BRANDEFENSE COUNTRY REPORT · GERMANY 2026

Brandefense Germany Cyber Threat Landscape Report 2026

Identity, extortion and service continuity across an interconnected economy

Odin by Brandefense
Research window: 1 January–22 November 2026
Version 1.0 · Public Research Edition · TLP:CLEAR · 8–22 November 2026

457
German ransomware listings, each recording an extortion claim

107 of 249
observed domains had a credential listed for sale when checked

6
illustrated claims; no confirmed-intrusion total

13 of 25
observed financial domains had a current credential offer

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Germany's digital and threat context	10
03	National exposure: a selected domain portfolio	14
04	Underground activity and claim interpretation	20
05	Confirmed incidents and targeting by sector	34
06	Hacktivism, DDoS and operational technology	53
07	Threat actors and evidence relationships	58
08	Fraud, identity and secondary harm	68
09	Banking and financial services	73
10	Regulatory and national response	78
11	Outlook and conditional planning	83
12	Action plan	87
A	Appendix A. Scope and evidence boundaries	94
B	Appendix B. Evidence register	97
C	Appendix C. Sources	100
D	Appendix D. Glossary	105
	About this report	107

Board and executives	01 05 11 12
CISO and security leads	03 04 05 07 12
SOC and identity teams	04 06 07 B
Fraud and customer protection	05 08 09
Legal and communications	05 06 10 12

About this edition

Prepared with AI assistance. Evidence and limitations are stated beside the findings.

Germany's visible threat picture connects stolen identities, extortion claims and interrupted services. The priority is to contain each confirmed exposure while preserving essential operations.

457

German ransomware listings in the requested window; criminal claims

1,221,949

observed Germany-associated posts; not an incident count

107 of 249

observed domains with a current credential offer

4

decisions for leaders, linked to completion evidence

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions should come first?
2 Context	Which German operating conditions shape the response?
3 Organisation exposure	Which measured signals need validation?
4 Underground activity	What do the retained posts actually establish?
5 Incidents by sector	What did organisations and authorities confirm?
6 DDoS and operational technology	How do availability claims differ from operational impact?
7 Actors and relationships	Which associations are supported, and by which source?
8 Fraud economy	How can stolen information become a second incident?
9 Banking	How do financial-domain observations inform response?
10 Regulation	Which reporting clocks and responsibilities apply?
11 Outlook	Which conditional scenarios justify preparation?
12 Action plan	Who acts, and what demonstrates completion?
Appendices A–D	Scope, evidence, sources and definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify immediate decisions for German organisations?

457

German ransomware listings, each recording an extortion claim

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Germany's evidence supports three priorities: identity security, recovery and supplier oversight. Ransompedia records 457 German listings, exceeding the full-year 2025 total of 311. Public disclosures distinguish data theft, credential misuse and service disruption. Recent university incidents, industrial-cooling warnings and provider notices reinforce that distinction. The exposure snapshot supports account validation across the selected portfolio. Confirm your own account and supplier alerts, rehearse recovery, and assign separate owners to operational continuity and notification decisions.

This report combines Brandefense's retained underground material and ransomware listings with public reporting. Posts, listings, public incidents and domain exposure observations are separate populations. They are never added into a national attack total. [S1][S2]

The requested window ends on 22 November. Evidence reflects what was available when reviewed on that date; the cut-off day was still in progress during collection. The closing fortnight is treated separately in §5.7. Publication dates do not establish when an intrusion began.

1. Extortion visibility is distributed across many claimant labels. Germany has 457 listings against 311 in all of 2025. Qilin, SafePay and The Gentlemen account for 161, or 35.2%, of the current-window listings. The remaining 296 belong to other labels. This compares a partial year with a full year; it is not a matched-period growth rate. A listing establishes a public criminal assertion, not encryption, theft or financial loss. [S2]

2. Confirmed identity misuse deserves a different response from an advertisement. TUM's disclosure describes central-login credentials, including an administrator's credential, being used against a campus system. Its recovery update required password changes and two-factor authentication. That supports account and session containment for an organisation with comparable evidence. It does not establish that every university account was stolen. [S11][S12]

3. Supplier events can continue as fraud after technical restoration. An official hospital-related warning describes direct extortion messages to patients using stolen information. A separate hotel-software warning describes follow-up fraudulent messages. These are documented routes from information loss to customer harm. Legal, customer operations and fraud teams should join the response before a system returns. [S16][S18]

4. Availability, data loss and physical-process safety require separate evidence. Deutsche Bahn confirmed February disruption of booking and information services. November's official cooling warning concerns industrial controls. The two justify different continuity exercises; neither supports assigning a common actor or assuming that a website outage means operational-system access. [S7][S8][S21]

5. Current credential offers require owned-account validation. Of 249 observed domains, 107 had a credential offered for sale. The selected portfolio records at least 636,397 device associations and 125,422,358 credential-record associations. These overlapping observations do not count unique people or confirmed intrusions. One selected domain has no complete exposure record. [S87]

Four decisions for leaders

1. **Validate identity alerts against your own environment.** Establish an alert route, confirm account ownership and freshness, inspect privileges, and revoke sessions where warranted. Record a disposition for each alert (§3.4, §12).
2. **Test restoration and minimum service together.** Restore a critical service in isolation and demonstrate a workable fallback while the normal identity or booking system is unavailable (§5–6).
3. **Bring suppliers into incident decisions early.** Identify who holds customer records, who controls remote maintenance, and who can provide timely evidence. Rehearse notification with a critical supplier (§8, §10).
4. **Separate communications by the facts established.** Say whether a claim, an outage, data access or operational manipulation is confirmed. Give an update time and an accountable spokesperson (§6, §12).

The year in numbers

1,221,949

Observed Germany-associated posts in the requested window

WHAT IT DOES NOT MEASURE

A national incident or unique-victim count

457

German ransomware listings dated within the requested 2026 window

WHAT IT DOES NOT MEASURE

Confirmed intrusions or unique people

311

German listings for all of 2025

WHAT IT DOES NOT MEASURE

A matched-period baseline

62 / 55 / 44

Listings under Qilin / SafePay / The Gentlemen labels

WHAT IT DOES NOT MEASURE

Unique operators or their success rates

77

Listings carrying the manufacturing sector label

WHAT IT DOES NOT MEASURE

A national manufacturing incident rate

295 / 77 / 56 / 61

Listings for France / Netherlands / Poland / Austria

WHAT IT DOES NOT MEASURE

Population-adjusted risk or detection effectiveness

249 of 250

Selected domains with exposure observations

WHAT IT DOES NOT MEASURE

Independent legal entities or national prevalence

107 of 249

Observed domains with a current credential offer

WHAT IT DOES NOT MEASURE

Accounts sold or confirmed intrusions

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

Sources: Odin by Brandefense [S1], Ransompedia [S2] and the exposure snapshot [S87]. Country labels and group names describe the listing population. Industry labels do not establish the precise operating activity of every listed organisation.

KEY TAKEAWAYS

01

Use extortion listings to prepare recovery, not to count confirmed intrusions.

02

Validate identity evidence before choosing disruptive containment.

03

Supplier, customer and operational responses need owners alongside technical recovery.

Report map

Twelve chapters, five reader paths. Follow the question that matches your responsibility; evidence limits travel with every conclusion.

Board and executives	Resource the response and test continuity	01 05 11 12
CISO and security leads	Prioritise exposures and dependencies	03 04 05 07 12
SOC and identity teams	Distinguish usable evidence from claims	04 06 07 B
Fraud and customer protection	Prevent secondary harm	05 08 09
Legal and communications	Apply the right clock and wording	05 06 10 12

The evidence labels are **observation**, **claim**, **official confirmation** and **analyst inference**. An observed advertisement remains a claim about its contents. A confirmed incident can leave the actor, data quantity and entry route unresolved.

CHAPTER 02

Germany's digital and threat context

02

THIS CHAPTER ANSWERS

Which operating conditions shape a proportionate German response?

5

evidence populations that must remain separate

2.1 Separate the clocks before comparing the figures 11

2.2 Shared services create shared response dependencies 11

2.3 Politically framed activity requires careful attribution 12

2.4 Regulation is already an operating requirement 12

2.5 What this context changes for leaders 12

CHAPTER 02

Germany's digital and threat context

IN SHORT

German organisations face overlapping identity, supplier and availability risks. National authorities describe these through different reporting systems and observation windows. Their statistics cannot be added to underground listings. Responsibility also spans information security, data protection and sector supervision. Map the service, the legal entity, the supplier and the competent reporting channel before an incident starts.

2.1 Separate the clocks before comparing the figures

The BSI's 2026 annual assessment covers 1 July 2025–30 June 2026. Its publication in November therefore supplies recent analysis of an earlier observation window. It is not a census through this report's cut-off. [S3]

The BKA's May publication reports 1,041 ransomware complaints for 2025. Ransompedia's 457 listings describe a different year, source and unit. Neither is the missing portion of the other. A complaint can remain unpublished, while a listing may never become a confirmed incident. [S4][S2]

The Berlin data-protection authority recorded 1,550 breach notifications during January–September 2026, split between 1,303 non-public and 247 public-sector notifications. These include personal-data incidents beyond malicious intrusions. They are regional notifications, not a national cyberattack count. [S35]

The following distinctions prevent false comparisons.

Population	Unit	Appropriate decision
Underground posts	Published messages and advertisements	Validate claims relevant to your assets
Extortion listings	Public criminal assertions	Test recovery and disclosure readiness
Police complaints	Offences reported under police definitions	Understand reported criminal activity
Data-protection notifications	Reported personal-data breaches	Assess risk to affected people
Confirmed disclosures	Organisation or authority statements	Compare mechanisms and response choices

2.2 Shared services create shared response dependencies

The public cases show several forms of dependency: campus identity, external customer-data services, communications providers and remotely maintained equipment. A single technology relationship can involve several legal entities and different operational owners. Count affected customers separately from incidents at the provider.

Our interpretation is practical. A service inventory should show the business function, identity dependency, data custodian, supplier contact and fallback mode. A contract list alone does not show how an outage reaches a ward, a passenger or a laboratory.

For a university, the necessary question is whether central authentication can be restored safely before registration deadlines. For a manufacturer, it is whether supplier access can be suspended while production remains safe. For a public body, it is whether citizens can obtain essential services while document review continues.

These are planning questions derived from the cases. The report does not claim that every organisation in a sector shares the same architecture or has failed to implement these controls.

2.3 Politically framed activity requires careful attribution

BSI and BfV describe messenger phishing against high-profile political, military, diplomatic and journalistic users. BSI considers state support plausible; its retrospective identifies other countries' attribution separately. This report reports each assessment as the source's position. [S5][S6]

A political target does not establish a political motive. In an October party-account case, the investigating authorities reported no indication of a political background at that stage. The appropriate lesson is to secure externally hosted mail and recovery routes across organisations, regardless of affiliation. [S41]

The report takes no position on elections, political parties, government decisions, Russia–Ukraine, Israel–Gaza or China. Language, a claimed cause and an actor's self-description are not evidence of nationality or state direction. No election outcome is attributed to a cyber incident here.

2.4 Regulation is already an operating requirement

Germany's NIS2 implementation took effect on 6 December 2025. Applicable organisations should therefore establish scope and operational obligations against the law in force. They should not carry over a neighbouring country's legislative timetable. [S30]

Data-protection reporting and financial-sector reporting have their own triggers. A supplier notice may start a controller's awareness assessment, while a service outage may require a separate sector determination. Chapter 10 distinguishes those decisions and identifies completion evidence.

2.5 What this context changes for leaders

Use the same incident record for shared facts, while recording each reporting decision separately. The record should distinguish the time of awareness, the service affected, the people potentially at risk and what remains unverified.

Assign a business owner to each critical dependency. Security can establish whether a credential was used, but the business owner must decide which minimum service remains acceptable. Legal and the data-protection officer determine the applicable reporting route and rationale.

KEY TAKEAWAYS

01

National statistics and underground listings describe different populations and periods.

02

Shared technology can create several affected organisations without several independent intrusions.

03

Establish legal scope and reporting ownership before an event forces the decision.

CHAPTER 03

National exposure: a selected domain portfolio

THIS CHAPTER ANSWERS

Which measured exposure signals require validation by the selected organisations?

107 of 249

observed domains had a credential listed for sale when checked

3.1 Universe card 15
3.2 Current listings and measured signals 16
3.3 Devices and credential records 17
3.4 Account validation and containment 18
3.5 Documents, lookalikes and passive controls 19
3.6 Response ownership 19

CHAPTER 03

National exposure: a selected domain portfolio

IN SHORT

107 of 249 observed domains had a credential listed for sale when checked. The selected portfolio records at least 636,397 device associations and 125,422,358 credential-record associations. These are overlapping observations, not unique people or confirmed intrusions. One of the 250 selected domains has no complete exposure record. Validate current listings, investigate relevant employee-device associations and route other account evidence to the appropriate service owner.

3.1 Universe card

Item	Definition
Selected population	250 purposively selected domains across 10 sector groups; 25 candidates per group
Observed population	249 domains; industry and technology has 24 observations from 25 selected domains
Selection	Service and sector relevance; no revenue ranking or nationally representative sample
Unit	Domain association; legal ownership and independence of the represented organisations remain unvalidated
Snapshot	21–22 November 2026; cumulative device, credential, document and market observations, not a 2026-only incident population
Lookalike period	Previous 30 days; similar naming does not establish abusive use
Mention observations	Previous 365 days ending 18 November 2026; separate from the exposure snapshot
Overlap	Records can recur across sources, domains and people; related services can share an operator
Passive results	No completed hygiene dataset; missing security-control measurements remain unavailable

The portfolio is selected, not representative. Its domain totals do not establish a count of independent legal entities. A missing record remains outside the observed denominator. The exposure snapshot and the report's incident window describe different periods. [S87]

3.2 Current listings and measured signals

The national Atlas headline is 61 out of 100 for the 249 domains with complete exposure observations. This is a portfolio figure, not national prevalence. The table contains signal counts, with no sector or organisation ratings. [S87]

Current credential listings require validation across the selected sectors

Cells show domains with the signal / observed domains in each sector. Current credential offers are shown in coral.

	Current offer	Listing history	Employee devices	Document observations
Public administration	2/25	2/25	10/25	18/25
Regional and local administration	9/25	9/25	19/25	23/25
Banking and finance	13/25	12/25	20/25	21/25
Insurance	10/25	10/25	18/25	21/25
Universities & research	21/25	21/25	24/25	23/25
Industry & technology	11/24	11/24	22/24	23/24
Energy & infrastructure	4/25	4/25	16/25	14/25
Transport and logistics	9/25	9/25	11/25	11/25
Consumer services & communications	22/25	22/25	22/25	23/25
Health & life sciences	6/25	6/25	18/25	15/25

Source: exposure observations for 249 of 250 selected domains, 21-22 November 2026. Cumulative, overlapping domain associations; not independent organisations, unique people or confirmed intrusions [S87].

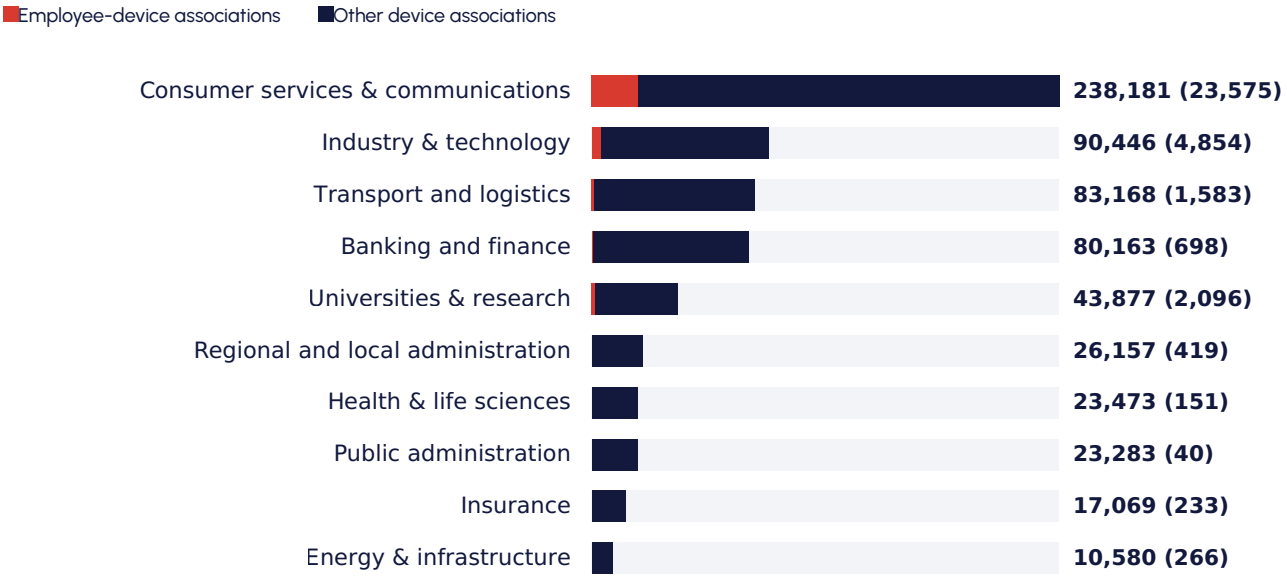
Sector	Observed domains	Current credential listings	Listing history	Employee-device associations present	Document observations present
Public administration	25	2	2	10	18
Regional and local administration	25	9	9	19	23
Banking and finance	25	13	12	20	21
Insurance	25	10	10	18	21

Sector	Observed domains	Current credential listings	Listing history	Employee-device associations present	Document observations present
Universities and research	25	21	21	24	23
Industry and technology	24	11	11	22	23
Energy and infrastructure	25	4	4	16	14
Transport and logistics	25	9	9	11	11
Consumer services and communications	25	22	22	22	23
Health and life sciences	25	6	6	18	15
ALL	249	107	106	180	192

Source: Brandefense Blackhole associations and Atlas exposure observations, snapshot dated 21–22 November 2026 [S87]. Listing counts concern domains with an offer, not accounts sold or confirmed breaches.

