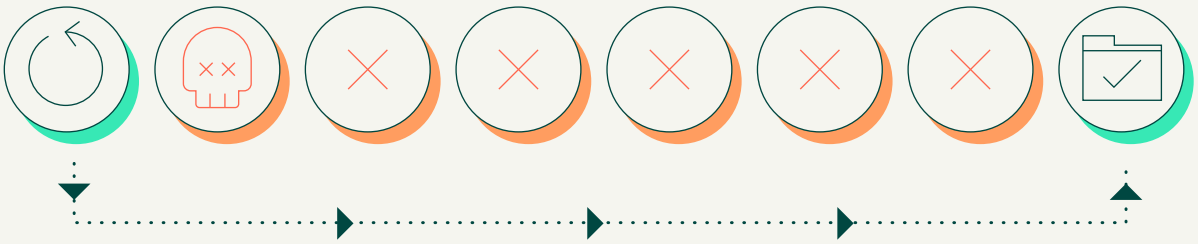
En parallèle, ils ont analysé les sauvegardes de données hors ligne, détecté un serveur potentiellement corrompu et monté ce serveur dans leur environnement d'analyse en vue d'une enquête plus poussée.

C'est là qu'ils ont touché le JACKPOT

L'université a mis la main sur les notes des hackers, notamment leur plan d'attaque, les comptes corrompus et la chronologie de l'intrusion. D'autres enquêtes ont permis de révéler sept autres serveurs corrompus et d'identifier le point d'intrusion initial.

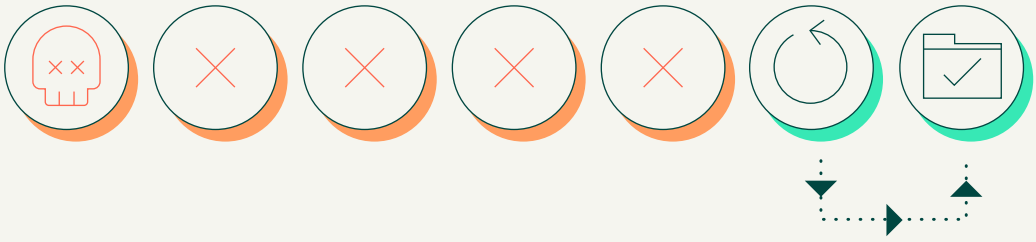
Ainsi encouragée, l'Université de Stone a commencé rapidement à reconstruire son environnement en deux temps :

Premièrement, les serveurs effectivement touchés par l'intrusion initiale



L'équipe de l'Université de Stone est parvenue à restaurer les huit serveurs corrompus hébergés dans cinq machines virtuelles à un point dans le temps correspondant à la veille de l'intrusion des hackers, ce qui a représenté une perte totale de six jours de données.

Deuxièmement, les serveurs chiffrés par le ransomware, mais qui ne faisaient pas partie de l'attaque initiale.



Il restait encore 145 machines virtuelles à restaurer. Mais ces systèmes, qui n'avaient subi qu'un simple chiffrement, ont nécessité moins d'efforts de la part de l'équipe. Ils ont été restaurés à partir de sauvegardes créées la veille du déploiement du ransomware, ce qui a évité de perdre cinq jours de données supplémentaires sur l'ensemble de ces 145 VM.

L'opération de restauration globale a également coûté à l'organisation de nouveaux hôtes ESXi, un nouveau vCenter et une reconstruction d'Active Directory.

Parmi toutes les issues possibles, celle-ci était la plus favorable que l'Université de Stone pouvait espérer. Rendue optimiste par les progrès réalisés, l'Université de Stone était bien décidée à ne pas payer de rançon.

Il peut sembler facile de passer sans voir le premier écueil majeur d'un incident de chiffrement :

Comment diagnostiquer et analyser quelque chose qui est chiffré ? Payer la rançon vaut-il vraiment la peine ? Une solide préparation à cette phase initiale de chiffrement, avec la création de copies, assure de bonnes chances de réussite. L'Université de Stone était préparée, mais comment s'assurer que l'on est vraiment prêt ?

Payer la rançon vaut-il vraiment la peine ? (WR)

46 %

Les organisations externes qui ont payé une rançon n'ont constaté qu'un intérêt limité à utiliser les solutions de déchiffrement proposées par les hackers : 46 % ont pu restaurer la moitié de leurs données, voire moins, avec l'aide des hackers.

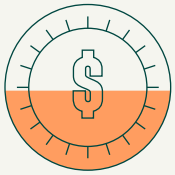
16 %

Seules 16 % de la totalité des organisations externes ont pu récupérer l'ensemble de leurs données à l'aide des outils de déchiffrement fournis par les cybercriminels.

