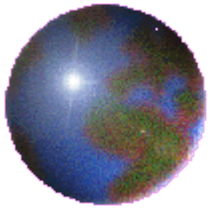
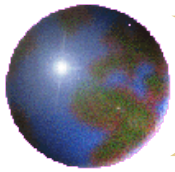


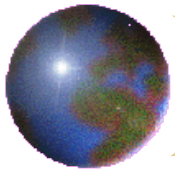
Administration réseau et sécurité : Les aspects juridiques

Denis Pugnère
CNRS / IN2P3 / IPNL
d.pugnere @ ipnl.in2p3.fr



Avant propos

- Je ne suis pas juriste
- Le droit évolue
- Les questions relatives aux droits au CNRS sont traitées par la DAJ



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

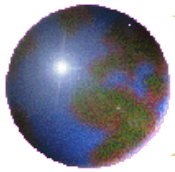
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Cas d'école

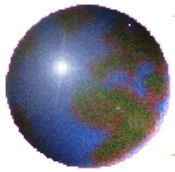
- Contexte
  - Un serveur web d'un laboratoire est compromis,
  - Il est utilisé pour diffuser un faux site bancaire (phishing),
  - Suite à une campagne de SPAM, des internautes déposent leurs accès (n° CB, login+password...) sur ce faux site,
  - Des dépôts de plaintes ont été faits
  - Des officiers de police judiciaire arrivent dans le laboratoire
  - ...
  - Autres cas : PC Zombies, DDoS, consultation de sites illégaux

Responsabilité de l'ASR[1] ? du CSSI[2] ? du directeur du laboratoire ?

De quoi sommes nous responsables juridiquement ?

[1] : ASR = Administrateur système et réseaux

[2] : CSSI = Chargé de la sécurité des Systèmes d'Information



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

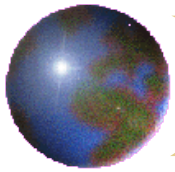
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

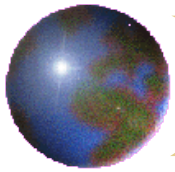
Informer / Contrôler, tracer / Agir, réagir

Bibliographie



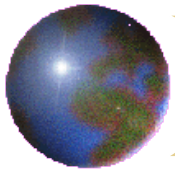
Quelques questions

- Documents nous étant applicables (chartes, guides, décrets, circulaires, recommandations, délibérations)
  - Avons nous une obligation de résultat ? De moyens ?
- Responsabilités de l'ASR et du CSSI ? Vis à vis du directeur d'unité.
  - Concernant le traitement des avis de sécurité et de l'application de la SSI ?
  - Si une mise à jour n'est pas appliqué dans les temps ?
  - Concernant la perte de données :
    - erreur de configuration,
    - Panne matérielle,
    - Avec une une restauration de données impossible
- Nécessité de porter plainte pour se couvrir : Qui porte plainte ?
- Quel canal de communication entre l'ASR et les personnels du laboratoire ?
  - Canal officiel ?
  - Comment prouver qu'un utilisateur a bien été informé ?



Quelques questions

- Gestion des données des utilisateurs
  - Accès aux données
    - en présence de l'utilisateur ?
    - en absence de l'utilisateur ?
  - Fin de compte des personnes : que faire des données ?
  - Les données ont un statut personnelles ? Professionnelles ?
  - Accès en monitoring / télémaintenance sur les postes clients ?
- Responsabilité et attitude vis-à-vis de la découverte de contenus illicites ?
- Dans l'exploitation du parc et du réseau
  - Droit de refuser la connexion d'un poste nomade sur le réseau local ?
  - Si il ne réponds pas aux exigences de sécurité ?



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

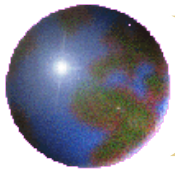
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie

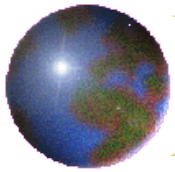


Que dit la PSSI du CNRS ?

- Quelle est la place de l'ASR dans la SSI ?

  Page 20 on parle de l'administration des serveurs.. on serait donc « responsable » de l'administration des serveurs.. point !

  Page 7 la PSSI dit que : ***« Protection juridique :*** *la mise en oeuvre des systèmes d'information s'inscrit dans un cadre législatif et réglementaire destiné en particulier à protéger les droits de propriété intellectuelle et industrielle et ceux de la vie privée (fichiers nominatifs, cybersurveillance…). Dans ce cadre, la responsabilité administrative et pénale de la hiérarchie et des administrateurs systèmes et réseaux peut être recherchée. »*



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

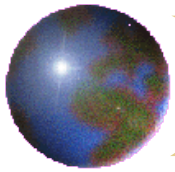
Bibliographie

Politique de gestion de traces du CNRS

Le CNRS a besoin d'enregistrer systématiquement certaines traces générées par les postes de travail, les serveurs, les équipements d'extrémité (routeurs, pare-feux, commutateur, borne d'accès, …), les équipements de surveillance du trafic réseau (IDS, antivirus, antispam, ...), certaines applications spécifiques, etc.

L'organisme a publié une « Politique de gestion de traces » afin :

- **d'assurer la métrologie du réseau** : réguler l'utilisation des ressources, détecter des anomalies afin de mettre en place de la qualité de service, faire évoluer les équipements en fonction des besoins ;
- **Vérifier que les règles** en matière de SSI sont correctement respectées et que la sécurité des systèmes d'information et du réseau telle qu'elle a été définie par la politique de sécurité de l'unité est assurée ;
- **Détecter toute défaillance** ou anomalie de sécurité, volontaire ou accidentelle, passive ou active, d'origine matérielle ou humaine ; Détecter toute violation de la loi ou tout abus d'utilisation des moyens informatiques pouvant engager la responsabilité du CNRS ;
- **Mettre à l'abri les preuves** nécessaires aux enquêtes en cas d'incident de sécurité et pouvoir répondre à toute réquisition officielle présentée dans les formes légales.



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

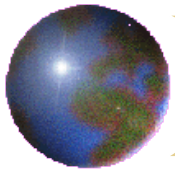
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



La réponse à la question ?

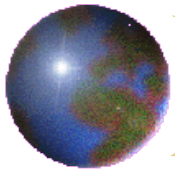
- Il n'y a aucune réponse définitive aux questions de responsabilité
- Aucun glossaire précis des responsabilités
- Nous sommes en présence « d'environnements juridiques » relatifs à la SSI

La question

Quelles sont nos responsabilités juridiques ?

Devient

Être sensibilisé à la Responsabilité et savoir ce que signifie la Responsabilité en terme de Droit ?



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

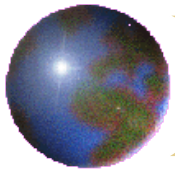
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Le statut d'opérateur ?

« Les personnes qui, au titre d'une activité professionnelle principale ou accessoire, offrent au public une connexion permettant une communication en ligne par l'intermédiaire d'un accès au réseau, y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques en vertu du présent titre »

Loi Sarkosy article 5

=> Nous sommes tous des Opérateurs de communications électroniques

LCEN : Loi pour la confiance dans l'économie numérique

La nouvelle définition des hébergeurs englobe désormais les organisateurs de **forum de discussion sans modérateur** qui, au même titre que les hébergeurs « classiques », bénéficient d'une responsabilité civile et pénale limitée.
Le texte impose aux hébergeurs "*une certaine discipline*" sur les pages qu'ils stockent ou les messages qui sont échangés, afin d'empêcher la diffusion d'informations "*faisant l'apologie des crimes de guerre ou des crimes contre l'humanité, incitant à la haine raciale, ou ayant un caractère pédophile*". Mais **il ne s'agit pas d'une "*obligation générale de surveiller les informations qu'ils transmettent ou stockent, ni [une] obligation générale de rechercher des faits ou des circonstances révélant des activités illicites*"**, stipule l'alinéa 7 de l'article 6.

Encadrement strict de la responsabilité civile : selon l'article 6 alinéa 2, les "*personnes physiques ou morales [...] ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits [...]*"

Obligation d'information sur les moyens techniques pour filtrer certains contenus : L'article 6 affirme par ailleurs que "*les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens*".

LCEN : le courrier électronique

La LCEN redéfinit la notion de « courrier électronique » :

« *On entend par courrier électronique 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* ». La notion englobe donc « l'utilisation du « chat », de la vidéoconférence ou de la téléphonie vocale sur Internet. Seront également visés les messages de type SMS, les messages laissés sur les répondeurs téléphoniques ou sur des boîtes vocales de GSM …

Cour d'appel de Paris 11ème chambre 17 décembre 2001

« Ne constituent pas une interception la lecture et la retranscription de messages dès lors que celles-ci ne nécessitent ni dérivation ou branchement et sont effectuées sans artifice ni stratagème ».

« Il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne entre autre, qu'ils aient accès aux messageries et à leur contenu »

« Par contre, la divulgation du contenu des messages, et notamment du dernier qui concernait le conflit latent dont le laboratoire était le cadre, ne relevait pas de cet objectif »

C. Appel de Bordeaux chambre sociale 4 juillet 2003

Le courrier électronique d'un salarié est considéré comme une correspondance privée quant il est **émis et reçu à partir du poste informatique du salarié**, même si l'employeur a interdit l'usage de la messagerie à titre privé et que l'adresse utilisée est une adresse générique de la société.

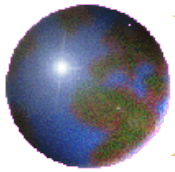
LCEN : le secret professionnel

Le secret professionnel et les obligation de révélation d'infraction (Art. 40 al 2 du Code de procédure pénale)

Toute autorité constituée, tout officier public ou fonctionnaire qui **dans l'exercice de ses fonctions**, **acquiert la connaissance d'un crime ou d'un délit** est tenu d'en donner avis sans délai au procureur de la République et de transmettre à ce magistrat tous les renseignements procès-verbaux et actes qui y sont relatifs.

Réponse ministérielle à la question N°50674 (J.O.A.N du 24/02/92 p 903) Ministère attributaire : fonction publique

« Il est précisé à l'honorable parlementaire que cette disposition a une portée générale ; elle est donc de nature à délier le fonctionnaire de son obligation de secret professionnel y compris en cas de délit commis par un membre de sa hiérarchie dans l'exercice de ses fonctions ».



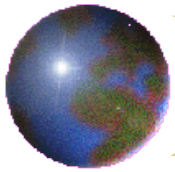
La CNIL : donnée à caractère personnel

~~Donné nominative~~ => L'article 2 de la loi modifiée définit ainsi une donnée à caractère personnel : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne ».

Au nouveau chapitre 2 relatif aux **« conditions de licéité des traitements de données à caractère personnel »**, les données à caractère personnel doivent remplir plusieurs conditions pour être licites (article 6 nouveau) :

- être collectées et traitées de manière loyale et licite,
- être collectées pour des finalités déterminées,
- être adéquates, pertinentes et non excessives face à leur finalité,
- être exactes, complètes et mises à jour,
- être conservées en respectant les délais de conservations.
- L'accent est mis sur le consentement de la personne concernée par la collecte et le traitement de ses données à caractère personnel (article 7 nouveau).

Tout traitement automatisé de donnée à caractère personnel, hormis les cas dérogatoires énumérés par la loi, **doit faire l'objet d'une déclaration préalable** auprès de la CNIL.



La CNIL : Exigence de sécurité

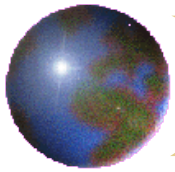
Exigence de sécurité des données personnelles

Article 34 nouveau.
Toute personne ordonnant ou effectuant un traitement d'informations nominatives s'engage de ce fait, vis à vis des personnes concernées, **à prendre toutes précautions utiles** afin de préserver la sécurité des informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisé.

Article 226-17 du Code Pénal.
Le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de **cinq ans d'emprisonnement et de 300 000 euros d'amende**.

Article 226-13 du Code Pénal : La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15000 euros d'amende.

=> Une erreur de sauvegarde entraînant la destruction de données ou une intrusion à l'origine de la divulgation publique d'informations protégées par la loi coûteront chers aux responsables concernés, y compris s'il s'agit d'une association de passionnés qui fait de l'hébergement libre.

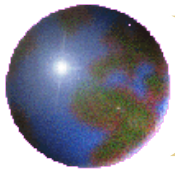


La CNIL : Obligations d'information

Obligation d'information des personnes élargie :

- Auparavant, les personnes auprès desquelles étaient recueillies des informations nominatives devaient seulement :
  - être informées du caractère obligatoire ou facultatif des réponses,
  - des conséquences d'un défaut de réponse,
  - des destinataires des données
  - d'un droit d'accès et de rectification.

