NEWS RELEASE

Baromètre Euler Hermes-DFCG 2019

Pour 6 entreprises sur 10, la lutte contre la fraude n'est pas une priorité

- 1 entreprise sur 5 a été visée par plus de 10 tentatives de fraude en 2018 (1 sur 10 en 2017).
- L'usurpation d'identité monopolise le podium des attaques subies, et les attaques cyber sont désormais utilisées comme clés d'entrée.
- 8 entreprises sur 10 craignent une accentuation du risque de fraude et de cybercriminalité en 2019. Pourtant, 6 répondants sur 10 n'ont pas alloué de budget spécifique pour y faire face.

PARIS, 18 AVRIL 2019 – Pour la 5ème année consécutive, Euler Hermes, le leader européen de l'assurance fraude, et le Réseau des Directeurs Financiers et de Contrôle de Gestion (DFCG), ont interrogé plus de 300 entreprises implantées en France sur leur exposition, leur ressenti et leurs mesures de prévention face aux risques de fraude et cybercriminalité. Décryptage des résultats de ce baromètre annuel.

En fréquence comme en sévérité, le risque de fraude et de cybercriminalité s'accroît

En 2018, plus de 7 entreprises sur 10 ont été victimes d'au moins une tentative de fraude. Un chiffre similaire à celui constaté en 2017, signe que le risque de fraude et de cybercriminalité reste fort pour les entreprises. Ce qui est plus inquiétant, c'est qu'en nombre d'attaques subies par les entreprises, la menace s'intensifie : 18% des répondants à l'enquête Euler Hermes-DFCG ont été visés par plus de 10 tentatives de fraude en 2018 (10% en 2017). Les fraudeurs n'hésitent pas à revenir à la charge plusieurs fois pour arriver à leurs fins, notamment grâce aux moyens informatiques.

Ces répétitions d'attaques leur permettent d'ailleurs de maintenir une efficacité résiliente : 26% des entreprises interrogées ont subi au moins une fraude avérée en 2018 (30% en 2017). En revanche, quand on regarde le préjudice, la facture semble s'alourdir pour les entreprises : 13% des entreprises attaquées en 2018 ont subi un préjudice supérieur à 100K € (10% en 2017). Pire encore, pour 5% des entreprises ayant subi une attaque en 2018, la perte consécutive a dépassé les 500K € (3% en 2017). De quoi fragiliser fortement la trésorerie des entreprises, et compromettre leur activité.

Le cyber au service de l'usurpation d'identité, technique favorite des fraudeurs

La fraude au faux fournisseur est toujours la plus utilisée par les pirates, citée par 47% des répondants. Elle est suivie par les autres usurpations d'identité (banques, avocats, commissaires au compte), citées par 30% des répondants, la fraude au faux président (29%), et la fraude au faux client (25%). L'usurpation d'identité est plébiscitée par les fraudeurs, et une seule cyber-attaque figure parmi le top 5 des attaques les plus citées : l'intrusion dans les systèmes d'information (28%). Ce résultat souligne le caractère critique des données hébergées par l'entreprise, ces dernières faisant office de point d'entrée pour construire une fraude.

« Après la vague d'attaques au ransomware, qui visait la récupération d'une somme d'argent sous forme de rançon via le blocage d'outils ou de données, nous constatons que les cyberattaques servent de plus en plus le montage de mécanismes de fraude classiques. Désormais, les fraudeurs s'introduisent dans les systèmes d'informations des entreprise afin de récupérer des données et d'affiner leur usurpation d'identité. Le cyber devient un outil au service de la fraude plus qu'une technique directe de détournement », explique Sébastien Hager, responsable souscription assurance fraude chez Euler Hermes France.

Les entreprises craignent de plus en plus le risque de fraude et de cybercriminalité…

L'autre conclusion de cette enquête, c'est que les entreprises sont conscientes de la menace qui plane. En effet, 78% des répondants craignent une accentuation du phénomène sur l'année à venir (+8 points par rapport à notre dernière enquête). De même, pour 77% des entreprises interrogées, le risque de fraude est une préoccupation majeure. Alors, que mettent-elles en place pour déjouer les attaques subies ?

« 74% des directions financières ont réussies à déjouer les tentatives de fraude. Encore une fois le facteur humain y est très important (80 % des réussites sont liées au bon sens et à la mise en place de contrôle interne). Les dispositifs techniques sont passés de 12 à 20% ; preuve, s'il en est, du rôle primordial des directeurs des systèmes d'information (DSI) dans cette lutte. Curieusement, 59% des sondés n'ont pas alloué de budget spécifique pour lutter contre la fraude. Il est urgent que les DSI élaborent avec le directeur financier le budget et la stratégie de protection de l'entreprise », déclare Bruno de Laigue, Président du Réseau des Directeurs Financiers et de Contrôle de Gestion.

