Baromètre Euler Hermes – DFCG 2021

1 entreprise sur 4 a subi une fraude avérée cette année

- 2 entreprises sur 3 ont subi au moins une tentative de fraude cette année, et 1 entreprise sur 5 a subi plus de 5 attaques ;
- 33% des entreprises victimes de fraude ont subi un préjudice supérieur à 10K €, et 14% ont subi un préjudice supérieur à 100K € ;
- Effet Covid-19 : près d'une entreprise sur deux a remarqué une recrudescence des attaques suite à la généralisation du télétravail ;

PARIS, 15 SEPTEMBRE 2021 – Pour la 7ème année consécutive, Euler Hermes, le leader européen de l'assurance fraude, et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), ont interrogé près de 300 entreprises implantées en France sur leur exposition, leur ressenti et leurs mesures de prévention face aux risques de fraude et cybercriminalité. En résulte le Baromètre Fraude et Cybercriminalité 2021, qui porte cette année une dimension inédite, relative au contexte sanitaire et économique : la crise Covid-19 a-t-elle accentué le risque de fraude pour les entreprises ?

Des attaques récurrentes, pour une efficacité croissante des fraudeurs

Le constat est clair : 2 entreprises sondées sur 3 déclarent avoir été victimes d'au moins une tentative de fraude cette année. Une tendance similaire à celle des précédentes éditions du Baromètre Euler Hermes – DFCG, qui atteste de la résilience des fraudeurs. Le risque de fréquence ne se dissipe pas non plus : cette année, 20% des entreprises interrogées ont subi au moins 5 tentatives de fraude, et 13% en ont subi au moins 15. Les fraudeurs multiplient les attaques… et cela semble payer.

« 28% des entreprises interrogées déclarent avoir subi au moins une fraude avérée cette année : en d'autres termes, les fraudeurs parviennent à leurs fins environ toutes les 4 tentatives. Les fraudeurs ne perdent pas de terrain face aux mesures de défense prises par les entreprises, et leur professionnalisation ne cesse de se renforcer. Le risque de fraude et de cybercriminalité pèse lourdement sur la trésorerie des entreprises », alerte Armelle Raillard, Experte assurance-fraude chez Euler Hermes France.

En effet, le coût de la fraude semble également en croissance : 33% des entreprises victimes d'une fraude cette année déclarent un préjudice supérieur à 10K € (+3 points par rapport à la précédente édition du Baromètre). Plus inquiétant encore, 14% des entreprises interrogées déclarent un préjudice supérieur à 100K € (+4 points). Le signe que le risque de sévérité s'accroît, et que la fraude et la cybercriminalité menacent la pérennité des entreprises françaises. Un constat d'autant plus alarmant dans le contexte d'incertitude sanitaire et économique actuel, qui pèse toujours sur les perspectives des entreprises.

La crise Covid-19, catalyseur du risque de fraude et de cybercriminalité ?

Autre symbole du renforcement du risque de fraude pour les entreprises : 64% d'entre elles déclarent avoir constaté une accentuation du phénomène en 2020. Pire encore, et preuve que les entreprises sont conscientes de la menace : alors que le risque de fraude est déjà particulièrement fort, 87% des interrogés craignent une accentuation lors des mois à venir. Une légère progression (+3 points), à mettre en relation avec la crise Covid-19 ?

Si l'on en croit les résultats du Baromètre Euler Hermes – DFCG 2021, le lien existe : près d'une entreprise sur deux a en effet remarqué une recrudescence particulière du nombre d'attaques suite à la généralisation du télétravail. Un cadre qui peut en effet paraître plus propice à la fraude et à la cybercriminalité, surtout dans un contexte qui a poussé les entreprises à une adaptation très rapide et donc potentiellement moins contrôlée. Mais les entreprises ont-elles pris les mesures nécessaires pour renforcer leurs défenses face au risque de fraude en contexte de crise Covid-19 ?

« Les entreprises semblent avoir adapté leurs systèmes de défense en parallèle de l'évolution des conditions de travail : 91% des sondés ont mis à disposition de leurs employés un équipement informatique professionnel et adéquat pour travailler à distance. 66% des entreprises interrogées ont adapté leurs procédures internes pour qu'elles correspondent mieux au cadre de généralisation du télétravail. Enfin, 67% des répondants ont renforcé leurs procédures de sécurité afin de se protéger d'éventuelles nouvelles vulnérabilités. Malgré un contexte économique complexe, les entreprises ont travaillé sur leurs dispositifs de défense et prévention pour limiter leur exposition au risque de fraude », répond Philippe Guillaumie, président du Comité scientifique de la DFCG.

