Rapport semestriel du Centre national pour la cybersécurité : focus sur les attaques contre la chaîne d'approvisionnement

Pauline Meyer, le 12 mai 2022

Le 5 mai 2022, le NCSC a publié son troisième rapport semestriel (Rapport semestriel 2021/II « Sécurité de l'information. Situation en Suisse et sur le plan international »). Le thème prioritaire porte sur les attaques contre la chaîne d'approvisionnement des produits informatiques.

Le Centre national pour la cybersécurité (NCSC) a publié son troisième rapport semestriel pour la période de juillet à décembre 2021. Il traite principalement des attaques contre la chaîne d'approvisionnement, avant de parcourir, comme dans ses rapports précédents, les évènements portés à sa connaissance durant la période susmentionnée. Il attire l'attention sur l'importance de l'ingénierie sociale dans le cadre des évènements signalés.

Les attaques contre la chaîne d'approvisionnement (*supply chain*) peuvent engendrer des conséquences dramatiques, en visant un cercle limité de cibles ou en se propageant à plus large échelle. De nombreuses entreprises collaborent avec plusieurs partenaires fournissant des matières premières, technologies ou prestations permettant d'aboutir à un produit final ou d'être intégrées à une prestation. La chaîne d'approvisionnement englobe toute la chaîne de création de valeur. Une attaque chez l'un de ces partenaires peut se répercuter sur les autres sociétés voire sur les consommateurs finaux. L'un des maillons du processus de création de valeur peut servir de porte d'entrée à un attaquant (attaque *via* la chaîne d'approvisionnement) ou une attaque peut chercher l'interruption de la chaîne d'approvisionnement (attaques *contre* la chaîne d'approvisionnement).

Le NCSC illustre notamment cette problématique avec la compromission d'un prestataire autrichien en septembre 2021 par un rançongiciel cherchant à cibler les PME clientes du prestataire. En parallèle, les attaques DDoS visant une société d'hébergement abritant le site internet du canton de Saint-Gall ont entravé la disponibilité de plusieurs sites de clients.

Ces exemples montrent que les relations avec les fournisseurs et prestataires doivent être régulièrement évaluées à la lumière du profil de risque. Le NCSC recommande aux petites entreprises ne disposant pas de leurs propres spécialistes de couvrir contractuellement les risques avec les partenaires externes si un risque accru existe pour l'entreprise.

Le NCSC parcourt ensuite les évènements portés à sa connaissance durant le second semestre de l'année 2021. Le Centre indique avoir enregistré 21 714 annonces, soit le double de ce qu'il avait reçu durant le premier semestre de l'année. Ce nombre élevé s'explique notamment par l'introduction du nouveau formulaire du NCSC que toujours plus de personnes utilisent, ainsi que par une recrudescence notable de certains phénomènes.

Les évènements signalés au NCSC présentent régulièrement une part d'ingénierie sociale. Grâce à la sensibilisation auprès des internautes, le taux de réussite des escrocs diminue. Ces derniers cherchent à mieux susciter la confiance de leurs cibles, parfois en perpétrant des attaques plus individualisées ou en combinant différentes techniques d'ingénierie sociale.

Les fraudes constituent les évènements les plus signalés, avec un nombre important de courriels provenant prétendument d'autorités, notamment pénales, exigeant le paiement d'amendes ou de cautions.

Les cas de phishing, également élevés, consistent typiquement en des notifications de colis réclamant des émoluments au nom de services de livraison ou de l'Administration fédérale des douanes. Certains auteurs de phishing créent des sites internet d'entreprises de livraison, conçus individuellement pour un produit, incitant les vendeurs sur des sites de petites annonces à dépasser leur scepticisme et à partager leurs données de carte de crédit sur le site.

Dans le cadre d'arnaques aux sentiments et au lieu de continuer de demander de l'argent aux lésés, certains escrocs vont se faire passer pour riches et faire miroiter un gain important à leurs cibles. Ils partagent leurs « connaissances » avec ces dernières pour qu'elles investissent sur une prétendue plateforme de placement et « gagnent des sommes importantes », alors que le titulaire du site internet et l'escroc collaborent.

Le NCSC parcourt également les maliciels principalement utilisés ces derniers mois, dont Flubot, lequel fait parvenir par SMS un lien renvoyant prétendument vers un message vocal, ou encore Gootkit, maliciel spécialisé dans le vol de données bancaires par des campagnes de spams et par des sites internet compromis incitant les utilisateurs à télécharger le programme.

Le NCSC émet systématiquement des recommandations à l'attention des parties prenantes. Au niveau de la population, la prévention demeure primordiale. Alors que le taux de réussite d'escroquerie diminue en raison notamment de cette sensibilisation, les acteurs malveillants

redoublent d'efforts. L'attention portée par les citoyens doit s'aligner avec ces évolutions, notamment par la prudence à conserver même lorsque l'on a l'impression de connaître son interlocuteur, d'autant plus lorsqu'une communication déjà effectuée est utilisée de manière incohérente.

Proposition de citation : Pauline MEYER, Rapport semestriel du Centre national pour la cybersécurité : focus sur les attaques contre la chaîne d'approvisionnement, 12 mai 2022 *in* www.swissprivacy.law/145