

Prävention und Meldepflichten bei Datenpannen

Ein Leitfaden für die Praxis



Tägliche Meldungen in die Medien

Collins Aerospace: Alte Passwörter und verzögerte Reaktion ermöglichen Datenklau

Neue Details zum Cyberangriff auf Collins Aerospace: Alte Passwörter ermöglichten Datenklau, wohl Millionen Passagierdaten betroffen – mehr als nur Ransomware.



(Bild: Nuno Andre/Shutterstock.com)

(Quelle: www.heise.de/news)

Tägliche Meldungen in die Medien

Angreifer können Authentifizierung bei Dell Storage Manager umgehen

In einer aktuellen Version von Dells Storage Manager haben die Entwickler drei Sicherheitslücken geschlossen.



(Bild: Artur Szczybylo/Shutterstock.com)

(Quelle: www.heise.de/news)

Tägliche Meldungen in die Medien

Ubiquiti UniFi Access: Angreifer können sich unbefugt Zugriff verschaffen

In Ubiquitis UniFi Door Access klappt eine kritische Sicherheitslücke, die Angreifern unbefugten Zugriff ermöglicht.

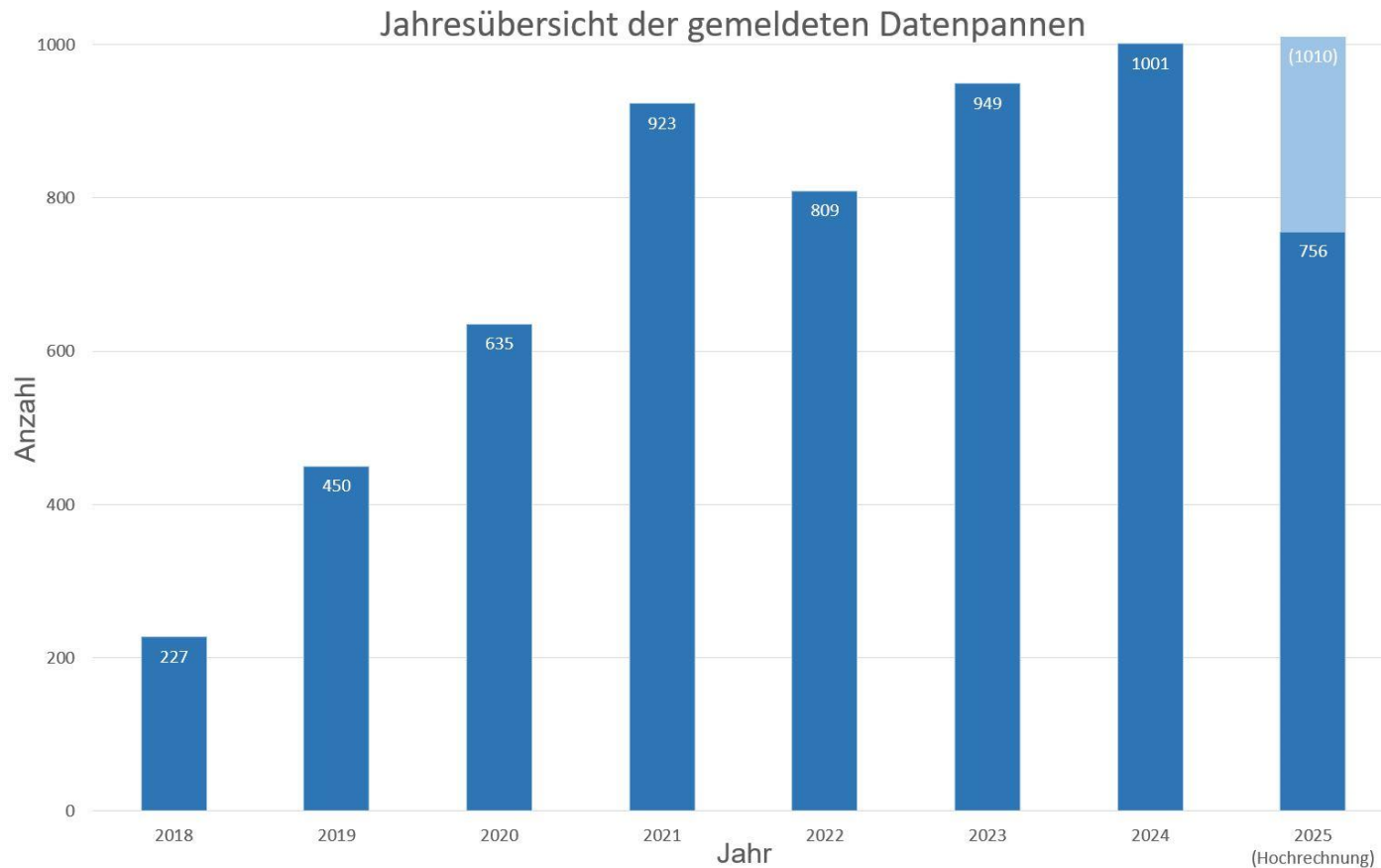


(Bild: Ubiquiti, Collage heise medien)

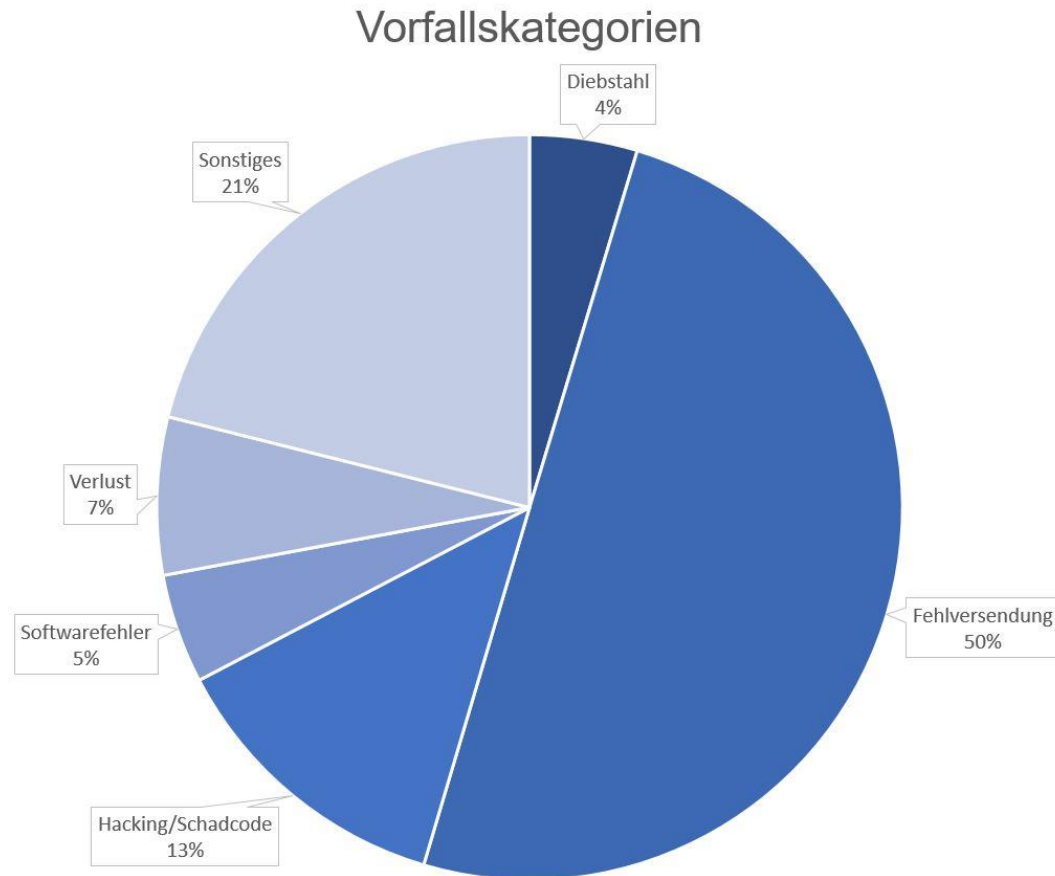
(Quelle: www.heise.de/news)



Zahlen und Fakten



Zahlen und Fakten



Was ist eine Datenpanne?

