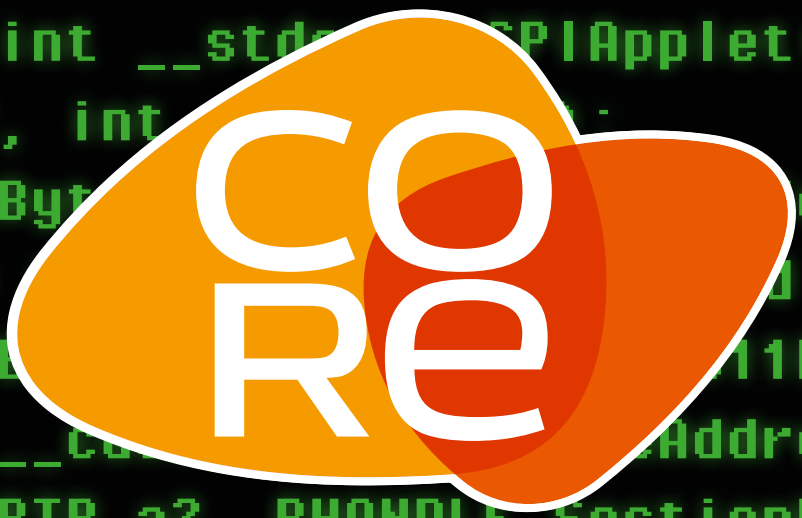
Le magazine clients de Coop Protection Juridique SA
Numéro 4



CYBERCRIME

_Cyberwar: la guerre silencieuse

_Hacking: dans la zone grise

_Dark web: en eaux troubles

L'ABC du cybercrime

Dark web

Ensemble de réseaux dont l'accès n'est généralement possible que sur invitation. La transmission des données est cryptée et les utilisateurs restent anonymes pour échapper à toute surveillance.

Distributed Denial of Service (DDoS)

Attaque d'un système informatique à l'aide d'une multitude de requêtes visant à le saturer et à le paralyser.

Hackers

Pirates qui s'infiltrent dans les systèmes informatiques. Les white hats respectent la loi, les black hats sont des criminels et les grey hats oscillent entre légalité et illégalité.

Deep web

Partie du web introuvable par les moteurs de recherche conventionnels. Le deep web est environ 500 fois plus volumineux que la partie visible de la toile.

Exploit

Elément de programme permettant d'exploiter les failles de sécurité d'un programme. Un must pour les malfrats du dark web!

Système de détection d'intrusion

Système qui reconnaît les attaques dirigées contre un réseau d'ordinateurs. Complète généralement les pare-feux.

Keylogger

Dispositif matériel ou logiciel qui enregistre les touches utilisées sur un clavier à des fins de piratage, de surveillance ou de reconstitution.

Malware

Programme malveillant installé par un hacker sur un ordinateur pour récupérer des données ou envoyer des spams. Aussi appelé maliciel.

Spyware

Logiciel espion qui collecte les données d'un utilisateur pour lui envoyer de la publicité ciblée. Aussi appelé mouchard ou espiogiciel.

Virus

Programme malveillant attaché à un fichier qui est capable de se dupliquer et d'infecter d'autres logiciels.

Zombie

Ordinateur contrôlé à distance par un hacker au moyen de vers, de virus ou de chevaux de Troie. Généralement, l'utilisateur ne remarque rien.

Phishing

Tentative d'accéder aux données personnelles d'un internaute en lui envoyant des e-mails ou des SMS trompeurs. Contraction de «password fishing».

Cheval de Troie

Programme informatique se faisant passer pour une application utile, mais qui remplit une autre fonction.

Ver

Programme malveillant qui se propage sans programme hôte via les réseaux ou les clés USB.

Editorial

Chères lectrices, chers lecteurs,

Nous faisons nos achats sur Internet et les payons en ligne, nos appareils sont connectés et nos données sont stockées sur un cloud: pour les criminels, le web est devenu un pays de Cocagne. Les pirates de la toile déversent du spam dans nos boîtes aux lettres, infectent nos ordinateurs à l'aide de chevaux de Troie et s'invitent sur nos disques durs sans y avoir été conviés. Désormais, le risque zéro n'existe plus et, avec l'augmentation de la cybercriminalité, tout un chacun ressent le besoin de mettre ses données à l'abri. En tant qu'assurance protection juridique, la sécurité informatique nous concerne bien sûr au plus haut point. Mais il ne suffit pas de réagir: il faut agir avant qu'il ne soit trop tard. C'est pourquoi nous avons décidé de vous expliquer comment vous pouvez vous protéger.

Nous sommes partis à la découverte du cybermonde et l'avons sondé jusque dans les sombres profondeurs du deep web et du dark web. Dans ce numéro de Core, nous partageons avec vous le fruit de nos recherches. Vous y trouverez une mine d'informations, des reportages passionnants et des portraits émouvants.

Daniel Siegrist
CEO, Coop Protection Juridique SA

<page=2>

Impressum
Editeur: Coop Protection Juridique SA. Responsables du projet: Petra Huser, Sibylle Lanz, Coop Protection Juridique SA. Rédaction: Matthias Mächler, www.diemagaziner.ch. Maquette/Réalisation: Baldinger & Baldinger AG, Aarau. Production: Christoph Zurfluh, www.diemagaziner.ch. Impression et expédition: Schwabe Druck, Bâle. Tirage: 5000 exemplaires. Parution: une fois par an. Commandes: Coop Protection Juridique SA, Entfelderstrasse 2, Case postale 2502, CH-5001 Aarau, petra.huser@cooprecht.ch. Les informations sur les prestations de service et les produits publiées dans ce magazine ne constituent pas des offres au sens juridique du terme.

Sommaire

<page=3>

<page=4>

CYBERHARCÈLEMENT

texte: Michèle Roten

<page=5>

Photo: Revolvermänner GmbH

Riposte sur le web: Christian Scherg de l'agence Revolvermänner lutte contre le harcèlement en ligne

<page=6>

Il vous est sûrement déjà arrivé de faire une plaisanterie douteuse. Mais cela s'est probablement passé en présence de personnes qui vous connaissent et vous apprécient. Elles ont donc fermé les yeux et n'ont pas donné suite.

Vous avez certainement déjà fait quelque chose d'embarrassant. Il en existe sans doute même une preuve: une vidéo où l'on vous voit tituber ivre en pleine chorégraphie du Lac des cygnes, vêtu d'un simple caleçon – que vous portez sur la tête. Heureusement, ce petit film a été enfermé à double tour dans une boîte qui pourrit au fond de votre cave.

Sur le web, point de salut. Impossible de revenir en arrière.

Il vous est peut-être déjà arrivé de commettre une infraction. Mais c'était il y a longtemps et, depuis, vous menez une vie exemplaire. Il n'est pas impossible non plus que quelqu'un vous trouve tellement stupide qu'il a jugé bon de le taguer sur un mur. Oui, mais le graffiti a été recouvert. Bref, le monde réel est indulgent.

Un monde sans pitié

Sur le web, par contre, il n'est point de salut et la fonction «Supprimer» ne sert pas à grand-chose. «Une fois qu'une information a été publiée et qu'elle a attiré l'attention, il est impossible de revenir en arrière», affirme Christian Scherg, directeur de l'agence allemande Revolvermänner (que l'on pourrait traduire par Les Pistoleros), qui gère la réputation en ligne de ses clients. La plupart du temps, il s'agit de grandes entreprises, de partis et d'organisations qui souhaitent maîtriser, du moins dans une certaine mesure, les informations qui circulent à leur sujet sur Internet.

Certains particuliers font également appel aux services de ces justiciers du web. Dès qu'une shitstorm (littéralement une «tempête de merde») menace, ces derniers tentent de limiter les dégâts. «Souvent, la seule solution consiste à participer au débat et à contre-argumenter», déclare Scherg. Or, généralement, seuls les grands groupes en ont les moyens. Pour contrer une attaque, il faut aussi disposer de contacts dans des médias puissants, ce qui n'est généralement pas le cas des particuliers. Scherg et ses hommes doivent donc faire preuve de créativité. Ils essaient par exemple de noyer le post indésirable sous un flot ciblé d'informations contraires. «En dernier recours, il reste la possibilité de changer de nom, d'apparence et d'adresse, et de tout faire pour ne plus être associé à ce qui a été publié», poursuit-il.

Parfois, il ne reste plus d'autre choix que de changer d'identité.

Mise à nu

Personne ne sait si la contre-attaque de la journaliste danoise Emma Holten a été fomentée par une agence similaire à celle de Scherg, mais force est de constater qu'elle a été très efficace. Suite à la publication par un tiers de photos d'elle nue, et voyant que les attaques ne faiblissaient pas, Emma Holten a tout simplement décidé de jouer le jeu. Pourtant, les clichés publiés par ses soins n'avaient rien d'érotique: ils la montraient nue dans des situations du quotidien, par exemple en train de se brosser

5 règles pour éviter le piège du harcèlement

1) Protégez-vous

Sur les réseaux sociaux tels que Facebook, limitez l'accès à vos données, photos et vidéos personnelles. Vérifiez et ajustez régulièrement vos paramètres de confidentialité.

2) Soyez sélectif

N'ajoutez pas n'importe qui à votre liste d'amis. Ignorez les inconnus et bloquez les intrus.

3) Evitez les provocations

Ne vous laissez pas entraîner dans des discussions insultantes sur des pages ou des profils tiers, ne répondez pas aux insultes par des insultes.

4) Parlez-en

Si vous êtes victime de harcèlement, parlez-en à vos proches, vos parents, vos enseignants. Ne restez pas seul devant votre ordinateur pour faire face à la vindicte des harceleurs.

5) Conservez les preuves

Si le mal est fait, gardez votre calme et faites des captures d'écran des insultes et des attaques. Même s'il n'existe aucune loi spécifique contre le harcèlement en ligne, il peut être puni.

<page=7>

les dents. Ce faisant, elle a réussi à reprendre la main, donnant au passage une belle leçon aux adeptes du slut-shaming («humiliation de salopes») sur Internet.

> On peut tenter de noyer l'information sous un flot de faux contenus – jusqu'à ce que les internautes s'en lassent.

«C'est un bon moyen pour désamorcer la situation», confirme Scherg. «Lorsque des données compromettantes circulent, le plus judicieux est souvent de disséminer une multitude de documents pseudo-sensationnels.» On peut par exemple poster des montages photo sur lesquels on est en train d'embrasser Poutine ou de circuler sur le dos d'un éléphant blanc. Au bout d'un moment, le flot de faux clichés est tellement dense que les internautes s'en désintéressent.

<page=8>

Web et vérité

«C'est le problème avec Google», explique Scherg. Nombre d'internautes croient encore que tout ce qui figure sur Internet est vrai et que les résultats de la recherche sont classés en fonction de leur pertinence. Les Revolvermänner cultivent donc leurs relations avec les journalistes d'investigation afin d'éviter de redorer le blason d'une crapule ou d'une entreprise qui trempe réellement dans des affaires louches. «Nous assurons nos arrières: dès que nous remarquons qu'on nous cache une partie de la vérité, nous refusons le mandat.»

Une enquête minutieuse

Les hommes de Scherg se chargent aussi de découvrir qui se cache derrière la campagne de diffamation. «Nous travaillons avec des psychologues et des experts en forensique informatique. Ils établissent des profils, notamment à partir d'analyses linguistiques, et fouillent les moindres recoins des forums et des blogs connus pour être des plates-formes de diffamation.» Mais parfois, l'auteur passe entre les mailles du filet et aucune poursuite n'est possible.

Dans d'autres cas, les internautes ne peuvent s'en prendre qu'à eux-mêmes. En quête de notoriété, ils commettent l'irréparable. Souvenez-vous de Justine Sacco. Juste avant de s'envoler pour l'Afrique du Sud, elle twitte: «En partance pour l'Afrique. J'espère que je n'attraperai pas le sida. Je plaisante, je suis blanche!» Cette boutade de mauvais goût lui coûte cher: onze heures plus tard, lorsqu'elle atterrit, elle est devenue le sujet de conversation n° 1 sur Twitter et a perdu son job.

