Cyberangriffe auf Krankenhäuser:

Rechtspflichten und Handlungsempfehlugnen

Montag, 11. August 2025

Steffen Groß, Rechtsanwalt für Datenschutz- und IT-Sicherheitsrecht

Über mich

Steffen Groß (Simpliant)

- Rund 10 Jahre Erfahrung als Datenschutzbeauftragter und Anwalt
- Tätigkeitsschwerpunkt: Gesundheitswesen und eHealth

E-Mail: steffen.gross@simpliant.eu

Website: www.simpliant.eu

Agenda

1. Einleitung & Relevanz

2. Datenschutzrechtliche Meldepflichten (DSGVO/BDSG)

3. IT-Sicherheitsrechtliche Meldepflichten (BSIG & NIS-2-Ausblick)

4. Weitere Meldungen & Kommunikation

5. Fazit und Handlungsempfehlungen

1. Einleitung - Relevanz und Zahlen

📈 +74 % Angriffe auf Krankenhäuser (2020–2024)

🏥 Gesundheitswesen: am stärksten betroffener KRITIS-Sektor

💰 83 % finanzielle Motive (53 % Ransomware)

⚠ 71 % mit Auswirkung auf Patientenversorgung

Kontext: Hacker-Industrie, Staatliche Akteure/hybride Kriegsführung (Russland-Ukraine)

Rechtliche Relevanz: Hackerangriff löst Rechtspflichten aus - Datenschutz- und IT-Sicherheitsrecht sind hier eng verwoben (und komplex).

1. Einleitung - Folgen von Hackerangriffen

 Hohe Schäden & lange Wiederherstellung

- Schäden oft in Millionenhöhe
- Wiederherstellung dauert Wochen bis Monate

 Eingeschränkte Patientenversorgung

- 71 % der Angriffe beeinträchtigen Behandlung
- Verzögerungen bei OPs, Behandlungen, Notfalldiensten

 Gefahr für Patientendaten

- Risiko der Veröffentlichung sensibler Daten
- Gefahr von Schadensersatzforderungen & Bußgeldern

1. Einleitung – Gesetzlicher Rahmen

📜 Datenschutzrecht (DSGVO, BDSG, Landeskrankenhausgesetze)

- Meldepflicht bei Datenschutzverstoß (Art. 33 ff. DSGVO)
- Schutz personenbezogener Daten, insb. Gesundheitsdaten

🛡 IT-Sicherheitsrecht (BSIG, KritisV, NIS2, § 391 SGB V, BSI B3S)

- Meldepflicht bei erheblicher IT-Störung (§ 8b Abs. 4 BSIG)
- Mindeststandards für IT-Sicherheit (BSI B3S Medizinische Versorgung)
- NIS2: Neuer Rechtsrahmen in Vorbereitung (Entwurf 25.07.2025)

⚖️ Strafrecht

- Datenveränderung (§ 303a StGB)
- Computersabotage (§ 303b StGB)
- Ausspähen von Daten (§ 202a StGB)
- Verletzung von Privatgeheimnissen (§ 203 StGB

2. Datenschutzrechtliche Meldepflicht

⏱️ Frist

- Unverzüglich, möglichst innerhalb von 72 Stunden

🕵️ Verantwortlichkeit

- Krankenhausleitung ist meldepflichtig
- Delegation möglich

📅 Fristbeginn

- Start: „Bekanntwerden“ der Datenschutzverletzung
- Verzögerung = Begründungspflicht gegenüber Aufsichtsbehörde
- Dringlichkeit Je höher das Risiko, desto schneller melden

✉️ Form der Meldung

- Formlos (E-Mail/Telefon) möglich, aber dokumentieren
- Empfehlung: offizielle Meldeformulare der Aufsichtsbehörden nutzen

2. Wann liegt meldepflichtiger Verstoß vor?

🎯 Schutzzweck: Schutz von Patienten sowie Wahrung ihrer Persönlichkeitsrechte

📣 Meldepflicht erforderlich bei Verletzung der Vertraulichkeit, Integrität oder Verfügbarkeit personenbezogener Daten (insbesondere Gesundheitsdaten):

- 🔒Vertraulichkeit:
  - Unbefugte Offenlegung von Patientendaten.
- 🛠 Integrität:
  - Unbefugte oder fehlerhafte Veränderung von Patientendaten.
- 📂 Verfügbarkeit:
  - Verlust oder vorübergehende/anhaltende Nichtzugänglichkeit von Patientendaten.

