Antwort der ENISA auf den Sonderbericht (Entwurf) des Rechnungshofes „Erkennung und Reaktion auf Cybersicherheitsvorfälle“

Antwort der ENISA auf Empfehlung 1:

Die ENISA nimmt diese Empfehlung an und wird die Kommission bei der Umsetzung der empfohlenen Maßnahmen unterstützen, wobei davon ausgegangen wird, dass diese zusätzlichen Aufgaben in das überarbeitete Mandat der ENISA (und insbesondere in ihr jährliches Programmplanungsdokument) aufgenommen und anschließend durch angemessene personelle und finanzielle Ressourcen unterstützt werden.

Darüber hinaus möchte die ENISA darauf hinweisen, dass sie für die Entwicklung der im Rechtsakt über die Widerstandsfähigkeit im Bereich der Cybersicherheit vorgesehenen einheitlichen Meldeplattform verantwortlich ist und diese derzeit entwickelt. In Zukunft könnte die Agentur möglicherweise mit der Entwicklung der zentralen Zugangsplattform gemäß dem „Digital-Omnibus-Vorschlag 2025“ beauftragt werden. Darüber hinaus hat die Agentur die Mitgliedstaaten auch bei der Meldung von Vorfällen im Rahmen der NIS-2-Richtlinie unterstützt. Diese legislativen Aufgaben werden von der Agentur im Rahmen ihrer Rolle begrüßt, die darin besteht, die Mitgliedstaaten zu unterstützen und den Informationsaustausch im Rahmen der europäischen Cybersicherheit zu erleichtern. Die ENISA verfügt derzeit weder über ein Mandat noch über eine rechtliche Befugnis, direkt auf Vorfälle zu reagieren, da diese Zuständigkeit bei den nationalen Cybersicherheitsbehörden bzw. den zuständigen lokalen Behörden liegt.

Antwort der ENISA auf Empfehlung 2:

Die ENISA nimmt diese Empfehlung an, wobei sie davon ausgeht, dass die Zuständigkeiten der einzelnen Beteiligten und die zugewiesenen Ressourcen ausdrücklich vereinbart werden müssen.

Antwort der ENISA auf Empfehlung 3:

Die ENISA nimmt diese Empfehlung an. Während die Cybersolidaritätsverordnung darauf abzielt, die grenzüberschreitende Solidarität zu stärken und sicherzustellen, dass sich die EU-Staaten bei Cybersicherheitsvorfällen großen Ausmaßes gegenseitig unterstützen können, ist es wichtig, darauf hinzuweisen, dass in diesem Rechtsrahmen Art und Umfang der Zusammenarbeit zwischen den grenzübergreifenden Cyber-Hubs und der ENISA nicht eindeutig festgelegt sind. Zwar ist die Bedeutung von Interoperabilitätsstandards für einen effektiven Informationsaustausch zwischen grenzübergreifenden Cyber-Hubs unbestritten, doch schränkt die Nichtbeteiligung der ENISA am Netz der grenzübergreifenden Cyber-Hubs diesen Austausch erheblich ein. Die ENISA erhält daher keine Informationen aus diesem Netzwerk und tauscht darüber auch keine Informationen aus. Folglich sind ihre Möglichkeiten, einen Mehrwert zur Stärkung der grenzüberschreitenden Solidarität zu erbringen, begrenzt. Damit die ENISA diesen Informationsaustausch auf EU-Ebene effizient erleichtern kann, sollte der bestehende Rechtsrahmen geändert werden.

Antwort der ENISA auf Kasten 1. - S. 17

Die ENISA möchte klarstellen, dass dieser Vorfall in Ermangelung einer vereinbarten Definition und/oder Leitlinien für einen „schwerwiegenden Sicherheitsvorfall“ von keinem Mitgliedstaat als ein schwerwiegender Sicherheitsvorfall oder als Sicherheitsvorfall großen Ausmaßes eingestuft wurde. Dieser Fall verdeutlicht, wie wichtig es ist, ein gemeinsames Verständnis davon zu entwickeln, worin ein „schwerwiegenden Vorfall“ besteht, und anschließend das koordinierte Management des Vorfalls zu unterstützen.