# Cybersécurité : 87 % des attaques ciblées sont évitées, en net progrès sur une année, alors même que leur nombre a doublé en 2018, d'après une étude d'Accenture

Une nouvelle étude d'Accenture révèle que malgré une amélioration de la cybersécurité, les entreprises connaissent encore 30 intrusions effectives par an, prouvant l'importance d'investir dans des technologies innovantes pour renforcer leur résilience en matière de sécurité

**Paris, le 10 septembre 2018.** Alors que le nombre moyen de cyberattaques ciblées par entreprise a plus que doublé cette année (232 en 2018 contre 106 en 2017), les entreprises ont sensiblement amélioré leur capacité à identifier et à contrer ces cyber-menaces d'après une étude d'Accenture. Néanmoins, seules deux organisations sur cinq investissent actuellement dans des technologies innovantes comme le machine learning, l'IA et l'automatisation pour améliorer leur cyber-résilience, alors que ces technologies sont parfaitement maîtrisées par les attaquants.

Réalisée entre janvier et mi-mars 2018, l'étude d'Accenture analyse les attaques ciblées qui peuvent causer des dommages en passant outre les défenses en place ou dérober des informations de valeur. Malgré la pression accrue des attaques de ransomware, dont la fréquence a plus que doublé l'an dernier, Accenture a constaté que les entreprises se renforcent et sont désormais en mesure d'éviter 87 % des attaques ciblées contre 70 % en 2017. Cependant, avec 13 % d'attaques ciblées capables de contourner les solutions de cybersécurité en place et en moyenne 30 attaques effectives par an engendrant des dommages et des pertes, les entreprises sont encore fragiles face aux cyberattaques.

« Désormais, seule une cyberattaque sur huit aboutit contre une sur trois l'an dernier. Les entreprises parviennent à mieux contrer le piratage, le vol et la divulgation de leurs données. » explique Eric Boulay, directeur d'Accenture Security en France et au Benelux. « Cette étude met en évidence une trajectoire très positive liée à la maturité croissante des directions générales vis-à-vis des promesses et des menaces du digital. Pour continuer à progresser en 2018, trois fois plus d'entreprises dépassent 10% des investissement IT en sécurité pour continuer à anticiper et s'adapter aux risques cyber. Pour cela, elles doivent utiliser et maitriser les mêmes armes que les attaquants, recourir aux meilleurs experts (hackeurs éthiques) et aux technologies innovantes basées sur l'IA ou l'analyse comportementale. Enfin l'automatisation des analyses et des réponses permet de compenser la rareté des compétences.»

## Les équipes de sécurité détectent plus rapidement les intrusions

La détection des failles de sécurité s'améliore également puisque le temps nécessaire pour les repérer se compte désormais en jours ou en semaines. En moyenne, 89 % des personnes interrogées ont déclaré que leurs équipes de sécurité détectait les intrusions sous un délai d'un mois, contre

seulement 32 % l'an dernier. Ainsi, cette année 55 % des intrusions ont été détectées en une semaine ou moins, contre 10 % l'an passé.

Mais si les entreprises détectent les attaques plus rapidement, les équipes de sécurité en interne ne détectent que 64 % des intrusions (autant que l'an passé) et collaborent avec des entreprises extérieures pour détecter le reste, soulignant l'importance d'une collaboration entre entreprises et administrations publiques. D'autant que les personnes interrogées indiquent que plus d'un tiers (38%) des intrusions non détectées par leurs équipes internes sont identifiées par des hackeurs experts en sécurité (*hackeurs éthiques*) où par des concurrents (contre 15 % en 2017).

**La cybersécurité s'applique aussi aux menaces internes**

Pour les personnes interrogées, leur entreprise n'est activement protégée par leur programme de sécurité qu'aux deux tiers (67 %). Si les incidents provenant de l'extérieur continuent à constituer une menace sérieuse, l'enquête révèle que les entreprises ne doivent pas négliger les attaques internes. Deux des trois types de cyberattaque les plus fréquentes et les plus dangereuses sont les attaques internes et la publication accidentelle de données. Pour les entreprises l'analyse des menaces ainsi que la surveillance sont les deux pratiques les plus susceptibles d'améliorer leur cybersécurité (à 46% pour chacune). Les entreprises sont donc conscientes des avantages à investir dans les technologies émergentes, puisque 83 % d'entre elles s'accordent à dire que l'intelligence artificielle, le machine learning, le deep learning, l'analyse des comportements utilisateurs ou encore la blockchain sont essentiels à la sécurité future des entreprises. Il est aussi utile de s'associer à des experts en sécurité connaissant les pratiques des cyber attaquants afin de mieux comprendre les menaces.

Pour renforcer leur résistance aux cyber-attaques, les entreprises doivent :

1. **Construire des fondations solides** en identifiant les actifs de valeur pour mieux les protéger y compris des risques internes. Il est essentiel de s'assurer que des contrôles soient mis en place tout au long de la chaîne de valeur de l'entreprise.
2. **Tester sa sécurité informatique** en entrainant les équipes de cybersécurité aux meilleures techniques des hackeurs. Les jeux de rôles mettant en scène une équipe d'attaque et de défense avec des entraîneurs peuvent permettre de faire émerger les points d'améliorations.
3. **Oser les nouvelles technologies.** Pour une entreprise il est recommandé d'investir dans des technologies capables d'automatiser la cyberdéfense et notamment de recourir à la nouvelle génération de gestion des identités qui s'appuie sur l'authentification multifacteur et l'analyse du comportement utilisateur.
4. **Etre force de proposition et identifier les menaces en amont** en développant une équipe stratégique (« threat intelligence ») chargée de faire évoluer un centre opérationnel de

sécurité (SOC) intelligent s'appuyant sur une collecte et une analyse massive de données (« data-driven approach »).

5. **Faire évoluer le rôle du responsable de la sécurité des systèmes d'information.** Le CISO est plus proche des métiers, il trouve le bon équilibre entre sécurité et prise de risque et il communique de plus en plus avec la direction générale qui détient maintenant 59% des budgets sécurité contre 33% il y a un an.

**Méthodologie**

Pour l'étude Bilan 2018 de la Cyber résilience, Accenture a interrogé 4 600 professionnels de la cybersécurité en entreprise et représentant des entreprises ayant un chiffre d'affaires annuel d'au moins 1 milliard de dollars et cela dans 15 pays. Le but de l'étude est de comprendre le niveau de priorité que les entreprises attribuent à la sécurité, l'efficacité des initiatives mises en place et le niveau de satisfaction quant aux investissements actuels. Plus de 98 % des personnes interrogées sont des décideurs principaux dans la stratégie et les dépenses de cybersécurité de leur entreprise. Dans le cadre de cette étude, une entreprise cyber-résiliente applique des stratégies de sécurité fluides pour répondre rapidement aux menaces, réduire les dommages et continuer son activité malgré l'attaque. Elle peut ainsi introduire des offres et des modèles d'affaires innovants en toute sécurité, renforcer la confiance du client et donc sa croissance.

Pour en savoir plus sur l'étude, téléchargez le rapport 2018 State of Cyber Resilience.

**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 449 000 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 :**

Clémence Caradec
+ 33 1 53 23 55 23
clemence.caradec@accenture.com

Giulia Goodwin
+33 1 56 03 13 83
giulia.goodwin@bm.com