

Panel

Supply Chain Cybersecurity & Open Source

Rechtliche Maßnahmen

Philipp Reusch | reuschlaw Legal Consultants

Steve Ritter | BSI

Christian Czychowski | NORDEMANN

Moderation: **Hendrik Schöttle** | Osborne Clarke

#bfoss22

Supply Chain Security & Open Source

Angriffspunkt für Cyberangriffe auf die Lieferkette immer häufiger auf vorgelagerten Stufen



- Vernetzung globaler Märkte führt zu **zunehmender Angriffsfläche und Risiken** für Cybersicherheit
- Zulieferer mit ggf. **geringerem Cybersicherheitsstandard**
- Supply Chain nur **so stark wie ihr "schwächstes Glied"**
- Steigender **Bedarf an Kontrolle** über Supply Chain Sicherheit
- Besonders **komplex bei Open Source** Bestandteilen

IT-Sicherheitsgesetz 2.0 als Lösung?

Pflichten beim Einsatz kritische Komponenten

- BSIG sieht nun in § 9b
 - **Anzeigepflichten**
 - Pflicht zur Abgabe einer **Garantieerklärung** und
 - **Untersagungsmöglichkeiten**für den Einsatz kritischer Komponenten vor
- Voraussetzung dafür ist, dass eine „**kritische Komponente**“ i.S.v. § 2 XIII BSIG vorliegt
 - In „kritischer Infrastruktur“ eingesetzt
 - Gefährdungspotenzial
 - Komponente oder Funktion auf Grund eines Gesetzes bestimmt
- Mögliche „**mittelbare**“ **Anwendung** auch darüber hinaus?

Bisher festgelegte kritische Komponenten/Funktionen:

Im Sektor Telekommunikation für öffentliche 5G-Mobilfunknetze, für

- Core network functions
- NFV management and network orchestration
- Management systems and supporting services
- Radio Access Network
- Transport and transmission functions
- Internetwork exchanges
- + Sicherheitsanforderungen der Bundesnetzagentur

Freiwillige oder vertragliche Anwendung der Voraussetzungen auch für andere Komponenten?

- Abgabe einer **Garantieerklärung** i.S.v. § 9b III BSIG
 - Sicherstellung, dass **keine gefährdenden technischen Eigenschaften** (§9b III)
 - Anzeige bei **sicherheitsrelevanten Änderungen**
 - Meldung von **erkannten Schwachstellen**
 - Einsatz eines **Informationssicherheitsmanagementsystems**
 - Erklärung zu bestimmten gesellschaftsrechtlichen **Einflussmöglichkeiten**
- Erfüllung der **erhöhten Sicherheitsanforderungen der Bundesnetzagentur** für Komponente/Funktionen mit erhöhtem Gefährdungspotenzial (z.B. bisher für öffentliche Telekommunikationsnetze und -dienste)
- **Zertifizierung** gem. TR-03163 des BSI

Besonderheiten bei OS-Komponenten

- idR keine Rückgriffmöglichkeiten bzw. Haftungsausschluss
- Dezentrale Entwicklung
- Begrenzte Kenntnisse über Hersteller / Hintergründe

Herzlichen Dank!

steve.ritter@bsi.Bund.de

p.reusch@reuschlaw.de

christian.czychowski@nordemann.de



Steve Ritter

Referatsleiter für IT-Sicherheit
und Recht im BSI

Bundesamt für Sicherheit in
der Informationstechnik



Philipp Reusch

Founding Partner | Rechtsanwalt |
Head of Regulatory Affairs &
Marktmaßnahmen | Lehrbeauf-
tragter für Produkthaftung und
Produktsicherheit an der RWTH
Aachen

reuschlaw Legal Consultants



Christian Czychowski

Partner | Rechtsanwalt |
Fachanwalt für Urheber- und
Medienrecht | Fachanwalt für
IT-Recht

NORDEMANN