L'usurpation d'identité plébiscitée, mais très complémentaire des outils cyber

L'usurpation d'identité reste la technique plébiscitée par les fraudeurs, comme lors des précédentes éditions. Mais changement notable, la fraude au faux-président devient, cette année, la plus subie par les entreprises (citée par 47% des répondants, +9 points par rapport au précédent Baromètre). Elle est suivie par la fraude au faux fournisseur (46%, -2 points), les autres usurpations d'identité (banques, avocats, commissaires au compte – 38%, +7 points) et la fraude au faux client (25%, +1 point). Parmi les cyberattaques, l'intrusion dans les systèmes informatiques est la plus citée (32%, +3 points), devant les rançongiciels / cyber-extorsion (21%, +6 points) et le vol ou destruction de données (8%, +2 points). Si ces attaques sont citées de manière distinctes par les répondants, il ne faut pas perdre de vue que l'usurpation d'identité et la cyberfraude sont très complémentaires.

« 3 entreprises interrogées sur 4 observent une augmentation du nombre de tentatives de phishing, qui consiste à récolter des données sur un utilisateur pour ensuite usurper son identité en vue de détourner des fonds. Cette tendance est très révélatrice des combinaisons de techniques utilisées par les fraudeurs : le cyber est devenu un outil au service de l'ingénierie sociale, qui permet de développer des scénarios d'usurpation d'identité extrêmement crédibles et donc d'accroître l'efficacité des fraudeurs », abonde Armelle Raillard.

Transparence et communication afin d'éviter le risque de contagion

Le vol de données peut également permettre à un fraudeur d'élargir son périmètre d'intervention par une stratégie de ramification. En effet, en s'introduisant dans le système d'information d'une entreprise, le fraudeur peut subtiliser des informations stratégiques concernant les partenaires, et ainsi les ajouter à sa liste de cibles potentielles. Une hypothèse d'ailleurs confirmée par les conclusions du Baromètre Euler Hermes – DFCG : 57% des répondants déclarent que leurs partenaires commerciaux ont déjà été victimes de fraudes (+10 points par rapport au dernier Baromètre).

« La fraude ne doit pas être un sujet tabou : quand on en est victime, on expose directement ses partenaires commerciaux, il faut donc les avertir au plus vite. La bonne nouvelle, c'est que les entreprises en sont conscientes : 84% des répondants à notre Baromètre affirment avoir informé leurs partenaires après avoir subi une attaque. La communication et la transparence sont essentielles pour limiter le risque de contagion », expose Armelle Raillard.

Des efforts supplémentaires à fournir pour améliorer la protection contre le risque de fraude

Face à l'accentuation du risque de fraude et de cybercriminalité, et alors qu'elles affirment craindre que la tendance continue de se renforcer, les entreprises ont-elles pris les mesures adéquates pour protéger leur activité et leur trésorerie ? Le constat est mitigé.

D'une part, plus de 6 entreprises sur 10 déclarent ne pas avoir alloué un budget spécifique pour lutter contre la fraude et la menace cyber. Inquiétant, mais compréhensible dans le contexte actuel où les structures de coûts des entreprises sont sous pression. Plus alarmant en revanche, seulement 44% des entreprises sondées ont établi une cartographie des risques, contre 60% lors de la précédente édition. Heureusement, parmi celles-ci, 90% ont bien identifié le risque de fraude et 80% le risque cyber sur leur cartographie.

« La cartographie des risques est non seulement un outil d'identification et de pilotage des risques majeurs de l'entreprise en matière de fraude mais aussi un dispositif qui permet de définir les plans

d'actions concrets pour agir et réagir en cas d'attaque. Néanmoins, seules 55% des entreprises interrogées disposent d'un plan d'urgence à activer en cas de fraude, soit -5 points par rapport à la précédente édition de notre Baromètre. Ce pourcentage n'est pas satisfaisant dans la mesure où la capacité de « réaction rapide » est déterminante pour arrêter une tentative de fraude. Il est donc paradoxal de constater que 7 entreprises sur 10 s'estiment satisfaites de leur dispositif de protection. Nous recommandons aux entreprises de ne pas baisser la garde et de fournir un effort supplémentaire afin d'accroître l'efficacité de leurs dispositifs en matière de lutte contre la fraude. », indique Christian Laveau, président du groupe Cyberfraude de la DFCG. Dans le domaine plus spécifique de la cyberfraude, Christian Laveau ajoute que la DFCG va prochainement publier un document de référence sur la cyberfraude et ses enjeux pour les directions financières.

