

Que devraient faire les autorités suisses face au fléau des cyberattaques ? (4)

Technologie

Abonné

Menées par des pirates de plus en plus efficaces, les attaques se multiplient à un rythme impressionnant. Plusieurs experts interrogés par «Le Temps» esquissent des pistes pour une implication accrue des autorités



[n/a — © Olivier Ploux](#)



[Anouch Seydtaghia](#)

Publié mercredi 12 janvier 2022 à 18:23

Modifié jeudi 13 janvier 2022 à 08:49

- -
- -
- -
- -
-
-

C'était prévisible. Et c'est déjà devenu réalité. Il n'est désormais plus possible de tenir à jour la liste des entreprises et administrations suisses victimes de cyberattaques. Les agressions sont incessantes. Depuis l'annonce, mardi soir, du piratage de l'importateur automobile Emil Frey, de

nouveaux incidents se seront certainement produits au moment où vous lisez ces lignes. Et de plus en plus, une question se pose: que font et que devraient faire les autorités pour lutter contre ce fléau?

La question avait été posée frontalement par Johanna Gapany l'automne dernier. Via une motion, la conseillère aux Etats (PLR/FR) avait demandé que le Conseil fédéral soit «chargé d'étendre la protection fédérale contre les cyberattaques aux cantons, aux communes et aux PME dans leur ensemble». Exclu, lui avait alors répondu le gouvernement: ce sont aux administrations et aux PME de se défendre elles-mêmes.

Lire aussi: [Face aux cyberattaques, «le canton de Vaud ne peut pas faire beaucoup plus», avertit Nuria Gorrite](#)

Mais l'histoire ne s'arrête pas là. *Le Temps* a interrogé plusieurs experts en cybersécurité, qui esquissent des pistes pour améliorer la situation. Les autorités devraient en faire davantage, affirment-ils, sans pour autant se transformer en nounous du numérique. «Les cyberattaques sont semblables aux cambriolages. La police peut informer et faire des recommandations, mais c'est aux particuliers et aux entreprises de faire installer des portes solides et de ne pas laisser traîner les clés», image Philippe Oechlin, directeur de la société Objectif Sécurité à Gland (VD). Selon le spécialiste, la grande majorité des intrusions sont dues à trois erreurs: «Les systèmes d'accès à distance (pare-feu, serveur VPN) qui ne sont pas tenus à jour. Des accès à distance qui ne nécessitent pas un deuxième facteur en plus d'un mot de passe. Et, enfin, des postes de travail configurés de manière à ce qu'il soit encore possible, en 2022, de s'infecter en ouvrant une pièce jointe.»

Lire également: [Le marché suisse de la cybersécurité dopé par les cyberattaques](#)

Aux responsables informatiques de se prendre en main, donc. Mais l'Etat peut aider, suggèrent les experts interrogés, esquissant cinq pistes.

1. Mieux partager les informations

Selon Tobias Ellenberger, directeur opérationnel de la société de cybersécurité Oneconsult basée à Thalwil (ZH), «chaque acteur, qu'il s'agisse d'un Etat ou d'une entreprise, dispose de ressources différentes, mais aussi de perspectives et de connaissances sur les incidents. Si l'on veut prendre des mesures efficaces contre la cybercriminalité, il faut partager ces informations, voire, éventuellement, les spécialistes.» Car les ingénieurs en cybersécurité se font rares. «Les autorités fédérales, mais aussi les entreprises privées, sont confrontées à une «guerre des talents» combinée au nombre croissant d'incidents liés aux *ransomwares*, poursuit Tobias Ellenberger. Il est important d'utiliser les ressources limitées de manière ciblée.»

Les autorités pourraient publier davantage d'informations techniques sur les attaques qui leur sont déclarées, suggère Philippe Oechlin: «Il serait intéressant de savoir exactement par quelle faille les criminels ont réussi à pénétrer le réseau d'une entreprise. Cela permettrait aux sociétés qui utilisent les mêmes configurations de se protéger.» Le directeur d'Objectif Sécurité note que sur sa page web, le Centre national pour la cybersécurité (NCSC) publie déjà des informations pertinentes et compactes à l'adresse des PME. «On y trouve des mesures techniques et organisationnelles, et même des formulaires d'autoévaluation quand les liens fonctionnent. Le NCSC pourrait investir davantage de ressources pour tenir à jour ces informations. Il pourrait aussi créer, pour les PME,

une copie du réseau d'information qu'elles utilisent pour échanger des informations sur les cyberattaques avec les entreprises jugées critiques en Suisse.»

2. Créer une hot-line

Lors d'une cyberattaque, qui appeler? «En l'état actuel, une famille victime d'une cyberattaque ne sait pas vraiment vers qui se tourner pour se défendre et réagir correctement, et ensuite pour réparer les dégâts occasionnés», constate Christophe Gerber, directeur de la division ELCA Security. Selon lui, «on pourrait imaginer une sorte de hot-line à disposition des entreprises et des particuliers. En cas de coup dur, une force d'intervention [de réponse aux incidents] pourrait intervenir sur le terrain. Comme la police le fait dans le monde physique.»

Christophe Gerber estime que la police «devrait se rapprocher des entreprises expertes dans le domaine et, cela, de manière proactive. Attendre qu'un événement se produise pour tisser des liens n'est pas une bonne stratégie et n'est pas particulièrement efficace.» Pour le spécialiste, les torts sont partagés: «Une minorité d'entreprises ont des capacités de détection des incidents et très peu savent qui appeler lorsqu'il y a une attaque. C'est dommageable et inquiétant.»

Lire l'éditorial: [Face aux cyberattaques, l'Etat n'est pas à la hauteur](#)

Et cela pose la question des moyens que possède la police... «Certains corps de police traitent les plaintes déposées par les victimes de manière très professionnelle. D'autres peuvent manifestement s'améliorer. Il est clair qu'aucune police ne peut enquêter sur absolument tous les incidents. Mais abandonner n'est pas la bonne décision, car cela légitimerait les activités de cybercriminalité», note Marc Ruef, de la société zurichoise de sécurité Scip.

3. Renforcer le Centre national pour la cybersécurité

Fin 2021, le Centre national pour la cybersécurité (NCSC) comptait une trentaine de collaborateurs et une dizaine de postes vacants. Insuffisant, selon les spécialistes interrogés. «La lutte contre les cyberattaques nécessite des ressources importantes en personnel: il faut surveiller les menaces, comprendre les attaques, diffuser les informations, améliorer la sécurité. Les statistiques montrent clairement qu'une augmentation des ressources en personnel serait très utile», martèle Marc Ruef.

Selon Christophe Gerber, le NCSC pourrait avoir davantage de pouvoir. «C'est un acteur clé dans la cybersécurité en Suisse. Le fonctionnement fédéral fait qu'il a néanmoins un rôle aujourd'hui limité... et des moyens qui vont dans ce sens.» Le spécialiste d'ELCA Security note que les cantons sont chargés de la sécurité sur leur territoire et le NCSC n'intervient que de manière subsidiaire. «On pourrait se poser la question de davantage centraliser la lutte afin de rechercher des synergies entre ces nombreux acteurs. Le NCSC a également la responsabilité de protéger des infrastructures de la Confédération. Son positionnement et son rôle pourraient être renforcés, notamment pour intervenir et imposer des mesures préventives et de défense.»

4. Des cantons plus impliqués

Les cantons ont un rôle capital à jouer, lance Tobias Ellenberger. «Il faudra régler les responsabilités entre la Confédération et les cantons ainsi que les communes. Qui est responsable de la sécurité des communes ou des écoles, par exemple en matière de protection contre les attaques par *ransomware*? Qui est responsable si les cyberattaques causent des dégâts? Comment faire avec les petites communes et écoles qui détiennent également des données dignes d'être protégées, qui disposent souvent d'un très petit budget, mais doivent néanmoins se protéger contre les mêmes menaces?

Lire aussi: [Les données de l'administration vaudoise ne sont pas assez protégées](#)

5. Un Secrétariat d'Etat spécialisé?

C'est la demande de l'organisation CH++, créée il y a un an pour que la Suisse passe à la vitesse supérieure en matière de numérisation. «Face à la cybercriminalité, il n'y a pas de solutions miracles: c'est plutôt un ensemble bien ajusté de mesures qui peut contribuer durablement à limiter l'ampleur du phénomène», note Olga Baranova, membre fondatrice de CH++. Elle donne des exemples: «Il y a l'obligation d'annoncer les cyberattaques d'une certaine ampleur, une analyse approfondie des cas, des mesures incitatives pour que les victimes ou leurs assurances ne paient pas de rançon. Pour que ces mesures puissent être mises en place de manière rapide et efficace, l'architecture institutionnelle et les ressources sont cruciales.» Mais pour l'heure, le Conseil fédéral ne veut pas entendre parler de création d'un Secrétariat d'Etat spécialisé...