Economie

+4%

LES FAILLITES DE SOCIÉTÉS EN SUISSE ONT AUGMENTÉ EN 2021 MAIS LEUR NOMBRE RESTE INFÉRIEUR À CELLES ENREGISTRÉES AVANT LE COVID. Quelque 3946 entreprises ont dû mettre la clé sous le paillasson, soit une hausse de 4% sur un an, a indiqué mercredi le cabinet Dun & Bradstreet. Les créations d'entreprises ont, elles, atteint un record. Au total 50 537 inscriptions au Registre du commerce ont été signalées (+8%).

10,2 millions

L'AÉROPORT DE ZURICH EST PARVENU À REDRESSER LA BARRE EN 2021, MAIS SE TROUVE EN DESSOUS DE SON NIVEAU DE 2019. L'année dernière, 10,2 millions de passagers ont transité par Kloten. C'est 22,7% de plus qu'en 2020. Mais l'aéroport est encore bien loin des 31,5 millions de passagers de 2019 - un record - avant la crise liée au Covid-19, a annoncé mercredi Flughafen Zürich.

WILLIE WALSH
Directeur général de l'Association du transport aérien international (IATA)

Les réservations de billets d'avion ont «brutalement chuté» ces dernières semaines en raison des restrictions pour contrer Omicron, a-t-il indiqué mercredi, déplorant que les Etats aient «surréagi». Deux fois moins de voyageurs ont pris l'avion en 2021 qu'en 2019, a annoncé mercredi l'agence OACI de l'ONU.

Que devraient faire les autorités suisses

TECHNOLOGIE Menées par des pirates de plus en plus efficaces, les attaques se multiplient. Plusieurs experts interrogés par «Le Temps» esquissent des pistes pour une implication accrue des autorités face à cette menace, mais sans appeler à une gestion étatique de la cybersécurité

ANOUCH SEYDTAGHIA
@Anouch

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.

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.»

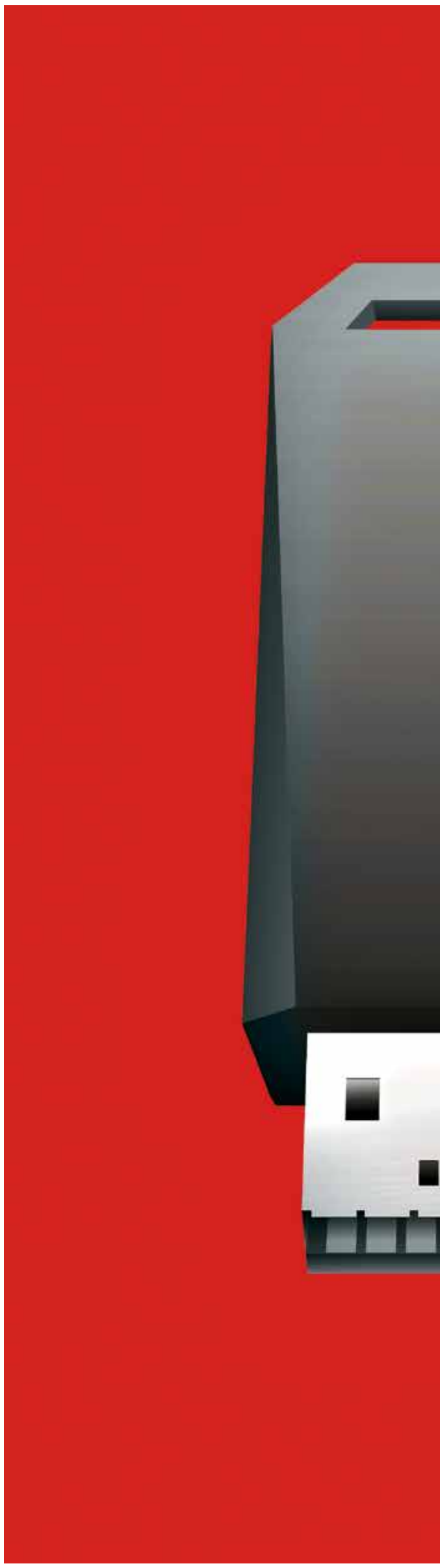
> «Les autorités fédérales, mais aussi les sociétés privées, sont confrontées à une «guerre des talents» combinée au nombre croissant d'incidents»
> TOBIAS ELLENBERGER, DIRECTEUR OPÉRATIONNEL DE ONECONSULT

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

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.»