Les données de télémétrie de Rubrik ont révélé la prévalence des signes précurseurs et les taux de chiffrement du ransomware. ®

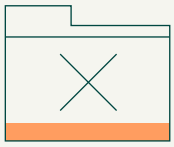
75 %

des organisations mondiale ont observé un certain niveau d'activité anormale.



48 %

des organisations mondiales ont observé une forme de tentative de ransomware à leur encontre.



15 %

des organisations mondiales ont observé au sein de leur environnement une forme de chiffrement réussi nécessitant une restauration des données.

Moins de **0,004 %** des données sécurisées ont été chiffrées. ®

CHIFFRES DE RÉFÉRENCE :

Détection des comportements anormaux
La détection des comportements anormaux constitue la première étape d'un processus en deux phases pour identifier le ransomware. Au cours de ce processus, Rubrik analyse les métadonnées du système de fichiers afin d'identifier tout comportement anormal, par exemple un nombre inhabituel de fichiers ajoutés, supprimés ou répliqués. La plupart des activités anormales ne sont pas imputables à du ransomware, mais elles nécessitent une enquête suivie.

Détection de fichiers suspects
La seconde étape du processus d'identification du ransomware consiste à détecter les fichiers suspects. Pour cette étape, on a recours à l'IA et au machine learning pour évaluer les fichiers identifiés au cours de l'étape de détection des comportements anormaux, en observant l'entropie des données, les extensions de fichiers, les opérations de compression, les actions malveillantes connues et associées au ransomware, ainsi que divers autres facteurs indiquant la présence de ransomware.

Analyse des snapshots
Un snapshot est une copie de la sauvegarde de données hors ligne qui est généralement exécutée selon un modèle récurrent et automatisé ou dans le cadre de tâches ponctuelles. Des tâches analytiques peuvent ensuite être réalisées à partir des snapshots créés.

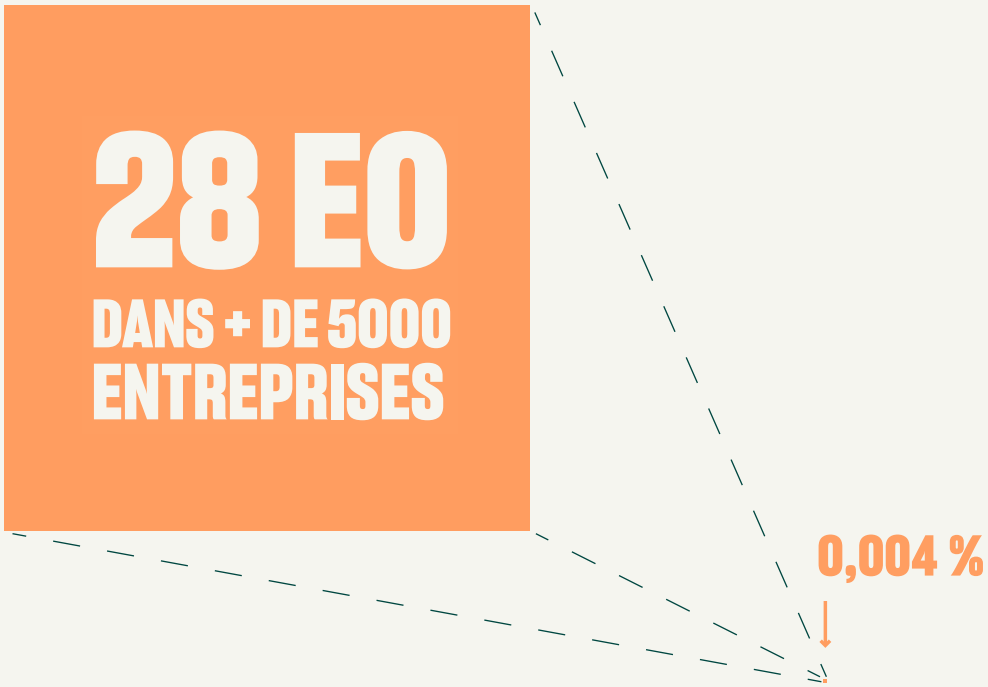
- 27 266 649 snapshots ont été évalués chez l'ensemble des clients Rubrik afin d'identifier des activités de ransomware.
- 20 692 snapshots, soit 0,07 % du nombre total de snapshots, contenaient une activité anormale.
- 1 198 de ces snapshots anormaux, soit 6 % de toutes les activités anormales, ont conduit à un chiffrement empêchant l'exécution des snapshots.
- Sur l'ensemble des snapshots évalués, seuls 0,004 % présentaient un problème de chiffrement. Tous les chiffrements avaient été précédemment identifiés comme une activité anormale.
- 100 % des chiffrements étaient liés à une absence d'authentification multifacteur.

