Plaidoyer en faveur d'un centre de compétence pour la cybersécurité

Lettre ouverte aux membres des Chambres fédérales

Zurich, le 24 juillet 2018

La motion Eder, qui demande la création d'un centre de compétence pour la cybersécurité, a été adoptée presque à l'unanimité à la fin de l'année dernière, contre l'avis du Conseil fédéral. Les services en ligne, et Internet en général, ont atteint depuis longtemps une taille critique, également en Suisse. Les menaces susceptibles de leur porter atteinte ne concernent plus seulement les grands acteurs. Une attaque de l'infrastructure suisse des technologies de l'information et de la communication (TIC) aurait des répercussions négatives durables pour la place économique helvétique. Mais des incidents TIC mineurs, en particulier dans les PME, affaiblissent déjà le pays sur le long terme. La majorité des États occidentaux, mais aussi asiatiques, l'ont compris depuis longtemps.

Le 4 juillet 2018, le Conseil fédéral a finalement réagi de mauvaise grâce à la motion Eder : il nommera un Monsieur ou une Madame Cyber, une personnalité de haut rang, qui n'aura cependant pas le pouvoir de donner des instructions, en dépit de ce que demandait la motion. De plus, les départements concernés n'arrivent apparemment pas à se mettre d'accord sur une procédure commune. Ce n'est guère une surprise dans le paysage politique suisse, mais cela garantira une fois de plus l'insatisfaction générale et l'absence de solution en perspective. Dans le domaine de la cybersécurité, la Suisse accumule du retard. La mise en œuvre de la motion Eder permettrait de passer à l'action et d'empêcher que la position actuelle ne s'éternise.

Le Parlement ne doit donc rien céder sur l'application de la motion Eder ; il doit sommer le Conseil fédéral d'accomplir cette mission et de ne pas ignorer la volonté du Parlement. Le Conseil fédéral et l'Administration, en procédant de la sorte, donnent l'impression de placer des intérêts particuliers avant la sécurité de la place économique suisse.

Il est à présent urgent d'élaborer une stratégie digne de ce nom. Dans l'idéal, elle devrait être mise au point conjointement par la Confédération et le secteur privé, avec la participation d'experts nationaux et internationaux. Il est indispensable que cette stratégie réponde aux questions suivantes. Une analyse détaillée de chaque point et de son contexte figure plus bas.

1. Comment coordonner concrètement les actuelles parties prenantes dans le domaine de la cybersécurité ? En particulier, les autorités cantonales, les autorités juridiques l'armée et le DFAE.
2. Comment assurer la pleine protection de l'ensemble de la place économique suisse ? Pas seulement celle de quelques infrastructures sensibles, mais aussi celle des PME ?
3. Quel est le pouvoir directionnel du centre de compétence ?
4. Comment les initiatives actuelles des différentes parties prenantes peuvent-elles être renforcées et intégrées à ce centre ?
5. Comment seront concrètement appliquées les mesures de la stratégie nationale de cybersécurité et comment seront-elles évaluées ? Comment le centre de cybersécurité peut-il davantage accroître la résilience et la responsabilité des autorités et de l'économie ?

Les questions stratégiques et leur contexte :

Comment coordonner les actuelles parties prenantes ?

Dans la Suisse fédérale, une multiplicité d'acteurs se préoccupent de cybersécurité. En règle générale, ils font du bon travail, mais demeurent mal connectés les uns avec les autres. Dans le meilleur des cas, il en résulte des doublons ; mais, dans le pire des cas, le manque de coordination anéantit les efforts et les initiatives. En outre, le système fédéral empêche que tous les sujets bénéficient de l'attention nécessaire, ce qui signifie que les activités existantes présentent des lacunes. Il est urgent qu'un service de coordination réunisse tous les acteurs autour d'une table pour consolider et développer les initiatives actuelles ou nouvelles.

Comment assurer la pleine protection de l'ensemble de la place économique suisse ?

Les initiatives actuelles se concentrent en général sur certains aspects de la répression (fraude, pornographie illégale), ainsi que sur des infrastructures critiques. Or les performances économiques de la Suisse sont avant tout fournies par les PME, qui ne reçoivent aucun soutien alors qu'elles s'avèrent nettement plus vulnérables. En effet, les exploitants d'infrastructures sensibles disposent souvent de départements informatiques bien développés.
Les menaces pesant sur les PME sont donc considérables. Là aussi, un centre de compétence contribuerait à renforcer les initiatives existantes et à combler les éventuelles lacunes, en collaborant le cas échéant avec des partenaires. Il importe à cet effet d'élaborer au préalable une stratégie ciblée, qui devra définir quelles sont les attentes relatives à ce centre de compétence et comment il doit être conçu. De plus, ce centre a besoin d'une direction forte, capable de convaincre les associations utiles à sa cause.

Quel est le pouvoir directionnel du centre de compétence ?

