Curtis PC
Pour
Une vie numérique plus simple!

Baromètre Violation de Données : Quels sont les chiffres de 2019 du FIC ?

Publié le - 31 janvier 2020

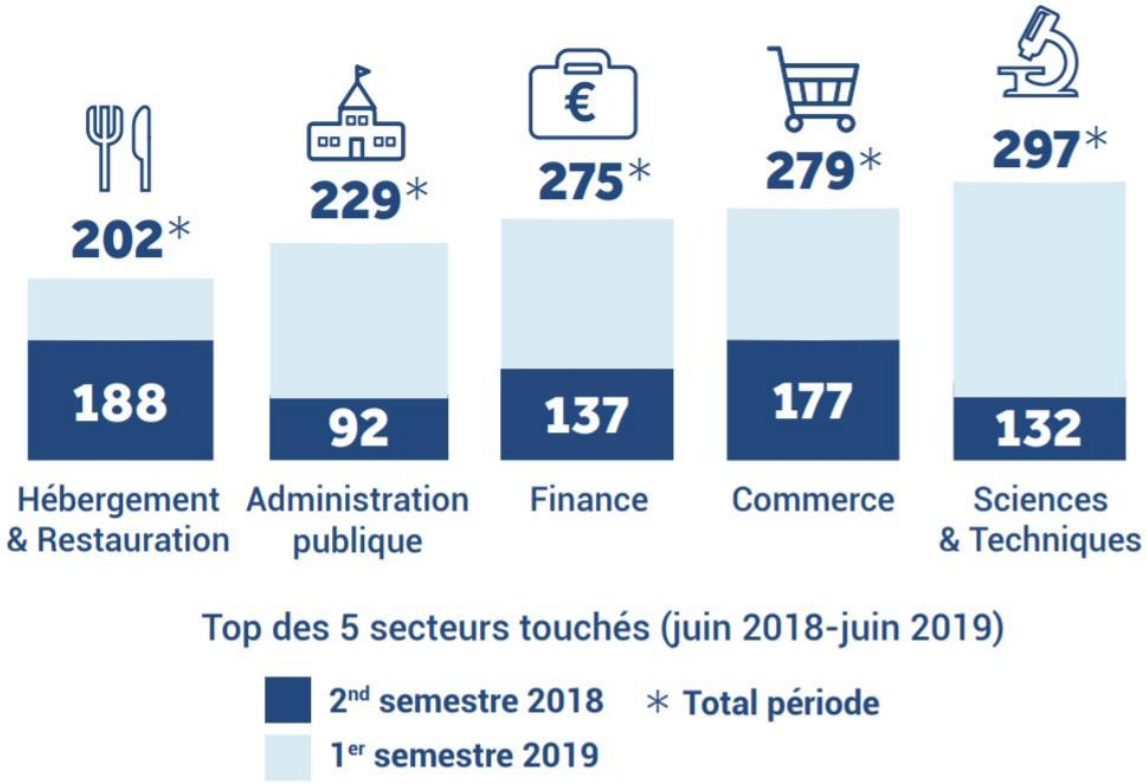
Cette semaine se déroulait le forum international de la cybersécurité (FIC). Pour cette occasion, en partenariat avec PwC et Bessé, et avec la participation de la CNIL, un baromètre Data Breach (violation de données) a été produit.

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'il traite 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.

TENDANCES GLOBALES :

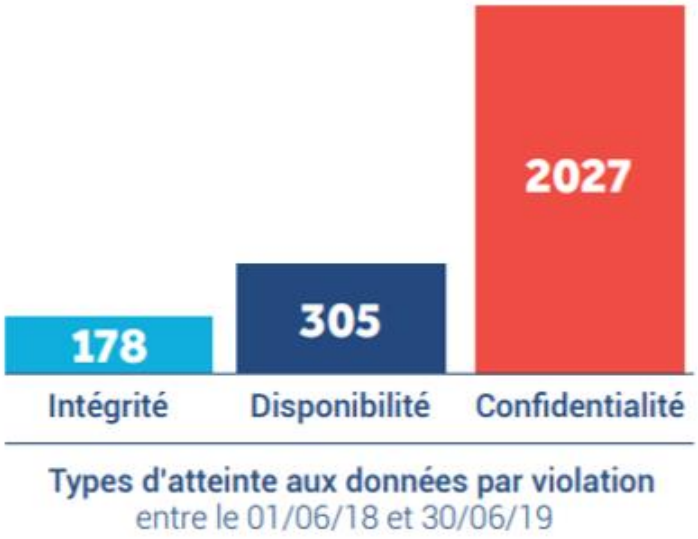
Concernant les tendances globales, le FIC nous rapporte une augmentation de, entre le deuxième semestre de 2018 et le premier semestre de 2019, 27% du nombre de violations par jour en moyenne ainsi qu'une augmentation de 24,5% du nombre de notifications. C'est en moyenne 812 600 personnes concernées au premier semestre de 2019 contre 804 000 au deuxième semestre de 2018.

Le baromètre nous présente aussi un schéma des secteurs les plus touchés en nombre de notifications :



QU'EST-CE QU'UNE VIOLATION DE DONNÉES A CARACTÈRE PERSONNEL?

Il s'agit de tout incident de sécurité, accidentel ou illicite, entraînant l'altération, la destruction, la perte ou la divulgation de données à caractère personnel. Toujours d'après les chiffres du FIC c'est 10,4% de données personnelles affectées par des violations de données entre Juin 2018 et Juin 2019. Plus d'info que le site de la CNIL.



Pour exemple, au sein d'un organisme, le schéma suivant peut se dérouler. Un collaborateur reçoit un email attrayant lui annonçant avoir été sélectionné pour gagner un voyage. L'email

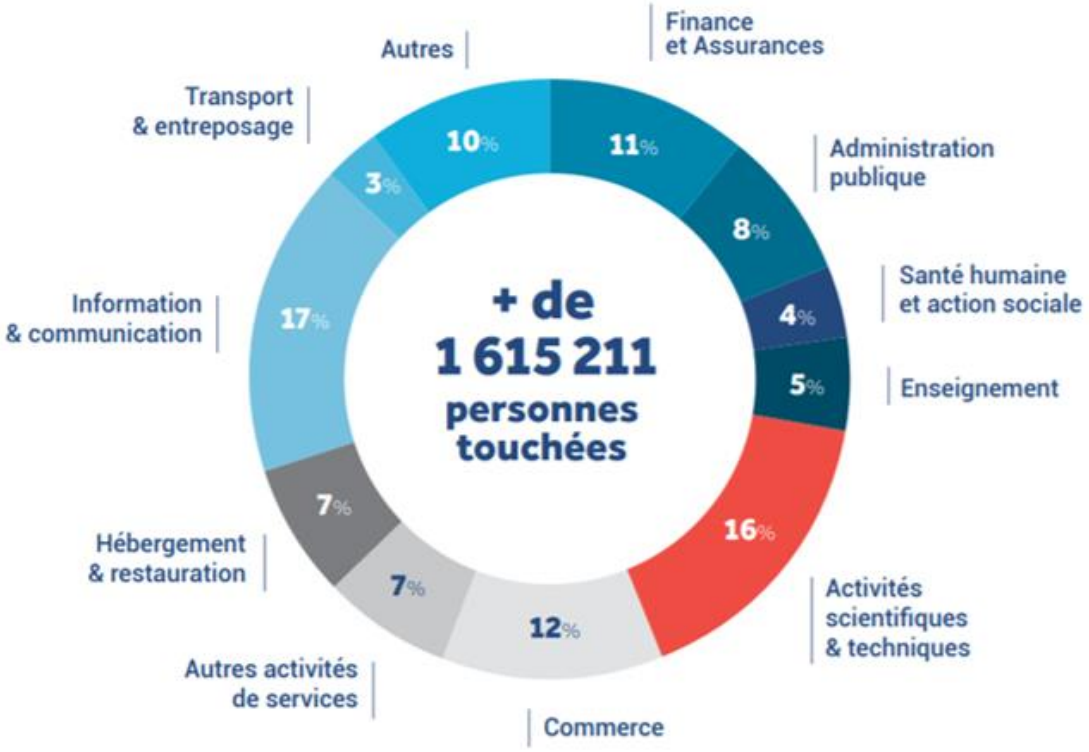
l'invite à cliquer sur un lien pour réclamer son dû, ce que fait le collaborateur. Ce qu'il ne sait pas c'est qu'il ouvre ainsi la porte à un virus qui va infecter son ordinateur et, part ce biais, le réseau de l'organisme. C'est par la suite plus 15 000 données de clients qui sont exfiltrées pour un simple clique sur un email.

