Expert-Comptable, Commissaire aux prévenir la cybercriminalité

STÉPHANE **BELLANGER** → EXPERT-COMPTABLE, COMMISSAIRE AUX COMPTES - CABINET CBM
MEMBRE DE LA COMMISSION INNOVATION ET PRODUCTIVITÉ

LA CYBERCRIMINALITÉ FAIT DÉSORMAIS PARTIE DES RISQUES MAJEURS AUXQUELS SONT EXPOSÉS TOUTES LES ENTREPRISES, QUELLE QUE SOIT LEUR TAILLE. CETTE NOUVELLE DONNE DOIT ÊTRE PRISE EN COMPTE DANS LA DIMENSION CONSEIL ET VEILLE JURIDIQUE DES CAC.

Dans le cadre de l'exercice professionnel (NEP 315), les missions du CAC comprennent :

- la prise de connaissance du système d'information,
- l'évaluation du contrôle interne du système d'information,
- la revue de la conformité réglementaire du système d'information,
- l'audit par les données afin de fiabiliser l'audit, gagner en image de marque et améliorer la productivité,
- le support méthodologique et la formation informatique pour vos collaborateurs auditeurs financiers,
- la mise en place d'outils de travail pour prendre connaissance du système d'information de l'entreprise.

NOTRE DÉMARCHE CONSISTE PRINCIPALEMENT À :

- Prendre connaissance des contrôles généraux informatiques mis en place par la société. Nous orientons plus particulièrement nos travaux sur les thèmes suivants :

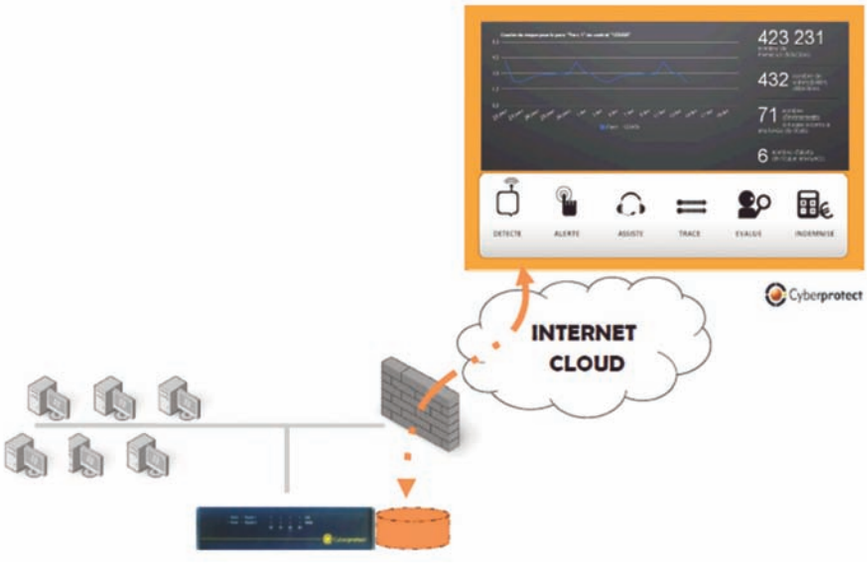
- Stratégie et planification,
- Sécurité informatique,
- Exploitation du système d'information,
- Gestion des sauvegardes et maintien permanent des activités.

- Vérifier que les dispositions essentielles en matière de sécurité et de contrôle ont été mises en œuvre autour de la fonction informatique afin de garantir la fiabilité, l'intégrité des traitements et la validité des informations.

- Un complément d'intervention peut être envisagé afin de réaliser des tests permettant de valider notre compréhension du contrôle interne, de finaliser notre analyse des faiblesses éventuelles et de proposer des voies d'amélioration.

Cette intervention vise à acquérir une meilleure compréhension des procédures et des systèmes concourant à la production de l'information comptable et à confirmer que les dispositions essentielles ont été prises en matière de contrôle interne pour assurer une fiabilité raisonnable des informations traitées.

Les travaux reposent principalement sur les informations collectées au travers d'entretiens avec des personnes de la société, sur un premier niveau de revue des documentations mises à notre disposition. Compte tenu de la portée de ces travaux, ceux-ci ne mettent pas en évidence l'en-



x comptes :

semble des faiblesses existantes et des améliorations potentielles des procédures et des systèmes, qu'une série de tests et qu'une étude plus approfondie pourraient éventuellement révéler, ni toutes les améliorations qui pourraient être apportées.

Or, incidemment, plusieurs rapports récents ont démontré que les menaces de la cybercriminalité ne sont plus dirigées exclusivement vers les grands groupes ou les entreprises les plus importantes. **D'après un rapport Information Security Breaches Survey PWC 2012, 93 % des grandes entreprises et 76 % des PME ont été victimes d'une cyber attaque en 2011 avec un impact financier moyen compris entre 15 000 et 30 000 € pour les PME et entre 110 et 250 000 € pour les grandes entreprises.**

Au cours des derniers mois, **des failles de sécurité dans les sites internet de 34 % des PME européennes** ont causé des dommages conséquents (suppression de fichiers, ajout de données erronées, récupération des coordonnées bancaires des clients...).

L'Union Européenne (UE) a réalisé des progrès décisifs en ce qui concerne la protection contre la cybercriminalité, notamment en créant, le 11 janvier 2013, le Centre européen de lutte contre la cybercriminalité, qui fait partie d'Europol et sert de point focal dans la lutte contre ce fléau au sein de l'UE. Au niveau national, le groupe de travail interministériel annoncé par le ministère de l'Intérieur devrait permettre d'adapter le dispositif législatif français en matière de cybercriminalité. En particulier, concernant les entreprises, le rapport du Sénateur Bockel établit 10 priorités dont **l'obligation pour les entreprises et les opérateurs d'importance vitale d'établir une déclaration d'incident à l'ANSSI en cas d'attaque importante.**

FACE À CE NOUVEAU RISQUE, FORCE EST DE CONSTATER QUE :

- Les entreprises ne sont pas organisées pour prévenir d'un risque et faire face aux nouvelles obligations réglementaires en préparation,

- Celles-ci ne sont pas plus préparées à assumer vis-à-vis des tiers, la responsabilité des dommages que peuvent occasionner la défaillance de leur système informatique,

- Les compagnies d'assurance n'acceptent pas de couvrir les conséquences financières liées à une défaillance causée par les brèches de sécurité.

Il s'agit alors de s'appuyer sur les conseils et services de prestataires proposant une **approche intégrée de la gestion des risques et de la continuité d'affaires, indépendante des éditeurs** de solution de sécurité informatique :

- Réalisation d'audits techniques (test d'intrusion) et d'audit de conformité (ISO 27000),

- Définition et mise en place de politiques de sécurité, de PCA (Plan de Continuité d'Activité), de PRA (Plan de Reprise d'Activité) en cas d'incident,

- Service managé de surveillance et gestion des cyberrisques (traçabilité, apport de preuve, assurance).

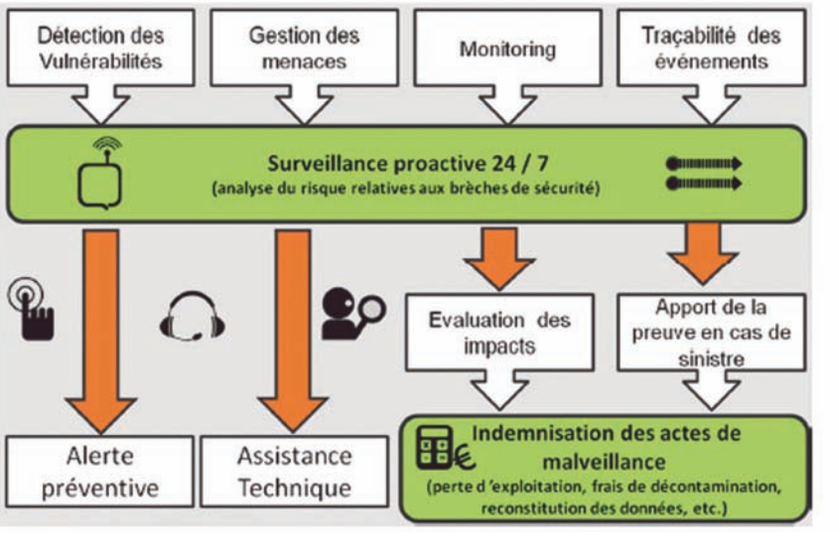
A titre illustratif, voici le service Cyberprotect soutenu par le Secrétariat Général de la Défense et de la Sécurité Nationale (SGDSN) et l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et délivré par la société BC3A (voir illustrations).

Par ailleurs, plus généralement, les professionnels du chiffre que sont les experts-comptables et les commissaires aux comptes doivent bien négocier le virage numérique porté par les grandes tendances telles que l'obligation de dématérialisation pour toutes les entreprises en 2015, la transition vers le Cloud Computing, le coffre-fort électronique et la signature

(SUITE PAGE 30)

Obligation pour les entreprises et les opérateurs d'importance vitale d'établir une déclaration d'incident à l'ANSSI en cas d'attaque importante

Cyberprotect



Expert-Comptable, Commissaire aux comptes : prévenir la cybercriminalité

(Suite de la page 29)
électronique, l'ouverture de la profession vers les réseaux sociaux. Ce virage doit s'opérer dans le cadre de contraintes règlementaires et légales de la profession avec, en particulier :

- Exigences réglementaires en matière de preuve selon l'article 410-4 du PCG (signature électronique en cas de dématérialisation, pérennité des documents 6 ans dont 3 ans sur support informatique), exigences en matière de conservation et de reconnaissance de données (article 420-3 du PCG) impliquant la garantie de l'intégrité des données, pour ce qui concerne les experts-comptables,

- Eventuelles exigences légales (LSF/SOX) pour les clients des commissaires aux comptes.

Il s'agit donc pour le professionnel d'être accompagné dans le respect de ces exigences, à la fois pour les besoins propres des experts-comptables et commissaires aux comptes et pour les besoins de leurs clients.

- **Pour ce qui concerne le volet réglementaire**, un audit de sécurité informatique permet de vérifier si les moyens ont été mis en place pour garantir la confidentialité, l'intégrité et la disponibilité des données. De la même façon, l'existence d'un plan de continuité d'affaires ou d'un plan de reprise d'activité ne suffit pas. Encore faut-il que ceux-ci soient opératoires et que l'entreprise ait la capacité de les mettre en œuvre, c'est l'objet de l'audit des plans de continuité et de reprise.

- **En matière de conformité légale**, l'existence d'un audit de sécurité informatique permet de conforter la fiabilité et l'intégrité des données financières utilisées dans l'établissement du rapport visé par le commissaire aux comptes. Cet audit peut être prescrit fortement conseillé, voire exigé par le CAC sur certains risques présents dans la cartographie des risques que lui fournit l'entreprise. En cas d'externalisation des moyens informatiques, le rapport d'audit de sécurité viendra compléter le rapport de l'audit ISAE 3402 que ne manquera pas de solliciter le commissaire aux comptes. Pour ce qui concerne la mise en place de la loi Sarbanes Oxley au sein du SI de l'entreprise, il faut noter un point clé de la loi portant sur la gestion des accès aux ERP et sur la traçabilité des accès aux applications financières et ressources humaines.

- **Enfin, au titre du rôle de conseil et de veille juridique** du commissaire aux comptes, il faut noter une récente jurisprudence dans laquelle l'absence de fraude (intention de frauder) a été invoquée parce qu'il n'y a pas de moyens en place pour détecter, prévenir et empêcher la fraude (TGI de Créteil, 11e chambre correctionnel, jugement du 23 avril 2013). ■

« Les professionnels du chiffre que sont les experts-comptables et les commissaires aux comptes doivent bien négocier le virage numérique »