Deutlicher Anstieg von Cyber-Bedrohungen bei kritischen Services und Infrastrukturen verlangt eine verbesserte Zusammenarbeit zwischen privaten und öffentlichen Sektoren

Mit der Studie zu kritischen Informationsinfrastrukturen (CIIs) analysiert die ENISA aktuelle CIIP-Praktiken und Governance-Modelle, die in den EU-Mitgliedstaaten eingesetzt werden. Diese Studie trägt zur Verbreitung und künftigen Umsetzung der NIS-Richtlinie bei.

Bürger und Unternehmen sind für die Unterstützung online-kritischer Dienstleistungen (z.B. Energie, Telekommunikation, Gesundheit) von der Informations- und Kommunikationsinfrastruktur abhängig. Der Anstieg von Cyber-Bedrohungen kann die Bereitstellung von Dienstleistungen erheblich beeinträchtigen und finanzielle Verluste sowie eine Beschädigung der Reputation von Unternehmen zur Folge haben.

Die EU-Mitgliedstaaten ebenso wie der private Sektor müssen zusammenarbeiten, wenn sie diese Bedrohungen heute effektiv angehen möchten. Doch nur die Hälfte der untersuchten Länder hat solche Modelle der Zusammenarbeit als öffentlich-private Partnerschaften, Arbeitsgruppen und Kontaktforen eingerichtet.

Da einige Sektoren wie Finanzen, Telekommunikation und Energie strenger reguliert sind als andere, unterscheiden sich die Sicherheitsanforderungen zwischen den Sektoren und für verschiedene Arten von CII-Betreibern erheblich. Nur eine kleine Anzahl von Ländern hat in allen Sektoren verpflichtende Sicherheitsanforderungen eingeführt.

Die Studie zeigt, dass wenige Länder, insbesondere solche mit einem stärker dezentralisierten CIIP-Ansatz, ihre nationalen Risikobeurteilungen an sektorspezifische Behörden oder Betreiber von CIIs delegieren. Einige Länder sind der Ansicht, dass der Marktdruck den CII-Betreibern ausreichend Anreize bietet, um in zusätzliche Sicherheitsmaßnahmen zu investieren. Jedoch hat fast keiner der untersuchten Mitgliedstaaten Anreize für Betreiber von CII geschaffen, damit sie in CIIP-verbundene Sicherheitsmaßnahmen investieren.

Nach der Validierung der Studienergebnisse schlägt die ENISA den Mitgliedstaaten und der EU-Kommission Folgendes vor:

- Durchführung einer gründlichen nationalen Risikobeurteilung
- Einführung einer Zusammenarbeit zwischen öffentlichen und privaten Sektoren
- Definition grundlegender Sicherheitsanforderungen, um die Entwicklung von CIIP in den Mitgliedstaaten zu unterstützen
- Schaffung von Anreizen, die CII-Betreiber dazu bewegen könnten, stärker in Sicherheitsmaßnahmen zu investieren

Udo Helmbrecht, geschäftsführender Direktor der ENISA, erklärt: *„Neue Bedrohungen für kritische Informationsinfrastrukturen stellen eine eindeutige und unmittelbare Gefahr dar. Eine Gefahr, der nur durch koordinierte Anstrengungen begegnet werden kann. ENISA arbeitet mit dem öffentlichen sowie dem privaten Sektor zusammen, um sicherzustellen, dass CIIP auf EU-Ebene Priorität einräumt.“*

ENISA unterstützt die EU-Mitgliedstaaten mit Beratung, Empfehlungen und praktischer Hilfe bei der Umsetzung der maßgeblichen EU-Gesetzgebung. Die Agentur bindet Anspruchsgruppen und die Industrie in den Austausch von Good Practices, Informationen und Ideen im Hinblick auf die Verbesserung von CIIP in Europa ein.

Angesichts der bevorstehenden Umsetzung der NIS-Richtlinie und basierend auf den Ergebnissen dieses Berichts

wird die ENISA weiterhin im Bereich CIIP tätig sein und dabei öffentliche und private Sektoren einbeziehen, um grundlegende Sicherheitsanforderungen und einen harmonisierten Ansatz zum Incident Reporting zu definieren.

Gesamter Bericht: Mehr Erkenntnisse und zusätzliche Informationen über die Studie
Für technische Informationen: Anna Sarri, Officer in NIS, Anna.sarri@enisa.europa.eu
Für Interviews und Presseanfragen wenden Sie sich bitte an **press@enisa.europa.eu, Tel:** +30 2814 409576