Les sociétés de services financiers ont amélioré leur cyber-résilience et ont évitées plus de 80 % des tentatives d'intrusions

Pourtant, les risques associés aux technologies émergentes, notamment l'apprentissage automatique et l'intelligence artificielle, sont autant de nouveaux défis pour les systèmes de sécurité existants

PARIS ; 4 décembre 2018 – Bien que le nombre de cyberattaques ait doublé en 2017, les sociétés de services financiers comblent leur retard sur les cybercriminels avec quatre tentatives d'intrusion sur cinq stoppées l'an dernier, contre deux sur trois en 2016, selon une nouvelle étude d'Accenture.

Réalisée entre janvier et mi-mars 2018, l'étude State of Cyber Resilience for Financial Services 2018 est basée sur une enquête menée auprès de plus de 800 professionnels de la cybersécurité au sein des entreprises du secteur des services financiers. Elle s'appuie également sur des investigations menées sur des cyberattaques ciblées qui auraient pu pénétrer les défenses d'un réseau et causer des dommages, ou accéder à des actifs et processus de grande valeur au sein des organisations.

Dans l'édition 2018, les sociétés de services financiers sont parvenues à stopper 81 % des tentatives d'intrusion, contre 66 % l'an dernier. Il n'est donc pas surprenant que plus de 80 % des décideurs interrogés se disent confiants dans les performances de leurs protocoles de sécurité, toutes technologies et capacités confondues.

On observe toutefois également que, si le nombre de tentatives d'intrusions contrecarrées a effectivement augmenté, plus de 71 % des intrusions en France sont, en moyenne, restées non détectées pendant plus d'une semaine, et 6 % pendant plus d'un mois. Cela semble indiquer que les décideurs accordent peut-être une confiance excessive dans les capacités de leurs systèmes de sécurité dans la mesure où il est bien sûr absolument indispensable d'identifier une intrusion en quelques jours, voire en quelques heures, pour éviter tout dommage.

« *Les entreprises du secteur des services financiers convergent vers un niveau de grande maîtrise pour ce qui est des systèmes de sécurité en place, y compris sur le plan de la cyber-résilience et de l'état de préparation aux interventions* », explique Richard Leroy, directeur exécutif chez Accenture Financial Services. « *Avec l'évolution des nouvelles technologies d'entreprise, la cybersécurité doit elle aussi évoluer. Les banques et les assureurs adoptent aujourd'hui tout un ensemble de nouvelles technologies - notamment le cloud, les microservices, les interfaces de programmation d'applications, le edge computing et la blockchain - qui engendrent inévitablement de nouveaux risques de sécurité, notamment dans un contexte où les cyberattaques sont, elles aussi, toujours plus sophistiquées*. »

Bien que les banques et les assureurs aient de plus en plus recours aux alliances et aux partenariats commerciaux pour leur croissance - ces partenariats s'appuyant même souvent sur des interfaces de programmation d'applications ouvertes -, un peu moins de la moitié (45 %) des répondants français déclarent qu'ils soumettent leurs partenaires à des normes de cybersécurité moins exigeantes que pour leur propre entreprise. Les entreprises restent donc vulnérables face aux risques de sécurité externes. De plus, les sociétés de services financiers étendent leurs infrastructures existantes à la « périphérie » (*edge*) de leurs réseaux et ont recours aux appareils connectés (caméras, capteurs et montres connectées notamment), ce qui contraint les professionnels de la sécurité à élargir leur champ d'action pour protéger ces nouveaux points d'entrée potentiels qui seront détectés et exploités par les criminels.

Pourtant, si les technologies sophistiquées peuvent engendrer de nouvelles menaces, elles peuvent aussi permettre de renforcer leur cyber-résilience. On remarque ainsi que 85 % des décideurs français estiment que les nouvelles technologies (comme l'intelligence artificielle (IA), l'apprentissage automatique, le *deep learning* et l'automatisation) sont indispensables pour assurer la sécurité de leur entreprise. Pour autant, seule la moitié des sociétés de services financiers françaises investissent actuellement dans les nouvelles technologies destinées à leur cyberdéfense, telles que

l'IA/l'apprentissage automatique et l'automatisation des processus robotisés (RPA) (55 % et 50 %, respectivement). En outre, seulement 18 % des décideurs français interrogés rapportent que leurs dépenses en matière de cybersécurité ont significativement augmenté (au moins doublé) au cours des trois dernières années, et que seulement 19 % envisagent de le faire au cours des trois prochaines années.

L'étude montre également que les collaborateurs, et non pas seulement l'équipe de cybersécurité, doivent être activement impliqués dans la protection de leurs entreprises. Si les équipes de cybersécurité interrogées ont identifié les deux tiers de l'ensemble des intrusions affectant leurs entreprises, en France les employés externes à ces équipes sont parvenus à identifier la majorité (70 %) des intrusions restantes, non détectées par les équipes de sécurité.

« *Les cyber-risques vont désormais au-delà des frontières traditionnelles des entreprises, sous l'effet de la numérisation accélérée des services financiers et de l'émergence de l'Open Banking et du partage de données à des tiers* », poursuit Luc Tentillier, directeur exécutif chez Accenture Security. « *L'IA, l'apprentissage automatique et l'automatisation des processus robotisés peuvent permettre de surveiller et de combattre ces menaces dans un cadre cohérent, mais les entreprises doivent pour cela faire les investissements nécessaires*. »

Méthodologie

Pour l'enquête « 2018 State of Cyber Resilience », Accenture a interrogé 4 600 professionnels de la cybersécurité en entreprise, dont 821 travaillant dans le secteur des services financiers (banque, assurance et marchés de capitaux), représentant des entreprises ayant un chiffre d'affaires annuel d'au moins 1 milliard de dollars et cela dans 15 pays. L'objectif 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. En France, 80 professionnels de la cybersécurité ont été interrogés, dont 40 dans le secteur de la banque et des marchés de capitaux et 40 dans celui de l'assurance.

À 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 459 000 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 :
Bonnie OLIVIER
+ 33 (0) 1 53 23 54 61
bonnie.olivier@accenture.com

François LUU
+ 33 (0) 1 53 23 68 55
francois.luu@accenture.com