Regulierte IT-Sicherheit nach NIS-2 und BSIG

Wie Recht der Wirtschaft auf öffentliche Träger und kommunale IT-Dienstleister anzuwenden ist

Dr. iur. Julian Zaudig

Doktor der Rechte, Magister iuris (Universität zu Köln)

Vortrag für den KDN am 04.06.2024.

Inhalt

1. **Wer** ist reguliert?
   Der Adressatenkreis
2. Der Normbefehl der IT-SiG.
   Was regeln BSIG und NIS-2 und was nicht?
3. **Wie?** Die Umsetzung in der Praxis.
   Best Practices und organisatorische Anforderungen

Sektion 1

Wer ist reguliert?

Der Adressatenkreis

Kommunen sind bisher nicht reguliert. Reguliert ist aber, was outsourced ist.

- Die IT-Sicherheitsgesetze sind Bundesgesetze und ergingen als "Recht der Wirtschaft" (Art. 74 Abs. 1 Nr.11 GG).

  Dies bedeutet, dass sie Kommunen nicht verpflichten können (Art. 84 Abs. 1 S. 7 GG).

- Landessicherheitsgesetze existieren noch nicht.

  Insoweit einzelne Vorgaben für Fachverfahren existieren, sind diese an der Selbstverwaltungsfreiheit der Kommunen zu messen (Art. 28 Abs. 2 S. 1 GG).

- Dem Recht der Wirtschaft unterliegen aber kommunale Unternehmen.

  Eine Ausnahme hierfür gibt es nicht. Wortlaut und Telos der Norm tragen dies.

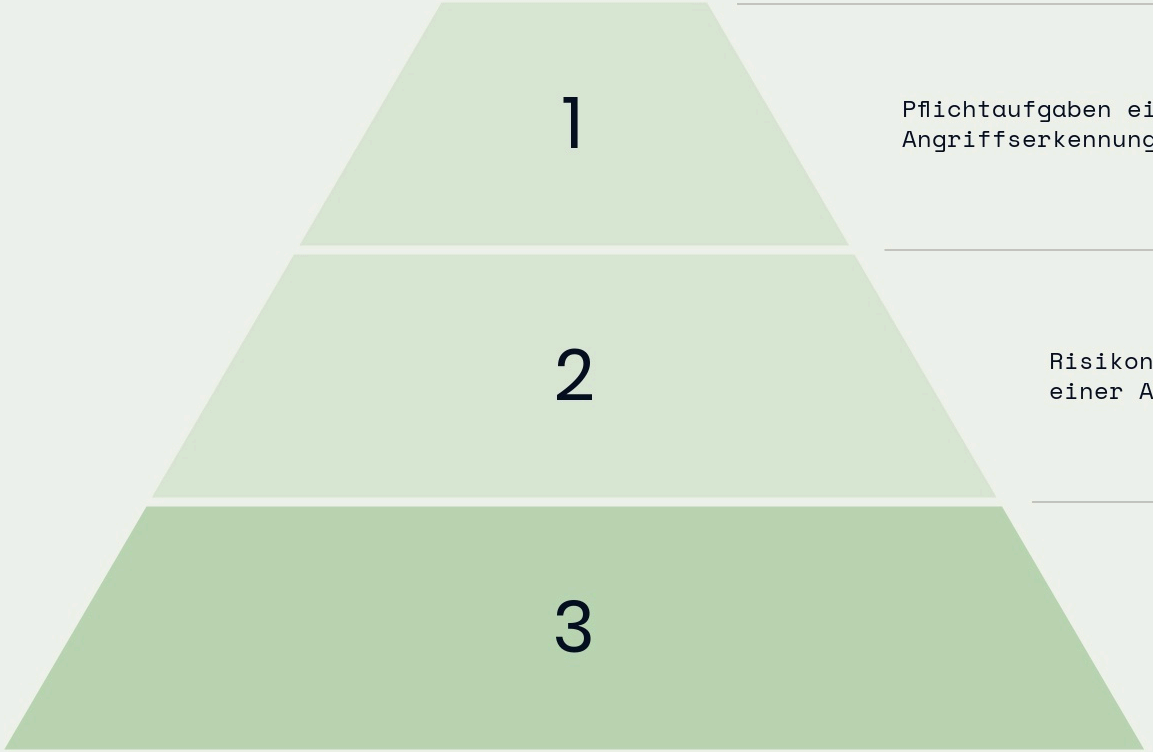
Aufgrund von NIS-2 **können** Kommunen den Sicherheitsgesetzen unterworfen werden.

Dies erfordert eine autonome Entscheidung des zuständigen (Landes-)Gesetzgebers. In dem Fall stellt sich die Frage: Wie wendet man "Recht der Wirtschaft" auf eine Kommune an?

Sektion 2

Der Normbefehl

Das BSIG regelt IT-Sicherheit nicht abschließend.



Pflichtaufgaben eines Betreibers, z. B. Angriffserkennungssystem.

Risikoneigung: "bestmögliche Verfügbarkeit" einer Anlage oder Dienstleistung.

Nicht geregelt: konkrete Sorgfaltsanforderungen.

Diese folgen aus allgemeinen Gesetzen, an welche angeknüpft wird, und sind rechtsformabhängig.

IT-Sicherheit soll nicht alleine in der betrieblichen Sphäre diskutiert werden.

Lehre aus dem Datenschutz: Sicherheit ist eine Rechtsfrage.

EuGH, Urt. v. 14.12.2023 – Az. C 340/21

1. **Sicherheitsmaßnahmen sind gerichtlich überprüfbar.**
   Zur Überprüfung steht das "richtige" Sicherheitsniveau (Rz. 43), die Umsetzung der Sicherheitsmaßnahmen und deren Wirksamkeit (Rz. 46).

2. **Es gibt einen "gewissen Entscheidungsspielraum" bei der Auswahl von Sicherheitsmaßnahmen.**
   Nach § 8a Abs. 1 S. 2 BSIG soll aber der Stand der Technik eingehalten werden.

3. **"Richtige" IT-Sicherheit ist keine Beweisfrage.**
   Die Einholung eines Sachverständigengutachtens ist nicht ausreichend (Rz. 64).

4. **Folgerung: IT-Sicherheit ist nun eine Frage der Legalitätspflicht. Organisatorisch ist sie eine Frage der Legalitätskontrolle.**

De lege ferenda: Die Risikoneigung in Kommunen muss nicht beeinflusst werden.

- Kommunen denken und planen langfristig. Dies ist auch gesetzlich erforderlich.

  "Die Gemeinde hat ihre Haushaltswirtschaft so zu planen und zu führen, dass die stetige Erfüllung ihrer Aufgaben gesichert ist." (§ 75 Abs. 1 S. 1 GO NRW).

- Beamte sind hieran gebunden.

  Die Beachtung des Haushaltsrechts ist Dienstpflicht (§ 36 Abs. 1 Satz 1 BeamtStG).

- Die Risikokultur des "Cowboys" gibt es im Kommunalrecht nicht.

  Deswegen muss sie auch nicht verboten werden.

De lege lata: Kommunale Unternehmen sind keine "Cowboys".

§ 109 Abs. 1 S. 1 GO NRW:

"Die Unternehmen und Einrichtungen sind so zu führen, zu steuern und zu kontrollieren, daß der öffentliche Zweck nachhaltig erfüllt wird."

- Der Grundsatz der Langfristigkeit gilt auch für kommunale Unternehmen.
- Dies verpflichtet den kommunalen Träger für Resilienz zu sorgen.

  Denn die Norm adressiert auch die Steuerung und Kontrolle kommunaler Unternehmen durch die Kommune.
- Die Entscheidungen binden die Organe des Unternehmensträgers.

  Dies wird als "innere Legalitätspflicht" bezeichnet und streng ausgelegt.

Sektion 3

Die Umsetzung in der Praxis

IT-Sicherheit ist kein erreichbarer **Zustand**, sondern verpflichtet auf einen Prozess.

Vorsicht vor der unbewussten (Fehl-)Entscheidung!

Auch keine Reaktion ist eine Managemententscheidung.

Und zwar im Zweifel für die (blinde) Hinnahme des Risikos.

IT-Sicherheit ist ein interdisziplinäres Thema.

1. **Die Risikoentscheidung und -organisation werden gerichtlich überprüft.**
   Beides muss also rechtlich begleitet werden, um dieser Prüfung gerecht zu werden.

2. **Nicht der Auditor entscheidet, sondern Sie.**
   IT-Sicherheit ist keine Tatfrage, ein Gericht darf sich nicht auf den Sachverständigen verlassen, also entbindet es auch sie nicht von einer eigenen (rechtlichen) Entscheidung.

3. **Jeder muss wissen, was gilt.**
   Anforderungen an IT-Sicherheit folgen in der Praxis auch weitgehend aus Verträgen. Diese müssen bekannt und harmonisiert sein, um verlässlich umgesetzt zu werden.

