Second rapport semestriel du Centre national pour la cybersécurité : focus sur les failles de sécurité

Pauline Meyer, le 4 janvier 2022

Le 2 novembre 2021, le NCSC a publié son second rapport semestriel (Rapport semestriel 2021/1 intitulé « Sécurité de l'information. Situation en Suisse et sur le plan international »). Le thème prioritaire choisi concerne les vulnérabilités des systèmes informatiques.

Le Centre national pour la cybersécurité (NCSC), centre de compétences de la Confédération pour la protection contre les cyberrisques, a publié son second rapport pour la période couvrant le premier semestre 2021. Il traite principalement des vulnérabilités des systèmes informatiques susceptibles d'être exploitées à des fins de cyberattaque.

Dans son chapitre consacré aux failles de sécurité, le NCSC traite tout d'abord des principales vulnérabilités révélées au premier semestre de l'année écoulée. Parmi celles-ci figure notamment « ProxyLogon », la faille critique de Microsoft Exchange et les vulnérabilités auxquelles elle a donné accès. Grâce à cette chaîne d'attaque, des intrus étaient parvenus à contourner l'authentification d'Exchange pour s'annoncer comme administrateurs. Ainsi, il leur était possible de prendre le contrôle complet des serveurs et lire ou manipuler la correspondance électronique, les données du calendrier, les coordonnées et les tâches à effectuer. Le NCSC analyse également la compromission du logiciel de partage de fichiers « Accellion ». Cette faille a permis à des acteurs malveillants de se procurer les données de centaines de clients comptant des institutions majeures aux quatre coins du globe, de demander des rançons et de partager les données en leurs mains. Il examine d'autres vulnérabilités, à l'instar de « PrintNightmare », qui a été utilisée par des attaquants afin de se déplacer latéralement au sein des réseaux, ce qui a notamment été exploité par des opérateurs de rançongiciels. Le NCSC fournit pour chaque vulnérabilité analysée des recommandations pour une meilleure protection face à ces vulnérabilités, allant de la mise en place d'un pare-feu ou d'un système d'authentification à deux facteurs à l'utilisation de divers correctifs et à la mise en place de mesures assurant la *security by design*.

Le NCSC poursuit en insistant sur l'importance des chaînes d'approvisionnement logicielles (*software supply chain*), en citant l'exemple d'une vulnérabilité découverte dans le produit « Bash-Uploader ». Dans la mesure où des milliers de clients utilisaient le script faisant partie intégrante de différents programmes, ces derniers n'étaient pas forcément au courant de la

menace réelle que cet incident faisait peser. Le rapport 2021/1 signale que la nomenclature logicielle (*software bill of materials*, SBOM), développée conjointement par l'administration nationale des télécommunications et de l'information américaine (NTIA) et ses partenaires, permettrait d'indiquer pour les produits numériques tous les composants entrant dans la fabrication d'un produit final, de la même manière que pour les denrées alimentaires. Néanmoins, vu la complexité des bases de données à mettre à jour, il est nécessaire de bénéficier d'un moyen de saisie et de traitement automatisé des avis de sécurité. Pour ce faire, un format comme le « *Common Security Advisory Framework* (CSAF 2.0) », développé par l'organisation OASIS Open (organisation d'utilité publique responsable de normes *open source*), pourrait typiquement servir à établir les avis de sécurité nécessaires sous forme standardisée et lisible à la machine.

Le rapport 2021/1 évoque ensuite les compétences de la division du NCSC habilitée à informer, sensibiliser et soutenir le public (dont font partie les particuliers, entreprises et services étatiques) sur les failles de sécurité et les précautions à prendre. Elle gère également une plateforme en vue de la divulgation coordonnée de vulnérabilités, permettant aux individus identifiant une faille d'annoncer anonymement leur découverte à un service étatique. Finalement, elle offre aux services étatiques une plateforme de primes aux bogues (*bug bounty*) permettant d'identifier les éventuelles lacunes de sécurité au sein des réseaux informatiques des collectivités publiques. Le NCSC cite l'exemple du projet pilote de primes aux bogues lancé du 10 au 21 mai 2021 visant le DFAE et les Services du Parlement, qui avait par ailleurs permis de découvrir dix vulnérabilités.

