Ecoutez les podcasts du Soir

Retrouvez le podcast quotidien du *Soir* pour s'informer, décrypter et s'inspirer.

« À propos », c'est l'information comme vous l'entendez, avec des sujets racontés et analysés par les journalistes de la rédaction pour mieux comprendre l'actualité.
Pas de pause pour À Propos ! Pendant les vacances, on vous propose une série de rétrospectives sur l'actualité qui a marqué cette année. La formule reste identique : des journalistes de la rédaction racontent, analysent et donnent des clés pour mieux comprendre. À Propos de 2022, c'est l'opportunité de jeter un œil dans le rétro sur les faits marquants de l'année écoulée (guerre en Ukraine, prix de l'énergie, bouleversement climatique). C'est aussi un micro ouvert à des personnalités comme Pierre Kroll, Marius Gilbert ou Béatrice Delvaux pour avoir leurs impressions sur les douze derniers mois.
À Propos de 2022, c'est du lundi au vendredi, du 26 décembre au 6 janvier, sur notre site, notre application et toutes vos plateformes de podcast préférées.

Découvrez « À propos » et tous les podcasts sur : *Le Soir* (podcasts.lesoir.be ou via l'application), « Podcast Addict », « Apple Podcasts», « Google Podcasts », Spotify et Amazon Music.

FRAUDE

La cybercriminalité pour battra certainement des

Rien que sur la première moitié de l'année, les chiffres de la « fraude informatique » et de « hacking » affichaient déjà une tendance à la hausse. Communes, hôpitaux et même zones de police ne sont définitivement plus à l'abri.

ARTHUR SENTE

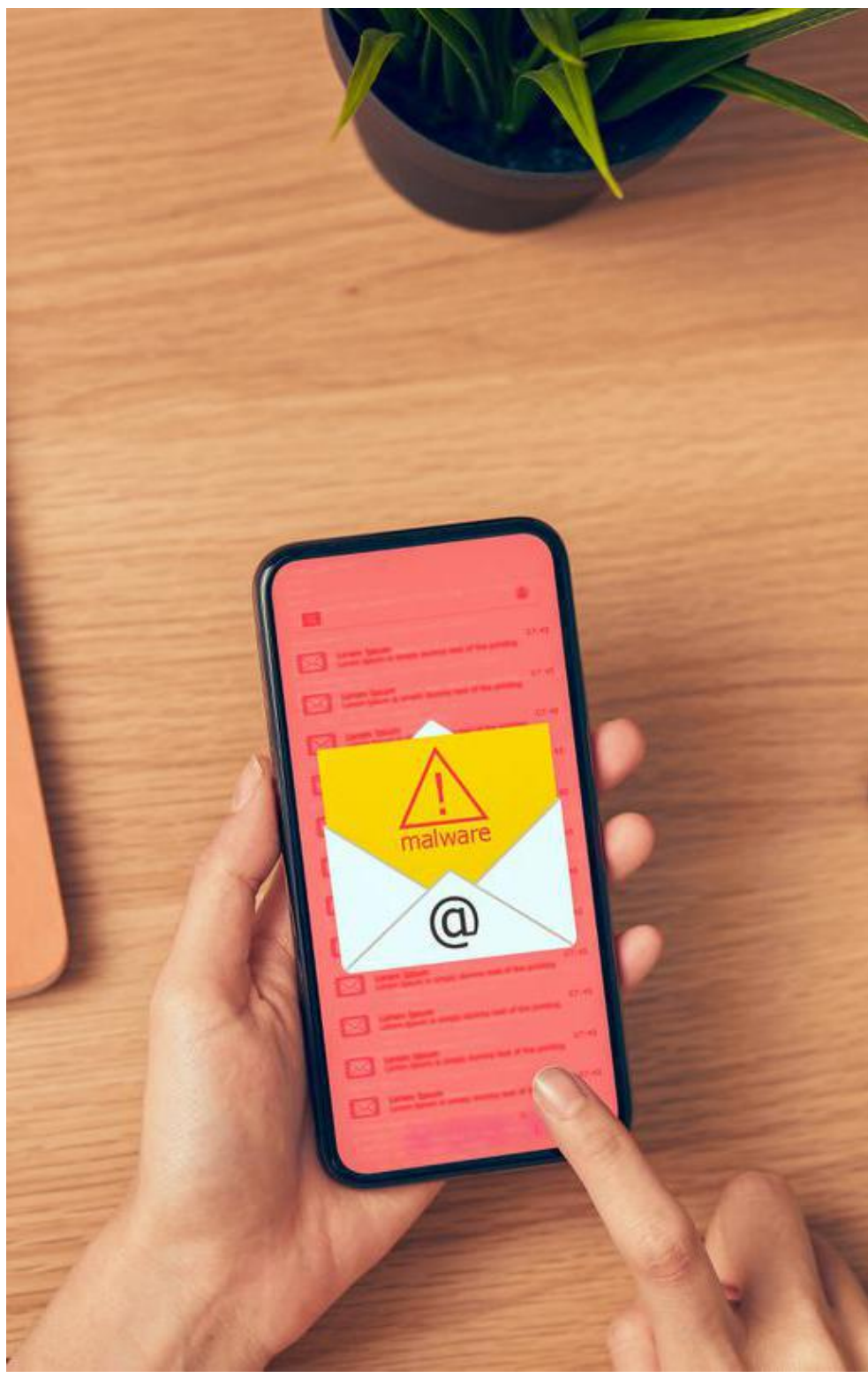
L'annonce relative à une fuite potentiellement massive de données qui concernerait entre autres des clients de Belfius – quand bien même cette fuite émanerait, comme cela semble se préciser, d'un *call center* étranger à la banque – sera-t-elle la dernière mauvaise nouvelle de l'année en matière de sécurité informatique ? Au rythme où vont les choses, cela n'est pas dit. Car 2022 a été marquée par une activité cybercriminelle très soutenue, visant par ailleurs des cibles toujours plus importantes, notamment dans notre pays.

Un premier semestre détonant

D'abord, il y a les chiffres. Que disent-ils ? Le rapport annuel du Centre pour la cybersécurité de Belgique (CCB) sur le sujet ne paraîtra qu'en janvier et les statistiques policières complètes relatives à l'année écoulée ne seront publiées que l'été prochain. Mais à en croire les données relatives au premier semestre 2022, déjà accessibles sur le site de la police fédérale, la criminalité en ligne semble se porter mieux que jamais.

De début janvier à fin juin 2022, les forces de l'ordre ont ainsi été avisées de l'existence de 50.087 délits « comportant un élément ICT/Online » (ce qui correspond à un spectre très large de faits allant du *hacking* à la production de faux en informatique, en passant par le « sabotage »). Comparativement, de janvier à décembre 2021, on en avait comptabilisé 92.763 en tout, ce qui laisse déjà imaginer un nouveau bilan annuel en hausse.

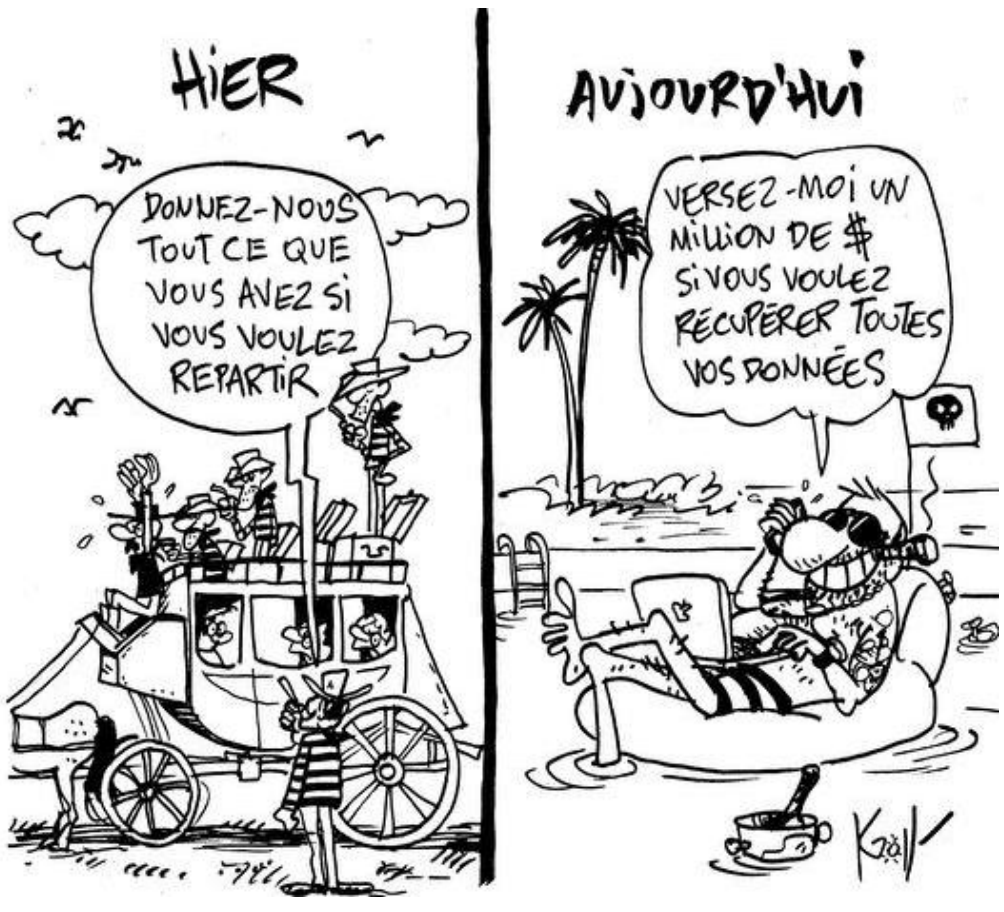
Sur cette même première moitié de l'année écoulée, 23.858 infractions de « fraude informatique » (ce qui est déjà plus précis), ont été enregistrées dans les bases de données policières. A titre d'information, c'est déjà 3.500 faits de plus (!) que sur l'ensemble des douze mois de l'année 2018. Sauf baisse de régime exceptionnelle entre juillet et décembre dernier, le record annuel de 39.716 faits (enregistré en 2021) sera sans difficulté dépassé, et même sans doute assez largement.



Quelques conseils pour éviter les cyberattaques

Olivier Bogaert, commissaire à la Computer Crime Unit, conseille de « vérifier les autorisations de ses applications » : « Sur Facebook, il y a des droits d'accès aux micros, aux informations des autres applications, il faut les désactiver. »
Pour les achats en ligne, la carte de crédit prépayée possède tous les avantages, d'après lui : « Elle permet de mettre soi-même de l'argent dessus. Si ses données sont fuitées, pas de souci, il n'y a pas de sous dessus. Je conseille de créer une adresse mail dédiée aux achats, une autre pour ses réseaux sociaux et une troisième personnelle, ça limite les risques. »
Concernant les SMS ou mails louches, il faut vérifier les adresses URL des liens ainsi que l'identité de l'expéditeur : « Avec l'usurpation d'identité, un *hacker* peut se faire passer pour un proche et vous envoyer un lien qui fera entrer un virus dans votre système. »
Le Centre pour la cybersécurité de Belgique conseille l'utilisation d'un antivirus et de l'utiliser régulièrement. Pour Olivier Dolbrechts, manager chez Mister Genius, il faut un antivirus puissant, ils le sont de plus en plus. Il conseille les EDR (pour *Endpoint detection and response*), qui vérifient en temps réel les activités et qui peuvent identifier très vite les suspectes. Il préconise aussi les sauvegardes : « Il faut toujours avoir un *back-up*, un *cloud*, deux si possible. » Les gestionnaires de mots de passe, qui en génèrent de très robustes et qui les gèrent ensuite, ont aussi sa bénédiction. LUCIE BOUDIN-DUFILS (ST.)

KROLL



couverture Face à la difficulté de pouvoi la cybercriminalité, les entreprises s'orga

JEAN-FRANÇOIS MUNSTER

Les entreprises peinent de plus en plus à s'assurer contre le risque cybercriminel. La fréquence des sinistres et les dommages potentiels sont devenus à ce point élevés que les assureurs deviennent extrêmement frileux. Les primes et les franchises s'envolent, les couvertures se réduisent… La situation est telle que certaines entreprises ont même renoncé à s'assurer. Dans le *Financial Times*, Mario Greco, le patron de Zurich, l'un des plus grands assureurs européens, estimait ce lundi que le risque cyber allait devenir « inassurable » et plaidait pour la mise en place de schémas public-privé pour gérer les cyber-risques systémiques sur le modèle de ce qui existe pour les tremblements de terre ou les attaques terroristes. Dans un entretien au *Soir* le mois dernier, la patronne d'AG Insurance, Heidi Delobelle, reconnaissait également « n'avoir pas encore trouvé de solutions pour véritablement aider les victimes de ce type de criminalité ».

Face aux manquements du marché, douze grandes sociétés européennes – les groupes chimiques belge et allemand Solvay et BASF, le géant de l'aéronautique Airbus, le fabricant de pneus Michelin, le groupe de services à l'environnement Veolia – ont décidé de prendre les choses en main et de s'associer. Elles ont créé leur propre compagnie d'assurances destinée à couvrir leurs risques cyber. Miris – c'est son nom – est basée en Belgique et a décroché le 20 décembre sa licence auprès de la Banque nationale. Elle débute son activité ce 1er janvier sous statut de mutuelle. Chaque entreprise a injecté un montant équivalent de capital pour pouvoir bénéficier de la couverture.

« L'idée a germé il y a un plus d'un an lors de rencontres entre directeurs des assurances de grands groupes européens », explique Sonia Cambier, directrice des assurances chez Solvay et présidente du conseil d'administration de Miris. « Face aux lacunes du marché, on s'est dit : "Pourquoi ne pas créer une mutuelle qui fournirait à ses membres les capacités d'assurance dont ils ont besoin ?" L'idée n'est pas de remplacer les assureurs traditionnels, mais de venir en complément de ceux-ci. Miris offre une couverture allant jusqu'à 25 millions pour chacun de ses membres. »

La prévention est centrale

Solvay ne trouvait plus son compte avec ce que le marché pouvait lui offrir. « Il y a pas mal d'assureurs actifs dans le domaine de la cybersécurité, mais leur capacité s'est restreinte », explique Sonia Cambier. « Ils limitent leur exposition à de petits montants : 5, 10 millions. On doit faire appel à beaucoup d'assureurs pour atteindre les 150 millions de couverture que l'on s'était fixés. On veut aujourd'hui aller au-delà et on ne trouve plus les capacités sur le marché. » Elle constate un durcissement de