2. Durchführung der Erstmeldung bei Datenschutzverstoß

🔍 Prüfung vor Erstmeldung

- Feststellung: Liegt ein Datenschutzverstoß vor?

⚖️ Risikobeurteilung:

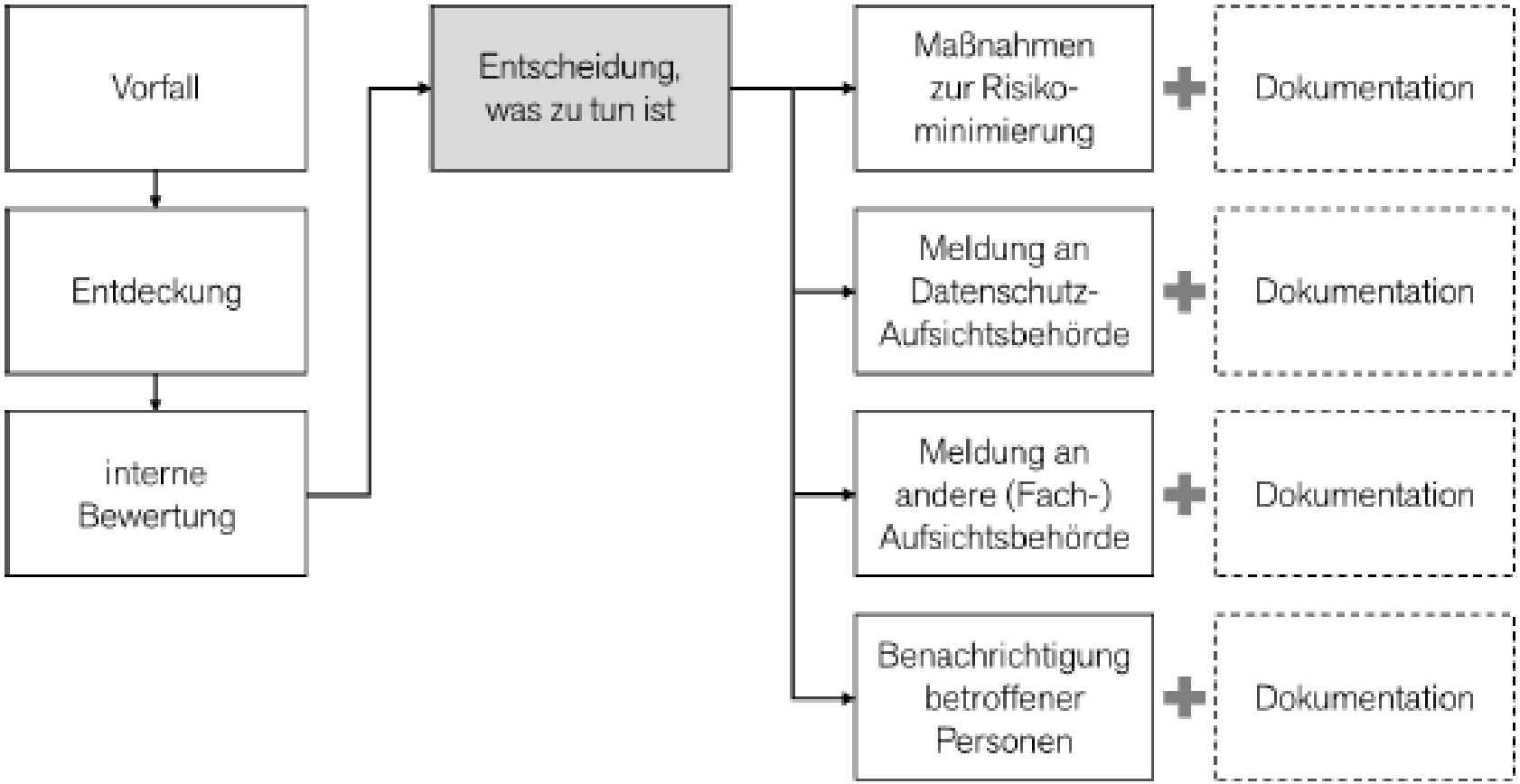
- Bewertung der möglichen Auswirkungen für die Betroffenen.
- Hinweis: Bei Patientendaten ist das Risiko in der Regel hoch.
- Abhängig von Risiko Meldung an Datenschutzbehörde und Betroffene erforderlich?