QUELLE IMPACT POUR L'ORGANISME ?

L'impact le plus visible est une perte financière pendant l'attaque, dues, pour exemple, à l'indisponibilité des données, mais aussi après l'attaque lorsque l'organisme doit remettre ses systèmes en marche et réparer les dégâts.
L'atteinte à la réputation est un autre impact qui s'inscrit dans la durée. En effet il est difficile de remédier à la perte de confiance issue d'une violation de données personnelles.
L'impact sur l'activité est une autre conséquence puisque une violation peut entraîner des pertes de propriétés intellectuelles.
Enfin une violation de donnée peut avoir des suites judiciaires en cas de plaintes ou de non-respect du RGPD. Cela peut entraîner des sanctions. Pour rappel, 114 millions d'euros d'amendes ont été infligées dans l'union européenne depuis l'entrée en vigueur du RGPD.

QUELS SONT LES SECTEURS AFFECTES ?

« Aucun secteur n'est à l'abri… » Thierry Delville, Associé Cyber Intelligence, PwC France.
Le schéma suivant a été réalisé par le FIC à partir du chiffre minimal indiqué dans les notifications de juin 2018 à juin 2019. Le nombre de personnes touchées par secteur est donc sans doute supérieur à celui présenté.



QUELLES SONT LES ORIGINES DES VIOLATIONS DE DONNÉES ?

Dans 54% des cas il s'agit de malveillance avec 15% de vol physique et 69,8% de piratage en ligne. Dans 26% des cas la violation est accidentelle. Pour le reste la violation est soit d'origine inconnue soit autre.
Les accidents d'origines internes ont une part non négligeable. Le facteur humain demeure au cœur des incidents de sécurité informatique. En effet, de nombreux salariés tombent encore dans le piège du phishing. *Errare humanum est, perseverare diabolicum* (L'erreur est humaine, persévérer est diabolique). Il faut replacer l'humain au cœur de la cybersécurité.

Le conseil : Multiplier les sensibilisations et les tests d'ingénierie social. Parlez-en à votre DPO, il est au cœur de la protection et de la sécurité des traitements de données au sein de votre organisme.
Les bons réflexes :

- Prévenir : c'est la préparation en amont, prévoir l'attaque avant qu'elle ne survienne, être prêt à réagir,
- Détecter: rester vigilent, intervenir au moindre doute,
- Assurer: souscrire à une assurance qui couvre les risques liés à une violation de données,
- Réagir: Mettre fin immédiatement à la violation, prévenir son DPO, enquêter sur la violation et notifier la CNIL dans les 72h.

Les mesures préventives :

- Sensibiliser les équipes aux bons réflexes (verrouillage des écrans, mots de passe, phishing, etc.),
- Interdire l'utilisation d'adresses mail professionnelles à des fins personnelles,
- Appliquer le principe du moindre privilège et du cloisonnement,
- Utiliser les technologies de protection des données (antivirus, chiffrement, vérification de l'authenticité, etc.).