Parmi tous les clients Rubrik en 2022 ®

moins de 0,004 % de toutes les données sécurisées nécessitaient une analyse complémentaire ou indiquaient une activité de ransomware.

Cela donne une bonne idée de la manière dont une organisation peut prendre le contrôle de sa surface de menace.

Il est pratiquement impossible de protéger votre organisation contre l'immense étendue des menaces, mais il existe de bons moyens d'éradiquer de grandes parties de la zone à risque sur cette surface d'attaque.



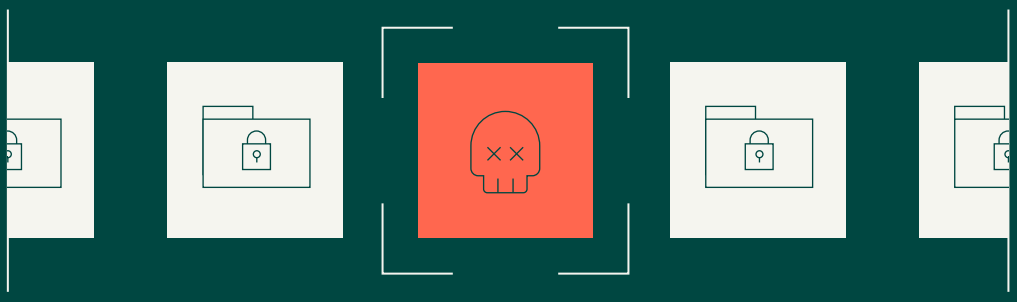
JOUR 8 :
DEUXIÈME DEMANDE DE RANÇON

MAIS QU'EST-CE QU'IL SE PASSE...?

Le chiffrement n'est pas la seule arme (ou l'arme de prédilection) des hackers

3 JOURS APRÈS

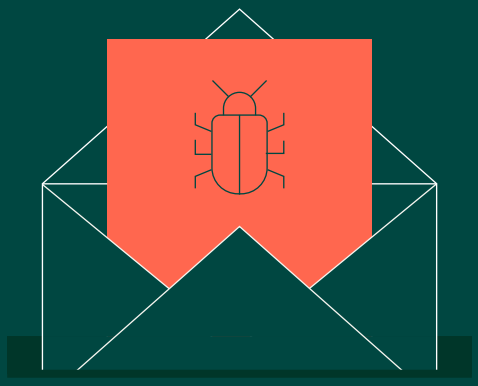
La première demande de rançon, les hackers en ont envoyé une deuxième, dans laquelle ils menaçaient de transmettre les 8 Go de données exfiltrées sur un site de fuite contrôlé par AvosLocker si l'université ne payait pas la rançon sous quatre jours.



Ils ont également tenté de corrompre de nouvelles parties de l'environnement de l'Université de Stone pour tenter de contrer ses réactions.

Après un début prometteur, ce revirement inattendu a ramené l'Université de Stone au point de départ et l'a laissée aux prises avec un lourd dilemme :

payer la rançon ou voir ses données divulguées en ligne.



72 %

des organisations non clientes de Rubrik disent avoir déjà payé une demande de rançon.[WR]

DANS LES PROFONDEURS DES DONNÉES :

Pour les organisations non clientes de Rubrik qui ont accepté de payer une rançon, les proportions sont les suivantes : (WR)

40 %

ont payé la demande de rançon à la suite de chiffrements.

37 %

ont payé une demande de rançon en raison de menaces de fuite de données.

Montants des rançons observés en 2022 dans le rapport Unit 42 Incident Responses de Palo Alto Networks : (ER)

+ de 50 M$

Demande de rançon la plus élevée

+ de 7 M$

Rançons les plus élevées payées[13]

13https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report

INSPIREZ

La visibilité sur les données crée des opportunités

Pour gérer la demande de rançon et éviter une fuite de ses données, l'Université de Stone a décomposé sa réponse en trois efforts distincts.

1

Premièrement, elle a entrepris des efforts de détection et de réponse afin d'identifier et contrer les tentatives d'intrusion ultérieures. Cette initiative lui a valu de remplacer plusieurs serveurs et pare-feu et de prendre d'autres mesures de durcissement.

2

Deuxièmement, elle a poursuivi ses efforts de restauration de données en testant des parties des environnements restaurés avant de les déplacer dans son environnement de production.

NEW
3

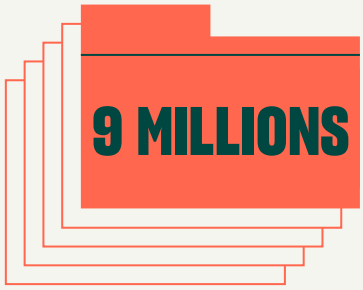
Troisièmement, l'Université de Stone a commencé à évaluer l'impact d'une divulgation en ligne de ses données volées.

