Grand angle

BAROMÈTRE DATA BREACH

Ce baromètre est animé par le 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. 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.

ANALYSE DES TENDANCES GLOBALES 2021

par Bessé

L'exploitation des données 2021 publiées par la CNIL en matière de notifications de violation de données à caractère personnel révèle une forte augmentation du nombre de notification enregistrées (+ 75%) entre 2020 et 2021. Ce n'est pas tant le nombre de notifications annoncées (5 000) qui surprend que le nombre moyen de notifications par jour ouvré (20).

Une analyse de ces données consultables sur le site de la CNIL (« notifications à la CNIL de violations de données à caractère personnel » – 31 mars 2022) permet de donner du relief à cet indicateur. **Ainsi sur 5 000 notifications, 620 d'entre elles affecteraient les données personnelles de plus de 5 000 personnes.**

Si on y ajoute les 1 131 notifications ayant affecté entre 300 et 5 000 personnes et en retenant une estimation moyenne de 2 000 personnes par fuite de données, c'est donc 2 millions de personnes supplémentaires qu'il convient d'ajouter aux 3 millions précédents.

Le raisonnement est certainement un peu simpliste mais l'extrapolation réalisée retient toutefois des hypothèses basses. **Au-delà du chiffre de 5 000 notifications, c'est donc *a minima* les données personnelles et parfois très sensibles de plus de 5 millions de personnes qui ont fuité.**

En sachant que le Règlement général sur la protection des données (RGPD) a créé un cadre strict pour préserver la confidentialité de ces données, ce volume de fuites de données ne peut que nous alerter voire nous interroger sur l'efficacité de la réglementation, sur le niveau de perméabilité des systèmes d'information ou l'ingéniosité des attaquants. Ce qui est cependant certain, c'est que la situation serait bien pire en l'absence de réglementation. Nous n'aurions peut-être aussi pas d'informations pour l'apprécier.

5 000
notifications à la CNIL
de violations de données
à caractère personnel

3 millions
de personnes
concernées

Sur ces **5 000 notifications, 3 200 sont classées comme relevant d'actes externes dont 2 981 de nature malveillante. Pas moins de 925 fuites proviendraient d'actes internes dont 200 malveillants !**

Certes, la cybercriminalité est à l'origine de la majorité des fuites de données. La proportion des actes accidentels et des actes d'origine interne n'en demeure pas moins une cause à ne pas négliger.

Quelle qu'en soit la cause ou l'origine, ces fuites de données conduisent à la mise en circulation d'informations qui représentent la matière première de la cybercriminalité. Non seulement ces informations se monnayent mais elles structurent des attaques cyber et des campagnes de *phishing* de plus en plus sophistiquées.

5 000
notifications

3 200
actes externes

2 981
de nature malveillante

925
actes internes

200
de nature malveillante

FUITE DE DONNÉES : COMMENT LES ÉVITER ?

RETOUR D'EXPÉRIENCE ET RECOMMANDATIONS DE PWC

Par Philippe Baumgart, Associé Cyber intelligence - Évaluation, réponse et anticipation de la menace, et Jamal Basrire, Associé responsable des activités Cyber Intelligence, PwC France et Maghreb.

Au cours de l'année, PwC a mené des investigations sur plusieurs dizaines d'incidents directement liés à des fuites de données et effectué des activités de cyber threat intelligence (reconnaissance, surveillance Deep et Dark web) qui ont permis d'identifier les 4 principaux facteurs à l'origine de ces incidents.

Chiffres clés

Plus de **800** **bases de données**

ont été vendues sur 3 des principaux forums de hacking durant le 4e semestre 2021.

3,61 millions d'euros

c'est la rançon que Colonial Pipeline, l'un des plus grands pipelines de produits raffinés aux États-Unis, a accepté de payer après une attaque par *ransomware* en mai 2021.

4,24 millions de dollars

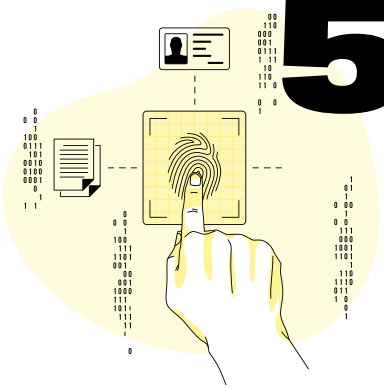
c'est le coût moyen d'une fuite de données en 2021. Un coût en augmentation par rapport à 2020 (3,86 millions de dollars).

Plus de **2 400** **fuites de données**

en lien avec des attaques par *ransomware* en 2021.

533 millions

c'est le nombre d'utilisateurs de Facebook dont les données ont été publiées sur un forum de hacking en 2021.



5 milliards

c'est le nombre de données « adresses emails, mots de passe » contenus dans une base de données non-protégée hébergée par Cognyte, société de logiciels d'analyse et d'enquête de sécurité.

Le nombre de données publiées en ligne a augmenté de 78% par rapport à 2020.

L'ensemble de ces données est issu de la plateforme de veille et d'anticipation de PwC France, Threat Watch.

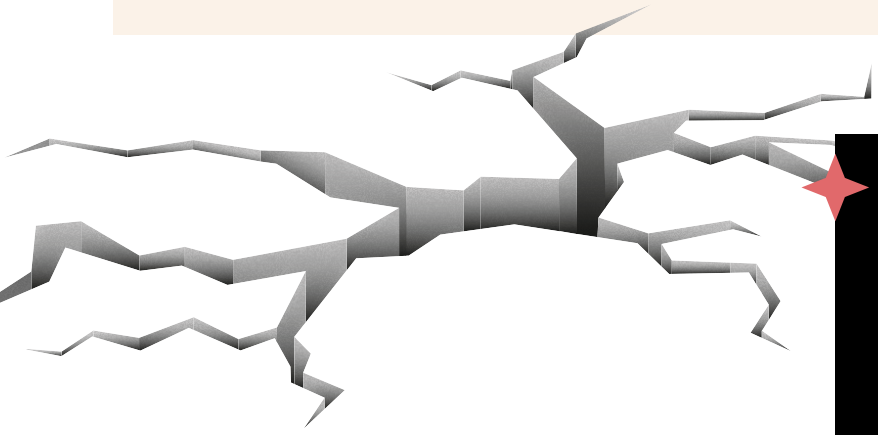
Vulnérabilités

L'une des principales causes des fuites de données est **l'exploitation d'une faille de sécurité du système d'information ou d'un élément du réseau informatique d'une entreprise par un groupe malveillant.**

Certaines vulnérabilités comme **ProxyShell, ProxyLogon** ou encore **Log4j** ont particulièrement marqué l'année 2021. En effet, les investigations menées par PwC sur ces vulnérabilités ont démontré qu'elles étaient exploitées à de multiples reprises par différents attaquants (acteurs étatiques, opportunistes...) qui ciblaient tous types d'organisations, sans distinction de taille.

Dans ce contexte, c'est plusieurs milliers d'entreprises qui ont été exposées à ces failles comme le démontre la Bundesamt für Sicherheit in der Informationstechnik (BSI), agence allemande chargée de la sécurité des systèmes d'information, qui a identifié plus de 60 000 serveurs vulnérables à la faille ProxyLogon début mars 2021.

À noter que certaines attaques ont été déclenchées plusieurs mois après la compromission de la faille initiale en raison des mécanismes de persistances déployés par des acteurs malveillants.



Notre recommandation

Identifier tous vos systèmes exposés sur Internet, vérifier en priorité l'existence de vulnérabilités les plus critiques sur ces actifs. Le cas échéant, installer rapidement les correctifs afin de réduire la fenêtre d'exposition et en parallèle, mener une levée de doute sur ces systèmes.

