La protection des infrastructures informatiques sensibles repose sur quatre piliers

Parmi les membres de l'OCDE, la Suisse est le pays qui dépense le plus d'argent par habitant et par année pour les technologies de l'information et de la communication (TIC). Cela renforce certes nos avantages économiques, mais nous rend aussi dépendants et nous expose à des risques. Les menaces sont nombreuses; elles vont des extorsions de fonds à l'espionnage économique, en passant par le dysfonctionnement des infrastructures sensibles du pays telles que l'approvisionnement en énergie, les activités financières, les transports, la logistique et le système de santé. Il est donc impératif de protéger ces infra-structures, y compris Internet.

Le concept de la sécurité de l'information repose, en Suisse, sur quatre piliers: prévention, dépistage précoce, lutte contre les incidents et gestion stratégique des crises.

Les systèmes de contrôle, pour la gestion des transports et du trafic par exemple, sont devenus, étant donné leur importance, synonymes d'infrastructures critiques. Les mesures pour les protéger sont d'autant plus nécessaires. En illustration: appareil d'enclenchement des CFF. Photo: Keystone

Les défauts des logiciels des systèmes de gestion du trafic, les pannes des réseaux de téléphonie mobile et les interruptions de fonctionnement des distributeurs automatiques de billets de banque sont des incidents qui nous rappellent les limites des TIC. Les pannes techniques mais aussi les attaques ciblées sur les infrastructures informatiques – comme l'accès non autorisé aux systèmes ou les dommages intentionnels qui leur sont causés – peuvent détruire les canaux d'approvisionnement en électricité, en eau ou en argent par exemple.

Ruedi Rytz
Chef des secrétariats des domaines infrastructure, Office fédéral pour l'approvisionnement économique du pays
OFAE, Berne

Le cas de l'Estonie

Les attaques perpétrées contre l'Estonie par le biais d'Internet l'année dernière donnent une idée des défis que doivent relever les sociétés modernes de l'information. Elles se sont produites lorsqu'il s'est agi de déplacer un monument de guerre soviétique. On soupçonne des nationalistes russes, mais on ne parviendra certainement jamais à connaître l'origine exacte de ces troubles. Ce qui est sûr, c'est que certaines banques estoniennes travaillant par Internet ont été bloquées pendant des jours suite à ces attaques, ce qui s'est traduit par une forte baisse de leur chiffre d'affaires. De plus, les services gouvernementaux informatisés, pourtant bien rodés, n'étaient plus disponibles. La population a eu beaucoup de peine à s'informer par Internet, les communications avec l'étranger étant même partiellement coupées. Cet exemple montre que les attaques sur les infrastructures TIC d'un pays peuvent provoquer des dommages économiques et mettre les gouvernements sous pression.

Les réseaux de zombies provoquent des attaques ayant des conséquences sur l'économie nationale

Ces attaques ont été causées par ce que l'on nomme les réseaux de zombies. Il s'agit d'un ensemble de machines contrôlées par des pirates informatiques, qui sont gérées à distance de façon centralisée et peuvent réaliser des «travaux». Les réseaux de zombies comptent des milliers d'ordinateurs, voire un million. Le piratage et l'intégration des appareils dans un tel réseau se font automatiquement au moyen de logiciels malveillants, qui profitent de certaines lacunes en matière de sécurité des systèmes d'exploitation ou des applications. Les appareils infestés et intégrés dans un réseau de zombies sont souvent les PC de particuliers; de nos jours, ces réseaux sont tellement puissants que leurs utilisateurs ont de la peine à imaginer que, pendant qu'ils travaillent sur un texte, leurs ordinateurs sont utilisés pour paralyser une banque en Estonie par exemple. On sait que, rien qu'en Suisse, des dizaines de milliers de PC sont intégrés dans des réseaux de zombies.

