# Connexions

La newsletter
du réseau
Crowe Horwath

# Sécurité informatique, le nouvel enjeu des PME

Crowe Horwath

#11

# Sommaire




Connexions est la revue trimestrielle de **Crowe Horwath France**
Comité de rédaction de ce numéro : Arnaud Devoucoux, Marc Luccioni, Julien Benatar
Conception, création : OneSelf
Crédits photos : 123RF olegdudko/ macrovector


Suivez nos actualités sur

**@CroweHorwath_fr**

**crowehorwathfrance.fr**

# Le chiffre

77% des cyberattaques visent les PME.
31% d'entre elles ne prennent aucune mesure de sécurité proactive.

Rapport annuel sur les cyber menaces de Symantec, avril 2016.

# Edito

## Qui dit digitalisation des processus de l'entreprise, dit aussi nouveaux risques…

Arnaud Devoucoux
Associé Crowe Horwath RSA

Aujourd'hui, dématérialisation des taches administratives, développement de plateformes collaboratives et des réseaux sociaux, explosion des données. Demain, généralisation des usages mobiles, du Cloud et de l'internet des objets, du Smart Data, de l'impression 3D, de la robotique collaborative.
La transformation numérique est en marche et dans les entreprises, il n'est pas un métier qui échappe à cette évolution. Le marketing, la relation client, la communication, les RH, la finance, la production, sont tous concernés.

Mais qui dit digitalisation des processus de l'entreprise, dit aussi nouveaux risques. Les systèmes d'information sont désormais au cœur du fonctionnement des organisations. Or, un système d'information mal paramétré ou mal sécurisé expose l'entreprise à des risques multiples : vols d'informations stratégiques, détournements d'actifs, attaques des serveurs, chiffrement des données… Le visage sombre de la digitalisation est la cybercriminalité, une menace qui ne connaît pas la crise. Les cybercriminels ont toujours une longueur d'avance sur les entreprises, créant et diffusant des virus de plus en plus nombreux, de plus en plus difficiles à déceler, de plus en plus dangereux.

Face à cette menace, les PME sont vulnérables. Elles sous-estiment le risque d'incidents, ne disposent pas toujours des moyens suffisants pour sécuriser leur système d'information, n'anticipent pas assez les conséquences d'un incident classé parmi les trois premiers risques d'entreprise selon le baromètre des risques Allianz pour 2016.
La cybersécurité n'est plus un sujet relevant de la compétence exclusive des informaticiens. Du top management aux collaborateurs, elle doit trouver sa place dans la gouvernance de l'entreprise. Quels sont ces risques ? Comment se protéger ? De quelle façon experts-comptables et commissaires aux comptes peuvent-ils aider leurs clients dans la gestion de ce nouveau risque ? Ce numéro de Connexions propose des réponses.

Bonne lecture !

# Philippe Arraou, Président du CSOEC

## "L'expert-comptable, un tiers de confiance numérique."

## Dans une économie en pleine révolution numérique, les règles du jeu changent et portent le germe de nouvelles opportunités pour les experts-comptables et leurs clients.

**En quoi la profession du chiffre est-elle concernée par les évolutions du numérique ?**
Le numérique généralise la dématérialisation de la donnée. Il convient de capter l'information le plus en amont possible pour la faire circuler, l'enrichir, l'exploiter, la restituer. Les cabinets sont acteurs de cette dématérialisation. Si aujourd'hui les tâches déclaratives sont totalement dématérialisées, il convient de porter les efforts sur le système d'information de l'entreprise. La transformation numérique doit être perçue comme une opportunité magnifique pour les cabinets de faire évoluer leur offre de services, et d'être plus utiles à leurs clients en apportant plus de valeur ajoutée.

**Quelle est l'action de l'Ordre des Experts-Comptables ?**
Le Conseil Supérieur a mis en place une stratégie numérique en lançant un programme d'accompagnement des cabinets : élaboration d'un support de sensibilisation sur la révolution numérique et ses impacts pour la profession, mise en place d'une journée de formation, mise en ligne de modules de e-learning thématiques, et élaboration d'un auto-diagnostic en ligne. Par ailleurs nous avons signé des partenariats avec BPI France pour le financement des investissements liés au numérique et avec le Conseil National du Numérique pour que les cabinets soient acteurs de la transition numérique des TPE. Enfin nous allons lancé un think-tank qui accompagnera l'action de l'Ordre : l'Académie du Numérique.

**Quelle est la fonction de l'expert-comptable dans cette économie numérique ?**
Notre profession a été conçue il y a plus de 70 ans pour apporter de la sécurité à l'économie de notre pays, ce qui est l'objet de nos règles d'encadrement et d'éthique. Aujourd'hui, notre fonction sécuritaire demande à être adaptée à l'économie numérique, du fait de la dématérialisation. Pour cela, nous avons développé des outils : le portail déclaratif "JeDéclare.com", la signature électronique "Signexpert" mais aussi la carte d'identité numérique "Expertpass". D'autres sont en cours d'élaboration. Nous avons besoin d'outils pour être de véritables tiers de confiance numérique. Mais la transition numérique ne se limite pas à de la technologie : c'est un véritable changement de fonction chez nos clients que nous devons engager. La profession doit entreprendre un virage important dans son évolution : elle est confrontée à son Histoire !