Le reste du rapport offre un aperçu des annonces de cybersécurité reçues par le NCSC et ses services et dresse un panorama des menaces actuelles. Il donne une vue d'ensemble des annonces reçues, par le biais du nouveau formulaire d'annonce, durant le premier semestre 2021, dont plus de la moitié concerne des cas de fraude, à l'instar de *fake sextorsion* ou de fraude au paiement anticipé. Le NCSC attire l'attention du lecteur sur la diffusion de maliciels ou rançongiciels, ayant retenu son attention durant cette première moitié d'année, en Suisse ou ailleurs. Il parcourt également les questions de fuites de données, en s'arrêtant sur le vol de données de passagers de la Société internationale de télécommunications aéronautiques (SITA), qui s'était fait dérober des données, dont des informations de passeport ou de carte de crédit, de quelques 4.5 millions de passagers de diverses compagnies aériennes lors d'une cyberattaque visant son système de gestion des passagers. Le NCSC revient dans ce contexte sur les cas de *data scraping* de Facebook et Linkedin, qui avaient eu pour conséquence la publication sur le Darkweb d'énormes quantités de données personnelles. Le *data scraping*, englobant toutes sortes de techniques permettant d'extraire systématiquement des

sites Web publics des contenus tels que des numéros de téléphone ou adresses électroniques, est toujours plus pratiqué à des fins d'optimisation du marketing notamment. Ces techniques permettent d'accéder à une quantité astronomique de données publiques ou privées relatives à des profils, de la même manière qu'elles permettent de regrouper les données provenant d'anciennes fuites pour créer une base de données agrégée. Pour ces raisons, le NCSC requiert des services Internet rendant accessibles au public leurs fichiers de données de protéger leur plateforme contre les consultations de masse automatisées. Il demande également à la population de restreindre l'accès public à ses profils sociaux, réfléchir aux contenus qu'elle publie en ligne et n'accorder aux applications que les autorisations nécessaires. Il est finalement nécessaire que toute entreprise dispose d'un plan de réponse aux incidents (*data breach response plan*).

Parmi les autres annonces de cybersécurité recueillies, les fraudes à l'investissement sont abordées et le NCSC invite les lecteurs à se méfier des promesses de rendements importants à court terme et des tiers proposant soudainement leur aide après une fraude. En plus de renvoyer à diverses pages de son site internet pour plus d'informations concernant les questions qu'il aborde, le NCSC soulève également la sensibilité, exacerbée par la pandémie et les conditions météorologiques extrêmes, de la technologie opérationnelle (OT) qui soutient et rend possible de nombreux processus et dont le pilotage est dépendant des systèmes de contrôle industriels (SCI). Il est nécessaire, pour assurer la disponibilité et l'intégrité des infrastructures critiques, de se préparer au mieux aux menaces qui pèsent sur ces systèmes ; pour y parvenir, les exploitants d'infrastructures critiques peuvent observer les nouvelles normes minimales par secteur adoptées par l'OFAE et les associations faîtières de certains secteurs d'approvisionnement.

Après le premier rapport publié par le NCSC (Rapport semestriel 2020/2, commenté sur swissprivacy/74) portant sur la santé numérique, ce second rapport, plaçant un focus sur les vulnérabilités, permet de comprendre l'importance pratique que revêt la prévention, la compréhension et la correction des failles de sécurité. Ces failles sont nombreuses en pratique et leur exploitation par des acteurs malveillants est susceptible d'engendrer des risques importants pour les données, notamment personnelles. Il est donc aujourd'hui primordial pour tout acteur, compte tenu de ses spécificités, d'adopter les mesures de sécurité techniques et organisationnelles pour prévenir les vulnérabilités informatiques au mieux, pour les détecter, empêcher les exploitations malveillantes de ces dernières et les réparer.

_swissprivacy.law

Proposition de citation : Pauline MEYER, Second rapport semestriel du Centre national pour la cybersécurité : focus sur les failles de sécurité, 4 janvier 2022 *in* www.swissprivacy.law/112