TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-"IT-Sicherheitsrechtstag" 2024

Berlin, 25.09.2024

Verarbeitung personenbezogener Daten zum Schutz gegen Cyber-Angriffe

RA Alexander Weidenhammer, LL.M.

Dresdner Institut für Datenschutz

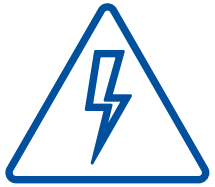
Agenda

- **Problemaufriss**
  - Angriffe und Bedrohungen
  - Ein datenschutzrechtliches Problem? - Bestimmung des Personenbezuges
  - Wechselwirkung zwischen Datenschutz und IT-Sicherheitsrecht
- **Datenschutzrechtliche Anforderungen**
  - Rechtmäßigkeit der Verarbeitung
  - Weitere datenschutzrechtliche Aspekte
- **Zusammenfassung**

Problemaufriss

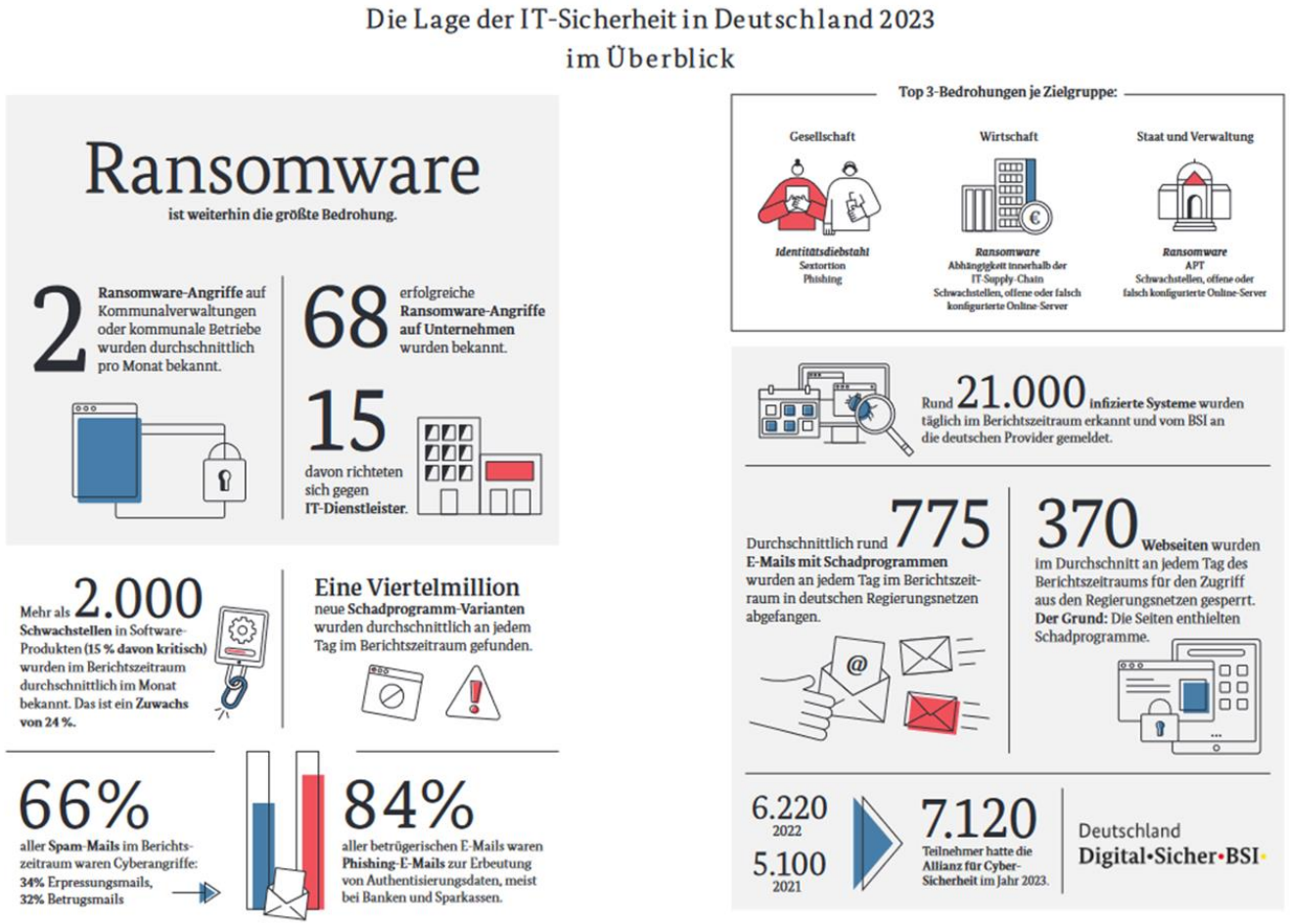
Regulatorische Anforderungen

Einschlägige Rechtsprechung



Aktuelle Bedrohungslage

Angriffe und Bedrohungen



Bundesamt für Sicherheit in der Informationstechnik

Angriffe und Bedrohungen

CYBER-ATTACKE

Hacker greifen Nutzerdaten einer Leipziger Hochschule a

26. Oktober 2022, 16:23 Uhr

Schulen, Krankenh
Attacken mehr sich
Studierenden und
Kultur in Leipzig zu
schaltete die Siche
Sicherheit geben.

CYBERKRIMINALITÄT

Nach Cyberangriff auf Bergakademie Freiberg: LKA übernimmt Ermittlungen

20. Januar 2023, 09:29 Uhr

le in

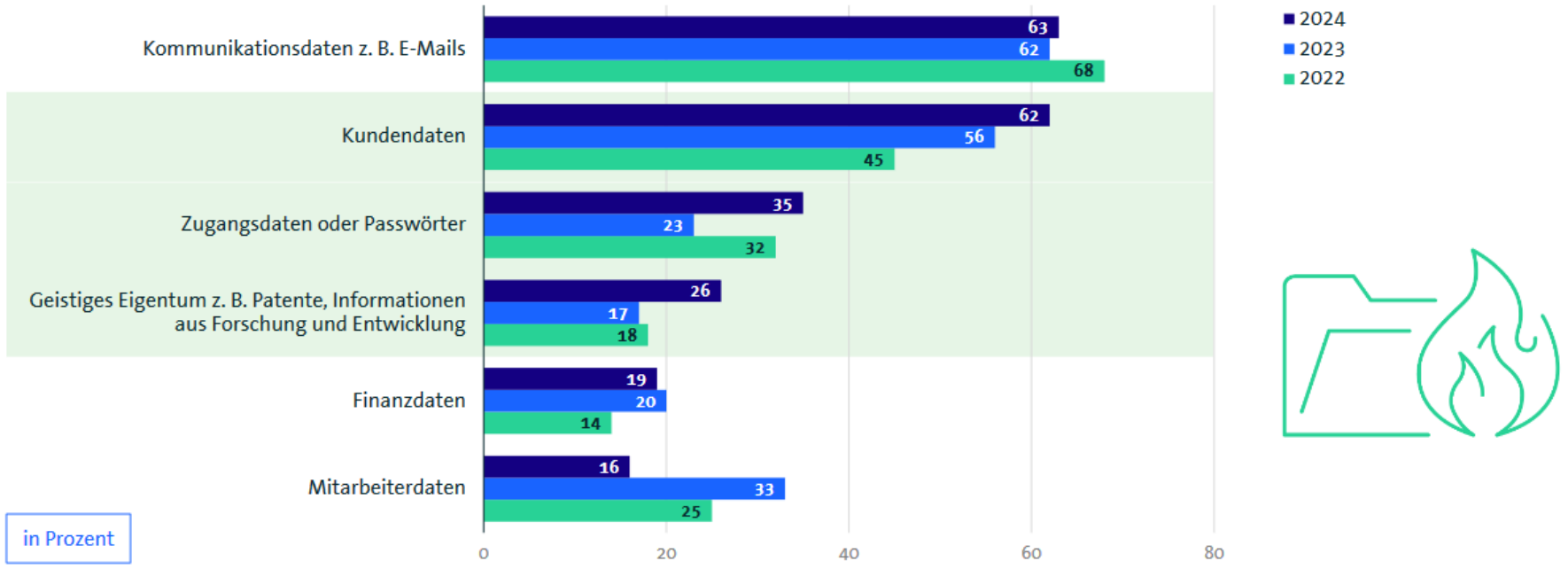
to: WHZ Bild: kein

www.mdr.de

Angriffe und Bedrohungen

Datendiebstahl: Kunden, Passwörter und Patente im Fokus

Welche der folgenden Arten von digitalen Daten wurden in Ihrem Unternehmen gestohlen?



