Pour faire face aux pirates numériques qui visent notre pays, certains préconisent la création d'un Secrétariat d'État à la cybersécurité. (Ev)

DES TROUS DANS LA CYBERSÉCURITÉ

par Thierry Oppikofer

MEMBRE DE LA TASK FORCE COVID FÉDÉRALE JUSQU'À SA DÉMISSION EN FÉVRIER 2021, MARCEL SALATHÉ EST COFONDATEUR ET PRÉSIDENT DE CH++ QUI VISE À FACILITER ET À ACCÉLÉRER LA TRANSITION NUMÉRIQUE DE LA SUISSE. ÉPIDÉMIOLOGISTE NUMÉRIQUE ET PROFESSEUR À L'EPFL, IL ESTIME QUE L'ÉTAT PEINE À PRENDRE LA MESURE DES ATTAQUES INFORMATIQUES QUI S'ABATTENT SUR NOTRE PAYS.

Une question faussement naïve pour commencer : peut-on dire que la sécurité numérique est globalement assurée en Suisse ?

Il y a deux aspects de la cybersécurité qui sont, d'ailleurs, liés. D'un côté, la sécurité générale des infrastructures à l'échelon des administrations et des entreprises ; de l'autre, la sécurité individuelle des citoyens quant à leurs données et leur intimité. Les enjeux sont clairs : comment bénéficier d'un cadre numérique général sûr, qui permette le développement des activités économiques, sociales, culturelles, sanitaires, sans risquer un piratage ou un blocage ? Sur le plan individuel, comment éviter d'être tracé, surveillé, voire harcelé ou escroqué ? Disons d'emblée que je ne juge pas la situation sécuritaire numérique suisse satisfaisante aujourd'hui. Il y a des lacunes et des écarts dangereux. L'essor d'Internet, encore agrémenté par la crise du Covid-19, a permis une accélération de la modernisation du pays, à l'instar des pays voisins, en matière numérique.

Mais comme on l'a vu avec les attaques informatiques contre des communes et des entreprises, la sécurité n'a pas suivi ; on ne l'a pas prise assez au sérieux. Or, c'est au plus haut niveau que l'impulsion doit être donnée et les mesures adéquates prises. Sinon, les infrastructures de base, transports, énergie, santé, pourraient être menacées.

Le risque principal est-il le vol de données ou le chantage ?
C'est finalement la même chose. On s'empare des informations sensibles et on les revend, à leur propriétaire légitime ou à d'autres. La Suisse est à cet égard extrêmement séduisante aux yeux des pirates informatiques : un pays riche et une méfiance insuffisante vis-à-vis des menaces invisibles.

« LA SUISSE EST EXTRÊMEMENT SÉDUISANTE AUX YEUX DES PIRATES INFORMATIQUES. »

Marcel Salathé, président de CH++

Qu'a-t-on fait à ce jour pour accroître la sécurité numérique et que devrait-on faire ?
Un premier pas a été la fondation du Centre national pour la cybersécurité (NCSC) à Berne. C'est une étape importante. Logiquement, l'accent a d'abord été mis sur la défense, mais chacun a compris que comme le numérique, la cybersécurité devait être approchée de façon transversale, interdépartementale. C'est la raison pour laquelle, à CH++, nous militons pour la création d'un Secrétariat d'État à la cybersécurité, doté des moyens nécessaires pour coordonner les actions publiques et privées, fédérales et locales. Car la petite centaine de collaborateurs du NCSC s'avère à l'évidence insuffisante. On compte des dizaines de spécialistes là où il faudrait en dénombrer des centaines !

Ne sommes-nous, selon vous, qu'au début du phénomène de piratage ?
On peut le craindre. La fréquence et la gravité des cas augmentent. On ne peut espérer « donner un coup de collier » et régler le problème une fois pour toutes. Il convient de se maintenir sans relâche au plus haut niveau. En matière de sécurité, l'attaque portera toujours sur le maillon le plus faible de la chaîne.

Les acteurs privés de l'économie ne sont-ils pas mieux armés que l'État fédéral ou les Cantons ? On pense évidemment aux banques, à l'horlogerie, à la chimie…
Le rôle des privés est bien entendu primordial : ils sont les responsables opérationnels de la sécurité. Mais il importe que les pouvoirs publics se préoccupent des systèmes d'infrastructure, assurant le fonctionnement du pays et de l'économie. Sécuriser les dispositifs utilisés par les CFF, le transport aérien, les grands hôpitaux, les fournisseurs d'énergie et de communication – sans parler de l'Armée – est à l'évidence une priorité absolue. Et si une société privée a des responsabilités stratégiques pour la santé, le bien-être ou l'approvisionnement de la population, l'État est obligatoirement concerné par sa sécurité.

Dispose-t-on de suffisamment de spécialistes en cybersécurité ?
Les écoles polytechniques et les HES en forment, mais la demande est forte et la surenchère salariale bien présente. Du côté étatique, il est difficile de dépasser les grilles de rémunération réglementaires.

Les budgets affectés à une cybersécurité telle que vous la décrivez risquent d'être imposants…
Mais toujours moins que ce que coûterait une importante cyberattaque !

Quels sont les buts et le rôle de CH++ ?
Nous cherchons à concrétiser notre vision d'une Suisse forte sur le plan numérique et technologique, partant du principe que les décisions politiques doivent se fonder sur des bases scientifiques. Dans le contexte des élections fédérales de 2023, nous allons tenter d'évaluer les compétences des candidats, de promouvoir des élus et des administrations capables de faire face aux défis du présent et de l'avenir, notamment aussi en matière de cybersécurité. CH++ est un groupe civique, indépendant des intérêts industriels ou académiques ; nous ne touchons aucune subvention. Coopérer, critiquer, lancer des alertes sont des aspects de notre mission.

Est-il intelligent, comme le prévoit la Berne fédérale, de confier le stockage de certaines données à des pays étrangers, par exemple à la Chine communiste ?
Précisons que des solutions entièrement suisses – jusqu'au niveau de la puce – ou même européennes sont illusoires. Mais il importe que le stockage de données à l'étranger soit limité à des domaines du type météorologique, par exemple. Les données sensibles doivent rester en Suisse. N'oublions pas que tout ce qui

est sur Internet, comme le contenu des posts sur les réseaux sociaux, y reste pour toujours et ne peut plus être effacé.

Peut-on imaginer un blocage général d'Internet ?
Non. Le réseau est trop décentralisé et les redondances multiples. En revanche, on sait que cela peut arriver à l'échelle d'un pays.

Les certificats Covid ont-ils été un moyen pour l'État de pister les citoyens ?
Bien utilisée, la technologie des passes sanitaires et des applications Covid fonctionne parfaitement, sans violation du tout de la vie privée. Pour SwissCovid, il s'agit d'avertir les personnes d'une contamination possible et de protéger la population. Peut-être que certains pays voisins ont mieux rentabilisé le système que la Suisse, où une partie du système de santé est malheureusement restée sceptique. ■

« IL FAUT RENDRE L'ANNONCE DE PIRATAGE OBLIGATOIRE »

Conseillère aux États fribourgeoise et vice-présidente du Parti libéral-radical suisse, Johanna Gapany a été la plus jeune élue à la Chambre haute du parlement, en 2018. Son élection avait alors été entachée d'une panne informatique. Autant dire que cette dynamique sénatrice est pleinement consciente des avantages, mais aussi des inconvénients, de la société numérisée !

Votre motion, déposée à la fin de l'an dernier après une série d'attaques informatiques contre des communes, des institutions et des entreprises, a été transmise en commission. Est-ce un bon ou un mauvais signe ?
C'est un bon signe. Actuellement, seules les infrastructures critiques font l'objet d'une protection fédérale contre les cyberattaques. Je demandais l'extension de cette protection aux Cantons, aux Communes et aux petites et moyennes entreprises. Le cambriolage numérique et le vol de données, même dans le cadre privé d'une PME, sont parfois d'importance nationale et peuvent mettre à mal la sécurité des citoyens. Je vous donne un exemple qui s'est passé chez nos voisins français : des informations sensibles sur le dossier *Charlie Hebdo* se sont retrouvées sur le *dark web*. Cela incite à prendre des mesures tant qu'il est encore temps.

Jugez-vous la situation actuelle alarmante ?
Elle l'est et c'est la raison pour laquelle la commission compétente doit prendre en main cette question au plus vite. L'un des freins actuels étant l'isolement des entreprises concernées, nous pouvons saisir l'occasion qu'offre la révision de la loi fédérale sur la sécurité de l'information pour, notamment, rendre l'annonce de piratage obligatoire. Cela ne signifie pas la publication de cette dernière, mais un signalement aux services de police pour que les victimes soient soutenues. Pour lutter efficacement contre les *hackers*, il est nécessaire d'avoir le plus d'informations possible. Le Centre national pour la cybersécurité (NCSC) doit également en être conscient afin d'étendre ses prestations et conseiller au mieux les pouvoirs publics et les entreprises.

La création d'un Secrétariat d'État à la cybersécurité vous paraît-elle une bonne idée ?
Davantage que le nom ou le statut, c'est la mission et l'organisation qui comptent. Le développement de la protection doit être coordonné et les prestations doivent découler de synergies entre les Communes, les Cantons et la Confédération, entre les secteurs privés et publics et les différents offices fédéraux. Nous avons dans ce pays suffisamment de gens compétents pour développer une protection efficace afin d'anticiper les menaces. Une clarification me semble essentielle quand on parle du rôle de l'État qui est chargé de la protection des citoyens et doit la garantir. Cela ne signifie pas que la Confédération doit tout financer. Certaines prestations, par exemple fournies aux entreprises, aux Communes ou aux Cantons, peuvent être payantes.

Justement, les grands groupes passent pour être mieux protégés grâce à leurs propres dispositifs que les administrations et les services publics. Ne devrait-on pas les laisser faire ?
Vu l'actualité, il ne semble pas y avoir de système sans faille. Certes, certaines entreprises sont conscientes des risques et prennent toutes les précautions possibles, mais ce n'est pas le cas de toutes celles qui détiennent des données privées, voire sensibles, de leurs clients. Pour ma part, je comprends bien que personne n'ait envie de rendre public un vol de données, mais une annonce à la police (qui ne signifie pas qu'elle est rendue publique) est nécessaire si on veut pouvoir anticiper d'autres attaques et adapter la protection à l'évolution des techniques utilisées par les *hackers*.
Propos recueillis par Thierry Oppikofer ■