Plaisanterie douteuse ou hilarante, ironie ou cynisme, racisme ou parodie d'ignorance raciste? On pourrait en discuter pendant des heures. Mais quoi qu'il en soit, ces phrases sont loin d'être les pires jamais écrites sur un réseau social dans la perspective d'éblouir ses contemporains par un trait d'esprit. Justine Sacco n'a tout simplement pas eu de chance.

«Le problème, c'est que son tweet a été diffusé par un journaliste», analyse Martin Steiger, avocat zurichois spécialisé en droit du numérique. «Or l'opinion publique ne s'enflamme généralement que lorsque les médias traditionnels s'emparent d'une affaire. A mon avis, il s'agit ici d'une simple gaffe. Cela peut arriver à n'importe qui.» Il faut savoir que, pour qu'une publication pose légalement problème, tout dépend du contexte, de l'intention et des conséquences négatives. Le premier garde-fou (après le bon sens de l'auteur) est en fait l'éthique du réseau social.

Le moins de censure possible

«Les opérateurs des réseaux sociaux sont confrontés à un dilemme. Même s'ils ne sont pas magistrats, ils peuvent décider de ne pas tolérer ce genre de propos. Dans un même temps, ils préfèrent exercer le moins de censure possible», poursuit Steiger. Mais moins ils interviennent, plus le risque de dérapage est grand. Et soudain, les défenseurs des droits fondamentaux, des droits de l'homme, de la sphère privée, de la liberté d'expression ou de l'autodétermination informationnelle montent au créneau. «Lorsqu'un réseau se contente de s'en remettre à la justice, il perd rapidement en convivialité et devient moins intéressant aux yeux des annonceurs.»

> Les réseaux sociaux ne sont pas des magistrats.

Où est la limite?

Au final, ce sont souvent les internautes eux-mêmes qui font la loi. Les insultes proférées pendant une shitstorm peuvent en effet être d'une violence inouïe. D'ailleurs, a-t-on le droit d'insulter quelqu'un sur le web et de lui souhaiter tous les malheurs du monde? «Non, c'est interdit, il s'agit d'une infraction, d'une atteinte à l'honneur. En droit civil, on parle d'atteinte à la personnalité», déclare Steiger. Mais la victime doit porter plainte. Or les actions en justice sont chronophages et onéreuses, leur issue est incertaine et, en cas de phénomène mondial, leur ampleur en décourage plus d'un. «A cela s'ajoute le fait que l'affaire se poursuit pendant des lustres, alors qu'on aimerait tourner la page», précise Steiger. «Beaucoup de victimes renoncent donc à se battre.» Se défendre a un prix parfois très élevé.

Réfléchir avant de poster

Internet nous permet de faire de l'humour, de dire ses quatre vérités à quelqu'un ou de se moquer de lui. Mais n'oublions pas de réfléchir avant de publier quoi que ce soit.

«Se défendre a un prix», déclare Martin Steiger, avocat spécialisé en droit du numérique.

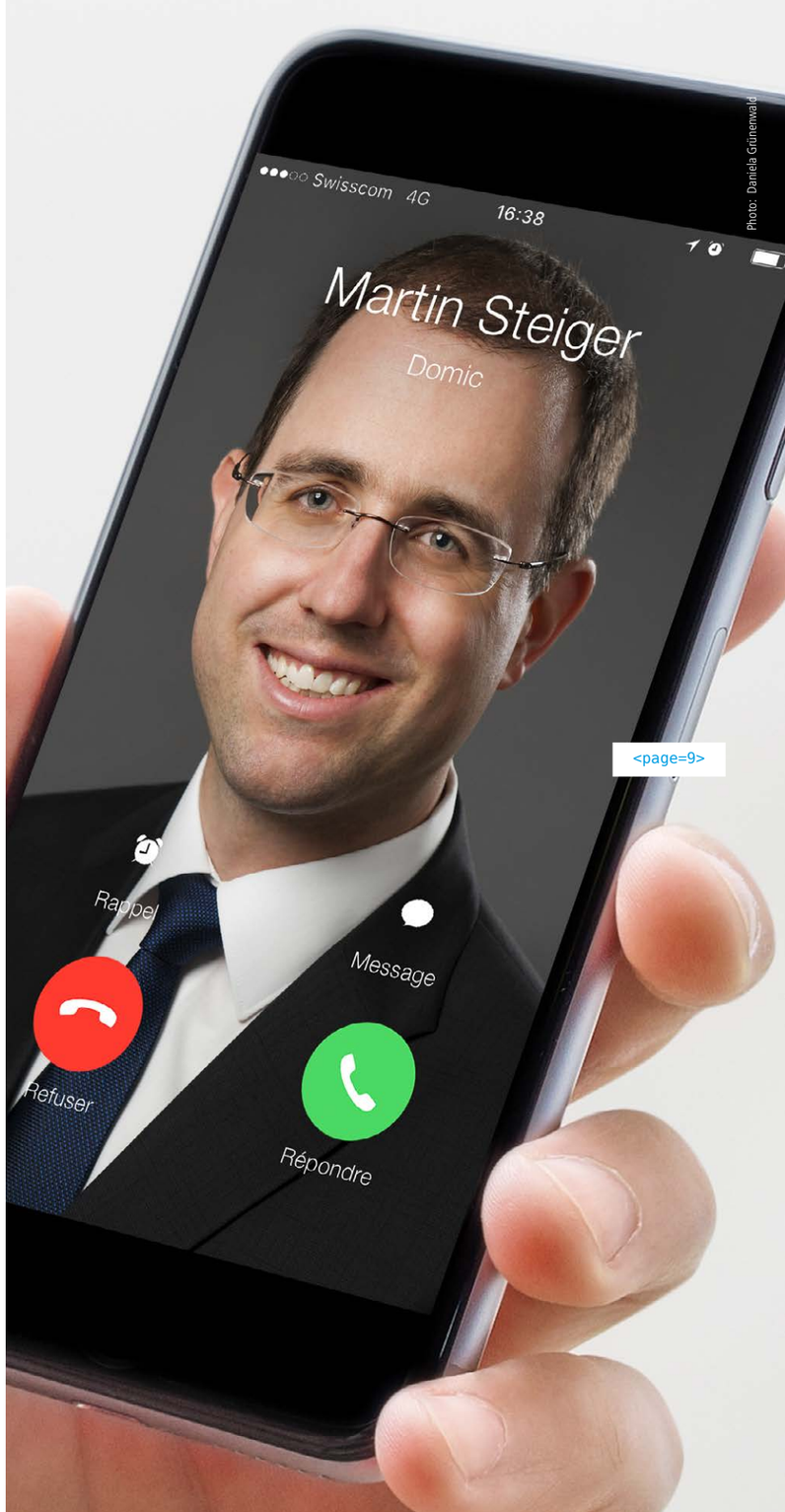


Photo: Daniela Grünenwald

<page=9>

Rien ne manque – mais tout a disparu

Selon Lionel Bloch, la cybercriminalité menace surtout les PME. Il pense qu'elles devraient mieux se protéger et qu'elles pourraient le faire assez facilement – sans se ruiner.

texte: Matthias Mächler photos: Roland Tännler

Nous sommes dans une PME bâloise. Les affaires marchent bien et les machines-outils à commande numérique tournent à plein régime. Les plans qui servent à la production de pièces pour l'industrie automobile et aéronautique sont considérés comme irréprochables, si bien que, ces derniers temps, le directeur de l'entreprise, Peter Portmann*, a été approché à plusieurs reprises pour savoir s'il ne voulait pas les confier à des sous-traitants.

Portmann a refusé, car ces plans constituent le trésor de son entreprise. Il sait que s'ils tombaient entre les mains de fabricants chinois, il serait riche, mais n'aurait plus de travail – une idée qui ne lui plaît pas du tout. Malgré cette convoitise, il n'a pas peur que quelqu'un lui les vole via Internet, puisqu'ils sont stockés sur des machines qui ne sont pas connectées au réseau. Un jour, il décide d'installer une nouvelle génération de machines. Tout se passe comme prévu. Sauf que le lendemain, elles sont déjà en service. Comment est-ce possible? Qui donc a copié les plans sur les nouvelles machines? Et comment? Il conserve en effet les originaux dans un coffre-fort et, sur les anciennes machines, ils sont protégés contre la copie. Mystère.

> «Les PME suisses prennent des risques inconsidérés.»

Aucun code ne lui résiste

Il décide d'appeler l'expert en inforensique Lionel Bloch. Bloch n'a que 28 ans, mais il est déjà un vétéran de sa spécialité. Avant de fonder sa société ForenTec, il a travaillé pour de grandes entreprises et des institutions renommées. Véritable crack de l'informatique, il lit dans les puces comme dans un livre ouvert et peut déterminer les habitudes de n'importe quel utilisateur d'une brosse à dents électrique. Il vient à bout des codes les plus complexes, ce qui lui permet de reconstituer la chronologie des faits en cas de cybercrime. Comme un détective classique, il recueille des indices jusqu'à ce que ceux-ci lui révèlent ce qui s'est passé.

Lorsqu'il reçoit l'appel de Portmann, Bloch est formel: soit il est déjà trop tard, soit ce n'est pas trop grave. Il ouvre une enquête et constate rapidement que quelqu'un a branché une clé USB sur les nouvelles machines. Qui donc? Il soupçonne le fournisseur des nouvelles machines.

Le fournisseur en ligne de mire

Bloch décide de ne pas engager une procédure en vue d'obtenir une perquisition. Il préfère demander au fournisseur un accès illimité à ses systèmes informatiques, ce que ce dernier accepte. «Nous avons vérifié tous les ordinateurs, tous les logiciels, tous les ports USB – en vain», raconte l'expert. Conclusion: soit les plans n'ont pas été copiés, soit les auteurs du cybercrime sont des pros de l'espionnage industriel.

L'espionnage est l'une des préoccupations majeures de Lionel Bloch. «Autrefois, les entreprises étaient attaquées au hasard par des loups solitaires ou de petits groupes de hackers. Mais aujourd'hui, nous avons presque toujours affaire à des bandes organisées qui travaillent à la commande. L'époque des petits génies qui s'amusaient à pénétrer dans un système juste pour le fun est révolue. Lorsqu'elles veulent subtiliser des données, les organisations mafieuses investissent des millions pour former leurs collaborateurs et acheter le matériel nécessaire. Désormais, ce marché pèse plus lourd que celui du trafic de drogue. Et, en raison de leur excellence, les firmes suisses sont très exposées. Dans les pays de production à bas coût, les logiciels et les plans de qualité sont ce qui intéresse le plus les dirigeants malhonnêtes», affirme le spécialiste.

Selon Bloch, les grandes sociétés comme l'UBS consacrent des sommes importantes à la sécurité des données et elles sont bien protégées. Par contre, il estime que la plupart des PME suisses prennent des risques inconsidérés: «Il y a quelque temps, nous avons travaillé pour une entreprise dont le système était victime d'un cheval de Troie depuis six ans. Tous les mois, ce logiciel malveillant détournait des données et personne n'avait rien remarqué.»

Quelques connaissances suffisent

C'est l'aspect le plus perfide de la nouvelle criminalité: on ne voit rien, on n'entend rien, rien ne manque – et tout a disparu. Bloch explique qu'il ne suffit pas de se déconnecter pour être à l'abri, car si les malfrats pénètrent dans les locaux, ils peuvent tout voler, même si leurs connaissances en informatique sont rudimentaires.

> «Ce marché pèse plus lourd que celui du trafic de drogue.»

