BRANDEFENSE COUNTRY REPORT · GERMANY 2026

# Brandefense Deutschland Bericht zur Cyberbedrohungslage 2026

Identitäten, Erpressung und Betriebsfähigkeit in einer vernetzten Wirtschaft

Odin by Brandefense
Untersuchungszeitraum: 1. Januar–22. November 2026
Version 1.0 · Öffentliche Forschungsausgabe · TLP:CLEAR · 8.–22. November 2026

**457**
deutsche Ransomware-Einträge, die jeweils eine Erpressungsbehauptung dokumentieren

**107 von 249**
beobachtete Domains mit einem aktuellen Zugangsdatenangebot

**6**
erläuterte Behauptungen; keine Zahl bestätigter Einbrüche

**13 von 25**
beobachtete Finanzdomains mit aktuellem Zugangsdatenangebot

INHALT

# Inhalt

**Translated with AI**

Diese Ausgabe wurde mit KI aus der englischen Originalfassung übersetzt. Bei Abweichungen ist die englische Fassung massgeblich.


| | | |
|---|---|---|
| 01 | Zusammenfassung | 05 |
| | Berichtskarte | 09 |
| 02 | Deutschlands digitaler und sicherheitsbezogener Kontext | 10 |
| 03 | Nationale Exposition: ein ausgewähltes Domainportfolio | 14 |
| 04 | Untergrundaktivität und Einordnung von Behauptungen | 21 |
| 05 | Bestätigte Vorfälle und Aktivitäten nach Branchen | 35 |
| 06 | Hacktivismus, DDoS und Betriebstechnik | 56 |
| 07 | Akteure und belegte Beziehungen | 61 |
| 08 | Betrug, Identität und Folgeschäden | 71 |
| 09 | Banken und Finanzdienstleistungen | 76 |
| 10 | Regulierung und nationale Reaktion | 81 |
| 11 | Ausblick und bedingte Planung | 86 |
| 12 | Maßnahmenplan | 90 |
| A | Anhang A. Geltungsbereich und Beleggrenzen | 97 |
| B | Anhang B. Belegregister | 100 |
| C | Anhang C. Quellen | 103 |
| D | Anhang D. Glossar | 108 |
| | Über diesen Bericht | 110 |



| | |
|---|---|
| Vorstand und Geschäftsleitung | 01 05 11 12 |
| CISO und Sicherheitsleitung | 03 04 05 07 12 |
| SOC und Identitätsteams | 04 06 07 B |
| Betrugsabwehr und Kundenschutz | 05 08 09 |
| Recht und Kommunikation | 05 06 10 12 |

# Über diese Ausgabe

Mit KI übersetzt. Diese Ausgabe wurde aus der englischen Fassung übersetzt. Bei Abweichungen ist die englische Ausgabe maßgeblich.

Mit KI-Unterstützung erstellt. Belege und Grenzen stehen unmittelbar bei den Ergebnissen.

Deutschlands sichtbare Bedrohungslage verbindet gestohlene Identitätsdaten, Erpressungsbehauptungen und unterbrochene Dienste. Bestätigte Gefährdungen müssen eingedämmt werden, während wesentliche Betriebsabläufe erhalten bleiben.

**457**

deutsche Ransomware-Einträge im angefragten Zeitraum; kriminelle Behauptungen

**1.221.949**

beobachtete Beiträge mit Deutschlandbezug; keine Vorfallzahl

**107 von 249**

beobachtete Domains mit aktuellem Zugangsdatenangebot

**4**

Führungsentscheidungen mit überprüfbaren Abschlusskriterien

# Inhalt und Lesewege

| Kapitel | Frage |
|---|---|
| 1 Zusammenfassung | Welche Entscheidungen haben Vorrang? |
| 2 Kontext | Welche deutschen Betriebsbedingungen prägen die Reaktion? |
| 3 Organisationsexposition | Welche gemessenen Signale brauchen eine Prüfung? |
| 4 Untergrundaktivitäten | Was belegen die gespeicherten Beiträge tatsächlich? |
| 5 Vorfälle nach Branchen | Was haben Organisationen und Behörden bestätigt? |
| 6 DDoS und Betriebstechnik | Wie unterscheiden sich Verfügbarkeitsbehauptungen und betriebliche Folgen? |
| 7 Akteure und Beziehungen | Welche Verbindungen sind durch welche Quelle belegt? |
| 8 Betrugsökonomie | Wie kann aus gestohlenen Informationen ein weiterer Schaden entstehen? |
| 9 Banken | Wie unterstützen Finanzdomainbeobachtungen die Reaktion? |
| 10 Regulierung | Welche Meldefristen und Verantwortlichkeiten gelten? |
| 11 Ausblick | Welche bedingten Szenarien rechtfertigen Vorbereitung? |
| 12 Maßnahmenplan | Wer handelt, und was belegt den Abschluss? |
| Anhänge A–D | Geltungsbereich, Belege, Quellen und Begriffe |

KAPITEL 01

# Zusammenfassung

01

DIESES KAPITEL BEANTWORTET

Welche Ergebnisse rechtfertigen unmittelbare Entscheidungen für deutsche Organisationen?

**457**

deutsche Ransomware-Einträge, die jeweils eine Erpressungsbehauptung dokumentieren


Vier Entscheidungen für Führungskräfte 07

Das Jahr in Zahlen 07

KAPITEL 01

# Zusammenfassung

KURZFASSUNG

Die Belege für Deutschland begründen drei Prioritäten: Identitätsschutz, Wiederherstellung und Dienstleisteraufsicht. Ransompedia verzeichnet 457 deutsche Einträge, mehr als die 311 des gesamten Jahres 2025. Öffentliche Mitteilungen unterscheiden Datendiebstahl, missbrauchte Zugangsdaten und Dienstunterbrechungen. Aktuelle Hochschulvorfälle, Kühlanlagenwarnungen und Dienstleistermeldungen unterstreichen diese Unterschiede. Die Expositionsmomentaufnahme unterstützt Kontoprüfungen im ausgewählten Portfolio. Prüfen Sie eigene Konto- und Dienstleisterwarnungen, üben Sie die Wiederherstellung und benennen Sie getrennte Verantwortliche für Betriebsfähigkeit und Meldeentscheidungen.

Dieser Bericht verbindet gespeichertes Untergrundmaterial und Ransomware-Einträge von Brandefense mit öffentlichen Quellen. Beiträge, Einträge, öffentliche Vorfälle und Domainexpositionsbeobachtungen bilden getrennte Populationen. Sie werden niemals zu einer nationalen Angriffszahl addiert. [S1][S2]

Der angefragte Zeitraum endet am 22. November. Der Bericht berücksichtigt die an diesem Tag verfügbaren Informationen; bei der Erhebung war der Stichtag noch nicht abgeschlossen. Kapitel 5.7 behandelt die letzten zwei Wochen gesondert. Das Veröffentlichungsdatum belegt keinen Angriffsbeginn.

**1. Die Erpressungseinträge verteilen sich auf viele Gruppenbezeichnungen.** Deutschland weist 457 Einträge auf, gegenüber 311 im gesamten Jahr 2025. Auf Qilin, SafePay und The Gentlemen entfallen 161 Einträge, entsprechend 35,2 %. Andere Bezeichnungen umfassen die übrigen 296. Verglichen werden ein Teiljahr und ein vollständiges Jahr; daraus folgt keine Wachstumsrate für gleiche Zeiträume. Ein Eintrag belegt eine öffentliche kriminelle Behauptung, weder Verschlüsselung noch Diebstahl oder finanziellen Verlust. [S2]

**2. Bestätigter Identitätsmissbrauch verlangt eine andere Reaktion als ein Verkaufsangebot.** Die TUM beschreibt, dass zentrale Zugangsdaten einschließlich eines Administratorkontos gegen ein Campussystem eingesetzt wurden. Ihre Wiederherstellungsmeldung verlangte Passwortwechsel und Zwei-Faktor-Authentifizierung. Vergleichbare Belege rechtfertigen die Eindämmung von Konto- und Sitzungszugriffen. Sie belegen keinen Diebstahl sämtlicher Hochschulkonten. [S11][S12]

**3. Dienstleistervorfälle können nach der Wiederherstellung als Betrug weiterwirken.** Ein behördlicher Krankenhauswarnhinweis beschreibt direkte Erpressungsnachrichten an Patienten mit gestohlenen Informationen. Ein gesonderter Hinweis zu Hotelsoftware nennt spätere betrügerische Nachrichten. Diese dokumentierten Abläufe verbinden Informationsverlust mit Folgeschäden. Recht, Kundenbetreuung und Betrugsabwehr sollten vor der Wiederinbetriebnahme eingebunden sein. [S16][S18]

**4. Verfügbarkeit, Datenverlust und Prozesssicherheit benötigen jeweils eigene Belege.** Die Deutsche Bahn bestätigte im Februar Störungen ihrer Buchungs- und Auskunftsdienste. Die amtliche Novemberwarnung zu Kühlanlagen betrifft industrielle Steuerungen. Die Fälle begründen unterschiedliche Notfallübungen. Sie belegen weder einen gemeinsamen Akteur noch, dass ein Websiteausfall Zugriff auf betriebliche Steuerungssysteme belegt. [S7] [S8][S21]

**5. Aktuelle Zugangsdatenangebote erfordern eine Prüfung eigener Konten.** Für 107 von 249 beobachteten Domains waren Zugangsdaten zum Verkauf angeboten. Das ausgewählte Portfolio enthält mindestens 636.397 Gerätezuordnungen und 125.422.358 Zugangsdatenzuordnungen. Diese überlappenden Beobachtungen zählen keine eindeutigen Personen oder bestätigten Einbrüche. Für eine ausgewählte Domain fehlt ein vollständiger Expositionsdatensatz. [S87]

## Vier Entscheidungen für Führungskräfte

1. **Gleichen Sie Identitätswarnungen mit der eigenen Umgebung ab.** Richten Sie einen Meldeweg ein, prüfen Sie Kontozugehörigkeit und Aktualität, kontrollieren Sie Berechtigungen und widerrufen Sie erforderlichenfalls Sitzungen. Dokumentieren Sie jede Bewertung (§3.4, §12).
2. **Testen Sie Wiederherstellung und Mindestbetrieb gemeinsam.** Stellen Sie einen kritischen Dienst isoliert wieder her. Zeigen Sie zugleich einen nutzbaren Ersatzablauf, wenn das normale Identitäts- oder Buchungssystem ausfällt (§5–6).
3. **Binden Sie Dienstleister früh in Vorfallentscheidungen ein.** Klären Sie, wer Kundendaten hält, Fernwartung steuert und zeitnah Belege liefern kann. Üben Sie Meldungen mit einem kritischen Dienstleister (§8, §10).
4. **Richten Sie Mitteilungen nach dem belegten Sachverhalt aus.** Unterscheiden Sie Behauptung, Ausfall, Datenzugriff und Prozessmanipulation. Benennen Sie eine verantwortliche Auskunftsperson und den nächsten Aktualisierungstermin (§6, §12).

## Das Jahr in Zahlen

**1.221.949**
Beobachtete Beiträge mit Deutschlandbezug im angefragten Zeitraum
WAS SIE NICHT MISST
Nationale Vorfall- oder eindeutige Opferzahl

**457**
deutsche Ransomware-Einträge im angefragten Zeitraum 2026
WAS SIE NICHT MISST
bestätigte Einbrüche oder einzelne Personen

**311**
deutsche Einträge im gesamten Jahr 2025
WAS SIE NICHT MISST
Vergleichswert für denselben Jahresabschnitt

**62 / 55 / 44**
Einträge unter Qilin / SafePay / The Gentlemen
WAS SIE NICHT MISST
einzelne Betreiber oder deren Erfolgsquoten

**77**
Einträge mit der Branchenbezeichnung Fertigung
WAS SIE NICHT MISST
nationale Vorfallrate der Fertigungsindustrie

**295 / 77 / 56 / 61**
Einträge für Frankreich / Niederlande / Polen / Österreich
WAS SIE NICHT MISST
bevölkerungsbereinigtes Risiko oder Erkennungsleistung

**249 von 250**
ausgewählte Domains mit Expositionsbeobachtungen
WAS SIE NICHT MISST
unabhängige Rechtsträger oder nationale Häufigkeit

**107 von 249**
beobachtete Domains mit aktuellem Zugangsdatenangebot
WAS SIE NICHT MISST
verkaufte Konten oder bestätigte Einbrüche

Die Vergleichsländer wurden ausschließlich als Beispiele zur Einordnung ausgewählt; ihre Auswahl beinhaltet weder eine Rangfolge noch eine politische Bewertung.

Quellen: Odin by Brandefense [S1], Ransompedia [S2] und die Expositionsmomentaufnahme [S87]. Länderzuordnungen und Gruppennamen beschreiben den Eintragsbestand. Branchenbezeichnungen belegen nicht die genaue Geschäftstätigkeit jeder genannten Organisation.

KERNAUSSAGEN

**01**

Nutzen Sie Erpressungseinträge zur Vorbereitung der Wiederherstellung, nicht als Zahl bestätigter Einbrüche.

**02**

Prüfen Sie Identitätsbelege vor einschneidenden Eindämmungsmaßnahmen.

**03**

Dienstleister-, Kunden- und Betriebsreaktionen benötigen Verantwortliche neben der technischen Wiederherstellung.

# Berichtskarte

Zwölf Kapitel, fünf Lesewege. Beginnen Sie bei Ihrer Verantwortung; die Grenzen der Belege gelten für jede Schlussfolgerung.

| | | |
|---|---|---|
| **Vorstand und Geschäftsleitung** | Reaktion ausstatten und Betriebsfähigkeit testen | 01 05 11 12 |
| **CISO und Sicherheitsleitung** | Gefährdungen und Abhängigkeiten priorisieren | 03 04 05 07 12 |
| **SOC und Identitätsteams** | Nutzbare Belege von Behauptungen unterscheiden | 04 06 07 B |
| **Betrugsabwehr und Kundenschutz** | Folgeschäden verhindern | 05 08 09 |
| **Recht und Kommunikation** | Richtige Fristen und Formulierungen anwenden | 05 06 10 12 |

Die Belegarten heißen **Beobachtung**, **Behauptung**, **offizielle Bestätigung** und **analytische Schlussfolgerung**. Ein beobachtetes Angebot bleibt hinsichtlich seines Inhalts eine Behauptung. Bei einem bestätigten Vorfall können Akteur, Datenmenge und Zugangsweg weiterhin ungeklärt sein.

KAPITEL 02

# Deutschlands digitaler und sicherheitsbezogener Kontext

02

DIESES KAPITEL BEANTWORTET

Welche Betriebsbedingungen bestimmen eine angemessene Reaktion in Deutschland?

**5**

Belegpopulationen, die getrennt bleiben müssen


2.1 Vor einem Zahlenvergleich die Zeiträume trennen 11

2.2 Gemeinsame Dienste schaffen gemeinsame Reaktionsabhängigkeiten 12

2.3 Politisch gerahmte Aktivitäten sorgfältig zuordnen 12

2.4 Regulierung ist bereits eine betriebliche Anforderung 12

2.5 Was dies für Führungskräfte ändert 13

KAPITEL 02

# Deutschlands digitaler und sicherheitsbezogener Kontext

KURZFASSUNG

Deutsche Organisationen stehen vor überlappenden Identitäts-, Dienstleister- und Verfügbarkeitsrisiken. Behörden beschreiben diese mit unterschiedlichen Meldesystemen und Beobachtungszeiträumen. Ihre Statistiken lassen sich nicht mit Untergrundeinträgen addieren. Zuständigkeiten umfassen Informationssicherheit, Datenschutz und Branchenaufsicht. Ordnen Sie Dienst, Rechtsträger, Dienstleister und zuständigen Meldeweg vor einem Vorfall zu.

## 2.1 Vor einem Zahlenvergleich die Zeiträume trennen

Der BSI-Lagebericht 2026 behandelt den Zeitraum 1. Juli 2025–30. Juni 2026. Seine Veröffentlichung im November bietet daher eine aktuelle Auswertung eines früheren Beobachtungszeitraums. Er ist keine Erfassung bis zum Stichtag dieses Berichts. [S3]

Die BKA-Veröffentlichung vom Mai nennt 1.041 angezeigte Ransomware-Angriffe für 2025. Die 457 Ransompedia-Einträge betreffen ein anderes Jahr, eine andere Quelle und eine andere Einheit. Keine Zahl bildet den fehlenden Teil der anderen. Eine Anzeige kann unveröffentlicht bleiben; ein Eintrag muss nie zu einem bestätigten Vorfall werden. [S4][S2]

Die Berliner Datenschutzaufsicht verzeichnete von Januar bis September 2026 insgesamt 1.550 Datenschutzmeldungen: 1.303 im nicht-öffentlichen und 247 im öffentlichen Bereich. Dazu gehören auch Datenschutzverletzungen ohne böswilligen Einbruch. Es handelt sich um regionale Meldungen, nicht um eine nationale Cyberangriffszahl. [S35]

Die folgenden Unterschiede verhindern unzutreffende Vergleiche.

| Population | Einheit | Passende Entscheidung |
|---|---|---|
| Untergrundbeiträge | veröffentlichte Nachrichten und Angebote | relevante Behauptungen zu eigenen Ressourcen prüfen |
| Erpressungseinträge | öffentliche kriminelle Behauptungen | Wiederherstellung und Mitteilungen vorbereiten |
| Polizeiliche Anzeigen | nach polizeilichen Definitionen gemeldete Straftaten | angezeigte Kriminalität einordnen |
| Datenschutzmeldungen | gemeldete Verletzungen des Schutzes personenbezogener Daten | Risiko für betroffene Personen bewerten |
| Bestätigte Mitteilungen | Aussagen einer Organisation oder Behörde | Abläufe und Reaktionsentscheidungen vergleichen |

## 2.2 Gemeinsame Dienste schaffen gemeinsame Reaktionsabhängigkeiten

Die öffentlichen Fälle zeigen verschiedene Abhängigkeiten: zentrale Hochschulidentitäten, externe Kundendatendienste, Kommunikationsanbieter und ferngewartete Anlagen. Eine technische Beziehung kann mehrere Rechtsträger und betriebliche Verantwortliche betreffen. Zählen Sie betroffene Kunden getrennt von Vorfällen beim Anbieter.

Unsere Schlussfolgerung ist praktisch. Ein Dienstverzeichnis sollte Geschäftsfunktion, Identitätsabhängigkeit, Datenverantwortlichen, Dienstleisterkontakt und Ersatzbetrieb zeigen. Eine reine Vertragsliste erklärt nicht, wie ein Ausfall eine Station, einen Fahrgast oder ein Labor erreicht.

Für eine Hochschule lautet die Frage, ob die zentrale Anmeldung vor Einschreibefristen sicher wiederhergestellt werden kann. Für einen Hersteller geht es um die sichere Sperrung von Dienstleisterzugängen bei fortlaufender Produktion. Eine Behörde muss wesentliche Bürgerdienste ermöglichen, während die Dokumentenprüfung weiterläuft.

Dies sind aus den Fällen abgeleitete Planungsfragen. Der Bericht behauptet weder eine einheitliche Architektur einer gesamten Branche noch, dass alle Organisationen die genannten Kontrollen versäumt hätten.

## 2.3 Politisch gerahmte Aktivitäten sorgfältig zuordnen

BSI und BfV beschreiben Messenger-Phishing gegen hochrangige Personen aus Politik, Militär, Diplomatie und Journalismus. Das BSI hält staatliche Unterstützung für plausibel; seine Rückschau nennt Zuordnungen anderer Länder gesondert. Der Bericht gibt jede Bewertung als Position der jeweiligen Quelle wieder. [S5][S6]

Ein politisches Ziel belegt kein politisches Motiv. Bei einem Parteikonto-Fall im Oktober meldeten die Ermittlungsbehörden zu diesem Zeitpunkt keine Hinweise auf einen politischen Hintergrund. Extern gehostete E-Mail- und Wiederherstellungswege sollten unabhängig von der Zugehörigkeit geschützt werden. [S41]

Der Bericht bezieht keine Position zu Wahlen, Parteien, Regierungsentscheidungen, Russland–Ukraine, Israel–Gaza oder China. Sprache, ein genannter Anlass und die Selbstbeschreibung eines Akteurs belegen weder Nationalität noch staatliche Steuerung. Kein Wahlergebnis wird hier einem Cybervorfall zugeschrieben.

## 2.4 Regulierung ist bereits eine betriebliche Anforderung

Deutschlands NIS2-Umsetzung trat am 6. Dezember 2025 in Kraft. Betroffene Organisationen sollten Geltungsbereich und betriebliche Pflichten anhand des geltenden Rechts bestimmen. Der Gesetzgebungsstand eines Nachbarlandes ist dafür kein Maßstab. [S30]

Datenschutz- und Finanzaufsichtsmeldungen haben eigene Auslöser. Eine Dienstleistermitteilung kann eine Kenntnisbewertung beim Verantwortlichen anstoßen; ein Ausfall kann eine zusätzliche branchenbezogene Prüfung verlangen. Kapitel 10 trennt diese Entscheidungen und nennt Nachweise.

## 2.5 Was dies für Führungskräfte ändert

Nutzen Sie einen gemeinsamen Vorfallakt für gemeinsame Fakten, dokumentieren Sie Meldeentscheidungen aber getrennt. Er sollte Kenntniszeitpunkt, betroffenen Dienst, möglicherweise gefährdete Personen und weiterhin ungeklärte Punkte unterscheiden.

Benennen Sie für jede kritische Abhängigkeit einen betrieblich Verantwortlichen. Die Sicherheit kann feststellen, ob Zugangsdaten eingesetzt wurden. Der Geschäftsverantwortliche entscheidet über den vertretbaren Mindestbetrieb. Recht und Datenschutz bestimmen Meldeweg und Begründung.

KERNAUSSAGEN

**01**

Nationale Statistiken und Untergrundeinträge beschreiben unterschiedliche Populationen und Zeiträume.

**02**

Gemeinsame Technik kann mehrere Organisationen betreffen, ohne mehrere unabhängige Einbrüche zu bedeuten.

**03**

Klären Sie rechtlichen Geltungsbereich und Meldeverantwortung vor dem Ereignis.

KAPITEL 03

# Nationale Exposition: ein ausgewähltes Domainportfolio

DIESES KAPITEL BEANTWORTET

Welche gemessenen Expositionssignale müssen die ausgewählten Organisationen prüfen?

**107 von 249**

beobachtete Domains mit einem aktuellen Zugangsdatenangebot


3.1 Universumskarte 15
3.2 Aktuelle Angebote und gemessene Signale 16
3.3 Geräte und Zugangsdaten 18
3.4 Kontoprüfung und Eindämmung 19
3.5 Dokumente, Ähnlichkeitsdomains und passive Kontrollen 19
3.6 Zuständigkeit für die Reaktion 20

KAPITEL 03

# Nationale Exposition: ein ausgewähltes Domainportfolio

KURZFASSUNG

Für 107 von 249 beobachteten Domains waren bei der Prüfung Zugangsdaten zum Verkauf angeboten. Das ausgewählte Portfolio enthält mindestens 636.397 Gerätezuordnungen und 125.422.358 Zugangsdatenzuordnungen. Diese Beobachtungen überschneiden sich; sie zählen keine eindeutigen Personen oder bestätigten Einbrüche. Für eine der 250 ausgewählten Domains fehlt ein vollständiger Expositionsdatensatz. Prüfen Sie aktuelle Angebote, untersuchen Sie relevante Mitarbeitergerätezuordnungen und übergeben Sie andere Kontobelege an den zuständigen Dienstverantwortlichen.

## 3.1 Universumskarte

| Punkt | Definition |
|---|---|
| Ausgewählte Population | 250 gezielt ausgewählte Domains in 10 Branchengruppen; 25 Kandidaten je Gruppe |
| Beobachtete Population | 249 Domains; Industrie und Technologie umfasst 24 Beobachtungen aus 25 ausgewählten Domains |
| Auswahl | Dienst- und Branchenrelevanz; keine Umsatzrangliste oder national repräsentative Stichprobe |
| Einheit | Domainzuordnung; rechtliche Eigentümerschaft und Unabhängigkeit der vertretenen Organisationen bleiben ungeprüft |
| Momentaufnahme | 21.–22. November 2026; kumulierte Geräte-, Zugangsdaten-, Dokument- und Marktbeobachtungen, keine reine Vorfallpopulation 2026 |
| Ähnlichkeitsdomains | Vorherige 30 Tage; ähnliche Benennung belegt keinen missbräuchlichen Einsatz |
| Erwähnungsbeobachtungen | Vorherige 365 Tage bis 18. November 2026; getrennt von der Expositionsmomentaufnahme |
| Überschneidung | Datensätze können in Quellen, Domains und Personen mehrfach vorkommen; verwandte Dienste können denselben Betreiber haben |
| Passive Ergebnisse | Kein abgeschlossener Konfigurationsdatensatz; fehlende Messwerte zu Sicherheitskontrollen bleiben nicht verfügbar |

Das Portfolio ist ausgewählt, nicht repräsentativ. Seine Domainzahlen belegen keine Anzahl unabhängiger Rechtsträger. Der fehlende Datensatz bleibt außerhalb des beobachteten Nenners. Expositionsmomentaufnahme und Vorfallzeitraum betreffen unterschiedliche Perioden. [S87]

## 3.2 Aktuelle Angebote und gemessene Signale

Die nationale Atlas-Kennzahl beträgt 61 von 100 für die 249 Domains mit vollständigen Expositionsbeobachtungen. Sie beschreibt das Portfolio, keine nationale Häufigkeit. Die Tabelle enthält Signalzahlen, keine Branchen- oder Organisationsbewertungen. [S87]

### Aktuelle Zugangsdatenangebote erfordern Prüfungen in den ausgewählten Branchen

Zellen zeigen Domains mit dem Signal / beobachtete Domains je Branche. Aktuelle Zugangsdatenangebote sind korallenrot dargestellt.

| | Aktuelles Angebot | Frühere Angebote | Mitarbeitergerätezuordnungen | Dokumentbeobachtun |
|---|---|---|---|---|
| Öffentliche Verwaltung | 2/25 | 2/25 | 10/25 | 18/25 |
| Regional- und Kommunalverwaltung | 9/25 | 9/25 | 19/25 | 23/25 |
| Banken und Finanzen | 13/25 | 12/25 | 20/25 | 21/25 |
| Versicherungen | 10/25 | 10/25 | 18/25 | 21/25 |
| Hochschulen und Forschung | 21/25 | 21/25 | 24/25 | 23/25 |
| Industrie und Technologie | 11/24 | 11/24 | 22/24 | 23/24 |
| Energie und Infrastruktur | 4/25 | 4/25 | 16/25 | 14/25 |
| Verkehr und Logistik | 9/25 | 9/25 | 11/25 | 11/25 |
| Verbraucherdienste und Kommunikation | 22/25 | 22/25 | 22/25 | 23/25 |
| Gesundheit und Lebenswissenschaften | 6/25 | 6/25 | 18/25 | 15/25 |

Quelle: Expositionsbeobachtungen für 249 von 250 ausgewählten Domains, 21.–22. November 2026. Kumulative, überlappende Domainzuordnungen; keine unabhängigen Organisationen, eindeutigen Personen oder bestätigten Einbrüche [S87].

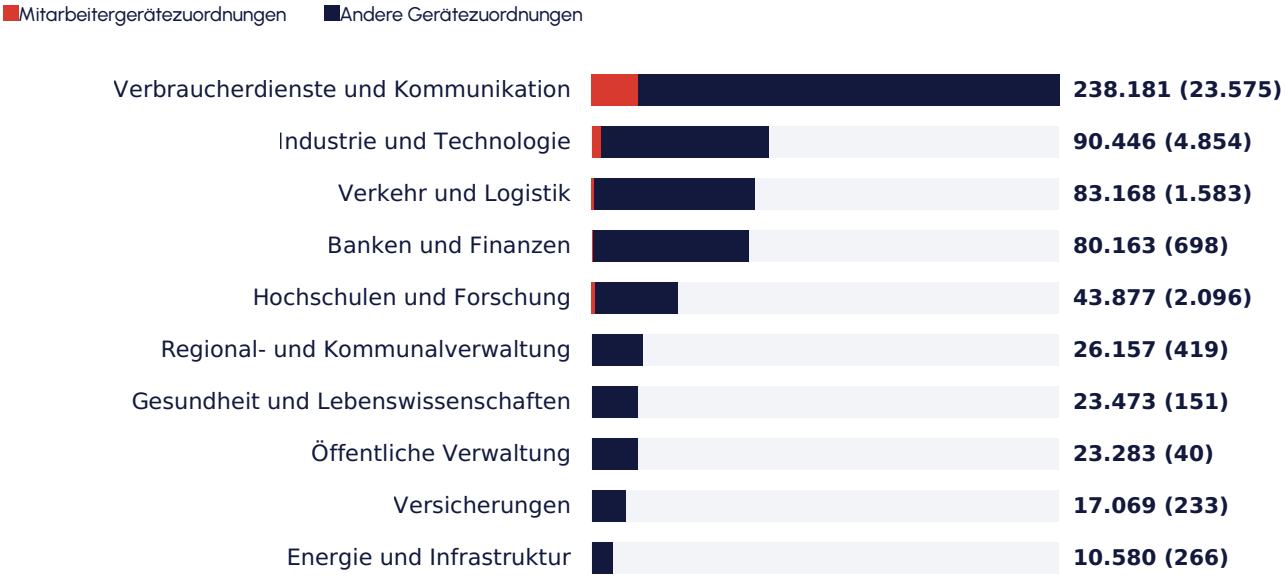
| Branche | Beobachtete Domains | Aktuelle Zugangsdatenangebote | Frühere Angebote | Domains mit Mitarbeitergerätezuordnungen | Domains mit Dokumentbeobachtungen |
|---|---|---|---|---|---|
| Öffentliche Verwaltung | 25 | 2 | 2 | 10 | 18 |
| Regional- und Kommunalverwaltung | 25 | 9 | 9 | 19 | 23 |

| Branche | Beobachtete Domains | Aktuelle Zugangsdatenangebote | Frühere Angebote | Domains mit Mitarbeitergerätezuordnungen | Domains mit Dokumentbeobachtungen |
|---|---|---|---|---|---|
| Banken und Finanzen | 25 | 13 | 12 | 20 | 21 |
| Versicherungen | 25 | 10 | 10 | 18 | 21 |
| Hochschulen und Forschung | 25 | 21 | 21 | 24 | 23 |
| Industrie und Technologie | 24 | 11 | 11 | 22 | 23 |
| Energie und Infrastruktur | 25 | 4 | 4 | 16 | 14 |
| Verkehr und Logistik | 25 | 9 | 9 | 11 | 11 |
| Verbraucherdienste und Kommunikation | 25 | 22 | 22 | 22 | 23 |
| Gesundheit und Lebenswissenschaften | 25 | 6 | 6 | 18 | 15 |
| Gesamt | 249 | 107 | 106 | 180 | 192 |

Quelle: Zuordnungen von Brandefense Blackhole und Atlas-Expositionsbeobachtungen vom 21.–22. November 2026 [S87]. Die Angebotszahlen betreffen Domains mit einem Angebot, keine verkauften Konten oder bestätigten Einbrüche.

