L'évolution des enjeux de la sécurité des systèmes d'information

Henri Serres (69),
Direction centrale de la Sécurité des systèmes d'information

"Les TIC sont porteuses de promesses dans tous les domaines [...]. Il nous appartient de libérer les énergies, créer la confiance et soutenir l'innovation [...]. Créer un climat de confiance en fixant des règles du jeu claires aux acteurs et en assurant une protection efficace des utilisateurs"... [1]

L'essor de la société de l'information, à l'origine provoqué par la diffusion des progrès des technologies de l'information et de la communication, procède assurément d'une démarche volontariste au niveau de l'État, comme l'a réaffirmé le Premier ministre devant l'*Electronic Business Group*. En ce qui concerne la sphère publique, cet essor devrait se traduire par une amélioration considérable de la productivité et de la qualité du travail des administrations ainsi que des services rendus aux usagers. Ces conséquences bénéfiques ne doivent cependant pas occulter le revers de la médaille : l'apparition de vulnérabilités nouvelles, l'accroissement des risques pesant sur les systèmes d'information et l'émergence de menaces caractérisées par leur ubiquité, leur soudaineté et une capacité de nuisance particulièrement forte.

Ainsi, la nécessité de protéger les systèmes d'information de l'État face à ces vulnérabilités, ces risques et ces menaces est à l'origine de la création, décidée en 2000 et officialisée à l'été 2001, de la Direction centrale de la sécurité des systèmes d'information (DCSSI) [2].

Depuis, la médiatisation de la diffusion de certains virus et surtout les événements du 11 septembre 2001 ont renforcé la prise de conscience des risques et des attaques possibles ou probables, et des progrès notables en matière de protection des systèmes d'information ont été accomplis.

Mais le cadre général dans lequel s'inscrit aujourd'hui l'action en matière de sécurité des systèmes d'information (SSI) est en évolution permanente : de nouvelles technologies apparaissent et se diffusent massivement sans que leur impact sur la sécurité ait été complètement pris en compte, les failles de sécurité se multiplient et engendrent de nouvelles vulnérabilités à caractère systémique, des menaces pernicieuses et inédites se font jour, dont la moindre n'est pas la menace cyberterroriste.

S'adapter à cette évolution et si possible l'anticiper apparaît donc comme un impératif majeur pour pouvoir assurer convenablement la sécurité des systèmes d'information, notamment ceux de l'État.

Les tendances d'évolution du contexte de la sécurité des systèmes d'information

Une évolution technologique pernicieuse et périlleuse

Certaines des évolutions technologiques en cours et de celles qui se dessinent ne vont pas dans le sens d'un renforcement intrinsèque de la sécurité. À titre d'exemple, on peut citer toutes les technologies sans fil qui émergent et devraient se diffuser rapidement et massivement, ainsi que l'Internet mobile dont la diffusion devrait être aussi rapide qu'a été celle du téléphone portable. La facilité avec laquelle il est possible de pénétrer les systèmes de sécurité des réseaux sans fil avec des équipements ordinaires a récemment amené les *hackers* à pratiquer un nouveau "sport" : le "*war driving*", qui consiste à se promener en voiture, muni d'un ordinateur portable doté d'un simple adaptateur, et à repérer puis attaquer les réseaux sans fil rencontrés.

Le caractère dangereux de ces technologies au regard de la sécurité des systèmes d'information est accentué du fait que bien souvent les équipements les incluent nativement sans que leurs utilisateurs en soient informés ou aient conscience des risques auxquels ils s'exposent.

L'internationalisation du cadre d'action

En matière de sécurité des systèmes d'information, une des évolutions récentes les plus marquantes est l'internationalisation du cadre d'action, concomitante de l'extension des réseaux à l'échelle planétaire et de l'expansion de l'Internet, et de leur corollaire, l'apparition d'une cybercriminalité qui ignore les frontières.

C'est ainsi que de nombreuses organisations internationales (Conseil de l'Europe, G8) s'attachent à définir des instruments politiques et juridiques

adaptés à la lutte contre la cybercriminalité. De son côté, l'Union européenne s'est saisie de la problématique de la sécurité des systèmes d'information et le plan d'action "eEurope 2005"[3] accorde une importance toute particulière à la sécurité du "monde en ligne". De même, l'OCDE vient récemment d'adopter une recommandation de son Conseil intitulée : "Lignes directrices régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité"[4].

L'offre industrielle française en SSI

L'offre française de produits de confiance en matière de sécurité des systèmes d'information est encore insuffisante par rapport aux enjeux et aux efforts consentis par les autres grands pays industrialisés. Les raisons en sont connues : étroitesse du marché, faiblesse des retours sur investissement, manque d'actions incitatives en la matière.

