Annexe Circulaire CBFA_2009_17-1 du 7 avril 2009

Saines pratiques en matière de gestion des risques de sécurité des opérations sur internet

Champ d'application:

Établissements de crédit, entreprises d'assurances, entreprises d'investissement et sociétés de gestion d'organismes de placement collectif, ainsi que les succursales belges de ces établissements qui relèvent du droit d'un État non membre de l'Espace économique européen (EEE).
La circulaire est également portée à la connaissance des établissements établis en Belgique qui relèvent du droit d'un État membre de l'EEE.

1. Introduction

Les établissements financiers qui utilisent l'internet pour fournir des services sont exposés à des risques divers en matière de sécurité.

C'est pourquoi les saines pratiques établissent des points d'attention et des recommandations liés à la sécurité :

- de l'infrastructure informatique propre (infrastructure informatique interne, pare-feu, serveurs courriel et internet, ...) face aux menaces de l'internet ;
- des opérations financières, des consultations et des actes de gestion sur internet.

Il est attendu des établissements financiers qu'ils respectent les saines pratiques ou qu'ils expliquent à la CBFA pourquoi ils s'en écartent (*comply or explain*).

2. Sécurité de l'infrastructure informatique propre

2.1. Justification

Tout établissement financier qui connecte son infrastructure informatique sur l'internet est tenu de prendre des mesures de sécurité adaptées pour garantir la sécurité et la continuité de ses systèmes informatiques ainsi que l'intégrité et la confidentialité de ses données financières et de ses données clients, face à tous les abus et risques prévisibles émanant de l'internet.

2.2. Exigences prudentielles

2.2.1. Politique de sécurité

Tout établissement qui connecte son infrastructure informatique sur l'internet dispose d'une politique de sécurité adaptée qui tient compte de :

- l'importance d'une sécurité adaptée de l'infrastructure informatique propre et des objectifs en la matière ;

- l'organisation interne et les responsabilités internes concernant :
    - le suivi des menaces internet et leur examen à la lumière des mesures de sécurité adoptées pour l'infrastructure informatique propre ;
    - la sécurité de l'infrastructure informatique propre ;
    - le traitement des incidents de sécurité internet ;
- les directives aux collaborateurs en matière d'utilisation sûre de l'internet ;
- le cadre de sécurité pour l'échange de courriels et d'autres fichiers et messages (par exemple l'*instant messaging*) avec l'extérieur ;
- la politique et la sécurité en ce qui concerne l'octroi de l'accès à l'infrastructure informatique propre via l'internet (*remote access*) ;
- les critères appliqués et les responsabilités pour la réalisation (en interne ou par des tiers) périodique d'examens spécialisés en matière de sécurité ;
- la création et l'archivage de fichiers « historiques d'événements » (*logs*) techniques adaptés et leur analyse, leur suivi et leur *reporting*.

2.2.2. Analyse et suivi des menaces et de la situation propre en matière de sécurité

L'établissement veille à :

- une bonne analyse et un bon suivi des menaces internet pour son infrastructure informatique, compte tenu des solutions de sécurité utilisées par l'établissement et de son utilisation de l'internet ;
- un suivi rigoureux des lacunes publiées en matière de sécurité dans l'infrastructure internet et les solutions de sécurité qu'il utilise (logiciel, matériel, langages de programmation, cryptographie, …). Lorsque cela s'avère nécessaire, l'établissement installe dans les meilleurs délais les solutions correctrices mises à disposition par les fournisseurs (patchs logiciels, mises à niveau, ...) ou utilise d'autres solutions pour couvrir les risques de sécurité.

Sur la base des analyses effectuées, et compte tenu de la nature et de l'échelle des menaces internet constatées, l'établissement effectue périodiquement une évaluation formelle des risques afin d'examiner si, et dans quelle mesure, les mesures de sécurité en vigueur, les technologies utilisées, les procédures ou les services fournis doivent être adaptés.

Les conclusions des suivis et des analyses de risques effectués sont, en fonction de leur degré d'urgence et d'importance, et au moins une fois par an, soumises à la direction effective.

2.2.3. Protection contre les accès non autorisés à l'infrastructure informatique propre et contre les modifications de cette infrastructure

L'établissement prend les mesures de sécurité nécessaires pour prévenir les accès non autorisés à son infrastructure informatique propre via l'internet et les utilisations malveillantes de cette infrastructure via l'internet.

L'établissement utilise à cet égard des passerelles contrôlées entre l'internet et l'infrastructure informatique propre, telles que des *firewalls*, des *proxy servers*, des *mail relays*, des scanners antivirus et des scanners de contenu, ou d'autres solutions de sécurité similaires. L'établissement veille à ce que ces passerelles soient correctement conçues, configurées et sécurisées, et à ce qu'elles fassent l'objet d'une gestion quotidienne professionnelle et d'un suivi rigoureux.

Il est très important, à cet égard, que toutes les liaisons directes et indirectes[1] avec l'internet passent par ces passerelles. Afin de garantir l'étanchéité du périmètre de protection ainsi établi, l'établissement est par ailleurs particulièrement attentif à la prévention des liaisons réseaux non contrôlées et insuffisamment protégées avec l'extérieur (réseaux sans fil, modems, etc.) (*back doors*).

[1] Il arrive par exemple que des succursales, des agences ou des filiales connectées à l'infrastructure informatique propre disposent de liaisons internet.

Les passerelles contrôlées précitées ne pouvant (généralement) pas neutraliser ou contrer de manière efficace et/ou étanche tous les flux d'informations présentant des risques, l'établissement accorde en outre l'attention nécessaire à la sécurisation adéquate des applications et bases de données internes qui reçoivent des informations ou des instructions par l'internet (principe de la *defense in depth*) [2].

2.2.4. Protection de sites internet publics

Les sites internet publics présentent un "risque de sécurité" accru en raison du nombre important de visiteurs et de leur grande accessibilité sur l'internet. L'établissement sera dès lors particulièrement attentif à la sécurité de ces sites internet publics afin de prévenir qu'ils soient la cible de modifications non autorisées ou qu'ils soient utilisés pour diffuser des logiciels malveillants.

Afin de limiter la vulnérabilité des sites internet et des serveurs qui y sont liés, l'établissement recourra à :

- des pare-feu, des serveurs mandataires ou d'autres solutions de sécurité similaires, afin de protéger dans toute la mesure du possible les sites internet, et les serveurs qui y sont liés, des menaces et abus par internet ;
- des techniques de sécurité qui « dépouillent » les serveurs de toutes les fonctions superflues dangereuses (*stripping*) et sécurisent au maximum les applications à risques (*hardening*). Afin de renforcer davantage la sécurité, l'accès des applications aux données et moyens dont elles ont besoin est également réduit au strict minimum (principe du *least privilege*).

Afin de rendre plus difficile les abus commis à l'aide de sites internet usurpatoires (*phishing sites* et *spoofed sites*) ressemblant à des sites légitimes d'établissements financiers, les sites transactionnels, et de préférence aussi les sites informatifs, sont identifiés à l'aide de certificats numériques de qualité[3] établis au nom de l'établissement financier, ou d'autres mécanismes d'authentification similaires.

2.2.5. Accès autorisés à l'infrastructure informatique propre via l'internet (accès à distance ou *remote access*)

L'établissement dispose, en matière d'accès autorisés à l'infrastructure informatique propre via l'internet, d'une politique qui consacre une attention particulière aux règles en matière d'octroi, d'approbation, de suivi, de révocation et de sécurité.

Ces accès utilisent des solutions de sécurité de haute qualité qui :

- s'appuient sur des solutions d'authentification solides qui permettent avec un degré d'assurance très élevé de vérifier l'identité des utilisateurs. Une description de ces solutions d'authentification solides est présentée au point 3.2.3.a. ;
- vérifient si les actes des utilisateurs sont autorisés ;
- limitent au strict minimum les accès externes vers l'infrastructure informatique (principe du *least privilege*) ;
- prévoient des mesures de sécurité adéquates pour éviter les accès non autorisés à l'infrastructure informatique propre et les modifications de cette infrastructure faisant suite à des lacunes de sécurité (virus, logiciels malveillants, *back doors*, ...) sur l'ordinateur ou l'infrastructure informatique des utilisateurs. Pour les accès à des composantes critiques et sensibles de l'infrastructure informatique, l'on recourt en principe exclusivement à des ordinateurs sécurisés destinés spécialement à cet usage.

