DANS LE FAR WEST DU NUMÉRIQUE

Le progrès au XXIe siècle s'incarne largement, sinon essentiellement, dans l'avènement de l'univers numérique. Un espace encore trouble, sans foi ni vraie loi, qu'il devient urgent de réguler.

PAR THIERRY OPPIKOFER

Tandis que la plupart des pays du globe se débattent pour échapper aux vagues et aux mutations successives du coronavirus, les cyberattaques se multiplient : du Pentagone à l'administration municipale de Rolle, de Facebook aux études de notaire ou aux hôpitaux romands, les logiciels malveillants et les piratages s'enchaînent, s'aggravent, se multiplient. Certaines données sont simplement volées à des fins d'escroquerie ; d'autres sont mises aux enchères sur le *darkweb* ; souvent, des rançons sont exigées, quand un « ver » informatique ne « dévore » pas tout simplement le contenu des ordinateurs.

Question d'éducation

L'analogie avec un accident de voiture ou la survenue d'un cancer est patente : la veille encore, on croyait que cela n'arrivait qu'à d'autres. Si les grandes entreprises, à commencer par les banques, ont su investir – parfois en catastrophe – pour protéger leurs infrastructures numériques, tel n'est pas le cas des artisans, des éditeurs, des médecins, des petites administrations. Le domaine de la sécurité informatique est probablement, dans l'économie du XXIe siècle, le secteur promis au plus bel avenir. Certains pays, notamment ceux d'Europe du nord, ont déjà adopté des mesures simples mais efficaces voilà des années : aucune clef USB, aucun CD extérieur n'est admis, aucun e-mail d'un expéditeur inconnu n'est ouvert sur un poste non sécurisé. En Suisse, à l'exception du secteur financier et d'institutions comme le CERN où il est impossible de faire aboutir un courriel sans être homologué, la méfiance n'est pas assez forte et de nombreuses victimes sont là pour en témoigner.

André Duvillard, le « Monsieur Sécurité » de la Confédération, insiste sur la prévention et sur l'éducation. L'ancien chef de la police neuchâteloise souligne que *« notre société a subi une transformation profonde du fait de la numérisation générale, encore accélérée par la crise du Covid »*, et que tout le monde n'a pas encore compris les risques qui allaient de pair avec cette évolution. Dès l'école, la cybersécurité devrait être enseignée. Encore faudrait-il que les enseignants eux-mêmes y soient formés…

L'argent, les données, la vie

Les cyberattaques ne concernent pas que les extorsions de fonds et la malveillance pure. Elles peuvent tuer, lorsque les pirates s'attaquent à des télécommunications (télémédecine, appels d'urgence) ou à des hôpitaux. Au début du mois d'août dernier, un logiciel malveillant a, par exemple, paralysé le site internet de la région de Rome, empêchant la prise de rendez-vous pour se faire vacciner contre le coronavirus. Peu de temps auparavant, le centre hospitalier d'Arles avait été bloqué par un cyberpirate exigeant une rançon. Aux États-Unis, une pénurie d'essence a frappé la Côte Est

Publicité

à cause d'une attaque informatique. Les systèmes de distribution d'eau ont aussi été visés.
Les délinquants, voire les criminels, ne se gênent nullement. «*La prostitution et les stupéfiants sont des activités assez risquées, et il y a peu de retour sur investissement, alors que sur internet, c'est l'inverse. Dans certains pays, même si vous vous faites prendre, les peines sont très faibles*», note Thierry Berthier, chercheur français en sécurité informatique, cité par le magazine *L'Express*. McAfee, éditeur du célèbre logiciel antivirus, estime que l'année dernière, ces actes criminels ont coûté près de 1000 milliards de dollars à l'économie, soit 1,3% du PIB mondial, contre «seulement» un peu plus de 800 milliards en 2019. Et encore, ces données ne tiennent pas compte des campagnes d'espionnage industriel, dont le préjudice reste très difficile à évaluer. Cette menace devrait encore s'amplifier, avec 28,5 milliards d'appareils reliés à internet en 2022 contre 18 milliards en 2017. Demain, tous les objets seront connectés, et le risque sera presque partout.

Maillons faibles

Les grands groupes ayant pris des mesures relativement efficaces, les pirates ont pris l'habitude d'identifier les points d'entrée moins surveillés, selon le bon vieux principe des cambrioleurs du «monde d'avant». Airbus, par exemple, a été *hacké* via un fournisseur de pièces détachées. Un photographe français, appelé pour une cérémonie familiale chez d'importants industriels, ne s'est pas non plus douté que les coordonnées et les accès par courriel des participants, qu'il avait scrupuleusement enregistrés pour leur envoyer leurs portraits, allaient servir à un malfaiteur pour pénétrer jusque dans le système de l'entreprise.

Un peu comme pour les «petits gestes» écologiques, le fait de changer de mot de passe régulièrement, de ne pas mélanger accès professionnel et privé à l'ordinateur ou au téléphone portable, d'effectuer des sauvegardes sur des serveurs indépendants, tous ces réflexes de bon sens – que personne n'a vraiment – pourraient déjà compliquer la tâche des pirates.
Soyons donc un peu paranos, mais sans peut-être aller jusqu'à imiter Joe Biden, qui, paraît-il, aurait interpellé son homologue russe lors de leur rencontre à Genève sous-entendant que nombre d'attaques informatiques venaient de son pays. «*Si nous nous retrouvons en guerre – une véritable guerre avec des échanges de tirs contre une grande puissance –, ce sera la conséquence d'une cyberattaque majeure*», a-t-il prophétisé. Une analyse qui a tout pour rassurer le reste du monde. ■

L'écosystème numérique occupe de plus en plus de place dans nos vies. Sa fragilité face aux hackers *est un sujet de préoccupation constante.* (DR)

Publicité