accenturesecurity
Communiqué de presse

Selon une nouvelle étude Accenture, la cybercriminalité pourrait coûter 4 600 milliards d'euros à l'économie les cinq prochaines années

Seules 30 % des entreprises ont une totale confiance aux mesures de sécurité sur internet

Paris, le 22 mai 2019 – Selon une étude menée par Accenture (NYSE : ACN), la cybercriminalité pourrait dans les 5 années à venir coûter à l'échelle mondiale 4 600 milliards d'euros aux entreprises. L'étude souligne notamment que la capacité des entreprises à valoriser et protéger leurs actifs stratégiques à une dépendance opérationnelle forte avec Internet.

L'étude « *Securing the Digital Economy: Reinventing the Internet for Trust* » menée auprès de plus de 1 700 cadres dirigeants d'entreprises du monde entier, analyse les difficultés que rencontrent les entreprises face à leur présence en ligne et décrypte les nouveaux rôles que doivent endosser les cadres dirigeants pour assurer la confiance digitale.
Le rapport relève notamment que la cybercriminalité, quelles que soient les formes qu'elle revêt menace les activités opérationnelles, les capacités d'innovation et la croissance, ainsi que la capacité à développer de nouveaux produits et services et cela pèse en centaine de milliards d'euros sur les entreprises. Le secteur le plus menacé est celui de *high-tech*, dont les pertes potentielles sont estimées à 753 milliards de dollars, suivent les sciences de la vie et de l'automobile, qui pourraient respectivement perdre 563 et 443 milliards de dollars.

« L'évolution de l'exposition des entreprises à de nouveaux risques engendre une érosion de la confiance dans l'économie numérique », estime Gilles Castéran, Directeur d'Accenture Security en France*. « Le renforcement de la confiance exige une collaboration forte entre les organisations avec une prise de leadership par des dirigeants. La cyber résilience de notre économie nécessite repenser nos modes de gouvernance, nos principes d'architecture business et les technologies sous-jacentes.* »

Résultats clés de l'étude :

79 % des participants reconnaissent que leur organisation adopte les technologies émergentes plus rapidement qu'elle ne parvient à résoudre les problèmes de cybersécurité qui en découlent et de garantir une économie digitale résiliente.

75 % estiment que la résolution des problèmes de cybersécurité nécessitera un effort collectif et réfléchi, dans la mesure où aucune organisation ne pourra à elle seule le résoudre.

80% estiment qu'il est de plus en plus difficile de protéger leur organisation des faiblesses dont souffrent leurs partenaires, compte tenu de la complexité et du caractère tentaculaire des écosystèmes connectés modernes

« *Aucune organisation ne peut, à elle seule, relever les défis engendrés par les cybermenaces. Il s'agit là d'un challenge mondial qui nécessite une réponse mondiale, dans laquelle la collaboration sera un enjeu clé. Pour construire un avenir fondé sur une économie numérique robuste et fiable, les dirigeants doivent avoir une approche allant au-delà des limites de leur propre organisation, travailler au sein d'un écosystème de partenaires et sécuriser l'ensemble de leurs chaînes de valeur, en prenant en compte chaque partenaire, chaque fournisseur et chaque client. »,* insiste Gilles Castéran.

À l'heure où l'émergence rapide des nouvelles technologies crée des défis supplémentaires, quatre participants sur cinq (79 %) reconnaissent que leur organisation adopte les technologies émergentes plus rapidement qu'elle ne parvient à résoudre les problèmes de cybersécurité qui en découlent, trois quarts (76 %) d'entre eux notent en outre que certains problèmes de cybersécurité ont échappé à leur vigilance du fait de nouvelles technologies telles que l'Internet

des objets (IoT) et l'Internet industriel des objets (IIoT). Une majorité (80 %) d'entre eux estiment également qu'il est de plus en plus difficile de protéger leur organisation des failles que présentent leurs partenaires, ce qui n'est pas surprenant compte tenu de la complexité et du caractère tentaculaire des écosystèmes connectés modernes.

Autre enjeu de taille pour les cadres dirigeants aujourd'hui : la protection des données des consommateurs. 76 % des participants estiment que les consommateurs ne peuvent avoir confiance dans la protection de leurs identités en ligne dans la mesure où une quantité non négligeable de leurs données personnelles est déjà accessible.

Pour en savoir plus sur les actions concrètes et essentielles à prendre pour construire une économie numérique fiable et sécurisée, téléchargez notre rapport « *Securing the Digital Economy: Reinventing the Internet for Trust* ».

Méthodologie
Accenture Research a interrogé 1 711 cadres dirigeants travaillant pour des entreprises dont le chiffre d'affaires annuel est supérieur ou égal à un milliard de dollars, cela en octobre et novembre 2018 et dans 13 pays : Allemagne, Australie, Brésil, Canada, Chine, Espagne, États-Unis, France, Inde, Italie, Japon, Royaume-Uni et Suisse. Des entretiens approfondis ont été menés avec des PDG (61 %), des directeurs opérationnels (20 %), des directeurs de l'innovation (9 %) et des directeurs de la stratégie (9 %). Le coût moyen de la cybercriminalité a été calculé en pourcentage des revenus pour chaque secteur, en incluant le coût engendré par une cyber-attaque de grande ampleur. Ces pourcentages sectoriels ont ensuite été appliqués aux revenus mondiaux de chaque secteur pour générer un modèle d'évaluation des risques sur cinq ans et pour chaque industrie.

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 477 000 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

# # #

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

Copyright © 2019 Accenture. Tous droits réservés. Accenture et son logo sont des marques commerciales d'Accenture