3.3 Devices and credential records

Most device associations are outside the employee classification



Source: exposure observations for 249 of 250 selected domains, 21–22 November 2026. Cumulative, overlapping domain associations; not independent organisations, unique people or confirmed intrusions [S87].

Sector	Observed domains	Device associations, at least	Employee-device associations	Credential-record associations
Public administration	25	23,283	40	54,026
Regional and local administration	25	26,157	419	869,088
Banking and finance	25	80,163	698	669,977
Insurance	25	17,069	233	333,920
Universities and research	25	43,877	2,096	939,422
Industry and technology	24	90,446	4,854	3,281,078
Energy and infrastructure	25	10,580	266	158,849
Transport and logistics	25	83,168	1,583	681,446
Consumer services and communications	25	238,181	23,575	118,214,739
Health and life sciences	25	23,473	151	219,813
ALL	249	636,397	33,915	125,422,358

Credential records comprise 48,809,419 breach-database associations, 9,068,279 stealer-log lines and 67,544,660 combolist entries. They do not establish unique people, working passwords or recent access. [S87]

The device population contains 33,915 employee-classified associations and 602,482 other associations. Other associations are not verified customer devices. Shared service domains, historical records and repeated associations can contribute to the totals. Domain ownership must be validated before contacting an affected party. [S87]

Consumer services and communications account for 118,214,739 credential-record associations. Public-facing services can contain customer identities as well as staff accounts. This concentration does not establish equivalent intrusion exposure at every represented organisation. [S87]

3.4 Account validation and containment

Confirm that an account and service belong to your organisation. Check record age, account status and prior remediation. For active privileged accounts, inspect sign-ins, session grants and administrative changes. Revoke sessions and rotate affected credentials when the evidence warrants containment.

A password reset is not the only closure test. Sessions, added authentication methods and linked devices can require separate action. Customer or student accounts need their own response owner. Record whether the evidence was current, historical, unrelated or unresolved.

3.5 Documents, lookalikes and passive controls

The snapshot contains 5,921 document observations and 153,973 lookalike observations. Document association does not establish confidential content or unauthorised access. Similar domain names do not establish impersonation. Check the specific asset, ownership and abusive behaviour before escalation. [S87]

No completed passive hygiene dataset is available. The report publishes no sector hygiene index values or email-control prevalence. A missing result does not establish a missing control. Owners should validate legitimate mail senders, authentication alignment, certificates and service dependencies locally.

3.6 Response ownership

Keep current-account validation, employee endpoint investigation, customer protection and configuration review in separate response queues. Each queue needs an accountable owner, supporting evidence and a closure test. The portfolio's counts cannot determine which specific system requires disruptive containment.

KEY TAKEAWAYS

01

Current listings are account-validation leads, not confirmed intrusions.

02

Device and credential associations overlap and retain their domain-based denominator.

03

Assign response owners while preserving missing records and unvalidated ownership.

CHAPTER 04

Underground activity and claim interpretation

04

THIS CHAPTER ANSWERS

What do the retained advertisements establish about access, documents and identity demand?

6

illustrated claims; no confirmed-intrusion total

4.1 Universe card 21

Monthly observed post population 22

4.2 Recent offers: a tenant account and organisational files 23

4.3 Documents as a fraud resource 25

4.4 A vulnerability assertion and a demand signal 27

4.5 Other retained claims and historical advertisements 28

4.6 Validation questions for common claim types 30

4.7 Publication platforms and languages 31

4.8 Closing-period trade claims 32

CHAPTER 04

Underground activity and claim interpretation

IN SHORT

The retained posts include advertised administrator access, organisational documents, project records and demand for German identity information. Six case cards show those propositions without adopting the sellers' claims. Two illustrated November offers belong to the recent-activity window. The observed post population is not a national incident census. No completed-sale estimate or crime-family ranking is established. Validate relevant claims against owned accounts and data, and distinguish an offer from possession, a repeat advertisement from corroboration, and demand from theft.

4.1 Universe card

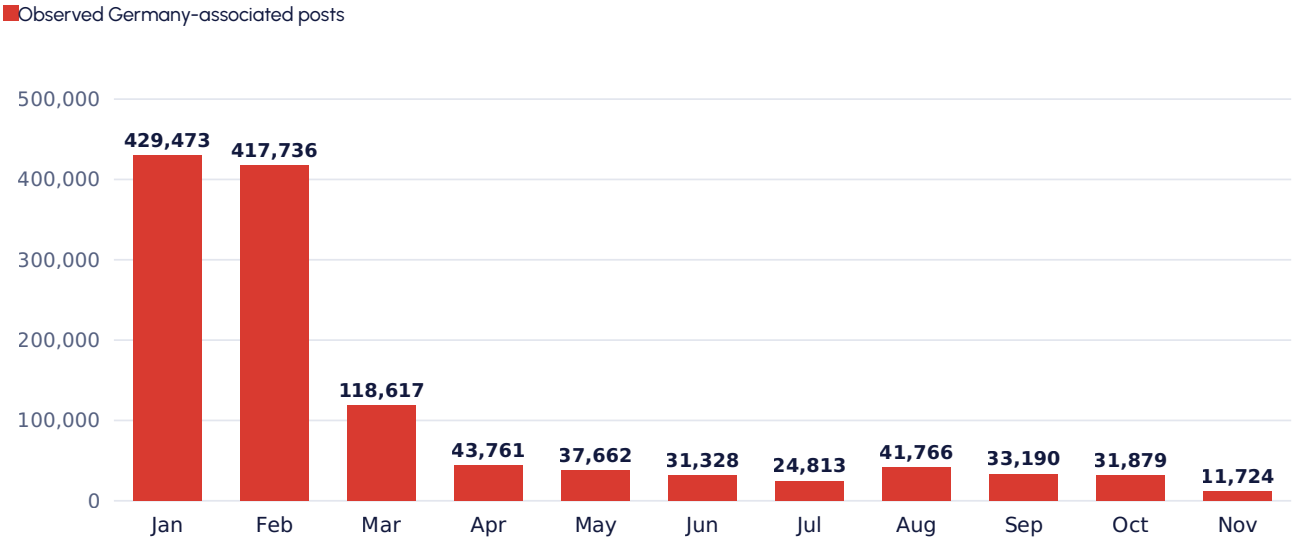
Item	Status
Requested window	1 January–22 November 2026, by post time
Observed Germany-associated post population	1,221,949 posts [S1]; no national incident count
Retained evidence	Forum posts discussing Germany and German-associated assets
Illustrated claims	6 case cards, each paired with a redacted source quotation
Composition	Platform and language observations below; no national crime-family ranking established
Complete forum and market inventory	Unavailable
Ransomware listings	Separate population: 457 German listings [S2]

The observations below establish what was published. They do not establish a complete underground population or verify the assets offered. A German reference can identify a claimed target, a customer group or a sales market. It does not by itself establish the organisation's location or the origin of every record. [S1]

The observed count and the source-content inventory answer different questions. Missing content does not establish absence of activity. Public disclosures and ransomware listings do not substitute for the post population. The six illustrated claims show different decisions; their number is not a prevalence estimate. [S1]

Monthly observed post population

Observed post volume is concentrated early in the year



Source: Brandefense observed Germany-associated posts, 1 January–22 November 2026; cutoff day partial. Posts, retained claims and incidents are separate populations [S1].

Month	Posts	Month	Posts
January	429,473	July	24,813
February	417,736	August	41,766
March	118,617	September	33,190
April	43,761	October	31,879
May	37,662	November through cut-off	11,724
June	31,328	Total	1,221,949

Source: Odin by Brandefense [S1]. January and February account for 69.3% of the observed population. Posts can be advertisements, discussion, repeated offers or international material with a German association. A change in publication volume does not establish a change in successful attacks or national exposure. November remains partial.

The post count does not supply a unique-person denominator, a completed-sale estimate or a verified geographic location for every asset. Its value is visibility context. Use the source-checked claim cards and public disclosures for the specific response questions.

The overall post total and monthly counts agree. The platform breakdown remains seven posts short (§4.7). [S1]

4.2 Recent offers: a tenant account and organisational files

CASE S

S

Advertised administrator access to a banking-related CRM tenant

Claim unverified

Evidence card B01 | 8 Nov 2026 | Forum | Banking-related services

CLAIM	A forum advertisement published on 8 November offers a full administrator account for a cloud CRM tenant associated in the text with a consumer bank. It describes customer contact information. [S1]
WHAT CAN BE ESTABLISHED	The offer and the asserted privilege were present in the retained post. The material does not establish that the account worked, remained active or belonged to a German legal entity. A banking-related tenant claim is not evidence that the cloud platform's own infrastructure was accessed.
ALTERNATIVES	The account could be stale, misrepresented, limited to a supplier tenant or advertised without possession. No successful sale, customer population or bank-wide intrusion is established.
RESPONSE	The identity owner should validate tenant ownership, administrator assignments, recent sign-ins and session grants through authorised records. Containment should follow the validated account evidence, with customer-data review handled separately.

Bottom line

The identity owner should validate tenant ownership, administrator assignments, recent sign-ins and session grants through authorised records. Containment should follow the validated account evidence, with customer-data review handled separately.

CASE T

T

An offer of files from German organisations

Claim unverified

Evidence card B02 | 16 Nov 2026 | Forum | Cross-sector documents

CLAIM	A 16 November post offers data described as originating from German organisations and says proof is available. Other retained posts contain similar advertising during the same period. [S1]

WHAT CAN BE ESTABLISHED	The source asserts possession and a German connection. The report does not verify the file origin, quantity, age or authenticity. Similar lists in later advertisements do not establish another theft or an independent confirming source.
ALTERNATIVES	Advertising can be copied; several bundles can contain overlapping or older records. A document naming a public body, supplier or bank does not establish access to that body's systems.
RESPONSE	Data owners should compare an authorised alert with their own document inventory and prior notifications. Record what is actually matched before assigning an incident date, affected population or reporting obligation.

Bottom line

Data owners should compare an authorised alert with their own document inventory and prior notifications. Record what is actually matched before assigning an incident date, affected population or reporting obligation.

Evidence card B01 — 8 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

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

Held

An advertisement asserts administrator access to a banking-related CRM tenant and describes customer information.

Not established

Usable access, a German legal-entity target, underlying platform intrusion, a completed sale or an affected-customer count.

Evidence card B02 — 16 Nov 2026

[alias withheld] Forum Forum English

ORIGINAL

SELLING Data from German [withheld] Proof available

Held

An advertisement offers files said to come from German organisations.

Not established

File authenticity, origin, freshness, a completed sale or a new intrusion each time similar advertising appears.

These November observations are publication events. They are not dated confirmations of two new intrusions. Neither is linked here to the university, political-party or bank disclosures in other chapters. The report has no concrete evidence of a shared operator or transaction chain. [S1]

4.3 Documents as a fraud resource

CASE U

U

Project contacts and budget records offered for sale

Evidence card B03 | 2 Feb 2026 | Forum | Project services

Claim unverified

CLAIM	On 2 February, a seller describes a database of regional project contacts and budget records from a German portal. [S1]
WHAT CAN BE ESTABLISHED	The advertisement combines contact and project-finance categories. The claimed record count and domestic origin are not independently verified. No transfer from the portal or completed transaction is established.
ALTERNATIVES	Contact material may be older, public, copied or combined from several sources. A plausible field list does not establish a current vulnerability or complete customer database.
RESPONSE	Procurement and fraud teams should authenticate changes to project payments through a known channel. A relevant alert should be checked with the data custodian, including whether the same material was already disclosed.

Bottom line

Procurement and fraud teams should authenticate changes to project payments through a known channel. A relevant alert should be checked with the data custodian, including whether the same material was already disclosed.

CASE V

V

A claimed release of administrative and financial files

Evidence card B04 | 6 Oct 2026 | Forum | Cross-sector documents

Claim unverified

CLAIM	A 6 October post announces a data release from an organisation it describes as located in Germany. It lists administrative and financial data, corporate email material and internal documents. [S1]
WHAT CAN BE ESTABLISHED	The release assertion and document categories were published. The underlying files, asserted size, intrusion route and freshness are not verified here.
ALTERNATIVES	A release announcement can concern an old export, a supplier copy or repackaged material. It does not establish that the organisation's current systems remained accessible.

RESPONSE

The incident owner should establish document ownership and age before choosing containment. Fraud teams should monitor for plausible invoice, supplier and executive impersonation using those document categories.

Bottom line

The incident owner should establish document ownership and age before choosing containment. Fraud teams should monitor for plausible invoice, supplier and executive impersonation using those document categories.

Evidence card B03 — 2 Feb 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

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

Held
A seller describes project-contact and budget records associated with a German portal.

Not established
A verified record count, portal intrusion, current flaw, authentic files or a completed sale.

Evidence card B04 — 6 Oct 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

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

Held
A post asserts release of administrative, financial and corporate email material from an organisation described as German.

Not established
Authentic files, a new intrusion, continued access, verified volume or a completed transaction.

The analytical relationship is between useful context and a later deceptive request. Project budgets or internal correspondence can make a fraudulent message more credible. These posts do not establish that such a message was actually sent. The confirmed follow-on warnings in Chapter 5 provide separate evidence of that behaviour; they are not matches to these advertisements.

4.4 A vulnerability assertion and a demand signal

W

CASE W

Automotive documents advertised with an access-control claim

Claim unverified

Evidence card B05 | 17 Feb 2026 | Forum | Automotive

CLAIM	A 17 February advertisement offers documents, including personal information, from a major automotive group described as German. It attributes acquisition to an insecure direct object reference, or IDOR, and separately offers the asserted exploit for sale. A second advertisement repeats the claim later that day. [S1]
WHAT CAN BE ESTABLISHED	The seller makes a document and vulnerability claim. The post does not verify a live flaw, exploitation, file possession or a new automotive intrusion. The repeat advertisement is not another incident.
ALTERNATIVES	The route may be guessed, copied or inaccurately described; documents can originate from a contractor or historical export. The seller's terminology is not an independent technical assessment.
RESPONSE	An application owner receiving a relevant alert should review object-level authorisation and access logs in the affected owned service. Use an authorised test and preserve evidence of the actual result, rather than treating the advertisement as a vulnerability finding.

Bottom line

An application owner receiving a relevant alert should review object-level authorisation and access logs in the affected owned service. Use an authorised test and preserve evidence of the actual result, rather than treating the advertisement as a vulnerability finding.

X

CASE X

Demand for German identity and home-address information

Claim unverified

Evidence card B06 | 5 Jan 2026 | Forum | Identity data

CLAIM	A 5 January post asks for information about German people, emphasising physical home addresses and requesting other identity details if available. [S1]

WHAT CAN BE ESTABLISHED	This is a request to obtain information. It does not establish that the author held a database, acquired records, completed a purchase or selected a particular victim.
ALTERNATIVES	The request may never have been fulfilled. It gives no supported number of people, source organisation or collection date.
RESPONSE	Treat a relevant identity alert as a data-protection and customer-safety question. Examine actual information disclosed and credible misuse, while avoiding a national affected-person count derived from a buyer's request.

Bottom line

Treat a relevant identity alert as a data-protection and customer-safety question. Examine actual information disclosed and credible misuse, while avoiding a national affected-person count derived from a buyer's request.

Evidence card B05 — 17 Feb 2026

[alias withheld] Forum Forum English

ORIGINAL

[victim withheld] Documents including [withheld] IDOR

Held
A seller advertises automotive documents and separately an IDOR exploit.

Not established
A real vulnerability, exploitation, possession of the documents, a sale or a second incident from the repeated advertisement.

Evidence card B06 — 5 Jan 2026

[alias withheld] Forum Forum English

ORIGINAL

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

Held
A buyer requests German identity information and emphasises real home addresses.

Not established
Possession, acquisition, a completed purchase, a specific affected person or an underlying intrusion.

