Des outils pour faire face à différents types de cyberattaque

Créé en septembre 2022, le Groupe de Travail « Gestion de Crise et Entraînement » mené par l'ANSSI publie régulièrement des ressources pour aider les organisations à améliorer leurs pratiques et leurs dispositifs, gérer efficacement les crises et maintenir l'activité face aux cybermenaces. Dernier outil en date : des fiches scénarios d'exercices accessibles à toutes les entreprises. Elles visent différentes typologies d'attaque : rançongiciel, supply chain, DDoS, défacement, exfiltration, systèmes industriels – OT… et donnent, pour chacune, des conseils et des points critiques à évaluer pour réussir la mise en œuvre.

S'appuyer sur des outils méthodologiques

Le groupe de travail met également à disposition des fiches pratiques pour permettre aux entreprises de s'appuyer sur des outils méthodologiques. Une fiche est ainsi consacrée aux rôles et fonctions en cas de crise d'origine cyber, qui aborde notamment la répartition claire des missions de chaque collaborateur en cas d'attaque. Une autre traite des enjeux relatifs aux technologies Cloud durant les crises cyber, par exemple son rôle de solution de rétablissement, si la sécurité

est intégrée dans le déploiement.

Pour en savoir plus : https://wiki.campuscyber.fr/Crise_cyber_et_entrainement_:_m%C3%A9thodologie_d%27entrainement#Livrables