Mais revenons-en à notre entreprise bâloise. Bloch poursuit son enquête et parvient à identifier le responsable. Il s'agit en fait du technicien qui a installé les nouvelles machines. Il n'a eu aucun mal à contourner la protection informatique et à copier les plans sur les nouvelles machines via une clé USB. Il l'a fait de son propre chef, pour rendre service. Bloch récupère la clé USB, il examine l'ordinateur personnel du technicien et lui demande de signer une déclaration dans laquelle celui-ci certifie n'avoir pas transféré les données ailleurs. «Ce n'est pas une

Lit dans les puces comme dans un livre ouvert: l'expert en inforensique Lionel Bloch.

garantie absolue. Mais comme ça, nous saurons à qui nous adresser si les plans refont surface ailleurs», précise Bloch.

Retrouver le sommeil

«Je ne dis pas ça pour vendre mes prestations», dit Bloch, «mais parce

> «Cryptez au moins vos données!»

que je le pense vraiment: chères PME suisses, cryptez au moins vos données! Et réagissez vite en cas de doute! Il serait stupide d'attendre que l'irréparable se produise.» Suite à cet incident, notre entreprise bâloise a demandé à ForenTec de repenser son infrastructure informatique, d'installer des capteurs dans ses locaux et de former ses collaborateurs. Désormais, elle bénéficie également d'un service d'intervention en cas d'urgence. Le tout pour un prix raisonnable si l'on tient compte des sommes en jeu: pour retrouver le sommeil, Peter Portmann n'a au final dépensé que 20000 francs.

* Le nom a été modifié par la rédaction

Les 10 commandements de Bloch

1) Soyez vigilants!
Dès que vous avez le moindre doute, appelez immédiatement un spécialiste.

2) Cryptez vos données!
Les logiciels de cryptage brouillent vos données, ce qui décourage la plupart des malfrats.

3) Méfiez-vous de vos ex-employés!
Dès qu'un collaborateur quitte l'entreprise, faites en sorte qu'il ne puisse plus accéder aux données.

4) Protégez vos appareils mobiles!
Si vous conservez des données sensibles sur des appareils mobiles, protégez-les: les smartphones et les tablettes sont très faciles à pirater.

5) Surveillez vos collaborateurs!
Rédigez un cahier des charges pour vos informaticiens et des directives strictes pour tous vos collaborateurs.

6) Sécurisez vos données!
On ne le dira jamais assez: sans sauvegardes régulières, pas de sécurité!

7) Protégez votre système!
Installez des antivirus et des pare-feux actuels.

8) Utilisez des mots de passe efficaces!
Le piratage des mots de passe est l'un des moyens les plus simples pour voler des données confidentielles. Découragez les voleurs!

9) Limitez l'accès à vos locaux!
Les pare-feux ne servent à rien si les aigrefins peuvent pénétrer dans vos locaux. Il faut donc les protéger à l'aide de systèmes efficaces. Vos clients et vos fournisseurs vous en seront reconnaissants.

10) Rangez vos dossiers!
S'ils sont bien rangés, les dossiers et les documents se perdent moins facilement. Ceci est également valable pour les ordinateurs!

Mettez vos données à l'abri

Google sait tout: ce que vous recherchez, quelles applications vous utilisez, quelle musique vous écoutez, où vous habitez, travaillez et faites vos courses. Voici comment stopper cette chasse aux données en quelques clics.

texte: Andreas Hirstein © NZZ am Sonntag

<page=14>

Google contrôle le plus grand moteur de recherche du web ainsi que le système d'exploitation pour smartphones le plus utilisé (Android) et domine le marché des navigateurs Internet (Chrome). Via tous ces canaux, le groupe recueille des données personnelles à partir des recherches effectuées et des applications utilisées. Récemment, les règles de confidentialité du navigateur Chrome ont été modifiées. Désormais, si l'internaute est connecté avec un compte Google et s'il donne son accord (opt-in), Google a le droit d'analyser tout son historique – et non plus uniquement ses recherches – pour afficher de la «publicité répondant à ses centres d'intérêt», en tenant également compte de son sexe et de son âge.

La plupart des clients ne se servent pas des options permettant de contrôler l'usage que Google fait de leurs données, car ils ignorent que la quasi-totalité des données enregistrées peuvent être consultées et supprimées, une par une ou sur une période donnée. A condition d'être connecté avec un compte Google, ce qui est obligatoire pour tout utilisateur d'Android, il est aussi possible de choisir quelles données la firme collectera à l'avenir. Les sites Google sont conçus de manière claire. Mais le nombre des modifications possibles peut en rebuter plus d'un. Pour modifier les principaux réglages sur un portable Android, on peut utiliser les «Paramètres Google» ou passer par Chrome.

1 Annonces personnalisées

Ouvrez Chrome et connectez-vous à Google. Cliquez sur votre photo de profil en haut à droite, puis sur «Mon compte». Sélectionnez «Paramètres des annonces», puis «Gérer les paramètres des annonces». Vous pouvez alors choisir d'autoriser ou non Google à utiliser l'historique de votre navigation pour vous proposer des annonces ciblées. Revenez au menu, sélectionnez «Applications et sites connectés». Vous y trouverez la liste des applis et des services web que vous avez autorisés à accéder à votre compte Google. Si vous n'utilisez plus telle ou telle application, cliquez sur «Supprimer».

2 Accès à votre compte

Ouvrez à nouveau le menu principal «Mon compte», puis cliquez sur «Activité sur les appareils et notifications». Ici, vous pouvez voir quel appareil a accédé à votre compte Google, quand et où. Si quelque chose vous paraît suspect, modifiez votre mot de passe. Sachez par ailleurs que les smartphones perdus ou volés sont localisables sur une carte Google Maps. Les smartphones Android enregistrés sur Google peuvent même être verrouillés ou réinitialisés à distance.

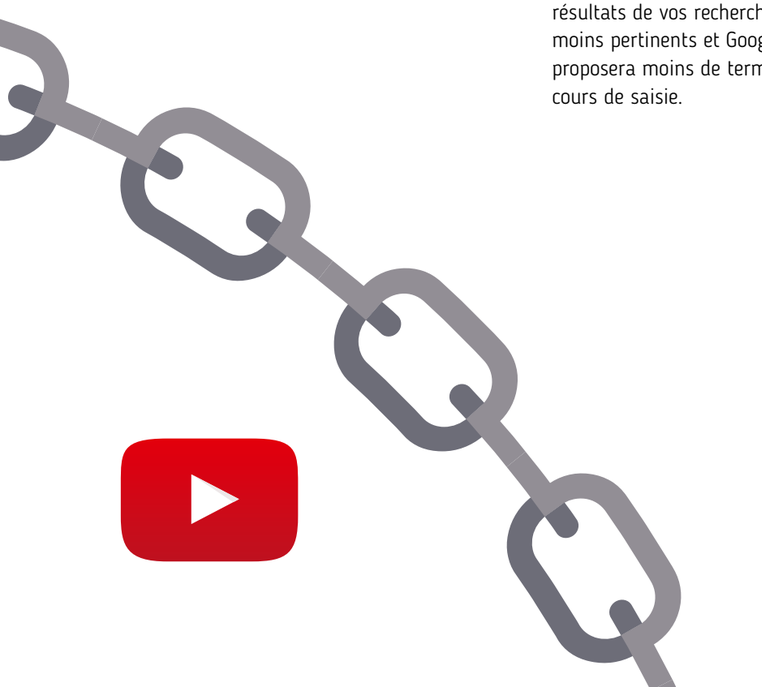
3 Données collectées

Google enregistre bien plus de données que vous ne le croyez. Le moteur de recherche mémorise les pages que vous avez consultées, mais aussi depuis où et à quel moment. Si vous utilisez un portable Android, Google note, pour chaque application, quand vous l'avez ouverte. A chaque recherche effectuée par reconnaissance vocale, Google archive le fichier audio et le texte retranscrit. Des années plus tard, vous pouvez donc écouter ce que vous avez bafouillé un jour dans le micro de votre smartphone. Tout cela a pour objectif de personnaliser les services Google et, bien sûr, de cibler les annonces. Pour consulter la liste des données enregistrées, revenez au menu principal. Cliquez sur «Gérer votre activité Google», puis sur «Accéder à mon activité». Vous découvrez alors la liste de toutes les activités recensées, à la minute près, depuis l'ouverture de votre compte Google – et donc parfois sur plusieurs années. Cette liste peut être filtrée par date et par service Google (vous retrouvez par exemple la musique écoutée sur Google Play). Il vous suffit de cliquer sur chaque activité pour obtenir tous les détails et la supprimer en un clic. Les activités peuvent aussi être effacées sur une période donnée.

<page=15>

4 Règles applicables

Après avoir choisi, en fonction de vos souhaits et de votre seuil de tolérance, quelles données vous acceptez de laisser sur les serveurs Google, définissez les paramètres concernant le futur archivage de vos données. Google opère une distinction entre différents types de données (recherches, localisation, fichiers audio des activités vocales, données Youtube, etc.), soumises à des règles différentes. Elles sont abordées séparément aux points suivants. Pour commencer, revenez à «Gérer votre activité Google», puis cliquez sur «Accéder aux commandes relatives à l'activité».

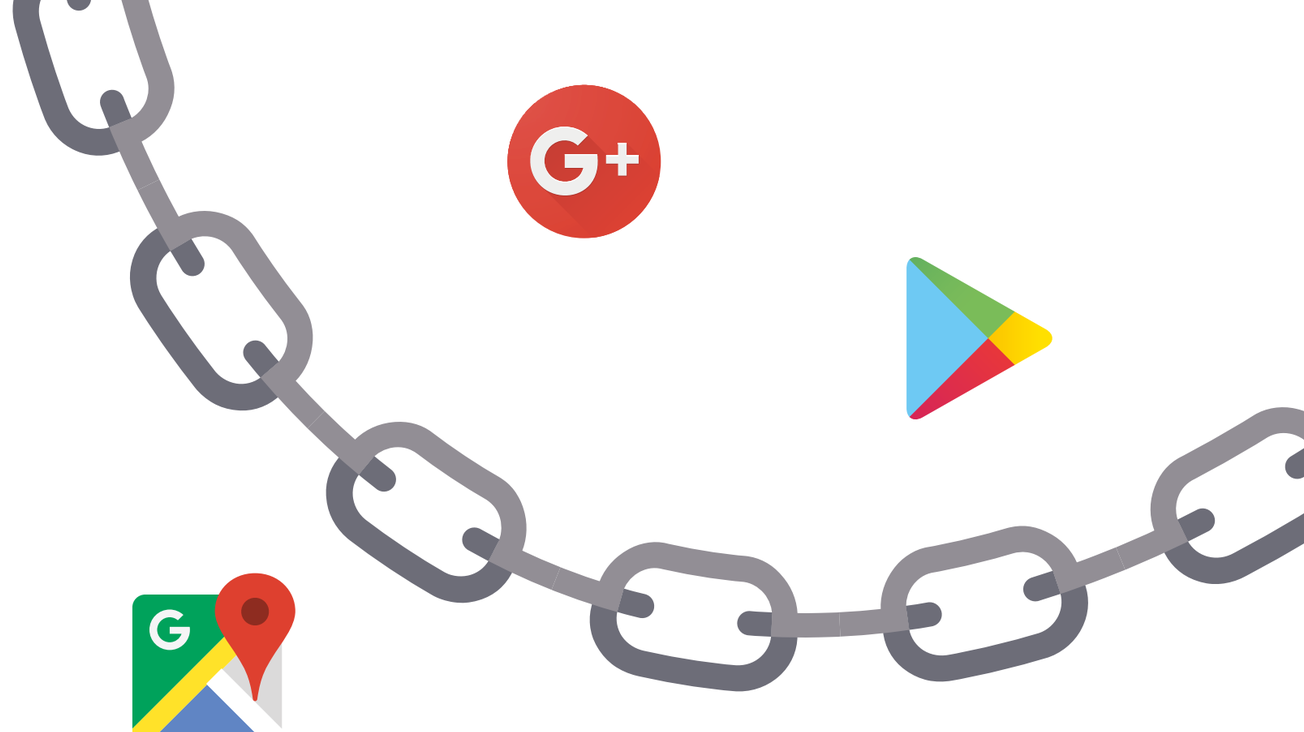


5 Activités

Commençons par vos activités sur le web et dans les applications, qui concernent les recherches effectuées sur Google et les données de Google Now, un service proposant des informations personnalisées sur smartphone (trafic routier, vols retardés, etc.). Pour autoriser Google à collecter des données, activez «Activité sur le web et dans les applications». Google archivera alors les mots-clés de vos recherches et les adresses IP utilisées, et saura si vous êtes passé par un navigateur ou par une application. Vous pouvez également autoriser Google à exploiter tout l'historique de votre navigateur. Si vous souhaitez vous y opposer, vous pouvez interrompre l'enregistrement des données. Dès lors, vous ne bénéficierez plus des services Google Now, les résultats de vos recherches seront moins pertinents et Google vous proposera moins de termes en cours de saisie.