The six examples distinguish advertised access, offered records, an asserted release, an asserted technical route and demand. These categories require different evidence. They should not be combined into a six-intrusion total. [S1]

4.5 Other retained claims and historical advertisements

The following additional observations widen the claim register without increasing the confirmed-incident population. Dates are publication dates. None validates possession, a completed transaction or the actor's asserted technical route. [S1]

Post date	Role and assertion	Boundary and response
1 February	Germany-labelled website database offered [S1]	The country label does not verify origin, age or an intrusion; the data owner should check any relevant alert.
31 March	German-language forum-account dataset shared [S1]	Language is not residence; inconsistent scale descriptions are omitted. Validate account ownership and prior remediation.
6 June	German business/contact dataset advertised as 2025 material [S1]	Older directory or public-source material is plausible; publication in 2026 does not establish a new intrusion.
17 June	German consumer-contact dataset advertised as 2025 material [S1]	Historical trade claim, without a verified source organisation or breach date; assess actual data categories.
12 August	Telephony service advertises a German-number capability restriction [S1]	Capability claim only, with no observed victim or successful impersonation; use independent call authentication.
22 August	German mobile-number and birth-date dataset claimed [S1]	Origin, age and possession are unverified; do not assign a telecom-provider intrusion.
7 September	A German retail/services group is named in a claimed customer-data event [S1]	The post calls it a 2026 event; no official confirmation or file authenticity is established.
3 October	Financial-user records described as German offered for sale [S1]	Customer fields do not establish bank-system access; provenance and claimed scale remain unverified.
7 October	German automotive client, document and financial data release asserted [S1]	No files or current access verified; compare a relevant alert against owned records before containment.
1 November	German manufacturer appears in a forum data-leak listing [S1]	Sparse claim, without verified theft date or mechanism; do not count another intrusion from a forum repost.
5 November	International travel/reservation dataset offered, with Germany among customer countries [S1]	The source organisation and a German organisation segment are unverified; no German provider intrusion inferred.
8 November	Research/recruitment cloud-tenant administrator access advertised [S1]	Domestic ownership, customer geography and usable access unverified; review only a validated owned tenant.

Post date	Role and assertion	Boundary and response
10 November	German forum/hosting-platform administrator access alleged [S1]	Customer and order categories are claimed; no active access or underlying platform intrusion is validated.
17 November	Multi-country banking leads include a German segment [S1]	A lead list does not establish a bank intrusion; freshness and sale assertions remain unverified.

These advertisements can concern different offers or overlapping older material. No shared operator, separate underlying intrusion for every row, or match to a public disclosure is established. The caller-ID and financial-contact rows support trusted verification routes, not claims about completed German fraud.

4.6 Validation questions for common claim types

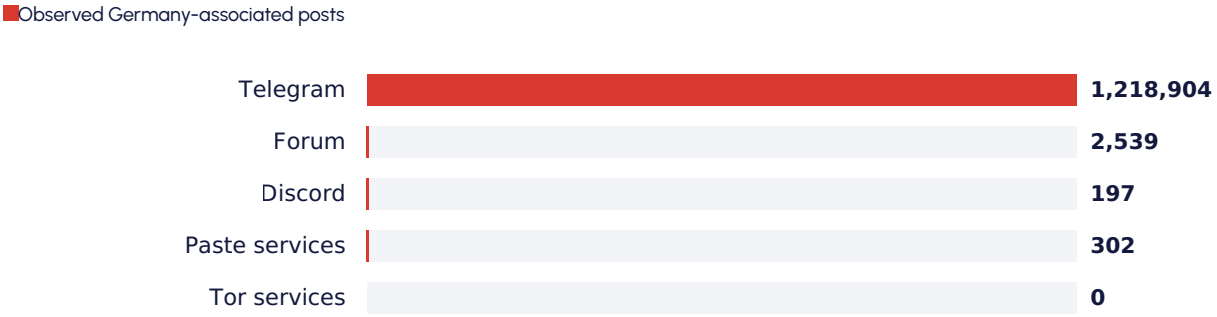
Claim type	What needs validation	What not to infer
Customer database	Origin, categories, age and ownership	Every claimed row represents a different person
Employee access	Account ownership, status and privilege	Domain association establishes employment
Remote access	A currently usable access path	An old screenshot establishes continuing access
Credential file	Freshness and previous remediation	Every line is valid or unique
Infrastructure inventory	Authenticity and current operational relevance	A document establishes control of the infrastructure
DDoS claim	Service state, duration and affected function	A momentary failed check establishes national disruption

The organisation's incident record should preserve the proposition being tested, the source date, the owned asset or data category and the result. Keep alternatives visible. Assign the next action to an owner: identity for an active account, data protection for personal records, and the service operator for disruption.

This edition publishes no national asking-price median and estimates no completed sales. The quoted excerpts preserve the original language, with identifying material removed. Their translations convey the claim without adding technical or attribution certainty. [S1]

4.7 Publication platforms and languages

Telegram has the largest observed platform count



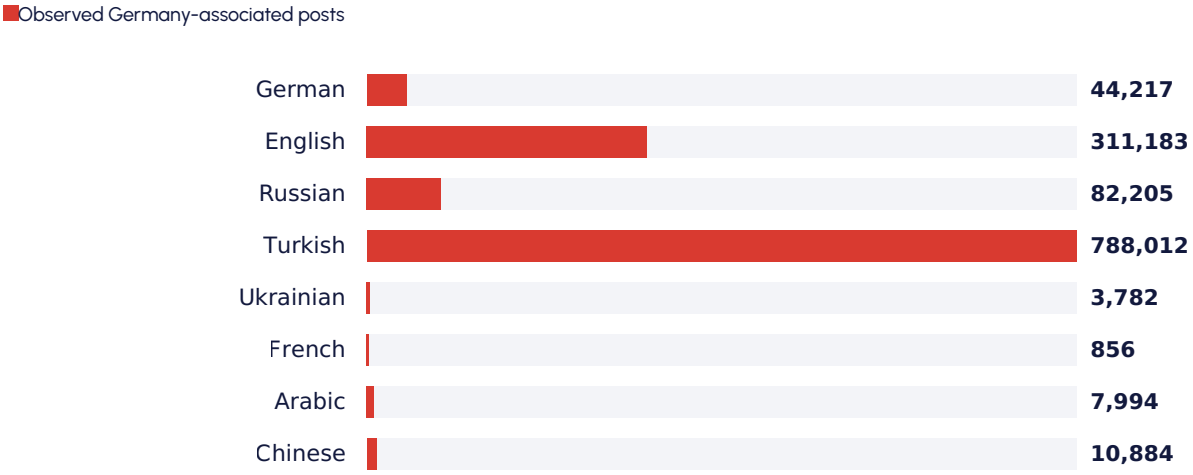
Platform counts total 1,221,942; seven of the 1,221,949 observed posts remain unassigned in this breakdown. Source: Brandefense observed Germany-associated posts, 1 January–22 November 2026; cutoff day partial. Posts, retained claims and incidents are separate populations [S1].

Platform label	Observed posts
Telegram	1,218,904
Forum	2,539
Discord	197
Paste services	302
Tor services	0

The platform rows total 1,221,942 posts, seven fewer than the overall post total. The available aggregates do not establish the platform assignment of that difference. These rows are not a fully reconciled breakdown. [S1]

These are observed Germany-associated posts in the requested window. The platform labels describe publication venues, not verified attacks, successful transactions or domestic victim populations. They are not a complete catalogue of every underground venue. [S1]

Language associations do not establish nationality



Language labels can overlap and do not establish nationality. Source: Brandefense observed Germany-associated posts, 1 January–22 November 2026; cutoff day partial. Posts, retained claims and incidents are separate populations [S1].

Language association	Observed posts
German	44,217
English	311,183
Russian	82,205
Turkish	788,012
Ukrainian	3,782
French	856
Arabic	7,994
Chinese	10,884

Language associations can overlap. They do not establish the nationality or residence of authors, customers or victims. Publication volume does not establish a national crime-family ranking or the frequency of successful intrusions. [S1]

4.8 Closing-period trade claims

The hosting offer disclaims live access. A 22 November offer advertises material associated with 16 websites and 10 small-business clients of a German hosting service. The seller expressly disclaims live SSH or root access. Possession, provenance, acquisition date and a completed sale remain unverified. Validate any relevant owned files and accounts before treating the offer as evidence of current access. [S1]

The credential posts repeat an advertising claim. Two 22 November posts advertise the same claimed 23,000-entry Germany credential list with matching cloud-access promotion. Their wording does not establish that the underlying records are identical, valid, current or independently stolen. Do not add the advertised counts or count the posts as separate breaches. [S1]

A 12 November offer advertises German investment and recovery leads. An 18 November offer labels German phone-contact material as 2023 data. Neither establishes the source breach, present accuracy or a new 2026 intrusion. Customer-protection teams should authenticate recovery contacts and payment requests through independent channels. [S1]

KEY TAKEAWAYS

01

Six illustrated claims show different validation tasks, not six confirmed intrusions.

02

Repeated advertising is not independent confirmation.

03

Route access, document and identity claims to the owner who can validate the specific proposition.

CHAPTER 05

Confirmed incidents and targeting by sector

05

THIS CHAPTER ANSWERS

Which disclosures support a concrete defensive response, and which outcomes remain unresolved?

2

separate November notices at one university

5.1 How to read the cases 35
5.2 Public administration: data review after service containment 35
5.3 Education: identity exposure and data access are different events 37
5.4 Healthcare: protect patients during the secondary phase 40
5.5 Supplier-held records and customer services 42
5.6 Transport and communications 43
5.7 Recent activity: 8–22 November 43
5.8 Other confirmed closing-period cases 45
5.9 Earlier incidents and important exclusions 49
5.10 Further priority-organisation findings 51
5.11 What the cases support 51

CHAPTER 05

Confirmed incidents and targeting by sector

IN SHORT

Public disclosures describe different failures: stolen credentials, copied administrative data, supplier-held customer records and interrupted services. The cases below retain each source's limits. A shared sector or nearby date does not establish a common campaign. Start with the affected function and the confirmed access, then choose containment, customer support and continuity measures that fit that evidence.

5.1 How to read the cases

A confirmed security incident does not confirm every subsequent leak claim. We record the organisation's or authority's statement, identify the remaining uncertainty, and give a proportionate response. A case can include several phases of one incident, such as intrusion followed by patient extortion.

Named cases require official confirmation and wider reporting. Other cases use broad roles. Source titles and article addresses that would restore a withheld name are shortened under the publication policy. The private register retains the exact supporting passage.

This chapter is a set of documented cases, not an exhaustive national count. Discovery, disclosure, publication and restoration dates are kept distinct. Follow-up fraud and a new intrusion are not automatically counted as two separate compromises.

5.2 Public administration: data review after service containment

A

CASE A

Berlin administration data loss

Public administration

Official statement; limits retained

CONFIRMED	The Berlin data-protection authority identifies copying from administration networks between 7 and 12 August. It says employee information and possibly residents' information were published. The Senate's information page separately describes the continuing review. [S9][S10]
BOUNDARY	An archive's public appearance does not establish that every file is authentic, that every person's data was published, or that access remains active. The reported incident must remain separate from any attacker's quantity or attribution.

INTERPRETATION	Unstructured shared folders make scoping a distinct response task. Restoring a system does not identify every person whose correspondence may have been copied.
RESPONSE	Inventory the affected document stores, record which categories can be confirmed, and maintain a contact route for people awaiting an individual assessment.

Bottom line

Inventory the affected document stores, record which categories can be confirmed, and maintain a contact route for people awaiting an individual assessment.

The case supports a document-governance decision beyond network recovery. An organisation should know which shared stores contain identity documents, contractual records or sensitive operational plans. The data owner should be able to identify retention rules and who can approve access.

For communications, use a staged notice. Distinguish the known event from the still-developing assessment of individual impact. Give the next update time, the responsible contact route and advice matched to the confirmed categories. Do not promise that publication equals misuse, or that restoration eliminates misuse risk.

B

CASE B

A state property agency's unresolved November incident

Public administration

Official statement; limits retained

CONFIRMED	A state ministry reported an IT security incident on 19 November. Telephone availability was restricted and email was unavailable. The cause, extent and possible data outflow remained under investigation. [S22]
BOUNDARY	The statement does not establish ransomware, copied data or an actor. A communications restriction is the confirmed operational consequence.
RESPONSE	Prepare alternate contact arrangements and preserve the investigation timeline. Update the public description when evidence establishes a more specific outcome.

Bottom line

Prepare alternate contact arrangements and preserve the investigation timeline. Update the public description when evidence establishes a more specific outcome.

This is a useful limit case. A public statement can responsibly confirm an incident before its mechanism is known. Defenders should not wait for an actor label to activate a fallback channel; analysts should not supply a label that the authority has not established.

5.3 Education: identity exposure and data access are different events

CASE C

C

TUM campus credentials

Education

Official statement; limits retained

CONFIRMED	TUM reported stolen central-login passwords, including an administrator's credential, and access against TUMonline. Its 9 November update restored the service with password changes and two-factor authentication required. [S11]
BOUNDARY	The disclosure does not establish a verified theft total for the university's entire population. The wider reporting supports naming the organisation, not expanding the official impact statement. [S12]
INTERPRETATION	An administrator credential can turn a portal event into a wider identity response. The response must address privileges and sessions alongside the original portal.
RESPONSE	Validate the affected accounts, revoke relevant sessions and review administrative changes before restoring normal access.

Bottom line

Validate the affected accounts, revoke relevant sessions and review administrative changes before restoring normal access.

The recovery decision should be owned jointly by identity, application and service teams. Restoring the application's availability is only one milestone. Safe reopening also requires checking privileged grants, recovery methods and the audit coverage needed to investigate subsequent activity.

Use a synthetic recovery exercise to test the sequence. The exercise should demonstrate that a locked account can recover through a trusted route, that unauthorised sessions lose access, and that legitimate users can reach critical functions. Record exceptions rather than treating all users as identical.

CASE D

D Universität Tübingen employee records

Education

Official statement; limits retained

CONFIRMED	On 10 November the university disclosed about 3,900 employee records, including identifying, contact and workplace information. It said students and passwords were not affected. It described a combination of recommended settings that exposed internal functions. [S13][S15]
BOUNDARY	The disclosure does not identify a common operator with other university cases. Knowing a username was part of the described access condition; it does not make the username itself a secret.
INTERPRETATION	Configuration combinations can create exposure even where each individual setting appears routine. Review the effective permissions of the whole service.
RESPONSE	Test authorisation at internal functions using an approved account, review supplier configuration guidance and warn affected employees about contextual phishing.

Bottom line

Test authorisation at internal functions using an approved account, review supplier configuration guidance and warn affected employees about contextual phishing.

CASE E

E Universität Tübingen webmail notice

Education

Official statement; limits retained

CONFIRMED	A separate 11 November notice described an overnight webmail attack and precautionary account restrictions. The university warned that passwords entered during the stated period might have been captured and initiated resets. [S14][S48]
BOUNDARY	This report does not merge that notice with the employee-record event. A common institution and nearby date do not establish the same entry route, dataset or perpetrator.
RESPONSE	Match reset scope to the service and time interval described. Review linked services and sessions for affected accounts without asserting that every mailbox was read.

Bottom line

Match reset scope to the service and time interval described. Review linked services and sessions for affected accounts without asserting that every mailbox was read.

The two Tübingen cases illustrate why incident units matter. One notice concerns employee records and explicitly excludes passwords. The other concerns possible password capture in a particular mail-service interval. A combined headline would erase information needed to choose the right response.

CASE F

F

LMU registration data

Education

Official statement; limits retained

CONFIRMED	LMU's 19 September disclosure describes unauthorised access to registration records and says it must assume retrieval. The source lists identity, contact and some financial or administrative categories, depending on the individual record. [S49]
BOUNDARY	The notice does not establish a public leak or a verified national student population. It distinguishes the affected registration material from examination and academic-performance information.
RESPONSE	Identify the affected data categories, support affected people and test authorisation on registration workflows before reopening them.

Bottom line

Identify the affected data categories, support affected people and test authorisation on registration workflows before reopening them.

Across these education cases, the evidence supports several controls rather than one assumed initial-access pattern. Identity recovery, administrative privilege, application authorisation and personal-data scoping each need an owner. The report does not infer that all cases began with phishing or a shared software vulnerability.

5.4 Healthcare: protect patients during the secondary phase

CASE G

G

Hospital intrusion followed by patient extortion

Healthcare

Official statement; limits retained

CONFIRMED	A hospital reported communications failure in February and a move to manual ward procedures. In March, the state data-protection authority and police warned that stolen patient information was being used in direct extortion messages. [S16]
BOUNDARY	The later messages are a follow-on phase, not evidence of a second hospital intrusion. Neither a patient total nor a named operator is established here.
INTERPRETATION	Sensitive information can reach the individual as an extortion demand after the institution begins recovery. The institution's response should include patient-facing support.
RESPONSE	Prepare scripts for recipients of extortion messages, preserve reports safely and explain that a payment does not establish deletion.

Bottom line

Prepare scripts for recipients of extortion messages, preserve reports safely and explain that a payment does not establish deletion.

The lesson is organisational. A service desk cannot investigate a medical-data incident by asking patients to send sensitive records to an unverified address. It needs an approved route, clear triage questions and a way to connect urgent concerns to the incident team.

Clinical continuity and personal-data response should be exercised together. Manual procedures need staffing, reliable contact details and a safe way to reconcile records later. The organisation should specify who can resume the normal workflow and what evidence supports that decision.

CASE H

H

Fresenius Medical Care's limited-system disclosure

Medical technology

Official statement; limits retained

CONFIRMED	The company reported unauthorised access to a limited number of internal systems on 22 September. It said medical devices, patient care, manufacturing and business continuity were unaffected. [S19][S20]

BOUNDARY	This establishes the company's stated incident scope. It does not confirm an extortion group's claimed dataset, a German patient count or disruption of clinical devices.
RESPONSE	Separate internal-system investigation from clinical assurance. Validate service impact using the relevant operational owners rather than a criminal listing alone.

Bottom line

Separate internal-system investigation from clinical assurance. Validate service impact using the relevant operational owners rather than a criminal listing alone.

These hospital and medical-technology disclosures should not be collapsed into a general claim that healthcare systems were unavailable. One reports a manual operational fallback and later patient extortion. The other expressly states that medical care and production were unaffected.

CASE I

Pharmaceutical cooling controls

Industrial cooling

Official statement; limits retained

CONFIRMED	LKA NRW's 18 November warning cites BSI reporting of attacks on a German pharmaceutical wholesaler's cooling systems. It separately discusses a French incident and states that direct effects on German blood banks had not been established. [S21]
BOUNDARY	No common actor or common technical cause is established between the reported cases. The warning does not justify claiming German blood-product loss.
RESPONSE	Validate remote-maintenance access, independent temperature alarms and contingency storage. A backup of IT data does not maintain physical temperature conditions.

Bottom line

Validate remote-maintenance access, independent temperature alarms and contingency storage. A backup of IT data does not maintain physical temperature conditions.

Chapter 6 develops the operational response. The immediate decision is to identify who receives an alarm, who can isolate remote access and who can protect stock while the system is investigated.

5.5 Supplier-held records and customer services

J

CASE J

Photo-service supplier warning

Supplier services

Official statement; limits retained

CONFIRMED	A state data-protection authority warned in May about a supplier attack affecting photo studios. Children's photographs and personal information were potentially involved. [S17]
BOUNDARY	Potential exposure is not a verified count of affected children. A common supplier does not establish a separate intrusion at every studio.
RESPONSE	Identify each controller's affected records and coordinate an accessible notice route. Confirm what deletion means across the supplier relationship before promising removal.

Bottom line

Identify each controller's affected records and coordinate an accessible notice route. Confirm what deletion means across the supplier relationship before promising removal.

K

CASE K

Hotel-software data and fraudulent messages

Hospitality

Official statement; limits retained

CONFIRMED	A July state-authority notice described another wave of hotel notifications after a software-supplier attack. Reservation and customer information were involved; the notice reported follow-up fraudulent messages. [S18]
BOUNDARY	The statement did not establish bank or payment-data loss at that stage. A convincing payment demand can exploit reservation context without containing stolen card data.
RESPONSE	Brief reservations staff, publish the real payment process and provide an independent way for guests to verify a request.

Bottom line

Brief reservations staff, publish the real payment process and provide an independent way for guests to verify a request.

The common response is to preserve useful context without disclosing additional information to the sender. A hotel should not authenticate a caller merely because the caller knows a booking date. A studio should not assume a record was erased everywhere because a user interface no longer displays it.

Contracts should identify how a provider will supply an affected-data list, preserve relevant logs and assist the controller's notification decision. The completion evidence is a rehearsed exchange of information, not a contractual promise whose practical timing has never been tested.

5.6 Transport and communications

CASE L

L

Deutsche Bahn's February booking disruption

Transport

Official statement; limits retained

CONFIRMED	Deutsche Bahn's official reporting describes February overload of booking and information systems. Contemporary reporting describes attack waves on 17–18 February. [S7][S8]
BOUNDARY	This is an availability case. It does not establish theft of passenger records, access to train-control systems or an official perpetrator attribution.
RESPONSE	Test customer information and ticket-access fallbacks alongside mitigation. Monitor the customer's completed task, rather than treating a responding homepage as full service restoration.

Bottom line

Test customer information and ticket-access fallbacks alongside mitigation. Monitor the customer's completed task, rather than treating a responding homepage as full service restoration.

The incident illustrates a useful continuity measure: whether a passenger can retrieve a ticket or obtain reliable information during degradation. A network team's traffic chart is necessary evidence for mitigation, but it is not the same as a restored booking journey.

For communications services, distinguish an upstream dependency from an intrusion into every downstream organisation. Confirm which services are unavailable, provide a fallback contact route and record the dependency when assessing sector reporting duties.

5.7 Recent activity: 8–22 November

The source records 7,111 Germany-associated posts dated 8–22 November. That is observed publication volume, not a count of new incidents or verified German victims. [S1]

The closing fortnight includes new incidents, updates to earlier incidents and enforcement announcements. The table separates them so that publication dates do not create an artificial late-year surge.

Date	Item	Evidence status	Immediate decision
8–17 November	Reservation-provider access and rebuilt-service restart	One supplier incident, with fraudulent guest messages [S58]	Coordinate guest warnings with technical recovery
8–20 November	Utility IT and customer-service disruption	Supply maintained; updates to one incident [S59]	Separate billing fallback from energy operation
8 November	Banking-related CRM access offer	Unverified administrator-tenant advertisement [S1]	Validate account and tenant ownership
9 November	Campus system recovery update	Update to TUM's 6 November disclosure [S11]	Validate reopening and account recovery
9 November	Fake-shop charge announced	Alleged conduct from 2023–early 2025 [S42]	Treat it as enforcement context
10 November	University employee records	Official data-access disclosure [S13]	Scope categories and warn staff
11 November	University webmail	Separate password-risk notice [S14]	Match resets to stated exposure
12 November	Malware disruption announced	Police action on 9–11 November [S23]	Act on relevant infection notifications
12 November	Social-service communications restrictions	Municipal confirmation; in-person work continues [S55]	Publish working contact routes
12 November	Defence supplier statement	Incident acknowledged; further details unresolved [S50] [S86]	Verify supplier updates through a trusted route
13 November	Political-party personal-data notice	September–October activity; recent notification [S56]	Scope records without assigning political motive
13–20 November	Hosting-provider access and scope updates	Later higher-risk instance notice [S54]	Make a tenant-specific determination
15–18 November	County hospital incident and reopening	One incident, several recovery milestones [S53]	Coordinate clinical diversion and reopening
16 November	German-organisation file offer	Unverified document advertisement [S1]	Validate origin and age through owned records
17 November	Bank response to document reporting	Statement disputes a current intrusion [S39][S40]	Preserve the distinction from historical disclosure
17 November	Municipal administration	Police confirm unauthorised access; theft still checked [S51]	Preserve logs and provide alternate contacts

Date	Item	Evidence status	Immediate decision
17–20 November	Local communications attack and recovery	Provider confirmation and service update [S52]	Test customer support and dependent services
18 November	Industrial cooling warning	Official operational-security warning [S21]	Test independent monitoring and maintenance access
19 November	State property agency	Security incident confirmed, possible outflow unresolved [S22]	Activate communications fallback
19–20 November	BSI annual assessment	New publication covering an earlier window [S3]	Update planning without re-dating the events
22 November	Hosting data-lot offer	Unverified data offer; seller disclaims live access [S1]	Validate owned files and accounts before containment
22 November	Matching credential-list advertisements	Two posts repeat an unverified advertised claim [S1]	Check account ownership, age and prior remediation

The table is not a complete list of fortnight incidents. Some late discoveries remain unresolved in the coverage register. This report makes no claim that missing recent posts or notices imply a reduction in threat activity.

5.8 Other confirmed closing-period cases

M

CASE M

Municipal access under investigation

Public administration

Official statement; limits retained

CONFIRMED	A 17 November police notice described unauthorised access to part of a municipal administration's IT, disruption and disconnection of systems. Investigators were checking possible data theft. [S51]
BOUNDARY	A message requesting contact does not establish encryption, a specific ransom demand or copied data.
RESPONSE	Preserve logs and the message, arrange alternative citizen contacts and update the scope as evidence develops.

Bottom line

Preserve logs and the message, arrange alternative citizen contacts and update the scope as evidence develops.

CASE N

N ■ A local communications provider's outage

Communications

Official statement; limits retained

CONFIRMED	A provider attributed telephone and internet disruption overnight on 17–18 November to a cyberattack. Its 20 November update reported stable services while customer-service telephone availability was being restored. [S52]
BOUNDARY	The notice did not establish data theft or a named actor. Restoration of network service and restoration of support channels are distinct milestones.
RESPONSE	Test alternate customer contact routes and track restoration by function, including dependent organisations.

Bottom line

Test alternate customer contact routes and track restoration by function, including dependent organisations.

CASE O

O ■ A county hospital's emergency-service interruption

Healthcare

Official statement; limits retained

CONFIRMED	A county reported an attack detected on 15 November and temporary withdrawal of emergency admission. Later notices reported emergency admission restored on 17 November and functioning operating theatres on 18 November. [S53]
BOUNDARY	These are phases of one incident. The notices do not establish a named actor or data theft.
RESPONSE	Rehearse diversion, manual operation and safe reopening with clinical leaders. Track postponed work after the technical recovery milestone.

Bottom line

Rehearse diversion, manual operation and safe reopening with clinical leaders. Track postponed work after the technical recovery milestone.

CASE P

P

Hosting-provider infrastructure access

Hosting

Official statement; limits retained

CONFIRMED	A hosting provider described unauthorised infrastructure access on 13–14 November, revoked access and rotated credentials. Its 20 November update identified a small higher-risk instance population for direct contact. [S54]
BOUNDARY	Earlier statements of no indication of personal-data leakage do not establish no customer impact. The later update does not establish universal customer access either.
RESPONSE	Follow trusted provider guidance, review your own access evidence and record a tenant-specific determination.

Bottom line

Follow trusted provider guidance, review your own access evidence and record a tenant-specific determination.

CASE Q

Q

A social-service provider's restricted communications

Social services

Official statement; limits retained

CONFIRMED	A municipal notice on 12 November described an attack affecting part of a social-service provider's IT and restricted email. In-person services continued, with telephone or on-site contact available. [S55]
BOUNDARY	No data outflow was known at that point. That is a time-bounded assessment, not proof of absence.
RESPONSE	Publish the working contact routes and preserve continuity for people who depend on the service.

Bottom line

Publish the working contact routes and preserve continuity for people who depend on the service.

CASE R

R

A political party's historical incident notice

Political organisation

Official statement; limits retained

CONFIRMED	AfD's 13 November notification described unauthorised access to mailboxes in September and further systems in October. It reported copied personal data and continuing investigation. Earlier press reporting also covered the incident. [S56][S57]
BOUNDARY	The notice date does not make the underlying activity a new November intrusion. No verified affected-person total or actor attribution is established here.
RESPONSE	Separate externally hosted mail from party administration systems, scope the affected records and preserve notification decisions. Apply the same privacy and response standards regardless of affiliation.

Bottom line

Separate externally hosted mail from party administration systems, scope the affected records and preserve notification decisions. Apply the same privacy and response standards regardless of affiliation.

No judgement about the party's policies, government decisions or election outcomes follows from this incident. The case is included for its documented security and personal-data consequences.

CASE Y

Y

Reservation-provider access followed by fraudulent messages

Hospitality supplier

Official statement; limits retained

CONFIRMED	A reservation software provider says an attacker entered through a customer account on 8 November and retrieved guest data on 8–9 November. It reports subsequent fraudulent emails seeking payments or card information. It took the application offline on 13 November because deeper access could not be excluded and restarted a rebuilt service on 17 November. [S58]
BOUNDARY	The exact data volume remained under investigation. These are phases of one supplier incident; downstream restaurant warnings are not separate confirmed restaurant intrusions. No common actor with earlier hotel-software incidents is established.
RESPONSE	Obtain a scoped provider assessment, warn guests through a trusted channel and authenticate payment requests independently. Service restoration does not close the customer-fraud response.

Bottom line

Obtain a scoped provider assessment, warn guests through a trusted channel and authenticate payment requests independently. Service restoration does not close the customer-fraud response.

CASE Z

Z

Utility IT disruption with energy supply maintained

Energy services

Official statement; limits retained

CONFIRMED	A municipal utility says it detected an attack on 8 November and isolated affected systems. Customer portals, email, meter appointments and several payment or collection processes were affected. Updates through 20 November said electricity, gas and district-heating supply remained uninterrupted. [S59]
BOUNDARY	The provider had no indication of personal-data outflow at the stated time. That is a qualified assessment. Neither an energy-supply outage, a specific actor nor an entry route is established.
RESPONSE	Test customer-service and billing fallback separately from energy operation. Record delayed payments and appointments so that restoration includes the accumulated customer work.

Bottom line

Test customer-service and billing fallback separately from energy operation. Record delayed payments and appointments so that restoration includes the accumulated customer work.

5.9 Earlier incidents and important exclusions

The record extends beyond the closing fortnight. The following notices add confirmed events and explicit exclusions. They preserve the distinction between an event, an update and a precautionary shutdown.

Period	Role and supported finding	Limit and response
21 January; 19 February notice	Police and prosecutors confirm an attack on a state cultural collection's IT [S60]	Route, actor and data quantity were not disclosed; preserve the investigation boundary
January; restored 23 January	A professional chamber removed website malware and warned that dashboard passwords might have been intercepted [S61]	Possible interception is not confirmed for every user; no pharmacy-care system impact is established

Period	Role and supported finding	Limit and response
16–24 April	A municipality confirmed ransomware and system isolation, followed by restored registry, civil-status and payment functions [S62]	The updates concern one incident; personal-data theft remained unresolved
April event; 22 May notice	A university hospital confirms that patient information was stolen at its external billing provider, while its own systems and patient care were unaffected [S75]	Initial disclosure only; later scope remains unresolved here, so no final patient total is published
Learned 10 June; 25 June notice	A research institute confirms access to file servers and stored files, followed by disconnection and resets [S65]	Which files were actually taken remained unresolved; no actor is established from its research subject
Detected 19 June; updated 31 July	A state museum confirms unlawful copying involving staff, partner and visitor information [S71]	No final affected-person count or actor; scope data categories and affected-person support
28 June–16 July	A municipal utility confirms disruption to portals, communications and payments, while maintaining supply [S63]	Its later assessment excluded loss of current customer data but left older customer-related data unresolved; one incident across recovery updates
16 July; 21 July statement	An official-origin municipal statement reports business-contact and technical-directory data escaping after an attack on an IT provider [S64]	It says citizen, private staff-contact and specialist-application data were unaffected; the republished statement is not independent editorial confirmation
July; August updates	A research institute reports an attack on a network component and precautionary communications disruption [S66]	Its investigation said internal-system access attempts failed; do not convert an outage into confirmed internal access
August and October; 8 October notice	A memorial foundation explicitly distinguishes a renewed website attack from its earlier IT attack [S67]	Two events, no established common actor or political motive; the October notice supplies the distinction
27 September; 29 September notice	A county describes preventive shared-system shutdown and patching [S73]	It expressly reports no successful attack or detected outflow; excluded from confirmed intrusions
15 October notice	A municipality confirms copied data and manual recovery processes, with data scope still under investigation [S68]	Its utility was expressly excluded; do not extend the incident to every affiliated entity

The January chamber and November university cases both raise password questions, but there is no evidence of a shared campaign. The two utility cases support separating supply continuity from customer operations, not a claim of one utility-sector actor. A research institution's subject area and a memorial's public role do not establish motive or state attribution.

A separate university-hospital notice on 22 May also confirms patient data lost at an external billing provider while the hospital's own systems and care remained unaffected. Its affected-client population is not added to another hospital's figures. The two client disclosures alone do not establish an additional provider incident or a combined patient total. [S83]

5.10 Further priority-organisation findings

Development supply chain. A vendor warned that four malicious open-source package versions were distributed through a public package registry on 29 April. It warns of credential extraction and attempted propagation after installation. This establishes a software-supply-chain incident, without a verified German downstream victim count. Development teams should identify affected builds, follow the vendor's mitigation and assess credentials reachable from those environments. [S76]

University maintenance and uncertainty. A university's 25 February notice describes emergency maintenance on 23 February after an external vulnerability report. It says student and former-student addresses might have been accessible, but exploitation could not be determined conclusively. The patch and interruption are confirmed; a successful intrusion is not. This belongs in the security-event record with that qualification. [S77]

Vehicle-retail supplier. A retailer's October notice describes unauthorised access to a shared provider during 8–30 September and possible customer, vehicle and purchase information exposure. It distinguishes confirmed client-record access from records whose access could not be excluded. Its statement that bank data were unaffected applies to its notice; it is not a blanket exclusion for every provider customer. Protect invoice verification and obtain a client-specific scope. [S80]

Certification services. A certification organisation acknowledges a September IT security incident in an October publication. The supporting passage does not establish a data category, actor or affected-client count. It is retained as a bounded service-provider notice, without assuming that certification customers' systems were accessed. [S84]

The Berlin case also has a recent federal-scope update. The 16 November parliamentary summary warns that names or abbreviations in file names can misidentify an affected authority, while other affected material may be missed by file names alone. Content review is required before assigning federal impact. This is a scope update to Case A, not another attack. [S82]

5.11 What the cases support

Evidence pattern	Supported interpretation	First response
Administrative records copied	Scoping can continue after containment	Assign data owners and affected-person support
Credentials used across services	Identity can extend the incident's reach	Review privileges, sessions and recovery methods
Supplier-held records exposed	Customer harm can occur outside the controller's own systems	Obtain a scoped record list and coordinate notices
Availability disrupted	Business tasks can fail without proven theft	Test the minimum service and alternate channel
Industrial control targeted	Operational safety requires physical verification	Validate independent alarms and safe fallback

The cases do not establish a national sector ranking. Public disclosure is uneven, and some incidents remain private. Their value lies in showing the response questions that similar organisations should be able to answer.

KEY TAKEAWAYS

01

Preserve the distinction between credential misuse, copied data and unavailable services.

02

The two Tübingen notices describe separate affected populations and responses.

03

Recent publications include historical enforcement and recovery updates as well as new incidents.