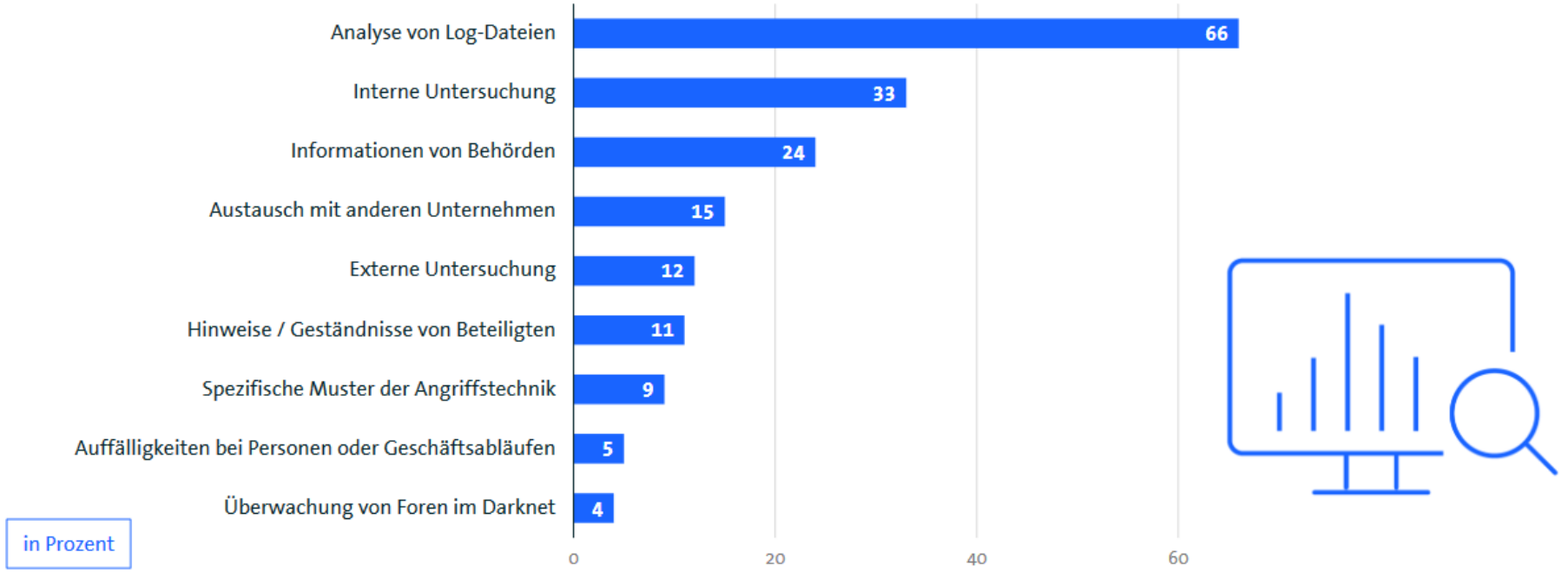
9 Basis: Unternehmen, die in den letzten 12 Monaten vom Diebstahl digitaler Daten betroffen waren (n=460) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2024

bitkom

Angriffe und Bedrohungen

Wie Taten aufgedeckt werden

Auf welcher Grundlage haben Sie die Erkenntnisse erlangt?



Basis:. Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren und Erkenntnisse über Herkunft, Täterkreis oder Motive hatten (n=783) | Mehrfachnennungen möglich | Quelle: Bitkom Research 2024

bitkom

Angriffe und Bedrohungen - Sicherheitsmaßnahmen

- **Technische Sicherheitsmaßnahmen**
  - Breites Spektrum an Maßnahmen – „von Logfile bis SIEM“
  - Problem: Klassische Maßnahmen (z.B. Firewall, Antivirensoftware) erkennen Zero-Day-Schwachstellen oder authentische Netzwerkzugriffe nicht
  - Zudem steigt Komplexität der Sicherheitsvorfälle

- **SIEM, IDS, EDR & Co.**
  - protokollieren Prozesse und Nutzeraktivitäten, in Systemen & Netzwerken,
  - detektieren potenzielle Sicherheitsereignisse,
  - reagieren z.T. bereits automatisch durch geeignete Gegenmaßnahmen,
  - …benötigen aber eine Unmenge an Daten

Angriffe und Bedrohungen – Beispiel SächsISichG

§ 12 Abwehr von Gefahren für die informationstechnischen Systeme im Freistaat Sachsen

(1) Zur **Erkennung und Abwehr von Gefahren für die informationstechnischen Systeme** im Freistaat Sachsen etwa durch **Schadprogramme, Sicherheitslücken oder unbefugte Datenverarbeitung** dürfen das Sicherheitsnotfallteam sowie die staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen innerhalb ihres jeweiligen Zuständigkeitsbereichs

1. **Protokolldaten** erheben und automatisiert auswerten sowie
2. die an den Schnittstellen der informationstechnischen Systeme anfallenden **Protokoll- und Inhaltsdaten** erheben und automatisiert auswerten,

soweit dies zur Verhinderung oder Abwehr von Angriffen auf informationstechnische Systeme der staatlichen und nicht-staatlichen Stellen im Freistaat Sachsen oder zum Erkennen, Eingrenzen oder Beseitigen dieser Störungen der Informationssicherheit **erforderlich ist**.

(2) [...]

Haben wir ein datenschutzrechtliches Problem?
Bestimmung des Personenbezuges

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Abgrenzung zwischen personenbezogenen Daten und Sach-/technischen Daten

- **Log- und Protokolldaten**
  - **…**sind regelmäßig **technische Daten** (können jedenfalls Ursachen für Funktionsstörungen oder Schäden in IT-System ermitteln)
  - ... können Informationen in Form von IP-Adressen, E-Mail-Adressen, Servernamen, Gerätekennungen und Ereignisdaten enthalten

- Ähnliches gilt für den **Netzwerkverkehr**, speziell bei Sitzungsdaten (Informationen zu Netzwerkverbindungen) sind IP-Adressen, Angaben über die Initiierung der Verbindung sowie Informationen über Sitzungslänge sowie übertragene Datenmenge enthalten

Bestimmung des Personenbezuges

Begriff der personenbezogenen Daten – *EuGH, Urt. v. 9.11.23 , Rs. C-319/22*

- EuGH: Eine FIN ist ein alphanumerischer Code, den Hersteller einem Fahrzeug zur eindeutigen Identifizierung eines Fahrzeugs zuweisen – der Zweck der FIN ist die Identifizierung des Fahrzeugs – sie kann trotzdem personenbezogen sein!
- Eine FIN ist dann personenbezogen, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person bezieht, die in den Fahrzeugpapieren zusammen mit der FIN genannt wird, d.h. **Daten können unter Hinzuziehung weiterer Informationen zu personenbezogenen Daten werden!**
- **Logdaten** und Daten über den Netzwerkverkehr enthalten **regelmäßig Merkmale mit Personenbezug**, da Verantwortliche vernünftigerweise über die zur Verfügung stehenden Mittel verfügen, um aus den rein technischen Daten einen Personenbezug herzustellen

Bestimmung des Personenbezuges

- Und wenn wir die Daten **anonymisieren**?
  - Problem, es gehen **Bezüge zwischen** den **Daten verloren**, welche für das Erkennen eines Angriffs zum Teil essenziell sind (z.B. Zuordnung über IP-Adressen und MAC-Adressen)
  - Zuverlässige Zuordnungen bei Störungsfällen nicht mehr möglich
  - Daten müssen z.T. über längeren Zeitraum ausgewertet werden, um Angriffe zu rekonstruieren und komplexe Strukturen aufzudecken

- **Pseudonymisierung** als Lösung?
  - Grundsätzlich denkbar, dann müsste eine Aufhebung des Pseudonyms bei Sicherheitsvorfällen durch zuständige Stellen erfolgen
  - Es können Schwierigkeiten bei der technischen Umsetzung eintreten

