RÉALISÉ PAR

EN PARTENARIAT AVEC

BAROMÈTRE DATA BREACH

PUBLICATION #2 // **2021**

Ce baromètre est animé par le Forum International de la Cybersécurité (FIC) en partenariat avec PwC et Bessé et avec la participation de la CNIL. Les données exploitées sont issues des publications de la CNIL, sur la plateforme data.gouv.fr, et de l'ANSSI. Les violations de données personnelles, notifiées à la CNIL et publiées en open data, représentent une source d'enseignements précieux pour tous les organismes traitant des données personnelles. Ce partage d'informations permet d'identifier quels sont, actuellement, les risques qui pèsent sur un organisme, sur les données qu'ils traitent et, finalement, sur les personnes concernées. Anticiper les incidents en se basant sur des cas concrets permet de cibler plus facilement les éléments à améliorer, chez soi, afin de ne pas être exposé et de se retrouver, à son tour, victime d'une violation. Valoriser ces informations profite au plus grand nombre et permet, in fine, de mieux protéger les données personnelles.

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

SOMMAIRE

1 TENDANCES GLOBALES
TOP 5 DES SECTEURS TOUCHÉS

2 LES VIOLATIONS DE DONNÉES
LES DONNÉES AFFECTÉES
LES ORIGINES DES FUITES DE DONNÉES
L'IMPACT SUR LES ENTREPRISES
L'ERREUR HUMAINE
LES PERSONNES TOUCHÉES

