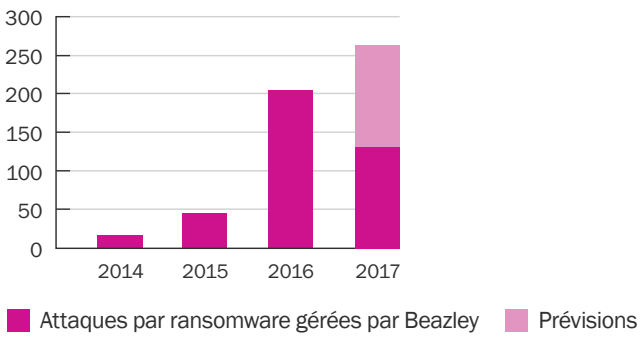
Les attaques par ransomware font la une, mais les violations de données accidentelles restent une cause importante de pertes

Le nombre d'attaques par ransomware a continué sa progression au cours du premier semestre 2017, en hausse de 50 % par rapport aux six premiers mois de l'année 2016.

Les actes de piratage et les logiciels malveillants (dont une part de plus en plus importante d'attaques par ransomware) restent la principale cause de violations de données. Elles représentent 32 % des 1 330 incidents, gérés par l'équipe Beazley Breach Response (BBR) Services, dont ont été victimes les clients de Beazley au cours du premier semestre de l'année.

Le secteur de la santé a subi la plus forte hausse de demandes de rançons (133 %).

Attaques par ransomware gérées par Beazley



Source: BBR Services

Toutefois, les failles accidentelles causées par une erreur d'un collaborateur ou les violations de données contrôlées par un fournisseur tiers continuent de poser un problème majeur. Elles sont à l'origine de 30 % de l'ensemble des violations, une part seulement légèrement inférieure à celle des actes de piratage et des logiciels malveillants. Dans le secteur de la santé, ces violations accidentelles représentent de loin la cause la plus fréquente de perte de données (42 %).

Ce niveau élevé constant de violations de données accidentelles semble indiquer que les entreprises n'ont pas encore mis en place de mesures fortes nécessaires à la protection des données et de la confidentialité des clients. Depuis 2014, le nombre de violations de données accidentelles géré par l'équipe de Beazley n'a cessé d'augmenter. Alors que les environnements réglementaires plus stricts deviennent la norme, ce manque de mesures expose les entreprises à des risques de sanctions réglementaires et financières plus importants.

L'équipe BBR Services a travaillé avec les clients assurés de Beazley afin de leur fournir des services juridiques et d'informatique légale face aux attaques par le ransomware NotPetya survenues en juin. La capacité à répondre rapidement à des attaques par ransomware est particulièrement cruciale pour les entreprises du secteur de la santé, car le Bureau des droits civils (OCR - Office for Civil Rights) considère toutes les attaques par ransomware comme une violation de données présumée.

CBSL441_FR_07/17

Violation de données – tendances 2017

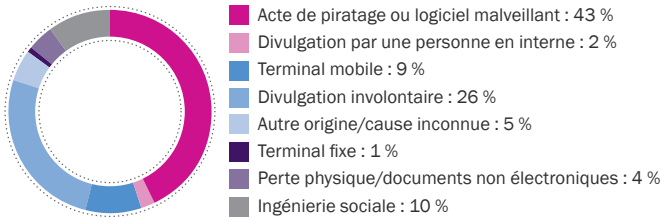
Des erreurs involontaires dans le secteur de l'enseignement supérieur
Les divulgations involontaires ont été à l'origine de 26 % des violations de données dans l'enseignement supérieur au premier semestre 2017. Bien qu'en légère baisse par rapport aux 28 % enregistrés sur la même période en 2016, cela représente encore un quart de l'ensemble des violations de données et pourrait être réduit grâce à des contrôles et des processus plus efficaces. Les actes de piratage et les logiciels malveillants ont causé près de la moitié des violations de données de l'enseignement supérieur au cours des six premiers mois de l'année 2017 (43 %), un chiffre similaire à celui du premier semestre 2016 pour les actes de piratage (45 %), dont 41 % d'incidents liés à de l'hameçonnage.

Des erreurs médicales
Les divulgations involontaires (courriels ou fax adressés à un mauvais destinataire ou documents jetés dans des conditions inadéquates) sont restées la principale cause des pertes du secteur de la santé. Elles ont occasionné 42 % des violations de données dont le secteur a été la cible au cours des six premiers mois de l'année 2017, une part semblable à celle observée sur la même période en 2016. Les actes de piratage et les logiciels malveillants ont été à l'origine de 18 % des violations de données du secteur au premier semestre 2017, contre 17 % sur les six premiers mois de 2016.