6 Localisation

Viennent ensuite les données de localisation. Si vous les désactivez, les serveurs Google ne mémoriseront plus où vous vous êtes rendu avec vos appareils enregistrés, l'historique de vos déplacements ne pourra plus être consulté dans Google Maps sur votre smartphone et vous devrez ressaisir à chaque fois toutes les adresses au lieu de les sélectionner dans une liste. Attention: même si vous désactivez cet historique, certaines informations continueront d'être archivées dans le cadre de l'«Activité sur le web et dans les applications», notamment quand vous utiliserez Google Maps ou que vous effectuerez une recherche. Pour qu'aucune donnée ne soit conservée, les deux options (points 5 et 6) doivent être désactivées. Important: ces paramètres n'ont aucune influence sur les services de localisation que l'on peut activer et désactiver sur un smartphone. Si l'on interrompt l'historique de localisation, seul l'enregistrement des données s'arrête. Les applications de navigation et Google Maps continuent de fonctionner. L'historique de localisation peut également être modifié et supprimé. Pour ce faire, cliquez sur «Gérer l'historique». La carte du monde s'affiche. Tous les endroits où vous vous êtes rendu sont indiqués par des points rouges, à condition d'y être allé avec un portable ou une tablette enregistrés sur Google. Cliquez sur la poubelle, en bas à droite, pour supprimer tout l'historique. Vous pouvez aussi effacer certaines journées en sélectionnant des dates précises en haut à gauche.



7 Appareils

Sous «Informations provenant des appareils», Google enregistre votre répertoire, vos rendez-vous, vos applications, votre musique et les caractéristiques techniques de votre portable afin d'optimiser vos recherches sur le web. Déplacez le curseur pour interrompre l'enregistrement de ces données. Celles qui sont déjà archivées peuvent être supprimées en choisissant «Gérer l'historique», puis «Options de suppression» dans le menu en haut à droite.

8 Activités vocales

Google enregistre aussi les fichiers audio de vos recherches vocales. Pour stopper l'archivage, il vous suffit de cliquer sur le bouton correspondant. La reconnaissance vocale sera toutefois moins performante, car les algorithmes auront moins d'exemples pour optimiser leurs fonctions. Pour supprimer les données déjà enregistrées, cliquez sur «Gérer l'historique», puis, en haut à droite, sur «Supprimer des activités par». Vous pouvez définir les périodes concernées.

9 Conséquences

Tous les réglages effectués sur «Mon compte» s'appliquent à tous les services Google, sur tous vos appareils: ordinateur, portable Android ou (dans une moindre mesure) iPhone si ce dernier est enregistré sur Google. Si vous choisissez de stopper l'archivage, les données ne seront plus enregistrées sur les serveurs Google, mais localement, dans les applications. Certains services ne fonctionneront plus ou perdront en précision et en confort d'utilisation.

Bruits de bottes

La guerre est devenue silencieuse. L'espionnage et le terrorisme se sont déplacés dans le cyberespace. Poudre aux yeux ou danger réel? Un entretien avec Myriam Dunn Cavelty, qui enseigne les politiques de sécurité à l'EPFZ.

interview: Matthias Mächler photos: Samuel Wimmer

NORSE: toutes les cyberattaques en temps réel
http://map.norsecorp.com

Vous avez étudié les relations internationales, l'histoire et le droit international. Pourquoi n'êtes-vous pas devenue espionne?

«Le marché noir des données est en plein boom.»

(Rires) On ne me l'a jamais proposé! Mais c'est surtout que ma spécialité me passionne vraiment. Dans le monde de la recherche, nous sommes peu nombreux à mettre en relation la politique et un aspect technologique comme le cyberespace. Contrairement à nombre de mes collègues, je jouis donc d'une très grande liberté.

Au lieu d'espionner, vous étudiez l'espionnage?
Oui, mais pas uniquement. En ce moment, je m'intéresse à l'impact des séries télévisées sur les risques cybernétiques. Des productions comme «24 heures chrono», «Homeland» ou même «Die Hard» décrivent des actes terroristes qui n'ont jamais eu lieu dans la réalité. Ce faisant, elles modifient la perception de la société et des politiques qui, par peur, dépensent mal l'argent de l'Etat.

La cyberguerre est planétaire. La Suisse est-elle menacée?
Cela dépend de quoi nous parlons. La Suisse n'est évidemment pas à l'abri de la cybercriminalité et, surtout, du cyberespionnage. Le marché noir des données est en plein boom.

La sécurité de nos données doit-elle nous préoccuper?
Le risque zéro n'existe pas. Cela dit, en Suisse, la plupart des acteurs concernés sont conscients de la situation. Le secteur financier dépense par exemple beaucoup d'argent pour protéger ses données et donc les nôtres. Mais les PME posent problème. Alors qu'elles jouent un rôle majeur en termes d'innovation et de croissance, elles sont souvent mal protégées. Elles manquent de moyens et de personnel.

Et qu'en est-il du cyberterrorisme?
Une cyberattaque contre une infrastructure sensible comme une centrale nucléaire est très peu probable. Pour créer un logiciel qui en soit capable, il faut des services secrets efficaces, beaucoup d'argent et des agents infiltrés qui puissent le tester. Bref, pour des terroristes, le jeu n'en vaut pas la chandelle. Surtout que l'effet n'est pas garanti. Pour terroriser la population, il vaut mieux faire exploser une voiture piégée sur une place très fréquentée.

Mais les terroristes se servent bien du cyberespace, non?
Oui, bien sûr. Les terroristes se servent d'Internet pour recruter, faire de la propagande et se financer. Il y a de plus en plus de liens entre le crime organisé et les groupes terroristes. C'est un aspect très important. Les terroristes gagnent notamment de l'argent en vendant des médicaments.

D'où vient le plus grand danger?
Comme toujours quand les services secrets sont impliqués, on ne peut le dire avec certitude. Mais le comportement des Etats est révélateur: depuis cinq ou six ans, ils font de plus en plus d'efforts diplomatiques pour tenter de contrôler les risques cybernétiques en collaborant à l'échelle internationale. Malheureusement, ils dépensent aussi beaucoup d'argent pour augmenter leurs capacités dans le domaine de la cyberoffensive. Et on observe une grande fébrilité, ce qui n'est jamais bon pour la stabilité internationale. Au moindre pépin, les conséquences pourraient être graves. Le risque d'escalade est assez élevé.

Ne faut-il pas s'étonner qu'il y ait eu si peu de problèmes à ce jour?
Récemment encore, on pensait que le cyberespace allait donner plus de moyens à de petits Etats comme la Corée du Nord. Mais aujourd'hui, c'est l'opinion inverse qui prédomine: les experts sont d'avis que seules les grandes puissances sont en mesure d'organiser des cyberattaques d'envergure. Or, elles n'ont pas intérêt à alimenter l'escalade.

Il ne faut donc pas s'inquiéter outre mesure?
Si les Etats parviennent à signer des accords et à les respecter, la situation ne devrait pas devenir trop inquiétante.

«Seules les grandes puissances peuvent organiser des cyberattaques d'envergure.»

Et dans le cas contraire?
Le nombre d'Etats qui jouent un rôle dans cet espace invisible ne cesse de croître, ce qui augmente le risque de déstabilisation. L'issue dépendra donc des relations internationales.

Peut-on donc dire qu'il y a de plus en plus de bruits de bottes, mais pas de véritables cyberattaques? Aurait-on affaire à une théorie du complot?
Les éléments évoquant une théorie du complot sont nombreux, mais il y a aussi des réalités. Il est très difficile d'obtenir des informations fiables sur les capacités réelles des Etats. Nous ne savons pas ce que les USA, la Chine, la Russie ou Israël veulent et peuvent faire. Les révélations d'Edward Snowden ne sont que la pointe de l'iceberg. Tout se passe dans l'ombre.

La cyberguerre est un immense marché. Nombre de sociétés gagnent beaucoup d'argent grâce à la peur qu'elle inspire.
Oui, c'est vrai, et cela pose des problèmes aux chercheurs. Nous devons travailler avec des données aussi fiables que possible. Mais, dans ce domaine, la neutralité n'existe pas. Toutes les données proviennent de firmes qui produisent des antivirus ou d'institutions semi-étatiques qui ont intérêt à ce que la peur persiste. Les conditions sont donc loin d'être optimales.

Qu'est-ce qui vous inquiète le plus?
Les situations qui pourraient dégénérer en raison de la bêtise de quelques acteurs isolés et tout ce qui pourrait réveiller des forces dormantes – surtout en ce moment avec la montée des nationalismes. Un jour, cela pourrait avoir de lourdes conséquences. L'instabilité est le principal danger qui nous guette.

> «Nous ne savons pas ce que les USA, la Chine, la Russie ou Israël veulent et peuvent faire. Tout se passe dans l'ombre.»

A quoi ressemblera le cybermonde dans quelques années?
Il me semble que nous nous dirigeons vers une stabilisation, car les grandes puissances n'ont pas intérêt à ce que l'instabilité augmente. Le cyberespace – qui sera peut-être bientôt constitué de différents réseaux avec différents niveaux de sécurité – est une réalité. Il sera utilisé, en bien et en mal, mais il va se normaliser, l'hystérie va diminuer. C'est comme avec le terrorisme: plus il y a d'actes terroristes, plus ils deviennent banals et moins ils sont efficaces pour les terroristes.

Vous ne nous avez toujours pas dit si vous rêviez de devenir une espionne…
Oh non! C'est un job très ennuyeux. De nos jours, la plupart des agents secrets sont assis devant un ordinateur et doivent analyser les données qu'on leur envoie alors qu'ils ne savent même pas de quoi il retourne. Ils rédigent ensuite un petit rapport qui finit généralement dans un tiroir. Sans compter qu'en Suisse, il n'y a pas beaucoup d'espions. Personnellement, je n'en connais pas un seul!

A surtout peur de la bêtise: la spécialiste du cyberespace Myriam Dunn Cavelty sur son lieu de travail à l'EPFZ.

Cyberwoman

Née en 1976, Myriam Dunn Cavelty enseigne les politiques de sécurité à l'EPFZ depuis 2008. Depuis 2014, elle est vice-directrice pour la recherche et l'enseignement du Center for Security Studies (CSS) de cette même école. Ses travaux portent sur la cybersécurité, la cyberguerre et la protection des infrastructures sensibles. Pour le reste, elle rédige un blog consacré aux séries télévisées coréennes et chinoises (6,5 millions de visiteurs à ce jour), elle écoute du heavy metal, elle a une fille et deux chats, et elle est mariée à l'auteur Gion Mathias Cavelty.