Philippe Arraou, Président du CSOEC

### Mini bio

Président du Conseil Supérieur de l'Ordre des Experts-Comptables (CSOEC), Philippe Arraou dirige son propre cabinet. Il mène sa carrière en conjuguant responsabilités professionnelles internationales et institutionnelles, au sein de la Compagnie des Commissaires aux Comptes, du syndicat ECF et de la Fédération Européenne des Conseillers Fiscaux (ETAF) dont il est le Président fondateur. Il est membre du Board de l'IFAC, l'organisation mondiale de la profession. Il est également l'auteur du livre "L'expert-comptable et l'économie numérique », publié en 2016 par le CSOEC, préface d'Emmanuel Macron.

# Anne Souvira, Commissaire Divisionnaire et Chargée de mission Cybercriminalité au cabinet du Préfet de police de Paris

## "Il y a une réelle responsabilité du chef d'entreprise à prendre la mesure de la cybersécurité."

Anne Souvira, Commissaire Divisionnaire et Chargée de mission Cybercriminalité au cabinet du Préfet de police de Paris

**Les cyberattaques sont la bête noire des gouvernements et des entreprises. Qu'est-ce qu'une cyberattaque ? Quelle panoplie d'infractions cela recouvre-t-il ?**
Cela peut prendre la forme d'une atteinte aux systèmes d'information de l'organisation et aux données qu'ils contiennent. Par exemple, l'accès frauduleux dans les réseaux et serveurs de données ou de messageries d'une entreprise, leur altération, leur destruction et les extractions de données, qui entraînent des pertes parfois irréparables.
Ainsi, l'infection par crypto-virus en l'absence de sauvegarde des données : le chiffrement des données rendues illisibles par ce maliciel conduit l'entreprise à payer une rançon pour récupérer, croit-elle, ses données. Mais même lorsqu'elle aura acheté sur le dark net de la crypto-monnaie, tels les bitcoins selon les prescriptions des hackers, qu'elle aura reçu la clef de déchiffrement et aura elle-même assuré le recouvrement des données, elle ne retrouvera pas tout et comprendra, trop tard, que la sauvegarde sur un serveur distinct lui aurait évité ces coûts, voire de mettre la clef sous la porte ! Une attaque peut aussi être un déni de service, à savoir des requêtes massives sur un site de e-commerce ou vitrine, qui l'empêche de rendre le service pour lequel il existe. L'acheteur se reportera sur un concurrent. La page d'accueil du site peut également avoir été défigurée et comporter un contenu inapproprié portant atteinte à la réputation de l'entreprise. Cette défiguration consiste à exploiter une faille très connue d'absence de mise à jour de logiciel d'édition de contenu, ce qui pourrait être facilement corrigé en ayant une véritable politique de sécurité informatique. Les bases de données peuvent donc, grâce à des maliciels, êtres exfiltrées, portant un préjudice financier et réputationnel à l'entreprise. Il convient de noter que l'employeur doit empêcher les infractions de téléchargement illégal (Loi HADOPI) et les infractions commises en interne avec son réseau (pédopornographie, contrefaçons de film musique, minage/fabrication de bitcoins…).

**Les PME sont-elles plus ou moins exposées que les grandes entreprises ?**
Elles sont visées au même titre que les grosses entreprises et sont plus vulnérables car elles ont moins mis de moyens en termes de sécurité, cette dépense n'étant pas vue comme un investissement, ni du point de vue technique ni du point de vue de la formation. La formation des personnels évite d'être une victime involontairement consentante, comme, par exemple, en matière d'ingénierie sociale. Cette technique d'escroc consiste à collecter des informations sur les personnes et leurs entreprises auprès des réseaux sociaux, de collègues imprudents ou bavards et de se faire passer pour un PDG qui, un vendredi soir, vous appelle pour vous demander dans le plus grand secret d'effectuer un virement très important sur un compte à l'étranger pour une opération économique secrète… Cette fraude de faux ordres de virement, très connue sous l'appellation fraude au Président, peut prendre plusieurs formes, tel le subit changement de RIB du loyer à verser à votre bailleur d'entreprise ! Elle fonctionne en dépit des efforts de sensibilisation. Les sommes dérobées sont faramineuses et ont conduit plusieurs entreprises à la ruine. Pareillement, le faux technicien informatique qui téléphone pour une prétendue mise à jour à distance de l'ordinateur et qui demande se connecter sur un site contenant des logiciels de hacking et d'exfiltration de

Vous êtes une entreprise et avez été victime d'intrusions au sein de votre société ? Des démarches sont à effectuer et des conseils à retenir :
prefecturedepolice.interieur.gouv.fr/Cybersecurite/Conseils-aux-entreprises

## Glossaire

**Espiogiciel (spyware)**
Logiciel dont l'objectif est de collecter et de transmettre à des tiers des informations sur l'environnement sur lequel il est installé, sur les usages habituels des utilisateurs du système, à l'insu du propriétaire et de l'utilisateur.

