Pour lutter contre les logiciels à risques

Noël Pons, CIA

conseiller au Service Central de Prévention de la Corruption

Pour tout manager, l'utilisation à son insu de logiciels à profil « pourri » dont le manque de sécurité rend possible quelques petits arrangements et, le plus souvent, des manipulations d'importance, génère un risque sérieux pour l'entreprise et pour lui-même. Ce risque peut affecter gravement le secteur financier comme l'image de l'entreprise.

Le manager donc, ainsi que le directeur d'audit peuvent, ensemble, mettre en place un programme de contrôle à deux niveaux. Le premier niveau relève de la prévention, il s'agit alors de se protéger de ce risque en exigeant le blocage des spécificités à risques exposées dans notre précédent article. Le second niveau relève de la détection du risque lui même et affecte la méthode de contrôle et la méthode d'analyse qui doit être mise en œuvre dans ce cas.

De ce fait, un manager peut exiger la réalisation, dans son dispositif de contrôle informatique de l'entreprise ou des filiales, d'un examen des procédures de saisie et de traitement des écritures comptables qui doivent respecter les principes définis par le plan comptable.
Ainsi, peuvent être cités :

- la mise en place d'une numérotation séquentielle des factures ;
- l'intégration irréversible des écritures dans la comptabilité ;
- la transposition du principe « sans blanc ni rature » à l'informatique ;
- la mise en place d'un fichier trace de toutes les opérations relatives aux écritures validées ;
- la vérification de l'impossibilité de modifier ou de supprimer des factures ou des écritures comptables ;
- la vérification de l'impossibilité de l'ouverture d'un exercice comptable après la clôture de fin d'exercice.

Ces points qui ne présentent que peu de difficultés de mise en œuvre pour des spécialistes constituent, me semble-t-il, un processus de protection efficient et des préconisations pertinentes dans le domaine de la prévention.

Par contre, il faut savoir que la manipulation des fichiers reste toujours possible ; ces opérations sont en général réalisées dans des périodes troubles puis les fichiers sont gardés en l'état sans régularisation. Il est donc fort possible que, dans beaucoup d'entreprises, il reste quelques cadavres dans les placards même si les pratiques ont été abandonnées.

Notons toutefois qu'il existe une norme assez peu connue et, qui, même si elle n'a pas été publiée, reste à mon sens très pertinente pour mettre en place un tel système, c'est la norme n°X50-702 de 1991, qui détaille avec une grande précision ce que doit être un progiciel « protégé » et sécurisé. Si les préconisations qu'elle contient sont suivies elle permet de maintenir un logiciel propre.

Le second niveau de prévention relève de l'analyse et du contrôle de ces logiciels de gestion.

La détection doit se faire à plusieurs stades de l'analyse :
- la prise de connaissance de l'organisation du système d'information pour connaître le « paysage » ;
- la détection des progiciels utilisés en entreprise et leur positionnement dans la gestion des flux (recettes, dépenses, trésorerie, gestion de stock, comptabilité…) ;
- l'évaluation des risques du progiciel dans son fonctionnement ainsi qu'au regard des facilités qu'il présente.

Cette analyse est non seulement recommandée en interne mais surtout lors de l'évaluation du système utilisé par certaines filiales dans l'analyse de la remontée d'informations. Dans les entreprises de dimension moyenne, l'emploi de progiciels est largement développé et les procédures de contrôle interne et externe, lorsqu'elles sont présentes, peuvent être défaillantes voire inexistantes. Or, dans un environnement de contrôle moins présent, la tentation est grande d'utiliser ces outils logiciels à son profit. Tout auditeur en entreprise peut donc être confronté à ce problème.

Le niveau de risque le plus important est situé essentiellement sur l'ensemble du domaine de la facturation, plus précisément lorsqu'il comprend des ventes au comptant réglées de préférence en espèces ou dans le cas où l'entreprise est utilisée pour blanchir des fonds illégaux. La problématique reste alors similaire, ce sont les flux qui sont inversés.

Pour ce faire, il est nécessaire d'établir une cartographie des risques générés par ce type de manipulation qui est lié, bien entendu, au type d'activité, aux pratiques du secteur professionnel et au niveau de surveillance qui s'exerce sur les recettes encaissées.

Gare à la facturation !

Généralement prise en charge par des progiciels de gestion commerciale, la **facturation** peut comporter certaines procédures qui permettent, par exemple, la diminution automatique des recettes encaissées (surtout en espèces) sans qu'aucune trace immédiatement identifiable ne soit laissée. En fonction du prélèvement opéré sur les encaissements, l'outil assure à la fois une répartition cohérente des modes de paiement et un retraitement pertinent des données de gestion issues de la partie commerciale. A ce stade, les auditeurs disposent donc de justificatifs qui présentent toutes les apparences de la régularité, les coefficients de répartition des moyens de paiement et des différentes catégories de produits sont aussi cohérents. D'après certaines évaluations, pour des prestations de services, la fraude peut affecter plus de 20 % du montant des recettes en espèces soit plus de 10 % du montant des recettes totales. Les conséquences financières sont donc significatives.

Ces possibilités affectent toutes les activités, les prestations de service payées en espèce sont privilégiées ; cependant il m'a été rapporté que de tels montages ont été utilisés dans certaines banques pour camoufler des détournements personnels par de faux prêts. Aucun service n'est donc à l'abri de telles manipulations.

Il est donc nécessaire de réaliser des recherches aléatoires par échantillonnage même (surtout) si tout est cohérent, puis d'effectuer des ressaisies à partir des ventes et des achats en intégrant les données et les fichiers sensibles de chacune des activités.

Dans le domaine du blanchiment, les espèces intégrées au système sont, bien évidemment, supérieures à celles générées par l'activité si elle existe, et afin de tromper les contrôles tout un système d'achats fictif est intégré dans les comptes à partir de sociétés écrans, ce qui donne une cohérence indiscutable au système. Ceci nécessite une analyse systématique des fournisseurs.

Une autre technique communément pratiquée consiste à réduire systématiquement les encaissements d'espèces après des opérations ponctuelles très attractives au plan commercial (ventes flash…) dont la clôture fait apparaître un potentiel « espèces » jugé intéressant.

Dans le domaine comptable, un procédé courant consiste à organiser un détournement de fonds par l'adjonction de **charges indues** au bénéfice d'un membre de l'entreprise. En effet avec ce type de progiciel, il est aisé de rétablir un suivi de justificatifs qui rend les analyses de doublons par exemple totalement illusoires. De plus, les pièces justificatives « alibi » peuvent être construites avec une réelle facilité au moyen des outils bureautiques utilisés au quotidien.

La connexion entre les **comptes Clients et la gestion de Trésorerie** est un point sensible, voire névralgique qui, lorsque les progiciels ne sont pas intégrés ou en phase sur le plan informatique, peut offrir des opportunités que les contrôleurs ou les financiers mettent un certain temps à découvrir.

Le contrôle entre le suivi de **trésorerie interne et les encaissements réels** des clients repose sur les relevés bancaires. Si une seule personne maîtrise ce rapprochement entre les données de banque et les informations contenues dans le logiciel de trésorerie qui sont modifiables, alors tout auditeur externe aura des grandes difficultés à repérer les chèques encaissés au bénéfice d'autrui. En effet, les ratios de trésorerie sont insuffisants pour détecter ce procédé installé dans le temps dont les détournements estimés importants au niveau individuel ne représentent pourtant qu'un faible pourcentage des flux de trésorerie de l'entreprise concernée.

Un audit de fraudes spécifique

Le plus souvent, il est impossible d'identifier, dans le cadre d'un audit classique même informatique, les manipulations du logiciel. Il est nécessaire d'engager un audit de fraudes dédié à ce risque. En tout état de cause, il apparaît essentiel que le management soit averti de l'éventualité de ces risques et que les auditeurs chargés de certifier les comptes y soient très attentifs. Les progiciels sont tous structurés sous un type modulaire, ils sont constitués de sous-systèmes de traitements utilisés suivant les nécessités locales. L'activation des modules de manière à bloquer les dérives relève d'un paramétrage détaillé dont la mise en œuvre n'est pas toujours très compliquée. Par ailleurs, il est parfois judicieux de s'intéresser à la traçabilité des actions effectuées ; ce type de surveillance existe sur les progiciels les plus élaborés.

Enfin, former les auditeurs informatiques à ce type d'intervention afin qu'ils puissent apprécier rapidement et avec pertinence la qualité du progiciel, nécessite de mettre à leur disposition une documentation détaillée sur les logiciels concernés.

Dans un prochain numéro de la revue Audit Interne, je terminerai cette analyse par l'évaluation des risques pénaux et fiscaux qui peuvent être rattachés à l'utilisation de ces outils.