



Dépôt de plainte

Pour plus de sécurité, adoptez les réflexes CASES !

Table des matières

1. Responsabilité de l'auteur de l'attaque
2. Que faire en cas d'attaque

L'insécurité informatique n'entraîne pas uniquement des risques techniques et économiques, elle est également une source de responsabilité civile et pénale pour les auteurs d'infractions informatiques.

Cette fiche a pour objet de présenter les risques et sanctions qui pèsent sur les auteurs d'attaques informatiques, ainsi que quelques conseils aux victimes sur la marche à suivre en cas d'attaque.



1

Responsabilité de l'auteur de l'attaque

La responsabilité de l'auteur d'une attaque informatique est d'abord d'ordre pénal. La loi réprime en effet certains actes commis à l'aide d'un ordinateur, et notamment :

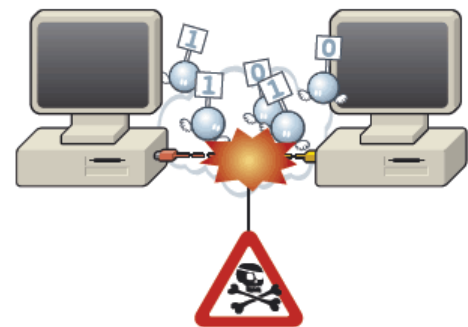
L'ACCES ILLEGAL A UN SYSTEME

L'accès illégal à un système vise le fait de **s'introduire et de se maintenir intentionnellement et frauduleusement** dans un système de traitement ou de transmission automatisé de données (STAD), par exemple :

(A) en utilisant directement un ordinateur (après s'être introduit dans les locaux d'une entreprise par exemple); où

(B) à distance, en entrant dans un réseau fermé ou prenant le contrôle d'une machine située dans un tel réseau.

Cette incrimination vise notamment le fait pour un employé d'utiliser un ordinateur mis à disposition



par son employeur pour accéder à des données confidentielles sans relation avec ses fonctions, ou

encore pour commettre un délit (par exemple, utiliser les ressources de l'entreprise pour diriger une attaque contre des tiers).

Ce que dit le texte: « Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de deux mois à deux ans et d'une amende de 500 euros à 25 000 euros ou de l'une de ces deux peines » (article 509-1 du Code pénal).

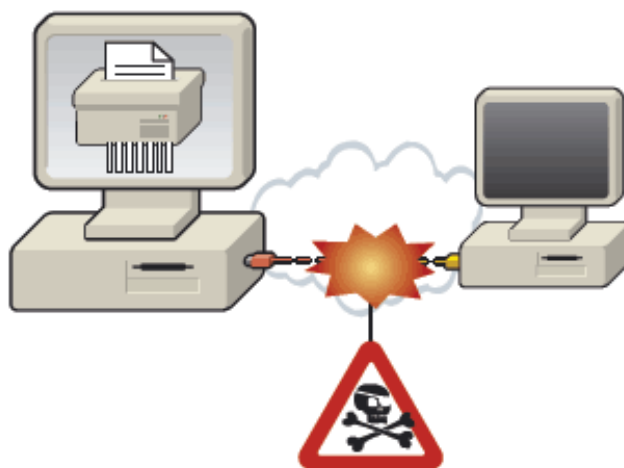
LA MODIFICATION OU SUPPRESSION DE DONNEES

La modification ou suppression de données est le fait de modifier ou de supprimer des données lors d'un accès illégal est une circonstance aggravante. Les peines minimales encourues sont donc encore plus importantes. Sont ici visés par exemple :

(A) le vandalisme informatique, c'est-à-dire l'accès à un système en vue d'en détruire les données ; ou encore

(B) l'étudiant qui **accède illégalement** au serveur de son école ou université et change ses notes ou celles de ses camarades.

Le fait d'introduire, de modifier les données d'un système ou son mode de traitement ou de transmission sans qu'il y ait eu accès illégal au



système est également passible de sanctions pénales.

Ce que dit le texte:

- Pour la modification ou suppression de données lors d'un accès illégal à un système : « Lorsqu'il [...] sera résulté [de l'accès illégal au système] soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, l'emprisonnement sera de quatre mois à deux ans et l'amende de 1 250 euros à 25 000 euros » (article 509-1, alinéa 2 du Code pénal).
- Pour la modification ou suppression de données sans accès illégal à un système : « Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement ou de transmission automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission, sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines » (article 509-3 du Code pénal).

L'ENTRAVE AU FONCTIONNEMENT D'UN SYSTEME

L'entrave au fonctionnement d'un système est également passible de sanctions pénales. Sont ici visés par exemple :

(A) le fait de **bloquer un système** en s'arrogeant des droits d'administrateur et en utilisant ces privilèges pour empêcher l'utilisateur légitime d'utiliser le système dans des conditions normales ;

(B) le fait de modifier ou d'altérer le fonctionnement du système et de **provoquer ainsi une baisse des performances, une altération des résultats**, etc. (par exemple par l'introduction volontaire et consciente d'un virus dans le système) ; ou encore



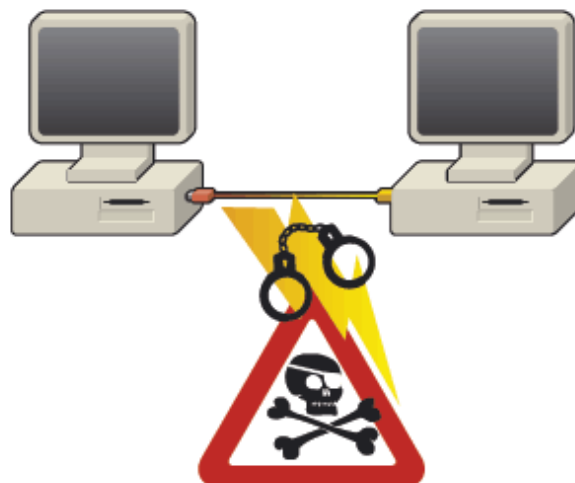
(C) le fait de détériorer ou détruire un système (au niveau matériel et/ou logiciel).

Ce que dit le texte: « Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement ou de transmission automatisé de données sera puni d'un emprisonnement de trois mois à trois ans et d'une amende de 1 250 euros à 12 500 euros ou de l'une de ces deux peines » (article 509-2 du Code pénal).

LA TENTATIVE

Il n'y a pas que lorsque l'attaque réussit que des sanctions pénales sont encourues. Le simple fait de tenter de commettre les infractions ci-dessus, même sans y parvenir, est répréhensible. Les *script-kiddies* et autres hackers débutants encourrent donc les mêmes peines que les hackers professionnels.

Ce que dit le texte: « La tentative des délits prévus par les articles 509-1 à 509-5 est punie des mêmes peines que le délit lui-même » (article 509-6 du Code pénal).



L'ASSOCIATION DE MALFAITEURS

INFORMATIQUES: le fait pour des personnes de s'associer ou de s'entendre en vue de commettre une des infractions ci-dessus est également puni, indépendamment du fait qu'une attaque ait finalement eu lieu ou pas. C'est le cas par exemple de ceux qui s'échangent des moyens de commettre une attaque (un ordinateur, un accès à un réseau ou même des logiciels, scripts ou informations permettant de commettre une attaque informatique) et planifient une attaque concertée sur un tiers.



Ce que dit le texte: « Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou de plusieurs infractions prévue par les articles 509-1 à 509-5 sera punie des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée » (article 509-7 du Code pénal).

La responsabilité de l'auteur d'une attaque informatique est ensuite d'ordre civil. En effet, lancer une attaque informatique contre quelqu'un ou contre une entreprise constitue une faute et ouvre le droit pour la victime à la réparation du préjudice qu'elle a subi en relation avec cette faute. La réparation de ce préjudice se fait selon les règles de la responsabilité civile (articles 1382 et suivants du Code civil).

La première chose à faire pour la victime est de recueillir des preuves en vue des suites judiciaires qu'elle entend donner à l'attaque dont elle a fait l'objet. Si la victime fait appel à une entreprise spécialisée en vue de réparer les dommages causés par l'attaque (par exemple, récupérer les fichiers détruits), le rapport de cette intervention pourra s'avérer précieux lors de la phase judiciaire. Il devra donc être le plus détaillé possible.

A. DEPOT DE PLAINTÉ

La victime d'une attaque informatique peut porter plainte, soit en se déplaçant dans un commissariat de police, soit par écrit au procureur d'Etat (voir encadré).

La plainte doit :

- (i) **énoncer clairement les faits**, de manière chronologique ;
- (ii) **inclure tout détail utile** (par exemple, qui possédait le mot de passe du système, qui a utilisé le système en dernier, etc.) ; et
- (iii) **décrire** (brièvement) **les dommages causés** par l'attaque (perte de données, système rendu inutilisable).

Il n'est pas nécessaire, à ce stade, de chiffrer de manière précise le préjudice, mais il peut être utile d'inclure une estimation (en prenant soin de préciser que cette estimation est faite sous toutes réserves) par exemple sur la base du temps perdu pour réparer le système et reconstituer les données endommagées.