Mais...

Les problèmes persistants de chiffrement empêchaient l'Université de savoir si les hackers avaient réellement volé 8 Go de données, ou de déterminer quelles données avaient été dérobées.

Résultat...

Elle a choisi de migrer ses opérations d'évaluation d'impact vers sa sauvegarde de données la plus récente.

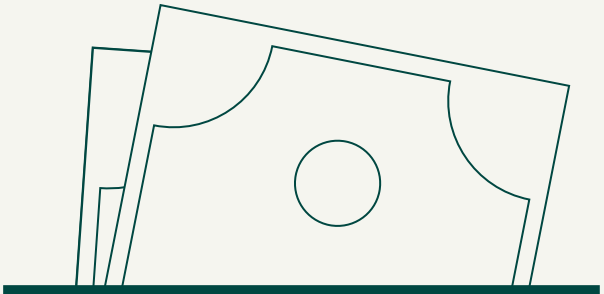


La bonne nouvelle

C'est que l'Université de Stone a trouvé des réponses en 24 heures et disposait alors de trois jours pour prendre des décisions en connaissance de cause.

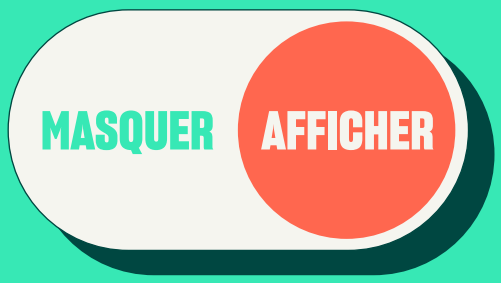
La mauvaise nouvelle

C'est que les hackers étaient parvenus à voler 8 Go de données contenant plus de 9 millions d'enregistrements sensibles remontant, pour les plus anciens, à 2013.



L'UNIVERSITÉ DE STONE A DÉCIDÉ DE NE PAS PAYER LA DEUXIÈME RANÇON POUR NE PAS REMPLIR LES POCHES DES CYBERCRIMINELS.

Bien qu'elle sache que la publication de ses données sensibles serait un énorme coup dur, elle a aussi pris conscience d'une cruelle vérité : il n'y avait aucune garantie **que ces données sensibles ne soient pas divulguées, même si elle payait la rançon.**



L'Université de Stone a préféré mettre à profit les trois jours dont elle disposait pour informer en amont les personnes physiques et morales concernées.

Avant que les données ne soient publiées, l'Université de Stone avait accompli une lourde tâche, et pourtant nécessaire : réaliser toutes les actions de réponse essentielles...

- ✓ Notifier les organismes de réglementation et de conformité
- ✓ Contacter les personnes concernées
- ✓ Entreprendre des améliorations à long terme et les autres mesures indispensables en lien avec une fuite de données

Effet domino

Dans l'ensemble, l'université de Stone est revenue à la normale une fois l'intrusion terminée. Cependant, l'attaque de ransomware longue de deux semaines a provoqué un effet domino dont a résolution a nécessité plusieurs semaines, voire plusieurs mois de travail et une série de décisions.

Un déplacement et une dispersion rapides des données présentent un risque réel pour les organisations.[RT]

Une organisation moyenne possède

fichiers renfermant des données sensibles

et

enregistrements de données sensibles au total

Différence entre fichiers et enregistrements de données sensibles : les fichiers contiennent des enregistrements de données. Certains de ces enregistrements peuvent être sensibles. Par exemple, une feuille de calcul peut contenir des centaines d'enregistrements de données sensibles, tandis que d'autres fichiers peuvent n'en contenir aucun.

Une organisation type contient suffisamment de données sensibles pour atteindre le plafond de toutes les pénalités financières

DANS LES PROFONDEURS DES DONNÉES :

Si chaque organisation mondiale est assise sur un immense volume de données, certaines de ces données peuvent potentiellement causer un terrible préjudice si elles deviennent subitement indisponibles ou corrompues.

Les données sensibles en sont un bon exemple : ces données sont couvertes par différentes normes ou réglementations sectorielles, notamment la PII, l'HIPAA, le RGPD et la CPAA[14,15,16,17].

Pour les consommateurs comme pour les organisations, il est difficile à plus d'un titre d'évaluer les impacts sur les données, mais les pénalités financières associées aux données sensibles ne laissent qu'une option[18,19,20].

QUELQUES EXEMPLES :

RGPD
Pénalité en cas d'exposition de données sensibles : jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires global de l'entreprise en cas de violations graves, en retenant la plus grande de ces valeurs.

Dans un environnement classique, il faudrait une amende de moins de deux euros par enregistrement pour atteindre un montant de 20 millions d'euros.

