

Réponse de l'ENISA au (projet de) rapport spécial de la Cour des comptes intitulé «Détecter les incidents de cybersécurité et y répondre»

Réponse de l'ENISA à la recommandation n° 1:

L'ENISA accepte cette recommandation et s'engage à soutenir la Commission dans la mise en œuvre des mesures recommandées, étant entendu que ces tâches supplémentaires seront intégrées dans le mandat révisé de l'ENISA (et en particulier dans son document de programmation annuel) et bénéficieront par la suite de ressources humaines et financières adéquates.

En outre, l'ENISA tient également à souligner qu'elle est responsable de la plateforme unique de signalement établie dans le cadre du règlement sur la résilience en matière de cybersécurité et qu'elle développe actuellement cette plateforme. À l'avenir, l'Agence pourrait être chargée du développement de la plateforme d'entrée unique conformément à la «proposition omnibus sur le numérique de 2025». Par ailleurs, l'Agence a également joué un rôle de soutien auprès des États membres en matière de notification des incidents dans le cadre de la directive NIS2. L'Agence se félicite de ces missions législatives, qui s'inscrivent dans le cadre de son rôle consistant à soutenir les États membres et à faciliter le partage d'informations au sein du cadre européen de cybersécurité. L'ENISA ne dispose actuellement d'aucun mandat ni d'aucune compétence légale pour répondre aux incidents de cybersécurité, cette compétence relevant des agences nationales de cybersécurité ou des autorités locales compétentes.

Réponse de l'ENISA à la recommandation n° 2:

L'ENISA accepte cette recommandation, tout en précisant que les responsabilités de chaque partie et les ressources allouées devront faire l'objet d'un accord explicite.

Réponse de l'ENISA à la recommandation n° 3:

L'ENISA accepte cette recommandation. En outre, alors que le règlement sur la cybersolidarité vise à renforcer la solidarité transfrontière, en veillant à ce que les nations de l'UE puissent se prêter mutuellement assistance en cas d'incidents de cybersécurité majeurs, il importe de souligner que ce cadre législatif n'établit pas clairement la nature et la portée de la coopération entre les cyberpôles transfrontières et l'ENISA. Bien que les normes d'interopérabilité soient essentielles pour garantir un partage efficace des informations entre les cyberpôles transfrontières, la restriction imposée à l'ENISA de ne pas faire partie du réseau des cyberpôles transfrontières entrave considérablement l'efficacité de ce partage. Par conséquent, l'ENISA ne reçoit ni n'échange d'informations provenant de ce réseau et sa contribution au renforcement de la solidarité transfrontalière est limitée. Afin que l'ENISA puisse faciliter efficacement ce partage d'informations au niveau de l'Union européenne, il convient donc de modifier le cadre réglementaire actuel.

Réponse de l'ENISA à l'encadré 1. - Page 17

L'ENISA tient à préciser qu'en l'absence persistante d'une définition et/ou de lignes directrices communes concernant la notion d'«incident significatif», aucun État membre n'a considéré cet incident comme étant significatif ou comme un incident transfrontière de cybersécurité majeur. Ce cas montre qu'il est nécessaire de s'accorder sur ce qui constitue un «incident significatif» et, par la suite, de soutenir la gestion coordonnée de tels incidents.