3 FOCUS SUR LES RANÇONGICIELS
ÉTAT DE LA MENACE DES RANÇONGICIELS
RETEX D'UNE ATTAQUE
TENDANCES
COMMENT S'EN PRÉMUNIR ?

4 TÉMOIGNAGE D'UN RSSI
LA VALORISATION FINANCIÈRE DES RISQUES

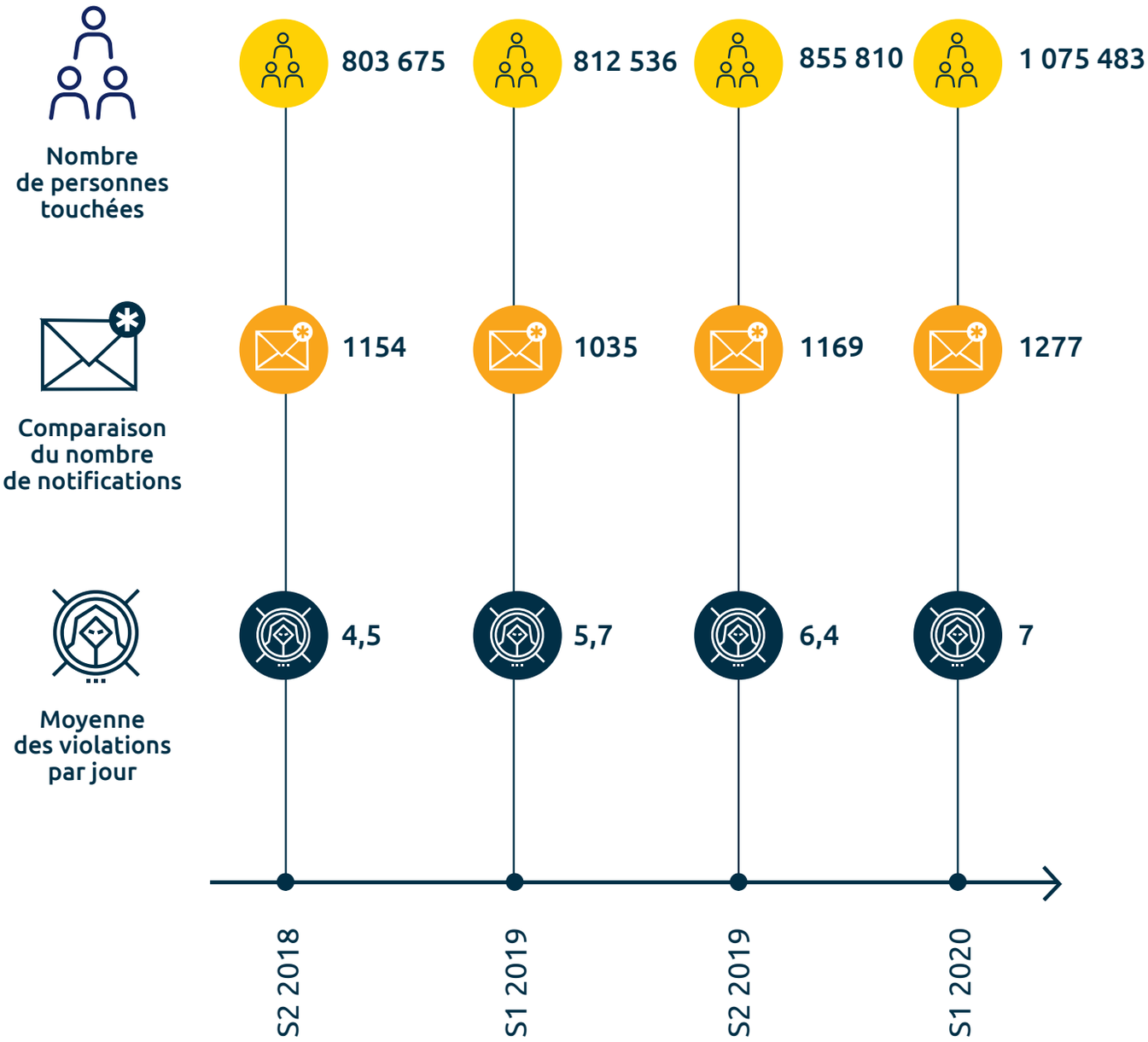
5 RGPD : 3 ANS DÉJÀ !
LES MISSIONS DU DPO
SON RÔLE CONTRE LES CYBERATTAQUES

6 TÉMOIGNAGE D'UN DPO
FACE AUX CYBERMENACES

7 LÉGISLATIONS
EN MATIÈRE DE PROTECTION
DES DONNÉES PERSONNELLES
DANS LE MONDE

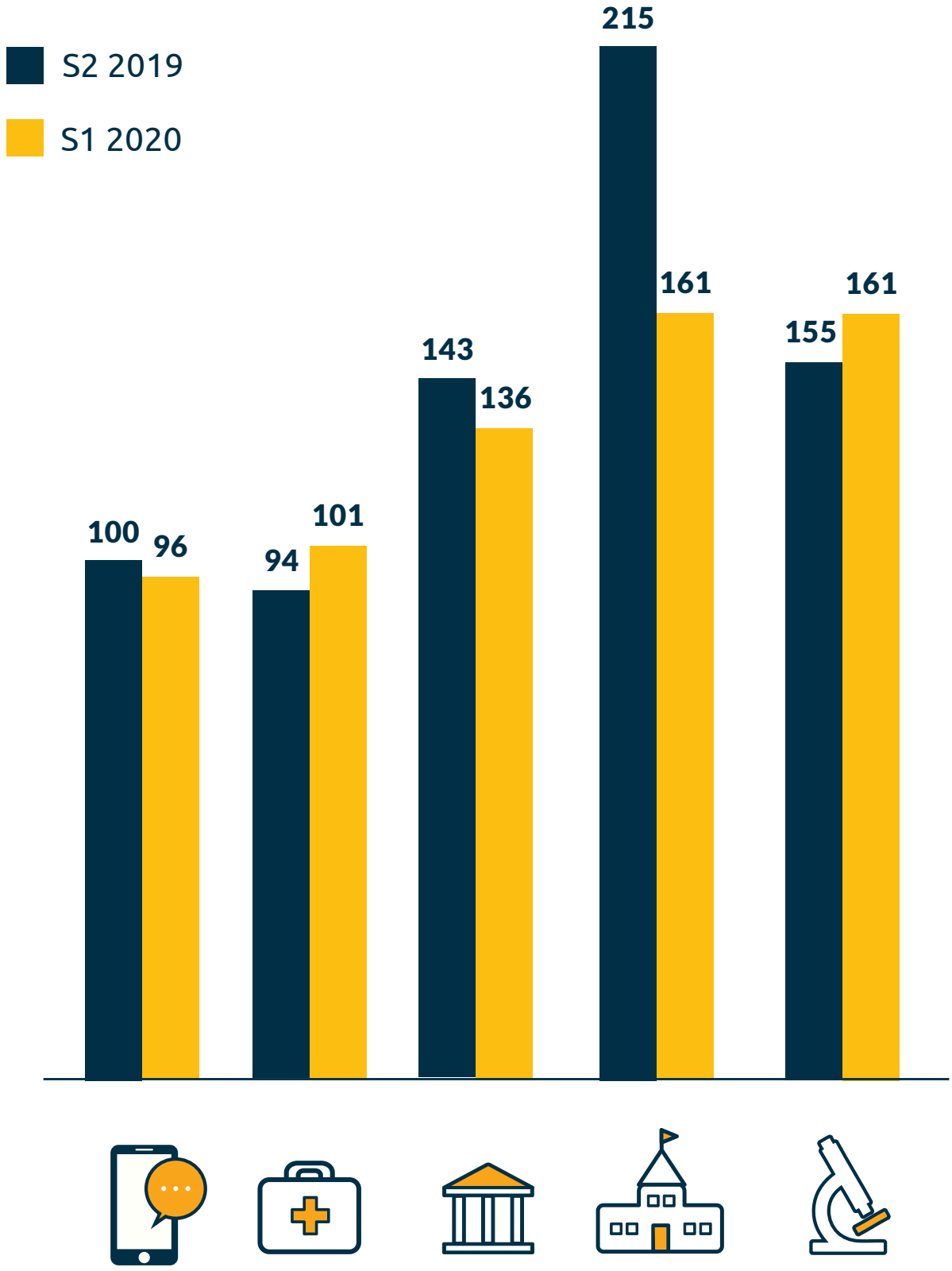
MATURITÉ DES ÉTATS EN MATIÈRE
DE LUTTE CONTRE LA CYBERCRIMINALITÉ

TENDANCES GLOBALES



En un an et demi, le nombre de violations de données personnelles par jour est passé de 4,5 à 7. Cette augmentation constante, quel que soit le marqueur sélectionné, témoigne à la fois de la progression des usages numériques, de la prise de conscience croissante des utilisateurs qui notifient davantage les incidents et d'une cybercriminalité qui progresse fortement.

TOP 5
DES SECTEURS TOUCHÉS
(S2 2019 - S1 2020)



Information & communication

Santé

Finances & assurances

Administration publique

Sciences & techniques

Sans surprise, les secteurs les plus touchés détiennent principalement des données personnelles sensibles ou à potentielle haute valeur ajoutée. Deux d'entre eux (santé / sciences & techniques) recensent plus de violations que l'année dernière.

QU'EST-CE QU'UNE VIOLATION DE DONNÉES ?

Une violation de données à caractère personnel est constituée par tout incident de sécurité, d'origine accidentelle ou malveillante, entraînant l'altération, la destruction, la perte ou la divulgation de données à caractère personnel (Art. 4.12 du RGPD). Depuis le 25 mai 2018, date d'entrée en vigueur du RGPD, les organismes qui traitent des données personnelles doivent non seulement mettre en place des mesures pour prévenir les violations de leurs données, mais également réagir pour endiguer la violation et en atténuer les effets (Art.33 et 34 du RGPD).

QUELLES SONT LES DONNÉES AFFECTÉES ?

En 2020, les violations concernent davantage les données personnelles sensibles (données de santé, origine raciale ou ethnique, opinions politiques, etc.).

10,4%

S2 2018 - S1 2019

12,6%

S2 2019 - S1 2020

Pourcentage de données personnelles sensibles affectées par des violations de données

ORIGINES DES FUITES DE DONNÉES

52%
Malveillance

54 %
S2 2018 - S1 2019

19,2%
Vols physiques

15 %
S2 2018 - S1 2019

64,3%
Piratages en ligne

69,8 %
S2 2018 - S1 2019

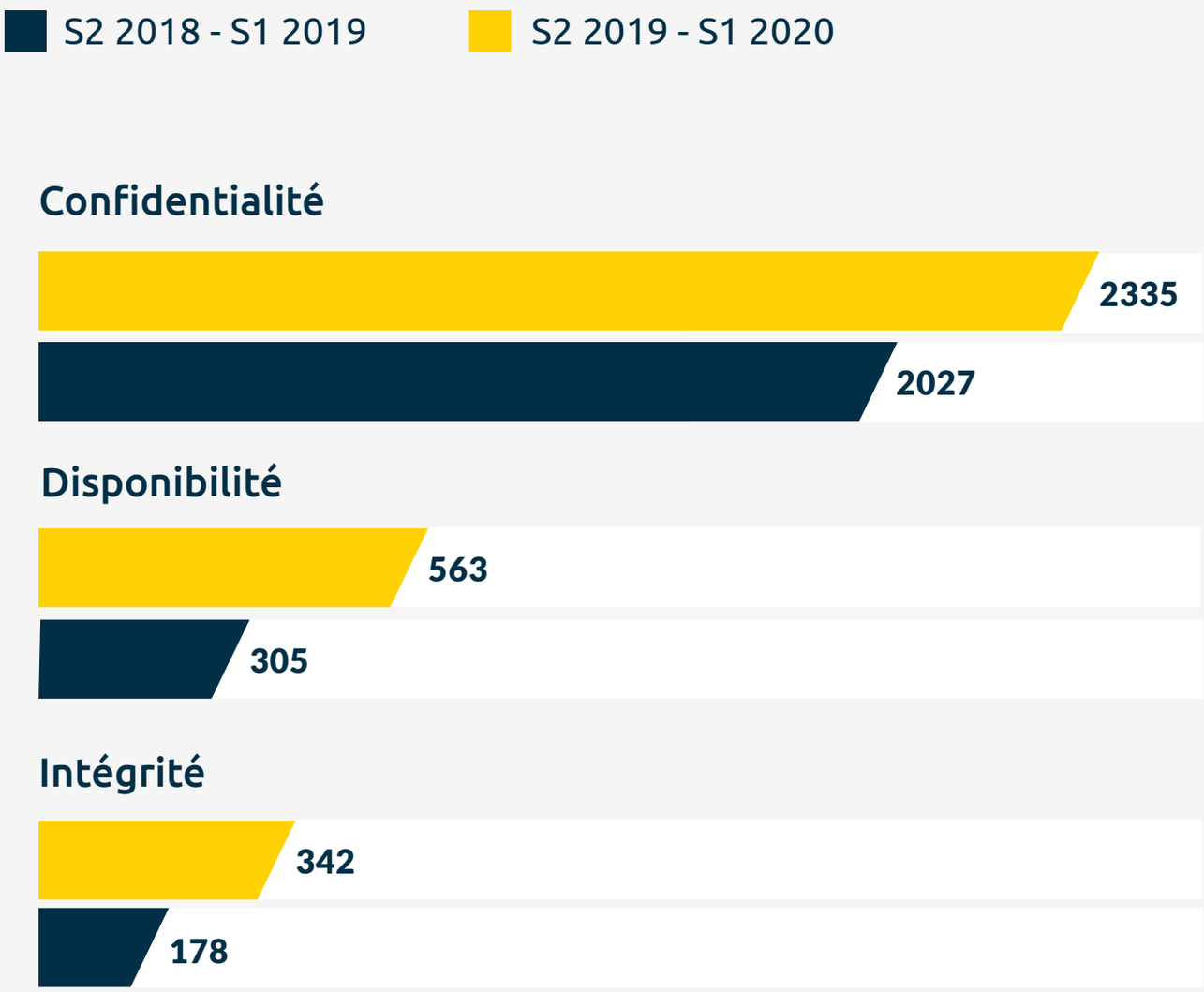
33%
Accidentelle

26 %
S2 2018 - S1 2019

La malveillance reste la première cause des violations même si les fuites de données ayant une origine accidentelle ont, en proportion, progressé de 7% en 2020.