La réponse est délicate : il est cependant évident que les directives d'un service indépendant sont bien mieux acceptées que celle d'une organisation qui poursuit également d'autres intérêts. L'expérience à l'étranger montre qu'un centre bien établi, qui soigne ses relations avec ses clients, fait plus rarement usage de son pouvoir directionnel. Mais cela implique qu'il soit fort et crédible.
Des représentants de l'économie privée ont déclaré à plusieurs reprises qu'ils ne voyaient aucun problème à collaborer avec un service étatique. En revanche, il est inacceptable pour eux de devoir travailler sur le même thème avec plusieurs services en même temps. Actuellement, les sociétés TIC sont régulièrement contactées par l'OFAE, MELANI, l'OFCOM et d'autres services fédéraux pour les demandes les plus diverses, ce qui n'est ni crédible, ni efficace.

Comment les initiatives actuelles des différentes parties prenantes peuvent-elles être renforcées et intégrées au centre ?

Aux Pays-Bas, le NCSC expérimente un modèle très prometteur : les partenaires importants envoient régulièrement des « liaison officers » au NCSC. Ces agents de liaison travaillent un jour par semaine sur place et peuvent inviter des personnalités, ce qui garantit une bonne circulation de l'information et permet d'établir une relation de confiance avec tous les partenaires. La fréquence et la forme de ce modèle peuvent naturellement être discutées. Mais un contact régulier et continu est essentiel. C'est le seul moyen de développer une relation de travail transparente et efficace en cas de crise.
Un élément important de la SNPC 2.0 repose sur l'état des lieux au niveau national. Il est peu probable qu'une organisation qui se préoccupe avant tout d'elle-même puisse établir un tel état des lieux. D'où proviennent les informations nécessaires ? Qui les rassemble ? Qui

garantit leur exhaustivité ? Qui les analyse ? Ces questions sont cruciales et les propositions actuelles n'y répondent pas.

La Confédération ne doit-elle pas se concentrer exclusivement sur des infrastructures sensibles ?

Le concept d'infrastructures sensibles implique qu'elles se différencient des autres infrastructures, comme par exemple une centrale nucléaire, qui se distingue clairement en tant que telle. Sur Internet, toutefois, cette différenciation n'existe plus. Quand ils sont infectés par millions, les plus petits appareils peuvent devenir une arme dangereuse. C'est ce qui est arrivé par exemple quand Mirai Botnet, à partir de simples webcams, a paralysé toute une journée le réseau internet aux États-Unis. Un service central s'avère donc nécessaire pour pouvoir à la fois avoir une vue d'ensemble et distinguer les cas individuels, lorsque la somme de petits problèmes informatiques se transforme en un incident de taille.

Comment évaluer les résultats des mesures planifiées ?

Toutes les initiatives actuelles s'attachent à des questions sectorielles. Il n'est donc pas évident de savoir comment est mesuré le résultat de chacune. Sans vision globale, il est difficile en effet d'estimer l'efficacité d'une activité. En s'appuyant sur un état des lieux exhaustif, un service central peut identifier et consolider les initiatives fructueuses.

Faire mieux avec moins

On pourrait objecter que le Conseil fédéral s'est au moins préoccupé de la question, qu'il a cherché la meilleure solution « en fonction des circonstances » et que la situation a progressé. Mais ce serait une conclusion erronée. Investir beaucoup d'argent dans une mauvaise solution provoque des dégâts. Si la démarche n'est pas coordonnée, ce sont les agresseurs qui seront les premiers gagnants. Ils profitent déjà aujourd'hui du manque de collaboration internationale. Amplifier cette situation avec des structures intercantonales et interdépartementales compliquées serait une erreur grave et coûteuse, qui rendrait la Suisse pratiquement impuissante dans la lutte contre les cybermenaces.

Conclusion

La solution proposée par le Conseil fédéral est insuffisante à bien des égards. Elle reflète l'attitude négative que l'exécutif a adoptée dès le départ sur la question.
Il est grand temps que la Suisse s'attelle à la problématique des cybermenaces et renonce à son esprit de clocher dans ce domaine. L'enjeu est énorme : le pays risque de se retrouver sur une « cyber-voie de garage ». Mais si la Suisse entend devenir un pôle de la Crypto Valley et un leader dans la recherche TIC, elle doit également garantir la cybersécurité. À cet égard, il faudra bien davantage qu'un Monsieur ou Madame Cyber et quelques experts, qui, de par la structure du système, devront avant tout se préoccuper d'eux-mêmes.

Il ne s'agit pas de réinventer entièrement la roue : une comparaison avec des initiatives fructueuses à l'étranger s'impose et fournira un élan utile au développement d'une solution adaptée à la Suisse.

Dr Daniel Stauffacher, fondateur et président, ICT4Peace Foundation, Zurich
Dr Stefanie Frey, directrice de Deutor Cyber Security Solutions, Berne
Dr Serge Droz, directeur du Forum of Incident Response and Security Team, Zurich

Anhang: NZZ Kommentar vom 26.6.2018

Für einen sicheren Internetplatz Schweiz

Im Bereich Cyber-Security besteht die Notwendigkeit der Schaffung eines integrierten Kompetenzzentrums, das alle Fäden zusammenführt.

Serge Droz, Stefanie Frey und Daniel Stauffacher26.6.2018, 10:50 Uhr

In der NZZ vom 6. 6. 18 berichtet der Bundeshauskorrespondent Lukas Mäder über Ansätze der Umsetzung eines parlamentarischen Vorstosses zur Schaffung eines zentralen Cyber-Security-Kompetenzzentrums. In typisch föderaler Manier und guteidgenössischer Gärtchenpflege wird um Hoheiten gestritten und ein Jekami-Modell favorisiert. Vergessen geht in der Bundesverwaltung, dass die Welt nicht schwarz oder weiss ist: Die Schaffung eines starken Kompetenzzentrums heisst nicht, dass bestehende und gut funktionierende Strukturen aufgelöst werden.

Melani

Tatsächlich besteht die Notwendigkeit für ein Kompetenzzentrum, das zentral alle Fäden zusammenführt. Beispielsweise ist der bundesrätliche Grundauftrag der Melde- und Analysestelle Informationssicherung (Melani) der Schutz kritischer IT-Infrastrukturen. Diese Aufgabe erledigt Melani trotz zum Teil erschwerten Umständen hervorragend. Herzlich wenig hilft dies jedoch KMU, die zwar in der Summe den Grossteil der wirtschaftlichen Leistung erbringen, aber einzeln keine kritische Infrastruktur sind. Auch besitzt Melani nicht die, richtigerweise, beim EDA angesiedelte Kompetenz, spezifische Interessen bei ausländischen Partnern einzubringen. Ausserdem stoppt das Internet bekanntlich nicht an den Kantonsgrenzen. Deshalb müssen sich auch die kantonalen Akteure, die schwergewichtig für die Strafverfolgung verantwortlich sind, in einer moderierten Plattform koordinieren können.

Ausserdem stoppt das Internet bekanntlich nicht an den Kantonsgrenzen.

Auch bei der Reaktion auf erfolgreiche Hackerangriffe kocht die Schweiz auf Sparflamme: GovCERT.ch, das nationale Computer Emergency Response Team des Bundes, ist zwar mit Topleuten besetzt, doch es fehlt an ausreichenden Ressourcen. Auch ist die IT-Industry (Produktehersteller) nur ungenügend in die heutige Konstellation eingebunden. Dass heute Industrieanlagen angegriffen werden, ist kein Geheimnis mehr, es fehlt jedoch an einer spezialisierten Organisation (ICS-CERT), welche sich dieses Themas annimmt. Die Schweiz ist nicht das einzige Land, das sich gegen Bedrohungen aus dem Cyber-Raum schützen muss.

Ein Blick auf europäische Länder lohnt sich. Er zeigt, dass sich die erfolgreichen Länder entwickelt haben: von einem dem Schweizer Modell ähnlichen Konstrukt, das sich auf den Schutz kritischer Infrastrukturen konzentriert hat, zu einem System mit einem starken nationalen Cyber-Security-Zentrum. So wurden in den Niederlanden, in Grossbritannien und Finnland National Cyber Security Centers (NCSC) geschaffen, welche alle bestehenden Akteure zusammenbringen. Exemplarisch und durchaus ein Vorbild für eine mögliche Schweizer Variante ist das NCSC.nl, das alle relevanten Stakeholder durch Liaison-Officers einbindet, welche mindestens einen Tag in der Woche, quasi als ständige Gäste, im Kompetenzzentrum arbeiten. Das physische Zusammenbringen aller Akteure impliziert auch, dass relevante Information zentral zur Verfügung steht und ausgewertet werden kann. Dies ist für das in der NCS-Strategie geforderte Lagebild unabdingbar.

Milizorganisationen

Wichtig ist in der Schweiz auch das Einbinden von Milizorganisationen: Hier könnte das lettische Modell Pate stehen, das zur Unterstützung der Behörden qualifizierte Freiwillige einbindet, welche ein bis zwei Tage im Monat zur Verfügung stehen. Die Schweiz ist mit solchen Arrangements bestens vertraut.

Der erwähnte parlamentarische Vorstoss zielt in die richtige Richtung. Es gilt nun, das Momentum zu nutzen, damit der Internetplatz Schweiz weiterhin zu den sichersten der Welt gehört. Und hier scheint ein NCSC an einem zentralen Ort notwendig zu sein. Von dem ewigen

Gerangel der Departemente, wer denn nun die prestigeträchtige Aufgabe Cyber-Security übernehmen könnte, profitieren gemäss der Doktrin «Divide and Conquer» vor allem ausländische Nachrichtendienste und Kriminelle.

Serge Droz ist Direktor des Forum of Incident Response and Security Team
Stefanie Frey ist Geschäftsführerin von Deutor Cyber Security Solutions
Daniel Stauffacher ist Gründer und Präsident von ICT4Peace Foundation