

# La Confédération veut développer la protection contre les cyberrisques

En cas de cyberattaque, les entreprises ou les particuliers risquent de se faire dérober leurs données et l'infrastructure électrique d'être paralysée à grande échelle. La Confédération s'est donc dotée d'un système de détection précoce, pour protéger les infrastructures d'importance vitale contre de tels incidents. Ses capacités dans ce secteur seront encore amenées à se développer. *Max Klaus*

**Abrégé** Le Conseil fédéral a compris très tôt l'importance de lutter contre les risques liés aux cyberattaques. Plusieurs unités administratives sont chargées de déjouer ces menaces. C'est le cas de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani), qui protège non seulement les services fédéraux, mais aussi les infrastructures d'importance vitale des banques, des fournisseurs d'énergie ou encore des entreprises de télécommunication. En outre, le cyberspace ne s'arrête pas aux frontières : la Suisse doit donc soigner son réseau de contacts et échanger des informations au niveau international. À ce titre, elle s'engage au sein d'organisations multilatérales pour davantage de coopération et de transparence dans le cyberspace. La Confédération est bien consciente de l'importance grandissante des dangers qu'il recèle. Elle entend donc renforcer, dans le cadre d'une nouvelle stratégie, les capacités dont disposent l'administration et l'économie, et par là accroître la résistance de la Suisse face aux cyberattaques.

Il y a quelques mois, les rançongiciels Wanna Cry et Petya ont fait les gros titres dans le monde entier. Wanna Cry a en effet infecté 200 000 ordinateurs dans 150 pays. Parmi ses victimes figuraient un grand nombre d'hôpitaux britanniques, les tableaux affichant les horaires de la Deutsche Bahn et une société de télécommunication en Espagne. Le maliciel cryptait certains fichiers des appareils infiltrés, puis demandait aux utilisateurs de verser

un montant donné en bitcoins, afin de ne pas perdre leurs données. De telles attaques sont loin d'être des cas isolés. En automne 2016, le groupe Internet Yahoo annonçait s'être fait pirater 500 millions de mots de passe de clients commerciaux. L'Ukraine a appris à ses dépens, en décembre 2015, l'impact qu'un tel incident peut avoir : une cyberattaque a paralysé son infrastructure électrique et plus de 250 000 personnes ont été privées de courant. Chacun

peut être victime n'importe quand d'une cyberattaque. Dans quelle mesure la Suisse est-elle armée contre de telles agressions et que fait la Confédération lorsque cela se produit ?

Dans l'administration fédérale, plusieurs unités s'occupent de cybersécurité (voir *illustration*). En premier lieu, elles mettent l'accent sur les réseaux de la Confédération. L'Office fédéral de l'informatique et de la télécommunication (Ofit) est responsable de la protection des réseaux civils. De son côté, la Base d'aide au commandement (BAC) du Département fédéral de la défense, de la protection de la population et des sports (DDPS) veille à la sécurité des réseaux militaires. Enfin, l'Unité de pilotage informatique de la Confédération (Upic) définit des directives de sécurité uniformes et contraignantes pour toutes les unités administratives de la Confédération. Parmi ces directives, il est par exemple exigé que les offices assurent une protection de base adéquate de leur informatique. À l'instar de l'administration fédérale qui se doit de protéger ses infrastructures, les entreprises veillent sur

## Organisations chargées au niveau fédéral de la protection contre les cyberrisques

DDPS Département fédéral de la défense, de la protection de la population et des sports		DFF Département fédéral des finances		DFJP Département fédéral de justice et police	MPC Ministère public de la Confédération
BAC Base d'aide au commandement	SRC Service de renseignement de la Confédération	UPIC Unité de pilotage informatique de la Confédération	OFIT Office fédéral de l'informatique et de la télécommunication	FEDPOL Office fédéral de la police	Criminalité économique
MilCERT Military Computer Emergency Readiness Teams	MELANI Centrale d'enregistrement et d'analyse pour la sûreté de l'information	UPICSEC Secteur Sécurité	CSIRT Computer Security Incident Response Team	PJF Police judiciaire fédérale (division Enquêtes, forensique et informatique)	SKT Protection de l'État, Terrorisme, Organisations criminelles
		Commandement stratégique		SCOCI Service national de coordination de la lutte contre la criminalité sur Internet	
		GovCERT Governmental Computer Emergency Response Team			



