Rapport MELANI 2020/1 – Quelques recommandations afin de déjouer les cyberattaques

Célian Hirsch, le 3 novembre 2020

Le Rapport semestriel 2020/1 de MELANI sur la sûreté de l'information présente les diverses cybermenaces qui ont pesé sur la Suisse durant la première moitié de l'année 2020. En raison de la crise du coronavirus, les cyberattaques ont été particulièrement plus nombreuses comparées aux années précédentes.

Le présent repérage du rapport MELANI 2020/1 n'a pas pour objectif de résumer les diverses cyberattaques qui y sont mentionnées, mais plutôt de mettre l'accent sur quelques-unes d'entre elles et souligner les recommandations proposées par MELANI.

Examinons tout d'abord le rançongiciel (*ransomware*) « Maze ». Ce dernier ne chiffre pas uniquement les données de sa victime, il la menace également de publier les données en clair si celle-ci ne paie pas la rançon. La victime risque ainsi de s'exposer à des conséquences juridiques si la fuite de données devait devenir publique. Bien que le rapport ne le mentionne pas, soulignons ici que même sans la publication des données volées par le *hacker*, la victime peut être civilement et administrativement responsable d'avoir perdu l'accès, même momentané, à ses données. En effet, le fait qu'un *hacker* réussisse à chiffrer des données peut être un indice sérieux que le principe de la sécurité des données (art. 7 LPD, art. 8nLPD et art. 32 RGPD) a été violé (cf. notamment swissprivacy.law/19/). Deux sociétés suisses auraient d'ailleurs été victimes de ce rançongiciel.

Un autre rançongiciel, nommé « Sodinokibi/REvil », a procédé de la même façon, à la différence près qu'il a décidé de vendre aux enchères les données subtilisées à sa victime. L'Étude d'avocats Grubman Shire Meiselas & Sacks, connue pour défendre des stars, a précisément été victime d'un tel procédé. Les *hackers* peuvent ainsi réaliser des gains même si la victime ne paie pas la rançon.

Afin de diminuer le plus possible la probabilité d'être victime de telles cyberattaques, lesquelles visent souvent les ports RDP (*Remote Desktop Protocol*), MELANI recommande notamment les mesures suivantes :

- protéger tous les accès à distance par une procédure d'authentification à deux facteurs ;
- adopter et mettre en œuvre une directive excluant l'emploi de mots de passe simple ;

- n'admettre que des adresses IP uniques, spécifiques ou situées en Suisse ;
- avoir des sauvegardes informatiques exhaustives (*backup*);
- adopter des directives en matière de sécurité, lesquelles doivent comprendre des plans d'action pour la gestion des incidents ;
- sensibiliser les employés à la cybersécurité ;
- imposer à des organes dirigeants la responsabilité de surveiller la mise en œuvre des mesures de sécurité.

Le rapport de MELANI 2020/1 se penche également sur les fuites de données. Il précise que ce nombre d'incidents a augmenté durant le premier semestre 2020 et que tout indique que cette tendance se poursuivra à l'avenir. MELANI mentionne ensuite les récentes fuites de données dont EasyJet et le groupe hôtelier Marriott ont été victimes. Le rapport souligne ensuite que les fuites de données sont de plus en plus fréquentes dans le *cloud*.

Afin d'adopter une action rapide et coordonnée lors d'une fuite de données, MELANI recommande en particulier que chaque entreprise élabore un plan de réponse aux violations de la sécurité des données (*data breach response plan* ; cf. swissprivacy.law/21/). Ce plan devrait inclure des processus servant à préciser l'ampleur du dommage, la manière d'informer les victimes, ainsi que les rapports à publier. En plus de cette analyse technique et de l'évaluation de l'incident, chaque entreprise devrait ensuite estimer les conséquences juridiques et financières possibles en raison de la fuite de données .

Le rapport MELANI 2020/1 mentionne également l'importance du *phishing* par SMS (*smishing*). Ce procédé est de plus en plus utilisé afin de déjouer l'authentification à deux facteurs, en particulier pour avoir accès aux plateformes de *e-banking*. À l'aide d'ingénierie sociale (*social engineering*), la victime va transférer un code d'authentification reçu par SMS ou par WhatsApp au *hacker*. Il est à noter que contrairement aux SMS, WhatsApp ne peut pas bloquer les spams puisque les messages sont chiffrés et qu'aucun intermédiaire ne peut en vérifier le contenu. La responsabilité de déjouer ce genre d'attaques appartient ainsi aux potentielles victimes, lesquelles doivent apprendre à ne jamais transférer les codes d'authentification et à vérifier qu'elles sont sur le bon site web avant d'inscrire ce code.

Enfin, le rapport MELANI 2020/1 souligne que l'espionnage économique est une réalité en Suisse aussi. En effet, selon une étude de janvier 2020 menée par l'*Institut für Strafrecht und Kriminologie* de l'Université de Berne, l'espionnage économique touche 15 à 33% des entreprises helvétiques, toutes tailles confondues. Les secteurs les plus exposés sont l'informatique, les télécommunications, les sciences de la vie, la construction mécanique,

l’industrie et la pharma.

Proposition de citation : Célian HIRSCH, Rapport MELANI 2020/1 – Quelques recommandations afin de déjouer les cyberattaques, 3 novembre 2020 *in* www.swissprivacy.law/24