CHAPITRE VII

LA SURVEILLANCE DES SYSTEMES D'INFORMATIONS

1. Les activités en 2004

2. La pratique de la surveillance

1. LES ACTIVITES EN 2004

1.1. Entrevues, contrôles sur place et participations aux groupes nationaux

L'audit informatique a participé en 2004 à 101 entrevues et a effectué six contrôles sur place sur des sujets ayant trait au fonctionnement et à la sécurité des systèmes informatiques des entités surveillées, plus particulièrement des entités aux statuts de PSF connexes, créés par la loi du 2 août 2003 et définis aux articles 29-1, 29-2 et 29-3 de la loi modifiée du 5 avril 1993 relative au secteur financier. Une forte proportion des entrevues a eu lieu avec des prestataires de services non financiers désireux d'obtenir des informations relatives à la procédure d'agrément ou soucieux de qualifier leurs activités en vue de déterminer si celles-ci peuvent être prestées sans agrément.

L'audit informatique a également contribué à sept séminaires ou conférences et à 38 réunions nationales dans le cadre de groupes de travail ou projets. A ce titre, l'audit informatique a participé activement ou en qualité d'observateur à certains travaux de la Banque centrale du Luxembourg, au Comité de Normalisation Luxembourgeois de la Sécurité de l'Information (CNLSI) qui contribue à la définition et à l'évolution des normes ISO en ce domaine, à l'élaboration du programme de formation d'un Master professionnel en «Management de la Sécurité des Systèmes d'Informations» au sein de l'Université du Luxembourg et au programme de recherche GRIF faisant partie du projet LIASIT (*Luxembourg International Advanced Studies in Information Technologies*) qui vise à créer au Luxembourg un centre d'excellence en matière de recherche appliquée dans le domaine, notamment, de la sécurité informatique.

1.2. Projet de recherche GRIF

La CSSF a signé en date du 30 juin 2003 une convention de collaboration avec le Centre de Recherche Public Henri Tudor (CRP-HT) qui porte sur la réalisation d'un projet de recherche appliquée, dénommé «Gestion des Risques Informatiques dans le Secteur Financier : nouvelles approches méthodologiques» (projet GRIF).

Ce projet, co-financé par le CRP-HT et la CSSF, s'inscrit dans le cadre de l'harmonisation internationale du contrôle bancaire telle que définie par le Nouvel Accord de Bâle (Bâle II) et en particulier en ce qui concerne la mission de surveillance de la CSSF au sein du pilier II qui se concentre sur la revue par l'autorité de surveillance de l'adéquation du capital et du processus interne d'évaluation des établissements de crédit.

L'objectif majeur visé par la CSSF et le CRP-HT consiste à rechercher de nouvelles approches méthodologiques permettant d'évaluer, de préférence de manière quantitative, les risques liés à l'informatique. Il s'agit d'un domaine de recherche très spécifique dont les résultats visent à formaliser et à quantifier la prise en compte des risques informatiques au sein des risques opérationnels globaux des établissements financiers.

Fin 2004, la CSSF et le CRP-HT ont défini une méthodologie normée qui ne couvre plus uniquement les risques opérationnels informatiques, mais qui s'étend à tout le volet du risque opérationnel tel qu'appréhendé dans Bâle II. De ce point de vue, les résultats du projet dépassent les objectifs initiaux et sont perçus comme suffisamment innovants pour que la CSSF envisage de promouvoir cette méthode auprès d'autres autorités concernées par le pilier II.

La CSSF et le CRP-HT communiqueront aux professionnels concernés et au public avant la fin du premier semestre 2005 les principaux résultats du projet. La méthodologie retenue dans le cadre du pilier II pourra également servir aux établissements dans le cadre du pilier I. Des travaux supplémentaires sont prévus avec les professionnels concernés (établissements de crédit, entreprises d'investissements, consultants et réviseurs) afin de consolider la méthode et de favoriser sa compréhension par tous les acteurs concernés.

A noter que cette méthode reste compatible avec toute autre méthode utilisée dans le cadre du pilier I, qu'il s'agisse de COSO[1] ou dans le domaine informatique, de Cobit, de Méhari, d'EBIOS, etc., et qu'elle présente de par sa normalisation une transparence dans l'évaluation spécifique au pilier II.