HIPAA
Pénalité en cas d'exposition de données sensibles : entre 50 et 50 000 $ par violation, avec un plafond de 1,5 million de dollars US.

En prenant seulement le nombre moyen de fichiers dans un environnement type, la pénalité maximale de 1,5 million de dollars US serait très largement dépassée, s'élevant à un total de 28 millions de dollars US en prenant la base de la pénalité la plus faible (50 $).

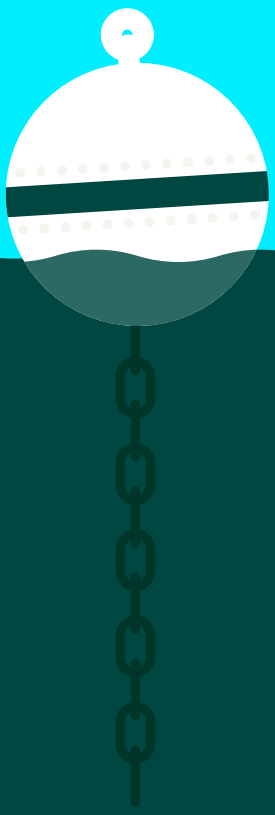
CPRA
Pénalité en cas d'exposition de données sensibles : jusqu'à 2 500 $ par violation, ou jusqu'à 7 500 $ pour chaque violation intentionnelle. Aucun plafond de pénalité.

Le nombre de fichiers d'une organisation type pourrait, à lui seul, entraîner une amende de 1,1 milliard de dollars.

14 https://gdpr-info.eu/art-4-gdpr/
15 https://www.cdc.gov/phlp/publications/topic/hipaa.html
16 https://www.dol.gov/general/ppii
17 https://oag.ca.gov/privacy/ccpa#:~:text=The%20right%20to%20limit%20the,personal%20information%20collected%20about%20them.
18 https://gdpr-info.eu/issues/fines-penalties/#:~:text=83(5)%20GDPR%2C%20the,fiscal%20year%2C%20whichever%20is%20higher.
19 https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/north-america/united-states/topics/penalties-for-non-compliance
20 https://cppa.ca.gov/

IMPACT

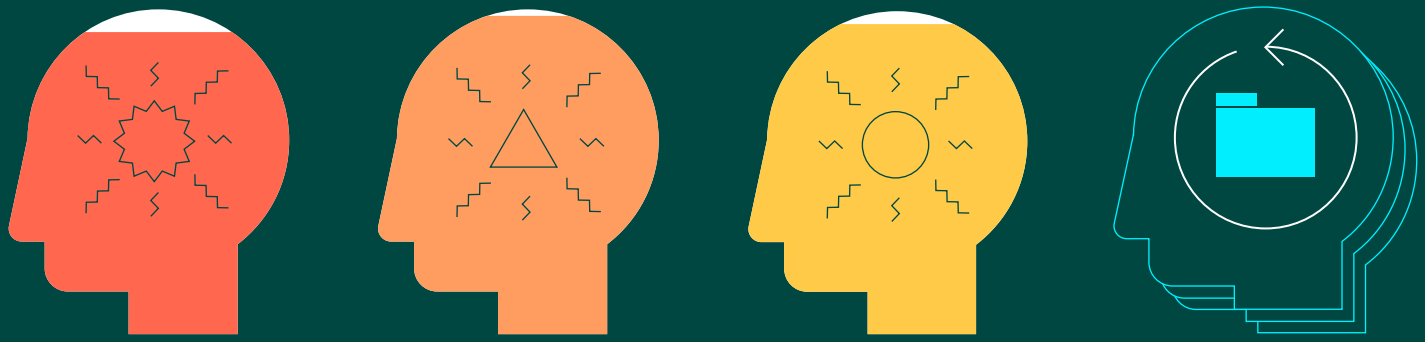
Chaque intrusion a sa conclusion naturelle,
mais nous ne devrions jamais relâcher notre attention
à la fin de l'incident. Imaginons plutôt que nous remontons
à la surface de notre océan de données.



Que faut-il retenir de notre aventure
dans les profondeurs de l'océan que représente
la sécurité des données ?
Que doit-on changer dès maintenant ?

Les intrusions ont un impact économique et humain ®

Les impacts de ces intrusions touchent aussi bien l'entreprise que les personnes, et cela bien après la fin du travail d'enquête et de l'application de mesures IT. Cette persistance nous fait douter de notre capacité à mener notre activité.



93 %

des organisations externes victimes d'une cyberattaque en 2022 ont constaté un impact négatif.

98 %

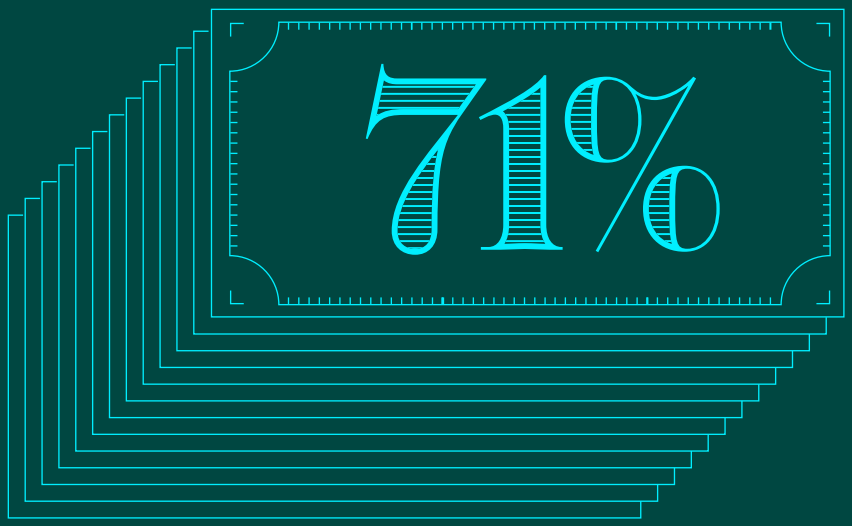
des DSI et RSSI disent avoir été fortement affectés, émotionnellement et/ou psychologiquement, par ces cyberattaques en 2022.

96 %

des DSI et RSSI craignent de ne pas pouvoir assurer la continuité des activités de leur organisation si celle-ci est victime d'une cyberattaque.

39 %

Plus d'un tiers des responsables interrogés pensent que leurs administrateurs ou cadres dirigeants n'ont que peu confiance, voire aucune confiance, dans la capacité de leur organisation à restaurer des données et applications stratégiques en cas de cyberattaque.



des organisations externes sont susceptibles de payer une demande de rançon

93 % des entreprises victimes d'une cyberattaque en 2022 indiquent avoir subi des impacts négatifs : ®

49 %
Perte de clients

45 %
Perte de revenus

44 %
Mauvaise presse ou une atteinte à la réputation

42 %
Changement forcé de direction

5 %
Impact négatif sur le cours de l'action

Ces attaques exercent une lourde pression sur les cadres dirigeants : 98 % signalent d'importants troubles émotionnels et/ou psychologiques liés à des cyberattaques l'an dernier.

53 %
Davantage d'anxiété face à leurs responsabilités

46 %
Inquiétude pour la sécurité de leur emploi

43 %
Perte de confiance entre collaborateurs et membres de l'équipe

41 %
Perte de sommeil ou difficulté à dormir

Des problèmes faisant suite à l'intrusion s'ajoutent aux problèmes déjà présents ®

Les intrusions ne sont pas des événements isolés. Il y avait des difficultés avant l'intrusion, et à ces obstacles existants s'ajoutent désormais des impacts post-intrusion prévisibles.

47 %

Près de la moitié (47 %) des RSI et des responsables de la sécurité pensent que leur budget 2023 dédié à la cybersécurité est insuffisant

27 %

27 % de ces mêmes responsables s'attendent à ce que leurs budgets IT/cybersécurité diminuent en 2023.

4 %

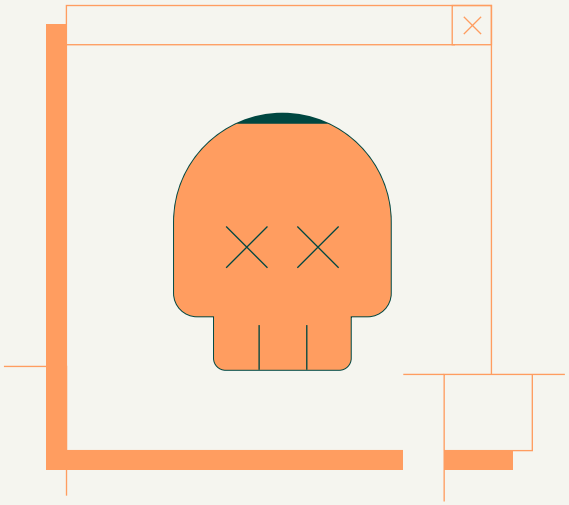
Les RSI et les responsables de la sécurité devront veiller à fédérer leurs équipes ; seuls 4 % d'entre eux estiment qu'il n'existe aucun facteur limitant l'alignement entre équipes IT et de sécurité.

Voici les cinq problèmes majeurs qui contribuent au décalage entre les équipes IT et de sécurité dans la défense contre les cyberattaques : (WR)

1. **52 %** — Suites d'outils distinctes
2. **51 %** — Écarts de visibilité
3. **50 %** — Priorités contradictoires
4. **47 %** — Absence de planification ou de processus formels
5. **45 %** — Désalignement des structures de direction

Les intrusions recèlent des opportunités positives (WR)

Mais il y a tout de même de la lumière au bout du tunnel : votre organisation peut survivre et surmonter victorieusement les menaces inévitables. Ces mêmes intrusions présentent des opportunités d'amélioration et d'évolution.



99 %

des organisations ayant été victimes d'une cyberattaque en 2022 ont mis en œuvre de nouvelles actions :

48 %

ont changé de fournisseur ou de partenaire tiers afin de produire de meilleurs résultats

54 %

ont augmenté leurs dépenses dans de nouvelles technologies ou de nouveaux services

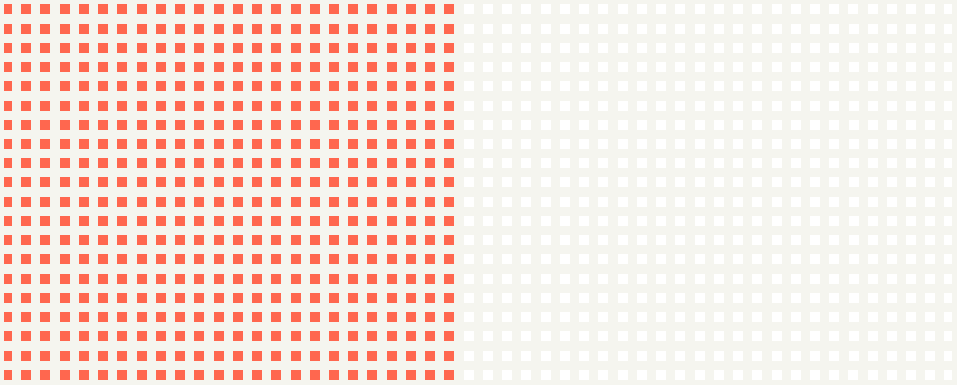
43 %

ont recruté du personnel supplémentaire

Malgré tous ces défis, les organisations s'améliorent dans l'ensemble ®

Mais il n'est pas nécessaire d'attendre une cyberattaque pour opérer des transformations. En nous préparant à saisir les opportunités qui se présentent en situation de crise, mais aussi en travaillant sur une résilience systémique, nous pouvons obtenir des résultats positifs.

Alors que **48 %** des clients Rubrik avaient subi une forme de ransomware...



Moins de **0,004 %** des données sécurisées ont été chiffrées.

Rubrik Zero Labs a constaté que certaines organisations avaient introduit des améliorations positives tout au long de l'année 2022, et s'attend à ce que cette tendance se poursuive en 2023.
Cette amélioration est perceptible dans tous les secteurs d'activité et dans l'ensemble des régions.

16 %

Ces changements ont conduit les entreprises moyennes à renforcer leur posture de sécurité de 16 % en 2022.

97 %

Selon Expel, 97 % des tentatives de ransomware ont été déjouées avant le déploiement du ransomware.[21]

21 https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

PERSPECTIVE D'EXPEL SUR LA SÉCURITÉ DES DONNÉES : ER

11 % de tous les incidents observés par Expel en 2022 auraient pu conduire au déploiement de ransomware

97 % de ces événements ont été stoppés avant le déploiement de ransomware. Si des équipes de défense parviennent à détecter une intrusion de ransomware et à y répondre avant la fin du cycle, elles ont de bonnes chances de pouvoir déjouer les plans malveillants[22].

Rubrik mesure pour ses clients un score cumulé de sécurité des données et a observé une tendance positive et continue à l'amélioration organisationnelle. Le score de sécurité des données est calculé toutes les 24 heures d'après les catégories suivantes :

1. Sécurité de la plateforme : mesure l'efficacité de la sécurité de l'infrastructure de stockage des données et couvre diverses thématiques, comme les contrôles utilisateur, l'authentification des administrateurs, les journaux d'audit, etc.
2. Protection et restauration des données : analyse le degré de sécurité des données de sauvegarde, évalue si une copie « propre » de la dernière sauvegarde est disponible et examine d'autres facteurs associés.
3. Enquête sur le ransomware : détermine la qualité et la fréquence de la surveillance des menaces de ransomware, et évalue si ces données sont récupérables après un incident de chiffrement.
4. Découverte des données sensibles : mesure le degré de protection des données sensibles, les contrôles d'accès pour ces données et si la restauration des données sensibles est priorisée.
5. Les scores sont évalués de la manière suivante :
   - 0-50 : non satisfaisant
   - 51-75 : besoin d'amélioration
   - 76-90 : satisfaisant
   - 91 et plus : excellent

Une organisation mondiale type a vu son score augmenter de **51,2** à **59,47** en 2022, soit une hausse de **16 %**.