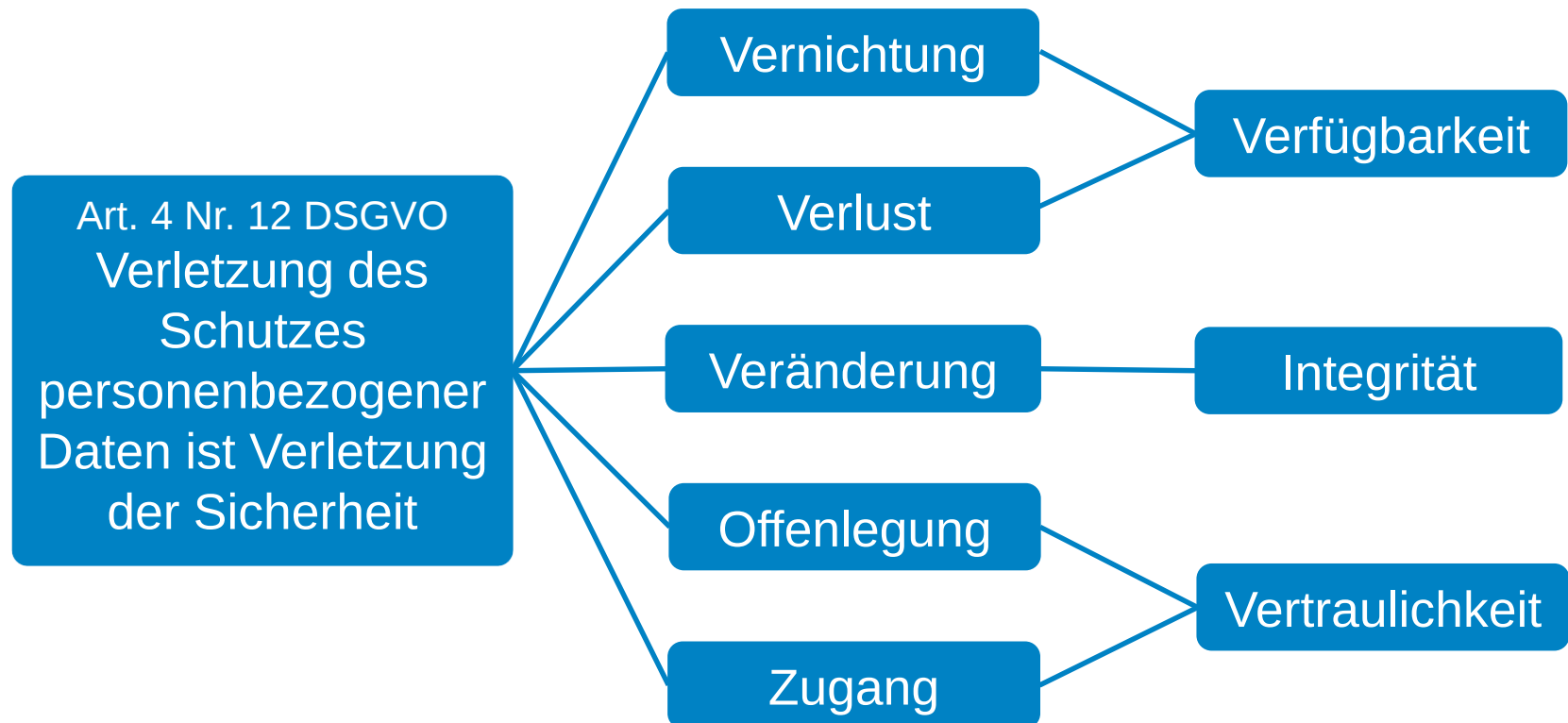
Gesetzliche Definition – Art. 4 Nr. 12 DSGVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

„Verletzung des Schutzes personenbezogener Daten“ eine **Verletzung der Sicherheit**, die, ob unbeabsichtigt oder unrechtmäßig, zur **Vernichtung**, zum **Verlust**, zur **Veränderung**, oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

→ **Verletzung des Schutzes personenbezogener Daten**

Was ist eine Datenpanne?



Was ist eine Datenpanne?

Verletzung der Vertraulichkeit

- unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten

Verletzung der Integrität

- unbefugte oder unbeabsichtigte Änderung personenbezogener Daten

Verletzung der Verfügbarkeit

- unbefugter oder unbeabsichtigter Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten

Datenpanne erkennen und wahrnehmen

- durch eigene Mitarbeiter
- durch interne IT
- durch Mitteilung eines Auftragsverarbeiters
- durch Mitteilung eines Hardware-/Software-Anbieters
- durch Beschwerden von betroffenen Personen
- durch Hinweise Dritter
- durch die Presse
- durch Anfragen der Aufsichtsbehörde

Was ist im Ernstfall zu tun?

- interne Beteiligung/Information der Verantwortlichen
- Sachverhaltsermittlung/Bewertung/Risikoanalyse
- Schadensmindernde Maßnahmen
- externe Beteiligung
- Melde-/Benachrichtigungspflichten
- Anzeigen/Mitteilungen
- technische und organisatorische Maßnahmen
- Dokumentation

Was ist im Ernstfall zu tun?

Melde-/Benachrichtigungspflichten – Art. 33 und 34 DSGVO

- Das maßgebliche Risiko



(Quelle: Abbildung aus Orientierungshilfe, Meldepflicht und Benachrichtigungspflicht des Verantwortlichen, BayLfD, 2019)



Was ist im Ernstfall zu tun?

Melde-/Benachrichtigungspflichten – Art. 33 und 34 DSGVO

- Risikobewertung
- Meldefrist von 72 Stunden, Art. 33 Abs. 1 S. 1 DSGVO
- Umfang der Meldung, Art. 33 Abs. 3 DSGVO
- Vorläufige/schrittweise Meldung, Art. 33 Abs. 4 DSGVO
- Auftragsverarbeiter, Art. 33 Abs. 2 DSGVO
- Dokumentation, Art. 33 Abs. 5 DSGVO

Was ist im Ernstfall zu tun?

- interne Beteiligung/Information der Verantwortlichen
- Sachverhaltsermittlung/Bewertung/Risikoanalyse
- schadensmindernde Maßnahmen
- externe Beteiligung
- Melde-/Benachrichtigungspflichten
- Anzeigen/Mitteilungen
- technische und organisatorische Maßnahmen
- Dokumentation

Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 5 Abs. 1 Buchstabe f DSGVO – Grundsätze

Personenbezogene Daten müssen

in einer Weise verarbeitet werden, die eine **angemessene Sicherheit** der personenbezogenen Daten **gewährleistet**, einschließlich **Schutz vor unbefugter oder unrechtmäßiger Verarbeitung** und **vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung** durch **geeignete technische und organisatorische Maßnahmen** („Integrität und Vertraulichkeit“);

Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 24 Abs. 1 DSGVO

Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen **geeignete technische und organisatorische Maßnahmen** um, um **sicherzustellen** und den **Nachweis** dafür erbringen zu können, dass die **Verarbeitung gemäß dieser Verordnung** erfolgt.

Diese Maßnahmen werden erforderlichenfalls **überprüft** und **aktualisiert**.

Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 24 Abs. 2 DSGVO

Sofern dies in einem angemessenen Verhältnis zu den Verarbeitungstätigkeiten steht, müssen die Maßnahmen gemäß Absatz 1 die Anwendung **geeigneter Datenschutzvorkehrungen** durch den Verantwortlichen umfassen.

Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 25 Abs. 1 DSGVO – Technikgestaltung

- geeignete technische und organisatorische Maßnahmen, wie z. B. Pseudonymisierung, um Datenschutzgrundsätze umzusetzen und um den Anforderungen dieser Verordnung zu genügen

Art. 25 Abs. 2 DSGVO – Voreinstellung

- geeignete technische und organisatorische Maßnahmen zur Sicherstellung der Zweckbindung

Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 32 Abs. 1 DSGVO

- geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten
 - a) Pseudonymisierung und Verschlüsselung
 - b) Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste
 - c) Verfügbarkeit / Zugang bei einem Zwischenfall rasch wiederherzustellen
 - d) Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.



Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 32 Abs. 2 DSGVO

Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch – ob unbeabsichtigt oder unrechtmäßig – **Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang** zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.



Präventive Maßnahmen

Normative Vorgaben in der DSGVO

Art. 33 DSGVO – Meldepflicht an die Aufsichtsbehörde

**Art. 34 DSGVO – Benachrichtigungspflicht an die betroffenen
Personen**

Präventive Maßnahmen

Datenschutzmanagement-System

Um den normativen Vorgaben zu entsprechen, empfiehlt sich ein Datenschutzmanagement-System mit einem Verfahren nach dem PDCA-Zyklus (Plan, Do, Check, Act) zu etablieren.

- kontinuierlicher Verbesserungsprozess
- Umsetzung der erforderlichen technische und organisatorische Maßnahmen
- Verringerung der Eintrittswahrscheinlichkeit für Datenschutzverstöße oder Datenpannen
- Begrenzung des Risikos für die betroffenen Personen und des Schadens
- Erfüllung der Nachweispflicht bei Dokumentation

Präventive Maßnahmen

- Risikobewertung
- Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen
- Erstellung eines Ablaufplans für Datenpannen
 - Festlegung von Verantwortlichkeiten und Rollen
 - Festlegung von Meldekettten, intern und extern
 - Festlegung von zu ergreifenden technischen und organisatorischen Maßnahmen
 - Dokumentation
- Schulung/Sensibilisierung

Präventive Maßnahmen

Technische und organisatorische Maßnahmen bei Postversehen

- Festlegung genauer Vorgaben – ohne Interpretationsspielraum – für den Versand von Briefen/E-Mails
- angemessene Schulung des Personals für den Versand von Briefen/E-Mails
- Anwendung des Vier-Augen-Prinzips
- Deaktivierung der automatischen Vervollständigung bei der Eingabe von E-Mail-Adressen
- eindeutige Bezeichnung von Verteilerlisten
- Aktualisierung/Pflege von Adressdatenbanken

Präventive Maßnahmen

Technische und organisatorische Maßnahmen bei Verlust oder Diebstahl von Datenträgern

- Aktivierung der Geräteverschlüsselung
- Verwendung sicherer Passwörter
- Verwendung einer mehrstufigen Authentifizierung
- Aktivierung von Lokalisierungsfunktionen
- Verwendung einer Software/Anwendung zur Verwaltung mobiler Geräte (Mobile Devices Management, MDM)

Präventive Maßnahmen

Technische und organisatorische Maßnahmen bei Verlust oder Diebstahl von Datenträgern

- soweit möglich und für die betreffende Datenverarbeitung geeignet:
Speicherung der personenbezogenen Daten nicht auf einem mobilen Gerät, sondern auf einem zentralen Back-End-Server
- Verwendung eines sicheren VPN (Virtual Private Network), um mobile Geräte mit Back-End-Servern zu verbinden
- Bereitstellung von physischen Schutzmaßnahmen

Empfehlung

Seien Sie stets auf eine Datenpanne vorbereitet,

- erstellen Sie ein Datenschutz-/pannen-Management-System und
- gehen Sie den Ablauf einer Datenpanne exemplarisch in Ihrem Unternehmen, Ihrer Behörde oder Ihrer Organisation regelmäßig durch.

Kontakt

-  Sächsische Datenschutz-
und Transparenzbeauftragte
Maternistr. 17
01067 Dresden
-  0351 85471101
-  post@sdtb.sachsen.de
-  PGP-Key: sdb.de/kontakt
-  www.datenschutz.sachsen.de
-  social.sachsen.de/@sdtb
-  sdb.de/newsletter

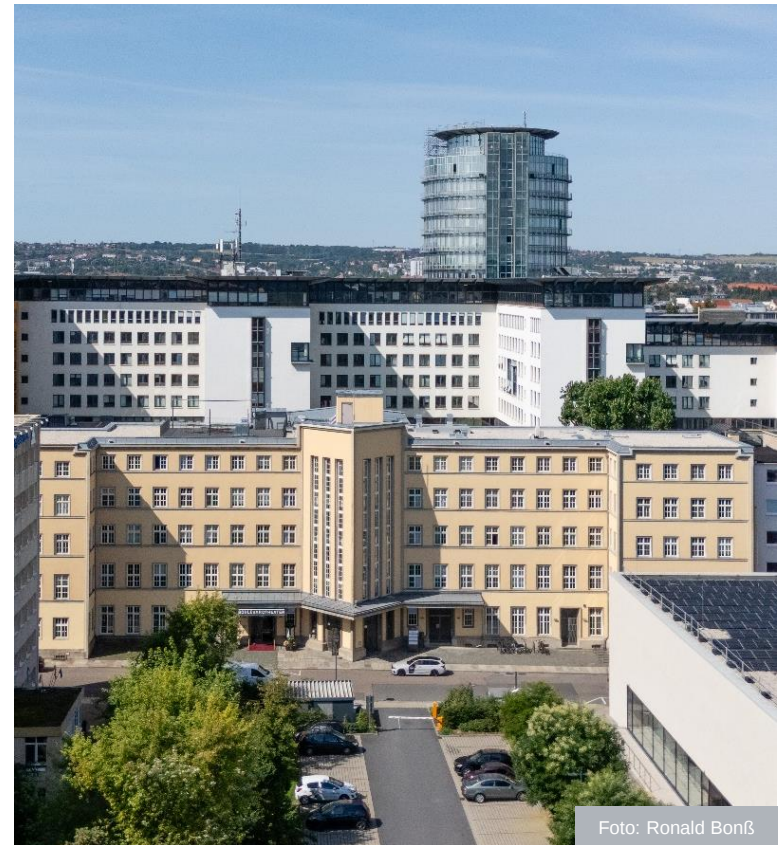


Foto: Ronald Bonß