Bundesamt
für Sicherheit in der
Informationstechnik

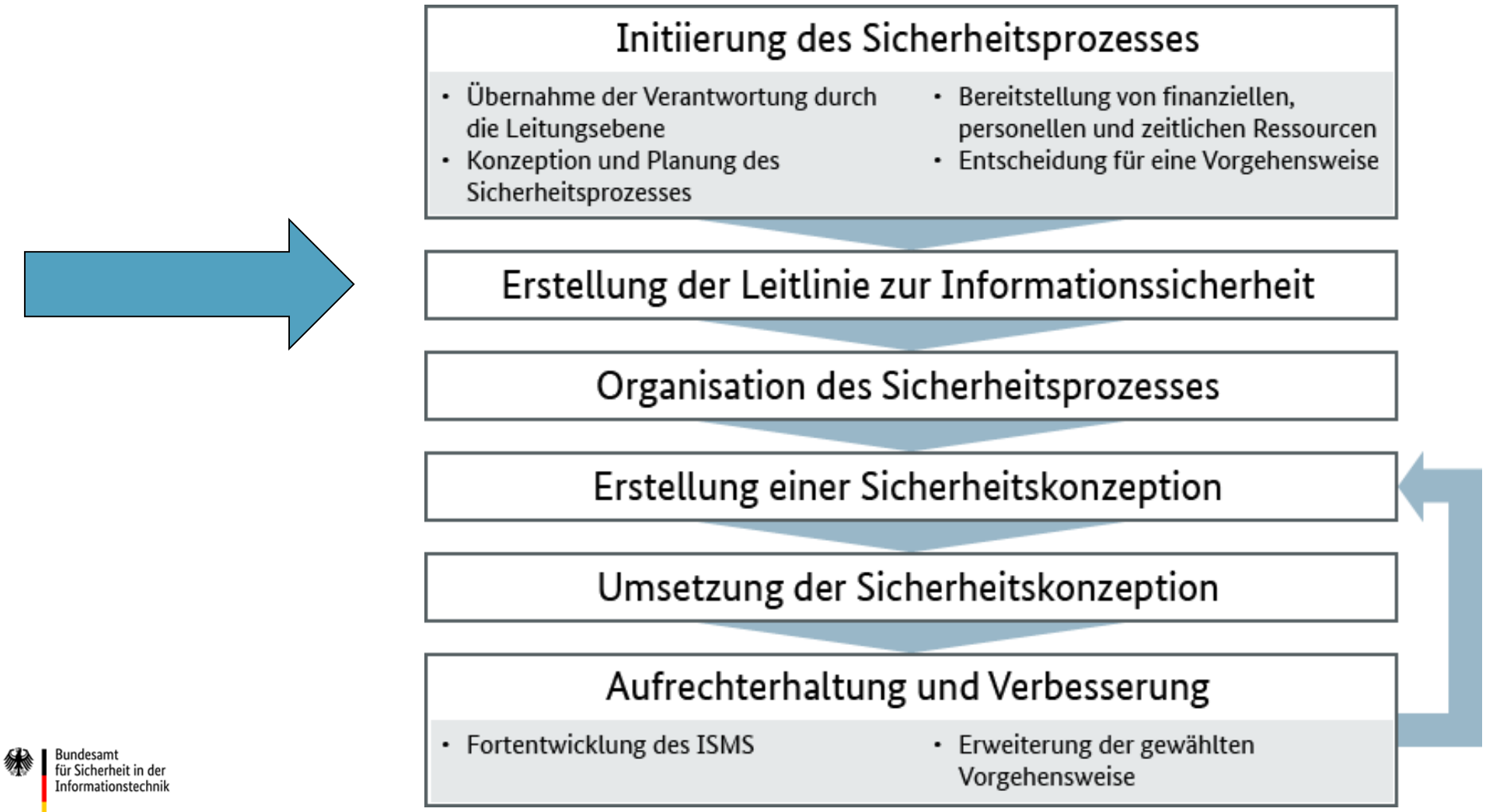
Deutschland
Digital•Sicher•BSI•

Herausforderung Gewährleistung eines einheitlichen Sicherheitsniveaus – Leitlinien für Informationssicherheit als Instrument

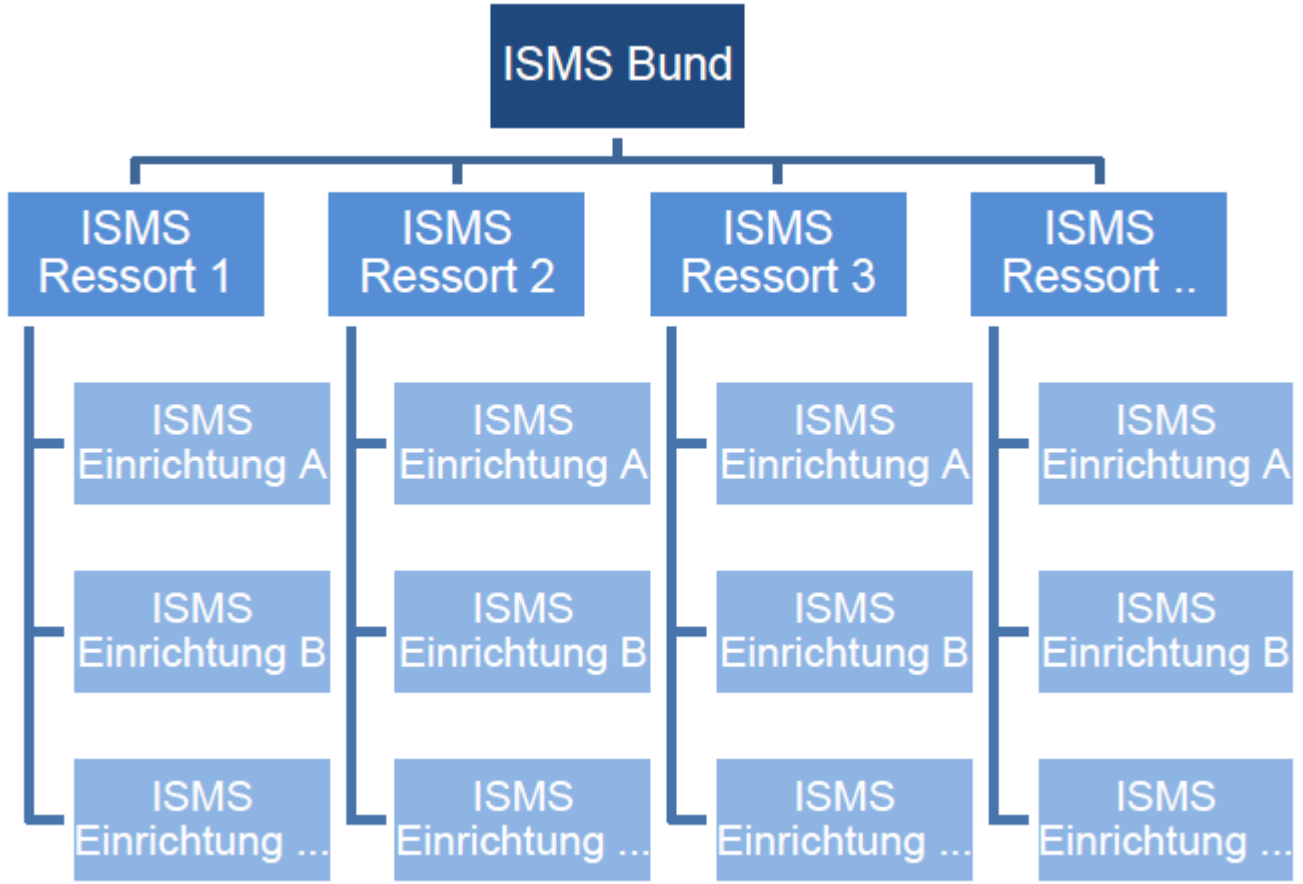
Stefanie Euler
Informationssicherheitsberatung für Länder und Kommunen
Bundesamt für Sicherheit in der Informationstechnik

EDV Gerichtstag , 24. September 2021

Die Leitlinie zur Informationssicherheit als Teil des Sicherheitsprozesses



ISMS im Bund – UP Bund



ISMS in den Bundesländern - Übergreifende Leitlinien (Beispiele)

Arbeitsgruppe Informationssicherheit des IT-PLR

Leitlinie für die Informationssicherheit

in der öffentlichen Verwaltung

- 2018 -

IT-Planungsrat

Stand 06.12.2018

Version 2.0

1 von 16

Ständige Konferenz der Innenminister und Senatoren der Länder

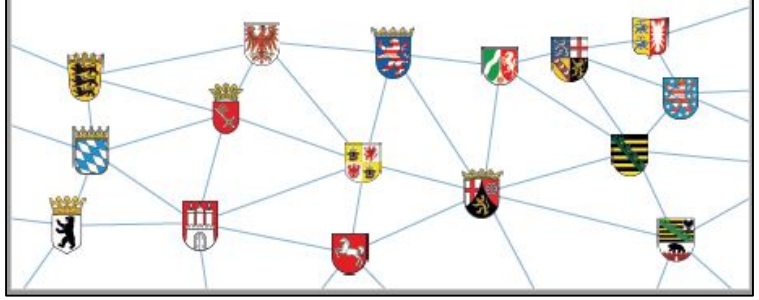
Länderarbeitsgruppe Cybersicherheit

Leitlinie zur Entwicklung föderaler Cybersicherheitsstrategien

Länderarbeitsgruppe Cybersicherheit der Innenministerkonferenz

Exposé

Die Leitlinie für Cybersicherheitsstrategien ist eine Empfehlung zum Aufbau und der Weiterentwicklung der Cybersicherheitsarchitektur in den Ländern und dient damit der Harmonisierung zwischen den Ländern. Durch Zusammenarbeit und fachlichen Austausch werden Interoperabilität und gemeinsame Innovationen gefördert.



Kommission IuK-Sicherheit

Leitlinie zur Informationssicherheit für den polizeilichen Informationsverbund Corporate Network Polizei – CNP

UA IuK

Leitlinie zur Informationssicherheit für den polizeilichen Informationsverbund Corporate Network Polizei – CNP

1. Bedeutung der polizeilichen IuK

Die Arbeit der Polizei ist eine der tragenden Säulen für die Gewährleistung der Inneren Sicherheit in der Bundesrepublik Deutschland. Informationen sind eine der zentralen Ressourcen für die Unterstützung in der polizeilichen Aufgabenwahrnehmung. Es ist deshalb essentiell für die Aufgabenerfüllung der Polizei, dass ihr diese Informationen stets ohne Verzug und unverfälscht überall dort, wo sie benötigt werden, zur Verfügung stehen, und dass ihre Informationen Unbefugten nicht zur Kenntnis gelangen. Im Einsatzfall sind polizeiliche Informationen Grundlage für den Schutz von Leib und Leben der am polizeilichen Handeln Beteiligten. Ohne funktionierende Informationsverarbeitung ist polizeiliche Arbeit und damit Gefahrenabwehr, Strafverfolgung und Kriminalitätsbekämpfung nicht zu leisten. Daher kommt dem Corporate Network Polizei (CNP) eine hohe Bedeutung zu.

Speziell in besonderen Lagefällen oder Großschadenslagen, wenn öffentliche Infrastrukturen möglicherweise durch Überlastung oder gezielte Angriffe nicht mehr zur Verfügung stehen, ist ein funktionierender polizeilicher Informationsverbund, der möglichst autark an lagebedingte Anforderungen angepasst werden kann, von großer Bedeutung.

Bei einem Ausfall oder einer gravierenden Beeinträchtigung der Informationsverarbeitung bzw. der für sie genutzten Kommunikationsinfrastruktur der Polizei können erhebliche Störungen der öffentlichen Sicherheit eintreten.

Darüber hinaus unterliegt die polizeiliche Informationsverarbeitung den gesetzlichen Vorgaben aus der EU-DSGVO sowie den Datenschutzgesetzen des Bundes und der Länder.

2. Zweck und Ziel der Leitlinie

Diese Leitlinie zur Informationssicherheit regelt die Voraussetzungen für die Teilnahme der Polizeien von Bund und Ländern am Corporate Network Polizei (CNP) und bildet die Grundlage für die Anbindung und den Zugriff von nicht polizeilichen Dritten, wie z. B. Staatsanwaltschaften, Meldebehörden, Ausländerämtern.

Verantwortlich für die Umsetzung der Leitlinie sind die Verbundteilnehmer in ihrem jeweiligen Zuständigkeitsbereich.

Die polizeilichen Verbundteilnehmer verpflichten sich auf die Einhaltung und Umsetzung der BSI-Standards und die regelmäßige, gegenseitige, im Verbund abgestimmte Überprüfung (IT-Grundschutzaudit bzw. IS-Revision) der getroffenen Maßnahmen des IT-Grundschutzes.

Die Einhaltung eines einheitlichen und hohen Mindest-Sicherheitsniveaus ist vor allem unter dem Aspekt unabdingbar, dass das Sicherheitsniveau im Netzverbund der Oberen Netzebene (ON) und aller Unteren Netzebenen (UN) im CNP nur so hoch ist wie das niedrigste der beteiligten Netze.

1

Informationssicherheitsleitlinie der öffentlichen Verwaltung

Handlungsfeld	Umsetzungsplanung (Kennzahlen, Zeitplan, Kosten)
Informationssicherheitsmanagement	z.B. Festlegung und Dokumentation von Verantwortlichkeiten im ISM und der Abläufe bei der Bewältigung von Vorfällen, verbindliche Leit- und Richtlinien, flächendeckende Erstellung von SiKos, Aus- und Weiterbildung, Sensibilisierung
Absicherung IT-Netzinfrastruktur öffentliche Verwaltung	z.B. Einhaltung der Anschlussbedingungen durch Bund und Länder
Einheitliches Sicherheitsniveau für Ebenen übergreifende IT-Verfahren	z.B. Erfassung aller Ebenen übergreifenden Verfahren, Anwendung des IT-Grundschutz und der Mindeststandards des BSI
Gemeinsame Abwehr von IT-Angriffen	z.B. Erarbeitung eines gemeinsamen, verbindlichen Mindeststandard CERT, Weiterentwicklung der Zusammenarbeit, Standards zur gemeinsamen Erkennung und Abwehr von IT-Angriffen
IT-Notfallmanagement (2013: Standardisierung und Produktsicherheit)	z.B. Aufbau des IT-Notfallmanagements

Vielen Dank für Ihre Aufmerksamkeit

Kontakt

Stefanie Euler
Referat BL12 – Informationssicherheitsberatung für Länder und Kommunen
Stefanie.Euler@bsi.bund.de
Sicherheitsberatung-Regional@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik