LE CYBERESPACE, FAR WEST DU XXIE SIÈCLE

par Sylvie Guggenheim

Pour les autorités publiques, les entreprises et les particuliers, la cybersécurité est devenue l'un des enjeux majeurs du XXIe siècle. Alors que les délits plus traditionnels sont en recul, les actions criminelles dans le cyberespace sont en nette augmentation. Les études, les stratégies et les formations en la matière se sont particulièrement multipliées en Suisse et ailleurs en 2018 et 2019.

En Suisse, le nombre d'infractions contre le patrimoine est en constant recul depuis 2013, en particulier en ce qui concerne les vols. Les cambriolages ont par exemple enregistré la valeur la plus basse depuis 2009. Par contre, certaines infractions sont en hausse par rapport à 2017, telles que les escroqueries (+23%), l'utilisation frauduleuse d'un ordinateur, l'extorsion et le chantage (+49,2%) ou l'accès indu à un système informatique (+46,3%). C'est ce qui ressort du rapport annuel 2018 de la statistique policière de la criminalité, publié par l'Office fédéral de la statistique (OFS).

CYBERCRIMINALITÉ EN HAUSSE

Si les infractions et délits traditionnels sont en forte baisse, « les nouvelles technologies permettent vraisemblablement l'essor et le développement de nouveaux modes opératoires pour ce qu'on appelle communément la cybercriminalité », relève-t-il. Ces chiffres ne reflètent cependant pas tout à fait la réalité, puisqu'ils n'indiquent que des infractions dont la police a eu connaissance. « Le comportement de dénonciation a ici toute son importance. Par exemple, si les dommages sont faibles, si la personne a contracté une assurance, si elle a honte, si elle pense que la police ne pourra pas l'aider, elle aura tendance à ne pas porter plainte. L'infraction a donc bien lieu, mais elle ne peut pas être répertoriée par les forces de l'ordre », explique Philippe Hayoz, licencié en sciences forensiques, Office fédéral de la statistique.

Par ailleurs, selon une enquête réalisée début 2019 par l'institut de sondages et d'études de marché gfs-zürich, environ un million de personnes en Suisse ont déjà subi »

Les nouvelles technologies favorisent la cybercriminalité, qui est en augmentation dans le monde entier.

© Gerd Altmann

une attaque sur Internet. Mandatée par plusieurs organismes actifs dans des domaines techniques en lien avec Internet, comme l'association faîtière ICTswitzerland ou SWITCH, cette enquête met en exergue l'insuffisance des connaissances de la population suisse quant aux questions de sécurité sur Internet, alors que 92% des sondés possédaient au moins un appareil connecté au Web.

DES MILLIERS DE FRANCS DE DÉGÂTS

La Chambre vaudoise du commerce et de l'industrie (CVCI) considère la cybersécurité comme un défi majeur pour les entreprises vaudoises. Souhaitant évaluer les connaissances et les pratiques de ses membres en la matière, elle a mandaté l'institut de recherches M.I.S Trend de Lausanne, qui a réalisé un sondage à cet égard dans le courant de 2018. La CVCI s'est basée sur ces résultats pour publier une étude en octobre de la même année. Il en ressort qu'un tiers des entreprises vaudoises ont subi au moins une attaque informatique, dont certaines ont même eu à déplorer plusieurs types d'entre elles. Pour réparer les dégâts, certaines ont dû débourser plusieurs dizaines de milliers de francs.

La recherche relève également le fait qu'un tiers des compagnies sondées ne se sentent pas concernées par les cyberrisques du fait de leur petite taille. Selon les experts, elles sous-estiment le danger. Enfin, l'étude souligne le manque de formations dispensées ou prévues dans la moitié des entreprises interrogées.

D'autres sondages sur différentes thématiques autour de la cybersécurité ont été réalisés en Europe et aux États-Unis par des groupes actifs dans le domaine des assurances, tels qu'Allianz, avec son Allianz Risk Barometer, ou Europ Assistance. Le premier a effectué son enquête auprès de quelque 3'000 entités, (clients, brokers, experts en assurance, consultants, etc.) entre octobre et novembre 2018 dans 86 pays différents. Les personnes interrogées devaient notamment énumérer les risques les plus importants pour des entreprises qu'ils connaissaient. Pour la première fois, les cyberrisques ont été mentionnés comme étant les menaces les plus graves, juste après les risques d'interruption des activités. Le rapport relève tout de même que si les cybercrimes font la une des journaux, il n'en reste pas moins que ce sont plutôt des erreurs techniques ou humaines qui causent la perte de données ou des dommages au système.

Europ Assistance a pour sa part effectué un sondage en décembre 2018 aux États-Unis et dans huit pays sur le continent européen, dont »

SÉLECTION DE QUELQUES LOGICIELS MALVEILLANTS

L'Office fédéral de la police cite différents types de cyberinfraction, escroquerie et logiciels malveillants. Pour chacun d'eux, une fiche détaillée décrit l'infraction, les auteurs, le mode opératoire et donne des renseignements à cet égard.

En voici un échantillon succinct.

- Rançongiciel : maliciel bloquant l'ordinateur et demandant le paiement d'une amende, en se faisant passer pour une instance officielle
- Scareware : prétendus programmes de sécurité infectant l'ordinateur, pour pousser les gens à télécharger un programme complet et payant
- Spyware : logiciel espion visant à obtenir des mots de passe, afin de causer des dommages notamment financiers
- Cheval de Troie : logiciel exécutant des programmes en tâche de fond sans que l'utilisateur s'en aperçoive, tout en effectuant de mauvaises actions
- Cryptolocker : maliciel qui s'installe lors de l'ouverture d'une pièce jointe à un courriel, par exemple.

Pour plus de détails, voir le site internet suivant :
www.fedpol.admin.ch/fedpol/fr/home/kriminalitaet/cybercrime/gefahren/betrugsarten.html ■

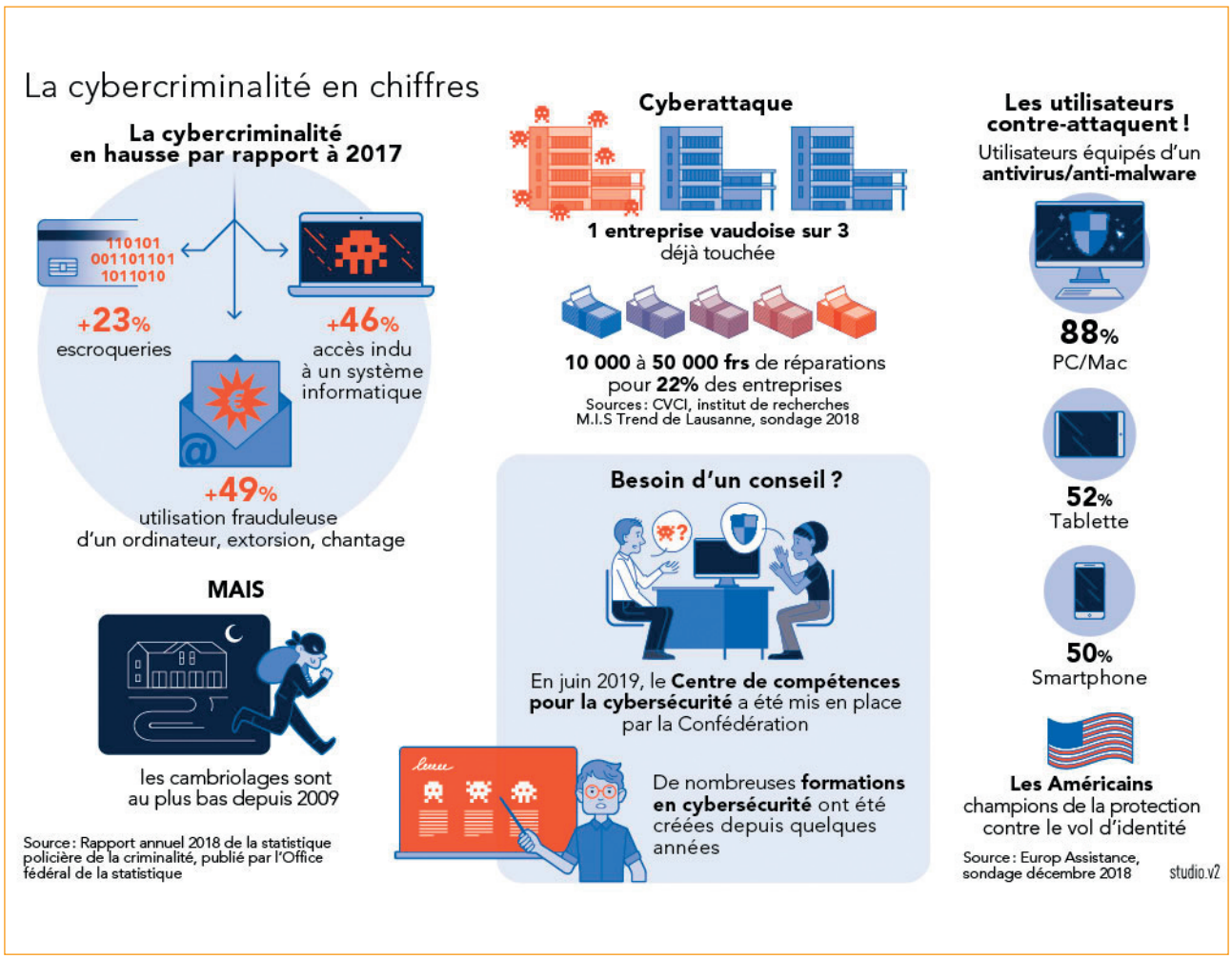
la Suisse. Il en ressort une prise de conscience élevée des cyberrisques en ce qui concerne les virus et les malwares. Par contre, les utilisateurs américains sont plus conscients du risque d'une usurpation d'identité que les Européens. De ce fait, les premiers savent mieux se protéger contre le vol d'identité. L'étude relève encore d'autres points intéressants que ce soit en termes de similitudes ou de différences entre les pays eux-mêmes.

MESURES DE PROTECTION

Conscient de l'augmentation des cas d'abus dans le cyberspace à des fins criminelles ou d'espionnage, les autorités fédérales ont mis en place une stratégie nationale de protection contre les cyberrisques (SNPC), dont le plan de mise en œuvre a été adopté par le Conseil fédéral le 15 mai 2019. La vision de la Confédération prônée par la SNPC 2018-2022: «Tout en utilisant les chances offertes par le numérique, la Suisse est protégée de façon appropriée contre les cyberrisques et est résiliente en cas de cyberincidents.» Pour y parvenir et répondre à une demande aussi bien des milieux économiques que politiques, la Confédération a créé un Centre de compétences pour la cybersécurité dont la direction stratégique est assumée par Florian Schütz, qui a été nommé délégué de la Confédération à la sécurité le 14 juin. Ce centre remplira la fonction de guichet national unique pour toutes les questions relatives aux cyberrisques.

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI (voir encadré) fera également partie de ce nouvel organisme et sera développée.

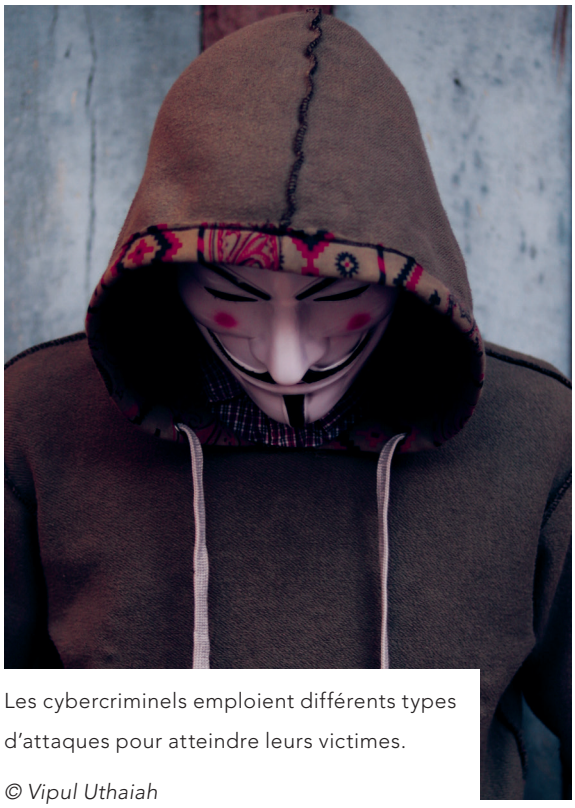
Par ailleurs, les polices de la Suisse romande viennent de créer fin février 2019 un Centre de compétence cyber, opérationnel dès »



le mois d'avril. Il est piloté par des spécialistes de la police cantonale de Genève et vise à coordonner les compétences et les ressources en Suisse romande dans ce domaine. Pour s'aider et obtenir une vision globale, les polices s'appuient sur une plateforme d'informations de la criminalité numérique, nommée Picsel.

LE BOOM DES FORMATIONS

Face à l'ampleur du phénomène, les formations en cybersécurité se sont multipliées, en particulier depuis le début de l'année 2019. En Suisse romande, l'EPFL, conjointement avec l'EPFZ, propose aux étudiants en informatique un nouveau master en cybersécurité qui débutera à la rentrée de septembre. À Genève, de même, le Centre universitaire informatique va lancer de nouvelles filières en sécurité de l'information dès janvier 2020. Les HES s'y mettent aussi, comme celle en Valais, qui offre une formation continue dans le domaine. Différents instituts privés ne sont pas en reste et proposent toutes sortes de cours plus ou moins approfondis en la matière, que ce soit à destination des particuliers ou des entreprises.



Les cybercriminels emploient différents types d'attaques pour atteindre leurs victimes.

© Vipul Uthaiah

La Chambre vaudoise du commerce et de l'industrie, même si elle n'organise pas directement de formations sur le thème de la cybersécurité, met en place régulièrement des événements autour de cette thématique avec des partenaires. Elle a aussi fait parvenir un exemplaire de son étude à chacun de ses membres. « Suite à sa publication, en octobre dernier, nous avons lancé une campagne de sensibilisation aux cyberrisques sur les réseaux sociaux. Nous avons également présenté les résultats de notre étude lors d'événements pour nos membres comme des Rencontres de chefs d'entreprise ou des ‹ 5 à 7 › », détaille Jean-François Krähenbühl, chargé de communication de la CVCI. ■

CENTRALE MELANI EN BREF

Le site internet de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI, qui s'adresse aussi bien aux particuliers qu'aux PME, donne des informations précieuses et actuelles sur les différents types de cyberattaques et la façon de procéder des délinquants ou des escrocs. Il donne des conseils sur la façon de protéger ses données informatiques et permet d'annoncer des incidents sur Internet. La centrale MELANI regroupe des partenaires travaillant aussi bien dans le domaine de la sécurité informatique que sur Internet et la protection des infrastructures nationales et vitales.

Site internet : www.melani.admin.ch/melani/fr/home.html ■