SecNumCloud : ce que l'ANSSI a changé après consultation

Du SDN dans SecNumCloud ? L'acronyme a fait son entrée dans la dernière version du référentiel, publiée ce 8 mars. En toile de fond, deux nouvelles exigences relatives aux données techniques. D'une part, leur stockage au sein de l'UE. De l'autre, leur protection vis-à-vis du droit extra-européen, en cas de recours à des sociétés établies hors de l'Union.

L'essentiel des modifications soumises à consultation publique fin 2021 ont été maintenues dans la version finale (voir notre article « SecNumCloud : ce que l'ANSSI veut changer »).

La définition du support technique fait partie des éléments qui ont évolué. Initialement, il était spécifié que dans le cadre de ces tâches, aucun accès aux données des commanditaires (= clients) n'était autorisé. La version finale instaure une tolérance explicite, au travers de l'expression « par défaut ».

Autre clarification dans la forme, sur la définition du CaaS (conteneurs *as a service*) : il ne s'agit plus de la mise à disposition d'environnements d'exécution, mais simplement d'outils.

Par rapport à la version précédente de SecNumCloud (publiée en 2018 pour tenir compte du RGPD), certains renvois à des recommandations de sécurité ont fait l'objet d'une mise à jour :

– À celle sur les mots de passe (datée de 2012) se substitue celle qui couvre aussi l'authentification multifacteur (2021)

– En cas de mise en œuvre de SSH, on ne se référera plus à la recommandation IPsec, mais à celle sur (Open)SSH

– Sur le contrôle d'accès physique, avec un renvoi vers une recommandation de mars 2020 en lieu et place de celle de novembre 2012 sur les technologies d'accès sans contact

SecNumCloud intègre le droit extraterritorial… et les événements naturels

Parmi les évolutions plus marquants à l'issue de la phase de consultation :

– L'ajout d'une disposition qui conditionne l'obtention de la qualification SecNumCloud à l'appréciation des risques liés aux événements naturels et sinistres physiques ; en plus de ceux liés à la séparation des tâches et aux environnements de développement (le référentiel comportait déjà des mentions de l'un et l'autre)

– Concernant la convention de service : elle doit indiquer que le prestataire doit mettre à disposition du client les éléments d'appréciation du risque liés à la soumission de ses données au droit d'un État non membre de l'UE

– Sur la protection contre le droit extra-européen : pour le prestataire, un délai d'un mois pour informer formellement le commanditaire de tout changement juridique, organisationnel ou technique pouvant avoir un impact en la matière

Photo d'illustration © OFC Pictures – Adobe Stock