CHAPTER 06

Hacktivism, DDoS and operational technology

06

THIS CHAPTER ANSWERS

What distinguishes a public availability claim from confirmed operational impact?

3

separate checks: service, data and physical process

6.1 Evidence timeline 54

6.2 Availability is a customer outcome 54

6.3 Criminal disruption is not always political 55

6.4 Industrial cooling changes the continuity question 55

6.5 A claim-to-response decision sequence 56

6.6 Completion evidence 56

CHAPTER 06

Hacktivism, DDoS and operational technology

IN SHORT

An availability claim can circulate before an operator understands the outage. A confirmed outage still does not establish data theft, an actor or physical-process access. Germany's railway case and November cooling warning illustrate different response needs. Prepare mitigation and public status messages, but verify operational consequences with the people responsible for the service and equipment.

6.1 Evidence timeline

6 Feb 2026	**BSI and BfV** Messenger-phishing warning; identity campaign, not a DDoS event [S5]
17 Feb 2026	**Deutsche Bahn** February availability disruption of booking and information services [S7][S8]
20 Mar 2026	**BKA and ZAC NRW** Announce action against infrastructure associated with Aisuru and Kimwolf [S24]
31 Aug 2026	**State criminal police** Announce a DDoS and attempted-extortion investigation; allegations remain under investigation [S25]
12 Nov 2026	**BKA and ZIT** Announce malware-infrastructure disruption during 9–11 November [S23]
18 Nov 2026	**LKA NRW** Warn about attacked cooling controls and operational contingency planning [S21]

Every row identifies its source type. The identity warning and malware enforcement rows are contextual events, not additional DDoS incidents. Their inclusion does not establish a shared campaign or operator.

6.2 Availability is a customer outcome

The February railway disclosure establishes service disruption. It does not attribute the event to a named claimant. The report therefore does not convert unrelated actor rhetoric, a foreign-policy theme or an availability-check result into official attribution. [S7][S8]

For a customer-facing service, test the complete task. A homepage may respond while authentication, ticket retrieval or payment fails. Record which functions work, from which user groups, and which fallback route remains usable. Keep the measurement date beside the public status.

The response should distinguish traffic mitigation from business restoration. Infrastructure teams can confirm that traffic is being absorbed. The service owner confirms that the essential user journey works. Communications should state the narrower fact until both are established.

Question	A claimant may assert	Established reporting	Defender's test
Is the site down?	A momentary failed check	Railway booking disruption was reported [S7][S8]	Test the essential customer task
Was data taken?	An outage presented as access	The cited availability case does not establish data theft	Review authenticated access and data-access evidence
Who caused it?	A self-identified actor takes credit	No official actor attribution established in this case	Preserve evidence and state attribution separately
Was an industrial process altered?	A claimed control-panel screenshot	The cooling warning identifies a distinct operational risk [S21]	Verify process readings with the operator

The claimant column is a general interpretation aid, not a quotation from a German post. It must not be read as evidence that a particular actor made each assertion during this window.

6.3 Criminal disruption is not always political

The August state-police notice describes a DDoS and attempted-extortion investigation. The March BKA/ZAC notice concerns botnet infrastructure. These official accounts support attention to criminal infrastructure and incentives; they do not prove that a specific German outage used those botnets. [S24][S25]

The BKA's retrospective discussion of NoName057(16) concerns 2025. Its assessment supplies historical context for public-service readiness. It cannot establish the group's responsibility for the February 2026 railway incident. [S4]

Treat an announced political cause as the speaker's framing. Response teams should assess traffic, impact and access evidence on their merits. The same protection and notification standards should apply to political organisations, government bodies, businesses and civil society.

ENISA's 4 November joint statement describes refrigeration incidents in several EU member states, including a further wave on 1–2 November. It gives no German victim count. Its regional scope supports reviewing exposed control systems, but it does not add German blood-bank incidents to the national record. [S70]

6.4 Industrial cooling changes the continuity question

The November warning adds a physical-process dimension. Its German and French examples remain separate. The source does not establish direct impact on German blood banks or identify an operator common to the reported events. [S21]

The practical question is whether staff can detect an unsafe condition independently of the controller under investigation. A screen showing a normal temperature is insufficient if the same system supplies the reading and the alarm. Validate an independent monitoring route with the equipment owner.

The response plan should specify who can isolate remote maintenance without creating a safety problem. It should identify alternative storage, escalation contacts and the maximum acceptable interruption for the relevant stock. Those decisions require facilities, operations and safety staff alongside information security.

Do not apply a generic shutdown instruction to every industrial system. Unplanned isolation can interrupt monitoring or a necessary safety function. Use the approved operational procedure and retain an authorised record of changes and physical observations.

An August state-security warning about programmable controllers primarily concerns attacks reported against US facilities. It recommends hardening, separation and monitoring, but provides no German victim count. The warning supports reviewing comparable equipment; it does not establish an intrusion into a German manufacturer or identify an actor in this report. [S79]

6.5 A claim-to-response decision sequence

1. **Establish the service state.** Confirm the affected function, duration and available fallback. Record customer or operational impact separately from a network symptom.
2. **Check access evidence.** Review whether there is evidence of unauthorised identity use or data access. Do not infer either from an outage alone.
3. **Verify the physical process.** Where industrial equipment is implicated, use independent readings and the operational owner. Preserve the distinction between a screenshot and confirmed manipulation.
4. **Publish a bounded statement.** Identify the known disruption, the action underway and the next update time. State what remains under investigation without promising an absence of impact.
5. **Retain the evidence for reporting.** Preserve the chronology and contact the competent route under the organisation's obligations. Record decisions even when no formal notification is required.

6.6 Completion evidence

Owner	Test	Completion evidence
Infrastructure	Activate contracted DDoS mitigation	Exercise log and escalation contact
Service owner	Complete the minimum user journey during degradation	Test record and fallback instructions
Communications	Issue a claim-aware service statement	Approved template and update schedule
OT and facilities	Detect an abnormal condition independently	Witnessed alarm and response test
Supplier management	Restrict maintenance access under the approved procedure	Named access owner and tested revocation

KEY TAKEAWAYS

01

A failed availability check does not establish theft, attribution or sustained outage.

02

Political framing and criminal infrastructure are separate propositions.

03

Industrial incidents require physical verification and an operational fallback alongside IT recovery.

CHAPTER 07

Threat actors and evidence relationships

07

THIS CHAPTER ANSWERS

Which actor-related propositions are supported, and which relationships remain unestablished?

35.2%

of German listings carry the three largest claimant labels

7.1 Relationship map 59
7.2 Ransomware and extortion 60
7.3 Monthly and sector composition 63
7.4 Messenger phishing and state-attributed campaigns 64
7.5 Hiring and supplier identity 65
7.6 Enforcement and the limits of disruption 66
7.7 Vulnerability handling as a cross-sector control 67

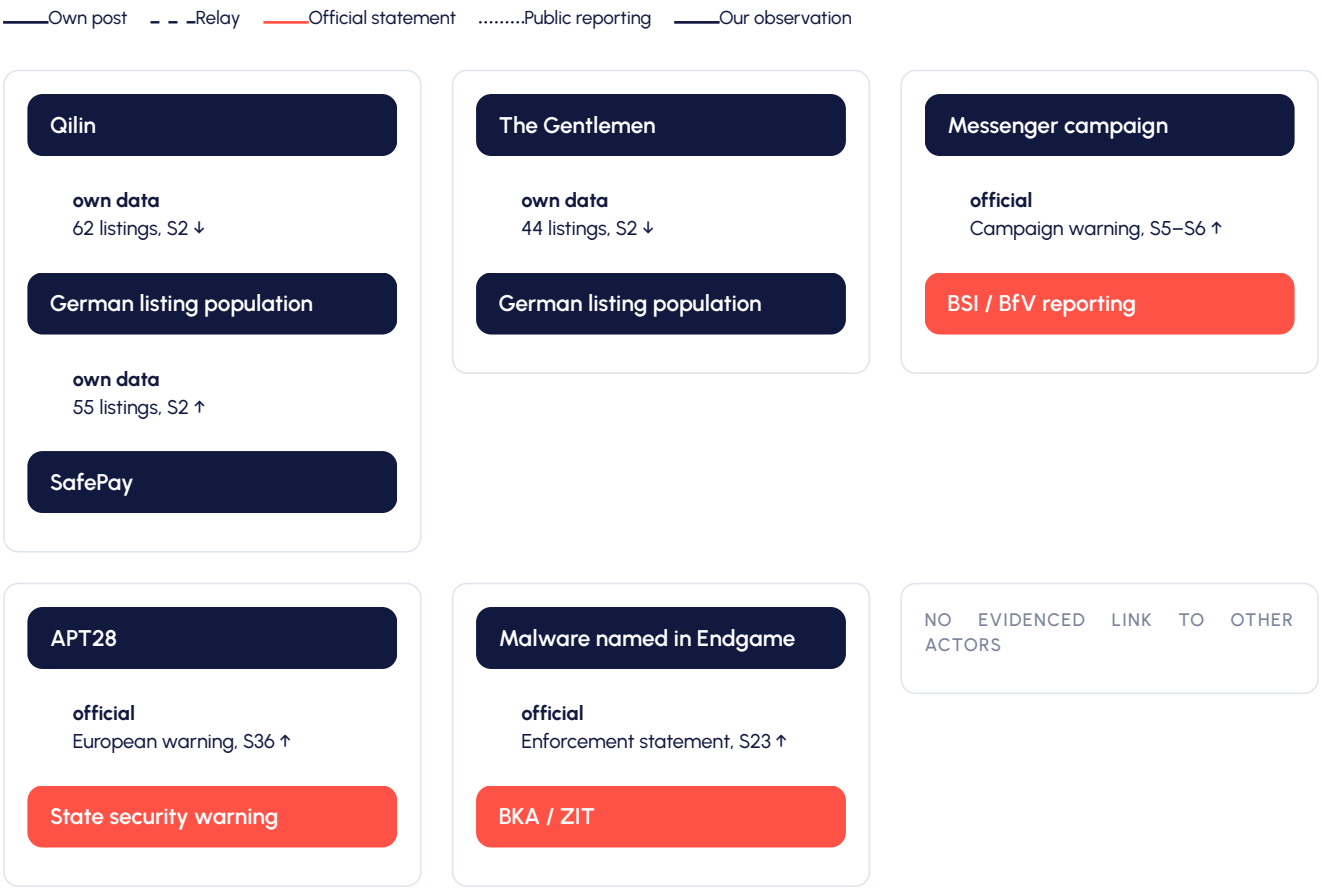
CHAPTER 07

Threat actors and evidence relationships

IN SHORT

Extortion listings provide the strongest comparable actor population in this edition. Qilin, SafePay and The Gentlemen lead, but most German listings carry other labels. Official campaign warnings add identity and espionage context without establishing a German victim in every case. Keep listing counts, state attribution and shared-operator hypotheses separate. Build response plans around the affected access and service rather than an actor's reputation.

7.1 Relationship map

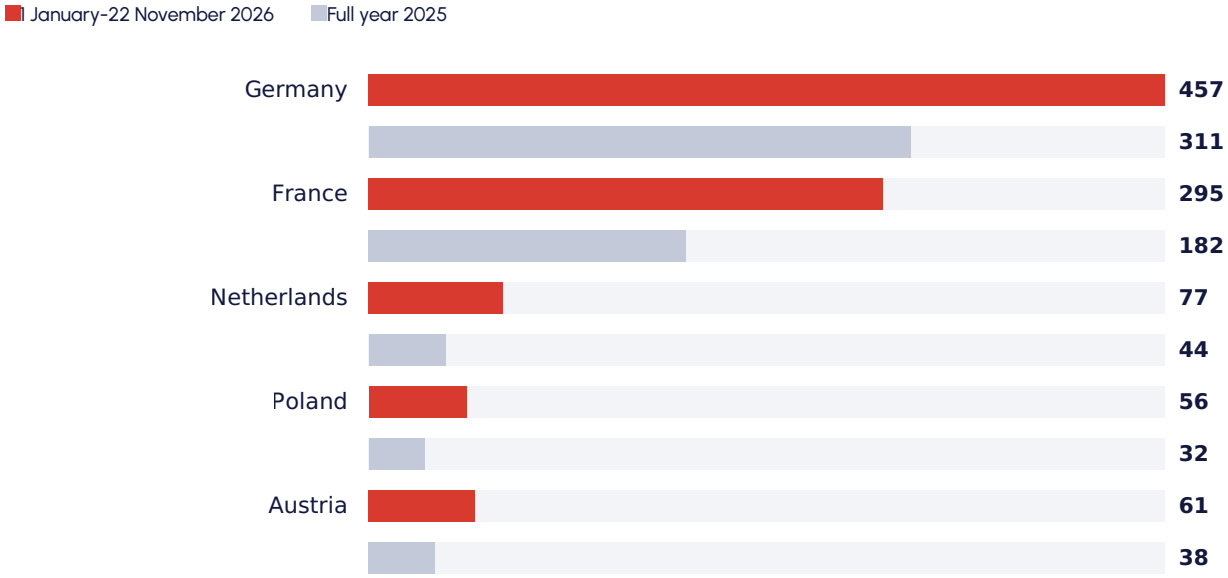


Each edge identifies a specific relationship: a listing label in the German population, a campaign warning or an official enforcement statement. An edge does not establish a common operator. Unconnected actors remain unconnected; a shared country or technique is not enough to join them.

The diagram is not a map of the entire German threat environment. Its purpose is to make the report's evidence relationships legible. A new claim must establish its own connection before it is added to an existing campaign.

7.2 Ransomware and extortion

German listings exceed each selected peer in this retained listing population



Unmatched periods and different country populations; not a national risk ranking. Source: Brandefense Ransompedia Germany-labelled listings, 1 January-22 November 2026; November partial. Listings record criminal claims, not confirmed intrusions [S2].

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

The five country counts are shown together for context. They are not adjusted for economic size, organisation population, disclosure behaviour or source coverage. They cannot establish which country's organisations are safer.

Country	Requested 2026 window	Full-year 2025	Largest current label
Germany	457	311	Qilin, 62
France	295	182	Qilin, 48
Netherlands	77	44	LockBit5, 15
Poland	56	32	The Gentlemen, 19
Austria	61	38	The Gentlemen, 11

Source: Ransompedia [S2]. Every current-window figure is compared with a full prior year, not the same elapsed period. No growth-rate claim is made.

Qilin

Extortion listing label | No state attribution assessed

IN GERMANY, 2026

2026
62 German listings in the requested window

CLAIMED TARGETS

Sector mix in the listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 62 German listings under this label.

OUR ASSESSMENT

Listing presence supports recovery and disclosure readiness. It does not establish encryption, theft, a shared operator or a completed payment.

CONFIDENCE
High for retained listing count; underlying assertions remain claims

SafePay

Extortion listing label | No state attribution assessed

IN GERMANY, 2026

2026
55 German listings in the requested window

CLAIMED TARGETS

Sector mix in the listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 55 German listings under this label.

OUR ASSESSMENT

Listing presence supports recovery and disclosure readiness. It does not establish encryption, theft, a shared operator or a completed payment.

CONFIDENCE
High for retained listing count; underlying assertions remain claims

The Gentlemen

Extortion listing label | No state attribution assessed

IN GERMANY, 2026

2026

44 German listings in the requested window

CLAIMED TARGETS

Sector mix in the listing population; no named victims here

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 44 German listings under this label.

OUR ASSESSMENT

Listing presence supports recovery and disclosure readiness. It does not establish encryption, theft, a shared operator or a completed payment.

CONFIDENCE

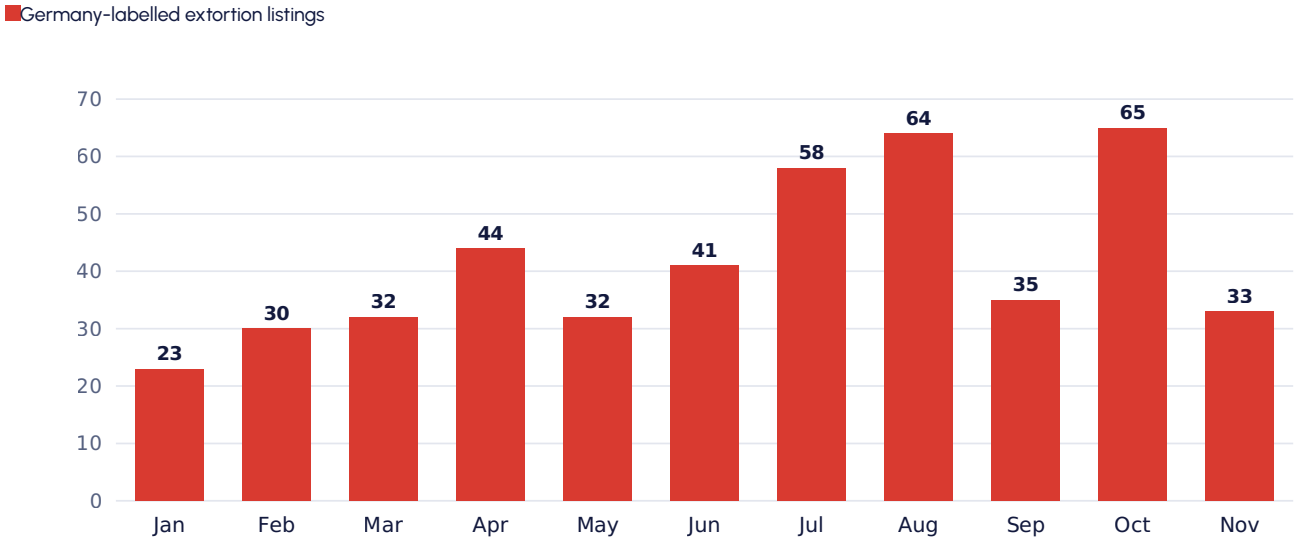
High for retained listing count; underlying assertions remain claims

The leading German labels account for 62, 55 and 44 listings. Their combined 161 represents 35.2% of 457. The remaining 67 labels account for 296. A preparedness plan limited to the leading three would therefore omit most of the retained listing population. [S2]

This distribution supports capability-oriented planning. Test how identity access can reach critical data, how backups are protected from the production identity system, and how a data-loss notice is prepared. Those decisions remain useful when a claimant changes its name.

