



NIS 2-Umsetzung des Landes Berlin im Hinblick auf konkrete Supply Chain Angriffe

Vortrag am 16. September 2026
Dr. Olaf Kroll-Peters

<mailto:olaf.kroll-peters@senatskanzlei.berlin.de>



Dr. Olaf Kroll-Peters



Wer bin ich?

Dr. in „Wie verstehen wir (Menschen)
Informationssicherheit?“

Informatiker

Psycholog

Privat:
• Zauberer
• Musiker
• Forscher

Beruf:
• Kernenergie
• Healthcare
• Telekommunikation
• Justiz
• Landes-InfSiBe (K)
• Landes-Beauftragter-IKT-BCM

Dr. Olaf Kroll-
Peters





Agenda

- NIS-2-RL das unbekannte Wesen
 - 312 Schritte - Wir schleichen uns dann mal an
- Magie
 - Fortbildung zum Zauberer
- Ein konkreter Angriff auf die Lieferkette
 - Wie kann man in der Realität zaubern
- Wie können wir in Zukunft zaubern?





Magie

Wie werde ich zum
Zauberer?





Ein wenig Magie – Festsetzungsschreiben Berlin

Die zuständige Behörde **stellt sicher**, dass die Verpflichtungen aus der **NIS-2-Richtlinie wirksam beaufsichtigt** werden und die **erforderlichen Maßnahmen getroffen werden**. Sie handelt in dieser Funktion unabhängig.

Um die Umsetzung der Anforderungen aus der NIS-2-Richtlinie sicherzustellen, kann die oder der Beauftragte für Informationssicherheit des Landes die **erforderlichen Auskünfte** und die **Überlassung von entsprechenden Unterlagen** der staatlichen Stellen nach dem EGovG Bln verlangen.





Ein wenig Magie – Festsetzungsschreiben Berlin

beaufsichtigt
getroffen werden.

stellt sicher,
NIS-2-Richtlinie wirksam
erforderlichen Maßnahmen



Auskünfte
Unterlagen

erforderlichen
Überlassung von entsprechenden





Der Angriff

Eine Firma baute für das Land viel Infrastruktur.
Dort sind Angreifer mehrere Monate im System.

Datenabfluss unklar!

Was bedeutet das?





Was der Vorfall gezeigt hat

Bewertung nach Aktenlage zum Bewertungsstichtag – der Ausgang des Vorfalls ist nicht bewertet.

rot

[KPI-012] Lieferketten-
sicherheitskonzept – am
Stichtag nicht vorhanden;
Risikobewertung des
Lieferanten nicht verfügbar

grün

[KPI-029] Meldekette
Dienstleister → ITDZ →
Berlin-CERT → SKZL
vollständig durchlaufen

ungeklärt

Datenabfluss –
Lieferantenangabe ohne
Beweisgrundlage; Protokolle
gelöscht ([KPI-007],
K2.4/T4.4)

offen

Ausgang der
Betroffenheitsklärung –
gesondert dokumentiert





Wie kriegen wir so ein Problem verhindert?

- Vertraglich festlegen was mit den Daten nachdem sie benutzt wurden geschehen soll.
Achtung das ist was anderes als nach Beendigung des Vertrages

- Sichern im Land Berlin
- Nachprüfbares Löschen bei der Firma

Überlegen was wie messbar ist

- Bereitstellung Umgebung

- Bereitstellung einer Umgebung im Land Berlin auf der alle Sensiblen Daten bereitgestellt und verwendet werden.
- Protokollierung wer wann wie auf diese Daten zug
- Protokollierung Datenbewegungen

KPI die ich sehen will

- Recht zu scannen
- Wasserzeichen, um zu sehen wo was abfließt?

KPI wann letzte mal gescannt

KPI Anzahl an Wasserzeichen

Geregelter dokumentierter Löschprozess





Wie kriegen wir so ein Problem verhindert?

- Überlegen was wo wie mit welcher Aussage gemessen werden kann?
- Abfragen wer mit Firmen außerhalb des Landes zusammenarbeitet?
- Abfragen wer welche Daten außerhalb des Landes hat?
- Zu definierender Rahmen:
 - Sämtliche Daten des Landes bleiben im Land.
 - Zugriffsmöglichkeiten darauf ?
 - Nur mit Dienstgeräte?
- In neuen Verträgen genau das definieren und als Bringschuld (für Reporting verankern).

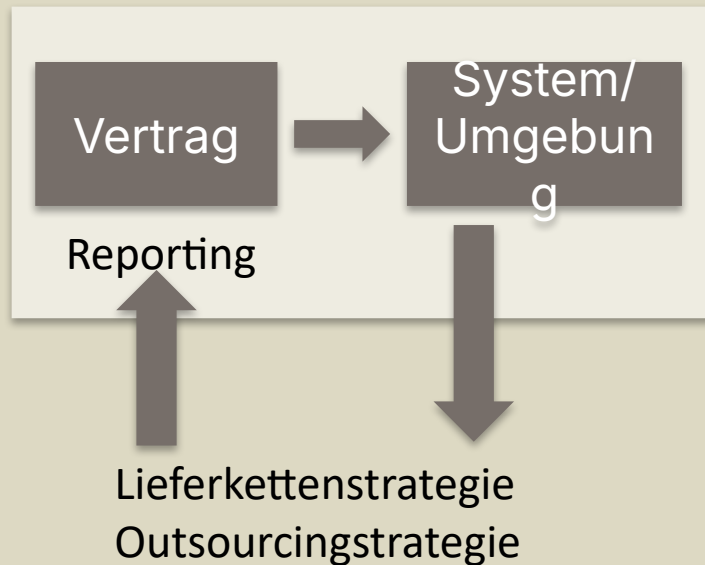
Bewertungsregel: „nicht feststellbar“ gilt als Verstoß

Ist der Klausel- und Bewertungsstand eines kritischen Lieferanten am Stichtag nicht feststellbar, wird dies wie ein Verstoß behandelt





Wie kriegen wir so ein Problem verhindert?



Vielen Dank für Ihre Aufmerksamkeit,
Lassen Sie uns gemeinsam nachts ruhiger schlafen, indem wir uns
auf vieles, nicht alles, vorbereiten!

Ich freue mich auch auf Ihre weiteren Fragen und beantworte diese
gerne!



Dr. Olaf Kroll-Peters

