Les cyberrisques sont une menace sérieuse

Les cyberattaques se multiplient en Suisse. La nouvelle stratégie du Conseil fédéral vise à soutenir également les entreprises et les particuliers dans la lutte contre la soustraction de données délictueuse. *Manuel Suter*

Abrégé Les cyberattaques sont omniprésentes et menacent aussi bien les particuliers que les entreprises et les autorités. Leur développement fulgurant met en péril l'utilité de la numérisation. La Confédération fait face à ces menaces en mettant sur pied une nouvelle Stratégie nationale de protection de la Suisse contre les cyberrisques. Un Centre de compétences pour la cybersécurité sera créé en vue de sa mise en œuvre, sous la direction d'un délégué du Conseil fédéral à la cybersécurité. À l'avenir, la défense contre les cyberattaques ne doit pas se contenter de protéger les infrastructures d'importance vitale, mais aussi les entreprises et les particuliers.

Chaque jour, des ordinateurs sont attaqués en Suisse. Ces cyberattaques menées à grande échelle dans le monde entier visent souvent à dérober des données ou détourner des transactions financières. Le nombre de cyberattaques à des fins d'extorsion a notamment augmenté. Les pirates informatiques verrouillent par exemple les données au moyen d'un cheval de Troie appelé rançongiciel, qui empêche l'utilisateur d'y accéder. Ils exigent ensuite de l'argent, le plus souvent sous forme de cryptomonnaie, pour déverrouiller les données. Une autre méthode d'extorsion consiste à envoyer à la victime des extraits d'enregistrements dérobés et à exiger une rançon en menaçant de publier des données personnelles sensibles. Toute la perfidie du procédé réside dans le fait que la victime ignore si les malfaiteurs sont réellement en possession de ces données.

Outre ces attaques à grande échelle, les entreprises et les autorités essuient aussi des attaques extrêmement ciblées. Les pirates informatiques investissent beaucoup de temps et de moyens pour s'introduire dans leurs systèmes. Pourtant, leur objectif n'est pas de gagner rapidement de l'argent. Il s'agit plutôt de se procurer des informations précieuses qui leur conféreront un avantage économique ou politique à long terme.

Nouvelle stratégie de protection contre les cyberrisques

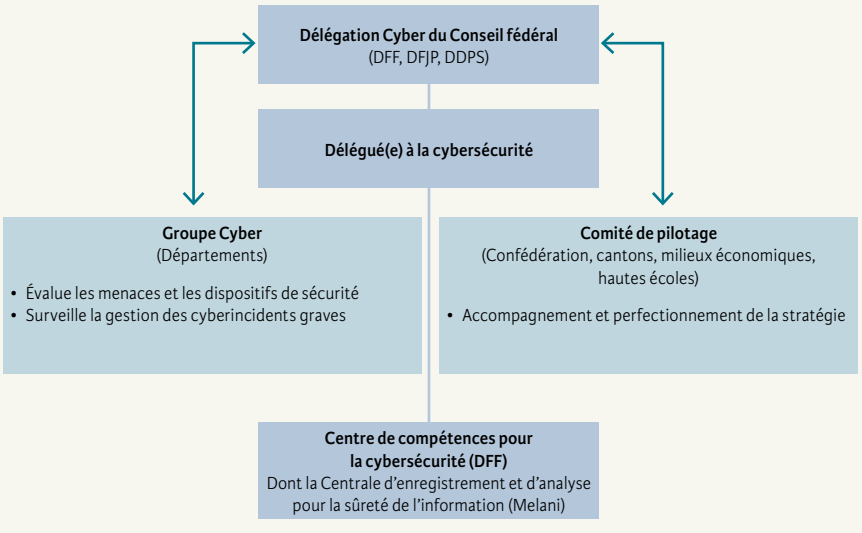
Comment la Suisse se protège-t-elle contre de telles cyberattaques ? Le Conseil fédéral a pris l'an dernier des décisions déterminantes dans ce domaine. En avril 2018 déjà, il a adopté la nouvelle Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)[1] pour les années 2018 à 2022 et défini son champ d'action ainsi que les mesures qu'elle impliquait. En comparaison avec la stratégie précédente qui portait sur les années 2012 à 2017, la nouvelle SNPC prend en compte le fait que les cyberrisques constituent désormais une menace pour toutes les entreprises ainsi que pour la sécurité et le bien-être de la population. Tandis que la stratégie précédente se concentrait essentiellement sur la protection des infrastructures d'importance vitale telles que les fournisseurs d'énergie, les opérateurs de télécommunications, les hôpitaux ou encore les banques, la nouvelle mouture exige expressément que la Confédération apporte son soutien à l'ensemble des entreprises et à la population dans le domaine de la protection contre les cyberrisques. La stratégie ne prévoit pas uniquement des mesures destinées à renforcer la protection immédiate : elle vise également à améliorer la cybersécurité grâce à des mesures à long terme, comme le développement des compétences et des connaissances en Suisse ou la promotion et le maintien des relations internationales. Les activités de l'Union européenne (UE) pour renforcer la cybersécurité en Europe revêtent en effet une importance particulière pour la Suisse. L'UE a déjà établi un règlement sur la cybersécurité[2], qui prévoit un cadre européen de certification des produits, des procédures et des services. La Suisse observera avec attention le développement de ce cadre de certification et prendra les mesures requises pour garantir la compatibilité de l'économie suisse avec les directives européennes en matière de cybersécurité.

