LE TEMPS

Le poste de contrôle du SOC vaudois, dans l'Ouest lausannois.
© Eddy Mottaz

TECHNOLOGIES

Les cantons boostent leurs cyberdéfenses, Berne reste à la traîne

Les administrations suisses investissent massivement dans la lutte contre les attaques informatiques. Vaud veut exporter son coûteux modèle de Centre opérationnel de sécurité (SOC) à l'ensemble du pays

9 minutes de lecture

Technologies **sécurité** **Vaud** **Genève** **Zurich**

Sylvain Besson
Anouch Seydtaghia

Publié lundi 30 avril 2018 à 18:15, modifié mardi 1 mai 2018 à 09:07.

En mai 2017, alors que le virus WannaCry infectait les hôpitaux anglais, perturbait les chemins de fer allemands et paralysait des centaines de milliers d'ordinateurs à travers le monde, un groupe de fonctionnaires vaudois observait placidement l'attaque se dérouler depuis leurs écrans de contrôle de l'Ouest lausannois.

Les membres du Centre opérationnel de sécurité (SOC) de l'Etat de Vaud savaient quelles vulnérabilités le virus utilisait, quelles machines risquaient d'être infectées, et comment s'en protéger.

«Quand la faille exploitée par WannaCry est apparue en mars 2017, on était au courant, explique Juan Ramos, responsable opérationnel du SOC vaudois. On suit sur internet le groupe de hackers Shadow Brokers [qui avait révélé la faille]. On avait récupéré des infos sur le Darkweb et TOR [un réseau sécurisé apprécié des cybercriminels]. C'est comme ça qu'on a su que WannaCry arrivait.»

Le SOC s'est ensuite assuré que les quelque 13 000 ordinateurs de l'Etat de Vaud ne risquaient rien. «Les règles de filtrage des firewalls ont été passées en revue [et] un scan de vulnérabilités spécifique a été effectué», explique un mémo résumant l'intervention.

Le SOC, c'est la botte secrète de l'Etat de Vaud contre les cyberpirates. Créée en 2015, cette unité de cinq personnes est «une tour de contrôle» qui offre une «vue consolidée» et permet de «mieux piloter les réponses aux attaques», résume Patrick Amaru, chef de la Direction des systèmes d'information du canton. «Avec un SOC, on voit beaucoup de choses.»

ıaru, chef de la
des systèmes
ıtion du canton de

ıtaz

Un modèle qui se répand

Partout en Suisse, des collectivités s'équipent de moyens analogues. Le canton de Genève vient de mettre en service son SOC. La ville de Zurich aura le sien en 2018. Et le modèle est voué à s'exporter plus loin. Réunie cette semaine à Zoug, la Conférence suisse sur l'informatique doit permettre aux cantons et aux villes de mettre leurs SOC à disposition des collectivités qui n'ont pas les moyens de s'offrir leur propre structure.

Mais à quoi ressemble un SOC? *Le Temps* a pu visiter la cellule vaudoise, nichée dans un bâtiment administratif de l'Ouest lausannois. Les vitres sont teintées: ne pénètrent ici que les personnels habilités. «On est isolé du reste de l'administration, on a nos propres serveurs, notre propre

fonctionnement, commente Marc Barbezat, responsable de la sécurité des systèmes d'information du canton. Il y a des portes à code et des caméras de surveillance.»

4 millions de spams par mois

A l'intérieur, une vaste salle munie d'écrans de contrôle forme le cœur physique du SOC.

Ce jour-là, on voit sur l'*intrusion detection dashboard* qu'il y a eu, à partir de 9h du matin, 417 tentatives d'attaques depuis les Etats-Unis. Un chiffre qui n'a rien d'inhabituel: l'administration vaudoise reçoit plus de 4 millions de spams par mois. Outre WannaCry, les spécialistes du SOC ont vu passer tous les virus les plus dangereux des derniers mois, comme Emotet, Retefe ou Gozi, destinés à voler des données bancaires ou commerciales confidentielles.

Par rapport à un simple service informatique, le SOC offre une capacité d'intervention 24 heures sur 24, 7 jours sur 7, explique Max Klaus, vice-directeur de Melani, l'unité chargée de la cybersécurité à la Confédération. Dans le canton de Vaud, l'entreprise Kudelski assure un support, en particulier les nuits et le week-end. Elle alerte les employés du SOC en cas d'incident confirmé.