📝 Mindestinhalte der Erstmeldung (gemäß Art. 33 Abs. 3 DSGVO)

- Art der Datenschutzverletzung (Hackerangriff, unbefugter Zugriff, Datenverlust)
- Kategorien und Anzahl der betroffenen Personen (z. B. Patienten, Mitarbeiter)
- Mögliche Folgen für Betroffene (z. B. Gefahr für Leib und Leben, Diskriminierung, Rufschädigung)
- Bereits ergriffene oder geplante Maßnahmen (z. B. Systemsicherung, Passwortänderung, Information der Betroffenen)

2. Risikobeurteilung bei Datenschutzverstoß

2. Vorfallbehandlung nach DSGVO



3. Meldepflichten BSIG/NIS2

🎯 Schutzzweck: Schutz der kritischen Infrastruktur

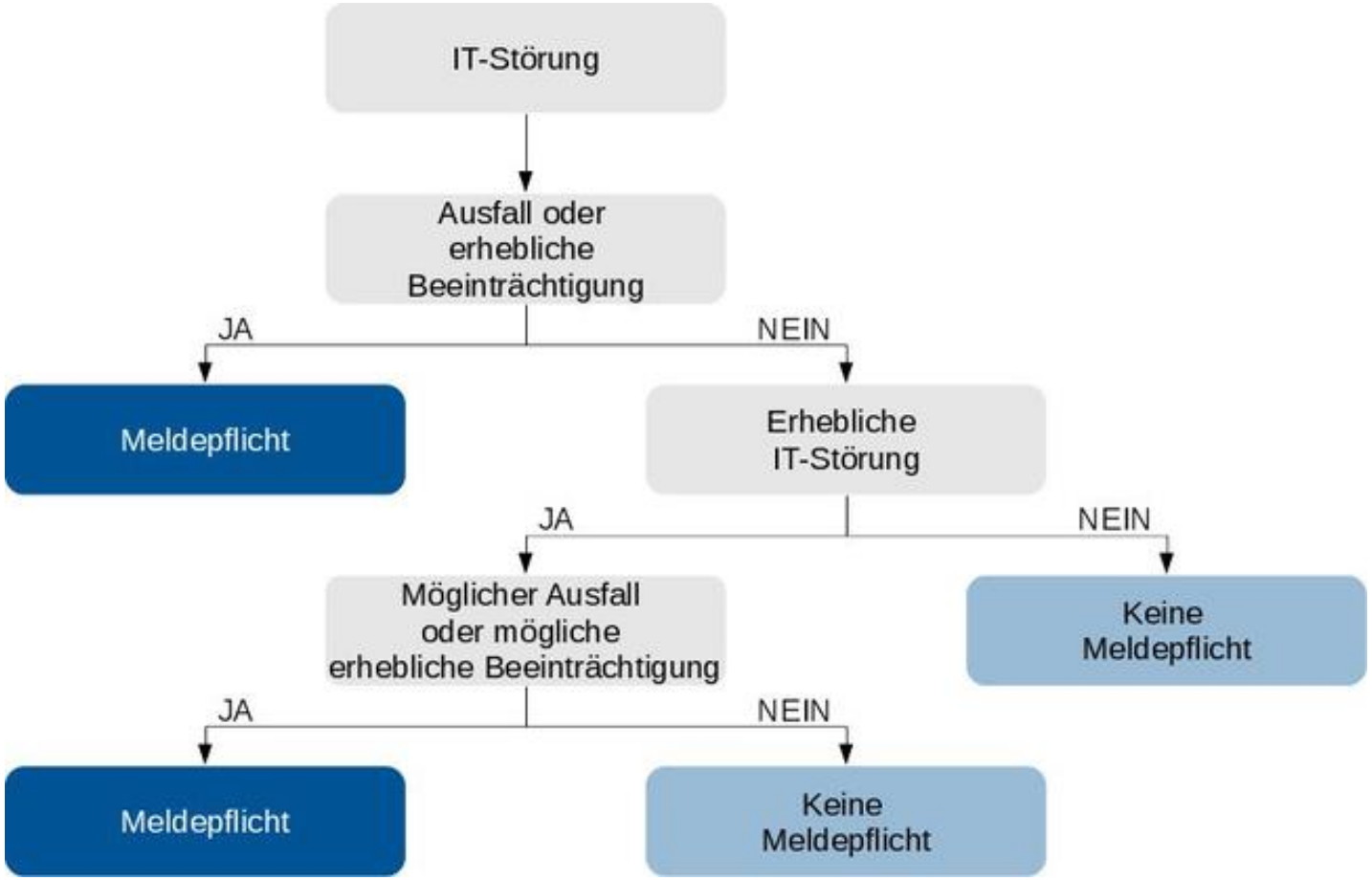
- Betrifft auch nicht-personenbezogene Daten: Gesamtheit der kritischen Krankenhaus-IT soll geschützt werden

