Sécurisation des données

Épisode 1 Et si ?

Un scénario proposé par Stordata COMMVAULT NetApp

Synopsis

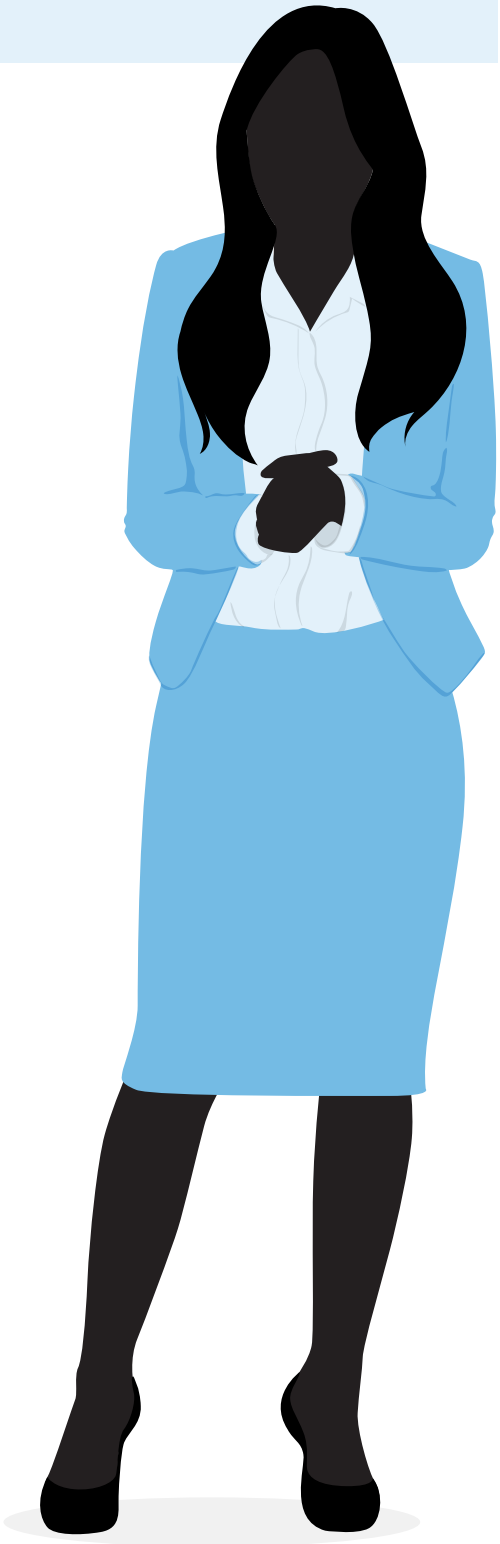
Responsable Sécurité des Systèmes d'information, Cristina Pérez mène un combat quotidien contre les attaques informatiques et le risque de ransomware. L'actualité ne cesse de lui rappeler l'urgence de prendre des mesures supplémentaires.

Pour protéger les données de son entreprise des conséquences d'un chiffrement frauduleux, Cristina opte pour une sauvegarde avec CommVault sur une baie NetApp StorageGrid en mode objet. Bien lui en prend au vu des évènements qui suivent.

Le personnage principal

Cristina Pérez est la nouvelle RSSI d'une ETI sous-traitante pour l'industrie aéronautique.

Son prédécesseur, à quelques jours de la retraite, lui remet les clés d'un système qui abrite des données hautement critiques partagées avec de grands constructeurs.



La séquence d'ouverture

FIN FÉVRIER 2020 — SIÈGE DE L'ENTREPRISE - BUREAU DE CRISTINA AU MATIN

Cristina souffle sur le café brûlant en écoutant le DSI faire le point sur les dernières formations dispensées aux collaborateurs en matière de sécurité.