Heureusement, la prise de conscience des entreprises semble se renforcer : 55% des entreprises sondées prévoient d'allouer ou d'augmenter leur budget de lutte contre la fraude l'année prochaine. Parmi les principales mesures qui feront l'objet d'un investissement : la sensibilisation interne (73%), les audits de sécurité des systèmes d'information (69%), les audits pour renforcer les procédures de contrôle interne (47%), les plans de reprise de l'activité (44%) et les solutions d'assurance (32%).

****

Contact médias

MAXIME DEMORY
Euler Hermes France
+33 (0)1 84 11 35 43
maxime.demory@eulerhermes.com

CHARLES BONATI
DFCG
+33 (0)1 40 20 94 50
charlesbonati@dfcg.asso.fr

Réseaux sociaux

Suivez-nous sur Twitter @eulerhermesFR
Suivez-nous sur LinkedIn Euler Hermes France
Suivez-nous sur YouTube Euler Hermes France

Suivez-nous sur Twitter @dfcgasso
Suivez-nous sur LinkedIn DFCG
Suivez-nous sur YouTube DFCG

****

A PROPOS D'EULER HERMES

Euler Hermes est le leader mondial de l'assurance-crédit et un expert reconnu dans les domaines de la caution, du recouvrement, du financement structuré et du risque politique. Notre réseau international de collecte et d'analyse d'informations nous permet de suivre l'évolution de la santé financière des entreprises dans des marchés représentant 92% du PIB mondial. Nous donnons aux entreprises la confiance nécessaire pour développer leurs échanges commerciaux sans s'exposer au risque d'impayés. Notre priorité est de vous éviter de subir des incidents de paiement grâce à notre système de protection prédictive. Mais si l'imprévu se matérialise, et que vous subissez un impayé, nous vous indemnisons. Notre notation de crédit AA et notre appartenance au Groupe Allianz, attestent de notre solidité financière et de notre capacité à vous aider à préserver votre entreprise. Basé à Paris, Euler Hermes est présent dans plus de 50 pays avec 5 800 employés. En 2020, Euler Hermes garantissait 824 milliards d'euros de transactions commerciales dans le monde. Plus d'informations : eulerhermes.com

A PROPOS DE LA DFCG

L'Association nationale des Directeurs Financiers et de Contrôle de Gestion, créée en 1964, constitue la communauté de référence des professionnels des directions financières d'entreprises privées ou des services publics. La DFCG rassemble, dans 15 régions, 3 000 dirigeants financiers d'entreprises de toute taille, représentatives du tissu économique français. La DFCG regroupe 1 800 sociétés (Grands groupes 13%, ETI-PME 70%, TPE 17%). Depuis 2021, l'association est présidée par Emmanuel Millard.
• Lieu de recherche opérationnelle en finance et contrôle de gestion, ses recherches donnent matière à une dizaine de publications annuelles. Ses prises de positions contribuent au débat économique et financier.
• Sphère pédagogique pour développer les compétences de ses membres, le Centre de Formation de la DFCG propose 90 formations allant de la sensibilisation pour dirigeant aux responsabilités nouvelles, à l'expertise plus pointue en financement ou en contrôle de gestion.
• Lieu de partage de bonnes pratiques et espace d'échanges et de business, la DFCG organise plus de 500 manifestations régionales et nationales. Financium, son grand congrès annuel rassemble en décembre plus de 1 000 professionnels.
• Espace de développement professionnel, l'association s'est notamment dotée de groupes transversaux pour accompagner ses adhérents à chaque instant de leur vie professionnelle.
• 23 groupes de travail, dont le groupe Cyberfraude présidé par Christian Laveau.
Plus d'information : www.dfcg.fr

Cautionary note regarding forward-looking statements: The statements contained herein may include prospects, statements of future expectations and other forward-looking statements that are based on management's current views and assumptions and involve known and unknown risks and uncertainties. Actual results, performance or events may differ materially from those expressed or implied in such forward-looking statements. Such deviations may arise due to, without limitation, (i) changes of the general economic conditions and competitive situation, particularly in the Allianz Group's core business and core markets, (ii) performance of financial markets (particularly market volatility, liquidity and credit events), (iii) frequency and severity of insured loss events, including from natural catastrophes, and the development of loss expenses, (iv) mortality and morbidity levels and trends, (v) persistency levels, (vi) particularly in the banking business, the extent of credit defaults, (vii) interest rate levels, (viii) currency exchange rates including the euro/US-dollar exchange rate, (ix) changes in laws and regulations, including tax regulations, (x) the impact of acquisitions, including related integration issues, and reorganization measures, and (xi) general competitive factors, in each case on a local, regional, national and/or global basis. Many of these factors may be more likely to occur, or more pronounced, as a result of terrorist activities and their consequences.