Menace interne

Même si moins connue, **la fuite ou la perte de données due à la malveillance ou à la négligence d'un employé** peut avoir de sérieuses conséquences. Néanmoins, ces attaques sont particulièrement difficiles à identifier, et les enquêtes n'obtiennent que rarement de résultat.

Notre recommandation

Porter l'effort sur la classification, le stockage et la gestion des accès à ces données. Une vigilance toute particulière doit être portée sur les accès temporaires aux systèmes qui hébergent les données sensibles.

Faiblesse de configuration

Les erreurs de configuration telles qu'une base de données non protégée ou un faible mot de passe provoquent souvent des fuites de données massives.

La sécurité d'une base de données face à de potentielles attaques est fortement dépendante de sa configuration.

Lorsque celle-ci est mal paramétrée, l'ensemble des données (y compris les plus sensibles) peuvent être exposées, comme en témoignent les incidents liés aux bases de données ElasticSearch et MongoDB. En 2021, PwC a mené des recherches sur plusieurs incidents provoqués par une faiblesse de configuration de bases de données entraînant la divulgation de données de santé ou d'informations sur des transactions financières.

Notre recommandation

Configurer votre base de données avec attention en mettant en place toutes les mesures de sécurité nécessaires. En parallèle, mener des activités régulières de découverte (reconnaissance) de votre exposition externe.

Pour les accès distants (bureau à distance, VPN, VDI), la configuration des options de connexion est également essentielle à la protection des données. En effet, bien souvent ces accès sont protégés par des mots de passe trop faibles ou utilisés plusieurs fois sans l'utilisation de l'authentification multifacteur. Cela rend possible de nombreuses attaques, tels que *"password spraying"*, *"credential stuffing"* ou l'utilisation des mots de passe achetés sur les forums de hacking.

Notre recommandation

Choisir des mots de passe complexes, les modifier régulièrement et étendre l'authentification multifacteur dans la mesure du possible.

À titre d'illustration, sur les trois dernières années, PwC a pu identifier le vecteur initial de compromission *via* la reconnaissance externe dans 2/3 des cas.

Tierces parties

Les crises **SolarWinds** et **Kaseya** ont montré les risques de fuites de données liées aux tiers et plus particulièrement à la chaîne d'approvisionnement.

Une entreprise doit non seulement se protéger au niveau interne et externe, mais également s'assurer de la sécurité de ses tiers. **En effet, 21% des cyberattaques réussies contre des entreprises en 2021 ont été des attaques dites « par rebond »** (*via* un prestataire, client ou fournisseur).

La problématique de l'attaque par rebond est d'autant plus significative que l'entreprise est fortement dépendante d'un seul fournisseur logiciel ou prestataire informatique. Dans cette configuration, une attaque sur ce prestataire peut engendrer des fuites de données en masse. Ce fut le cas en juillet 2021, lorsque le gestionnaire informatique Kaseya fut attaqué par un *ransomware*, affectant par ricochet entre 800 et 2 000 de ses clients.

Notre recommandation

Créer un inventaire précis, identifier les tiers qui manipulent vos données sensibles ou disposent d'un accès privilégié à votre SI. Pour ces tiers critiques, mettre en place un système de veille portant sur plusieurs aspects : les clauses contractuelles en lien avec la notification des incidents, les mesures d'urgence d'isolation, les fuites de données et les incidents. En complément, réaliser des audits de sécurité récurrents.

PRÉVENTION DE LA MENACE CYBER

QUELLES SONT LES PRINCIPALES ACTIONS JURIDIQUES À METTRE EN ŒUVRE ?

Par Sandrine Cullaffroz-Jover, Avocate, Associée, et Jamal Basrire, Associé responsable des activités Cyber Intelligence, PwC France et Maghreb

La cybercriminalité s'est professionnalisée. Organisée, protéiforme, souvent internationale, elle expose les organisations publiques et privées à des violations de données personnelles.

Face à la complexité de ces menaces, **la prévention des risques doit s'appréhender de façon pluridisciplinaire** et passe par l'anticipation. Dans ce contexte, la **planification d'actions juridiques** devrait compléter avantageusement le dispositif des mesures techniques et organisationnelles.

1. Des actions de **veille juridique** permettent de suivre l'évolution du cadre légal et réglementaire applicable aux traitements mis en œuvre au sein des entreprises, *a fortiori* dans un environnement plurijuridictionnel. Dans les secteurs interréglementés, l'articulation des normes est par ailleurs essentielle à la définition d'une stratégie de conformité, prérequis d'une bonne gouvernance de la donnée.
2. Des actions de **sensibilisation et formation**, dont le contenu doit permettre d'appréhender avec pédagogie les différents enjeux du Règlement général sur la protection des données (RGPD), peuvent être prises en charge, complétées ou encore animées, en tout ou partie, par la direction juridique et/ou le délégué à la protection des données auprès des diverses fonctions métiers.
3. Des actions de **gouvernance juridique interne** peuvent notamment se décliner selon les grands axes de réflexion suivants :
    - rédaction et opposabilité d'une charte d'utilisation (utilisateurs/ administrateurs) des systèmes d'information / encadrement des mesures de cybersurveillance au sein de l'entreprise ;
    - contribution à la classification des données composant le patrimoine informationnel de l'entreprise ;
    - détermination des durées de conservation légales ou réglementaires ;
    - gestion des délégations de pouvoirs et de signatures ;
    - contribution à la documentation de conformité interne (registre des activités de traitements, politiques de protection des données et de confidentialité, étude d'impacts sur la vie privée - *PIA* -, etc.) ;
    - recommandations en matière probatoire ;
    - contribution à la rédaction de politiques et de procédures de sécurité, remontée d'incidents et de gestion de crise, en coordination avec les autres directions fonctionnelles.
4. Des actions de **gestion contractuelle des risques avec les tierces parties,** pour déterminer la répartition des obligations et responsabilités, s'assurer de l'auditabilité des prestations externalisées et suivre la bonne exécution des contrats.
5. La souscription de **polices d'assurance** adaptées.

L'ensemble des mesures susvisées, sans tendre à l'exhaustivité, permet de mettre en lumière les différents axes de définition d'une **véritable stratégie juridique d'entreprise** comme **moyen contributif de prévention** des menaces cyber. **Cette stratégie, pour être efficace, doit pouvoir s'articuler autour des objectifs fixés par la politique de l'entreprise en matière de cybersécurité**. Une entreprise organisée en silo ne pourra déployer qu'une réponse partielle.

> **“ Les attaques cyber sont de loin la première cause d’une perte de confidentialité des données „**

L’ASSURANCE, UNE BRIQUE DE LA CYBER-RÉSILIENCE

Par Christophe Madec, Référent Cyber Bessé

Toute fuite de données personnelles résulte soit d’un acte de malveillance soit d’un acte accidentel. Les attaques cyber sont de loin la première cause de cette perte de confidentialité des données.

Face à ce type de risque, il est aujourd’hui possible de s’assurer en souscrivant une assurance cyber. L’un des avantages de ce type d’assurance est de proposer une palette de services en cas de sinistre pour accompagner l’entreprise et lui permettre de gérer aux mieux cet incident.

Les services proposés incluent une assistance juridique pour toute déclaration à la CNIL, un support en communication et une expertise en *forensic* (mesures d’investigations numériques) pour qualifier et mesurer le niveau de compromission du système d’information. Dans l’hypothèse où l’entreprise viendrait à être mise en cause, une police d’assurance cyber prévoit également un volet Responsabilité civile avec une prise en charge des frais de défense et autres frais de procédure.

Cette assurance cyber ne constitue en aucune manière une solution face à ce type de risque. Elle apporte une protection face à un risque qui n’est jamais nul et vient intelligemment compléter la politique de cybersécurité de chaque organisation.


Grand angle • Grand angle • Grand angle