En adoptant la SNPC, le Conseil fédéral a également décidé de réorganiser les services fédéraux dans le domaine de la cybersécurité

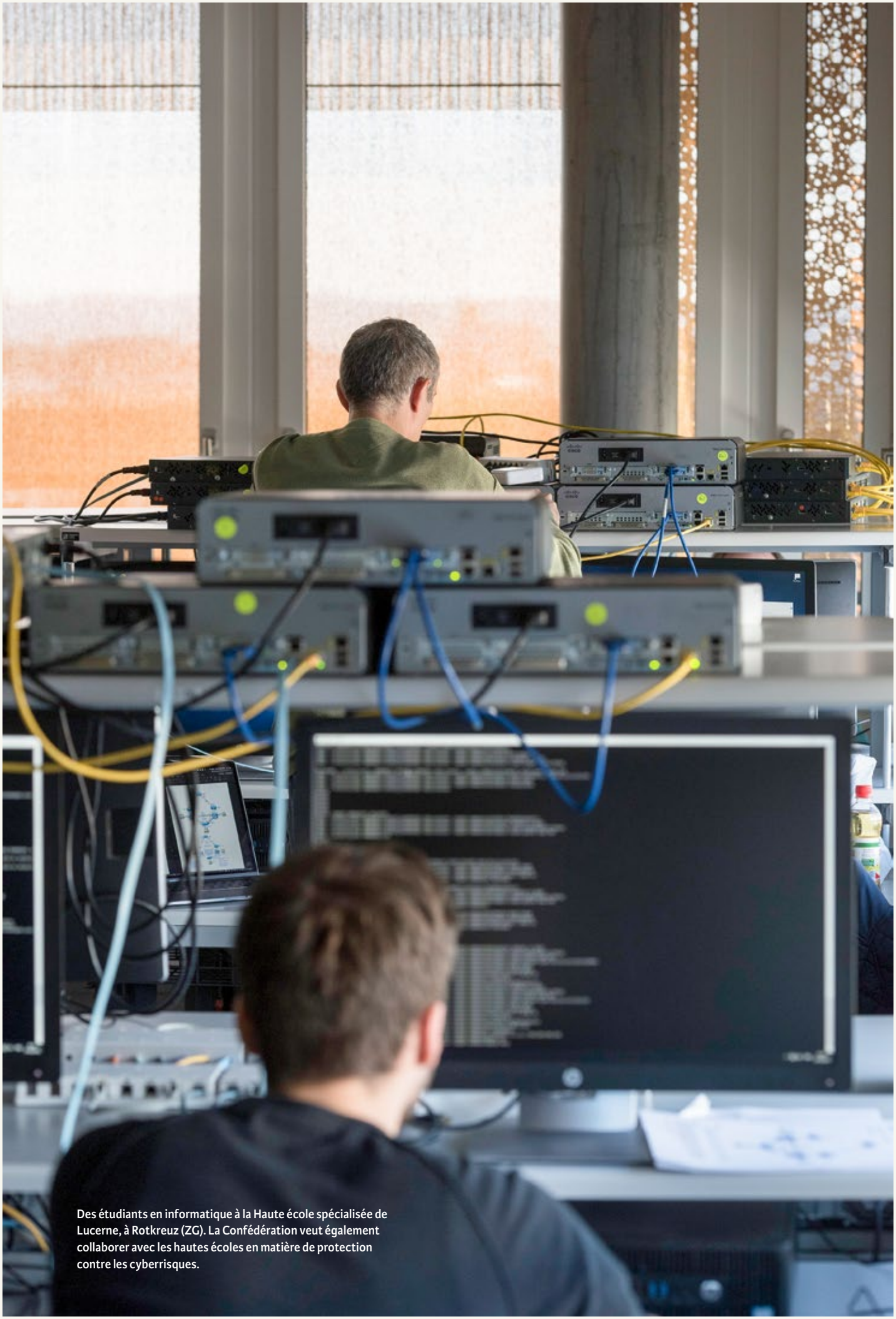
1 La stratégie complète est disponible en ligne sur le site isb.admin.ch.

2 Voir Commission européenne (2017). Règlement du Parlement européen et du Conseil relatif à l'Enisa, Agence de l'Union européenne pour la cybersécurité, et abrogeant le règlement (UE) no 526/2013, et relatif à la certification des technologies de l'information et des communications en matière de cybersécurité (règlement sur la cybersécurité).

Organisation du domaine de la cybersécurité souhaitée par le Conseil fédéral



CHANCELLERIE FÉDÉRALE / LA VIE ÉCONOMIQUE



Des étudiants en informatique à la Haute école spécialisée de Lucerne, à Rotkreuz (ZG). La Confédération veut également collaborer avec les hautes écoles en matière de protection contre les cyberrisques.

KEYSTONE

(voir *illustration*). En janvier dernier, il a pris les décisions nécessaires et créé une «Délégation pour la cybersécurité» (délégation Cyber), dans laquelle sont représentés le Département fédéral des finances (DFF), le Département fédéral de justice et police (DFJP) et le Département fédéral de la défense, de la protection de la population et des sports (DDPS), affirmant ainsi son rôle de conduite dans ce domaine. À l'avenir, les chefs des trois départements échangeront régulièrement des informations concernant la cybersécurité et s'assureront que la stratégie est mise en œuvre conformément à ses objectifs. Ils bénéficient pour cela du soutien de deux organes : le groupe Cyber et le comité de pilotage de la SNPC. Au sein du groupe Cyber, des représentants des trois départements fournissent une appréciation de la situation dans le domaine cybernétique en s'adjoignant les services d'autres départements et des cantons si les circonstances l'exigent. Ils évaluent par ailleurs les dispositifs techniques et organisationnels de protection de la Confédération. Le comité de pilotage de la SNPC garantit quant à lui une mise en œuvre coordonnée et ciblée des mesures de la SNPC et soumet au Conseil fédéral un rapport annuel sur l'avancement des travaux. Le comité de pilotage réunit des représentants des organes fédéraux compétents, mais aussi des cantons, des milieux économiques et des hautes écoles.

Un Centre de compétences pour la cybersécurité

Outre le renforcement du rôle de conduite du Conseil fédéral et l'amélioration de la coordination, les nouveautés comprennent la création d'un centre de compétences et la nomination d'un délégué ou d'une déléguée à la cybersécurité. Le ou la titulaire du poste servira d'interlocuteur principal de la Confédération pour tout ce qui concerne la cybersécurité et dépendra directement du chef du DFF. Son cahier des charges englobe la direction stratégique du Centre de compétences pour la cybersécurité ainsi que la présidence des organes de coordination «groupe Cyber» et «comité de pilotage de la SNPC». Le ou la délégué(e) sera donc à la tête des principaux organes de la Confédération dans le domaine de la cybersécurité civile. Il lui incombera en outre de faire avancer la mise en œuvre de la SNPC, de poursuivre le développement stratégique et organisationnel de la Confédération et de représenter la Confédération dans le domaine de la cybersécurité.

En instaurant le Centre de compétences pour la cybersécurité, le Conseil fédéral répond aux demandes des milieux politiques et économiques qui requéraient la création d'un guichet national unique. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (Melani) servira de base à la nouvelle entité et sera développée de manière à pouvoir assumer ce rôle de guichet national unique. De plus, le Centre de compétences s'engagera davantage pour la sensibilisation et contribuera à informer la population sur la cybersécurité avec le concours des partenaires économiques et des cantons.

Collaboration de tous les acteurs

Les cyberrisques concernent tout un chacun, raison pour laquelle il est nécessaire d'unir ses forces pour les combattre. Pour protéger la Suisse contre les cyberrisques, la Confédération doit donc collaborer avec les cantons, les milieux économiques et les hautes écoles. Le plan de mise en œuvre de la SNPC, encore en cours d'élaboration, définit les rôles de chacun. Il servira de base pour coordonner la collaboration entre les différents acteurs. La plateforme commune du comité de pilotage vise à organiser les travaux de mise en œuvre de la SNPC avec les principaux partenaires.

L'adoption de la SNPC, la clarification et la consolidation des structures de la Confédération ainsi que la mise sur pied d'organes de collaboration créent les conditions requises pour assurer une protection efficace contre les cyberrisques. La tâche qui attend les services et organes responsables est cependant immense. Les mesures fixées dans la SNPC doivent être mises en œuvre dans les plus brefs délais. Il faut aussi identifier rapidement les nouveaux défis et s'y atteler. En effet, si les stratégies et structures organisationnelles sont des bases indispensables pour améliorer la protection contre les cyberrisques, elles ne peuvent remplir leur fonction que si elles sont portées par un engagement large et indéfectible. Tous les acteurs concernés doivent en outre comprendre que, dans le domaine de la mutation numérique, la cybersécurité est une mission permanente et relève de la responsabilité de tous.

Manuel Suter
Chef de l'organe de coordination de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), Département fédéral des finances (DFF), Berne