Rapport semestriel du Centre national pour la cybersécurité : cybersécurité des PME

Pauline Meyer, le 22 juin 2023

Le 11 mai 2023, Le NCSC a publié son rapport semestriel pour la période de juillet à décembre 2022, dont le thème prioritaire porte sur la cybersécurité des PME.

Le Centre national pour la cybersécurité (NCSC) a publié son rapport semestriel couvrant la période de juillet à décembre 2022. Celui-ci traite principalement de la cybersécurité des PME et, comme il le fait habituellement, relate les différents évènements portés à sa connaissance et commente l'évolution des cybermenaces en Suisse.

Les PME (englobant les entreprises de moins de 250 employés) représentent 99.7% des entreprises en Suisse. Comme le reste de la société, elles n'échappent pas à la numérisation. Le NCSC recommande aux PME d'envisager la transition numérique avec précaution et de prendre la cybersécurité en compte à chaque étape de ce processus.

Les PME doivent également veiller à la maintenance de leurs ressources informatiques, en profitant des soutiens à disposition. Les PME peuvent typiquement s'appuyer sur des recommandations telles que les normes minimales TIC non contraignantes élaborées par l'OFAE et les associations économiques.

Il est également important de scinder, notamment dans l'allocation des ressources, la cybersécurité de l'exploitation de l'infrastructure informatique. Dans les faits, de nombreuses PME confient en effet ces fonctions à des responsables identiques, qui ne sont en mesure d'accomplir leur tâche de cybersécurité qu'à titre accessoire.

Le NCSC précise que les PME doivent également veiller à la cybersécurité dans leurs relations contractuelles avec des prestataires externes, que ce soit en prévoyant des mesures de protection et de défense contre les cyberattaques ou en abordant des questions telles que les sauvegardes ou les obligations de signaler des incidents.

Finalement, comme l'éventualité d'un cyberincident ne peut jamais être complètement écartée, des plans de gestion de cyberincidents doivent être élaborés et appliqués. Les communications internes et externes doivent aussi faire l'objet de réflexions préalables.

Après avoir partagé les contributions d'une infrastructure de transports publics et de la police au sujet de cyberattaques passées, le NCSC fait état dans son rapport des annonces de cyberincidents reçues. Leur nombre a considérablement augmenté en 2022, passant de 21 714 en 2021 à 34 527 l'année suivante (en raison notamment de la notoriété croissante du NCSC, de son formulaire et de l'évolution de certaines cybermenaces).

L'escroquerie demeure la première menace rapportée au NCSC, avec comme variante principale les courriels envoyés prétendument par la police (5 179 annonces). Parmi les cas d'escroquerie, des attaques visant les administrateurs de sites Internet ou des cas de fraude à l'investissement ont également été annoncées au NCSC durant le second semestre de 2022. Les cas de phishing signalés illustrent comment les escrocs calculent des probabilités et privilégient des opérations courantes, comme la notification de services d'expédition avec un colis à récupérer.

Alors que le nombre d'attaques par rançongiciel semble être demeuré stable, le nombre d'annonces de piratage a fortement augmenté, avec des cas de *fake sextorsion* basés sur des attaques réelles. Ces cas impliquent le piratage d'un compte de victime, p.ex. sur un réseau social sur lequel du contenu pornographique est publié, pour l'effrayer avant de la faire chanter.

Le NCSC émet quelques recommandations générales pour éviter que des intrus trouvent un accès initial à un système informatique, en préconisant l'authentification à deux ou plusieurs facteurs ou la fonction de mise à jour intégrée et automatique des logiciels. Il est également possible de se référer aux informations accessibles sur le site Internet du NCSC en cas d'attaque par rançongiciel ou de fuite de données. Le rapport du NCSC se termine avec un point sur la situation en Ukraine qui se semble se défendre avec succès contre les cyberattaques russes.

Proposition de citation : Pauline Meyer, Rapport semestriel du Centre national pour la cybersécurité : cybersécurité des PME, 22 juin 2023 *in* www.swissprivacy.law/234

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.