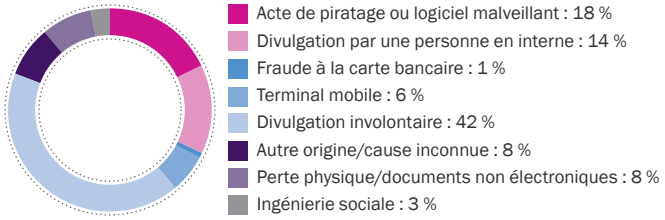
Des divulgations involontaires au sein d'établissements financiers
Les divulgations involontaires (envoi de coordonnées bancaires ou d'informations personnelles au mauvais destinataire) ont progressé de 29 % au cours du premier semestre 2017, contre 25 % sur la même période en 2016, un niveau qui est resté constant depuis 2014. La part des actes de piratage et des logiciels malveillants a baissé sur les six premiers mois de l'année 2017. Ceux-ci représentaient 37 % des violations de données, contre 46 % au cours du premier semestre 2016.

Les sociétés de services professionnels s'égarent
Au premier abord, les entreprises de services professionnels semblent avoir de meilleurs contrôles internes en place. Les violations de données involontaires ont été à l'origine de seulement 14 % de l'ensemble des incidents, un chiffre bien inférieur à la moyenne de la période considérée. Cependant, cette tendance est trompeuse, car elle est en hausse par rapport aux 9 % enregistrés au premier semestre 2016. Les entreprises du secteur n'étaient pas à l'abri des actes de piratage et de logiciels malveillants, ces incidents représentant 44 % des violations de données au cours des six premiers mois de l'année 2017, contre 53 % sur la même période en 2016. Les arnaques par ingénierie sociale, comme les demandes de virement bancaire frauduleuses et les attaques visant les formulaires de déclaration d'impôts, ont été à l'origine d'un nombre important d'incidents depuis le début de l'année 2017.

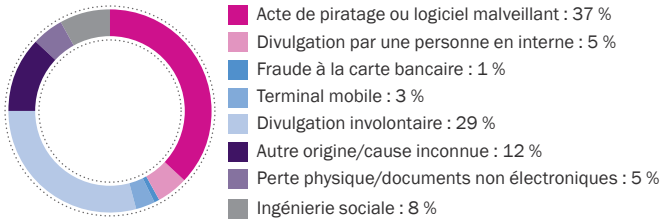
Incidents dans l'enseignement supérieur au premier semestre 2017



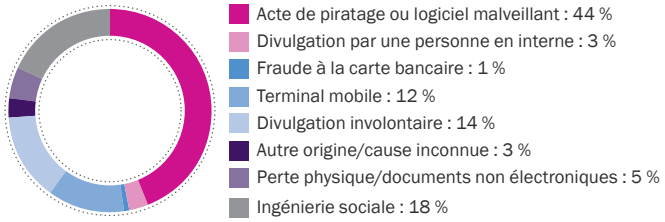
Incidents dans le secteur de la santé au premier semestre 2017



Incidents au sein des services financiers au premier semestre 2017



Incidents au sein des services professionnels au premier semestre 2017



Les quatre étapes à suivre pour aider les entreprises à protéger leurs données

S'il leur est impossible d'atteindre un niveau de protection parfait contre les cyber-attaques, les entreprises peuvent néanmoins adopter certaines mesures afin de protéger leurs données. Voici les quatre étapes clés que les entreprises peuvent suivre afin de minimiser leurs risques :

- Déployer des outils de prévention et de détection d'intrusion ;
- Faire appel à des services de veille externe sur les menaces informatiques ;
- Former leurs collaborateurs à la cyber-sécurité et les sensibiliser aux menaces potentielles ;
- Réaliser des évaluations des risques centrées sur l'identification et la protection des données sensibles qu'elles détiennent.

À propos de Beazley Breach Response (BBR) Services

Depuis le lancement de l'équipe BBR Services en 2009, Beazley a aidé ses clients à gérer plus de 6 000 violations de données. La société est actuellement le seul assureur à disposer d'une équipe interne exclusivement dédiée à la prise en charge des violations de données dont sont victimes ses clients. L'équipe BBR Services de Beazley coordonne les services juridiques ainsi que les services d'expertise après sinistre, de notification et de suivi de la notoriété dont les clients ont besoin afin de respecter l'ensemble des exigences légales et de préserver la confiance de leur clientèle. Au-delà de la coordination de la réponse face aux violations de données, l'équipe BBR Services met à jour et développe la suite de services de gestion des risques de Beazley, spécialement conçus pour minimiser les risques de violations de données.

beazley

www.beazley.fr/bbr