Les essentiels d'Euler Hermes 2018

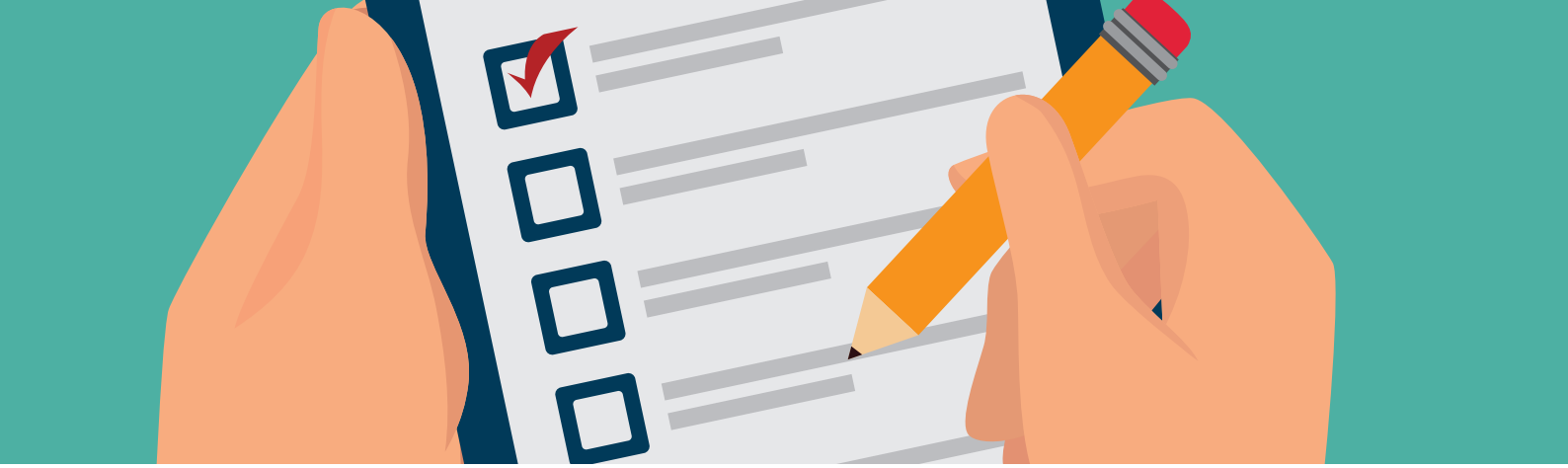
Fraude : 5 actions pour protéger son entreprise

Des outils et bonnes pratiques à mettre en place sans attendre

www.eulerhermes.fr

EULER HERMES
Our knowledge serving your success*

A company of Allianz



Sommaire

Éditorial

La transformation digitale de l'économie repose sur l'interconnexion croissante des équipements et des services à l'intérieur de l'entreprise, mais aussi entre l'entreprise, ses clients, ses fournisseurs et ses partenaires. Si elle favorise la compétitivité et la performance des entreprises, elle constitue également son talon d'Achille. La fraude a toujours existé, mais elle a pris un nouvel essor avec la diffusion des technologies comme le Big Data ou l'Internet des objets (IoT) - élargissant ainsi considérablement le terrain de jeu des escrocs.

Heureusement des mesures de précaution existent face à l'augmentation des risques. Certaines ont une base technologique, pour protéger les réseaux et les logiciels, prévenir les intrusions ou pour donner l'alerte. Mais c'est avant tout sur le facteur humain que les entreprises doivent travailler. Les escrocs ont toujours exploité la crédulité humaine pour réussir leurs manœuvres frauduleuses ; il n'en va pas autrement aujourd'hui.

Euler Hermes peut vous accompagner dans la réalisation d'un diagnostic efficace pour évaluer vos risques de fraude – internes, externes, cyber – quelle que soit la taille et l'activité de votre entreprise. Nous proposons des solutions d'assurance qui vous permettent de limiter les conséquences d'un sinistre lorsqu'il se produit. Ces réponses s'adaptent à la nouvelle donne de l'économie numérique, avec des solutions à la hauteur des nouveaux enjeux. Nous avons réuni dans ce guide les outils et les bonnes pratiques pour protéger votre entreprise contre tous les types de fraudes. Nous espérons qu'il vous sera utile et vous en souhaitons bonne lecture.

Sébastien Hager
Responsable Souscription Assurance Fraude,
Euler Hermes France

Un phénomène lourd de conséquences

Si les données de l'entreprise, qui constituent un actif critique et donc précieux, sont plus que jamais exposées à des risques réels, les fraudes traditionnelles d'origine externe et interne n'en demeurent pas moins des dangers lourds pour toutes les entreprises.

Cyber attaques

Selon la Commission européenne, **80 % des entreprises de l'Union européenne** ont déjà été victimes de piratage informatique. Le rançongiciel (ransomware) reste la cyber attaque plus fréquente, si l'on en croit le 3e baromètre annuel du CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) : 73 % des entreprises déclarent en avoir subi au moins une tentative. Le principe est simple : l'escroc envoie une pièce jointe qui, une fois ouverte, crypte l'ensemble des données ; il réclame alors une rançon en échange de leur restauration.

Un phénomène lourd de conséquences

Les attaques externes

Il existe deux grands types d'attaques externes :

- **L'usurpation d'identité.** L'escroc se fait passer pour le président (59 % des tentatives d'escroquerie, selon l'étude DFCG/Euler Hermes 2017), un fournisseur (56 %), un client (25 %), un banquier, un commissaire au compte, faux avocat (29 %), etc. ;
- **Le phishing ou hameçonnage ;** un pseudo organisme (banque ou administration par exemple) demande une « confirmation » de coordonnées confidentielles pour soutirer des accès et des données.

Toujours la fraude interne

La fraude interne est toujours là, insidieuse et d'autant plus dangereuse qu'elle peut s'exercer sur une longue période avant d'être découverte. Un collaborateur peut agir pour son propre compte avec de fausses notes de frais, des factures falsifiées, etc. Il peut aussi se faire complice d'un escroc extérieur à l'entreprise. Souvent, il s'agit d'un salarié avec de l'ancienneté… et possédant la confiance du management. **Les détournements d'origine interne représenteraient 18 % des fraudes enregistrées** (étude Euler-Hermes- DFCG 2017).

Et maintenant, le risque réglementaire avec la RGPD

Les nouvelles obligations de la RGPD (Règlement Général sur la Protection des Données Personnelles) s'imposent à toutes les données personnelles des citoyens européens. Toute « fuite » de ces données, quelle qu'en ait été l'origine, entraîne un risque d'amende dont le montant est extrêmement élevé : jusqu'à **4% du chiffre d'affaires mondial** en cas d'injonction, 2% sinon.

Pour savoir où vous en êtes dans la préparation de la mise en œuvre du RGPD, faites le test

http://rgpd.medef.com

Un phénomène lourd de conséquences

Des conséquences bien réelles

Le principal risque est évidemment financier, avec des conséquences sur la trésorerie et les résultats des entreprises. En 2014, l'Union européenne chiffrait à 285 milliards d'euros le coût global annuel de la seule cybercriminalité. Pour 2017, l'éditeur de solutions de sécurité informatique McAffee en partenariat avec le Center of Strategic and International Studies annonce une **perte de 600 milliards de dollars** à l'échelle de la planète (485 milliards d'euros).

Selon l'étude Euler-Hermes- DFCG 2017, 10 % des entreprises victimes de fraudes ont subi une perte supérieure à 100,000 euros. Au-delà, c'est l'image de l'entreprise qui est atteinte, avec des conséquences commerciales qui peuvent être dramatiques si les clients perdent confiance dans la capacité de protéger leurs données confidentielles. Enfin, en interne, les fraudes font également des ravages, d'autant plus si l'acte est le fait d'un collaborateur. Elles bouleversent l'organisation, sapent la confiance… et coûtent d'autant plus cher qu'elles ont mis de temps à être découvertes.

Les entreprises en première ligne

Du grand groupe à la PME, tout le monde est concerné. Selon le dernier rapport sur la violation des données de Vérizon, le géant américain des Télécoms, 61 % des victimes de compromission de données sont des entreprises de moins de 1,000 salariés.
L'étude Euler-Hermes- DFCG 2017 démontre que :

- 8 entreprises sur 10 ont subi au moins une tentative de fraude,
- ¼ d'entre elles ont connu plus de 5 tentatives,
- 1 sur 5 a souffert d'une fraude avérée.

L'interconnexion croissante entre clients et fournisseurs élargit le champ des attaques. Un fournisseur peut ainsi servir de porte d'entrée pour atteindre la cible…

5 actions pour protéger son entreprise

N°1 - Mettre en place des procédures solides, acceptées et exécutables par tous

Les fraudeurs cherchent et utilisent les failles dans les organisations et les process. La première mesure de précaution consiste donc à mettre en place des procédures solides et valables pour tout le monde, aussi bien les sédentaires que les travailleurs nomades comme les commerciaux. Encore faut-il que ces procédures ne soient pas contraignantes au point d'inciter à les négliger.

Mais attention : les procédures les plus efficaces ne sont pas synonymes de risque zéro et, surtout, ne doivent pas nuire au bon sens, l'un des plus sûrs moyens de se protéger.

Multiplier les protections

Règle de base en matière de sécurité : le donneur d'ordre et l'exécutant d'un paiement doivent être deux personnes différentes, afin de **séparer les tâches et dupliquer les contrôles.**

Par ailleurs, il se révèle indispensable de se doter de procédures de vérification et de signatures multiples, en particulier pour les paiements internationaux et pendant les congés et les absences - des périodes

qui nécessitent une vigilance accrue. Tout virement ou changement de coordonnées bancaires d'un client ou d'un fournisseur nécessite une double validation. Des plafonds d'engagement peuvent être définis en fonction des degrés de responsabilité.

Contrôler l'identité de ses clients et fournisseurs

Le processus de vérification « KYC » (Know Your Customer) permet de vérifier l'identité d'un client ou d'un prestataire par différents moyens :

- Extrait de KBIS récent,
- Copie de RIB, statuts de la société certifiés conformes,
- Justificatif d'identité du gérant de la société, etc.

Ce n'est toutefois pas suffisant, le processus KYC gagne à s'appuyer sur des vérifications d'authenticité ; il existe aujourd'hui des logiciels de contrôle de cohérence des documents présentés, permettant par exemple de croiser l'information donnée avec d'autres sources, de manière automatique (voir page 17).

S'assurer de l'identité de son interlocuteur apparaît comme la base de la protection. Ce qui n'est pas toujours simple. Par exemple, certains escrocs piratent des adresses mail pour envoyer des malwares cachés dans des pièces jointes, si bien que le destinataire est en confiance puisqu'il reconnaît l'identité de l'auteur du mail. Une confiance que cherchent aussi les fraudeurs dans les réseaux sociaux, en créant de fausses identités, ou en hackant des comptes.

Gérer les exceptions et les contraintes opérationnelles

Il arrive parfois que certaines situations ou contraintes empêchent ou compliquent l'application stricte des procédures de sécurité prévues. C'est notamment le cas des collaborateurs nomades, qui peuvent être amenés à se connecter au Wifi d'un hôtel ou à des réseaux publics mal protégés. À ne pas oublier également, les procédures en cas d'absence d'un responsable clé, pendant les congés, en cas d'événement exceptionnel…
Ces exceptions et ces contraintes opérationnelles doivent être repérées, décrites, et faire l'objet d'un contrôle spécifique.

Auditer pour apprécier les risques

Le COSO (Committee Of Sponsoring Organizations de la Commission Treadway), qui définit les standards de l'audit internet, a récemment introduit dans son référentiel un principe consacré au risque de fraude.
Ce référentiel permet à l'auditeur d'identifier au sein de l'organisation les risques de fraude, en les cartographiant et en les hiérarchisant. Il tient compte de la probabilité qu'il existe des erreurs significatives, des cas de fraude et de non-conformité et d'autres risques importants.

N°2 - Informer et former

89 % des entreprises interrogées par l'étude DFCG/Euler Hermes – contre 63% en 2016 – déclarent avoir mis en place un dispositif de lutte contre la fraude, sous forme de sensibilisation et de formations internes. En effet, les fraudeurs s'appuient souvent sur des comportements humains pour opérer. Ce phénomène s'amplifie notamment depuis le développement des smartphones et autres tablettes qui rendent de plus en plus poreuses les frontières entre la sphère privée et la sphère professionnelle.
L'implication des collaborateurs est d'autant plus importante qu'ils sont encore nombreux à estimer que la question de la fraude est une affaire de spécialiste, notamment la cyber fraude, dont ils ont tendance à faire le domaine réservé des informaticiens.

Informer les nouveaux arrivants

Informer les nouveaux arrivants des règles de base en matière de sécurité anti- fraude s'avère essentiel. Cela vaut pour les salariés, mais également pour les intérimaires, et aussi pour les prestataires extérieurs. Le guide d'accueil ou l'Intranet de l'entreprise peut utilement comporter des informations sur :

- **L'organisation et les procédures mises en place :** qui fait quoi, comment réagir en cas d'incident, à qui s'adresser en cas de soupçons, comment donner l'alerte, etc. ;

- **Les bonnes et les mauvaises pratiques notamment sur Internet,** avec des règles de base, comme ne jamais ouvrir une pièce jointe contenue dans un courriel dont on ne connaît pas l'expéditeur ;

- **Des exemples de fraude, si possible pris dans l'entreprise,** avec les conséquences et les parades mises en œuvre.

Une charte de bonne conduite peut se révéler très utile.

Sensibiliser les collaborateurs

Pour beaucoup, la lutte contre la fraude est une question de bon sens - qu'il convient de cultiver. Mais la force des escrocs réside également dans leur imagination et leur capacité à toujours avoir un coup d'avance sur les dispositifs de sécurité. D'où l'intérêt de **sensibiliser régulièrement** les collaborateurs en les amenant à se poser les bonnes questions et à développer leur esprit critique et leur capacité d'analyse.
Sous différentes formes (mails, affichage, réunions, espace Intranet dédié, etc.), il convient de rappeler un minimum d'éléments :

Enjeux en matière de fraude de l'entité considérée

Informations considérées comme sensibles

Réglementations et obligations légales

Consignes de sécurité sur l'activité quotidienne

Moyens disponibles pour sécuriser l'activité

Signes qui doivent alerter

Règles en cas d'urgence

Par ailleurs, certains publics sont davantage exposés que d'autres. Par exemple, les commerciaux qui voyagent à l'étranger savent-ils que, dans de nombreux pays, les hôtels, les cafés, les lieux publics ou les bureaux de passage n'offrent aucune garantie de confidentialité, ou que certains centres d'affaires et réseaux téléphoniques sont surveillés, y compris dans des États démocratiques ? Une formation à ces risques est plus que recommandée : elle devient tout simplement cruciale.

Tester en grandeur nature

Comment sensibiliser les collaborateurs aux risques de fraudes ? En octobre dernier, le ministère des Finances a réalisé un test grandeur nature en envoyant à ses 145,000 agents un courriel de phishing, avec une pièce jointe. 20 % des agents ont mordu à l'hameçon, alors que les messages provenaient d'expéditeurs dénommés Jean-Baptiste Poquelin ou Emma Bovary - cette dernière les invitant à gagner des places de cinéma. Cette opération a été suivie d'une séance d'explications aux collaborateurs. Elle a également permis de tester les procédures d'urgence du ministère en cas de cyber attaque. Des actions équivalentes sont menées par des entreprises, avec la plupart du temps de grosses surprises sur l'état de conscience de leurs collaborateurs et de leurs cadres…

N°3 - Sécuriser les systèmes

Mettre à jour les applications et les matériels

Outre la correction des bugs, les mises à jour visent à parer les nouvelles attaques. Il est donc indispensable de se doter d'une politique en la matière, avec des procédures précises qui permettent de s'assurer :

De l'inventaire des composants du système

Des sources d'information concernant la publication des mises à jour

Des outils disponibles pour déployer les mises à jour

Du déploiement en lui-même

Attention aux composants obsolètes qui constituent des portes d'entrée idéales pour les attaques !

Protéger les réseaux

Un réseau totalement décloisonné est particulièrement vulnérable.
En effet, le moindre incident peut se propager à tous les équipements, jusqu'aux serveurs critiques. Dès la conception de l'architecture du réseau, il faut donc penser à **distinguer les postes de travail** utilisateurs, ceux des administrateurs, les serveurs métiers, les infrastructures, etc.
Internet étant la porte d'entrée des cyber fraudeurs, il faut sécuriser son accès avec une passerelle comprenant **au minimum un pare-feu**. Il est également important de protéger les accès Wi-Fi et de **séparer les usages** avec notamment un réseau dédié aux visiteurs.

Sauvegarder les données, les logiciels et les systèmes

Certaines PME sont contraintes d'interrompre leur activité suite à une attaque qui leur a fait perdre l'ensemble de leurs données.

Une conséquence terrible quand on sait qu'une simple sauvegarde aurait suffi pour éviter cette mésaventure.
Une procédure spécifique permet de définir les données considérées comme critiques, le nombre de sauvegardes, leur fréquence, leur localisation externe et sécurisée, les autorisations d'accès, etc.
Au moins une fois par an, il est conseillé de réaliser un exercice de restauration des données et de conserver une trace technique des résultats.

Auditer le système d'information

L'audit régulier du système d'information est nécessaire pour évaluer si les mesures prises pour assurer la sécurité sont efficaces, et si cette efficacité se maintient dans le temps. Il permet également de mesurer les écarts entre la théorie et la pratique.
Réalisés en interne ou par une société spécialisée, ces audits peuvent être obligatoires pour des entreprises qui doivent se conformer à des réglementations. Le RGPD (Règlement Général sur la Protection des Données) pourrait d'ailleurs conduire un certain nombre d'entités à s'assurer de l'efficacité de leur système de sécurité.
Tout audit débouche sur des pistes d'amélioration. Mais un audit réussi ne veut pas dire que le risque a disparu…

Préparer un Plan de Reprise d'Activité

Le plan de reprise d'activité (PRA) recense l'ensemble des dispositifs et infrastructures à mettre en place, ainsi que les démarches à entreprendre pour restaurer un système informatique en cas de sinistre : incendie, panne, dégât des eaux, cyber attaque… Il prévoit notamment une bascule du système endommagé vers un autre, la mobilisation des collaborateurs, les délais d'intervention, etc. Ce plan doit être testé régulièrement pour s'assurer qu'il reste toujours efficace malgré les changements intervenus dans l'organisation ou le parc informatique.

Que faire en cas d'urgence ?

Si malgré toutes les procédures et protections mises en place, le système d'information est attaqué, il existe quelques bons réflexes.

1. **Eviter la propagation en déconnectant l'équipement incriminé du réseau,**
2. **… tout en le maintenant sous tension, sans le redémarrer pour conserver les informations utiles à l'analyse de l'incident.**
3. **Prévenir sa hiérarchie et/ou le responsable sécurité des systèmes informatiques, solliciter l'intervention d'un expert.**

Un bon réflexe en cas de cyberattaque :
CYBERMALVEILLANCE.GOUV.FR

La plateforme en ligne du dispositif gouvernemental est là pour vous accompagner :
- établissement d'un diagnostic précis de votre situation ;
- mise en relation avec les spécialistes et organismes compétents proches de chez vous ;
- mise à disposition d'outils et de publications dispensant de nombreux conseils pratiques.

N°4 - Dématérialiser les procédures

Protéger l'intégrité des documents

La fraude documentaire a été largement facilitée par la démocratisation des outils bureautiques – avec comme conséquence la production de pièces crédibles en apparence : bulletins de paie, bons de commande, bons de livraison, RIB, etc. Pour lutter contre cette fraude et sécuriser les données échangées, administrations d'abord, compagnies d'aviation, et aujourd'hui la plupart des grands facturiers ont choisi d'insérer dans le document un code à barres 2D qui comprend les informations clés du document (le type de document, le nom et le prénom de l'émetteur, la civilité, l'adresse, le numéro de facture) et la date d'émission du document ou du code à barres. Toutes ces informations sont verrouillées par une signature électronique qui garantit l'identification de l'organisme émetteur et l'intégrité du document.

Cette solution permet de sécuriser tout type de document, aussi bien papier que numérique, en particulier les justificatifs (factures eau, téléphone, EDF, quittances d'assurance et de loyer, RIB, revenus, …) utilisés par les professionnels dans leurs relations avec les entreprises et les services de l'administration.

Des solutions pour s'assurer de la régularité des pièces transmises

Différents outils existent contre la fraude documentaire. Certains donnent un score de conformité au document, par exemple sur la base de contrôles logarithmiques, d'autres réalisent des contrôles de cohérence par rapport à des bases de données externes. A chacun de comparer et choisir sa solution.

Modéliser les comportements

Le big data et l'analyse prédictive ont ouvert la voie vers une modélisation affinée des comportements anormaux. Ils permettent aussi de réduire considérablement la durée de traitement des opérations de détection et de contrôle, un point clé pour éviter les transgressions « pour raisons de productivité ». L'intelligence artificielle et le machine learning ont vocation à renforcer les technologies existantes.

Le cloud : un univers sécurisé

Pour 83 % des DAF (contre 31 % en 2016), le cloud est devenu incontournable pour dématérialiser les documents, les dossiers de clôture, la gestion de trésorerie, la fiscalité, ou l'ERP, selon une étude de la DFCG et du cabinet PWC portant sur les priorités des directeurs financiers français. Parmi les atouts du cloud selon les DAF interrogés : la réduction des coûts, la fiabilisation des données, la facilité de déploiement des applications, la simplification des mises à jour et la sécurité. Les prestataires peuvent proposer des environnements techniques robustes, sécurisés et certifiés ISO, jusque-là hors de portée financière pour beaucoup d'entreprises.
Encore faut-il s'assurer que le stockage des données se situe en Europe continentale, qui a opté pour une politique de protection des données inverse de celle choisie par les Etats-Unis.

N°5 - Souscrire une assurance fraude

Pourquoi se couvrir ?

L'assurance fraude permet d'indemniser l'entreprise en cas de sinistre : fraude externe, interne ou cyber attaque. L'indemnisation limite les pertes financières directes et certains frais induits : restauration et/ou décontamination des données, frais de prestataire en cas de cyber-extorsion, frais de téléphonie. **Ce qui permet de de préserver sa trésorerie.**

L'assurance fraude, comment ça marche ?

Avant la signature, un simple questionnaire permet de faire le point sur l'organisation et les mesures élémentaires de prévention, les points clés de sécurité informatique et les antécédents. Ce questionnaire permet à l'entreprise de passer en revue les points clés de sa sécurité vis à vis des fraudes.

Certains assureurs, comme Euler Hermes, fournissent un kit de prévention et proposent leur assistance pour :

- Rappeler les bonnes pratiques en matière de procédures internes,
- Sensibiliser les collaborateurs,
- Mettre à jour les consignes de prévention,
- Etre alerté sur les nouvelles menaces au fur et à mesure de leur apparition.

En cas de sinistre, l'assureur doit pouvoir proposer un accompagnement personnalisé et vous indemniser rapidement.

Les solutions Euler Hermes

Pour les petites entreprises : EH Fraud Reflex

La 1ère offre d'assurance 3 en 1 en ligne des petites et moyennes entreprises

Conçu spécialement pour les petites entreprises à partir de 150 K€ de chiffre d'affaires*, EH Fraud Reflex couvre contre les conséquences des fraudes et cyber-fraudes.

*entreprises ayant leur siège en France, de 150,000 à 10 millions d'euros de chiffre d'affaires.

Pour en savoir plus :

ehfraudreflex.fr

Caractéristiques-clés :

- La sécurité accessible à tous : dès 75 €/mois (-10% pour 2 ans)
- Simplicité : Souscription 100% en ligne, pédagogique et sans audit
- Sur-mesure : Couverture, franchise et durée personnalisées et modulables
- Modularité : 3 niveaux de couverture possibles

Pour les moyennes et grandes entreprises : EH Fraud Cover

La garantie contre le risque de fraude et ses conséquences*.

EH Fraud Cover vous couvre contre les pertes consécutives à une fraude commise par un employé ou par un tiers, et aux cyberfraudes, ainsi que certains frais induits :

- Frais de restauration d'image,
- Frais de communication,
- Frais de restauration/ décontamination de données,
- Frais de prestataire consécutifs à une Cyber-extorsion,
- Frais de procédures judiciaires

Caractéristiques-clés :

- Couverture immédiate et sans audit
- Accompagnement personnalisé dès la découverte du sinistre
- Indemnisation dans les 30 jours après accord sur son montant
- Prime adaptée et fixée à la souscription

*dans les conditions du contrat.

Euler Hermes, votre assureur contre la fraude

Euler Hermes est d'abord connu comme le leader mondial de l'assurance-crédit, avec 6,000 collaborateurs, 55,000 clients et 2,6 milliards d'euros de chiffre d'affaires. Mais c'est aussi le **1er assureur fraude en Europe**, qui assure les entreprises allemandes contre la fraude depuis près de **30 ans**.

En France, Euler Hermes protège toutes les entreprises contre la fraude, de la TPE à la multinationale.

750
collaborateurs

Plus de
400 millions
d'euros de chiffre d'affaires

Numéro 1
de l'assurance-crédit en France

Contactez-nous : 01 84 11 50 54

Assurance

Euler Hermes France
Succursale française d'Euler Hermes SA
RCS Nanterre B 799 339 312

Délivrance de garanties et surveillance de la situation financière des entreprises

Euler Hermes Crédit France
Société par actions simplifiée
au capital de 51 200 000 EUR
RCS Nanterre B 388 236 853
Société de financement soumise au CoMoFi

Recouvrement

Euler Hermes Recouvrement France
Société par actions simplifiée
au capital de 800 000 EUR
RCS Nanterre B 388 237 026

Euler Hermes France / Euler Hermes Crédit France / Euler Hermes Recouvrement France
Adresse postale : 1, place des Saisons - 92048 Paris La Défense Cedex - Tél. + 33 1 84 11 50 50 - www.eulerhermes.fr
Euler Hermes SA
Entreprise d'assurance belge agréée sous le code 418
Siège social : avenue des Arts 56 -1000 Bruxelles, Belgique - Immatriculée au RPM Bruxelles sous le n° 0403 248 596

Plus d'informations ?

Contactez-nous au : **01 84 11 50 54**
ou consultez notre site : **www.eulerhermes.fr**