Prix de l'innovation EPS Reto Habermacher →

Interventions policières secrètes en cas de cybercriminalité

Damian Broger a récemment reçu le Prix de l'innovation EPS Reto Habermacher pour son travail de diplôme «Proaktive Massnahmen zur Bekämpfung der digitalen Kriminalität bei der Kantonspolizei St. Gallen» (Mesures proactives de la police cantonale de St-Gall pour combattre la cybercriminalité). Dans une interview accordée à *police*, le lauréat explique pourquoi la répression traditionnelle n'a que peu d'effet sur la criminalité numérique et quelles mesures sont plus prometteuses.

Interview : Markus Nobs ; photos : ISP

Interview

Stefan Aegerter, directeur de l'ISP, le lauréat Damian Broger et le vice-président de la FSFP, Emmanuel Fivaz (de g. à dr.).

Toutes nos félicitations pour cette distinction honorifique ! Que signifie pour toi l'obtention de ce prix ?
Merci beaucoup pour les félicitations. Je suis très heureux d'avoir remporté le Prix de l'innovation EPS Reto Habermacher et cela signifie plusieurs choses pour moi. D'une part, il s'agit d'une grande reconnaissance pour tous les efforts que mon équipe, toutes les personnes impliquées – plus particulièrement le client, le mentor, les personnes interviewées, les participants à l'enquête et à l'atelier – et moi-même avons fournis pendant la réalisation du travail de diplôme. Il ne faut pas non plus oublier les nombreuses contraintes vécues par ma famille puisque j'ai rédigé la majeure partie du travail de diplôme pendant mon temps libre. D'un autre côté, ce prix signifie pour moi, et probablement pour tous ceux qui s'engagent dans la lutte contre la criminalité numérique, que nous sommes sur la bonne voie avec nos méthodes et approches innovantes et souvent inédites. Dans le domaine d'activité relativement nouveau de la « lutte contre la criminalité numérique », les approches d'investigation traditionnelles atteignent rapidement leurs limites. Des approches créatives et un échange ouvert intercantonal, voire international dans l'idéal, sont ici nécessaires.

Pourquoi la répression dans le cadre de la criminalité numérique n'a-t-elle que très peu d'effet sur les auteurs agissant au niveau international ?
Contrairement à la criminalité « analogique » classique, les actes commis dans l'espace nu-

mérique n'exigent pas d'agir sur le lieu de leur réalisation. Ainsi, les délits numériques peuvent être perpétrés à partir de n'importe quel pays du monde, de plus, les auteurs peuvent utiliser une multitude de services en ligne disponibles dans le monde entier qui les aide à dissimuler leurs traces. Cette dimension internationale des enquêtes nécessite des procédures d'entraide administrative et judiciaire efficaces avec les pays concernés afin d'identifier les auteurs et de les déférer à la justice via des poursuites pénales et ce, tant en fonction du lieu de séjour de l'auteur que de la localisation des services utilisés. Mais dans la réalité, nous constatons que certains des pays sollicités soit ne coopèrent pas, soit, s'ils coopèrent, les procédures sont très inefficaces, formelles et longues. En ce qui concerne l'effet répressif sur les auteurs de délits, les valeurs suivantes apparaissent comme conséquence de la situation actuelle :

Dans ce domaine de criminalité, la coopération internationale ne fonctionne pas de manière satisfaisante.

- → Dans près de 90 % des cas, l'auteur de la criminalité numérique vient de l'étranger. Toutefois, l'auteur ne peut être attribué à un pays concret que dans quatre cas sur dix.
- → Dans un cas sur 40, l'auteur peut être identifié grâce à l'entraide administrative ou judiciaire internationale.
- → Mais, en fin de compte, l'auteur étranger n'a pu être poursuivi que dans 0,5 % des cas. En l'absence de données statistiques, il s'agit de valeurs moyennes estimées par 25 spécialistes du NEDIK (ndlr : réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique), qui ont été recueillies par le biais d'un sondage en ligne. Je déduis de ces chiffres que dans ce domaine de criminalité, la coopération internationale ne fonctionne pas de manière satisfaisante et que la focalisation purement répressive ne produit pas l'effet escompté.

Quelles mesures proactives sont-elles donc plus prometteuses dans la lutte contre la criminalité numérique ?

En principe, toutes les mesures qui permettent de perturber à temps l'auteur lors de la préparation du délit et/ou de l'exécution de l'acte, voire qui l'empêchent d'initialiser son méfait. Par perturbation précoce de l'auteur, j'entends ici les mesures possibles visant à interrompre la communication entre l'auteur et la victime, comme par exemple les annonces d'abus aux hébergeurs, le blocage de domaines, l'annonce de faux profils en vue de leur vérification ou de leur suppression, ainsi que le flux d'argent, en particulier l'annonce d'informations sur le compte de l'auteur aux intermédiaires financiers. Une autre approche consiste à attaquer la réputation ou la confiance dans l'auteur de l'infraction, par exemple en donnant délibérément de mauvaises évaluations sur les places de marché du Darknet pour les offres criminelles. Idéalement, les mesures choisies devraient avoir un effet sur l'auteur dans plusieurs domaines. C'est le cas par exemple de la collaboration avec une start-up suisse où les autorités, mais aussi les particuliers, peuvent signaler des ressources d'adressage criminelles qui, après vérification, sont inscrites sur une liste de surveillance interne. Tous les partenaires affiliés, par exemple les intermédiaires financiers et autres prestataires de services Internet, peuvent à leur tour intégrer sans délai cette liste de surveillance dans leurs systèmes de conformité internes.

Pour lutter contre cette criminalité, je recommande une intervention discrète de la police sur les réseaux.

L'une des mesures proposées est que la police se fasse elle-même passer pour une « money mule ». De quoi s'agit-il et quel en est l'intérêt ?

Dans le cas des phénomènes de cybercriminalité et de criminalité économique, les auteurs ont pour motif d'obtenir un transfert de patrimoine des victimes vers les auteurs. L'augmentation constante du nombre de cas ainsi que les montants de plus en plus élevés des délits ont conduit les banques à introduire des mesures de prévention de la fraude. Suite aux campagnes de prévention, la population considère également d'un œil critique tout paiement sur un compte étranger. Les auteurs de ces infractions ont réagi à ces mesures en installant des intermédiaires nationaux, appelés « money mules », comme relais dans le flux financier. L'utilisation des money mules suggère aux victimes un paiement en Suisse et rend en même temps l'analyse du flux financier plus difficile pour les enquêteurs. Comme solution proactive à ce problème, je recommande une intervention policière discrète sur la base de la loi cantonale sur la police. En réagissant à diverses dénonciations criminelles pour recruter des mules, en se laissant recruter et en autorisant les paiements délictueux sur des comptes de police cachés, la police obtient simultanément deux effets souhaités : d'une part, le flux de paiement des fonds délictueux peut être interrompu et ces fonds restitués aux personnes lésées ; d'autre part, la réputation des recruteurs de money mules, respectivement la confiance de leurs clients, peut être diminuée. C'est pourquoi il n'est pas problématique, voire même souhaitable, que l'auteur de l'infraction apprenne à la fin des opérations secrètes de la police ce qui s'est passé avec la money mule. Ainsi, lorsqu'il recrute de nouvelles money mules, il ne peut plus être sûr qu'il s'agit vraiment d'un particulier qui ne se doute de rien ou d'un agent de la police.

Tu parles aussi d'une mesure proactive qui consiste à ce que la police – incognito, bien entendu – donne délibérément de mauvaises

évaluations pour des attaques criminelles. Comment faut-il imaginer cela, comme sur Ricardo ?
En principe, cette mesure proactive utilise les possibilités d'évaluation du vendeur, comme c'est le cas par exemple avec les étoiles et les remarques correspondantes sur Ricardo ou Amazon. L'utilisation de cette mesure est toutefois particulièrement judicieuse sur les places de marché où les exploitants ne coopèrent pas avec la police, par exemple sur le Darknet ou sur les canaux Telegram. Dans ces cas, il n'est généralement pas possible de faire supprimer directement l'offre.

Notre expérience montre toutefois que, notamment dans le domaine de la criminalité high-tech, les auteurs s'organisent souvent en fonction de la division du travail. Il existe un vaste réseau de partenaires et d'acteurs, chacun avec ses propres spécialistes et des domaines d'activité clairement définis. Les prestations respectives sont proposées principalement sur le Darknet dans des forums ou sur des places de marché. Sur ces plateformes également, il existe souvent un système d'évaluation pour les acheteurs comme pour les vendeurs. Cela offre à la police la possibilité proactive de procéder à une attaque durable contre la réputation des vendeurs au moyen de mauvaises évaluations intentionnelles pour des offres illégales.

La cérémonie a eu lieu dans l'élégante Marianischer Saal de Lucerne.

Il ressort de ton travail que le ministère public ne donne parfois pas suite à la demande de la police de bloquer rapidement les comptes concernés, mais se contente de les éditer (ndlr : demande de renseignements des ayant droits économiques). Cela ne fait-il pas le jeu d'un délinquant ?
Oui, c'est malheureusement le cas. Notre expérience montre qu'un compte money mule est utilisé plusieurs fois en peu de temps par les auteurs pour blanchir de l'argent. C'est pourquoi il est extrêmement important de bloquer ces comptes money mule le plus rapidement possible et, dans l'idéal, de mettre en sûreté les fonds délictueux qui se trouvent sur le chemin entre la victime et l'auteur du délit. Malheureusement, le ministère public se contente souvent d'éditer les comptes concernés, ce qui a pour conséquence que ceux-ci peuvent encore être utilisés pour le blanchiment d'argent. À cet égard, je connais beaucoup trop de cas dans lesquels les mêmes comptes money mule ont été édités par plusieurs ministères publics cantonaux sur une longue période, mais n'ont pas été bloqués. ←

Les réponses aux questions représentent l'opinion de la personne interrogée et ne reflètent pas automatiquement la position de la FSFP.