_

Link encap: Ethernet HWaddr 08:00:27:40:04

Dans la zone grise

Marc Rubin se promène souvent sur les réseaux et pense que le hacking fait l'objet de nombreux malentendus. Rencontre avec un grey hat.

texte: Florian Leu photos: Roberto Ceccarelli

Enfant, il pénétrait chez les autres. Mais de manière virtuelle, armé de son seul ordinateur. Il lui arrivait d'envoyer des e-mails signés George W. Bush à ses copains. Ou d'entrer par effraction dans le système informatique d'une entreprise pour voir comment il était fait. Bref, il se promenait dans le cybermonde et faisait du tourisme sans sortir de chez lui. Chaque voyage était une aventure, même lorsqu'il se retrouvait nez à nez avec le business plan d'un fabricant

> Un hacker bienveillant.

de bétonnières. Bref, il était un cambrioleur qui ne volait rien. Membre du Chaos Computer Club (CCC) et fondateur du Parti Pirate zurichois, Marc Rubin a aujourd'hui 25 ans et il se considère comme un grey hat, un hacker qui agit généralement dans la légalité.

Pour la bonne cause

Généralement, mais pas toujours. Il pourrait par exemple tout à fait imaginer imiter ses collègues du CCC Allemagne et pirater des ordinateurs électoraux. Pas pour faire gagner tel ou tel candidat, mais pour attirer l'attention du public sur les risques de la démocratie numérique. D'ailleurs, avec ses amis de la section suisse du CCC, il l'a déjà fait – à l'invitation de la Haute école spécialisée bernoise. Ce faisant, il a découvert quelques petites failles dans le système de sécurité. Et, en bon hacker bienveillant, il les a révélées aux responsables.

Un écran dans la nuit

Rubin a fait un apprentissage d'informaticien spécialisé dans la technique des systèmes. Puis il a commencé des études d'informatique de gestion. Mais il n'a pas encore son diplôme, car il n'a pas l'intention de pirater le mémoire d'un autre, si bien qu'il doit encore le rédiger. Ces trois dernières années, il a travaillé en tant qu'ingénieur en sécurité informatique pour des banques et des entreprises de télécommunication. Il est d'ailleurs assez fier d'avoir conçu le script du site de Cablecom. Lors de ses missions, il lui arrive souvent de passer la nuit devant son écran,

> Rubin n'a pas encore son diplôme en informatique de gestion, car il n'a pas l'intention de pirater la mémoire d'un autre.

comme quand, enfant, il piratait des jeux, ce qui lui permettait de progresser plus rapidement.

A seulement dix ans, tel un dieu du virtuel, il s'amusait aussi à colorier en rose le ciel d'un jeu d'action ou à équiper son avatar d'un porte-monnaie inépuisable. Adolescent, il a ensuite commencé à s'introduire dans les réseaux des entreprises. Cela ressemblait à un jeu, mais cette fois-ci les sociétés étaient bien réelles – et elles le payaient.

Lorsqu'il parle à des gens qui ne connaissent pas le monde des hackers, Rubin est souvent obligé d'invoquer l'histoire. Car les pratiques des pirates ne datent pas d'hier. Il y a 60 ans, les premiers hackers étaient des étudiants et collaborateurs du Massachusetts Institute of Technology de Cambridge. Mais ils ne se servaient pas d'ordinateurs. Sur le campus de leur école, ils avaient construit un circuit de train miniature et parlaient de «hack» lorsqu'ils parvenaient à améliorer les performances du système. Avant eux, dès le 19e siècle, il y avait déjà eu les premiers phreaks, des employés des PTT qui utilisaient leurs connaissances pour téléphoner gratuitement. Ce faisant, ils enfreignaient la loi, mais juste pour pouvoir se parler sans payer.

Trucs et astuces

«Un hack est neutre. Le but du jeu est de trouver des trucs et des astuces pour améliorer un système existant et en faire profiter les autres», explique Rubin, affalé dans un fauteuil. Nous sommes dans les locaux du CCC, le lieu de

> Il y a 60 ans, les hackers jouaient au petit train. Lorsqu'ils parvenaient à améliorer le circuit, ils parlaient de «hack».

Dans les locaux du Chaos Computer Club: derrière Marc Rubin, un ancien serveur de l'EPFZ qui sert désormais de chauffage.

Un groupe qui porte bien son nom: le Chaos Computer Club.

rendez-vous des hacktivistes zurichois. Derrière Rubin, on aperçoit une pièce de musée: un ancien serveur de l'EPFZ. Les membres du CCC ne l'utilisent pratiquement plus, car il consomme trop d'énergie. Mais il est pratique en tant que chauffage. Entre deux phrases, notre grey hat s'accorde une gorgée de maté, la boisson fétiche du groupe, sa haute teneur en caféine permettant de rester éveillé toute la nuit si le hack l'exige.

L'image que le grand public a du hacker semble tout droit tirée du film «Matrix»: le pirate informatique est un geek blafard vêtu de noir qui passe ses nuits devant des écrans pour s'approprier ce qui ne lui appartient pas. Si on se fie aux apparences, Rubin est parfait pour le rôle. Il est pâle, maigre, habillé en noir et semble un peu perdu. Mais il ne veut pas être assimilé à ce cliché. Car il n'a pas l'intention de voler des données bancaires, d'escroquer les plus démunis ou de piller les comptes d'inconnus vivant à l'autre bout du monde. «Ceux qui font ça sont de simples criminels», dit-il.

> Ceux qui pillent les comptes d'inconnus vivant à l'autre bout du monde sont de simples criminels.

Il pense que le risque de se faire subtiliser les données de sa carte bancaire sur Internet est très faible. Si l'on est vigilant et que l'on effectue ses achats sur de gros sites, il est inutile de se faire trop de souci: «On a une chance sur cent d'avoir un problème, voire moins.»

Les petits sont plus faibles

Lorsque l'on passe une commande sur les sites des petits fournisseurs, c'est une autre paire de manches. Car ils sont beaucoup plus faciles à hacker. Par jour, on estime qu'environ 2000 cartes de crédit se font pirater – ce qui, proportionnellement, est relativement peu – et la plupart d'entre elles le sont via de petits sites mal protégés. «La probabilité de se faire voler son portefeuille est par ailleurs plus grande que celle de se retrouver assis à côté de quelqu'un qui a un appareil permettant de lire à distance la bande magnétique de notre carte de crédit, ou de tomber sur un distributeur automatique doté par des pirates d'un faux lecteur de carte et d'une caméra pour filmer le code», souligne Rubin.

> Notre cerveau est le seul disque dur sûr.

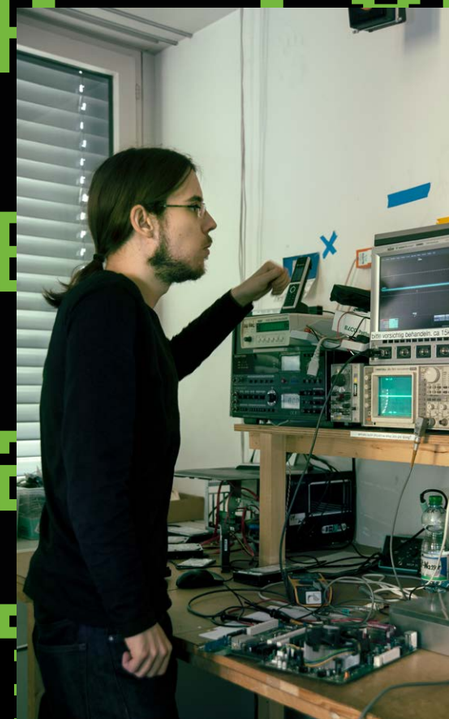
Rubin est davantage préoccupé par la protection des données. Il avoue qu'il ne stockerait jamais une idée commerciale sur un ordinateur. «Notre cerveau est le seul disque dur sûr. Sans compter que le logiciel de filtrage est au point: on oublie facilement les mauvaises idées.» Il est aussi d'avis que la peur qu'inspirent les hackers est exagérée et qu'elle sert même de manœuvre de diversion. Lorsque les pouvoirs publics développent des chevaux de Troie surpuissants afin que la police puisse procéder à des perquisitions virtuelles sans mandat, le hack est d'une toute autre ampleur. Ces logiciels malveillants peuvent en effet activer les micros et les caméras des ordinateurs de l'ensemble de la population: «Aujourd'hui, les gouvernements essayent de surveiller notre vie privée. C'est une évolution très regrettable.»

World Wild West

Rubin a la nostalgie de l'époque où le web était une sorte de Wild West mondial: «Désormais, nous sommes entrés dans l'ère industrielle, l'insouciance a disparu.»

Avec le temps, il est devenu un fervent défenseur de lanceurs d'alerte comme Edward Snowden et reconnaît qu'il a des sympathies pour les Anonymous, même s'il ne sait pas très bien qui ils sont: «Ce mouvement est aussi difficile à cerner que celui des hippies en leur temps. Mais j'approuve les valeurs qu'ils défendent, à savoir la liberté, la protection de la sphère privée et la lutte contre la censure.» Voilà belle lurette qu'il ne s'infiltre plus chez les gens pour s'amuser. Aujourd'hui, c'est l'inverse. Il craint que la police ne pirate son disque dur, car il trouve que de telles pratiques mettent en danger la présomption d'innocence: «De nos jours, il faut sans cesse prouver son innocence.» Il n'est par contre pas très inquiet pour ses données. Il sait en effet que les policiers ne trouveraient pas grand-chose à se mettre sous la dent, si ce n'est le vieux business plan d'un fabricant de bétonnières.

> Les Anonymous sont aussi difficiles à cerner que les hippies.



Se méfie désormais de ses semblables: le pirate Marc Rubin.

Une main de fer dans un gant de velours: Carole Aubert traque tous ceux qui vendent de fausses montres sur Internet.

Le vrai et le faux

Le nombre des fausses montres suisses produites dans le monde dépasse celui des vraies et ces contrefaçons sont principalement vendues sur Internet. A Bienne, une petite équipe de la Fédération de l'industrie horlogère combat ce fléau.

texte: Barbara Meier photos: Roberto Ceccarelli

«Voilà», dit Carole Aubert, «nous allons les coincer.» L'espace d'un instant, le regard de l'élégante avocate évoque celui de Diane chasseresse. Son bureau est situé à Bienne, dans le bâtiment Art déco qui abrite le siège de la Fédération de l'industrie horlogère suisse. Membre de la petite équipe chargée de lutter contre la contrefaçon, elle en dirige l'Internet Unit, créée en 2004. De nos jours, les fausses montres ne sont en effet plus vendues que sur les marchés des grandes villes ou sur les plages, mais aussi et surtout sur le web.

Une page du site AliExpress, qui appartient au groupe chinois de vente en ligne Alibaba, s'affiche sur l'écran de Carole Aubert. On y voit des montres qui ressemblent comme deux gouttes d'eau à des modèles classiques d'Omega, Cartier ou Hublot. Pourtant, le logo de la marque a disparu. «Regardez bien les aiguilles», nous dit l'experte. Et de fait: sur toutes les montres, il est midi moins cinq ou midi cinq, si bien qu'elles cachent le nom de la marque, les lettres restantes ayant été effacées à l'aide de Photoshop.

«Ce commerçant a recours à deux astuces», souligne Carole Aubert. D'une part, il n'emploie aucun mot-clé référencé par le moteur de recherche utilisé par les spécialistes, comme «réplique» ou «imitation». D'autre part, il ne mentionne aucune marque déposée. Il est certes interdit de copier le design d'une montre, mais les responsables de plateformes comme AliExpress n'acceptent de bloquer un commerçant que si celui-ci a imité un logo.

> Depuis peu, les faussaires ont infiltré des réseaux sociaux comme Facebook ou Instagram.

Vrai logo, fausse montre
Aucun client n'accepterait d'acheter une montre ressemblant à une Omega, mais sans logo. Du coup, le commerçant a ajouté dans un anglais approximatif la mention «All watches come with correct known logo». «C'est là qu'il se trahit», explique l'avocate. Sans plus attendre, elle contacte AliExpress. Peu de temps après, l'offre a disparu.

L'Hydre de Lerne
Les résultats obtenus par Carole Aubert et ses collègues sont impressionnants: en 2015, ils ont réussi à faire disparaître plus de 600 000 annonces proposant de fausses montres. Mais ces détectives du Net se battent contre un monstre qui évoque l'Hydre de Lerne: lorsqu'ils tranchent l'une de ses multiples têtes, deux autres repoussent ailleurs. Depuis peu, les faussaires ont par exemple infiltré des réseaux sociaux comme Facebook ou Instagram. Or, sur ces plateformes, ce sont des algorithmes qui décident qui reçoit quelle publicité, si bien que les logiciels de recherche ne les trouvent pas. Afin de combattre les escrocs avec leurs propres armes, Carole Aubert a créé une ribambelle de faux profils Facebook et Instagram – en vain: «J'ai beau liker toutes les marques de montres et tous les statuts qui les concernent, je n'ai encore jamais reçu de pub pour une montre. C'est étrange.»

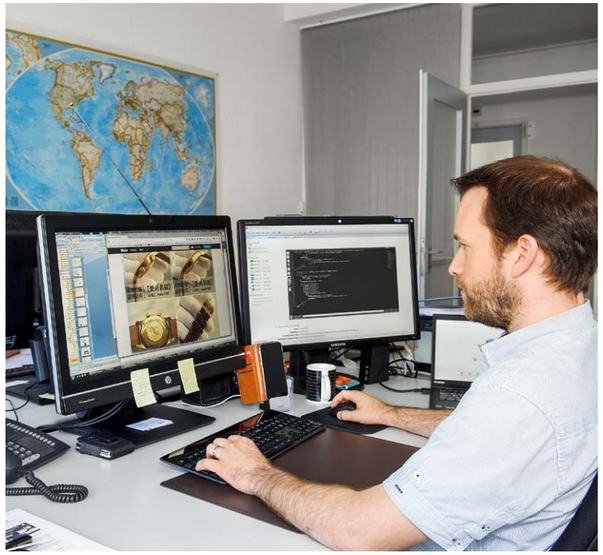
Heureusement, elle a aussi des informateurs. Sur son smartphone, elle nous montre une photo qu'elle a reçue. Il s'agit d'une publicité qui vante les mérites d'une Rolex proposée avec un «super rabais»: 119 francs au lieu de 1117. Cependant, le lien sur lequel il faut cliquer dirige l'utilisateur sur une page anonymisée. Mais Carole Aubert a plus d'un tour dans son sac. Elle a remarqué que les colis utilisés pour l'expédition de ces montres se ressemblent tous et qu'ils proviennent généralement de Rotterdam. Elle a donc informé les douaniers et, ces dernières semaines, ils ont ainsi pu intercepter des centaines de fausses Rolex.

Des clients d'un nouveau genre
Les réseaux sociaux ne sont pas uniquement une cachette idéale pour les criminels. «Ils leur permettent aussi de s'adresser à des clients d'un nouveau genre», dit Carole Aubert. Alors qu'autrefois, les acheteurs d'une «Hublot Replica» ou d'une Omega sans logo savaient qu'ils achetaient une contrefaçon, les usagers des réseaux sociaux sont persuadés d'acquérir une vraie Rolex. Malheureusement pour eux, la seule chose qu'ils reçoivent est une lettre de la Fédération horlogère qui précise que leur montre a été saisie, qu'elle va être détruite et qu'ils vont devoir payer cette opération. Les clients sont rarement en colère: généralement, ils ont plutôt honte. «Certains d'entre eux nous écrivent même pour s'excuser», précise l'avocate. Pour elle, ces bonnes relations avec les acheteurs déçus sont un atout majeur, car ces derniers lui communiquent des informations de première importance: URL de pages Internet cachées, adresses, données de comptes bancaires, tout y passe. Et elle n'a plus

> Par an, 40 millions de fausses montres suisses sont fabriquées dans le monde – contre 29 millions de vraies.

Pas de pitié: les contrefaçons saisies par les douaniers sont systématiquement détruites.

Repèrent même les meilleures contrefaçons: Michel Arnoux, Carole Aubert et Yves Brouze forment l'Internet Unit de la Fédération horlogère.



Dans la jungle virtuelle d'Internet.

qu'à remonter jusqu'aux faussaires. En contrepartie, elle aide ces clients à récupérer leur argent auprès des sociétés de cartes de crédit. Lorsqu'un internaute a commandé une réplique, ce n'est pas possible. Mais quand il croit en toute bonne foi

> Les acheteurs déçus deviennent de précieux informateurs.

avoir acheté une vraie montre, il peut être considéré comme victime d'une escroquerie. Désormais, Carole Aubert espère que les cas de ce type vont se multiplier, afin de faire pression sur les banques chinoises qui sont nombreuses à profiter de ce marché de plusieurs milliards.

2000 saisies rien qu'en Chine

Chaque année, près de 40 millions de fausses montres suisses sont fabriquées dans le monde – alors que l'industrie horlogère suisse ne produit pour sa part que 29 millions de vraies montres par an. Pour combattre ce fléau, les chasseurs de contrefaçons utilisent toutes les armes dont ils disposent, qu'elles soient virtuelles, juridiques ou policières. Rien qu'en Chine, la Fédération horlogère a été à l'origine de quelque 2000 saisies et, à l'échelle planétaire, les autorités ont réussi à intercepter un million de fausses montres.

La petite différence

«Les faussaires visent tous les segments du marché», nous confie Michel Arnoux, le chef du service anti-contrefaçon. «De la montre bon marché pour le tiers-monde au modèle haut de gamme pour des pays comme la Suisse, il y en a pour tout les goûts.» Certaines de ces imitations sont tellement bien faites que seuls des horlogers chevronnés sont capables de faire la différence. Dans une vitrine, il saisit une fausse Hublot Big Bang. Comme le modèle original, elle a un tourbillon. «Mais il a été fabriqué en Chine, pas en Suisse», précise-t-il. Ces modèles lui permettent de former les douaniers et de leur donner des indices: «La fausse Rolex GMT-Master a un bracelet en plastique et non en caoutchouc. Sur l'étiquette de cette fausse Tissot, on peut lire qu'elle est étanche jusqu'à 200 mètres. Or, sur les montres suisses, cette valeur est indiquée en bars, pas en mètres.»

L'avidité rend créatif

Mais certains escrocs sont particulièrement inventifs. Arnoux nous raconte une anecdote. Un internaute achète pour une somme très importante une Rolex ayant appartenu à Eric Clapton, accompagnée d'un document signé de la main du musicien. Assailli par le doute, il s'adresse à la Fédération horlogère. Arnoux mène l'enquête et la montre s'avère être une authentique Rolex. Seul bémol: le document signé par Clapton est un faux. Le guitariste n'a jamais possédé de montre comme celle-ci.

Que risquent les clients?

Depuis 2008, il est interdit d'importer en Suisse des articles de marque contrefaits, même pour un usage privé, qu'il s'agisse d'un faux sac à main Gucci acheté pendant ses vacances ou d'une fausse Omega commandée sur Internet. Pour les particuliers, aucune peine n'est prévue, mais les douanes peuvent saisir les articles et les détruire. La Fédération de l'industrie horlogère prélève en outre une indemnité de 250 francs par colis saisi.

Cependant, comme le précise le service anti-contrefaçon, acheter un faux sur Internet comporte aussi d'autres risques. C'est ainsi que les fausses montres peuvent contenir des substances dangereuses pour la santé. De plus, les organisations criminelles revendent au plus offrant les informations concernant les cartes de crédit de leurs acheteurs. Actuellement, cela leur rapporte environ 100 dollars par carte, soit souvent davantage que la fausse montre.

Pour de plus amples informations, veuillez vous rendre sur www.fhs.ch

QU'EST-CE QUE LE DARK WEB, MARC RUEF?

Pour protéger ses clients contre les cyberattaques, il sonde la partie la plus profonde du web, parfois à la limite de la légalité: Marc Ruef nous présente la face cachée de la toile mondiale.

interview: Christine Brand photos: Roland Tännler

Le dark web fait penser à un endroit sombre où l'on peut engager un tueur à gages ou acheter une ceinture d'explosifs. Qu'en est-il?
Aussi appelé dark net, le dark web est complexe. D'un côté, il abrite des services d'anonymisation légitimes, qui ne sont pas uniquement utilisés par des criminels. Pendant le printemps arabe, les manifestants s'en servaient pour communiquer entre eux sans se faire repérer par le régime. De l'autre, le dark web est effectivement un repère de gens peu recommandables.

C'est-à-dire?
Sur cette partie de la toile, on découvre des choses vraiment choquantes. Récemment, nous avons travaillé sur les données d'un groupe terroriste afin d'en savoir plus sur leurs moyens techniques et nous sommes tombés sur des photos de gens décapités. De telles images sont difficilement supportables. Sur certains forums, on voit même pire, mais il m'est difficile d'en parler.

Essayez quand même…
Pour le dire simplement: quand j'étais jeune, j'adorais les films d'horreur et je pensais donc que j'étais un peu différent des autres. Mais maintenant, je sais que mes fantasmes étaient de la petite bière par rapport à la réalité.

Le dark web offre donc vraiment la possibilité d'acheter des armes et de la drogue ou d'engager un tueur à gages?
Certaines pages ne sont que des attrape-nigauds. Mais, sur d'autres, il est possible de s'assurer les services d'un tueur. Quant aux trafiquants d'armes et de stupéfiants, ils sont effectivement très actifs sur le dark web, tout comme ceux qui vendent des numéros de cartes de crédit, des adresses e-mail, des médicaments ou de la pornographie.

L'anonymat est la clé du succès du dark web. Comment fonctionne-t-il au juste?
C'est un peu compliqué. Il y a d'une part le web public, que nous utilisons tous, et d'autre part le deep web, difficile d'accès. Le dark web fait partie du deep web.

Vous comparez le rapport entre le web public et le deep web à un iceberg.
Oui, sous la partie émergée – le web public ou clear web – il y a le deep web. Pour y accéder, il faut utiliser des logiciels spéciaux comme le navigateur Tor, qui crypte les données et dissimule les coordonnées de l'expéditeur et du destinataire. Souvent, l'accès est aussi protégé par différentes mesures, afin que les autorités ne puissent pas pénétrer dans le réseau. Pour accéder à certains forums, il faut être coopté par un utilisateur qui y participe déjà.

Il ne suffit donc pas d'installer le navigateur Tor pour accéder à la face cachée du web?

Tor vous permet d'y accéder. Et, avec un peu de persévérance, vous trouverez sans doute des pages

> «On découvre des choses vraiment choquantes.»

sur lesquelles vous pourrez acheter cinq kilos d'héroïne ou de cocaïne. Mais si vous voulez en commander 15 kilos, l'affaire se corse.

Pourquoi?
Pour exploiter les possibilités du dark web, il faut avoir des relations. Il ne suffit pas de taper www.traficdedrogue.ch. Les URL des sites illégaux sont généralement longues, cryptiques et elles changent souvent. Lorsque les responsables de la page pensent que les autorités sont à leurs trousses, ils déménagent et créent une nouvelle adresse. Si l'on ne connaît personne qui peut nous révéler cette nouvelle URL, impossible de la retrouver.

Comment faites-vous pour entretenir des relations sur le dark web?
Il faut communiquer avec les autres utilisateurs, connaître leur jargon et avoir quelque chose à leur proposer. J'utilise bien sûr une fausse identité, mais elle doit être crédible. Sinon, je risque de commettre des erreurs. Parfois, c'est assez compliqué. Sur le marché noir des armes, je ne peux pas me présenter comme un trafiquant suisse, cela n'aurait aucun sens. Mais si je feins d'être Russe, il faut que je parle parfaitement le russe.

Sans compter que quelqu'un va peut-être me demander où je suis allé à l'école et quel était le nom de mes professeurs. Or ces questions sont souvent des pièges. Il est très difficile de se mouvoir dans ces cercles.

Vous êtes une sorte de détective privé secret. Vos activités sont-elles légales?
Nous travaillons entre autres pour les autorités et pour des compagnies d'assurance. Mais il est vrai que, parfois, nous frisons l'illégalité. Nous nous demandons donc en permanence quels risques nous sommes prêts à courir. Et il arrive que nous décidions de ne pas franchir telle ou telle limite afin de respecter la loi.

Vous êtes en contact avec des criminels et prévenez vos clients lorsque vous pensez qu'ils vont être attaqués. Pourtant, vous n'alertez pas la police. N'est-ce pas un peu délicat?
Nous serions obligés d'envoyer des dizaines d'e-mails par jour aux policiers et ils nous répondraient qu'ils n'ont pas assez de personnel pour mener l'enquête ou qu'ils ne sont pas en charge des affaires internationales. Outre les problèmes technologiques liés au dark web, ce manque de moyens est l'une des raisons pour lesquelles il y a peu d'enquêtes. Pour démanteler un réseau de trafiquants d'armes, il faut interagir avec eux pendant des mois.

En d'autres termes, le dark web est une zone de non-droit?
Le dark web n'est en fait que l'un des outils qu'utilisent les criminels. Au final, l'infraction reste la même que dans le monde réel. Je ne pense pas qu'il y ait davantage d'actes criminels en raison de l'existence du dark web. Pour le dire autrement: je ne crois pas que, si l'on supprimait le dark web, il y aurait moins de crimes et de délits.

CLEAR WEB

Le web public, soit l'ensemble des sites librement accessibles et référencés par des moteurs de recherche comme Google.

DEEP WEB

Le web privé, qui regroupe notamment les sites des banques en ligne, les forums exigeants une authentification ou les réseaux nécessitant le recours à un logiciel spécial (peer-to-peer, chat, etc.).

DARK WEB

La partie illégale du deep web. L'accès aux réseaux, sites et forums du dark web est réservé à des utilisateurs triés sur le volet, souvent recrutés par cooptation. Ils sont en outre protégés par des mesures techniques (cryptage et routage complexe).

Plus tard, je serai malfaiteur

Quand il était petit, Marc Ruef disait qu'il voulait devenir le meilleur malfaiteur du monde. Mais il est passé de l'autre côté de la barrière: il protège ses clients contre les cyberattaques et les aide à identifier les failles de leur système de sécurité. Co-propriétaire de la société SCIP à Zurich, il publie régulièrement des articles dans des revues spécialisées. Son livre «Die Kunst des Penetration Testing» (L'art du test d'intrusion) est considéré comme un ouvrage de référence.

Ouvrons les yeux!

texte: Christine Brand

C’est l’aspect le plus désespérant de la cybercriminalité et nous n’avons pas le droit de l’ignorer: sur le dark web, la pédopornographie est omniprésente. Mais les enquêteurs se battent souvent contre des moulins à vent.

Pantalon beige, pull bleu, cheveux courts, visage poupin: Michael Meier* n'a aucun signe particulier, si ce n'est ces yeux graves qui en ont trop vu. Sur les murs de son bureau, il a punaisé des photos, des articles de presse et des procès-verbaux qui évoquent des affaires résolues par son équipe. «Cela me motive. A chaque fois que, grâce à nous, un enfant arrête de souffrir, je me souviens pourquoi je fais ce métier difficile», explique-t-il.

Enquête en eaux troubles

Meier, qui préfère rester anonyme, enquête sur des crimes dont les victimes sont sans défense. Il appartient en effet à une équipe de l'Office fédéral de la police (fedpol) qui a pour mission de combattre la pédopornographie sur Internet. Dans des locaux simplement équipés de quelques ordinateurs et d'où on entend le bruit de la ville, Meier et ses collègues arpentent le monde virtuel pour tenter de retrouver des pédophiles bien réels. A l'aide de logiciels spéciaux, ils sondent le web jusque dans ses zones les plus sombres. Pour parvenir à leurs fins dans cet environnement d'un genre nouveau, ils procèdent comme l'ont toujours fait les policiers. «Pour identifier les coupables, les moyens techniques ne suffisent pas. Nous devons communiquer avec les pédophiles, ce qui exige des connaissances psychologiques. Nous devons leur inspirer confiance, jusqu'à ce qu'ils nous révèlent une adresse mail ou un autre indice que nous pourrons utiliser», souligne Michael Meier.

Son job n'est pas à la portée du premier venu. Dès l'entretien d'embauche, les candidats sont confrontés à des images horrifiantes. «Tous les jours, nous sommes obligés de regarder des photos et des vidéos insupportables, dont le grand public n'imagine même pas le contenu», poursuit-il. «On ne s'y habitue pas. Mais on développe un regard professionnel qui nous permet de repérer les détails importants en faisant abstraction du reste. En l'espace de quelques secondes, nous sommes en mesure d'évaluer si les images sont répréhensibles ou pas, mais nous ne mémorisons pas forcément la couleur des yeux de l'enfant.»

Un travail d'équipe

Les membres de l'équipe de Meier ne travaillent pas plus de quatre heures par jour sur des cas de pédopornographie. Et aucun enquêteur ne se retrouve seul dans un bureau: «L'isolation est néfaste. Entre nous, nous parlons de ce que nous voyons et de ce que nous ressentons.» Les policiers ont en outre l'obligation de se rendre deux fois par an chez un psychologue. Chacun d'entre eux a sa propre manière de gérer le stress émotionnel auquel il est soumis. «Personnellement, pour prendre mes distances, je m'occupe de mes enfants et je me promène dans la nature», dit Meier, «cela me fait beaucoup de bien.»

Selon des estimations récentes, la pédopornographie génère un chiffre d'affaires de 20 milliards de dollars par an. Grâce à Internet, les pédophiles peuvent facilement communiquer entre eux, se procurer des prises de vue ou en vendre. Il va de soi que les organisations criminelles sont nombreuses à sévir sur ce marché. Pourtant, comme toujours, la majorité des actes pédophiles ont lieu dans le cadre familial et souvent dans les pays les plus pauvres. Dans les villes qui accueillent des touristes sexuels, de nouvelles pratiques ont vu le jour: le pédophile peut commander un live stream transmis en temps réel via Skype. Ainsi, le crime ne laisse pas de trace sur son ordinateur.

Un combat inégal

Lutter contre la pédopornographie sur Internet revient souvent à se battre contre des moulins à vent. «Si nous avions en permanence en tête l'ensemble du problème, nous baisserions les bras», affirme Michael Meier. «C'est pourquoi nous nous intéressons toujours au destin particulier de l'enfant concerné et essayons de le sauver, lui. Ensuite, nous nous penchons sur un autre cas particulier. Et ainsi de suite.» Afin d'illustrer sa démarche et d'expliquer pourquoi il pense que la pédopornographie devrait faire l'objet d'un vaste débat public, il nous raconte une histoire. Un vieil homme se promène sur une plage et croise un enfant qui remet à l'eau des étoiles de mer échouées sur le sable, sans se soucier du fait que d'autres étoiles de mer sont en permanence rejetées par l'océan. «Pourquoi fais-tu cela, puisque ça ne change rien au problème?» demande le vieil homme à l'enfant. L'enfant hoche la tête et rétorque: «Pour chacune de ces étoiles de mer prise individuellement, ça fait une différence, non?»

Garder le moral

Pour tenir le coup, Michael Meier et ses collègues ont besoin d'une bonne dose d'idéalisme. Les échecs sont nombreux et très douloureux. Par moments, ils se demandent si leur tâche a un sens et ils sont au bord du désespoir. Notamment lorsque, pendant plusieurs années, ils voient le même enfant être la victime de maltraitances sans rien pouvoir faire pour lui. «Il nous est arrivé de travailler pendant trois ans sur la même affaire», raconte Meier. «Au bout d'un moment, cet enfant faisait partie de notre vie, nous avions l'impression de le connaître. Mais nous n'avons jamais réussi à identifier ses bourreaux.»

Parfois, heureusement, ils parviennent aussi à leurs fins. Et ces victoires, dont parlent les documents accrochés aux murs du bureau de Michael Meier, sont essentielles pour garder le moral. Car les policiers savent qu'ils ont réussi à stopper le supplice de ces enfants – et que chaque destin compte. «En tant qu'enquêteur, j'ai travaillé dans de nombreux domaines», conclut Meier. «Mais en luttant contre la pédopornographie, j'ai vraiment le sentiment de contribuer à rendre le monde meilleur.»

* Le nom a été modifié par la rédaction

Au moins trois cas par jour

Au sein de l'Office fédéral de la police (fedpol), une équipe d'informaticiens, de psychologues, de juristes et d'analystes traque sur Internet les contenus qui tombent sous le coup de la loi et examine les signalements enregistrés. En 2015, fedpol a reçu 1193 signalements concernant des contenus pédopornographiques, soit plus de trois par jour. Le nombre de signalements a certes tendance à diminuer. Ceci n'est pourtant pas dû à une baisse du nombre d'actes répréhensibles, mais au fait que les pédophiles se réfugient de plus en plus souvent sur le dark web, où leurs activités sont quasiment indétectables.

JEUX, CHAT, NAVIGATION

Des collaborateurs de Coop Protection Juridique SA nous dévoilent leurs applis phares et ce qui les fascine dans le cyberespace.

photos: Valentina Verdesca

Gian Hess
Apprenti, 3e année

Je passe beaucoup de temps à jouer en ligne, surtout à Counter-Strike. J'entre dès lors dans un monde virtuel où je rencontre des gens passionnants. Les amitiés qui en résultent sont bien réelles: ce printemps, je suis allé voir à Hambourg un joueur que je connaissais depuis des années sur Internet. Nous avons passé un week-end inoubliable.

Sur mon iPhone, je n'ai plus que les applications qui me sont vraiment utiles: Mobile CFF, RTS Trafic, Supercard, Banque Coop, Facebook, WhatsApp et TomTom Europe. Je ne pourrais plus me passer de l'appli TomTom. Grâce à elle, je suis sûr de toujours savoir où j'ai garé ma voiture, même dans une ville que je ne connais pas. Il me suffit de prendre une photo à la sortie du parking. Si je suis perdu, je lance TomTom, je choisis «TomTom, ramène-moi à la photo» et je n'ai plus qu'à suivre les instructions pour retrouver mon véhicule. Parfait!

Paolo Schincariol
Responsable de la comptabilité

Tobias Mani
Responsable de l'équipe de juristes, Service juridique

Je trouve formidable de pouvoir travailler dans le train grâce aux nouvelles technologies. Je profite de cette possibilité pour mon activité professionnelle, mais aussi pour mes projets personnels. Dès que je suis chez moi, en famille, j'essaie d'utiliser le moins possible mon portable et mon ordinateur. J'ai toutes sortes d'applications sur mon smartphone. Guitar Tuner me permet par exemple d'accorder ma guitare à tout moment, sans le moindre câble. C'est une application simple et très intuitive.

Un monde sans Internet? Impensable! Consulter la météo, trouver un itinéraire sur Google Maps, vérifier une information sur Google – les possibilités sont quasi illimitées. Je prépare aussi mes vacances à l'aide de mon smartphone. Je passe des heures sur TripAdvisor et consorts pour trouver le meilleur hôtel, repérer des restaurants ou préparer mes futures excursions. Et je réserve aussi mes vols, mes chambres d'hôtel ou mes appartements Airbnb depuis mon portable. Sans Internet, je ne vois vraiment pas comment je m'y prendrais.