Le DSI : « *Pour la plupart des salariés, le risque est encore trop hypothétique. Néanmoins, ils ont progressé dans l'adoption des bonnes pratiques.* »

Cristina : « *C'est une bonne chose. Cela dit, face à de l'ingénierie sociale agressive et intelligente, je doute que tous soient armés. Non, il faut renforcer encore la protection des données.* »

Le DSI : « *Le budget n'est pas illimité…* »

Cristina : « *Raison de plus pour ne pas avoir à payer de rançon et essuyer des pertes pharaoniques de chiffre d'affaires.* »

L'élément déclencheur

MARS 2020 — SIÈGE DE L'ENTREPRISE — SALLE DE RÉUNION — CODIR

Le Directeur général adjoint fait part aux directeurs et responsables de service d'une note reçue récemment.

DGA : « *Notre plus gros client s'apprête à nous transférer des informations particulièrement sensibles et souhaite connaître les mesures de sécurité mises en place chez nous.* »

DSI : « *L'équipe est sous l'eau, entre les formations aux nouveaux outils, l'administration journalière, le déploiement des équipements mobiles. Nous risquons de ne pas pouvoir livrer l'information avant plusieurs semaines.* »

Cristina : « *C'est l'occasion pour nous de faire réaliser un état des lieux, de nos sauvegardes notamment. L'évaluation nous permettra de fournir au client une réponse exhaustive et objective. D'autant que ça n'a pas été fait depuis longtemps et j'ai besoin d'une vue complète pour décider d'un éventuel outillage sécurité supplémentaire.* »

Les alliés

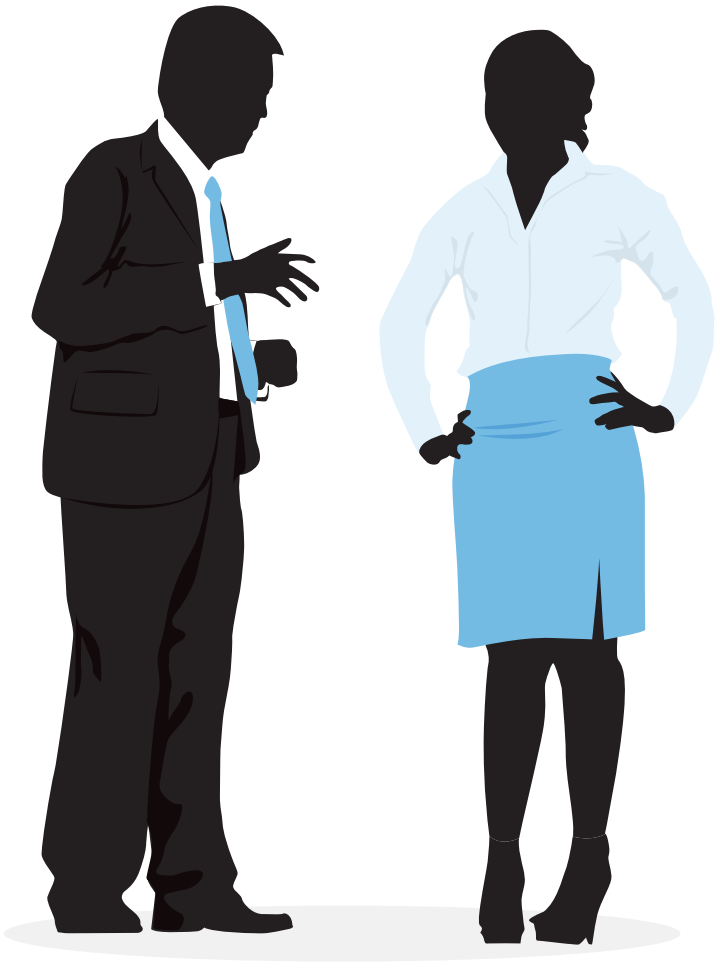
Au fil du temps et de ses expériences professionnelles, Cristina a dressé une liste de partenaires de confiance. Elle apprend que Stordata est déjà intervenue pour installer les baies de stockage NetApp que l'entreprise exploite aujourd'hui. Elle choisit de contacter l'intégrateur, qu'elle sait très compétent pour dresser l'état des lieux de ses solutions de protection de données et dont l'approche est formatrice pour l'interne.