7.3 Monthly and sector composition

Listing counts vary through the year, while the final month remains partial



Source: Brandefense Ransompedia Germany-labelled listings, 1 January–22 November 2026; November partial. Listings record criminal claims, not confirmed intrusions [S2].

Month	German listings	Month	German listings
January	23	July	58
February	30	August	64
March	32	September	35
April	44	October	65
May	32	November to cut-off	33
June	41	Total	457

Source: Ransompedia [S2]. The counts describe publication timing. October's 65 listings do not establish 65 intrusions beginning that month. November is incomplete and is not directly comparable with a full month.

The largest retained industry label is manufacturing, with 77 listings. Consulting follows with 55. These labels describe the listing records; they are not a denominator for the number of organisations operating in each industry. [S2]

Manufacturing leaders should read this as a continuity-planning reason to test recovery and supplier access. Consulting and service providers should test whether access or data held for customers increases the consequences of an incident. The listing figures alone do not establish either entry route.

7.4 Messenger phishing and state-attributed campaigns

Unattributed messenger-phishing campaign

Campaign described by authorities | State support considered plausible by BSI; other authorities' attribution remains theirs

IN GERMANY, 2026

2026
Official reporting context; dates in Chapter 7

CLAIMED TARGETS

Only as described by the cited source

SEEN IN PUBLIC REPORTING

[S5] Official supporting passage read

[S6] Official supporting passage read

OUR ASSESSMENT

Legitimate messenger features and social engineering are described. No software-encryption failure is established. Review linked devices and trusted recovery.

CONFIDENCE
As bounded in the cited official reporting

The messenger case is an official warning about social engineering of legitimate features. It is not evidence that the encryption protocol or application software was broken. Attribution remains as described by BSI, BfV and the authorities named in their reporting. [S5][S6]

For leadership teams, the defensive unit is the conversation and its participants. Review linked devices, recovery arrangements and trusted contact routes. Train staff to verify a security request through a known channel before approving an account action.

APT28

Espionage, per official warning | Association stated by LfV Baden-Württemberg

IN GERMANY, 2026

2026
Official reporting context; dates in Chapter 7

CLAIMED TARGETS

Only as described by the cited source

SEEN IN PUBLIC REPORTING

[S36] Official supporting passage read

OUR ASSESSMENT

The source warns about European policy-research targets. It does not establish a named German victim or connect unrelated German incidents.

CONFIDENCE
As bounded in the cited official reporting

A January state-security warning relays credential-phishing activity against European think tanks and associates it with APT28. It supports planning for policy and research organisations. It does not establish a named German victim or justify assigning an unrelated German incident to that group. [S36]

The maritime warning is similarly bounded. The authority discusses espionage in seven unspecified EU states and states its own attribution. Germany cannot be inserted into an unnamed country list merely because the warning is published by a German authority. [S38]

A 30 April state-security warning describes fake conferencing messages that lead users to execute a command and install macOS malware. The authority attributes that campaign to Lazarus. This is a campaign warning, not a confirmed German victim count. For business meetings, provide a known support route and train staff to stop when an invitation asks them to run an unexpected command. [S72]

7.5 Hiring and supplier identity

A state-security warning describes remote IT applicants using false identities and gives the authority's North Korea linkage. The defensible response is identity, qualification and access verification. It is not screening based on appearance, language or an assumed nationality. [S37]

Apply the same process to every supplier worker. Verify the contracting entity, employment relationship, access purpose and device arrangements. Review who can approve remote access and how it is revoked when the assignment ends.

These checks also help distinguish an authorised contractor from an unknown session. An organisation should be able to connect each privileged identity to a current accountable person and engagement without relying on a supplier's email introduction alone.

7.6 Enforcement and the limits of disruption

Malware named in Operation Endgame

Official enforcement context | No state attribution assessed

IN GERMANY, 2026

2026
Official reporting context; dates in Chapter 7

CLAIMED TARGETS

Only as described by the cited source

SEEN IN PUBLIC REPORTING

[S23] Official supporting passage read

OUR ASSESSMENT

BKA and ZIT name Gootloader, CastleRAT and StealC in the November action. Global quantities are not German victim totals. Local infection validation remains necessary.

CONFIDENCE
As bounded in the cited official reporting

The November BKA/ZIT statement identifies Gootloader, CastleRAT and StealC in an operation conducted on 9–11 November. It reports global infrastructure and credential findings, including infrastructure in Germany. Those quantities are not German victim totals. [S23]

An infrastructure action does not demonstrate that every previously infected device has been cleaned. Organisations receiving a relevant notification should validate the host, credentials and active sessions through their own incident process. Preserve notification dates and the resulting disposition.

The March botnet and August DDoS investigations belong to different official case populations. This report does not connect them to Endgame, the railway disruption or the cooling incidents without a concrete shared element. Suspicions and enforcement announcements remain distinct from convictions. [S24][S25]

7.7 Vulnerability handling as a cross-sector control

The BSI's retrospective account of mobile-device-management exploitation describes vulnerable systems in Germany and distinguishes confirmed data outflow from cases where it could not be excluded. No German victim total is established in that account. [S45]

Separately, the following verified vulnerability is a control example, not evidence of exploitation at a German organisation in this report.

Reference	Affected products	Verified remediation	Limit
CVE-2026-1731	BeyondTrust Remote Support 25.3.1 and earlier; Privileged Remote Access 24.3.4 and earlier	Vendor patches BT26-02-RS / BT26-02-PRA; Remote Support 25.3.2 or later; use Privileged Remote Access 25.1.1 or later as the vendor's explicit upgrade guidance	Confirm supported upgrade path and patch eligibility with the vendor

Sources: NVD record and vendor advisory [S33][S34]. Older unsupported releases need a supported upgrade path. Applying an update does not by itself establish whether an earlier intrusion occurred.

For an exposed remote-support service, the completion evidence should include the installed version, patch confirmation, access restrictions and an investigation decision. Do not claim a German exploitation campaign from a global vulnerability record.

KEY TAKEAWAYS

01
Most German listings sit outside the three leading claimant labels.

02
State attribution belongs to its named source and does not transfer to unrelated incidents.

03
Enforcement and patching require local validation of hosts, identities and continuing access.

CHAPTER 08

Fraud, identity and secondary harm

08

THIS CHAPTER ANSWERS

How can information loss produce further harm after an incident is contained?

2

documented follow-on patterns: patient extortion and booking fraud

8.1 A supported chain, with explicit limits 69
8.2 What customer operations should be able to answer 69
8.3 Police and regulator reporting on fraud 70
8.4 Public authorities as a trusted verification route 70
8.5 Card material in posts: a narrow view 71
8.6 Prices and market size 71
8.7 Completion evidence for customer protection 72

CHAPTER 08

Fraud, identity and secondary harm

IN SHORT

Official warnings show stolen information being reused against patients and hotel guests. These cases support customer protection alongside technical recovery. Recent enforcement also concerns fake shops and investment-fraud contact infrastructure, but those quantities measure different things. Prepare a trusted verification route, brief customer-facing teams and record reports of follow-up contact without promising that the institution can prevent every attempted fraud.

8.1 A supported chain, with explicit limits

The patient-extortion and hotel-software notices establish that copied information was used in further contact with affected people. They do not establish the entire criminal supply chain, a completed sale or a common operator between the cases. [S16][S18]

The following is an **analytical model** for defensive planning. It connects data exposure, plausible impersonation, an induced action and monetisation. The model is not a finding that the same seller, caller and recipient account operated together in the German cases.

Stage	Possible abuse	Defender's interruption
Information exposed	Real identity or reservation details supply credibility	Identify the affected categories and warn users proportionately
Contact initiated	A message imitates a familiar institution	Offer a separately verified contact route
Action requested	Recipient is asked to pay or disclose a code	Publish the legitimate process and brief staff
Value moved	Payment reaches a fraudulent destination	Escalate promptly to the payment provider and police
Repeat contact	Another message uses the same information	Retain incident context and update support guidance

The business implication is that confidential information can remain useful after passwords have changed. A person cannot easily replace a medical history or a past reservation. Support should therefore address the information's sensitivity and context, not only authentication.

8.2 What customer operations should be able to answer

A recipient needs a simple way to determine whether a message is authentic. The organisation should identify its genuine payment and support processes, a route for independent verification and what information staff will need to assess a report.

The first conversation should avoid adding sensitive details to an untrusted exchange. Staff should not authenticate a caller solely because the caller quotes a booking, an address or a treatment. Those details may be the very information involved in the incident.

For affected people, the institution should distinguish recommended action from a guarantee. A warning can explain how to verify requests and preserve suspicious contact. It cannot establish that a criminal no longer holds the data or that paying an extortion demand causes deletion.

8.3 Police and regulator reporting on fraud

Published	Official action	Unit and limitation
September	Authorities reported disabling 9,304 German telephone numbers associated with suspected investment-fraud activity over the preceding period [S43]	Telephone numbers; not victims or separate criminal groups
October	Investigators described misuse of a local party email account to send almost 5,000 messages [S41]	Messages; no political motive established at that stage
November	Prosecutors announced a fake-shop charge concerning alleged earlier conduct [S42]	Enforcement announcement; charge is not conviction

The investment-fraud action illustrates an interruption point outside the victim organisation's perimeter. The account-misuse case illustrates that a familiar sender can become a fraud channel. Neither establishes a new national loss estimate.

The recent fake-shop announcement concerns alleged conduct from 2023 to early 2025. It belongs in the recent enforcement section because of the announcement date. It must not become a count of fake shops newly created in November 2026.

A separate May BKA/ZIT notice describes disabling a rebuilt illegal marketplace and arresting its alleged operator. It is an enforcement action, not a count of German victim organisations or evidence that every advertised product was delivered. [S47]

The Hessian data-protection authority also warns that authentic booking details can make fraudulent guest messages convincing. Its broader accommodation warning does not establish that payment data were taken in the specific November reservation-provider case. [S69]

8.4 Public authorities as a trusted verification route

A public body should explain its real process for payments, document requests and account recovery. The explanation must be findable without following a link from the suspicious message. Customer-facing staff should know how to redirect a concerned user to that process.

For an email-account incident, verify mailbox rules, delegated access and authorised applications alongside the password. Preserve the messages needed for investigation. Coordinate a recipient warning when there is evidence that an account was used to contact others.

For a bank or merchant, the relevant controls include new payment destinations, unusual account activity and customer reports of pressure to act. A leaked contact list alone does not establish that a transfer is fraudulent. The fraud process must validate the transaction and the customer's circumstances.

8.5 Card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

The figures describe payment-card records in the retained post corpus. They do not measure national card exposure, card theft or fraud loss.

The retained post material contains 15 distinct German-associated payment-card records across 16 posts. This is a narrow observation of published card material, not a German issuer census. Country association does not independently establish the cardholder's residence or current card usability. No issuer ranking, completed fraudulent transaction or loss total is inferred. [S1]

An issuer should validate an exposure through its established compromise-handling process. A post's assertion that a card is usable does not establish an authorised transaction, a completed fraudulent payment or a loss. Do not use the narrow post population to rank national payment security.

8.6 Prices and market size

This edition publishes no German national underground price index. Asking prices, where observed in a specific advertisement, are claims about an offer. They do not establish a completed transaction, the seller's possession of the material or the value of the underlying crime.

An estimate of national fraud proceeds would require evidence that this report does not hold. Repeated advertisements can reflect the same offer, and a message can name several countries. The appropriate action is validation of a relevant claim, not multiplication of posts by an asking price.

8.7 Completion evidence for customer protection

Owner	Required capability	Evidence of completion
Customer operations	Recognise incident-related contact	Approved scripts and a staff exercise
Fraud	Assess suspicious payment requests	Documented escalation and transaction review
Data protection	Determine affected categories and people	Scoped assessment with remaining uncertainty
Communications	Provide independent verification	Published trusted contact route
Security	Link follow-up reports to the incident	Incident record with a dated disposition

KEY TAKEAWAYS

01

Copied information can support later extortion or impersonation after systems recover.

02

Enforcement counts of numbers, messages and historical charges are not national fraud totals.

03

Give affected people a trusted verification route and trained support staff.

CHAPTER 09

Banking and financial services

09

THIS CHAPTER ANSWERS

Which financial-domain observations require account and fraud validation?

13 of 25

observed financial domains had a current credential offer

9.1 Financial-domain exposure observations 74
9.2 A recent bank statement is not a new-intrusion count 75
9.3 Customer-side and institution-side evidence 75
9.4 Supplier and payment-process dependencies 76
9.5 Reporting and third-party resilience 76
9.6 Validation and closure 77

CHAPTER 09

Banking and financial services

IN SHORT

The selected financial portfolio has 25 observed domains, with current credential offers for 13. It records at least 80,163 device associations and 669,977 credential-record associations. These observations do not establish bank intrusions or unique customers. Validate current accounts, distinguish staff from other users and keep customer-fraud evidence separate from institution-access claims.

9.1 Financial-domain exposure observations

Measurement	Result	Interpretation
Financial domains with observations	25	Selected services; no census of independent banks
Domains with current credential offers	13	Account-validation leads, not confirmed intrusions
Domains with device associations	21	Association does not establish device ownership
Device associations, at least	80,163	Overlapping cumulative domain associations
Employee-device associations	698	Validate employment and account context
Other device associations	79,465	Not verified customer devices
Credential-record associations	669,977	Not unique people or active credentials

Exposure source: dated observations [S87]. The separate payment-card observations in §8.5 do not establish the source of card exposure. [S1]

SCOPE OF THE CARD FIGURES

These figures describe selected financial-domain exposure observations. They do not establish independent banks, unique customers or confirmed intrusions.

No bank or sector rating is published. The measured counts above retain their separate denominators.

9.2 A recent bank statement is not a new-intrusion count

On 17 November, Deutsche Bank said the documents described in recent media reporting were historical. It stated that its checks had found no indication of current IT access or access to account information, logins or payment data. Its analysis continued. [S39]

Russian-language reporting covered the disclosure and regulatory attention. That supplies reporting context, not independent confirmation that the bank suffered a new intrusion during this report's window. This report takes no position on the unrelated political or client matters discussed in that reporting. [S40]

Proposition	Media disclosure	Bank's statement	Report treatment
Documents exist	Reporting describes internal material [S40]	Bank describes it as historical [S39]	Document disclosure, with age unresolved at individual-file level
Current IT access	Not independently established here	Bank says no indication from its checks [S39]	Not counted as a confirmed new intrusion
Login or payment access	Not established by a document-volume headline	Bank says no indication [S39]	No exposure total inferred
Public interest reporting	Reporting examines the material	Bank states its position	No inference about a cyber operator or motive

The correct defensive question is whether your own evidence shows a currently usable identity, session or access path. A document's publication date does not answer that question. Equally, an institution's statement of no indication remains its assessment at that time.

A 14 August BKA/ZIT announcement concerns an investigation into unauthorised online-banking debits allegedly made in November 2023 after a faulty provider update. It reports international enforcement activity in August 2026. The authority does not name the affected bank. This is historical alleged conduct with a recent enforcement phase, not a new German bank intrusion or a 2026 loss total. [S81]

9.3 Customer-side and institution-side evidence

If an alert names a bank login, determine whether the account belongs to a customer, employee, contractor or unknown person. A service-domain association alone does not establish a device owner or an intrusion into bank infrastructure.

For a validated employee identity, examine privilege, sessions and recent access. For a customer, combine the alert with account-security and fraud evidence. Apply the bank's established authentication and support processes before requesting a disruptive action.

The different owners should share a common disposition vocabulary: confirmed and contained, already remediated, unrelated, unresolved or escalated. The evidence should show why the case was closed. A dashboard count without dispositions does not demonstrate reduced risk.

9.4 Supplier and payment-process dependencies

The hotel and healthcare warnings show how accurate contextual information can make a fraudulent request plausible. Banks should prepare customer-support routes for requests that appear to quote real institutional details. This is a defensive inference from those cases, not a measurement of banking fraud prevalence.

For the institution itself, map payment operations to identity, communications and third-party services. Include a fallback channel for authenticating urgent instructions when normal email or telephony is unavailable. Test who can approve the exception and how the decision is recorded.

For a changed payee or supplier instruction, use a known independent contact route. Do not accept a new number supplied in the same message as independent verification. The completion evidence is a documented control and a passed exercise using synthetic data.