## 3.3 Geräte und Zugangsdaten

### Die meisten Gerätezuordnungen liegen außerhalb der Mitarbeiterklassifikation




Quelle: Expositionsbeobachtungen für 249 von 250 ausgewählten Domains, 21.–22. November 2026. Kumulative, überlappende Domainzuordnungen; keine unabhängigen Organisationen, eindeutigen Personen oder bestätigten Einbrüche [S87].

| Branche | Beobachtete Domains | Gerätezuordnungen, mindestens | Mitarbeitergerätezuordnungen | Zugangsdatenzuordnungen |
|---|---|---|---|---|
| Öffentliche Verwaltung | 25 | 23.283 | 40 | 54.026 |
| Regional- und Kommunalverwaltung | 25 | 26.157 | 419 | 869.088 |
| Banken und Finanzen | 25 | 80.163 | 698 | 669.977 |
| Versicherungen | 25 | 17.069 | 233 | 333.920 |
| Hochschulen und Forschung | 25 | 43.877 | 2.096 | 939.422 |
| Industrie und Technologie | 24 | 90.446 | 4.854 | 3.281.078 |
| Energie und Infrastruktur | 25 | 10.580 | 266 | 158.849 |
| Verkehr und Logistik | 25 | 83.168 | 1.583 | 681.446 |
| Verbraucherdienste und Kommunikation | 25 | 238.181 | 23.575 | 118.214.739 |

| Branche | Beobachtete Domains | Gerätezuordnungen, mindestens | Mitarbeitergerätezuordnungen | Zugangsdatenzuordnungen |
|---|---|---|---|---|
| Gesundheit und Lebenswissenschaften | 25 | 23.473 | 151 | 219.813 |
| Gesamt | 249 | 636.397 | 33.915 | 125.422.358 |

Die Zugangsdaten umfassen 48.809.419 Zuordnungen aus Datenbanken früherer Datenlecks, 9.068.279 Stealer-Protokollzeilen und 67.544.660 Combolist-Einträge. Sie belegen weder eindeutige Personen noch gültige Passwörter oder aktuelle Zugriffe. [S87]

Die Gerätepopulation enthält 33.915 als Mitarbeiter klassifizierte und 602.482 andere Zuordnungen. Andere Zuordnungen sind keine bestätigten Kundengeräte. Gemeinsame Dienstdomains, historische Datensätze und wiederholte Zuordnungen können zu den Summen beitragen. Prüfen Sie die Domainzugehörigkeit vor der Kontaktaufnahme. [S87]

Verbraucherdienste und Kommunikation umfassen 118.214.739 Zugangsdatenzuordnungen. Öffentlich angebotene Dienste können Kundenidentitäten und Mitarbeiterkonten enthalten. Diese Konzentration belegt keine gleichwertige Einbruchsexposition sämtlicher vertretener Organisationen. [S87]

## 3.4 Kontoprüfung und Eindämmung

Bestätigen Sie, dass Konto und Dienst Ihrer Organisation gehören. Prüfen Sie Alter, Kontostatus und frühere Abhilfemaßnahmen. Untersuchen Sie bei aktiven privilegierten Konten Anmeldungen, Sitzungsfreigaben und administrative Änderungen. Widerrufen Sie Sitzungen und erneuern Sie betroffene Zugangsdaten bei entsprechendem Befund.

Ein Passwortwechsel ist nicht das einzige Abschlusskriterium. Sitzungen, zusätzliche Authentisierungsmethoden und verbundene Geräte können gesonderte Maßnahmen benötigen. Kunden- und Studierendenkonten brauchen eigene Verantwortliche. Dokumentieren Sie, ob der Beleg aktuell, historisch, sachfremd oder ungeklärt war.

## 3.5 Dokumente, Ähnlichkeitsdomains und passive Kontrollen

Die Momentaufnahme enthält 5.921 Dokumentbeobachtungen und 153.973 Beobachtungen ähnlich benannter Domains. Eine Dokumentzuordnung belegt weder vertraulichen Inhalt noch unbefugten Zugriff. Ähnliche Domainnamen belegen keine Identitätsnachahmung. Prüfen Sie vor einer Eskalation das konkrete Objekt, seine Zugehörigkeit und missbräuchliches Verhalten. [S87]

Ein abgeschlossener passiver Konfigurationsdatensatz fehlt. Der Bericht veröffentlicht keine Branchenindexwerte zur Konfigurationshygiene oder Häufigkeit von E-Mail-Kontrollen. Ein fehlendes Ergebnis belegt keine fehlende Kontrolle. Verantwortliche sollten legitime Absender, Authentisierungsabgleich, Zertifikate und Dienstabhängigkeiten vor Ort prüfen.

## 3.6 Zuständigkeit für die Reaktion

Führen Sie getrennte Vorgänge für aktuelle Kontoprüfung, Mitarbeiterendgeräte, Kundenschutz und Konfigurationsprüfung. Jeder Vorgang braucht Verantwortliche, Belege und ein Abschlusskriterium. Die Portfoliozahlen bestimmen nicht, welches konkrete System einschneidende Eindämmung benötigt.

KERNAUSSAGEN

**01**

Aktuelle Angebote sind Hinweise zur Kontoprüfung, keine bestätigten Einbrüche.

**02**

Geräte- und Zugangsdatenzuordnungen überschneiden sich und behalten ihren Domainnenner.

**03**

Weisen Sie Verantwortliche zu und erhalten Sie fehlende Datensätze sowie ungeprüfte Zugehörigkeiten sichtbar.

KAPITEL 04

# Untergrundaktivität und Einordnung von Behauptungen

04

DIESES KAPITEL BEANTWORTET

Was belegen die aufbewahrten Anzeigen über Zugänge, Dokumente und die Nachfrage nach Identitätsdaten?

**6**

erläuterte Behauptungen; keine Zahl bestätigter Einbrüche


4.1 Abgrenzung der betrachteten Daten 22

Monatliche beobachtete Beitragszahlen 23

4.2 Aktuelle Angebote: ein Mandantenkonto und Organisationsdateien 24

4.3 Dokumente als Grundlage für Betrug 26

4.4 Eine Schwachstellenbehauptung und ein Nachfragesignal 28

4.5 Weitere aufbewahrte Behauptungen und historische Anzeigen 30

4.6 Prüffragen zu häufigen Behauptungen 31

4.7 Veröffentlichungsplattformen und Sprachen 32

4.8 Handelsbehauptungen am Ende des Zeitraums 33

KAPITEL 04

# Untergrundaktivität und Einordnung von Behauptungen

KURZFASSUNG

Die aufbewahrten Beiträge enthalten Angebote für Administratorzugänge, Organisationsdokumente und Projektdaten sowie Nachfrage nach deutschen Identitätsdaten. Sechs Fallkarten zeigen diese Aussagen, ohne sie als Tatsachen zu übernehmen. Zwei Novemberangebote fallen in den aktuellen Beobachtungszeitraum. Die beobachtete Beitragsgesamtheit ist keine nationale Vorfallzählung. Abgeschlossene Verkäufe oder eine Rangfolge der Deliktsarten sind nicht belegt. Prüfen Sie relevante Hinweise anhand eigener Konten und Daten. Unterscheiden Sie Angebot und Besitz, Wiederholung und Bestätigung sowie Nachfrage und Diebstahl.

## 4.1 Abgrenzung der betrachteten Daten

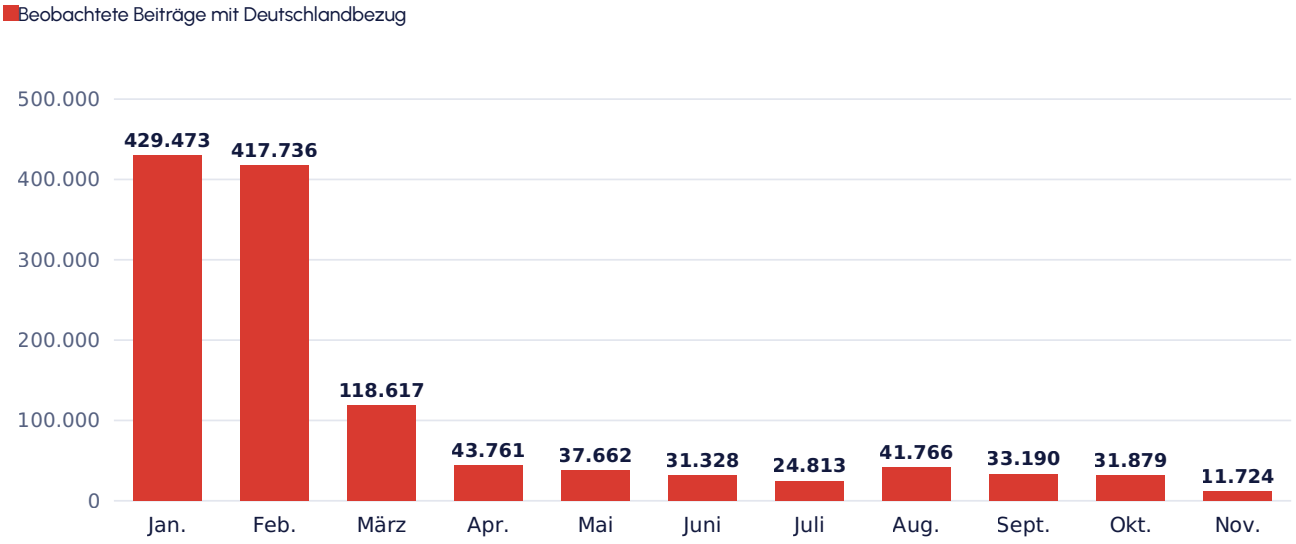
| Punkt | Stand |
|---|---|
| Angefragter Zeitraum | 1. Januar–22. November 2026, nach Beitragszeit |
| Beobachtete Beitragsgesamtheit mit Deutschlandbezug | 1.221.949 Beiträge [S1]; keine nationale Vorfallzahl |
| Aufbewahrte Belege | Forenbeiträge über Deutschland und Vermögenswerte mit Deutschlandbezug |
| Erläuterte Behauptungen | 6 Fallkarten mit jeweils einem gekürzten, anonymisierten Originalzitat |
| Zusammensetzung | Plattform- und Sprachbeobachtungen unten; keine nationale Deliktrangfolge belegt |
| Vollständiges Foren- und Marktinventar | Nicht verfügbar |
| Ransomwareeinträge | Eigene Gesamtheit: 457 deutsche Einträge [S2] |

Die folgenden Beobachtungen belegen Veröffentlichungen. Sie belegen weder eine vollständige Untergrundgesamtheit noch die angebotenen Vermögenswerte. Ein Deutschlandbezug kann ein behauptetes Ziel, eine Kundengruppe oder einen Absatzmarkt bezeichnen. Er belegt für sich weder den Standort einer Organisation noch die Herkunft jedes Datensatzes. [S1]

Beitragszahl und inhaltliches Quelleninventar beantworten unterschiedliche Fragen. Fehlende Inhalte belegen keine Abwesenheit von Aktivität. Öffentliche Mitteilungen und Ransomwareeinträge ersetzen den Beitragsbestand nicht. Die sechs Beispiele zeigen verschiedene Entscheidungen. Ihre Zahl ist keine Häufigkeitsschätzung. [S1]

# Monatliche beobachtete Beitragszahlen

## Die beobachtete Beitragszahl konzentriert sich auf den Jahresanfang




Quelle: beobachtete Beiträge mit Deutschlandbezug, 1. Januar–22. November 2026; Stichtag unvollständig. Beiträge, aufbewahrte Behauptungen und Vorfälle sind getrennte Populationen [S1].

| Monat | Beiträge | Monat | Beiträge |
|---|---|---|---|
| Januar | 429.473 | Juli | 24.813 |
| Februar | 417.736 | August | 41.766 |
| März | 118.617 | September | 33.190 |
| April | 43.761 | Oktober | 31.879 |
| Mai | 37.662 | November bis Stichtag | 11.724 |
| Juni | 31.328 | Gesamt | 1.221.949 |

Quelle: Odin by Brandefense [S1]. Januar und Februar umfassen 69,3 % der beobachteten Gesamtheit. Beiträge können Werbung, Diskussion, wiederholte Angebote oder internationales Material mit Deutschlandbezug enthalten. Geänderte Veröffentlichungszahlen belegen keine Veränderung erfolgreicher Angriffe oder nationaler Exposition. November ist unvollständig.

Die Beitragszahl liefert weder eine Zahl unterschiedlicher Personen noch eine Verkaufsschätzung oder einen bestätigten Standort jedes Vermögenswerts. Sie beschreibt Sichtbarkeit. Nutzen Sie die inhaltlich geprüften Fallkarten und öffentlichen Mitteilungen für die konkreten Reaktionsfragen.

Gesamtzahl und monatliche Beitragszahlen stimmen überein. In der Plattformaufschlüsselung fehlen weiterhin sieben Beiträge (§4.7). [S1]

## 4.2 Aktuelle Angebote: ein Mandantenkonto und Organisationsdateien

FALL S

S

### Angebotener Administratorzugang zu einem bankbezogenen CRM-Mandanten

Belegkarte B01 | 8 Nov. 2026 | Forum | Bankbezogene Dienste

Behauptung unbestätigt

| | |
|---|---|
| BEHAUPTUNG | Eine Forenanzeige vom 8. November bietet ein Konto mit vollen Administratorrechten für einen Cloud-CRM-Mandanten an. Der Text ordnet ihn einer Privatkundenbank zu und beschreibt Kundenkontaktdaten. [S1] |
| WAS SICH BELEGEN LÄSST | Angebot und behauptete Berechtigung standen im aufbewahrten Beitrag. Daraus folgt nicht, dass das Konto funktionierte, noch aktiv war oder zu einer deutschen juristischen Person gehörte. Eine Aussage über einen bankbezogenen Mandanten belegt keinen Zugriff auf die Infrastruktur des Cloudanbieters. |
| ALTERNATIVEN | Das Konto könnte veraltet, falsch beschrieben, auf einen Dienstleistermandanten beschränkt oder ohne tatsächlichen Besitz angeboten worden sein. Weder Verkauf noch Kundenumfang oder bankweiter Einbruch sind belegt. |
| REAKTION | Die Identitätsverantwortlichen sollten Mandantenzugehörigkeit, Administratorrechte, Anmeldungen und Sitzungsfreigaben anhand autorisierter Unterlagen prüfen. Eindämmung folgt dem bestätigten Kontobefund; die Prüfung von Kundendaten wird gesondert geführt. |

**Fazit**

Die Identitätsverantwortlichen sollten Mandantenzugehörigkeit, Administratorrechte, Anmeldungen und Sitzungsfreigaben anhand autorisierter Unterlagen prüfen. Eindämmung folgt dem bestätigten Kontobefund; die Prüfung von Kundendaten wird gesondert geführt.

FALL T

T

### Angebotenes Dateipaket deutscher Organisationen

Belegkarte B02 | 16 Nov. 2026 | Forum | Branchenübergreifende Dokumente

Behauptung unbestätigt

| | |
|---|---|
| BEHAUPTUNG | Ein Beitrag vom 16. November bietet Daten an, die laut Text von deutschen Organisationen stammen, und verweist auf verfügbare Belege. Weitere aufbewahrte Beiträge enthalten ähnliche Werbung im selben Zeitraum. [S1] |

| | |
|---|---|
| WAS SICH BELEGEN LÄSST | Die Quelle behauptet Besitz und Deutschlandbezug. Herkunft, Menge, Alter und Echtheit der Dateien werden hier nicht bestätigt. Ähnliche Listen in späteren Anzeigen belegen weder einen weiteren Diebstahl noch eine unabhängige Bestätigung. |
| ALTERNATIVEN | Werbung kann kopiert werden; verschiedene Pakete können überlappende oder ältere Unterlagen enthalten. Ein Dokument mit dem Namen einer Behörde, eines Dienstleisters oder einer Bank belegt keinen Zugriff auf deren Systeme. |
| REAKTION | Datenverantwortliche sollten einen autorisierten Hinweis mit dem eigenen Dokumentenbestand und früheren Meldungen vergleichen. Halten Sie konkrete Übereinstimmungen fest, bevor Vorfallsdatum, Betroffenenumfang oder Meldepflicht zugeordnet werden. |

**Fazit**

Datenverantwortliche sollten einen autorisierten Hinweis mit dem eigenen Dokumentenbestand und früheren Meldungen vergleichen. Halten Sie konkrete Übereinstimmungen fest, bevor Vorfallsdatum, Betroffenenumfang oder Meldepflicht zugeordnet werden.

**Belegkarte B01** — 8 Nov. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

Access full admin account in [victim withheld] [platform withheld]

ÜBERSETZUNG

Zugang zu einem vollständigen Administratorkonto in [Betroffener zurückgehalten] [Plattform zurückgehalten]

**Belegt**
Eine Anzeige behauptet Administratorzugriff auf einen bankbezogenen CRM-Mandanten und beschreibt Kundeninformationen.

**Nicht festgestellt**
Nutzbarer Zugriff, eine deutsche juristische Person als Ziel, Einbruch in die Plattform, Verkauf oder betroffene Kundenzahl.

**Belegkarte B02** — 16 Nov. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

SELLING Data from German [withheld] Proof available

ÜBERSETZUNG

VERKAUFE Daten von deutschen [zurückgehalten] Belege verfügbar

**Belegt**
Eine Anzeige bietet Dateien an, die laut Text von deutschen Organisationen stammen.

**Nicht festgestellt**
Echtheit, Herkunft, Aktualität, Verkauf oder ein neuer Einbruch bei jeder ähnlichen Anzeige.

Diese Novemberbeobachtungen sind Veröffentlichungen. Sie bestätigen keine zwei neuen Einbrüche zu diesen Zeitpunkten. Hier wird keine Verbindung zu den Hochschul-, Partei- oder Bankmitteilungen anderer Kapitel hergestellt. Für einen gemeinsamen Betreiber oder eine Transaktionskette liegen keine konkreten Belege vor. [S1]

## 4.3 Dokumente als Grundlage für Betrug

U

FALL U

### Angebotene Projektkontakte und Budgetdaten

Belegkarte B03 | 2 Feb. 2026 | Forum | Projektdienste

Behauptung unbestätigt

| | |
|---|---|
| BEHAUPTUNG | Am 2. Februar beschreibt ein Verkäufer eine Datenbank mit regionalen Projektkontakten und Budgetdaten aus einem deutschen Portal. [S1] |
| WAS SICH BELEGEN LÄSST | Die Anzeige verbindet Kontakt- und Projektfinanzdaten. Behauptete Datensatzzahl und inländische Herkunft sind nicht unabhängig bestätigt. Weder eine Übertragung aus dem Portal noch ein abgeschlossener Verkauf sind belegt. |
| ALTERNATIVEN | Kontaktdaten können älter, öffentlich, kopiert oder aus mehreren Quellen zusammengeführt sein. Eine plausible Feldliste belegt weder eine aktuelle Schwachstelle noch eine vollständige Kundendatenbank. |
| REAKTION | Einkauf und Betrugsabwehr sollten Änderungen an Projektzahlungen über einen bekannten Kanal bestätigen lassen. Ein relevanter Hinweis gehört zum Datenverantwortlichen, einschließlich der Frage, ob dieselben Daten schon früher offengelegt wurden. |

**Fazit**

Einkauf und Betrugsabwehr sollten Änderungen an Projektzahlungen über einen bekannten Kanal bestätigen lassen. Ein relevanter Hinweis gehört zum Datenverantwortlichen, einschließlich der Frage, ob dieselben Daten schon früher offengelegt wurden.

V

FALL V

### Behauptete Veröffentlichung von Verwaltungs- und Finanzdateien

Belegkarte B04 | 6 Okt. 2026 | Forum | Branchenübergreifende Dokumente

Behauptung unbestätigt

| | |
|---|---|
| BEHAUPTUNG | Ein Beitrag vom 6. Oktober kündigt eine Datenveröffentlichung einer laut Text in Deutschland ansässigen Organisation an. Genannt werden Verwaltungs- und Finanzdaten, geschäftliche E-Mail-Unterlagen und interne Dokumente. [S1] |
| WAS SICH BELEGEN LÄSST | Die Veröffentlichungsbehauptung und die Dokumentkategorien wurden publiziert. Dateien, behauptete Größe, Zugangsweg und Aktualität sind hier nicht bestätigt. |

| | |
|---|---|
| ALTERNATIVEN | Eine solche Ankündigung kann einen alten Export, eine Dienstleisterkopie oder neu gebündelte Daten betreffen. Sie belegt keinen fortbestehenden Zugriff auf aktuelle Systeme. |
| REAKTION | Die Vorfallsleitung sollte vor der Eindämmungsentscheidung Eigentum und Alter der Unterlagen feststellen. Die Betrugsabwehr sollte auf plausible Rechnungs-, Lieferanten- und Führungskräfte-Imitation anhand solcher Dokumentkategorien achten. |

**Fazit**

Die Vorfallsleitung sollte vor der Eindämmungsentscheidung Eigentum und Alter der Unterlagen feststellen. Die Betrugsabwehr sollte auf plausible Rechnungs-, Lieferanten- und Führungskräfte-Imitation anhand solcher Dokumentkategorien achten.

**Belegkarte B03** — 2 Feb. 2026

**[Alias zurückgehalten]** | Forum | Forum | Englisch

ORIGINAL

regional project contacts and budget records from the [victim withheld] Germany portal

ÜBERSETZUNG

regionale Projektkontakte und Budgetdaten aus dem Portal [Betroffener zurückgehalten] in Deutschland

**Belegt**

Ein Verkäufer beschreibt Projektkontakte und Budgetdaten eines als deutsch bezeichneten Portals.

**Nicht festgestellt**

Bestätigte Datensatzzahl, Portaleinbruch, aktuelle Schwachstelle, echte Dateien oder Verkauf.

**Belegkarte B04** — 6 Okt. 2026

**[Alias zurückgehalten]** | Forum | Forum | Englisch

ORIGINAL

administrative and financial data [withheld] Germany Including corporate emails internal [withheld] documents

ÜBERSETZUNG

Verwaltungs- und Finanzdaten [zurückgehalten] Deutschland einschließlich geschäftlicher E-Mails und interner [zurückgehalten] Dokumente

**Belegt**

Ein Beitrag behauptet die Veröffentlichung von Verwaltungs-, Finanz- und geschäftlichen E-Mail-Unterlagen einer als deutsch beschriebenen Organisation.

**Nicht festgestellt**

Echte Dateien, neuer Einbruch, fortbestehender Zugriff, bestätigte Datenmenge oder abgeschlossene Transaktion.

Der analytische Zusammenhang besteht zwischen brauchbaren Hintergrundinformationen und einer späteren Täuschung. Projektbudgets oder interne Korrespondenz können betrügerische Nachrichten glaubwürdiger machen. Die Beiträge belegen nicht, dass solche Nachrichten versandt wurden. Die bestätigten Folgewarnungen in Kapitel 5 sind eigenständige Belege für dieses Verhalten. Sie werden diesen Anzeigen nicht zugeordnet.

## 4.4 Eine Schwachstellenbehauptung und ein Nachfragesignal

FALL W

W

### Angebotene Automobildokumente mit behauptetem Berechtigungsfehler

Behauptung unbestätigt

Belegkarte B05 | 17 Feb. 2026 | Forum | Automobil

| | |
|---|---|
| BEHAUPTUNG | Eine Anzeige vom 17. Februar bietet Dokumente einschließlich personenbezogener Informationen eines als deutsch bezeichneten großen Automobilkonzerns an. Sie führt die Beschaffung auf eine unsichere direkte Objektreferenz, kurz IDOR, zurück und bietet den behaupteten Exploit gesondert zum Verkauf an. Eine zweite Anzeige wiederholt die Behauptung später am selben Tag. [S1] |
| WAS SICH BELEGEN LÄSST | Der Verkäufer behauptet Dokumentbesitz und eine Schwachstelle. Der Beitrag bestätigt weder einen bestehenden Fehler noch Ausnutzung, Dateibesitz oder einen neuen Einbruch beim Konzern. Die Wiederholung ist kein weiterer Vorfall. |
| ALTERNATIVEN | Der Zugangsweg kann vermutet, kopiert oder falsch beschrieben sein. Dokumente können von einem Auftragnehmer oder aus einem früheren Export stammen. Die Wortwahl des Verkäufers ist keine unabhängige technische Bewertung. |
| REAKTION | Bei einem relevanten Hinweis sollte der Anwendungsverantwortliche objektbezogene Berechtigungen und Zugriffsprotokolle im eigenen betroffenen Dienst prüfen. Ein autorisierter Test und sein tatsächliches Ergebnis sind maßgeblich; die Anzeige allein ist kein Schwachstellenbefund. |

**Fazit**

Bei einem relevanten Hinweis sollte der Anwendungsverantwortliche objektbezogene Berechtigungen und Zugriffsprotokolle im eigenen betroffenen Dienst prüfen. Ein autorisierter Test und sein tatsächliches Ergebnis sind maßgeblich; die Anzeige allein ist kein Schwachstellenbefund.

FALL X

X

### Nachfrage nach deutschen Identitätsdaten und Wohnanschriften

Behauptung unbestätigt

Belegkarte B06 | 5 Jan. 2026 | Forum | Identitätsdaten

| | |
|---|---|
| BEHAUPTUNG | Ein Beitrag vom 5. Januar fragt nach Informationen über deutsche Personen. Er betont physische Wohnanschriften und bittet um weitere Identitätsangaben, soweit verfügbar. [S1] |

| | |
|---|---|
| WAS SICH BELEGEN LÄSST | Dies ist eine Beschaffungsanfrage. Sie belegt nicht, dass der Verfasser eine Datenbank besaß, Datensätze erhielt, einen Kauf abschloss oder eine bestimmte Person auswählte. |
| ALTERNATIVEN | Die Anfrage könnte unerfüllt geblieben sein. Sie enthält keine belastbare Personenzahl, Herkunftsorganisation oder Erhebungszeit. |
| REAKTION | Ein relevanter Identitätshinweis gehört in Datenschutz und Kundenschutz. Prüfen Sie tatsächlich offengelegte Informationen und glaubhaften Missbrauch. Aus einer Käuferanfrage lässt sich keine nationale Betroffenenzahl ableiten. |

**Fazit**

Ein relevanter Identitätshinweis gehört in Datenschutz und Kundenschutz. Prüfen Sie tatsächlich offengelegte Informationen und glaubhaften Missbrauch. Aus einer Käuferanfrage lässt sich keine nationale Betroffenenzahl ableiten.

Belegkarte B05 — 17 Feb. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

[victim withheld] Documents including [withheld] IDOR

ÜBERSETZUNG

[Betroffener zurückgehalten] Dokumente einschließlich [zurückgehalten] IDOR

**Belegt**

Ein Verkäufer bietet Automobildokumente und gesondert einen IDOR-Exploit an.

**Nicht festgestellt**

Tatsächliche Schwachstelle, Ausnutzung, Dokumentbesitz, Verkauf oder ein zweiter Vorfall durch die Wiederholungsanzeige.

Belegkarte B06 — 5 Jan. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

LOOKING FOR GERMAN [withheld] FULLZ [withheld] REAL [withheld] ADDRESS AND OTHER DETAILS

ÜBERSETZUNG

SUCHE DEUTSCHE [zurückgehalten] IDENTITÄTSDATEN [zurückgehalten] ECHTE [zurückgehalten] ADRESSE UND WEITERE ANGABEN

**Belegt**

Ein Käufer fragt nach deutschen Identitätsangaben und betont echte Wohnanschriften.

**Nicht festgestellt**

Besitz, Beschaffung, abgeschlossener Kauf, eine bestimmte betroffene Person oder ein zugrunde liegender Einbruch.