En quelques jours, l'équipe Stordata réalise sa mission de conseil. Son intervention porte sur l'état des installations, l'évaluation de la couverture du plan de sauvegarde en place et les nouveaux éléments qui ont pu être oubliés au fur et à mesure de l'évolution du système, la fréquence des sauvegardes et sa correspondance avec les SLA fixés, le contrôle des mises à jour et l'application des best practices sécurité.

Cristina est soulagée, il n'y a pas, ou peu, de corrections à faire. Mais, pour aller plus loin, l'équipe Stordata soumet à Cristina une matrice de décisions qui lui permet d'y voir plus clair. La plupart des scénarios sont manifestement couverts, sauf la sécurité des sauvegardes, le grand enjeu de Cristina.

> C'était l'occasion pour nous de faire réaliser un état des lieux, de nos sauvegardes notamment. »

Cristina Pérez, Responsable de la Sécurité des Systèmes d'Information



Matrice de décision et plan de sécurité (extrait)

Situation	Réponse	État
Et si un serveur tombe en panne ?	Restauration de la sauvegarde	✔
Et si le réseau tombe en panne ?	Intervention de l'entreprise X (SLA contractuels)	✔
Et si mon datacenter est attaqué ?	Déclenchement du PRA	✔
Et si tout ou partie de mes données est chiffré ?	Restauration de la dernière sauvegarde	✔
Et si le serveur de sauvegarde (ou les sauvegardes) est attaqué ?	Externalisation des sauvegardes	Néant

La révélation

MARS 2020 — SIÈGE DE L'ENTREPRISE – BUREAU DE CRISTINA

Cristina : « *Oui, c'est bien ma crainte. Les logiciels malveillants deviennent assez sophistiqués aujourd'hui pour cibler spécifiquement les sauvegardes. Mais nous n'entendons pas externaliser, compte tenu de l'extrême confidentialité de nos données.* »

Stordata : « *Dans ce cas, il faut vous équiper en interne. Face aux ransomwares, les solutions de stockage basées sur du filesystem, que vous utilisez, sont devenues trop permissives. Nous préconisons de doubler les sauvegardes sur le stockage objet pour toutes vos sauvegardes d'entreprise, que les logiciels pirates ne savent pas pénétrer, en l'état actuel des connaissances.* »

Cristina : « *Nous apprécions les baies NetApp, s'il est possible de continuer avec ce constructeur.* »

Stordata : « *Mieux encore, l'association de votre actuelle solution de sauvegarde CommVault et de NetApp StorageGRID répond entièrement à votre besoin.* »

Cristina : « *Tant mieux, nous n'avions pas l'intention de changer de solution de sauvegarde non plus, vu tous les environnements qu'elle couvre ! En combien de temps pouvez-vous nous fournir ?* »

Stordata : « *En moins de 10 jours, le temps de l'intégration et du paramétrage de CommVault. Sur la base de vos 190 To de données, nous préconisons 5U et un tiroir d'extension pour vos besoins futurs. Vous serez larges.* »

Le nœud (pas si) dramatique

JUIN 2020 — SIÈGE DE L'ENTREPRISE – SALLE DES SERVEURS

L'équipe technique, son directeur et Cristina sont réunis au chevet d'un serveur de données infecté. S'ils sont irrités, ils ne sont pas inquiets.