4. **Die rechtlichen Anforderungen an IT-Sicherheit folgen nicht den technischen Best Practices.**
   Best Practice im Bereich der IT-Sicherheit sind beispielsweise regelmäßige Audits. Compliance erfordert aber "stichprobenartige, überraschende Kontrollen".

BGH, Beschl. v. 24.03.1981 – Az. KRB 4/80.

Also?

Sie sollten Rücksprache halten, wenn…

- **…rechtliche Bindungen auf der Führungs- oder Arbeitsebene unbekannt sind.**
  Wer nicht weiß, was erforderlich ist, wird nicht rechtzeitig fragen und sich nicht gesetzestreu verhalten.

- **…IT-Sicherheit als technisches Thema verstanden wird.**
  Über 60% der Cyberangriffe nutzen Mängel in der Betriebsorganisation aus. Gegenmaßnahmen müssen auch organisatorisch funktionieren.

- **…die Sicherheitsorganisation unzureichend ausgestattet ist.**
  Hierzu zählt auch der Zugriff auf externen Sachverstand (BSI Standard 200-2, S. 50). Die reine Papierlage hilft im Ernstfall nicht weiter.

Proofpoint, Inc., Eine Studie unter IT-Sicherheitsverantwortlichen in Deutschland, Österreich und der Schweiz (DACH), 2020.

Sie müssen **wenigstens** die folgenden Fragen beantworten können:

1. Woher kennen Ihre Mitarbeiter die rechtlichen Anforderungen an die IT-Sicherheit ihrer konkreten Systeme?
2. Welche Systeme sind am gefährdetsten und wie hängen diese mit anderen zusammen?
3. Wer entscheidet im Falle eines Angriffs wie es weitergeht? Wie schnell geht das?
4. Woher wissen Sie, dass Ihre Maßnahmen und Pläne funktionieren?

Fangfrage: Welche Sicherheitsmaßnahme war Ihnen zuletzt zu teuer?

Der Aufwand einer Maßnahme steht ihr nämlich nur noch im Ausnahmefall entgegen. Sicherheit muss sich nicht lohnen, sondern im angemessenen Verhältnis zu den Folgen des Ausfalls einer Anlage stehen (§ 8a Abs. 1 S. 3 BSIG)

Last but not least: Bußgelder.

- **Die Bußdrohung bei Zuwiderhandlungen trifft auch Beamte persönlich.**

  § 9 Abs. 2 OWiG.

- **Im Einzelfall ist ihre Wirksamkeit aber sehr zweifelhaft.**

  Aus einem Schaden darf nicht auf einen Fehler der Sicherheitsabteilung geschlossen werden (EuGH, Urt. v. 25. Januar 2024, Az. C 687/21 Rz. 40).

  Strafbar darf nur sein, was erkennbar falsch ist. Dies setzt der Bußdrohung innere Grenzen (Nomos, im Erscheinen begriffen).

- **In jedem Fall mitigiert ein sorgfältiges Compliance-System Risiken aus Bußgeldern.**

  Bundesgerichtshof, Urt. v. 09.05.2017 – Az. 1 StR 265/16 Tz, 132; zitiert nach openJur 2017, 117.

Sektion 4

Ihre Fragen und Anmerkungen

Dr. iur. Julian Zaudig

Promotion zur Regulierung des Umgangs mit ungewissen Entwicklungen im Bereich der IT-Sicherheit nach BSIG und NIS-2 an der Universität zu Köln

Lehrstuhl **Prof.** Dr. Dr. h. c. **Barbara Dauner-Lieb**

Ausbildung:

Friedrich Graf von Westphalen & Partner, mbB

ZAC NRW, **Schwerpunktstaatsanwaltschaft für herausgehobene Cyberkriminalität** in NRW

Innenministerium NRW, Referat 73 (Cybersicherheit)

Stiftung Familienunternehmen & Politik

Praxis:

Gesellschafter und Counsel eines **MedTech-Unternehmens**, Begleitung auf einen siebenstelligen Umsatz - 2021

laufende strategische Beratung eines **führenden Legal Tech-Unternehmens im Bereich der Künstlichen Intelligenz und Datensicherheit** - seit 2020

Beratung des **IT-Boards eines international tätigen mittelständischen Unternehmens bei der IT-Sicherheitsstrategie und Datenklassifizierung** - 2023

laufende strategische Beratung eines **großen Wachstumsunternehmens im Bereich HR-Tech** – seit 2023