Rapport semestriel du Centre national pour la cybersécurité : cyberespace et conflits armés

Pauline Meyer, le 9 novembre 2022

Le 3 novembre 2022, le Centre national pour la cybersécurité publie son rapport semestriel pour la période de janvier à juin 2022, dont le thème prioritaire porte sur la dimension cybernétique des conflits armés et les attaques perpétrées dans ce contexte.

Le NCSC publie son quatrième rapport semestriel couvrant la période de janvier à juin 2022 (Rapport semestriel 2022/1). Il traite principalement de la dimension cybernétique des conflits armés avant de retracer, à son habitude, les évènements portés à sa connaissance en se penchant sur quelques problématiques clés.

La composante cyber des conflits armés fait écho à la guerre actuelle entre la Russie et l'Ukraine. Le cyberespace est exploité en amont et durant les conflits armés. Des maliciels sont typiquement utilisés pour créer des pannes de courant par l'infection de systèmes de contrôle industriels assurant l'approvisionnement en électricité ou pour infecter des systèmes informatiques gouvernementaux et supprimer les données qu'ils traitent. Ces diverses attaques, cherchant tant à influencer des individus qu'à engendrer des répercussions physiques ou porter atteinte à la sécurité des données, sont perpétrées par différents acteurs et il peut être difficile d'établir la fiabilité des informations à leur sujet.

Le nombre de cyberincidents enregistrés par le NCSC au cours du premier semestre 2022 a augmenté de 70% par rapport au premier semestre 2021, en raison principalement d'une forte augmentation de de faux courriers électroniques ayant pour but l'extorsion des destinataires. En opposition, le nombre d'annonces au sujet de maliciels a quelque peu diminué par rapport à la même période de l'année précédente.

En parallèle, les annonces de numéros de téléphone usurpés ont explosé, passant de 17 à 319. Plus précisément, des centres d'appels douteux utilisent régulièrement des numéros appartenant à des particuliers. La situation peut être pesante pour les réels propriétaires des numéros usurpés, qui peuvent être submergés de rappels et qui sont à l'heure actuelle limités dans les démarches qu'ils peuvent entreprendre pour se protéger de ces retombées (FF 2017 6207, 6221).

Le NCSC se penche sur la question de l'accès à distance à des systèmes informatiques ou à des comptes utilisateurs, première étape de nombreuses cyberattaques. Le plus simple pour accéder à un compte ou à un système est de passer par un nom d'utilisateur, souvent constitué de l'adresse électronique et d'un mot de passe. Les délinquants peuvent ensutie faire un bourrage d'identifiants (tester les données d'accès pour différents services informatiques, voir le rapport et les lignes directrices de Global Privacy Assembly, à la rédaction desquels le PFPDT a participé) pour vérifier si les identifiants sont utilisés pour plusieurs sites et finalement les vendre. L'authentification à double facteurs peut ici aider à protéger les utilisateurs.

Les délinquants peuvent également utiliser des maliciels pour s'infiltrer dans des systèmes, notamment par le biais de courriels infectés, ou exploiter les vulnérabilités pour s'introduire dans un système, raison pour laquelle il faut toujours procéder aux mises à jour.

Le rapport aborde également les maliciels actifs entre janvier et juin 2022, les failles de vulnérabilités connues, les évènements survenus à l'étranger, les acteurs malveillants les plus actifs et leurs méthodes d'attaques ainsi que les problématiques à composante cyber concernant les systèmes de contrôle industriels et la technologie opérationnelle.

Finalement, le NCSC soulève l'importance de la sécurité des données en lien avec les fuites de données. Ces fuites peuvent malheureusement facilement avoir lieu en raison d'attaques, d'erreurs ou de systèmes informatiques insuffisamment protégés ou entretenus. Elles peuvent engendrer diverses conséquences dommageables, allant du chantage et des menaces à la perte de maîtrise sur les données ou aux risques pour la réputation et pour la personnalité (selon les données visées).

Il n'existe aujourd'hui aucune obligation légale de signaler les fuites de données, situation qui changera dans certaines circonstances avec d'une part la future obligation d'annoncer les violations de la sécurité des données au PFPDT (art. 24 nLPD) et, d'autre part, la future obligation pour certaines infrastructures critiques de signaler des cyberattaques au NCSC (art. 74a ss AP-LSI2).

Alors que l'art. 24 nLPD entrera en vigueur l'année prochaine, la date de l'entrée en vigueur de la Loi fédérale sur la sécurité de l'information révisée (dont la première partie entrera en vigueur également en 2023) n'est pas encore fixée. En attendant, le NCSC met à disposition sur son site internet quelques mesures techniques et organisationnelles pour l'entreprise confrontée à une fuite de données.

Proposition de citation : Pauline MEYER, Rapport semestriel du Centre national pour la cybersécurité : cyberespace et conflits armés, 9 novembre 2022 *in* www.swissprivacy.law/183