Kammer der Ziviltechniker:innen |
Architekt:innen und Ingenieur:innen
Wien. Niederösterreich. Burgenland

zt:

Herzlich willkommen zum zt: Mediengespräch

zt:

Von der Pflicht zur Praxis:

Datenschutz für KMU einfach gemacht

TOMs – technische und organisatorische Maßnahmen

Gesprächspartner

DI Wolfgang Fiala
Fachgruppe Informationstechnologie der zt: Kammer,
Autor der TOMs-Standards

DI Dr. Peter Gelber
Fachgruppe Informationstechnologie der zt: Kammer,
Autor der TOMs-Standards

DI Dr. Wolfgang Prentner
Vorsitzender der Fachgruppe Informationstechnologie
der zt: Kammer

Dr. Matthias Schmidl
Leiter der Österreichischen Datenschutzbehörde

Heinz Tuma
Vorstandsmitglied des Verbands Österreichischer
Software Innovationen (VÖSI)

dsb
Republik Österreich
Datenschutz
behörde

VÖSI
VERBAND ÖSTERREICHISCHER SOFTWARE INNOVATIONEN
DATENSCHUTZinICT

zt:

Agenda

Begrüßung Kammer	**VP Peter Bauer**	**3–5 min**	
Begrüßung VÖSI	**Heinz Tuma**	**3–5 min**	
Begrüßung FG IT	**Wolfgang Prentner**	**3–5 min**	
Keynote	**Matthias Schmidl**	**15–20 min**	
TOMs-Standards	**Wolfgang Fiala**	**6–8 min**	**ca. 09.30 Uhr**
Praxisbeispiel 1	**Peter Gelber**	**5–7 min**	
Praxisbeispiel 2	**Wolfgang Prentner**	**5–7 min**	
Praxisbeispiel 3	**Wolfgang Fiala**	**5–7 min**	

Ende des offiziellen Teils | Weiterführendes Gespräch am Buffet ca. 10.00 Uhr

Begrüßung

Heinz Tuma
Vorstandsmitglied des VÖSI,
Mentor der SIG Datenschutz,
Geschäftsführer der InfraSoft
Datenservice Ges.m.b.H.

Zielsetzungen des VÖSI

Verband Österreichischer Software Innovationen (VÖSI)
Besteht seit 39 Jahren

Aufgabenbereich

- Stärkung der österreichische Softwarebranche national und international
- Rahmenbedingungen für nachhaltige wirtschaftliche Erfolge in diesem Segment schaffen
- Gesellschaftlichen Diskurs zu Software fördern

Zielsetzungen des VÖSI

Der VÖSI

- Aktive Interessensvertretung der Softwarebranche in Österreich
- Möglichst große Zahl an Mitgliedern
- Gesellschaftliche Akzeptanz von Software als Baustein eines modernen Lebens

Kommunikation mit Politikern über

- wirtschaftliche und gesellschaftliche Rahmenbedingungen für die Softwarebranche in Österreich

Optimierung der internationalen Vernetzung

- Bedeutung der österreichischen Softwarebranche nach außen tragen und durch gezielte Nutzung von Exportchancen das Wachstum stärken

Zielsetzungen des VÖSI

Mission

- Vernetzung der Mitglieder durch direkten Wissensaustausch in Arbeitskreisen
- VÖSI-Mitglieder lernen voneinander und entwickeln gemeinsame Positionen und Aktivitäten
- Stellung von Software als zentraler Bestandteil der österreichischen Wertschöpfung
- Software-Business ausbauen

Zielsetzungen des VÖSI

SIG Datenschutz

- Unser VÖSI-Mitglied DSGVO-zt GmbH ist die erste Datenschutz-Zertifizierungsstelle in Österreich
- Leitung der Special Interest Group Datenschutz des VÖSI:
  ZT DI Wolfgang Fiala und DI Dr. Peter Gelber

Ziele der SIG Datenschutz

- Datenschutz sichtbar machen
- Unternehmen können mit einem eigenen DSGVO-Zertifikat die DSGVO-Konformität stärken

