

La pénurie de compétences en cybersécurité en Europe : la réponse complète de l'ENISA

Cybersécurité aujourd'hui

L'Europe fait face à une pénurie critique de compétences en cybersécurité : on estime entre 260 000 et 500 000 le nombre de postes vacants sur le continent. Ce déficit intervient à un moment où les menaces informatiques se multiplient et gagnent en sophistication. Par exemple, les attaques liées au vol de mots de passe ont augmenté de 74 % en 2022, tandis que les technologies émergentes, telles que l'IA et l'informatique quantique, créent des vulnérabilités inédites. Les enjeux sont majeurs : les incidents cyber perturbent déjà les services essentiels, les entreprises et les administrations, menaçant la souveraineté numérique et la stabilité économique de l'Europe.

Le cadre européen des compétences en cybersécurité

Pour répondre à cette crise, l'Agence de l'Union européenne pour la cybersécurité (ENISA) a mis en place une stratégie à multiples volets, centrée sur le Cadre européen des compétences en cybersécurité (ECSF). Ce référentiel standardise douze rôles clés — des spécialistes de la réponse aux incidents aux juristes en cybersécurité — et a été adopté par plus de 20 États membres de l'UE. En alignant les programmes académiques sur les besoins de l'industrie — via des partenariats avec plus de 40 universités — l'ENISA veille à ce que la formation soit en adéquation avec les exigences du terrain. Par ailleurs, des initiatives sectorielles ciblées abordent les domaines à haut risque : les établissements de santé reçoivent des formations contre le ransomware, les fournisseurs d'énergie se concentrent sur la sécurité des réseaux intelligents, et des collaborations avec l'Agence spatiale européenne (ESA) visent à protéger les systèmes satellitaires.

Effectifs en cybersécurité

Pour l'avenir, l'ENISA priorise une expansion rapide et inclusive des effectifs. Les principales initiatives prévues pour 2024 sont :

- l'extension des exercices Cyber Europe, qui forment actuellement plus de 1 200 professionnels par an ;
- l'application d'exigences de cartographie des compétences pour les secteurs régulés par la directive NIS2 ;
- la lutte contre les disparités de genre (les femmes ne représentent que 19 % des spécialistes TIC) ;
- le lancement de programmes spécialisés en sécurité de l'IA et en cryptographie résistante au calcul quantique.

Cependant, l'ENISA souligne que pour combler cet écart de compétences, une collaboration sans précédent est nécessaire. L'agence plaide pour la création d'un Fonds européen pour l'éducation à la cybersécurité (200 millions d'euros) afin de subventionner la formation, la mise en place de ratios de personnel obligatoires dans les infrastructures critiques et la délivrance accélérée de visas aux talents internationaux du secteur cyber. Sans ces mesures, l'Europe risque de prendre du retard dans la course mondiale à la résilience numérique.