Die sechs Beispiele unterscheiden angebotenen Zugang, angebotene Datensätze, behauptete Veröffentlichung, behaupteten technischen Zugangsweg und Nachfrage. Diese Kategorien verlangen unterschiedliche Belege. Sie ergeben keine sechs bestätigten Einbrüche. [S1]

## 4.5 Weitere aufbewahrte Behauptungen und historische Anzeigen

Die folgenden Beobachtungen erweitern das Behauptungsregister, ohne die Zahl bestätigter Vorfälle zu erhöhen. Genannt sind Veröffentlichungsdaten. Keine Zeile bestätigt Besitz, abgeschlossene Transaktion oder den behaupteten technischen Zugangsweg. [S1]

| Beitragsdatum | Rolle und Behauptung | Grenze und Reaktion |
|---|---|---|
| 1. Februar | Angebot einer als deutsch bezeichneten Website-Datenbank [S1] | Die Länderangabe bestätigt weder Herkunft noch Alter oder Einbruch; relevante Hinweise gehören zum Datenverantwortlichen. |
| 31. März | Behauptete Weitergabe von Kontodaten eines deutschsprachigen Forums [S1] | Sprache belegt keinen Wohnsitz; widersprüchliche Mengenangaben bleiben weg. Kontozugehörigkeit und frühere Maßnahmen prüfen. |
| 6. Juni | Als Material aus 2025 beworbene deutsche Geschäfts-/Kontaktdaten [S1] | Ältere Verzeichnisse oder öffentliche Quellen sind möglich; die Veröffentlichung 2026 belegt keinen neuen Einbruch. |
| 17. Juni | Als Material aus 2025 beworbene deutsche Verbraucherkontakte [S1] | Historische Handelsbehauptung ohne bestätigte Herkunftsorganisation oder Einbruchsdatum; tatsächliche Datenkategorien prüfen. |
| 12. August | Telefoniedienst bewirbt eine Einschränkung bei deutschen Rufnummern [S1] | Nur eine Funktionsbehauptung, ohne beobachtetes Opfer oder erfolgreiche Imitation; Anrufe unabhängig prüfen. |
| 22. August | Behauptetes deutsches Mobilnummern-/Geburtsdatum-Paket [S1] | Herkunft, Alter und Besitz sind unbestätigt; daraus keinen Einbruch bei einem Telekommunikationsanbieter ableiten. |
| 7. September | Behaupteter Kundendatenvorfall einer deutschen Handels-/Dienstleistungsgruppe [S1] | Der Beitrag nennt 2026; offizielle Bestätigung und Dateiechtheit sind nicht belegt. |
| 3. Oktober | Als deutsch beschriebene Finanznutzer-Datensätze angeboten [S1] | Kundenfelder belegen keinen Zugriff auf Banksysteme; Herkunft und behaupteter Umfang bleiben unbestätigt. |
| 7. Oktober | Veröffentlichung deutscher Automobil-Kunden-, Dokument- und Finanzdaten behauptet [S1] | Dateien und aktueller Zugriff sind nicht bestätigt; relevante Hinweise vor Eindämmung mit eigenen Unterlagen abgleichen. |
| 1. November | Deutscher Hersteller in einem Foren-Datenleckeintrag genannt [S1] | Knappe Behauptung ohne bestätigtes Diebstahldatum oder Verfahren; ein Forenrepost ist kein weiterer Einbruch. |

| Beitragsdatum | Rolle und Behauptung | Grenze und Reaktion |
|---|---|---|
| 5. November | Internationales Reise-/Reservierungsdatenpaket mit Deutschland unter den Kundenländern angeboten [S1] | Herkunftsorganisation und deutsches Organisationssegment sind unbestätigt; kein deutscher Anbietereinbruch abgeleitet. |
| 8. November | Administratorzugriff auf einen Forschungs-/Rekrutierungs-Cloudmandanten angeboten [S1] | Inländische Zugehörigkeit, Kundenstandort und nutzbarer Zugriff unbestätigt; nur einen bestätigten eigenen Mandanten prüfen. |
| 10. November | Administratorzugriff auf eine deutsche Foren-/Hostingplattform behauptet [S1] | Kunden- und Bestellkategorien werden behauptet; aktiver Zugriff und Plattformeinbruch sind nicht bestätigt. |
| 17. November | Mehrländer-Bankkontakte mit deutschem Segment angeboten [S1] | Eine Kontaktliste belegt keinen Bankeinbruch; Aktualität und Verkaufsbehauptungen bleiben unbestätigt. |

Die Anzeigen können unterschiedliche Angebote oder überlappendes älteres Material betreffen. Weder gemeinsamer Betreiber noch ein eigener Einbruch je Zeile oder eine Verbindung zu öffentlichen Mitteilungen ist belegt. Rufnummern- und Finanzkontaktzeilen begründen vertrauenswürdige Prüfwege, keine Aussagen über abgeschlossenen Betrug in Deutschland.

## 4.6 Prüffragen zu häufigen Behauptungen

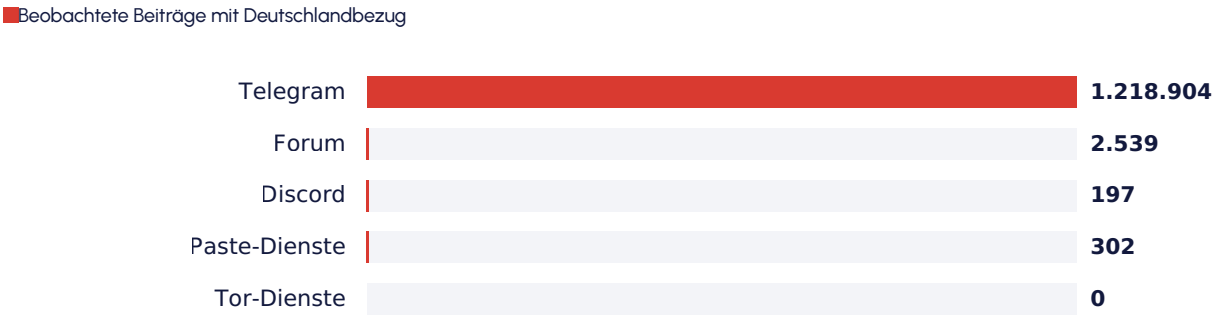
| Behauptungstyp | Was zu prüfen ist | Was daraus nicht folgt |
|---|---|---|
| Kundendatenbank | Herkunft, Kategorien, Alter und Eigentum | Jede behauptete Zeile steht für eine andere Person |
| Beschäftigtenzugang | Kontozugehörigkeit, Status und Berechtigungen | Ein Domainbezug belegt ein Arbeitsverhältnis |
| Fernzugriff | Ein aktuell nutzbarer Zugangsweg | Ein altes Bildschirmfoto belegt fortbestehenden Zugriff |
| Zugangsdaten-Datei | Aktualität und frühere Bereinigung | Jede Zeile ist gültig oder eindeutig |
| Infrastrukturverzeichnis | Echtheit und aktuelle betriebliche Bedeutung | Ein Dokument belegt die Kontrolle über die Infrastruktur |
| DDoS-Behauptung | Dienstzustand, Dauer und betroffene Funktion | Ein kurzzeitig fehlgeschlagener Test belegt eine landesweite Störung |

Die Vorfallsakte sollte die geprüfte Aussage, das Quelldatum, den eigenen Vermögenswert oder die Datenkategorie sowie das Ergebnis enthalten. Halten Sie Alternativen sichtbar. Benennen Sie Verantwortliche: Identitätsmanagement für aktive Konten, Datenschutz für Personendaten und Dienstbetreiber für Störungen.

Diese Ausgabe nennt keinen nationalen Median der Angebotspreise und schätzt keine abgeschlossenen Verkäufe. Die Zitate behalten die Originalsprache bei; identifizierende Angaben wurden entfernt. Die Übersetzungen geben die Behauptung wieder, ohne technische oder zuordnungsbezogene Gewissheit hinzuzufügen. [S1]

## 4.7 Veröffentlichungsplattformen und Sprachen

### Telegram hat die größte beobachtete Plattformzahl



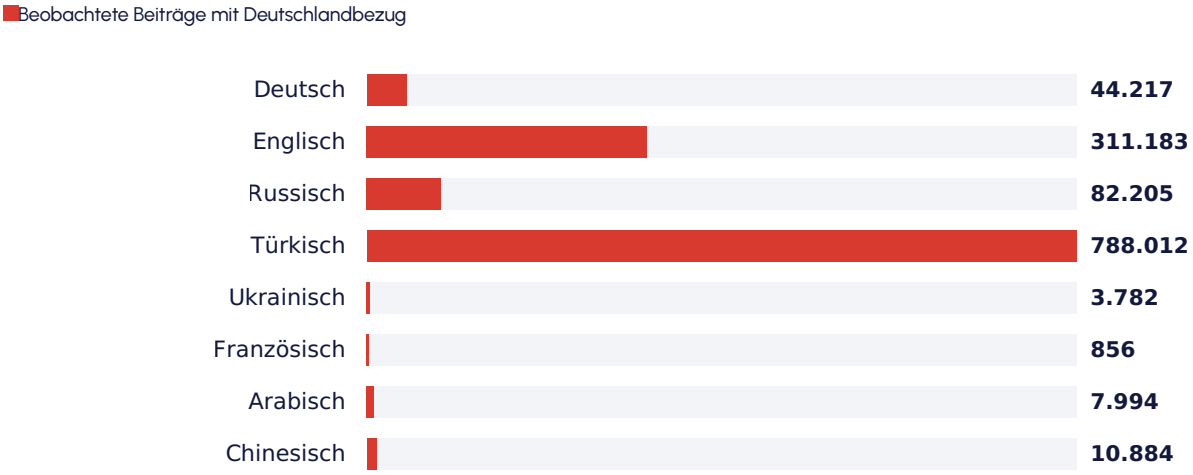

Die Plattformzahlen ergeben 1.221.942; sieben der 1.221.949 beobachteten Beiträge bleiben in dieser Aufschlüsselung ohne Zuordnung. Quelle: beobachtete Beiträge mit Deutschlandbezug, 1. Januar–22. November 2026; Stichtag unvollständig. Beiträge, aufbewahrte Behauptungen und Vorfälle sind getrennte Populationen [S1].

| Plattformbezeichnung | Beobachtete Beiträge |
|---|---|
| Telegram | 1.218.904 |
| Foren | 2.539 |
| Discord | 197 |
| Paste-Dienste | 302 |
| Tor-Dienste | 0 |

Die Plattformzeilen ergeben 1.221.942 Beiträge, sieben weniger als die Gesamtzahl. Die verfügbaren Aggregate belegen keine Plattformzuordnung dieser Differenz. Die Zeilen sind keine vollständig abgestimmte Aufschlüsselung. [S1]

Dies sind beobachtete Beiträge mit Deutschlandbezug im angefragten Zeitraum. Die Plattformbezeichnungen beschreiben Veröffentlichungsorte, keine bestätigten Angriffe, erfolgreichen Transaktionen oder inländischen Opferpopulationen. Sie bilden keinen vollständigen Katalog sämtlicher Untergrundorte. [S1]

### Sprachzuordnungen belegen keine Staatsangehörigkeit




Sprachzuordnungen können sich überschneiden und belegen keine Staatsangehörigkeit. Quelle: beobachtete Beiträge mit Deutschlandbezug, 1. Januar–22. November 2026; Stichtag unvollständig. Beiträge, aufbewahrte Behauptungen und Vorfälle sind getrennte Populationen [S1].

| Sprachzuordnung | Beobachtete Beiträge |
|---|---|
| Deutsch | 44.217 |
| Englisch | 311.183 |
| Russisch | 82.205 |
| Türkisch | 788.012 |
| Ukrainisch | 3.782 |
| Französisch | 856 |
| Arabisch | 7.994 |
| Chinesisch | 10.884 |

Sprachzuordnungen können sich überschneiden. Sie belegen weder Staatsangehörigkeit noch Wohnsitz von Verfassern, Kunden oder Betroffenen. Veröffentlichungszahlen belegen keine nationale Deliktrangfolge oder Häufigkeit erfolgreicher Einbrüche. [S1]

## 4.8 Handelsbehauptungen am Ende des Zeitraums

**Das Hostingangebot schließt aktiven Zugriff aus.** Ein Angebot vom 22. November bewirbt Material zu 16 Websites und 10 kleinen Geschäftskunden eines deutschen Hostingdienstes. Der Verkäufer schließt aktiven SSH- oder Root-Zugriff ausdrücklich aus. Besitz, Herkunft, Beschaffungsdatum und ein abgeschlossener Verkauf bleiben unbestätigt. Prüfen Sie relevante eigene Dateien und Konten, bevor Sie das Angebot als Beleg aktuellen Zugriffs behandeln. [S1]

**Die Beiträge wiederholen dieselbe Angebotsbehauptung.** Zwei Beiträge vom 22. November bewerben dieselbe behauptete deutsche Zugangsdatenliste mit 23.000 Einträgen und übereinstimmender Cloudzugangswerbung. Die Formulierungen belegen weder identische, gültige oder aktuelle Datensätze noch unabhängige Diebstähle. Addieren Sie die beworbenen Zahlen nicht und zählen Sie die Beiträge nicht als getrennte Einbrüche. [S1]

Ein Angebot vom 12. November bewirbt deutsche Anlage- und Rückgewinnungskontakte. Ein Angebot vom 18. November bezeichnet deutsches Telefonkontaktmaterial als Daten von 2023. Beides belegt weder Ursprungseinbruch noch heutige Richtigkeit oder einen neuen Einbruch 2026. Kundenschutzteams sollten Rückgewinnungskontakte und Zahlungsaufforderungen über unabhängige Wege authentisieren. [S1]

KERNAUSSAGEN

**01**

Sechs erläuterte Behauptungen zeigen unterschiedliche Prüfaufgaben, keine sechs bestätigten Einbrüche.

**02**

Wiederholte Werbung ist keine unabhängige Bestätigung.

**03**

Zugang, Dokumente und Identitätsdaten gehören zu den jeweils zuständigen Prüfern.

KAPITEL 05

# Bestätigte Vorfälle und Aktivitäten nach Branchen

DIESES KAPITEL BEANTWORTET

Welche Mitteilungen tragen konkrete Schutzmaßnahmen, und welche Folgen bleiben ungeklärt?

**2**

getrennte Novembermitteilungen einer Hochschule


5.1 Wie die Fälle zu lesen sind 36
5.2 Öffentliche Verwaltung: Datenprüfung nach der Eindämmung 37
5.3 Hochschulen: Identitätsgefährdung und Datenzugriff sind unterschiedliche Ereignisse 39
5.4 Gesundheitswesen: Patienten auch in der Folgephase schützen 42
5.5 Dienstleisterdaten und Kundendienste 44
5.6 Verkehr und Kommunikation 46
5.7 Aktuelle Aktivitäten: 8.–22. November 46
5.8 Weitere bestätigte Fälle am Ende des Zeitraums 48
5.9 Frühere Vorfälle und wichtige Ausschlüsse 52
5.10 Weitere Befunde zu priorisierten Organisationen 54
5.11 Welche Schlüsse die Fälle tragen 55

KAPITEL 05

# Bestätigte Vorfälle und Aktivitäten nach Branchen

KURZFASSUNG

Öffentliche Mitteilungen beschreiben unterschiedliche Probleme: gestohlene Zugangsdaten, kopierte Verwaltungsdaten, Kundendaten bei Dienstleistern und unterbrochene Dienste. Die folgenden Fälle bewahren die Grenzen jeder Quelle. Gleiche Branche oder nahe Daten belegen keine gemeinsame Kampagne. Beginnen Sie bei betroffener Funktion und bestätigtem Zugriff. Wählen Sie darauf abgestimmte Eindämmungs-, Unterstützungs- und Kontinuitätsmaßnahmen.

## 5.1 Wie die Fälle zu lesen sind

Ein bestätigter Sicherheitsvorfall bestätigt nicht jede spätere Leak-Behauptung. Wir erfassen die Aussage der Organisation oder Behörde, nennen offene Punkte und leiten eine angemessene Reaktion ab. Ein Fall kann mehrere Phasen umfassen, etwa Einbruch und spätere Patientenerpressung.

Benannte Fälle benötigen offizielle Bestätigung und breitere Berichterstattung. Andere Fälle verwenden allgemeine Rollen. Quellentitel und Artikeladressen, die einen zurückgehaltenen Namen offenlegen würden, werden entsprechend der Veröffentlichungsregeln gekürzt. Das private Register enthält die genaue Belegstelle.

Dieses Kapitel ist eine Sammlung dokumentierter Fälle, keine vollständige nationale Zählung. Entdeckung, Mitteilung, Veröffentlichung und Wiederherstellung bleiben getrennte Daten. Folgebetrug und ein neuer Einbruch werden nicht automatisch als zwei Einbrüche gezählt.

## 5.2 Öffentliche Verwaltung: Datenprüfung nach der Eindämmung

A

FALL A

### Datenverlust in der Berliner Verwaltung

Öffentliche Verwaltung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die Berliner Datenschutzaufsicht nennt Kopiervorgänge aus Verwaltungsnetzen zwischen 7. und 12. August. Sie beschreibt veröffentlichte Beschäftigtendaten und möglicherweise Bürgerdaten. Die Informationsseite des Senats erläutert gesondert die fortlaufende Prüfung. [S9][S10] |
| GRENZE | Ein öffentliches Archiv belegt weder die Echtheit jeder Datei noch die Veröffentlichung jeder Person oder einen fortdauernden Zugriff. Der gemeldete Vorfall bleibt von Mengen- und Zuordnungsangaben der Täter getrennt. |
| EINORDNUNG | Unstrukturierte gemeinsame Ablagen machen die Umfangsbestimmung zu einer eigenen Aufgabe. Ein wiederhergestelltes System zeigt nicht, wessen Korrespondenz möglicherweise kopiert wurde. |
| REAKTION | Erfassen Sie betroffene Dokumentenspeicher und bestätigbare Kategorien. Halten Sie einen Kontaktweg für Menschen bereit, deren individuelle Betroffenheit noch geprüft wird. |

**Fazit**

Erfassen Sie betroffene Dokumentenspeicher und bestätigbare Kategorien. Halten Sie einen Kontaktweg für Menschen bereit, deren individuelle Betroffenheit noch geprüft wird.

Der Fall begründet eine Entscheidung zur Dokumentenverwaltung über die Netzwerkwiederherstellung hinaus. Eine Organisation sollte wissen, welche gemeinsamen Ablagen Ausweisdokumente, Vertragsdaten oder sensible Betriebspläne enthalten. Datenverantwortliche sollten Aufbewahrungsregeln und Zugriffsfreigaben benennen können.

Nutzen Sie stufenweise Mitteilungen. Trennen Sie das bekannte Ereignis von der noch laufenden Prüfung individueller Folgen. Nennen Sie nächste Aktualisierung, Kontaktweg und Hinweise zu bestätigten Datenkategorien. Veröffentlichung bedeutet nicht automatisch Missbrauch; Wiederherstellung beseitigt dessen Risiko nicht zwangsläufig.

FALL B

B

## Ungeklärter Novembervorfall einer staatlichen Liegenschaftsstelle

Öffentliche Verwaltung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Landesministerium meldete am 19. November einen IT-Sicherheitsvorfall. Telefonische Erreichbarkeit war eingeschränkt, E-Mail nicht verfügbar. Ursache, Umfang und möglicher Datenabfluss wurden noch untersucht. [S22] |
| GRENZE | Die Mitteilung belegt weder Ransomware noch kopierte Daten oder einen Akteur. Bestätigte betriebliche Folge ist die eingeschränkte Kommunikation. |
| REAKTION | Bereiten Sie Ersatzkontakte vor und sichern Sie den zeitlichen Verlauf der Untersuchung. Präzisieren Sie die öffentliche Beschreibung, sobald belastbarere Erkenntnisse vorliegen. |

**Fazit**

Bereiten Sie Ersatzkontakte vor und sichern Sie den zeitlichen Verlauf der Untersuchung. Präzisieren Sie die öffentliche Beschreibung, sobald belastbarere Erkenntnisse vorliegen.

Der Fall zeigt eine wichtige Grenze. Eine Mitteilung kann einen Vorfall bestätigen, bevor dessen Ablauf geklärt ist. Ersatzkanäle sollten nicht auf einen Gruppennamen warten. Analysten sollten keine Zuordnung ergänzen, die eine Behörde nicht festgestellt hat.

## 5.3 Hochschulen: Identitätsgefährdung und Datenzugriff sind unterschiedliche Ereignisse

C

FALL C

### Zentrale TUM-Zugangsdaten

Bildung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die TUM meldete gestohlene zentrale Passwörter einschließlich eines Administratorkontos und Zugriffe gegen TUMonline. Ihre Aktualisierung vom 9. November meldete die Wiederinbetriebnahme mit verpflichtendem Passwortwechsel und Zwei-Faktor-Authentifizierung. [S11] |
| GRENZE | Die Mitteilung belegt keine gesicherte Diebstahlszahl für die gesamte Hochschulpopulation. Breitere Berichterstattung trägt die Namensnennung, nicht die Erweiterung der offiziellen Folgenbeschreibung. [S12] |
| EINORDNUNG | Ein Administratorkonto kann aus einem Portalvorfall eine weitergehende Identitätsreaktion machen. Neben dem ursprünglichen Portal sind Berechtigungen und Sitzungen zu prüfen. |
| REAKTION | Validieren Sie betroffene Konten, widerrufen Sie relevante Sitzungen und prüfen Sie administrative Änderungen vor der normalen Freigabe. |

**Fazit**

Validieren Sie betroffene Konten, widerrufen Sie relevante Sitzungen und prüfen Sie administrative Änderungen vor der normalen Freigabe.

Identitäts-, Anwendungs- und Dienstteams sollten die Wiederherstellung gemeinsam verantworten. Verfügbarkeit ist nur ein Meilenstein. Sicheres Öffnen verlangt auch die Prüfung privilegierter Freigaben, Wiederherstellungsmethoden und ausreichender Protokolle für spätere Untersuchungen.

Testen Sie den Ablauf mit einer synthetischen Wiederherstellungsübung. Ein gesperrtes Konto muss über einen vertrauenswürdigen Weg zurückkehren. Unberechtigte Sitzungen müssen Zugriff verlieren, berechtigte Nutzer kritische Funktionen erreichen. Dokumentieren Sie Ausnahmen statt alle Konten gleichzusetzen.

D

FALL D

## Beschäftigtendaten der Universität Tübingen

Bildung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Am 10. November meldete die Universität etwa 3.900 Beschäftigtendatensätze mit Identitäts-, Kontakt- und Dienststellenangaben. Studierende und Passwörter seien nicht betroffen. Eine Kombination empfohlener Einstellungen habe interne Funktionen zugänglich gemacht. [S13][S15] |
| GRENZE | Die Mitteilung belegt keinen gemeinsamen Betreiber mit anderen Hochschulfällen. Ein bekannter Benutzername war Teil der beschriebenen Zugangsbedingung. Er wird dadurch nicht selbst zum Geheimnis. |
| EINORDNUNG | Zusammenspielende Einstellungen können Gefährdungen schaffen, obwohl jede einzelne gewöhnlich erscheint. Prüfen Sie die tatsächlichen Berechtigungen des gesamten Dienstes. |
| REAKTION | Testen Sie interne Funktionen mit einem autorisierten Konto. Prüfen Sie Dienstleistervorgaben und warnen Sie Beschäftigte vor gezieltem Phishing mit echten Kontextangaben. |

**Fazit**

Testen Sie interne Funktionen mit einem autorisierten Konto. Prüfen Sie Dienstleistervorgaben und warnen Sie Beschäftigte vor gezieltem Phishing mit echten Kontextangaben.

E

FALL E

## Webmail-Mitteilung der Universität Tübingen

Bildung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Eine gesonderte Mitteilung vom 11. November beschrieb einen nächtlichen Webmail-Angriff und vorsorgliche Kontobeschränkungen. In dem genannten Zeitraum eingegebene Passwörter könnten erfasst worden sein; die Universität leitete Zurücksetzungen ein. [S14][S48] |
| GRENZE | Der Bericht verbindet diese Meldung nicht mit dem Beschäftigtendatenfall. Gleiche Hochschule und nahe Daten belegen weder denselben Zugang noch denselben Datenbestand oder Täter. |
| REAKTION | Richten Sie Zurücksetzungen nach Dienst und genanntem Zeitfenster aus. Prüfen Sie verknüpfte Dienste und Sitzungen betroffener Konten, ohne die Einsicht in jedes Postfach zu behaupten. |

**Fazit**

Richten Sie Zurücksetzungen nach Dienst und genanntem Zeitfenster aus. Prüfen Sie verknüpfte Dienste und Sitzungen betroffener Konten, ohne die Einsicht in jedes Postfach zu behaupten.

Die beiden Fälle zeigen die Bedeutung einer klaren Vorfalleinheit. Eine Mitteilung betrifft Beschäftigtendaten und schließt Passwörter ausdrücklich aus. Die andere betrifft mögliche Passworterfassung in einem Maildienst-Zeitfenster. Eine gemeinsame Schlagzeile würde entscheidungsrelevante Unterschiede verdecken.

F

FALL F

## LMU-Immatrikulationsdaten

Bildung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die LMU-Mitteilung vom 19. September beschreibt unberechtigten Zugriff auf Immatrikulationsdaten und geht von einem Abruf aus. Sie nennt je nach Datensatz Identitäts-, Kontakt-, Finanz- oder Verwaltungsangaben. [S49] |
| GRENZE | Die Mitteilung belegt weder einen öffentlichen Leak noch eine nationale Studierendenzahl. Sie trennt Immatrikulationsangaben von Prüfungs- und Leistungsinformationen. |
| REAKTION | Bestimmen Sie betroffene Kategorien, unterstützen Sie Betroffene und testen Sie die Berechtigungen der Immatrikulationsabläufe vor der Wiederöffnung. |

**Fazit**

Bestimmen Sie betroffene Kategorien, unterstützen Sie Betroffene und testen Sie die Berechtigungen der Immatrikulationsabläufe vor der Wiederöffnung.

Die Hochschulfälle tragen mehrere Kontrollen, nicht einen unterstellten gemeinsamen Erstzugang. Identitätswiederherstellung, Administrationsrechte, Anwendungsberechtigungen und Datenschutzumfang benötigen jeweils Verantwortliche. Der Bericht leitet keinen gemeinsamen Phishing-Beginn oder dieselbe Softwarelücke ab.

## 5.4 Gesundheitswesen: Patienten auch in der Folgephase schützen

FALL G

### IT-Vorfall im Krankenhaus und anschließende Patientenerpressung

Gesundheit

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Krankenhaus meldete im Februar Kommunikationsausfälle und manuelle Stationsabläufe. Im März warnten Landesdatenschutzaufsicht und Polizei vor direkten Erpressungsnachrichten mit gestohlenen Patienteninformationen. [S16] |
| GRENZE | Die späteren Nachrichten sind eine Folgephase, kein Beleg eines zweiten Krankenhauseinbruchs. Weder eine Patientenzahl noch ein benannter Betreiber sind hier festgestellt. |
| EINORDNUNG | Sensible Informationen können Einzelne als Erpressungsforderung erreichen, nachdem die Einrichtung die Wiederherstellung begonnen hat. Patientenbezogene Unterstützung gehört deshalb zur Reaktion. |
| REAKTION | Bereiten Sie Gesprächshilfen für Empfänger vor und sichern Sie Meldungen über einen geeigneten Weg. Erklären Sie, dass Zahlung keine Löschung belegt. |

**Fazit**

Bereiten Sie Gesprächshilfen für Empfänger vor und sichern Sie Meldungen über einen geeigneten Weg. Erklären Sie, dass Zahlung keine Löschung belegt.

Die Lehre betrifft die Organisation. Ein Servicedesk sollte Patienten nicht bitten, sensible Unterlagen an eine ungeprüfte Adresse zu senden. Er benötigt einen freigegebenen Weg, klare Erstfragen und eine Verbindung zum Vorfallteam für dringende Anliegen.

Üben Sie klinischen Ersatzbetrieb und Datenschutzreaktion gemeinsam. Manuelle Verfahren brauchen Personal, verlässliche Kontakte und eine sichere spätere Zusammenführung von Aufzeichnungen. Legen Sie fest, wer den Normalbetrieb freigibt und welche Belege dafür nötig sind.

FALL H

H

## Begrenzte Systembetroffenheit bei Fresenius Medical Care

Medizintechnik

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Das Unternehmen meldete am 22. September unbefugten Zugriff auf eine begrenzte Zahl interner Systeme. Medizinprodukte, Patientenversorgung, Produktion und laufender Betrieb seien nicht betroffen. [S19][S20] |
| GRENZE | Dies beschreibt den vom Unternehmen genannten Umfang. Es bestätigt weder beworbene Daten einer Erpressungsgruppe noch eine deutsche Patientenzahl oder ausgefallene klinische Geräte. |
| REAKTION | Trennen Sie interne Systemuntersuchung und klinische Absicherung. Prüfen Sie Auswirkungen mit den betrieblichen Verantwortlichen statt anhand eines kriminellen Eintrags allein. |

**Fazit**

Trennen Sie interne Systemuntersuchung und klinische Absicherung. Prüfen Sie Auswirkungen mit den betrieblichen Verantwortlichen statt anhand eines kriminellen Eintrags allein.

Die Krankenhaus- und Medizintechnikmeldungen erlauben keine pauschale Aussage über ausgefallene Gesundheitssysteme. Eine beschreibt manuelle Abläufe und spätere Patientenerpressung. Die andere schließt Folgen für Versorgung und Produktion ausdrücklich aus.

FALL I

I

### Kühlanlagen im Pharmabereich

Industriekühlung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die LKA-NRW-Warnung vom 18. November verweist auf BSI-Angaben zu angegriffenen Kühlsystemen eines deutschen Pharmahändlers. Sie behandelt einen französischen Fall gesondert. Unmittelbare Folgen für deutsche Blutbanken seien nicht festgestellt. [S21] |
| GRENZE | Zwischen den Fällen sind weder ein gemeinsamer Akteur noch dieselbe technische Ursache belegt. Die Warnung trägt keine Behauptung verlorener deutscher Blutprodukte. |
| REAKTION | Prüfen Sie Fernwartung, unabhängige Temperaturalarme und Ersatzlagerung. Eine IT-Datensicherung erhält keine physische Temperaturbedingung. |

**Fazit**

Prüfen Sie Fernwartung, unabhängige Temperaturalarme und Ersatzlagerung. Eine IT-Datensicherung erhält keine physische Temperaturbedingung.