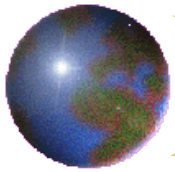
- **Dorénavant, elles doivent également être averties :**
  - des informations relatives à l'identité du responsable du traitement,
  - de la finalité poursuivie par le traitement,
  - du droit de s'opposer à ce que ces informations soient transférées à des tiers
  - des transfert, le cas échéant, de données envisagés vers un État non membre de la Communauté européenne.



La CNIL : ses pouvoirs

La CNIL a désormais le pouvoir de faire une enquête

- pouvoir d'opérer des vérifications sur place
- pouvoir d'aller n'importe où dans le SI
- pouvoir d'instrumentaliser la procédure
- pouvoir de condamner à une amende



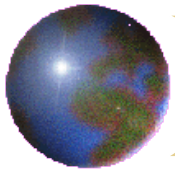
Les principes de la CNIL

Principes actuels :

- tous les éléments qui sont dans un bureau d'un employeur sont réputés professionnels... De ce fait l'employeur peut y avoir accès même en l'absence du collaborateur
- Tous les mails (messagerie électronique) sont réputés à caractère professionnel sauf si la mention [PERSONNEL] apparait dans le sujet
- face à une situation de risque on « peut » ouvrir de la correspondance privée pour des raisons de sécurité ou d'urgence
- En cas de “doute” sur utilisation des moyens qui “dépassent” la vie privée résiduelle : La direction peut faire appel à un juge des requêtes : ordonne à un huissier une intervention en urgence (48h).

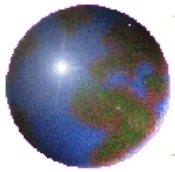
Quelques exemples : Cas du départ d'un personnel, que faire des données ?

- il est légitime de basculer sa boîte de Mails d'une personne vers une autre.
- Il est nécessaire d'informer et d'écrire dans les procédures d'ouverture et fermeture de compte que les données seront détruites ou transférées au Responsable au départ de l'utilisateur.
- De même il est nécessaire d'indiquer ce qui sera fait du répertoire [PRIVE] dans le règlement



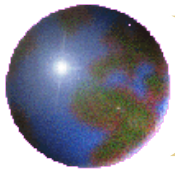
Loi Godfrain : Article 323-1

- Le fait **d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données** : 1 an, 30 000 €
- Lorsqu'il en est résulté soit la **suppression** ou la **modification de données contenues dans le système, soit une altération du fonctionnement de ce système** : 1 an, 45 000 €
- Exemples :
  - TGI, Paris, 25 fév.2000, Serge Humpich / GIE Cartes bancaires
    La mise en évidence des failles du système de sécurité des terminaux de paiement de CB, à travers la recherche et l'identification de l'algorithme de cryptage sur des systèmes inertes, caractérise l'accès et le maintien frauduleux dans un système de traitement automatisé des données .
  - CA, Paris, 30 oct. 2002, Antoine Champagne / Ministère Public, SA TATI " .
    Il ne peut être reproché à un internaute d'accéder aux données, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation ".
  - TGI, Le Mans, 7 nov.2003, Société SMITH et NEPHEW c/ L.
    " L'usage de fausses adresses électroniques ", pour envoyer des messages diffamatoires, sur les services d'une messagerie électronique " constituent de façon incontestable un moyen frauduleux d'accès dans le système de traitement automatisé des données ".



Loi Godfrain : Articles 323-2 à 323-7

- Article 323-2
  - Le fait d'**entraver ou de fausser le fonctionnement** d'un système de traitement automatisé de données : 5 ans et 75 000 €
  - Exemple : TGI, Le Mans, 7 nov.2003, Société SMITH et NEPHEW c/ L.
    L'envoi massif de courriels, afin de bloquer le serveur informatique d'une messagerie électronique, constitue une entrave au fonctionnement d'un système de traitement automatisé des données.
- Article 323-3
  - Le fait d'**introduire frauduleusement des données** dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient : 5 ans et 75 000 €
  - Exemple : 2003, NOOS contre Philippe P. pour atteinte illicite à un système (Mail Bombing). 4 mois de prison avec sursis et 20 000 € d'amende.
- L'article 323-7 indique que la **tentative** des délits est punie des mêmes peines



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

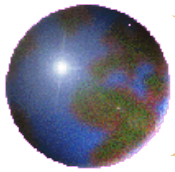
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

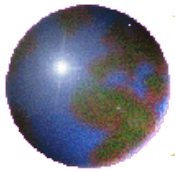
Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Éléments constitutifs de l'infraction

- L'éléments légal : violation de la loi sans application rétroactive
- L'élément moral : le caractère intentionnels de la violation de la loi.
- L'élément matériel : réalité des faits (pas seulement intention). Cela comprend :
  - la tentative,
  - la complicité,
  - l'association de malfaiteur



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

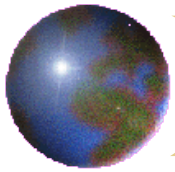
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

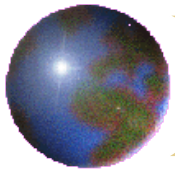
Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Scans de ports réseau

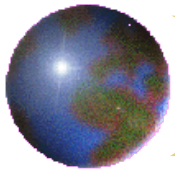
- Scan protocolaire = déterminer les protocoles fonctionnels (ICMP, TCP, UDP)
  - Faible risque de DoS, pas d'accès au SI, simple envoi de paquets pour réponse
- Scan de ports TCP, UDP : déterminer les ports ouverts, fermés, filtrés : pas de confirmation que le port est dédié à l'application supposée
  - Faible risque de DoS, pas d'accès au SI, simple envoi de paquets pour réponse
- Identification des services ainsi que leur version
  - Risque de DoS : Il y a transfert de données, requête et accès au service applicatif.



Tests d'intrusion

- Définition : Recherche de vulnérabilités et de l'exploitation de failles. Eventuellement test poussé jusqu'à compromission machines (direct ou par rebond).
- Risques :
  - Le déni de service
  - L'atteinte de confidentialité
  - Atteinte aux droit de propriété intellectuelle / industrielle
- Est-ce un accès illégal au Système de Traitement automatisé de données ?
- Légal par le biais d'une autorisation explicite (contrat, NDA) et respect des autorisations contractuelles

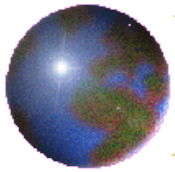
- **Détention de moyens de piratages : Et les logiciels de tests d'intrusion ?**
- Art.46 : Après l'article 323-3 du code pénal, il est inséré un article 323-3-1 ainsi rédigé : « Art. 323-3-1. - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, 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 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée. »



Écoute réseau

- Pas d'intrusion, mais écoute des informations transitant (mots de passe...)
  - Ecoute passive (Article 226-15 du code pénal) :
    Le fait, commis de mauvaise foi, **d'ouvrir**, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45000 euros d'amende.
    Est puni des mêmes peines le fait, commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises ou reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions.
  - Ecoute active : ajout d'information dans les paquets ou modification de certains messages => **Loi Godfrain**

Nécessité d'une autorisation même quand écoute passive



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

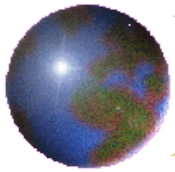
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Les responsabilités

- Types :
  - Responsabilité **Civile** (avec contrat liant les parties, hors contrat),
  - Responsabilité **pénale,**
  - Responsabilité **administrative,**
  - Responsabilité **personnelle,**
  - Responsabilité **partagée**
- Les responsabilités civiles et pénales sont couramment invoquées
- Peu de cas de jurisprudence en responsabilité administrative en SSI (sanctions disciplinaires)

Responsabilité civile

Articles 1382, 1383 et 1384 du Code civil: la faute directe, la négligence fautive et la faute du fait des autres.

Art. 1382 : *Tout fait quelconque de l'homme, qui cause un dommage à autrui, oblige celui par la faute duquel il est arrivé, à le réparer.*

En cas de faute, il faut réparer le dommage (exemple : téléchargement 7j/7, lecture d'un mail privé)

Art. 1383: *Chacun est responsable du dommage causé non seulement par son fait, mais encore par sa négligence ou par son imprudence.*

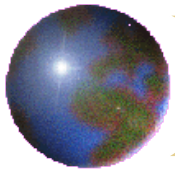
Cela concerne les fautes par négligence fautive ou l'imprudence de son propre fait

Exemple de négligence fautive (= « laisser faire ») sur un SI : si un hébergeur a connaissance d'un contenu illicite et qu'il ne fait rien pour l'enlever *(jurisprudence Cyberlex)*

Art. 1384 : *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde.*

Exemple: employeur responsable des agissements de ses employés. Enseignants, artisans sont responsables des fautes des élèves, apprentis sous leur garde.

La responsabilité de l'employeur est engagée lors d'un fait d'un salarié, lors d'un dommage ou d'un fait « commis dans le cadre de ses fonctions ». *(ex: jurisprudence "lucent")*

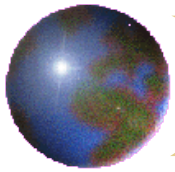


Responsabilité pénale

Concerne les délits de :

Contrefaçon, diffamation, Injures, Racisme, Révisionnisme, Incitation, ouverture correspondance privées, intrusion SI, Altération SI, Modification Suppression de données preuves, Mise à disposition, Enregistrement audio/vidéo sans autorisation, Diffusion et stockage d'image à caractère « pédophile »..., non déclaration à la CNIL, pas de notices Légale sur site Web etc...

Lors de l'accès aux données des utilisateurs, L'ASR a obligation de Confidentialité... Mais a obligation de “dénoncer” eu égard au Droit Pénal si on découvre des données illicites concernant la pédopornographie , le révisionnisme etc.

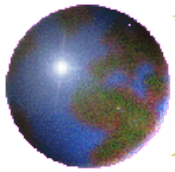


Responsabilité personnelle

La responsabilité personnelle pourrait être engagée dans quelques cas comme :

- refus illégitime d'accomplir un acte, ou
- manquement à une obligation.
- Faute professionnelle

Exemple : si on télécharge massivement des données à titre personnel, notre responsabilité personnelle est engagée



Responsabilité partagée

C'est le fait de déléguer une responsabilité pénale à quelqu'un.

Par exemple un chef d'Entreprise délègue sa responsabilité à un chef de chantier

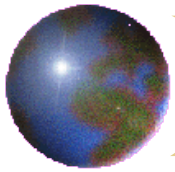
Il n'existe pas de délégation dans les organismes publics. L'ASR n'a pas de délégation pénale : il n'a pas la responsabilité de l'employeur au niveau pénal.

==> un Directeur d'unité ne peut pas déléguer sa Responsabilité sur le plan Pénal

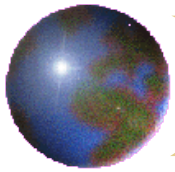
Pour qu'il y ait délégation de responsabilité pénale : il faut un document signé par la personne qui accepte la délégation. La personne doit avoir l'autorité et les moyens.

L'acte de Délégation DOIT définir ce sur quoi on fait porter la Délégation !

Si on n'a pas les moyens d'appliquer correctement une politique de sécurité, il faut l'indiquer PAR ECRIT! « Pour agir efficacement il me faut .... »



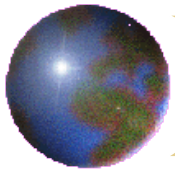
PLAN



Responsabilité : Facteurs de risques

Facteurs de risques pouvant impacter la responsabilité :

- Dans l'absence de mise en oeuvre
- Dans la mise en oeuvre
- Dans le fait de faire faire par un autre
- Le facteur humain (erreurs...)



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

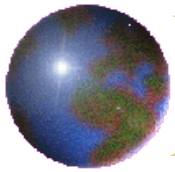
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Obligations d'informer, tracer, sécuriser

Jurisprudence tati : Un individu rentre dans le Si de tati... prend possession d'un répertoire client... jugement : “aucune méthode de piratage utilisée mais une manipulation "accessible à tout internaute averti »

=> Mauvaise sécurité du site, pas d'information, pas de frontière délimitant l'intranet... pas coupable !

Jurisprudence lucent : Site web « escroca » établi par un employé de lucent pendant ses heures de travail...

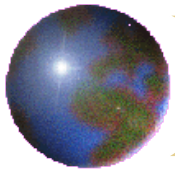
=> Diffamation, et responsabilité de l'employeur, « non charte »

Affaire “cyberlex” : Site web de cyberlex «comment (ne pas) payer sur l'internet » citait des logiciels qui génèraient des numéros de cartes bleues bidon. Le site condamne ces activités mais donnait sur son site 2 liens sur 2 logiciels.

le magazine « Que Choisir » : cite l'article et l'auteur est cité comme un *!$?? ... Cyberlex demande au magasine "Que Choisir?" de retirer l'article ou d'avoir un droit de réponse.. qui est refusé.

Procès plainte pour diffamation contre plainte pour « contrefaçon »

Jugement : on est dans un cas d'imprudence et de négligence fautive de la part de Cyberlex qui avait laissé des liens vers des sites de pirates, qui malgré l'objectif pédagogique, ont été jugés comme une «incitation au délit»



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie

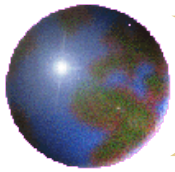
Données et ordinateurs personnels

Chambre sociale de la Cour de cassation a affirmé dans un arrêt du 17 mai 2005 :
« sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé ».

Notion de vie privée résiduelle : «espace» de vie privée au travail. Ex: C'est la possibilité de faire usage personnel de la messagerie et un dossier personnels.

Comment traiter une machine personnelle qu'on doit connecter dans le réseau du Laboratoire ? Au niveau du Laboratoire , il est nécessaire de *définir les règles du Jeu :*

- La considérer (ou pas) comme un élément qui fait partie intégrante du SI du Laboratoire. L'écrire dans le règlement
- Mettre en place des éléments de distinction entre vie privée personnelle ou professionnelle
- Ex: Indiquer le droit de brancher un portable personnel dans le réseau de l'entité ? Avec contrôle ? Sans contrôle ?
- Si contrôle : ils doivent répondre à des objectifs légitimes : exigence de sécurité, de prévention, gestion et optimisation des ressources, protection des intérêts de l'institution.



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

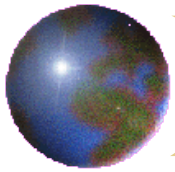
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Responsabilité et SSI

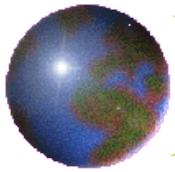
La donne est inversée en matière de responsabilité dans la sécurité des Systèmes d'Information : i.e; un intrus n'est un intrus que si on lui a donné “conscience” d'être un intrus.

En matière de SSI, pour sécuriser un espace privé il faut donc :

- *Bien entendu **sécuriser**, mais aussi*
- ***signifier** et mettre en place clairement les règles d'accès*...
- et **délimiter** les zones protégées (vous êtes sur un site privé...)

Sans quoi un intru peut se réfugier derrière le fait de ne pas savoir qu'il était en terrain “privé”. *(ex: jurisprudence tati)*. Par exemple :

- dans un intranet, il faut que les pages soient marquées comme « appartenant à l'intranet » ou confidentielles.
- Sur la bannière de login d'un serveur/routeur : indiquer que tout accès non autorisé est interdit



Les règles du jeu de la SSI

Les "bonnes pratiques" dans le cadre juridique de la SSI pour se prémunir de responsabilités civiles et pénale est de mettre en place le triptyque :

Information -> **Contrôle** -> **Action**

Dans un contexte de faute, un juge analysera si on a "informé", "contrôlé" et si on a "agit »

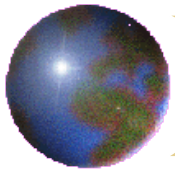
Nécessité cependant de PROUVER qu'on aura mis en place les éléments de la chaîne Information / Contrôle / Action ..... (preuves écrites archivées)

Pb : dans nos milieux Universitaires et Recherche il y a une faible culture de l'écrit administratif. On ne trace pas beaucoup par écrit les actions qui ont été entreprises.

- Il faut donc pour nous ASR tracer nos actions : rubrique sécurité sur notre site Web, main courante..., rapport annuel d'activités
- Montrer qu'on a informé et donc tout écrire : Par des alertes, des mises en gardes, par des mails où figurent les mots « Alertes », « Mises en garde »

Principes à retenir :

- **tryptique Information / Contrôle / Action**
- **politique de l'écrit**
- **traçabilité**



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

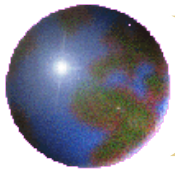
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



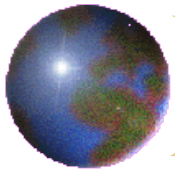
Informer

L'ASR, le RSSI se doit d'avertir, *de **renseigner, d'informer, de mettre en garde***, aussi bien le responsable légal, les autorités compétentes, et surtout les utilisateurs, des risques dont il a connaissance de préférence par écrit

- **Informer et former:** faire des rapports réguliers ou sur situation particulière de risque

  Alerte et conseil: En tant qu'experts sur un domaine technique classé « dangereux » les ASR sont tenus à une ***obligation de conseil renforcé***.
- Il peuvent émettre des **alertes** (sur des risques connus) ou des **mises en garde** (sur des risques possibles)...

La ***présence de ces mot-clés*** CONSEIL, MISE EN GARDE, ALERTE dans un rapport peut avoir un poids utile en cas de contentieux ultérieur



Contrôler, tracer

Depuis la LCEN le droit à TRACER les utilisateurs dans un SI est *total et complet, participer au maintien de la preuve : Collaboration et coopération (CNIL, DCRI..)*

On n'a plus à se demander si on a le droit de mettre en place les outils de contrôle pour :

- *Surveiller le réseau, les systèmes : outils de métrologie, de monitoring, de conservation et analyse des logs...*
- Effectuer des statistiques sur le débit, les sites consultés, la consultation du site du labo, la place occupée sur les disques, ...
- avoir des remontées en cas problème... etc...

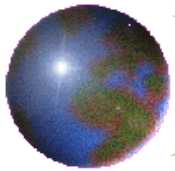
Respecter cependant la réglementation sur la conservation des traces et l'information et la vie privée résiduelle des utilisateurs

Les contrôles doivent répondre aux obligations légales de sécurité et de traçabilité: *exigence de sécurité, de prévention, gestion et optimisation des ressources, protection des intérêts de l'institution*.

Ex: En cas de téléchargement massif par un utilisateur, l'ASR a le droit de stopper le flux réseau. On peut couper un service *sans plus se poser la question du droit de le faire*, mais en informant largement ... la Direction, les utilisateurs

Si découverte de contenu illicite? :

En règle générale les administrateurs sont tenus au secret professionnel, mais ont l'obligation de dénoncer des actes délictueux: contenus illicites, notamment la pédo-pornographie ou la diffamation.



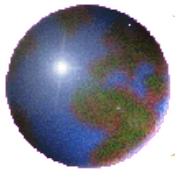
Agir, réagir

Préserver la sécurité du SI, maintenir la continuité de service :

- empêcher que les données soient déformées endommagées *(intégrité)* ou
- que des tiers non autorisés aient accès au SI *(confidentialité)*
- *exécuter les patchs de sécurité*
- *réagir vite pour enlever un contenu illicite « immédiatement ».*

Droit d'agir en refusant des demandes qui mettraient le SI en danger :

- diagnostic, analyse, contrôle,
- identifier des comportements illicites
- maintenance préventive,



PLAN

Cas d'école

Quelques questions

Que dit la PSSI du CNRS ?

Politique de gestion de trace du CNRS

La réponse à la question

La législation : Statut d'opérateur ? La LCEN, La CNIL, Loi Godfrain

Éléments constitutifs d'une infraction

Les tests réseau : Les scans de ports réseau, Tests d'intrusion, Écoute réseau

Les responsabilités (civile, pénale, administrative, personnelle, partagée)

Responsabilité : Facteurs de risque

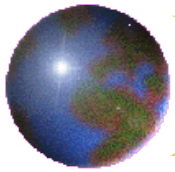
Obligation d'informer, tracer, sécuriser

Les données et ordinateurs personnels

La SSI : Responsabilité et SSI, Les règles du jeu de la SSI

Informer / Contrôler, tracer / Agir, réagir

Bibliographie



Bibliographie

Contexte juridique du métier d'ASR
http://www.resinfo.cnrs.fr/IMG/pdf/ContexteJuridiqueMetierASR.pdf

Le risque juridique vu du coté SSI : Robert Longeon

Politique de gestion de traces du CNRS :
https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po_gest_traces.pdf

« Charte pour l'usage des ressources informatiques et de service internet » du CNRS (DEC070007DAJ) du 18/01/2007 :
http://www.dsi.cnrs.fr/cnil/textes-de-reference/textes/Charte-informatique.pdf

Dossier « Relations du travail et internet » du Forum des droits sur l'internet :
http://www.foruminternet.org/specialistes/publications/dossier-relations-du-travail-et-internet.html

CNIL : Guide Informatique et Libertés pour l'enseignement supérieur et la recherche :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_CNIL_AMUE_2009.pdf

CNIL : Guide pour les employeurs et les salariés :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf