Le côté obscur de la technologie

Chris Wellisz

La médaille du numérique a son revers

LE NUMÉRIQUE nous a apporté un confort et une commodité à peine concevables il y a une génération de cela. Internet épargne aux étudiants et universitaires de fastidieuses recherches en bibliothèque, tout en permettant une communication visuelle, orale et écrite instantanée quasi gratuite. Le GPS des smartphones permet de se repérer dans une ville inconnue ou de trouver le Starbucks le plus proche. Le shopping et la gestion des comptes se font en ligne. Même les médecins trouvent des aides au diagnostic sur le Web. Cette ère numérique est tellement merveilleuse que les universitaires Erik Brynjolfsson et Andrew McAfee l'ont surnommée «Le Deuxième âge de la machine», estimant que les ordinateurs sont pour notre cerveau ce que la machine à vapeur a été pour nos muscles.

Ce progrès ne va pourtant pas sans écueils. Certains détracteurs du numérique regrettent l'influence de quelques géants des médias sociaux sur l'opinion. D'autres pointent des fléaux tels que le cyberharcèlement et la cyberpornographie. D'autres encore s'inquiètent pour le respect de la vie privée et des libertés civiques, à une époque où le moindre mouvement, appel ou courriel laisse une trace exploitable par un voisin indiscret ou un gouvernement intrusif.

Bien que légitimes, ces inquiétudes sont impossibles à quantifier. Cependant, certains aspects du numérique engendrent des coûts chiffrables qui contrebalancent, en partie au moins, l'efficacité offerte par ce deuxième âge de la machine.

Les hackers peuvent prendre le contrôle de voitures ou couper un réseau électrique. Les cyberescrocs subtilisent des informations personnelles pour siphonner des comptes ou effectuer des achats frauduleux. Révolutionnaires, le courriel, les téléphones mobiles et les réseaux sociaux nuisent aussi à la productivité d'employés de bureau pendus à leur fil Twitter ou leur messagerie instantanée.

Risques pour la cybersécurité

Lorsque d'anciens officiers de l'unité 8200 israélienne, chargée du renseignement d'origine électromagnétique, ont créé une société de cybersécurité privée, ils voyaient dans les voitures connectées la prochaine percée.

«Ils ont observé les marchés et conclu qu'il y aurait bientôt des millions de voitures connectées», explique Yoni Heilbronn, Vice-président du marketing chez Argus Cyber Security.

Trois ans plus tard, cette entreprise de Tel-Aviv ouvrait des bureaux en Allemagne, au Japon et aux États-Unis. Les prises de contrôle de voitures — sans parler des accidents causés par le pilote automatique des véhicules Tesla Motors où aucun piratage n'était en cause — soulignent la nécessité d'améliorer la cybersécurité automobile. De quoi nourrir la prospérité d'Argus.

Bienvenue dans l'Internet des objets (IdO) — connectés à un réseau leur permettant d'envoyer et de recevoir des données —, qui ne cesse de grandir pour englober équipements de diagnostic hospitalier, machines à café ou autres appareils ménagers. Cette année, le nombre d'appareils connectés va augmenter de 30 % pour atteindre 6,4 milliards d'unités selon Gartner, acteur majeur de la recherche et du conseil dans les technologies de l'information. À l'échelle mondiale, les dépenses consacrées à la sécurité sur l'IdO vont bondir de 24 % jusqu'à 348 millions de dollars.

Qui dit monde connecté dit plus d'occasions de prélever des informations personnelles pour effectuer des transactions frauduleuses ou pour alimenter des «rançongiciels», ces logiciels malveillants qui immobilisent des appareils ou cryptent des données puis monnayent une clé de déblocage.

«C'est un nouveau point d'entrée pour les arnaqueurs», résume Bradley J. Wiskirchen, directeur général de Kount, spécialiste de la sécurité Internet basé à Boise (Idaho). «Pas besoin d'entrer dans mon ordinateur s'ils parviennent à pirater mon imprimante ou mon réfrigérateur.»

Les appareils domestiques connectés sont souvent faciles à pirater, car leur protection intégrée est basique, voire inexistante. Les entreprises telles que Nest Labs (Palo Alto, Californie), qui fabrique des appareils intelligents dotés de fonctionnalités de sécurité avancées, sont rares.

«Les autres se contentent souvent d'installer des logiciels *open source* sur leurs appareils. La sécurité n'est pas vraiment prise en compte», explique Chris King, analyste en vulnérabilité au CERT Coordination Center, antenne du Software Engineering Institute de l'université Carnegie-Mellon. Même des jouets comme la poupée Hello Barbie connectée via Wi-Fi peuvent être pris pour cible.

La liste des appareils vulnérables s'allonge proportionnellement à l'expansion de l'univers connecté. Des pirates ont bloqué des systèmes de diagnostic hospitalier pour obtenir des rançons, raconte King. L'an dernier dans l'Ouest de l'Ukraine, c'est un réseau électrique qui a été coupé, laissant plus de 200.000 habitants sans courant. En Allemagne, des cybervandales ont provoqué de lourds dégâts matériels dans une aciérie.

> Les cybercriminels prélèvent des informations personnelles pour effectuer des transactions frauduleuses ou pour utiliser des «rançongiciels».

Le spectre des voitures piratables fait froid dans le dos lorsque l'on pense au risque d'un accident mortel. Gartner estime que d'ici à 2020, environ 250 millions de véhicules dans le monde auront à bord une forme de connectivité sans fil.

Dans un véhicule moderne, pratiquement toutes les fonctions — freinage, direction, pression des pneus, phares — sont gérées par des commandes informatisées reliées entre elles par un «bus», système de communication inventé il y a 30 ans, c'est-à-dire avant Internet. Le bus est donc intrinsèquement vulnérable, tout comme de nombreux autres appareils d'une voiture.

«Un système qui se retrouve connecté sans avoir été conçu pour est soudain vulnérable à tout un tas de choses jamais envisagées par ses concepteurs», souligne King.

Échaudé par deux piratages majeurs, le secteur automobile prend cette menace au sérieux et redouble les mesures de sécurité.

Des chercheurs de l'entreprise Argus se sont introduits dans un Zubie, un dispositif de suivi des performances de la voiture qui envoie des données sans fil et en temps réel sur le smartphone du conducteur via le nuage, lequel reçoit aussi des notifications sur son véhicule et son comportement au volant. Après avoir pris la main sur la direction, les freins et le moteur, ils en ont informé Zubie, qui a annoncé avoir depuis corrigé cette vulnérabilité.

L'an dernier, Fiat Chrysler Automobiles a rappelé 1,4 million de véhicules suite à un article du magazine *Wired* relatant comment des chercheurs avaient pris le contrôle d'une Jeep Cherokee avec un ordinateur portable en passant par l'ordinateur de bord.

«Qui dit voiture connectée, dit protection», résume Heilbronn, chez Argus. ■

Cyberbraquage

Dans son bureau de l'Association for Financial Professionals à Bethesda (Maryland), Magnus Carlsson reçoit un courriel de son directeur général lui demandant de l'aider à effectuer un virement.

Or en cliquant sur «Répondre», il voit une adresse inhabituelle s'afficher. «J'ai tout de suite repéré l'arnaque-type», relate Carlsson. Encore heureux : en tant que responsable de la trésorerie et des paiements au sein du représentant mondial des professionnels de la finance, son rôle consiste en partie à mettre en garde les membres dans le monde entier contre les nombreuses sources de fraude financière, parmi lesquelles les arnaques sur Internet.

Le «*business email compromise*» fait de plus en plus recette chez les cybercriminels. Cette tactique consiste à inciter des employés

Cyberbraquage *(suite)*

à effectuer des virements à des fournisseurs ou créanciers fictifs, ceci en imitant généralement un courriel d'instruction en provenance d'un supérieur. Un sondage auprès des membres de l'association a révélé que 64 % d'entre eux y ont été exposés.

Mais les cyberescrocs ont de plus en plus de cordes à leur arc numérique, qui comprend des tactiques et outils aux noms fantaisistes, voire sinistres : rançongiciel, hameçonnage, cheval de Troie, *etc.* De plus en plus pointus, actifs et audacieux, les cybercriminels pêchent au gros — JPMorgan Chase & Co., British Airways, commission électorale des Philippines et fisc américain —, avant de se replier sur le menu fretin une fois que les cadors bétonnent leur défense.

> Un cybercriminel ayant l'intention de provoquer le chaos pourrait très bien anéantir le système financier mondial tout entier.

La cybercriminalité progresse, car «de plus en plus de pays et d'entreprises débarquent sur Internet avec de simples rudiments de cybersecurité. Ce sont des proies faciles», analyse James Andrew Lewis, Vice-président senior au Center for Strategic & International Studies (CSIS) de Washington et auteur de nombreux ouvrages sur la cyberfraude. «L'application des lois est très hétérogène à travers le monde. S'il est futé, le hacker va s'installer dans un pays laxiste».

Lewis estime à plus de 500 milliards de dollars les dégâts causés par la cybercriminalité chaque année dans le monde, soit davantage que le PIB de la Suède. Cette évaluation comprend l'argent et la propriété intellectuelle volés, le coût de la réparation des effractions et l'impact négatif sur l'innovation, le commerce et la croissance économique.

Les institutions financières sont des proies alléchantes, comme l'a montré le vol de 81 millions de dollars à la banque centrale du Bangladesh cette année. En usurpant les identifiants d'un employé, les pirates ont envoyé plus d'une trentaine de demandes de virement à la Federal Reserve Bank de New York.

Pour un pays comme le Bangladesh, la perte a été colossale. Mais c'est un risque encore plus sérieux qui inquiète les régulateurs. En effet, un cybercriminel ayant l'intention de provoquer le chaos pourrait très bien anéantir le système financier mondial tout entier, déclenchant une déconfiture similaire à la crise de 2007–08.

«Nous parlons là de la possibilité de bloquer aux acteurs du marché l'accès à des éléments clés de notre réseau», pose Greg Medcraft, Président de l'Australian Securities and Investment Commission. «Les cyberattaques sont probablement le prochain phénomène mondial de cygne noir.»

Mené par la Depository Trust & Clearing Corporation, le dépositaire central américain, un sondage consacré aux menaces pesant sur la stabilité financière mondiale a montré que 25 % des personnes interrogées placent la cybercriminalité en tête. Cette proportion, qui s'élevait à 46 % l'an dernier, a baissé sous l'effet des investissements dans la protection, mais aussi de la montée d'autres risques, comme le ralentissement économique en Asie.

Cependant, les régulateurs ne veulent rien laisser au hasard. Conformément aux directives émises en juin par la Banque des règlements internationaux et l'Organisation internationale des commissions de valeurs, les systèmes de paiement et de règlement, rouages essentiels de la finance, devraient se doter de dispositifs de protection et de riposte, et désigner un superviseur.

Selon une étude de PwC, la cybercriminalité est le deuxième délit en col blanc le plus courant après le détournement de biens. Or si 61 % des PDG se disent préoccupés par la cybersecurité, seules 37 % des organisations analysées disposent d'un mécanisme de riposte.

La criminalité sur Internet relève de deux grandes catégories : les effractions monnayables comme les vols de données de carte bancaire ou les usurpations d'identité et le cyberespionnage, à savoir le vol de secrets commerciaux, de stratégies de négociation et d'informations sur des produits.

Selon le rapport annuel sur les menaces de sécurité Internet de Symantec, le nombre d'identités exposées a bondi de 23 % en 2015 pour atteindre 429 millions. Le chiffre réel doit probablement dépasser 500 millions, car de nombreuses entreprises ne signalent pas les incidents.

Suite aux vols de données colossaux dont ont été victimes l'assureur-maladie Anthem Inc ou le site de vente aux enchères eBay, pratiquement toutes les identités des États-Unis ont été exposées, estime Bradley J. Wiskirchen, chez Kount.

Les identités volées sont commercialisées sur un marché noir électronique en plein essor, où des produits sont proposés sur des sites Web rivalisant avec les meilleurs distributeurs, le tout avec garanties de remboursement, prix de gros et tutoriels.

Le coût moyen d'une fuite de données est passé de 3,79 millions à 4 millions de dollars selon une récente étude menée par IBM et le Ponemon Institute auprès de 383 entreprises dans 12 pays. C'est en Afrique du Sud et au Brésil que ces incidents sont les plus susceptibles de se produire, l'Allemagne et l'Australie offrant les terrains les moins propices.

L'attaque de 2014 sur JPMorgan Chase & Co. a exposé 83 millions de fichiers clients contenant noms, adresses électroniques et postales, et coordonnées téléphoniques, soit le piratage le plus important jamais subi par une institution financière américaine. Si la banque n'a pas ébruité le coût de l'opération, elle a annoncé une augmentation de 250 millions de dollars par an de ses dépenses consacrées à la protection.

Le coût du vol de propriété intellectuelle est plus difficile à estimer, mais ses répercussions économiques peuvent être plus amples. Cette pratique, qui concerne aussi bien des formules de peintures que des plans de fusées, réduit les bénéfices potentiels de l'innovation, rappelle Lewis, du CSIS. «Ce sont les retombées financières qui motivent l'invention. En l'absence de retombées, les gens se tournent vers autre chose», développe-t-il.

Résultat? Un sous-investissement dans les nouvelles technologies, des pertes d'emplois et une croissance économique

ralentie. Même les pays qui gagnent finissent par perdre à long terme, car en s'appuyant sur des technologies volées, ils n'apprennent pas à développer les leurs. «Du coup, le monde entier progresse plus lentement», constate Lewis.

Selon lui, le coût total de la cybercriminalité, vol de propriété intellectuelle compris, représente en moyenne 0,5 % du PIB mondial : jusqu'à 0,9 % dans les pays à revenu élevé, où l'innovation pèse davantage; plutôt 0,2 % dans ceux en développement. Cette conjonction de facteurs alimente la croissance spectaculaire de la demande de services de protection, qui atteindra 170 milliards de dollars en 2020 contre 75 milliards l'année dernière, selon les prévisions de Cybersecurity Ventures, spécialiste de l'étude et de la connaissance des marchés.

Le volume de transactions de Kount connaît une croissance annuelle à trois chiffres, «et nous avons à peine gratté la surface des opportunités potentielles», ajoute Wiskirchen. «J'opère hélas dans un secteur à très forte croissance.» ■

Distraction numérique

Jeune programmeur à Silicon Valley, Laurie Voss s'était vu donner un mois pour boucler un projet extrêmement rébarbatif. «J'ai passé beaucoup de temps sur Twitter ce mois-là.»

Pour Voss, aujourd'hui Directeur technologique dans sa propre startup, NPM, tweeter au travail est la version XXIe siècle de la bonne vieille procrastination.

Les applis et gadgets à la mode offrent des moyens novateurs et irrésistibles de perdre du temps. Partout dans le monde, les employés de bureau sont assaillis par un flux incessant de notifications visuelles et sonores. Alors que les nouvelles technologies se répandent à travers le monde et que l'économie du savoir prospère, la distraction numérique et sa cousine, la surinformation, freinent de plus en plus la productivité.

> La distraction numérique et sa cousine, la surinformation, freinent de plus en plus la productivité.

Selon un sondage publié en juin par CareerBuilder, conseiller en ressources humaines basé à Chicago, trois employeurs américains sur quatre estiment que la distraction du personnel représente au moins deux heures gâchées par jour.

L'utilisation du téléphone mobile et le «textotage» sont cités comme les activités les plus chronophages, devant Internet, le bavardage et les réseaux sociaux. Cette perte de temps impacte la qualité du travail, le moral des employés devant rattraper le relâchement de leurs collègues distraits, et le respect des délais.

Consultant en organisation basé à Jérusalem, Nathan Zeldes incrimine particulièrement le courriel et reproche aux employeurs de ne pas en limiter l'utilisation. Selon lui, un employé de bureau peut recevoir entre 50 et 300 messages professionnels par jour.

«Impossible de lire ou de traiter tout cela intelligemment», assène-t-il. «Et ça n'arrête pas...»

Les courriels superflus et les interruptions inutiles coûtent au travailleur du savoir moyen une journée de productivité par semaine, précise Zeldes, citant une étude qu'il a menée en 2006 alors qu'il était ingénieur chez le fabricant de puces électroniques Intel Corporation. Pour une entreprise de 50.000 employés, la facture s'élève à environ 1 milliard de dollars par an.

Difficile de résister au courriel, poursuit Zeldes. On se sent obligé de lire ses messages et d'y répondre 24h/24 de peur de manquer une communication importante, ou pour impressionner ses collègues ou son patron.

«Je compare cela au dilemme du prisonnier. Tout le monde rêve d'envoyer moins de courriels et de rentrer plus tôt, mais personne n'ose être le premier à décrocher», conclut Zeldes.

Docteure en psychologie, Gloria Mark enseigne au département informatique de l'Université de Californie. Elle utilise le parallèle avec le jeu pour décrire le conditionnement à l'utilisation du courriel.

«Je parle du phénomène Las Vegas. Un joueur de machine à sous est récompensé à intervalles aléatoires par un gain occasionnel. La perspective de toucher un autre gain suffit à le pousser à jouer encore et toujours.»

«Il est d'autant plus difficile de se débarrasser d'une habitude qu'elle est renforcée aléatoirement», explique Mark.

Dans une étude réalisée en 2012, elle avait conclu que la durée de concentration maximale sur un écran d'ordinateur était de 75,5 secondes en moyenne. L'an dernier, cette durée était passée à 47 secondes.

Employés et employeurs ont élaboré toute une batterie de stratégies de lutte contre la distraction et la surinformation. Ils sont nombreux à réserver des créneaux au traitement des courriels pour ignorer ces derniers le reste du temps.

«Je passe beaucoup de temps à optimiser mes courriels», confie Voss, chez NPM. Sa recette? «Filtrer sans pitié» tout message «qui est répétitif, tout ce qui est routinier, tout ce que je n'ai pas besoin de savoir ou de traiter.»

«Désactivez toutes les notifications. Ne laissez pas des informations vous sauter devant les yeux», recommande Cliff Williams, concepteur senior chez Nextdoor, un «réseau social privé pour votre voisinage» basé à San Francisco.

Pourtant, Williams reconnaît qu'éviter les distractions relève d'un «combat perpétuel».

«C'est comme le régime. On perd du poids puis on en reprend.» ■

Chris Wellisz est un journaliste financier basé à Washington.