Kapitel 6 entwickelt die betriebliche Reaktion. Zuerst ist zu klären, wer Alarme erhält, Fernzugänge sperren darf und Bestände während der Untersuchung schützt.

## 5.5 Dienstleisterdaten und Kundendienste

FALL J

J

### Warnung zu einem Fotodienstleister

Dienstleisterdienste

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Eine Landesdatenschutzaufsicht warnte im Mai vor einem Dienstleisterangriff mit Folgen für Fotostudios. Kinderfotos und personenbezogene Daten könnten betroffen sein. [S17] |
| GRENZE | Mögliche Offenlegung ist keine bestätigte Zahl betroffener Kinder. Ein gemeinsamer Anbieter belegt keinen eigenen Einbruch bei jedem Studio. |
| REAKTION | Bestimmen Sie die betroffenen Daten jedes Verantwortlichen und koordinieren Sie erreichbare Mitteilungen. Klären Sie die Bedeutung einer Löschung in der Dienstleisterbeziehung, bevor Sie Entfernung versprechen. |

**Fazit**

Bestimmen Sie die betroffenen Daten jedes Verantwortlichen und koordinieren Sie erreichbare Mitteilungen. Klären Sie die Bedeutung einer Löschung in der Dienstleisterbeziehung, bevor Sie Entfernung versprechen.

FALL K

K

## Hotelsoftwaredaten und betrügerische Nachrichten

Beherbergung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Eine Landesmitteilung vom Juli beschrieb eine weitere Welle von Hotelmeldungen nach einem Softwareanbieterangriff. Reservierungs- und Kundendaten waren betroffen; später wurden betrügerische Nachrichten gemeldet. [S18] |
| GRENZE | Die Mitteilung stellte zu diesem Zeitpunkt keinen Abfluss von Bank- oder Zahlungsdaten fest. Reservierungswissen kann eine plausible Zahlungsforderung ermöglichen, ohne dass Kartendaten gestohlen wurden. |
| REAKTION | Schulen Sie Reservierungsteams, veröffentlichen Sie den echten Zahlungsablauf und bieten Sie Gästen einen unabhängigen Prüfweg. |

**Fazit**

Schulen Sie Reservierungsteams, veröffentlichen Sie den echten Zahlungsablauf und bieten Sie Gästen einen unabhängigen Prüfweg.

Die gemeinsame Reaktion bewahrt hilfreichen Kontext, ohne einem Absender weitere Daten zu geben. Ein Hotel sollte einen Anrufer nicht allein aufgrund bekannter Buchungsdaten authentifizieren. Ein Studio sollte verschwundene Oberflächenanzeigen nicht als Nachweis vollständiger Löschung verstehen.

Verträge sollten erklären, wie der Anbieter betroffene Datensätze, relevante Protokolle und Unterstützung für die Meldeentscheidung liefert. Nachweis ist ein geübter Informationsaustausch, nicht eine praktisch ungetestete Vertragszusage.

## 5.6 Verkehr und Kommunikation

L

FALL L

### Buchungsstörung der Deutschen Bahn im Februar

Verkehr

Offizielle Mitteilung:
Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die Deutsche Bahn beschreibt in ihrem offiziellen Bericht überlastete Buchungs- und Auskunftssysteme im Februar. Zeitnahe Berichte nennen Angriffswellen am 17.–18. Februar. [S7][S8] |
| GRENZE | Dies ist ein Verfügbarkeitsfall. Er belegt weder gestohlene Fahrgastdaten noch Zugsteuerungszugriff oder eine offizielle Täterzuordnung. |
| REAKTION | Testen Sie Ersatzwege für Kundeninformation und Ticketabruf gemeinsam mit der Abwehr. Prüfen Sie abgeschlossene Kundenaufgaben statt eine antwortende Startseite mit vollständiger Wiederherstellung gleichzusetzen. |

**Fazit**

Testen Sie Ersatzwege für Kundeninformation und Ticketabruf gemeinsam mit der Abwehr. Prüfen Sie abgeschlossene Kundenaufgaben statt eine antwortende Startseite mit vollständiger Wiederherstellung gleichzusetzen.

Ein nützlicher Kontinuitätsmaßstab ist, ob Fahrgäste während einer Störung Tickets oder verlässliche Informationen erhalten. Verkehrsgrafiken sind für die Abwehr nötig. Sie entsprechen aber nicht einem wieder funktionierenden Buchungsablauf.

Bei Kommunikationsdiensten ist eine vorgelagerte Abhängigkeit von einem Einbruch bei jedem Kunden zu unterscheiden. Bestätigen Sie die betroffenen Dienste, stellen Sie Ersatzkontakte bereit und erfassen Sie die Abhängigkeit für branchenbezogene Meldeentscheidungen.

## 5.7 Aktuelle Aktivitäten: 8.–22. November

Die Quelle verzeichnet 7.111 Beiträge mit Deutschlandbezug vom 8.–22. November. Dies ist beobachtetes Veröffentlichungsvolumen, keine Zahl neuer Vorfälle oder bestätigter deutscher Opfer. [S1]

Die letzten zwei Wochen enthalten neue Vorfälle, Aktualisierungen früherer Ereignisse und Ermittlungsmitteilungen. Die Tabelle trennt diese Arten, damit Veröffentlichungsdaten keinen künstlichen Jahresendanstieg erzeugen.

| Datum | Gegenstand | Belegstatus | Unmittelbare Entscheidung |
|---|---|---|---|
| 8.–17. November | Reservierungsanbieter: Zugriff und Neustart | Ein Dienstleistervorfall mit betrügerischen Gästenachrichten [S58] | Gästewarnung und technische Wiederherstellung koordinieren |
| 8.–20. November | Versorger-IT und Kundenservice gestört | Versorgung aufrechterhalten; Aktualisierungen eines Vorfalls [S59] | Abrechnungsersatz und Energiebetrieb trennen |
| 8. November | Bankbezogenes CRM-Zugangsangebot | Unbestätigte Anzeige eines Administratormandanten [S1] | Konto- und Mandantenzugehörigkeit prüfen |
| 9. November | Wiederherstellung eines Campussystems | Aktualisierung der TUM-Mitteilung vom 6. November [S11] | Freigabe und Kontowiederherstellung prüfen |
| 9. November | Anklage zu Fakeshops | mutmaßliche Taten von 2023 bis Anfang 2025 [S42] | als Ermittlungskontext behandeln |
| 10. November | Hochschul-Beschäftigtendaten | offizielle Datenzugriffsmitteilung [S13] | Kategorien abgrenzen und Beschäftigte warnen |
| 11. November | Hochschul-Webmail | gesonderte Passwortwarnung [S14] | Zurücksetzung am genannten Risiko ausrichten |
| 12. November | Bekanntgabe einer Malware-Aktion | Polizeimaßnahmen vom 9.–11. November [S23] | relevante Infektionshinweise bearbeiten |
| 12. November | Eingeschränkte Sozialdienstkommunikation | Kommunal bestätigt; persönliche Dienste laufen weiter [S55] | Nutzbare Kontaktwege veröffentlichen |
| 12. November | Mitteilung eines Verteidigungszulieferers | Vorfall anerkannt; weitere Einzelheiten offen [S50][S86] | Anbieterupdates über vertrauten Weg prüfen |
| 13. November | Personendatenmitteilung einer Partei | Aktivität im September–Oktober; aktuelle Benachrichtigung [S56] | Daten ohne politische Motivzuordnung abgrenzen |
| 13.–20. November | Hostingzugriff und Umfangsaktualisierung | Späterer Hinweis auf Instanzen mit höherem Risiko [S54] | Mandantenspezifische Entscheidung treffen |
| 15.–18. November | Kreiskrankenhaus und Wiedereröffnung | Ein Vorfall, mehrere Wiederherstellungsschritte [S53] | Klinische Umleitung und Wiedereröffnung koordinieren |
| 16. November | Dateipaket deutscher Organisationen angeboten | Unbestätigte Dokumentenanzeige [S1] | Herkunft und Alter anhand eigener Unterlagen prüfen |
| 17. November | Bankreaktion auf Dokumentenberichte | Stellungnahme widerspricht aktuellem Einbruch [S39] [S40] | historische Offenlegung getrennt halten |
| 17. November | Kommunalverwaltung | Polizei bestätigt Zugriff; Diebstahlprüfung läuft [S51] | Protokolle sichern und Ersatzkontakte bieten |

| Datum | Gegenstand | Belegstatus | Unmittelbare Entscheidung |
|---|---|---|---|
| 17.–20. November | Kommunikationsangriff und Wiederherstellung | Anbietermitteilung und Dienstaktualisierung [S52] | Kundenservice und abhängige Dienste testen |
| 18. November | Warnung zu Industriekühlung | behördlicher Betriebssicherheitshinweis [S21] | unabhängige Überwachung und Fernwartung testen |
| 19. November | Staatliche Liegenschaftsstelle | Vorfall bestätigt, möglicher Abfluss offen [S22] | Ersatzkommunikation aktivieren |
| 19.–20. November | BSI-Jahreslagebericht | neue Veröffentlichung über früheren Zeitraum [S3] | Planung aktualisieren, Ereignisse nicht umdatieren |
| 22. November | Hostingdatenangebot | Unbestätigtes Datenangebot; Verkäufer schließt aktiven Zugriff aus [S1] | Eigene Dateien und Konten vor der Eindämmung prüfen |
| 22. November | Übereinstimmende Zugangsdatenanzeigen | Zwei Beiträge wiederholen eine unbestätigte Angebotsbehauptung [S1] | Kontozugehörigkeit, Alter und frühere Abhilfe prüfen |

Die Tabelle ist keine vollständige Vorfallliste der zwei Wochen. Einige späte Funde bleiben im Abdeckungsregister ungeklärt. Fehlende aktuelle Beiträge oder Hinweise belegen keinen Rückgang der Bedrohung.

## 5.8 Weitere bestätigte Fälle am Ende des Zeitraums

M

FALL M

### Kommunaler Zugriff unter Untersuchung

Kommunalverwaltung

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Eine Polizeimitteilung vom 17. November beschreibt unbefugten Zugriff auf Teile einer Kommunal-IT, Störungen und die Netztrennung. Möglicher Datendiebstahl wurde geprüft. [S51] |
| GRENZE | Eine Kontaktaufforderung belegt weder Verschlüsselung noch konkrete Lösegeldforderung oder kopierte Daten. |
| REAKTION | Sichern Sie Protokolle und Nachricht, organisieren Sie Bürger-Ersatzkontakte und aktualisieren Sie den Umfang mit neuen Erkenntnissen. |

**Fazit**

Sichern Sie Protokolle und Nachricht, organisieren Sie Bürger-Ersatzkontakte und aktualisieren Sie den Umfang mit neuen Erkenntnissen.

FALL N

## N ■ Ausfall eines lokalen Kommunikationsanbieters

Kommunikation

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Anbieter führte Telefon- und Internetausfälle in der Nacht vom 17.–18. November auf einen Cyberangriff zurück. Die Aktualisierung vom 20. November meldete stabile Dienste; die Kundendiensttelefonie wurde noch wiederhergestellt. [S52] |
| GRENZE | Die Mitteilung belegt weder Datendiebstahl noch einen benannten Akteur. Netzbetrieb und erreichbarer Support sind unterschiedliche Wiederherstellungsmeilensteine. |
| REAKTION | Testen Sie Ersatzkontakte und verfolgen Sie die Wiederherstellung nach Funktionen, einschließlich abhängiger Organisationen. |

### Fazit

Testen Sie Ersatzkontakte und verfolgen Sie die Wiederherstellung nach Funktionen, einschließlich abhängiger Organisationen.

FALL O

## O ■ Unterbrochene Notfallaufnahme eines Kreiskrankenhauses

Gesundheit

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Landkreis meldete einen am 15. November entdeckten Angriff und die vorübergehende Abmeldung der Notaufnahme. Weitere Meldungen nannten die Wiederaufnahme am 17. November und funktionierende Operationssäle am 18. November. [S53] |
| GRENZE | Dies sind Phasen eines Vorfalls. Die Mitteilungen belegen weder Täterzuordnung noch Datendiebstahl. |
| REAKTION | Üben Sie Umleitung, manuellen Betrieb und sichere Wiederöffnung mit der klinischen Leitung. Verfolgen Sie verschobene Leistungen auch nach dem technischen Meilenstein. |

### Fazit

Üben Sie Umleitung, manuellen Betrieb und sichere Wiederöffnung mit der klinischen Leitung. Verfolgen Sie verschobene Leistungen auch nach dem technischen Meilenstein.

FALL P

P

## Infrastrukturzugriff bei einem Hostinganbieter

Hosting

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Hostinganbieter beschrieb unbefugten Infrastrukturzugriff am 13.–14. November, beendete Zugänge und änderte Zugangsdaten. Am 20. November wurden wenige Instanzen mit höherem Risiko für direkte Kundenkontakte benannt. [S54] |
| GRENZE | Frühere Aussagen ohne Hinweise auf personenbezogenen Datenabfluss belegen keine fehlenden Kundenfolgen. Die spätere Aktualisierung belegt ebenso wenig Zugriff auf sämtliche Kunden. |
| REAKTION | Folgen Sie authentischen Anbieterhinweisen, prüfen Sie eigene Zugriffsbelege und dokumentieren Sie eine mandantenspezifische Bewertung. |

### Fazit

Folgen Sie authentischen Anbieterhinweisen, prüfen Sie eigene Zugriffsbelege und dokumentieren Sie eine mandantenspezifische Bewertung.

FALL Q

Q

## Eingeschränkte Kommunikation eines Sozialdienstleisters

Sozialdienste

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Eine kommunale Mitteilung vom 12. November beschrieb einen Angriff auf Teile der IT eines Sozialdienstleisters und eingeschränkte E-Mail-Nutzung. Leistungen vor Ort liefen weiter; Telefon oder persönlicher Kontakt blieben möglich. [S55] |
| GRENZE | Zu diesem Zeitpunkt war kein Datenabfluss bekannt. Das ist eine zeitgebundene Bewertung, kein Abwesenheitsbeweis. |
| REAKTION | Veröffentlichen Sie funktionierende Kontakte und erhalten Sie Leistungen für Menschen, die auf den Dienst angewiesen sind. |

### Fazit

Veröffentlichen Sie funktionierende Kontakte und erhalten Sie Leistungen für Menschen, die auf den Dienst angewiesen sind.

FALL R

R

## Mitteilung einer Partei zu früheren Vorfällen

Politische Organisation

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Die AfD-Mitteilung vom 13. November beschrieb unbefugten Postfachzugriff im September und weitere Systeme im Oktober. Sie nannte kopierte personenbezogene Daten und laufende Untersuchungen. Frühere Presseberichte behandelten den Vorfall ebenfalls. [S56][S57] |
| GRENZE | Das Mitteilungsdatum macht frühere Aktivitäten nicht zu einem neuen Novembereinbruch. Eine verifizierte Personenzahl oder Täterzuordnung ist hier nicht festgestellt. |
| REAKTION | Trennen Sie extern gehostete Postfächer von Parteiverwaltungssystemen. Grenzen Sie betroffene Daten ab und dokumentieren Sie Meldeentscheidungen. Datenschutz und Reaktion müssen unabhängig von politischer Zugehörigkeit denselben Maßstäben folgen. |

**Fazit**

Trennen Sie extern gehostete Postfächer von Parteiverwaltungssystemen. Grenzen Sie betroffene Daten ab und dokumentieren Sie Meldeentscheidungen. Datenschutz und Reaktion müssen unabhängig von politischer Zugehörigkeit denselben Maßstäben folgen.

Aus diesem Vorfall folgt keine Bewertung von Parteipositionen, Regierungsentscheidungen oder Wahlergebnissen. Er wird wegen seiner dokumentierten Sicherheits- und Datenschutzfolgen aufgenommen.

FALL Y

Y

## Zugriff beim Reservierungsanbieter und anschließende Betrugsnachrichten

Beherbergungsdienstleister

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein Anbieter von Reservierungssoftware erklärt, ein Angreifer sei am 8. November über ein Kundenkonto eingedrungen und habe am 8.–9. November Gästedaten abgerufen. Danach seien betrügerische E-Mails mit Zahlungs- oder Kartendatenforderungen versandt worden. Weil weitergehender Zugriff nicht ausgeschlossen werden konnte, nahm der Anbieter die Anwendung am 13. November offline und startete am 17. November einen neu aufgebauten Dienst. [S58] |
| GRENZE | Die genaue Datenmenge wurde weiter untersucht. Dies sind Phasen eines Dienstleistervorfalls. Warnungen einzelner Restaurants belegen keine jeweils eigenen Restauranteinbrüche. Ein gemeinsamer Täter mit früheren Hotelsoftwarevorfällen ist nicht belegt. |

| | |
|---|---|
| REAKTION | Fordern Sie eine abgegrenzte Bewertung des Anbieters an, warnen Sie Gäste über einen vertrauenswürdigen Kanal und bestätigen Sie Zahlungsforderungen unabhängig. Die Dienstwiederherstellung beendet nicht den Schutz vor Kundenbetrug. |

**Fazit**

Fordern Sie eine abgegrenzte Bewertung des Anbieters an, warnen Sie Gäste über einen vertrauenswürdigen Kanal und bestätigen Sie Zahlungsforderungen unabhängig. Die Dienstwiederherstellung beendet nicht den Schutz vor Kundenbetrug.

Z

FALL Z

### Gestörte Versorger-IT bei aufrechterhaltener Energielieferung

Energiedienste

Offizielle Mitteilung: Grenzen beibehalten

| | |
|---|---|
| BESTÄTIGT | Ein kommunaler Versorger erklärt, am 8. November einen Angriff erkannt und betroffene Systeme getrennt zu haben. Kundenportale, E-Mail, Zählertermine sowie mehrere Zahlungs- und Einzugsabläufe waren betroffen. Mitteilungen bis zum 20. November bezeichneten die Strom-, Gas- und Fernwärmeversorgung als ununterbrochen. [S59] |
| GRENZE | Zum genannten Zeitpunkt gab es laut Anbieter keinen Hinweis auf einen Abfluss personenbezogener Daten. Das ist eine eingeschränkte Bewertung. Weder Versorgungsausfall noch bestimmter Täter oder Zugangsweg sind belegt. |
| REAKTION | Testen Sie Ersatzabläufe für Kundenservice und Abrechnung getrennt vom Energiebetrieb. Erfassen Sie aufgeschobene Zahlungen und Termine, damit die Wiederherstellung auch aufgelaufene Kundenaufgaben einschließt. |

**Fazit**

Testen Sie Ersatzabläufe für Kundenservice und Abrechnung getrennt vom Energiebetrieb. Erfassen Sie aufgeschobene Zahlungen und Termine, damit die Wiederherstellung auch aufgelaufene Kundenaufgaben einschließt.

## 5.9 Frühere Vorfälle und wichtige Ausschlüsse

Die Dokumentation reicht über die letzten beiden Wochen hinaus. Die folgenden Mitteilungen ergänzen bestätigte Ereignisse und ausdrückliche Ausschlüsse. Ereignis, Aktualisierung und vorsorgliche Abschaltung bleiben getrennt.

| Zeitraum | Rolle und belegter Befund | Grenze und Reaktion |
|---|---|---|
| 21. Januar; Mitteilung am 19. Februar | Polizei und Staatsanwaltschaft bestätigen einen Angriff auf die IT einer staatlichen Kultursammlung [S60] | Zugangsweg, Täter und Datenmenge wurden nicht genannt; Ermittlungsgrenze beibehalten |
| Januar; wiederhergestellt am 23. Januar | Eine Berufskammer entfernte Schadsoftware von ihrer Website und warnte vor möglicherweise abgegriffenen Dashboard-Passwörtern [S61] | Ein möglicher Abgriff ist nicht für alle Nutzer bestätigt; Auswirkungen auf Apothekenversorgungssysteme sind nicht belegt |
| 16.–24. April | Eine Kommune bestätigte Ransomware und Netztrennung; danach wurden Melde-, Standesamts- und Zahlungsfunktionen wiederhergestellt [S62] | Die Mitteilungen betreffen einen Vorfall; Personendatendiebstahl blieb ungeklärt |
| Ereignis im April; Mitteilung am 22. Mai | Ein Universitätsklinikum bestätigt gestohlene Patientendaten beim externen Abrechnungsdienstleister; eigene Systeme und Versorgung waren nicht beeinträchtigt [S75] | Ursprüngliche Mitteilung; späterer Umfang bleibt hier ungeklärt, daher keine abschließende Patientenzahl |
| Bekannt am 10. Juni; Mitteilung am 25. Juni | Ein Forschungsinstitut bestätigt Zugriff auf Dateiserver und gespeicherte Dateien sowie anschließende Trennung und Passwortwechsel [S65] | Welche Dateien tatsächlich entwendet wurden, blieb offen; aus dem Forschungsthema folgt keine Täterzuordnung |
| Erkannt am 19. Juni; aktualisiert am 31. Juli | Ein staatliches Museum bestätigt unrechtmäßiges Kopieren von Beschäftigten-, Partner- und Besucherdaten [S71] | Keine abschließende Betroffenenzahl und kein Täter; Datenkategorien und Betroffenenhilfe abgrenzen |
| 28. Juni–16. Juli | Ein kommunaler Versorger bestätigt Störungen von Portalen, Kommunikation und Zahlungen bei gesicherter Versorgung [S63] | Die spätere Bewertung schloss Verlust aktueller Kundendaten aus, ließ ältere Kundeninformationen aber offen; ein Vorfall über die Wiederherstellungsphasen hinweg |
| 16. Juli; Erklärung am 21. Juli | Eine kommunale Erklärung berichtet nach einem Angriff auf einen IT-Anbieter vom Abfluss dienstlicher Kontakt- und technischer Verzeichnisdaten [S64] | Bürgerdaten, private Beschäftigtenkontakte und Fachverfahrensdaten seien nicht betroffen; der nachgedruckte Text ist keine unabhängige redaktionelle Bestätigung |
| Juli; Augustaktualisierungen | Ein Forschungsinstitut meldet einen Angriff auf eine Netzkomponente und vorsorgliche Kommunikationsunterbrechungen [S66] | Laut Untersuchung scheiterten Zugriffsversuche auf interne Systeme; ein Ausfall ist kein bestätigter interner Zugriff |
| August und Oktober; Mitteilung am 8. Oktober | Eine Gedenkstättenstiftung unterscheidet ausdrücklich einen erneuten Websiteangriff vom früheren IT-Angriff [S67] | Zwei Ereignisse; kein belegter gemeinsamer Täter oder politischer Beweggrund; die Oktobermitteilung begründet die Trennung |

| Zeitraum | Rolle und belegter Befund | Grenze und Reaktion |
|---|---|---|
| 27. September; Mitteilung am 29. September | Ein Kreis beschreibt vorsorgliche Abschaltung gemeinsamer Systeme und Aktualisierungen [S73] | Ausdrücklich kein erfolgreicher Angriff oder festgestellter Abfluss; aus bestätigten Einbrüchen ausgeschlossen |
| Mitteilung am 15. Oktober | Eine Kommune bestätigt kopierte Daten und manuelle Wiederanlaufabläufe; der Datenumfang wird noch untersucht [S68] | Der Versorger wurde ausdrücklich ausgenommen; den Vorfall nicht auf alle verbundenen Einrichtungen ausweiten |

Die Kammermitteilung vom Januar und die Hochschulfälle im November werfen Passwortfragen auf, belegen aber keine gemeinsame Kampagne. Die beiden Versorgerfälle begründen die Trennung von Lieferkontinuität und Kundenbetrieb, keinen gemeinsamen Branchentäter. Weder das Forschungsthema eines Instituts noch die öffentliche Rolle einer Gedenkstätte belegt Motiv oder staatliche Zuordnung.

Eine weitere Universitätsklinik bestätigt am 22. Mai ebenfalls entwendete Patientendaten bei einem externen Abrechnungsanbieter. Eigene Systeme und Versorgung seien nicht beeinträchtigt gewesen. Ihre Betroffenenzahl wird keiner anderen Klinikzahl zugeschlagen. Allein die beiden Kundenmitteilungen belegen weder einen weiteren Anbietervorfall noch eine gemeinsame Patientengesamtzahl. [S83]

## 5.10 Weitere Befunde zu priorisierten Organisationen

**Softwarelieferkette.** Ein Hersteller warnte, dass am 29. April vier schädliche Open-Source-Paketversionen über ein öffentliches Paketregister verbreitet wurden. Die Warnung beschreibt mögliche Entnahme von Zugangsdaten und versuchte Weiterverbreitung nach der Installation. Dies belegt einen Vorfall in der Softwarelieferkette, aber keine Zahl betroffener deutscher Folgeorganisationen. Entwicklungsteams sollten betroffene Builds bestimmen, Herstellermaßnahmen anwenden und erreichbare Zugangsdaten prüfen. [S76]

**Hochschulwartung und Unsicherheit.** Eine Hochschulmitteilung vom 25. Februar beschreibt eine Notfallwartung am 23. Februar nach einem externen Schwachstellenhinweis. Adressdaten Studierender und Ehemaliger könnten zugänglich gewesen sein; eine Ausnutzung ließ sich technisch nicht abschließend feststellen. Korrektur und Unterbrechung sind bestätigt, ein erfolgreicher Einbruch nicht. Der Sicherheitsvorfall gehört mit dieser Einschränkung in die Dokumentation. [S77]

**Dienstleister des Fahrzeughandels.** Eine Händlerwarnung vom Oktober beschreibt unbefugte Zugriffe beim gemeinsamen Anbieter vom 8.–30. September und mögliche Offenlegung von Kunden-, Fahrzeug- und Kaufdaten. Sie unterscheidet bestätigte Datenabrufe von Datensätzen, deren Abruf nicht ausgeschlossen werden konnte. Die Aussage zu nicht betroffenen Bankdaten gilt für diese Kundenmitteilung, nicht pauschal für alle Anbieter-Kunden. Sichern Sie Rechnungsprüfungen und fordern Sie den kundenspezifischen Umfang an. [S80]

**Zertifizierungsdienste.** Eine Zertifizierungsorganisation bestätigt in einer Oktoberveröffentlichung einen IT-Sicherheitsvorfall vom September. Die Belegstelle nennt weder Datenkategorie noch Täter oder Zahl betroffener Kunden. Der Hinweis bleibt entsprechend begrenzt; daraus folgt kein Zugriff auf die Systeme der Zertifizierungskunden. [S84]

Zum Berliner Fall liegt außerdem eine aktuelle Bewertung möglicher Bundesbezüge vor. Die parlamentarische Zusammenfassung vom 16. November warnt, dass Namen oder Abkürzungen in Dateinamen eine falsche Behördenzuordnung bewirken können. Andere betroffene Inhalte bleiben anhand des Dateinamens womöglich unerkannt. Vor einer belastbaren Zuordnung ist eine Inhaltsprüfung nötig. Dies ist eine Umfangsaktualisierung zu Fall A, kein weiterer Angriff. [S82]

## 5.11 Welche Schlüsse die Fälle tragen

| Belegmuster | Gestützte Einordnung | Erste Reaktion |
|---|---|---|
| Verwaltungsdaten kopiert | Umfangsprüfung kann nach Eindämmung weiterlaufen | Datenverantwortliche und Betroffenenunterstützung benennen |
| Zugangsdaten dienstübergreifend genutzt | Identitäten können die Reichweite erweitern | Rechte, Sitzungen und Wiederherstellung prüfen |
| Dienstleisterdaten offengelegt | Kundenschaden kann außerhalb eigener Systeme entstehen | abgegrenzte Datenliste beschaffen und Mitteilungen koordinieren |
| Verfügbarkeit gestört | Aufgaben können ohne belegten Diebstahl ausfallen | Mindestdienst und Ersatzkanal testen |
| Industriesteuerung angegriffen | Betriebssicherheit verlangt physische Prüfung | unabhängige Alarme und sicheren Ersatzbetrieb prüfen |

Die Fälle begründen keine nationale Branchenrangliste. Öffentliche Mitteilungen sind unterschiedlich detailliert; manche Vorfälle bleiben privat. Ihr Nutzen liegt in Reaktionsfragen, die vergleichbare Organisationen beantworten können sollten.

KERNAUSSAGEN

**01**

Trennen Sie missbrauchte Zugangsdaten, kopierte Daten und ausgefallene Dienste.

**02**

Die Tübinger Mitteilungen betreffen getrennte Populationen und Reaktionen.

**03**

Aktuelle Veröffentlichungen umfassen historische Ermittlungen und Wiederherstellungsupdates neben neuen Vorfällen.

KAPITEL 06

# Hacktivismus, DDoS und Betriebstechnik

06

DIESES KAPITEL BEANTWORTET

Was unterscheidet öffentliche Verfügbarkeitsbehauptungen von bestätigten Betriebsfolgen?

**3**

getrennte Prüfungen: Dienst, Daten und physischer Prozess


6.1 Belegzeitleiste 57

6.2 Verfügbarkeit ist ein Kundenergebnis 57

6.3 Kriminelle Störungen sind nicht immer politisch 58

6.4 Industriekühlung verändert die Kontinuitätsfrage 58

6.5 Von der Behauptung zur Reaktion 59

6.6 Nachweise 59

KAPITEL 06

# Hacktivismus, DDoS und Betriebstechnik

KURZFASSUNG

Eine Verfügbarkeitsbehauptung kann kursieren, bevor der Betreiber den Ausfall versteht. Auch ein bestätigter Ausfall belegt weder Datendiebstahl noch Täter oder Prozesszugriff. Der Bahnfall und die Novemberwarnung zu Kühlanlagen zeigen unterschiedliche Reaktionsbedarfe. Bereiten Sie Abwehr und öffentliche Statusmeldungen vor. Prüfen Sie betriebliche Folgen mit den Verantwortlichen für Dienst und Anlage.

