COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Luxembourg, le 11 mars 2011

A tous les établissements soumis à la surveillance de la CSSF*

CIRCULAIRE CSSF 11/504

Concerne : Fraudes et incidents dus à des attaques informatiques externes

Mesdames, Messieurs,

Au regard de l'apparition régulière de nouvelles attaques informatiques externes pouvant mener à des fraudes ou incidents, la CSSF estime utile de dresser un bilan régulier de la situation afin :

- de suivre l'évolution du phénomène d'une manière plus rapprochée,
- de pouvoir renseigner les établissements surveillés sur les types et la fréquence des attaques,
- d'anticiper autant que possible les cycles en relation avec les phases d'attaque, ainsi que les conséquences probables pour la place financière,
- de contribuer à une meilleure protection de l'activité de la place financière par des recommandations adaptées aux incidents rapportés.

A cet effet, la CSSF demande à tous les établissements sous sa surveillance de lui rapporter dans les meilleurs délais toutes les fraudes et tous les incidents dus à des attaques informatiques externes et de tenir de leur propre initiative cette information à jour après la date du rapport en question.

La présente circulaire entre en vigueur avec effet immédiat.

Veuillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments distingués.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Claude SIMON	Andrée BILLON	Simone DELCOURT	Jean GUILL
Directeur	Directeur	Directeur	Directeur général

Annexe : Incidents et informations à rapporter

* La circulaire est uniquement applicable aux entités 2 e) to j) de la section 1.1 de la circulaire CSSF 24/847

Annexe : Incidents et informations à rapporter

1. Nature des incidents à rapporter

Un incident est considéré comme à rapporter à partir du moment où une attaque effective a pu aboutir (ex : tentative de détournement avérée, système informatique corrompu) et ce même si l'attaque n'a pas conduit à une fraude (ex : absence de détournement effectif de fonds).

Il est à noter que les attaques de type « phishing » sont exclues du périmètre et ne sont donc pas à rapporter.

2. Services potentiels visés par les attaques

Bien que les services financiers par Internet soient des cibles privilégiées des attaques informatiques, ces dernières peuvent également viser d'autres types de service ou activité interne. Sont donc concernés par les rapports toute fraude ou incident découlant d'une attaque informatique externe en relation avec :

a) Les services financiers par Internet comprenant tous les services offerts en ligne par un établissement luxembourgeois, via Internet, par voie directe ou indirecte, à la clientèle privée ou professionnelle indépendamment du fait que la plateforme informatique soit opérée par l'établissement lui-même ou par un tiers.

La voie directe concerne les services financiers en ligne offerts directement à la clientèle privée ou professionnelle pour la gestion de leurs avoirs. Par voie indirecte, il faut comprendre les services utilisés par des professionnels ou par le personnel de l'établissement pour la gestion d'un ou plusieurs clients.

Ne sont donc pas uniquement concernés les établissements proposant des services de e-banking ou e-brokerage en ligne à la clientèle privée, mais également les établissements qui ont mis en place une gestion ou un accès en ligne pour leurs gestionnaires ou qui mettent un pareil dispositif aux services d'autres professionnels agissant pour compte d'un ou de plusieurs clients.

b) Tout autre service ou activité interne ou externe des établissements surveillés, afin d'inclure dans le périmètre les attaques par Internet portant par exemple sur le réseau interne, des serveurs internes ou encore sur les échanges de données entre un établissement et un tiers (partenaire, correspondant, maison-mère, sous-traitant,…).

3. Informations à rapporter

Le rapport à envoyer à la CSSF contient une description de l'incident (points a–f, et selon le cas les points g et h ou i et j en sus) :

a) le type d'incident ou de fraude accompagné d'une description,
b) le montant total du préjudice s'il peut être déterminé, avec indication de la répartition sur la période :
   - montant total des transactions frauduleuses, tous cas confondus,
   - montant total du préjudice pour les clients,
   - montant minimum et maximum du préjudice individuel,
   - montant total du préjudice pour l'établissement, y compris les frais administratifs et judiciaires, l'application de mesures correctrices et le remboursement éventuel au client.
c) une indication par incident ou fraude si l'établissement a porté plainte auprès des instances judiciaires,
d) toute autre information marquante, y compris de nature technique, susceptible d'aider à la compréhension de l'incident ou de la fraude,
e) la classification de l'incident par l'établissement (ex : mineur, significatif, majeur, critique) en précisant le positionnement sur l'échelle de classification utilisée (ex : incident classé « 2-significatif » sur une échelle allant de 1 à 4),
f) les mesures éventuelles prises par l'établissement pour compenser ou réduire les risques.

Concernant les fraudes ou incidents découlant d'une attaque informatique externe en relation avec des services financiers par Internet, les informations additionnelles à rapporter sont les suivantes :

g) la nature et le nom du service Internet en ligne concerné avec indication des spécificités (consultatif, transactionnel, gestion mono- ou multi-clients, clientèle privée et/ou professionnelle, accès par le client ou accès par le gérant/employé, plateforme informatique propre ou partagée, en interne ou sous-traitée [avec indication du sous-traitant] …),
h) le nombre de clients concernés par chaque type d'incident ou de fraude sur la période indiquée.

Concernant les fraudes ou incidents découlant d'une attaque informatique externe en relation avec tout autre service ou activité interne ou externe des établissements surveillés, les informations additionnelles à rapporter sont les suivantes :

i) la nature et le nom de la (des) cible(s) technique(s) (serveur, flux…) et du (des) service(s) ou activité(s) concerné(s) avec indication des spécificités (plateforme informatique propre ou partagée, en interne ou sous-traitée [avec indication du sous-traitant] …),
j) la nature et le nombre des utilisateurs directs ou indirects concernés par chaque type d'incident ou de fraude sur la période indiquée (un utilisateur peut être ici un client, un employé ou service interne, un partenaire, une entité du groupe,…).