Moyennes globales des scores : 59,47

Taux d'amélioration en 2022 : 16,2 %

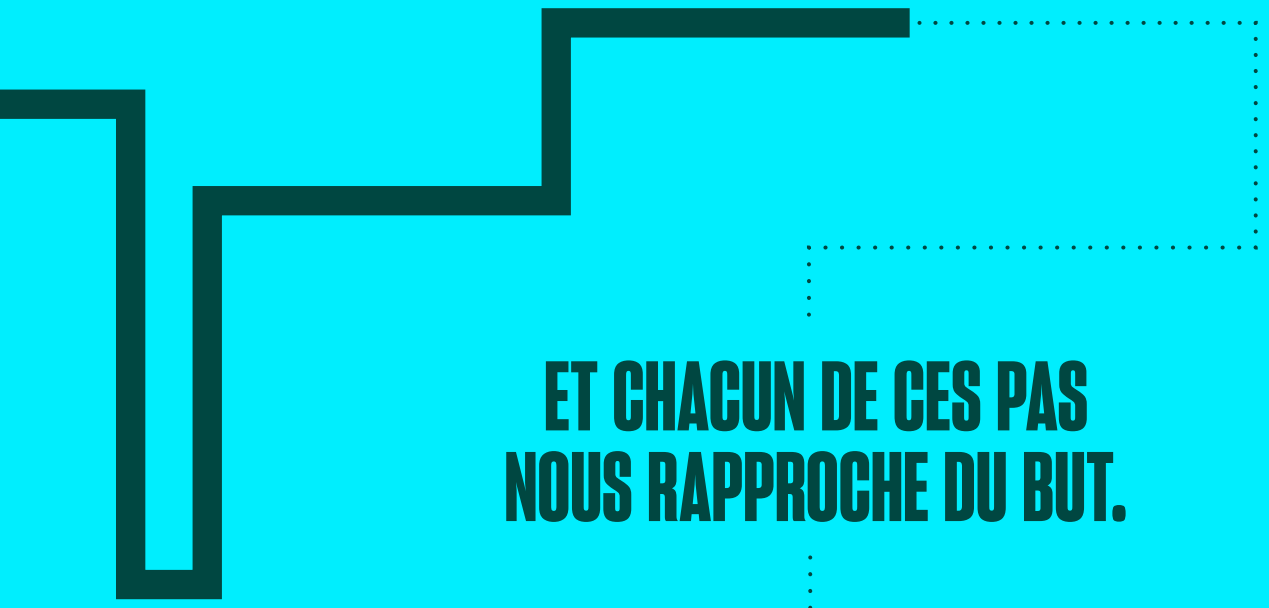
« Nous ne devons pas oublier que la sécurité n'est pas isolée de tout le reste. Alors que les entreprises cherchent à en faire plus avec moins de ressources, il y a urgence à miser sur des technologies aussi efficaces et évolutives que des options cloud. Mais une adoption rapide implique des risques, en particulier pour les entreprises qui ne sont pas nées dans le cloud. Face à l'adoption de nouvelles technologies destinées à suivre l'évolution des marchés, les équipes de sécurité peuvent probablement s'attendre à une légère hausse des incidents de sécurité, généralement dus à des mauvaises configurations qui passent facilement inaperçues et qui peuvent être tout aussi facilement exploitées, ou bien encore à des clés d'accès exposées. »

Jonathan Hencinski, VP, Opérations de sécurité, Expel

22https://expel.com/blog/2023-great-expeltations-report-top-six-findings/

Plus les attaques à l'encontre de nos communautés se multiplient, plus nous devons nous épauler les uns les autres.

Nous pouvons concevoir de meilleurs produits et services et défendre des pratiques d'excellence, mais nous devons aussi partager ce que nous avons appris. Chaque nouvel enseignement est un pas en avant.



ET CHACUN DE CES PAS NOUS RAPPROCHE DU BUT.

Dans cette logique, le Rubrik Zero Labs tient à terminer là où il a commencé : en remerciant les quatre organisations qui nous ont autorisés à exploiter leurs données, en témoignant notre reconnaissance à Wakefield Research pour le travail accompli, en remerciant Shaped By pour son travail de rédaction de cette étude de cas, et en saluant les contributions d'Amanda O'Callaghan, Ajay Kumar Gaddam, Sham Reddy, Kumar Subramanian, Linda Nguyen, Lynda Hall, Kelsey Shively, Kelley Cooper, tous collaborateurs de Rubrik, pour leur participation directe à cet effort. Sans oublier les équipes Creative et Dev de Rubrik.

Rubrik Zero Labs