Cyber : "L'échec n'est pas une option"

Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

Une des trois discussions de la rencontre du RNS à Safenwil.
Toutes les illustrations © A+V.

Politique de sécurité

Cyber : « L'échec n'est pas une option »

Lt col EMG Alexandre Vautravers
Rédacteur en chef, RMS+

Le 4 mai dernier à Safenwil a eu lieu la troisième rencontre du Réseau national de sécurité (RNS). Le thème était la mise en œuvre de la stratégie de protection contre les cyber risques. Plus de 400 personnes ont répondu présent, témoignant d'une grande diversité d'origines professionnelles. Ainsi, 25 cantons, 7 départements fédéraux, 18 offices fédéraux et 11 villes étaient représentés.

Ricardo Sibilla, Chef analyse de risques cyber à la Base d'aide au commandement (BAC) de l'armée, a fait la démonstration que la conjugaison du « social engineering » et du « phishing » était pratiquement imparable. Les campagnes de prévention sont nécessaires mais ne sont pas efficaces à 100 %. Il faut donc une surveillance des systèmes.

Pierre-François Regamey, directeur des systèmes d'information au CHUV, a montré qu'avec l'internet des objets, les risques augmentent considérablement. Jusque ici l'électronique interconnectée ne pouvait pas causer de mal ou de morts physiques. Les objets connectés peuvent devenir une nouvelle cible. Pour Jean-Pierre Therre, de la banque Pictet, « *les risques cyber sont devenus les 'top risques.'* » Les partenariats publics-privés (PPP) existent mais sont généralement peu efficaces/utiles. L'Etat doit donc faire davantage.

Pour Roland Charrière, remplaçant du directeur de l'Office fédéral de la santé, les objets connectés induisent un « repli sur soi » psychologique. Comme dans le domaine de la santé, il faut que les individus se responsabilisent. La réglementation ne suffit pas, parce que les évolutions techniques dépassent les possibilités de mettre en place une législation adéquate. Il faut viser une philosophie 'safe by design' basée sur des tests avant la mise en service.

Le conseiller fédéral Guy Parmelin, chef du DDPS, a été clair « *L'échec n'est pas une option. (...) Nous n'avons pas non plus droit à l'erreur. (...) Les défis liés aux cyber risques sont clairement là. Nous n'avons pas d'autre choix que de les affronter. Il y a un peu plus de 100 ans, il nous a fallu apprendre à défendre notre pays dans les airs. Aujourd'hui, c'est la même chose dans le domaine du cyber espace.* » La cyber sécurité est devenue un thème à part entière dans les discussions avec France, l'Allemagne ou l'Autriche. « *Il s'agit d'un domaine central de notre politique de sécurité. (...) Le retour en arrière n'est ni possible, ni souhaitable.* »

« *Anticiper doit être plus qu'un slogan.* (...) *Simplement répéter le mantra 'résilience' ne sert à rien.* » Des mesures sont ainsi prises :

- La Stratégie nationale pour la sécurité informatique (SNPC) a été présentée le 26 avril dernier.
- Une nouvelle stratégie sera mise au point d'ici la fin de l'année.
- Un campus cyber sera mis en chantier d'ici 2020 avec trois domaines : anticipation, capacités, formation.

Peter Fischer, délégué au pilotage informatique de la Confédération, a présenté les lignes directrices de la SNPC :

- Responsabilité individuelle ;
- Flexibilité ;
- Coopération.

Michael Lauber, le procureur général de la Confédération (MPC), explicite le paradoxe du cyber : les cantons sont responsables pour l'ordre, y compris dans le domaine du cyber. Mais une attaque contre l'Etat ou contre une infrastructure critique sont du ressort de la Confédération. Les collaborations internationales sont essentielles, dans le cadre de la Cyber crime convention.

Beat Oppliger, procureur général du canton de Zurich, présente le centre de compétence mis sur pied en 2013, qui compte 20 postes, dont 10 issus de la police et 10 du MP. Pour lui, les facteurs de succès sont la rapidité, les compétences; la flexibilité dans l'attribution des cas/ tribunaux; enfin les ressources et moyens suffisants. La collaboration entre la police et le ministère publique est essentielle: ils travaillent donc sous le même toit et utilisent les processus. Il y a toujours une dimension intercantonale et internationale. A terme, il faudra donc créer des centres régionaux.

Le conseiller d'Etat bernois Hansjörg Käser voit le risque augmenter avec le nombre des objets intelligents. Des groupes de travail ont été mis sur pied:

- Concept conduite & processus en cas de crise (novembre 2016 exercice cadre EM à Schwarzenburg, 50 participants).
- Amélioration des processus de gestion des risques au sein des cantons.
- En 2014, 15 cantons (ainsi que la Principauté du Liechtenstein) ont participé à une évaluation de l'exercice en cours, afin de réduire les risques cyber.

En bref

La criminalité se déplace graduellement vers la cybercriminalité, en raison des mesures de protection et de surveillance de plus en plus efficaces dans le domaine physique (ex cameras, alarmes...).

Il faut distinguer entre deux échelons: local et national. Dans le domaine local des règles et exigences doivent être édictées (normes, standards minimaux). A l'échelle nationale, il faut davantage de moyens et un réel *leadership*.

A+V

Le conseiller fédéral Guy Parmelin a montré l'importance de la cyber défense dans les travaux du DDPS.

> *suite de l'article de la page 6*

Enfin il convient de rappeler que l'engagement des ressources encore disponibles ou l'acquisition des moyens supplémentaires requis se fait selon les priorités définies par l'autorité politique à qui incombe la responsabilité de trancher en dernier lieu.

Les systèmes d'information et de conduite

Le développement de la société de l'information et des systèmes de communication a pour conséquence que les autorités et acteurs sécuritaires doivent être en mesure de communiquer dans toutes les situations. Cela implique de pouvoir disposer de systèmes dédiés et sécurisés. L'exercice du Réseau national de sécurité 2014 a mis clairement en évidence que la Suisse avait des lacunes dans ce domaine. Le rapport final préconise ainsi la création d'un réseau de données sécurisé englobant la Confédération, les cantons et les exploitants d'infrastructures critiques.

Dans l'intervalle, l'Office de la protection de la population a mis en consultation un rapport sur l'avenir des systèmes d'alarme et de télécommunication. Sur cette base, il s'agira de fixer les priorités dans la réalisation des divers projets pour les prochaines années. Parallèlement Confédération et cantons devront définir les modalités de financement de ces systèmes. La révision de la loi fédérale sur la protection de la population et la protection civile offre une opportunité de fixer quelques principes de base qui vaudront pour l'ensemble des projets qui seront réalisés à l'avenir. Toute la difficulté résidera à trouver un équilibre entre les besoins avérés en matière de communication et les ressources financières disponibles tant au niveau de la Confédération et que des cantons.

Conclusions

Le système coordonné de la protection de la population restera à l'avenir également un élément essentiel du Réseau national de sécurité. Le développement des risques et dangers auxquels sont confrontés nos sociétés modernes en font un instrument incontournable de la politique de sécurité. Mais pour répondre à l'évolution de notre environnement sécuritaire, il convient d'adapter l'outil aux exigences et défis actuels. La révision législative engagée nous offre cette opportunité. Dans ce contexte, il convient également de réfléchir aux rôles respectifs de la Confédération et des cantons. Pour rappel, la quasi-totalité des moyens de la protection de la population sont en main des cantons qui ont une responsabilité primaires dans la gestions des catastrophes et situations d'urgence. Par conséquent, la Confédération au travers de l'Office fédéral de la protection de la population doit avant tout créer des conditions cadres qui permettent au système de la protection de la population d'être un instrument efficace, essentiellement sous la responsabilité des cantons, mais qui s'inscrit dans un référentiel commun.

A. D.