

Forum Eurosec 2007

Apprendre à vivre dans un monde sans frontière

Publié le 23-mai-2007



Par Guy Hervier. Pour sa 18e édition, le Forum Eurosec organisé par Devoteam a mis l'accent sur la dimension internationale, mondiale, de la société des technologies de l'information et des conséquences sur la sécurité. « *Depuis toujours, les hommes ont vécu dans des espaces limités, avec Internet, l'abolition des frontières est une idée plutôt dérangeante, mais avec laquelle il faut s'habituer pour dépasser les réflexes locaux alors que les problèmes sont globaux* », rappelait

Michel Bon, président du Conseil de surveillance du groupe Devoteam. Dans cette vision géopolitique de la sécurité, l'exemple de L'Estonie, qui fut rappelé comme un exemple tout récent, apporte une éclatante confirmation.

L'Estonie ne répond plus

« *En quelques années, et plus spécialement depuis septembre 2001, le problème de la sécurité s'est considérablement développé* », présentait Andrea Servida, directeur adjoint de la commission « Internet, réseau et sécurité de l'information » à la commission européenne. L'exemple récent de l'Estonie qui est des pays les plus avancés au niveau européen en matière d'administration électronique constitue une illustration plus que pertinente. L'utilisation des attaques informatiques étant désormais un moyen naturel de protestation ou d'intimidation.

Suite à la décision de Tallim de déplacer un monument aux morts soviétiques du centre-ville, les Estoniens d'origine russes ont organisé de larges manifestations. Simultanément, les sites Internet du gouvernement, des partis politiques, des médias et de certaines entreprises ont été dans l'obligation de fermer suite à des attaques de déni de services. Et les internautes qui se connectaient à ces différents sites étaient redirigés vers des images de soldats soviétiques. Les coupables n'ont pas été identifiés, mais des soupçons pèsent sur les autorités et des responsables politiques estoniens ont fait des déclarations dans ce sens. Bien entendu, le gouvernement russe a nié toute implication, notamment par la voix de son porte-parole Dimitri Peskov, qui a assuré que « *l'Etat [russe] ne saurait en aucune façon être impliqué dans le cyber-terrorisme* ».

Evolution du contexte global sur 5 dimensions

- Politique : instabilité, terrorisme, énergie
- Juridique : réglementation, protection de la vie privée, gestion numérique des droits
- Economique : e-économie, crime organisé, catastrophes naturelles
- Socioculturelle : techno-génération, travail à distance
- Technologique : accroissement de la complexité, convergence numérique

L'objectif de la Commission européenne, a précisé Andrea Servida, est de revitaliser la stratégie définie en 2001 en matière de sécurité, précisément parce que l'environnement général a beaucoup évolué. La Commission entend travailler sur deux axes : améliorer la coordination des initiatives lancées dans ce domaine de la sécurité : lutte anti-spam, CIIP (Protection des infrastructures critiques de l'information), 2006 Review, cybercrime, RFID... et mobiliser toutes les parties prenantes, c'est-à-dire à la fois les entreprises et organisations et les particuliers.



La Commission entend aussi renforcer le rôle de l'ENISA (European Network and Information Security Agency). Cette agence travaille en particulier sur la faisabilité au niveau européen d'un système de partage d'information et d'alertes.

Omniprésence des technologies de l'information



« On oublie un peu trop que plus aucun processus essentiel de la société n'est possible sans informatique, proposait comme réflexion liminaire Patrick Pailloux, Directeur Central de la Sécurité des Sécurité au Secrétariat général de la Défense national (SGDN). Mais paradoxalement, tout arrêt de système d'information a des conséquences qu'il est difficile de mesurer ». Parmi les menaces constatées en matière d'attaques, qui sont assez développées en France, Patrick Pailloux en a retenu quatre principales :

- La défiguration des sites Web : 2400 sites en .fr au deuxième semestre 2006 contre 1500 au premier semestre ;
- Le phishing a touché toutes les grandes banques, et s'attaque désormais aux principaux sites de e-commerce (eBay, sncf.fr...) ;
- Les botnets sont désormais organisés au niveau mondial et peuvent être activés à la demande d'organisations criminelles ;
- Les chevaux de Troie sont largement utilisés pour mener des attaques ciblées et, par nature, sont difficiles à détecter.

En terme de sécurité informatique, l'Etat français poursuit deux missions : protéger ses propres infrastructures, et aider les acteurs administratifs et économiques grâce à un centre opérationnel de la sécurité. Mais comment cette ressource centralisée peut-elle aider les collectivités territoriales et les PME ? « Il ne faut sans doute pas tout attendre de la réglementation, considère Patrick Pailloux, il faut aussi compter sur une autorégulation des prestataires de services et dans ce domaine il y a encore beaucoup de progrès à accomplir. Pour s'en convaincre, il suffit de constater par exemple que certains hébergeurs de site Web proposent les patches de sécurité en tant qu'option payante ». Le pire n'est jamais certain, cela ne doit pas empêcher de s'y préparer.

Gestion des risques et continuité d'activité : deux priorités pour 2007

La sécurisation des Systèmes d'information représente un enjeu stratégique pour 63 % des entreprises, c'est ce que montre la dernière enquête réalisée par Devoteam Consulting auprès de 150 sociétés européennes.

En matière de gouvernance, deux priorités sont apparues : faire évoluer le cadre de la sécurité incluant la politique de sécurité, les chartes, l'organisation... et la continuité. 89% des entreprises ont défini une politique générale, mais seulement 60 % la tiennent à jour.

Viennent ensuite la prise en compte de la sécurité dans les projets (44%), la sensibilisation (35%), la conformité juridique (35%), la conformité juridique et réglementaire (33%) et la gestion globale des risques (33%).

Les problématiques liées à l'intelligence économique et de lutte contre la fraude sont rarement prioritaires.

Au niveau des infrastructures, la protection des accès et la mise en oeuvre des solutions de continuité vis-à-vis des risques de panne système ou réseau ont été les deux principaux chantiers, alors que les thèmes tels que la protection des technologies sans fil, de la messagerie instantanée, contre les intrusions ou contre les attaques DoS ou DDoS ont été clairement délaissés.

Cela n'arrive-t-il qu'aux autres ? Seulement 8 % des personnes interrogées déclarent avoir subi des attaques aux conséquences significatives. Tout dépend de ce que l'on entend par significatif. Par ailleurs, les entreprises n'aiment pas trop communiquer sur ce type de problèmes.



Copyright © 2004 ITRManager.com - All rights reserved.