Wechselwirkung zwischen Datenschutz und IT-Sicherheitsrecht

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

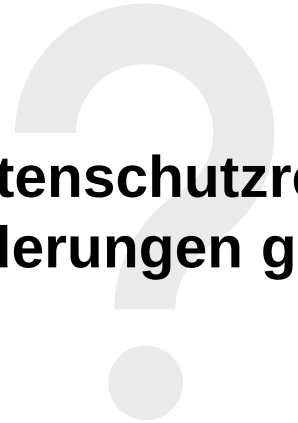
Datenschutzrecht

- Intelligente Sicherheitslösungen verarbeiten eine Vielzahl pbD, d.h. Eingriff in das Recht auf informationelle Selbstbestimmung
- insb. Art. 5 DS-GVO kann Sicherheitsmaßnahmen beschränken
- Datenschutzrecht darf gleichwohl nicht Sicherheitsaspekte vollständig aushebeln

IT-Sicherheitsrecht

- Steigen Bedrohungslage erfordert aktive Abwehr von Cyber-Angriffen
- Sicherheit der Systeme bedingt gleichwohl Sicherheit der Daten
- Sicherheitsmaßnahmen müssen Datenschutzrecht wahren
- Angemessenes Sicherheitsniveau ist von Bedeutung für Grundrechte und Grundfreiheiten

Wechselwirkung zwischen Datenschutz und IT-Sicherheitsrecht



Welche datenschutzrechtlichen Anforderungen gelten?

