
KEYSTONE

JAPON

Abe affiche ses ambitions

Le premier ministre japonais entend réviser la constitution qui limite le rôle de l'armée. Celle-ci a été conçue pour ne pas être changée. Sa tâche s'annonce difficile. **PAGE 19**

L'ACTU

SUISSE | MONDE | ÉCONOMIE

CYBERATTAQUES Dans des sociétés toujours plus connectées, la technologie profite aussi aux pirates des réseaux. Etats, entreprises, particuliers, tous sont visés.

De petits clics pour de grands chocs

PROPOS RECUEILLIS PAR
PHILIPPE VILLARD

Des Suisses arnaqués au moyen d'une vague de SMS douteux venant d'Angleterre ou, hier encore, une déferlante de «pourriels» visant les clients du distributeur français d'électricité EDF… Les cyberattaques géantes motivées par l'extorsion de données bancaires se multiplient dans l'opacité des réseaux. Elles conduisent les Etats à intégrer ce risque et à développer une cyberstratégie.

Rencontre avec Solange Ghernaouti, experte internationale en cybersécurité et professeure à l'Université de Lausanne.

Comment perçoit-on l'ensemble des cybermenaces?

Selon les pays et les organisations, la prise de conscience en matière de cyberrisques est déjà très forte. Les grandes sociétés sont au fait des dangers, relativement bien sensibilisées et ont mis en œuvre des mesures de protection et de réaction.

La question reste plus délicate dans les petites et moyennes entreprises où l'on dispose de peu de moyens. Enfin, les universités et les laboratoires de recherches peuvent être également menacés, car l'espionnage, le vol de données existent, il faut toujours être vigilant quand on y accueille des stagiaires et /ou des étudiants étrangers.

Quels facteurs expliquent cette prise de conscience?

La cybercriminalité fait partie de l'actualité car elle engendre de plus en plus de victimes.

Elle n'épargne pas non plus les particuliers qui peuvent se faire voler leur identité numérique, des données personnelles ou être confrontés à des escroqueries en ligne. On mesure ainsi que malveillants et organisations criminelles sont de plus en plus performants grâce aux technologies de l'information, les escrocs ont une imagination sans limite. Rappelez-vous les premières automobiles, les voyous en ont disposé avant les policiers, ils ont su en tirer partie.

Comment s'organise cette cyberdélinquance?

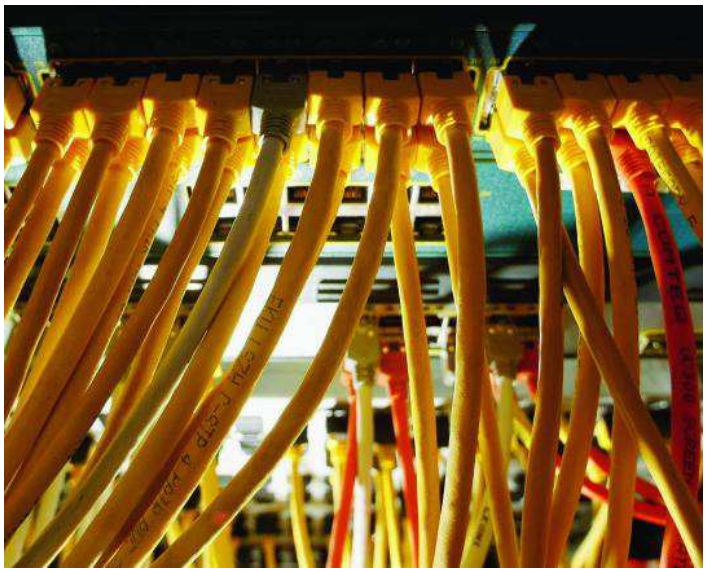
Quand elles ont besoin d'un savoir-faire, les organisations criminelles sont capables de recruter les meilleurs comptables et les meilleurs chimistes. Il en va de même en informatique.

Dans ce domaine les équipes sont dynamiques, les membres sont recrutés en vue d'une opération particulière et mobilisés en fonction des besoins pour s'appuyer sur des compétences spécifiques. Enfin, l'informatique et le mode opératoire des cyberattaques permettent de dissocier les actions de piratage. Ce «saucissonnage» des tâches et la pluralité des acteurs criminels impliqués minimisent le risque pour chacun d'entre eux.

Ce n'est donc pas un sport à la portée de tout le monde?

Pas forcément, cela dépend de l'ampleur et de la sophistication de l'attaque. Avec la démocratisation des outils de hacking qui s'opère à travers des groupes comme Anonymous par exemple, n'importe qui peut contribuer, grâce à la disponibilité de logiciels d'attaque, à la saturation d'un serveur dans le cadre d'un déni de service.

Internet permet de démultiplier les cibles et les acteurs malveillants tout en offrant à ces derniers une couche d'isolation autorisant un certain anonymat et une relative impunité.


La complexité des réseaux favorise la dissimulation des sources d'une cyberattaque. KEYSTONE

La menace est donc aussi soudaine qu'insaisissable?

Les cybermenaces peuvent générer de la peur car on ne sait pas forcément prédire quand elles vont se concrétiser, quels vont être les impacts et les victimes, qui est l'agresseur.

Il peut se trouver dans un pays, faire transiter son attaque par d'autres pour en viser un autre, en piratant des machines parfois à l'insu de leurs propriétaires.

Les Etats élaborent-ils un corps de doctrine pour aborder ces questions?

Les technologies informatiques constituent aussi des armes de guerre.

Dans la logique des Etats, les territoires sont à conquérir, à maîtriser, à dominer. Le cyberespace comme les autres. Mais je pense qu'il faut élargir la perspective.

Aujourd'hui, on sait que les ressources naturelles et énergétiques diminuent et que tous les moyens vont être bons pour s'en emparer et les protéger.

Dans des Etats hyperconnectés et dépendant des infrastructures informatiques, la cybersécurité est aussi bien offensive que défensive.

Qu'en est-il de la Suisse?

La Suisse développe une stratégie de protection. Le monde politique est en train de prendre conscience des risques et un dégagement de moyens semble s'opérer, ce qui est une bonne chose.

EXERCICE STRATÉGIQUE

En mai, l'administration fédérale et le gouvernement vont être confrontés à un exercice de conduite stratégique. Il aura pour thème «*une attaque cybernétique massive et anonyme contre la Suisse*», résume Stéphane Derron, chef suppléant de la section formation à la gestion des crises par la Confédération. But de l'opération: voir comment implémenter dans les rouages étatiques la stratégie de protection contre les cyberrisques.

«*Il s'agit, dans un contexte de situation extraordinaire, de gérer les conséquences politiques découlant de problèmes dans les systèmes-clés de l'administration fédérale et de proposer au Conseil fédéral des mesures pour gérer la crise*», décrypte-t-il encore. Cet exercice-cadre pour états-majors se déroulera sur deux jours. Il a été précédé durant l'automne 2012 de trois séminaires de réflexion stratégique. Les exercices de conduite stratégiques sont organisés tous les quatre ans.

En 2005, il avait pour thème la transmission à l'homme d'un virus d'origine porcine dans une exploitation agricole de la région de Saint-Gall. «*Les enseignements tirés nous ont été utiles pour affronter la grippe porcine survenue en 2009*», souligne encore Stéphane Derron. En 2009, l'exercice stratégique était bâti sur le scénario d'une pénurie d'électricité.

«La cybersécurité est aussi bien offensive que défensive.»

SOLANGE GHERNAOUTI EXPERTE INTERNATIONALE EN CYBERSÉCURITÉ

La clé USB, première des menaces

«*Quand on en trouve une, il n'y a qu'une seule chose à faire: l'écraser d'un coup de talon, même si elle est dans son emballage d'origine et accompagnée de son ticket de caisse*», s'emporte un spécialiste des questions de cyberdéfense. L'objet de sa colère n'est rien d'autre qu'une simple clé USB. Et le geste se veut un réflexe de prudence car l'outil peut servir de vecteur banal, mais efficace, à une cyberattaque.

Derrière cette attitude décidée et pragmatique se pose la question de savoir où caler le curseur entre la paranoïa aiguë et l'angélisme béat, à l'heure où l'informatique, les réseaux et les nouvelles technologies de l'information et de la communication (NTIC) infiltrent tous les instants de notre vie. Cybercriminalité et cyberterrorisme rappellent aux entreprises, aux Etats et aux particuliers, que la technologie bénéficie aussi aux moins bien attentionnés. Car les menaces élaborées dans le monde virtuel produisent des impacts réels.

Ainsi une étude de l'EPFL a dernièrement estimé qu'une impossibilité générale d'accès à internet pourrait coûter six milliards de francs par semaine au pays! Sans aller jusqu'à la paralysie totale, les cyberattaques peuvent produire des dégâts bien réels (lire ci-contre).

Quelles réponses

Devant la multiplicité des cyberrisques, il faut arriver «*à la collaboration de tous les acteurs concernés, car, des simples dangers aux grosses menaces, les réponses doivent être graduées entre les politiques criminelles qui ressortent du domaine civil et les politiques de sécurité qui relèvent du militaire*», analyse Gérald Vernez, ex-directeur suppléant du projet de cyberdéfense au Département de la défense (DDPS).

Mais pour apporter des réponses à ces menaces technologiques complexes, encore faut-il avoir identifié l'ennemi. Savoir qui se profile derrière la piraterie et les attaques numériques. Selon une étude française, le peloton de tête des Etats les plus cyberbelliqueux serait constitué de l'Allemagne, des Etats-Unis, de la Chine et de la Russie.

Le cybermonde connaît lui aussi sa course aux armements. Les réseaux ne cessent de se déployer (smartphones, cloud computing…) et toujours plus de données s'échangent. Cette situation génère de nouveaux besoins en termes de vitesse et de capacité. En parallèle, toute cette technique influe sur nos modes de vie et de consommation (e-administration, e-business).

Elle favorise aussi le dévoilement de la sphère privée et la collecte d'information via les réseaux sociaux.

Dès lors, les cyberattaques se doivent d'être aussi soudaines qu'anonymes, aussi rapides que «délocalisées»…

Et si la vigilance commence par un coup de talon sur une clé USB, elle se poursuit par la vérification du câblage de son ordinateur. Il est aussi très facile d'intercaler un intercepteur de données entre l'unité centrale et la prise clavier. Une petit «bitonio» aussi anodin que vicieux. Il passe inaperçu tout en étant capable d'enregistrer ce qui a été saisi dans la journée…

CONSÉQUENCES DES CYBERATTAQUES

AUTHENTICITÉ Falsifications de contenus web.

CONFIDENTIALITÉ Accès à des informations sensibles.

PROPRIÉTÉ Vol de données, de savoirs, de valeurs, etc.

FONCTIONNALITÉ Perturbations et altération du matériel informatique et/ou des appareils pilotés par ordinateur.

INTÉGRITÉ Destruction logique, physique ou électromagnétique de composants.

RÉPUTATION Dégradation d'une image individuelle ou collective.

INFO+

Voir:
www.melani.admin.ch. Melani est la centrale d'enregistrement et d'analyse pour la sûreté de l'information. Elle œuvre dans le domaine de la sécurité des systèmes informatiques, d'internet et dans celui de la protection des infrastructures nationales et vitales.
www.cybercrime.admin.ch. Il s'agit du site du Service national de coordination de la lutte contre la criminalité sur internet (SCOCI).

Lire:
Ouvrages de Solange Ghernaouti: «La cybercriminalité, le visible et l'invisible», collection Le savoir suisse, Presses polytechniques et universitaires romandes, 123p. «Sécurité informatique et réseaux», Editions Dunod, 384 p. En collaboration avec Arnaud Dufour, «Internet édition 2012», collection Que sais-je? Presses universitaires de France, 128p.