QUEL IMPACT SUR LES ENTREPRISES ?

Types d'atteinte aux données par violation



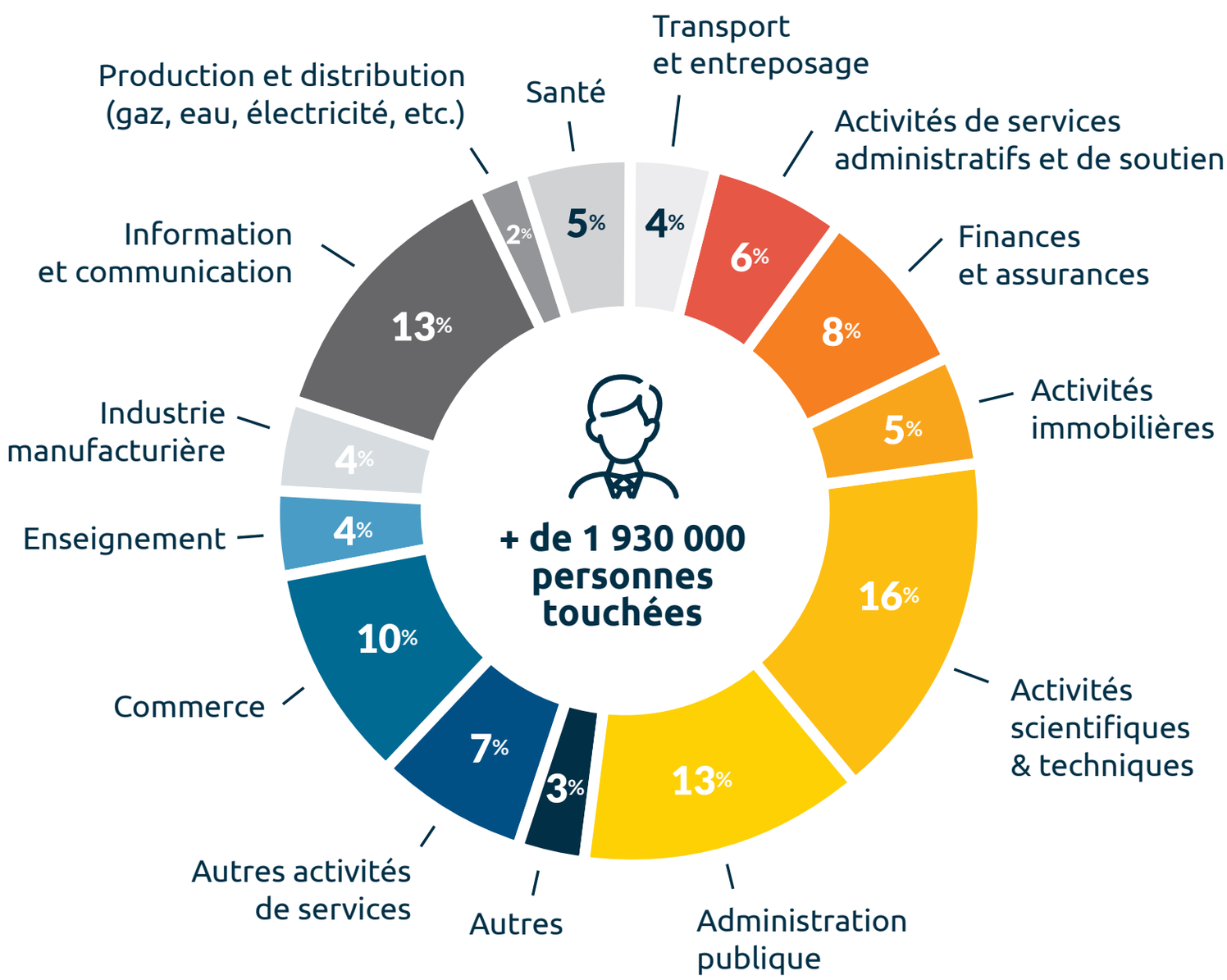
Si les atteintes à la confidentialité progressent légèrement, les violations liées à l'intégrité et à la disponibilité ont presque doublé en un an, conséquence notamment de l'accroissement des menaces de type rançongiciel.

L'ERREUR HUMAINE EST AU COEUR DE NOMBREUSES FUITES DE DONNÉES

Jean-Bernard Rambaud, Associé Cybersécurité, PwC

De nombreuses fuites de données sont liées à des actions commises involontairement au sein de l'entreprise. Sans qu'il n'y ait nécessairement de malveillance associée, la sensibilisation des collaborateurs sur l'application des règles d'hygiène de la sécurité constitue une première réponse qu'il faut compléter par des actions plus dynamiques comme des tests (de *phishing* par exemple) ou des exercices de crise qui permettent d'accroître la résilience face à ce risque.

Répartition des personnes touchées par secteur d'activité (S2 2019 - S1 2020)



+19%

de personnes touchées
par des fuites de données par rapport
à la période S2 2018 - S1 2019

Le nombre de personnes touchées (près de 2 millions) progresse de près de 20% sur la dernière période étudiée.

FOCUS SUR LES RANÇONGICIELS

Wandrille Krafft,
Responsable de l'équipe DFIR, Lexfo

ÉTAT DE LA MENACE DES RANÇONGICIELS

QU'EST-CE QU'UN RANÇONGICIEL ?

Un rançongiciel, ou ransomware en anglais, est un code malveillant rendant inaccessibles des données d'un utilisateur afin de lui demander de payer une rançon (bien souvent de l'argent en cryptomonnaie).

Le nombre d'attaques de ce type ne cesse d'augmenter (192 incidents signalés à l'ANSSI en 2020 contre 54 en 2019, soit une hausse de 255 %) et s'accompagne de nouvelles pratiques comme la double extorsion qui consiste à ajouter une pression supplémentaire sur la victime en la menaçant de publier les données dans le but qu'elle paye la rançon.

Aucun secteur d'activité ni zone géographique ne sont épargnés par les attaques non ciblées par rançongiciel. Certaines attaques, plus ciblées, vont privilégier les entreprises et institutions dont l'interruption d'activité peut conduire à des conséquences économiques importantes.
De plus, les groupes cybercriminels vont préférer cibler des entreprises suffisamment rentables pour payer des rançons conséquentes.

AUGMENTATION CONTINUE DU NOMBRE D'ATTAQUES PAR RANÇONGICIEL EN FRANCE

En 2020, la majorité des signalements en France a concerné un nombre limité de rançongiciels, fonctionnant tous selon le modèle économique du Rançongiciel as a Service (RaaS) : Sodinokibi (alias REvil), DoppelPaymer, Maze, Netwalker et Egregor. Le modèle du RaaS consiste à proposer des rançongiciels « prêts à l'emploi » en louant des infrastructures de paiement et de distribution ainsi qu'à un ensemble de services malveillants à des affiliés en échange d'une partie des revenus (rançons).

DES IMPACTS SOUVENT SOUS-ESTIMÉS

La perte de données liée à une attaque peut avoir de lourdes conséquences financières dues au paiement de la rançon mais aussi à la restauration du SI. À titre d'exemple, les pertes de l'entreprise Sopra Steria, victime de Ryuk lors d'une attaque en octobre 2020 ayant touché uniquement quelques dizaines d'ordinateurs, sont estimées à environ 50 millions d'euros. Parfois méconnus ou sous-estimés, d'autres coûts peuvent s'ajouter :

- une perte d'exploitation ;
- un risque sur la santé des patients ;
- une perte de clients ;
- une perte de confiance à l'égard de l'organisation victime ;
- des pertes de données : R&D, comptabilité, facturation, projets, données de clients ;
- l'atteinte à l'intégrité des données sensibles ou classifiées ;
- l'impossibilité de verser les salaires des employés au cas où l'application RH fait partie du SI endommagé ;
- un impact psychologique de la résolution de l'incident, dû à un manque de ressources et de compétences, dans le cas notamment de petites structures ;
- des victimes collatérales en cas de déploiement du rançongiciel sur des réseaux interconnectés.

LA CRYPTOGRAPHIE D'UN RANÇONGICIEL

Pour prendre en otage les données, la grande majorité des rançongiciels chiffrent les fichiers présents sur le disque du poste. Toutefois, dans le but d'afficher la rançon et ses instructions, ce sont les fichiers métiers qui sont visés et non ceux indispensables au bon fonctionnement du système.

Si la technique du chiffrement a été très largement adoptée, c'est parce qu'il est impossible d'effectuer le processus inverse dans un temps raisonnable, même après une étude très fine du rançongiciel, si celle-ci est correctement mise en œuvre.
Elle repose le plus souvent sur une cryptographie hybride avec l'utilisation d'algorithmes asymétrique et symétrique largement éprouvés comme RSA et AES.

Dans le rançongiciel, la clé RSA publique de l'attaquant est embarquée et va permettre de chiffrer et protéger la clé AES symétrique utilisée pour chiffrer les fichiers. Cette clé symétrique, aussi appelée clé de session, est générée dynamiquement sur chaque poste infecté et parfois pour chaque fichier. Une fois la clé de session AES chiffrée avec la clé RSA publique, elle est ajoutée à la fin de chaque fichier où elle a été utilisée. De cette manière, seul le possesseur de la clé RSA privée sera en mesure de récupérer la clé de session et de déchiffrer le fichier lié. C'est cette clé privée que les attaquants fournissent contre le paiement de la rançon.

RETEX D'UNE ATTAQUE

J+0 : ACCÈS INITIAL

- Campagne de phishing non ciblée reçue par un directeur de filiale
- Lien Dropbox vers un fichier ZIP (script .vbe)
- Déploiement de GOOTKIT
  - Malware Bancaire « file-less » (charge utile uniquement présente en mémoire vive)
  - Injection de certificats système, Man-in-the-Browser, Mécanisme de download/upload de fichier, exécution de programmes (WMIC, PowerShell), capture vidéo

J+2 : DÉCOUVERTE & PIVOT

- Cartographie (commandes PowerShell, AdScan.exe)
- Pivot : ProcDump et Mimikatz
  - L'utilisateur était « administrateur local » sur le poste compromis
  - Premier pivot vers un compte de service (depuis la base SAM du poste compromis) pour se connecter au serveur de déploiement des mises à jour
  - Second pivot sur ce serveur vers un compte administrateur de domaine (éxécution de ProcDump et Mimikatz via une tâche planifiée)
- Création d'un « bastion interne » (un serveur compromis offre une meilleure persistance qu'un poste de travail)

J+10 / J+20 : COMPROMISSION

- Changement de C&C et de TTP : vente d'accès ?
- Nouveaux outils : SharpHound (BloodHound), TinyMet (meterpreter) et CobaltStrike
- Déploiement de TinyMet via PowerShell sur le Bastion et de CobaltStrike sur l'ensemble des serveurs du parc
- Obtention de l'accès à la console de supervision de l'antivirus

J+24 : PREMIER RANÇONGICIEL

- Désactivation des mécanismes anti-tampering de l'antivirus et suppression des alias courriel des administrateurs sur les solutions de monitoring
- Destruction des partitions RAID des serveurs de sauvegarde et arrêt des services métiers (base de données, services Web, anti-virus, etc.)
- Chiffrement du système d'information (exécution avec PsExec, environ 7 minutes pour l'ensemble des 120 serveurs)
- Actions anti-forensiques : suppression des VSS, de clé de registre (donnée temporaire + persistance), des services GOOTKIT

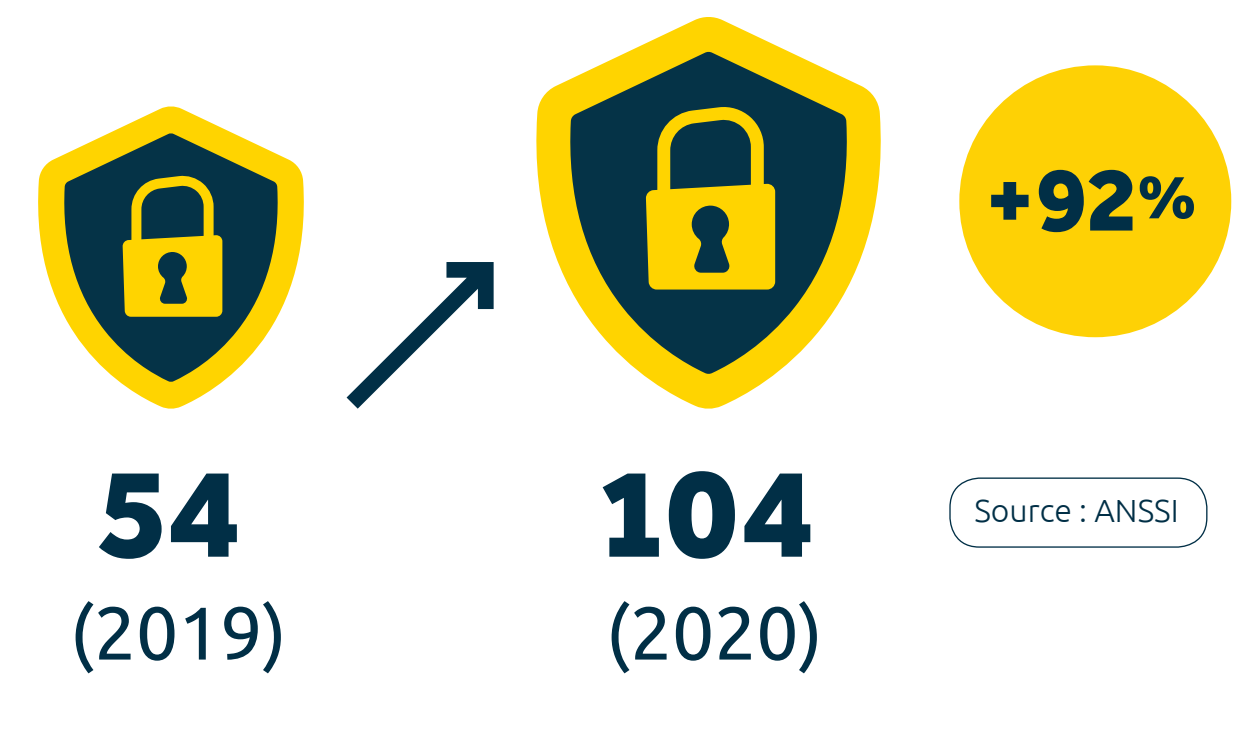
J+26 / J+33 : NÉGOCIATION

- Dépôt de plainte au C3N de Pontoise (Gendarmerie) qui met en place une cellule de négociation avec le client
- La rançon n'est pas payée et le parc vérolé est remis en service prématurément (pertes financières)
- Les journaux des pare-feux montrent des connexions actives vers les C&C et quelques heures après, un second rançongiciel frappe le SI

BILAN DE L'ATTAQUE

- Une entreprise bien rodée : RaaS, service après-vente, négociation de la rançon, etc.
- Attaquants déterminés et organisés : destruction des sauvegardes, bannissement des administrateurs
- Utilisation d'outils en vente sur le marché noir et d'outils publics
- Vente d'accès très probable (changement de TTP)
- Développement d'un « decryptor » : C&C non public identifié durant la RIS, clés de chiffrement rendues publiques
- Après 6 jours d'interruption de services, un nouveau SI sain est partiellement remis en production
- Les analyses forensiques se poursuivront sur 2 mois et la reconstruction du SI sur 7 mois

NOMBRE D'INTERVENTIONS DE L'ANSSI À LA SUITE D'ATTAQUES EN RANÇONGICIEL



COMMENT S'EN PRÉMUNIR ?

Jean-Bernard Rambaud, Associé Cybersécurité, PwC

Le risque de rançongiciel est rendu possible par l'absence d'un certain nombre de mesures de sécurité comme par exemples la mise à jour des systèmes d'information, les sauvegardes régulières de données, la sensibilisation des personnels ou encore la limitation et la protection de comptes à privilèges.

TÉMOIGNAGE

Julien Guyon,
Responsable de la Sécurité des Systèmes d'Information (RSSI),
Direction du Numérique de la Région Grand Est

1. Selon vous, quel niveau de menace pèse actuellement sur les données des collectivités en France ?

La menace est de plus en plus forte et atteint des niveaux jamais rencontrés. Chaque semaine ce sont plusieurs collectivités qui sont victimes, allant du simple mail d'hameçonnage jusqu'à la destruction partielle du système d'information via les « rançongiciels » qui restent la menace la plus crainte. Cela touche des collectivités de toute taille, de la simple mairie à la métropole ou conseil départemental/régional.

2. Pouvez-vous rappeler les circonstances et le déroulé de l'incident de février 2020 ?

En ce vendredi matin, un ingénieur d'exploitation constate qu'une demande de rançon apparait sur l'un de nos contrôleurs de domaine en relation avec des alertes remontées par notre plateforme de supervision. Nous sortions la veille d'une session de présentation de l'état de l'art sur le cyber risque avec l'un de nos prestataires. La question n'est pas « si » mais « quand ». C'est donc aujourd'hui. Nos infrastructures disparates, fruit de la fusion des trois régions historiques, n'ont pu être rationalisées et il est difficile de trouver la source de l'attaque. Nous contactons une société spécialisée ainsi que nos partenaires essentiels et les autorités puis nous engageons une démarche de gestion de crise.

3. Comment ce piratage a-t-il affecté vos systèmes ? Quelles ont été les conséquences sur les données contenues ? Quel impact sur l'image de la Région ?

La grande majorité de notre infrastructure « Windows » est affectée, rendant l'essentiel de nos services inopérants. De nombreuses données ne sont plus accessibles.
Si des informations contradictoires sont sorties dans la presse, notre capacité à revenir à une situation normale en une semaine a permis de minimiser l'impact sur l'image de notre institution.
Nous avons pu restaurer l'ensemble de nos données et avons perdu quelques jours de travail.

4. Quels enseignements avez-vous tiré de cet incident et quelles sont les mesures mises en place afin de parer à d'éventuelles nouvelles attaques ?

L'analyse de l'attaque a permis de mettre en avant certaines défaillances qui ont permis de prioriser les actions techniques et organisationnelles nécessaires.
La désaffection du parc a été assurée par le déploiement d'une solution de type EDR qui a été pérennisée. Nous avons accéléré les projets de rationalisation et de modernisation de nos infrastructures techniques et avons réalisé des actions sur la centralisation des évènements de sécurité, de la gestion de crise et de la création de notre plan de continuité et de reprise informatique.

5. D'après vous, quelles mesures pourraient être mises en place nationalement et localement pour mieux protéger les collectivités contre cette menace croissante ?

La bonne mise en œuvre des recommandations de l'ANSSI devrait faire l'objet d'un accompagnement plus fort. La sensibilisation à l'image de cybermalveillance devrait être plus largement diffusée.

LA VALORISATION FINANCIÈRE DES RISQUES, UN OUTIL DE PILOTAGE CONTRE LA CYBERCRIMINALITÉ

Cédric Lenoire,
Analyste financier, pertes d'exploitation, Bessé

La résilience organisationnelle est devenue pour de nombreuses entreprises industrielles ou de services aux modèles fortement digitalisés un outil indispensable de lutte contre la cybercriminalité. L'objectif est simple, maitriser autant que possible les impacts d'une cyber-interruption, qu'ils soient immédiats (pertes d'exploitation, amendes, dépenses associées aux opérations de communication de crise, coûts liés aux actions immédiates de remédiation, de recouvrement des activités et d'amélioration de la cybersécurité) ou à plus long terme lorsqu'ils remettent en cause la survie de l'entreprise (dégradation de la notoriété, pertes de parts de marché, diminution des opportunités de croissance, augmentation du coût du capital).

Le développement d'un modèle d'activité résilient se faisant au prix d'investissements conséquents, certains dirigeants d'entreprise, accompagnés de leur DSI et DAF, n'hésiteront pas à faire appel à des techniques de valorisation d'entreprise et de méthodes de quantification financières pour développer un outil de pilotage visant à prioriser les axes d'amélioration en fonction des enjeux mesurés. Tout comme pour une opportunité de croissance dont l'évaluation du retour sur investissement guidera sa prise de décision, le dirigeant chiffre les conséquences de la menace cyber et définit le niveau optimal de résilience à assurer pour préserver la valeur patrimoniale de l'entreprise.

La cyber résilience est sans aucun doute devenue un vecteur important de bonne santé financière lorsque son développement est correctement piloté. Obtenir une vision financière, présente et future, des vulnérabilités de l'entreprise ne peut que représenter un avantage compétitif qui assurera une rentabilité quasi certaine face à une menace en constante évolution.

RGPD : 3 ANS DÉJÀ !

QUELLES SONT LES MISSIONS DU DPO ?

Institué par le Règlement général sur la protection des données (RGPD) entré en vigueur en mai 2019, le Délégué à la protection des données (DPO) a pour mission de s'assurer que son organisation traite les données personnelles dans le respect des règles communautaires.

Selon l'article 38 du Règlement, le DPO est tenu d'agir en toute autonomie, sans recevoir « aucune instruction en ce qui concerne l'exercice des missions ». En raison des conflits d'intérêts parfois posés par le cumul des fonctions, de nombreuses organisations choisissent donc de faire appel à un délégué externe.

En conséquence, le DPO doit disposer d'une connaissance accrue de l'utilisation des données faite par son organisation et de la législation applicable. Le RGPD prévoit également que le DPO dispose des ressources nécessaires pour exercer ses missions et cela sans restriction d'accès.

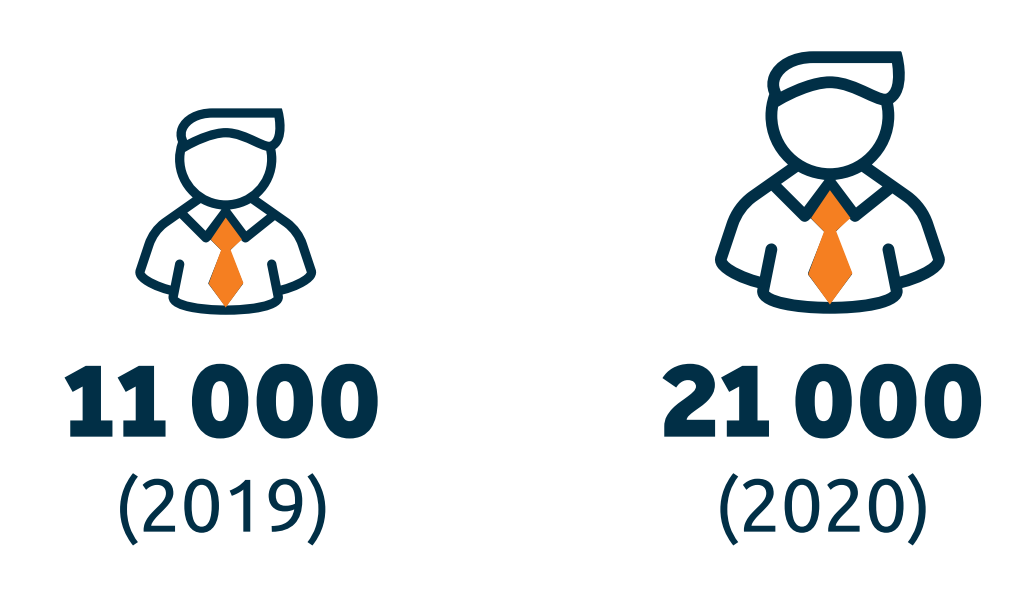
Bien que toutes les organisations ne soient pas concernées par l'obligation de désigner un délégué à la protection des données, la CNIL recommande fortement son implication dans tous les projets de traitement de données à caractère personnel.

SON RÔLE CONTRE LES CYBERATTAQUES ?

Loin d'être une simple formalité ou de se limiter à faire le lien avec les autorités compétentes, le DPO permet aux organisations de se préparer en amont contre les cyberattaques. Avec le concours du RSSI, le délégué à la protection des données met en place des mesures de prévention à destination du personnel afin de combler les failles de sécurité. L'erreur humaine est souvent la porte d'entrée des auteurs de cybermalveillances !

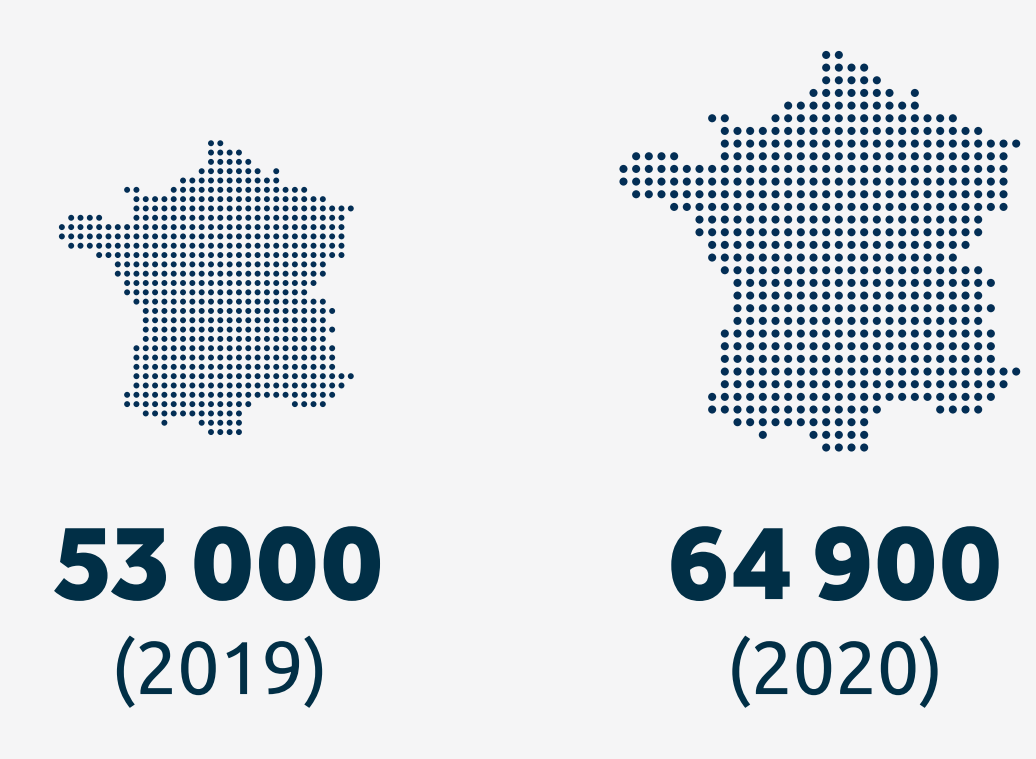
Si malgré ces précautions un incident doit survenir, le DPO peut également mettre en place des processus adéquats de gestion des cyberattaques afin de limiter leur impact sur l'organisation et de préparer la réponse légale contre les auteurs.

Nombre de DPO en France



Conséquence positive de la mise en application du RGPD, le nombre de DPO a pratiquement doublé en France en seulement un an. Reste à savoir si la création de cette fonction « métier » s'accompagne des équipes et du budget nécessaires à sa concrétisation.

Organismes couverts en France



TÉMOIGNAGE

Gilles Alsac, Directeur juridique et conformité – DPO, Bessé

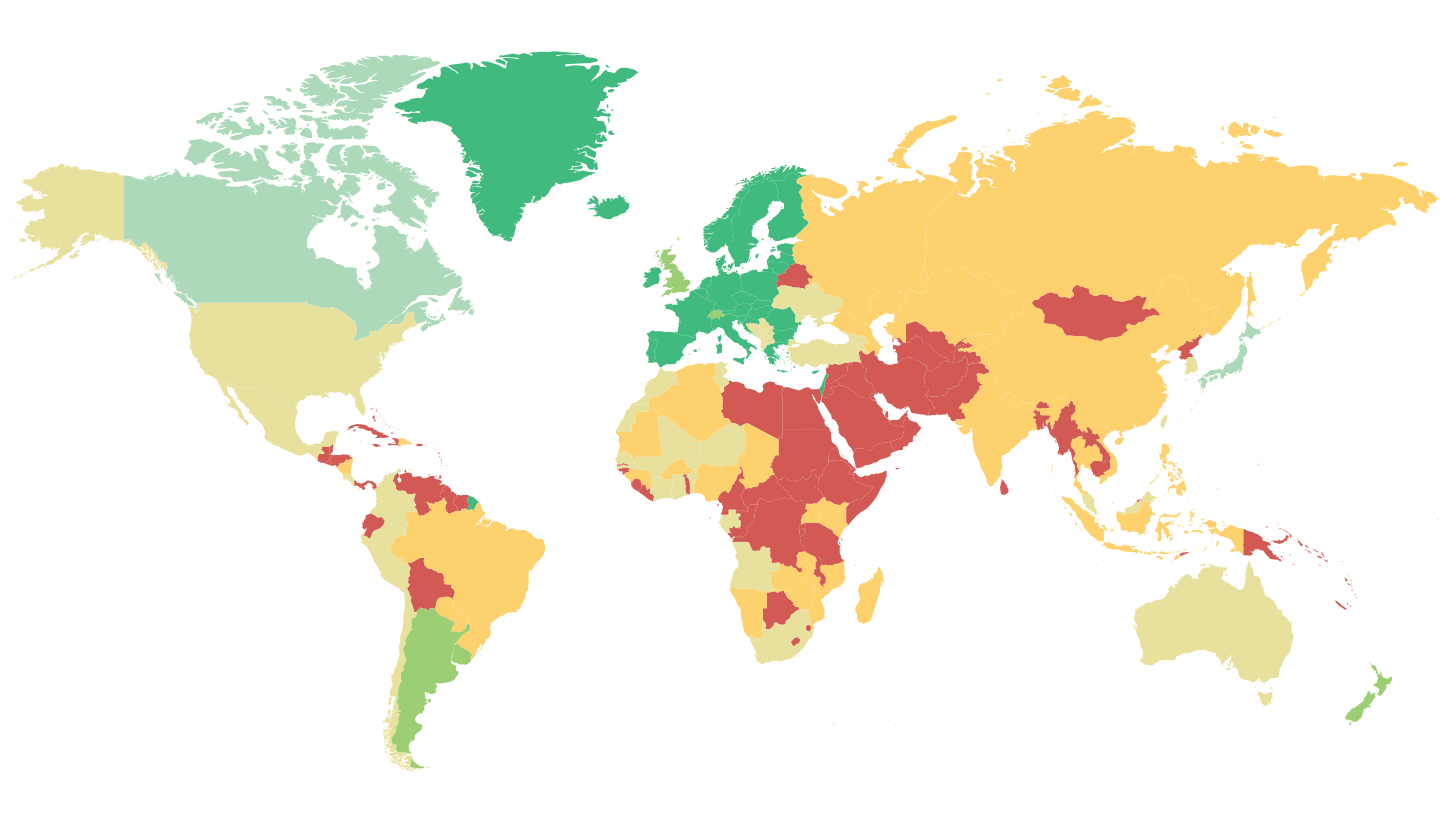
Le DPO face aux cybermenaces

Il est évident que l'intensification du risque cyber a considérablement fait évoluer l'approche de notre fonction de DPO. En lien très étroit avec la RSSI et la Direction des risques, nous avons résolument décidé d'être plus rigoristes.

Cela se traduit notamment par une sélection beaucoup plus drastique de nos partenaires. En d'autres termes, le choix n'est pas uniquement effectué sur leur savoir-faire mais aussi sur leur véritable connaissance et maîtrise des traitements qu'ils opèrent sur les données personnelles que nous leur confions et sur les mesures de sécurité mises en œuvre pour les protéger. Ceci fait l'objet de discussions et de vérifications approfondies. Il peut donc arriver qu'un candidat qui sur le papier présentait l'offre technique et commerciale la plus aboutie, ne soit finalement pas retenu car n'apportant pas suffisamment de garanties en matière de cybersécurité et de protection des données.

À ce titre, nous sommes régulièrement confrontés à des clauses de limite de responsabilité beaucoup trop faibles qui ne sont plus adaptées au contexte actuel des cybermenaces. Comment pourrions-nous donner notre confiance à un prestataire informatique externe, si finalement celui-ci s'exonère de toute responsabilité sur la question des données personnelles ? Nous avons besoin de partenaires engagés et capables d'assumer pleinement leurs responsabilités. C'est un gage de confiance sur lequel les entreprises du secteur informatique seront à n'en pas douter de plus en plus attendues. Il est urgent pour elles d'évoluer, d'autant plus que les solutions assurantielles existent.

LÉGISLATIONS EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES DANS LE MONDE



Pays pour lequel le transfert des données personnelles ne nécessite pas d'encadrement par des outils de transfert

- Pays membre de l'Union européenne ou de l'Espace économique européen
- Pays reconnu comme adéquat par l'UE
- Pays en adéquation partielle (Canada)
  Pays reconnu adéquat par l'UE pour certains traitements spécifiques (activités commerciales), les autres transferts de données personnelles nécessitant d'être encadrés par des outils de transfert

Pays non reconnu comme adéquat par l'UE et dont le transfert des données personnelles nécessite d'être encadré par des outils de transfert

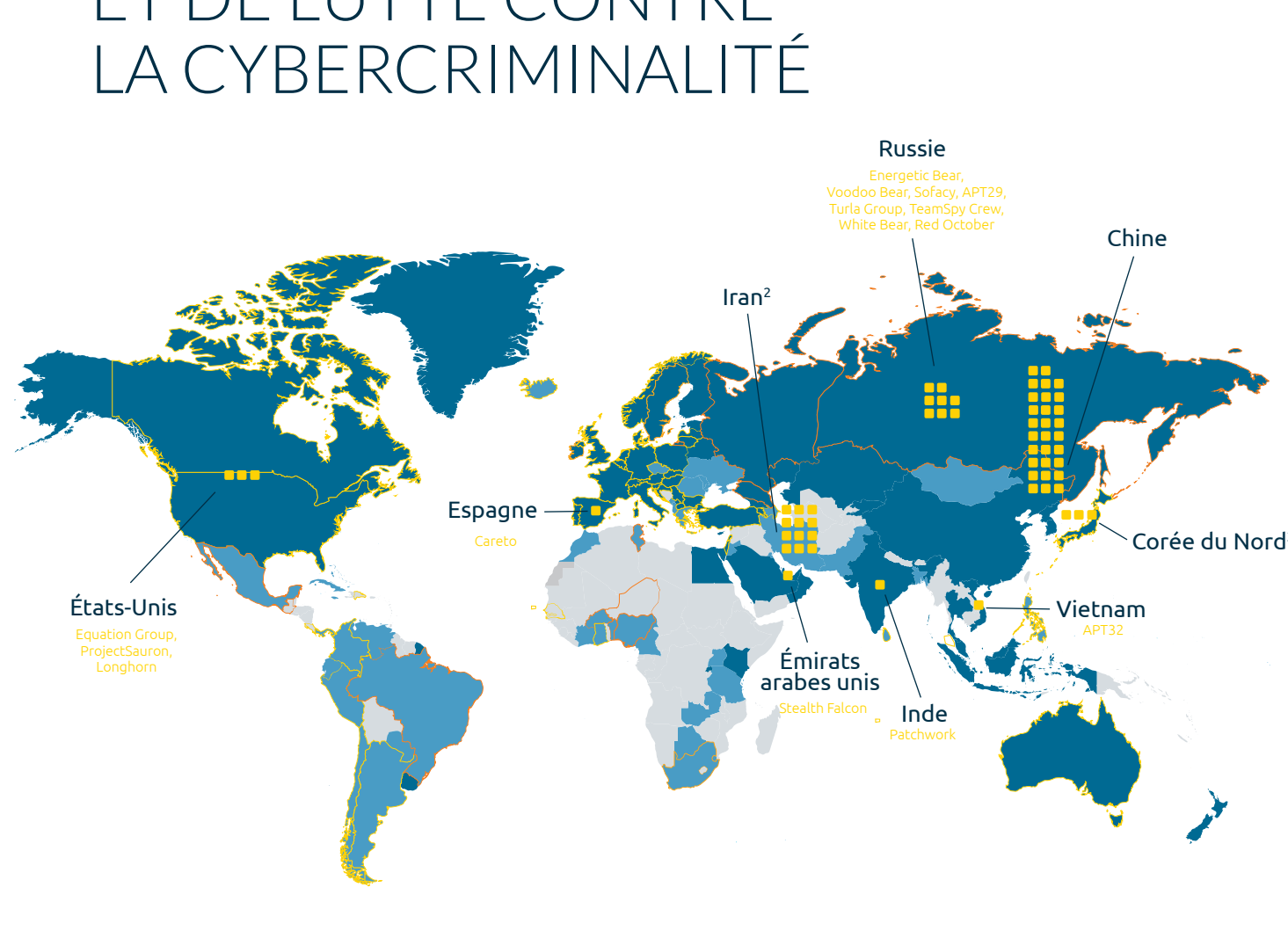
- Autorité indépendante et loi
- Avec législation
- Pas de loi

Source : CNIL // Données compilées par Avisa Partners

En trois ans, le RGPD est devenu la pierre angulaire de la transition numérique européenne. Ses dispositions ont façonné la manière dont nous traitons les données personnelles en Europe, mais ont aussi inspiré la législation de nombreux pays du monde – du Japon à l'Argentine en passant par la Nouvelle-Zélande – pour devenir un standard international.

Dans une économie reposant de plus en plus sur le traitement des données, le RGPD réconcilie innovation et confiance des utilisateurs. Bien qu'elle montre une homogénéisation progressive des normes, cette carte, construite à partir des données mises à disposition par la CNIL, montre toutefois qu'il reste nécessaire d'évaluer les risques à l'international avant d'engager des projets d'envergure en matière de traitement des données pour s'assurer que les données personnelles des citoyens et clients sont bien protégées.

MATURITÉ DES ÉTATS EN MATIÈRE DE CYBERSÉCURITÉ ET DE LUTTE CONTRE LA CYBERCRIMINALITÉ



Convention de Budapest sur la cybercriminalité

Entré en vigueur en 2004, ce traité international, aussi connu sous le nom de Convention du Conseil de l'Europe sur la cybercriminalité, a pour objectifs d'harmoniser les législations nationales concernant les infractions pénales commises via les réseaux informatiques, depuis la fraude, la pédopornographie jusqu'aux atteintes à la sécurité des réseaux, et de favoriser la coopération internationale.

- État ayant signé et ratifié le traité
- État ayant signé le traité
- État n'ayant ni signé ni ratifié le traité

Maturité en cybersécurité

L'indice, élaboré par l'Union internationale des télécommunications (UIT), est un agrégat de 25 indicateurs qui permet de comparer l'engagement national sur la cybersécurité. Il se fonde sur cinq piliers : l'aspect juridique, les compétences techniques, la coordination des institutions, le développement des compétences et la coopération internationale.

- Elevé de 0,670 à 0,931 (Royaume-Uni)
- Moyen de 0,340 à 0,669
- Faible de 0,004 (Maldives) à 0,339

Groupes d'attaquants

Un carré correspond à une entité
Cette liste non exhaustive recense les principaux groupes de pirates informatiques pratiquant le cyberespionnage et le cybercrime à l'échelle internationale.

1. APT40, APT41, APT27, Comment Crew, Putter Panda, UPS, IXESHE, APT16, Aurora Panda, Wekby, Shell Crew, Naikon, Lotus Blossom, Stone Panda, Hellsing, Mirage, Anchor Panda, NetTraveler, Ice Fog, Beijing Group, Samurai Panda, Temper Panda, DragonOK, APT30, Tick, Mofang, Maverick Panda, RANCOR et Mustang Panda
2. APT33, APT34, Leafminer, Flying Kitten, Cutting Kitten, Charming Kitten, Rocket Kitten, Cleaver, OilRig, Infy, CopyKittens et MuddyWater
3. Lazarus Group, DarkHotel et Kimsuky

N.B. : APT pour Advanced Persistent Threat (menace persistante avancée)

Sources : International Telecommunication Union, The Global Cybersecurity Index 2018, 2019 ; Conseil de l'Europe, janvier 2021 ; Lexfo / Avisa Partners, janvier 2021

Disposer d'un indice de maturité pays en cybersécurité est intéressant pour toutes les entreprises qui disposent d'activités ou d'implantations à l'international. Les pays européens et les États-Unis figurent parmi les pays les plus matures dans le domaine.

FAQ

COMMENT SE PRÉMUNIR DES DATA BREACH ?

Un bon niveau de prévention nécessite la coopération de plusieurs fonctions de l'entreprise et une prise de conscience des risques face à une cybercriminalité qui s'est fortement professionnalisée et structurée.

L'article 32 du RGPD précise que compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant doivent mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Quelle que soit la nature des mesures prises, elles devront être réévaluées autant que de besoin pendant le cycle de vie des traitements de données à caractère personnel.

Outre la sensibilisation des personnels et la protection des systèmes d'information contre les risques d'intrusion, la prévention des fuites de données repose sur la connaissance des données de l'entreprise, de leur localisation, de savoir qui y accède et pourquoi… connaître et pouvoir ordonner ses données c'est savoir comment les stocker, les sauvegarder et mieux les protéger.

Jean-Bernard Rambaud, Associé Cybersécurité et Sandrine Cullaffroz-Jover, Associé Droit des activités numériques, PwC

QUELS SONT LES RISQUES POUR UNE ENTREPRISE ?

Les risques liés aux fuites de données sont importants et nombreux. Outre les sanctions comme celles liées au RGPD mais aussi d'autres législations étrangères, c'est le risque réputationnel de l'entreprise qui est en jeu.
La perte des données aura des impacts sur le business, la confiance, la compétitivité… Elle peut aussi affecter la recherche et l'innovation et mettre en péril l'avenir de l'entreprise. Pour l'entreprise cotée, c'est aussi la garantie d'une perte de valorisation durable comme le montre certaines études. Et si le problème vient à se répéter, alors les conséquences peuvent être dramatiques voire fatales pour l'entreprise.

Jean-Bernard Rambaud, Associé Cybersécurité et Sandrine Cullaffroz-Jover, Associé Droit des activités numériques, PwC

EST-CE QUE LES DATAS BREACH PEUVENT S'ASSURER ?

Les risques liés à une compromission de données et en particulier les fuites de données personnelles rentrent dans le champ des polices d'assurance Cyber. Ce risque est donc assurable.

Christophe Madec,
Chargé de clientèle et expert cyber, Bessé

QUE PEUVENT PRENDRE EN COMPTE LES ASSURANCES ?

Sont notamment assurées les conséquences d'une fuite de données, à savoir et à titre d'illustration, les frais de notifications ainsi que les potentielles réclamations qui peuvent en découler. Dans ce cadre, les frais de défense engagés par l'entreprise seront également pris en charge. Concernant les sanctions prononcées par toute autorité réglementaire, notamment dans le cadre du RGPD, celles-ci ne sont normalement pas couvertes car considérées comme des amendes et donc inassurables par nature.

Christophe Madec,
Chargé de clientèle et expert cyber, Bessé

FAUT-IL SYSTÉMATIQUEMENT NOTIFIER LES VICTIMES ?

L'Article 34 du RGPD relatif à la communication à la personne concernée d'une violation de données à caractère personnel rend celle-ci obligatoire sous conditions « lorsqu'une violation de données à caractère **personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique**, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais. » Dès lors, toutes les violations ne devront pas faire l'objet d'une communication aux victimes.

En revanche, il est recommandé lorsque de tels faits surviennent de mettre en place un dispositif de communication ou d'avis aux victimes, tierces parties de l'entreprise. Une communication efficace permettra aux personnes concernées de prendre des mesures pour se protéger ou limiter les conséquences négatives de la violation, le cas échéant.

Jean-Bernard Rambaud, Associé Cybersécurité et Sandrine Cullaffroz-Jover, Associé Droit des activités numériques, PwC

Y A-T-IL UN RISQUE À PAYER UNE RANÇON ?

Le paiement de la rançon est plus que déconseillé, notamment par les autorités ainsi que par l'ANSSI. Dans les faits, le nombre d'entreprises qui, en France, auraient accepté de payer une rançon s'avèrerait très limité. Peu d'informations fiables ou complètes sont en revanche disponibles pour étayer cette affirmation. Ceci étant, le paiement d'une rançon n'est pas le gage d'une solution optimum pour recouvrer rapidement et dans les meilleures conditions le bon fonctionnement de son système d'information ainsi que l'ensemble de ses données. Le paiement de la rançon induit en effet plusieurs risques qu'il convient de prendre en considération.
À titre d'illustration :

• Incertitude d'obtenir la clé de décryptage permettant de récupérer intégralement des données intègres ;

• Des données ont été exfiltrées et restent en possession des hackers qui pourront en faire usage ou les revendre ultérieurement bien que la rançon ait été payée ;

• Le paiement d'une rançon expose l'entreprise à être plus facilement prise pour cible lors d'une prochaine attaque.

Face à la multiplication des attaques par rançongiciel, certaines rançons ont bien été payées par les entreprises victimes, voire par leurs assureurs quand ces entreprises disposaient de police d'assurance cyber. Face à ce constat, certaines autorités gouvernementales, telles que l'OFAC aux États-Unis, ont attiré l'attention sur le risque de sanctions à l'encontre de toute organisation qui, au travers du paiement de toute rançon, participerait directement ou indirectement au financement du terrorisme. Certains soulignent aussi, non sans raison, que le paiement des rançons participe au développement de la cybercriminalité. Il serait aussi pour certains, contraire à l'ordre public, et devrait donc être interdit légalement.

Christophe Madec,
Chargé de clientèle et expert cyber, Bessé

RESSOURCES

• Notifier une violation de données à caractère personnel auprès de la CNIL : http://www.cnil.fr

• Porter plainte : https://www.pre-plainte-en-ligne.gouv.fr/

• Trouver un prestataire référencé grâce à la plateforme d'assistance aux victimes d'actes de Cybermalveillance ACYMA : http://www.cybermalveillance.gouv.fr

• Retrouver le cadre européen : https://edpb.europa.eu

CONTACT

Estelle Augat
estelle.augat@avisa-partners.com
www.forum-fic.com

RÉALISÉ PAR

EN PARTENARIAT AVEC