Begrüßung

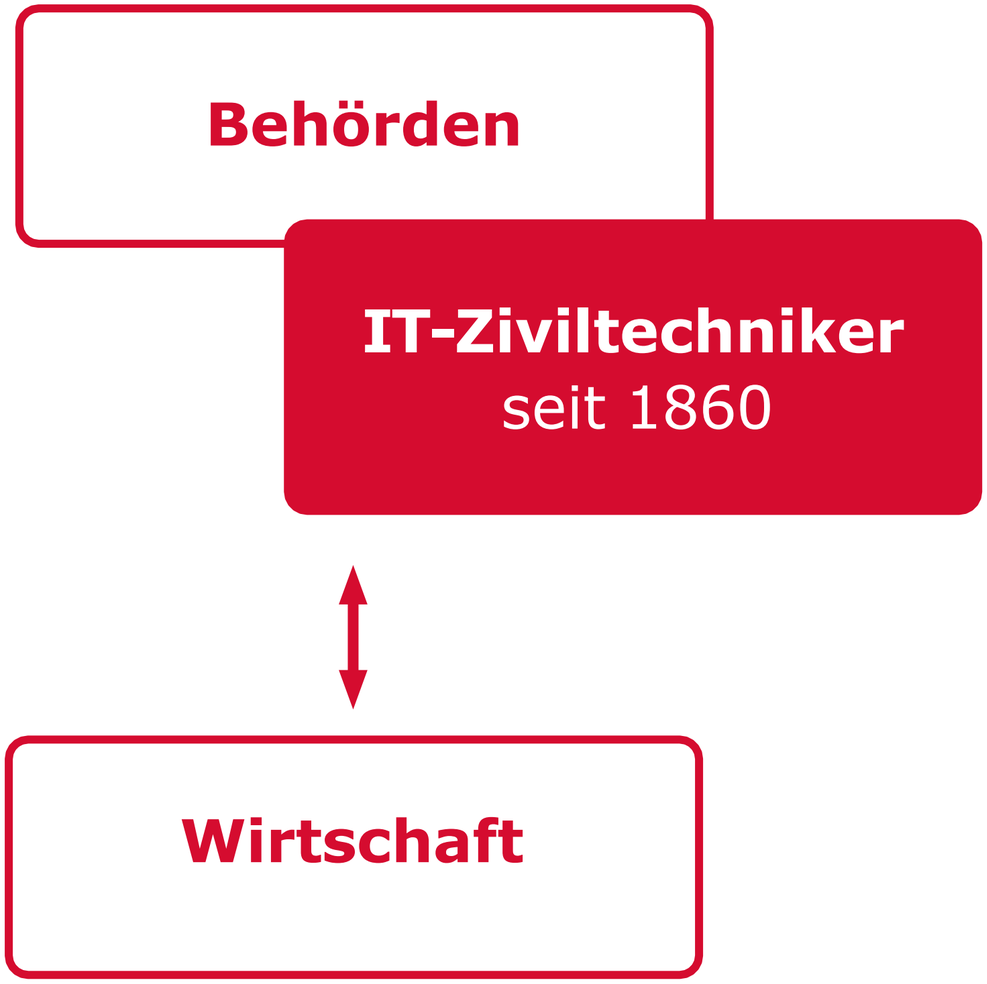
DI Dr. Wolfgang Prentner
Fachgruppe Informationstechnologie

Unabhängig.
Planen.
Prüfen.

Nur sicher mit dem Siegel.
Ihre Ziviltechniker:innen

zt:

IT-Ziviltechniker: behördennahe Prüfungen

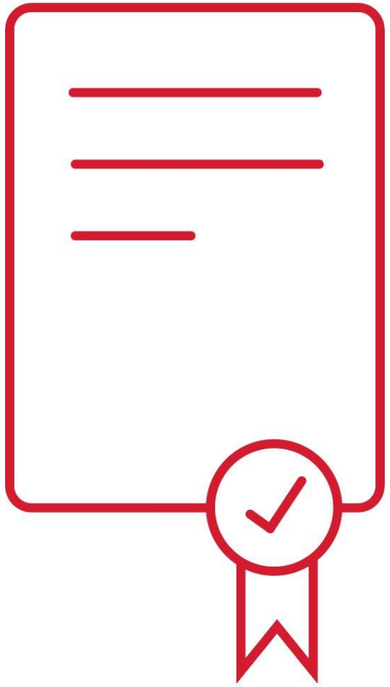


Befugnis des IT-Ziviltechnikers

- IT-Beratung
- IT-Planung
- IT-Prüfung
- IT-Mediation
- IT-Überwachung
- Beurkundungen
- Rechnungs-prüfung
- Software-Treuhandschaft

Ausgefertigte Befunde sind öffentliche Urkunden

Die von **IT-Ziviltechnikern** ausgefertigten und gesiegelten **Befunde** sind öffentliche Urkunden gemäß § 3 Abs. 3 Ziviltechnikergesetz und § 292 Zivilprozessordnung (ZPO) und werden von **Gerichten sowie Verwaltungsbehörden** in derselben Weise anerkannt, als wären sie von **Behörden ausgestellt.**



Flyer der IT-Ziviltechniker

Download Flyer

Kontakt

Fachgruppe Informationstechnologie

Vorsitzender:
DI Dr. Wolfgang Prentner

Mitglieder:
DI Wolfgang Fiala, stellvertretender Vorsitzender
DI Dr. Peter Gelber
DI Thomas Hrdinka
DI Dr. Kurt P. Judmann
DI (FH) Oliver Pönisch
DDI Mag. Gernot W. Schmied
DI Andreas Tomasek
DI Dr. Johannes Weidl-Rektenwald

Referentin:
Katharina Schöck

Verzeichnis der Ziviltechniker unter:
https://ziviltechniker.at

Karlsgasse 9
1040 Wien

T: 01 505 17 81
E: fg_it@arching.at
W: wien.arching.at

Keynote

Datensicherheit und Informationssicherheit

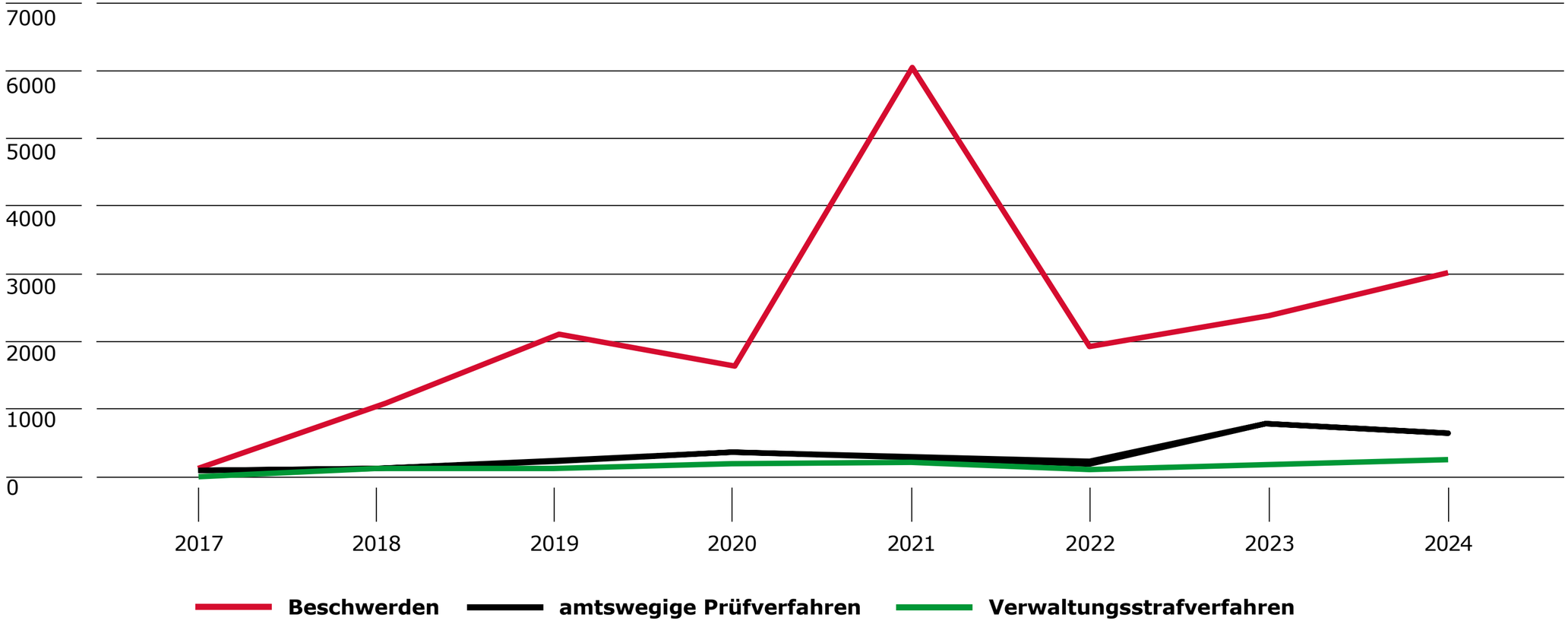
Dr. Matthias Schmidl
Leiter der Österreichischen Datenschutzbehörde

1. Allgemeines

Datensicherheit und Informationssicherheit

Verfahrenszahlen

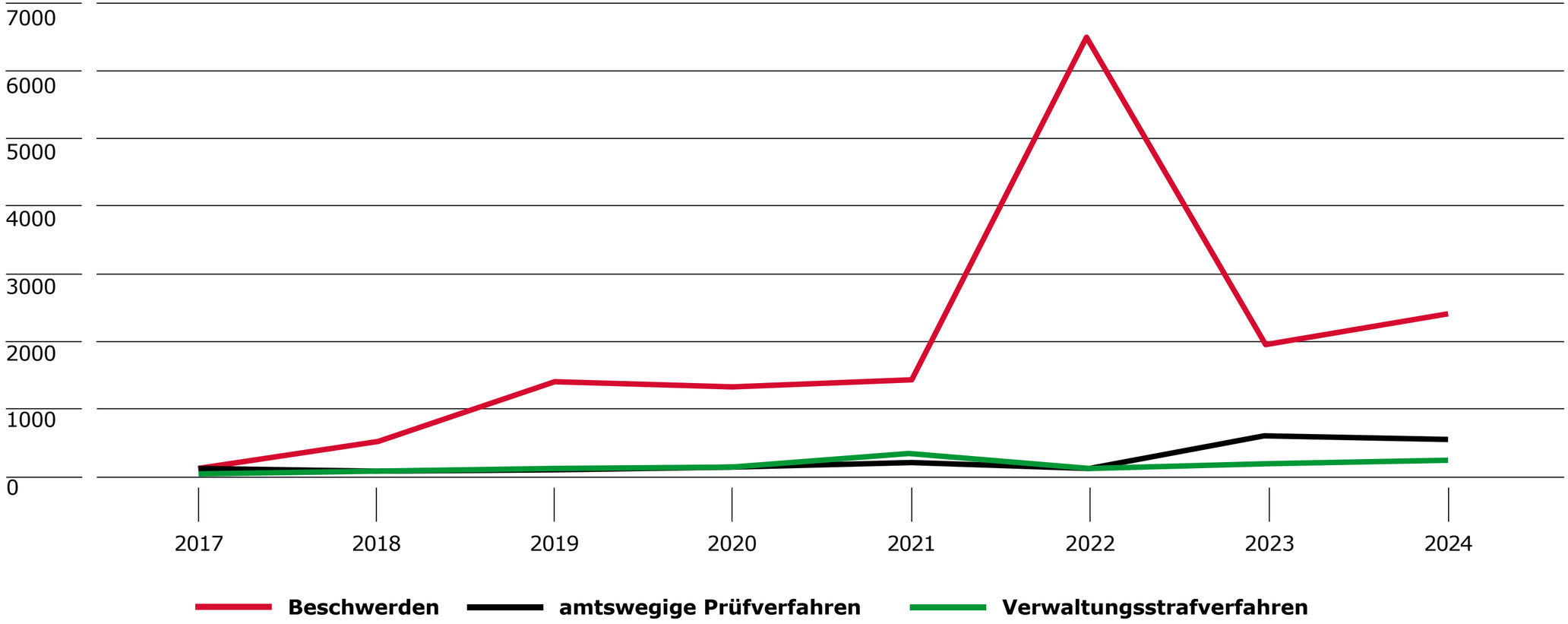
Entwicklung der Verfahrenszahlen (Quelle: Datenschutzberichte)



Datensicherheit und Informationssicherheit

Erledigungszahlen

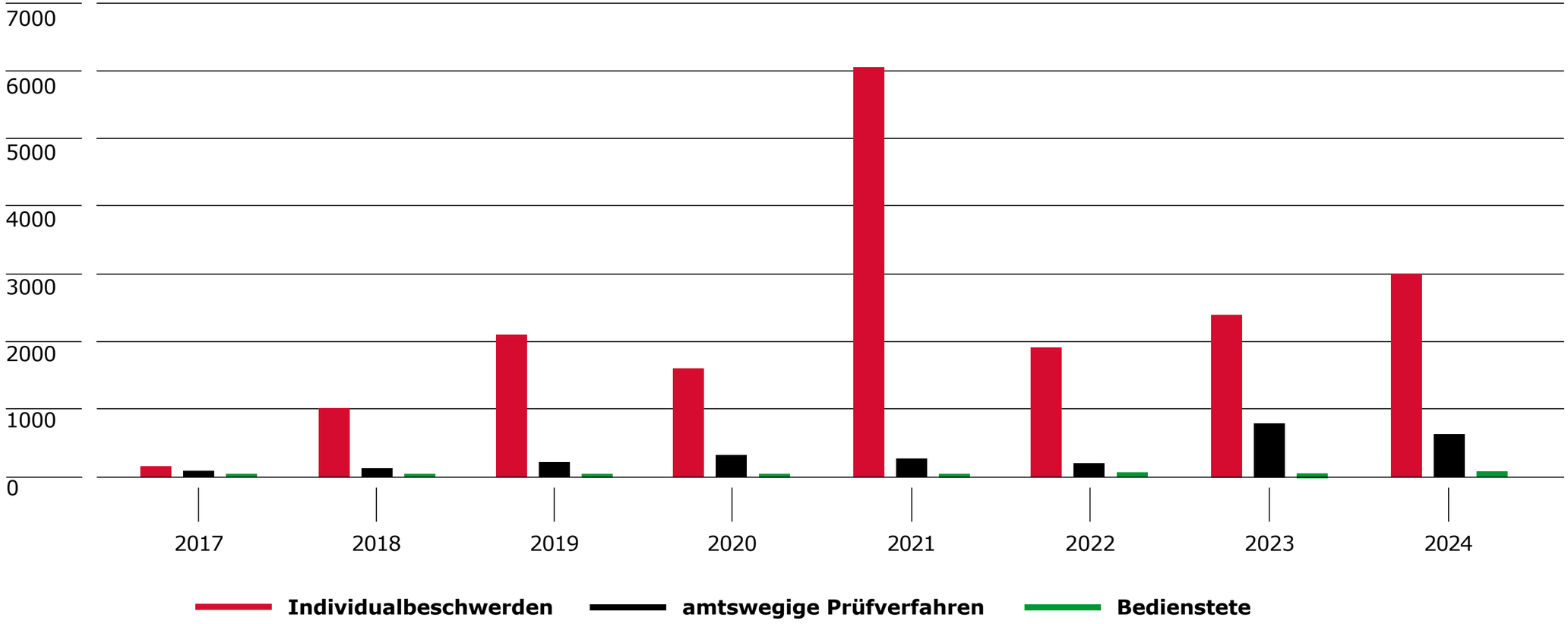
Entwicklung der Erledigungszahlen (Bescheide und Einstellungen, Quelle: Datenschutzberichte)



Datensicherheit und Informationssicherheit

Verhältnis Individualbeschwerden/amtswegige Prüfverfahren/Bedienstete

(Quelle: Datenschutzberichte)



Netzwerk Digitalisierung 1

„Netzwerk Digitalisierung“: Erklärung am 6.11.2024 unterzeichnet

Strukturierte Zusammenarbeit zwischen:

- Bundeswettbewerbsbehörde (BWB)
- Datenschutzbehörde (DSB)
- Energie Control Austria (e-control)
- Finanzmarktaufsicht (FMA)
- Kommunikationsbehörde Austria (KOA)
- RTR, Fachbereich Telekom (RTR)
- Schienen Control GmbH (Schienen Control)
- Telekom-Control-Kommission (TKK)

Datensicherheit und Informationssicherheit

Netzwerk Digitalisierung 2

- Strukturierte Kontakte zu den genannten (unabhängigen) Aufsichts- und Regulierungsbehörden in Österreich
- Ziel: unterschiedliche und widersprüchliche Entscheidungen im Digitalbereich verhindern (Erinnerung: Datenschutz = Querschnittsmaterie)
- Regelmäßiger Informations- und Erfahrungsaustausch
- Gemeinsame Veranstaltungen
- ABER: jeweilige Eigenständigkeit und Unabhängigkeit bleibt gewahrt

2. Datensicherheits-maßnahmen nach Art. 32 DSGVO

Verordnung (EU) 2016/679 – DSGVO

Artikel 32: Sicherheit der Verarbeitung (Auszug)

(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.

Verordnung (EU) 2016/679 – DSGVO

Artikel 32: Sicherheit der Verarbeitung (Auszug)

(2)
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.

(3)
Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

Datensicherheit und Informationssicherheit

Verordnung (EU) 2016/679 – DSGVO

Artikel 32: Sicherheit der Verarbeitung (Auszug)

(4)
Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

Datensicherheit und Informationssicherheit

Verordnung (EU) 2016/679 – DSGVO

- Artikel 32 normiert eine **Pflicht** des Verantwortlichen/Auftragsverarbeiters
- Artikel 32 normiert einen **risikobasierten Ansatz**
- **Datensicherheitsmaßnahmen können/müssen variieren,** je nachdem, wie die Verarbeitung erfolgt (kein „Schema F")
- **Wirtschaftliche Überlegungen** (Implementierungskosten) können eine Rolle spielen, sind aber **nur einer von mehreren zu beachtenden Faktoren**
- Programme, mit denen bspw. Gesundheitsdaten verarbeitet werden, unterliegen folglich anderen Datensicherheitsmaßnahmen als Programme, die bspw. lediglich der Rechnungslegung dienen

Datensicherheit und Informationssicherheit

Verordnung (EU) 2016/679 – DSGVO

Mangelnde Datensicherheitsmaßnahmen können Gegenstand

- einer **Beschwerde** an die DSB gemäß Art. 77 DSGVO,
- eines **amtswegigen Prüfverfahrens** nach Art. 57 Abs. 1 lit. h DSGVO,
- eines **Verwaltungsstrafverfahrens** nach Art. 58 Abs. 2 lit. i i. V. m. Art. 83 DSGVO,
- eines **Zivilverfahrens (einschließlich Schadenersatz, auch immateriell!)** nach Art. 79 und Art. 82 DSGVO

sein.

3. Rechtsprechung der DSB zu Art. 32 DSGVO

Rechtsprechung DSB 1

Bescheid vom 13.9.2018, GZ DSB-D123.070/0005-DSB/2018 (RIS):

- Beschwerde nach Art. 77 DSGVO
- Beschwerdeführerin behauptete unzureichende Datensicherheitsmaßnahmen zu ihrem Nachteil (keine Pseudonymisierung ihrer Daten)
- Abweisung der Beschwerde
- Beschwerdeführerin konnte keine sie betreffende Rechtsverletzung nachweisen (potenzielle Hackerangriffe sind unzureichend)
- **Kein subjektives Recht auf Ergreifung spezifischer Datensicherheitsmaßnahmen**

Datensicherheit und Informationssicherheit

Rechtsprechung DSB 2

Bescheid vom 9.10.2019, GZ DSB-D130.073/0008-DSB/2019 (RIS):

- Beschwerde nach Art. 77 DSGVO
- Minderjähriger Beschwerdeführer, vertreten durch den Vater, behauptete unzureichende Datensicherheitsmaßnahmen, weil er E-Mail-Nachrichten von einer Datingplattform erhält, ohne dort angemeldet zu sein
- Stattgabe der Beschwerde
- Beschwerdeführer wurde in seinem **subjektiven Recht auf Geheimhaltung (§ 1 DSG) verletzt,** weil es die Beschwerdegegnerin (= Betreiberin der Datingplattform) verabsäumt hat, adäquate Datensicherheitsmaßnahmen zu ergreifen
- Hier: kein „Double-Opt-in-Verfahren“, obwohl es geboten gewesen wäre

Rechtsprechung DSB 3

Straferkenntnis vom 17.2.2021, GZ 2020-0.675.335 (D550.325) (nicht rechtskräftig):

- Strafe: **4 Mio. EUR** wegen unzureichender Datensicherheitsmaßnahmen durch ein **Kreditinstitut**
- Ungesicherte Excel Liste mit Kundendaten (einschließlich Kontoinformationen) wurde verwendet
- Auszüge dieser Liste wurden versehentlich an (andere) Kunden versendet und damit unbefugten Dritten offengelegt
- Verantwortlicher hat es verabsäumt, adäquate Datensicherheitsmaßnahmen (hier: zumindest Verschlüsselung der Excel-Liste) zu ergreifen, und dadurch gegen seine Pflicht nach Art. 32 DSGVO verstoßen
- Verstöße gegen Art. 32 DSGVO werden nach Art. 83 Abs. 4 lit. a mit Geldbuße von bis zu 10 Mio. EUR bzw. bis zu 2 % des gesamten weltweiten Jahresumsatzes des Vorjahres bestraft, **je nachdem, welcher Betrag höher ist**
- **BVwG:** Reduzierung der Strafe auf 50.000 EUR; Beschluss vom 26.3.2024, W137 2241630-1; Amtsrevision erhoben

4. Rechtsprechung des EuGH zu Art. 32 DSGVO

Rechtsprechung EuGH 1

Urteil vom 14.12.2023, C 340/21:

Die **Art. 24 und 32 [DSGVO]** sind dahin auszulegen, dass

eine unbefugte Offenlegung von bzw. ein unbefugter Zugang zu personenbezogenen Daten durch „Dritte“ im Sinne von Art. 4 Nr. 10 dieser Verordnung **allein nicht ausreicht,** um anzunehmen, dass die technischen und organisatorischen Maßnahmen, die der für die betreffende Verarbeitung Verantwortliche getroffen hat, nicht „geeignet“ im Sinne der Art. 24 und 32 dieser Verordnung waren.

Rechtsprechung EuGH 2

Urteil vom 14.12.2023, C 340/21:

Art. 32 [DSGVO] ist dahin auszulegen, dass

die Geeignetheit der vom Verantwortlichen nach diesem Artikel getroffenen technischen und organisatorischen Maßnahmen von den nationalen Gerichten **konkret zu beurteilen** ist, wobei die mit der betreffenden Verarbeitung verbundenen Risiken zu berücksichtigen sind und zu beurteilen ist, **ob Art, Inhalt und Umsetzung dieser Maßnahmen diesen Risiken angemessen sind.**

Rechtsprechung EuGH 3

Urteil vom 14.12.2023, C 340/21:

Der in **Art. 5 Abs. 2 [DSGVO]** formulierte und in **Art. 24** dieser Verordnung konkretisierte **Grundsatz der Rechenschaftspflicht des Verantwortlichen** ist dahin auszulegen, dass

im Rahmen einer auf Art. 82 der Verordnung gestützten Schadenersatzklage der für die betreffende Verarbeitung Verantwortliche **die Beweislast dafür trägt, dass die von ihm getroffenen Sicherheitsmaßnahmen im Sinne von Art. 32 dieser Verordnung geeignet waren.**

5. EDSA

Datensicherheit und Informationssicherheit

Case Digest

- One Stop Shop case digest on Security of Processing and Data Breach Notification
- www.edpb.europa.eu/our-work-tools/our-documents/support-pool-experts-projects/one-stop-shop-case-digest-security_en

Datensicherheit und Informationssicherheit

EU-gefördertes Projekt „DSGVO4KMU“

- Zusammenarbeit zwischen Wirtschaftskammer Österreich und Datenschutzbehörde
- Förderung im Rahmen von Citizens , Equality, Rights and Values Programme (CERV)
- Ziel ist Stärkung von **Datenschutzwissen für kleine und mittelständische Unternehmen**
- Selfcheck-Tool samt Reifegradbewertung hinsichtlich Umsetzung der DSGVO im Unternehmen
- Informationen, Templates, Checklisten (u. a. zur Datensicherheit)
- Umsetzung bis **Februar 2027**

Datensicherheit und Informationssicherheit

EU-gefördertes Projekt „Arc II“ – Olivia

- EU-gefördertes Projekt, umgesetzt von HR-Datenschutz-Aufsichtsbehörde
- Ähnlich wie DSGVO4KMU, aber bereits abgeschlossen
- Webseite: https://olivia-gdpr-arc.eu/en/topic/
- Enthält u. a. Informationen zu „organisational measures“ und „technical measures“

Einführung

Art. 32 DSGVO und TOMs

DI Wolfgang Fiala
Fachgruppe Informationstechnologie

Technische und organisatorische Maßnahmen

Art. 32 DSGVO:
geeignete technische und organisatorische Maßnahmen

Problem: **Stand der Technik** – dafür gibt es keine Norm

- Fachgruppe IT veröffentlichte einen allgemein gültigen Standard unter Berücksichtigung des Stands der Technik
- **Creative-Commons-Lizenz**

Artikel 32 DSGVO – technische und organisatorische Maßnahmen

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.

Die Maßnahmen schließen u. a. Folgendes ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten; die Fähigkeit, die **Vertraulichkeit,** Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der **Wirksamkeit der technischen und organisatorischen Maßnahmen** zur Gewährleistung der Sicherheit der Verarbeitung.

Zusammenhänge grafisch dargestellt

Stand der Technik ist keine Norm!

Allgemeine Anerkennung

Stand der Wissenschaft und Forschung	**Stand der Technik**	Allgemeine anerkannte Regeln der Technik

Bewährung in der Praxis

Motivation für ein Standard-Werk

Schaffung eines Standards für TOMs. Dieser dient als

- **Unterstützung für Unternehmen (KMU)**
- **Leitfaden für Gutachten von Sachverständigen**
- **Benchmark für die Datenschutzbehörde**

Medienpräsenz der Fachgruppe Informationstechnologie

Nutzungsrechte

Eigentümer und Herausgeber
- **Fachgruppe Informationstechnologie der zt: Kammer**

Freier Download – **kostenfrei** und
- beliebig änderbar (löschen, hinzufügen)
- vervielfältigbar
- verkaufbar

Einzige Auflage:
- Die **Autoren** Wolfgang Fiala und Peter Gelber **müssen genannt** werden

Praxisbeispiel 1

Ransomware-Angriff

DI Dr. Peter Gelber
Fachgruppe Informationstechnologie

Praxisbeispiel 1: Ransomware-Angriff, unzureichende TOMs? (1/4)

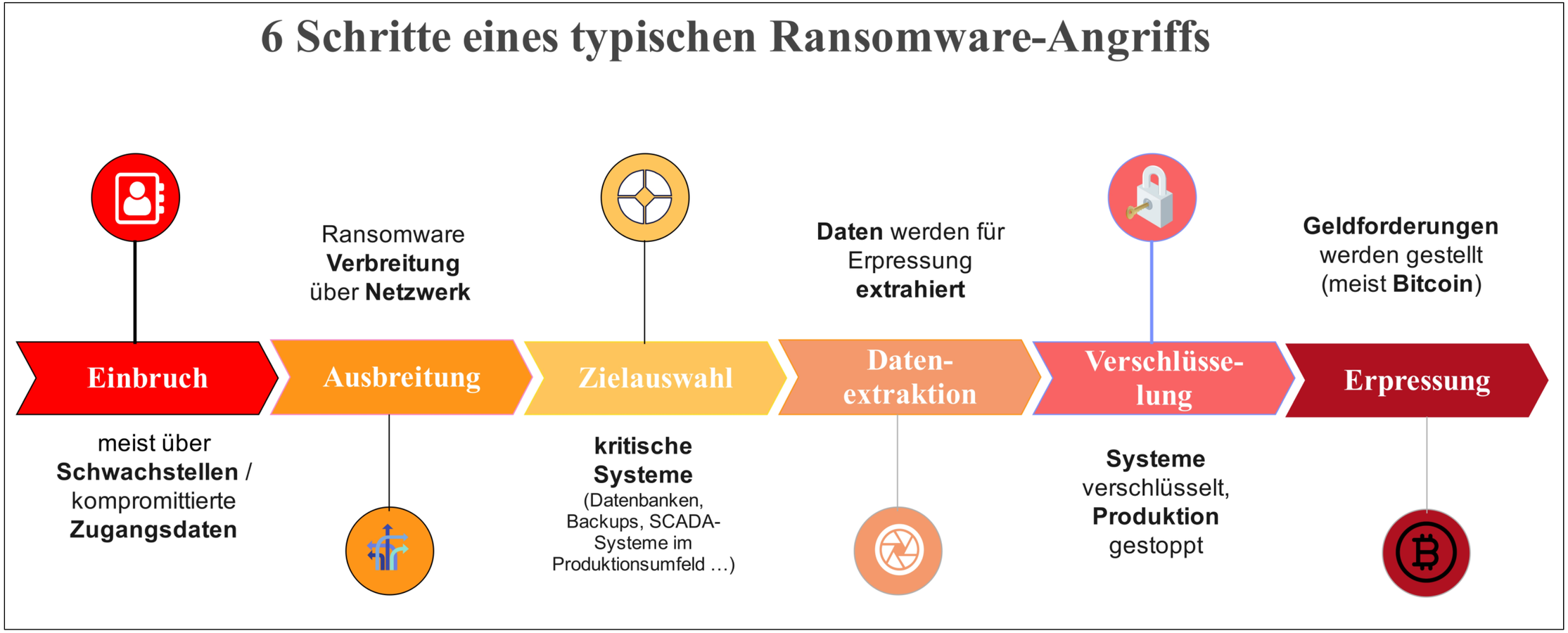
Dokumentierte Cyberangriffe 2025 in Deutschland

Top-3 dokumentierten Cyberangriffe in Deutschland von 1.Jän bis 9.Sep 2025

Anzahl von Cyberangriffen	Spalten										
Zeilenbeschriftungen	Jän	Feb	Mär	Apr	Mai	Jun	Jul	Aug	Sep	Insgesar	%
Ransomware	11	13	32	5	13	5	3	5	3	90	44%
Datendiebstahl	1	4	2	7	8	4	3	5		34	17%
Denial of Service				1	3		2	1		7	3%
Insgesamt	**14**	**26**	**39**	**29**	**35**	**15**	**19**	**21**	**5**	**203**	

Quelle: https://www.security-insider.de/cyberangriffe-auf-unternehmen-in-deutschland-2025-analyse-a-f71268d8ef2cc593d2cc64a82df23ee2/

Praxisbeispiel 1: Ransomware-Angriff, unzureichende TOMs? (2/4)



1. **Einbruch:** Angreifer nutzen Schwachstellen bzw. kompromittierte Zugangsdaten
2. **Ausbreitung:** Ransomware verbreitet sich über das Netzwerk

3. **Zielauswahl:** kritische Systeme wie Datenbanken, Backups, SCADA-Systeme …
4. **Datenextraktion:** Daten werden für Erpressung extrahiert und übermittelt

5. **Verschlüsselung:** Systeme werden verschlüsselt, Produktionsbereiche gestoppt
6. **Erpressung:** Geldforderungen werden gestellt (Kryptowährung)

Ransomware-Angriff, unzureichende TOMs? (3/4)

Zuordnung der Schritte zu den „Standards für TOMs“

Ransomware-Schritte	Kapitel in „Standards für TOMs"
1. Einbruch ins System	
a) Kompromittierte Passwörter	4 „Authentifizierung“, 5 „Rollen-/Rechtekonzept“, 6 „Endgeräte“ (6.4–6.19),
b) Bekannte Schwachstellen	8 „Serversysteme“, 9 „Webservices und Webanwendungen“, 10 „Netzwerk“
2. Ausbreitung im System	
a) Client	4 „Authentifizierung“, 5 „Rollen-/Rechtekonzept“, 6 „Endgeräte“(6.4–6.19),
b) Server	8 „Serversysteme“, 10 „Netzwerk“
3. Zielauswahl	
a) Zugriff auf Clients	Siehe 1.a)
b) Zugriff auf Serverdienste	8 „Serversysteme“, 10 „Netzwerk“
c) Notfallpläne torpedieren	14 „Business Continuity“
4. Datenextraktion	
a) Clientsysteme	4 „Authentifizierung“, 5 „Rollen-/Rechtekonzept“
b) Serversysteme	8 „Serversysteme“, 10 „Netzwerk“
5. Verschlüsselung	
a) Begrenzung der Bereiche	10 „Netzwerk“, 14 „Business Continuity“
6. Erpressung	
a) Geldforderungen	14 „Business Continuity“

Ransomware-Angriff, unzureichende TOMs? (4/4)

Präventivmaßnahmen

Technische Maßnahmen
- Aktuelle Software-Updates, Patches, Antivirus-Software und Firewalls
- Regelmäßige Datensicherungen (Backups)
- Netzwerksegmentierung

Mitarbeiterschulung
- Sicherheitsbewusstsein, Phishing usw.

Vereinbarung mit dem Betriebsrat
- Betriebsurlaub (bei Betriebsunterbrechung)

Festlegung des Notbetriebs (Krisenplan)
- Im Office
- In der Produktion (Ablaufdaten), alternative Produktion mit veralteten Maschinen

Manueller Notbetrieb
- Lieferscheine, Rechnungen, Zeitaufzeichnung usw.
- Überweisungen

Bankvereinbarung für Lösegeld
- Bereitstellung Kryptowährung
- Vermittler-Präventiv-Vereinbarung (Geldwäsche)

Praxisbeispiel 2

Ransomware-Angriff durch IT-Ziviltechniker

DI Dr. Wolfgang Prentner
Fachgruppe Informationstechnologie

Cybersicherheit: Lagebild 9/2025 (BM für Inneres)

Lage CYBERCRIME

Cyberkriminalität

Trendsymbole: stark steigend | mäßig steigend | gleichbleibend | mäßig rückläufig | stark rückläufig

Ringfarbe: hohe Anzahl | geringe Anzahl

Trendabweichung 12 Monate: über Ø | unter Ø

Trends basierend auf bei der Polizei eingelangten Anzeigen

Bundesministerium Inneres | Bundesministerium Landesverteidigung | Bundeskanzleramt | Bundesministerium Europäische und internationale Angelegenheiten

Social Hacking – Red Team Operations

Praxisbeispiel 3

Bußgelder wegen mangelnder TOMs

DI Wolfgang Fiala
Fachgruppe Informationstechnologie

Bußgeld u. a. wegen unzureichender TOMs

Ausgangssituation: Österreichische Datenschutzbehörde

- Der Verantwortliche hatte es versäumt, **ausreichende technische und organisatorische Maßnahmen** zu ergreifen, was zu einer Datenpanne führte
- Darüber hinaus weigerte sich der Verantwortliche, **die betroffenen Personen über die Datenpanne zu informieren**
- Die Datenschutzbehörde stellte außerdem fest, dass der Verantwortliche bestimmte **Daten ohne ausreichende Rechtsgrundlage** verarbeitet, einen Auftragsverarbeiter ohne den erforderlichen Vertrag eingesetzt und keinen geeigneten Datenschutz-beauftragten benannt und gemeldet hat

Bescheid der Datenschutzbehörde

- Covid-19-Testlabor
- Bescheiddatum: 6.6.2024
- Begründung: Art. 5 Abs. 1 lit. f, Art. 25 Abs. 1, **Art. 32 Abs. 1 und 2 DSGVO**

Bußgeld: 100.000 EUR

Bußgeld wegen unzureichender TOMs

Ausgangssituation: Deputy Data Protection Ombudsman

- Aufgrund eines **Softwarefehlers** konnten sich Kunden des Verantwortlichen in die Bankkonten anderer Kunden einloggen, **was zu finanziellen Verlusten führte**

Bescheid der Datenschutzbehörde

- Bank S-Pankki Oyj
- Keine angemessenen technischen und organisatorischen Maßnahmen
- Kein angemessenes Sicherheitsniveau gewährleistet
- Bescheiddatum: 8.9.2025
- Begründung: Art. 5 Abs. 1 lit. f, Art. 25 Abs. 1, **Art. 32 Abs. 1 und 2 DSGVO**

Bußgeld: 1,8 Mio. EUR

Europaweite Bußgelder

EU-Strafen

- Anzahl verhängter Bußgelder: **318**
- Gesamtsumme aller Bußgelder: **1.190.036.370 EUR**

Davon mit Art. 32 DSGVO als Begründung:

- Anzahl der Strafen: **73**
- % der Strafen mit Art. 32: **23 %**
- Strafvolumen: **250 Mio. EUR**
- Strafvolumen im Schnitt: **3,4 Mio. EUR**

Europaweite Bußgelder

Länder	Summe Bußgelder
IRELAND	652.069.500
THE NETHERLANDS	325.456.040
ITALY	120.488.777
FRANCE	32.522.225
SPAIN	26.462.146
CZECH REPUBLIC	13.900.000
SWEDEN	5.216.400
FINLAND	3.256.950
GREECE	3.251.980
LITHUANIA	2.406.276
POLAND	2.212.915
AUSTRIA	1.630.200
Insgesamt	**1.190.036.370**

Länder	Anzahl
SPAIN	113
ITALY	59
ROMANIA	26
FRANCE	22
GERMANY	21
POLAND	19
GREECE	8
THE NETHERLANDS	7
CROATIA	6
AUSTRIA	5
IRELAND	5
SWEDEN	4
Insgesamt	**318**

zt:

Kammer der Ziviltechniker:innen |
Architekt:innen und Ingenieur:innen
Wien. Niederösterreich. Burgenland

zt: