Dr. Dennis-Kenji Kipker
IGMR
Universität Bremen

INFORMATIONSFLÜSSE UND SCHUTZPROZESSE IN DER IT-SICHERHEIT KRITISCHER INFRASTRUKTUREN

ITS KRITIS
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Bedrohungen für Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von IT

Gegenmaßnahmen

BETREIBER

Anwendbarkeit gem. §§ 2 Abs. 10, 10 Abs. 1 BSIG

§ 8a BSIG – Technisch-organisatorische Vorkehrungen (TOV) zur Sicherheit in der Informationstechnik von KRITIS

- ►Technischer Schutz der IT-Systeme, die für die Funktionsfähigkeit von KRITIS maßgeblich sind
- ►Maßnahmen entsprechen „Stand der Technik“
  - ISMS (ISO 27001)
  - B3S (UP KRITIS)
- ►Kosten-Nutzen-Kalkulation zur Angemessenheitsbeurteilung
- ►Nachweis durch Audits, Prüfungen und Zertifizierungen

PDCA
plan – do – check - act
BCM

Auswertung

Kontaktstelle BSI

Kontaktstelle Betreiber

ZUSAMMENSPIEL

BSI

ENISA
Zusammenarbeit/ Kooperation/ Informationsaustausch gem. EU NIS-RL

§ 8b BSIG – Meldepflichten und zentrale Stelle für die IT-Sicherheit von KRITIS

Einmeldungen der Betreiber an das BSI:

- ►Erhebliche Störungen der IT, die zu Ausfall/Beeinträchtigung der Funktionsfähigkeit von KRITIS führen können ODER geführt haben
- ►Angaben zu Störung, technischen Rahmenbedingungen, vermuteter/tatsächlicher Ursache, Art der betroffenen Einrichtung/Anlage und Branche des Betreibers
- ►Pseudonymisierte Meldung genügt grds., nur in Ausnahmefällen konkrete Namensnennung des Betreibers erforderlich

BSI als zentrale Stelle der IT-Sicherheit von KRITIS:

- ►Sammlung und Auswertung der Betreiberinformationen (z. T. zusammen mit BBK)
- ►Warn- und Alarmierungsmeldungen
- ►Aktualisierung Lagebild Informationssicherheit
- ►Informationen für Betreiber und Aufsichtsbehörden
- ►Langfristige Jahresberichte für die Öffentlichkeit

CYBER-SICHERHEITSSTRATEGIE DER BUNDESREGIERUNG

(BSIG ergänzt durch Spezialregelungen wie § 109 TKG, § 11 EnWG, § 44b AtG; Öffnungsklausel in § 8c Abs. 2 Nr. 5, Abs. 3 Nr. 5 BSIG, z. B. für Telematik im Gesundheitswesen)