EU-Agentur für Cyber-Sicherheit ENISA veröffentlicht Leitfaden zum Aufbau effektiver Public-Private-Partnerships (PPPs) für IT-Sicherheit

Die EU-Agentur für Cyber-Sicherheit ENISA veröffentlichte heute einen neuen Leitfaden mit 36 Empfehlungen für den erfolgreichen Aufbau effektiver Öffentlich-Privater Partnerschaften für stabile IT-Sicherheit.

Die wesentlichste Infrastruktur der meisten EU-Mitgliedsstaaten befindet sich im Besitz der Privatwirtschaft. Um Bürgern und Unternehmen einen sicheren und zuverlässigen Systemzugang zu ermöglichen, bedarf es daher der Zusammenarbeit von Industrie und Regierungen. Die kritischen Informations-Infrastrukturen (CII) in Europa sind fragmentisiert, sowohl geografisch als auch aufgrund des Wettbewerbs zwischen Telekommunikationsanbietern. Eine Steigerung der CII-Belastbarkeit ist daher für Europa von grundlegender Bedeutung. Um diesen Bedarf zu decken, haben sich in vielen Mitgliedsstaaten Public Private Partnerships (PPPs) zum Schutz der digitalen Wirtschaft gebildet – zu verschiedenen Zeiten und unter diversen rechtlichen Rahmenbedingungen. Diese natürliche Entwicklung zeigt, dass es keine allgemein gültige Definition zur Errichtung einer PPP gibt. In einer Welt, in der Bedrohungen der Infrastruktur nicht vor Landesgrenzen Halt machen, betont der neue PPP-Leitfaden der Europäischen Agentur für Netzwerk- und Informationssicherheit ENISA mit 36 Empfehlungen für den erfolgreichen Aufbau einer PPP die Wichtigkeit eines gemeinsamen Verständnisses innerhalb Europas. Von besonderer Bedeutung ist dies für die Europäische öffentlich-private Partnerschaft für Robustheit (EP3R), einer Initiative der Europäischen Union, die mit nationalen PPPs an Problemstellungen beim Schutz wichtiger Informationsinfrastrukturen (CIIP) zusammenarbeitet.

Professor Udo Helmbrecht, Geschäftsführende Direktor von ENISA, kommentiert: „*Es braucht ein wirklich internationales, weltweites Herangehen an Cyber-Sicherheit und den Schutz wichtiger Informationsinfrastrukturen. Kein Land kann eine isolierte CIIP-Strategie entwickeln, weil es im Cyberspace keine Grenzen gibt. Genau deswegen stehen PPPs auf der Tagesordnung der speziellen EU-US-Arbeitsgruppe für Cyber-Sicherheit und Cyber-Kriminalität.*“

PPP Klassifikationsschema

Der Leitfaden unterteilt PPPs für Sicherheit und Robustheit in drei Typen: **präventionsorientierte PPPs, reaktionsorientierte PPPs und Schirm-PPPs.** Der Leitfaden konsolidiert und bestätigt ein PPP-Klassifikationsschema und benennt fünf wesentliche Komponenten für Empfehlungen:

- **Warum sollte eine PPP geschaffen werden? (Umfang/Bedrohungen)**
- **Wer sollte daran beteiligt werden? (Anwendungsbereich, geografisch/inhaltlich, wechselseitige Anknüpfungspunkte)**
- **Wie sollte eine PPP verwaltet werden?**
- **Welche Dienste und Impulse sollten angeboten werden?**
- **Wann sollte eine PPP gegründet und wie sollten andere Terminfragen gelöst werden?**

Diese Ergebnisse wurden anhand von 30 Fragebögen und 15 ausführlichen Interviews mit Interessenvertretern des öffentlichen wie des privaten Sektors aus zwanzig Ländern ermittelt. Der Leitfaden beschreibt und lokalisiert außerdem PPPs aus den **USA, Kanada und Australien** und benennt damit entscheidende Erfolgsfaktoren für den Informationsaustausch und Wege zur internationalen Zusammenarbeit.

Für den kompletten Bericht

Hintergründe: Mitteilung der Europäischen Kommission zu CIIP und EP3R

Für Interviews: Ulf Bergstrom, Sprecher von ENISA, press@enisa.europa.eu, Mobil: + 30-6948-460-143, oder Lionel Dupre, Experte, ENISA, lionel.dupre@enisa.europa.eu

http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch

Übersetzung. Das Englische Original bleibt die maßgebliche Fassung.