KRISENKOMMUNIKATION NACH EINEM DATENSCHUTZRECHTLICHEN VORFALL

VORBEREITET AUF DEN ERNSTFALL – KOMMUNIKATION IN DER KRISE

KONGRESS DIGITALE STÄDTE – DIGITALE REGIONEN, 28.09.2022

Fraunhofer SIT

ATHENE
Nationales Forschungszentrum für angewandte Cybersicherheit

IM BLICKPUNKT: ÖFFENTLICHE STELLEN ALS ANGRIFFSZIELE – AUSZUG 2022 BISHER

- Stadtverwaltung **Suhl** (März 2022)
- Stadtverwaltung **Bochum** (März 20229
- Stadt **Dingolfing** (März 2022)
- Cyberangriff auf **Donau-Stadtwerke** (April 2022)
- Stadt **Schriesheim** (April 2022)
- **Universitätsbibliothek** Leipzig (April 2022)
- Website **LKA Hessen** vorübergehend offline (April 2022)
- **IT-Dienstleister** Count+Care angegriffen, großflächige Auswirkungen (Juni 2022)
- **FH Münster** angegriffen (Juni 2022)
- Stadtverwaltung **Burladingen** (Juli 2022)
- Gemeinde **Egelsbach** (September 2022)

Quelle: https://pixabay.com/

KOMMUNIKATION IM CYBERKRISENFALL – VORÜBERLEGUNGEN

- **Gemeinsames Verständnis der Lage** – zwischen IT-Abteilung, Kommunizierenden, Führungsebene
  - Krisenkommunikation sollte „Chefsache“ sein
- Nicht zu früh, aber auch nicht erst nach Öffentlichwerden („vor die Welle“ kommen)
  - **Schnelles proaktives Handeln**
- **Weder zu wenig noch zu viel**:
  - Fehlende Meldung können Konsequenzen haben
  - Nach außen weder Verschleierung noch Wortklauberei
- Im **Nachgang** kontrollierte Selbstkritik

- **Vorab: Notfallplan** inkl. Krisenkommunikationsplan
  - Und: üben!

Quelle: https://pixabay.com/

GEMEINSAM IST MAN WENIGER ALLEIN

- **Wen** muss man hinzuziehen
  - Intern
  - extern
- **Wer** kann und sollte mich unterstützen
  - CERT
  - Polizei
  - BSI
  - Versicherung
- Welche zusätzlichen **Experten**
  - Datenschutz – und IT-Sicherheitsexperten
  - Z.B. Forensiker

Quelle: https://pixabay.com/

RECHTLICHE ANKNÜPFUNGSPUNKTE

- Kritische Infrastrukturen (BSI-Gesetz, BSI-KritisV)
- Strafrecht und Strafverfolgung (Computerbetrug oder –sabotage, Ausspähen von Daten etc.)
- Haftungsrechtliche Fragestellungen
- Versicherungsrechtliche Fragestellungen
- Geheimschutz (Verschlusssachen, Steuer- und Geschäftsgeheimnisse)
- Datenschutzrecht

Quelle: https://pixabay.com/

RECHTLICHE ANKNÜPFUNGSPUNKTE

- Kritische Infrastrukturen (BSI-Gesetz, BSI-KritisV)
- Strafrecht und Strafverfolgung (Computerbetrug oder –sabotage, Ausspähen von Daten etc.)
- Haftungsrechtliche Fragestellungen
- Versicherungsrechtliche Fragestellungen
- Geheimschutz (Verschlusssachen, Steuer- und Geschäftsgeheimnisse)
- **Datenschutzrecht**

Quelle: https://pixabay.com/

WAS DATENSCHUTZ MIT CYBERSICHERHEIT ZU TUN HABEN KANN

- Nicht jeder **datenschutzrechtliche** Vorfall ist auch ein Cybersicherheitsvorfall
- Aber viele **Cybersicherheitsvorfälle** sind datenschutzrechtlich relevant

Quelle: https://pixabay.com/

PERSONENBEZOGENE DATEN IN KOMMUNALEN EINRICHTUNGEN

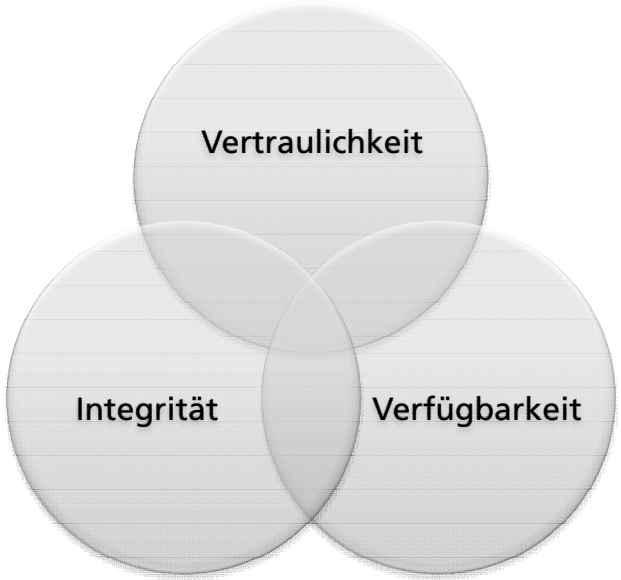
- Personal- und IT-Nutzungsdaten von **MitarbeiterInnen und Abgeordneten/Mitgliedern** der Gemeindevertretungen
- **Meldedaten**
- **Einkommens- und Steuerdaten**
- Bezug von **Sozialleistungen**
- Daten zu **Ordnungswidrigkeiten**
- Daten von **besonders schützenswerten Personen** wie Kinder oder Opfer von Gewalt und Missbrauch
- Daten zu **Ethnizität, Religionszugehörigkeit, Gesundheitsdaten** (Besondere Kategorien personenbezogener Daten, Art. 9 Abs. 1 DSGVO)

Quelle: https://pixabay.com/

CYBERSICHERHEITSVORFÄLLE
DEFINITION

Ungewollte oder unerwartete Ereignisse, wie Angriffe oder unautorisierte Zugriffe, die nachteilige Auswirkungen haben in dem sie eines oder mehrere der Schutzziele der Cybersicherheit beeinträchtigen

- **Vertraulichkeit**
- **Verfügbarkeit**
- **Integrität**



DATENSCHUTZVERLETZUNGEN
DEFINITION

„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; (Art. 4 Nr. 12 DSGVO)

RISIKOBEWERTUNG
FAKTOREN

Eintrittswahrscheinlichkeit des Schadens x Schwere des möglichen Schadens

- **Mögliche Schäden** durch Datenschutzverletzungen: materieller oder immaterieller Natur; bspw. Diskriminierung, Identitätsdiebstahl oder -betrug, finanzieller Verlust, Rufschädigung, wirtschaftliche oder gesellschaftliche Nachteile

- Faktoren zur **Bemessung der Schwere des Schadens** durch Datenschutzverletzungen: Sensibilität der Daten, Schutzbedürftigkeit der Personen, Anzahl betroffener Personen, besondere Eigenschaften des Verantwortlichen

RISIKOBEWERTUNG
BEISPIELE

- Von einem hohen Risiko für die Rechte und Freiheiten betroffener Personen ist beispielsweise auszugehen:

  - **Ransomware-Angriffe** mit Exfiltration von personenbezogenen Daten, wie Personalausweisnummern oder Finanzdaten
  - **Verlust von Speichergeräten**, die in großem Umfang unverschlüsselte Daten, wie Namen, Adressen, Geburtsdatum enthalten

(Europäischer Datenschutzausschuss, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification)

MELDE- UND BENACHRICHTIGUNGSPFLICHT
IM BEREICH DATENSCHUTZ

- **Meldung von Datenschutzverletzungen an die Aufsichtsbehörde**, es sei denn die Datenschutzverletzung führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen (Art. 33 DSGVO).

- **Benachrichtigung betroffener Personen zur Datenschutzverletzung**, wenn die Datenschutzverletzung voraussichtlich zu einem hohen Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person führt (Art. 34 DSGVO).

MELDEPFLICHT IM BEREICH DATENSCHUTZ
INHALT UND FRIST

- **Meldung** bei der zuständigen Aufsichtsbehörde:
  - In Hessen: der Hessische Beauftragte für Datenschutz und Informationsfreiheit

- **Frist: 72 Stunden** nach Bekanntwerden der Verletzung, Verzögerungen sind bei Meldung zu begründen
  - Informationen, die noch nicht vorhanden sind können schrittweise nachgemeldet werden

MELDEPFLICHT IM BEREICH DATENSCHUTZ
INHALT UND FRIST

- **Inhalt der Meldung:**
  - **Beschreibung der Art der Verletzung** (Angabe von Kategorien, Zahl der betroffenen Personen/Datensätze)
  - **Kontakt** des Datenschutzbeauftragten
  - wahrscheinlichen **Folgen** der Datenschutzverletzung
  - Ergriffene oder vorgeschlagene **Maßnahmen** zur Behebung/Abmilderung der Datenschutzverletzung

BENACHRICHTIGUNGSPFLICHT IM BEREICH DATENSCHUTZ

INHALT UND ZEITPUNKT

- Benachrichtigung **betroffener Personen**, in Absprache mit Aufsichtsbehörde und ggf. Strafverfolgungsbehörden
- **Frist: „unverzüglich“,** sofort zur Abmilderung unmittelbarer Schäden, längere Benachrichtigungsfrist kann gerechtfertigt sein, wenn dies notwendig ist, um geeignete Maßnahmen gegen Verletzung zu treffen.
- Inhalt:
  - Mindestangaben: Kontakt Datenschutzbeauftragte, wahrscheinliche Folgen, Maßnahmen zur Behebung/Abmilderung

BENACHRICHTIGUNGSPFLICHT IM BEREICH DATENSCHUTZ

BENACHRICHTIGUNGSKANÄLE

- **Verantwortlicher** benachrichtigt die betroffene Person (Grundsatz **Direktbenachrichtigung**)
  - Ausnahme: unverhältnismäßiger Aufwand, dann stattdessen öffentliche Bekanntmachung oder ähnliche Maßnahme, die betroffene Personen wirksam informiert (Art. 34 Abs. 3 lit. c DSGVO)

- Benachrichtigung per E-Mail, Post, Meldungen auf der Webseite, Pressemeldungen oder in lokalen Zeitungen
- **Keine Kommunikationskanäle**, die durch den Vorfall selbst betroffen sein können

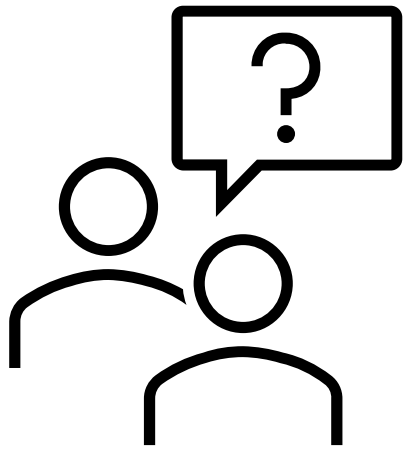
BENACHRICHTIGUNGSPFLICHT IM BEREICH DATENSCHUTZ

SPRACHE UND TRANSPARENZ

- **Benachrichtigungen** haben in klarer und einfacher Sprache zu erfolgen (Art. 34 Abs. 2 DSGVO)
  - Benachrichtigung soll betroffene Personen in die Lage versetzen Vorkehrungen zur Minderung nachteiliger Auswirkungen treffen zu können
  - Grundverständnis eines durchschnittlichen Internetnutzenden kann nicht vorausgesetzt werden
  - ggf. alternative Sprachversionen

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT.

- **Gibt es Fragen?**



LITERATUR

- Artikel-29-Datenschutzgruppe, Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten, zuletzt überarbeitet und angenommen am 6.02.2018
- Europäischer Datenschutzausschuss, Guidelines 01/2021 on Examples regarding Personal Data Breach Notification, Version 2.0, Stand 14.12.2021.
- Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Kurzpapier Nr. 18 Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018.
- Heise Online „Witten: Bei Cyberangriff erbeutete Daten im Darknet veröffentlicht“, 17.11.2021 https://www.heise.de/news/Hacker-veroeffentlichen-Wittener-Daten-Buergermeister-warnt-6269952.html