Commission européenne

La cybercriminalité

L'importance croissante qu'occupe l'internet dans notre vie quotidienne, du fait notamment du développement des services de banque en ligne et du commerce électronique, s'accompagne parallèlement d'une augmentation de la criminalité organisée dans le cyberespace. De nos jours, les cyberdélinquants volent des coordonnées bancaires et des données de cartes de crédit qu'ils revendent pour seulement 1 EUR par carte ou 60 EUR lorsqu'il s'agit d'identifiants bancaires. La cybercriminalité est une activité lucrative qui traverse les frontières, mais comporte peu de risques. Il s'agit d'un problème qui nous concerne tous et auquel nous devons nous attaquer ensemble.

Qu'est-ce que la cybercriminalité?

La cybercriminalité désigne les infractions pénales commises en ligne via les réseaux de communications électroniques et les systèmes d'information. Il s'agit d'un problème sans frontières, qui peut revêtir différentes formes, mais qui présente toujours les deux caractéristiques suivantes: les infractions peuvent être commises à grande échelle et la distance géographique entre le lieu où se trouve l'auteur et les effets de l'infraction commise peut être considérable.

Au sens strict, le terme de cybercriminalité recouvre la fraude et la falsification en ligne. Les fraudes à grande échelle peuvent être commises par le biais de divers instruments, tels que l'usurpation d'identité, le «phishing» (technique consistant à obtenir des informations sensibles, telles que des mots de passe ou des données de carte de crédit, en se faisant passer pour une personne digne de confiance), les pourriels et les codes malveillants (virus informatiques).

La publication en ligne de contenus illicites constitue une autre forme de cybercriminalité. Ces contenus portent notamment sur la pédopornographie, l'incitation à la haine raciale, l'incitation aux actes de terrorisme et l'apologie de la violence, du terrorisme, du racisme et de la xénophobie. Ces faits sont considérés comme des infractions pénales dans de nombreux pays, mais pas dans tous.

© iStockphoto/kryczka, I. Radkov, Zmeel, Don Bayley

Une autre forme encore de cybercriminalité englobe les attaques contre les systèmes d'information, les attaques par déni de service et le piratage. Les systèmes d'information sont souvent attaqués par l'intermédiaire de «botnets», terme désignant un réseau d'ordinateurs infectés par un virus (machines «zombies» ou «bots», abréviation de «robots») qui, à l'insu de leurs utilisateurs, sont contrôlés par un autre ordinateur.

© iStockphoto/TommL, Zmeel, alengo

Qui est touché par la cybercriminalité?

Personne n'est à l'abri de la cybercriminalité. Elle touche aussi bien les citoyens, les entreprises et les administrations que les infrastructures critiques.

La cybercriminalité fait chaque jour plus d'un million de victimes dans le monde. Certaines subissent un vol de données bancaires et de carte de crédit par le biais de courriels semblant provenir de leur banque. D'autres se font escroquer par de faux sites marchands ou sont victimes d'un piratage de leur téléphone intelligent. Les médias sociaux sont également la cible d'attaques; à titre d'exemple, jusqu'à 600 000 comptes Facebook subissent chaque jour des tentatives de piratage.

Les cyberattaques contre les infrastructures critiques peuvent être lourdes de conséquences pour les entreprises, les administrations et même la société. Les attaques à grande échelle contre des infrastructures de technologies de l'information et de la communication (TIC) réalisées à l'aide de logiciels malveillants ou de réseaux zombies («botnets») peuvent perturber la fourniture de biens ou services vitaux. Ce type d'attaques peut également perturber le fonctionnement d'autres infrastructures critiques, comme les réseaux de transport et d'énergie.

Quelle réponse l'UE apporte-t-elle à la cybercriminalité?

Étant une activité à faible risque et à forte rentabilité, la cybercriminalité est devenue un problème très répandu qui ne connaît pas de frontières. Une collaboration au niveau de l'Union européenne est donc essentielle pour la combattre.

L'UE s'attache à améliorer la coopération opérationnelle entre les services répressifs ainsi que la coordination entre États membres, notamment par le biais d'activités de sensibilisation, de formation et de recherche. Elle favorise en outre le dialogue avec l'industrie, qui contrôle une grande partie des infrastructures d'information.

Coopération opérationnelle entre États membres de l'UE

En 2011, les services répressifs de 26 pays de l'UE, soutenus et coordonnés par Europol, ont mené une vaste opération policière contre des réseaux de partage de fichiers de pédopornographie sur l'internet. Cette intervention baptisée «opération Icare», qui se poursuit actuellement, a permis à ce jour d'identifier 269 suspects et d'en interpeller 112 à travers 22 pays européens.

Plusieurs mesures législatives de l'UE contribuent également à la lutte contre la cybercriminalité. Il s'agit notamment de:

- la décision cadre de 2001 concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces, qui définit les pratiques frauduleuses que les États membres doivent considérer comme des infractions pénales passibles de sanctions;
- la directive vie privée et communications électroniques de 2002, qui prévoit que les fournisseurs de services de communications électroniques doivent garantir la sécurité de leurs services et la confidentialité des informations concernant leurs abonnés;
- la décision cadre de 2005 relative aux attaques visant les systèmes d'information, et la proposition de directive de 2010 destinée à la remplacer, qui a pour but de remédier plus efficacement aux attaques massives simultanées et aux réseaux zombies;
- la directive de 2011 relative à la lutte contre l'exploitation sexuelle des enfants sur l'internet et la pédopornographie, qui prévoit des mesures plus efficaces à l'égard de nouveaux phénomènes qui apparaissent dans l'environnement de l'internet, tels que le «grooming» (pratique consistant à se faire passer pour des enfants afin d'attirer des mineurs à des fins sexuelles).

L'Agence européenne chargée de la sécurité des réseaux et de l'information aide les États membres de l'UE à traiter les problèmes de sécurité de l'information, à y répondre et à les prévenir et encourage la coopération entre les secteurs public et privé. Il a également été proposé de créer un centre européen de la cybercriminalité qui doit servir de source d'information et permettre de mutualiser les compétences afin de soutenir le renforcement des capacités des pays de l'UE ainsi que d'aider ces derniers dans leurs enquêtes. Ce centre mettra les États membres en garde contre les menaces cybercriminelles majeures qui se profilent et leur signalera les failles éventuelles dans leurs défenses informatiques. Il établira en outre une cartographie des activités criminelles en repérant les tendances que suivent, par exemple, les attaques de virus, de manière à tenir les autorités et les citoyens informés de tout nouveau phénomène éventuel.

Pour obtenir davantage d'informations à propos de l'action de l'Union européenne dans le domaine de la lutte contre la cybercriminalité, visitez notre site internet: ec.europa.eu/home-affairs