Intrusions ciblées

Un SOC est aussi plus efficace pour détecter les attaques sophistiquées appelées APT *(advanced persistent threats)*. Des intrusions silencieuses et de longue durée, perpétrées notamment par des Etats ou des hackers à leur solde.

Dans les cantons, les pirates pourraient lancer des attaques ciblées pour s'emparer de «données fiscales ou en rapport avec la justice», selon Paul Such, directeur de la société Hacknowledge, qui a construit le SOC genevois.

L'outil de base d'un SOC, ce sont des sondes informatiques qui filtrent chaque événement (un ordinateur qui se connecte au réseau, par exemple) et identifient ceux qui sont jugés anormaux. Toute la difficulté est de bien paramétrer les sondes, et de corréler les alertes entre elles pour détecter ce qui est vraiment suspect.

Les employés du SOC vaudois ont développé une capacité à traiter eux-mêmes les menaces. «On préfère analyser nous-mêmes les codes malveillants, ne pas les transmettre [sur des sites publics], pour ne pas donner le message à l'attaquant qu'il a été découvert», ajoute Marc Barbezat.

Le SOC, un sport de riches

Mais développer des capacités «maison» a son prix. Lorsque le développement du SOC a démarré, en 2012-2013, Vaud a investi 8 millions de francs pour mettre à niveau ses cyberdéfenses. Le canton consacre quelque 2,5 à 3 millions de francs par an à la sécurité de ses systèmes informatiques, ce qui comprend les coûts du SOC et le contrat confié – pour un montant non précisé – à Kudelski.

«Disposer d'une cyberunité coûte cher, confirme Steven Meyer, directeur de la société de cybersécurité ZENData, à Genève. Il faut former les agents, les tenir à jour, leur donner accès à des logiciels et matériels spécifiques qui ne sont pas sur le marché libre…»

Même avec des moyens conséquents, le SOC n'est pas parfait. A l'automne 2017, la page d'accueil du site du canton de Vaud a été bloquée durant une demi-heure par une attaque de type DDoS – un flot de demandes qui rend le site inaccessible.

Les défenses du SOC ont été déjouées: le pirate a utilisé les serveurs d'une entreprise vaudoise mal protégée pour lancer son attaque. Or les sondes étaient réglées pour détecter ce type d'agression uniquement si elle venait de l'étranger.

Il a fallu changer les paramètres. Quant au pirate, malgré le dépôt d'une plainte pénale, il n'a jamais été identifié.

Expérience désagréable

En Suisse, les cantons sont responsables de la cybersécurité de leurs administrations. Autant dire qu'un équipement adéquat est crucial, face à des hackers de plus en plus habiles. Pour un grand canton, en particulier, un SOC est un «atout important», estime Patrick Amaru.

Après avoir soigneusement étudié le concept vaudois, Genève vient de mettre en service son propre SOC. Conçu avec la société Hacknowledge, il est décentralisé et moins cher que son homologue vaudois: 170 000 francs d'investissement de départ et 100 000 francs de fonctionnement estimés par an pour le canton, selon Jean-Pierre Gilliéron, secrétaire général adjoint chargé des systèmes d'information. Un avantage dû à la mutualisation des coûts avec les 12 autres partenaires du projet: université, Transports publics genevois, hôpital cantonal, etc.

OC, c'est très cher et peu de cantons peuvent se l'offrir. on espère que les 26 cantons auront à terme une ion efficace »

Jermann, Conférence suisse sur l'informatique

Fin 2016, Genève a lui aussi eu une expérience de piratage désagréable: certaines de ses données ont été «cryptolockées» par un rançongiciel de type WannaCry. Il a fallu aller rechercher les données du jour précédent pour rétablir le fonctionnement du système. «C'était ce que j'appelle du travail à la pince à sucre, explique Jean-Pierre Gilliéron. Ça a été du boulot, mais on n'a perdu aucune donnée.»

En Suisse, toutes les grandes collectivités publiques réfléchissent à des structures de type SOC. Le patron de Hacknowledge, Paul Such, explique travailler pour «diverses entités étatiques, notamment des cantons, que je ne peux nommer».

