Deutsche Stiftung für Recht und Informatik

# Homeland Security Act vs. BSIG

## Eine rechtsvergleichende Betrachtung der IT-Sicherheit kritischer Infrastrukturen in den USA und Deutschland

**Dirk Müllmann**

**Andreas Ebert**

**Loïc Reissner**

Kompetenzzentrum für Angewandte Sicherheitstechnologie
(„KASTEL“) - Karlsruher Institut für Technologie

Herbstakademie 2020

www.dsri.de

# Die USA als Cybersicherheitsvorbild für Europa?






# Die USA als Cybersicherheitsvorbild für Europa?

## US offers up to $10 million reward for info on foreign hackers interfering in upcoming election

By Allen Kim, CNN

Updated 1724 GMT (0124 HKT) August 6, 2020

THE HILL

## Officials warn of increasing cyber threats to critical infrastructure during pandemic

BY MAGGIE MILLER - 08/05/20 05:25 PM EDT

USA TODAY

## A game of 'cat and mouse': Hacking attacks on hospitals for patient data increase during coronavirus pandemic

Karen Weintraub | USA TODAY
Published 3:02 PM EDT Jul 13, 2020


3 AUGUST 2020 ANALYSIS

## Covid-19 pandemic: Russian hackers target UK, US and Canadian research

By Allie Nawrat SHARE

# USA: Begrifflichkeiten

kritische Infrastrukturen:

- Presidential Directive 21: 16 Sektoren
- relevant für Sicherheit, Wirtschaftssicherheit und öffentliche Gesundheit

Cybersicherheit:

- Definition im National Infrastructure Protection Plan (NIPP)
- Schutz vor Schaden an elektronischen Informationen und Kommunikationssystemen

leitende Behörde:

- Cybersecurity and Infrastructure Security Agency als Teil des Department of Homeland Security

# USA: Rechtlicher Rahmen

- kein Bundesgesetz, das einheitliche Pflichten festlegt
- bundesstaatliche und sektorspezifische Regelungen
- Cybersecurity State Coordinator Act
- Sector Specific Plans (SSP) als Ausprägung des NIPP

# USA: Rechtlicher Rahmen

- Framework for Improving Critical Infrastructure Cybersecurity (NCF)
- Freiwilligkeit als Leitmotiv
- National Cybersecurity and Communications Integration Center → Automated Indicator Sharing (AIS) Program
- Cybersecurity Information Sharing Act

# Rechtslage zur Cybersicherheit kritischer Infrastrukturen in Deutschland und Europa

## Verständnis kritischer Infrastrukturen und Cybersicherheit

- Mindeststandard in der EU durch NIS-Richtlinie
- Umsetzung in Deutschland im BSIG

**§ 2 II BSIG**: Sicherheit in der Informationstechnik

*Einhaltung bestimmter Sicherheitsstandards, mit der die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen durch Sicherheitsvorkehrungen in informationstechnischen Systemen, Komponenten oder Prozessen oder bei deren Anwendung sichergestellt wird.*

# Rechtslage zur Cybersicherheit kritischer Infrastrukturen in Deutschland und Europa

## Verständnis kritischer Infrastrukturen und Cybersicherheit

**§ 2 X BSIG**: Kritische Infrastrukturen

*Einrichtungen, Anlagen oder Teile davon, die:*

*1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*

*2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*

→ Keine öffentlichen Einrichtungen als solche!

# Rechtslage zur Cybersicherheit kritischer Infrastrukturen in Deutschland und Europa

## Verständnis kritischer Infrastrukturen und Cybersicherheit

Dreistufige Prüfung:

- Zugehörigkeit zu kritischer Dienstleistung
- Sektorspezifische Anlage
- Relevanz für Gemeinwesen

→ Kriterien und Schwellenwerte in KritisV und deren Anlagen

# Rechtslage zur Cybersicherheit kritischer Infrastrukturen in Deutschland und Europa

## Gesetzliche Regelungen

- § 8a I BSIG: Organisatorische und technische Vorkehrungen
  - Beachtung des Standes der Technik
  - Empfehlungen und Anforderungskatalog des BSI
  - § 8a II BSIG: ggf. sektorspezifische Standards

- § 8b IV BSIG: Meldepflicht bei Möglichkeit erheblicher Beeinträchtigungen von IT-Systemen
  - BSI als zentrale Meldestelle

# Rechtslage zur Cybersicherheit kritischer Infrastrukturen in Deutschland und Europa

## Gesetzliche Regelungen

- § 5a I BSIG: Notfallmaßnahmen durch BSI
  - § 5a II BSIG: „Angriff besonderer technischer Qualität“; „öffentliches Interesse“

- Bereichsspezifische Sonderregelungen
  - Energieversorgungsnetze, § 11 I a-c EnWG
  - Atomanlagen, AtG
  - Telematik im Gesundheitswesen, SGB V
  - Öff. Kommunikationsnetze, TKG

# Vergleich der Rechtslagen in den USA, Deutschland und Europa

- Regelungsebenen
- Verbindlichkeit
- Umfang der Definition „kritische Infrastruktur“
- Verständnis des Bergriffs Cybersicherheit

# Fazit

- Deutschland/EU fördern Verbindlichkeit und Einheitlichkeit durch Mindeststandards
- USA: Kompetenz der Bundesstaaten führt zu Flickenteppich; kein einheitliches Anforderungsprofil
- Anwendungsbereich der US-amerikanischen Regelungen deutlich weiter
- Institutionalisierung in DE/EU weiter; CISA als „zahnloser Tiger“
- Nachholbedarf bei EU-internem Austausch

# Wir freuen uns auf Ihre Fragen!

**Dirk Müllmann**
**Andreas Ebert**
**Loïc Reissner**


Kompetenzzentrum für Angewandte Sicherheitstechnologie (KASTEL) – Karlsruher Institut für Technologie

**dirk.muellmann@kit.edu**
**andreas.ebert@kit.edu**
**l.reissner@stud.uni-frankfurt.de**