Laurent Bloch
RSSI de l'INSERM

Sécurité des Systèmes d'Information : quelques réflexions

http://mssi.auteuil.inserm.fr/

Principaux dilemnes :

- Sécurité « dure » et sécurité « molle »
- Sécurité par les normes ? par les procédures ?
- Sécurité procédurale ou sécurité substantielle ?
- Sécurité système et sécurité applicative
- « Tout ce qui n'est pas autorisé est interdit », ou ...
- « Tout ce qui n'est pas interdit est autorisé... mais filmé »
- La sécurité périmétrique est-elle encore possible ?
- Défense en profondeur

Des techniques et des usages peu propices à la sécurité

- *Wiki, AJAX, Mashup, BitTorrent, RSS...*
- *Partage, rencontres, mutualisation, collaboration, interopérabilité...*

> On va sortir un peu du cadre habituel mais comme certains admin
> de FAI sont sur la liste ainsi que certains juristes, je voudrais avoir
> quelques précisions.

Je répond sur un plan technique.

...

> Le terme harcèlement est juridiquement réservé au domaine du
> travail, le harcèlement par mail n'a donc aucune place aujourd'hui
> (je viens de l'apprendre).

Cela m'étonne beaucoup. De mon point de vue le harcèlement n'est pas lié à un domaine particulier et il peut se présenter de diverses manières bruit, odeur, pollution, etc. C'est une gêne de nature quelconque et elle est qualifiée de harcèlement par sa répétition régulière ou par épisode et si il a été clairement signifié au gêneur qu'il l'était.

Le SPAM est une forme de harcèlement et il me semble qu'il l'est aussi sur le plan juridique puisqu'il y a eu des condamnés.

« Idées stupides » selon Ranum

- Par défaut, tout est autorisé
- dresser la liste des menaces
- tester par intrusion, puis corriger
- les pirates sont sympa
- compter sur l'éducation des utilisateurs
- l'action vaut mieux que l'inaction (il est souvent plus facile de ne pas faire quelque chose d'idiot que de faire quelque chose d'intelligent).

Exemple de plan de PSSI, 1

- Contexte et objectifs
  - périmètres de sécurité
  - lignes directices
  - menaces, risques, vulnérabilités

Soit : que veut-on protéger

quels risques sont acceptables

comment les évalue-t-on

risque = préjudice x possibilité d'occurrence

Exemple de plan de PSSI, 2

- Organisation et mise en œuvre
  - Référentiel SSI
  - Chaîne fonctionnelle SSI
    - correspondants informatiques
  - responsabilités
  - chartes et référentiel
  - protection des données
  - sécurité des systèmes et des réseaux
  - mesures, audit, plan de continuité

Mais :

« La rationalité procédurale a du bon, sauf lorsqu'elle se construit au prix du renoncement à toute rationalité substantielle. »

Jean-Pierre Dupuy

Pour un catastrophisme éclairé - Quand l'impossible est certain.

Rationalité procédurale

« Dire que la rationalité est procédurale, c'est dire qu'une fois l'accord réalisé sur les justes et bonnes procédures, ce qu'elles produiront sera *ipso facto*, par propriété héritée en quelque sorte, juste et bon. C'est donc renoncer à chercher, indépendamment de et antérieurement à toute procédure, les critères du juste et du bien... »

Jean-Pierre Dupuy

Pour un catastrophisme éclairé - Quand l'impossible est certain.

Normes SSI

- IS 9000 : systèmes de management
- visée : la certification
- IS 27001 : systèmes de management de la SSI (SMSI)
- IS 27000 : vocabulaire
- IS 27002 (ex-17799) : catalogue de mesures de sécurité
- IS 27003 : implémentation
- IS 27004 : indicateurs SMSI
- IS 27005 : évaluation et traitement du risque, pour 2008
  - cf. EBIOS
- IS 27006 : certification de SMSI
- IS 27007 : audit de SMSI

Pourquoi se soumettre aux normes SSI ?

Trois motifs valables :

- obligation règlementaire
- clause contractuelle
- recherche d'une élévation morale

À signaler : les règlementations de type Sarbanes-Oxley ou Bâle 2 imposent le respect d'une norme de ce type, au choix ; or IS 27001 est la moins lourde.

Comment adopter une norme SSI comme IS 27001 ?

- Erreur à éviter : périmètre trop large
- Impliquer le management
- Audit « à blanc »
- Les cabinets qui font du conseil ou de la formation s'interdisent de faire de la certification, et inversement
- Il y a des pays où c'est plus facile
- En France : voir LSTI
- Formation : HSC

Sécurité substantielle 1

Ce dont il faut se convaincre au départ :

- le pare-feu sera franchi
- le site de secours sera hors d'usage
- les sauvegardes seront illisibles
- l'ingénieur système sera malade
- il y aura un rootkit et un keylogger sur le serveur
- etc.

Mais pas tout le même jour !

Sécurité substantielle 2

Il n'y a pas de solution toute cuite

- un pare-feu n'est efficace que bien paramétré...
- ... c'est-à-dire par un ingénieur compétent ...
- ... et chaque jour de l'année (jardinage vs. plomberie)
- D'où : le meilleur pare-feu est celui que maîtrise l'ingénieur en question

Trois ou quatre notions clé pour la sécurité demain (et aujourd'hui !)

- Identité
- Responsabilité
- Réputation
- Confiance

Identité sur le Web

Quelques réflexions...

suscitées par les questions suivantes :

- *spam* ;
- anonymat sur Wikipédia ;
- échanges poste à poste ;
- quelques évolutions législatives et juridiques.

Notions clé

- identité ;
- confiance ;
- réputation.

La confiance et la réputation sont des institutions invisibles. La confiance s'accorde, pour de bonnes raisons, à des humains précis et nommés.

La confiance est une spéculation sur un comportement futur.

Remarque liminaire :

Les exemples historiques de tentatives pour abolir le sujet et conférer le monopole de la confiance à une entité collective, telle que le parti, le peuple ou les masses, devant laquelle l'individu devait s'effacer, n'ont pas donné de bons résultats.

suite de la remarque liminaire :

- Tentation informatique : fonder la confiance sur des procédures algorithmiques.
- Les *moyens* de la confiance peuvent être algorithmiques, ce qui n'est pas la même chose.

Édition sur l'Internet

Anonymat et gratuité

- L'Internet suscite de nouveaux modes de création et de diffusion des œuvres ;
- la création est parfois anonyme (cf. Wikipédia) ;
- la diffusion est souvent gratuite.

Anonymat et gratuité

- Gratuité : liberté ?
- Anonymat : création collective ? démocratie?

Anonymat et gratuité

- Gratuité : souvent médiocrité. Marché à deux versants, TV hertzienne.
- Anonymat :
  - un système anonyme ne peut pas avoir de règles ;
  - un système sans règles ne peut pas être démocratique (Larry Sanger) ;
  - responsabilité personnelle.

Édition, prescription

- Les œuvres sont des biens d'expérience (Olivier Bomsel) : ce n'est qu'après vision que l'on sait que le film est bon.
- D'où l'utilité de procédures de sélection et de signalisation.

Édition, prescription

- Le public choisit selon des indices ou des prescriptions : le *Star System* exploite le pouvoir d'identification des acteurs.
- Rôle des séries, feuilletons, etc.
- Les œuvres mieux signalées seront plus souvent choisies.

Signalisation, sélection
(Olivier Bomsel)

- La signalisation est (serait ?) très intense en capital (prix de sortie d'un film).
- La diversité demande une signalisation efficace.
- L'espoir de diversité accrue par la vertu de la diffusion bon marché sur l'Internet est, en partie, une illusion. Cf. les radios libres.

Élargissement, diversité

- La diversité demande toujours une signalisation efficace...
- mais l'espoir de diversité accrue par la vertu de la diffusion bon marché sur l'Internet est, quand même, une réalité.

La signalisation aujourd'hui

Google

La signalisation aujourd'hui

- Google : et après ?

- identité ;
- réputation ;
- confiance.

Deux voies pour la confiance

- publications scientifiques : processus de validation par les pairs ; c'est un système d'autorité ;
- publications « ordinaires » : le nom de l'auteur.

La notoriété du nom est créée par divers relais de signalisation : critique, bouche à oreille, diffusion radio...

Qu'est un identifiant ?

Un identifiant discriminant permet de :

- distinguer une donnée des autres ;
- distinguer l'entité ou les entités auxquelles elle se rapporte des autres entités présentes dans l'univers étudié.

Ainsi est défini le processus d'identification, si l'on admet que « les entités sont des choses qui existent et qui peuvent être distinguées les unes des autres » (Sophie Le Pallec, JRES 2005).