📠 Verpflichtende Meldung an BSI (Melde- und Informationsportal)

⏱️ Für Meldefristen Orientierung an Art. 23 NIS-2

- Erstmeldung (“early warning“): Innerhalb von **24 Stunden** nach Kenntnis eines signifikanten Vorfalls
- Folgemeldung („incident notification“): Spätestens nach **72 Stunden** inkl. Bewertung Schwere/Impact
- Abschlussbericht („final report“): Innerhalb von etwa **1 Monat** nach Folgemeldung

3. Wann besteht Meldepflicht nach § 8b BSIG?



4. Weitere Meldungen & Kommunikation

👮 Strafverfolgungsbehörden

- Polizei / Zentrale Ansprechstellen Cybercrime (LKA) sowie BKA kontaktieren
- Ziel: Strafanzeige erstatten, forensische Sicherung, Einleitung strafrechtlicher Ermittlungen

🛡 Cyberversicherung

- Unverzügliche Schadensmeldung zur Aktivierung des Versicherungsschutzes
- Inanspruchnahme von Krisenunterstützung, IT-Forensik, PR-Beratung und Rechtsbeistand (je nach Police)

💻 IT-Dienstleister, Auftragsverarbeiter & Security-Partner

- Vertraglich geregelte Unterstützungspflicht gem. Art. 28 DSGVO und Notfall-SLAs
- Schnelle Einbindung für technische Analyse, Eindämmung, Wiederherstellung und Härtung der Systeme
- Dokumentation aller Maßnahmen für Behörden, Versicherung und interne Auswertung

5. Fazit und Handlungsempfehlungen

1. 🛠️ Sofortmaßnahmen einleiten
    - Sachverhalt ermitteln, Incident-Response-Team aktivieren, erste Forensik starten

2. 📢 Meldepflichten erfüllen
    - DSGVO: Meldung an Datenschutzaufsicht unverzüglich bzw. binnen 72 h
    - NIS2 / BSIG: Frühwarnung binnen 24 h, Folgemeldung binnen 72 h an BSI

3. 👮 Anzeige bei Polizei/LKA/BKA

4. 🗣️ Kommunikation steuern
    - Interne Information an Klinikleitung, IT, Datenschutz, relevante Fachbereiche
    - Externe Kommunikation mit Behörden, Versicherung, Partnern und ggf. Medien

5. 🔄 Nachbereitung & Prävention
    - Abschlussbericht mit Ursachenanalyse und Lessons Learned
    - Prozesse, Richtlinien und TOM anpassen, um künftige Angriffe abzuwehren

Fragen oder Unterstützungsbedarf?
–
Kontaktieren Sie uns jederzeit gern.

Simpliant GmbH
Fasanenstr. 12
10623 Berlin
Deutschland

info@simpliant.eu
www.simpliant.eu