Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2018)
Heft: [2]: Numéro Thématique 2

Artikel: Une norme pour régler un problème hors norme?
Autor: Koch, Stéphane
DOI: https://doi.org/10.5169/seals-823450

Le bâtiment du Ministère public de la Confédération (MPC), à Berne.

Cyber

Une norme pour régler un problème hors norme?

Stéphane Koch
Digital strategist & digital literacy coach

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) à publié un ensemble de recommandations, sous la dénomination suivante: norme minimale pour améliorer la résilience informatique. Il s'agit d'une recommandation, voire d'une ligne directrice pour améliorer la résilience informatique. Elle s'adresse en premier lieu aux exploitants d'infrastructures critiques, mais toute entreprise peut appliquer ces conseils gratuits.

La norme comprend trois parties:
- Principes de base ou guide de référence fournissant des informations sur la résilience des TIC.
- Le cadre (Framework) propose aux utilisateurs une série de mesures concrètes à mettre en œuvre. Il est subdivisé en cinq thèmes : identifier, protéger, détecter, réagir et récupérer.
- L'outil d'appréciation permet aux entreprises d'évaluer le degré de leur résilience informatique, ou de le faire vérifier par des externes (audit).

Dans la présentation de son document, l'OFAE indique: « *Il incombe à chaque entreprise d'assumer sa protection en la matière. Toutefois, comme à chaque fois qu'il en va du bon fonctionnement des infrastructures critiques, il existe une responsabilité étatique, fondée sur un mandat ancré dans la Constitution fédérale et dans la loi sur l'approvisionnement du pays. La présente norme minimale pour les TIC traduit la responsabilité de l'État qui doit protéger ses citoyens, le secteur privé, les institutions et l'administration publique.* »

Ce document est apparu le même jour où le Ministère public de la Confédération (MPC) a annoncé qu'il suspendait la procédure pénale en lien avec l'enquête visant à identifier les auteurs et/ou commanditaires des cyberattaques dont RUAG avait été victime, entre 2015 et 2016. Cette décision et ses conséquences ne sont pas anodines. Ce n'est ni plus ni moins qu'un aveu public d'échec. Et c'est aussi la troisième fois que le MPC classe un cas de ce type. Les départements des Affaires étrangères et de la Défense, avaient également subi des cyberattaques en 2017.

C'est un message inquiétant qui a été envoyé à tous ceux qui pourraient viser les intérêts de la Suisse. Que cela soit au niveau économique, politique, ou stratégique. Ce type de cyberattaques pourrait être considéré comme une version moderne et dématérialisée d'une stratégie asymétrique. La nouvelle (cyber) arme de la géopolitique et de la guerre économique.

A la différence que ce n'est pas nécessairement le faible qui attaque le fort, du moins si on réfléchit en termes de capacité à se défendre par celui qui est attaqué. Dans cette nouvelle dynamique, le fort peut aussi être le faible. La Suisse est forte économiquement, mais faible dans sa capacité à se défendre, ce qui en fait une cible d'autant plus intéressante. Et l'annonce du MPC sonne comme une confirmation de cette situation de faiblesse.

Il est véritablement temps qu'une prise de conscience s'opère de manière transversale, d'abandonner le fédéralisme de la gouvernance, comme celui des idées, afin de faire fi des dissensions et laisser enfin la place à une stratégie unie et concertée, à même d'anticiper et au besoin, d'avoir la capacité d'endiguer ou de stopper des attaques cybernétiques dont notre pays est l'objet.

Il ne s'agit pas de uniquement de protéger les infrastructures critiques de notre pays, mais de comprendre que la sécurité de ces infrastructures, entre autres, protège l'économie et la souveraineté de la Suisse.

Pour y arriver, il s'agit aussi de réussir à protéger les entreprises et les particuliers, des risques cyber. Il faut

augmenter le niveau de conscience et de connaissance de chaque citoyen en la matière.

Mais la Suisse accumule les retards dans les domaines de la cybersécurité. En mai 2017, le Conseil fédéral avait rejeté le projet de création d'un office dédié à la cybersécurité. Et ce n'est qu'en juillet 2018, que le celui-ci a pris les premières décisions de principe en vue de la création d'un centre de compétence matière de prévention et de lutte contre les cyber risques. Ce centre devait ensuite être rattaché au Département fédéral des finances (DFF), ce qui ne fait pas nécessairement sens, par rapport à la problématique traitée.

Il en va de même avec le Règlement général de l›UE sur la protection des données (RGPD). La Suisse est non seulement restée sur la touche concernant cette nouvelle réglementation européenne entrée en force en mai 2018, mais sa loi sur la protection des données (LPD) sera obsolète dès sa sortie. Cela alors même que la Suisse veux se positionner comme le « futur coffre-fort numérique du monde Ingénieur en gestion de fréquences, Armasuisse ».

Quel est le message que l'on envoie, quand on refuse d'adopter un cadre contraignant pour les entreprises en matière de cyber sécurité ? Dans le même temps, les failles informatiques et les négligences en termes de sécurité, de certains fleurons de notre industrie, font la une des médias ? Que dire, quand la Suisse accuse deux jours de retard dans la communication d'informations sur les failles « Spectre » et « Meltdown », début janvier, alors que tous les centres nationaux européens et internationaux de cybersécurité avaient communiqué en temps et en heure ?

La cybersécurité est non seulement indissociable de tout ce qui touche à la transformation numérique de notre société, mais c'est aussi la garantie de notre capacité à protéger un patrimoine économique qui est de plus en plus dématérialisé - le nôtre, mais aussi celui des entreprises étrangères qui sont établies ici, ou celles que l'on cherche à faire venir.

Toute perte financière liée soit à une faille de sécurité ou à un acte cybercriminel, représente un montant qui ne sera pas dépensé, investi ou épargné, sur le territoire helvétique. Cela a un impact non seulement sur la confiance des ménages, mais aussi sur le dynamisme économique des entreprises et potentiellement sur leur capacité à innover.

De plus, à l'heure actuelle, il n'existe aucunes statistique fiables sur l'impact de la cybercriminalité en Suisse. Ce genre de données essentielles devrait figurer en bonne place sur le site du SECO, dans les « prévisions conjoncturelles » et respectivement au niveau de « l'indice du climat de consommation ».

Comme on ne peut que le constater, la Suisse est confrontée à de multiples risques et défis, mais elle peine à y faire face. Malheurseument, plus par manque de conscience que par manque de moyens.

S. K.