## 6.1 Belegzeitleiste

| | |
|---|---|
| 6 Feb. 2026 | **BSI und BfV**<br>Messenger-Phishing-Warnung; Identitätskampagne, kein DDoS-Ereignis [S5] |
| 17 Feb. 2026 | **Deutsche Bahn**<br>Verfügbarkeitsstörung von Buchungs- und Auskunftsdiensten im Februar [S7][S8] |
| 20 März 2026 | **BKA und ZAC NRW**<br>Maßnahmen gegen Aisuru und Kimwolf zugeordnete Infrastruktur bekanntgegeben [S24] |
| 31 Aug. 2026 | **Landeskriminalamt**<br>DDoS- und Erpressungsermittlungen bekanntgegeben; Vorwürfe weiter untersucht [S25] |
| 12 Nov. 2026 | **BKA und ZIT**<br>Malware-Infrastrukturmaßnahmen vom 9.–11. November bekanntgegeben [S23] |
| 18 Nov. 2026 | **LKA NRW**<br>Warnung zu angegriffenen Kühlsteuerungen und betrieblicher Notfallplanung [S21] |

Jede Zeile kennzeichnet ihren Quellentyp. Identitätswarnung und Malware-Ermittlung sind Kontextereignisse, keine zusätzlichen DDoS-Vorfälle. Ihre Aufnahme belegt weder eine gemeinsame Kampagne noch gemeinsame Betreiber.

## 6.2 Verfügbarkeit ist ein Kundenergebnis

Die Bahnmitteilung vom Februar belegt eine Dienststörung. Sie ordnet das Ereignis keinem benannten Akteur zu. Der Bericht macht daher weder unverbundene Rhetorik noch außenpolitische Themen oder einzelne Verfügbarkeitsprüfungen zu einer offiziellen Zuordnung. [S7][S8]

Testen Sie bei einem Kundendienst die vollständige Aufgabe. Eine Startseite kann antworten, während Anmeldung, Ticketabruf oder Zahlung ausfallen. Erfassen Sie funktionierende Abläufe, Nutzergruppen und Ersatzwege. Nennen Sie das Messdatum beim öffentlichen Status.

Trennen Sie Verkehrsabwehr und betriebliche Wiederherstellung. Infrastrukturteams bestätigen die Abwehr des Verkehrs. Der Dienstverantwortliche prüft die wesentliche Nutzeraufgabe. Die Kommunikation sollte die engere Aussage verwenden, bis beides festgestellt ist.

| Frage | Mögliche Akteursbehauptung | Festgestellte Berichterstattung | Prüfung durch Verteidiger |
|---|---|---|---|
| Ist die Website ausgefallen? | momentane fehlgeschlagene Prüfung | Bahnbuchungsstörungen wurden gemeldet [S7][S8] | wesentliche Kundenaufgabe testen |
| Wurden Daten entwendet? | Ausfall als Zugriff dargestellt | der Verfügbarkeitsfall belegt keinen Datendiebstahl | authentifizierte Zugriffe und Datenzugriffsbelege prüfen |
| Wer verursachte den Ausfall? | selbsternannter Akteur beansprucht Verantwortung | keine offizielle Täterzuordnung für diesen Fall festgestellt | Belege sichern und Zuordnung getrennt behandeln |
| Wurde ein Prozess verändert? | behaupteter Steuerungsbildschirm | die Kühlwarnung betrifft ein anderes Betriebsrisiko [S21] | Prozesswerte mit dem Betreiber prüfen |

Die Behauptungsspalte ist eine allgemeine Auslegungshilfe, kein Zitat aus einem deutschen Beitrag. Sie belegt nicht, dass ein bestimmter Akteur jede dieser Aussagen im Berichtszeitraum machte.

## 6.3 Kriminelle Störungen sind nicht immer politisch

Die Landespolizeimitteilung vom August beschreibt Ermittlungen wegen DDoS und versuchter Erpressung. Die BKA-/ZAC-Mitteilung vom März betrifft Botnetzinfrastruktur. Sie begründen Aufmerksamkeit für kriminelle Infrastruktur und Anreize. Sie belegen nicht deren Nutzung bei einem bestimmten deutschen Ausfall. [S24][S25]

Die BKA-Rückschau zu NoName057(16) betrifft 2025. Sie liefert historischen Kontext für die Vorbereitung öffentlicher Dienste. Sie belegt keine Verantwortung der Gruppe für den Bahnvorfall im Februar 2026. [S4]

Behandeln Sie einen genannten politischen Anlass als Darstellung des Sprechers. Reaktionsteams sollten Verkehr, Folgen und Zugriffsbelege eigenständig bewerten. Für Parteien, Behörden, Unternehmen und Zivilgesellschaft sollten dieselben Schutz- und Meldemaßstäbe gelten.

Die gemeinsame ENISA-Mitteilung vom 4. November beschreibt Kühlanlagenvorfälle in mehreren EU-Mitgliedstaaten und eine weitere Welle am 1.–2. November. Sie nennt keine deutsche Betroffenenzahl. Der regionale Befund begründet eine Prüfung exponierter Steuerungen, ergänzt aber keine deutschen Blutbankvorfälle. [S70]

## 6.4 Industriekühlung verändert die Kontinuitätsfrage

Die Novemberwarnung ergänzt eine physische Prozessebene. Deutsche und französische Beispiele bleiben getrennt. Die Quelle belegt weder unmittelbare deutsche Blutbankfolgen noch gemeinsame Betreiber der gemeldeten Ereignisse. [S21]

Die praktische Frage lautet, ob Beschäftigte unsichere Zustände unabhängig von der untersuchten Steuerung erkennen. Ein normaler Bildschirmwert reicht nicht, wenn dasselbe System Messung und Alarm liefert. Prüfen Sie mit dem Anlagenverantwortlichen einen unabhängigen Überwachungsweg.

Der Reaktionsplan muss festlegen, wer Fernwartung ohne Sicherheitsproblem isolieren darf. Er sollte Ersatzlagerung, Eskalationskontakte und vertretbare Unterbrechungen für den jeweiligen Bestand nennen. Dafür braucht es Betrieb, Gebäudetechnik und Sicherheit neben der Informationssicherheit.

Wenden Sie keine pauschale Abschaltanweisung auf jedes Industriesystem an. Ungeplante Trennung kann Überwachung oder notwendige Sicherheitsfunktionen unterbrechen. Nutzen Sie freigegebene Betriebsverfahren und dokumentieren Sie autorisierte Änderungen sowie physische Beobachtungen.

Eine Warnung der Landesbehörde vom August zu speicherprogrammierbaren Steuerungen betrifft vor allem gemeldete Angriffe auf US-Anlagen. Sie empfiehlt Härtung, Trennung und Überwachung, nennt aber keine deutsche Betroffenenzahl. Dies begründet die Prüfung vergleichbarer Geräte, belegt jedoch keinen Einbruch bei einem deutschen Hersteller und keine Täterzuordnung durch diesen Bericht. [S79]

## 6.5 Von der Behauptung zur Reaktion

1. **Dienstzustand feststellen.** Bestätigen Sie betroffene Funktion, Dauer und Ersatzweg. Dokumentieren Sie Kunden- oder Betriebsfolgen getrennt vom Netzsymptom.
2. **Zugriffsbelege prüfen.** Suchen Sie nach unbefugter Identitätsnutzung oder Datenzugriff. Leiten Sie beides nicht allein aus einem Ausfall ab.
3. **Physischen Prozess prüfen.** Nutzen Sie bei Anlagen unabhängige Messungen und den Betriebsverantwortlichen. Trennen Sie Bildschirmabbildung und bestätigte Manipulation.
4. **Begrenzte Mitteilung veröffentlichen.** Nennen Sie bekannte Störung, laufende Maßnahme und nächsten Termin. Beschreiben Sie offene Untersuchungen, ohne fehlende Folgen zu versprechen.
5. **Meldebelege aufbewahren.** Sichern Sie den Verlauf und nutzen Sie den zuständigen Meldeweg. Dokumentieren Sie Entscheidungen auch ohne formelle Meldepflicht.

## 6.6 Nachweise

| Verantwortlich | Test | Nachweis |
|---|---|---|
| Infrastruktur | vertragliche DDoS-Abwehr aktivieren | Übungsprotokoll und Eskalationskontakt |
| Dienstverantwortlicher | Mindestaufgabe während Störung ausführen | Testnachweis und Ersatzanleitung |
| Kommunikation | behauptungsbewusste Statusmeldung ausgeben | freigegebene Vorlage und Aktualisierungsplan |
| Betriebstechnik und Gebäudemanagement | ungewöhnlichen Zustand unabhängig erkennen | beobachteter Alarm- und Reaktionstest |
| Dienstleistersteuerung | Wartungszugang nach freigegebenem Verfahren beschränken | benannter Verantwortlicher und getesteter Entzug |

KERNAUSSAGEN

01

Eine fehlgeschlagene Verfügbarkeitsprüfung belegt weder Diebstahl noch Zuordnung oder dauerhaften Ausfall.

02

Politische Rahmung und kriminelle Infrastruktur sind getrennte Aussagen.

03

Industrievorfälle brauchen physische Prüfung und betrieblichen Ersatz neben der IT-Wiederherstellung.

KAPITEL 07

# Akteure und belegte Beziehungen

07

DIESES KAPITEL BEANTWORTET

Welche akteursbezogenen Aussagen sind belegt, welche Beziehungen bleiben offen?

**35,2%**

der deutschen Einträge tragen die drei häufigsten Gruppenbezeichnungen


7.1 Beziehungskarte 62
7.2 Ransomware und Erpressung 63
7.3 Monats- und Branchenverteilung 66
7.4 Messenger-Phishing und staatlich zugeordnete Kampagnen 67
7.5 Identität bei Personal und Dienstleistern 68
7.6 Ermittlungsmaßnahmen und ihre Grenzen 69
7.7 Schwachstellenbehandlung als branchenübergreifende Kontrolle 70

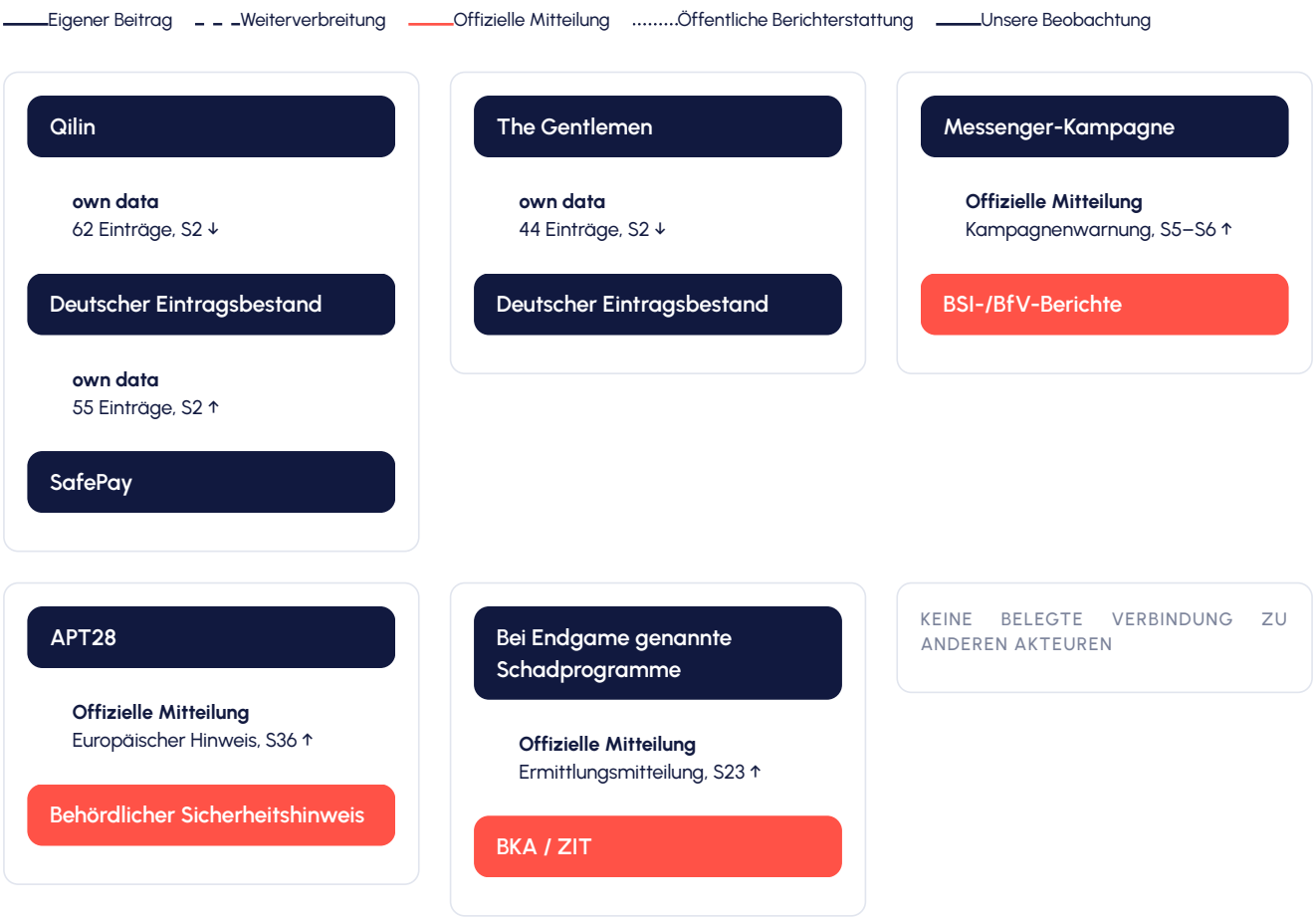
KAPITEL 07

# Akteure und belegte Beziehungen

KURZFASSUNG

Erpressungseinträge liefern in dieser Ausgabe die am besten vergleichbaren Angaben über Akteure. Qilin, SafePay und The Gentlemen führen; die meisten deutschen Einträge tragen jedoch andere Bezeichnungen. Behördliche Kampagnenhinweise ergänzen Identitäts- und Spionagekontext, ohne stets ein deutsches Opfer zu belegen. Trennen Sie Eintragszahlen, staatliche Zuordnung und Betreiberhypothesen. Richten Sie Reaktionen nach betroffenem Zugang und Dienst statt nach Akteursreputation aus.

## 7.1 Beziehungskarte

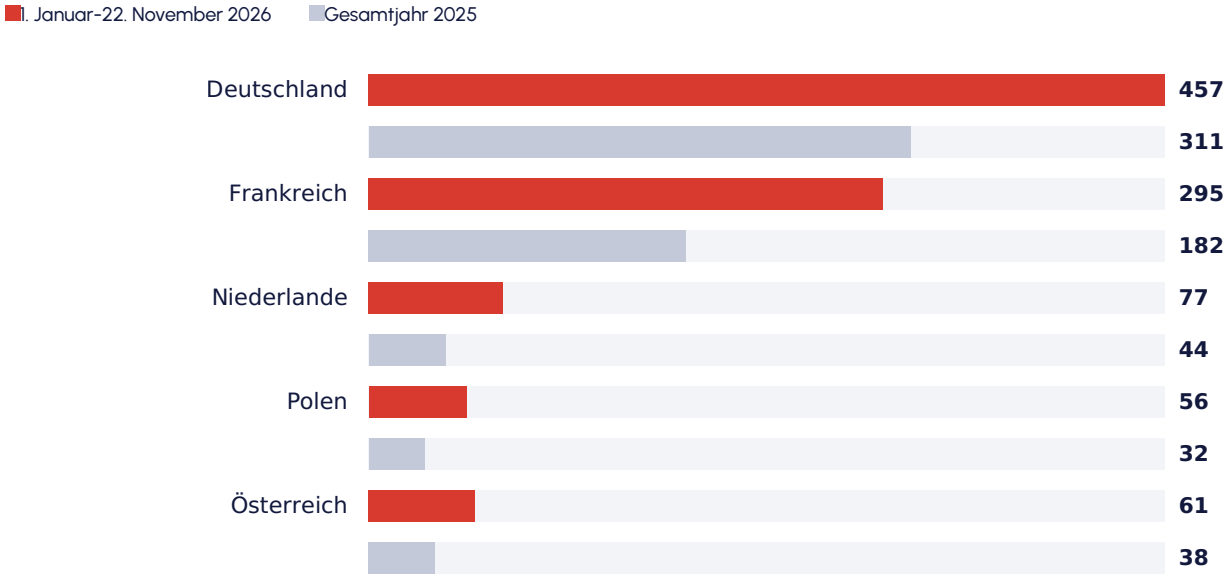



Jede Verbindung bezeichnet eine konkrete Beziehung: Gruppenbezeichnung im deutschen Eintragsbestand, Kampagnenwarnung oder amtliche Ermittlungsmitteilung. Sie belegt keine gemeinsamen Betreiber. Unverbundene Akteure bleiben getrennt; gleiches Land oder gleiche Technik reichen nicht für eine Verbindung.

Das Diagramm kartiert nicht die gesamte deutsche Bedrohungslage. Es macht die Belegbeziehungen dieses Berichts verständlich. Eine neue Behauptung muss ihre eigene Verbindung belegen, bevor sie einer bestehenden Kampagne zugeordnet wird.

## 7.2 Ransomware und Erpressung

### Deutsche Einträge übersteigen im gespeicherten Bestand jeden ausgewählten Vergleichspartner




Ungleiche Zeiträume und unterschiedliche Länderpopulationen; keine nationale Risikorangliste. Quelle: deutsche Brandefense-Ransompedia-Einträge, 1. Januar–22. November 2026; November unvollständig. Einträge dokumentieren kriminelle Behauptungen, keine bestätigten Einbrüche [S2].

Die Vergleichsländer wurden ausschließlich als Beispiele zur Einordnung ausgewählt; ihre Auswahl beinhaltet weder eine Rangfolge noch eine politische Bewertung.

Die fünf Länderzahlen dienen der Einordnung. Sie sind nicht nach Wirtschaftsgröße, Organisationspopulation, Veröffentlichungspraxis oder Quellenabdeckung bereinigt. Daraus lässt sich nicht bestimmen, welches Land sicherere Organisationen hat.

| Land | Angefragter Zeitraum 2026 | Gesamtes Jahr 2025 | Häufigste aktuelle Bezeichnung |
|---|---|---|---|
| Deutschland | 457 | 311 | Qilin, 62 |
| Frankreich | 295 | 182 | Qilin, 48 |
| Niederlande | 77 | 44 | LockBit5, 15 |
| Polen | 56 | 32 | The Gentlemen, 19 |
| Österreich | 61 | 38 | The Gentlemen, 11 |

Quelle: Ransompedia [S2]. Aktuelle Zahlen werden jeweils einem vollständigen Vorjahr gegenübergestellt, nicht demselben Jahresabschnitt. Eine Wachstumsrate wird nicht behauptet.

## Qilin

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

### IN DEUTSCHLAND, 2026

2026
62 deutsche Einträge im angefragten Zeitraum

### BEHAUPTETE ZIELE

Branchen im Eintragsbestand; hier keine Opfernamen

### IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 62 deutsche Einträge unter dieser Bezeichnung.

### UNSERE EINSCHÄTZUNG

Einträge begründen Vorbereitung auf Wiederherstellung und Mitteilungen. Sie belegen weder Verschlüsselung noch Datendiebstahl, gemeinsame Betreiber oder eine Zahlung.

VERTRAUENSGRAD
Hoch für die gespeicherte Anzahl; die zugrunde liegenden Aussagen bleiben Behauptungen

## SafePay

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

### IN DEUTSCHLAND, 2026

2026
55 deutsche Einträge im angefragten Zeitraum

### BEHAUPTETE ZIELE

Branchen im Eintragsbestand; hier keine Opfernamen

### IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 55 deutsche Einträge unter dieser Bezeichnung.

### UNSERE EINSCHÄTZUNG

Einträge begründen Vorbereitung auf Wiederherstellung und Mitteilungen. Sie belegen weder Verschlüsselung noch Datendiebstahl, gemeinsame Betreiber oder eine Zahlung.

VERTRAUENSGRAD
Hoch für die gespeicherte Anzahl; die zugrunde liegenden Aussagen bleiben Behauptungen

## The Gentlemen

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

### IN DEUTSCHLAND, 2026

2026
44 deutsche Einträge im angefragten Zeitraum

### BEHAUPTETE ZIELE

Branchen im Eintragsbestand; hier keine Opfernamen

### IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 44 deutsche Einträge unter dieser Bezeichnung.

### UNSERE EINSCHÄTZUNG

Einträge begründen Vorbereitung auf Wiederherstellung und Mitteilungen. Sie belegen weder Verschlüsselung noch Datendiebstahl, gemeinsame Betreiber oder eine Zahlung.

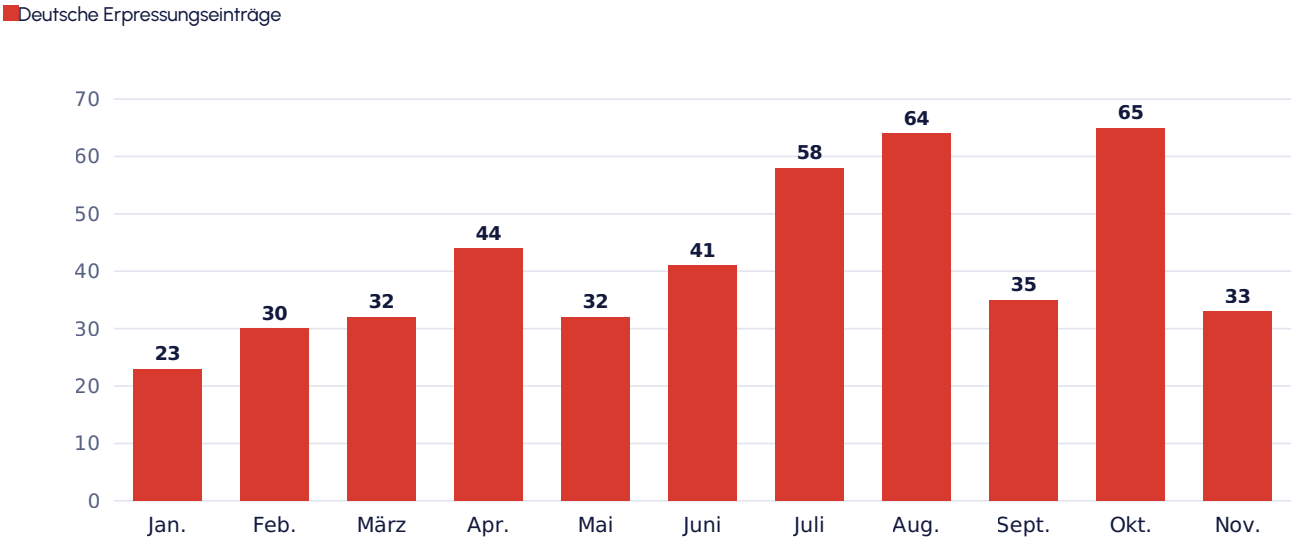
VERTRAUENSGRAD
Hoch für die gespeicherte Anzahl; die zugrunde liegenden Aussagen bleiben Behauptungen

Die führenden deutschen Bezeichnungen umfassen 62, 55 und 44 Einträge. Zusammen sind dies 161 oder 35,2 % von 457. Weitere 67 Bezeichnungen umfassen 296 Einträge. Eine auf die drei führenden Gruppen begrenzte Vorbereitung würde den Großteil des Bestands auslassen. [S2]

Diese Verteilung legt nahe, die Vorbereitung an Schutz- und Reaktionsfähigkeiten auszurichten. Prüfen Sie, wie Identitätszugriffe kritische Daten erreichen können, wie Backups gegen das produktive Identitätssystem abgesichert sind und wie Datenverlustmitteilungen vorbereitet werden. Diese Entscheidungen bleiben bei wechselnden Gruppennamen nützlich.

## 7.3 Monats- und Branchenverteilung

### Eintragszahlen schwanken im Jahresverlauf; der letzte Monat bleibt unvollständig




Quelle: deutsche Brandefense-Ransompedia-Einträge, 1. Januar–22. November 2026; November unvollständig. Einträge dokumentieren kriminelle Behauptungen, keine bestätigten Einbrüche [S2].

| Monat | Deutsche Einträge | Monat | Deutsche Einträge |
|---|---|---|---|
| Januar | 23 | Juli | 58 |
| Februar | 30 | August | 64 |
| März | 32 | September | 35 |
| April | 44 | Oktober | 65 |
| Mai | 32 | November bis Stichtag | 33 |
| Juni | 41 | Gesamt | 457 |

Quelle: Ransompedia [S2]. Die Zahlen beschreiben Veröffentlichungszeiten. Die 65 Oktobereinträge belegen nicht 65 in diesem Monat begonnene Einbrüche. November ist unvollständig und nicht unmittelbar mit einem vollen Monat vergleichbar.

Die häufigste Branchenbezeichnung ist Fertigung mit 77 Einträgen, gefolgt von Beratung mit 55. Diese Bezeichnungen beschreiben Einträge. Sie bilden keinen Nenner der in der jeweiligen Branche tätigen Organisationen. [S2]

Fertigungsleitungen sollten dies als Anlass für Wiederherstellungs- und Dienstleisterzugangstests lesen. Beratung und andere Dienstleister sollten prüfen, ob Kundenrechte oder Kundendaten die Folgen eines Vorfalls erweitern. Die Einträge allein belegen keinen dieser Zugangswege.

## 7.4 Messenger-Phishing und staatlich zugeordnete Kampagnen

### Nicht zugeordnete Messenger-Phishing-Kampagne

Von Behörden beschriebene Kampagne | Staatliche Unterstützung laut BSI plausibel; Zuordnungen anderer Behörden bleiben deren Bewertung

IN DEUTSCHLAND, 2026

2026
Behördlicher Berichtskontext; Daten in Kapitel 7

BEHAUPTETE ZIELE

Nur wie in der genannten Quelle beschrieben

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S5] Behördliche Belegstelle gelesen

[S6] Behördliche Belegstelle gelesen

UNSERE EINSCHÄTZUNG

Beschrieben werden legitime Messenger-Funktionen und soziale Täuschung. Ein Versagen der Softwareverschlüsselung ist nicht belegt. Prüfen Sie verknüpfte Geräte und sichere Wiederherstellung.

VERTRAUENSGRAD
Mit den Grenzen des behördlichen Berichts

Der Messenger-Fall ist eine behördliche Warnung vor Täuschung bei legitimen Funktionen. Er belegt keinen Bruch des Verschlüsselungsprotokolls oder der Anwendungssoftware. Zuordnungen bleiben Aussagen von BSI, BfV und den in ihren Berichten genannten Behörden. [S5][S6]

Für Führungsteams ist die Unterhaltung mit ihren Teilnehmern die maßgebliche Schutzeinheit. Prüfen Sie verknüpfte Geräte, Wiederherstellung und vertraute Kontaktwege. Beschäftigte sollten Sicherheitsaufforderungen vor der Freigabe einer Kontoaktion über einen bekannten Kanal überprüfen.

## APT28

Spionage laut behördlichem Hinweis | Zuordnung durch das LfV Baden-Württemberg

### IN DEUTSCHLAND, 2026

2026
Behördlicher Berichtskontext; Daten in Kapitel 7

### BEHAUPTETE ZIELE

Nur wie in der genannten Quelle beschrieben

### IN ÖFFENTLICHER BERICHTERSTATTUNG

[S36] Behördliche Belegstelle gelesen

### UNSERE EINSCHÄTZUNG

Die Quelle warnt vor Angriffen auf europäische Politikforschung. Sie belegt hier weder ein benanntes deutsches Opfer noch Verbindungen zu anderen deutschen Vorfällen.

VERTRAUENSGRAD
Mit den Grenzen des behördlichen Berichts

Eine Warnung der Landesbehörde vom Januar beschreibt Zugangsdaten-Phishing gegen europäische Denkfabriken und ordnet es APT28 zu. Er trägt die Vorbereitung von Politik- und Forschungseinrichtungen. Er belegt weder ein benanntes deutsches Opfer noch die Zuordnung unverbundener Vorfälle. [S36]

Auch der maritime Hinweis bleibt begrenzt. Die Behörde beschreibt Spionage in sieben ungenannten EU-Staaten und nennt ihre Zuordnung. Deutschland kann nicht allein deshalb ergänzt werden, weil eine deutsche Behörde den Hinweis veröffentlicht. [S38]

Eine Warnung der Landesbehörde vom 30. April beschreibt fingierte Konferenznachrichten, durch die Nutzer einen Befehl ausführen und macOS-Schadsoftware installieren sollen. Die Behörde ordnet die Kampagne Lazarus zu. Das ist eine Kampagnenwarnung, keine bestätigte deutsche Betroffenenzahl. Stellen Sie für Geschäftstermine einen bekannten Supportweg bereit. Beschäftigte sollten abbrechen, wenn eine Einladung zur Ausführung eines unerwarteten Befehls auffordert. [S72]

## 7.5 Identität bei Personal und Dienstleistern

Eine Warnung der Landesbehörde beschreibt IT-Bewerber mit falschen Identitäten und nennt die behördliche Nordkorea-Zuordnung. Die angemessene Reaktion prüft Identität, Qualifikation und Zugang. Sie sortiert nicht nach Erscheinungsbild, Sprache oder unterstellter Nationalität aus. [S37]

Wenden Sie dasselbe Verfahren auf alle Dienstleisterbeschäftigten an. Prüfen Sie Vertragspartner, Beschäftigungsbeziehung, Zugriffsgrund und Gerätevereinbarungen. Klären Sie Freigabe und Entzug von Fernzugängen nach Auftragsende.

Diese Prüfungen helfen auch, autorisierte Auftragnehmer von unbekannten Sitzungen zu unterscheiden. Jede privilegierte Identität sollte einer aktuell verantwortlichen Person und einem Auftrag zugeordnet werden können. Eine Einführung per Dienstleister-E-Mail allein reicht dafür nicht.

## 7.6 Ermittlungsmaßnahmen und ihre Grenzen

### In Operation Endgame genannte Schadprogramme

Behördlicher Ermittlungskontext | Keine staatliche Zuordnung bewertet

IN DEUTSCHLAND, 2026

2026
Behördlicher Berichtskontext; Daten in Kapitel 7

BEHAUPTETE ZIELE

Nur wie in der genannten Quelle beschrieben

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S23] Behördliche Belegstelle gelesen

UNSERE EINSCHÄTZUNG

BKA und ZIT nennen Gootloader, CastleRAT und StealC bei der November-Aktion. Globale Zahlen sind keine deutschen Opferzahlen. Lokale Infektionen müssen weiter geprüft werden.

VERTRAUENSGRAD
Mit den Grenzen des behördlichen Berichts

Die BKA-/ZIT-Mitteilung nennt Gootloader, CastleRAT und StealC bei den Maßnahmen vom 9.–11. November. Sie beschreibt globale Infrastruktur- und Zugangsdatenfunde einschließlich Infrastruktur in Deutschland. Diese Mengen sind keine deutschen Opferzahlen. [S23]

Infrastrukturmaßnahmen zeigen nicht, dass jedes zuvor infizierte Gerät bereinigt ist. Empfänger relevanter Hinweise sollten Rechner, Zugangsdaten und aktive Sitzungen im eigenen Vorfallprozess prüfen. Bewahren Sie Hinweisdaten und die daraus folgende Bewertung auf.

Die Botnetzermittlungen vom März und DDoS-Ermittlungen vom August bilden andere amtliche Fallbestände. Ohne konkretes gemeinsames Element verbindet der Bericht sie weder mit Endgame noch mit Bahn- oder Kühlvorfällen. Verdacht und Ermittlungsmitteilung bleiben von Verurteilungen getrennt. [S24][S25]

## 7.7 Schwachstellenbehandlung als branchenübergreifende Kontrolle

Die BSI-Rückschau zur Ausnutzung von Mobilgeräteverwaltung beschreibt gefährdete Systeme in Deutschland. Sie unterscheidet bestätigten Datenabfluss und Fälle, in denen er nicht ausgeschlossen werden konnte. Eine deutsche Opfergesamtzahl wird nicht genannt. [S45]

Die folgende verifizierte Schwachstelle ist davon unabhängig ein Kontrollbeispiel. Sie belegt keine Ausnutzung bei einer deutschen Organisation dieses Berichts.

| Referenz | Betroffene Produkte | Verifizierte Abhilfe | Grenze |
|---|---|---|---|
| CVE-2026-1731 | BeyondTrust Remote Support 25.3.1 und älter; Privileged Remote Access 24.3.4 und älter | Herstellerkorrekturen BT26-02-RS / BT26-02-PRA; Remote Support 25.3.2 oder neuer; Privileged Remote Access 25.1.1 oder neuer entsprechend der ausdrücklichen Upgrade-Empfehlung | unterstützten Upgrade-Weg und Korrekturberechtigung beim Hersteller prüfen |

Quellen: NVD-Datensatz und Herstellerhinweis [S33][S34]. Ältere, nicht unterstützte Versionen benötigen einen unterstützten Upgrade-Weg. Ein Update allein klärt keinen früheren Einbruch.

Bei einem exponierten Fernwartungsdienst sollten installierte Version, Korrekturbestätigung, Zugangsbeschränkung und Untersuchungsentscheidung als Nachweise vorliegen. Ein globaler Schwachstellendatensatz belegt keine deutsche Ausnutzungskampagne.

KERNAUSSAGEN

**01**

Die meisten deutschen Einträge liegen außerhalb der drei führenden Gruppenbezeichnungen.

**02**

Staatliche Zuordnung gehört zur genannten Quelle und überträgt sich nicht auf unverbundene Vorfälle.

**03**

Ermittlungsmaßnahmen und Updates verlangen lokale Prüfung von Geräten, Identitäten und fortdauernden Zugängen.

KAPITEL 08

# Betrug, Identität und Folgeschäden

08

DIESES KAPITEL BEANTWORTET

Wie kann Informationsverlust nach der Eindämmung weitere Schäden verursachen?

**2**

dokumentierte Folgemuster: Patientenerpressung und Buchungsbetrug


8.1 Eine belegte Kette mit klaren Grenzen 72

8.2 Was Kundenbetreuung beantworten können sollte 73

8.3 Polizeiliche und behördliche Betrugsmeldungen 73

8.4 Behörden als vertrauenswürdiger Prüfweg 74

8.5 Kartenmaterial in Beiträgen: enger Ausschnitt 74

8.6 Preise und Marktgröße 74

8.7 Nachweise für Kundenschutz 75

KAPITEL 08

# Betrug, Identität und Folgeschäden

KURZFASSUNG

Behördliche Warnungen beschreiben die erneute Nutzung gestohlener Informationen gegen Patienten und Hotelgäste. Sie begründen Kundenschutz neben technischer Wiederherstellung. Aktuelle Ermittlungen betreffen außerdem Fakeshops und Kontakte für Anlagebetrug. Deren Zahlen messen jedoch anderes. Bereiten Sie einen vertrauenswürdigen Prüfweg vor, schulen Sie Kundenbetreuung und dokumentieren Sie Folgekontakte. Versprechen Sie nicht, jeden Betrugsversuch verhindern zu können.

## 8.1 Eine belegte Kette mit klaren Grenzen

Die Patienten- und Hotelwarnungen belegen weitere Kontaktversuche mit kopierten Informationen. Sie belegen weder die gesamte kriminelle Lieferkette noch einen abgeschlossenen Verkauf oder gemeinsame Betreiber. [S16] [S18]

Das folgende **analytische Modell** dient der Schutzplanung. Es verbindet Datenoffenlegung, plausible Täuschung, ausgelöste Handlung und Verwertung. Es behauptet nicht, dass Verkäufer, Anrufer und Empfängerkonto in den deutschen Fällen gemeinsam handelten.

| Phase | Möglicher Missbrauch | Unterbrechung durch Verteidiger |
|---|---|---|
| Informationen offengelegt | echte Identitäts- oder Buchungsdetails schaffen Glaubwürdigkeit | betroffene Kategorien bestimmen und angemessen warnen |
| Kontakt aufgenommen | Nachricht ahmt eine bekannte Einrichtung nach | unabhängig geprüften Kontaktweg bieten |
| Handlung verlangt | Empfänger soll zahlen oder einen Code nennen | echten Ablauf veröffentlichen und Beschäftigte schulen |
| Wert übertragen | Zahlung erreicht betrügerisches Ziel | zeitnah Zahlungsdienstleister und Polizei einschalten |
| Erneuter Kontakt | weitere Nachricht nutzt dieselben Daten | Kontext aufbewahren und Unterstützung aktualisieren |

Die betriebliche Folge: Vertrauliche Informationen können nach Passwortwechseln weiter nutzbar bleiben. Eine Krankengeschichte oder frühere Buchung lässt sich nicht einfach ersetzen. Unterstützung sollte daher Sensibilität und Kontext berücksichtigen, nicht nur Anmeldung.

## 8.2 Was Kundenbetreuung beantworten können sollte

Empfänger brauchen einen einfachen Weg zur Echtheitsprüfung. Die Organisation sollte echte Zahlungs- und Unterstützungsabläufe, unabhängige Prüfwege und erforderliche Informationen für eine Meldungsbewertung erklären.

Im Erstgespräch sollten keine zusätzlichen sensiblen Daten in einen ungeprüften Austausch gelangen. Beschäftigte sollten Anrufer nicht allein wegen bekannter Buchungen, Anschriften oder Behandlungen authentifizieren. Genau diese Angaben können vom Vorfall betroffen sein.

Trennen Sie für Betroffene Handlungsempfehlung und Garantie. Eine Warnung erklärt Prüfwege und Beweissicherung verdächtiger Kontakte. Sie belegt weder, dass ein Täter die Daten nicht mehr besitzt, noch, dass eine Zahlung deren Löschung bewirkt.

## 8.3 Polizeiliche und behördliche Betrugsmeldungen

| Veröffentlicht | Amtliche Maßnahme | Einheit und Grenze |
|---|---|---|
| September | Behörden meldeten die Abschaltung von 9.304 deutschen Rufnummern mit Bezug zu mutmaßlichem Anlagebetrug im vorherigen Zeitraum [S43] | Rufnummern; keine Opfer oder eigenständigen Tätergruppen |
| Oktober | Ermittler beschrieben ein missbrauchtes lokales Parteipostfach mit fast 5.000 Nachrichten [S41] | Nachrichten; zu diesem Zeitpunkt kein politisches Motiv festgestellt |
| November | Staatsanwaltschaft meldete eine Fakeshop-Anklage wegen mutmaßlicher früherer Taten [S42] | Ermittlungsmitteilung; Anklage ist keine Verurteilung |

Die Anlagebetrugsmaßnahme zeigt einen Unterbrechungspunkt außerhalb des eigenen Netzes. Der Postfachfall zeigt einen vertrauten Absender als möglichen Betrugskanal. Keiner der Fälle begründet eine neue nationale Verlustschätzung.

Die aktuelle Fakeshop-Ankündigung betrifft mutmaßliche Taten von 2023 bis Anfang 2025. Wegen ihres Veröffentlichungsdatums gehört sie zum aktuellen Ermittlungskontext. Sie ist keine Zahl neu im November 2026 erstellter Fakeshops.

Eine gesonderte Mitteilung von BKA und ZIT vom Mai beschreibt die Abschaltung eines neu aufgebauten illegalen Marktplatzes und die Festnahme seines mutmaßlichen Betreibers. Dies ist eine Strafverfolgungsmaßnahme, keine Zahl deutscher Opferorganisationen und kein Beleg für die Lieferung aller angebotenen Produkte. [S47]

Auch die hessische Datenschutzbehörde warnt davor, dass echte Buchungsangaben betrügerische Gästenachrichten glaubwürdig machen. Ihre allgemeine Beherbergungswarnung belegt keinen Zahlungsdatendiebstahl im konkreten Reservierungsanbieterfall vom November. [S69]

## 8.4 Behörden als vertrauenswürdiger Prüfweg

Eine öffentliche Stelle sollte echte Abläufe für Zahlungen, Dokumentenanfragen und Kontowiederherstellung erklären. Diese Informationen müssen ohne einen Link aus der verdächtigen Nachricht auffindbar sein. Beschäftigte sollten wissen, wie sie Ratsuchende dorthin verweisen.

Prüfen Sie bei einem Postfachvorfall neben dem Passwort auch Regeln, delegierte Zugriffe und autorisierte Anwendungen. Sichern Sie ermittlungsrelevante Nachrichten. Koordinieren Sie Empfängerwarnungen, wenn Kontonutzung zur Kontaktaufnahme belegt ist.

Für Banken und Händler sind neue Zahlungsempfänger, ungewöhnliche Aktivität und gemeldeter Handlungsdruck relevante Kontrollen. Eine veröffentlichte Kontaktliste allein belegt keine betrügerische Überweisung. Die Betrugsabwehr muss Zahlung und Kundensituation prüfen.

## 8.5 Kartenmaterial in Beiträgen: enger Ausschnitt

UMFANG DER KARTENANGABEN

Die Zahlen beschreiben Zahlungskartendatensätze im aufbewahrten Beitragskorpus. Sie messen weder die nationale Kartenexposition noch Kartendiebstahl oder Betrugsverluste.

Das aufbewahrte Beitragsmaterial enthält 15 unterschiedliche Zahlungskartendatensätze mit Deutschlandbezug in 16 Beiträgen. Dies ist eine enge Beobachtung veröffentlichter Kartendaten, keine Vollerhebung deutscher Herausgeber. Der Länderbezug bestätigt weder unabhängig den Wohnsitz des Karteninhabers noch die aktuelle Nutzbarkeit. Daraus werden weder Herausgeberrangfolge noch abgeschlossene Betrugszahlung oder Verlustsumme abgeleitet. [S1]

Ein Herausgeber sollte eine Offenlegung über seinen etablierten Bearbeitungsprozess prüfen. Die behauptete Nutzbarkeit einer Karte belegt weder eine autorisierte Transaktion noch abgeschlossenen Zahlungsbetrug oder Verlust. Der enge Beitragsausschnitt erlaubt keine nationale Zahlungssicherheitsrangliste.

## 8.6 Preise und Marktgröße

Diese Ausgabe veröffentlicht keinen nationalen deutschen Untergrundpreisindex. Angebotspreise einzelner Anzeigen sind Aussagen über ein Angebot. Sie belegen weder abgeschlossene Transaktionen noch den Materialbesitz des Verkäufers oder den Wert der zugrunde liegenden Straftat.

Für eine Schätzung nationaler Betrugserlöse fehlen die nötigen Belege. Wiederholte Werbung kann dasselbe Angebot betreffen; eine Nachricht kann mehrere Länder nennen. Angemessen ist die Prüfung relevanter Behauptungen, nicht die Multiplikation von Beiträgen mit Angebotspreisen.

## 8.7 Nachweise für Kundenschutz

| Verantwortlich | Erforderliche Fähigkeit | Nachweis |
|---|---|---|
| Kundenbetreuung | vorfallbezogene Kontakte erkennen | freigegebene Gesprächshilfen und Übung |
| Betrugsabwehr | verdächtige Zahlungsforderungen bewerten | dokumentierte Eskalation und Zahlungsprüfung |
| Datenschutz | betroffene Kategorien und Personen bestimmen | abgegrenzte Bewertung mit offenen Punkten |
| Kommunikation | unabhängige Prüfung ermöglichen | veröffentlichter vertrauenswürdiger Kontaktweg |
| Sicherheit | Folgehinweise mit dem Vorfall verbinden | Vorfallsakte mit datierter Bewertung |

KERNAUSSAGEN

**01**

Kopierte Informationen können nach Wiederherstellung weitere Erpressung oder Täuschung ermöglichen.

**02**

Rufnummern, Nachrichten und historische Anklagen sind keine nationalen Betrugssummen.

**03**

Geben Sie Betroffenen einen vertrauenswürdigen Prüfweg und geschulte Unterstützung.

KAPITEL 09

# Banken und Finanzdienstleistungen

09

DIESES KAPITEL BEANTWORTET

Welche Finanzdomainbeobachtungen erfordern Konto- und Betrugsprüfungen?

## 13 von 25

beobachtete Finanzdomains mit aktuellem Zugangsdatenangebot


9.1 Expositionsbeobachtungen zu Finanzdomains 77

9.2 Aktuelle Bankstellungnahme ist keine neue Einbruchszahl 78

9.3 Kunden- und institutionsbezogene Belege 78

9.4 Dienstleister- und Zahlungsabhängigkeiten 79

9.5 Meldungen und Dienstleisterresilienz 79

9.6 Prüfung und Abschluss 80

KAPITEL 09

# Banken und Finanzdienstleistungen

KURZFASSUNG

Das ausgewählte Finanzportfolio umfasst 25 beobachtete Domains; für 13 gibt es aktuelle Zugangsdatenangebote. Es enthält mindestens 80.163 Gerätezuordnungen und 669.977 Zugangsdatenzuordnungen. Diese Beobachtungen belegen weder Bankeinbrüche noch eindeutige Kunden. Prüfen Sie aktuelle Konten, unterscheiden Sie Beschäftigte von anderen Nutzern und trennen Sie Kundenbetrugsbelege von Behauptungen über Institutszugriffe.

## 9.1 Expositionsbeobachtungen zu Finanzdomains

| Messwert | Ergebnis | Einordnung |
|---|---|---|
| Finanzdomains mit Beobachtungen | 25 | Ausgewählte Dienste; keine Zählung unabhängiger Banken |
| Domains mit aktuellem Zugangsdatenangebot | 13 | Kontoprüfungshinweise, keine bestätigten Einbrüche |
| Domains mit Gerätezuordnungen | 21 | Zuordnung belegt keine Gerätezugehörigkeit |
| Gerätezuordnungen, mindestens | 80.163 | Überlappende kumulierte Domainzuordnungen |
| Mitarbeitergerätezuordnungen | 698 | Beschäftigung und Kontokontext prüfen |
| Andere Gerätezuordnungen | 79.465 | Keine bestätigten Kundengeräte |
| Zugangsdatenzuordnungen | 669.977 | Keine eindeutigen Personen oder aktiven Zugangsdaten |

Expositionsquelle: datierte Beobachtungen [S87]. Die gesonderten Kartenbeobachtungen in §8.5 belegen keine Herkunft der Kartenexposition. [S1]

UMFANG DER KARTENANGABEN

Diese Zahlen beschreiben ausgewählte Expositionsbeobachtungen zu Finanzdomains. Sie belegen weder unabhängige Banken noch eindeutige Kunden oder bestätigte Einbrüche.

Banken- oder Branchenbewertungen werden nicht veröffentlicht. Die Messwerte oben behalten ihre getrennten Nenner.

## 9.2 Aktuelle Bankstellungnahme ist keine neue Einbruchszahl

Am 17. November erklärte die Deutsche Bank, die in Medienberichten beschriebenen Dokumente seien historisch. Ihre Prüfungen hätten keine Hinweise auf aktuellen IT-Zugriff oder Zugriff auf Kontoinformationen, Anmeldedaten oder Zahlungsdaten ergeben. Die Analyse werde fortgesetzt. [S39]

Russischsprachige Berichte behandelten die Offenlegung und die Aufmerksamkeit der Aufsicht. Dies ist Berichtskontext, keine unabhängige Bestätigung eines neuen Einbruchs im Untersuchungszeitraum. Der Bericht bezieht keine Position zu unverbundenen politischen oder kundenbezogenen Inhalten dieser Berichterstattung. [S40]

| Aussage | Medienoffenlegung | Bankstellungnahme | Behandlung im Bericht |
|---|---|---|---|
| Dokumente vorhanden | Berichte beschreiben interne Unterlagen [S40] | Bank nennt historische Unterlagen [S39] | Dokumentenoffenlegung; Alter einzelner Dateien nicht abschließend geprüft |
| Aktueller IT-Zugriff | hier nicht unabhängig festgestellt | laut Prüfungen keine Hinweise [S39] | kein bestätigter neuer Einbruch gezählt |
| Anmelde- oder Zahlungszugriff | nicht durch eine Mengenüberschrift belegt | Bank meldet keine Hinweise [S39] | keine Expositionssumme abgeleitet |
| Berichterstattung im öffentlichen Interesse | Berichte untersuchen Unterlagen | Bank erläutert ihre Position | keine Zuordnung eines Cyberbetreibers oder Motivs |

Entscheidend ist, ob eigene Belege aktuell nutzbare Identitäten, Sitzungen oder Zugangswege zeigen. Ein Dokumenten-Veröffentlichungsdatum beantwortet diese Frage nicht. Ebenso bleibt eine Erklärung fehlender Hinweise die zeitgebundene Bewertung des Instituts.

Eine BKA-/ZIT-Mitteilung vom 14. August betrifft Ermittlungen zu unbefugten Onlinebanking-Abbuchungen im November 2023 nach einem fehlerhaften Anbieterupdate. Sie berichtet über internationale Strafverfolgungsmaßnahmen im August 2026. Die Behörde nennt die betroffene Bank nicht. Dies sind mutmaßliche historische Taten mit aktueller Ermittlungsphase, kein neuer deutscher Bankeinbruch und keine Verlustsumme für 2026. [S81]

## 9.3 Kunden- und institutionsbezogene Belege

Wenn eine Warnung eine Bankanmeldung nennt, bestimmen Sie, ob das Konto zu Kunden, Beschäftigten, Auftragnehmern oder unbekannten Personen gehört. Ein Dienst-Domainbezug belegt allein weder den Gerätebesitzer noch einen Einbruch in die Bankinfrastruktur.

Prüfen Sie bei bestätigten Beschäftigtenidentitäten Rechte, Sitzungen und Zugriffe. Verbinden Sie Kundenwarnungen mit Kontosicherheits- und Betrugsbelegen. Nutzen Sie vor einschneidenden Maßnahmen die etablierten Authentifizierungs- und Unterstützungsverfahren der Bank.

Verantwortliche sollten gemeinsame Bewertungsbegriffe verwenden: bestätigt und eingedämmt, bereits behoben, nicht zugehörig, ungeklärt oder eskaliert. Der Beleg muss den Abschluss erklären. Eine bloße Gesamtzahl ohne Einzelbewertungen zeigt keine Risikominderung.

## 9.4 Dienstleister- und Zahlungsabhängigkeiten

Hotel- und Gesundheitswarnungen zeigen die Glaubwürdigkeit präziser Kontextinformationen bei betrügerischen Anfragen. Banken sollten Unterstützung für Kunden mit scheinbar echten Institutionsangaben vorbereiten. Dies ist eine Schutzschlussfolgerung aus den Fällen, keine Messung der Bankenbetrugshäufigkeit.

Ordnen Sie bankinterne Zahlungsabläufe Identitäts-, Kommunikations- und Drittdiensten zu. Planen Sie einen Ersatzweg zur Prüfung dringender Anweisungen bei ausgefallener E-Mail oder Telefonie. Testen Sie Ausnahmefreigabe und Dokumentation.

Nutzen Sie bei geänderten Empfängern oder Lieferantenanweisungen einen bekannten unabhängigen Kontakt. Eine neue Nummer aus derselben Nachricht ist kein unabhängiger Prüfweg. Nachweise sind eine dokumentierte Kontrolle und eine bestandene Übung mit synthetischen Daten.

## 9.5 Meldungen und Dienstleisterresilienz

Die Bundesbank-DORA-Hinweise nennen BaFin als zuständigen Empfänger relevanter Finanzinstitutsmeldungen. Sie erläutern die Weitergabe an andere Behörden und das Register vertraglicher IKT-Dienstleistungsvereinbarungen. [S32]

Für schwerwiegende IKT-bezogene Vorfälle legt Artikel 5 der Delegierten Verordnung (EU) 2025/301 diese Fristen fest. [S88]

| Meldung | Frist |
|---|---|
| Erstmeldung | So früh wie möglich; binnen 4 Stunden nach Einstufung als schwerwiegend und grundsätzlich binnen 24 Stunden nach Kenntnis |
| Späte Einstufung | Bei Einstufung als schwerwiegend erst nach 24 Stunden seit Kenntnis: binnen 4 Stunden nach Einstufung melden |
| Zwischenmeldung | Binnen 72 Stunden nach Erstmeldung, auch ohne Änderungen; unverzüglich und bei Wiederaufnahme regulärer Tätigkeiten aktualisieren |
| Abschlussmeldung | Binnen 1 Monat nach Zwischenmeldung oder letzter aktualisierter Zwischenmeldung |

Artikel 5 erlaubt die Abgabe bis mittags am nächsten Arbeitstag, wenn eine Frist auf ein Wochenende oder einen Feiertag fällt. Kreditinstitute, zentrale Gegenparteien, Handelsplatzbetreiber sowie wesentliche oder wichtige NIS2-Einrichtungen dürfen diese Verlängerung für Erst- und Zwischenmeldungen nicht nutzen. Behörden können weitere bedeutende oder systemrelevante Finanzunternehmen ausschließen. Bei unmöglicher Fristeinhaltung ist die Behörde unverzüglich, spätestens jedoch bis zur jeweiligen Frist, mit Begründung zu informieren. [S88]

Praktisch muss eine Dienstunterbrechung mit der eigenen Klassifizierung und dem Meldeprozess verbunden werden. Ein Anbieter kann einen Vorfall haben, ohne dass jeder Kunde denselben Meldeauslöser erfüllt. Dokumentieren Sie die Feststellung und fehlende Informationen.

Das Register sollte im Ernstfall nutzbar sein. Ein Team muss Anbieter, kritische Funktion, technische Verantwortung, Eskalationskontakt und Alternative finden können. Ein getesteter Abruf ist aussagekräftiger als eine ungetestete Tabelle als Resilienznachweis.

## 9.6 Prüfung und Abschluss

Nutzen Sie beobachtete Finanzdomainsignale zur Prüfung eigener Konten. Bestätigen Sie Beschäftigung, Dienstzugehörigkeit, Kontostatus und frühere Abhilfe vor der Eindämmung. Verwandte Dienste können zum selben Rechtsträger gehören. Eine aktuelle Anzeige belegt keinen internen Institutszugriff.

Die engen Kartenbeobachtungen messen keine nationale Kartenexposition. Kundenschutz und Mitarbeiterkontenreaktion benötigen getrennte Verantwortliche.

KERNAUSSAGEN

**01**

Prüfen Sie Finanzdomainbeobachtungen anhand der betroffenen Konten und Dienste.

**02**

Historische Dokumentenoffenlegung und aktueller Zugriff benötigen unterschiedliche Belege.

**03**

Prüfen Sie Identitäten, Zahlungsänderungen und Dienstleisterabhängigkeiten mit etablierten Bankenverfahren.

KAPITEL 10

# Regulierung und nationale Reaktion

10

DIESES KAPITEL BEANTWORTET

Welche Pflichten muss ein deutsches Vorfallteam vor einem Ereignis betriebsfähig machen?

## 24 / 72 Stunden

getrennte Fristen für Erstwarnung und Vorfallmeldung nach der einschlägigen BSIG-Pflicht


10.1 Regeln und Verantwortung 82
10.2 Meldefristen brauchen einen Kenntnisnachweis 83
10.3 Ein Vorfall, mehrere zuständige Wege 83
10.4 Leitungsaufsicht braucht betriebliche Nachweise 84
10.5 Nationale Reaktion und praktische Zusammenarbeit 84
10.6 Eine Meldeübung 84

KAPITEL 10

# Regulierung und nationale Reaktion

KURZFASSUNG

Deutschlands NIS2-Umsetzung gilt bereits. Betroffene Einrichtungen müssen Schutzmaßnahmen, Leitungsaufsicht, Registrierung und erhebliche Vorfallmeldungen verbinden. Datenschutz- und Finanzmeldungen haben andere Auslöser und Empfänger. Ein Vorfall kann mehrere Prüfungen verlangen. Benennen Sie Entscheidungsverantwortliche, sichern Sie Kenntniszeitpunkte und üben Sie gemeinsam mit einem kritischen Anbieter.

Dieses Kapitel dient der Planung, nicht der Rechtsberatung.

## 10.1 Regeln und Verantwortung

Die Tabelle nennt ausgewählte betriebliche Pflichten. Sie bestimmt weder die Betroffenheit einzelner Kandidaten noch sämtliche gesetzlichen Ausnahmen.

| Regel | Gilt bei | Betriebliche Anforderung | Entscheidungsverantwortung |
|---|---|---|---|
| BSIG §30 | rechtlicher Einordnung unter die deutschen Geltungsbereichsregeln | angemessene Risikomaßnahmen einschließlich Kontinuität, Lieferkettensicherheit und Authentifizierung; Einhaltung dokumentieren [S26] | CISO und Geschäftsleitung |
| BSIG §32 | erheblichem Vorfall einer erfassten Einrichtung | Erstwarnung und Meldung unverzüglich, spätestens jedoch binnen 24 beziehungsweise 72 Stunden nach Kenntnis. Abschluss gewöhnlich binnen eines Monats nach der Meldung [S27] | Vorfallleitung und Recht |
| BSIG §33 | erstmaliger oder erneuter rechtlicher Betroffenheit | Registrierung binnen drei Monaten; Änderungen innerhalb der gesetzlichen Frist aktualisieren [S28] | Recht und verantwortlicher Rechtsträger |
| BSIG §38 | Leitung einer erfassten Einrichtung | Risikomaßnahmen umsetzen und überwachen; regelmäßig schulen lassen [S29] | Geschäftsleitung |

| Regel | Gilt bei | Betriebliche Anforderung | Entscheidungsverantwortung |
|---|---|---|---|
| DSGVO Artikel 33–34 | Datenschutzverletzung mit einschlägigem Risiko | Verantwortlicher meldet unverzüglich, möglichst binnen 72 Stunden an zuständige Aufsicht; Betroffeneninformation prüfen [S31] | Datenschutz und Verantwortlicher |
| DORA | relevantem Finanzunternehmen und schwerwiegendem IKT-bezogenem Vorfall | Meldefolge und Ausnahmen in §9.5 anwenden; zuständigen Behördenweg nutzen und IKT-Dienstleisterregister führen [S32][S88] | Finanzvorfallfunktion und Compliance |

Die deutsche Umsetzung trat am 6. Dezember 2025 in Kraft. Die Registrierungsfrist hängt vom Eintritt der rechtlichen Betroffenheit ab. Sie ist keine jährliche Schonfrist. Maßgeblich sind der tatsächliche Rechtsträger und seine Tätigkeit. [S30][S28]

Eine gesonderte Parlamentsmitteilung meldet die Annahme eines Cybersicherheitsgesetzentwurfs am 12. November. Der Parlamentsbeschluss allein belegt kein Inkrafttreten. Ohne Prüfung des verkündeten Gesetzes und seines Geltungsdatums ersetzt er nicht die hier verwendeten geltenden Pflichten. Der Bericht bewertet die politischen Entscheidungen nicht. [S85]

## 10.2 Meldefristen brauchen einen Kenntnisnachweis

Die einschlägige BSIG-Pflicht unterscheidet Inhalt und Frist der frühen und folgenden Meldung. Die Abschlussfrist folgt auf die Vorfallmeldung. Bei fortdauerndem Ereignis sieht das Gesetz eine Fortschrittsmeldung und spätere Abschlussmeldung vor. [S27]

Nach DSGVO hängt die Aufsichtsmeldung vom Risiko für Menschen ab. Auftragsverarbeiter informieren den Verantwortlichen unverzüglich. Hohes Risiko kann Betroffeneninformation verlangen, vorbehaltlich der geltenden Ausnahmen. Dokumentieren Sie die Bewertung auch bei einer Entscheidung gegen die Meldung. [S31]

Beginnen Sie nicht jede Frist mit einem bequemen Pressemitteilungsdatum. Sichern Sie, wann der Rechtsträger Kenntnis erlangte, was damals bekannt war und welche Angaben später eintrafen. Recht sollte Auslöser und gestufte oder ergänzte Meldungen begründen.

## 10.3 Ein Vorfall, mehrere zuständige Wege

Empfänger können von Rechtsträger, Branche und Zuständigkeit abhängen. Bei Datenschutz ist die zuständige Aufsicht zu bestimmen. Finanzvorfälle folgen dem einschlägigen Finanzrahmen. Eine Strafanzeige erfüllt einen anderen Zweck als eine Aufsichtsmeldung.

Der Vorfallakt sollte jeden Weg, Verantwortlichen und Termin nennen. Eine gemeinsame Chronologie kann mehrere Meldungen tragen. Eine Einreichung unter einem Regelwerk erfüllt nicht automatisch ein anderes; dies muss geprüft werden.

Dienstleistereskalation sollte diese Entscheidungen ermöglichen. Verlangen Sie Entdeckungs- und Kenntnisverlauf, betroffenen Dienst, Datenkategorien, mögliche Kundenfolgen und Eindämmungsstand. Trennen Sie bestätigte Fakten von Schätzungen, damit Recht anhand vorhandener Belege entscheiden kann.

## 10.4 Leitungsaufsicht braucht betriebliche Nachweise

BSIG-Leitungspflichten betreffen Umsetzung und Überwachung, nicht nur den Empfang einer Sicherheitspräsentation. Auch die Schulungspflicht verlangt wiederkehrende Beschäftigung mit Risiken und ihren Folgen für die Dienste der Einrichtung. [S29]

Verknüpfen Sie im Leitungsbericht jede wesentliche Abhängigkeit mit Verantwortlichem und Test. Dazu gehören Identitätswiederherstellung, kritische Dienstleistermeldungen, Dienstwiederherstellung und Ersatzbetrieb. Nennen Sie offene Ausnahmen, ihre Eigentümer und Abschlussdaten.

Der Bericht nennt keine universelle Bußgeldzahl und leitet keine Haftungsfolge aus einem Vorfall ab. Dies hängt von Vorschrift, Rechtsträger und Sachverhalt ab. Prüfen Sie geltendes Recht vor einer Aussage über Sanktionen.

## 10.5 Nationale Reaktion und praktische Zusammenarbeit

BKA-/ZIT- und Landespolizeimitteilungen zeigen Ermittlungen zu Malware, DDoS und Betrugsinfrastruktur. Ihre Veröffentlichung bescheinigt keine Bereinigung aller betroffenen Systeme. Relevante Hinweise gehören in den eigenen Reaktions- und Prüfprozess. [S23][S24][S25][S43]

Die Berliner Datenschutzstatistik zeigt außerdem, warum Datenschutzmanagement nicht auf Malwarezahlen reduziert werden kann. Die Population umfasst anders definierte Datenschutzverletzungen. Sie unterstützt Meldevorbereitung, ohne zu nationalen Polizei- oder Eintragssummen addiert zu werden. [S35]

## 10.6 Eine Meldeübung

| Übungsanlass | Erforderliche Entscheidung | Beleg |
|---|---|---|
| Anbieter meldet möglichen Datenzugriff | besteht ausreichende Kenntnis für den Prüfungsbeginn? | Kenntniszeit und rechtliche Begründung |
| Kritischer Dienst fällt aus | greift der branchenspezifische Erheblichkeitstest? | Folgenaufzeichnung und Klassifizierung |
| Umfang bleibt unklar | was kann jetzt gemeldet und später ergänzt werden? | gestufte Meldung und Liste fehlender Angaben |
| Wahrscheinlich hohes Personenrisiko | ist eine erreichbare Direktinformation nötig? | freigegebene Nachricht und Unterstützung |
| Vorfall dauert an | welche Fortschritts- oder Abschlussmeldung ist fällig? | Meldekalender mit Verantwortlichem |

Üben Sie mit Sicherheit, Recht, Datenschutz, Kommunikation und Anbieter. Bestanden ist eine rechtzeitige dokumentierte Entscheidung einschließlich Unsicherheit. Ein sofortiger vollständiger Forensikbericht ist kein realistisches Übungsziel.

KERNAUSSAGEN

**01**

Deutschlands NIS2-Umsetzung gilt; klären Sie jetzt die Betroffenheit des Rechtsträgers.

**02**

Sichern Sie Kenntniszeiten und prüfen Sie jedes Melderegime gesondert.

**03**

Leitungsaufsicht zeigt sich durch verantwortete Kontrollen, getestete Entscheidungen und dokumentierte Ausnahmen.

KAPITEL 11

# Ausblick und bedingte Planung

11

DIESES KAPITEL BEANTWORTET

Welche Vorbereitung folgt aus den Belegen, und was würde die Bewertung ändern?

6

begrenzte Planungsurteile


11.1 Wesentliche Bewertungen 87

11.2 Signale für eine geänderte Reaktion 88

11.3 Bedingte Szenarien 88

11.4 Was nicht prognostiziert werden kann 89

KAPITEL 11

# Ausblick und bedingte Planung

KURZFASSUNG

Bereiten Sie sich auf Erpressung, Identitätsmissbrauch, Dienstleisterdatenverlust und Ausfälle vor. Dies sind beleggestützte Reaktionsprioritäten, keine künftigen Angriffswahrscheinlichkeiten. Der Eintragsbestand schafft Vergleichbarkeit; öffentliche Fälle zeigen Abläufe und Folgen. Ausgewählte Domainbeobachtungen unterstützen Prüfungen; Branchenbewertungen werden nicht veröffentlicht. Benennen Sie Verantwortliche für die folgenden Signale und passen Sie den Plan bei relevanten Änderungen an.

## 11.1 Wesentliche Bewertungen

| Bewertung | Sicherheit | Grundlage und Grenze |
|---|---|---|
| Erpressungsvorbereitung bleibt branchenübergreifend wichtig | hoch für sichtbare Einträge | 457 deutsche Einträge unter 70 Bezeichnungen; Einträge bleiben Behauptungen [S2] |
| Führende Bezeichnungen decken den Großteil nicht ab | hoch für gespeicherten Bestand | drei führende umfassen 161; andere Bezeichnungen 296 [S2] |
| Identitätsreaktion sollte Sitzungen und privilegierte Freigaben umfassen | hoch als Schutzschluss | Campusmitteilung trägt Identitätseindämmung; keine nationale Häufigkeitsschätzung [S11] |
| Kundenschutz kann nach technischer Eindämmung nötig bleiben | hoch für dokumentierte Folgemuster | behördliche Patienten- und Buchungswarnungen; keine Gesamtverlustschätzung [S16][S18] |
| Industriekontinuität braucht physische Prüfung | hoch als Planungsanforderung | amtliche Kühlwarnung; keine gemeinsamen Betreiber abgeleitet [S21] |
| Domainexposition unterstützt Kontoprüfungen | hoch für das ausgewählte Portfolio | datierte Geräte-, Zugangsdaten- und Angebotsbeobachtungen; keine Branchenbewertungen oder nationale Häufigkeit [S87] |

Sicherheit bezieht sich auf die jeweilige Aussage, nicht auf sämtliche Fähigkeiten eines Akteurs. Keine Zeile prognostiziert Angriffsdatum, nationalen Verlust oder Angriffswahrscheinlichkeit einer einzelnen Organisation.

## 11.2 Signale für eine geänderte Reaktion

| Aktuelle Grenze | Neue Belege | Geänderte Entscheidung |
|---|---|---|
| Nur Anzeige | validiertes aktuelles Konto oder Zugang | Identitäts- oder Vorfalleindämmung aktivieren |
| Verfügbarkeitsvorfall | bestätigter Datenzugriff | Datenabgrenzung und Meldeprüfung ergänzen |
| Möglicher Anlagenzugriff | unabhängiger physischer Manipulationsbeleg | Betriebssicherheitsprozess eskalieren |
| Dienstleisterumfang unklar | belastbare Daten- und Kundenliste | Unterstützung und rechtliche Kommunikation ausrichten |
| Zuordnung offen | belegte amtliche oder technische Zuordnung | Akteursbewertung ergänzen, frühere Belege nicht umschreiben |
| Veränderte Domainexposition | validierte und datierte Konto- oder Dienstbeobachtungen | Umfang und Zugehörigkeit vor neuen Reaktionsprioritäten abgleichen |

## 11.3 Bedingte Szenarien

**Szenario 1: Eine aktuelle Identität wird angeboten.** Bestätigt die Prüfung ein aktives Konto eines kritischen Dienstes, prüfen Sie Rechte, Sitzungen und Nutzung. Signal ist der Abgleich mit eigenen Systemen. Entscheidung ist eine angemessene Eindämmung, kein pauschaler Reset allein aufgrund einer Anzeige.

**Szenario 2: Ein Anbieter meldet Kundendatenzugriff.** Liefert er glaubwürdige Belege zu betroffenen Kategorien, binden Sie Recht und Kundenbetreuung ein. Signal ist eine abgegrenzte Anbietermitteilung. Entscheidung sind zeitgebundene Meldeprüfung und Unterstützung bei fortlaufender technischer Untersuchung.

**Szenario 3: Ein Akteur kündigt Störungen an.** Bestätigt die Überwachung die Beeinträchtigung, aktivieren Sie Kontinuitäts- und Abwehrverantwortliche. Signal ist die fehlschlagende wesentliche Aufgabe, nicht nur die Nachricht. Entscheidung sind begrenzte Statusmeldung und vereinbarter Ersatzbetrieb.

**Szenario 4: Anlagenwerte widersprechen sich.** Zeigt unabhängige Messung einen unsicheren Zustand, nutzen Sie das freigegebene Betriebsverfahren. Signal sind physische Belege und Betreiberbewertung. Die Entscheidung umfasst Bestands- und Personenschutz statt nur IT-Wiederherstellung.

**Szenario 5: Eine amtliche Infektionsmeldung trifft ein.** Identifiziert eine vertrauenswürdige Behörde eine eigene Ressource, prüfen Sie Zustand und zugehörige Identitäten. Signal sind zugeordnete Ressource und Beleg. Entscheidung sind Gerätebereinigung, Sitzungswiderruf und dokumentierte Untersuchung, auch nach Infrastrukturmaßnahmen.

Dies sind Planungsannahmen. Sie sind weder gemessene Reaktionsintervalle noch Ereignisprognosen. Sie behaupten auch nicht, dass eine Organisation die empfohlenen Kontrollen bereits umgesetzt hat.

## 11.4 Was nicht prognostiziert werden kann

Der Eintragsanstieg gegenüber einem vollständigen Vorjahr begründet keine künftige Wachstumsrate. Beitragsvolumen liefert keine Angriffswahrscheinlichkeit. Unvollständige Organisationsmessungen tragen keinen nationalen Sicherheitswert.

Öffentliche Fälle spiegeln auch Veröffentlichungspraxis. Eine Branche mit detaillierten Meldungen kann sichtbarer erscheinen, ohne eine höhere tatsächliche Vorfallrate zu haben. Nutzen Sie Fälle für Reaktionstests und Einträge zur Sichtbarkeitseinordnung, jeweils mit diesen Grenzen.

KERNAUSSAGEN

**01**

Bereiten Sie sich auf belegte Abläufe und Folgen vor.

**02**

Ordnen Sie jedem Szenario ein Signal und einen Entscheidungsverantwortlichen zu.

**03**

Ändern Sie Bewertungen bei auflösenden Belegen statt allein bei neuer Akteursrhetorik.

KAPITEL 12

# Maßnahmenplan

12

DIESES KAPITEL BEANTWORTET

Was sollen Teams in den nächsten 90 Tagen liefern, und wie prüft die Leitung dies?

20

Maßnahmen mit Verantwortung und Nachweisen


12.1 Der 30/60/90-Tage-Plan 91

12.2 Verantwortung nach Rollen 93

12.3 Leitungsübersicht 94

12.4 Wie Brandefense helfen kann 94

KAPITEL 12

# Maßnahmenplan

KURZFASSUNG

Beginnen Sie mit Warnungsverantwortung, Kontoprüfung, kritischer Dienstkontinuität und Meldepflichten. Testen Sie anschließend Dienstleistermeldungen, Identitätswiederherstellung, Kundenprüfwege und Betriebszugänge. Zeigen Sie der Leitung bis Tag 90 eine Wiederherstellung und eine verbundene Vorfallübung. Dies sind Planungsziele. Ein aktueller wesentlicher Vorfall gehört sofort in den Reaktionsprozess, ohne auf den Planungsabschnitt zu warten.

## 12.1 Der 30/60/90-Tage-Plan

Die Maßnahmen richten sich nach Diensten und rechtlicher Betroffenheit. Verwenden Sie für Übungen synthetische Daten und freigegebene Verfahren.

### 1Tage 1–30

Meldeweg für Identitäts-, Dienstleister- und relevante öffentliche Behauptungswarnungen einrichten

VERANTWORTLICH
CISO und Threat Intelligence

NACHWEIS
benannte Quelle, Verantwortung und Eskalationstest

jede relevante Identitätswarnung auf Zugehörigkeit, Aktualität, Status und Rechte prüfen

VERANTWORTLICH
Identitätsmanagement und SOC

NACHWEIS
datierte Bewertung jeder eingegangenen Warnung

Sitzungswiderruf und Rechteprüfung bei validierten Vorfällen bestätigen

VERANTWORTLICH
Identitäts- und Anwendungsteams

NACHWEIS
Widerrufsbeleg und Freigabenprüfung

kritische Dienste und vertretbaren Mindestbetrieb bestimmen

VERANTWORTLICH
Notfallmanagement und Dienstverantwortliche

NACHWEIS
Dienstkarte und freigegebener Ersatzbetrieb

BSIG-, DSGVO- und Branchenpflichten sowie Kenntnisaufzeichnung klären

VERANTWORTLICH
Recht, Datenschutz und CISO

NACHWEIS
Pflichtenregister und Fristenübung

### Statusformulierungen für Behauptung, Ausfall und möglichen Datenzugriff freigeben

VERANTWORTLICH
Kommunikation und Vorfallleitung

NACHWEIS
Vorlagen mit Zuständigkeit und Aktualisierungstermin

## 2Tage 31–60

### Vorfallmeldung und Belegaustausch mit kritischem Anbieter testen

VERANTWORTLICH
Dienstleistersteuerung und Recht

NACHWEIS
zeitlich gemessene Übung und offene Punkte

### Kontowiederherstellung ohne alleinige Abhängigkeit von normaler E-Mail testen

VERANTWORTLICH
Identitätsmanagement und Servicedesk

NACHWEIS
synthetischer Fall und Prüfspur

### Administrationsrechte, delegierte Postfachrechte und Wiederherstellungsmethoden prüfen

VERANTWORTLICH
Identitäts- und Anwendungsverantwortliche

NACHWEIS
abgeglichenes Berechtigungsverzeichnis

### öffentlich erreichbare Fernwartung und einschlägige Updates prüfen

VERANTWORTLICH
Infrastruktur

NACHWEIS
Versions-, Korrektur- und Untersuchungsentscheidungen

### Anwendungsberechtigungen kritischer interner Funktionen testen

VERANTWORTLICH
Anwendungssicherheit

NACHWEIS
autorisierter Test und behobene Befunde

### legitime Absender erfassen und kontrollierte DMARC-Durchsetzung planen

VERANTWORTLICH
E-Mail-Team

NACHWEIS
validiertes Absenderverzeichnis und Änderungsplan

### vertragliche Abwehr und Kundenersatzabläufe üben

VERANTWORTLICH
Infrastruktur und Dienstverantwortliche

NACHWEIS
Mindestaufgabe funktioniert im Test

### industrielle Wartungszugänge nach freigegebenem Verfahren beschränken

VERANTWORTLICH
Betriebstechnik, Gebäude und Dienstleisterverantwortliche

NACHWEIS
Zugangsverzeichnis und Entzugstest

unabhängige Alarme und nötige Ersatzlagerung prüfen

VERANTWORTLICH
Betrieb und Sicherheit

NACHWEIS
beobachtete Alarm- und Notfallübung

vertrauenswürdige Zahlungs- und Kontaktprüfwege veröffentlichen

VERANTWORTLICH
Kundenbetreuung und Betrugsabwehr

NACHWEIS
öffentliche Hinweise und Beschäftigtenübung

### 3Tage 61–90

kritischen Dienst isoliert wiederherstellen

VERANTWORTLICH
Infrastruktur und Notfallmanagement

NACHWEIS
Wiederherstellungsnachweis gegen vereinbartes Ziel

Dienstleisterdatenverlust, Behauptungen und Meldungen gemeinsam üben

VERANTWORTLICH
Vorfallleitung, Recht und Kommunikation

NACHWEIS
zeitgerechte Entscheidungen und gestufte Meldungen

Aufbewahrung und Rechte sensibler gemeinsamer Ablagen prüfen

VERANTWORTLICH
Datenverantwortliche und Datenschutz

NACHWEIS
Aufbewahrungsentscheidungen und Zugriffsbelege

Ergebnisse und verantwortete Ausnahmen der Leitung vorlegen

VERANTWORTLICH
CISO und Geschäftsleitung

NACHWEIS
Übersicht mit Verantwortlichen und Terminen

## 12.2 Verantwortung nach Rollen

**Vorstand und Geschäftsleitung.** Fragen Sie nach zuerst ausfallender wesentlicher Funktion, auslösendem Anbieter und getesteter Alternative. Verlangen Sie Verantwortliche und Termine für Ausnahmen. Eine nationale Bedrohungsschlagzeile ersetzt keine lokalen Nachweise.

**CISO und Vorfallleitung.** Bewahren Sie die Belegart jeder Aussage. Verbinden Sie Sicherheitsbefunde mit Dienstverantwortlichen, Rechtsprüfung und Kundenfolgen. Eskalieren Sie Unsicherheit ausdrücklich, wenn Belege keine abschließende Aussage tragen.

**SOC und Identitätsteams.** Prüfen Sie relevante Konten und Ressourcen, Sitzungen und Rechte. Bewahren Sie die Entscheidungsspur auf. Gleichen Sie mit früherer Abhilfe ab, damit alte Offenlegung nicht wiederholt als neues Ereignis behandelt wird.

**Infrastruktur und Anwendungen.** Prüfen Sie installierte Versionen und tatsächliche Berechtigungen. Untersuchen Sie frühere Gefährdungen erforderlichenfalls. Zeigen Sie Wiederherstellung durch die Nutzeraufgabe. Halten Sie Wiederherstellungsabhängigkeiten soweit architektonisch möglich außerhalb desselben Ausfallpfads.

**Betriebstechnik und Gebäudemanagement.** Verantworten Sie physische Werte, sichere Zustände und Ersatzbetrieb. Informationssicherheit unterstützt die Zugriffsuntersuchung. Eine pauschale Trennanweisung ersetzt nicht die Sicherheitsentscheidung des Anlagenverantwortlichen.

**Betrugsabwehr und Kundenbetreuung.** Ermöglichen Sie unabhängige Prüfung von Nachrichten und Zahlungsforderungen. Erklären Sie Grenzen von Löschungsbehauptungen. Verlangen Sie keine weiteren sensiblen Angaben über ungeprüfte Kanäle.

**Recht, Datenschutz und Kommunikation.** Dokumentieren Sie Kenntnis, Risiko und Meldeentscheidungen. Formulieren Sie öffentliche Aussagen nach dem bekannten Sachverhalt. Bewahren Sie Einschränkungen bei Übersetzung und Zusammenfassung für andere Zielgruppen.

## 12.3 Leitungsübersicht

Dies sind empfohlene Planungsziele, keine gemessene Kontrollleistung deutscher Organisationen.

| Maß | Ziel | Beleg |
|---|---|---|
| Warnungsverantwortung | bis Tag 30 eingerichtet | bestandener Weiterleitungstest |
| Relevante eingegangene Warnungen | jede bis Tag 30 datiert bewertet oder verantwortete Ausnahme | Fallregister |
| Meldepflichten | bis Tag 30 erfasst | rechtsträgerspezifisches Register |
| Kritischer Dienstleister | Übung bis Tag 60 abgeschlossen | gemessene Meldung und Belegaustausch |
| Privilegierte Wiederherstellung | bis Tag 60 getestet | synthetischer Fall und Sitzungsprüfung |
| Mindestdienst | bis Tag 60 demonstriert | Nutzeraufgabe und Ersatzablauf dokumentiert |
| Wiederherstellung | bis Tag 90 bestanden oder terminierte Abhilfe | isolierter Test |
| Leitungsprüfung | bis Tag 90 abgeschlossen | dokumentierte Entscheidungen und Ausnahmen |

## 12.4 Wie Brandefense helfen kann

Brandefense verbindet Threat Intelligence, digitalen Risikoschutz und externes Angriffsflächenmanagement. Passende Anwendungsfälle sind validierte Identitätsexposition, Überwachung von Nachahmung und die Bearbeitung externer Befunde bis zur dokumentierten Bewertung. [S44]

Nutzen Sie für eine Demonstration eine repräsentative eigene Domain und einen kritischen Dienst. Fragen Sie nach Weiterleitung, Belegen und Abschlusskriterien einer Warnung. Eine Produktvorführung bedeutet nicht, dass Ihre Organisation in diesem Bericht bewertet wurde.

Brandefense-Demo anfordern.

KERNAUSSAGEN

**01**

Klären Sie Belegverantwortung und Meldepflichten bis Tag 30.

**02**

Testen Sie Dienstleister-, Identitäts-, Kunden- und Betriebsreaktionen bis Tag 60.

**03**

Zeigen Sie Wiederherstellung und berichten Sie verantwortete Ausnahmen bis Tag 90 an die Leitung.

ANHÄNGE

# Anhänge

A–D

DIESES KAPITEL BEANTWORTET

Welche Populationen, Daten und Grenzen gelten für die Ergebnisse?

## Getrennt

Beiträge, Einträge, Vorfälle und Organisationsmessungen


Anhang A. Geltungsbereich und Beleggrenzen 97

Anhang B. Belegregister 100

Anhang C. Quellen 103

Anhang D. Glossar 108

# Anhang A. Geltungsbereich und Beleggrenzen

Die Vergleichsländer wurden ausschließlich als Beispiele zur Einordnung ausgewählt; ihre Auswahl beinhaltet weder eine Rangfolge noch eine politische Bewertung.

## A.1 Zeitraum und Daten

Der angefragte Beobachtungszeitraum reicht vom 1. Januar bis 22. November 2026. Untergrundbeobachtungen beziehen sich auf das Beitragsdatum. Bei Ransomware gilt das Veröffentlichungsdatum des Eintrags, soweit verfügbar. Öffentliche Quellen unterscheiden Ereignis-, Mitteilungs- und Aktualisierungsdaten, wenn sie genannt werden.

Die Recherche erfolgte am 22. November Ortszeit. Während der Erhebung war der Stichtag noch nicht abgeschlossen. Der Bericht behauptet daher keine vollständige Tagesendzählung. Der aktuelle Abschnitt behandelt verfügbare Angaben für 8.–22. November, einschließlich gekennzeichneter Updates und Ermittlungsmitteilungen.

Der BSI-Jahresbericht behandelt einen früheren Zeitraum von Juli bis Juni. Polizeistatistiken und Datenschutzmeldungen behalten ihre eigenen Jahre und Definitionen. Keine dieser Populationen wird zum Eintragsbestand addiert. [S3][S4][S35]

## A.2 Quellen und Priorität

Eigene Quellen umfassen Untergrundmaterial von Odin by Brandefense und Ransomware-Einträge von Ransompedia. Externe Primärquellen sind unter anderem BSI, BfV-bezogene Hinweise, Bundestag, Polizei, Staatsanwaltschaften, Datenschutzaufsichten und Organisationsmitteilungen. Breitere Berichterstattung stützt Namensnennung und Kontext.

Die Fünfländertabellen verwenden Ransompedia-Einträge. Beobachtete Beitragsgesamtzahl und Plattform-/Sprachbeobachtungen mit Deutschlandbezug beschreiben Veröffentlichungssichtbarkeit. Die breitere inhaltliche Abdeckung bleibt unvollständig. Datierte Domainexpositionsbeobachtungen behalten ihren eigenen beobachteten Nenner. Diese Unterschiede stehen in den jeweiligen Kapiteln statt nur in einem allgemeinen Hinweis. [S1][S2]

## A.3 Ransomware-Einträge

Ransompedia verzeichnet 457 deutsche Einträge im angefragten Zeitraum. Die Vergleichszahlen lauten Frankreich 295, Niederlande 77, Polen 56 und Österreich 61. Einträge dokumentieren kriminelle Behauptungen. Sie belegen weder einzelne Einbrüche noch Verschlüsselung, kopierte Daten, Zahlung oder betroffene Personen. [S2]

Vorjahreszahlen betreffen das gesamte Jahr 2025. Die verglichenen Zeiträume sind nicht gleich lang. Länder unterscheiden sich außerdem in Wirtschaftsgröße, Veröffentlichungspraxis und Sichtbarkeit. Die Zahlen sind keine nationalen Risikoranglisten.

Gruppen- und Monatstabellen ergeben dieselbe deutsche Gesamtsumme. Branchenangaben beschreiben den Eintragsbestand, nicht die Vorfallhäufigkeit einer Branche. Kleinere Branchengruppen werden in den öffentlichen Diagrammdaten zusammengefasst.

## A.4 Organisationsexposition

Die Momentaufnahme vom 21.–22. November 2026 umfasst 249 von 250 ausgewählten Domains. Sie enthält mindestens 636.397 Gerätezuordnungen, 33.915 Mitarbeitergerätezuordnungen und 125.422.358 Zugangsdatenzuordnungen. Für 107 beobachtete Domains wurden Zugangsdaten zum Verkauf angeboten. Diese Beobachtungen überschneiden sich; sie zählen keine eindeutigen Personen oder bestätigten Einbrüche. [S87]

Rechtliche Zugehörigkeit und organisatorische Unabhängigkeit bleiben ungeprüft. Verwandte Domains können denselben Betreiber vertreten. Ein Industriedomaindatensatz fehlt. Die nationale Atlas-Kennzahl für das beobachtete Portfolio beträgt 61 von 100. Branchen- oder Organisationsbewertungen werden nicht veröffentlicht.

Ein abgeschlossener passiver Konfigurationsdatensatz fehlt. Eine unvollständige oder nicht beobachtete Messung belegt keine fehlende Kontrolle. Geräte-, Zugangsdaten-, Angebots-, Karten- und Vorfallpopulationen bleiben getrennt.

## A.5 Kartenmaterial

Die Zahlen beschreiben Zahlungskartendatensätze im aufbewahrten Beitragskorpus. Sie messen weder die nationale Kartenexposition noch Kartendiebstahl oder Betrugsverluste.

Persönliche Kartendaten oder Herausgeberkennungen werden nicht veröffentlicht. Die Kartenpopulation darf nicht zu Zugangsdaten, Geräten oder Vorfällen addiert werden. Ergebnis und Verfügbarkeit stehen in §8.5.

## A.6 Vorfallabdeckung

Das Vorfallregister enthält dokumentierte Fälle, Kampagnenhinweise, Ermittlungen, Ausschlüsse und ungeklärte Funde. Diese Kategorien bilden keinen einheitlichen Vorfallnenner. Der Bericht behauptet keine vollständige nationale Vorfallabdeckung.

Einige Quellenseiten und späte Funde bleiben ungeklärt. Manche Vorfälle werden nie veröffentlicht. Ein Dienstleisterereignis kann mehrere Organisationen betreffen, mehrere Updates dagegen nur ein Ereignis. Fehlt ein Vorfall hier, belegt das nicht seine Abwesenheit.

## A.7 Belege und Sicherheit der Aussagen

| Bezeichnung | Bedeutung |
|---|---|
| Beobachtung | gespeicherter Nachweis trägt die genannte Messung oder Veröffentlichung |
| Behauptung | Aussage über Zugang, Folge oder Besitz ist hier nicht unabhängig festgestellt |
| Offizielle Bestätigung | Organisation oder Behörde bestätigt genau die genannte Aussage |
| Analytische Schlussfolgerung | erklärte Einordnung mit Grundlage und Grenze |
| Analytisches Modell | Planungsbeziehung ohne bewiesenen gemeinsamen Betreiber oder Geschäftsvorgang |

Hohe Sicherheit bezieht sich auf eine reproduzierbare Zahl oder gut gestützte Aussage. Sie bestätigt nicht die gesamte Behauptung eines Akteurs. Unverifiziert bedeutet nicht erfunden; ein bestätigter Vorfall bestätigt nicht jede beworbene Einzelheit.

## A.8 Namen, Datenschutz und Neutralität

Organisationen werden nur bei offizieller Bestätigung und breiterer Berichterstattung als Vorfallbetroffene benannt. Andere Fälle verwenden allgemeine Rollen. Quellentitel und Artikeladressen werden teilweise zurückgehalten, um diese Rollen zu erhalten. Die privaten Belege enthalten die unterstützenden Stellen.

Akteursmotive und staatliche Beziehungen bleiben ihren Quellen zugeordnet. Der Bericht bezieht keine Position zu Parteien, Wahlen, Regierungen, Territorien, Religion oder Außenpolitik. Persönliche Identitäten, kriminelle Kontakte, Opferzugänge und sensible Probedatensätze werden nicht veröffentlicht.

## A.9 Prüfgrenzen

Jede verwendete externe Aussage wurde anhand einer Belegstelle geprüft. Die Rechtstabelle trennt Inkrafttreten, Geltungsbereich und Meldeauslöser. Die Schwachstelle wurde mit NVD und Herstellerabhilfe abgeglichen. Sie ist kein Beleg deutscher Ausnutzung. [S33][S34]

Automatische Konsistenzprüfungen belegen weder vollständige Abdeckung noch Veröffentlichungsfreigabe. Englische Hauptfassung und deutsche Übersetzung behalten Zahlen, Quellen- und Fallkennungen sowie Direktiven bei. Bei Abweichungen gilt die englische Ausgabe.

# Anhang B. Belegregister

Das folgende Register zeigt die Aussagegrenzen der Fälle. Es zählt keine eindeutigen nationalen Cyberangriffe. Kartenmetadaten und Textzeilen müssen dieselben Einschränkungen behalten.

| Fall | Datum oder Phase | Branche | Beleg und Grenze |
|---|---|---|---|
| A | August; spätere Mitteilungen | Öffentliche Verwaltung | Kopieren bestätigt; individuelle Folgenprüfung läuft |
| B | 19. November | Staatliche Liegenschaften | Sicherheitsvorfall; möglicher Abfluss ungeklärt |
| C | 6.–9. November | Bildung | Zugangsdaten und Campuszugriff; keine Gesamtpopulations-Diebstahlszahl |
| D | 10. November | Bildung | Beschäftigtendaten; Studierende und Passwörter in dieser Mitteilung ausgeschlossen |
| E | 10.–11. November | Bildung | gesonderter Webmail-Fall; mögliche Passworterfassung |
| F | 19. September | Bildung | Immatrikulationsdaten; keine Feststellung eines öffentlichen Leaks |
| G | Februar–März | Gesundheit | Einbruch und spätere Patientenerpressung, ein Fall |
| H | 22. September | Medizintechnik | begrenzte interne Systeme; genannte betriebliche Ausschlüsse |
| I | Warnung vom 18. November | Pharma-Betriebstechnik | Kühlangriffe gemeldet; keine deutschen Blutbankfolgen festgestellt |
| J | Mai | Dienstleisterdienste | mögliche Kinderdatenoffenlegung; keine bestätigte Zahl |
| K | Julimitteilung | Beherbergung | Dienstleisterdaten und spätere betrügerische Nachrichten |
| L | Februar | Verkehr | Buchungs- und Auskunftsverfügbarkeit gestört |
| M | 17. November | Kommunalverwaltung | unberechtigter Zugriff; Diebstahlprüfung läuft |
| N | 18.–20. November | Kommunikation | Angriff und Wiederherstellung; kein Diebstahl festgestellt |

| Fall | Datum oder Phase | Branche | Beleg und Grenze |
|---|---|---|---|
| O | 15.–18. November | Gesundheit | ein Krankenhausvorfall mit Wiederherstellungsphasen |
| P | 13.–20. November | Hosting | Infrastrukturzugriff; späteres Update zu höherem Instanzrisiko |
| Q | Mitteilung vom 12. November | Sozialdienste | teilweise IT-Beschränkung; Leistungen vor Ort laufen weiter |
| R | September–November | Politische Organisation | früherer Zugriff, aktuelle Mitteilung; keine verifizierte Personenzahl |
| S | Beitrag am 8. November | Bankbezogene Dienste | Administratormandant angeboten; aktiver Zugriff und deutsche juristische Person unbestätigt |
| T | Beitrag am 16. November | Branchenübergreifende Dokumente | Dateien deutscher Organisationen angeboten; Herkunft, Alter und Besitz unbestätigt |
| U | Beitrag am 2. Februar | Projektdienste | Kontakt-/Budgetdatenbank angeboten; Echtheit und Beschaffung unbestätigt |
| V | Beitrag am 6. Oktober | Branchenübergreifende Dokumente | Verwaltungs-/Finanzdatenveröffentlichung behauptet; Dateien und aktueller Zugriff unbestätigt |
| W | Beiträge am 17. Februar | Automobil | Dokumente und Exploit angeboten; Schwachstelle und Besitz unbestätigt; Wiederholung ist kein weiterer Vorfall |
| X | Beitrag am 5. Januar | Identitätsdaten | Käufernachfrage nach Identitäten und Anschriften; kein Besitzbeleg |
| Y | 8.–17. November | Beherbergungsdienstleister | Gästedatenzugriff, Betrugsnachrichten und Wiederanlauf; ein Dienstleistervorfall |
| Z | 8.–20. November | Energiedienste | IT-/Kundenservicestörung; Energielieferung aufrechterhalten |

## B.1 Beziehungen zwischen Fällen lesen

Eine Einrichtung kann in mehreren Fällen erscheinen, wenn getrennte Mitteilungen verschiedene Ereignisse beschreiben. Umgekehrt können mehrere Daten Phasen desselben Falls sein. Die Tübinger Hinweise sind getrennt; Krankenhauseinbruch und spätere Patientennachrichten bilden einen Fall.

Gemeinsame Betreiber mehrerer Fälle werden nicht behauptet. Ransomware-Gruppenbezeichnungen gehören zur Eintragspopulation, amtliche Kampagnenhinweise behalten ihre geografischen Grenzen. Öffentliche Mitteilung und krimineller Eintrag gelten nur dann als verbunden, wenn der Bericht dies ausdrücklich belegt.

## B.2 Beitragszitate

| Karte | Fall | Beitragsdatum | Aussage |
|---|---|---|---|
| B01 | S | 2026-11-08 | Eine Anzeige behauptet Administratorzugriff auf einen bankbezogenen CRM-Mandanten und beschreibt Kundeninformationen. |
| B02 | T | 2026-11-16 | Eine Anzeige bietet Dateien an, die laut Text von deutschen Organisationen stammen. |
| B03 | U | 2026-02-02 | Ein Verkäufer beschreibt Projektkontakte und Budgetdaten eines als deutsch bezeichneten Portals. |
| B04 | V | 2026-10-06 | Ein Beitrag behauptet die Veröffentlichung von Verwaltungs-, Finanz- und geschäftlichen E-Mail-Unterlagen einer als deutsch beschriebenen Organisation. |
| B05 | W | 2026-02-17 | Ein Verkäufer bietet Automobildokumente und gesondert einen IDOR-Exploit an. |
| B06 | X | 2026-01-05 | Ein Käufer fragt nach deutschen Identitätsangaben und betont echte Wohnanschriften. |

# Anhang C. Quellen

Jeder Eintrag nennt das Prüfdatum der Belegstelle. Einige öffentliche Adressen sind zum Schutz allgemein beschriebener Betroffener gekürzt. Zugangsbeschränkungen werden gesondert erfasst. Indexierte Stellen werden von erfolgreich abgerufenen Seiten unterschieden.

**S1:** Odin by Brandefense. Retained Germany underground post evidence. Eigene Quelle; keine öffentliche Adresse. Geprüft am 22. November 2026.

**S2:** Ransompedia. Germany and regional-peer ransomware listing aggregates. Eigene Quelle; keine öffentliche Adresse. Geprüft am 22. November 2026.

**S3:** BSI. Die Lage der IT-Sicherheit in Deutschland 2026. https://bsi-lagebericht.de/ Geprüft am 22. November 2026.

**S4:** BKA. Bundeslagebild Cybercrime 2025, press statement, 12 May 2026. https://www.presseportal.de/blaulicht/pm/7/6273717 Geprüft am 22. November 2026.

**S5:** BSI. Vorfall: Phishing-Angriffe via Messenger. https://bsi-lagebericht.de/node/44 Geprüft am 22. November 2026.

**S6:** Deutscher Bundestag. Signal-Phishing-Angriffe beschäftigen Digitalausschuss, 7 May 2026. https://www.bundestag.de/presse/hib/kurzmeldungen-1174610 Geprüft am 22. November 2026.

**S7:** Deutsche Bahn. Interim Report 2026: Digitalization. https://zbir.deutschebahn.com/2026/en/interim-group-management-report-unaudited/digitalization-and-technology/digitalization/ Geprüft am 22. November 2026.

**S8:** Tagesschau. Booking systems disrupted by cyberattack, 18 February 2026. https://www.tagesschau.de/inland/gesellschaft/bahn-stoerung-it-cyberangriff-100.html Geprüft am 22. November 2026.

**S9:** Berlin data-protection authority. Cyberangriff auf das Landesnetz Berlin. https://www.datenschutz-berlin.de/datenschutz/hinweise-zum-hackerangriff-auf-berlin/ Geprüft am 22. November 2026.

**S10:** Berlin Senate. Cyberangriff auf das Landesnetz: Informationen für Bürgerinnen und Bürger. https://www.berlin.de/cyberangriff/informationen-fuer-buergerinnen-und-buerger/ Geprüft am 22. November 2026.

**S11:** Technische Universität München. IT-Sicherheitsvorfall an der TUM, 6 November; update 9 November 2026. https://www.tum.de/aktuelles/alle-meldungen/pressemitteilungen/details/it-sicherheitsvorfall-an-der-tum Geprüft am 22. November 2026.

**S12:** BR24. Erneut Hackerangriff auf bayerische Uni: TUM betroffen. https://www.br.de/nachrichten/bayern/erneut-hackerangriff-auf-bayerische-uni-tum-betroffen,VaCjyBT Geprüft am 22. November 2026.

**S13:** Universität Tübingen. IT-Sicherheitsvorfall an der Universität Tübingen, 10 November 2026. https://uni-tuebingen.de/universitaet/aktuelles-und-publikationen/pressemitteilung/it-sicherheitsvorfall-an-der-universitaet-tuebingen/ Geprüft am 22. November 2026.

**S14:** Universität Tübingen. Nutzersperrungen nach Angriff auf Webmail, 11 November 2026. https://uni-tuebingen.de/newsfullview-landingpage/article/nutzersperrungen-nach-angriff-auf-webmail/ Geprüft am 22. November 2026.

**S15:** SWR / Tagesschau. Cyberangriff auf die Uni Tübingen: 3.900 Datensätze abgegriffen. https://www.tagesschau.de/inland/regional/badenwuerttemberg/swr-cyberangriff-auf-die-uni-tuebingen-3-900-datensaetze-abgegriffen-100.html Geprüft am 22. November 2026.

**S16:** LfDI Mecklenburg-Vorpommern and LKA Mecklenburg-Vorpommern. Hospital incident and follow-on patient extortion warning, 26 March 2026. https://www.datenschutz-mv.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S17:** LfDI Mecklenburg-Vorpommern. Photo-service supplier incident and possible child-data exposure, 22 May 2026. https://www.datenschutz-mv.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S18:** LfDI Mecklenburg-Vorpommern. Hotel-software incident and follow-up fraud warning, 29 July 2026. https://www.datenschutz-mv.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S19:** Fresenius Medical Care. Statement Regarding Cybersecurity Incident, 22 September 2026. https://freseniusmedicalcare.com/en/media/newsroom/statement-regarding-cybersecurity-incident/ Geprüft am 22. November 2026.

**S20:** Hessenschau. Hacker greifen Fresenius Medical Care an, 23 September 2026. https://www.hessenschau.de/wirtschaft/hacker-greifen-fresenius-medical-care-an-mehrere-systeme-betroffen-v2,fresenius-hackerangriff-100.html Geprüft am 22. November 2026.

**S21:** LKA Nordrhein-Westfalen. Cyberangriffe auf Kühlanlagen, 18 November 2026. https://www.presseportal.de/blaulicht/pm/58451/6392866 Geprüft am 22. November 2026.

**S22:** State ministry. IT security incident at a state property agency, 19 November 2026. https://mkbwk.rlp.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S23:** BKA and ZIT. Operation Endgame action, 12 November 2026. https://www.presseportal.de/blaulicht/pm/7/6389442 Geprüft am 22. November 2026.

**S24:** BKA and ZAC NRW. Action against botnet infrastructure, 20 March 2026. https://www.presseportal.de/blaulicht/pm/7/6239788 Geprüft am 22. November 2026.

**S25:** LKA Schleswig-Holstein. DDoS and attempted-extortion investigation, 31 August 2026. https://www.presseportal.de/blaulicht/pm/2256/6343014 Geprüft am 22. November 2026.

**S26:** Gesetze im Internet. BSIG 2025 §30: risk-management measures. https://www.gesetze-im-internet.de/bsig_2025/__30.html Geprüft am 22. November 2026.

**S27:** Bundesgesetzblatt / Bundesnetzagentur. NIS2 implementation act, BGBl. 2025 I Nr. 301, original §32 and Article 30. https://www.bundesnetzagentur.de/DE/Fachthemen/ElektrizitaetundGas/Versorgungssicherheit/IT_Sicherheit/_DL/NIS-2-Richtlinie.pdf?__blob=publicationFile&v=1 Geprüft am 22. November 2026.

**S28:** Gesetze im Internet. BSIG 2025 §33: registration. https://www.gesetze-im-internet.de/bsig_2025/__33.html Geprüft am 22. November 2026.

**S29:** Gesetze im Internet. BSIG 2025 §38: management duties. https://www.gesetze-im-internet.de/bsig_2025/__38.html Geprüft am 22. November 2026.

**S30:** Bundesregierung. NIS2 implementation commenced on 6 December 2025. https://www.bundesregierung.de/breg-de/service/fragen-und-anworten/nis-2-richtlinie-deutschland-2373174 Geprüft am 22. November 2026.

**S31:** BfDI. Info 1: GDPR and BDSG, Articles 33–34. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.pdf?__blob=publicationFile&v=24 Geprüft am 22. November 2026.

**S32:** Deutsche Bundesbank. DORA incident reporting and third-party information register. https://www.bundesbank.de/de/service/meldewesen/finanzaufsicht/europaeisches-meldewesen/digital-operational-resilience-act-dora--951046 Geprüft am 22. November 2026.

**S33:** NVD. CVE-2026-1731 record. https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Geprüft am 22. November 2026.

**S34:** BeyondTrust. Security Advisory BT26-02. https://www.beyondtrust.com/trust-center/security-advisories/bt26-02 Geprüft am 22. November 2026.

**S35:** Berlin data-protection authority. Höchststand bei Datenschutzvorfällen, 22 October 2026. https://www.datenschutz-berlin.de/pressemitteilung/hoechststand-bei-datenschutzvorfaellen/ Geprüft am 22. November 2026.

**S36:** LfV Baden-Württemberg. APT28 greift Think Tanks in Europa an, 15 January 2026. https://www.verfassungsschutz-bw.de/,Lde_DE/Startseite/Arbeitsfelder/APT28+greift+Think+Tanks+in+Europa+an Geprüft am 22. November 2026.

**S37:** LfV Baden-Württemberg. Remote IT-worker warning, 24 July 2026. https://www.verfassungsschutz-bw.de/,Lde_DE/Startseite/Arbeitsfelder/Nordkoreanische+IT-Worker Geprüft am 22. November 2026.

**S38:** LfV Baden-Württemberg. Maritime-sector espionage in seven EU states, 25 September 2026. https://www.verfassungsschutz-bw.de/,Lde_DE/Startseite/Arbeitsfelder/Chinesische+Cyberspionage+gegen+den+maritimen+Sektor Geprüft am 22. November 2026.

**S39:** Deutsche Bank. Statement on recent media reports, 17 November 2026. https://www.db.com/news/detail/20261117-deutsche-bank-statement-on-recent-media-reports Geprüft am 22. November 2026.

**S40:** Euronews Russian edition. Reporting on historical bank-document disclosure, 18 November 2026. https://ru.euronews.com/2026/11/18/data-watchdog-investigates-massive-deutsche-bank-leak-involving-15-million-files Geprüft am 22. November 2026.

**S41:** CCZ Baden-Württemberg and LKA Baden-Württemberg. Email-account phishing investigation, 19 October 2026. https://generalstaatsanwaltschaft-karlsruhe.justiz-bw.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S42:** CCZ Baden-Württemberg. Fake-shop charge, 9 November 2026. https://generalstaatsanwaltschaft-karlsruhe.justiz-bw.de/pb/,Lde/Startseite/Presse/PM+v_+09_11_2026/?LISTPAGE=1222232 Geprüft am 22. November 2026.

**S43:** Bundesnetzagentur and partner authorities. Operation Herakles telephone-number action, 25 September 2026. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2026/20260925_Herakles.html Geprüft am 22. November 2026.

**S44:** Brandefense. Platform and demonstration information. https://brandefense.io/request-a-demo/ Geprüft am 22. November 2026.

**S45:** BSI. Vorfall: Ausnutzung von Zero-Day-Schwachstellen. https://bsi-lagebericht.de/node/30 Geprüft am 22. November 2026.

**S47:** BKA and ZIT. Criminal marketplace operation, 8 May 2026. https://www.presseportal.de/blaulicht/pm/7/6271239 Belegstelle geprüft am 22. November 2026. Direkter Abruf: HTTP 200, vollständige Mitteilung am 22. November 2026 gelesen.

**S48:** SWR. Webmail attack at Universität Tübingen, 12 November 2026. https://www.swr.de/swraktuell/baden-wuerttemberg/tuebingen/cyberangriff-auf-webmail-der-universitaet-tuebingen-100.html Geprüft am 22. November 2026.

**S49:** LMU Munich. Information about a personal data breach, 19 September 2026. https://www.lmu.de/en/about-lmu/structure/central-university-administration/media-relations-and-communications/press-room/press-release/information-about-a-personal-data-breach-f446c16e.html Geprüft am 22. November 2026.

**S50:** TechRadar. Defence supplier incident and company statement, 19 November 2026. https://www.techradar.com/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S51:** Police. Municipal unauthorised-access investigation, 17 November 2026. https://www.presseportal.de/blaulicht/pm/110975/6392627 Geprüft am 22. November 2026.

**S52:** Local utility communications provider. Cyber incident and service-restoration notices, 18–20 November 2026. https://www.stadtwerke-wittenberg.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S53:** County authority. Hospital incident and recovery notices, 15–18 November 2026. https://www.landkreis-greiz.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S54:** Hosting provider. Infrastructure-access incident, updates through 20 November 2026. https://help.contabo.com/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S55:** Municipal authority. Social-service provider communications notice, 12 November 2026. https://www.offenbach.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S56:** AfD. Public personal-data incident notification, 13 November 2026. https://www.afd.de/wp-content/uploads/2026/11/2026-11-13-_-Allgemeine-AfD-Info-an-Betroffene-_-afd-de-datenpanne.pdf Geprüft am 22. November 2026.

**S57:** Tagesschau. AfD confirms email-account attack, October 2026. https://www.tagesschau.de/inland/innenpolitik/afd-hackerangriff-102.html Geprüft am 22. November 2026.

**S58:** Reservation software supplier. Guest-data access and fraudulent messages; updates 12–17 November 2026. https://reservision.world/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S59:** Municipal energy utility. IT incident detected 8 November; updates through 20 November 2026. https://www.stadtwerke-achim.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S60:** State police and prosecution. Cultural-collection attack on 21 January; investigation notice 19 February 2026. https://www.medienservice.sachsen.de/medien/news/1095116 Geprüft am 22. November 2026.

**S61:** Professional chamber. Website malware, possible password interception and 23 January 2026 restoration. https://www.aknr.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S62:** Municipal authority. 16 April ransomware; 20 and 24 April 2026 recovery updates. https://www.sprendlingen-gensingen.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S63:** Municipal energy utility. 28 June incident and updates through 16 July 2026. https://gsw-kamen.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S64:** Municipal authority statement, republished by local newspaper. 16 July service-provider attack; 21 July 2026 statement. https://www.l-iz.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S65:** Research institute. File-server access; notification 25 June 2026. https://www.zois-berlin.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S66:** Research institute. July network-component incident; updates 17 and 20 August 2026. https://www.idos-research.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S67:** Memorial foundation. 8 October 2026 notice of renewed website attack, distinct from earlier August incident. https://www.sachsenhausen-sbg.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S68:** Municipal authority. 15 October 2026 cyberattack and recovery notice. https://www.eichstaett.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S69:** Hessian data-protection authority. Warning about accommodation-sector attacks and fraudulent guest messages; undated. https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/in-hessen-haeufen-sich-weiterhin-cyberangriffe-im-zusammenhang-mit-beherbergungsbetrieben Geprüft am 22. November 2026.

**S70:** ENISA. Joint statement on cyber incidents in refrigeration systems across the EU, 4 November 2026. https://www.enisa.europa.eu/news/joint-statement-on-cyber-incidents-in-refrigeration-systems-across-the-eu Geprüft am 22. November 2026.

**S71:** State museum. Incident detected 19 June; personal-data update 31 July 2026. https://www.landesmuseum.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S72:** LfV Baden-Württemberg. Mach-O Man: Modulares macOS-Schadprogramm, 30 April 2026. https://www.verfassungsschutz-bw.de/,Lde_DE/Startseite/Arbeitsfelder/Macho-O-Man+Lazarus Geprüft am 22. November 2026.

**S73:** County authority. Preventive shared-system shutdown, 29 September 2026 notice. https://www.kreis-bad-duerkheim.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S75:** University hospital. External billing-provider incident notice, 22 May 2026; later final scope unresolved. https://www.uksh.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S76:** Enterprise software vendor. 29 April 2026 malicious development-package versions; vendor mitigation notice. https://community.sap.com/ (Artikeladresse zurückgehalten) Belegstelle in der indexierten Originalmitteilung am 22. November 2026 geprüft. Direkter Artikelabruf: HTTP 403.

**S77:** University. 23 February emergency maintenance; 25 February 2026 notice. https://www.uni-hamburg.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S79:** LfV Baden-Württemberg. Programmable-controller security warning, 20 August 2026. https://www.verfassungsschutz-bw.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S80:** Vehicle retailer. Service-provider security notice, published 16 October and updated 29 October 2026. https://www.jepsen-autogruppe.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S81:** BKA and ZIT. International investigation after online-banking fraud, 14 August 2026. https://www.presseportal.de/blaulicht/pm/7/6333329 Geprüft am 22. November 2026.

**S82:** Deutscher Bundestag. Response on possible federal interests affected by Berlin incident, 16 November 2026. https://www.bundestag.de/presse/hib/kurzmeldungen-1233476 Geprüft am 22. November 2026.

**S83:** University hospital. External billing-provider incident notice, 22 May 2026. https://www.ukbnewsroom.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S84:** Certification organisation. 27 October 2026 publication acknowledging September IT security incident. https://www.gut-cert.de/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S85:** Deutscher Bundestag. Cybersecurity bill passage announcement, 12 November 2026. https://www.bundestag.de/dokumente/textarchiv/2026/kw46-de-cybersicherheit-1231534 Geprüft am 22. November 2026.

**S86:** Defence technology supplier. Incident statement, 12 November 2026; detection at end of October. https://quantum-systems.com/ (Artikeladresse zurückgehalten) Geprüft am 22. November 2026.

**S87:** Brandefense. Blackhole device and credential associations and Atlas exposure observations for a selected German domain portfolio, snapshot 21–22 November 2026. Eigene Quelle; keine öffentliche Adresse. Geprüft am 22. November 2026.

**S88:** European Commission. Delegated Regulation (EU) 2025/301, Article 5: major ICT-related incident reporting deadlines and exceptions. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32025R0301 Belegstelle geprüft am 22. November 2026. Abruf: vollständigen amtlichen Text gelesen.

**S89:** Polizei Rheinland-Pfalz. Zentrale Ansprechstelle Cybercrime (ZAC). https://www.polizei.rlp.de/die-polizei/dienststellen/landeskriminalamt-rheinland-pfalz/service-und-ansprechstellen/zentrale-ansprechstelle-cybercrime-zac Belegstelle geprüft am 22. November 2026. Abruf: vollständige amtliche Seite gelesen.

**S90:** Have I Been Pwned. Frequently Asked Questions: stealer logs. https://haveibeenpwned.com/FAQs Geprüft am 22. November 2026.

**S91:** Mozilla. Mozilla Monitor: Frequently asked questions, combolist definition. https://support.mozilla.org/en-US/kb/mozilla-monitor-faq Geprüft am 22. November 2026.

**S92:** Salesforce Architects. Platform Multitenant Architecture: tenant environments. https://architect.salesforce.com/docs/architect/fundamentals/guide/platform-multitenant-architecture Geprüft am 22. November 2026.

**S93:** Salesforce. What Is CRM (Customer Relationship Management)? https://www.salesforce.com/crm/what-is-crm/ Geprüft am 22. November 2026.

# Anhang D. Glossar

| Begriff | Einfache Bedeutung |
|---|---|
| Kontowiederherstellung | Verfahren zur Rückgabe berechtigten Zugangs nach Verlust oder Beschränkung |
| Kenntniszeitpunkt | dokumentierte Zeit, ab der ein Rechtsträger genug für die Vorfallbewertung weiß |
| BfV | deutsche Bundesbehörde für Verfassungsschutz |
| BKA | Bundeskriminalamt |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | deutscher Rechtsrahmen für BSI und einschlägige Informationssicherheitspflichten |
| CERT-Bund | Computer-Notfallreaktionsfunktion des Bundes im BSI |
| Combolist | Zusammengeführte Liste von E-Mail-Adressen und Passwörtern aus verschiedenen Datenlecks [S91] |
| Zugangsdaten | Angaben zur Authentifizierung, etwa Passwort oder Token |
| CRM-Mandant | Separate Umgebung einer Organisation innerhalb cloudbasierter Software für Kundenbeziehungsmanagement, englisch Customer Relationship Management [S92][S93] |
| Verantwortlicher | Stelle, die Zweck und Mittel personenbezogener Verarbeitung bestimmt |
| Auftragsverarbeiter | Stelle, die personenbezogene Daten für einen Verantwortlichen verarbeitet |
| DDoS | verteilter Verkehr mit dem Ziel, einen Dienst unerreichbar zu machen |
| DMARC | E-Mail-Richtlinie für Authentifizierung und Ausrichtung zur Absenderdomain |
| DORA | EU-Rahmen für digitale operationale Resilienz im Finanzsektor |
| Erpressungseintrag | kriminelle Veröffentlichung mit einer Behauptung über eine Organisation |
| Identitätssitzung | authentifizierter Zugang, dessen Widerruf neben einem Passwortwechsel nötig sein kann |
| LKA | Landeskriminalamt |
| MFA | Authentifizierung mit mehr als einem Faktor |
| NIS2 | EU-Richtlinie mit national umgesetzten Informationssicherheitspflichten |

| Begriff | Einfache Bedeutung |
|---|---|
| OT | Systeme und Anlagen zur Steuerung oder Überwachung physischer Prozesse |
| Phishing | täuschender Kontakt zur Erlangung von Angaben oder Auslösung unsicherer Handlungen |
| Ransompedia | Brandefense-Quelle für Ransomware-Einträge; Einträge dokumentieren Behauptungen |
| Stealer-Log-Material | Von informationsstehlender Schadsoftware auf infizierten Geräten erzeugte Datensätze, darunter Anmeldedaten und zugehörige Websites [S90] |
| Dienstleisterabhängigkeit | fremdgesteuerte Funktion, Datenablage oder Zugangsbeziehung |
| TLP:CLEAR | Information darf vorbehaltlich anderer Pflichten frei weitergegeben werden |
| ZAC (Polizei) | zentrale polizeiliche Ansprechstellen für Cybercrime bei Organisationen [S89] |
| ZAC NRW | Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, die in [S24] genannte Strafverfolgungsstelle bei der Generalstaatsanwaltschaft Köln |
| ZIT / CCZ | in den amtlichen Mitteilungen genannte spezialisierte Strafverfolgungsstellen |

# Über diesen Bericht

Erstellt von Odin by Brandefense für Sicherheitsleitung, Vorfallreaktion, Betrugsabwehr, Recht und Dienstverantwortliche. Version 1.0 nutzt den angefragten Zeitraum 1. Januar–22. November 2026 und eine getrennte aktuelle Sicht für 8.–22. November.

Domainzugehörigkeit und unvollständige Belegabdeckung bleiben ausdrücklich sichtbar. Die deutsche Ausgabe wurde aus der englischen Hauptfassung übersetzt; bei Abweichungen gilt die englische Fassung.

© 2026 Brandefense. Alle Rechte vorbehalten.

ABOUT BRANDEFENSE

# Attackers See You First. We make sure you do.

Brandefense is an AI-driven platform that sees your organization the way attackers do, continuously monitoring the open, deep, and dark web to detect phishing campaigns, credential leaks, exposed assets, and threat actor activity before they translate into breaches.

Built for security teams that can no longer afford to wait for threats to arrive at the perimeter, it processes millions of external signals in real time and returns only what demands attention.

Unifying Digital Risk Protection, External Attack Surface Management, and Cyber Threat Intelligence under a single interface, Brandefense gives CISOs and SOC teams the external visibility they have always been missing and the intelligence to act on it with confidence.

GARTNER PEER INSIGHTS
**4.7** / 5

COVERAGE
**3** pillars
CTI, DRPS, EASM

MONITORING
**24** / 7
Open, deep and dark web

REQUEST A DEMO

## Request A Demo. See what attackers see.

Discuss your domains, brands and security priorities in a 30-45 minute session with Sales and Presales. A Brandefense team member or a partner in your region will follow up.

Request a demo →

AWARDS

# Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.




### Top InfoSec Innovator

2026




### Deloitte Technology Fast 500 EMEA

2024




### Global InfoSec Awards

2025




### Cybersecurity Excellence Awards

2025

## See Brandefense In Action.

Bring your domains, brands and security priorities to a 30-45 minute conversation with Sales and Presales.

Request a demo →

BRANDEFENSE

# See what attackers see. Before they act.


UNITED STATES

300 Delaware Ave. Ste 210 #328
Wilmington, DE 19801

TÜRKIYE

Üniversiteler Mh., 1605 Cd.
Cyberpark Vakıf Binası No: B25
Çankaya, Ankara

BRANDEFENSE.IO