DSI : « *Du code s'est installé silencieusement. J'ignore pour l'instant depuis combien de temps il se promène dans nos systèmes, mais il est certain que les fichiers en production et plusieurs de nos bases de données sont bel et bien chiffrés.* »

Cristina : « *Nous nous y attendions, ce n'est pas une surprise, même si le savoir-faire des pirates continue de m'épater. J'imagine que les flux de sauvegarde sont corrompus ?* »

DSI : « *Très probablement.* »

Cristina : « *Bon. Avant de restaurer une Golden Copy propre, nous allons devoir investiguer. Je contacte Stordata et nos fournisseurs d'application pour procéder à un nettoyage et une réinstallation en règle.* »

CommVault Complete Backup & Recovery

- *Cryptage intégré de bout en bout, y compris des données au repos et en transit*
- *Autodécouverte pour une protection proactive des nouveaux ensembles de données*
- *Processus automatisés et personnalisés d'instantanés et de conservation*
- *Couverture de sauvegarde pour les systèmes de fichiers, les applications, les bases de données, les machines virtuelles, les conteneurs, le SaaS et les terminaux*
- *Récupération d'un système complet, d'une instance, d'une application ou d'un seul fichier*

NetApp StorageGrid

- *Stockage capacitif et scale out*
- *Conservation WORM*
  - ✔ *Intégrité des données renforcée avec la conformité WORM*
  - ✔ *Conservation en cas de litiges*
- *Fonctionnalités avancées de sécurité et de chiffrement*
  - ✔ *Stockage objet avec compression sans perte*
  - ✔ *Chiffrement TSL (Transport Layer Security) 1.2 et AES 256 bits*
  - ✔ *Protection de l'intégrité avec faible consommation de ressources*

Le dénouement

JUILLET 2020 — SIÈGE DE L'ENTREPRISE – SALLE DE RÉUNION

Cristana expose à l'ensemble du CODIR les événements passés et les mesures qui ont été prises pour rétablir au plus vite l'entreprise dans son environnement ordinaire.

Cristina : « *En conséquence de quoi la création d'une copie immuable de nos sauvegardes a permis de rétablir la situation dans les délais les plus brefs, une fois la plateforme réinstallée. Et ce, pour un coût tout à fait contenu, qu'il s'agisse de l'achat de la baie StorageGRID, du paramétrage de notre solution CommVault vers cette destination supplémentaire ou de l'intervention de Stordata pour la remise en route.* »

DG : « *Et qu'en est-il de la rançon ?* »

Cristina : « *Nous n'avons rien payé aux hackers, je considère cela comme une victoire en soi. Comme nous n'avons jamais été dépendants de leur bon vouloir, les systèmes ont pu redémarrer avec toutes leurs données, ce qui a considérablement réduit la période d'inactivité, et donc de perte de chiffre d'affaires.* »

Le clap de fin

JUILLET 2020 — SIÈGE DE L'ENTREPRISE – BUREAU DE CRISTINA

Cristina : « *Nous aurons beau faire, l'erreur humaine reste un paramètre que nous ne maîtriserons jamais complètement. Cette sauvegarde immuable était indispensable, je suis heureuse que l'entreprise ait sauté le pas vers StorageGrid.*

Stordata : « *Et varier les types de stockage et les protocoles d'accès complique sérieusement la tâche des pirates.* »

Cristina : « *Encore faut-il avoir une solution de sauvegarde comme CommVault, capable d'écrire sur l'ensemble de ces technologies.* »

> La création d'une copie immuable de nos sauvegardes a permis de rétablir la situation dans les délais les plus brefs, une fois la plateforme réinstallée. Et ce, pour un coût tout à fait contenu… ».

Cristina Pérez, Responsable de la Sécurité des Systèmes d'Information

Stordata

Agence Île-de-France & Nord
28, rue Saint-Honoré - 78000 Versailles
Tél. : +33 1 30 21 42 42

Agence Ouest
34, quai Magellan - 44000 Nantes
Tél : +33 2 28 08 09 93

Agence Sud-Ouest
6, rue Maurice Caunes - 31200 Toulouse
Tél. : + 33 5 34 50 49 00

Agence Sud-Est
28, rue Louis Guérin - 69100 Villeurbanne
Tél. : + 33 4 78 48 09 47

Agence Est
9, rue Icare - 67960 Entzheim
Tél. : +33 3 88 76 47 64

Agence Méditérannée
Tél. : + 33 5 34 50 49 00

www.stordata.fr