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

PIRATAGE La conseillère d'Etat vaudoise Nuria Gorrite veut accroître la prévention et envisage de renforcer le Centre cantonal de cybersécurité. Mais cela aura un coût financier, avance-t-elle

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.

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? 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.

> «L'Etat ne peut pas prendre le contrôle des données des entreprises ou des communes pour les protéger»
> NURIA GORRITE, CONSEILLÈRE D'ÉTAT VAUDOISE

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.

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.

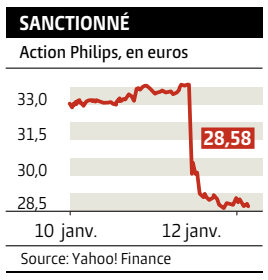
Lors de cyberattaques, communes et entreprises font très souvent appel à des entreprises privées de sécurité. Est-ce que cela ne devrait pas être le rôle de l'Etat? Pas nécessairement. La discussion quant à l'ampleur de l'intervention attendue du canton par les communes est en cours. Cela étant, le canton 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. ■

INTERVIEW

PROPOS RECUEILLIS PAR A. S.

Finance

Philips rappelle des respirateurs
Le géant néerlandais de l'électronique a provisionné 225 millions d'euros pour le rappel de millions d'appareils respiratoires défectueux pouvant être dangereux pour la santé.



FRANÇOIS VILLEROY DE GALHAU
Gouverneur de la Banque de France (BdF)
La BdF et la Banque centrale européenne «feront ce qu'il faut» pour ramener l'inflation dans la zone euro autour de 2%, a-t-il assuré, alors qu'elle a atteint +5% en décembre sur un an.

+9,8%
LES PRIX DE GROS EN ALLEMAGNE ONT GRIMPÉ DE 9,8% EN 2021 SUR UN AN, DU JAMAIS VU DEPUIS 1974. Les variations de prix sur un an des produits pétroliers (+32%) ainsi que des minerais, métaux et demi-produits métalliques (+44,3%) ont eu «une influence déterminante», selon Destatis.

SMI 12 670,47 -0,31%	↓	Dollar/franc	0,9135 ↓
		Euro/franc	1,0454 ↓
Euro Stoxx 50 4316,39 +0,81%	↑	Euro/dollar	1,1443 ↑
		Livre st./franc	1,2522 ↓
FTSE 100 7551,72 +0,81%	↑	Baril Brent/dollar	85,12 ↑
		Once d'or/dollar	1826 ↑

face au fléau des cyberattaques?


(OLIVIER PLOUX)

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.»

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.

Un Centre national pour la cybersécurité renforcé?

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.»

> «Une famille victime d'une cyberattaque ne sait pas vers qui se tourner pour se défendre et réagir correctement»
>
> CHRISTOPHE GERBER, DIRECTEUR DE LA DIVISION ELCA SECURITY

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?

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...

MAIS ENCORE

Obligation de signaler les cyberattaques: ouverture de la consultation
Le Conseil fédéral a ouvert mercredi la procédure de consultation sur son avant-projet de modification de la loi sur la sécurité de l'information. Il introduit notamment une obligation de signaler les cyberattaques contre les infrastructures critiques. (LT)

CPH rétablit son système informatique
CPH Chemie + Papier Holding a rétabli son système informatique après une cyberattaque le week-end dernier. La production devrait pouvoir reprendre sur les sites concernés au plus tard jeudi, a indiqué mercredi la société chimique. (AWP)

Les données vaudoises ne sont pas assez protégées

ADMINISTRATION Dans un audit publié ce mercredi, la Cour des comptes pointe des manquements parfois importants au sein de l'administration vaudoise en termes de protection des données personnelles des citoyens. Elle demande des mesures «sans délai». Dans la foulée, le Conseil d'Etat a fait savoir qu'il renforcerait ses dispositifs