1.3. La collaboration internationale

L'année 2004 a été marquée par l'arrêt des travaux de l'Electronic Banking Group (EBG) qui seront intégrés au sein d'un autre groupe du Comité de Bâle. Le groupe devant accueillir la suite des travaux de l'EBG n'est pas encore défini, mais les groupes traitant des risques opérationnels constituent de bons candidats.

L'arrêt des réunions ne signifie cependant pas l'absence de communication. Les membres de l'EBG s'informent régulièrement des nouveaux enjeux dans le domaine de l'e-banking international. Ainsi, la CSSF a pu suivre la progression du phénomène de «phishing» qui a connu une expansion importante au départ des Etats-Unis et de l'Asie, avant de toucher l'Europe.

Le «phishing[2]» est une forme d'escroquerie en ligne qui a pour but d'obtenir, à travers Internet et par des moyens détournés, en trompant la vigilance des utilisateurs, des informations confidentielles qui seront utilisées de manière illégale.

Le phénomène du «phishing» démontre bien qu'actuellement, la sécurité des informations dans le domaine financier n'est plus uniquement de la responsabilité et de la compétence des professionnels financiers, mais que l'utilisateur de services financiers par Internet doit également être sensibilisé par rapport aux menaces et doit assumer ses propres responsabilités en ce domaine. C'est pourquoi la CSSF ne peut qu'approuver les établissements financiers qui ont informé leur clientèle de l'existence du «phishing» et les initiatives qui visent à informer le public, comme le projet CASES[3].

2. LA PRATIQUE DE LA SURVEILLANCE

Dans le cadre de la surveillance des aspects opérationnels des PSF connexes, l'audit informatique de la CSSF s'attache particulièrement à vérifier l'application du cadre légal et réglementaire visant directement ou indirectement à maintenir ou à améliorer le professionnalisme des activités de manière à ce que la qualité des prestations réalisées en sous-traitance réponde aux mêmes critères prudentiels que ceux des établissements financiers qui y font appel.

2.1. Ségrégation des environnements au sein des PSF connexes

La CSSF souligne que la ségrégation des environnements et des données par client du prestataire PSF connexe est un élément fondamental de qualité et de pérennité des activités, notamment parce qu'elle contribue à minimiser les risques de réputation et indirectement les risques juridiques et financiers. En effet, un prestataire chargé de traiter les travaux de plusieurs établissements financiers doit à tout moment pouvoir distinguer pour lequel d'entre eux il réalise une prestation. Il doit également être en mesure d'assurer une parfaite étanchéité entre les entités qu'il assiste, de manière à garantir à chacune une parfaite confidentialité des données confiées.

---

1 COSO Enterprise Risk Management – Integrated Framework. COSO a été constituée en 1985 pour promouvoir la Commission Nationale aux Etats-Unis, dénommée «National Commission on Fraudulent Financial Reporting» et connue sous le nom de «Treadway Commission» (www.coso.org).

2 Phishing = (Phreaking + Fishing). Phreaking : hacking des centrales téléphoniques, depuis la blue Box de John Draper dans les années 70. Fishing : allusion à la pêche aux mots de passe dans l'océan Internet.

3 Cyberworld Awareness Security Enhancement Structure - Portail de la sécurité de l'information du Ministère de l'Economie (www.cases.lu).

La CSSF rappelle qu'il incombe aux établissements surveillés d'appliquer les principes de prudence lors de l'évaluation de solutions techniques. Ainsi, l'audit informatique ne se prononce en faveur ou en défaveur d'une solution proposée par un établissement qu'après avoir évalué la manière dont celui-ci aura apprécié les risques, ainsi qu'en situant cette solution par rapport aux bonnes pratiques du moment et à l'expérience accumulée auprès de cas similaires par le passé.

L'expérience tirée du passé incite l'audit informatique à être très prudent vis-à-vis des solutions de ségrégation d'environnements essentiellement basées sur des procédures, sans l'appui de garde-fous techniques. En effet, le bon fonctionnement des procédures repose sur une discipline de la part des personnes concernées et l'expérience montre malheureusement que cette discipline tend à s'amoindrir avec le temps et au fur et à mesure des changements de personnel.

Un autre aspect de prudence concerne la fiabilité des solutions techniques proposées afin de garantir un partage des environnements. La CSSF n'impose pas la mise en place d'un ordinateur par entité financière traitée par le PSF, ce qui serait à l'encontre de toute économie d'échelle visée par la sous-traitance. Par contre, il convient d'être prudent lorsqu'un système (ordinateurs et autres périphériques) est partagé par plusieurs établissements financiers. Il existe de multiples façons de partager les ressources, mais l'analyse devrait tenir compte de la fiabilité des différents systèmes d'exploitation et des applications financières utilisées. En ce sens, la CSSF n'est actuellement pas favorable à l'utilisation d'une application partagée fonctionnant sur une seule partition du système, à moins que ce mode de fonctionnement ait déjà fait ses preuves depuis plusieurs années. Le partage d'une application par plusieurs établissements est *a fortiori* inacceptable lorsque chaque établissement utilisateur se connecte sur une application unique partagée, car dans ce cas la ségrégation ne dépend que des identifiants (numéro d'utilisateur et mot de passe) utilisés. Une erreur de configuration des accès ou tout simplement la connaissance de l'identifiant et du mot de passe d'un autre établissement (lors d'un changement d'employeur par exemple) permettrait une connexion dans l'environnement tiers.

Aujourd'hui, la solution la plus courante en mode ASP[4] reste le multipartitionnement pour lequel fonctionne une instance du logiciel financier par établissement utilisateur.

Le problème se pose de façon encore plus complexe en ce qui concerne l'utilisation de systèmes permettant un partitionnement virtuel multi système d'exploitation. Il s'agit de solutions basées sur des produits comme VMware, par exemple. Ces solutions sont prometteuses en termes de sécurité, notamment lorsque les processeurs incorporeront la technologie de ces machines virtuelles. Dans ce cas, on pourra s'attendre à un partitionnement au niveau du processeur de l'ordinateur et non plus au niveau du système d'exploitation de la machine virtuelle. Dans ces circonstances, la CSSF ne se prononce pas encore quant à la fiabilité des solutions actuelles et incite à la prudence.

2.2. Prestations d'intérimaires et statut PSF d'opérateurs de systèmes et de réseaux

Un certain nombre de sociétés de services informatiques ont approché la CSSF afin de déterminer si leurs activités relèvent du statut d'opérateur de systèmes informatiques et de réseaux de communication du secteur financier.

Ces sociétés incluent dans leur catalogue de services la mise à disposition de personnel spécialisé pour opérer des systèmes ou réseaux de production des établissements financiers. Il s'agit de profils d'ingénieurs réseaux, d'administrateurs systèmes, voire d'opérateurs spécialisés dans l'écriture de scripts d'exploitations.

[4] Application Service Provider. Fournisseur d'un service applicatif qui se traduit souvent par une location à la demande d'une application informatique opérée par le prestataire.

La CSSF a déjà pris position l'année passée en ce qui concerne la qualification de ces services en indiquant qu'elle considère l'administration d'un système de production comme une fonction faisant partie d'opérations du système ou du réseau. En ce sens, ces services relèvent donc bien *stricto sensu* du statut de PSF selon l'article 29-3 de la loi modifiée du 5 avril 1993 relative au secteur financier.

Toutefois, cette position nécessite certaines précisions en fonction de la responsabilité contractuelle prise par le sous-traitant et en fonction du caractère temporaire du service, auquel peut s'ajouter la finalité de l'intervention du sous-traitant.

Concernant la responsabilité du sous-traitant, il doit être clairement établi dans le contrat de services que le sous-traitant n'est responsable que du profil des personnes mises à disposition auprès de l'établissement. Le contrat ne peut en aucune façon prévoir une responsabilité de maîtrise d'œuvre d'un projet et les travaux et tâches à effectuer par le personnel du sous-traitant doivent être entièrement définis par l'établissement financier. De plus, la prestation doit être limitée dans le temps et ne doit ni s'étendre au-delà des périodes admissibles pour les prestations d'intérimaires, conformément à la législation en vigueur dans ce domaine, ni être reconduite au moyen d'un personnel différent, ce qui reviendrait à proposer une prestation d'opérateur déguisée en prestation d'intérimaire.

La finalité de l'intervention du sous-traitant est un élément important dans la qualification de l'activité. Si les services ont une durée raisonnable et limitée dans le temps afin de répondre à des travaux non répétitifs, comme, par exemple, une conversion d'un système vers un autre, l'activité peut s'apparenter à un projet de développement et non d'exploitation, car la prestation devenant caduque dès la migration terminée. Dans ce cas, le sous-traitant pourra également s'engager sur le résultat de la prestation et en garantir la maîtrise d'œuvre, étant donné que la prestation ne sera plus assimilée par la CSSF à une opération des systèmes, mais à un projet spécifique non répétitif.

Lors de l'évaluation de prestations situées à la frontière entre celles relevant d'un agrément PSF d'opérateur de systèmes et de réseaux et celles ne nécessitant pas d'agrément, la CSSF vérifie en particulier si la société concernée remplit les conditions décrites ci-après. A noter que les activités situées à la limite sont celles consistant à fournir un personnel spécialisé en fonctions informatiques d'exploitation (ingénieurs systèmes ou réseaux, opérateurs, agents de production, développeurs de scripts, etc.).

Ainsi, les conditions permettant à un prestataire de qualifier ses services de travail intérimaire, et non d'opération de systèmes et de réseaux qui nécessite un agrément en tant que PSF, sont les suivantes :

- le prestataire ne renouvelle pas la prestation auprès d'un même établissement financier de manière consécutive,
- il ne s'engage pas sur la finalité de l'exploitation, qui comporterait une obligation de résultat, mais il s'engage uniquement sur la qualité du profil de la personne mise à disposition de l'établissement financier, ce qui entraîne donc une obligation de moyens,
- il prévoit contractuellement que les travaux et tâches soient attribués par l'établissement financier,
- *a priori*, la prestation doit avoir lieu auprès de l'établissement financier,
- il réalise cette prestation pour une durée conforme à la législation en vigueur dans le domaine du droit du travail intérimaire.

La CSSF tente ainsi d'éviter que des prestations d'opérateurs de systèmes et de réseaux ne soient fournies sans agrément et de manière déguisée sous la forme, notamment, de contrats d'intérimaires renouvelés systématiquement.

De plus, la CSSF rappelle aux établissements surveillés qu'une bonne organisation administrative et comptable repose sur un contrôle des activités essentielles de support. De ce point de vue, les établissements financiers doivent éviter de faire appel de manière systématique à des ressources intérimaires pour des fonctions informatiques, en particulier liées à des systèmes et réseaux de production.

Il est tout à fait acceptable pour un établissement financier de remplacer par un intérimaire un spécialiste informatique (un administrateur de systèmes par exemple) indisponible pour des raisons de santé ou autres, mais il est inacceptable que l'établissement financier finisse par ne faire appel qu'à des intérimaires. En effet, le bon fonctionnement des systèmes qui assurent la continuité des services financiers offerts n'est possible que si l'établissement financier conserve leur maîtrise.

Le renouvellement périodique du personnel entraîne pour le moins un appauvrissement des connaissances de l'outil de production, en particulier au regard de la connaissance historique des événements et problèmes rencontrés. Il peut également mener à une dilution des responsabilités selon le degré de motivation et d'implication des intérimaires dans l'entreprise.

Il ne faut pas négliger non plus les responsabilités propres aux administrateurs de systèmes dans la définition des droits d'accès des utilisateurs. Cette activité fait de ces personnes des acteurs stratégiques.

La CSSF demande dans ce contexte une attention particulière de la part des réviseurs externes lors de leur audit annuel.

Il est primordial pour chaque établissement financier de s'assurer que les sous-traitances se fassent en conformité avec la loi, tout en respectant les principes de prudence liés aux prestations d'intérimaires énoncées ci-dessus. Un établissement financier ne peut faire appel à un sous-traitant ne disposant pas de l'agrément requis et se verrait contraint de renoncer à recourir à ce sous-traitant. Le sous-traitant pourrait faire l'objet de poursuites pénales pour exercice illégal d'une activité relevant du secteur financier.

2.3 Les nouvelles technologies en matière de téléphonie : VoIP

La technologie VoIP, c'est-à-dire «Voice over IP», consiste à véhiculer la parole sur un réseau utilisant le protocole IP qui n'est rien d'autre que le protocole Internet. Concrètement, VoIP est un nouveau mode de téléphonie permettant d'utiliser Internet (public ou propre à l'entreprise ou à son groupe) pour communiquer.

L'utilisation par un professionnel financier de la technologie VoIP pose de nouvelles questions prudentielles, notamment au regard de la confidentialité des informations. En effet, en téléphonie classique, les communications internes à un établissement qui possède sa propre centrale téléphonique, restent confinées physiquement auprès de celui-ci. Les communications externes passent par un opérateur téléphonique qui relève de la loi sur les télécommunications lui imposant le secret des communications.

Les questions que soulève l'usage de la technologie VoIP sont multiples, à savoir par exemple :

- La technologie est-elle suffisamment maîtrisée pour s'assurer que les équipements de réseau de l'établissement soient correctement configurés et sécurisés ? En effet, un équipement mal configuré permet de dupliquer le lien et d'écouter les communications par n'importe quel équipement (téléphone VoIP ou ordinateur de bureau) qui y est connecté grâce au réseau local.

- Le réseau servant à véhiculer les communications VoIP internes est-il géré exclusivement par l'établissement luxembourgeois ? Si ce réseau, qui peut être le réseau informatique de l'établissement, est géré par exemple par une entité du groupe ou par la maison mère, les principes énoncés dans la circulaire IML 96/126 ne seront pas respectés puisque la confidentialité ne sera pas assurée.
- Si la technologie VoIP est utilisée pour communiquer en dehors de l'établissement, par exemple avec les autres entités du groupe, voire avec le monde extérieur non-VoIP, la question du statut de l'opérateur du réseau se pose. Il est effectivement possible que l'opérateur ne soit pas un opérateur de téléphonie au sens de la loi sur les communications (ou d'une loi analogue au sein de l'UE) et qu'il ne soit donc pas tenu au secret par cette loi. De plus, en cas d'interconnexion des réseaux IP, il est nécessaire de protéger l'entreprise des intrusions. Or, les firewalls et IDS[5] se heurtent pour VoIP à des limites techniques et ne sont pas suffisamment évolués pour permettre une protection efficace. VoIP peut donc servir de moyen d'intrusion dans un réseau informatique.

Ces questions ne visent pas à décourager les professionnels financiers d'utiliser VoIP, mais elles montrent que la mise en œuvre de cette technologie doit se faire sérieusement, en analysant correctement les vulnérabilités et les menaces. L'utilisation de VLAN[6] peut être souhaitable pour segmenter les réseaux locaux et la mise en œuvre de VPN[7] est plus que jamais à étudier dans ce contexte.

Une approche prudentielle consisterait à appréhender les solutions VoIP de la même manière que les réseaux informatiques. Le plus grand danger est à rechercher dans la mise en œuvre de VoIP par certains spécialistes de la téléphonie traditionnelle qui ne cumulent pas la spécialité de réseaux de données et, surtout, qui ne connaissent pas les impératifs prudentiels de la CSSF. Un projet VoIP ne peut en effet en aucun cas être considéré comme un projet relevant simplement de la téléphonie.

[5] IDS : Intrusion Detection System. Systèmes servant à détecter des comportements anormaux (patterns) d'un réseau qui laissent supposer une tentative d'intrusion. Un IDS s'apparente à un anti-virus de réseau.

[6] VLAN : Virtual Local Area Network. Cette technique permet de séparer des réseaux physiques en leur attribuant une sécurité logique au niveau du protocole de transport (Ethernet).

[7] VPN : Virtual Private Network. Cette technique se base sur une cryptographie des informations transmises, garantissant la confidentialité entre deux ou plusieurs participants pré-configurés au sein d'un réseau informatique.

Première rangée de gauche à droite :
Marie-Anne VOLTAIRE (Audit interne)
Monique REISDORFFER | Marcelle MICHELS | Joëlle DELOOS | Karin FRANTZ (Secrétaires de direction)
Pascale DAMSCHEN (Coordination informatique)

Deuxième rangée de gauche à droite :
Pascal DUCARN (Audit informatique) | Constant BACKES (Sécurité des systèmes)
David HAGEN | Claude BERNARD (Audit informatique)

Absents :
Geneviève PESCATORE | Marc WEITZEL (Conseillers du Directeur général)