**Hameçonnage (Phishing)**
Vol d'identités ou d'informations confidentielles (codes d'accès, coordonnées bancaires) par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

**Maliciel (Malware)**
Tout programme développé dans le but de nuire au moyen d'un système informatique ou d'un réseau. Les virus ou les vers sont deux types de codes malveillants connus.

Glossaire complet sur : ssi.gouv.fr/administration/glossaire/

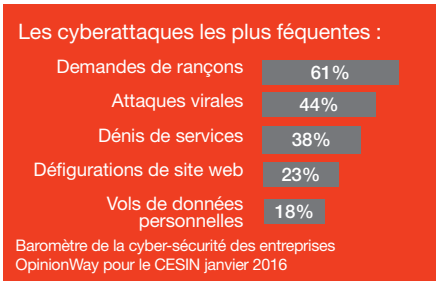
données. Il demandera de cliquer sur des fichiers de mise à jour introduisant ainsi dans l'entreprise des espiogiciels qui déroberont savoir-faire et informations utiles à l'ennemi peut-être concurrent.

**Quelles sont les voies de recours d'une PME victime d'une cyberattaque ?**
Lorsque la menace s'est réalisée, l'entreprise peut déposer plainte et l'enquête recherchera, grâce aux traces informatiques préservées, les auteurs sans doute situés à l'étranger.
Cela pourra être long et aboutir, ou non, car la coopération internationale n'est pas toujours facile et les hackers, forts habiles.

**Face à cette menace croissante, quelles sont les mesures mises en place par les pouvoirs publics ?**
Les pouvoirs publics, par le ministère de l'Intérieur et notamment la préfecture de Police de Paris, travaillent sur la prévention, pour faire connaître la menace, et sur la répression, lorsque les entreprises déposent plainte ou dénoncent des faits. Cela se traduit par exemple par la collaboration avec la Fédération Bancaire Française sur la précision des modes opératoires recensés par des échanges d'informations, des vidéos de sensibilisation[1] , des guides de bonnes pratiques[2] pour éviter aux TPE-PME d'être victimes. Nombre de conférences pour informer les personnels sont données par différents services de police (l'OCRGDF[3] , la mission "cybercriminalité" du préfet de Police, la BFMP[4] et la BEFTI[5] , la Police Judiciaire) dans le cadre du MEDEF, des CCI ou Chambres des Métiers, la CGPME et autres réseaux d'entreprises, tel celui des experts-comptables et par la participation active à divers clubs professionnels (CDSE, CESIN[6], CLUSIF[7]). En zone gendarmerie, la sensibilisation est plus de proximité. La DGSI[8] intervient auprès des entreprises qui ont une activité essentielle pour la Nation.

**Que peut faire la profession du chiffre pour accompagner ses clients sur ce sujet ?**
Proches de leurs clients, les experts-comptables peuvent venir en support de tous les efforts de sensibilisation, transmettre les bonnes pratiques, identifier des risques, y remédier, évaluer les possibilités d'investissement pour sensibiliser les collaborateurs. Ils pourront également les aider à prendre conscience de la nécessité de se mettre en conformité avec le règlement européen du 24 mai 2016 sur le traitement informatique des données à caractère personnel qui sanctionnera très sévèrement, dès mai 2018, les manquements. L'expert-comptable est un relais de choix pour conseiller les entreprises et les accompagner dans ce changement numérique, source de rapidité des économies et de nouvelles activités, à condition toutefois d'en maîtriser les risques par l'application des principes de cybersécurité pour ses réseaux, ses systèmes et leurs données. Celles-ci sont le patrimoine informationnel de l'entreprise. Il est fondamental de le protéger des prédateurs afin d'éviter de conduire l'entreprise à sa perte et ses collaborateurs, au chômage. Il y a une réelle responsabilité du chef d'entreprise à prendre la mesure de la cybersécurité.

[1] http://www.fbf.fr/fr/la-banque-des-entreprises-et-des-professionnels/moyens-de-paiement/prevenir-les-escroqueries-aux-ordres-de-virements-internationaux-dans-les-entreprises-(video-explicative)
[2] http://www.fbf.fr/fr/la-banque-des-particuliers/moyens-de-paiement/securite-des-moyens-de-paiement/ordres-de-virement-des-entreprises---9-reflexes-securite
[3] Office central de répression de la grande délinquance financière
[4] Brigade des fraudes aux moyens de paiement
[5] Brigade d'enquêtes sur les fraudes aux technologies de l'Information
[6] Club des experts de la sécurité de l'information et du numérique
[7] Club de la sécurité de l'information français
[8] Direction générale de la sécurité Intérieure



