Comment se protéger dans un monde hyperconnecté

■ C'est un secteur en plein développement, très utile dans un monde où les objets connectés se multiplient.

■ Quelques conseils tirés du FIC de Lille et du commissaire belge Olivier Bogaert.

Dossier réalisé par
Christophe Lamfalussy

Savez-vous combien il y a de technologies de l'information dans votre maison, combien il y a d'ordinateurs dans votre voiture? Non? Bonne nouvelle pour les pirates!"

Avec Eugène Kaspersky, présent au dernier Forum international de la cybersécurité (FIC) de Lille, le ton est très vite donné. Ce Russe est à la tête de l'une des plus anciennes sociétés d'antivirus du monde et n'aime pas faire de grandes phrases. En revanche, il adore alerter. Le public est ravi, d'autant que ses apparitions sont rares. "*Chaque jour, nous collectons 380 000 codes maliciels contre 50 en 1998*, poursuit-il. *Les langages les plus utilisés sont l'espagnol, le portugais, le chinois et le russe. Il y a trois menaces aujourd'hui. En un, des pirates junior. En deux, les attaques ciblées* (comme Stuxnet en 2010 contre les installations nucléaires iraniennes, NdlR). *En trois, les attaques contre des installations*" comme un réseau électrique ou la surveillance aérienne.

Le message est clair, venant du Russe comme d'une kyrielle d'entreprises spécialisées dans la cybersécurité: comme notre monde est de plus en plus connecté, il devient de plus en plus facile à des individus peu scrupuleux de voler des informations confidentielles, de bloquer des installations vitales ou de paralyser des entreprises.

En Belgique, la priorité reste de conscientiser le public

La Belgique était présente au FIC de Lille avec un stand du Centre de la cybersécurité belge (CCB), qui dépend de la chancellerie du Premier ministre. Une quarantaine de personnes y travaillent, dont 25 issues du Cert, l'organisme chargé de détecter et d'analyser les problèmes de sécurité en ligne. Les experts belges reçoivent "*plus de 2 000 mails et cela donne l'occasion de bloquer 2 à 5 sites par jour*", explique sa porte-parole.

Et aussi de poursuivre l'essentiel, selon les responsables belges: conscientiser l'opinion publique sur la cybersécurité. Il ne se passe pas un jour sans qu'un faux message de Belgium.be, de Microsoft, d'Apple ou un chantage imposteur à la consultation de sites pornos (dit *sextortion mail*) n'alarme un citoyen belge.

L'un des meilleurs manuels pour aider le consommateur à se protéger d'éventuels pirates vient d'être publié par la Sûreté de l'État, en collaboration avec le CCB et le service de renseignement de l'armée. Il est intitulé "Surfer en toute sécurité pendant la campagne électorale" et téléchargeable sur le site de la Sûreté. (www.vsse.be/fr).

Un plan européen de neuf milliards

Dans ce domaine, la Russie et les États-Unis ont pris plusieurs longueurs d'avance. "*L'Europe dépense dix fois moins que les États-Unis en matière de cybersécurité*", souligne la commissaire européenne à l'Économie et à la société numérique, Mariya Gabriel. Et elle manque cruellement de geeks, de spécialistes en IT: près de 300 000 postes sont à pourvoir auprès des entreprises. C'est pourquoi la Commission a lancé un plan de 9 milliards d'euros visant à développer en Europe l'intelligence artificielle, la cybersécurité ou encore des pôles d'innovation.

L'Europe est pénalisée par son désintérêt historique dans l'informatique et le manque d'investissements publics en la matière.

L'itinéraire de Kaspersky

Rappelons-le: l'Internet est une invention qui fut soutenue par l'armée américaine, tandis qu'Eugène Kaspersky est, lui, un petit génie formé à l'école du KGB (ce qui lui vaut les soupçons de l'administration Trump, qu'il dément).

Dès l'âge de 16 ans, ce fils d'ingénieur fréquente l'Institut de cryptographie, de télécommunications et de sciences informatiques du KGB. Il découvrira son premier virus informatique en 1989, à la chute du mur de Berlin. Son ordinateur avait été infecté par le maliciel Cascade qui faisait chuter les lettres sur l'écran pour former un petit tas. Le virus infectait les fichiers .com (ancêtres des .exe) et avait surtout un effet visuel. Ce qui décida le Russe à lancer des programmes antivirus au début des années 1990.

Aujourd'hui, la fortune de Kaspersky est évaluée par Forbes à 1,3 milliard de dollars.

Le meilleur mot de passe sur le Net

Vous n'en sortez plus dans les mots de passe que l'on vous demande pour surfer sur Internet, à la maison ou au travail?

Olivier Bogaert, commissaire de la Computer Crime Unit (CCU) de la police fédérale, conseille d'utiliser des phrases qui peuvent être facilement mémorisées et d'en retirer par exemple la première lettre de chaque mot.

Par exemple, la phrase "*Le père du roi des Belges est Albert 2*" devient "*LpdrdBeA2*".

Vous ajoutez des points d'exclamation pour sécuriser un peu plus le mot de passe: "*!LpdrdBeA2!*"

Choisi par l'UE

Ce qui donne en fin de compte un mot de passe comprenant des lettres, des capitales, des signes de ponctuation et un chiffre.

Olivier Bogaert a été choisi par l'Union européenne comme l'un des héros de la campagne "EU protects". Il tient des chroniques régulières sur Classic 21, *Surfons tranquille.*

Face aux messageries, le retour en grâce du SMS

Les messageries instantanées telles que WhatsApp et Telegram sont très à la mode, mais sont-elles sûres pour autant?

L'an dernier, le gouvernement français a annoncé qu'il mettait au point avec la société Matrix.org un outil de messagerie chiffrée. Son intention? Sécuriser ses communications et ne plus dépendre des grandes sociétés qui thésaurisent les informations échangées.

La messagerie est développée à partir du protocole Matrix et d'une souche appelée Riot, qui sont tous les deux *open source*, c'est-à-dire téléchargeables gratuitement sur le Net. Matthew Hodgson, l'un des fondateurs de Matrix.org, est très critique à l'égard des messageries grand public.

> La France se méfie. Elle développe sa messagerie chiffrée.

Certaines, comme Facebook, stockent les informations, messages et photos échangées par les utilisateurs. D'autres ne sont pas aussi sûres que cela. "*Telegram n'est pas encrypté sauf si on active la forme Secret Chat. Facebook privilégie constamment sa propre croissance par rapport aux intérêts de ses utilisateurs. Vous devez reprendre le contrôle de vos communications plutôt que de laisser Slack ou Facebook décider pour vous*", a-t-il dit récemment au Forum international de la cybersécurité de Lille. Certaines messageries sont encryptées, comme WhatsApp, Cisco Spark ou Signal, c'est-à-dire que le message est crypté de son expéditeur à son destinataire.

L'inconnue du stockage

Mais que font-ils des photos et messages que nous échangeons? Dans le cas de WhatsApp, les données sont stockées dans les centres de données de Facebook. Les données sont cryptées, mais est-ce que la société dispose d'une clé universelle de décryptage? On l'ignore. Hodgson conseille les messageries cryptées de même que Riot/Matrix, le futur outil de l'État français.

Mais il recommande aussi les bons vieux emails (malgré les risques de piratage) et SMS. C'est encore mieux si le SMS est envoyé par un bon vieux Nokia non relié au réseau wifi. Il n'est pas le seul à se méfier des messageries et du smartphone: Eugène Kaspersky, le pape russe de l'antivirus, préfère correspondre avec des mails que par téléphone.

Quand des milliers d'internautes ont vue sur votre jardin

En principe, une caméra de surveillance est un gage de sécurité. Mais que diriez-vous si l'image de votre caméra apparaissait en live sur Internet, visible à tous? Votre jardin, votre entrée garage, le hall de l'immeuble, le bureau où vous travaillez, le restaurant où vous déjeunez, la file dans le supermarché, la plage où vous vous prélassez...

Tout cela existe depuis plusieurs années. Il suffit de taper "insecam.org" et vous aboutissez sur un site russe qui héberge plus de 73 000 caméras de surveillance dans le monde. "*Ces caméras ne sont pas piratées*, précise l'administrateur du site russe.*Toutes les caméras hébergées sur ce site n'ont pas de mot de passe de protection.*"

> En Belgique, 67 caméras sont répertoriées. Dans le monde, 73 000.

Un restaurant à Louvain-la-Neuve

Du coup, on est au balcon d'une incroyable palette de vues sur la vie quotidienne de la Russie aux États-Unis, en passant par une boulangerie à Paris ou un magasin à Téhéran. En Belgique, 67 caméras étaient répertoriées jeudi, y compris dans un café-restaurant de Louvain-la-Neuve où l'on peut voir qui mange avec qui et dans un bureau de Malines où on peut constater l'assiduité du personnel à la machine à café.

"*Ces endroits sont identifiables puisqu'il y a la longitude et la latitude. On sait exactement où est la caméra ou, en tout cas, le point wifi qui est généralement dans la maison*", explique Olivier Bogaert, policier fédéral à la Crime Computer Unit.

La caméra de surveillance peut être utile pour un touriste qui veut savoir quel temps il fait à la mer ou s'il y a du monde à Times Square. Mais le problème est que de nombreux particuliers n'ont pas protégé leur caméra avec un mot de passe ou ont gardé le mot de passe d'origine. Comme celle-ci est connectée au réseau wifi, elle devient accessible à tous, y compris aux candidats voleurs.

Insecam.org donne la possibilité aux propriétaires des caméras de l'enlever du site, mais les avertit que ces caméras resteront visibles de tous, grâce à des softwares de recherche, sauf à mettre un nouveau mot de passe.

Il y a deux ans, les autorités belges avaient alerté l'opinion publique, notamment via l'émission de la RTBF, *On n'est pas des pigeons*. Le buzz avait permis de descendre d'environ 120 caméras répertoriées à une soixantaine. "*Le problème*, souligne Olivier Bogaert, *est que de nouvelles installations non sécurisées ont été installées entre-temps.*"