1. Systèmes d'informations : définir les limites des compétences des acteurs

Présentation faite par M. Antoine Champagne, webmestre du site Kitetoa.com
Support : http://www.ossir.org/resist/supports/cr/20051128/Kitetoa.pdf

M. Champagne, journaliste, s'intéresse à la sécurité informatique, en prenant un point de vue de non-spécialiste et non-technicien. Il s'est notamment interrogé sur le niveau réel de sécurité des systèmes informatiques par rapport à la communication institutionnelle qui est faite autour de ce niveau de sécurité.

Cette interrogation l'a amené à discuter du seuil de compétence ou d'incompétence en matière de sécurité des acteurs des projets, que ces acteurs soient internes ou externes à l'entreprise cliente. De nombreuses fois, il a observé des discours du style « nos développements/projets/produits/... sont sécurisés parce que nos clients sont des institutions bancaires/grandes entreprises/sites sensibles/... ». Le lien n'est pourtant pas automatique entre le type des clients d'une société et le niveau de sécurité que cette dernière est capable d'assurer. Il ne s'agit là que d'un argumentaire de type commercial qui, s'il n'est pas corroboré par des faits tangibles dans l'organisation et la façon de produire de la société, n'apporte rien en matière de sécurité.

M. Champagne tire la conclusion que, trop souvent, les entreprises ne semblent pas se poser la question de ce qui leur est vendu réellement, se reposant sur diverses suppositions quant aux aspects de sécurité. Cette conclusion repose essentiellement sur les observations faites sur différents sites où, à l'aide de son navigateur, des informations confidentielles ou sensibles ont été extraites de systèmes pourtant présentés comme sécurisés. Il en déduit que le discours officiel « de se protéger des dangers du réseau » est plus facile à mettre en œuvre que les actions effectives de protection contre les risques et problèmes effectifs.

En outre, il a constaté une apparente méconnaissance, de la part des entreprises, de la loi du 6 janvier 1978 et de ce qu'elle impose vis-à-vis de la protection des données personnelles. D'une façon très globale, si un système répond à une sollicitation, qu'elle soit légitime (GET /index.html) ou non (injection SQL, mauvaise configuration, accès au système de fichiers), il considère que les informations ainsi obtenues sont publiques. A l'inverse, donc, les informations non publiques (sensibles, confidentielles, privées, etc.) doivent être clairement inaccessibles, quelles que soient les techniques mises en place pour atteindre cet objectif. S'il est possible de passer outre les protections, les données « deviennent » publiques.

Enfin, ses observations l'amènent à penser que non seulement le niveau de sécurité général ne s'améliore pas, mais il a tendance à se dégrader. Sa question est simple : si un journaliste non technicien parvient, avec un simple navigateur, à voir ce qu'il voit, qu'en est-il de personnes mal intentionnées et beaucoup plus compétentes techniquement parlant ?

Question : Pourquoi n'utiliser qu'un simple navigateur ?

Réponse : C'est un outil simple, non technique, non spécialisé et omniprésent. Il ne peut pas être qualifié d'outil d'attaque dédié, ce qui fait donc courir moins de risques en cas de plainte de la parti du site testé.

Les entreprises disposent de peu d'outils, peu de compétences en matière de sécurité, et il leur est demandé d'atteindre des objectifs élevés en ce domaine. Comment peuvent-elles faire ? Est-ce même un objectif atteignable ?

- Les projets sont rarement finalisés, en cela qu'ils sont en évolution permanente (ajout de nouvelles fonctions, version N+1, etc.). Cette évolutivité pousse les équipes de développement vers des choix rapides en matière de calendrier de réalisation, donc sans se préoccupper d'un quelconque niveau de sécurité.
- Une entreprise, surtout lorsqu'elle est de taille importante (grande administration, société nationale ou multi-nationale), ne peut prétendre connaître parfaitement son périmètre informatique. Ce dernier est en évolution constante, parfois de façon autonome, non planifiée et non concertée. Que devient alors le niveau de sécurité de l'ensemble ?
- Les directions générales voient clairement l'aspect financier de la dépense en sécurité informatique. Elles sont souvent incapables de mettre des bénéfices (généralement non financiers) en face de ces sommes, ce qui les pousse à minorer les dépenses.

Que valent les tests d'intrusion ? M. Champagne distingue deux angles d'approche de ces tests (et, par extension, des sociétés les réalisant), désignés sous les termes d'institutionnels et de hippies. L'approche dite institutionnelle concerne des tests bien carrés, bien marketés, bien normés, qui donnent lieu à des rapports dûment structurés, comme s'il s'agissait d'un bilan comptable. L'approche hippie est moins structurée, plus réactive et intuitive et, d'après lui, plus pertinente.

Comment faire réaliser de bons tests d'intrusion ? D'après M. Champagne, il faut laisser agir le marché, en faisant des audits réguliers, par des sociétés différentes, chacune étant informée de cette procédure. Ainsi, se sachant en compétition avec d'autres pour la récurrence des audits, les intervenants auront à cœur d'analyser réellement le niveau de sécurité de leur client, voire à chercher la petite bête pour prouver leurs compétences.

Question : que pensez-vous du full disclosure ?

Réponse : Il y a quelques années, il présentait un certain avantage pour la communauté de la sécurité. Aujourd'hui, il constitue une source importante d'informations pour les personnes indélicates, sans amener d'avantage notable pour les particuliers voire pour les entreprises concernées.

2. Retour d'expérience sur le filtrage de la navigation Internet

Présentation faite par M. Fabrice Prigent, Université Toulouse 1
Support : http://www.ossir.org/resist/supports/cr/20051128/Filtrage_web.pdf

L'Université de Toulouse 1 représente environ 20 000 personnes (18 000 étudiants et 2 000 enseignants/administratifs). Le besoin de filtrage de la navigation est venu initialement d'un contrôle du débit Internet, en 1997, alors que l'Université ne disposait que d'une ligne à 256 kbits/s. En cette époque, il avait été remarqué que près de 30% du trafic était à destination de sites non recommandables.

A ce besoin de contrôle du débit s'ajoutent aujourd'hui :

- Des obligations légales (contenus, protection des mineurs, etc.). Fabrice Prigent souligne que, au sens de la jurisprudence, une entreprise peut être assimilée à un fournisseur d'accès Internet pour ses salariés, et donc devoir respecter les mêmes obligations qu'un FAI plus classique.
- Des raisons de productivité, la consommation d'Internet non professionnel (sites pornographiques, jeux, presse, recherche d'emploi) allant à l'encontre de la productivité dans l'entreprise.

Fabrice Prigent souligne que la protection des mineurs, notamment contre la pornographie, s'applique quand bien même on pourrait penser que les utilisateurs du réseau de l'Université sont tous majeurs. Chaque année, des étudiants mineurs s'inscrivent (qui, pour la plupart, seront majeurs avant la fin de l'année scolaire). Ils doivent, pendant les quelques mois qu'il leur reste à attendre ce 18ème anniversaire, être protégés contre les contenus discutables. Il en est de même dans une entreprise recevant des stagiaires, d'autant plus si ceux-ci sont encore en collège ou lycée. Comme dans tout ce qui touche à la sécurité, il est important de bien connaître « sa » population d'utilisateurs.

Quelles sont les techniques de filtrage disponibles ?

- ICRA (Internet Content Rating Association, www.icra.org) : il s'agit d'une classification volontaire de la part des sites. S'agissant d'une action volontaire, elle n'est exécutée (quand elle est mise en place) que par des

sites légitimes, quels que soient le contenu qu'ils diffusent. De ce fait, tous les sites à contenu clairement illégal, ou des sites temporaires comme il s'en crée de nombreux chaque jour, ne mettent pas en place une classification ICRA. Un système de filtrage ne reposant que sur la classification ICRA n'a donc que très peu de chances d'être efficace.

- Des listes d'URLs : c'est le principe connu des listes noires (URLs interdites d'accès) ou blanches (seules URLs autorisées). L'UT1 se sert d'un robot d'indexation, qui ajoute entre 2 et 300 nouvelles URLs par jour aux différentes listes gérées par l'Université. Fabrice Prigent fait remarquer que l'UT1 n'utilise pas toutes les listes qu'elle alimente de cette manière, et que ces listes sont disponibles sur le site du Centre de Ressources.
- Une analyse du contenu des pages : à l'aide de mots-clés, de filtres de type bayésien ou de toute autre méthode d'analyse de contenu. L'utilisation de cette technique doit être précédée par une bonne estimation des performances de filtrage qui seront obtenues, en fonction du nombre d'utilisateurs, du début de la connexion, etc. Un outil filtrant une page en une seconde sur un système sans aucune sollicitation risque de ne pas offrir une expérience de navigation particulièrement agréable lorsque 3000 personnes s'en serviront en parallèle.
- Une analyse du contenu des images : divers produits prétendent être capables de différencier une image de type pornographique d'une image que l'on dira normale. De l'avis général, cela reste tout à fait discutable, et particulièrement facile à contourner.

Les différentes questions à résoudre avant de mettre en place un filtrage de la navigation sont :

- Définir le contexte d'ouverture aux contenus sur Internet,
- Définir le taux de problèmes acceptables (faux positifs, faux négatifs, lenteur),
- Définir le mode de fonctionnement du filtrage (par utilisateur, par adresse IP, par tranches horaires...)
- Définir l'implantation et l'architecture du filtrage,
- Définir la gestion du système, les possibilités de contournement, les cas spéciaux...

Fabrice décrit ensuite les éléments mis en place à l'Université. La politique mise en place permet de distinguer des zones plus ou moins exposées (par exemple les accès depuis les postes implantés dans les bibliothèques sont filtrés de manière plus sévère que pour d'autres postes).

Par effet de bord, elle permet aussi de détecter des infections virales sur un poste interne (accès à des URLs de mise à jour du virus/spyware, accès répétés et rapides à des sites discutables, etc.). Dans ces cas-là, les accès sortants du poste sont

bloqués et routés automatiquement vers des pages d'information internes présentant la procédure de décontamination. Une telle approche, outre qu'elle limite la propagation, permet à l'utilisateur, dans la très grande majorité des cas, de faire sa propre décontamination sans intervention du service informatique.

Question : quel effort cela a-t-il représenté pour mettre en place cette politique et les outils associés ?

Réponse : environ un mois de travail.