9.5 Reporting and third-party resilience

The Bundesbank's DORA guidance identifies BaFin as the competent recipient for relevant financial-entity incident reports and explains onward sharing with other authorities. It also describes the register of contractual ICT service arrangements. [S32]

For major ICT-related incidents, Article 5 of Delegated Regulation (EU) 2025/301 sets these clocks. [S88]

Submission	Deadline
Initial notification	As early as possible; within 4 hours of major-incident classification and generally within 24 hours of awareness
Late classification	If classified as major after 24 hours of awareness, notify within 4 hours of classification
Intermediate report	Within 72 hours of initial notification, even without changes; update without undue delay and upon recovery of regular activities
Final report	Within 1 month of the intermediate report or latest updated intermediate report

Article 5 allows submission by noon of the next working day when a deadline falls on a weekend or bank holiday. Credit institutions, central counterparties, trading-venue operators and NIS2 essential or important entities cannot use that extension for initial or intermediate reports. Authorities may also exclude other significant or systemic financial entities. If unable to meet a deadline, inform the authority without undue delay, at the latest by that deadline, and explain why. [S88]

The practical requirement is to connect a service interruption to the organisation's classification and reporting process. A supplier may have an incident without every affected customer meeting the same reporting trigger. Record the determination and the information still required.

The register should be usable in an incident. A team should be able to identify the provider, critical function, technical owner, escalation contact and alternative arrangement. Testing that lookup is more useful than treating an untested spreadsheet as completed resilience.

9.6 Validation and closure

Use the observed financial-domain signals for owned-account checks. Confirm employment, service ownership, account status and earlier remediation before containment. Related services can belong to the same legal entity. A current advertisement does not establish that institution's internal access was obtained.

The narrow payment-card observations do not measure national card exposure. Keep customer-fraud controls and staff-account response under separate accountable owners.

KEY TAKEAWAYS

01

Validate financial-domain observations against the relevant accounts and services.

02

Historical document disclosure and current access require different evidence.

03

Validate identities, payment changes and provider dependencies through established bank processes.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which obligations should a German incident team operationalise before an event?

24 / 72 hours

distinct early-warning and incident-notification deadlines under the relevant BSIG duty

10.1 Rules and responsibilities 79
10.2 Notification clocks require an awareness record 80
10.3 One incident, several competent routes 80
10.4 Management oversight needs operational evidence 81
10.5 National response and practical cooperation 81
10.6 A reporting rehearsal 81

CHAPTER 10

Regulatory and national response

IN SHORT

Germany's NIS2 implementation is in force. In-scope entities must connect security measures, management oversight, registration and significant-incident reporting. Personal-data reporting and financial-sector reporting have different triggers and recipients. An incident may require several assessments. Name the decision-makers, preserve awareness times and rehearse a joint exercise with a critical provider.

This chapter is a planning aid, not legal advice.

10.1 Rules and responsibilities

The table records selected operational obligations. It does not determine whether a particular candidate organisation is in scope or reproduce every statutory exception.

Rule	Applies where	Operational requirement	Decision owner
BSIG §30	Entity qualifies under the relevant German scope provisions	Proportionate security risk measures, including continuity, supplier security and authentication; document compliance [S26]	CISO and management
BSIG §32	In-scope entity has a significant incident	Early warning and notification without undue delay, at the latest within 24 and 72 hours of awareness, respectively. Final report normally within one month after notification [S27]	Incident lead and legal
BSIG §33	Relevant entity first qualifies or qualifies again	Register within three months; update changed details within the statutory period [S28]	Legal and accountable entity owner
BSIG §38	Management of an in-scope entity	Implement and oversee required risk measures; attend recurring training [S29]	Management

Rule	Applies where	Operational requirement	Decision owner
GDPR Articles 33–34	A personal-data breach meets the relevant risk test	Controller notifies the competent authority without undue delay and, where feasible, within 72 hours; assess affected-person communication [S31]	Data-protection officer and controller
DORA	Relevant financial entity and major ICT-related incident	Apply the notification sequence and exceptions in §9.5; use the competent-authority route and maintain ICT third-party records [S32] [S88]	Financial incident function and compliance

Germany's implementation commenced on 6 December 2025. Registration timing depends on when the entity qualifies; it is not a recurring annual grace period. Scope must be established for the actual legal entity and activity. [S30][S28]

A separate parliamentary announcement records passage of a cybersecurity bill on 12 November. Passage alone does not establish commencement. It does not replace the in-force obligations used in this table without checking the promulgated law and applicable date. This report takes no position on the policy choices. [S85]

10.2 Notification clocks require an awareness record

For the relevant BSIG duty, the early and subsequent notices have different content and deadlines. The final-report timing follows the incident notification. Where an incident continues, the statute provides for a progress report and subsequent final reporting. [S27]

Under GDPR, the controller's authority notification depends on the risk to people. A processor informs the controller without undue delay. High risk can require communication to affected people, subject to the applicable exceptions. Document the assessment even where the conclusion is not to notify. [S31]

Do not start every clock from a convenient press-release date. Preserve when the relevant entity became aware, what was known then and which information arrived later. Legal should record the trigger assessment and the rationale for any staged or updated submission.

10.3 One incident, several competent routes

The recipient can depend on the entity, sector and jurisdiction. A personal-data question should identify the competent supervisory authority. A financial incident follows the relevant financial framework. A police report addresses a different purpose from regulatory notification.

The incident record should identify each route, named decision-maker and deadline. A shared chronology can support several notifications, but a submission under one regime should not be assumed to satisfy another without checking the applicable rule.

Supplier escalation should support those determinations. Ask for the discovery and awareness timeline, affected service, data categories, possible customer impact and current containment status. Separate confirmed facts from estimates so that legal can decide with the evidence available.

10.4 Management oversight needs operational evidence

BSIG management duties concern implementation and oversight, not merely receipt of a security presentation. The statutory training duty also requires recurring attention to risk and the consequences for the entity's services. [S29]

For board reporting, connect each material dependency to an accountable owner and a test. Examples include identity recovery, a critical supplier's incident notice, a service restoration and an operational fallback. Record the remaining exception, its owner and the date for closure.

The report does not offer a universal fine figure or infer a liability outcome from an incident. Those depend on the applicable provision, entity and facts. Verify the current legal text before relying on an enforcement conclusion.

10.5 National response and practical cooperation

The BKA/ZIT and state-police notices demonstrate investigations across malware, DDoS and fraud infrastructure. Their publication does not certify that every affected system is clean. Relevant notifications should enter the organisation's own response and validation process. [S23][S24][S25][S43]

The Berlin authority's notification statistics also show why breach management cannot be reduced to malware counts. The population includes personal-data incidents under a different reporting definition. It should inform notification readiness without being added to national police or listing totals. [S35]

10.6 A reporting rehearsal

Exercise prompt	Required decision	Evidence
Provider reports possible data access	Does the controller have sufficient awareness to start assessment?	Awareness time and legal rationale
Critical service becomes unavailable	Does the sector significance test apply?	Service-impact record and classification
Scope remains uncertain	What can be submitted and updated now?	Staged notice and missing-information list
People face likely high risk	Is direct communication required and accessible?	Approved notice and support route
Incident continues	Which progress or final report is due?	Reporting calendar with responsible owner

Run the exercise with security, legal, data protection, communications and the provider. The pass condition is a documented decision at the required time, including the uncertainty. It is not an unrealistically complete forensic report produced immediately.

KEY TAKEAWAYS

01

Germany's NIS2 implementation is in force; establish entity-specific scope now.

02

Preserve awareness times and assess each reporting framework separately.

03

Management oversight should be demonstrated through owned controls, tested decisions and recorded exceptions.

CHAPTER 11

Outlook and conditional planning

11

THIS CHAPTER ANSWERS

Which preparations follow from the evidence, and what would change the assessment?

6

bounded planning judgements

11.1 Key judgements 84

11.2 Signals that should change the response 85

11.3 Conditional scenarios 85

11.4 What this report cannot project 86

CHAPTER 11

Outlook and conditional planning

IN SHORT

Prepare for extortion, identity misuse, supplier-held data loss and service disruption. These are supported response priorities, not probabilities of a future attack. The listing population provides comparative visibility; the public cases provide mechanisms and consequences. The selected domain observations support validation, with no sector ratings. Assign an owner to the signals below and revise the plan when a relevant signal changes.

11.1 Key judgements

Judgement	Confidence	Basis and limit
Extortion readiness remains a cross-sector priority	High for observed listing visibility	457 German listings across 70 labels; listings are claims [S2]
Leading claimant labels do not cover most observed listings	High for the retained population	Top three hold 161; the other 296 carry different labels [S2]
Identity response should include sessions and privileged grants	High as a defensive implication	Campus disclosure supports identity-focused containment; not a national prevalence estimate [S11]
Customer protection can continue after technical containment	High for documented follow-on patterns	Official patient and booking warnings; no estimate of total losses [S16][S18]
Industrial continuity needs physical verification	High as a planning requirement	Official cooling warning; no common operator inferred [S21]
Domain exposure supports account validation	High for the selected portfolio	Dated device, credential and listing observations; no sector ratings or prevalence claim [S87]

Confidence attaches to each proposition. It is not an assessment of an actor's overall capability. None of the rows predicts an attack date, a national loss amount or a particular organisation's likelihood of being attacked.

11.2 Signals that should change the response

Current boundary	New evidence	Changed decision
Advertisement only	Validated current account or access path	Activate identity or incident containment
Availability incident	Confirmed data access	Add data scoping and notification assessment
Possible industrial access	Independent physical evidence of manipulation	Escalate to the operational safety process
Supplier incident scope uncertain	Reliable affected-data and customer list	Target support and legal communications
Attribution unresolved	A sourced official or technical attribution	Update actor assessment without rewriting the earlier evidence
Changed domain exposure	Validated and dated account or service observations	Reconcile scope and ownership before changing response priorities

11.3 Conditional scenarios

Scenario 1: a current identity is advertised. If validation confirms an active account tied to a critical service, review its privilege, sessions and recent use. The signal is validation against owned systems. The decision is proportionate containment, not a blanket reset based solely on an advertisement.

Scenario 2: a provider reports customer-data access. If the provider supplies credible evidence of affected categories, involve legal and customer operations immediately. The signal is a scoped provider notice. The decision is a timed notification assessment and support plan while technical investigation continues.

Scenario 3: a claimant announces disruption. If monitoring confirms degraded service, activate the continuity and mitigation owners. The signal is the essential task failing, not only the actor's message. The decision is a bounded public status statement and the agreed fallback.

Scenario 4: industrial readings become inconsistent. If an independent measurement shows an unsafe condition, use the approved operational procedure. The signal is physical evidence and the operator's assessment. The decision includes stock protection and safety, rather than an IT-only restoration objective.

Scenario 5: official infection notification arrives. If a trusted authority identifies an owned asset, validate its status and related identities. The signal is a matched asset and supporting evidence. The decision is host remediation, session revocation and a documented investigation, even after infrastructure disruption.

These are planning assumptions. They are not measured response-time intervals, forecasts that an event will occur, or claims that any organisation has implemented the recommended controls.

11.4 What this report cannot project

The observed listing increase over a full-year baseline does not establish a future growth rate. Underground post volume cannot supply an attack probability. Incomplete organisation measurement cannot support a national security score.

Public cases also reflect disclosure choices. A sector with more detailed notices can appear more prominent without having a higher underlying incident rate. Use the cases to test response capabilities and the listing counts to understand visibility, while retaining those limits.

KEY TAKEAWAYS

01

Prepare for mechanisms and consequences supported by the evidence.

02

Assign a signal and decision owner to each scenario.

03

Change the assessment when new evidence resolves an uncertainty, rather than when an actor's rhetoric changes.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

What should teams deliver in the next 90 days, and how will leaders verify it?

20

actions with an owner and completion evidence

12.1 The 30/60/90-day plan 88
12.2 What each role should own 90
12.3 Leadership scorecard 91
12.4 How Brandefense can help 91

CHAPTER 12

Action plan

IN SHORT

Start with alert ownership, account validation, critical-service continuity and reporting scope. Then test supplier notice, identity recovery, customer verification and operational access. By day 90, demonstrate restoration and a combined incident exercise to leadership. These are planning targets. A current material incident should enter the response process immediately, with no wait for the relevant planning period.

12.1 The 30/60/90-day plan

The actions are conditional on the organisation's services and legal scope. Use synthetic data and approved procedures for exercises.

1Days 1–30

Establish a route for identity, supplier and relevant public-claim alerts

OWNER
CISO and threat intelligence

COMPLETION EVIDENCE
Named alert source, owner and escalation test

Validate each relevant identity alert for ownership, freshness, status and privilege

OWNER
Identity and SOC

COMPLETION EVIDENCE
Dated disposition for every received alert

Confirm session revocation and privileged-access review for validated incidents

OWNER
Identity and application teams

COMPLETION EVIDENCE
Revocation evidence and grant review

Identify critical services and their minimum acceptable fallback

OWNER
Business continuity and service owners

COMPLETION EVIDENCE
Service map and approved fallback

Establish BSIG, GDPR and sector-reporting scope and awareness recording

OWNER
Legal, data protection and CISO

COMPLETION EVIDENCE
Obligation register and clock exercise

Approve status wording for claims, outages and possible data access

OWNER
Communications and incident lead

COMPLETION EVIDENCE
Templates with update owner and timing

2Days 31–60

Test incident notice and evidence exchange with a critical provider

OWNER
Supplier management and legal

COMPLETION EVIDENCE
Timed exercise and unresolved items

Test account recovery without relying solely on ordinary email

OWNER
Identity and service desk

COMPLETION EVIDENCE
Synthetic recovery case and audit trail

Review administrative grants, delegated mail access and recovery methods

OWNER
Identity and application owners

COMPLETION EVIDENCE
Reconciled privilege inventory

Review internet-facing remote support and verify applicable updates

OWNER
Infrastructure

COMPLETION EVIDENCE
Version, patch and investigation decisions

Test application authorisation on critical internal functions

OWNER
Application security

COMPLETION EVIDENCE
Approved test record and fixes

Inventory legitimate mail senders and plan controlled DMARC enforcement

OWNER
Messaging

COMPLETION EVIDENCE
Validated sender inventory and change plan

Exercise contracted mitigation and customer-service fallbacks

OWNER
Infrastructure and service owners

COMPLETION EVIDENCE
Minimum user task works during test

Restrict industrial maintenance access under approved procedures

OWNER
OT, facilities and supplier owner

COMPLETION EVIDENCE
Access inventory and revocation test

Verify independent operational alarms and fallback storage where relevant

OWNER
Operations and safety

COMPLETION EVIDENCE
Witnessed alarm and contingency exercise

Publish trusted payment and contact verification routes

OWNER
Customer operations and fraud

COMPLETION EVIDENCE
Public guidance and staff exercise

3Days 61–90

Restore a critical service in an isolated environment

OWNER
Infrastructure and business continuity

COMPLETION EVIDENCE
Restore record against agreed objective

Exercise supplier data loss, claim handling and reporting together

OWNER
Incident lead, legal and communications

COMPLETION EVIDENCE
Timed decisions and staged notices

Review retention and access on sensitive shared document stores

OWNER
Data owners and data protection

COMPLETION EVIDENCE
Retention decisions and access evidence

Present results and owned exceptions to management

OWNER
CISO and management

COMPLETION EVIDENCE
Scorecard with owners and closure dates

12.2 What each role should own

Board and management. Ask which essential function fails first, which provider can trigger that failure and what evidence shows the fallback works. Require a named owner and closure date for each exception. Do not substitute a national threat headline for local completion evidence.

CISO and incident lead. Preserve the evidence type on every claim. Connect security findings to a service owner, legal determination and customer impact assessment. Escalate uncertainty explicitly when the available evidence cannot support a decisive statement.

SOC and identity. Validate relevant accounts and assets, review sessions and grants, and retain the decision trail. Reconcile the record with known remediation so that old exposure is not repeatedly treated as a new event.

Infrastructure and application teams. Verify installed versions and effective permissions, then investigate earlier exposure where appropriate. Demonstrate service restoration through the user's task. Keep recovery dependencies outside the same failure path where the architecture permits it.

OT and facilities. Own physical readings, safe-state decisions and operational fallback. Security supports the access investigation; it should not replace the equipment owner's safety judgement with a generic instruction to disconnect everything.

Fraud and customer operations. Prepare independent verification of messages and payment requests. Explain the limits of deletion claims and avoid asking affected people to disclose additional sensitive material through an unverified channel.

Legal, data protection and communications. Record awareness, risk and reporting determinations. Make public statements specific to what is known. Preserve qualifications when translating or summarising the incident for another audience.

12.3 Leadership scorecard

These are recommended planning targets, not measured control performance in German organisations.

Measure	Target	Evidence
Alert ownership	In place by day 30	Successful routing test
Relevant received alerts	Every alert has a dated disposition by day 30 or an owned exception	Case register
Reporting scope	Recorded by day 30	Entity-specific obligation register
Critical-provider exercise	Completed by day 60	Timed notice and evidence exchange
Privileged recovery	Tested by day 60	Synthetic case and session checks
Minimum service	Demonstrated by day 60	User-journey and fallback record
Restoration	Passed or dated remediation by day 90	Isolated restore test
Management review	Completed by day 90	Signed decisions and exception owners

12.4 How Brandefense can help

Brandefense combines threat intelligence, digital risk protection and external attack-surface management. Relevant use cases include validating identity exposure, monitoring impersonation and tracking external findings through a disposition process. [S44]

Request a demonstration using a representative owned domain and a critical service. Ask how an alert reaches your team, which evidence supports it and what demonstrates closure. A product demonstration does not establish that your organisation has been assessed in this report.

Request a Brandefense demo.

KEY TAKEAWAYS

01

Establish evidence ownership and reporting scope by day 30.

02

Test provider, identity, customer and operational response by day 60.

03

Demonstrate restoration and report owned exceptions to management by day 90.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which populations, dates and limits apply to the report's findings?

Separate

posts, listings, incidents and organisation measurements

Appendix A. Scope and evidence boundaries 94

Appendix B. Evidence register 97

Appendix C. Sources 100

Appendix D. Glossary 105

Appendix A. Scope and evidence boundaries

Comparison countries were selected as examples to provide context only; they do not imply a ranking or political assessment.

A.1 Window and dates

The requested observation window is 1 January–22 November 2026. Underground observations use post publication time. Ransomware observations use listing publication dates where available. Public reporting distinguishes incident, disclosure and update dates where the source provides them.

Research was conducted on 22 November local time. The cut-off day was still in progress during collection. The report therefore does not claim a completed end-of-day census. The recent-activity section covers information available for 8–22 November and includes clearly labelled updates and enforcement announcements.

BSI's annual assessment covers an earlier July-to-June period. Police statistics and data-protection notifications retain their own years and definitions. None is added to the report's listing population. [S3][S4][S35]

A.2 Sources and priority

Own-source populations are underground material from Odin by Brandefense and ransomware listings from Ransompedia. External primary sources include BSI, BfV-related warnings, the Bundestag, police, prosecutors, data-protection authorities and organisational disclosures. Wider reporting supports naming and provides context.

The five-country tables use Ransompedia listing counts. The observed Germany-associated post total and platform/language observations describe publication visibility. Broader content coverage remains incomplete. The dated domain exposure observations retain their own assessed denominator. The distinction is reflected in the relevant chapters rather than hidden in a general disclaimer. [S1][S2]

A.3 Ransomware listings

Ransompedia records 457 German listings within the requested window. The comparator counts are France 295, Netherlands 77, Poland 56 and Austria 61. Listings record criminal claims. They do not establish unique intrusions, encryption, copied data, payment or affected people. [S2]

Prior-year figures describe all of 2025. The current-window and prior-year figures are not matched periods. Comparisons between countries also reflect different economic scale, disclosure and visibility. They are not national risk rankings.

The group-label and monthly tables reconcile to the same German listing total. Industry information describes the listing population. It does not measure sector prevalence. Smaller listing-sector groups are combined in the public chart data.

A.4 Organisation exposure

The snapshot dated 21–22 November 2026 covers 249 of 250 selected domains. It records at least 636,397 device associations, 33,915 employee-device associations and 125,422,358 credential-record associations. In all, 107 observed domains had a credential listed for sale. These are overlapping records, not unique people or confirmed intrusions. [S87]

Legal ownership and independent organisation identity remain unvalidated. Related domains can represent the same operator. One industry-domain record is unavailable. The national Atlas headline for the observed portfolio is 61 out of 100. No sector or organisation ratings are published.

Passive hygiene results remain unavailable as a completed dataset. An unfinished or unobserved measurement is not an absent control. Device, credential, listing, card and incident populations remain separate.

A.5 Card material

The figures describe payment-card records in the retained post corpus. They do not measure national card exposure, card theft or fraud loss.

No personal card data or issuer-level identifier is published. The card population must not be added to credentials, devices or incident counts. The result and its availability are stated in §8.5.

A.6 Incident coverage

The incident register contains documented cases, campaign notices, enforcement, exclusions and unresolved discoveries. Those categories are not a single incident denominator. The report does not claim exhaustive national incident coverage.

Some source pages and late discoveries remain unresolved. Some incidents are never disclosed. A supplier event can affect several organisations, and several updates can concern one event. Absence from this report does not establish absence of an incident.

A.7 Evidence and confidence

Label	Meaning
Observation	A retained record supports the stated measurement or publication
Claim	A source asserts access, impact or possession that is not independently established here
Official confirmation	The organisation or authority confirms the particular proposition stated
Analyst inference	A stated interpretation with a basis and a limit
Analytical model	A planning relationship, without a proven shared operator or transaction chain

High confidence attaches to a reproducible quantity or well-supported proposition. It does not certify an actor's entire assertion. Unverified does not mean fabricated, and a confirmed incident does not confirm every advertised detail.

A.8 Naming, privacy and neutrality

Organisations are named as incident subjects only where official confirmation and wider reporting support the specific case. Other subjects use broad roles. Some source titles and article addresses are withheld to preserve those roles; the supporting passages remain in the private evidence register.

Actors' motives and state associations remain attributed to their sources. The report takes no position on political parties, elections, governments, territory, religion or foreign-policy decisions. No personal identities, criminal contacts, victim access details or sensitive sample records are published.

A.9 Verification limits

Every external proposition used was checked against a supporting passage. The legal table distinguishes commencement, scope and reporting triggers. The vulnerability reference was checked against NVD and the vendor's remediation guidance. It is not evidence of a German exploitation incident. [S33][S34]

Automatic consistency checks do not establish exhaustive coverage or release approval. The English master and German translation retain the same figures, source identifiers, case identifiers and directives. The English edition prevails if the language editions differ.

Appendix B. Evidence register

The case register below identifies what each case establishes. It is not a list of unique national cyberattacks. Card metadata and in-text rows must retain the same limitations.

Case	Date or phase	Sector	Evidence and boundary
A	August; later notices	Public administration	Data copying confirmed; individual impact review continues
B	19 November	Public property	Security incident; possible outflow unresolved
C	6–9 November	Education	Credentials and campus access; no whole-population theft total
D	10 November	Education	Employee records; students and passwords excluded in that notice
E	10–11 November	Education	Separate webmail event; possible credential capture
F	19 September	Education	Registration records; no public-leak conclusion
G	February–March	Healthcare	Intrusion and later patient extortion, one case
H	22 September	Medical technology	Limited internal systems; stated operational exclusions
I	18 November warning	Industrial health supply	Cooling attacks reported; no German blood-bank impact established
J	May	Supplier services	Possible child-data exposure; no verified count
K	July notice	Hospitality	Supplier-held records and later fraudulent messages
L	February	Transport	Booking and information availability disruption
M	17 November	Municipal administration	Unauthorised access; theft still investigated
N	18–20 November	Communications	Attack and service restoration; no theft established
O	15–18 November	Healthcare	One hospital event and recovery phases

Case	Date or phase	Sector	Evidence and boundary
P	13–20 November	Hosting	Infrastructure access; later higher-risk instance update
Q	12 November notice	Social services	Partial IT restrictions; in-person work continues
R	September–November	Political organisation	Earlier access, recent notice; no verified people total
S	8 November post	Banking-related services	Administrator-tenant offer; live access and domestic legal entity unverified
T	16 November post	Cross-sector documents	German-organisation file offer; origin, age and possession unverified
U	2 February post	Project services	Contact/budget database offer; authenticity and acquisition unverified
V	6 October post	Cross-sector documents	Administrative/financial release assertion; files and current access unverified
W	17 February posts	Automotive	Documents and exploit offered; vulnerability and possession unverified; repeat is not another incident
X	5 January post	Identity data	Buyer demand for identities and addresses; no possession evidence
Y	8–17 November	Hospitality supplier	Guest-data access, fraudulent messages and rebuilt-service restart; one supplier incident
Z	8–20 November	Energy services	IT/customer-service disruption; energy supply maintained

B.1 Reading cross-case relationships

An affected institution can appear in more than one case when separate notices describe different events. Conversely, several dates can be phases of a single case. The Tübingen notices are separate; the hospital intrusion and subsequent patient messages are one case.

No cross-case common operator is asserted. Named ransomware labels belong to the listing population, and official campaign warnings retain their geographic limits. A public disclosure is not automatically matched to a criminal listing unless the report explicitly establishes that relationship.

B.2 Post quotations

Card	Case	Post date	Proposition
B01	S	2026-11-08	An advertisement asserts administrator access to a banking-related CRM tenant and describes customer information.
B02	T	2026-11-16	An advertisement offers files said to come from German organisations.
B03	U	2026-02-02	A seller describes project-contact and budget records associated with a German portal.
B04	V	2026-10-06	A post asserts release of administrative, financial and corporate email material from an organisation described as German.
B05	W	2026-02-17	A seller advertises automotive documents and separately an IDOR exploit.
B06	X	2026-01-05	A buyer requests German identity information and emphasises real home addresses.

Appendix C. Sources

Every entry records the supporting-source review date. Some public addresses are shortened to protect role-based subjects. Access limitations are recorded separately; an indexed passage is distinguished from a successful page retrieval.

S1: Odin by Brandefense. Retained Germany underground post evidence. Own-source evidence; no public address. Verified on 22 November 2026.

S2: Ransompedia. Germany and regional-peer ransomware listing aggregates. Own-source evidence; no public address. Verified on 22 November 2026.

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

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

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

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

S9: Berlin data-protection authority. Cyberangriff auf das Landesnetz Berlin. https://www.datenschutz-berlin.de/datenschutz/hinweise-zum-hackerangriff-auf-berlin/ Verified on 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/ Verified on 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 Verified on 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 Verified on 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/ Verified on 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/ Verified on 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 Verified on 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/ (article URL withheld) Verified on 22 November 2026.

S17: LfDI Mecklenburg-Vorpommern. Photo-service supplier incident and possible child-data exposure, 22 May 2026. https://www.datenschutz-mv.de/ (article URL withheld) Verified on 22 November 2026.

S18: LfDI Mecklenburg-Vorpommern. Hotel-software incident and follow-up fraud warning, 29 July 2026. https://www.datenschutz-mv.de/ (article URL withheld) Verified on 22 November 2026.

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

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

S22: State ministry. IT security incident at a state property agency, 19 November 2026. https://mkbwk.rlp.de/ (article URL withheld) Verified on 22 November 2026.

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

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

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

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

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

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

S33: NVD. CVE-2026-1731 record. https://nvd.nist.gov/vuln/detail/CVE-2026-1731 Verified on 22 November 2026.

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

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

S41: CCZ Baden-Württemberg and LKA Baden-Württemberg. Email-account phishing investigation, 19 October 2026. https://generalstaatsanwaltschaft-karlsruhe.justiz-bw.de/ (article URL withheld) Verified on 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 Verified on 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 Verified on 22 November 2026.

S44: Brandefense. Platform and demonstration information. https://brandefense.io/request-a-demo/ Verified on 22 November 2026.

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

S47: BKA and ZIT. Criminal marketplace operation, 8 May 2026. https://www.presseportal.de/blaulicht/pm/7/6271239 Passage verified on 22 November 2026. Direct retrieval: HTTP 200, full statement read on 22 November 2026.

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 Verified on 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 Verified on 22 November 2026.

S50: TechRadar. Defence supplier incident and company statement, 19 November 2026. https://www.techradar.com/ (article URL withheld) Verified on 22 November 2026.

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

S52: Local utility communications provider. Cyber incident and service-restoration notices, 18–20 November 2026. https://www.stadtwerke-wittenberg.de/ (article URL withheld) Verified on 22 November 2026.

S53: County authority. Hospital incident and recovery notices, 15–18 November 2026. https://www.landkreis-greiz.de/ (article URL withheld) Verified on 22 November 2026.

S54: Hosting provider. Infrastructure-access incident, updates through 20 November 2026. https://help.contabo.com/ (article URL withheld) Verified on 22 November 2026.

S55: Municipal authority. Social-service provider communications notice, 12 November 2026. https://www.offenbach.de/ (article URL withheld) Verified on 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 Verified on 22 November 2026.

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

S58: Reservation software supplier. Guest-data access and fraudulent messages; updates 12–17 November 2026. https://reservision.world/ (article URL withheld) Verified on 22 November 2026.

S59: Municipal energy utility. IT incident detected 8 November; updates through 20 November 2026. https://www.stadtwerke-achim.de/ (article URL withheld) Verified on 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 Verified on 22 November 2026.

S61: Professional chamber. Website malware, possible password interception and 23 January 2026 restoration. https://www.aknr.de/ (article URL withheld) Verified on 22 November 2026.

S62: Municipal authority. 16 April ransomware; 20 and 24 April 2026 recovery updates. https://www.sprendlingen-gensingen.de/ (article URL withheld) Verified on 22 November 2026.

S63: Municipal energy utility. 28 June incident and updates through 16 July 2026. https://gsw-kamen.de/ (article URL withheld) Verified on 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/ (article URL withheld) Verified on 22 November 2026.

S65: Research institute. File-server access; notification 25 June 2026. https://www.zois-berlin.de/ (article URL withheld) Verified on 22 November 2026.

S66: Research institute. July network-component incident; updates 17 and 20 August 2026. https://www.idos-research.de/ (article URL withheld) Verified on 22 November 2026.

S67: Memorial foundation. 8 October 2026 notice of renewed website attack, distinct from earlier August incident. https://www.sachsenhausen-sbg.de/ (article URL withheld) Verified on 22 November 2026.

S68: Municipal authority. 15 October 2026 cyberattack and recovery notice. https://www.eichstaett.de/ (article URL withheld) Verified on 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 Verified on 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 Verified on 22 November 2026.

S71: State museum. Incident detected 19 June; personal-data update 31 July 2026. https://www.landesmuseum.de/ (article URL withheld) Verified on 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 Verified on 22 November 2026.

S73: County authority. Preventive shared-system shutdown, 29 September 2026 notice. https://www.kreis-bad-duerkheim.de/ (article URL withheld) Verified on 22 November 2026.

S75: University hospital. External billing-provider incident notice, 22 May 2026; later final scope unresolved. https://www.uksh.de/ (article URL withheld) Verified on 22 November 2026.

S76: Enterprise software vendor. 29 April 2026 malicious development-package versions; vendor mitigation notice. https://community.sap.com/ (article URL withheld) Passage verified in the indexed primary notice on 22 November 2026. Direct article retrieval: HTTP 403.

S77: University. 23 February emergency maintenance; 25 February 2026 notice. https://www.uni-hamburg.de/ (article URL withheld) Verified on 22 November 2026.

S79: LfV Baden-Württemberg. Programmable-controller security warning, 20 August 2026. https://www.verfassungsschutz-bw.de/ (article URL withheld) Verified on 22 November 2026.

S80: Vehicle retailer. Service-provider security notice, published 16 October and updated 29 October 2026. https://www.jepsen-autogruppe.de/ (article URL withheld) Verified on 22 November 2026.

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

S83: University hospital. External billing-provider incident notice, 22 May 2026. https://www.ukbnewsroom.de/ (article URL withheld) Verified on 22 November 2026.

S84: Certification organisation. 27 October 2026 publication acknowledging September IT security incident. https://www.gut-cert.de/ (article URL withheld) Verified on 22 November 2026.

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

S86: Defence technology supplier. Incident statement, 12 November 2026; detection at end of October. https://quantum-systems.com/ (article URL withheld) Verified on 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. Own-source evidence; no public address. Verified on 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 Passage verified on 22 November 2026. Retrieval: full official text read.

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 Passage verified on 22 November 2026. Retrieval: full official page read.

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

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

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

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

Appendix D. Glossary

Term	Plain meaning
Account recovery	The process for restoring legitimate access after loss or restriction
Awareness time	The recorded time at which the relevant entity knows enough to begin an incident assessment
BfV	Germany's federal domestic intelligence authority
BKA	Germany's federal criminal police authority
BSI	Germany's federal information-security authority
BSIG	The German statutory framework for the BSI and relevant information-security duties
CERT-Bund	The federal computer emergency response function within BSI
Combolist	A combined list of email addresses and passwords from different data breaches [S91]
Credential	Information used to authenticate, such as a password or token
CRM tenant	An organisation's separate environment within cloud customer relationship management software [S92][S93]
Data controller	The party determining why and how personal data are processed
Data processor	A party processing personal data for a controller
DDoS	Distributed traffic intended to make a service unavailable
DMARC	Email policy connecting authentication and sender-domain alignment
DORA	EU financial-sector digital operational resilience framework
Extortion listing	A criminal publication asserting a claim about an organisation
Identity session	An authenticated period of access that may need revocation separately from a password
LKA	A state criminal police authority
MFA	Authentication requiring more than one factor
NIS2	EU directive implemented through national information-security duties
OT	Equipment and systems controlling or monitoring physical processes

Term	Plain meaning
Phishing	Deceptive contact intended to induce disclosure or an unsafe action
Ransompedia	Brandefense's ransomware-listing source; listings record claims
Stealer-log material	Records produced by information-stealing malware on infected devices, including login details and associated websites [S90]
Supplier dependency	A function, data store or access path controlled by another organisation
TLP:CLEAR	Information may be shared without restriction, subject to other applicable duties
ZAC (police)	Central police contact points for cybercrime affecting organisations [S89]
ZAC NRW	Zentral- und Ansprechstelle Cybercrime Nordrhein-Westfalen, the prosecution unit at Cologne's General Prosecutor's Office named in [S24]
ZIT / CCZ	Specialist prosecution structures named in the relevant official notices

About this report

Prepared by Odin by Brandefense for security leadership, incident responders, fraud teams, legal and service owners. Version 1.0 uses the requested research window of 1 January–22 November 2026 and a separate recent-activity view for 8–22 November.

Domain ownership and incomplete evidence coverage remain explicit. The German edition is translated from the English master; the English edition prevails where the editions differ.

© 2026 Brandefense. All rights reserved.

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