# Cédric Caléro, Architecte en technologies Microsoft et Expert Collaboratif & Cloud chez Neos-SDI

## "La messagerie email est l'un des principaux vecteurs d'entrée des cyberattaques, donc l'un des points clés à protéger. "

**Quels types d'attaques transitent par la messagerie email ?**
Les attaques les plus fréquemment constatées sont celles impliquant des virus, des liens malveillants et des ransomwares. L'attaque par ransomware est devenue la plus fréquente et occupe la première place du podium, suivie par l'attaque par déni de service (DDoS) et l'attaque virale générale. Les ransomwares restreignent l'accès à votre système informatique par le chiffrement des données et exigent le paiement d'une rançon afin que la restriction soit levée par la livraison de la clé de déchiffrement. Ces logiciels peuvent être introduits dans votre ordinateur par l'ouverture d'une pièce jointe infectée ou par un clic sur un lien hypertexte menant le navigateur sur un site web infecté.
Une fois l'ordinateur contaminé, il tente souvent d'atteindre les autres postes de l'entreprise, par l'envoi de mails à votre insu sur le réseau local ou les serveurs de fichiers.

**Comment reconnaître ces attaques ?**
Il n'est pas toujours facile de reconnaître un email suspect. Il peut provenir d'un expéditeur inconnu ou d'un expéditeur connu mais falsifié et déjà infecté.
Le contenu de l'email varie, le plus connu étant la fausse facture en fichier zip (compressé) ou en fichier docx (Word). Plus de 290 types différents de ransomwares sont connus à ce jour. Certains peuvent être localisés (en français) et ciblés (pour votre entreprise, pour certains collaborateurs) par les escrocs qui les diffusent. Il faut parfois du temps pour se rendre compte que l'ordinateur est infecté. Il commence par ralentir, certains documents ne s'ouvrent plus, d'autres deviennent illisibles. Le réflexe est alors d'éteindre l'ordinateur et de le rallumer, mais l'utilisateur apprend alors qu'il est infecté, et c'est déjà trop tard pour lui. Certains détails doivent mettre la puce à l'oreille : recevoir un cahier des charges en urgence d'un client dont on sait qu'il est en vacances ou un email avec une facture (fausse) destinée au service comptabilité qu'il faut transférer…
Certains malwares sont également trop récents pour être reconnus par les bases de signature d'un antivirus classique ou exploitent une faille encore non corrigée du système d'exploitation, du logiciel de messagerie ou du navigateur web. Cette première vague d'infection peut survenir de façon épidémique : c'est le zero-day. Une fois la menace identifiée, les bases antivirales et les systèmes et logiciels impactés sont mis à jour par les éditeurs, mais charge à votre service informatique de déployer ces mises à jour de sécurité rapidement sur l'ensemble de votre parc informatique pour que le risque de cliquer sur la pièce jointe infectée disparaisse.

**Comment protéger son entreprise ?**
Un service de mise à jour des systèmes d'exploitation et des applications est indispensable pour diffuser rapidement et efficacement les correctifs de sécurité, destinés à ralentir ou empêcher la diffusion des menaces. Une sauvegarde de toutes les données des serveurs de fichiers, des postes de travail et des boîtes mail, hors de portée de votre réseau, s'impose également pour annuler le risque de pertes de données. D'un point de vue technique, de nombreuses solutions de sécurité existent, que les entreprises ont tendance à empiler. Concernant les flux de messagerie, un administrateur IT peut aujourd'hui avoir à jongler avec de multiples dispositifs :

- un antivirus mail,
- un antivirus client,
- un anti-spam,
- un pare-feu,
- un proxy redirecteur d'URL,
- une authentification centralisée SSO,
- une authentification multi-facteurs,
- un chiffrement des données sensibles en pièce jointe,
- une vérification de l'expéditeur réel des emails pour prévenir l'usurpation d'identité,
- une gestion de flotte via Mobile Device Management (MDM) permettant de gérer tous les terminaux (PC, laptops et smartphones) accédant aux données d'entreprise …

Le challenge consiste à faire cohabiter tous ces outils de manière intelligente et efficace, tout en faisant le grand écart entre l'infrastructure physique classique et l'usage croissant du cloud. Il faut également rationaliser le coût de ces solutions hétérogènes, qui doivent être comprises et entretenues par le service informatique, régulièrement mises à jour et monitorées, et rester suffisamment flexibles pour accompagner des entreprises dans leurs nouveaux usages.

**Comment optimiser les solutions de défense ?**

L'enjeu principal est de répondre aux nouveaux défis du cloud et des infrastructures hybrides, deux types d'architecture que nous rencontrons de plus en plus souvent chez nos clients, y compris en messagerie avec les produits Microsoft Office 365 et Exchange Online. La réponse à ces menaces passe par la protection des identités d'utilisateur, des applications, des appareils et des données, pour des échanges qui couvrent tous les employés, mais aussi les échanges avec les partenaires et les clients.
Les solutions de sécurité de Microsoft proposent une offre complète, intégrant de nombreuses solutions de sécurité complémentaires qui fonctionnent réellement ensemble et s'intègrent nativement avec les produits professionnels habituels de l'utilisateur et des administrateurs : Windows 10, Office 2016, Exchange, Active Directory …Ces offres commerciales sont disponibles via un mécanisme d'abonnement mensuel par utilisateur, choisi individuellement ou souscrit en plans complets.
Leur tarif s'ajuste donc toujours au plus juste selon vos besoins, en intégrant automatiquement toutes les mises à jour des produits Microsoft.
Une entreprise qui s'ouvre au cloud peut ainsi se protéger contre les nouvelles menaces de cyber-sécurité avec la suite EM+S (Enterprise Mobility + Security) et les antivirus ATP (Advanced Threat Protection) pour Office 365 et pour Windows 10, mais aussi mettre en oeuvre une sauvegarde hors-site efficace avec Azure Backup, ou encore élaborer un Plan de Reprise d'Activité (PRA) avec Azure Site Recovery.

## En chiffre

**80%** des entreprises ont constaté au moins une cyberattaque sur leur système d'information durant l'année 2016. Sur cette période, le nombre d'attaques détectées a fortement augmenté pour près de la moitié d'entre elles.

Baromètre de la Cyber-sécurité, 2e édition en date du 24/01/2017, publié par le Club des Experts de la Sécurité de l'Information et du Numérique (CESIN).

Cédric Caléro, Architecte en technologies Microsoft et Expert Collaboratif & Cloud chez Neos-SDI

## À propos de Neos-SDI

Neos-SDI est une société spécialisée dans le conseil et l'intégration de solutions dédiées aux usages et aux technologies Microsoft dont il est partenaire. Neos-SDI intervient sur des sujets tels que le Cloud, l'Infrastructure, le Développement, le Collaboratif, la CRM et la Business Intelligence. Neos-SDI accompagne ses clients de la phase conseil jusqu'au maintien des solutions, via son Centre de Services de Dijon. Fort de 190 consultants et d'une présence sur 4 sites (Paris, Lyon, Dijon, Toulouse), Neos-SDI, acteur majeur de la transformation digitale des ETI et Grands Comptes, aide ses clients dans la mise en place de systèmes d'information fiables et de messageries sécurisées via les solutions Office 365 et Azure.

# Corinne Thiérache, Avocat au barreau de Paris, Associée de la société d'avocats Alerion

## Êtes-vous bien armés contre les cyberattaques ? Des solutions organisationnelles et juridiques permettent de se protéger des cyberattaques ou d'en réduire l'impact.

La question n'est plus de savoir "si" mais quand vous allez être attaqués. Toutes les entreprises, y compris les TPE-PME, sont concernées par des cyberattaques toujours plus sophistiquées. Il n'existe "pas de sécurité absolue mais une sécurité au juste niveau, c'est-à-dire adaptée au risque" (Guillaume Poupard, Directeur de l'ANSSI[1] ). Le meilleur moyen de gérer ces risques est d'adopter une approche cyber-résiliente, à la fois stratégique, proactive, pragmatique et, surtout, anticipative.

> La cybersécurité n'est pas un coût, c'est un investissement.

**Être proactif dans la prévention du risque**

La cybersécurité n'est pas un coût, c'est un investissement. Elle doit être envisagée globalement, à tous les niveaux de l'entreprise, dans la gestion des risques et la gouvernance et conduire à une nouvelle philosophie de "compliance" et de responsabilité ("accountability"), à l'instar des obligations issues du nouveau Règlement général sur la protection des données, applicable à compter du 25 mai 2018. La cybersécurité passe aussi par une sensibilisation des salariés à son importance pour l'entreprise, ses clients et ses partenaires. Ainsi, en complément de formations régulières, une charte informatique réactualisée sera utile pour définir les modalités et les limites d'utilisation des outils informatiques. La surveillance du réseau intranet, dans le respect du droit du travail, permettra de détecter d'éventuels comportements ou fichiers suspects. L'entreprise doit également disposer d'un service informatique proactif et d'un correspondant Informatique et Libertés (CIL), tous deux garants d'une meilleure sécurité juridique et informatique (ou d'un Délégué à la Protection des Données à compter du 25 mai 2018).

Corinne Thiérache, Avocat au barreau de Paris, Associée responsable du département Propriété Intellectuelle / Technologies de l'information et de la communication de la société d'avocats Alerion

**Sécuriser les contrats avec ses prestataires informatiques externes**

Un audit des contrats conclus avec les prestataires informatiques est impératif. L'intégrité, la confidentialité et la disponibilité des systèmes informatiques et des données doivent être respectées. La vigilance est de mise dans la rédaction de clauses de sécurité, de garanties et de responsabilité.

**Éviter d'être victime de ses propres négligences**

En présence d'importants préjudices matériels, immatériels et réputationnels générés par des cyberattaques, les tribunaux civils et pénaux pourraient être tentés de revoir à la baisse l'indemnisation si les dommages résultent d'une négligence de l'entreprise. Par ailleurs, des sanctions pécuniaires, jusqu'à 3M€, peuvent être prononcées par la CNIL en cas de manquement par les entreprises à la loi Informatique et Libertés. Pour s'assurer de la meilleure protection de ses systèmes informatiques et de ses données face aux cyberattaques, des revues technico-juridiques s'imposent ![1]

[1]Agence nationale de la sécurité des systèmes d'information

51 %
Hausse du nombre de cyber-attaques recensées en France en 2015
Ifop janvier 2016

A partir du 25 mai 2018, le règlement général sur la protection des données sera directement applicable à tous les acteurs de l'Union européenne. Les nouvelles règles consistent à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises tout en réduisant leurs charges déclaratives et à renforcer le rôle des autorités de protection des données.

cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

# Que faire si vous êtes victime d'une cyber-attaque ?

## Une attaque informatique paralyse souvent les entreprises qui en sont victimes. L'idéal est donc de s'y préparer pour avoir les bons réflexes le moment venu.

Marc Luccioni
Associé Crowe Horwath Avvens,
Responsable de la Commission informatique de Crowe Horwath France

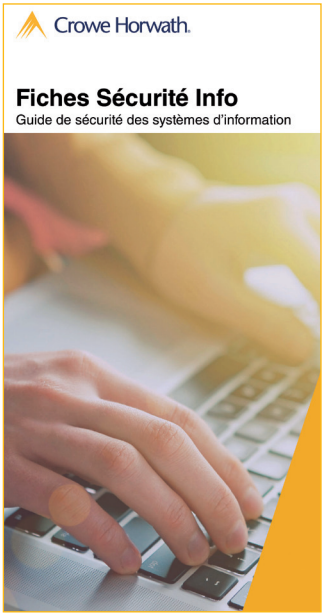
**Les 10 étapes de la procédure à suivre :**

1. Déconnectez-vous d'internet.
2. Faites un balayage de votre ordinateur au moyen de votre logiciel antivirus pour vérifier s'il est infecté et éliminez le virus.
3. Procédez à une restauration complète de votre ordinateur si besoin.
4. Faites appel à un expert si vous croyez que le fonctionnement de votre ordinateur est toujours compromis.
5. Modifiez tous vos mots de passe.
6. Procédez ensuite au dépôt de plainte au commissariat ou à la gendarmerie.
7. Signalez votre problème sur la plateforme en ligne PHAROS ou la plateforme téléphonique Info Escroqueries (0811 02 02 17).
8. Conservez des images de ce que vous voyez en utilisant la fonction "Imprimer écran". Ces captures d'écran aideront éventuellement l'enquête.
9. Listez tous les préjudices subis.
10. Munissez-vous de tous les éléments qui vous semblent pertinents : traces informatiques qui vous font penser à une attaque, fichier encrypté suite au virus, etc.

**Votre expert-comptable peut vous aider à vous assurer de la bonne intégrité de votre système d'information.**

### Quelques bonnes pratiques pour se protéger :

- Utiliser un mot de passe constitué d'au minimum 12 caractères, contenant des minuscules, majuscules, chiffres et caractères spéciaux et ne pas utiliser le même mot de passe pour des accès différents.
- Un logiciel antivirus régulièrement mis à jour protège votre ordinateur contre les virus et les logiciels indésirables.
- Une barrière de protection dite "firewall" permet de filtrer les données échangées entre votre ordinateur et le réseau. Elle peut être réglée de manière à bloquer ou autoriser certaines connexions et aussi empêcher les piratages (intrusions) dans votre ordinateur personnel ou sur un réseau informatique.
- Vous pouvez configurer votre ordinateur pour que le système d'exploitation procède automatiquement et régulièrement à une mise à jour régulière de tous vos logiciels avec les derniers correctifs de sécurité.
- Prudence en ce qui concerne vos courriels, particulièrement lorsque vous ne connaissez pas l'expéditeur. Un simple clic sur une image ou un lien suffit pour installer à votre insu un logiciel ou code malveillant (cheval de Troie) sur votre ordinateur. La pièce jointe piégée peut être : une page html, une image JPG, un GIF, un document Word ou Open office, un PDF, etc. Donc, ne jamais ouvrir une pièce jointe ou suivre un lien dont l'expéditeur est soit inconnu, soit d'une confiance relative.



# Protéger ses données : l'apport du contrôle interne.

## La mise en place d'un contrôle interne contribue à réduire le risque d'attaques externes et internes des données de l'entreprise.

Sarah Guréreau
Associée Crowe Horwath
Dauge & Associés

Si l'intégrité des données d'une entreprise peut être mise à mal par une attaque externe (intrusion sur le réseau d'une entreprise par un pirate informatique), elle peut également l'être par une attaque interne commise par un collaborateur. Un système d'information mal paramétré expose l'entreprise à un risque de vol de fichiers clients/prospects ou d'informations stratégiques confidentielles (données comptables, business modèle, futures campagnes etc.) mais aussi à un risque de fraude, notamment à un risque de détournement d'actifs. Fraude la plus fréquemment rencontrée, elle consiste à dissimuler, voler ou détourner des biens appartenant à l'entreprise (non-enregistrement d'opérations dans les systèmes d'information, enregistrement d'opérations fictives, création de faux…).

**Réduire le risque de fraude lié aux nouvelles technologies**

Mieux vaut être actif pour se protéger de ce type de risque. Les entreprises doivent se doter de méthodes de prévention et de détection des fraudes. La première étape consiste à évaluer les risques de fraude et identifier ses vulnérabilités. L'entreprise peut établir une cartographie afin d'identifier des zones de vigilance en face desquelles proposer des procédures adaptées : Quels sont les risques ? Des contrôles existent-ils ? Comment organiser la vigilance ?...

La deuxième étape consiste à mettre en œuvre un dispositif de contrôle interne afin de mieux maîtriser les opérations identifiées à risques. Des contrôles permanents permettent d'obtenir l'assurance raisonnable que les procédures établies fonctionnent correctement et se prémunir contre le préjudice subi.

**La règle des 4S, une approche simple et efficace**

En termes de contrôle interne, certains principes simples conduisent à limiter les risques : séparer les fonctions clés, sensibiliser les collaborateurs aux risques, sécuriser et superviser certaines procédures.

- **Séparation des fonctions :** une personne qui a des fonctions de saisie/modification au sein de l'entreprise doit être différente de celle qui valide les opérations et/ou celle qui le réalise. Cette mesure essentielle facilite la détection des erreurs et rend la fraude intentionnelle difficile à réaliser car elle nécessite une collusion entre deux personnes ou plus.
- **Sensibilisation :** l'efficacité des mesures de prévention repose avant tout sur le degré de sensibilisation des dirigeants et des salariés. Être informé et se préparer est une bonne manière d'anticiper le problème.
- **Sécurité :** construire une relation avec sa banque contribue à sécuriser les flux financiers et lutter contre des fausses demandes de virement. Cela peut passer par la mise en place d'un système de double signature, d'une alerte sur un montant, d'une informatisation des process.
- **Supervision :** le contrôle continu des opérations de l'entreprise est nécessaire, surtout s'il n'est pas possible de séparer les fonctions. Le commissaire aux comptes a, à cet égard, un rôle important. Il analyse les procédures internes, aide à mettre en place des indicateurs clés et accompagne ses clients dans la mise en œuvre des systèmes anti-fraude.

**La vigilance doit être accrue en matière de contrôle interne. Les entreprises doivent se doter de méthodes de prévention et de détection des fraudes. Le commissaire aux comptes a un rôle d'alerte sur ces risques.**

# Comment tester la sécurité de vos systèmes d'information ?

## Focus sur le diagnostic sécurité et l'Ethical hacking.

Christian Gabenesch
Ingénieur spécialiste des systèmes d'information et de la sécurité numérique, Crowe Horwath Fideliance

Il est possible d'évaluer la sécurité d'un système d'information, de l'infrastructure informatique, des réseaux ou des serveurs en les soumettant à des diagnostics. Objectifs : déceler puis combler les failles de sécurité.

**Le test de restauration des données**

Le "B.A.B.A" du diagnostic de sécurité est le test de restauration des données. Que se passerait-il si toutes les données stockées dans les serveurs étaient perdues après un incendie, un vol, le chiffrement et la prise en otage des données par un virus crypto-locker ? La seule issue : restaurer les données à partir de la dernière sauvegarde. Encore faut-il que celle-ci soit utilisable ! Un test de restauration des données doit obligatoirement être réalisé sur une base régulière et faire partie des procédures de sécurité standard dans toutes les organisations.

**L'Ethical hacking**

Autre diagnostic de sécurité : le test de pénétration, appelé aussi Ethical hacking. Le hacking, soit le piratage informatique, est une activité interdite et lourdement sanctionnée, l'article 323-1 du code pénal le punissant de deux ans d'emprisonnement et de 60 000 € d'amende.
C'est pourquoi l'Ethical hacking doit être réalisé par des auditeurs spécialisés dans le cadre d'une mission clairement définie par contrat ou lettre de mission.
Comment procède t-on ? Le test de pénétration se déroule selon le même scénario qu'un piratage. La première phase est la découverte de l'organisation visée et de son infrastructure informatique. Les moteurs de recherche Internet et les réseaux sociaux permettent de découvrir une quantité importante d'informations : les noms des dirigeants et des salariés, le nom des logiciels utilisés et des prestataires…
Des outils automatiques, appelés "scanners de vulnérabilités" (par exemple NESSUS ou NMAP) parcourent le réseau, analysent les connexions Internet et les accès aux bases de données. La quantité d'informations recueillies lors de cette phase de découverte stupéfie généralement les dirigeants des organisations auditées. La seconde phase est l'exploitation des vulnérabilités découvertes. Parmi les vulnérabilités les plus courantes :

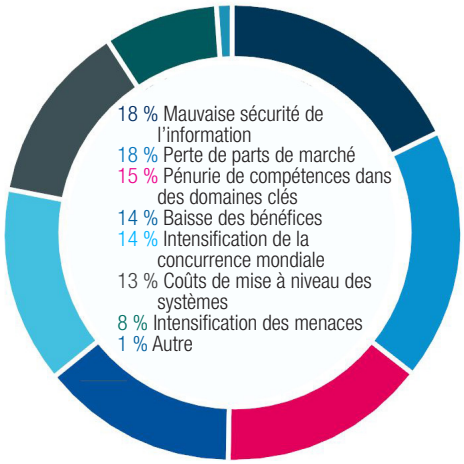
- les connexions wifi, même protégées avec des clés WPA ou WPA2, "crackables" avec des outils spécialisés facilement disponibles sur Internet,
- des équipements réseau, imprimantes multifonctions, caméras, routeurs, switch, trop souvent installés avec des identifiants et des mots de passe par défaut, identifiables en quelques secondes,
- la vulnérabilité "injection SQL" permettant de se connecter sans mot de passe valide, fréquente car trop de développeurs et de concepteurs web ne sont pas formés à la sécurité.

Une phase ultérieure fait appel à l'ingénierie sociale, c'est-à-dire la manipulation de l'utilisateur, qui est un humain, donc une faille potentielle du système d'information s'il est insuffisamment formé aux règles de sécurité. Plus de la moitié des utilisateurs, persuadés d'obéir à des demandes légitimes, acceptent de livrer des informations confidentielles ou d'installer des logiciels potentiellement dangereux...

### En chiffres

**Pour 18 % des personnes interrogées, une mauvaise sécurité de l'information reste le risque n° 1 pour leur entreprise, à égalité avec la perte de parts de marché au profit d'un concurrent. En d'autres termes, une protection inadaptée des informations de l'entreprise est désormais perçue comme un danger plus grand que la concurrence mondiale et la baisse des bénéfices.**

Rapport Risk Value 2016 NTT Communications.



# Le FEC : quels sont les points d'attention ?

## 3 ans après la mise en place du fichier des écritures comptables (FEC), l'administration fiscale a précisé ses exigences, mettant fin à une période de tolérance.

Thierry Grattery,
Crowe Horwath RSA

Lorsque la comptabilité est tenue au moyen de systèmes informatisés, le contribuable doit présenter ses documents comptables en remettant à l'administration une copie des fichiers des écritures comptables sous forme dématérialisée, dès le début des opérations de contrôle (LPF art. L 47 A-I). Sont concernées, toutes les entreprises, tenant une comptabilité informatisée, soumises à l'IS, BIC, BNC ou BA selon un régime réel, y compris les établissements stables de sociétés étrangères, redevables de l'IS en France. Les associations qui exercent une activité lucrative soumise à l'IS sont aussi tenues de fournir un FEC.

Quels sont les points sur lesquels il convient d'être vigilant ?

- Les écritures de report à nouveau doivent être incluses dans le FEC (Fichier des Écritures Comptables) et non plus remises dans un fichier à part.
- Les libellés d'écritures doivent être en français.
- Le plan de compte utilisé est le PCG ou un plan comptable sectoriel. Aucun transcodage ligne à ligne depuis une comptabilité étrangère n'est de fait possible.
- La date de validation des écritures confère un caractère définitif aux écritures comptables. Les écritures fournies dans le FEC doivent être intangibles et irréversibles. L'administration s'assure qu'elles n'ont pas été modifiées. Une comptabilité établie à l'aide d'un logiciel permettant de modifier a posteriori les écritures initiales malgré la validation, n'a aucun caractère probant (CAA Marseille 13/04/2012, n°09MA01619).
- Les écritures justifiant une déclaration fiscale doivent avoir été validées. Ainsi, les écritures mensuelles d'achat et de ventes qui auraient servi de base de calcul de la TVA déductible et collectée doivent être validées avant l'envoi de la CA3. Il en est de même pour l'envoi de la liasse fiscale.
- La sanction applicable reste une amende de 5 000 € par exercice non conforme (y compris l'exercice en cours) ou 10% des rectifications si ce montant est supérieur à 5 000 €. L'opposition à la transmission du FEC justifie dorénavant une évaluation d'office des bases fiscales dans le cadre du contrôle fiscal (LPF, art.74).

### En chiffres

**8 % de rejet**
Depuis 2014, sur 1030 experts-comptables dont les clients ont fait l'objet de contrôles fiscaux, 83 ont rencontré des rejets de FEC.

**24 %** des contrôles ont fait l'objet d'observations orales concernant le FEC.

### Les nouveautés de la Loi de Finance rectificative 2016

Deux nouvelles procédures de contrôle fiscal sont proposées à partir de la comptabilité dématérialisée :

- Un contrôle fiscal ciblé des entreprises, depuis les locaux de la DGFIP.
- Un contrôle spécifique des remboursements de crédits de TVA (vecteur important de fraude).