La nouvelle stratégie de la Confédération vise d'abord à protéger la population.

leurs systèmes informatiques. Le Conseil fédéral a cependant reconnu dès 2003 la nécessité de soutenir dans toute la Suisse les exploitants d'infrastructures considérées d'importance vitale dans leurs efforts déployés contre les cyberattaques. Il a donc chargé le Département fédéral des finances (DFF) de mettre en place la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (« Melde- und Analysestelle Informationssicherung », Melani). Opérationnelle depuis octobre 2004, celle-ci est informée au quotidien des cyberattaques en tous genres.

Conformément à la mission reçue du Conseil fédéral, Melani s'occupe essentiellement de protéger les infrastructures d'importance vitale des grandes entreprises suisses, comme les banques, les fournisseurs d'énergie ou les opérateurs de télécommunication. Elle échange au quotidien avec ces acteurs des informations sur les attaques et les menaces actuelles. Ces renseignements, souvent issus de sources inaccessibles au grand public, apportent une précieuse plus-value à la sécurité des entreprises.

C'est notamment pour mieux accéder à de telles informations que Melani relève de deux départements fédéraux. Sa direction stratégique, qui assume la responsabilité globale, et le Swiss Government Computer Emergency Response Team (Govcert)

se trouvent au DFF. Ce dernier<sup>1</sup> constitue l'équipe technique de Melani. Ses spécialistes sont à même d'analyser les maliciels pour découvrir des indices sur les intentions des agresseurs et leur provenance. Quant à l'Operation and Information Centre (OIC), il constitue l'équipe opérationnelle de Melani, laquelle est basée au Service de renseignement de la Confédération (SRC), au DDPS. L'OIC est l'interlocuteur des exploitants d'infrastructures vitales et peut, par exemple, requérir le blocage de pages Internet mêlées à des cyberattaques.

### Lutte contre la cybercriminalité

Melani n'est toutefois pas le seul service fédéral engagé dans la lutte contre les nouvelles menaces numériques. Le Département fédéral de justice et police (DFJP) a créé dès 2001, à l'Office fédéral de la police (Fedpol), le Service national de coordination de la lutte contre la criminalité sur Internet (Scoci).

Ce service, fruit de la coopération entre la Confédération et les 26 corps de police cantonaux, sert de guichet unique aux particuliers et aux PME victimes de cyberattaques. Les annonces reçues sont examinées, puis transmises aux autorités de poursuite péna-

le compétentes en Suisse et à l'étranger. Le Scoci possède, au même titre que le Ministère public de la Confédération (MPC), un mandat général d'enquête qui l'amène à rechercher activement sur Internet des contenus pénalement répréhensibles.

### Rôle crucial de la coopération internationale

Il serait illusoire de croire qu'une centrale d'enregistrement peut protéger les infrastructures d'importance vitale présentes sur son territoire sans soutien étranger. La grande majorité des cyberattaques ignorent les frontières nationales. Beaucoup d'entreprises et de particuliers basés dans de très nombreux pays en font souvent les frais. Un réseau international d'organisations similaires à Melani s'avère donc indispensable, en Europe et dans le monde entier, pour accéder rapidement et à toute heure à des informations fiables, issues de sources dignes de confiance.

C'est pourquoi il existe des organisations comme l'European Government Certs (EGC) et le Forum for Incident Response and Security Teams (First). Melani en fait partie.

L'EGC est un groupe européen d'organismes étatiques chargés de protéger sur

<sup>1</sup> Pour de plus amples informations, voir le site govcert.ch.

leur territoire les infrastructures d'importance vitale face aux cyberattaques. Les États membres y échangent au quotidien des informations sur les agressions subies ou sur les menaces imminentes. Le First est, par contre, une organisation d'experts en sécurité active dans le monde entier, qui compte aussi dans ses rangs des représentants du secteur privé. Comme les membres du forum viennent surtout d'Amérique du Nord et d'Asie, Melani peut soigner ses contacts et étendre son réseau sur ces deux continents.