Le risque, évidemment, serait que les administrations s'équipent de façon anarchique, en gaspillant beaucoup d'argent au passage. C'est pour cela que la mise en commun des SOC est à l'ordre du jour de la Conférence suisse sur l'informatique qui doit se tenir les 2 et 3 mai. Vaud y présentera un concept de mutualisation, avec l'idée de pouvoir mettre son SOC à disposition des cantons et villes intéressées.

Plateforme commune

«On a des questions de cantons, de grandes communes, qui demandent si on peut leur fournir des prestations, confie Patrick Amaru. On étudie ça.»

Selon Urs Jermann, directeur de la Conférence suisse sur l'informatique, «un SOC, c'est très cher et peu de cantons peuvent se l'offrir. Mais on espère que les 26 cantons auront à terme une solution efficace.» Et ce, grâce à la création d'une plateforme juridique commune, baptisée eOperations Suisse et intégrant à la fois des villes, les cantons et la Confédération.

A Berne, les choses bougent aussi, mais lentement. La Confédération possède une unité militaire, baptisée MilCERT, et un centre civil, CSIRT, qui dépend de l'Office fédéral de l'informatique. S'y ajoute une centrale de coordination et d'information au public, Melani, dotée de huit personnes. Elle est divisée entre le Département des finances et le Service de renseignement de la Confédération.

a pas de visibilité au sein de la Confédération, la

sécurité n'a pas de visage »

him Eder (PLR/ZG), Conseiller aux Etats

Certains jugent cette structure trop éclatée, sous-dotée et peu lisible. Il n'y a pas de tour de contrôle unique, qui permettrait d'avoir une vue d'ensemble des menaces, et de centraliser les informations sur les cyberattaques émanant de l'intérieur du pays et de l'étranger.

«Ce qui nous manque, c'est le cockpit de l'avion», résume un fonctionnaire au fait de ces questions. Selon lui, aucune instance fédérale n'a pour l'instant de capacités de type SOC, même si l'armée a décidé de s'en doter après l'attaque informatique qui a visé le Département de la défense en septembre dernier.

«Il n'y a pas de visibilité au sein de la Confédération, la cybersécurité n'a pas de visage», regrette le conseiller aux Etats Joachim Eder (PLR/ZG), très actif sur la question.

Après des dizaines d'interventions parlementaires sur le sujet, la Confédération a fini par promettre plus de centralisation dans sa nouvelle «stratégie nationale contre les cyberrisques», parue la semaine dernière.

Outre l'inertie politique, le principal problème, pour la cyberdéfense suisse, sera celui des ressources humaines. Elles sont rares et risquent de devenir de plus en plus chères à mesure que le thème prend de l'importance.

Ce que confirme le responsable d'un SOC romand: «On nous appelle parfois pour nous dire: «On ne sait pas combien vous gagnez, mais on double votre salaire si vous nous rejoignez.»

Cybermenaces cantonales

- En 2017, lors d'un dimanche de votation, le SOC vaudois a repéré un flux de données venant d'une commune et partant vers l'étranger. Le flux a été stoppé. Il s'agissait en réalité d'une simple sauvegarde – mais la commune ignorait que ses informations partaient en Allemagne. Elle a depuis ramené ses données en Suisse.

- Plusieurs cantons suisses ont été victimes de rançongiciels, ces virus qui permettent de crypter et bloquer des données. Les pirates demandent alors une rançon pour les libérer. Aucun canton ne communique sur le sujet, mais Genève admet avoir subi une attaque de ce type en 2016. Les données cryptées ont dû être reconstituées grâce aux sauvegardes de la veille.

- Les cantons se méfient du risque de cryptominage: des ordinateurs sont piratés pour produire des bictoins, la monnaie virtuelle dont le cours a explosé depuis un an. Mais aucun incident de ce type n'a encore été répertorié.

Le SOC vaudois en chiffres

Les sondes du SOC filtrent chaque jour 30 millions d'événements, qui génèrent 400 alertes et 6 investigations plus approfondies.

Le SOC traite en moyenne trois campagnes de *phishing* (vols de données grâce à des courriels astucieux) par semaine.

Le SOC surveille 13 000 postes de travail et 65 536 adresses IP pour le canton de Vaud.

Sylvain Besson
@SylvainBesson

Rédacteur en chef adjoint et journaliste d'investigation. Intérêt notamment pour les enquêtes complexes, les malversations financières, les super-riches et les services de renseignement.