… Mais ne se donnent toujours pas les moyens de s'en protéger !

De l'autre côté du spectre, une conclusion du baromètre parait particulièrement inquiétante : 6 entreprises sur 10 n'ont pas alloué ou transféré de budget spécifique pour lutter contre le risque de fraude et de cybercriminalité. Le paradoxe persiste et reste saisissant : les entreprises sont inquiètes, ont peur de voir la menace se renforcer… mais ne se donnent pas les moyens financiers de s'en protéger !

Les entreprises ont également des progrès à faire en matière d'anticipation de la fraude. Encore près d'un répondant sur deux ne dispose pas de plan d'urgence à activer en cas d'attaque, alors que la réactivité est primordiale pour limiter les conséquences d'une fraude. Dans le même temps, près d'une entreprise sur deux ne dispose pas de plan de reprise de l'activité (PRA) à déclencher en cas de cyberattaque. De quoi craindre d'importantes pertes d'exploitation pour les entreprises concernées, le temps de remettre les outils en état de service.

Les consciences seraient-elles en train de s'éveiller ?

Malgré ces constats sans appel, 69% des entreprises interrogées jugent leur dispositif de protection face à la fraude satisfaisant. C'est beaucoup, comparé aux faiblesses constatées, mais on peut y voir une amélioration : lors de notre enquête précédente, 73% des répondants partageaient cette opinion. Une preuve que les entreprises commencent à prendre conscience de leur retard en matière de protection ?

« On note quand même quelques progrès de la part des entreprises. Même si elles sont peu à dédier un budget spécifique à leur protection contre le risque de fraude et de cybercriminalité, certaines ont compris que des actions peu coûteuses pouvaient être menées afin d'anticiper les attaques. Ainsi, 64% des répondants ont investi dans l'audit de sécurité des SI, 62% dans l'audit des procédures de contrôle interne, et 61% dans des actions de sensibilisation et de formation interne de la direction financière. La route est encore longue, mais les consciences s'éveillent », estime Sébastien Hager.

« La mise en place du RGPD a permis la prise de conscience du risque cyber. Paradoxalement, plus des ¾ des directions financières, essentiellement de PME / ETI, craignent une accentuation du risque de fraude sur l'année qui vient alors qu'une entreprise sur deux ne dispose d'aucun plan d'urgence à activer en cas d'attaque. Au-delà des investissements et de l'impérieuse nécessité de coopérer entre DAF et DSI, les entreprises doivent faire preuve de bon sens, être discrètes, éviter toute négligence, et surtout ne pas se dire que cela n'arrive qu'aux autres », affirme Bruno de Laigue.

****

Contacts médias

EULER HERMES FRANCE
Maxime Demory +33 (0)1 84 11 35 43
maxime.demory@eulerhermes.com

DFCG
Florence Sabourin +33 (0)6 07 62 47 36
florencesabourin@dfcg.asso.fr

****

A propos d'Euler Hermes

Prévoir les risques commerciaux et d'impayés aujourd'hui, c'est protéger la trésorerie demain

Euler Hermes est le leader mondial des solutions d'assurance-crédit et un spécialiste reconnu dans les domaines du recouvrement et de la caution. Avec plus de 100 années d'expérience, Euler Hermes offre une gamme complète de services pour la gestion du poste clients. Son réseau international de surveillance permet d'analyser la stabilité financière de PME et de grands groupes actifs dans des marchés représentant 92% du PNB global. Basée à Paris, la société est présente dans plus de 50 pays avec plus de 5 800 employés. Membre du groupe Allianz, Euler Hermes est noté AA par Standard & Poor's. La société a enregistré un chiffre d'affaires consolidé de 2,7 milliards d'euros en 2018 et garantissait 962 milliards d'euros de transactions commerciales dans le monde fin 2018. Plus d'informations: https://www.eulerhermes.com

A propos de la DFCG

Le réseau des Directeurs Financiers et de Contrôle de Gestion (DFCG) créé en 1964 regroupe plus de 3 000 financiers d'entreprises privées et publiques, qui représentent environ 1 800 sociétés (ETI, PME, TPE) dans 14 régions françaises et outre-mer. Le réseau assure près d'une centaine de formations par an et accompagne financièrement ou par du « mentoring », plus d'une cinquantaine de jeunes qui n'ont pas les moyens d'accéder aux études supérieures de finance et de gestion d'entreprises via sa fondation, placée sous l'égide de la Fondation de France. Le réseau décerne chaque année le « trophée du directeur financier de l'année » en décembre. Depuis 2018, le réseau est présidé par Bruno de Laigue (DAF de Business Partners SAS).