accenturesecurity
Communiqué de presse

Selon une étude d'Accenture et du Ponemon Institute, les logiciels malveillants et les attaques internes ont représenté un tiers des coûts liés à la cybercriminalité l'année dernière.

L'étude souligne une nette augmentation de la fréquence et du coût des attaques par ransomware

Paris, le 2 Avril 2019 - Selon l'étude d'Accenture (NYSE : ACN) et du Ponemon Institute, intitulée « Cost of CyberCrime Study », le coût pour les entreprises des logiciels malveillants et des cyberattaques perpétrées en interne, a bondi de 12 % en 2018, pour représenter un tiers du coût total des cyber-attaques.

En 2018, les entreprises installées aux États-Unis sont celles qui ont connu la plus forte augmentation (29 %) des coûts liés à la cybercriminalité, avec en moyenne 27,4 millions de dollars par entreprise – soit deux fois plus que les autres pays sondés. Le Japon arrive en deuxième position avec 13,6 millions de dollars, suivi par l'Allemagne avec 13,1 millions de dollars et le Royaume-Uni avec 11,5 millions de dollars. Les pays où les coûts moyens sont les moins élevés sont le Brésil et l'Australie, avec respectivement 7,2 et 6,8 millions de dollars.

Les chiffres pour la France :

- **31** entreprises françaises ont participé à l'étude sur un échantillon total de 355 sociétés
- **248** experts en sécurité et en IT ont été interrogés au sein du panel français
- Le coût de la cybercriminalité 2018 est de **9,7** millions de dollars soit **8,6** millions d'euros
- **23 %** d'augmentation par rapport à 2017.

Cette étude menée à travers le monde auprès de plus de 2 600 experts en sécurité et technologies de l'information de 355 entreprises, démontre que le coût imputé aux logiciels malveillants a augmenté en moyenne de 11% et atteint 2,6 millions de dollars par entreprise. Le coût des attaques internes perpétrées par les collaborateurs, le personnel temporaire, les sous-traitants ou les partenaires commerciaux a quant à lui bondi de 15 % pour atteindre en moyenne 1,6 million de dollars par entreprise.

Ces deux types de cyberattaques représentent un tiers des coûts (13 millions de dollars) lié à la cybercriminalité pour les entreprises, soit une augmentation de 1,3 million par rapport à l'année précédente. De même, le coût du phishing et de l'ingénierie sociale a augmenté en moyenne de 1,4 million de dollars par entreprise.

Ce calcul a été obtenu en additionnant les dépenses liées à l'identification, à la résolution et à la réparation des dégâts causés par les cyberattaques sur une période de quatre semaines consécutives. S'ajoutent à cela les dépenses engendrées à posteriori pour la mise en place de mesures de protection, ainsi que celles visant à réduire les impacts sur l'activité de l'entreprise et la perte de clients.

«*Cette étude démontre qu'en matière de gestion des cyber-risques, il est temps d'adopter une approche plus globale, proactive et préventive. Cela nécessite un engagement total des acteurs des entreprises et de l'écosystème de partenaires. Les équipes en charge de la cybersécurité ne sont pas encore assez impliquées en amont des innovations, et doivent développer de nouvelles compétences pour accompagner ces innovations »,* déclare Gilles Castéran, Directeur d'Accenture Security pour la France.

L'étude indique également que:

• En 2018, chaque entreprise interrogée a connu en moyenne 145 cyberattaques, qui se sont manifestées par des intrusions dans des réseaux centraux ou les systèmes de l'entreprise, ce qui équivaut à une augmentation de 11 % par rapport à 2017 et de 67 % par rapport à 2012.

• Les attaques via des logiciels malveillants sont les plus coûteuses: elles représentent en moyenne 2,6 millions de dollars pour les entreprises et sont suivies par les attaques venues du web (2,3 millions de dollars).

• Le nombre d'entreprises confrontées à des attaques par ransomware a augmenté de 15 % en 2018, entrainant une augmentation des coûts de 21 %, soit en moyenne 650 000 dollars par entreprise. Le nombre d'attaques par ransomware a plus que triplé au cours des deux dernières années.

• 85 % des entreprises ont subi des cyber-attaques par phishing et ingénierie sociale en 2018, ce qui représente une augmentation de 16 % par rapport à 2017 et 76 % ont connu des attaques basées sur le web.

• Les technologies d'automatisation, d'orchestration et d'apprentissage automatique sont les moins utilisées par les entreprises, seules 28 % d'entre elles les ont déployés. Pourtant, avec 2,9 millions de dollars elles présentent le deuxième meilleur rendement en matière de réduction des coûts de sécurité.

Pour rappel, l'étude d'Accenture « Securing the Digital Economy : Reinventing the Internet for Trust » publiée en janvier 2019 à l'occasion du forum de Davos, prévoit que dans les cinq prochaines années, la cybercriminalité pourrait coûter à l'échelle mondiale 5,2 milliards de dollars aux entreprises.

Pour plus d'informations sur les investissements susceptibles d'aider les entreprises à gérer efficacement les cyber-risques, rendez-vous sur : https://www.accenture.com/fr-fr/insights/security/etude-cout-du-cybercrime

Méthodologie
L'étude, commandée par Accenture et réalisée par le Ponemon Institute analyse divers coûts associés aux cyber-attaques, au cyber-espionnage économique, à la perturbation de activités, à la violation de propriété intellectuelle et aux pertes de revenus. Les données ont été recueillies à travers 2 647 entretiens menés sur une période de sept mois auprès d'un échantillon de référence de 355 entreprises dans 11 pays : Allemagne, Australie, Brésil, Canada, Espagne, États-Unis, France, Italie, Japon, Royaume-Uni et Singapour. L'étude détaille le coût par an annualisé de tous les événements de cybercriminalité recensés sur une période d'un an allant de 2017 à 2018. Ils incluent les coûts liés à l'investigation, à la maîtrise et à la réparation des dégâts causés par les cyber-attaques. S'ajoutent à cela les dépenses à posteriori pour se protéger d'attaques similaires – ainsi que celles visant à réduire les l'impact sur l'activité de l'entreprise et la perte de clients.

# # #

accenturesecurity
Communiqué de presse

A propos d'Accenture
Accenture, un des leaders mondiaux des services aux entreprises et administrations, propose une large gamme de services et solutions en stratégie, conseil, digital, technologie et gestion déléguée d'opérations. Combinant son expérience et son expertise dans plus de 40 secteurs d'activité et pour toutes les fonctions de l'entreprise - en s'appuyant sur le plus grand réseau international de centres de services - Accenture intervient à l'intersection de l'activité de ses clients et de la technologie pour les aider à renforcer leur performance et créer de la valeur sur le long terme pour leurs parties prenantes. Avec 469 000 employés intervenant dans plus de 120 pays, Accenture favorise l'innovation pour améliorer notre environnement de demain. Site Internet : www.accenture.com/fr

Accenture Security aide les entreprises à devenir résilientes, pour qu'elles puissent se concentrer avec confiance sur l'innovation et la croissance. Grâce à son réseau global de laboratoires de cybersécurité et à son expertise approfondie de l'ensemble du cycle de vie de la sécurité dans les différents secteurs d'activité, Accenture offre aux entreprises une protection intégrale de leurs actifs sensibles. À travers des services tels que la stratégie et la gestion des risques, la cyberdéfense, l'identité numérique, la sécurité applicative et la sécurité managée, Accenture permet aux entreprises du monde entier de se protéger des menaces connues et inconnues. Suivez-nous sur Twitter @AccentureSecure ou consultez notre site www.accenture.com/security

Contact Presse :

Farida Koulibale-Ikonga
01 56 52 74 14
f.koulibale-ikonga@accenture.com