Une autre façon de tirer profit de la haute performance des réseaux de zombies, comme ce fut le cas en Estonie, consiste à inonder les serveurs (p. ex. banque ou commerce électroniques) avec une telle quantité de requêtes au même moment qu'ils s'effondrent sous cet énorme volume et ne sont plus disponibles pour les clients autorisés. Ces attaques par déni de service (en anglais «Denial of Service», DoS) contre les serveurs commerciaux vont souvent de pair avec des extorsions de fonds; elles peuvent toucher toutes les entreprises qui proposent des services par l'intermédiaire d'Internet. Les pertes économiques sont parfois très élevées et, dans les cas extrêmes, peuvent même provoquer des faillites. Il y a trois ans, une attaque DoS contre Worldpay, la filiale de la Royal Bank of Scotland qui s'occupe des paiements par cartes de crédit, a paralysé presque entièrement les transactions financières. Les clients de 30 000 magasins dans 70 pays ne pouvaient plus utiliser leurs cartes de crédit pour payer et ont donc laissé les marchandises sur les rayons. Pendant cette attaque qui a duré trois jours, les pertes se sont élevées à 50%–80% du chiffre d'affaires, ce qui a eu des conséquences sur les économies nationales. Les attaques par les réseaux de zombies peuvent se répercuter rapidement sur des infrastructures sensibles, comme le système financier dans ce cas-là.

En plus des attaques DoS, les réseaux de zombies sont utilisés à d'autres fins, l'envoi de pourriels par exemple (voir *encadré 1*). Généralement, les pirates ne créent pas les réseaux de zombies eux-mêmes, mais les louent. Des listes de prix se cachent dans les tréfonds d'Internet et des démonstrations gratuites de leurs performances sont même proposées. Les personnes qui créent les réseaux de zombies gagnent de l'argent en les louant (des revenus annuels de l'ordre de 200 000 USD ne sont pas rares) et les «locataires» rentrent dans leurs frais par l'extorsion de fonds et l'envoi de pourriels, par exemple. La division du travail dans les abysses d'Internet est très claire et augmente manifestement la productivité; Adam Smith en sourirait d'aise.

L'hypothèse angoissante d'une attaque sur des systèmes de contrôle

En plus des menaces décrites plus haut et des nombreuses autres variantes qui existent et qui se manifestent presque tous les jours par des incidents, rien n'a stimulé autant l'imagination humaine que l'attaque des systèmes de contrôle des infrastructures TIC. Par systèmes, on entend ceux utilisés pour contrôler et gérer les complexes industriels (p. ex. usines chimiques ou centrales électriques), pour assurer la distribution des biens vitaux (p. ex. électricité, eau, carburant) ou pour régler les transports et la circulation (trains, gestion du trafic, poste). Étant donné leur importance, les systèmes de contrôle sont devenus synonymes d'infrastructures sensibles. Il est proprement effrayant de s'imaginer que, dans les montagnes de Kaboul, des terroristes, leur ordinateur portable sur les genoux, éteignent les lumières des grandes villes occidentales. Toutefois, disons-le d'emblée: des scénarios de ce genre sont moins une menace réelle que de la matière passionnante pour le cinéma, du moins pour le moment. Il ne faut, toutefois, pas non plus prendre le problème à la légère.

Le développement et l'exploitation des systèmes de surveillance et de commande ont une longue tradition. Au départ, ces systèmes n'avaient pas grand-chose à voir avec les TIC traditionnelles. Ils étaient isolés des réseaux d'ordinateurs (comme Internet); pour communiquer, ils utilisaient leur propre matériel, leurs logiciels et des protocoles particuliers. Ces dernières années, des appareils à moindres prix, possédant une interface intégrée, sont apparus en grand nombre et ont provoqué d'énormes changements. En bref: les systèmes de contrôle ressemblent de plus en plus aux PC et à Internet. Nous payons cette technologie bon marché par le fait que les systèmes de contrôle sont soumis aux mêmes menaces que nous connaissons en utilisant Internet. Les maliciels (virus, vers) et les pirates font leur apparition.

Encadré 1

Réseaux de zombies: l'envoi de pourriels

Plus de 90% des pourriels (courriers publicitaires indésirables ou, en anglais, «spams») sont envoyés par l'intermédiaire de réseaux de zombies. L'envoi de pourriels est expressément interdit en Suisse depuis le 1er avril 2007. La loi fédérale contre la concurrence déloyale (LCD) prévoit diverses mesures contre les pourriels et la loi sur les télécommunications (LTC) réglemente les actions que doivent entreprendre les fournisseurs de services en télécommunication. Si le pourriel est envoyé depuis la Suisse à des destinataires suisses, le fournisseur de services Internet de l'expéditeur doit agir; les autres cas (expéditeur en Suisse, destinataires à l'étranger et inversement) relèvent de la compétence du Secrétariat d'État à l'économie (Seco).

À ce jour, peu de cas attestant les attaques sur les systèmes de contrôle ont été répertoriés. Le plus connu est celui qui s'est produit dans le Queensland (Australie) en 2000. Depuis son ordinateur portable, un homme de 49 ans a réussi à pénétrer dans le Service des eaux géré par informatique. Il s'est fait passer pour la «station de pompage 4» et a pu déjouer toutes les alarmes. Il a obtenu le contrôle illimité sur 300 points de commande du système d'approvisionnement en eau potable et d'évacuation des eaux usées. Il a réussi à faire se déverser des millions de litres d'eaux usées dans des parcs, des rivières et même sur le terrain d'un hôtel. La faune marine a été gravement endommagée; l'eau des rivières s'est colorée en noir et la puanteur a été insupportable pendant longtemps. Ce n'est qu'au 46e essai que la police a mis la main sur cet homme.

Dans le cas de l'Estonie, on n'a pas observé d'attaques sur les systèmes de contrôle, mais, suite à ces événements, de nombreux pays ont réfléchi, au moyen de rapports d'enquêtes, à la portée de ces attaques[1].

Les efforts entrepris en Suisse au niveau de l'État

La Suisse, en sa qualité de place économique de premier plan, subirait de grandes pertes en cas de perturbation majeure de l'infrastructure informatique. À plusieurs reprises, le Conseil fédéral a signalé sa volonté de les protéger contre les abus, les pannes et les attaques, notamment en adoptant le concept *Information Assurance* (sûreté de l'information) en 2000, en créant le *Service de coordination de la lutte contre la criminalité sur Internet (Scoci)* en 2001 et en mettant en place la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani)* en 2003.

Dans le domaine de la protection des infrastructures informatiques sensibles, le Conseil fédéral poursuit la stratégie qu'il a présentée dans le concept «Information Assurance». Celle-ci repose sur les quatre piliers que sont la prévention, le dépistage précoce, la lutte contre les incidents et la gestion stratégique des crises.

En ce qui concerne la *prévention*, des analyses de risque sont élaborés par le domaine de l'infrastructure TIC de l'Office fédéral de l'approvisionnement économique du pays (OFAE) – avec les organes concernés de l'économie – à savoir les exploitants des infrastructures informatiques sensibles, telles que l'approvisionnement en énergie, les transports, la santé, etc. Elles se focalisent sur les liens de dépendance qui unissent ces secteurs aux infrastructures TIC et proposent des mesures préparatoires de protection.

Le *dépistage précoce* et la *lutte contre les incidents* font partie du domaine de compétence de Melani. Il s'agit de la coopération entre l'Unité de stratégie informatique de la Confédération (Usic) et le Service de l'analyse et de la prévention de l'Office fédéral de la police (Fedpol). L'objectif de Melani est de mettre des moyens subsidiaires à la disposition des exploitants d'infrastructures informatiques sensibles, ce qui est seulement à la portée d'un organe étatique. Cela est le cas notamment dans les domaines du service des renseignements (estimations des menaces), des autorités de poursuites pénales et des équipes d'intervention en cas d'urgence informatique nationales (govcert.ch). Dans ce but, Melani travaille en étroite collaboration avec les gestionnaires de ces infrastructures (p. ex. approvisionnement en énergie, activités bancaires et télécommunications).

La *gestion stratégique des crises* prévoit la convocation de l'*État-major de la sûreté de l'information (Sonia)* dans le cas de perturbations de longue durée, qui se répercutent sur le fonctionnement des infrastructures de l'information et de la communication. Cet organe est constitué de représentants de l'administration fédérale et de décideurs expérimentés de l'infrastructure TIC pour l'approvisionnement économique du pays.

Grâce à une collaboration étroite entre l'économie et l'État, et dans le cadre de l'approvisionnement économique du pays et de Melani, la Suisse possède un modèle de protection des infrastructures sensibles étendu, souple et avantageux, qui est aussi considéré comme exemplaire à l'étranger. ▮

1 Voir la Suède par exemple: *www.krisberedskapsmyndigheten.se*, «Publications», «Other Documents», «Large Scale Internet Attacks, SEMA's Educational Series 2008:2».