# « L'expérience est une bonne école. Mais elle a un prix »[1].
# L'ENISA encourage les décideurs à prendre des mesures avant qu'une cyber-crise majeure ne se produise en Europe

***L'ENISA a analysé les mécanismes de gestion de crises au niveau européen dans cinq secteurs différents afin de formuler des recommandations en vue de renforcer l'efficacité de la coopération et de la gestion de cyber-crises. Le rapport issu de cette étude souligne les enseignements qui peuvent être tirés d'autres secteurs et appliqués dans le domaine cybernétique. Pour conclure, l'étude propose une série de recommandations concernant les priorités au niveau de l'UE afin de modifier l'impact d'une potentielle cyber-crise. L'ENISA a récemment publié une vidéo liée à cette étude qui résume les conclusions basées sur les témoignages d'experts issus d'autres secteurs.***

Cette étude de l'ENISA fournit un aperçu de l'état actuel de la gestion de crises au niveau de l'UE et offre une analyse (de la perspective d'une cyber-crise) des nombreux enseignements tirés et des défis rencontrés au cours des décennies de gestion de crises dans les secteurs suivants : **l'aviation, la protection civile, la surveillance des frontières, le contre-terrorisme** et **le contrôle de la santé et des maladies**. L'étude va même plus loin en proposant **cinq recommandations clés** pour améliorer **la gestion de cyber-crises au niveau de l'UE**. Cette étude se base sur un examen approfondi des documents juridiques et politiques clés ainsi que sur des entrevues avec des experts issus des secteurs cités.

À l'heure actuelle, la gestion de cyber-crises au niveau de l'UE manque de mécanismes appropriés et d'uniformité pour aider efficacement la cybercommunauté européenne en cas de crise cybernétique, et ce malgré les récentes initiatives prises par la communauté NIS.

***« Le message que nous voulons transmettre par le biais de cette étude est que l'atténuation effective de tout type de crise causée par des incidents cybernétiques ne dépend pas seulement de l'atténuation des conséquences de cette crise. Cela dépend également et surtout de l'atténuation effective des incidents cybernétiques qui sont à l'origine de la crise. À l'heure actuelle, les décideurs européens sont dans une position privilégiée pour prendre des mesures avant qu'une telle cyber-crise ne se produise ; cette étude donne un aperçu des mesures qui peuvent être prises »* a expliqué Udo Helmbrecht, le Directeur exécutif de l'ENISA.**

Les cinq recommandations clés présentées par l'ENISA au sujet des priorités quant au renforcement des capacités au niveau de l'UE afin de gérer de manière efficace la prochaine cyber-crise sont les suivantes :

- La Commission européenne et les États membres de l'UE devraient revoir la législation européenne actuelle en matière de gestion de cyber-crises afin de mieux **distinguer la différence entre cause et conséquence** et d'avoir une plus grande influence sur le développement du domaine de la gestion de cyber-crises en tant qu'outil essentiel pour l'atténuation des crises causées par les incidents cybernétiques.
- Les États membres de l'UE devraient élaborer et adopter un **plan de gestion de crises au niveau européen** spécifique aux crises causées par des incidents cybernétiques.

[1] Heinrich Heine

- La Commission européenne et les États membres de l'UE devraient créer un **groupe de cyber-experts** européens dont l'objectif principal serait l'échange d'informations et de meilleures pratiques.
- Les États membres devraient élaborer et adopter des **procédures opérationnelles standard** (POS) au niveau de l'UE dans le domaine cybernétique.
- La Commission européenne devrait financer **la conception et la réalisation d'une plateforme de coopération en matière de cyber-crises au niveau de l'UE** afin de soutenir les activités de coopération et de gestion de cyber-crises entre les États membres, en lien avec la plateforme de service principale de l'infrastructure de services numériques de cybersécurité (du programme de financement des infrastructures transeuropéennes Connecting Europe Facility).
  L'ENISA s'engage à soutenir entièrement la Commission européenne et les États membres de l'UE dans la mise en œuvre de ces recommandations.

Avant de lire le rapport, afin d'avoir un aperçu de l'enjeu, regardez la vidéo introductive présentant des experts européens en matière de gestion de crises issus du SEAE, de Eurocontrol et de l'ACI.

**Notes aux éditeurs :** L'ENISA soutient le domaine de la gestion européenne de cyber-crises depuis de nombreuses années avec des activités allant de la simulation de crises à des entraînements, aidant ainsi les États membres de l'UE à développer leurs plans et structures de crise en organisant des conférences internationales et en publiant des rapports tels que celui-ci.

**Regarder** la **vidéo**
Le **sommaire exécutif** est disponible **ici**
Le **rapport complet** est disponible **ici**
**Pour toutes les informations techniques sur le sujet,** veuillez contacter l'équipe de coopération en charge des cyber-crises à l'adresse suivante **c3@enisa.europa.eu**

**Pour les demandes de presse,** veuillez contacter **press@enisa.europa.eu** , **Tél :** +30 2814 409 576