---

[2] La *defense in depth* est une stratégie de sécurisation qui consiste à placer plusieurs lignes de défense dans l'objet à défendre ainsi que sur son pourtour. Toute intrusion qui aurait percé la première ligne de défense est prise en charge par la ligne suivante.

[3] Certificats SSL "*extended validation*" contenant au minimum un encryptage 128 bits et établis par des organismes de certification réputés et généralement acceptés.

2.2.6. Directives aux collaborateurs en matière de sécurité

La direction opérationnelle approuve les directives adressées aux collaborateurs en ce qui concerne l'utilisation sûre de l'internet, et veille à leur respect. À cet égard, une attention particulière est accordée :

- aux risques liés au téléchargement et à l'installation de fichiers à risques ;
- aux mesures de sécurité concernant l'utilisation du courriel (courriels suspects, spam, ...) et d'autres techniques de communication par internet (par exemple l'*Instant Messaging*) ;
- aux mesures de prévention et aux conditions d'encadrement pour le transfert de fichiers ((s)ftp[4], ...) ;
- aux risques liés aux accès et autorisations souvent étendus de certains utilisateurs ou informaticiens sur l'internet.

À la lumière des courriels de *phishing*[5] destinés à induire ses clients en erreur, et étant donné le très faible degré de sécurisation des courriels sur le plan de la confidentialité et de l'intégrité de leur contenu, l'établissement élabore des directives quant à l'utilisation acceptable du courriel dans les différents contacts externes commerciaux et autres. L'établissement est également attentif aux autres solutions de communication internet utilisées, telles que l'*Instant Messaging*.

2.2.7. Procédure de gestion d'incidents

L'établissement dispose d'une procédure de gestion d'incidents pour traiter les incidents de sécurité internet. Cette procédure expose les tâches et compétences attribuées en cas d'incidents de sécurité internet graves et les procédures d'escalade à suivre. Cette procédure de gestion d'incidents explique également les tâches et responsabilités en matière de communication interne et externe quant aux incidents de sécurité internet importants.

2.2.8. *Audit trails*, analyses et *reporting*

Afin de pouvoir détecter et analyser les irrégularités ou les attaques contre les services internet fournis, et, si nécessaire, prendre les mesures qui s'imposent, l'établissement établit et conserve les *logs* techniques et *audit trails* nécessaires des accès à ses systèmes informatiques (en ce compris les applications) et composants réseaux et des activités qui y sont réalisées. Ces *logs* et ces *audit trails* doivent être sécurisés et archivés de manière adéquate afin de garantir leur intégrité et leur qualité de pièces probantes. Il est important à cet égard de pouvoir garantir leur valeur juridique.

En règle générale, les *logs* et les *audit trails* sont conservés pendant au moins 6 mois afin de pouvoir servir ultérieurement lors d'éventuels litiges ou à des fins d'analyses d'abus.

En fonction du profil de risque et de l'importance des services internet fournis, l'établissement analyse avec une fréquence appropriée les *logs* et les *audit trails* en vue d'identifier les irrégularités et les abus. L'établissement prévoit à cet égard les moyens et effectifs spécialisés nécessaires.

Les irrégularités ou abus constatés sont rapportés de manière appropriée à la direction effective.

2.2.9. Réalisation d'examens indépendants en matière de sécurité

Les établissements qui connectent leur infrastructure informatique sur l'internet font examiner par un expert indépendant les mesures de sécurité internet mises en place. Ces examens comprennent des tests de pénétration et sont réalisés de manière proactive avant de connecter pour la première fois l'infrastructure informatique propre ou un nouvel élément à l'internet. Ils sont répétés par la suite en fonction de l'évolution des menaces, de l'utilisation ou de l'importance des modifications apportées à l'infrastructure (de sécurité) internet utilisée.

---

[4] (*Secured*) *File Transfer Protocol.*

[5] Courriels de *phishing* frauduleux qui imitent les courriels légitimes dans l'intention d'induire en erreur leur destinataire et d'en retirer un avantage déterminé. Dans le domaine financier, les courriels usurpatoires sont souvent destinés à obtenir les données secrètes d'authentification d'une carte de crédit ou d'une application de banque électronique (nom d'utilisateur et mot de passe, …).

De manière générale, il est attendu des établissements qu'ils fassent effectuer ces examens spécialisés par des experts externes indépendants disposant en la matière du savoir-faire et de l'expérience nécessaires ainsi que des moyens appropriés. Dans des cas exceptionnels, l'on peut accepter que l'établissement réalise lui-même ces examens, à la condition qu'il dispose en la matière de l'expertise nécessaire, et que le réalisateur du test ne soit en aucune façon mêlé au développement, à la mise en œuvre ou à la gestion opérationnelle des services internet fournis (par exemple l'audit informatique interne).

3. Sécurité des opérations financières par internet

3.1. Justification

Les établissements financiers qui permettent à leurs clients de consulter ou de gérer leur données et/ou d'effectuer et/ou d'envoyer (par lots) des opérations via l'internet (ci-après « services transactionnels ») sont exposés à des risques de sécurité supplémentaires qui viennent s'ajouter aux risques liés à la connexion de l'infrastructure informatique (interne) à l'internet (cf. le chapitre 2).

Étant donné que les établissements financiers doivent toujours disposer, pour leurs services transactionnels par internet, d'une connexion entre l'infrastructure informatique propre et l'internet, les exigences en matière de sécurité qui suivent constituent un complément aux directives en matière de sécurité exposées au chapitre 2.

Les établissements financiers qui permettent à leurs clients de participer, par l'intermédiaire de leurs solutions de sécurité internet et/ou de leur infrastructure de sécurité internet, à des services usuels de paiement internet fournis par des tiers (par exemple des paiements *3D secure* auprès de commerçants sur internet) doivent, pour ce faire, satisfaire à des mesures d'encadrement complémentaires (cf. le point 3.2.8.).

3.2. Exigences prudentielles

3.2.1. Politique de sécurité

L'établissement consacre de manière appropriée, dans sa politique de sécurité, une attention supplémentaire :

- à l'importance d'une sécurité adaptée des services internet transactionnels fournis et des objectifs en la matière ;
- à l'organisation et aux responsabilités concernant :
  - le suivi des menaces internet pour les services transactionnels fournis ;
  - la sécurité des services internet transactionnels fournis ;
  - la centralisation, le traitement et le suivi des plaintes liées à la sécurité, en ce compris les plaintes de clients ;
- à la protection et à la sécurité des données d'authentification des clients et de l'établissement financier utilisées pour le besoin de services transactionnels internet ;
- à la protection et à la sécurité des informations et opérations de clients échangées via l'internet ;
- à la sécurité des applications internet transactionnelles utilisées ;
- à la communication avec la clientèle en ce qui concerne les services internet fournis, et à la manière dont les clients sont censés contribuer à la sécurité des services internet fournis ;
- à la création et à l'archivage de *logs* techniques et d'*audit trails* logiques des opérations internet et à leur analyse, leur suivi et leur reporting.

3.2.2. Analyse et suivi des menaces et de la situation propre en matière de sécurité

L'établissement veille à une bonne analyse et à un bon suivi des menaces pour les services internet transactionnels fournis, compte tenu des solutions de sécurité qu'il utilise et qu'il fournit à ses clients. À cet égard, la sécurité est évaluée tant dans son ensemble que composant par composant.

Sur la base des analyses effectuées, et compte tenu de la nature et de l'échelle des services internet fournis, l'établissement effectue au moins une fois par an une évaluation formelle des risques afin d'examiner si, et dans quelle mesure, les mesures de sécurité en vigueur et les technologies ou procédures utilisées doivent être adaptés. À cet égard, l'établissement tient également compte du temps nécessaire pour mettre en œuvre les adaptations requises (en ce compris le *roll-out* auprès des clients) ainsi que de l'évolution attendue des menaces au cours de cette période.

Les conclusions des suivis et des analyses de risques effectués sont, en fonction de leur degré d'urgence et d'importance, et au moins une fois par an, soumises pour approbation à la direction effective.

3.2.3. Protection de l'authentification

Il est essentiel que tous les accès aux services internet fournis et toute utilisation de ces services soient légitimes. L'établissement utilise dès lors des solutions d'authentification solides qui soient adaptées à la nature et aux risques des services internet fournis et qui permettent de vérifier avec un degré très élevé d'assurance l'identité des utilisateurs qui se manifestent.

L'établissement tient compte, dans le choix de la solution d'authentification utilisée, des risques de sécurité internet du côté des clients, ainsi que de la possibilité qu'ont les clients d'évaluer ces risques et de se prémunir contre eux.

a) Solutions d'authentification pour les particuliers

Dans le contexte précité, et compte tenu de la forte montée en puissance des menaces, notamment en ce qui concerne :

- les attaques de type *phishing* ;
- les sites internet usurpatoires ;
- la diffusion croissante de logiciels malveillants sur les ordinateurs des clients, logiciels qui essaient de dérober diverses informations confidentielles telles que les données d'authentification (par exemple les noms d'utilisateurs, les mots de passe, ...) et les données financières (par exemple les données des cartes de crédit, ...) ;

les solutions d'authentification reposant uniquement sur un nombre limité de secrets réutilisables (par exemple le nom d'utilisateur et le mot de passe, le cas échéant en combinaison avec des cartes TAN[6] ou des suites de chiffres personnelles ou des clés privées *software* PKI[7], ...), qui peuvent être dérobés sur l'internet sans laisser de traces, ne sont plus acceptables pour les services internet exposés aux risques de fraude. Pour les services internet de nature purement consultative, l'établissement doit effectuer une analyse de sensibilité et déterminer une politique de confidentialité et de sécurité adaptée. Dans leur utilisation de mots de passe à usage unique à des fins d'authentification, les établissements doivent en outre veiller à ce que la période de validité de ces mots de passe à usage unique soit limitée au strict minimum (c'est-à-dire tout au plus quelques minutes).

b) Solutions d'authentification pour les entreprises et les professionnels

Pour les services internet transactionnels aux entreprises et aux professionnels, l'établissement peut recourir à des solutions d'authentification adaptées dans lesquelles la contrepartie se charge en tout ou en partie de la sécurité de ses propres données personnelles d'authentification ainsi que de son matériel informatique et de son logiciel au sein de son infrastructure informatique propre. Le cas échéant, les entreprises et/ou les contreparties professionnelles sont informées par l'établissement de ce qui est attendu d'elles sur le plan de leurs mesures de sécurité internes, et les responsabilités en la matière sont clairement définies dans le contrat.

---

6 Cartes ou autres supports de données comportant un nombre limité de mots de passe préalablement établis que le client doit saisir pour s'identifier ou effectuer des opérations. L'application internet indique à cet égard quel mot de passe le client doit saisir.

7 Dans le cas d'une *software PKI* (Public Key Infrastructure), chaque utilisateur est identifié de manière unique à l'aide d'une clé privée *software* qui lui est attribuée et qui est souvent enregistrée sur l'ordinateur du client.

c) Mesures de sécurité internes

L'établissement veille à ce que toutes les données d'authentification nécessaires aux clients ainsi que le matériel informatique et les logiciels liés aux clients soient remis aux clients d'une manière sûre. Les logiciels qui sont mis à la disposition du client et qui sont destinés à être utilisés par lui sont verrouillés de manière physique et/ou munis d'une signature numérique par les soins de l'établissement financier, afin de permettre aux clients d'en vérifier l'authenticité.

Afin d'identifier ses sites internet transactionnels à l'égard de ses utilisateurs, l'établissement recourt à des certificats numériques (*digital certificates*) de qualité[8] établis à son nom, ou à d'autres mécanismes d'authentification similaires.

L'établissement veille à ce que l'ensemble des données et fichiers destinés à identifier ses clients et ses propres sites internet soient protégés de manière appropriée contre le vol et les consultations et modifications non autorisées.

L'établissement limite le nombre maximum de tentatives fautives d'identification après lesquelles l'accès au service internet est bloqué de manière temporaire ou définitive, ainsi que la durée maximum au terme de laquelle les sessions internet ouvertes mais inactives sont interrompues (généralement 15 minutes maximum). L'établissement dispose d'une procédure sécurisée permettant de déverrouiller les accès qui ont été bloqués.

3.2.4. Protection et sécurité des opérations

Afin de garantir la confidentialité des opérations entre l'ordinateur du client et l'établissement financier, ce dernier utilise des techniques d'encryptage solides et généralement reconnues.

L'établissement dispose de contrôles techniques d'authenticité (par exemple des *message authentication codes* (MAC), …) afin de détecter les modifications accidentelles des opérations de clients à la suite de perturbations techniques.

L'établissement dispose par ailleurs de solutions appropriées et efficaces en matière de sécurité et/ou de *monitoring* permettant d'empêcher ou de détecter avec un degré de probabilité élevé les opérations frauduleuses avant qu'elles soient effectuées. Parmi les exemples de solutions de sécurité efficaces sur ce plan figurent les mots de passe à usage unique ou signatures électroniques créés à partir de caractéristiques pertinentes de l'opération effectuée par le client (par exemple le montant et/ou une partie du numéro de compte du bénéficiaire) ou les solutions de haute qualité de type *dual channel*[9] qui permettent de confirmer l'opération internet du client par l'intermédiaire d'un canal de communication secondaire indépendant (par exemple un téléphone portable). Les services internet aux entreprises et aux professionnels font en outre souvent appel à des séparations de fonctions intégrées à l'application internet, séparations de fonctions en vertu desquelles l'opération à effectuer doit être encodée et/ou approuvée par plusieurs personnes (principe de l'*independent checker* ou *validator*).

L'établissement vérifie de manière appropriée, pour toute opération de clients[10], en fonction de la nature et du risque de l'opération, l'identité du client et les autorisations dont il bénéficie.

3.2.5. Sécurité des applications et serveurs internet

Dans le développement et la maintenance des applications internet, l'établissement reste suffisamment attentif aux points suivants :

- les caractéristiques et risques de sécurité de l'architecture applicative utilisée et des techniques et routines de programmation qu'il utilise, afin de réduire autant que possible la vulnérabilité de

[8] Certificats SSL « Extended Validation » contenant au minimum un encryptage 128 bits et établis par des organismes de certification réputés et généralement acceptés.

[9] C'est-à-dire des solutions de type *dual channel* dans lesquelles le canal de communication secondaire n'est pas exposé aux mêmes risques que le premier. Comme un nombre toujours croissant de canaux de communication se connectent à l'internet et recourent aux technologies de l'internet, l'indépendance des deux canaux de communication doit être réévaluée au moins tous les ans.

[10] L'établissement est autorisé à rassembler plusieurs opérations « clients » similaires, à condition que cela ne porte pas préjudice au nécessaire degré élevé de sécurité des opérations.

l'application face aux attaques malveillantes (par exemple *session hijacking*, *SQL injection*, *cross site scripting*, *buffer overflows*, …) ;
- les conséquences, en matière de sécurité du côté du client, des choix technologiques opérés par l'établissement (par exemple l'utilisation d'applications multimédias, de *plug-ins*, de liens vers des sites tiers, …).

Il importe à cet égard que tant les développeurs des applications que les gestionnaires des passerelles contrôlées entre l'internet et l'infrastructure informatique interne (cf. point 2.2.3.) disposent d'une connaissance solide concernant l'organisation et le fonctionnement des différents lignes de défense (*defense in depth*)[11], et l'interaction entre eux.

Pour le reste, la sécurité des sites et des serveurs internet transactionnels doit répondre aux mêmes exigences que les sites internet publics (cf. le point 2.2.4).

3.2.6. Communication avec les clients

Bien que l'utilisation de solutions technologiques soit nécessaire pour la sécurisation des services financiers sur l'internet, ces solutions ne suffisent généralement pas à garantir cette sécurité. L'utilisation, par le client, des technologies et applications mises à sa disposition, ainsi que sa prise en charge de la sécurité de l'ordinateur ou de l'infrastructure informatique qu'il utilise, constituent en effet souvent les maillons les plus faibles de la chaîne de sécurité.

À cet égard, l'établissement élabore pour le client des manuels simples et accessibles qui informent le client de ses responsabilités pour une utilisation sûre des services internet fournis.

Parmi les aspects à prendre en compte à cet égard figurent :
- la nécessité pour le client de garder secrets les codes d'authentification ou codes PIN ;
- les règles en matière d'utilisation correcte et sûre de tout le matériel informatique et de tous les logiciels utilisés par le client (ordinateur du client, ...) ;
- les procédures à suivre en cas de vol ou de perte des données utilisateurs secrètes ou du matériel et des logiciels liés aux clients qui sont nécessaires pour accéder aux applications et effectuer des opérations ;
- la procédure à suivre lorsque' on constate ou que l'on soupçonne un abus ;
- la politique menée par l'établissement en matière d'envoi de courriels ou d'autres messages électroniques aux clients (par exemple *instant messaging*, SMS, …).

L'établissement dispose en outre d'une politique de communication adaptée pour les cas où il s'agit d'informer à temps la clientèle de nouvelles évolutions et de nouveaux points d'attention en matière d'utilisation sûre, par le client, des services internet fournis, et/ou de sensibiliser les clients à ces aspects.

3.2.7. Réalisation d'examens indépendants en matière de sécurité

Les établissements qui utilisent l'internet à des fins transactionnelles (par exemple pour conclure des polices d'assurance, pour transmettre des instructions de paiement et/ou effectuer des opérations boursières, ...) et/ou qui permettent à leurs clients de consulter des informations confidentielles, font analyser la sécurité de leurs services internet transactionnels par un expert indépendant avant le lancement de ces services, puis font effectuer des analyses spécialisées indépendantes en matière de sécurité en fonction de l'évolution des menaces ou des modifications technologiques ou fonctionnelles apportées aux services internet fournis. Les tests réalisés comprennent tant des tests de pénétration[12] que des tests d'application[13] pour les différents types d'attaques en ligne.

Les exigences en matière de compétence et d'indépendance des experts auxquels il est fait appel sont identiques à celles qui sont exposées dans le point 2.2.9.

---

[11] La *defense in depth* est une stratégie de sécurisation qui consiste à placer plusieurs lignes de défense dans l'objet à défendre ainsi que sur son pourtour. Toute intrusion qui aurait percé la première ligne de défense est prise en charge par la ligne suivante.

[12] Un test de pénétration porte sur la sécurité du périmètre de l'infrastructure informatique propre.

[13] Il s'agit d'un test d'*application cracking* visant à vérifier si l'application est vulnérable sur le plan des attaques de type *SQL injection*, *cross site scripting*, *buffer overflows*, etc.

3.2.8. Participation à des services usuels de paiement par internet fournis par des tiers

Les établissements financiers qui permettent à leurs clients de participer, par l'intermédiaire de leurs solutions de sécurité internet et/ou de leur infrastructure internet, à des services usuels (internationaux) de paiement par internet fournis par des tiers (par exemple des paiements *3D secure*) développent en la matière une politique d'acceptation qui soit attentive aux points suivants :

- la réputation ainsi que la solidité financière et opérationnelle du prestataire de services de paiement par internet ;
- la nature et les risques des aspects des services de paiement fournis pris dans leur ensemble (montants, bénéficiaires, ...), compte tenu des solutions et/ou des possibilités de sécurité fournies ;
- la délimitation des responsabilités entre les parties concernées pour la sécurité des opérations et la compensation au client en cas d'abus et/ou de litige ;
- le statut (de contrôle) légal du prestataire des services de paiement par internet ;
- les éventuels risques de réputation pour l'établissement financier.

La direction effective (en règle générale, le Comité de direction) approuve la politique d'acceptation et veille à son respect. L'établissement veille en outre annuellement à une bonne analyse et à un bon suivi des menaces pour les services de paiement par internet tiers qu'il a acceptés, compte tenu des solutions de sécurité utilisées.