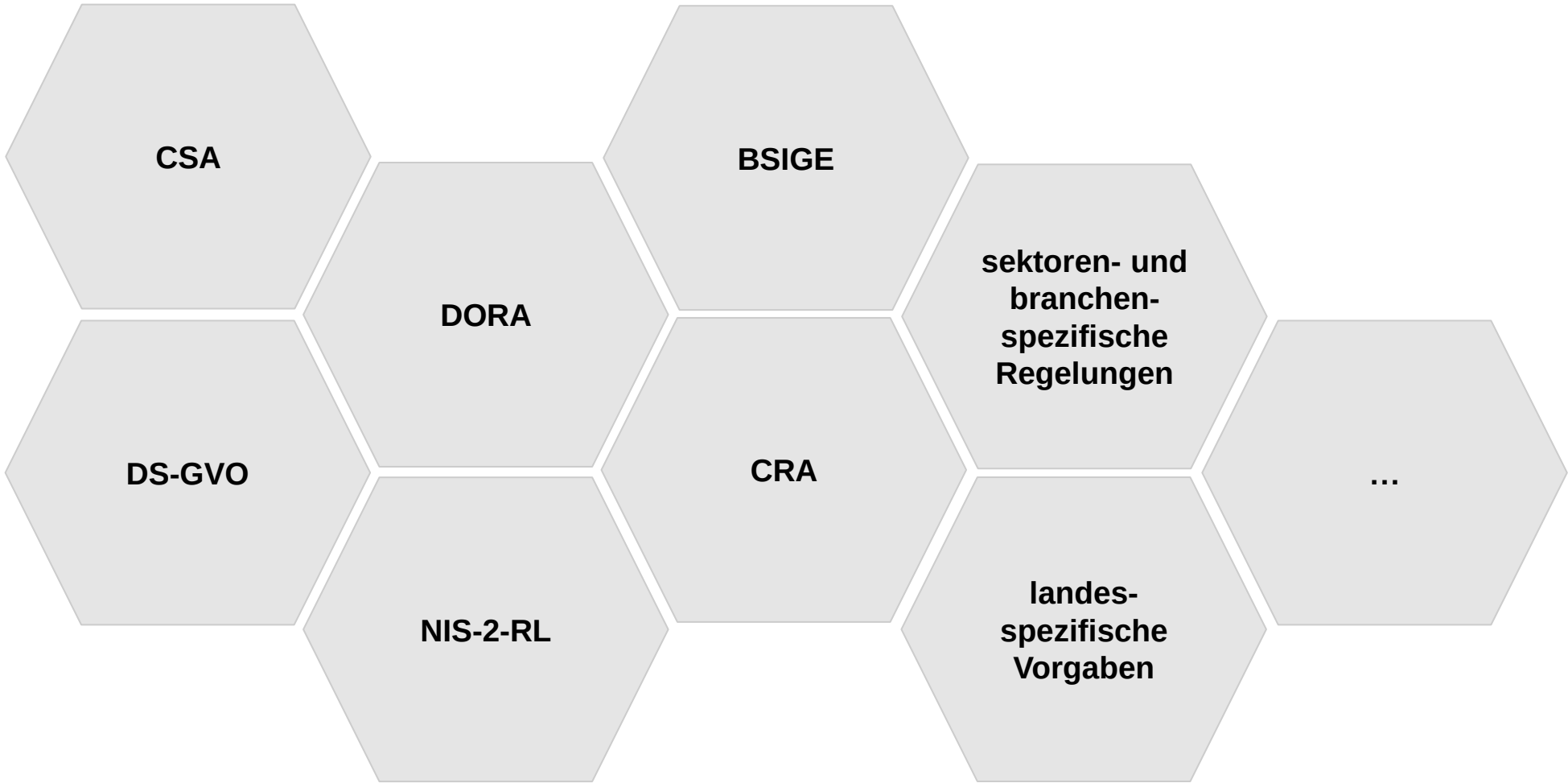
Rechtmäßigkeit der Verarbeitung

- **Rechtsgrundlagen des Art. 6 Abs. 1 DS-GVO**
  - Einwilligung
  - Vertragsanbahnung und -durchführung
  - Erfüllung einer rechtlichen Pflicht
  - Schutz lebenswichtiger Interessen
  - Wahrnehmung einer öffentlichen Aufgabe
  - Berechtigtes Interesse nach Abwägung

Art. 6 Abs. 1 UAbs. 1 lit c) DS-GVO

- Rechtliche Verpflichtung – Art. 6 Abs. 2 und 3 DS-GVO – im Zusammenhang einer **Rechtsvorschrift**
- Umstritten, ob direkte Datenverarbeitungsverpflichtung normiert sein muss (Arg. ErwG 45 DS-GVO), d.h. konkrete Nennung wäre notwendig
- Vorzugswürdig genügt jedoch eine **Zweckbestimmung** in der jeweiligen Rechtsgrundlage **keine Spezifizierung**
- Gesetzgeber positioniert sich nunmehr selbst in **ErwG 121 NIS-2-RL** und **ErwG 34 DORA**

Potenzielle Rechtsgrundlagen



Potenzielle Rechtsgrundlagen

- Art. 32 Abs. 1 DS-GVO
- Art. 33 Abs. 1 DS-GVO
- § 8a Abs. 1a BSIG, § 8c Abs. 1 BSIG bzw. Art. 21 Abs. 2 NIS-2-RL bzw. § 31 Abs. 2 Satz 1 BSIGE
- Art. 4 Abs. 1 DORA
- § 30 Abs. 1 BSIGE
- §§ 12, 19 Abs. 4 TDDDG
- …

Art. 32 Abs. 1 DS-GVO – Sicherheit der Verarbeitung

(1) Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter **geeignete technische und organisatorische Maßnahmen**, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten […].

§ 30 Abs. 1 BSIGE – Risikomanagementmaßnahmen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, **geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen**, die nach Absatz 2 konkretisiert werden, zu **ergreifen**, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten […].

§ 31 Abs. 2 Satz 1 BSIGE

(2) Betreiber kritischer Anlagen sind verpflichtet, **Systeme zur Angriffserkennung einzusetzen**. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Dabei soll der **Stand der Technik** eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO – Berechtigtes Interesse

- **IT-Sicherheit** als **berechtigtes Interesse**, nicht allein aufgrund von ErwG 49 (Netz- und Informationssicherheit)
- ErwG 49 Satz 2 Adressiert den **Schutz vor Zugang Unbefugter** und **Schädigungen** von Computer- und elektronischen Kommunikationssystemen
- Interesse besteht im Schutz eigener IT-Systeme (wirtschaftliche Relevanz und wettbewerbsrechtliche Pflichten oder auch **Kernpflicht der Organe** vgl. § 91 Abs. 2 und § 93 Abs .1 Satz 1 AktG)
- Einhaltung der Compliance und präventive Verhinderung von Risiken

Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO – Erforderlichkeit

- Maßnahmen dürften überwiegend objektiv geeignet sein
- **Kritisch** hingegen: **Umfang der Datenverarbeitung** bei komplexen Systemen wie SIEM, IDS oder EDR
- Zum Zeitpunkt der Datenerhebung häufig nicht abschätzbar, welche Daten künftig relevant sind, um Cyber-Angriffe aufzuklären
- Mögliche Lösungsansätze ebenfalls über **Benutzer- und Berechtigungskonzepte** („need-to-know-Prinzip“) und **Pseudonymisierung**

Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO – Interessenabwägung

- Aspekte jedenfalls **Schwergrad** des Sicherheitsvorfalls und **Wahrscheinlichkeit** der Abwehr sowie **Umfang der Auswirkungen**
- **Gefahrenprognose** zu Angriffsdruck sowie drohender Schäden
- Andererseits **vernünftigen Erwartungen** der **betroffenen Personen** (Aspekte der aktuellen Bedrohungslage nicht zu vernachlässigen)
- Vorbeugen, Detektieren und Abwehren von Sicherheitsvorfällen ist in der Regel großer Nutzen zuzuschreiben
- Aspekte: Kategorie betroffener Personen und Daten, Kritikalität der betroffenen IT-Systeme, Umfang und Dauer des tatsächlichen Datenzugriffs

Und was ist mit Art. 9 DS-GVO?

- Verarbeitung **besonderer Kategorien pbD** z.B. iRV E-Mail-Screenings, DLP-Tools, Penetration Tests denkbar
- Verhältnis von Art. 6 und Art. 9 DS-GVO durch Urteil des EuGH v. 21.12.2023, Rs. C-667/21 geklärt
- Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO hier nicht anwendbar
- Abgestellt werden kann auf **Art. 9 Abs. 2 lit. g) DS-GVO** (erhebliches öffentliches Interesse: *Interesse der gesamten Bevölkerung oder von größeren Teilen davon bzw. der sozialen Gemeinschaft*)
- Teilaspekt ist die Unversehrtheit der Rechtsordnung → Rückgriff auf die dargestellten Anforderungen & Pflichten im IT-Sicherheitsrecht

Weitere datenschutzrechtliche Aspekte

- Grundsätze der Datenverarbeitung
  - Zweckbindung: Welchen Zweck verfolgt bspw. Erhebung von Logfiles?
  - Speicherbegrenzung: Zukünftige Bedürfnisse – Wie lange darf ich speichern?
- Informationspflichten – Problem ist die Weitergabe/Veröffentlichung sicherheitsrelevanter Aspekte – Wie viel ist wirklich geschuldet?
- Auftragsverarbeitung (Art. 28 DS-GVO) bei SaaS-Lösungen
- Durchführung einer DSFA nach Art. 35 DS-GVO (lt. Whitelist der Datenschutzaufsicht insb. bei DLP-Tool)
- Übermittlung pbD in Drittländer (Artt. 40 bis 50 DS-GVO)

Zusammenfassung

- Enorme Bedrohungslage erfordert immer häufiger Einsatz komplexer Sicherheitslösungen
- Gleichzeitig steigen die rechtlichen Anforderungen und Pflichten auf dem Gebiet des IT-Sicherheitsrechts
- Technische Maßnahmen bedingen stets die Verarbeitung pbD
- Erforderlich ist Balance zwischen Datenschutz- und IT-Sicherheitsrecht
- Potenzielle Rechtfertigung ist über Art. 6 Abs. 1 UAbs. 1 lit. c), Abs. 3 DS-GVO iVm Rechtsvorschrift möglich
- Art. 6 Abs. 1 UAbs. 1 lit. f) DS-GVO erscheint auch möglich, ist höheren Anforderungen unterworfen (Interessenabwägung, Widerspruchsrecht)
- Dokumentation iRd Nachweispflichten

Zeit für Ihre Fragen!

Dozent

RA Alexander Weidenhammer, LL.M.

Dresdner Institut für Datenschutz
Hospitalstraße 4 | 01097 Dresden | Deutschland
Telefon: +49 (0)351 / 655 772 0
Telefax: +49 (0)351 / 655 772 22
E-Mail: a.weidenhammer@dids.de | Internet: www.dids.de

Das Dresdner Institut für Datenschutz berät Unternehmen und Behörden zu allen Fragen in den Bereichen des Datenschutzes und der Informationssicherheit.