# Que devraient faire les autorités suisses face au fléau des cyberattaques? (1)

## 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 Oechslin, 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 Oechslin: «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…

# Face aux cyberattaques, l’Etat n’est pas à la hauteur (2)

## Éditorial

[?]

ÉDITORIAL. Il faut une meilleure coordination au niveau de la Confédération et une véritable prise de conscience des risques. Question d’ambition

Image d'illustration — © Alex - stock.adobe.com

Anouch Seydtaghia

Publié jeudi 13 janvier 2022 à 08:46
Modifié jeudi 13 janvier 2022 à 08:46

Allons droit au but: l'Etat n'est, aujourd'hui, pas à la hauteur face à la vague massive de cyberattaques qui nous frappe. Que ce soit au niveau fédéral, cantonal ou communal, les autorités n'ont visiblement pas encore pris la mesure des enjeux liés à ces piratages. Or ce sont nos données personnelles qui sont en jeu, celles que nous confions à des administrations, des banques ou des assurances.

La liste des manques actuels est longue. Aujourd'hui, une entreprise ou un particulier qui se fait pirater ne sait pas très bien à qui s'adresser. Tous les services de police ne sont pas suffisamment formés pour traiter les plaintes. On ne connaît pas précisément la répartition des compétences entre les échelons communal, cantonal et fédéral. Il n'y a aucune campagne de communication sur les bonnes pratiques numériques pour prévenir les cyberattaques.

**Lire aussi:** Que devraient faire les autorités suisses face au fléau des cyberattaques?

### De nombreux griefs

Les griefs adressés à nos autorités sont nombreux. Il suffirait déjà d'une meilleure coordination au niveau de la Confédération et, auparavant, d'une véritable prise de conscience des risques par les décideurs politiques, pour améliorer sensiblement la situation.

Attention, loin de nous l'idée d'étatiser la protection contre les cybercriminels, en donnant aux autorités le mandat de surveiller en permanence l'intégrité de nos données. Sans aller à ces extrêmes, il y a déjà tant à faire en matière de prévention, voire d'éducation, face aux cyberattaques.

### Une incongruité…

Et au niveau fédéral, les ambitions doivent également être accrues. Un exemple: pourquoi le Centre national pour la cybersécurité, doté seulement d'une trentaine de personnes, n'a-t-il pas pour mandat de scruter ce qui est publié sur le darknet lorsqu'une administration a été attaquée? Espérons que cette incongruité disparaisse rapidement.

La future loi sur la protection des données, qui doit entrer en vigueur cette année, imposera, dans certains cas, aux victimes de piratage de contacter les autorités. C'est un pas positif vers une sensibilisation accrue face à ces cyberattaques. Mais cela ne doit en rien exonérer les autorités de mieux nous protéger face à ces menaces qui nous concernent tous.

# Face aux cyberattaques, «le canton de Vaud ne peut pas faire beaucoup plus», avertit Nuria Gorrite (3)

## Technologie

Abonné

La conseillère d'Etat vaudoise veut accroître la prévention et envisage de renforcer le Centre cantonal de cybersécurité. Mais cela aura un coût financier, avance Nuria Gorrite

Nuria Gorrite. — © keystone-sda.ch, Keystone

Publié mercredi 12 janvier 2022 à 18:42
Modifié mercredi 12 janvier 2022 à 18:42

Qu'ont fait les autorités vaudoises depuis les révélations sur l'ampleur du piratage de la commune de Rolle en août 2021? Nuria Gorrite, conseillère d'Etat vaudoise chargée du Département des infrastructures et des ressources humaines (DIRH), répond à nos questions.

**Lire aussi, notre dossier du jour:**

**Le Temps: Ces dernières semaines, plusieurs entreprises basées dans le canton de Vaud ont été piratées, telles Matisa et DBS Group. Sont-elles livrées à elles-mêmes?**

**Nuria Gorrite:** Non. Récemment, une étude locale a montré que de nombreuses entreprises accusaient un important retard dans les compétences numériques. Leurs systèmes informatiques étaient obsolètes, mal entretenus et les employés n'étaient pas suffisamment bien formés. Avec la Chambre vaudoise du commerce et de l'industrie, nous avons mis au point une application pour sensibiliser les entreprises à ces problèmes. Mais, clairement, une app n'est pas suffisante. La médiatisation des attaques est utile pour prendre conscience des dangers des cyberattaques. Mais il faut faire davantage.

**Du coup, est-ce à l'Etat d'en faire plus?**

L'Etat ne peut pas tout faire, notamment il ne peut pas prendre le contrôle des données des entreprises ou des communes pour les protéger. Par contre, nous avons développé des modules de formation et de prévention, que nous mettons à leur disposition, permettant de réduire certains risques. Ce sont des éléments importants pour diminuer l'exposition des entreprises et des communes. Nous sommes également en appui en cas de crise, pour des interventions urgentes. Mais juridiquement et matériellement, le canton ne peut pas faire beaucoup plus.

**Depuis le piratage de Rolle, il n'y a donc eu qu'une réflexion sur des formations de prévention?**

L'attaque de Rolle a mis en évidence l'exposition de certaines communes au piratage et leur manque de préparation à ce risque. Dans le cas des attaques de Rolle et Montreux, les experts cantonaux sont intervenus sur place en urgence pour aider au rétablissement du fonctionnement informatique, protéger les systèmes et assister dans la gestion de crise. Le 11 novembre dernier, le canton a rencontré les faîtières des communes pour leur proposer un catalogue d'interventions possibles en cas d'attaques, une liste des bonnes pratiques, des formations pour leur personnel et la mise à jour de l'application précitée pour correspondre à leurs besoins. En outre, nous avons évoqué avec elles la possibilité de constituer ensemble un groupe d'intervention rapide conjoint pour faire face, le cas échéant, à de nouvelles attaques. Le travail se poursuit avec elles pour définir leurs besoins.

**Lire aussi:**

**Aujourd'hui, le Centre cantonal de cybersécurité est doté de cinq personnes. N'est-ce pas totalement insuffisant pour assister les communes?**

Ce centre a pour mission de protéger les systèmes et les données de l'Etat, pas ceux des communes. Il est intervenu en urgence auprès des communes, mais s'il devait voir ses missions étendues de manière pérenne, il faudrait le renforcer et trouver les financements nécessaires à ces missions élargies. Cette discussion est en cours entre l'Etat et les faîtières communales, qui devront se déterminer sur l'option qu'elles préfèrent: confier cette mission à l'Etat, se regrouper et mettre leurs ressources en commun, ou passer par un prestataire privé.

**Lors de cyberattaques, communes et entreprises font très souvent appel à des entreprises privées de sécurité. Est-ce que cela ne devrait pas être le rôle de l'Etat?**

Pas nécessairement. La discussion quant à l'ampleur de l'intervention attendue du canton par les communes est en cours. Cela étant, le canton travaille aussi très bien avec des entreprises privées de cybersécurité, depuis des années. Chaque entité est naturellement responsable de ses propres données et d'en assurer la sécurité. Mais une collaboration, un partage des expertises et une mutualisation des forces – sur le plan de la sensibilisation, de la prévention et en cas d'intervention d'urgence – est parfaitement envisageable.

# 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

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:**

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 Oechslin, 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:**

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 Oechslin: «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:**

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:**

## 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…

(5)

(6)


Economie & Finance

+4%

10,2 millions

+9,8%

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

«Le canton de Vaud ne peut pas faire beaucoup plus»

Les données vaudoises ne sont pas assez protégées