Andrea Mathys
Responsable Front Office, Particuliers

Joël Fischer
Juriste, Service juridique

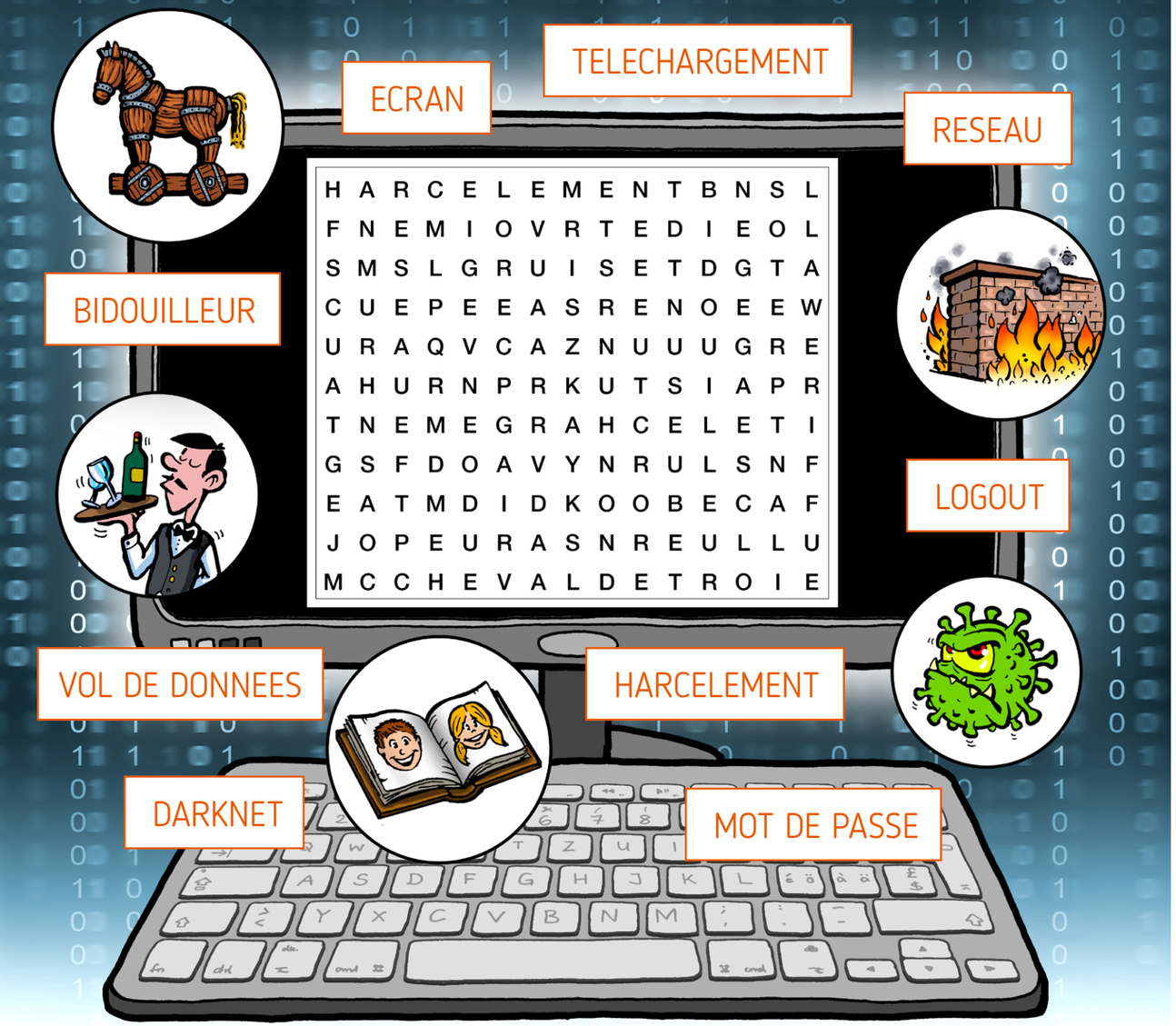
J'utilise teamplanbuch.ch pour gérer le planning de l'équipe de lacrosse que je dirige. En quelques clics, ce site permet d'organiser des rendez-vous (entraînements, matchs), de répartir les tâches et d'administrer la liste des membres. Grâce à l'appli pour mobile simple et claire qu'ils ont développée, chaque membre de l'équipe peut dire aux autres, dans la seconde, s'il participe à un événement ou non. D'autres fonctions permettent d'échanger des idées, un peu comme sur un blog, tous les joueurs pouvant poster des messages. C'est un formidable outil d'organisation et de coordination, idéal pour les associations.

J'utilise des applications comme WhatsApp, Facebook ou Snapchat et celles des journaux en ligne. En un clin d'œil, je peux envoyer des messages à mes amis ou partager des photos. Je ne pourrais plus me passer de WhatsApp. La première fois que j'en ai entendu parler, j'ai refusé de l'installer. Je n'avais pas envie d'avoir une icône de plus sur mon portable et les SMS me suffisaient amplement. Deux ans plus tard, j'ai fini par la télécharger. Depuis, je peux chatter avec toute la classe et envoyer des émoticônes amusantes à qui je veux. En plus, je fais des économies, car WhatsApp est gratuite: elle fonctionne avec le Wi-Fi.

Martina Frey
Apprentie, 2e année

CYBERCRIME, LE JEU
Trouverez-vous le mot-clé?

Dans la grille ci-dessous, rayez les mots qui apparaissent dans les encadrés orange ainsi que ceux qui correspondent aux dessins. Ils peuvent se croiser, se lire de haut en bas et vice versa, de gauche à droite et inversement ou même en diagonale. Un seul terme manque dans la grille: le mot-clé que vous devez trouver.



H	A	R	C	E	L	E	M	E	N	T	B	N	S	L
F	N	E	M	I	O	V	R	T	E	D	I	E	O	L
S	M	S	L	G	R	U	I	S	E	T	D	G	T	A
C	U	E	P	E	E	A	S	R	E	N	O	E	E	W
U	R	A	Q	V	C	A	Z	N	U	U	U	G	R	E
A	H	U	R	N	P	R	K	U	T	S	I	A	P	R
T	N	E	M	E	G	R	A	H	C	E	L	E	T	I
G	S	F	D	O	A	V	Y	N	R	U	L	S	N	F
E	A	T	M	D	I	D	K	O	O	B	E	C	A	F
J	O	P	E	U	R	A	S	N	R	E	U	L	L	U
M	C	C	H	E	V	A	L	D	E	T	R	O	I	E

Gagnez un MacBook!

Faites usage de vos talents de «cyberflic»! Lorsque vous aurez trouvé le mot-clé, envoyez-le nous par Internet via le site www.core-magazin.ch – et, avec un peu de chance, vous gagnerez l'un des trois prix que nous mettons en jeu!

1ER PRIX

Vive la mobilité: le MacBook est un poids plume. Très performant, il peut aussi être utilisé à la maison.

2E PRIX

Imbattable: pratique, élégant et puissant, l'iPad vous permet de vous connecter au monde numérique en toute liberté.

<page=47>

3E PRIX

Le son parfait: le casque Beats On-Ear tient toutes ses promesses. Vous n'allez pas en croire vos oreilles.

Le mot-clé:

Dernier délai de participation: 30 novembre 2016

Envoyez le mot-clé via www.core-magazin.ch

Les gagnants seront avisés par écrit. Les prix ne pourront pas être convertis en espèces. Tout recours juridique est exclu. Aucune correspondance ne sera échangée au sujet de ce concours. Les collaborateurs de Coop Protection Juridique SA et les membres de leur famille ne sont pas autorisés à participer à ce concours.

COMPLÈTEMENT SPACE

Le nouvel album de Yello vient de sortir. Intitulé «Toy», il a été enregistré sans instruments réels, à l'aide de sons numériques provenant du monde entier. Pour Boris Blank, le cyberespace est synonyme de liberté.

interview: Matthias Mächler photos: Ben Wolf

En quoi le cyberespace est-il synonyme de liberté?
Sans les nouvelles technologies, je n'aurais pas pu collaborer avec Fifi Rong, une chanteuse qui participe à cet album: elle a enregistré sa voix à Pékin et m'a envoyé le fichier audio par Internet.

Avez-vous peur du monde virtuel?
Non. Je me fais juste du souci pour les infrastructures sur lesquelles repose toute notre société de consommation. Un jour, le réseau va peut-être imploser.

Les téléchargements illégaux menacent l'industrie du disque et les groupes ne gagnent presque plus rien. Comment gérez-vous ça?
Avec Yello, nous avons de la chance: 60 pour cent de nos fans continuent à acheter des supports physiques. Mais il est clair que le streaming prend de plus en plus d'importance, ce qui pose des problèmes de revenus aux musiciens.

Via l'appli Yellofier, vous mettez gratuitement vos sons à la disposition des autres. Pourquoi?
Sur cette appli, il y a 6 banques de 8 sons, ce qui fait 48 sons au total. Yello a 38 ans. Je trouve qu'il était temps de remercier nos fans en leur offrant ces sons.

Vous composez toute votre musique sur ordinateur, sans musiciens. Ne vous sentez-vous pas un peu seul? Ou êtes-vous content de travailler en solitaire, vu que personne n'est aussi perfectionniste que vous?
J'ai toujours travaillé seul, même avant Yello. J'ai besoin de calme pour créer ma musique. Je ne peux pas faire autrement.

Est-ce que vous avez toujours un enregistreur sur vous pour capter les sons qui vous intéressent, comme par exemple la plainte de la rosée que vous avez entendue lors de vos vacances en Sardaigne?
Oui! Je découvre presque tous les jours des sons intéressants. Je les archive et, parfois, ils finissent dans un de mes morceaux.

«JE DÉCOUVRE PRESQUE TOUS LES JOURS DES SONS INTÉRESSANTS.»

Qu'est-ce qui est plus rentable: un nouvel album de Yello ou la production d'une bande-son pour un spot publicitaire?
Aujourd'hui, pour maintenir en vie ce que j'appelle le cirque Yello, j'ai besoin de gagner de l'argent en composant pour la pub. Si je ne disposais que des revenus reversés par Spotify, je pourrais à peine financer un vague numéro de music-hall.

Presque chaque année, vous recevez un prix pour l'ensemble de votre œuvre. Récemment, c'était l'IMS Pioneer Legend Award. On veut vous pousser à prendre votre retraite?
Comme je l'ai dit lors de la remise du prix Echo à Berlin: nous avons de la chance de recevoir ces distinctions alors que nous sommes encore bien là et pleins d'énergie.

Un petit miracle va se produire bientôt: fin octobre, Yello va donner quatre concerts à Berlin. Or on a toujours dit que vous n'aimiez pas la scène.
C'est Ian Tregoning, un ami londonien de longue date, qui m'a convaincu. Il m'a dit qu'à son avis, «Toy» était le meilleur album jamais publié par Yello et qu'il trouverait vraiment dommage que nous refusions de partager cette musique avec nos fans.

Revenons-en au cyberespace: si vous pouviez pirater le compte d'une institution ou d'une personne, qui attaqueriez-vous — et pourquoi?
Je n'en sais rien. Cette idée ne m'a jamais traversé l'esprit et je ne dispose pas des compétences nécessaires.

Merci!

Chères lectrices, chers lecteurs,

Depuis de longues années, Coop Protection Juridique a la chance de pouvoir compter sur des partenaires de premier plan. Sans eux, notre entreprise ne serait pas ce qu'elle est.

Nous aimerions donc remercier: Employés Suisse, Atupri, Beobachter, Collecta, Coop, Européenne Assurances Voyages, Syndicat du personnel de la douane et des garde-frontières garaNto, Helsana, Helvetia, CPT, ASLOCA du canton de Berne, ÖKK, Association du Personnel de la Confédération APC, Association du personnel de la Suva, Association suisse des employés de banque, Syndicat du personnel des transports SEV, Schweizerischer Bühnenkünstlerverband, smile.direct, Organisation suisse des patients OSP, SWICA, Sympany, Syna, Syndicom, Unia, Association transports et environnement ATE, Syndicat des services publics SSP.

coop protection juridique

tout simplement différente.

Coop Protection Juridique SA
Entfelderstrasse 2, Case postale 2502, 5001 Aarau
T. +41 62 836 00 00, info@cooprecht.ch
www.cooprecht.ch, www.core-magazin.ch