Cybersécurité : ce que l'ANSSI ambitionne avec les CSIRT territoriaux

Le saviez-vous ? L'acronyme CERT, pour « Computer emergency and response team », est une marque déposée de l'université Carnegie-Mellon. Cette dernière ne s'oppose toutefois pas à son utilisation par des tiers.

Pour autant, l'ANSSI lui préfère le terme générique de CSIRT (Computer security incident response team). En tout cas dans le cadre de France Relance.

Le volet cybersécurité de ce plan national réunit une enveloppe de 136 millions d'euros pour 2021-2022. Il est question de la répartir comme suit :

Les CSIRT régionaux ciblent les « acteurs de taille intermédiaire ». Nommément, les PME, les ETI, les collectivités territoriales de plus de 5000 habitants et les associations de dimension nationale. Objectif : leur fournir un service de réponse à incident de premier niveau, complémentaire à ce que proposent les prestataires locaux*. Idéalement, cela couvrira :

– Centraliser les déclarations d'incidents cyber
– Les qualifier et transmettre les premiers bons réflexes aux bénéficiaires
– Mettre les victimes en relation avec les organisations chargées de les accompagner dans la résolution (prestataires ; police et gendarmerie)
– Effectuer une veille des vulnérabilités et des correctifs de sécurité
– Analyser l'état de la menace cyber visant les bénéficiaires
– Partager les connaissances en la matière au sein du réseau des CSIRT

Les acteurs étatiques, OIV/OSE, métropoles, départements et régions sont hors du périmètre ciblé : la gestion de leurs incidents se fait avec l'ANSSI. Les particuliers, les TPE, les collectivités de moins de 5000 habitants et les associations locales sont quant à eux invités à déclarer leurs incidents sur Cybermalveillance.gouv.fr.

Du C2RC aux CSIRT

La création des CSIRT régionaux mobilise deux leviers principaux. D'une part, un apport financier, sous forme de subventions. Montant maximal : un million d'euros par bénéficiaire, pour soutenir les deux premières années d'activité. De l'autre, un accompagnement méthodologique, à travers un programme d'incubation. D'une durée de quatre mois, il devra permettre de :

– Rédiger la charte d'utilisation et de fonctionnement du CSIRT (base : RFC 2350)
– Concevoir une feuille de route de mise en œuvre (base : référentiel SIM3)

La première session d'incubation devait, à l'origine, se tenir entre septembre et décembre 2021. Finalement, on a pris un peu de retard sur le calendrier initial : ce sera de février à juin 2022. Avec

un premier panel de 7 régions officialisé ce 11 janvier.

– Bourgogne-Franche-Comté
– Centre-Val de Loire
– Corse
– Grand Est
– Normandie
– Nouvelle-Aquitaine
– Région Sud

Cette dernière fait office de précurseur. Un C2RC (Centre de ressources régional cyber) y a effectivement été inauguré en octobre 2020, à Toulon.

« Parcours de cybersécurité » : une initiative en amont

Une deuxième session est prévue pour la période septembre-décembre 2022. Chaque région aura alors – espère l'ANSSI – son CSIRT. Il s'agira alors de les rendre pleinement opérationnels pour fin 2024 au plus tard. Et, sans attendre, les intégrer à l'InterCERT-FR. Ce réseau réunit des organismes qui ont des activités d'IRT (Incident response team) sur le territoire français. Une cinquantaine d'entités en sont aujourd'hui membres. Dont une bonne partie du CAC 40.

À son lancement, un CSIRT « [pourra] réunir 3 à 4 [sic] analystes dont 2 jeunes diplômés », nous explique-t-on. Avec une référence aux formations initiales labellisées SecNumedu.

L'ANSSI déploie une autre offre de service dans le cadre de France Relance. Son objet : élever le niveau de sécurité des SI existants. Elle prend deux formes, détaillées ci-dessous. Par « organisations au service des citoyens », il faut entendre « social, santé, formation, audiovisuel et sécurité ».

Parcours de cybersécurité

Quoi ? Accompagnement par un prestataire cyber pour :

- dresser un état des lieux ;
- identifier les mesures de sécurisation les plus urgentes ;
- piloter l'ensemble des actions menées.

Pour qui ? Collectivités territoriales et organismes au service du citoyen ayant *a minima* un service informatique, interlocuteur indispensable au déploiement du plan de relance.

Niveau de cybersécurité ? Des parcours pour tous : **Fondation** / **Intermédiaire** / **Avancé** / **Renforcé**.

Appels à projet

Quoi ? Co-financement de projets de sécurisation de systèmes d'information existants, s'intégrant dans une stratégie globale de cybersécurité et de transformation numérique du bénéficiaire.

Pour qui ? Ministères et certaines collectivités territoriales.

Niveau de cybersécurité ? **Avancé** / **Renforcé**.

Le dispositif a démarré en avril 2021. Avec une centaine de bénéficiaires. Il est question d'en ajouter autant tous les trimestres jusqu'à fin 2022.

** Les CSIRT référenceront les prestataires labellisés par l'ANSSI et/ou par Cybermalveillance.gouv.fr (« ExpertCyber »).*

Illustration principale © Per Bengtsson – Shutterstock