Plus de la moitié des organisations ne disposent pas de défenses efficaces contre les cyberattaques, selon une étude d'Accenture

Le rapport State of Cyber Resilience (*État de la cyber-résilience*) révèle certaines des principales caractéristiques des leaders en matière de cyber-résilience

Paris, le 14 décembre 2021 – Plus de la moitié (55 %) des grandes entreprises ne sont pas efficaces dans la lutte contre les cyberattaques, l'identification et la correction rapides des failles de sécurité ou la réduction de l'impact de ces failles, selon une nouvelle étude d'Accenture (NYSE : ACN).

Basée sur une enquête menée auprès de 4 700 cadres dans le monde, l'étude State of Cybersecurity Resilience 2021 (*État de la cybersécurité et de la cyber-résilience en 2021*) d'Accenture examine la place qu'accordent les organisations à la sécurité, l'efficacité de leurs efforts actuels et la performance de leurs investissements en matière de sécurité.

Cette étude révèle également que quatre personnes interrogées sur cinq (81 %) estiment que « maintenir une avance sur les attaquants est un combat sans fin dont le coût n'est pas soutenable » – une augmentation par rapport aux 69 % de l'étude de l'an dernier. Dans le même temps, bien que 82 % des personnes interrogées aient augmenté leurs dépenses de cybersécurité durant l'année écoulée, le nombre de failles effectivement exploitées – ce qui inclut les accès non autorisés à des données, applications, services, réseaux ou appareils – a bondi de 31 % par rapport à l'année précédente pour atteindre une moyenne de 270 par entreprise.

« Depuis les cybercriminels débutants jusqu'aux pirates perfectionnés commandités par des États-nations, les cyber-attaquants développent de nouvelles capacités pour mener leurs attaques » déclare Michaël Bittan, responsable des activités cybersécurité d'Accenture en France. « Notre analyse révèle que les organisations se concentrent trop souvent sur les seuls résultats commerciaux aux dépens de la cybersécurité : les risques qu'elles encourent sont ainsi largement accrus. Et bien qu'il soit difficile de trouver le bon équilibre, les organisations qui se dotent d'une vision claire du panel des menaces et qui visent à aligner priorités et résultats opérationnels sur cette vision obtiennent des niveaux plus élevés de cyber-résilience. »

Le rapport souligne la nécessité d'étendre les efforts de cybersécurité hors des murs de l'entreprise elle-même pour englober tout son écosystème et constate que les attaques indirectes – c'est-à-dire les attaques menées contre une organisation via sa chaîne d'approvisionnement – continuent de croître. Par exemple, bien que les deux tiers (67 %) des organisations considèrent leur écosystème comme sûr, les attaques indirectes ont représenté 61 % de l'ensemble des cyberattaques au cours de l'année écoulée - chiffre qui se limitait à 44 % l'année précédente.

Par ailleurs, l'étude a permis d'identifier un petit groupe d'entreprises qui non seulement excellent en matière de cyber-résilience, mais également parviennent à l'aligner sur leur stratégie d'entreprise. Résultats : une amélioration de leurs résultats opérationnels et du retour sur leurs investissements en cybersécurité. Par rapport aux autres organisations, ces « cyber-champions », comme les a nommés Accenture, sont nettement plus susceptibles :

- de réaliser un juste équilibre entre cybersécurité et objectifs commerciaux ;
- de s'adresser directement au DG et au Conseil d'administration et d'entretenir une relation étroite avec le commerce et le CFO ;
- de fréquemment consulter les DG et CFO pour développer la stratégie de cybersécurité de leur organisation ;
- de protéger leur organisation contre les pertes de données ;
- d'intégrer la sécurité dans leurs initiatives de cloud, et
- de mesurer la maturité de leur programme de cybersécurité au moins une fois par an.

« Dépenser plus en cybersécurité sans aligner finement la démarche sur l'opérationnel ne rend pas votre organisation plus sûre », continue Michaël Bittan. « En matière de gestion des cyber-risques, les organisations ne peuvent pas se permettre de sélectionner une voie au détriment d'une autre. Pour atteindre une cyber-résilience durable et mesurable, les Chief Information Security Officers doivent renoncer aux silos sécuritaires pour pouvoir collaborer avec les cadres concernés dans leur organisation : c'est ainsi qu'ils obtiendront une vision à 360 degrés des risques et priorités de l'entreprise. »

Pour en savoir plus sur cette étude, téléchargez ici le rapport State of Cybersecurity Resilience 2021.

Méthodologie
Accenture Research a interrogé 4 744 cadres représentant des entreprises dotées d'un chiffre d'affaires annuel supérieur à 1 milliard de dollars US, de 23 secteurs d'activité et 18 pays, en Amérique du Nord et du Sud, en Europe et en Asie-Pacifique. Pour définir quatre niveaux de cyber-résilience, une analyse a été réalisée sur un échantillon de 3 455 organisations, dont les cyber-champions représentaient 5 %. L'étude a été réalisée entre mars et avril 2021.

A propos d'Accenture
Accenture est un des leaders mondiaux des services aux entreprises et administrations, avec une expertise de pointe dans les domaines du numérique, du cloud et de la sécurité. Combinant une expérience unique et une expertise spécialisée dans plus de 40 secteurs d'activité, Accenture s'appuie sur le plus grand réseau international de centres de technologie avancée et d'opérations intelligentes pour offrir à ses clients des services Strategy & Consulting, Interactive, Technology et Operations. Avec 624 000 employés, Accenture s'engage chaque jour auprès de ses clients dans plus de 120 pays, à réaliser la promesse de la technologie alliée à l'ingéniosité humaine. Accenture s'appuie sur le changement pour générer de la valeur et créer une réussite partagée avec ses clients, ses collaborateurs, ses actionnaires, ses partenaires et ses communautés.
Site Internet : www.accenture.com/fr

Contacts :

Accenture

Camille Garcia
+33 1 53 23 54 94
camille.garcia@accenture.com

Velislava Le Fevre
+33 1 53 23 46 18
velislava.lefevre@accenture.com