LËTZ PREPARE! STRATÉGIE NATIONALE DE RÉSILIENCE

SÄULE 6

Die Cyberresilienz

Wir sind in unserem Alltagsleben, unserer Wirtschaft und unseren Institutionen zunehmend von digitalen Technologien abhängig. Um die Stabilität des Landes und das Vertrauen seiner Bürger zu gewährleisten, müssen wir nicht nur in der Lage sein, Cyberangriffe zu verhindern, sondern ihnen auch standhalten, uns von ihnen erholen und uns an sie anpassen können. Angesichts immer komplexerer Bedrohungen, die von staatlichen und nichtstaatlichen Akteuren ausgehen, ist für die Cyberresilienz ein systemischer und koordinierter Ansatz erforderlich: Eine wirksame Governance, eine Kultur des Krisenmanagements und der Kommunikation sowie der Zugang zu technischen Ressourcen sind essenziell, um unsere Netzwerke und Informationssysteme zu schützen und zu verteidigen.

Ziel: Die Cyberresilienz-Fähigkeiten Luxemburgs zu stärken.

Kernmaßnahmen

SCHÜTZEND
Gemeinsam die Zukunft sichern

Um dieses Ziel zu verfolgen, werden verschiedene Maßnahmen umgesetzt, darunter:

Um die nationale Governance und strategische Koordinierung zu steigern:

- Wir überarbeiten die nationale Strategie zur Cybersicherheit, um das öffentliche Vertrauen in die digitale Welt zu steigern, die Menschenrechte im Internet zu schützen, die Sicherheit und Resilienz digitaler Infrastrukturen zu erhöhen und zur Entwicklung einer zuverlässigen, nachhaltigen und sicheren digitalen Wirtschaft beizutragen.
- Wir bauen die Führungsstruktur und Koordinierung des nationalen Cybersicherheits-Ökosystems aus, um die Steuerung und Harmonisierung der Cybersicherheitsbemühungen auf nationaler Ebene zu optimieren, indem wir die für Cybersicherheit und Cyberabwehr zuständigen öffentlichen Institutionen und Behörden sowie Kritische Einrichtungen, Unternehmen und Bürger einbeziehen.

Um die operativen Kapazitäten zu erweitern:

- Wir schützen kritische Informationssysteme, indem wir die operativen Kapazitäten verbessern, fortschrittliche Erkennungskapazitäten implementieren, ein gemeinsames Lagebewusstsein entwickeln, Frühwarnungen herausgeben und systematisch verwertbare Informationen über Bedrohungen, Angriffe und das versuchte Eindringen in Systeme austauschen sowie mit den zuständigen nationalen Akteuren zusammenarbeiten, um das Niveau der Vorbereitung auf die Bewältigung schwerwiegender Vorfälle und Cyberkrisen zu steigern.
- Wir steigern die zivil-militärische Zusammenarbeit durch integrierte Krisenmanagementsysteme, Informationsaustausch, die Entwicklung interoperabler Standards, gemeinsame Risikobewertungen und die Organisation gemeinsamer Übungen.
- Wir fördern Innovationen im Bereich der Cybersicherheit und beschleunigen den Einsatz luxemburgischer oder europäischer Lösungen durch Finanzierungs- oder Förderprogramme in den Bereichen Digitalisierung, Cybersicherheit, Quantencomputing und künstliche Intelligenz.

Aufbau von Expertise und Sensibilisierung:

- Wir bauen in Zusammenarbeit mit öffentlichen Forschungseinrichtungen weiterhin nationales Fachwissen im Bereich Cyberresilienz auf, indem wir ein hohes Maß an Fachkompetenz und unabhängiger Beherrschung von Fähigkeiten aufrechterhalten, Fachwissen in neuen Technologien und autonomen Tools für kleine und mittlere Unternehmen entwickeln und den Fachkräftemangel im Bereich Cybersicherheit angehen.
- Wir fördern Bildung, Ausbildung und Sensibilisierung im Bereich der Sicherheit von Informationssystemen durch die Schaffung spezifischer Programme in den Lehrplänen der Schulen sowie durch Informations- und Sensibilisierungskampagnen.
- Wir unterstützen regulierte Einrichtungen, insbesondere kleine und mittlere Unternehmen, durch die Entwicklung von Empfehlungen und Instrumenten.