De tels contacts portent leurs fruits. Dans le cas du cheval de Troie Wanna Cry, Melani a par exemple reçu d'un État membre de l'EGC, plusieurs heures avant que l'attaque ne soit rendue publique, des informations importantes qui lui ont permis de prévenir les exploitants d'infrastructures vitales et d'empêcher le malicieux de sévir en Suisse. Le SRC, qui dispose d'un vaste réseau au niveau international, constitue lui aussi un précieux informateur dans ce domaine.

## Politique de sécurité extérieure dans le cyberspace

Au-delà des questions techniques et opérationnelles, la coopération internationale est également importante sur le terrain diplomatique. Outre les frontières terrestres, l'espace aérien et les eaux territoriales, l'espace numérique est devenu un champ d'interaction étatique (politique d'intimidation, cyberguerre, activités de renseignement). Le Département fédéral des affaires étrangères (DFAE) s'engage, dans le cadre de processus multilatéraux et de consultations bilatérales, pour que le cyberspace ne soit utilisé qu'à des fins pacifiques et ne devienne pas le théâtre de conflits ou un catalyseur de tensions interétatiques.

Dans un contexte politique où règnent la méfiance et l'incertitude, il est essentiel de

promouvoir jusque dans l'espace numérique la confiance entre États. D'où l'utilité des mesures propres à améliorer l'échange d'informations et la transparence, et donc à jeter les bases d'une coopération plus étroite. Un tel échange volontaire d'informations peut par exemple amener les pays à s'indiquer leurs points de contact nationaux en cas de cyberattaque ou à publier leurs infrastructures jugées d'importance vitale. La Suisse est très engagée, au sein de l'Organisation pour la sécurité et la coopération en Europe (OSCE) notamment, dans l'élaboration et la réalisation de ce genre de mesures.

## Stratégie nationale contre les cyberrisques

Les activités décrites ci-dessus contribuent à protéger la Suisse contre les cybermenaces. Ce sont autant d'éléments clés de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)<sup>2</sup>, approuvée en 2012 par le Conseil fédéral.

La SNPC comprend au total seize mesures, mises en œuvre conjointement par les autorités compétentes, les milieux économiques et les exploitants d'infrastructures d'importance vitale. En outre, des analyses de risques et de vulnérabilités ont été effectuées dans les secteurs identifiés comme vitaux. Les activités de recherche et de formation ont été intensifiées dans le domaine des cyberrisques. L'on a également renforcé les capacités du SRC dans le domaine de la détection précoce et de l'identification des agresseurs. Les travaux liés à la SNPC s'achèveront cette année. L'Upic, qui coordonne la stratégie, va donc élaborer d'ici à la fin de 2017, en collaboration avec tous les services concernés de l'administration et avec des partenaires du secteur pri-

vé, une deuxième stratégie pour les années 2018 à 2022.

La nouvelle stratégie s'inscrit dans la continuité de la première, qu'elle vise à poursuivre et à optimiser. Il s'agira d'étendre les capacités de la Confédération en matière de détection et d'évaluation des cyberrisques, de réaction aux incidents et de poursuites pénales. La collaboration au sein de l'administration fédérale sera renforcée dans ces domaines et les ressources nécessaires seront revues à la hausse.

La collaboration entre l'État et les milieux économiques reste au cœur de la SNPC. Si la première stratégie se concentrait sur la protection des infrastructures d'importance vitale, les PME et la population joueront aussi un rôle clé dans celle qui lui succédera. En effet, la Confédération prévoit d'aider davantage ces groupes cibles à gérer les cyberrisques, sans pour autant faire concurrence aux prestataires privés spécialisés dans les solutions de sécurité. Entre autres mesures susceptibles d'améliorer la cyberrésilience de l'économie, il convient de citer l'évaluation et l'introduction de normes minimales pour les branches, l'étude d'une obligation de notifier les incidents de sécurité, ainsi que la transmission aux milieux économiques et à la population d'informations relatives aux cybermenaces.



**Max Klaus**

Responsable adjoint de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani), Unité de pilotage informatique de la Confédération (Upic), Berne

<sup>2</sup> Voir Upic (2012), Stratégie nationale de protection de la Suisse contre les cyberrisques.