BRANDEFENSE COUNTRY REPORT · AUSTRIA 2026

Brandefense Austria Cyber Threat Landscape Report 2026

Identity, supplier access and payment trust across connected services

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

250
selected domains in the descriptive portfolio

17
detailed official or source-reported case narratives

61
Austrian ransomware listings in the requested window; criminal claims

1 October 2026
full commencement of Austria's NISG 2026

CONTENTS

Contents

01	Executive summary	05
	Report map	09
02	Austria's digital and threat context	10
03	National exposure: the selected domain portfolio	15
04	Dark-web offers and their evidence boundaries	28
05	Targeting examples by sector	42
06	Hacktivism, DDoS and service availability	60
07	Threat actors and supported relationships	68
08	The fraud economy: identity, context and payment	82
09	Banking deep dive	87
10	Regulatory and national response	92
11	Outlook: conditional planning assumptions	98
12	Action plan	102
	Appendices	108
A	Appendix A. Scope, sources and confidence	109
B	Appendix B. Evidence register	113
C	Appendix C. Sources	116
D	Appendix D. Glossary	119
	About this report	121

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

About this edition

Prepared with AI assistance. Evidence, uncertainty and coverage limits accompany the findings.

Austria's documented campaigns connect account misuse, supplier exposure and payment deception. Defenders should verify each signal, contain confirmed access and preserve the service people need.

34,261

Austria-associated posts across monthly and platform views; not an incident count

61

Austrian ransomware listings across 56 distinct names; criminal claims

49 of 249

observed domains had a credential offered for sale when checked

47 / 100 (B)

national Atlas headline for the observed selected portfolio; 23 November snapshot

Contents and reading routes

Chapter	Question
1 Executive summary	Which decisions deserve priority?
2 Austria's digital and threat context	Which Austrian dependencies change the response?
3 National exposure: the selected domain portfolio	What does the selected portfolio establish?
4 Dark-web offers and their evidence boundaries	What does an observed offer actually mean?
5 Targeting examples by sector	What did organisations and authorities confirm?
6 Hacktivism, DDoS and service availability	How should claims and service impact be separated?
7 Threat actors and supported relationships	Which associations and technical warnings are supported?
8 The fraud economy: identity, context and payment	How can trusted context become a payment instruction?
9 Banking deep dive	Which identity, payment and supplier decisions need coordination?
10 Regulatory and national response	Which scope tests, duties and reporting clocks apply?
11 Outlook: conditional planning assumptions	Which conditional scenarios justify preparation?
12 Action plan	Who acts, and what demonstrates completion?
Appendices A–D	Scope, evidence register, sources and definitions

CHAPTER 01

Executive summary

01

THIS CHAPTER ANSWERS

Which findings justify immediate decisions for Austrian organisations?

4

decisions linking the evidence to practical closure

Four decisions for leaders 07

The year in numbers 07

CHAPTER 01

Executive summary

IN SHORT

Austrian notices describe recruitment lures linked to extortion, phishing from real business mailboxes and payment requests built around credible context. Confirmed disclosures also show that administrative access, document exposure and operational disruption require different evidence. The recent period adds supplier updates and urgent software advisories. Validate relevant accounts, confirm payment changes independently, rehearse supplier recovery and assign reporting decisions before an incident forces them.

This report combines Odin by Brandefense observations, Ransompedia listings, selected-domain observations and source-read public notices. Posts, listings, notifications and confirmed incidents remain separate populations. They are not added into an Austrian attack total. [S1][S2][S3][S6]

The reporting window runs from 1 January through 22 November 2026, using post time for underground material. Linked external sources, NVD records and authority notices were verified on 27 November 2026; each source's verification date appears in Appendix C. Later verification does not extend the incident window. Dated updates in the closing period are distinguished from the incident's start.

1. **Identity validation has consequences beyond a password reset.** CERT.at's July warning describes phishing sent through Austrian companies' real mailboxes. An early-2026 education-sector disclosure separately describes administrative directory access and an account reset. The appropriate response examines sessions, privileges, recovery routes and connected data access. [S10][S25]

2. **A convincing business context does not authorise a payment.** Austrian campaign notices describe recruitment correspondence, invoice changes and messages carrying genuine booking details. These mechanisms use different routes, but all reward an independent confirmation step before an attachment, credential submission or payment. [S9][S11][S12]

3. **Supplier scope determines the customer's next decision.** November disclosures concern hosted infrastructure, accommodation suppliers and an externally operated public-facing service. They do not establish that every customer's systems were entered or that all service functions stopped. Each customer needs a scoped assessment from the relevant supplier. [S28][S29][S56][S57]

4. **Current credential offers require owned-account validation.** Of 249 observed domains, 49 (19.7%) had a credential offered for sale when checked on 23 November. The portfolio records at least 124,110 device associations and 3,900,001 credential-record associations. These overlapping observations are not unique people or confirmed intrusions. The national Atlas headline is 47/100 (B) for this selected portfolio. [S4]

5. **Austria's reporting requirements have distinct scopes and clocks.** NISG 2026 fully took effect on 1 October. DORA has applied since 17 January 2025. Personal-data breach reporting remains a separate determination, and NISG section 44(7) bars a NISG fine for conduct the Datenschutzbehörde has already fined under GDPR. [S30][S36][S38][S40]

Four neighbouring economies provide regional comparative context: Germany, Switzerland, Czechia and Hungary. They share German-language, manufacturing, financial-service and EU cross-border supplier links with Austria. Passive security-control observations cover all 250 selected domains (23–27 November snapshot). Overall, 149 domains (59.6%) publish DMARC enforcement policies, 239 (95.6%) publish SPF and 240 (96.0%) returned valid TLS. [S3]

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

Four decisions for leaders

1. **Own the identity investigation.** Give a named team authority to validate account evidence, review administrative changes and revoke relevant sessions. Close each alert with evidence and a business owner.
2. **Require independent payment confirmation.** Finance should verify changed instructions through a previously established channel. Test whether the process still works when the sender is a real business contact.
3. **Rehearse a supplier incident.** Include the service owner, privacy lead and customer operations. Require a usable fallback and a customer-specific scope decision, rather than treating a provider's restoration message as closure.
4. **Prepare separate reporting decisions.** Legal, privacy and financial compliance should share an event record while recording each applicability test, trigger, deadline and submission receipt independently.

The year in numbers

The following figures retain their original populations and timeframes.

34,261

Observed Austria-associated posts in the requested window (same total in monthly and platform views)

WHAT IT DOES NOT MEASURE

A national incident or unique-victim count

61

Austrian ransomware listings across 56 distinct entity names in the requested window

WHAT IT DOES NOT MEASURE

Confirmed intrusions, unique people or payments

250

Selected domains in this report's portfolio

WHAT IT DOES NOT MEASURE

A verified census of independent Austrian organisations

249 of 250

Selected domains with complete exposure observations

WHAT IT DOES NOT MEASURE

A verified census of independent organisations

49 of 249

Observed domains with a current credential offer (19.7%)

WHAT IT DOES NOT MEASURE

Valid credentials, completed sales or confirmed intrusions

47 / 100 (B)

National Atlas headline for the observed selected portfolio

WHAT IT DOES NOT MEASURE

Attack probability or national prevalence

149 of 250

Selected domains with observed DMARC quarantine or reject policies (59.6%)

WHAT IT DOES NOT MEASURE

Message-level enforcement across every sending service

23

Case dossiers: 6 underground claim cases and 17 official or source-reported cases

WHAT IT DOES NOT MEASURE

A deduplicated national incident count

21,988

Police-recorded narrow cyber-crime cases for 2025 (up from 20,246 in 2024)

WHAT IT DOES NOT MEASURE

Incidents during this report's 2026 window

31,001

Police-recorded internet-fraud cases for 2025

WHAT IT DOES NOT MEASURE

Confirmed organisational intrusions

About 5,000

Reported phishing cases during January–September 2026 (about 7,000 across full-year 2025)

WHAT IT DOES NOT MEASURE

All Austrian phishing attempts or unique victims

About EUR 19 million

Loss associated with that January–September 2026 police phishing account (about EUR 22 million in 2025)

WHAT IT DOES NOT MEASURE

This report's measured cyber-crime loss

1,855

Security breach notifications received by DSB in 2025 (up from 1,319 in 2024)

WHAT IT DOES NOT MEASURE

Confirmed 2026 intrusions or ransomware totals

843

Fraud cases reported to FMA for 2025 (EUR 19.6 million associated loss)

WHAT IT DOES NOT MEASURE

Financial-sector intrusions in 2026 or the police total

Sources: own observations [S1][S2][S3][S4][S6], Bundeskriminalamt [S15][S16], Datenschutzbehörde [S39] and FMA [S41]. These populations overlap in unknown ways. No addition or ratio between them is warranted.

The recent-activity section in §5.7 separates a newly disclosed event, an update, an advisory and a retrospective law-enforcement account. Chapters 3–4 and 7 retain the limits of their own-data populations. Chapter 12 turns those distinctions into work with a clear finish.

KEY TAKEAWAYS

01

Validate identities and sessions before selecting containment.

02

Make payment verification independent of message credibility.

03

Prepare supplier scope, service fallback and reporting ownership together.

Report map

Twelve chapters support five reader paths. Follow the decision you own; the evidence limits apply wherever a finding is reused.

Board and executives	Resource continuity and accountable response	01 05 11 12
CISO and security leads	Validate exposure and supplier dependencies	03 04 05 07
SOC and identity teams	Distinguish claims, access and persistence	04 06 07 B
Fraud and customer teams	Interrupt payment diversion and secondary harm	05 08 09
Legal and communications	Establish scope, clocks and defensible statements	05 06 10 12

Evidence label	Meaning	Reader's next check
Observation	A retained post, listing or measured signal exists	Identify its unit, date and relevance
Claim	A person or criminal label asserts an event or capability	Seek authorised evidence of the underlying assertion
Official confirmation	An organisation or authority confirms the stated facts	Retain the statement's exact scope and remaining uncertainty
Analyst inference	A conclusion or planning decision follows from stated evidence	Review the alternative explanation and change signal

A confirmed incident can still leave the actor, record count or entry route unresolved. A source's attribution remains that source's assessment. The report does not transform an actor's statement into an official account.

CHAPTER 02

Austria's digital and threat context

THIS CHAPTER ANSWERS

Which dependencies make an Austrian incident harder to contain?

3

dependencies connecting the cited cases: identity, suppliers and payments

2.1 Start with the unit and the year 11
2.2 Shared services create several responsibility boundaries 12
2.3 German-language familiarity does not establish trust 12
2.4 An updated national framework changes preparation 13
2.5 Political and international context requires source boundaries 13
2.6 Continuity includes non-malicious failures 13

CHAPTER 02

Austria's digital and threat context

IN SHORT

The Austrian cases cross organisational boundaries through identity services, hosted infrastructure and ordinary business correspondence. National authorities also describe different populations across different years. Treating these as one threat count would obscure the response. Map each critical service to its identity dependency, supplier, data owner and fallback, then establish which authority and reporting route apply.

2.1 Start with the unit and the year

Austria's high connectivity shapes how impersonation and fraud scale. DataReportal's Digital 2026 baseline (published November 2025 from October 2025 data) records 9.11 million residents and 8.69 million internet users (95.3% penetration). It also records 13.5 million cellular mobile connections (148% of population) and 6.98 million active social media user identities (76.6%). Those late-2025 adoption figures provide reach context rather than 2026 incident totals. [S63]

The Bundeskriminalamt's report published in August 2026 describes 2025. Its narrow cybercrime figure increased from 20,246 cases in 2024 to 21,988 in 2025. That retrospective provides context; it does not measure activity through November 2026. [S15]

The same publication records 31,001 internet-fraud cases for 2025. Its categories include conduct beyond attacks on organisations' systems. A change in that category cannot be used as the missing denominator for ransomware listings or exposed credentials. [S15]

The October phishing-prevention notice reports approximately 5,000 phishing cases and EUR 19 million in associated loss during January–September 2026. For comparison across a full year, the same release records roughly 7,000 cases and EUR 22 million in 2025. Those figures span unequal period lengths and reflect police-reported cases rather than all attempted messages or unreported losses. [S16]

In the same October release, the Austrian National Bank (OeNB) notes that roughly 1 in 16,000 payments in Austria is affected by fraud. It cites about EUR 115 million in prior-year payment-fraud losses. It observes that criminals increasingly manipulate people rather than bypass technical payment systems. Separately, the telecommunications regulator RTR-GmbH highlights targeted regulation of alphanumeric SMS sender IDs to curb sender spoofing. [S16]

Austria's Datenschutzbehörde (DSB) supplies a separate privacy-notification baseline. Its 2025 activity report (published March 2026) records 1,855 security breach notifications in 2025, up 40.6% from 1,319 in 2024. The 2025 total comprises 1,704 national GDPR notifications, 48 cross-border notifications, 20 notifications referred through other EU authorities and 83 telecom notifications under section 164 TKG 2021. DSB noted ransomware, booking and payroll software incidents, misdirected correspondence and technical or organisational errors. DSB's public announcement board (20 July–19 November 2026, verified 27 November) lists no interim 2026 breach-notification statistics, leaving the 2025 report as the latest public baseline. [S39][S64]

The practical distinction is whether a number should change prevention, investigation or recovery. Fraud complaints can inform customer-protection preparation. A specific account alert can justify validation. A public extortion listing can justify continuity and disclosure readiness without establishing its underlying claim.

This report uses no single national denominator to combine these observations. In the same window (1 January–22 November 2026), Austria recorded 34,261 country-associated underground posts, including 293 on forums. Neighbouring totals are Germany (1,222,222 total; 2,554 forum), Switzerland (60,135; 887), Czechia (53,067; 420) and Hungary (32,125; 1,885). Raw totals reflect visibility and bulk messaging rather than comparative incident rates or rankings. [S1]

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

2.2 Shared services create several responsibility boundaries

One early-2026 education-sector case concerns a directory with administrative importance. The November supplier cases concern hosted infrastructure and hospitality booking systems. The public-sector disclosure concerns an externally operated website. These are different relationships, despite their shared requirement for a scoped access assessment. [S25][S28][S29][S56][S57]

A useful service record therefore names more than the procurement owner. It should identify the account authority, the system administrator, the data controller and the business function that must continue. Those roles can sit in different organisations.

For example, a supplier can restore infrastructure while a customer still needs to assess information that was accessible there. A central identity service can resume while old sessions remain a separate question. A functioning homepage does not establish that the customer's complete business process works.

These are planning implications, rather than findings that every Austrian organisation uses the same architecture. The service owner should validate the actual dependency before applying a control or accepting a supplier's assurance.

2.3 German-language familiarity does not establish trust

CERT.at's recruitment campaign notice describes correspondence tailored to German-speaking business contexts. The July mailbox campaign uses familiar senders. The August BEC warning describes requests embedded in normal commercial relationships. The credibility comes from context as well as wording. [S9][S10][S12]

The defensive implication is to verify the requested action. A correctly written message can request an unauthorised payment. A genuine mailbox can distribute a deceptive link. A longstanding discussion can acquire an unexpected attachment or instruction.

Train staff to pause at the change: a different payment account, a request to bypass normal approval, a document requiring a new login, or an unusual software installation. The standard should be the action's legitimacy, not a language-quality test.

A caller's accent, a post's language or a seller's chosen alias is not a nationality finding. This report does not infer an operator's location or state sponsorship from those characteristics.

2.4 An updated national framework changes preparation

Austria's new cyber-security authority began operating under the framework described by BMI in its September and October notices. The official legal FAQ states that NISG 2026 fully entered into force on 1 October 2026. [S30] [S49]

The important reader decision is applicability. A large portfolio, a public function or a familiar sector name does not automatically settle statutory status. The law's essential and important entity categories, exclusions and sector rules require a legal-entity assessment. [S31]

The report does not assess the merits of the institutional change or government policy. It uses the published framework to identify current responsibilities and reporting routes. Chapter 10 distinguishes legal facts from the operational preparation recommended here.

2.5 Political and international context requires source boundaries

DSN's report announcement published in May concerns the security picture for 2025. Its discussion of espionage supplies authority context, rather than attribution for every incident subsequently disclosed in Austria. The publication year and observation year must remain visible. [S43]

A public body's involvement does not establish a political motive. A supplier relationship does not establish a supply-chain intrusion technique. A public-sector disclosure reproduced by the press names neither an operator nor a state sponsor. [S29]

This report takes no position on elections, political parties, coalition politics, neutrality policy, international conflicts or government decisions. It omits actor slurs and political slogans. A source's state attribution, where relevant, is identified as that source's assessment.

Security teams should apply the same validation, privacy and continuity standards regardless of political affiliation. Protecting an account or restoring a public service does not require an assessment of the institution's political position.

2.6 Continuity includes non-malicious failures

CERT.at's June account describes a bridge fire interrupting fibre routes and records a formal NIS notification. That is continuity evidence, not evidence of a cyberattack. Physical causes should not be relabelled as malicious because the affected service is digital. [S13]

The broader planning question is whether apparent diversity has a shared dependency. Separate contracts do not establish separate physical routes, identities or administrative planes. A continuity exercise should ask the providers and service owner to demonstrate the distinction that matters.

The exercise result should be recorded at the business-process level. Can staff communicate, issue a service, authorise a payment or support a customer through the fallback? A diagram is useful only when its assumed separation has been checked.

KEY TAKEAWAYS

01

Keep publication year, observation year and evidence unit visible.

02

Map shared identities and suppliers to the business functions they support.

03

Attribute political assessments to sources and test continuity without inventing hostile causes.

CHAPTER 03

National exposure: the selected domain portfolio

THIS CHAPTER ANSWERS

Which organisation-level signals warrant a closer investigation?

250

selected domains in the descriptive portfolio

3.1 Universe card 16
3.2 Sector coverage 16
3.3 Measured exposure signals and the national headline 17
3.4 Passive email and web observations 22
3.5 Turn an external signal into a decision 26
3.6 Measure closure rather than alarm volume 27

CHAPTER 03

National exposure: the selected domain portfolio

IN SHORT

49 of 249 observed domains had a credential offered for sale when checked on 23 November. The portfolio records at least 124,110 device associations and 3,900,001 credential-record associations. Its national Atlas headline is 47/100 (B), not an attack probability. Across all 250 selected domains, 149 (59.6%) publish DMARC enforcement and 240 (96.0%) returned valid TLS. Related services and records can overlap. Validate owned accounts, data age and associated services before disruptive containment.

3.1 Universe card

The portfolio definition determines what its observations can support.

Item	Definition
Selected population	250 purposively selected domains across ten sector groups
Unit	Selected domain and its associated service; not necessarily an independent legal entity
Selection purpose	Descriptive coverage of significant public functions and commercial services
Independence	Related companies, shared operators and institutional services can overlap
Time	Dated observations identify the measured snapshot; they are not automatically 2026 incident counts
National scope	No estimate of Austrian organisation prevalence or national loss

The term organisation is used for readability where a selected service represents an institution. Numerical interpretation remains tied to domains. A parent and subsidiary can have separate domains while sharing accounts, suppliers or records. [S6]

3.2 Sector coverage

The sector table describes the selected portfolio. It is not a sector-risk table.

Sector group	Selected domains	Reader's validation question
Public administration	25	Which citizen or administrative service depends on the selected identity?
Regional and local administration	25	Which shared provider or central service supports local delivery?
Banking and finance	25	Which records describe employees, customers or a financial-service provider?
Universities and research	25	Which central accounts also reach research, teaching or administration?
Industrial manufacturing and construction	25	Which supplier or recruitment route can reach a sensitive workstation?
Consumer manufacturing and technology	25	Which customer or technical service needs a separate scope assessment?
Energy and utilities	25	Which business and operational functions require separate containment?
Transport and logistics	25	Which mailbox, booking or operating service is actually implicated?
Commerce communications and business services	25	Which customer interaction could continue as fraud after restoration?
Health insurance and social services	25	Which fallback preserves care, laboratory or administrative service?
Total	250	Retain the domain unit and the overlapping-entity limit

The sector table describes the selected portfolio. Its counts do not establish national sector size, exposure prevalence or a sector-risk rating. [S6]

3.3 Measured exposure signals and the national headline

49 of 249 observed domains (19.7%) had a credential offered for sale when checked. Complete exposure observations cover 249 of the 250 selected domains on 23 November. One domain has no complete record and is absent from the measured totals; it is not treated as zero. [S4]

The national Atlas headline is 47/100 (B) for the observed portfolio. Higher values indicate greater observed exposure within this portfolio. Only this single national headline is published. No per-sector ratings, per-group ratings or individual domain scores appear anywhere in this report. The result is a descriptive model output, not an attack probability, national prevalence estimate or confirmation of intrusion. [S4]

The following table counts observed domains with each exposure signal. Prior history counts domains with earlier market listing records (899 historical entries across 48 domains). In banking and finance, four domains have a current offer while three have earlier history records, because one domain carries a current offer with zero earlier entries. These columns overlap and should not be added. [S4]

Sector group	Observed	Current offers	Prior history	With devices	With employee devices	With credentials	With documents
Public administration	25	2	2	14	10	19	16
Regional and local administration	25	3	3	20	10	23	16
Banking and finance	25	4	3	21	11	25	12
Universities and research	25	5	5	24	21	25	22
Industrial manufacturing and construction	25	2	2	21	20	24	18
Consumer manufacturing and technology	24	5	5	22	17	24	14
Energy and utilities	25	3	3	24	15	25	13
Transport and logistics	25	6	6	23	16	25	13
Commerce communications and business services	25	17	17	23	17	25	12
Health insurance and social services	25	2	2	22	14	22	11
Total (249 of 250)	249	49	48	214	151	237	147

In `c03_exposure_signals.csv` and `c04_sector_exposure.csv`, column headers such as `orgs`, `orgs_listed_for_sale_now`, `orgs_with_sale_history`, `orgs_with_employee_devices`, `orgs_with_exposed_docs` and `non_employee_devices` count observed domains and device associations rather than verified independent legal entities or confirmed non-employees. Both files retain the domain unit explicit in `c03` metadata. [S4]

Current offers and other exposure signals occur across the observed domain portfolio

	Current offers	Prior history	With devices	Employee devices	With credentials	With documents
Public administration	2/25	2/25	14/25	10/25	19/25	16/25
Regional and local administration	3/25	3/25	20/25	10/25	23/25	16/25
Banking and finance	4/25	3/25	21/25	11/25	25/25	12/25
Universities and research	5/25	5/25	24/25	21/25	25/25	22/25
Industrial manufacturing and construction	2/25	2/25	21/25	20/25	24/25	18/25
Consumer manufacturing and technology	5/24	5/24	22/24	17/24	24/24	14/24
Energy and utilities	3/25	3/25	24/25	15/25	25/25	13/25
Transport and logistics	6/25	6/25	23/25	16/25	25/25	13/25
Commerce communications and business services	17/25	17/25	23/25	17/25	25/25	12/25
Health insurance and social services	2/25	2/25	22/25	14/25	22/25	11/25

Current credential offers by sector (coral). Each cell shows observed domains / assessed domains (24 or 25); signals overlap. Source: Brandefense exposure observations for 249 of 250 selected Austrian domains, 23 November 2026 snapshot (one domain remains unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

The association totals below answer a different question from domain counts. They are cumulative records that can overlap across domains, sources and people. Device role labels do not establish verified employment or unique corporate workstations. [S4]

Sector group	Observed	Devices, at least	Employee devices	Credential records	Documents	Similar names (30d)
Public administration	25	8,683	60	40,818	223	12,263
Regional and local administration	25	3,782	90	47,783	97	5,722
Banking and finance	25	3,728	47	53,514	53	202

Sector group	Observed	Devices, at least	Employee devices	Credential records	Documents	Similar names (30d)
Universities and research	25	9,800	412	343,614	185	14,167
Industrial manufacturing and construction	25	11,386	599	214,905	174	11,402
Consumer manufacturing and technology	24	20,866	485	222,786	120	780
Energy and utilities	25	5,847	111	69,376	64	20,307
Transport and logistics	25	25,246	209	90,420	66	21,599
Commerce communications and business services	25	32,592	4,046	2,755,179	429	11,701
Health insurance and social services	25	2,180	70	61,606	67	1,163
Total (249 of 250)	249	124,110	6,129	3,900,001	1,478	99,306

Device associations extend beyond the employee-related population in every sector



Values show total device associations, at least (employee-related subset in parentheses). Source: Brandefense exposure observations for 249 of 250 selected Austrian domains, 23 November 2026 snapshot (one domain remains unknown) [S4]. Cumulative associations can overlap; they are not unique people or confirmed intrusions.

Five portfolio patterns guide prioritisation across the 249 observed domains [S4]:

- **Employee-related devices are a small subset of total device associations.** The portfolio holds at least 124,110 device associations across 214 domains: 6,129 employee-related (4.9% across 151 domains) and 117,981 other associations (95.1%). Employee-related devices sit inside the device total and must never be added to it. Separately, associated devices hold at least 2,676,495 captured credential lines across all services, not solely the assessed domain. [S4]
- **Combolists and breach databases dominate historical credential records.** Across 237 domains, the 3,900,001 credential records comprise 2,259,831 combolist entries (57.9%), 1,439,520 breach-database records (36.9%) and 200,650 stealer-log lines (5.1%; rounded shares sum to 99.9%). Historical presence does not establish current password validity or recent compromise. [S4]
- **A small number of heavy domains skew sector sums.** Commerce, communications and business services holds 2,755,179 credential records (70.6%) and 4,046 employee-related devices (66.0%). Across the portfolio, two domains account for 60.4% of credential records (top five: 72.1%) and two domains hold 19.1% of device associations. The median observed domain holds 46 device associations and 1,136 credential records, confirming why each organisation needs its own asset triage. [S4]
- **Documents and similar domain names provide triage context.** Across 249 observed domains, 147 carry 1,478 document associations and 206 carry 99,306 similar-name observations (19 October–18 November). Document matches can include public brochures, while short brand strings match unrelated global domains. [S4]

- **Rolling 365-day domain mentions span both dark-chat and Tor venues.** Over 365 days ending 22 November, 44 of 250 selected domains (17.6%) recorded 456 dark-chat mentions. Another 38 domains (15.2%) recorded 241 dark-web (Tor) mentions. Dark-chat mentions led in commerce, communications and business services (8 domains; 215), banking and finance (3; 119) and transport and logistics (3; 30). Dark-web mentions led in universities and research (10 domains; 116) and regional administration (10; 42). Within 1 January–22 November 2026, 23 of 250 domains (9.2%) recorded 221 posts. [S4]

Device, credential, document and current-offer observations form a 23 November snapshot. Similar-name observations cover 19 October–18 November. Rolling message associations cover 365 days ending 22 November, with the 2026 subset stated separately. None is a count of 2026 intrusions. [S4]

A current offer warrants account validation, rather than an assumption that access remains usable. Establish ownership, data age, validity, privileges and relevant sessions. A historical credential for an expired account needs a different response from a current privileged account with suspicious activity.

Documents can be public, historical or duplicated. Similar naming or a domain mention alone does not establish abusive use, breach or common control. Ask the relevant owner to validate the actual service or record before assigning a breach, customer impact or malicious-domain finding.

3.4 Passive email and web observations

Passive checks provide a dated view of externally visible email and web controls. They do not test every sending service, user journey or application. The denominator for each observation must be retained separately. [S3]

DMARC, SPF and DKIM support different parts of email authentication. A monitoring policy is not an enforcement policy. A record's presence does not establish that all legitimate senders are correctly configured or that all recipients reject spoofed messages.

The July trusted-mailbox campaign explains an additional limit. Domain authentication can coexist with deceptive content sent through an account the recipient already knows. Authentication controls and account-response procedures therefore address different parts of the problem. [S10]

A valid TLS certificate indicates a particular secure-transport observation. It does not establish application authorisation, safe customer payment instructions or the absence of unauthorised access. A missing observation should remain unknown until the relevant owner checks it.

The public controls table should be read as a worklist with measured denominators. A service team should explain an unexpected result, identify the affected sending or web service and demonstrate the correction before closing it.

The passive snapshot (completed across 23–27 November 2026) covers all 250 selected domains, with 25 domains in each of the ten sector groups. Positive observations are reported beside their measured denominators without treating an unobserved or unavailable result as an absent control. [S3]

149 of 250

selected domains with DMARC quarantine or reject observed (59.6%)

239 of 250

selected domains with an SPF record observed (95.6%)

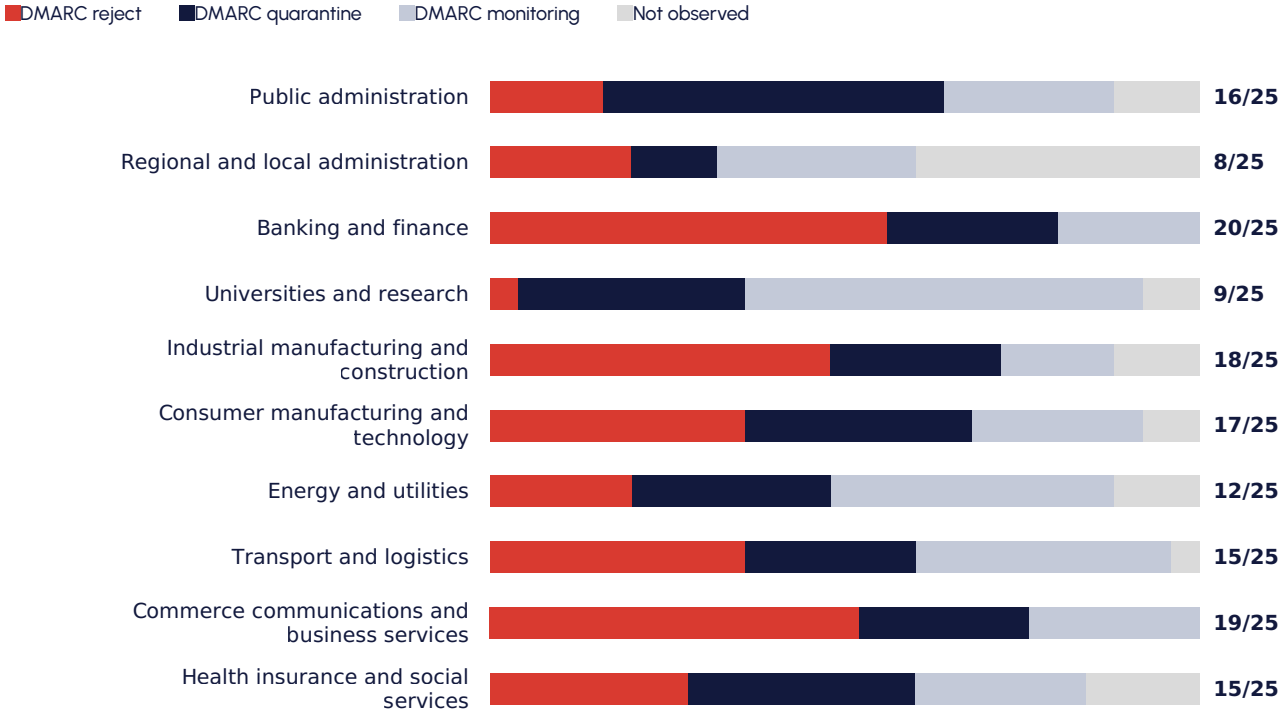
240 of 250

selected domains with a valid TLS observation (6 unsuccessful; 4 unavailable)

184 of 247

domains with a recorded HTTP response carrying HSTS (3 unavailable)

Banking, commerce and industrial domains lead observed DMARC enforcement, while regional administration and universities lag



Right-hand values show enforced (reject or quarantine) / 25 selected domains per sector. Source: passive DNS and email-policy observations for 250 selected Austrian domains, 23-27 November 2026 snapshot [S3]. Published policies do not establish message-level enforcement across every sending service.

Control observation	Domains	Assessed population
DMARC enforcement observed (79 reject; 70 quarantine)	149	250 domains
DMARC monitoring policy observed (`none`)	73	250 domains
DMARC record not observed	28	250 domains
SPF record observed	239	250 domains
DKIM key observed	150	250 domains

Control observation	Domains	Assessed population
DNSSEC delegation record observed	30	250 domains
CAA record observed	48	250 domains
Valid TLS observation	240	250 domains
TLS validation not successful	6	250 domains
TLS observation unavailable	4	250 domains
HSTS observed	184	247 domains with recorded HTTP responses (3 unavailable)

The table below shows per-sector passive counts across all 250 selected domains. No per-sector hygiene rating or ranking is published. [S3]

Sector group	Observed	DMARC reject	DMARC quarantine	DMARC monitoring	DMARC not observed	SPF	DKIM	DNSSEC DS	CAA	Valid TLS	HSTS (of recorded HTTP)
Public administration	25	4	12	6	3	25	5	5	11	25	18 of 25
Regional and local administration	25	5	3	7	10	23	10	4	5	25	17 of 25
Banking and finance	25	14	6	5	0	24	17	5	4	25	23 of 25
Universities and research	25	1	8	14	2	22	14	2	7	23	12 of 24
Industrial manufacturing and construction	25	12	6	4	3	24	20	1	3	23	22 of 25

Sector group	Observed	DMARC reject	DMARC quarantine	DMARC monitoring	DMARC not observed	SPF	DKIM	DNSSEC DS	CAA	Valid TLS	HSTS (of recorded HTTP)
Consumer manufacturing and technology	25	9	8	6	2	25	15	4	7	24	17 of 25
Energy and utilities	25	5	7	10	3	25	17	1	1	23	19 of 24
Transport and logistics	25	9	6	9	1	24	19	1	1	24	19 of 25
Commerce communications and business services	25	13	6	6	0	23	15	6	2	24	20 of 25
Health insurance and social services	25	7	8	6	4	24	18	1	7	24	17 of 24
Total (250 of 250)	250	79	70	73	28	239	150	30	48	240	184 of 247

Three operational patterns stand out from the completed 250-domain snapshot [S3]:

- **DMARC enforcement reaches 149 of 250 domains (59.6%), while 101 domains (40.4%) stay in monitoring or lack an observed policy.** Enforcement comprises 79 reject (31.6%) and 70 quarantine (28.0%) policies, beside 73 monitoring-only (29.2%) and 28 unobserved (11.2%) domains. Banking and finance (20 of 25; 14 reject), commerce, communications and business services (19; 13 reject) and industrial manufacturing (18; 12 reject) show the highest enforcement counts. Regional and local administration (8 of 25, with 10 unobserved and 7 monitoring) and universities and research (9 of 25, with 14 monitoring and 1 reject) show the widest gaps. [S3]

- **SPF is widespread (239 of 250, 95.6%) and observed DKIM keys appear on 150 domains (60.0%), even where DMARC enforcement lags.** Regional and local administration publishes SPF on 23 of 25 domains while only 8 show DMARC enforcement. Universities and research publish SPF on 22 domains and observed DKIM keys on 14, yet 14 stay in DMARC monitoring mode. Energy and utilities publish SPF on all 25 domains and observed DKIM keys on 17, yet 10 remain in monitoring mode and 3 lack an observed DMARC record. [S3]
- **Valid TLS is broad (240 of 250, 96.0%) and HSTS appears on 184 of 247 recorded HTTP responses (74.5%), while DNSSEC and CAA remain concentrated.** Six domains returned unsuccessful TLS validation, and 4 returned no TLS observation. Three domains returned no HTTP response (1 each in universities, energy and health services), leaving 247 recorded HTTP responses for HSTS. DNSSEC delegation records appear on 30 domains (12.0%), led by commerce (6), public administration (5) and banking (5). CAA records appear on 48 domains (19.2%), led by public administration (11), universities (7), consumer technology (7) and health services (7). [S3]

A DNSSEC delegation record is a positive record observation, rather than a full validation of the DNS chain. A DKIM key observation does not establish that every sending workflow signs correctly, and an unobserved DKIM key does not establish that no workflow signs mail. Unavailable TLS or HTTP results remain unknown rather than confirmed misconfigurations. The organisation should verify the relevant service before choosing corrective action.

3.5 Turn an external signal into a decision

The following workflow is a recommended operating model. It is not a claim that every organisation in the portfolio has an incident.

Stage	Accountable owner	Completion evidence
Establish relevance	Asset or identity owner	Domain, tenant and account belong to the organisation or a documented supplier
Establish time	Incident response	Observation date separated from alleged event date and data age
Establish access	Identity and application teams	Privileges, validity, sessions and service reach assessed
Select action	Incident commander and business owner	Containment decision with service consequences and fallback
Assess people	Privacy and customer teams	Data categories, plausible harm and communication decision recorded
Close and review	Control owner	Technical correction verified and residual uncertainty assigned

The first stage prevents unnecessary disruption. A historical credential for an expired account should not receive the same response as a valid privileged account with suspicious access. Both deserve a recorded disposition, but their containment choices differ.

Where a supplier owns the account, the customer still needs its service-specific answer. Ask which tenant, data categories and functions were reachable. A generic statement that infrastructure is restored does not answer whether the customer's information was viewed.

Keep evidence handling inside the authorised investigation. The report does not recommend contacting sellers, buying records or testing credentials against third-party services. Validation should use records and systems the organisation is entitled to examine.

3.6 Measure closure rather than alarm volume

A useful operational metric is the share of relevant alerts with an owner and an evidence-based disposition. Its denominator should be the organisation's own reviewed alert population. This report supplies no national target or claim of measured effectiveness.

For an account issue, closure can include session revocation, removal of an unauthorised rule and review of privileged changes. For an email policy issue, closure can include a verified sending-service inventory and an authentication result for an authorised test message.

Record exceptions explicitly. Some legitimate workflows need a temporary allowance or a staged migration. The owner should state the service impact, review date and compensating control. An unexplained exception is harder to assess during a later incident.

KEY TAKEAWAYS

01

Read the portfolio as selected domains, with possible organisational overlap.

02

Preserve the denominator and unknown outcome for every measurement.

03

Close relevant signals through owned account, service and data assessments.

CHAPTER 04

Dark-web offers and their evidence boundaries

THIS CHAPTER ANSWERS

What does an observed Austrian-related advertisement actually establish?

5

questions before an offer becomes an incident decision

4.1 Universe card 29
4.2 Separate the product from the claim 31
4.3 Read the chronology without inventing an intrusion date 31
4.4 Six claim and demand cases 31
4.5 Credential procurement is also a demand observation 38
4.6 Recent underground activity: 8–22 November 39
4.7 A proportionate validation brief 40
4.8 Close the observation and the customer risk separately 40

CHAPTER 04

Dark-web offers and their evidence boundaries

IN SHORT

An observed post establishes that its content was published. Its assertions about access, records and prices still require validation. Repeated advertising can increase visibility without creating a new incident. A country association can describe a seller's market rather than a verified target. Establish ownership, data age, authenticity, access and operational impact before selecting a response.

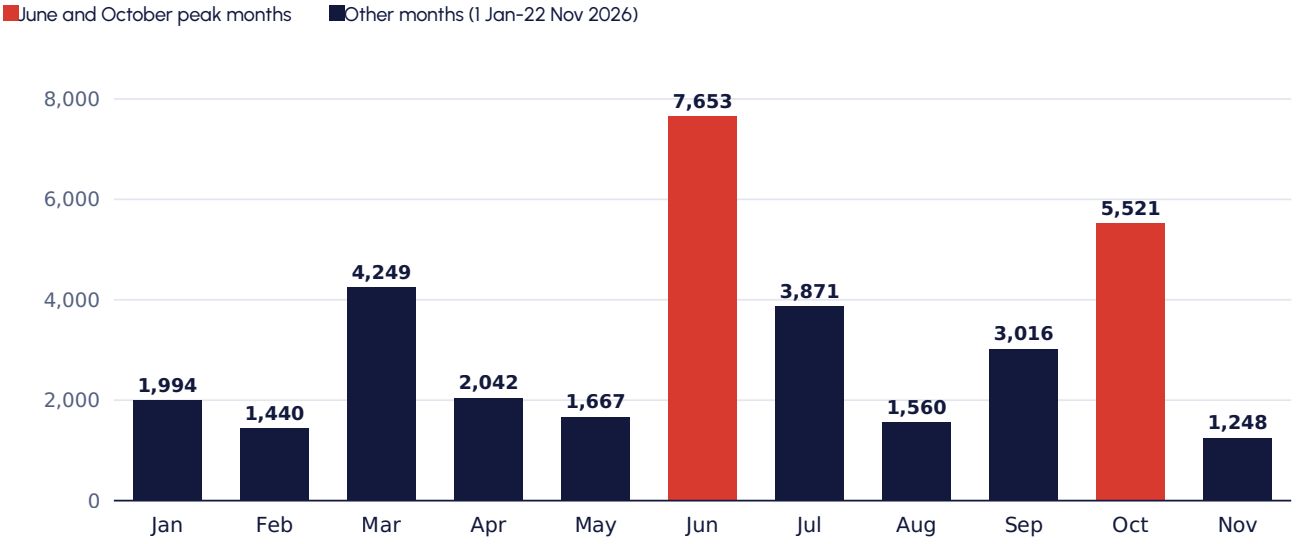
4.1 Universe card

The underground population is defined by its retained observations and dates. It is distinct from public disclosures and Ransompedia listings. [S1][S2]

Item	Meaning
Window	Posts dated 1 January–22 November 2026
Recent activity	Posts dated 8–22 November 2026
Observation unit	Published post; repeated offers do not automatically represent independent incidents
Country association	Content associated with Austria; not verified targeting or nationality
Market assertion	Seller or requester wording; not confirmation of usable access, authenticity or a transaction
Visibility limit	Retained observations do not represent all private exchanges or unpublished incidents

Across 1 January–22 November 2026, Odin by Brandefense recorded 34,261 Austria-associated underground posts across both monthly and platform views. Monthly volume peaked in June (7,653) and October (5,521), while November covers only the partial period through 22 November (1,248). These are message publication counts, not dates or counts of intrusions. [S1]

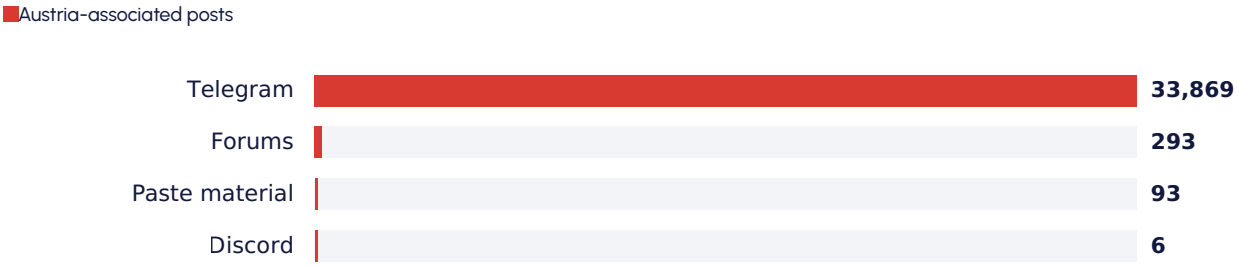
Monthly Austria-associated posts total 34,261, peaking in June and October



Source: Odin by Brandefense, 34,261 Austria-associated underground posts, 1 January-22 November 2026; November partial [S1]. Publication counts are not confirmed incidents.

Within those 34,261 posts, Telegram accounts for 33,869 (98.9%), forums for 293 (0.9%), paste material for 93 (0.3%), Discord for 6 (under 0.1%) and Tor hidden services for 0. High-volume OTC trading and multi-country promotion chats dominate raw Telegram traffic, whereas targeted access offers and data requests concentrate on forums. Neither total counts independent incidents. [S1]

Telegram accounts for 33,869 of 34,261 Austria-associated posts, while targeted offers concentrate on forums



Tor hidden services recorded 0 posts in this breakdown. Source: Odin by Brandefense, 34,261 Austria-associated underground posts, 1 January-22 November 2026; November partial [S1]. Publication counts are not confirmed incidents.

Language tags across the 34,261 posts can overlap when a message contains multiple scripts or languages. Observed tag totals are English (22,049), Russian (11,548), German (939), Chinese (924), Turkish (512), Ukrainian (217) and Arabic (46). A message's language reflects the venue or intended audience; it does not establish an operator's nationality or state sponsorship. [S1]

4.2 Separate the product from the claim

A contact list, a credential offer and administrative access are different propositions. Their response should depend on the specific material described. A large advertised volume does not make the claim more authentic or its records more recent.

A credential offer calls for account ownership, validity and session review. A document claim calls for authorised comparison with the organisation's records and earlier disclosures. An access claim requires evidence of the service, privilege and time involved.

A request to buy information establishes demand, rather than possession. A seller's stated price establishes an asking price, rather than a completed sale or the buyer's willingness to pay. A relayed screenshot establishes a relay, rather than independent verification.

These distinctions also limit actor analysis. Similar descriptions can reflect copied advertising, a shared dataset, a common intermediary or separate people following a familiar template. A shared operator needs a concrete link beyond the similarity itself.

4.3 Read the chronology without inventing an intrusion date

The date of a post is an observation about publication. The material can refer to an older event, previously published information or a service that no longer exists. The first observed post does not establish the date of access or theft.

When similar offers recur, retain the publication sequence while leaving file identity unresolved unless the evidence supports it. A recurring title or volume is insufficient to show that the same file moved between venues.

For a service owner, the useful question is whether the claim changes the current response. Evidence that an account is still valid can change containment. Another copy of a known historical claim can instead justify customer-protection or communications work.

4.4 Six claim and demand cases

The following cases use retained posts, with source wording shown in the associated evidence cards. The dates identify publication, not access or theft. Neither the case selection nor the card count is a national incident total. [S1]

CASE U

U

Demand for contact records and banking identifiers

Evidence card B01 | Evidence card B02 | 8 Jan 2026 | 27 Jan 2026 | Forum | Personal-data demand

Demand observed

OBSERVATION	Two January forum posts request Austrian-related personal contact information; one also requests IBAN information. [S1]
CHRONOLOGY	B01 is dated 8 January and B02 is dated 27 January. Their similar subject does not establish one buyer or a completed transfer.
ESTABLISHED	The retained material supports demand for specified data fields, rather than possession of an authentic database.
ALTERNATIVE	A requested contact list could come from different sources, including older or compiled material; origin is not established here.
LIMIT	An IBAN-related request does not establish control of a bank account, a valid credential or a payment.
RESPONSE	Fraud and privacy owners should assess a relevant record match through authorised evidence and prepare independent verification for identity-based payment requests.

Bottom line

Validate an owned alert; a request does not establish possession or a completed sale.

The decision value is the requested combination of context and identifiers. A financial detail can make a later conversation more convincing without granting authority. The report does not link these requests to the separate police-confirmed fraud campaigns.

Evidence card B01 — 8 Jan 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Hello I am looking for an Austrian database Austrian data Name, Phone Number, Address, Postal Code, Date of Birth

Held

A buyer requests Austrian personal-data fields. The request is evidence of demand.

Not established

Data possession, authenticity, purchase, delivery or a new intrusion.

Evidence card B02 — 27 Jan 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Looking for database leads from Austria and Germany [...] IBAN

Held

A buyer seeks Austrian and German contact records with IBAN information.

Not established

Account access, payment authority, authentic records or a transaction.

CASE V

V

Professional-services access is advertised without verified access

Claim unverified

Evidence card B03 | 1 Feb 2026 | Forum | Professional services

OBSERVATION	A 1 February post advertises access described as Austrian professional services, with a legal-services sector label. [S1]
CHRONOLOGY	The date establishes the advertisement's publication. No access-start, verification or sale date is established.
ESTABLISHED	The retained post exists and asserts access. It does not establish a price or a verified target identity.
ALTERNATIVE	An advertisement can describe stale, limited or unusable access; the organisation and actual privilege remain unresolved.
LIMIT	The technology wording does not establish a vulnerability, exploitation route or connection with a separate product advisory.
RESPONSE	A relevant organisation should validate account ownership, privilege and session evidence before choosing containment, with the service owner assessing business impact.

Bottom line

Confirm account ownership, privileges and recent access before choosing containment.

The receiving team should identify the relevant account and service privately. No victim name or working access route is published here. The advertisement does not establish a transaction.

Evidence card B03 — 1 Feb 2026

[alias withheld] | Forum | Forum | Russian and English

ORIGINAL

Доступ Austria [...] Law Firms & Legal Services forti domain user

TRANSLATION

Access Austria [...] Law Firms & Legal Services forti domain user

Held

An advertisement describes Austrian professional-services access. No sale price is established.

Not established

Usable access, victim identity, a sale price, vulnerability or completed sale.

CASE W

W

A directory-style offer does not establish an intrusion

Evidence card B04 | 2 Feb 2026 | Forum | Directory data

Origin unverified

OBSERVATION	A 2 February advertisement describes a regional directory dataset and says it contains 21 attributes. [S1]
CHRONOLOGY	The publication date does not establish when the records were collected or whether they were previously public.
ESTABLISHED	The advertisement names contact-related fields and describes email addresses as verified; that verification remains the seller's assertion.
ALTERNATIVE	Public-directory compilation, older commercial leads or reused material could produce similar descriptions without a new intrusion.
LIMIT	File authenticity, record origins, freshness, permissions and the advertised attributes were not independently validated.
RESPONSE	A relevant data owner should compare authorised examples with public and previously disclosed records, then assess plausible misuse before describing an incident.

Bottom line

Compare the fields with public directories and authorised records before calling this a new intrusion.

A directory theme can matter for impersonation even when no intrusion is established. The organisation should assess the actual information and credible use case. It should not equate a field count with a count of affected people.

Evidence card B04 — 2 Feb 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

The set includes 21 attributes, specifically titles, physical addresses, telephone numbers, and verified email addresses.

Held

A seller describes a directory-style dataset with 21 attributes. The word verified is the seller's description.

Not established

Freshness, lawful origin, accuracy, a new intrusion or an affected-person count.

CASE X

Financial-interest leads include an older date signal

Evidence card B06 | 18 Apr 2026 | Forum | Financial marketing

Claim unverified

OBSERVATION	An 18 April post advertises Austria-labelled forex and cryptocurrency leads, claiming 13,967 rows. [S1]
CHRONOLOGY	Material shown with the claim contains a 2024 date signal. Publication in 2026 therefore does not establish new 2026 theft.
ESTABLISHED	The retained post asserts the country label and row quantity; neither establishes distinct people or authentic records.
ALTERNATIVE	Older lead material, compilation and repeated advertising remain plausible explanations for the description.
LIMIT	No current account access, completed sale, investment loss or cause of a subsequent fraud is established.
RESPONSE	Fraud teams should treat a relevant match as context for targeted deception, while validating data age and authenticity through authorised records.

Bottom line

Preserve the claimed date and record unit; do not equate rows with people or new theft.

The comparison with official investment-fraud reporting is functional, rather than a demonstrated supply chain. Contact information can support a convincing approach, but the report has no evidence that this advertiser supplied the investigated call centres. [S19]

Evidence card B06 — 18 Apr 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Country :Austria Quantity :13967

Held

A post advertises 13,967 Austria-labelled forex or cryptocurrency leads.

Not established

Distinct people, new theft, authentic records or completed fraud.

CASE Y

Y

Household-contact demand describes an audience, not an actor's nationality

Evidence card B07 | Evidence card B08 | 22 Sep 2026 | 15 Oct 2026 | Forum | Household contacts

Demand observed

OBSERVATION	September and October requests seek household telephone contacts; one specifies Russian-speaking people aged 45 and older. [S1]
CHRONOLOGY	B07 is dated 22 September and B08 is dated 15 October. Repeated subject matter does not establish a shared operator.
ESTABLISHED	The posts show requested audience characteristics, rather than possession of a list or completed contact with those people.
ALTERNATIVE	Demographic and language criteria can reflect a buyer's intended audience without identifying the data source or proposed use.
LIMIT	Russian-language preference establishes neither nationality, state sponsorship nor a connection with Russia-related political activity.
RESPONSE	Customer-protection teams should offer an independently verifiable support route and assess relevant suspected misuse without treating the audience as culpable.

Bottom line

Prepare accessible fraud warnings without inferring actor nationality from the requested language.

The report does not infer a measured fraud rate for that age or language group. A requested audience is a demand observation. Any allegation about a specific campaign would require separate communication, payment and victim evidence.

Evidence card B07 — 22 Sep 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Priority is given to home phone numbers (from phone directories) Is there such a database?

Held

A buyer prioritises household telephone contacts drawn from directories.

Not established

Possession of a database, a completed purchase or subsequent fraud.

Evidence card B08 — 15 Oct 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

Home phone numbers of RUSSIAN-speaking individuals aged 45+

Held

A buyer specifies older Russian-speaking contacts as an intended audience.

Not established

Actor nationality, state direction, possession of records or completed fraud.

Z

CASE Z

A repeated phishing-panel advertisement asserts authentication support

Evidence card B09 | Evidence card B10 | 20 Nov 2026 | 22 Nov 2026 | Forum | Customer-facing finance

Claim unverified

OBSERVATION	Posts dated 20 and 22 November advertise a phishing panel. They assert support involving one-time passwords (OTP), transaction authentication numbers (TAN), two-factor authentication, QR codes and PhotoTAN. [S1]
CHRONOLOGY	The later post repeats the advertised product and names Austria among several countries; it is not a second demonstrated intrusion.
ESTABLISHED	The retained material establishes advertised capabilities and claimed market coverage.
ALTERNATIVE	A product description can exaggerate functionality or refer to an untested service; advertising alone does not establish efficacy.
LIMIT	No successful authentication bypass, banking-system access, victim count or completed sale is demonstrated.
RESPONSE	Identity and fraud owners should review the actual customer journey and trusted confirmation routes, then validate any account-specific evidence before selecting containment.

Bottom line

Review customer deception and transaction safeguards; an advertisement is not a demonstrated authentication bypass.

A statement that a kit supports an authentication method is not evidence that every implementation of that method fails. The defensive review should consider the real service, user action and available telemetry. It should not adopt the seller's claim as a tested result.

Evidence card B09 — 20 Nov 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

OTP/TAN/2FA support including QR Codes and PhotoTAN method.

Held
A phishing-panel advertisement claims OTP, TAN, QR and PhotoTAN support.

Not established
Demonstrated efficacy, successful authentication evasion or access to bank systems.

Evidence card B10 — 22 Nov 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

The kit targets multiple countries, including Ireland, the Netherlands, Finland, Austria, Germany, France, Belgium, Greece, Luxembourg, and Italy.

Held
A later advertisement again includes Austria among several intended markets.

Not established
A second intrusion, common operators, sales, functioning software or bank-system access.

4.5 Credential procurement is also a demand observation

A separate 11 April post seeks continuing suppliers associated with Germany, Austria and Switzerland. The retained excerpt supports procurement interest. It does not establish a delivery, tested credentials or an agreed commercial relationship. [S1]

The defensive implication is conditional: if a relevant credential appears, validate the owned account and its history. A general request is not sufficient grounds for broad resets or a claim that the advertised countries' organisations were entered.

Evidence card B05 — 11 Apr 2026

[alias withheld] | Forum | Forum | English

ORIGINAL

We are seeking suppliers from Germany, Austria, and Switzerland.

Held
A post seeks regular suppliers with Austria among the listed markets.

Not established
Possession of credentials, usable accounts, delivery or a completed transaction.

A separate advertisement asserts remote-desktop web access associated with a telecommunications provider and claims administrative privileges. Its exact publication date is uncertain within the reporting window and is out-
side the recent period. No current access, affected data, transaction or link to an official incident is established. [S1]

Evidence card B19 2026 (date unresolved)

[alias withheld] Forum Forum English

ORIGINAL

RDWeb access to Telecommunications company in Austria. Cloud Admin (Owner) privileges

Note. Publication date unresolved within the window; outside the recent period.

Held
An advertisement asserts RDWeb access and cloud owner privileges at an Austria-related telecommunications organisation.

Not established
Usable access, the target identity, current privilege, a completed sale or a resolved publication date.

4.6 Recent underground activity: 8–22 November

The 20 and 22 November panel advertisements belong in the closing-period view because of their publication dates. Their repeated appearance establishes continued promotion, rather than a measured increase in successful attacks. [S1]

An 18 November advertisement also describes contact data and displays a quantity of "115k". That is an unverified advertised quantity, rather than a confirmed number of records or distinct people. Origin, data age, accuracy and any completed transaction remain unresolved. [S1]

Evidence card B20 18 Nov 2026

[alias withheld] Chat message Telegram English

ORIGINAL

People DB
Qty: 115k

Held
A message advertises an Austria-associated contact dataset with a claimed quantity of 115,000. The quantity is unverified.

Not established
Authentic files, unique people, freshness, new theft or an intrusion into any organisation.

A place or business reference in sample context does not establish access to any organisation. The report does not connect this advertisement to the separately disclosed official incidents.

The official November advisories and the panel's advertised capabilities remain separate evidence. Shared timing does not show that the seller used a named vulnerability, supplied an official-case operator or caused a bank incident.

Route any matching service or account observation to its owner. Keep the advertised product claim, the actual access evidence and the customer's payment event as separate propositions until a concrete link supports joining them.

4.7 A proportionate validation brief

An escalation brief should tell the receiving team what decision the observation could change. It should preserve the claim's uncertainty and avoid circulating personal records more widely than necessary.

Question	Evidence sought	Decision supported
Is it relevant?	Authorised match to domain, tenant, record or account	Assign the correct owner
Is it current?	Data age, account state and previous remediation	Select urgency and scope
Is it authentic?	Comparison with records the organisation may lawfully examine	Confirm or reject the material's relevance
Was access used?	Access, session and application evidence	Choose containment and investigation
Who could be harmed?	Confirmed data categories and credible misuse	Make privacy and customer-protection decisions

Do not instruct a team to acquire criminal material or test a third party's account as the first verification step. Work from authorised records, existing evidence and a documented chain of responsibility. Escalate uncertainty rather than treating it as an assurance.

4.8 Close the observation and the customer risk separately

An account investigation can close while a person still faces impersonation using information already disclosed. Conversely, a suspicious message can be fraudulent without showing that its recipient's organisation lost information.

Record those outcomes independently. The technical owner should state the access findings. The customer or privacy owner should state the plausible harm and advice. Communications should describe the confirmed result without adopting a seller's broader narrative.

KEY TAKEAWAYS

01

A published offer and its underlying assertion are separate propositions.

02

Use post dates as publication dates, with data age assessed independently.

03

Route validation and customer-protection work to accountable owners.

CHAPTER 05

Targeting examples by sector

THIS CHAPTER ANSWERS

What do source-read Austrian cases establish about access, impact and response?

17

detailed official or source-reported case narratives

5.1 Read the cases through their evidence boundaries 43
5.2 Identity and institutional recovery 44
5.3 Trust-based fraud affecting customers and staff 46
5.4 Supplier and commercial correspondence 48
5.5 Later-year commercial and hosted-service incidents 52
5.6 Additional official notices and explicit exclusions 57
5.7 Recent activity: 8–22 November 2026 57

CHAPTER 05

Targeting examples by sector

IN SHORT

The public cases span identity access, recruitment lures, customer-directed fraud and hosted-service incidents. Their confirmation levels differ. Campaign notices can establish Austrian activity without supplying a victim count. An organisation's statement can confirm a narrow data event while leaving attribution unresolved. Use the cases to test the matching business process, and preserve each source's scope in your own response.

5.1 Read the cases through their evidence boundaries

These case narratives are selected for their response value. They are not a disjoint national incident census. A campaign notice can describe several events, while a later update can revisit a case already reported. A preliminary authority statement confirming an investigation does not establish confirmed intrusion or customer impact.

Sector or function	Observed issue	Evidence boundary	Response focus
Education	Administrative directory access; bounded ransomware scope	Source-confirmed notices; unresolved full data scope retained	Identity recovery, isolation and scoped review
Industry and recruitment	Extended recruiter correspondence and malicious archive	CERT confirms Austrian cases; no public total	Contact-form, mail and endpoint investigation
Construction-related SMEs	Phishing from real business mailboxes	CERT campaign warning; scope not quantified	Sessions, connected access and partner warning
Service operators	Historical mailbox documents online	Spokesperson's narrow confirmation differs from wider claim	Mailbox and document scope
Hospitality and hosted services	Booking-context deception and supplier-hosted systems	Separate campaign and incident populations	Payment verification and supplier scope
Public administration	Staff business contacts or widened data-category scope	Official accounts reproduced in press; actor not named	Supplier access, privacy updates and impersonation preparation
Banking customers	SMS, fake telephone support and payment manipulation	Customer-directed fraud; bank-system intrusion not established	Independent contact and transaction response

The case letters identify narratives. They are not a confidence scale. Every action below is a proportionate recommendation for an organisation facing comparable evidence.

5.2 Identity and institutional recovery

A

CASE A

Administrative access requires a scoped recovery decision (O01)

Education

Official notice

OBSERVATION	An Austrian education institution confirmed administrative directory access and an account reset in early 2026. [S25]
CHRONOLOGY	The institution detected the incident, dated the access to shortly before detection, carried out an account reset and published a concluding update several weeks later.
ESTABLISHED	Its concluding account found no indications of extensive access or corruption, while not excluding some data access.
ALTERNATIVE	Administrative reach and categories that were accessible do not establish wholesale extraction.
LIMIT	The public statement does not settle every account's exposure or assign an actor in this report.
RESPONSE	Validate administrative changes, restore accounts through trusted recovery routes and record which data-access questions remain open.

Bottom line

Validate administrative changes and trusted recovery before closing the incident.

The transferable decision concerns how identity recovery is authorised. A reset can inconvenience many legitimate users, so the organisation needs capacity for exceptions and people who cannot use the normal route. Recovery verification should not rely on a message sent through the affected account.

Staff handling exceptions should know which evidence they may request and how to escalate uncertainty. The incident record should distinguish an account restored for legitimate use from an account whose historical activity has been fully reviewed.

CASE B

B

An education institution's notice clarifies ransomware scope (O02)

Education

Primary notice

OBSERVATION	An education institution's early-2026 notice confirms a ransomware incident in a bounded area of its IT environment. [S58]
CHRONOLOGY	Initial containment and restoration preceded the institution's formal notice describing the personal-data scope used here.
ESTABLISHED	The institution describes unauthorised account and network access and personal information from some user accounts taken, with the exact information scope unresolved.
ALTERNATIVE	A bounded system description and continued teaching do not establish that no personal information was accessed.
LIMIT	The primary notice retains uncertainty about server access and full data scope. It names no responsible actor.
RESPONSE	Validate affected identities, isolate and verify restoration, and assess personal-data scope before describing the recovery as complete.

Bottom line

Validate identities and restoration while retaining the primary statement on personal-data scope.

The formal primary statement governs this narrative's scope rather than earlier narrow reassurances. No claimant's label is adopted as the officially established operator. The incident's teaching and data-protection consequences remain separate questions.

5.3 Trust-based fraud affecting customers and staff

CASE C

C

A bank-themed SMS becomes a telephone payment instruction (O03)

Official warning

Banking customers

OBSERVATION	On 1 April, Bundeskriminalamt warned of mass SMS to Austrian numbers using a German bank's identity. [S18]
CHRONOLOGY	The message led recipients to a false telephone support route, followed by a deceptive bank page and a requested transfer.
ESTABLISHED	Police reported actual losses in an approximate high double-digit victim population.
ALTERNATIVE	The customer deception does not establish access to the imitated bank's systems.
LIMIT	Approximate police descriptions do not justify an exact victim or national loss figure.
RESPONSE	Reject instructions to move money to a supposed safe account and contact the bank through an established channel.

Bottom line

Use an established bank contact and assess the actual transaction.

A fraud team should rehearse the point at which a worried customer believes the caller is protecting them. A technically valid payment approval can still reflect deception. The escalation process should allow staff to pause, explain the pretext and contact the customer safely.

CASE D

D

An identity-renewal pretext extends into device and bank access (O04)

Official warning

Customer identity

OBSERVATION	Bundeskriminalamt's 7 April notice describes digital-identity certificate-renewal messages followed by deceptive support contact. [S17]
CHRONOLOGY	The scenario moves from an unsolicited SMS to bank impersonation and a request to install remote-support software.

ESTABLISHED	The warning concerns a real fraud campaign; certificates approaching expiry supply the pretext, rather than an affected-account total.
ALTERNATIVE	A message naming an identity service does not show that the identity service itself was entered.
LIMIT	October's later discussion revisits this spring cohort and must not be counted as a separate campaign. [S16]
RESPONSE	Verify renewal through the known official service and refuse unsolicited device-control or bank-support instructions.

Bottom line

Start renewal independently and refuse unsolicited remote control.

This is a cross-channel response problem. A person can leave the original message and continue the deception by telephone. A warning focused only on malicious links can miss the later request for remote control or an authorised payment.

CASE E

E

Investment fraud continues through a false recovery offer (O05)

Police release

Financial customers

OBSERVATION	An April police investigation describes manipulated public-figure content, false investment platforms and later recovery-fee requests. [S19]
CHRONOLOGY	The published account followed coordinated action on 17 April against call-centre infrastructure and residences.
ESTABLISHED	The official account describes a cross-border investigation, including Austrian victims and more than one fraud stage.
ALTERNATIVE	An apparent endorsement, displayed investment balance or promised recovery is not independent validation of an investment.
LIMIT	Its investigation-wide loss estimate is not an Austria-only or 2026-only national loss figure.
RESPONSE	Verify authorisation independently, restrict unsolicited remote control and warn affected customers that recovery approaches can be another fraud stage.

Bottom line

Verify authorisation and protect against further recovery-fee approaches.

A customer-support script should avoid blame. Someone already deceived can be particularly receptive to a person claiming to resolve the loss. Keep the protective action concrete: use a known bank contact, preserve relevant communications and evaluate further requests independently.

5.4 Supplier and commercial correspondence

F

CASE F

A recruitment conversation precedes extortion-related access (O06)

Industry and recruitment

CERT assessment

OBSERVATION	CERT.at's May ZipLine notice says it has confirmed Austrian cases and indications of access being acquired for Qilin operations. [S9]
CHRONOLOGY	The described recruiter approach begins through public contact forms and develops over days or weeks before an archive arrives.
ESTABLISHED	CERT.at links its campaign assessment to Austrian observations; it does not publish a complete Austrian victim count.
ALTERNATIVE	Ordinary recruiter contact is legitimate; the later action and supporting evidence determine the investigation.
LIMIT	The source's access relationship does not establish that every recruiter lure or Qilin listing used the same route.
RESPONSE	Review relevant correspondence, attachment handling and endpoint evidence, then contain confirmed access rather than blocking business communication indiscriminately.

Bottom line

Review relevant correspondence and endpoint evidence before selecting containment.

Procurement, reception and recruitment staff can be the first people to see the approach. Their escalation route should reach security without requiring them to diagnose malware. The report does not reproduce the campaign's lure domains or a procedure for reproducing the attack.

G

CASE G

Old documents online do not establish a wider operational incident (O07)

Service operator

Press report

OBSERVATION

Press reporting in 2026 quotes an Austrian organisation's spokesperson acknowledging older documents taken from one mailbox. [S26]

CHRONOLOGY	The reporting concerns documents dating from 2025, rather than establishing a new intrusion date for every document.
ESTABLISHED	The spokesperson's account is narrower than the criminal narrative and denies a wider operational-system event under the information then available.
ALTERNATIVE	Document exposure and continuing service can coexist; one does not negate the other.
LIMIT	The report does not validate the claimant's total volume, complete data scope or actor identity.
RESPONSE	Investigate the mailbox and document set while separately validating customer and operational service impact.

Bottom line

Scope the mailbox and assess operational impact separately.

A communications team should avoid a single yes-or-no phrase that collapses the two accounts. It can acknowledge the document finding, state the tested service boundaries and identify the next review point. That is more useful than repeating an unverified claim timeline or volume.

H

CASE H

A familiar sender distributes another credential lure (O08)

Business services

Official warning

OBSERVATION	CERT.at's 24 July warning describes phishing through real Austrian business mailboxes, especially among construction-related SMEs. [S10]
CHRONOLOGY	The stated pattern uses a document-viewing lure, captures account credentials and sends further messages to known contacts.
ESTABLISHED	The source reports an unusual increase in that campaign pattern; it gives no national victim total.
ALTERNATIVE	Domain authentication or a familiar sender does not establish that the requested login is authorised.
LIMIT	The warning does not identify every connected service or confirm that each recipient entered credentials.

RESPONSE	Reset affected accounts, end relevant sessions, review connected access and warn business contacts through a trusted route.

Bottom line

Review sessions and connected access, then warn partners safely.

The partner warning should explain the action that was unsafe. It should not ask recipients to reply to the suspect conversation for reassurance. Security and business owners should agree which contacts need a warning and how they can verify its authenticity.

CASE I

Correct booking details do not validate a payment demand (O09)

Official warning

Tourism customers

OBSERVATION	CERT.at's 14 August notice describes fraud using credible travel-booking information and deceptive payment requests. [S11]
CHRONOLOGY	A person receives a request after a real booking, or encounters a false listing or imitation support route.
ESTABLISHED	The notice distinguishes several mechanisms; it does not attribute them to one data event or operator.
ALTERNATIVE	Correct details can reflect account misuse or other information exposure without a platform-wide incident.
LIMIT	The warning supplies no Austrian count of stolen bookings or successful payment diversions.
RESPONSE	Confirm unexpected payment requests independently and give guests a known route to verify the real payment process.

Bottom line

Confirm the requested payment through a known independent route.

Hospitality teams should prepare for the guest who already sees real booking details in the message. A general instruction to look for spelling mistakes is insufficient. The practical question is whether the requested payment matches the established process for that booking.

CASE J

J

A business conversation acquires an unauthorised payment change (O10)

Official warning

Cross-sector business

OBSERVATION	CERT.at's 26 August BEC notice reports increased attempts involving Austrian organisations. [S12]
CHRONOLOGY	Its scenarios include executive impersonation, changed supplier instructions, misuse of an existing mail discussion and requests for employee data.
ESTABLISHED	The source describes a family of deception scenarios, rather than one uniform technical attack.
ALTERNATIVE	Some cases can use a genuine mailbox; others can use impersonation without access to the imitated organisation.
LIMIT	A suspicious invoice does not alone establish which mailbox, if any, was accessed.
RESPONSE	Confirm changed instructions through a previously held contact and separate payment approval from execution.

Bottom line

Confirm changed instructions independently and separate payment approval from execution.

The second approval should test independent evidence, rather than ask a colleague to read the same convincing email. Where an invoice is genuine but its bank details changed, finance needs the supplier's trusted confirmation and security needs the related mail evidence.

5.5 Later-year commercial and hosted-service incidents

CASE K

K

Apparent online work becomes a sequence of deposits (O11)

Consumer fraud

Official warning

OBSERVATION	Bundeskriminalamt's 29 October warning describes social-media job offers followed by tasks and payment requests. [S20]
CHRONOLOGY	Contact moves through messaging services; initial small payouts precede larger deposits and supposed higher-status or repair tasks.
ESTABLISHED	Police describe Austrian losses, using an approximate low single-digit-million range.
ALTERNATIVE	An initial payment to the participant does not establish a legitimate employer or guarantee future withdrawal.
LIMIT	The warning provides no exact national victim count or link to this report's underground sellers.
RESPONSE	Reject demands to pay for work or release earnings, preserve the conversation and contact the payment provider promptly after a suspected loss.

Bottom line

Stop further deposits and contact the payment provider when fraud is suspected.

An organisation's relevance can be customer protection rather than an internal intrusion. Banks and consumer-facing services should recognise a repeated-deposit explanation and provide a safe escalation route. The presence of an app or group with many participants does not settle legitimacy.

CASE L

L

A project organisation's data incident leaves operational continuity separate (O12)

Project-based industry

Press report

OBSERVATION	Autumn press reporting describes a company-confirmed cyber incident at an Austrian organisation with project operations. [S27]
CHRONOLOGY	The incident occurred during autumn 2026; subsequent November updates do not create a second incident.

ESTABLISHED	The company account distinguishes the information-system event from continuing project activity.
ALTERNATIVE	A claimant's account can exceed what the organisation confirms.
LIMIT	This report does not assign the extortion claimant's identity as an independently established operator.
RESPONSE	Assess affected business records and recovery while separately verifying project operations and critical supplier access.

Bottom line

Assess records and project operations through separate owners.

The service owner should ask which functions were tested when describing continuity. A project can continue while administrative data, correspondence or a supplier relationship remains under investigation. Restoration and the privacy assessment need separate completion records.

M

CASE M

Hosting-infrastructure access requires customer-specific scope (O13)

Software and hosting supplier

Supplier notice

OBSERVATION	A commercial software and hosting supplier reported unauthorised access to part of its hosted infrastructure in November 2026. [S28]
CHRONOLOGY	Its account says authorities and customers were informed promptly after detection, followed by mid-November updates.
ESTABLISHED	The supplier states that online systems remained available and reports no known alteration, deletion or encryption.
ALTERNATIVE	Continuing operation and an absence of known alteration do not establish that no data was viewed.
LIMIT	Its statement says the actor and motive remain unknown while distinguishing its service scope from unrelated software advisories and separate customer-booking workflows.
RESPONSE	Obtain a scoped supplier assessment and maintain customer-protection monitoring without inventing a link to unrelated advisories or fraud.

Bottom line

Obtain customer-specific scope without inventing a link to unrelated advisories or fraud.

A supplier's statement about which data types it processes is critical. Sector proximity alone does not justify assuming that every customer dataset was exposed. Each customer should verify its actual data categories and functions before issuing downstream warnings.

CASE N

N Staff contact viewing through an externally operated website (O14)

Public administration

Press report

OBSERVATION	November press reporting reproduced an Austrian public body's statement about unauthorised viewing of staff business contacts. [S29]
CHRONOLOGY	The reproduced statement describes brief access in November that was detected and interrupted promptly.
ESTABLISHED	The described website was externally operated. The stated records concerned staff names and work contacts, without a citizen-data finding.
ALTERNATIVE	Brief viewing of business contacts does not establish copying or the entry route.
LIMIT	The account says citizens' personal data was not affected and does not identify an actor. The original release was not available for this review.
RESPONSE	Review supplier-held directories and service privileges, and prepare staff for targeted impersonation using business-contact information.

Bottom line

Review service privileges and prepare for staff impersonation.

The available account names no operator and supports no attribution conclusion. The confirmed business-contact categories justify a focused impersonation warning while technical investigation and attribution remain separate.

CASE O

O A public-administration update widens the stated data categories (O15)

Public administration

Press report

OBSERVATION	November press reporting revisited an earlier 2026 incident at a public-administration body and described a widened data scope. [S55]
CHRONOLOGY	Initial findings covered narrower record categories before a broader scope became apparent later in the year.

ESTABLISHED	The reported account says affected people were informed personally and police and the data-protection authority had been informed.
ALTERNATIVE	A later scope revision is not evidence of a second independent intrusion or the access date of every record.
LIMIT	A complete original notice was unavailable for this review.
RESPONSE	Update the record of affected categories, risk and communication as evidence develops, while keeping the incident chronology and notification rationale intact.

Bottom line

Update affected data categories and communication decisions as evidence develops.

The response lesson concerns changing knowledge. An early statement is a dated account of what was known then. A later assessment can change the privacy decision without showing that the earlier statement was wrong for what was known at the time.

P

CASE P

A hospitality supplier event is followed by guest payment deception (O16)

Hospitality

Press report

OBSERVATION	November press reporting quoted a hospitality operator's notice about guest information exposed through an external supplier. [S56]
CHRONOLOGY	The reporting describes an ongoing investigation rather than establishing a precise initial access date.
ESTABLISHED	The company account identifies names, contact details, booked properties and stay dates. It says payment data was unaffected and bookings remain valid.
ALTERNATIVE	The supplier event does not establish entry into the operator's own systems or all of its service providers.
LIMIT	The report describes deceptive messaging requests for bank or card details, while the exact access route remains under investigation.
RESPONSE	Give guests a trusted verification route and explain that real booking details do not authorise an unexpected payment-data request.

Bottom line

Provide a trusted guest verification route and preserve the stated scope of valid bookings and unaffected payment data.

The customer-protection work can be necessary while the technical route remains unresolved. Reassure guests about bookings only within the company's stated scope, and separate that statement from the investigation into information exposure and subsequent messages.

CASE Q

An operator discloses two separate supplier incidents (O17)

Accommodation services

Operator notice

OBSERVATION	An accommodation operator's autumn 2026 notice describes separate incidents at its booking-software and guest-communication suppliers. [S57]
CHRONOLOGY	The two supplier events occurred weeks apart during autumn 2026, with the later event involving account-level data retrieval.
ESTABLISHED	The notice says guest and booking information was involved and both incidents were reported to the Datenschutzbehörde. It also reports booking-related deceptive messages to guests.
ALTERNATIVE	Two supplier notices do not establish an intrusion into the operator's own systems or a common operator behind both events.
LIMIT	The later supplier account identifies a four-figure number of bookings and guest records as potentially affected. The actual retrieval count is unresolved; these are not confirmed unique people.
RESPONSE	Keep separate supplier chronologies, assess the operator's actual data categories and warn guests through a known channel while retaining the suppliers' stated exclusions.

Bottom line

Keep the supplier events separate and distinguish potential booking or guest-record totals from confirmed unique people.

The suppliers' exclusions cover payment or card data, identity documents, credentials and access codes under their current accounts. Those exclusions do not negate the reported guest-data access. A potential booking count must not become a confirmed affected-person total.

5.6 Additional official notices and explicit exclusions

The following publications broaden the response picture without becoming additional confirmed organisational intrusions.

Publication	Source-read subject	Disposition
15 January	Fabricated tax-payment reminders and official-looking notices [S23]	Government-themed fraud campaign context
27 February	Tax-themed messages, calls and fake service websites [S24]	Multi-channel impersonation context
12 March	International action against a proxy service [S22]	Law-enforcement response; its earlier Austrian investigation population is historical
12 August	Romance-scam prevention warning [S51]	Thematic prevention notice; no new breach total inferred
9 October	Phishing prevention, 2025–2026 figures and OeNB/RTR statements [S16]	Context; spring renewal campaign overlaps Case D
12 November	Operation TorNado [S21]	Retrospective response; Austrian actions occurred in February
20 November	Seasonal online-shopping fraud warning [S52]	Preventive warning, with no incident count
May 2026	Healthcare logistics exercise [S53]	Exercise, excluded from actual-incident counts
19 June	Fire-related fibre interruption [S13]	Physical continuity event, excluded from cyberattack counts

The finance ministry's January and February warnings describe criminal use of its identity. They do not establish an intrusion into the ministry. A government-themed lure and a government data incident require different evidence and different response owners. [S23][S24]

The proxy-operation account contains Austrian investigation findings from before 2026. Its publication during this window does not make all those affected networks new 2026 incidents. The same principle applies to law-enforcement totals spanning several countries or years. [S22]

5.7 Recent activity: 8–22 November 2026

Recent publication is not synonymous with a recent intrusion. The following distinctions guide the closing-period response; withheld-organisation items retain month-level dating to prevent indirect identification.

Date	Item	What changed	Appropriate decision
Autumn 2026 (November update)	Accommodation-operator notice [S57]	Two separate supplier events and a guest warning	Keep supplier records separate and verify the real payment process
November 2026	Project-organisation reporting [S27]	Further reporting about an autumn event	Separate record scope from continuing operations
12 November	TorNado release [S21]	Publication of an international operation account	Retain the historical and global scope
November 2026	Hosted-supplier update [S28]	Further statement about a November hosted-infrastructure event	Obtain customer-specific scope and preserve the stated exclusions
18 November	Java advisory [S44]	Product- and platform-dependent urgent remediation	Check applicable builds and vendor guidance
18 November	NGINX and national warning [S48]	Critical software warning and response coordination	Identify applicable deployments and verify correction
18 November	Financial-sector dialogue [S42]	Supervisory engagement with information and communication technology (ICT) providers	Rehearse reporting and supplier escalation
19 November	PHP advisory [S45]	Fixes and configuration-dependent conditions	Check versions and relevant session or backend settings
November 2026	Hospitality supplier report [S56]	Guest information and subsequent payment-deception warning	Provide a trusted customer contact route
November 2026	Public-sector disclosure [S29]	Public account of staff business-contact viewing	Review hosted staff data and targeted impersonation risk
20 November	Shopping-fraud warning [S52]	Seasonal prevention guidance	Use independent merchant and payment verification
November 2026	Public-administration data update [S55]	Revised scope of an earlier 2026 event and personal notifications	Update the data-risk and communication assessment

Nothing in this table establishes a common operator or a numerical late-November surge. Its value lies in identifying which decision changes: patching, customer support, supplier review or interpretation of an earlier event.

KEY TAKEAWAYS

01

A campaign, a disclosure and a retrospective operation are different records.

02

Carry every case's confirmed scope and unresolved propositions into the response.

03

Treat recent updates as decision changes, without multiplying incidents or assigning unsupported actors.

CHAPTER 06

Hacktivism, DDoS and service availability

06

THIS CHAPTER ANSWERS

Which evidence separates an availability claim from a verified service impact?

3

independent questions: reachability, data access and business function

6.1 A claimant's target list is not an impact assessment 61
6.2 Retained website and access claims 61
6.3 A relayed building-controller claim keeps its own caveat 64
6.4 Claim versus official scope 64
6.5 A timeline of different evidence types 65
6.6 Politically framed activity requires the same proof standard 66
6.7 Availability rehearsal with an observable finish 66
6.8 Physical and technical dependencies need separate owners 67

CHAPTER 06

Hacktivism, DDoS and service availability

IN SHORT

A claimed outage, an interrupted website and an operational-system incident are different propositions. Political language does not establish the cause of a technical event. The cited Austrian cases also show why continuing service does not settle data exposure. Assess the customer's actual task, retain the provider's scope and use an independent status route before describing impact or attribution.

6.1 A claimant's target list is not an impact assessment

A post naming a service can establish an actor's expressed interest or claim. It cannot establish the full duration, affected users, business consequence or responsible operator. A screenshot is evidence of what the poster chose to show, unless independently corroborated. [S1]

Reachability can differ by service, user, network and time. A responding homepage does not establish that login, booking or payment works. A failed check does not by itself establish malicious traffic or an Austrian-wide outage.

The incident team should separate the propositions in its working record. State which function failed, how that failure was established, what period is supported and whether service-owner evidence corroborates the criminal assertion. Preserve unresolved causes as unresolved.

For essential operations, a useful measure is completion of the customer's task through the normal or fallback route. Security telemetry can explain an interruption, but the service owner must establish whether people could obtain the required service.

6.2 Retained website and access claims

A 26 March post from a 313 Team-labelled source claims disruption of a public-sector website and announces a one-hour duration. The duration is a plan in the post, rather than a measured outage. No official case-specific confirmation is held with the card. [S1]

Evidence card B16 — 26 Mar 2026

313 Team | Chat message | Telegram | Arabic and English

ORIGINAL

The attack is scheduled to last for one hour.

Held
A 313 Team-labelled message announces a public-sector website operation and a planned one-hour duration.

Not established
A measured one-hour outage, official confirmation, data access or a verified effect on public-sector operations.

Posts dated 8 and 17 May from a NoName057(16)-labelled source claim activity involving transport-related, retail, public-sector and energy-sector websites. Some entries describe geolocation restrictions. Such a description does not establish a successful denial of service or the effect on legitimate users. [S1]

Evidence card B13 — 8 May 2026

NoName057(16) | Chat message | Telegram | English

ORIGINAL

"Traveling" through the Austrian internet infrastructure

Held
A NoName057(16)-labelled message asserts targeting of transport-related, retail and public-sector websites.

Not established
Measured availability, duration, service interruption, data access or operational transport impact.

Evidence card B14 — 17 May 2026

NoName057(16) | Chat message | Telegram | English

ORIGINAL

(closed by geolocation)

Held
A later NoName057(16)-labelled message lists energy-related and other websites, describing some as restricted by geolocation.

Not established
Successful denial of service, data access, energy-supply interruption or access to operational technology.

The same labelled publication source also carries an 8 May energy-related claim attributed in its text to Darkstorm. That is a relay. It is not an independently held original Darkstorm post, an official service account or evidence of shared operator control. [S1]

Evidence card B15 — 8 May 2026

[relay alias withheld] | Chat relay | Telegram | English

ORIGINAL

#DARKSTORM

Held
A retained relay attributes an energy-sector website claim to Darkstorm. This is not a primary Darkstorm post.

Not established
A verified outage, operational impact, primary actor authorship, collaboration or common control.

A May post from the same NoName057(16)-labelled source claims access to a retail outlet's video-surveillance system and describes a recording. The recording and access were not independently authenticated. The claim does not establish intrusion into a broader corporate network, a persistent connection or exposure of customer records. [S1]

Evidence card B17 — May 2026

NoName057(16) | Chat message | Telegram | English

ORIGINAL

We have gained access to the internal video surveillance system

Held
A NoName057(16)-labelled message claims access to a retail location's video-surveillance system.

Not established
Authenticated video, current access, the site, entry route, data exposure or access to a broader corporate network.

The following panel compares the claims with the evidence held for those propositions. A missing official account is a limit of this evidence, rather than an official denial.

Point	Actor or relay assertion	Official evidence held	Report conclusion
Duration	B16 announces one hour [S1]	No case-specific official duration retained	Planned duration is not measured downtime
Availability	B13 and B14 list websites or note geolocation restrictions [S1]	No case-specific service-impact confirmation retained	Reachability and user impact remain unestablished
Energy	B15 relays a website claim attributed to Darkstorm [S1]	No operational-energy confirmation retained	Website targeting does not establish an energy-process incident
Surveillance	B17 describes retail-camera access [S1]	No independently authenticated access or recording retained	Broader network access and persistence remain unestablished

The corresponding defender task is to validate the actual service. Ask the website owner about the affected function and period. For a camera claim, ask the authorised owner to establish the device, account, recording provenance and access history.

Do not treat a later software warning or an unrelated official incident as either corroboration or refutation. The proposition, service and timeframe must match before two sources can support the same case.

6.3 A relayed building-controller claim keeps its own caveat

A separate May roundup from a NoHeartz-labelled source relays a NoName057(16)-attributed building-controller access claim. The roundup itself expressly says that industrial control system (ICS) access is not officially confirmed. That caveat must travel with any summary of the allegation. [S1]

Evidence card B18 May 2026

[relay alias withheld] Chat relay Telegram Russian

ORIGINAL

⚠ ICS-доступ официально не подтверждён.

TRANSLATION

ICS access is not officially confirmed.

Held
A relay describes an alleged Austrian networked building-controller incident and explicitly says ICS access is not officially confirmed.

Not established
A verified site, current control, changed settings, unsafe process, manufacturer-system intrusion or primary actor authorship.

The retained material does not independently authenticate the site, country, controller or recording. It establishes neither a completed setting change nor an unsafe physical process. It also does not establish intrusion into the manufacturer's infrastructure.

The response is conditional on an authorised match. The actual equipment owner should review access records, remote-maintenance arrangements and independent state information. The report does not recommend testing an unknown controller or contacting the claimant.

A building-control claim and an energy-company website claim belong to different technical populations. Combining them under a single operational-technology incident would erase the central uncertainty in both.

6.4 Claim versus official scope

The mailbox-document case illustrates how wider advertising and a narrow official account can coexist. The appropriate comparison preserves both propositions without a ratio or an assumption that one cancels the other. [S26]

Point	Criminal narrative	Official account	Report conclusion
Material	Wider extortion-related claims	Spokesperson acknowledges older documents from one mailbox	Document exposure is supported within that account
Systems	Advertising can imply a broader event	Spokesperson denies a wider operational-system attack under then-current knowledge	Broader system access remains unestablished here
Time	Publication is a visible claim event	Confirmed material dates from 2025	Neither establishes a fresh intrusion for every posted item
Impact	A claim can imply extensive disruption	Core operational and customer scope is denied in the source account	Validate the relevant function separately
Actor	Claim label and advertising identity	No independently established operator in this report	Retain the allegation without assigning responsibility

The panel is not a verdict about a claimant's honesty. Its purpose is to prevent a service team from answering the wrong question. A document investigation and an operational assurance can both be necessary.

The autumn project-organisation case supplies a similar caution. Its company account concerns an information-system event while project work continued. That is the company's stated operational boundary, rather than a general assurance about every related organisation. [S27]

6.5 A timeline of different evidence types

The timeline retains dated official notices, campaign warnings and retained actor or relay messages. Withheld-organisation disclosures retain year-, seasonal or month-level dating in Chapter 5 to prevent indirect identification. The sequence does not imply a common campaign.

26 Mar 2026 — **313 Team-labelled source**
Claims website disruption and announces a planned one-hour duration. [S1]

8 May 2026 — **NoName057(16)-labelled source**
Publishes website claims; service impact is not independently established. [S1]

8 May 2026 — **Same labelled publication source**
Relays an energy-website claim attributed to Darkstorm. [S1]

17 May 2026 — **NoName057(16)-labelled source**
Publishes further website claims, including geolocation descriptions. [S1]

26 May 2026 — **CERT.at**
Recruitment-lure campaign linked by the source to confirmed Austrian cases. [S9]

19 Jun 2026 — **CERT.at**
Fire-related fibre interruption; physical continuity event. [S13]

24 Jul 2026	**CERT.at** Warning about phishing from genuine Austrian business accounts. [S10]
26 Aug 2026	**CERT.at** Increased BEC attempts against Austrian organisations. [S12]
9 Oct 2026	**Bundeskriminalamt, OeNB and RTR** Phishing prevention release with 2025–2026 case context and SMS sender-ID controls. [S16]
29 Oct 2026	**Bundeskriminalamt** Warning on social-media task and job deposit fraud. [S20]
18 Nov 2026	**CERT.at and BMI** Urgent Java advisory and national coordination around the NGINX security warning. [S44][S48]
19 Nov 2026	**CERT.at** Critical PHP security corrections and configuration conditions. [S45]

The rows distinguish detection, actor assertions, relays, campaign warnings and later updates. They are not equivalent incident-start observations. The fire row is explicitly outside cyberattack counts.

6.6 Politically framed activity requires the same proof standard

An actor can present its actions as support for a political cause. That self-description establishes rhetoric, not a verified state relationship, nationality or motive for a separate incident. The report omits slurs and does not amplify ideological slogans.

Election timing or a public body's prominence does not itself demonstrate an influence operation. Any assertion about election impact would require separate evidence. No such conclusion is made here.

Security teams can preserve the original message privately while communicating the operational facts publicly. A useful public update explains the affected function, available alternative, confirmed data consequences and next update time. Political interpretation is unnecessary to that task.

Apply the same standard to claims that invoke any state or international conflict. Attribute another source's assessment when it is relevant, state its limits and avoid turning a claimed cause into the authors' own explanation.

6.7 Availability rehearsal with an observable finish

The following exercise is a planning recommendation. It is not an account of an actual attack.

Give the team an unavailable public website, a circulating claim and uncertainty about data access. The service owner should establish which customer functions fail. The technical team should distinguish cause investigation from immediate service mitigation.

Then make the normal status channel unavailable too. Communications should publish through a pre-agreed independent route. Customer support should demonstrate that people can find the alternative without following links in the claimant's post.

End the exercise only when the business owner verifies the critical tasks and the incident commander records the unresolved scope. Restoration alone should not close a separate data-access or notification assessment.

6.8 Physical and technical dependencies need separate owners

The bridge-fire account is relevant because it tests assumptions about continuity without supplying hostile attribution. The service owner should identify whether supposedly independent connections share a physical route, a facility or a management dependency. [S13]

The same question applies to logical fallbacks. An alternative website dependent on the same identity provider can fail with the primary route. An emergency contact list stored only in the unavailable service might not help during the outage.

Document the fallback's assumptions and test them with the relevant provider. The completion evidence should show the business task working under the assumed failure, rather than a second contract or untested design diagram.

KEY TAKEAWAYS

01

Verify service functions, data access and attribution independently.

02

Use an independent status route and preserve the source's operational boundary.

03

Exercise physical and logical dependencies without relabelling failures as attacks.

CHAPTER 07

Threat actors and supported relationships

07

THIS CHAPTER ANSWERS

Which actor-related conclusions are supported by listings and official reporting?

61

Austrian ransomware listings in the requested window; criminal claims

7.1 Extortion labels describe the listing population 69
7.2 Regional peers supply listing context 70
7.3 An access relationship needs a source-specific edge 72
7.4 State-linked activity: retain the authority's assessment 75
7.5 Personas and relays remain distinct 75
7.6 Service-provider management access deserves early attention 76
7.7 Recent patch readiness: match product, build and configuration 76
7.8 Hacktivist labels and listing relays 77
7.9 What would strengthen an actor assessment 80

CHAPTER 07

Threat actors and supported relationships

IN SHORT

Ransompedia records 61 Austrian listings across 56 distinct names and 22 claimant labels in the requested window. CERT.at separately describes an assessed access relationship between ZipLine actors and Qilin. These observations have different proof boundaries. Listings do not establish encryption, theft or a shared operator for every case. Use the supported relationships to choose validation and recovery work, and preserve the source behind each attribution.

7.1 Extortion labels describe the listing population

The 61 Austrian listings compare with 38 for all of 2025. This is a partial-year window beside a full-year total, not a matched-period growth rate. Four entities appear more than once (three twice and one three times, accounting for five repeat entries), leaving 56 distinct listed entity names. Each listing records a criminal assertion, not an independently confirmed intrusion or payment. [S2]

The three most frequent labels account for 28 of 61 listings, or 45.9%. The other 33 listings fall under additional labels. This distribution supports preparation across several extortion narratives rather than a response designed around one name. [S2]

Listing label	Austrian listings	Interpretation
The Gentlemen	11	Criminal label attached to listed assertions
Qilin	9	Criminal label; entry route is not inferred from the name
LockBit 5	8	Listing label, not a verified operator count
Other labels	33	Remaining claims across the listing population
Total	61	Dated listings within the requested window

Manufacturing carries 11 listings, or 18.0% of the Austrian population. Consulting and the broad global label each carry six; retail and education each carry five. These are listing-sector labels, not national sector incidence or independently verified business classifications. [S2]

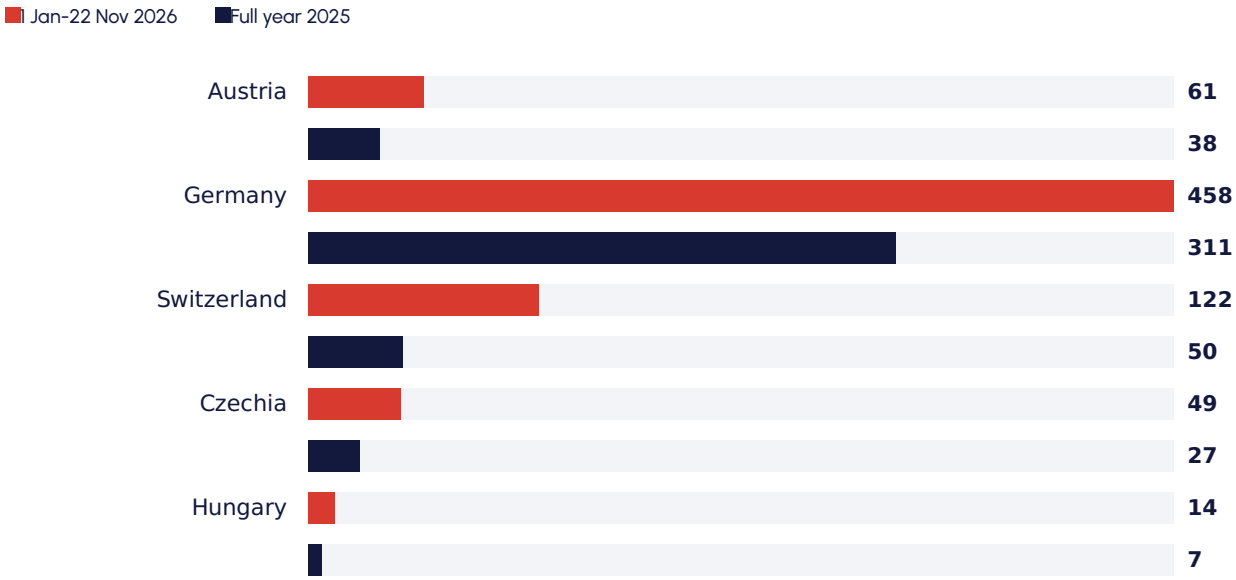
An organisation can appear more than once or have a complex group structure. The reader should not convert listing volume into unique victims or assume that a feed's country label establishes the affected legal entity.

7.2 Regional peers supply listing context

Germany, Switzerland, Czechia and Hungary provide neighbouring economic, supplier and service context. The comparison uses the same requested period and the same listing unit. It does not estimate the probability of an Austrian organisation experiencing an incident. [S2]

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

Austria has 61 listings in the same window, beside different regional listing populations



Source: Brandefense Ransompedia country-labelled extortion listings, 1 January-22 November 2026 versus full-year 2025 [S2]. Unequal periods and different country populations; not a national risk ranking.

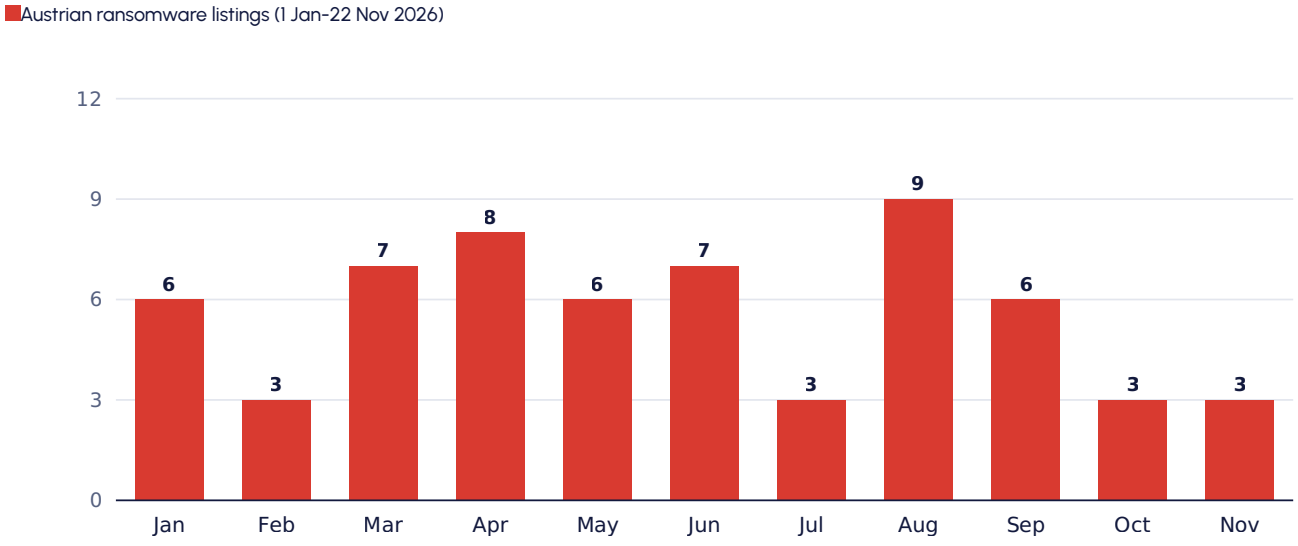
Country	Listings	Supported reading
Austria	61	Austrian-labelled extortion claims in the observed population
Germany	458	Larger visible listing population in the same window
Switzerland	122	Separate national listing population
Czechia	49	Separate national listing population
Hungary	14	Separate national listing population

Country size, group composition, public disclosure and visibility differ. The figures are not adjusted for those factors. No ratio between them is presented as comparative cyber-security effectiveness or national risk.

The Austrian monthly sequence is useful for the timing of visible claims. November is incomplete relative to a full calendar month because the window ends on 22 November.

Month	Austrian listings	Time boundary
January	6	Full calendar month
February	3	Full calendar month
March	7	Full calendar month
April	8	Full calendar month
May	6	Full calendar month
June	7	Full calendar month
July	3	Full calendar month
August	9	Full calendar month
September	6	Full calendar month
October	3	Full calendar month
November	3	Through 22 November
Total	61	Requested window

The Austrian listing sequence describes claim publication, with November ending on 22 November



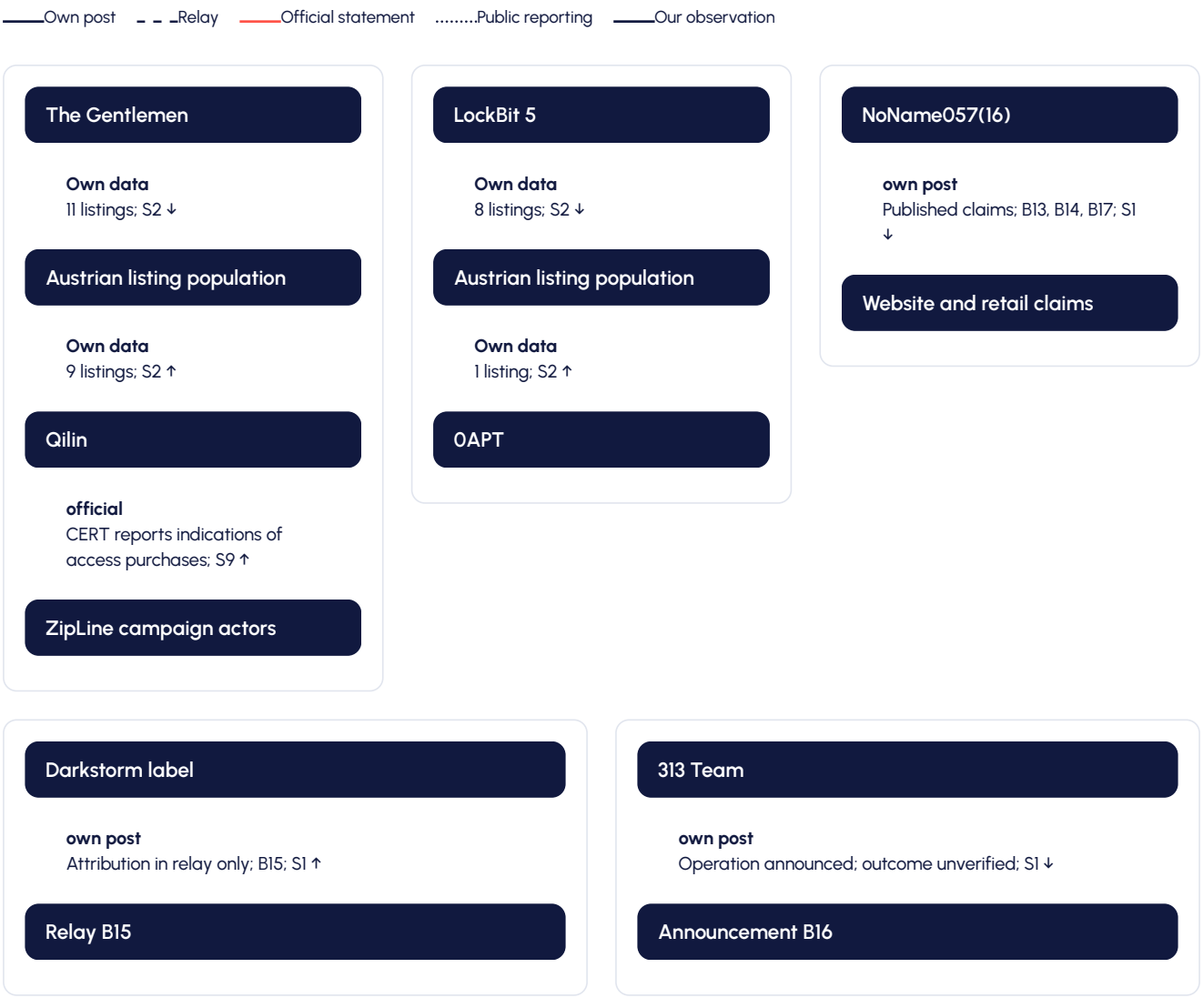
Source: Brandefense Ransompedia Austria-labelled extortion listings, 1 January–22 November 2026; November partial [S2]. Listings record criminal claims, not confirmed intrusions.

The sequence does not establish intrusion dates or an underlying national attack trend. A listed event can be older than its publication, and an unlisted incident remains outside this population. [S2]

7.3 An access relationship needs a source-specific edge

CERT.at says it has indications that Qilin acquires access from actors associated with the ZipLine phishing campaign. Its notice also says confirmed Austrian cases exist. This supports the source's stated relationship, with its uncertainty retained. [S9]

That edge does not establish one operator across every related post or listing. Nor does a Qilin label justify applying the recruitment route to an individual company without case-specific evidence. The incident team still needs the relevant account and endpoint record.



The relationship map should distinguish three kinds of edge: an observed post association, an own-data listing label and a public source's assessed access relationship. An edge represents the proposition in its label, rather than general membership in a single criminal organisation.

Any broader chain connecting identity theft, access resale, extortion and payment fraud is an **analytical model** unless a concrete shared element links the individual observations. The model can help assign control owners without becoming attribution for a particular incident.

Qilin

Label in the retained listing population

Extortion listing label | No state attribution assessed

IN AUSTRIA, 2026

2026

9 Austrian listings in the requested window

May 2026

CERT.at reports indications of access acquisition from ZipLine actors, S9

CLAIMED TARGETS

Listing population; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 9 Austrian listings under this label.

[S9] CERT.at reports confirmed Austrian ZipLine cases and indications that Qilin acquires initial access from ZipLine actors.

OUR ASSESSMENT

The listing observations justify recovery and disclosure readiness, while CERT.at's May assessment supports reviewing recruiter-themed correspondence when case evidence warrants it. Neither establishes a single operator across all Qilin listings.

CONFIDENCE

High for the retained listing count and official notice; individual listings remain claims

The Gentlemen

Label in the retained listing population

Extortion listing label | No state attribution assessed

IN AUSTRIA, 2026

2026

11 Austrian listings in the requested window

CLAIMED TARGETS

Listing population; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 11 Austrian listings under this label.

OUR ASSESSMENT

The listing observations justify recovery and disclosure readiness. They do not establish data theft, encryption, common operators, completed sales or financial loss.

CONFIDENCE
High for the retained listing count; the underlying assertions remain claims

LockBit 5

Label in the retained listing population

Extortion listing label | No state attribution assessed

IN AUSTRIA, 2026

2026
8 Austrian listings in the requested window

CLAIMED TARGETS

Listing population; identities and sectors withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 8 Austrian listings under this label.

OUR ASSESSMENT

The listing observations justify recovery and disclosure readiness. They do not establish data theft, encryption, common operators, completed sales or financial loss.

CONFIDENCE
High for the retained listing count; the underlying assertions remain claims

ZipLine campaign actors

Recruitment-lure initial-access campaign (CERT.at)

Initial-access phishing campaign | No state attribution assessed

CLAIMED TARGETS

Manufacturing and export-oriented SMEs as described by CERT.at; no victim total published

IN AUSTRIA, 2026

26–28 May 2026
CERT.at reports confirmed Austrian cases and DACH recruiter-themed lure domains, S9

SEEN IN PUBLIC REPORTING

[S9] CERT.at update describing contact-form recruiter correspondence leading to malicious archive delivery and indications of access reuse by Qilin.

OUR ASSESSMENT

CERT.at confirms Austrian cases and reports indications of access acquisition by Qilin. Defenders should review extended recruiter correspondence and endpoint records before assuming every recruitment lure shares one operator.

CONFIDENCE
High for the official CERT.at assessment; national victim count unquantified

7.4 State-linked activity: retain the authority's assessment

The DSN announcement for its 2025 report discusses espionage as an ongoing security concern. That authority context is not proof of a state relationship for any incident or criminal listing in this report. [S43]

A state-attribution proposition needs its own evidence and source. A public institution or a geopolitical subject can be relevant context, but none identifies an operator by itself.

This report therefore separates criminal claim labels, source-assessed relationships and unresolved attribution. It does not assign nationalities from language or carry an attribution from one incident to another without case-specific evidence.

For a high-consequence case, the incident commander should preserve the attribution question separately from containment. An organisation can restrict an abused account and protect staff without resolving the operator's identity.

7.5 Personas and relays remain distinct

A persona is a public-facing identity in the retained material. It can be shared, renamed, imitated or operated by more than one person. A platform account is therefore not a verified human operator count. [S1]

A relay can increase an allegation's reach without supplying a second independent source. Repeated descriptions, matching counts and copied samples require careful interpretation. They can establish advertising similarity while leaving file identity and transfer unresolved.

The same caution applies to a claim that material is exclusive or current. Those are seller assertions until the relevant proposition is corroborated. Confidence belongs to the specific statement, rather than the persona as a whole.

7.6 Service-provider management access deserves early attention

CERT.at's September N-central warning describes active exploitation and an emergency correction. The NVD record identifies affected versions before 2026.3.1.14; CERT.at names the corrected release as 2026.3 HF4. [S7] [S46]

The immediate reader question is whether the organisation or its provider runs an applicable build. A provider should identify the actual management service, patch state and downstream access relationships. The report does not claim a count of Austrian affected providers.

A management service can have authority over many customer systems, but that architectural possibility is not evidence that every customer was accessed. Obtain a tenant-specific assessment and preserve the distinction between product exposure, demonstrated use and downstream impact.

For continuity, the customer should know how to suspend a provider's privileged access while keeping essential administration available. The exercise needs a restoration and reauthorisation route; disabling access without a workable alternative can create another service problem.

7.7 Recent patch readiness: match product, build and configuration

The November advisories support prompt asset review, with their conditions retained. They are not a count of successful Austrian exploitation. All five cited CVE records were verified on NVD on 27 November 2026 alongside the cited advisories. [S7][S44][S45][S46][S47]

Record	NVD status (27 Nov)	Relevant affected scope	Corrected releases or action
CVE-2026-114938	Analyzed; CVSS 3.1 8.1 High (modified 24 Nov)	Specific Oracle Java and related distributor builds; demonstrated processor conditions matter	Corrected Oracle releases are listed below; check the distributor's matching advisory
CVE-2026-129289	Awaiting Analysis; CNA CVSS 4.0 9.2 Critical	Relevant PHP branches before their listed fixes; the described FastCGI Process Manager (FPM) attack depends on persistent backend connections and an unread request-body path	8.2.36, 8.3.37, 8.4.28, 8.5.13; 8.6.0 includes corrections
CVE-2026-115560	Awaiting Analysis; CNA CVSS 4.0 9.2 Critical	Relevant PHP branches before the same fixes; session-upload progress, shared storage and different serializers create specific conditions	Apply the branch fix and review explicitly enabled upload progress and shared-session configuration

Record	NVD status (27 Nov)	Relevant affected scope	Corrected releases or action
CVE-2026-86218	Analyzed; NVD CVSS 3.1 9.8 Critical	N-central versions before 2026.3.1.14	2026.3 HF4; verify the installed build and provider guidance
CVE-2026-41940	Analyzed; CVSS 3.1 9.8 Critical	Affected cPanel and WHM release tracks after 11.40 before branch exclusions (authentication bypass)	86.0.41, 94.0.28, 102.0.39, 110.0.97, 118.0.63, 124.0.35, 126.0.54, 130.0.19, 132.0.29, 134.0.20 or 136.0.5 (11.x branch fixes as listed on NVD); review retrospective access [S7][S47]

The selected Java advisory lists these corrected Oracle release identifiers. They are software versions. [S44]

`17.0.21.1`
`21.0.13.1`
`25.0.5.1`
`27.0.1.1`

For Java, NVD identifies particular affected Oracle builds, including 8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3 and 27.0.1.0.3, plus listed GraalVM releases. Other distributor lines need their own matching notice. The demonstrated processor condition is x86-64 with AVX-512 VBMI support. [S7][S44]

For PHP request handling, a version inventory is only the first check. Both cited PHP records remain in NVD Awaiting Analysis status on 27 November, carrying PHP CNA CVSS 4.0 scores of 9.2 (Critical). The described FPM scenario depends on backend connection reuse and a relevant request path. Standard close-per-request configurations are outside the demonstrated FPM scenario described by the advisory. [S7][S45]

For the session issue, an update does not itself ensure that separate configurations use the same serializer with shared session data. Review explicitly enabled session-upload progress and the actual deployment. Do not infer remote code use from version presence alone. [S7][S45]

The 18 November NGINX warning should likewise trigger a product- and configuration-specific review. BMI's announcement describes coordination around the warning, not the number of Austrian vulnerable servers. Use the current vendor notice for the installed distribution. [S48]

Earlier hosting-management warnings also justify retaining retrospective access evidence after a correction. CERT.at's April cPanel and WHM notice (CVE-2026-41940) describes active exploitation and contact with known vulnerable Austrian operators. It does not quantify successful Austrian intrusions. [S7][S47]

7.8 Hacktivist labels and listing relays

The actor-related cards in Chapter 6 establish what the labelled publication sources said. They do not establish operator nationality, state direction or successful impact. No state attribution is assessed for those claims in this report. [S1]

NoName057(16)

Labelled publication source

Availability and access claims | No state attribution assessed

IN AUSTRIA, 2026

2026-05-08
Website claims, B13

May 2026
Retail surveillance claim, B17

2026-05-17
Website and geolocation assertions, B14

CLAIMED TARGETS

Public-sector, transport-related, energy-related and retail services, described only by broad roles

IN THEIR WORDS

"(closed by geolocation)" B14

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

Messages retained under a NoName057(16)-labelled source establish published claims. They do not establish measured outages, current access, operational disruption or state direction. Source: S1.

CONFIDENCE
High for retained publication; underlying outcome and attribution remain unverified

Darkstorm

Attributed label in relayed posts

Attribution inside a relay | No state attribution assessed

IN AUSTRIA, 2026

2026-05-08
Energy-related website claim attributed in B15

CLAIMED TARGETS

Energy-sector website; no operational grid outcome established

IN THEIR WORDS

"#DARKSTORM" B15

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

The retained item is a relay that names Darkstorm. It does not establish primary authorship, collaboration with the publishing source, common control, a verified outage or a state relationship. Source: S1.

CONFIDENCE
High for retained publication; underlying outcome and attribution remain unverified

313 Team

Labelled publication source

Public-sector availability claim | No state attribution assessed

IN AUSTRIA, 2026

2026-03-26
Planned operation and duration announced in B16

CLAIMED TARGETS

Public-sector website, without a victim identifier

IN THEIR WORDS

"scheduled to last for one hour" B16

SEEN IN PUBLIC REPORTING

OUR ASSESSMENT

A source using this label announces an operation and a planned duration. The duration is not a measured outage. Data access, public-service impact and operator identity remain unverified. Source: S1.

CONFIDENCE
High for retained publication; underlying outcome and attribution remain unverified

Darkstorm's appearance through another labelled source is a relay association. It does not establish collaboration or common control. Likewise, a NoHeartz roundup's attribution is retained as the roundup's assertion, with the controller-access caveat intact.

Multiple feed relays repeated a single 0APT-labelled Austrian listing during 2026. These are distribution observations, rather than multiple independently confirmed attacks or an original 0APT publication. Target details and sector labels remain withheld because the listing is an unverified claim. [S1][S2]

0APT

Label in the retained listing population

Extortion listing label | No state attribution assessed

IN AUSTRIA, 2026

2026

1 Austria-labelled listing in Ransompedia (S2), repeated by multiple relays (S1)

CLAIMED TARGETS

Austria-labelled entry; identity and sector withheld

SEEN IN PUBLIC REPORTING

[S2] Ransompedia records 1 Austria-labelled listing under this label.

OUR ASSESSMENT

Multiple feed relays of a single listing do not create separate attacks, and the name does not establish a state-linked operator. Underlying theft, encryption and official confirmation remain unverified. Sources: S1, S2.

CONFIDENCE

High for the retained listing count; underlying outcome and attribution remain unverified

The 0APT label should not be read as proof of state sponsorship because its name includes APT. A match between a feed's actor label and another dataset also requires case-specific identity checks before joining the records.

7.9 What would strengthen an actor assessment

A stronger assessment would connect observations through an independently meaningful shared element. Examples include corroborated infrastructure, a common campaign artefact or a source-confirmed access relationship. Similar political rhetoric or a common target sector is insufficient.

Keep the proposition narrow even when a link is strong. A shared contact can support a contact association while leaving operator identity unresolved. A common dataset can establish reuse without showing who first obtained it.

For the defender, the value of stronger attribution is whether it changes a decision. It can guide a focused hunt or supplier question. It should not delay an urgent account, service or customer-protection action already justified by direct evidence.

KEY TAKEAWAYS

01

Listing labels describe claims rather than unique operators or successful intrusions.

02

Preserve CERT.at's assessed relationship without applying it to every labelled case.

03

Match urgent remediation to the actual product, build and configuration.

CHAPTER 08

The fraud economy: identity, context and payment

08

THIS CHAPTER ANSWERS

How does credible information become an unauthorised financial instruction?

3

different decisions: identity validation, payment approval and customer protection

8.1 Context is not authority 83

8.2 Recruitment and work offers need different escalation routes 83

8.3 Government and bank identity can bridge channels 84

8.4 Recovery fraud can extend the harm 84

8.5 Underground account and identity services remain claims 84

8.6 Payment-card material in posts: a narrow view 85

8.7 A joined response without a joined incident total 86

CHAPTER 08

The fraud economy: identity, context and payment

IN SHORT

Austrian warnings describe fraud that moves between messages, calls, websites and remote-support sessions. Correct context can make a request persuasive without making it legitimate. Underground offers show a market assertion or demand, while official notices describe actual reported mechanisms. Confirm the requested action independently, preserve a safe contact route and support people who have already acted.

8.1 Context is not authority

The booking notice describes messages containing correct personal and itinerary details. The BEC notice describes credible supplier or executive requests. Both illustrate why knowing a real fact does not authorise the next action. [S11][S12]

An organisation should identify the point at which trusted context becomes a request for something new: a payment, an account login, an attachment, a device-control session or employee information. That change is a useful place for an independent check.

The independent channel should already be known. A telephone number supplied in the disputed message can belong to the deception. A confirmation by replying to the same mailbox does not resolve whether that mailbox is under someone else's control.

This operating principle does not require assuming that every unexpected message is criminal. It requires a process that can confirm a legitimate change without relying only on the channel carrying the change.

8.2 Recruitment and work offers need different escalation routes

The recruitment case and the task-job case both use an employment context, but their intended actions differ. The first involves a business correspondence route and an archive. The second asks individuals to make deposits while expecting earnings. [S9][S20]

A corporate training programme should not collapse them into one generic warning. Reception and recruitment teams need a way to escalate unusual correspondence or files. Customer-facing teams need to recognise a person being asked to pay for work or unlock a balance.

For the first scenario, preserve the correspondence and ask security to assess the relevant endpoint and account evidence. For the second, help the person stop further transfers and contact the payment provider. Neither response requires inferring a common operator.

8.3 Government and bank identity can bridge channels

The finance ministry's warnings distinguish its real delivery process from fabricated tax demands. The bank-impersonation and renewal scenarios show how a message can lead into a persuasive telephone conversation. [S23][S24][S17][S18]

The organisation's customer guidance should explain how to start an authentic interaction. A person who independently opens the established app or uses a previously held contact is in a stronger position than someone checking only a display name.

A support script should also address remote access. A caller may frame device control as a security measure. Staff should explain the organisation's real support practice and provide an accessible route for someone who already installed software or approved a payment.

Do not infer that an imitated body was itself accessed. Brand misuse, an affected customer's device and intrusion into an institution are separate propositions. The reporting owner needs the actual facts before selecting a legal or public description.

8.4 Recovery fraud can extend the harm

The April investment investigation describes a later approach promising to recover lost money for another fee. That second stage can exploit the person's knowledge of a real earlier loss. It is not an assurance that the new contact is authorised. [S19]

A bank or support team should therefore ask about subsequent approaches when assisting a person after fraud. A request framed as a recovery, investigation or legal fee still needs independent verification.

The protective message should be practical and respectful. Provide a known contact, explain the next legitimate step and state which requests the organisation will not make. A person should not need to diagnose a criminal network before obtaining help.

8.5 Underground account and identity services remain claims

An advertisement for an account, identity document or financial service establishes an offer. It does not show that the account is usable, that its owner consented or that the described verification can be bypassed. [S1]

Prices are similarly limited. An asking price can reflect advertising strategy, a package description or a repeated template. It is not a completed transaction or an estimate of the loss a buyer can cause.

A useful escalation compares the advertised category with the organisation's actual risk. A claimed employee account can affect identity response. A customer identity record can affect fraud and privacy teams. A generic service offer might warrant monitoring without establishing an organisation-specific incident.

Two retained price statements illustrate why the unit and geographic scope matter. Neither establishes an Austrian bank-account price or a completed transaction. [S1]

Card	Price statement	Unit and limit
B11	Buyer offers USD 100	Per requested personal account; Austrian relevance is unverified
B12	Seller asks USD 2,000	Full advertised worldwide phone-data package; not an Austria-only price

B11 is a buyer's stated willingness to pay. B12 is a seller's asking price for a different product. They should not be averaged or treated as two observations of the same market. No common operator or dataset identity is established. [S1]

Evidence card B11 21 Jun 2026

[alias withheld] Forum Forum Russian

ORIGINAL

За каждое ЛК готов заплатить 100$

TRANSLATION

For each personal account, I am ready to pay $100.

Held
A buyer states a bid of USD 100 per requested personal account; Austrian relevance is unverified.

Not established
An Austrian bank-account price, usable access, account ownership or a completed transaction.

Evidence card B12 20 Oct 2026

[alias withheld] Forum Forum English

ORIGINAL

Price (full): 2000 $

Held
A seller states an asking price of USD 2,000 for a worldwide phone-data aggregation package.

Not established
A price for an Austrian slice, authentic files, a new intrusion or a completed sale.

8.6 Payment-card material in posts: a narrow view

SCOPE OF THE CARD FIGURES

Any figures in this section cover only payment cards that appeared in clear text in dark-web posts collected for this report. Brandefense detects stolen cards through other methods outside this view. These figures do not measure total card theft, valid cards, completed payments or fraud loss.

The country-labelled message population contains 88 distinct payment cards appearing in clear text across 100 posts. The country labels are not independent confirmation of issuing country, current validity or actual misuse. [S5]

Card observations from posts are a narrow population. They should not be compared with police loss totals or treated as the number of affected bank customers. A criminal message can include stale information, repetition or an unverified status assertion. [S5]

The response begins with an authorised issuer assessment. Review ownership, validity, previous remediation and actual misuse before selecting a disruptive action. A post alone should not justify automatic card replacement for a broad customer population.

8.7 A joined response without a joined incident total

The fraud, identity and incident teams can share relevant facts while keeping their decisions separate. A mailbox investigation does not establish payment loss. A fraudulent payment does not establish how an account was obtained. A disclosed contact record does not establish that it caused a later call.

Use a case record with separate fields for the observed message, confirmed access, payment event and customer harm. Record links only where evidence supports them. An unverified link should remain a hypothesis with an owner and a next check.

A successful response can include a prevented transfer, a contained account and a well-supported customer notice. Those are different outcomes. Measuring them separately makes it easier to see which control needs improvement.

KEY TAKEAWAYS

01

Correct details and familiar channels do not authorise a new action.

02

Prepare for deception that continues through calls, device control and recovery offers.

03

Keep card-post observations narrow and validate issuer action against authorised evidence.

CHAPTER 09

Banking deep dive

09

THIS CHAPTER ANSWERS

Which banking decisions connect identity evidence, payment fraud and supplier disruption?

3

populations that must remain distinct: domain observations, card observations and reported fraud

9.1 Define the financial population before interpreting it 88

9.2 Customer deception can bypass the expected technical narrative 89

9.3 Financial suppliers need a customer-specific assessment 90

9.4 Keep the clocks separate 90

9.5 A banking exercise grounded in the cited warnings 90

9.6 Practical completion evidence for financial teams 91

CHAPTER 09

Banking deep dive

IN SHORT

The banking picture includes customer-directed impersonation, selected financial-domain observations and a sector-specific resilience framework. None should be substituted for the others. A reported fraud can occur without a bank-system intrusion, while a supplier event can require a separate ICT assessment. Validate the relevant account or transaction, establish the actual service impact and assign financial reporting ownership early.

9.1 Define the financial population before interpreting it

The portfolio includes a banking and finance group of selected domains. It is not a verified list of independent licensed card issuers. Group entities, service providers and overlapping domains can affect the unit of interpretation. [S6]

The financial-domain population and the card-post population therefore need separate denominators. A card observation associated with an issuer does not establish exposure of its core systems. A device association does not automatically represent a bank employee.

A banking exposure result should identify what was observed, when it was observed and which domain or service population it describes. Where the underlying measurement is unavailable, the missing result stays unknown. No banking or sector rating is inferred.

The 23 November exposure snapshot covers all 25 selected financial domains. Four had a credential offered for sale, and three carried earlier listing-history records (one domain carries a current offer with zero earlier entries). Across those 25 domains, 21 carry device associations (3,728 total; 47 employee-related across 11 domains and 3,681 other associations). All 25 carry credential-record associations (53,514), and 12 carry document associations (53). These are overlapping observations, not unique employees, customers or confirmed intrusions. [S4]

Financial-domain signal	Observed quantity	Interpretation limit
Domains with a current offer	4 of 25	Usable access and a transaction remain unestablished
Domains with prior listing history	3 of 25	Separate from current offer status; one domain carries a current offer only
Device associations	3,728	Across 21 domains; includes 47 employee-related (11 domains) and 3,681 other associations
Credential-record associations	53,514	Across 25 domains; not a unique-person or current-account total
Document associations	53	Across 12 domains; not automatically a new disclosure

The clear-text card material in §8.6 establishes no validated card-to-bank relationship and no issuer ranking. [S5]

The 23–27 November passive snapshot covers all 25 selected financial domains. It is a different observation population, not a licensed-issuer census. No bank or sector rating is published. [S3][S6]

Banking control observation	Domains	Assessed population
DMARC enforcement observed (14 reject; 6 quarantine)	20	25 domains (5 monitoring; 0 not observed)
SPF record observed	24	25 domains
DKIM key observed	17	25 domains
DNSSEC delegation record observed	5	25 domains
CAA record observed	4	25 domains
Valid TLS observation	25	25 domains
HSTS observed	23	25 domains with recorded HTTP responses

The observations do not measure every mail workflow or financial application. An unobserved key or delegation record does not establish an absent organisation-wide control. A valid TLS result does not establish transaction authorisation or application security. [S3]

9.2 Customer deception can bypass the expected technical narrative

The April SMS-to-call case describes a customer persuaded to transfer money. The renewal scenario adds remote-support deception. In October, the Austrian National Bank (OeNB) noted that roughly 1 in 16,000 payments in Austria is affected by fraud, with about EUR 115 million in prior-year losses. It added that criminals increasingly manipulate people rather than bypass technical systems. RTR-GmbH separately highlighted alphanumeric SMS sender-ID regulation to curb sender spoofing. These warnings justify customer-protection preparation without establishing access to an imitated bank's infrastructure. [S16][S17][S18]

The operational question is whether support can recognise the story while the payment is still actionable. A customer might describe a security emergency and trust the caller's knowledge. The escalation should reach staff able to assess the transaction and explain a safe contact route.

Fraud teams should distinguish an attempted payment, an authorised but deceived payment and confirmed account misuse. Those distinctions affect the evidence to preserve, the customer explanation and the response available through the payment channel.

This report assigns no national loss estimate to those mechanisms beyond the official figures with their original scope. It also makes no inference about one bank's effectiveness from the number of posts naming its brand.

9.3 Financial suppliers need a customer-specific assessment

A financial entity can depend on a hosted platform, managed service or communications provider. The supplier's general incident account may not determine whether the entity's critical or important function was affected.

The service owner should establish the tenant, function and information involved. Compliance should assess the relevant DORA classification and reporting conditions. Security should preserve the technical evidence needed to support that decision. [S40]

Do not wait for a perfectly complete narrative before assigning ownership of the reporting assessment. Equally, do not label a routine provider notice as a major ICT incident without applying the actual criteria and scope.

FMA's November dialogue with ICT providers is relevant supervisory context. It is not evidence that participating providers or banks experienced an intrusion. The practical response is to ensure that supplier escalation and reporting responsibilities are already usable. [S42]

9.4 Keep the clocks separate

For an applicable DORA event, the ordinary initial-report rule combines four hours after major classification with twenty-four hours after awareness. A late-classification exception and qualified calendar provisions also apply; see §10.5. [S59]

A personal-data breach assessment can run alongside that process under a different legal test. The privacy team should record awareness and risk to individuals separately. A DORA submission does not automatically settle the GDPR decision. [S38]

The shared event log should therefore preserve discovery, awareness, classification, supplier notification and report submission as separate timestamps. A single field labelled incident date is insufficient for those different purposes.

9.5 A banking exercise grounded in the cited warnings

The following is a planning scenario, not an account of a measured bank incident.

A customer receives an SMS about an identity renewal. A caller then asks for remote support and a transfer to protect the balance. At the same time, an external service sends a notice about uncertain access to staff business contacts.

The fraud team should assess the customer interaction and transaction. Identity staff should review any actual account evidence. The service owner should obtain the supplier's financial-entity-specific scope. Compliance and privacy should record separate reporting decisions.

Add an instruction that the normal contact person is unavailable. The exercise should demonstrate a trusted alternative rather than accepting a number supplied by the caller or disputed message.

Completion requires evidence that the customer received a safe contact route, relevant payment action was considered, supplier scope was assessed and statutory clocks were recorded. It does not require assuming that the two observations share an operator.

9.6 Practical completion evidence for financial teams

Workstream	Owner	Evidence of completion
Customer impersonation	Fraud operations	Contact verified and transaction disposition recorded
Employee account signal	Identity response	Account role, privileges and relevant sessions assessed
Card-post observation	Authorised issuer team	Validity, prior remediation and misuse reviewed
Supplier incident	ICT service owner	Entity-specific function, tenant and data scope documented
DORA assessment	Financial compliance	Classification, clocks and required submissions recorded
Personal-data assessment	Data-protection officer	Risk and notification decisions with reas-ons

The board should ask whether those responsibilities can operate together during an urgent event. Counting alerts or holding a policy is less informative than demonstrating that the owners can make the required decisions with incomplete information.

KEY TAKEAWAYS

01

Customer fraud does not establish intrusion into a bank's core systems.

02

Obtain financial-entity-specific supplier scope and record discovery separately from classification.

03

Join the response teams while preserving separate transaction, ICT and privacy decisions.

CHAPTER 10

Regulatory and national response

10

THIS CHAPTER ANSWERS

Which duties apply, and which event starts each reporting clock?

1 October 2026

full commencement of Austria's NISG 2026

10.1 Responsibilities are related, but not interchangeable 93
10.2 NISG 2026: current duties, with an entity-specific scope test 94
10.3 NISG reporting: the three deadlines do not share one starting point 94
10.4 Governance and controls require evidence of operation 95
10.5 DORA: preserve discovery and classification separately 95
10.6 GDPR: assess risk to people and the controller's awareness 96
10.7 Penalties: preserve the provision and category 96
10.8 One evidence record, several accountable decisions 97

CHAPTER 10

Regulatory and national response

IN SHORT

NISG 2026, DORA and GDPR use different applicability tests and reporting triggers. The registration period does not postpone NISG incident duties. Financial reporting requires awareness and major-classification times, while privacy reporting concerns risk to individuals. Establish the responsible legal entity and competent route, preserve separate timestamps and rehearse an initial report with incomplete but accurate information.

10.1 Responsibilities are related, but not interchangeable

The official framework distinguishes operational assistance, law enforcement, personal-data supervision and financial supervision. An organisation should identify the appropriate route before an urgent event. Sending one message does not establish that every applicable duty has been met. [S14][S30][S38][S40]

The following table summarises the source-read framework. It is an operational reference, not an entity-specific legal opinion.

Framework	Applicability question	Trigger or duty	Practical owner
NISG 2026	Is the entity essential, important or otherwise covered under the relevant provisions?	Significant cyber incident and the applicable security duties	Legal scope owner and incident response
DORA	Is the financial entity within the applicable Article 2 categories?	Relevant ICT management and major-incident reporting	Financial compliance and ICT risk
GDPR	Is there a personal-data breach and the relevant risk to individuals?	Controller notification and, where required, communication to people	Controller and data-protection officer
Criminal investigation	Does the evidence indicate potentially criminal conduct?	Preserve relevant evidence and assess a police report	Incident commander and legal
Supplier contract	Which party owes information, recovery or assistance?	Contractual and service-specific obligations	Procurement and service owner

GovCERT describes a public-administration remit. That does not mean a public body can omit its statutory applicability assessment or the data-protection decision. Operational support, supervision and criminal reporting serve different purposes. [S14]

10.2 NISG 2026: current duties, with an entity-specific scope test

The official legal FAQ says NISG 2026 fully entered into force on 1 October 2026. BMI states that initial registration is due by 1 January 2027. The registration interval does not defer the already applicable security and incident-reporting duties. [S30][S54]

Section 24 distinguishes essential and important entities by sector, size and specified categories. Its exclusions include defined security and law-enforcement public bodies, educational institutions, judiciary, legislation and the Austrian National Bank, subject to the provision's qualification for trust services. [S31]

Relevant DORA rules take precedence for entities in its scope; that is not a blanket statement that every financial entity is outside all NISG provisions. The law separately addresses ICT third-party providers. [S31]

The selected-domain portfolio is therefore not a legal-scope register. An organisation's sector label in this report cannot settle whether a statutory category, exclusion or size rule applies. Document the actual entity and the relevant provision.

Section 29 requires registration information and subsequent updates within the stated periods. Keep the entity's contacts and scope decision usable. A registration receipt should be associated with the legal entity, rather than only a technology team or an informal group name. [S33]

10.3 NISG reporting: the three deadlines do not share one starting point

Section 34 requires significant incidents to be reported without delay to the responsible sectoral CSIRT, or the national CSIRT where no relevant sectoral CSIRT exists. The CSIRT forwards the report to the authority. [S32]

The sequence matters.

Step	Ordinary timing	Starting point
Early warning	Without delay; no later than 24 hours	Awareness of the significant incident
Incident notification	Without delay; no later than 72 hours	Awareness of the significant incident
Final report	No later than one month	Submission of the incident notification
Ongoing incident	Progress report at the final-report due point	Final report follows within one month after incident handling ends
Trust-service exception	Relevant incident notification no later than 24 hours	Awareness of an incident affecting trust-service provision

The ordinary 72-hour notification and the final report do not both run from the same timestamp. Nor does an ongoing investigation remove the duty to provide the required progress account. [S32]

The reporting lead should record the awareness basis, significant-incident determination and required recipient. The initial submission can state what is unknown. Uncertainty should be visible, with later updates following the applicable requirements.

10.4 Governance and controls require evidence of operation

Section 31 requires governing bodies to ensure and supervise risk measures and attend tailored cyber-security training. Staff must be offered relevant training regularly. Section 32 covers proportionate technical, operational and organisational measures. [S34][S35]

Its subjects include incident handling, continuity and recovery, supply chains, vulnerability management, effectiveness review, hygiene, cryptography, access and secure communications. Those headings should become owned work, with evidence that the control operates for the relevant service. [S35]

For leadership, an attendance record alone does not demonstrate that a supplier fallback works. A policy alone does not demonstrate that staff can verify an urgent payment change. The recommended test is an exercise or authorised control check with a documented result.

This is the report's practical interpretation of preparation, not an assertion that every failed exercise is a statutory violation. Legal and control owners should distinguish a discovered improvement from a conclusion about compliance.

10.5 DORA: preserve discovery and classification separately

FMA states that DORA has applied since 17 January 2025, without a transitional period. Applicability follows the defined financial-entity categories, rather than a general assumption that every business handling payments is covered. [S50]

Article 5 sets the ordinary initial report as soon as possible, within four hours of major classification and twenty-four hours of ICT-incident awareness. Intermediate reporting follows within seventy-two hours after the initial notification. The final report follows within one month of the latest intermediate report. [S59]

If major classification occurs later than twenty-four hours after awareness, Article 5(2) allows the initial report within four hours after classification. An entity unable to meet a deadline must inform the authority without delay, by that deadline, with reasons. [S59]

Weekend and holiday extensions are qualified. Initial and intermediate extensions exclude credit institutions, central counterparties, trading venues and other NIS essential or important financial entities. Authorities can exclude other significant or systemic entities. Final reports follow a different calendar provision. [S59]

The incident team should therefore retain both discovery and classification evidence. A supplier's message can require assessment, but it is not automatically the classification decision. Keep the function, scope and reason for that determination in the record.

The reporting package should also preserve responsibility, relevant evidence and the communication plan. A handoff between ICT, compliance and the supplier must not erase who can make the decision or submit the report.

10.6 GDPR: assess risk to people and the controller's awareness

The Datenschutzbehörde states that a controller notifies a personal-data breach without undue delay and, where feasible, within 72 hours of awareness, unless risk to individuals is unlikely. High risk requires informing affected people without undue delay. In its 2025 activity report, the authority recorded 1,855 security breach notifications, up from 1,319 in 2024. That total includes 1,704 national GDPR notifications and 83 telecom notifications under section 164 TKG 2021. [S38][S39]

Incomplete information can be supplied in phases without undue further delay. Record the risk assessment and reason for the notification decision. A small number of records can still matter if the information or misuse creates serious harm. [S38]

A processor or supplier notice should tell the controller enough to assess its own records and affected people. An assurance about system availability does not answer the privacy question. Conversely, a security alert does not automatically establish a personal-data breach.

A public communication should distinguish confirmed categories from categories still under review. Avoid turning a negative finding at one stage into a permanent guarantee. State the source and date of the assurance and provide an update route.

10.7 Penalties: preserve the provision and category

For the core violations listed in section 45, the maximum NISG bands differ by entity category. They should not be attached indiscriminately to every procedural issue. [S37]

Provision	Relevant category	Maximum stated in the provision
Section 45(2)	Essential entity; listed core violations	EUR 10 million or 2% of the previous worldwide annual turnover, whichever is higher
Section 45(3)	Important entity; listed core violations	EUR 7 million or 1.4% of the previous worldwide annual turnover, whichever is higher
Section 45(4)	Listed registration, cooperation and other procedural violations	EUR 50,000; EUR 100,000 for repetition
GDPR notification guidance	Articles 33 and 34 notification violations	Up to EUR 10 million or 2% of the previous worldwide annual turnover, whichever is higher

Sources: NISG section 44 [S36], NISG section 45 [S37] and Datenschutzbehörde guidance [S38]. These are statutory maximum descriptions, not expected fines or a calculation of exposure for any case in this report.

Under NISG section 44(7), district administrative authorities may not impose a NISG fine for conduct already fined by the Datenschutzbehörde under Article 58(2)(i) GDPR. The different GDPR maximum often quoted for other infringements should not be substituted for the notification provision. The report also does not add statutory maxima across regimes to produce an invented combined fine. [S36][S38]

10.8 One evidence record, several accountable decisions

Use a shared chronology while retaining separate decision records. The chronology should distinguish first observation, discovery, awareness, major classification, supplier notice, containment and restoration. Each reporting owner should state its legal test and submission receipt.

Decision	Evidence required	Completion record
NISG scope	Legal entity, activity and applicable category or exclusion	Approved scope rationale
NISG incident report	Significance and awareness basis	Required reports and follow-up schedule
DORA classification	Entity scope, ICT impact and classification basis	Classification time and applicable reports
GDPR notification	Personal-data breach, awareness and risk assessment	Notification or reasoned non-notification
Customer communication	Confirmed harm, useful action and safe contact route	Approved statement with update ownership
Police report	Potential offence and preserved evidence	Decision and report receipt where made

An exercise should reveal who covers absence, weekends and supplier uncertainty. It should end with evidence that the organisation can submit an accurate initial account while the investigation continues.

KEY TAKEAWAYS

01

Establish legal-entity scope before applying a reporting timetable.

02

Record awareness, discovery and major classification as distinct events.

03

Demonstrate reporting and control ownership through usable evidence and rehearsed handoffs.

CHAPTER 11

Outlook: conditional planning assumptions

11

THIS CHAPTER ANSWERS

Which plausible developments should change a defender's preparation?

4

scenarios with observable triggers and alternative explanations

11.1 Key judgements and confidence 99
11.2 Scenario one: a familiar business account requests a new action 99
11.3 Scenario two: a supplier restores service before data scope is known 100
11.4 Scenario three: an extortion claim appears during recovery 100
11.5 Scenario four: urgent patching exposes a service dependency 101
11.6 Review signals rather than calendar predictions 101

CHAPTER 11

Outlook: conditional planning assumptions

IN SHORT

The evidence justifies preparation for trusted-channel fraud, supplier uncertainty and extortion-related recovery. It does not support a numerical forecast of Austrian incidents. The scenarios below are conditional planning assumptions. Each has a trigger, an alternative explanation and a decision owner. Review the signals against your own environment and change the response when the evidence changes.

11.1 Key judgements and confidence

Confidence attaches to each proposition and its supporting population. It is not a general reputation score for a source or actor.

Judgement	Confidence	Basis	Important limit
Trusted-channel validation deserves near-term attention	High for the cited mechanism	CERT.at's mailbox, booking and BEC notices [S10][S11] [S12]	No measured national control-effectiveness claim
Recruitment-related access should inform relevant industrial response	Moderate for transfer to another organisation	CERT.at's source-assessed relationship and confirmed Austrian cases [S9]	Entry route must be verified for the individual case
Supplier incidents need customer-specific decisions	High for the response requirement	The different scopes in the November accounts [S28] [S29]	No prediction that a particular supplier will experience an incident
Extortion preparation should cover several claim labels	High for the listing distribution	61 listings across 22 labels [S2]	Claims are not confirmed outcomes or operator counts
Recent advisories justify conditional asset review	High for the advisories	Verified records and official technical notices [S7][S44] [S45]	Product exposure is not evidence of successful use

These judgements support a work programme. They do not estimate attack probability, expected loss or a deadline derived from how quickly advertisements recur.

11.2 Scenario one: a familiar business account requests a new action

Planning assumption. A trusted supplier's real mailbox sends a plausible document link or changed payment instruction. The organisation recognises the sender but has not independently confirmed the action.

Trigger. A change from the normal process, a new credential prompt, unexpected account access or a supplier warning makes the request relevant for review.

Alternative. The supplier can be making a legitimate change, or its display identity can be imitated without mailbox access. The message alone does not distinguish those possibilities.

Decision. The identity team reviews relevant access evidence; finance or the business owner confirms the requested action through an established channel. Do not make the technical team the sole authority for a payment decision.

Change signal. A confirmed legitimate instruction closes the fraud concern while any technical anomaly remains assessed separately. Confirmed misuse justifies scoped account and partner-response work. [S10][S12]

11.3 Scenario two: a supplier restores service before data scope is known

Planning assumption. A provider reports an incident and normal service, while it is still assessing which customer records were accessible.

Trigger. A customer uses the affected service, tenant or information category. That direct relevance requires an owned assessment, rather than a generic declaration of no impact.

Alternative. The incident can concern infrastructure outside the customer's tenant or data. A preliminary provider notice does not establish that every customer is affected.

Decision. The service owner obtains entity-specific scope. Privacy and compliance assess their triggers from the facts available. Customer operations prepares a safe verification route if follow-on impersonation becomes credible.

Change signal. Evidence excluding the tenant narrows the response. Confirmed access or credible misuse changes containment and communication. An operational restoration does not itself close those separate decisions. [S28][S29]

11.4 Scenario three: an extortion claim appears during recovery

Planning assumption. A criminal label lists the organisation while internal teams are restoring a service or assessing suspicious access.

Trigger. An authorised match between the claim and the organisation's actual records, systems or recent event makes the allegation relevant.

Alternative. The listing can reuse old information, misidentify an entity or assert an unsupported volume. Its presence is not enough to assign the incident's entry route or full scope.

Decision. Preserve the claim privately, validate its relevant elements and continue service recovery. Legal and communications should use the organisation's confirmed facts rather than the claimant's suggested narrative.

Change signal. Authentic, relevant evidence changes the data assessment. A repeated old claim can instead require a targeted customer warning or correction. Neither outcome makes every listed assertion true. [S2]

11.5 Scenario four: urgent patching exposes a service dependency

Planning assumption. A current advisory applies to a critical product, but correcting it requires a supplier change or a temporary service interruption.

Trigger. The installed build and configuration match the affected conditions. The owner should not substitute general brand recognition for that check.

Alternative. The service can run a corrected distributor build or a configuration outside the demonstrated condition. That needs evidence, rather than an assumption based on a version label alone.

Decision. The technical and business owners agree the correction, fallback and access review. A documented exception needs a review point and compensating action appropriate to the actual exposure.

Change signal. A verified correction changes exposure status. Evidence of earlier unauthorised access changes the investigation. A clean service test establishes restoration for that function, rather than proving that no earlier access occurred. [S7][S44][S45][S46]

11.6 Review signals rather than calendar predictions

The scenarios should be reviewed when relevant evidence changes. Useful signals include an owned account match, a supplier's revised tenant scope, a confirmed access event or a product-specific advisory update.

A changed count of visible posts is insufficient on its own. Visibility and repeated publication can change without an equivalent change in incidents. The analyst should state which new evidence changes the judgement and why.

Leadership should ask for the decision that follows. If the new observation changes no containment, recovery, payment or reporting choice, it can remain monitored context. If it changes a high-consequence choice, assign an owner and a time for the next evidence review.

KEY TAKEAWAYS

01

Use scenarios as planning assumptions with explicit evidence triggers.

02

Record alternatives that could narrow or reverse the response.

03

Update a judgement when the supporting proposition changes, rather than treating visibility as probability.

CHAPTER 12

Action plan

12

THIS CHAPTER ANSWERS

Which actions can teams finish and demonstrate over the next planning cycle?

30 / 60 / 90

days for prioritised work, subject to earlier incident and legal deadlines

12.1 Thirty, sixty and ninety days 103
12.2 Identity and incident response 104
12.3 Finance and customer protection 105
12.4 Service and supplier owners 105
12.5 Legal, privacy and communications 106
12.6 Leadership and assurance 106
12.7 How Brandefense can help 106

CHAPTER 12

Action plan

IN SHORT

Prioritise relevant identity signals, independent payment checks and critical supplier dependencies. Use the next planning cycle to prove that account containment, service fallback and reporting handoffs work together. The schedule below does not postpone an urgent incident action or statutory deadline. Assign each action to an owner, record a result and close the remaining uncertainty explicitly.

12.1 Thirty, sixty and ninety days

The schedule is a recommended planning sequence. Start incident response immediately where current evidence requires it; apply the actual reporting timetable from Chapter 10.

30 days		
Review relevant account and supplier alerts against owned assets	OWNER Identity lead and service owners	COMPLETION EVIDENCE Account, tenant, date and disposition recorded
Verify the process for supplier bank-detail changes	OWNER Finance operations	COMPLETION EVIDENCE Independent callback and separate approval demonstrated
Confirm critical suppliers' incident and escalation contacts	OWNER Procurement and service owners	COMPLETION EVIDENCE Tested contacts, data roles and required evidence identified
Establish NISG, DORA and GDPR applicability for each relevant entity	OWNER Legal, compliance and privacy	COMPLETION EVIDENCE Scope register with named reporting owners
Review applicable urgent advisories and critical-service exceptions	OWNER Infrastructure and application owners	COMPLETION EVIDENCE Correct build or documented remediation and fallback plan

260 days

Exercise a real-mailbox fraud scenario with finance and customer support

OWNER

CISO and fraud lead

COMPLETION EVIDENCE

Safe verification, containment and transaction decisions demonstrated

Restore a critical service under an identity or supplier outage assumption

OWNER

Business continuity and technical owner

COMPLETION EVIDENCE

Essential task completed through a tested route

Test supplier information handoffs with privacy and compliance

OWNER

Vendor management and reporting leads

COMPLETION EVIDENCE

Entity-specific scope and first-report information produced

Review mail rules, privileged changes and emergency account recovery

OWNER

Identity and mail teams

COMPLETION EVIDENCE

Authorised checks, exceptions and escalation route recorded

390 days

Rehearse the extortion and data-scope communication process

OWNER

Incident commander and communications

COMPLETION EVIDENCE

Confirmed facts, unknowns, safe contact and update time approved

Retest corrections and close service-dependent exceptions

OWNER

Control and business owners

COMPLETION EVIDENCE

Evidence of correction, residual risk and next review

Review programme outcomes with leadership

OWNER

CISO and executive sponsor

COMPLETION EVIDENCE

Open decisions, completion evidence and resourcing agreed

12.2 Identity and incident response

Begin with account authority. A relevant alert should reach a team that can establish whether the account exists, what it can access and whether it remains active. The analyst should not need to guess which administrator owns the service.

When misuse is established, select containment around the actual identity and sessions. Review privileges, recovery methods, forwarding and connected applications where relevant. Record which actions were completed and which questions still require evidence.

Include a safe recovery route for legitimate users. A broad reset without usable recovery can leave people dependent on an unsafe workaround. The support team should be able to verify an exception without relying only on the affected account.

Completion is a reviewed case with an owner, an access determination and a documented outcome. A closed alert queue is not enough if the affected service or recovery route remains untested.

12.3 Finance and customer protection

Finance should demonstrate an independent confirmation of a changed payment instruction. The confirming number or channel should come from a previously established record. A second person approving the same deceptive message is not the same control.

Customer teams should know the organisation's genuine payment and support process. Their explanation must be useful to someone who sees real booking details, a familiar sender or an apparent security emergency.

Provide an escalation for people who have already transferred money, installed remote-control software or shared credentials. The next action can be time-sensitive. Support should reach the appropriate authorised payment, identity or incident team without asking the person to collect dangerous material.

A completed exercise should show the actual handoff and decision, including how it works outside normal hours. It should also reveal whether staff understand recovery-fee fraud and can give a safe alternative contact.

12.4 Service and supplier owners

For each critical service, identify the function that must continue, the identity dependency and the supplier's administrative reach. Record the data categories and legal roles. A supplier name and annual contract value do not answer those questions.

Ask for incident evidence relevant to your service: affected tenant, relevant access period, information categories and containment status. A provider's general status update should be retained as that provider's statement, rather than expanded into your own assurance.

Demonstrate a fallback under a stated failure. The result should show that staff or customers can complete the essential task. It should also show how normal access is restored and who authorises reopening.

Completion can reveal a limitation that cannot be corrected immediately. Record the business consequence, interim control and review owner. Leaving that limitation explicit is more useful than calling the service resilient without a tested basis.

12.5 Legal, privacy and communications

Legal and compliance should maintain the entity-specific scope record. The record needs a responsible person and a substitute, not only a link to legislation. Recheck it when an activity, supplier relationship or legal category changes.

During an event, record the different clock-starting propositions. Discovery, awareness and major classification can occur at different times. A clear chronology supports later review and prevents a handoff from erasing an earlier decision.

Communications should distinguish an allegation, confirmed access, information viewed and service disruption. State what people should do and how they can verify the message. Preserve the source and date when repeating an organisation's assurance or unresolved limitation.

The completion evidence is a usable first account, a reasoned notification decision and an owned update schedule. A perfectly complete attribution narrative is unnecessary before those preparations can work.

12.6 Leadership and assurance

Leadership should review a small set of decisions with evidence. Which relevant accounts remain unresolved? Which critical service has an untested fallback? Which supplier cannot supply scoped incident information? Which reporting role lacks cover?

These questions are more useful than asking for a national risk ranking inferred from posts. They connect the cited mechanisms to responsibilities the organisation can change and demonstrate.

The executive sponsor should resolve resource conflicts revealed by exercises. Security cannot unilaterally decide the acceptable loss of a customer service, while a business owner should not waive an urgent correction without understanding the exposure.

12.7 How Brandefense can help

Brandefense supports threat-intelligence, digital-risk and external-attack-surface workflows. [S8] In this report, retained posts, Ransompedia listings and dated observations support validation priorities. They do not replace the organisation's own access evidence or statutory decisions.

A useful engagement starts with the assets, services and decisions the organisation needs to protect. Relevant external signals can then be assigned to identity, service, fraud or incident owners with a clear validation question.

Discuss the report's findings and an organisation-specific validation workflow with Brandefense: https://brandefense.io/request-a-demo/ . The engagement should retain the same evidence boundaries as the report.

KEY TAKEAWAYS

01

Assign each action to the owner who can validate and finish it.

02

Test payment, supplier and reporting handoffs alongside technical containment.

03

Close work with service and evidence outcomes, while keeping residual uncertainty owned.

APPENDICES

Appendices

A–D

THIS CHAPTER ANSWERS

Which definitions and source boundaries support the report's decisions?

4

appendices for scope, evidence, sources and terminology

Appendix A. Scope, sources and confidence 109
Appendix B. Evidence register 113
Appendix C. Sources 116
Appendix D. Glossary 119

Appendix A. Scope, sources and confidence

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

A.1 Window and timestamp meaning

The report covers Austria from 1 January through 22 November 2026. The recent-activity period is 8–22 November. Underground dates refer to publication time, rather than proving when access began, information was obtained or a transaction occurred. [S1]

Ransomware listings use the dated listing population within that requested window. The comparison countries use the same period. A listing can refer to an older event; its date is not automatically an intrusion date. [S2]

Linked external sources, NVD records and authority notices were verified on 27 November 2026. Retained own-data snapshots and withheld primary notices carry their individual verification dates in Appendix C. Verification after 22 November does not extend the reporting window beyond 22 November. An annual report about 2025 remains a 2025 population even when published during 2026.

Passive observations form a dated snapshot completed across 23–27 November 2026. They do not describe every day of the reporting window. The report does not infer a control's earlier state from that later observation. [S3]

A.2 Source populations

The report combines the following kinds of evidence without adding them into one national incident total.

Source population	Unit	Important limit
Underground material collected by Odin by Brandefense	Published posts and advertisements	Claims, repeats and country associations do not establish independent incidents
Ransompedia	Dated extortion listings	Criminal assertions; repeated organisations and uncertain country labels can occur
Selected-domain portfolio	Domain and associated service	Related groups and unresolved legal ownership limit organisational interpretation
Passive DNS and TLS observations	Dated control observation	Partial service view; unobserved does not automatically mean absent
Official disclosures	Source-confirmed facts within a statement	Actor, record count and full scope can remain unresolved

Source population	Unit	Important limit
Campaign notices	Authority's described mechanism or campaign	No complete national victim count is inferred
Police or regulator statistics	Defined reports or cases in the source's period	Different categories, years and overlap prevent simple addition

Sources [S1][S2][S3][S6] define the report's own-data populations. Appendix C identifies the external notices used for context and case interpretation.

A.3 The selected portfolio and measured coverage

The portfolio comprises 250 selected domains across ten sector groups. It is not a revenue ranking, a random sample or a nationally representative census. A selected domain does not establish independent legal identity or validated ownership for every represented service. [S6]

Passive observations cover all 250 selected domains (23–27 November snapshot). Overall, 149 domains (59.6%) publish DMARC enforcement policies and 239 (95.6%) publish SPF. Valid TLS appears on 240 domains (96.0%, with 6 unsuccessful and 4 unavailable), and HSTS appears on 184 of 247 recorded HTTP responses (3 unavailable). Each control retains its measured denominator, and no hygiene rating or sector ranking is published. [S3]

Exposure observations cover 249 of 250 selected domains on 23 November; one has no complete record. 49 observed domains (19.7%) have a current credential offer. The national Atlas headline is 47/100 (B) for the observed selected portfolio. Missing quantities remain unknown, and no sector ratings are published. [S4]

Similar-name observations cover 19 October–18 November. Rolling message associations cover 365 days ending 22 November across all 250 selected domains, with the 2026 subset reported separately. Device, credential and document associations can overlap across domains, sources and people. Their totals do not measure unique people, confirmed intrusions or national prevalence. [S4]

A.4 Ransomware and comparison interpretation

Ransompedia records 61 Austrian listings across 56 distinct entity names within the requested window (four entities appear more than once, accounting for five repeat entries). The 38 listings for all of 2025 are a full-year retrospect-
ive, rather than a matched-period comparison. Group and sector labels describe that listing population. [S2]

The peer figures describe separate national listing and underground-post populations. They are not adjusted for population, economic structure, organisational size or visibility. No attack probability, political assessment or control-effectiveness ranking is derived from them.

A.5 Card material has a separate narrow scope

SCOPE OF THE CARD FIGURES

Card figures cover only payment cards that appeared in clear text in dark-web posts collected for the report. Brandefense detects stolen cards through other methods outside this view. These figures do not measure total theft, valid cards, completed payments or fraud loss.

The 88-card population comes from 100 country-labelled posts and remains within this narrow scope. [S5]

A card-post observation is distinct from issuer confirmation, a valid account and a fraudulent transaction. Issuer action requires an authorised assessment of relevance, freshness, previous remediation and actual misuse. The report makes no national extrapolation from that material. [S5]

A.6 Public reporting and remaining coverage limits

The official source review considers campaign publications as well as organisation disclosures. It distinguishes current events, retrospective statistics, preventive warnings, exercises and unrelated physical outages. A source with no published notice for a month does not establish that no incidents occurred.

The reviewed BK, BMI and DSN archives cover the requested calendar window. Official pages for NISG 2026 statutory sections, BCS legal guidance, BMI registration notices, DSB breach guidance and FMA DORA guidance were verified on 27 November. DSB's public announcement board (20 July–19 November 2026, verified 27 November) contains no interim 2026 breach statistics, leaving the 2025 activity report as the latest published baseline. FMA publishes no chronological public news archive, so coverage of FMA notices for February–May 2026 is incomplete. No complete national incident-notification census for 2026 is inferred from them. [S30][S31][S38][S39][S40][S54][S64]

A press report quoting an official statement is identified as that form of evidence. Where an original release was unavailable, the report does not claim to have read it. A source's negative finding retains its date and stated scope.

A.7 Confidence and alternative explanations

Evidence proposition	Confidence language	What remains separate
A retained message or listing exists	High for the observation	Authenticity and truth of the underlying assertion
An official statement confirms specified access	High for the stated confirmation	Unresolved record counts, actor and wider system reach
A source assesses a campaign relationship	Attribute the assessment and its uncertainty	Identity of every participant or applicability to every case
A defensive scenario follows from mechanisms	Conditional planning assumption	Probability or predicted loss
A post or dataset resembles another	Association with a stated limit	Common operator, file identity or completed transfer

Alternative explanations matter because they can change containment. Historical records, copied advertising, related entities and legitimate service use can all affect interpretation. Their possibility does not prove a claim false; it identifies the evidence still needed.

A.8 Naming, technical details and political neutrality

Victims are described through broad roles unless the naming requirements are met. Dates, regional publisher roots and narrow descriptors are generalised where their combination could indirectly identify a withheld organisation. Source entries omit a withheld organisation's own domain. A press or official publisher's national root can replace an identifying article URL, with the withholding stated.

The report publishes no credentials, personal records, card numbers, criminal contact routes or operational attack instructions. Technical warnings support defensive product and configuration review. They do not reproduce an exploit procedure.

Political claims remain attributed to their source where relevant. The authors take no position on government decisions, parties, elections, neutrality or international conflicts. Language, a claimed cause and a public target do not establish nationality or sponsorship.

Appendix B. Evidence register

The register links case narratives to their public source references. A campaign entry is not a count of independent victims. Withheld-organisation cases use year-, seasonal or month-level dating to prevent indirect identification. The letter and evidence identifier name the narrative, rather than its confidence.

Evidence	Date	Type	Case and section	Sources
O01	Early 2026	Institution disclosure and updates	A · §5.2	S25
O02	Early 2026	Institution ransomware and scope notice	B · §5.2	S58
O03	2026-04-01	Police campaign warning	C · §5.3	S18
O04	2026-04-07	Police campaign warning	D · §5.3	S17, S16
O05	2026-04-29	Police investigation account	E · §5.3	S19
O06	2026-05-26	CERT campaign assessment	F · §5.4	S9
O07	2026	Spokesperson account in press	G · §5.4	S26
O08	2026-07-24	CERT campaign warning	H · §5.4	S10
O09	2026-08-14	CERT campaign warning	I · §5.4	S11
O10	2026-08-26	CERT campaign warning	J · §5.4	S12
O11	2026-10-29	Police campaign warning	K · §5.5	S20
O12	Autumn 2026	Company account in press	L · §5.5	S27
O13	November 2026	Supplier statement and updates	M · §5.5	S28
O14	November 2026	Public-body statement in press	N · §5.5	S29
O15	November 2026	Press-quoted scope update	O · §5.5	S55

Evidence	Date	Type	Case and section	Sources
O16	November 2026	Company account in press	P · §5.5	S56
O17	Autumn 2026	Operator notice on two supplier events	Q · §5.5	S57

The retained-post cards preserve redacted source wording. Venues are described by type. Private seller aliases and contact routes are withheld; selected public actor labels are retained. The table does not identify independent human operators.

Evidence	Date	Venue and language	Case and section	Source
B01	2026-01-08	Forum; English	U · §4.4	S1
B02	2026-01-27	Forum; English	U · §4.4	S1
B03	2026-02-01	Forum; Russian and English	V · §4.4	S1
B04	2026-02-02	Forum; English	W · §4.4	S1
B05	2026-04-11	Forum; English	§4.5	S1
B06	2026-04-18	Forum; English	X · §4.4	S1
B07	2026-09-22	Forum; English	Y · §4.4	S1
B08	2026-10-15	Forum; English	Y · §4.4	S1
B09	2026-11-20	Forum; English	Z · §4.4	S1
B10	2026-11-22	Forum; English	Z · §4.4	S1
B11	2026-06-21	Forum; Russian	§8.5	S1
B12	2026-10-20	Forum; English	§8.5	S1
B13	2026-05-08	Messaging source; English	§6.2	S1
B14	2026-05-17	Messaging source; English	§6.2	S1
B15	2026-05-08	Relayed claim; English	§6.2	S1
B16	2026-03-26	Messaging source; Arabic and English	§6.2	S1
B17	May 2026	Messaging source; English	§6.2	S1
B18	May 2026	Roundup relay; Russian	§6.3	S1

Evidence	Date	Venue and language	Case and section	Source
B19	2026 (date unresolved)	Forum; English	§4.5	S1
B20	2026-11-18	Messaging source; English	§4.6	S1

Appendix C. Sources

The entries below identify the sources used for this report and each entry's verification date. Linked external sources, NVD records and passive observations were verified on 27 November 2026. Verification after 22 November does not extend the reporting window beyond 22 November. An article-URL withholding or an empty victim URL protects the organisation without changing the source's evidence status.

S1: Odin by Brandefense. Austria-associated underground message observations. Retained own evidence; source records are private. Verified on 23 November 2026.

S2: Ransompedia. Austria and regional-peer extortion listings. Retained own evidence; source records are private. Verified on 23 November 2026.

S3: Odin by Brandefense. Selected-domain passive control observations across all 250 selected domains (23–27 November 2026 snapshot). Retained own evidence; source records are private. Verified on 27 November 2026.

S4: Brandefense Atlas and Odin by Brandefense. Selected-domain exposure observations, dated 23 November 2026, with source-specific periods stated in the report. Retained own evidence; identifiers remain private. Verified on 23 November 2026.

S5: Odin by Brandefense. Country-labelled payment-card observations in posts. Retained own evidence; source records are private. Verified on 23 November 2026.

S6: Odin by Brandefense. Selected Austria domain portfolio. Retained own evidence; source records are private. Verified on 27 November 2026.

S7: NIST National Vulnerability Database. Selected vulnerability records: CVE-2026-114938; CVE-2026-129289; CVE-2026-115560; CVE-2026-86218; CVE-2026-41940. Verified on 27 November 2026.

S8: Brandefense. Threat-intelligence, digital-risk and attack-surface capabilities. https://brandefense.io/request-a-demo/ Verified on 27 November 2026.

S9: CERT.at. Recruitment-lure campaign and source-assessed access relationship. https://www.cert.at/de/aktuelles/2026/5/zipline-qilin-raas-update. Verified on 27 November 2026.

S10: CERT.at. Phishing from legitimate Austrian business email accounts. https://www.cert.at/de/aktuelles/2026/7/vermehrt-phishing-mails-von-legitimen-e-mail-adressen-aus-osterreich. Verified on 27 November 2026.

S11: CERT.at. Fraud involving travel-booking platforms. https://www.cert.at/de/aktuelles/2026/8/vermehrt-betrugsversuche-auf-buchungsplattformen-bookingcom. Verified on 27 November 2026.

S12: CERT.at. Increased business-email fraud attempts. https://www.cert.at/de/aktuelles/2026/8/vermehrt-betrugsversuche-durch-business-email-compromise-bec. Verified on 27 November 2026.

S13: CERT.at. Fire-related fibre interruption. https://www.cert.at/de/aktuelles/2026/6/brand-der-floridsdorfer-brucke-glasfaserausfalle-in-wien. Verified on 27 November 2026.

S14: GovCERT. Public-administration remit. https://www.govcert.gv.at/en/. Verified on 27 November 2026.

S15: Bundeskriminalamt. Cybercrime Report 2025: official retrospective. https://www.bundeskriminalamt.at/newsb0e5.html?id=42307473384354634638 6f3d. Verified on 27 November 2026.

S16: Bundeskriminalamt. October phishing prevention, 2025–2026 case context and OeNB/RTR statements. https://www.bundeskriminalamt.at/newsdb49.html?id=654461744b54696b6d66453d. Verified on 27 November 2026.

S17: Bundeskriminalamt. Digital-identity renewal impersonation warning. https://www.bundeskriminalamt.at/news7481.html?id=6f45367243466c735631633d. Verified on 27 November 2026.

S18: Bundeskriminalamt. Bank-themed SMS and false support calls. https://www.bundeskriminalamt.at/newsea73.html?id=687574376f3455315132733d. Verified on 27 November 2026.

S19: Bundeskriminalamt. Investment and recovery-fraud investigation. https://www.bundeskriminalamt.at/newsb7b9.html?id=6d4b6c4b525341374c7a633d. Verified on 27 November 2026.

S20: Bundeskriminalamt. Social-media task and job fraud. https://www.bundeskriminalamt.at/newsd00f.html?id=74776d6a304e646536346f3d. Verified on 27 November 2026.

S21: Bundeskriminalamt. Operation TorNado retrospective. https://www.bundeskriminalamt.at/news3d42.html?id=446763694e4c42574733383d. Verified on 27 November 2026.

S22: Bundeskriminalamt. International proxy-service operation. https://www.bundeskriminalamt.at/newsb165.html?id=426e%342784932736949683 43d. Verified on 27 November 2026.

S23: Bundesministerium für Finanzen. Fraudulent payment reminders and official-looking notices. https://www.bmf.gv.at/presse/pressemeldungen/2026/jaenner-2026/email-phishing.html. Verified on 27 November 2026.

S24: Bundesministerium für Finanzen. Fraudulent messages, calls and imitation service websites. https://www.bmf.gv.at/presse/pressemeldungen/2026/februar-2026/phishing.html. Verified on 27 November 2026.

S25: Education institution. Directory-access notice and updates (early 2026). URL withheld to protect the organisation. Verified on 23 November 2026.

S26: Heute. Mailbox-document disclosure (2026). https://www.heute.at/ (article URL withheld). Verified on 27 November 2026.

S27: ORF. Project-based organisation: autumn 2026 cyber incident. https://orf.at/ (article URL withheld). Verified on 27 November 2026.

S28: Commercial software and hosting supplier. Hosted-infrastructure incident updates (November 2026). URL withheld to protect the organisation. Verified on 23 November 2026.

S29: ORF. Public-administration externally operated website disclosure (November 2026). https://orf.at/ (article URL withheld). Verified on 27 November 2026.

S30: Bundesamt für Cybersicherheit. NISG 2026 commencement and official legal FAQ. https://www.bundesamt-cybersicherheit.gv.at/faq/gesetzgebung.html. Verified on 27 November 2026.

S31: RIS. NISG 2026 section 24: scope and exclusions. https://ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273885/NOR40273885.html. Verified on 27 November 2026.

S32: RIS. NISG 2026 section 34: reporting duties. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273895/NOR40273895.html. Verified on 27 November 2026.

S33: RIS. NISG 2026 section 29: entity register. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273890/NOR40273890.html. Verified on 27 November 2026.

S34: RIS. NISG 2026 section 31: governance. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273892/NOR40273892.html. Verified on 27 November 2026.

S35: RIS. NISG 2026 section 32: risk-management measures. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273893/NOR40273893.html. Verified on 27 November 2026.

S36: RIS. NISG 2026 section 44: general penalty conditions and GDPR non-stacking. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273905/NOR40273905.html. Verified on 27 November 2026.

S37: RIS. NISG 2026 section 45: administrative penalties. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273906/NOR40273906.html. Verified on 27 November 2026.

S38: Datenschutzbehörde. Personal-data breach notification guidance. https://dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach. Verified on 27 November 2026.

S39: Datenschutzbehörde. Activity Report 2025: security breach notifications. https://dsb.gv.at/sites/site0344/media/downloads/taetigkeitsbericht_2025_v4.pdf. Verified on 27 November 2026.

S40: FMA. DORA: ICT-related incidents. https://www.fma.gv.at/querschnittsthemen/dora/dora-ikt-bezogene-vorfaelle/. Verified on 27 November 2026.

S41: FMA. Official retrospective of fraud trends in 2025. https://www.fma.gv.at/deepfakes-whatsapp-gruppen-und-ki-bots-waren-die-trends-des-jahres-2025/. Verified on 27 November 2026.

S42: FMA. DORA supervisory activities. https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/. Verified on 27 November 2026.

S43: DSN. Announcement of the 2025 security assessment. https://www.dsn.gv.at/news4c8c.html?id=51326d6a3669786c3674773d. Verified on 27 November 2026.

S44: CERT.at. Java4Shell advisory and corrected releases. https://www.cert.at/de/warnungen/2026/11/kritische-sicherheitslucke-in-java-java4shell-updates-verfugbar-cve-2026-114938. Verified on 27 November 2026.

S45: CERT.at. PHP security corrections and configuration conditions. https://www.cert.at/de/warnungen/2026/11/kritische-sicherheitslucken-in-php-updates-verfugbar2. Verified on 27 November 2026.

S46: CERT.at. N-central active-exploitation warning. https://www.cert.at/de/aktuelles/2026/9/schwerwiegende-sicherheitslucke-in-n-able-n-central-aktiv-ausgenutzt. Verified on 27 November 2026.

S47: CERT.at. Hosting-management active-exploitation warning. https://www.cert.at/de/aktuelles/2026/4/aktive-ausnutzung-einer-schwerwiegenden-sicherheitslucke-in-cpanel-und-whm. Verified on 27 November 2026.

S48: BMI. National response to the NGINX warning. https://www.bmi.gv.at/news9983.html?id=4d506163634349312b716f3d. Verified on 27 November 2026.

S49: BMI. Cyber-security authority begins its published responsibilities. https://www.bmi.gv.at/news84e1.html?id=766f584a777255376d66513d. Verified on 27 November 2026.

S50: FMA. DORA: general applicability questions. https://www.fma.gv.at/querschnittsthemen/dora/dora-allgemeine-fragen/. Verified on 27 November 2026.

S51: Bundeskriminalamt. Romance-scam prevention warning. https://www.bundeskriminalamt.at/newsb89e.html?id=694a5669486857434163383d. Verified on 27 November 2026.

S52: Bundeskriminalamt. Seasonal online-shopping fraud warning. https://www.bundeskriminalamt.at/newsbb44.html?id=725a476d7a5342547269553d. Verified on 27 November 2026.

S53: ORF. Healthcare logistics cyber exercise (May 2026). https://orf.at/ (article URL withheld). Verified on 27 November 2026.

S54: BMI. NISG 2026 framework, registration and reporting. https://www.bmi.gv.at/504/. Verified on 27 November 2026.

S55: ORF. Public-administration update concerning an earlier 2026 data incident. https://orf.at/ (article URL withheld). Verified on 27 November 2026.

S56: ORF. Hospitality operator supplier event and guest payment-deception warning (November 2026). https://orf.at/ (article URL withheld). Verified on 27 November 2026.

S57: Accommodation operator. Notice concerning two separate supplier incidents (autumn 2026). URL withheld to protect the organisation. Verified on 23 November 2026.

S58: Education institution. Notice concerning ransomware and unresolved data scope (early 2026). URL withheld to protect the organisation. Verified on 23 November 2026.

S59: European Commission / EUR-Lex. Delegated Regulation 2025/301, Article 5: incident reporting time limits. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng. Verified on 27 November 2026.

S60: NIST. Terminology for OTP, ICS and ICT, and one-time-code authentication guidance. https://csrc.nist.gov/glossary/term/one_time_password; https://csrc.nist.gov/glossary/term/ics; https://csrc.nist.gov/glossary/term/ict; https://pages.nist.gov/800-63-4/sp800-63b.html. Verified on 27 November 2026.

S61: PHP. FastCGI Process Manager manual. https://www.php.net/manual/en/book.fpm.php. Verified on 27 November 2026.

S62: Bundesverband deutscher Banken. Online banking with PIN and TAN: transaction authorisation. https://bankenverband.de/verbraucher/onlinebanking-sicher-mit-pin-und-tan. Verified on 27 November 2026.

S63: DataReportal. Digital 2026: Austria (published 8 November 2025; late-2025 baseline context). https://datareportal.com/reports/digital-2026-austria. Verified on 27 November 2026.

S64: Datenschutzbehörde. Public announcement board (Bekanntmachungen). https://dsb.gv.at/aktuelles. Verified on 27 November 2026.

Appendix D. Glossary

The definitions support interpretation of the report. They are not claims that every technique was used in an Austrian case.

Term	Plain definition
Account session	A continuing authenticated interaction that can remain relevant after a password changes
Administrative directory	A service holding identities and permissions used to manage access across systems
BEC	Business email compromise: deception using business identity or correspondence to obtain money or information
CAA	Certification Authority Authorization: a DNS record specifying which certificate authorities are authorised to issue certificates for a domain
Claim	An assertion whose underlying event is not established merely by its publication
Credential record	Recorded authentication-related information; its presence does not establish current validity
CSIRT	A team responsible for coordinating or assisting response to computer-security incidents
DMARC	A domain policy connecting email authentication results to requested handling and reporting
DKIM	A method that lets a sending service sign email for verification by recipients
DORA	The EU financial-sector digital operational resilience framework, with defined entity scope and ICT duties
DS record	A DNS delegation record associated with DNSSEC; observing one is not a full chain validation
DDoS	Traffic intended to overwhelm a service's availability; a claim requires impact verification
FPM	FastCGI Process Manager: PHP software that manages processes handling web requests through FastCGI [S61]
HSTS	A web policy instructing supporting browsers to use secure transport for the covered service
ICS	Industrial control system: a system used to control industrial processes [S60]
ICT	Information and communication technology: technology used to process, store and exchange information [S60]

Term	Plain definition
Identity recovery	A process that restores legitimate account access through trusted verification
Listing	A public extortion-related entry; it records a criminal assertion rather than a verified outcome
MFA	Authentication using more than one type of factor; the implementation and recovery routes matter
NISG 2026	Austria's Network and Information Systems Security Act 2026, with defined security and reporting duties
OTP	One-time password: an authentication code accepted only once while valid [S60]
Persona	A public-facing account or alias; not necessarily one independently identified person
Phishing	Deceptive communication intended to induce unsafe disclosure or action
Ransomware	Malicious software associated with extortion, often through disruption or encryption; a listing alone does not establish its use
SPF	An email-domain record identifying authorised sending infra-structure
Supplier scope	The specific services, tenants, data and time affected in the supplier relationship
TAN	Transaction authentication number: a one-time code used to authorise an online banking instruction [S62]
Tenant	A logically separated customer environment within a shared service
TLS	A secure-transport protocol; a valid observation does not establish application authorisation

About this report

This report supports security leadership, incident response, infrastructure, fraud, privacy and customer-service decisions. It is public research by Odin by Brandefense, using explicit evidence labels and source-specific limitations.

Its selected cases and observations do not represent every Austrian incident or every affected person. A country's visible posts and listings should not be interpreted as a national risk score. Operational and reporting decisions require the organisation's own facts and competent advice.

The English master is the reference edition. Translated editions preserve its figures, evidence identifiers, source references and directives, with a visible AI-translation notice.

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