Dans ces conditions, le risque serait grand de devoir s'en remettre exclusivement, à relativement court terme, à des produits ou logiciels de sécurité d'origine étrangère alors que de grands groupes français ou des PME innovantes ont les capacités de proposer des produits ou des technologies intéressants.

Une coordination accrue des efforts de développement et d'industrialisation des produits européens est parallèlement souhaitable.

Une cybercriminalité durable

La complexité croissante des systèmes d'information, même si tout est fait pour rendre leur utilisation transparente aux utilisateurs, est en elle-même une source de vulnérabilités. On sait que l'ingéniosité des attaquants est sans limite pour détecter et exploiter ces vulnérabilités.

Par ailleurs, la dématérialisation des flux financiers et le développement du commerce électronique multiplient les tentations pour des malfaiteurs versés dans la haute technologie, agissant seuls ou dans le cadre du crime organisé, de réaliser des gains lucratifs avec un sentiment de relative impunité.

De nombreuses études ou rapports sont publiés régulièrement sur le sujet. Toutes ces études et ces rapports convergent pour souligner l'augmentation considérable et permanente de la cybercriminalité et, plus généralement, des atteintes portées aux systèmes d'information des entreprises et des organisations de toute nature. Ainsi le nombre total d'attaques recensées dans le monde a augmenté de 160 % de 2000 à 2001 (source CERT). Autre exemple : si en 2000, un courrier électronique sur 700 contenait un virus, en 2001 un courrier électronique sur 350 véhiculait une forme d'attaque malveillante (même source).

Vers une interconnexion généralisée des réseaux

La diffusion et l'utilisation des TIC dans les entreprises et les administrations devraient se poursuivre à un rythme au moins équivalent au rythme actuel. Si des évolutions notables ne sont pas à attendre dans le domaine de la bureautique, sauf un usage sans doute plus répandu des logiciels libres, en revanche les échanges d'information par l'intermédiaire des réseaux locaux et étendus devraient se multiplier et l'utilisation des téléprocédures entre les administrations, impliquant donc l'interconnexion de réseaux, devrait se généraliser, du fait d'une démarche volontariste de l'État et de la recherche d'une meilleure productivité au sein des administrations.

La mise en place de l'administration électronique et la généralisation des téléservices publics d'ici 2005 nécessiteront des dispositions techniques, et notamment l'interconnexion des réseaux ministériels avec les réseaux publics et Internet.

Les vulnérabilités engendrées par l'interconnexion des réseaux internes avec des réseaux ouverts sont croissantes et doivent être évaluées et traitées au sein de chaque entreprise et administration avec la plus grande attention.

Quelques pistes de progression

Avec l'avènement des TIC, l'environnement des entreprises et des administrations évolue sans cesse. La sécurité devient alors une tâche de tous les instants, qui requiert une attention, une adaptabilité et une anticipation permanentes. Si les problèmes actuels trouvent une réponse, de nouvelles failles apparaissent ; des progrès restent à accomplir, d'autres voies à explorer :

- renforcer les capacités de Recherche & Technologie, et d'évaluation en matière de sécurité des systèmes d'information permettant de couvrir le spectre des technologies et de réduire à un niveau acceptable les risques liés à l'utilisation des technologies de l'information et de la communication ;
- disposer, pour la fonction sécurité des systèmes d'information, de ressources humaines et de compétences suffisantes en nombre et en qualité : toutes les évolutions analysées ci-dessus convergent pour faire ressortir cette impérieuse nécessité ;
- accroître les actions de sensibilisation à la sécurité des systèmes d'information, au sein des administrations, auprès des entreprises et des citoyens, de façon à permettre la diffusion progressive d'une "culture SSI" au sein de la société tout entière.

La communauté polytechnicienne est particulièrement bien placée sur ces différents aspects, par sa place éminente dans le monde de la recherche, publique ou privée, par les capacités techniques et décisionnelles qu'elle porte dans le monde des utilisateurs comme dans celui des concepteurs et réalisateurs de systèmes d'information.

La réalisation de ce numéro exceptionnel de *La Jaune et la Rouge* contribue donc à l'amélioration de la prise de conscience des risques, et fait ressortir l'importance de l'engagement de tous dans la recherche de solutions et de leur mise en pratique dans un monde où l'interdépendance nécessite une vigilance renforcée. n

---

1 - Extraits du discours du Premier ministre Jean-Pierre RAFFARIN devant L'*Electronic Business Group* le 12 novembre 2002 – Présentation du plan RE/SO 2007 (Pour une REpublique numérique dans la SOciété de l'information).
2 - http://www.ssi.gouv.fr
3 - http://europa.eu.int/information_society/eeurope/action_plan/index_fr.htm
4 - http://www.oecd.org/pdf/M00033000/M00033183.pdf