Une fois les preuves recueillies, la victime peut envisager des suites judiciaires. A ce titre, la victime d'une attaque informatique a la choix entre :

- (a) **porter plainte** et laisser au Ministère Public le soin de poursuivre les auteurs ;
- (b) **se constituer partie civile** en vue d'obtenir réparation du préjudice subi ; et
- (c) poursuivre elle-même les auteurs (si ceux-ci sont connus) **en procédant à une citation directe**.

Il n'est pas non plus nécessaire de qualifier juridiquement les faits, c'est-à-dire de préciser quelles infractions ont été commises ou quels textes sont applicables : ces tâches reviennent au Ministère Public. Le plaignant peut néanmoins mentionner l'une ou l'autre incrimination ou l'un ou l'autre texte qu'il considère applicable (en prenant soin de préciser que cette indication est faite sous toutes réserves).

Il n'est enfin pas nécessaire pour porter plainte de connaître l'identité de l'auteur de l'attaque, ni même d'avoir des soupçons sur telle ou telle personne. En vertu du principe d'opportunité des poursuites, il revient ensuite au Ministère Public de décider si une instruction et des poursuites doivent être initiées. Le cas échéant, le Ministère Public peut décider de classer l'affaire sans suites.

Il faut porter plainte auprès du procureur d'Etat du lieu où l'infraction a été commise :

Pour l'arrondissement judiciaire de Luxembourg (cantons de Luxembourg, Capellen, Esch, Grevenmacher, Mersch et Remich)
Procureur d'Etat
Palais de Justice de Luxembourg
B.P.15
L-2010 Luxembourg

Pour l'arrondissement judiciaire de Diekirch (cantons de Diekirch, Clervaux, Echternach, Redange, Vianden et Wiltz)
Procureur d'Etat
Tribunal d'Arrondissement de Diekirch
B.P. 164
L-9202 Diekirch

B. PLAINTE AVEC CONSTITUTION DE PARTIE CIVILE

La constitution de partie civile est un acte formel par lequel la victime manifeste son intention de réclamer réparation pour le dommage qu'elle a subi en relation avec une infraction. Cela peut être le cas, par exemple, lorsqu'un pirate informatique est parvenu à détruire des données sur le système informatique d'une entreprise et qu'il en est résulté un préjudice pour celle-ci.

Le plaignant qui se prétend lésé par une attaque informatique et qui désire provoquer l'ouverture d'une instruction pour amener les autorités à enquêter sur les faits dont il a été la victime peut déposer une plainte avec constitution de partie civile.

Il faut se constituer partie civile auprès du juge d'instruction (article 56 du Code d'instruction criminelle).

Pour l'arrondissement judiciaire de Luxembourg (cantons de Luxembourg, Capellen, Esch, Grevenmacher, Mersch et Remich)
Cabinet d'instruction Palais de Justice de Luxembourg
B.P.15
L-2010 Luxembourg

Pour l'arrondissement judiciaire de Diekirch (cantons de Diekirch, Clervaux, Echternach, Redange, Vianden et Wiltz)
Cabinet d'instruction Tribunal d'Arrondissement de Diekirch
B.P. 164
L-9202 Diekirch

La constitution de partie civile diffère du dépôt de plainte en ce que :

(i) elle a pour effet de déclencher l'action publique ;
(ii) elle oblige le plaignant (c'est-à-dire, la victime) à consigner une somme que le juge d'instruction détermine, correspondant aux frais présumés de la procédure ; et

(iii) si le plaignant "succombe", c'est-à-dire n'obtient pas gain de cause, il peut se voir condamner à supporter les frais de procédure (en tout ou partie).

C. CITATION DIRECTE

La citation directe est la procédure par laquelle la victime et l'action publique en mouvement et saisit directement la juridiction de jugement. En procédant par voie de citation directe, la victime poursuit l'auteur présumé d'une infraction devant le tribunal, sans enquête ni instruction préalables du Ministère Public ou du juge d'instruction.

Une conséquence pratique importante de l'absence d'instruction de l'affaire est que le plaignant doit apporter lui-même l'ensemble des preuves au tribunal. Il importe donc de préparer un dossier complet et convaincant, ce qui peut s'avérer complexe.

Evidemment, la citation directe n'est possible que lorsque l'auteur présumé de l'attaque est connu.

Il est important de noter qu'il n'est plus possible de procéder par voie de citation directe lorsqu'une constitution de partie civile a déjà été effectuée.

Retrouvez les dossiers, fiches thématiques, alertes et actualités sur:

www.cases.lu

CASES 2008/09