YAN PAUCHARD
@YanPauchard

Les données personnelles des Vaudoises et des Vaudois ne sont pas suffisamment protégées. L'administration cantonale doit s'investir davantage dans leur sécurisation. Et cela «sans délai». C'est le constat sans appel de la Cour des comptes qui, dans un audit publié ce mercredi, pointe différents manquements, «parfois importants», en termes de respect des dispositions de la loi vaudoise sur la protection des données (LPrD), mais aussi de sécurité informatique. «Certaines entités de l'Etat sont très peu au fait de la protection des données, qui est encore trop souvent perçue comme une encouble ou un frein», regrette Valérie Schwaar, la présidente de la Cour des comptes, pour qui «le changement culturel nécessaire n'a pas encore été opéré».

Les enjeux sont pourtant devenus cruciaux, la numérisation permettant de copier, dupliquer et transmettre facilement des données personnelles. L'idée de cet audit est née en 2020, au début de la pandémie de Covid-19. L'explosion du télétravail durant cette période a impliqué l'usage de nouveaux outils informatiques, accentuant le besoin de sécurité. Les auditeurs ont ensuite été rattrapés par une actualité brûlante, celle d'une vague de cyberattaques qui ont notamment touché des communes vaudoises comme Rolle et Montreux. «Les conséquences de telles opérations sont graves: dégâts d'images, coût de récupération des données, paralysie temporaire de fonctionnement», ajoute Valérie Schwaar.

Concrètement, la Cour des comptes s'est concentrée sur un certain nombre d'entités de l'administration cantonale, dont le point commun est de gérer des données dites sensibles. On y retrouve la Direction générale de l'enseignement obligatoire, le Service des automobiles et de la navigation, l'Office du médecin cantonal ou la Direction finances et affaires juridiques de la Direction générale de la santé. La situation diffère d'une entité à une autre, mais la liste des lacunes mises au jour est longue: envoi d'e-mails sans sécurisation adéquate, données pas anonymisées ou conservées indéfiniment, absence de traçabilité, gestion des accès insuffisamment contrôlée... Sans oublier des lacunes dans les contrats de sous-traitance.

> «Le personnel demeure le cheval de Troie»
>
> VALÉRIE SCHWAAR, PRÉSIDENTE DE LA COUR DES COMPTES DU CANTON DE VAUD

Pour la Cour des comptes, ces problèmes sont principalement dus à un manque de connaissances du personnel, à tous les étages hiérarchiques de l'administration. «Lors d'un récent test d'hameçonnage (*phishing*), un quart des collaborateurs se sont fait piéger», précise Valérie Schwaar. De plus, certaines entités n'ont aucune directive interne de protection des données. Les mesures sont généralement prises au coup par coup, sans stratégie globale. Les auditeurs relèvent néanmoins que les employés «sont rompus aux questions de confidentialité des informations traitées dans le cadre professionnel», ce qui «permet de garantir un certain niveau de protection des données».

L'audit souligne encore l'important travail de rattrapage en matière de sécurité informatique effectué depuis 2011 par la Direction générale du numérique et des systèmes d'information, qui a également renforcé ses compétences en la matière. «L'architecture est bonne, résume Valérie Schwaar, mais le personnel demeure le cheval de Troie».

Vingt recommandations

Au total, la Cour des comptes a adressé 20 recommandations, insistant sur l'importance d'améliorer les compétences en informatique et en protection des données, ainsi que sur le renforcement de la surveillance. Certaines recommandations ont été directement faites au Conseil d'Etat, qui a d'ores et déjà accepté de les mettre en œuvre: création d'un délégué à la protection des données dans chaque entité de l'Etat et obligation d'annonce de toute violation en matière de cybersécurité, entre autres. Dans un communiqué de presse, le gouvernement a salué mecredi la démarche de la Cour des comptes et assuré qu'il mettra en œuvre ses recommandations.

«Il n'y a pas péril en la demeure», image la présidente de la Cour des comptes. Mais pour la socialiste, il est grand temps que la LPrD, entrée en vigueur en 2008, soit pleinement appliquée, afin de garantir la protection des données des citoyennes et citoyens. «Le développement harmonieux de la cyberadministration ne se fera qu'avec la confiance de la population», conclut Valérie Schwaar.