BRANDEFENSE COUNTRY REPORT · AUSTRIA 2026

Brandefense Bericht zur Cyberbedrohungslage in Österreich 2026

Identitäten, Dienstleisterzugriff und Zahlungsvertrauen über verbundene Dienste hinweg

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

250
ausgewählte Domains im beschreibenden Portfolio

17
ausführliche amtliche oder quellenbasiert berichtete Falldarstellungen

61
österreichische Ransomware-Einträge im angefragten Zeitraum; kriminelle Behauptungen

1. Oktober 2026
vollständiges Inkrafttreten des österreichischen NISG 2026

INHALT

Inhalt

Translated with AI

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

01	Zusammenfassung	05
	Berichtskarte	10
02	Österreichs digitaler Kontext und Bedrohungsumfeld	11
03	Nationale Exposition: das ausgewählte Domainportfolio	16
04	Angebote im Dark Web und die Grenzen ihrer Belege	30
05	Beispiele für Zielauswahl nach Sektor	45
06	Hacktivismus, DDoS und Dienstverfügbarkeit	63
07	Bedrohungsakteure und belegte Beziehungen	72
08	Betrugsökonomie: Identität, Kontext und Zahlung	87
09	Banken im Detail	93
10	Regulierung und nationale Reaktion	99
11	Ausblick: bedingte Planungsannahmen	106
12	Maßnahmenplan	111
	Anhänge	117
A	Anhang A. Umfang, Quellen und Vertrauen	118
B	Anhang B. Belegregister	122
C	Anhang C. Quellen	125
D	Anhang D. Glossar	128
	Über diesen Bericht	130

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

Über diese Ausgabe

Mit KI übersetzt. Bei Abweichungen ist die englische Ausgabe maßgeblich.

Mit KI-Unterstützung erstellt. Belege, Unsicherheit und Abdeckungsgrenzen begleiten die Ergebnisse.

Österreichs dokumentierte Kampagnen verbinden Kontomissbrauch, Dienstleistergefährdung und Zahlungstäuschung. Die Abwehr sollte jedes Signal prüfen, bestätigten Zugriff eindämmen und die von Menschen benötigten Dienste erhalten.

34.261

Beiträge mit Österreichbezug in Monats- und Plattformansichten; keine Vorfallzahl

61

österreichische Ransomware-Einträge über 56 eindeutige Namen; kriminelle Behauptungen

49 von 249

beobachtete Domains hatten bei der Prüfung ein Zugangsdatenangebot

47 / 100 (B)

nationaler Atlas-Gesamtwert für das beobachtete ausgewählte Portfolio; Momentaufnahme vom 23. November

Inhalt und Lesewege

Kapitel	Frage
1 Zusammenfassung	Welche Entscheidungen haben Vorrang?
2 Österreichs digitaler Kontext und Bedrohungsumfeld	Welche österreichischen Abhängigkeiten verändern die Reaktion?
3 Nationale Exposition: das ausgewählte Domainportfolio	Was belegt das ausgewählte Portfolio?
4 Angebote im Dark Web und die Grenzen ihrer Belege	Was bedeutet ein beobachtetes Angebot tatsächlich?
5 Beispiele für Zielauswahl nach Sektor	Was haben Organisationen und Behörden bestätigt?
6 Hacktivismus, DDoS und Dienstverfügbarkeit	Wie lassen sich Behauptungen und Dienstfolgen trennen?
7 Bedrohungsakteure und belegte Beziehungen	Welche Zuordnungen und technischen Warnungen sind belegt?
8 Betrugsökonomie: Identität, Kontext und Zahlung	Wie kann vertrauter Kontext zur Zahlungsanweisung werden?
9 Banken im Detail	Welche Identitäts-, Zahlungs- und Dienstleisterentscheidungen brauchen Abstimmung?
10 Regulierung und nationale Reaktion	Welche Geltungsbereichsprüfungen, Pflichten und Meldefristen gelten?
11 Ausblick: bedingte Planungsannahmen	Welche bedingten Szenarien rechtfertigen Vorbereitung?
12 Maßnahmenplan	Wer handelt, und was belegt den Abschluss?
Anhänge A–D	Umfang, Belegregister, Quellen und Definitionen

KAPITEL 01

Zusammenfassung

01

DIESES KAPITEL BEANTWORTET

Welche Ergebnisse rechtfertigen unmittelbare Entscheidungen für österreichische Organisationen?

4

Entscheidungen verbinden die Belege mit einem praktischen Abschluss

Vier Entscheidungen für Führungskräfte 07

Das Jahr in Zahlen 07

KAPITEL 01

Zusammenfassung

KURZFASSUNG

Österreichische Hinweise beschreiben erpressungsbezogene Bewerbungsköder, Phishing über echte Geschäftspostfächer und Zahlungsforderungen mit glaubhaftem Kontext. Bestätigte Mitteilungen zeigen, dass administrativer Zugriff, Dokumentenoffenlegung und Betriebsstörung unterschiedliche Belege brauchen. Das jüngste Zeitfenster ergänzt Dienstleisteraktualisierungen und dringende Softwarehinweise. Prüfen Sie relevante Konten, bestätigen Sie Zahlungsänderungen unabhängig, üben Sie Dienstleisterwiederherstellung und weisen Sie Meldeentscheidungen zu, bevor ein Vorfall sie erzwingt.

Dieser Bericht verbindet Beobachtungen von Odin by Brandefense, Ransompedia-Einträge, ausgewählte Domainbeobachtungen und in ihren Quellen gelesene öffentliche Hinweise. Beiträge, Einträge, Meldungen und bestätigte Vorfälle bleiben getrennte Populationen. Sie werden nicht zu einer österreichischen Angriffssumme addiert. [S1] [S2][S3][S6]

Der Berichtszeitraum reicht vom 1. Januar bis 22. November 2026; für Untergrundmaterial gilt die Veröffentlichungszeit. Verlinkte externe Quellen, NVD-Einträge und Behördenhinweise wurden am 27. November 2026 geprüft; das Prüfdatum jeder Quelle steht in Anhang C. Die spätere Prüfung erweitert das Vorfallfenster nicht. Datierte Aktualisierungen im Schlusszeitraum werden vom Vorfallbeginn unterschieden.

1. Identitätsprüfung wirkt über eine Passwortzurücksetzung hinaus. Die CERT.at-Warnung vom Juli beschreibt Phishing über echte Postfächer österreichischer Unternehmen. Eine Mitteilung aus dem Bildungsbereich von Anfang 2026 beschreibt gesondert administrativen Verzeichniszugriff und eine Kontozurücksetzung. Die passende Reaktion prüft Sitzungen, Berechtigungen, Wiederherstellungswege und verbundenen Datenzugriff. [S10][S25]

2. Überzeugender Geschäftskontext autorisiert keine Zahlung. Österreichische Kampagnenhinweise beschreiben Bewerbungskorrespondenz, Rechnungsänderungen und Nachrichten mit echten Buchungsdetails. Die Mechanismen nutzen unterschiedliche Wege. Alle sprechen aber für unabhängige Bestätigung vor Anhang, Zugangsdatenübermittlung oder Zahlung. [S9][S11][S12]

3. Der Dienstleisterumfang bestimmt die nächste Kundenentscheidung. Novembermitteilungen betreffen gehostete Infrastruktur, Beherbergungsdienstleister und einen extern betriebenen öffentlich zugänglichen Dienst. Sie belegen weder ein Eindringen in sämtliche Kundensysteme noch den Ausfall aller Dienstfunktionen. Jeder Kunde braucht eine eingegrenzte Bewertung des jeweiligen Anbieters. [S28][S29][S56][S57]

4. Aktuelle Zugangsdatenangebote erfordern die Prüfung eigener Konten. Von 249 beobachteten Domains hatten 49 (19,7%) bei der Prüfung am 23. November Zugangsdaten im Angebot. Das Portfolio erfasst mindestens 124.110 Gerätezuordnungen und 3.900.001 Zugangsdatenzuordnungen. Diese überlappenden Beobachtungen sind keine eindeutigen Personen oder bestätigten Einbrüche. Der nationale Atlas-Gesamtwert beträgt für dieses ausgewählte Portfolio 47/100 (B). [S4]

5. Österreichs Meldepflichten haben unterschiedliche Geltungsbereiche und Fristen. Das NISG 2026 trat am 1. Oktober vollständig in Kraft. DORA gilt seit dem 17. Januar 2025. Die Meldung personenbezogener Datenverletzungen bleibt eine eigene Feststellung, und NISG § 44(7) schließt eine NISG-Geldstrafe für Verhalten aus, das die Datenschutzbehörde bereits nach der DSGVO geahndet hat. [S30][S36][S38][S40]

Vier Nachbarvolkswirtschaften liefern regionalen Vergleichskontext: Deutschland, die Schweiz, Tschechien und Ungarn. Sie teilen deutschsprachige, industrielle, finanzwirtschaftliche und grenzüberschreitende EU-Dienstleisterbeziehungen mit Österreich. Passive Sicherheitskontrollbeobachtungen umfassen alle 250 ausgewählten Domains (Momentaufnahme vom 23.–27. November). Insgesamt veröffentlichen 149 Domains (59,6%) durchgesetzte DMARC-Richtlinien, 239 (95,6%) SPF und 240 (96,0%) zeigten gültiges TLS. [S3]

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

Vier Entscheidungen für Führungskräfte

1. **Übernehmen Sie Verantwortung für die Identitätsuntersuchung.** Geben Sie einem benannten Team Befugnis zur Prüfung von Kontobelegen, administrativen Änderungen und zum Widerruf relevanter Sitzungen. Schließen Sie jede Warnung mit Belegen und einem Geschäftsverantwortlichen ab.
2. **Verlangen Sie unabhängige Zahlungsbestätigung.** Finanzen sollten geänderte Anweisungen über einen bereits bekannten Kanal prüfen. Testen Sie den Prozess auch mit einem echten Geschäftskontakt als Absender.
3. **Üben Sie einen Dienstleistervorfall.** Beteiligen Sie Dienstverantwortung, Datenschutzleitung und Kundenbetreuung. Verlangen Sie einen nutzbaren Ersatzablauf und kundenspezifischen Umfang. Eine Wiederherstellungsmitteilung des Anbieters ist kein automatischer Abschluss.
4. **Bereiten Sie getrennte Meldeentscheidungen vor.** Recht, Datenschutz und Finanz-Compliance sollten einen Ereignisakt teilen, aber Geltungsbereichsprüfung, Auslöser, Frist und Übermittlungsbeleg jeweils getrennt dokumentieren.

Das Jahr in Zahlen

Die folgenden Zahlen behalten ihre ursprünglichen Populationen und Zeiträume.

34.261

Beobachtete Beiträge mit Österreichbezug im angefragten Zeitraum (gleiche Summe in Monats- und Plattformansicht)

WAS SIE NICHT MISST

Nationale Vorfall- oder eindeutige Opferzahl

61

Österreichische Ransomware-Einträge über 56 eindeutige Einrichtungsnamen im angefragten Zeitraum

WAS SIE NICHT MISST

Bestätigte Einbrüche, eindeutige Personen oder Zahlungen

250

Ausgewählte Domains im Portfolio dieses Berichts

WAS SIE NICHT MISST

Überprüfte Erhebung unabhängiger österreichischer Organisationen

249 von 250

Ausgewählte Domains mit vollständigen Expositionsbeobachtungen

WAS SIE NICHT MISST

Überprüfte Erhebung unabhängiger Organisationen

49 von 249

Beobachtete Domains mit aktuellem Zugangsdatenangebot (19,7%)

WAS SIE NICHT MISST

Gültige Zugangsdaten, abgeschlossene Verkäufe oder bestätigte Einbrüche

47 / 100 (B)

Nationaler Atlas-Gesamtwert des beobachteten ausgewählten Portfolios

WAS SIE NICHT MISST

Angriffswahrscheinlichkeit oder nationale Häufigkeit

149 von 250

Ausgewählte Domains mit beobachteter DMARC-Durchsetzung in Quarantäne oder Ablehnung (59,6%)

WAS SIE NICHT MISST

Durchsetzung auf Nachrichtenebene über jeden Versanddienst

23

Falldossiers: 6 Untergrund-Behauptungsfälle und 17 amtliche oder quellenbasiert berichtete Fälle

WAS SIE NICHT MISST

Deduplizierte nationale Vorfallzahl

21.988

Polizeilich erfasste Cybercrime-Fälle im engeren Sinn für 2025 (Anstieg von 20.246 im Jahr 2024)

WAS SIE NICHT MISST

Vorfälle im Berichtszeitraum 2026

31.001

Polizeilich erfasste Internetbetrugsfälle für 2025

WAS SIE NICHT MISST

Bestätigte Organisationseinbrüche

Ungefähr 5.000

Gemeldete Phishing-Fälle von Januar–September 2026 (ungefähr 7.000 im Gesamtjahr 2025)

WAS SIE NICHT MISST

Alle österreichischen Phishing-Versuche oder eindeutigen Opfer

Ungefähr EUR 19 Millionen

Schaden im Zusammenhang mit dieser polizeilichen Phishing-Darstellung Januar–September 2026 (ungefähr EUR 22 Millionen 2025)

WAS SIE NICHT MISST

Vom Bericht gemessener Cybercrime-Schaden

1.855

2025 bei der DSB eingegangene Meldungen von Sicherheitsverletzungen (Anstieg von 1.319 im Jahr 2024)

WAS SIE NICHT MISST

Bestätigte Einbrüche 2026 oder Ransomware-Summen

843

Für 2025 an die FMA gemeldete Betrugsfälle (EUR 19,6 Millionen zugehöriger Schaden)

WAS SIE NICHT MISST

Einbrüche im Finanzsektor 2026 oder polizeiliche Gesamtsumme

Quellen: eigene Beobachtungen [S1][S2][S3][S4][S6], Bundeskriminalamt [S15][S16], Datenschutzbehörde [S39] und FMA [S41]. Die Populationen überschneiden sich in unbekannter Weise. Weder Addition noch Verhältnisbildung sind gerechtfertigt.

Der Abschnitt zu aktuellen Aktivitäten in §5.7 trennt neu bekannt gegebenes Ereignis, Aktualisierung, Sicherheitshinweis und rückblickende Strafverfolgungsdarstellung. Kapitel 3–4 und 7 erhalten die Grenzen ihrer eigenen Datenpopulationen. Kapitel 12 übersetzt die Unterschiede in Arbeit mit überprüfbarem Abschluss.

KERNAUSSAGEN

01

Prüfen Sie Identitäten und Sitzungen vor der Auswahl von Eindämmungsmaßnahmen.

02

Machen Sie Zahlungsprüfung unabhängig von der Glaubwürdigkeit einer Nachricht.

03

Bereiten Sie Dienstleisterumfang, Ersatzbetrieb und Meldeverantwortung gemeinsam vor.

Berichtskarte

Zwölf Kapitel unterstützen fünf Lesewege. Folgen Sie Ihrer Entscheidungsverantwortung; die Beleggrenzen gelten bei jeder Wiederverwendung eines Ergebnisses.

Vorstand und Geschäftsleitung	Betriebsfähigkeit und verantwortete Reaktion ausstatten	01 05 11 12
CISO und Sicherheitsleitung	Gefährdung und Dienstleisterabhängigkeiten prüfen	03 04 05 07
SOC und Identitätsteams	Behauptungen, Zugriff und Dauerhaftigkeit unterscheiden	04 06 07 B
Betrugsabwehr und Kundenteams	Zahlungsumleitung und Folgeschäden unterbrechen	05 08 09
Recht und Kommunikation	Umfang, Fristen und belastbare Aussagen bestimmen	05 06 10 12

Belegkennzeichnung	Bedeutung	Nächste Prüfung des Lesers
Beobachtung	Ein gespeicherter Beitrag, Eintrag oder gemessenes Signal existiert	Einheit, Datum und Relevanz bestimmen
Behauptung	Eine Person oder kriminelle Bezeichnung behauptet ein Ereignis oder eine Fähigkeit	Berechtigte Belege für die zugrunde liegende Aussage suchen
Offizielle Bestätigung	Organisation oder Behörde bestätigt die genannten Fakten	Genauen Aussageumfang und verbleibende Unsicherheit erhalten
Analytische Schlussfolgerung	Aus benannten Belegen folgt eine Bewertung oder Planungsentscheidung	Alternative Erklärung und Änderungssignal prüfen

Auch ein bestätigter Vorfall kann Akteur, Datensatzzahl oder Zugangsweg ungeklärt lassen. Eine Quellenzuschreibung bleibt deren Bewertung. Der Bericht macht aus einer Akteursaussage keine amtliche Darstellung.

KAPITEL 02

Österreichs digitaler Kontext und Bedrohungsumfeld

02

DIESES KAPITEL BEANTWORTET

Welche Abhängigkeiten erschweren die Eindämmung eines Vorfalls in Österreich?

3

Abhängigkeiten verbinden die zitierten Fälle: Identitäten, Dienstleister und Zahlungen

2.1 Zuerst Einheit und Jahr klären 12

2.2 Gemeinsame Dienste schaffen mehrere Verantwortungsgrenzen 13

2.3 Vertraute deutsche Sprache begründet kein Vertrauen 13

2.4 Der aktualisierte nationale Rahmen verändert die Vorbereitung 14

2.5 Politischer und internationaler Kontext braucht klare Quellengrenzen 14

2.6 Betriebsfähigkeit umfasst auch nicht böswillig verursachte Ausfälle 15

KAPITEL 02

Österreichs digitaler Kontext und Bedrohungsumfeld

KURZFASSUNG

Die österreichischen Fälle überschreiten Organisationsgrenzen über Identitätsdienste, gehostete Infrastruktur und gewöhnliche Geschäftskorrespondenz. Auch die nationalen Behörden beschreiben unterschiedliche Gruppen und Jahre. Eine gemeinsame Bedrohungszahl würde die erforderlichen Reaktionen verschleiern. Ordnen Sie jedem kritischen Dienst seine Identitätsabhängigkeit, Dienstleister, Datenverantwortlichen und Ersatzabläufe zu. Klären Sie anschließend die zuständige Behörde und den Meldeweg.

2.1 Zuerst Einheit und Jahr klären

Die hohe digitale Vernetzung Österreichs prägt die Reichweite von Imitation und Betrug. Die Digital-2026-Basislinie von DataReportal (veröffentlicht im November 2025 auf Basis von Oktober-2025-Daten) nennt 9,11 Millionen Einwohner und 8,69 Millionen Internetnutzer (95,3% Verbreitung). Sie nennt zudem 13,5 Millionen Mobilfunkanschlüsse (148% der Bevölkerung) und 6,98 Millionen aktive Social-Media-Nutzeridentitäten (76,6%). Diese Nutzungszahlen von Ende 2025 liefern Reichweitenkontext, keine Vorfallzahlen für 2026. [S63]

Der im August 2026 veröffentlichte Bericht des Bundeskriminalamts beschreibt 2025. Die Zahl der Cybercrime-Fälle im engeren Sinn stieg von 20.246 im Jahr 2024 auf 21.988 im Jahr 2025. Dieser Rückblick liefert Kontext; er misst keine Aktivitäten bis November 2026. [S15]

Dieselbe Veröffentlichung nennt 31.001 Fälle von Internetbetrug für 2025. Die Kategorien umfassen auch Handlungen außerhalb von Angriffen auf Organisationssysteme. Ihre Entwicklung liefert keinen fehlenden Bezugswert für Ransomware-Einträge oder offengelegte Zugangsdaten. [S15]

Der Präventionshinweis zu Phishing vom Oktober nennt ungefähr 5.000 Phishing-Fälle und damit verbundene Schäden von EUR 19 Millionen für Januar–September 2026. Zum Vergleich über ein Gesamtjahr nennt dieselbe Mitteilung rund 7.000 Fälle und EUR 22 Millionen für 2025. Diese Zahlen umfassen ungleiche Zeiträume und zeigen polizeilich gemeldete Fälle, nicht alle versuchten Nachrichten oder ungemeldeten Schäden. [S16]

In derselben Oktobermitteilung hält die Oesterreichische Nationalbank (OeNB) fest, dass in Österreich ungefähr 1 von 16.000 Zahlungen von Betrug betroffen ist, bei rund EUR 115 Millionen Zahlungsbetrugsschäden im Vorjahr. Sie beobachtet, dass Täter zunehmend Menschen manipulieren statt technische Zahlungssysteme zu umgehen. Gesondert hebt die Telekommunikationsregulierungsbehörde RTR-GmbH die gezielte Regulierung alphanumerischer SMS-Absenderkennungen gegen Absenderfälschung hervor. [S16]

Österreichs Datenschutzbehörde (DSB) liefert eine gesonderte Basislinie für Datenschutzmeldungen. Ihr Tätigkeitsbericht 2025 (veröffentlicht im März 2026) weist 1.855 Meldungen von Sicherheitsverletzungen für 2025 aus, ein Plus von 40,6% gegenüber 1.319 im Jahr 2024. Die Gesamtzahl 2025 umfasst 1.704 nationale DSGVO-Meldungen, 48 grenzüberschreitende Meldungen, 20 über andere EU-Behörden übermittelte Meldungen und 83 Telekommunikationsmeldungen nach § 164 TKG 2021. Die DSB nennt Ransomware, Vorfälle in Buchungs- und Lohnverrech-

nungssoftware, fehlgeleitete Korrespondenz sowie technische oder organisatorische Fehler. Die öffentliche Bekanntmachungsseite der DSB (20. Juli–19. November 2026, geprüft am 27. November) enthält keine Zwischenstatistiken für 2026, sodass der Bericht 2025 die jüngste öffentliche Basislinie bleibt. [S39][S64]

Entscheidend ist, ob eine Zahl Prävention, Untersuchung oder Wiederherstellung verändern sollte. Betrugsanzeigen können die Vorbereitung des Kundenschutzes unterstützen. Eine konkrete Kontowarnung kann eine Überprüfung rechtfertigen. Ein öffentlicher Erpressungseintrag kann Vorsorge für Betriebsfähigkeit und Mitteilungen begründen, ohne seine Behauptung zu bestätigen.

Dieser Bericht verwendet keinen gemeinsamen nationalen Nenner für diese Beobachtungen. Im selben Zeitraum (1. Januar–22. November 2026) verzeichnete Österreich 34.261 Untergrundbeiträge mit Länderbezug, davon 293 in Foren. Die Nachbarsummen betragen für Deutschland 1.222.222 (2.554 Foren), für die Schweiz 60.135 (887), für Tschechien 53.067 (420) und für Ungarn 32.125 (1.885). Rohsummen spiegeln Sichtbarkeit und Massenwerbung wider, keine vergleichbaren Vorfallraten oder Rangfolgen. [S1]

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

2.2 Gemeinsame Dienste schaffen mehrere Verantwortungsgrenzen

Ein Fall aus dem Bildungsbereich von Anfang 2026 betrifft ein Verzeichnis mit administrativer Bedeutung. Die Dienstleisterfälle vom November betreffen gehostete Infrastruktur und Buchungssysteme im Beherbergungsbereich. Die Mitteilung aus dem öffentlichen Bereich betrifft eine extern betriebene Website. Diese Beziehungen unterscheiden sich, obwohl alle eine eingegrenzte Prüfung der Zugriffe erfordern. [S25][S28][S29][S56][S57]

Ein hilfreiches Dienstverzeichnis nennt daher mehr als die zuständige Beschaffungsstelle. Es sollte Kontoverantwortung, Systemadministration, datenschutzrechtlich Verantwortliche und die fortzuführende Geschäftsfunktion festhalten. Diese Rollen können bei unterschiedlichen Organisationen liegen.

Ein Dienstleister kann beispielsweise die Infrastruktur wiederherstellen, während ein Kunde noch die dort zugänglichen Informationen prüfen muss. Ein zentraler Identitätsdienst kann wieder laufen, während alte Sitzungen eine eigene Prüfung erfordern. Eine funktionierende Startseite belegt keinen vollständig funktionierenden Geschäftsprozess des Kunden.

Das sind Folgerungen für die Planung, keine Feststellungen über eine einheitliche Architektur aller österreichischen Organisationen. Der Dienstverantwortliche sollte die tatsächliche Abhängigkeit überprüfen, bevor er eine Kontrolle anwendet oder eine Zusicherung des Dienstleisters akzeptiert.

2.3 Vertraute deutsche Sprache begründet kein Vertrauen

Der CERT.at-Hinweis zur Bewerbungskampagne beschreibt auf deutschsprachige Geschäftsumfelder zugeschnittene Korrespondenz. Die Mailbox-Kampagne vom Juli nutzt vertraute Absender. Die BEC-Warnung vom August beschreibt Anfragen innerhalb gewöhnlicher Geschäftsbeziehungen. Glaubwürdigkeit entsteht durch den Kontext ebenso wie durch die Formulierung. [S9][S10][S12]

Für die Abwehr folgt daraus: Prüfen Sie die verlangte Handlung. Eine sprachlich korrekte Nachricht kann eine unbefugte Zahlung verlangen. Ein echtes Postfach kann einen betrügerischen Link verbreiten. In einem langjährigen Austausch können plötzlich ein unerwarteter Anhang oder eine ungewöhnliche Anweisung auftauchen.

Schulen Sie Beschäftigte darauf, bei Änderungen innezuhalten: bei einem anderen Zahlungskonto, einer umgangenen Freigabe, einem Dokument mit neuer Anmeldeaufforderung oder einer ungewöhnlichen Softwareinstallation. Maßstab sollte die Berechtigung der Handlung sein, nicht die sprachliche Qualität.

Der Akzent eines Anrufers, die Sprache eines Beitrags oder das Pseudonym eines Verkäufers belegen keine Nationalität. Der Bericht leitet daraus weder einen Standort noch staatliche Unterstützung ab.

2.4 Der aktualisierte nationale Rahmen verändert die Vorbereitung

Österreichs neue Cybersicherheitsbehörde nahm ihre Arbeit unter dem vom BMI in den September- und Oktoberhinweisen beschriebenen Rahmen auf. Laut amtlichen Rechts-FAQ trat das NISG 2026 am 1. Oktober 2026 vollständig in Kraft. [S30][S49]

Die wichtige Entscheidung für Leser betrifft den Geltungsbereich. Ein großes Portfolio, eine öffentliche Aufgabe oder ein vertrauter Branchenname klären den gesetzlichen Status nicht automatisch. Wesentliche und wichtige Einrichtungen, Ausnahmen und Branchenregeln erfordern eine Prüfung des jeweiligen Rechtsträgers. [S31]

Der Bericht bewertet weder die institutionelle Änderung noch die Regierungspolitik. Er nutzt den veröffentlichten Rahmen, um aktuelle Zuständigkeiten und Meldewege zu bestimmen. Kapitel 10 trennt Rechtsfakten von der hier empfohlenen betrieblichen Vorbereitung.

2.5 Politischer und internationaler Kontext braucht klare Quellengrenzen

Die im Mai veröffentlichte DSN-Mitteilung zum Bericht betrifft das Sicherheitsbild für 2025. Die Aussagen zur Spionage liefern behördlichen Kontext. Sie sind keine Zuschreibung für jeden später in Österreich bekannt gewordenen Vorfall. Veröffentlichungs- und Beobachtungsjahr müssen sichtbar bleiben. [S43]

Die Beteiligung einer öffentlichen Stelle belegt kein politisches Motiv. Eine Dienstleisterbeziehung belegt keine Angriffstechnik über die Lieferkette. Eine von der Presse wiedergegebene Mitteilung aus dem öffentlichen Bereich nennt weder einen Betreiber noch einen staatlichen Unterstützer. [S29]

Dieser Bericht bezieht keine Position zu Wahlen, politischen Parteien, Koalitionspolitik, Neutralitätspolitik, internationalen Konflikten oder Regierungsentscheidungen. Beleidigungen und politische Parolen von Akteuren werden ausgelassen. Soweit eine staatliche Zuschreibung relevant ist, wird sie als Bewertung der jeweiligen Quelle gekennzeichnet.

Sicherheitsteams sollten unabhängig von politischen Zugehörigkeiten dieselben Maßstäbe für Überprüfung, Datenschutz und Betriebsfähigkeit anwenden. Der Schutz eines Kontos oder die Wiederherstellung eines öffentlichen Dienstes erfordert keine Bewertung der politischen Position der Einrichtung.

2.6 Betriebsfähigkeit umfasst auch nicht böswillig verursachte Ausfälle

Der CERT.at-Bericht vom Juni beschreibt unterbrochene Glasfaserverbindungen durch einen Brückenbrand und hält eine formelle NIS-Meldung fest. Das belegt eine Beeinträchtigung der Betriebsfähigkeit, keinen Cyberangriff. Physische Ursachen werden nicht böswillig, weil der betroffene Dienst digital ist. [S13]

Die weitergehende Planungsfrage lautet, ob scheinbare Vielfalt eine gemeinsame Abhängigkeit verbirgt. Getrennte Verträge belegen keine getrennten physischen Leitungen, Identitäten oder Verwaltungsebenen. In einer Notfallübung sollten Anbieter und Dienstverantwortliche die jeweils entscheidende Trennung nachweisen.

Das Übungsergebnis sollte auf Ebene des Geschäftsprozesses dokumentiert werden. Können Beschäftigte über den Ersatzablauf kommunizieren, eine Leistung erbringen, eine Zahlung freigeben oder einen Kunden unterstützen? Ein Diagramm hilft erst, wenn die angenommene Trennung geprüft wurde.

KERNAUSSAGEN

01

Halten Sie Veröffentlichungsjahr, Beobachtungsjahr und Belegeinheit sichtbar.

02

Ordnen Sie gemeinsame Identitäten und Dienstleister den unterstützten Geschäftsfunktionen zu.

03

Kennzeichnen Sie politische Bewertungen als Aussagen der Quellen und testen Sie Betriebsfähigkeit ohne erfundene feindliche Ursachen.

KAPITEL 03

Nationale Exposition: das ausgewählte Domainportfolio

03

DIESES KAPITEL BEANTWORTET

Welche organisationsbezogenen Signale rechtfertigen eine genauere Untersuchung?

250

ausgewählte Domains im beschreibenden Portfolio

3.1 Datengrundlage auf einen Blick 17

3.2 Branchenabdeckung 17

3.3 Gemessene Expositionssignale und nationaler Gesamtwert 18

3.4 Passive E-Mail- und Webbeobachtungen 23

3.5 Ein externes Signal in eine Entscheidung überführen 27

3.6 Abschluss statt Warnungsmenge messen 28

KAPITEL 03

Nationale Exposition: das ausgewählte Domainportfolio

KURZFASSUNG

49 von 249 beobachteten Domains hatten bei der Prüfung am 23. November Zugangsdaten im Angebot. Das Portfolio erfasst mindestens 124.110 Gerätezuordnungen und 3.900.001 Zugangsdatenzuordnungen. Sein nationaler Atlas-Gesamtwert beträgt 47/100 (B), keine Angriffswahrscheinlichkeit. Über alle 250 ausgewählten Domains zeigen 149 (59,6%) durchgesetzte DMARC-Richtlinien und 240 (96,0%) gültiges TLS. Verbundene Dienste und Datensätze können sich überschneiden. Prüfen Sie eigene Konten, Datenalter und zugehörige Dienste vor eingreifender Eindämmung.

3.1 Datengrundlage auf einen Blick

Die Portfoliodefinition bestimmt, welche Aussagen seine Beobachtungen tragen.

Punkt	Definition
Ausgewählte Population	250 gezielt ausgewählte Domains aus zehn Branchengruppen
Einheit	Ausgewählte Domain und zugehöriger Dienst; nicht zwingend ein unabhängiger Rechtsträger
Auswahlzweck	Beschreibende Abdeckung bedeutender öffentlicher Aufgaben und kommerzieller Dienste
Unabhängigkeit	Verbundene Unternehmen, gemeinsame Betreiber und institutionelle Dienste können sich überschneiden
Zeit	Datierte Beobachtungen kennzeichnen die gemessene Momentaufnahme; sie zählen nicht automatisch Vorfälle von 2026
Nationaler Umfang	Keine Schätzung österreichischer Organisationshäufigkeiten oder nationaler Schäden

Der Begriff Organisation dient der Lesbarkeit, wenn ein ausgewählter Dienst eine Einrichtung vertritt. Zahlen bleiben an Domains gebunden. Mutter- und Tochterunternehmen können getrennte Domains haben und trotzdem Konten, Dienstleister oder Datensätze teilen. [S6]

3.2 Branchenabdeckung

Die Branchentabelle beschreibt das ausgewählte Portfolio. Sie ist keine Branchenrisikotabelle.

Branchengruppe	Ausgewählte Domains	Prüffrage für Leser
Öffentliche Verwaltung	25	Welcher Bürger- oder Verwaltungsdienst hängt von der ausgewählten Identität ab?
Regionale und lokale Verwaltung	25	Welcher gemeinsame Anbieter oder zentrale Dienst unterstützt die lokale Leistung?
Banken und Finanzen	25	Welche Datensätze beschreiben Beschäftigte, Kunden oder einen Finanzdienstleister?
Hochschulen und Forschung	25	Welche zentralen Konten erreichen auch Forschung, Lehre oder Verwaltung?
Industrielle Fertigung und Bau	25	Welcher Dienstleister- oder Bewerbungsweg erreicht einen sensiblen Arbeitsplatz?
Konsumgüterfertigung und Technologie	25	Welcher Kunden- oder technische Dienst braucht eine getrennte Umfangsprüfung?
Energie und Versorgung	25	Welche geschäftlichen und betrieblichen Funktionen brauchen getrennte Eindämmung?
Verkehr und Logistik	25	Welches Postfach, Buchungs- oder Betriebssystem ist tatsächlich betroffen?
Handel, Kommunikation und Unternehmensdienste	25	Welcher Kundenkontakt kann nach Wiederherstellung als Betrug fortwirken?
Gesundheits-, Versicherungs- und Sozialdienste	25	Welcher Ersatzablauf erhält Versorgung, Labor- oder Verwaltungsdienst?
Gesamt	250	Domaineinheit und Grenze überlappender Rechtsträger erhalten

Die Branchentabelle beschreibt das ausgewählte Portfolio. Ihre Zahlen belegen weder nationale Branchengröße, Expositionshäufigkeit noch einen Branchenrisikowert. [S6]

3.3 Gemessene Expositionssignale und nationaler Gesamtwert

49 von 249 beobachteten Domains (19,7%) hatten bei der Prüfung Zugangsdaten im Angebot. Vollständige Expositionsbeobachtungen umfassen am 23. November 249 der 250 ausgewählten Domains. Für eine Domain fehlt ein vollständiger Datensatz. Sie bleibt außerhalb der gemessenen Summen und wird nicht als null behandelt. [S4]

Der nationale Atlas-Gesamtwert beträgt 47/100 (B) für das beobachtete Portfolio. Höhere Werte zeigen darin mehr beobachtete Exposition. Es wird nur dieser eine nationale Gesamtwert veröffentlicht. Per-Sektor-Werte, Gruppenwerte oder Einzeldomain-Werte erscheinen nirgendwo in diesem Bericht. Das Ergebnis ist ein beschreibendes Modellergebnis, keine Angriffswahrscheinlichkeit, nationale Häufigkeitsschätzung oder Einbruchsbestätigung. [S4]

Die folgende Tabelle zählt beobachtete Domains mit dem jeweiligen Expositionssignal. Historie zählt Domains mit früheren Markteintragsdaten (899 historische Einträge über 48 Domains). Bei Banken und Finanzen haben 4 Domains ein aktuelles Angebot und 3 frühere Historieneinträge, weil eine Domain ein aktuelles Angebot mit null früheren Einträgen aufweist. Die Spalten überschneiden sich und sollten nicht addiert werden. [S4]

Branchengruppe	Beobachtet	Aktuelle Angebote	Historie	Mit Geräten	Mit Mitarbeitergeräten	Mit Zugangsdaten	Mit Dokumenten
Öffentliche Verwaltung	25	2	2	14	10	19	16
Regionale und lokale Verwaltung	25	3	3	20	10	23	16
Banken und Finanzen	25	4	3	21	11	25	12
Hochschulen und Forschung	25	5	5	24	21	25	22
Industrielle Fertigung und Bau	25	2	2	21	20	24	18
Konsumgüterfertigung und Technologie	24	5	5	22	17	24	14
Energie und Versorgung	25	3	3	24	15	25	13
Verkehr und Logistik	25	6	6	23	16	25	13
Handel, Kommunikation und Unternehmensdienste	25	17	17	23	17	25	12

Branchen-gruppe	Beobachtet	Aktuelle An-gebote	Historie	Mit Geräten	Mit Mitarbei-tergeräten	Mit Zugangs-daten	Mit Dokumen-ten
Gesund-heits-, Versi-cherungs- und Sozial-dienste	25	2	2	22	14	22	11
Gesamt (249 von 250)	249	49	48	214	151	237	147

In `c03_exposure_signals.csv` und `c04_sector_exposure.csv` zählen Spaltenköpfe wie `orgs`, `orgs_listed_for_sale_now`, `orgs_with_sale_history`, `orgs_with_employee_devices`, `orgs_with_exposed_docs` und `non_employee_devices` beobachtete Domains und Gerätezuordnungen, nicht überprüfte unabhängige Rechtsträger oder bestätigte Nicht-Beschäftigte. Beide Dateien halten die Domaineinheit ausdrücklich in den Metadaten von `c03` fest. [S4]

Aktuelle Angebote und weitere Expositionssignale treten über das beobachtete Domainportfolio verteilt auf

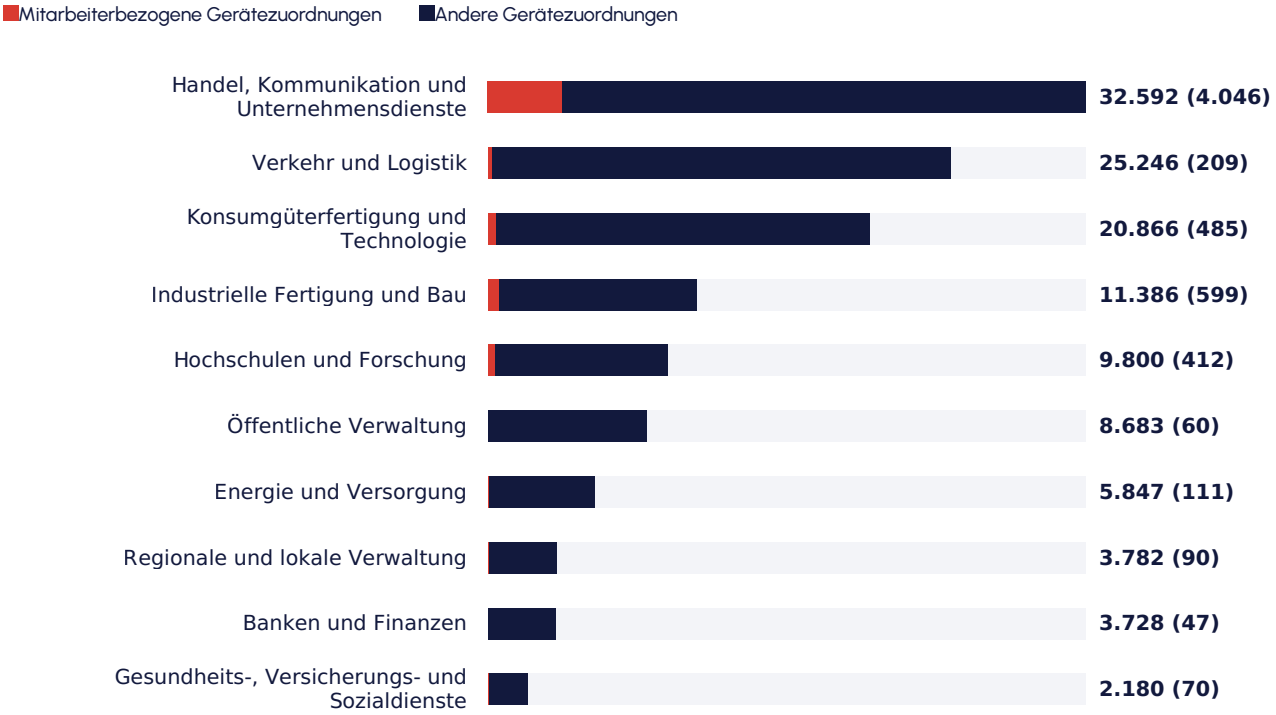
	Aktuelle Angebote	Historie	Mit Geräten	Mitarbeiter-geräte	Mit Zugangsdaten	Mit Dokumenten
Öffentliche Verwaltung	2/25	2/25	14/25	10/25	19/25	16/25
Regionale und lokale Verwaltung	3/25	3/25	20/25	10/25	23/25	16/25
Banken und Finanzen	4/25	3/25	21/25	11/25	25/25	12/25
Hochschulen und Forschung	5/25	5/25	24/25	21/25	25/25	22/25
Industrielle Fertigung und Bau	2/25	2/25	21/25	20/25	24/25	18/25
Konsumgüterfertigung und Technologie	5/24	5/24	22/24	17/24	24/24	14/24
Energie und Versorgung	3/25	3/25	24/25	15/25	25/25	13/25
Verkehr und Logistik	6/25	6/25	23/25	16/25	25/25	13/25
Handel, Kommunikation und Unternehmensdienste	17/25	17/25	23/25	17/25	25/25	12/25
Gesundheits-, Versicherungs- und Sozialdienste	2/25	2/25	22/25	14/25	22/25	11/25

Aktuelle Zugangsdatenangebote nach Branchengruppe (korallenrot). Jede Zelle zeigt beobachtete Domains / geprüfte Domains (24 oder 25); Signale überschneiden sich. Quelle: Brandefense-Expositionsbeobachtungen für 249 von 250 ausgewählten österreichischen Domains, Momentaufnahme vom 23. November 2026 (eine Domain bleibt unbekannt) [S4]. Kumulative Zuordnungen können sich überschneiden; sie sind keine eindeutigen Personen oder bestätigten Einbrüche.

Die folgenden Zuordnungssummen beantworten eine andere Frage als Domainzahlen. Sie sind kumulative Datensätze, die sich über Domains, Quellen und Personen hinweg überschneiden können. Gerätekennzeichnungen belegen weder überprüfte Beschäftigungsverhältnisse noch eine Zahl eindeutiger Unternehmensarbeitsplätze. [S4]

Branchengruppe	Beobachtet	Geräte, mindestens	Mitarbeitergeräte	Zugangsdatensätze	Dokumente	Ähnliche Namen (30T)
Öffentliche Verwaltung	25	8.683	60	40.818	223	12.263
Regionale und lokale Verwaltung	25	3.782	90	47.783	97	5.722
Banken und Finanzen	25	3.728	47	53.514	53	202
Hochschulen und Forschung	25	9.800	412	343.614	185	14.167
Industrielle Fertigung und Bau	25	11.386	599	214.905	174	11.402
Konsumgüterfertigung und Technologie	24	20.866	485	222.786	120	780
Energie und Versorgung	25	5.847	111	69.376	64	20.307
Verkehr und Logistik	25	25.246	209	90.420	66	21.599
Handel, Kommunikation und Unternehmensdienste	25	32.592	4.046	2.755.179	429	11.701
Gesundheits-, Versicherungs- und Sozialdienste	25	2.180	70	61.606	67	1.163
Gesamt (249 von 250)	249	124.110	6.129	3.900.001	1.478	99.306

Gerätezuordnungen reichen in jedem Sektor über die mitarbeiterbezogene Population hinaus



Werte zeigen gesamte Gerätezuordnungen, mindestens (mitarbeiterbezogene Teilmenge in Klammern). Quelle: Brandefense-Expositionsbeobachtungen für 249 von 250 ausgewählten österreichischen Domains, Momentaufnahme vom 23. November 2026 (eine Domain bleibt unbekannt) [S4]. Kumulative Zuordnungen können sich überschneiden; sie sind keine eindeutigen Personen oder bestätigten Einbrüche.

Fünf Portfoliomuster leiten die Priorisierung über die 249 beobachteten Domains [S4]:

- **Mitarbeiterbezogene Geräte sind eine kleine Teilmenge der gesamten Gerätezuordnungen.** Das Portfolio enthält mindestens 124.110 Gerätezuordnungen über 214 Domains: 6.129 mitarbeiterbezogene (4,9% über 151 Domains) und 117.981 andere Zuordnungen (95,1%). Mitarbeiterbezogene Geräte sind in der Gesamtzahl enthalten und dürfen nicht hinzugerechnet werden. Gesondert enthalten zugeordnete Geräte mindestens 2.676.495 erfasste Zugangsdatenzeilen über alle Dienste hinweg, nicht nur die geprüfte Domain. [S4]
- **Combolists und Datenleck-Sammlungen prägen historische Zugangsdatensätze.** Über 237 Domains umfassen die 3.900.001 Zugangsdatensätze 2.259.831 Combolist-Einträge (57,9%), 1.439.520 Datenleck-Datensätze (36,9%) und 200.650 Stealer-Log-Zeilen (5,1%; gerundete Anteile ergeben 99,9%). Historisches Vorkommen belegt weder aktuelle Passwortgültigkeit noch einen jüngsten Einbruch. [S4]
- **Wenige stark vertretene Domains verzerren Branchensummen.** Handel, Kommunikation und Unternehmensdienste vereinigen 2.755.179 Zugangsdatensätze (70,6%) und 4.046 mitarbeiterbezogene Geräte (66,0%). Über das Portfolio entfallen auf zwei Domains 60,4% der Zugangsdatensätze (Top fünf: 72,1%) und auf zwei Domains 19,1% der Gerätezuordnungen. Der Median liegt bei 46 Gerätezuordnungen und 1.136 Zugangsdatensätzen je beobachteter Domain und zeigt, warum jede Organisation eine eigene Prüfung braucht. [S4]
- **Dokumente und ähnliche Domainnamen liefern Prüfkontext.** Von 249 beobachteten Domains weisen 147 insgesamt 1.478 Dokumentenzuordnungen und 206 insgesamt 99.306 Beobachtungen ähnlicher Namen (19. Oktober–18. November) auf. Dokumententreffer können öffentliche Broschüren enthalten, und kurze Markenzeichenfolgen treffen unverbundene globale Domains. [S4]

- **Rollierende 365-Tage-Domainnennungen umfassen Dark-Chat- und Tor-Quellen.** Über alle 250 ausgewählten Domains in den 365 Tagen bis 22. November verzeichneten 44 Domains (17,6%) insgesamt 456 Dark-Chat-Nennungen und 38 Domains (15,2%) insgesamt 241 Dark-Web-Nennungen (Tor). Dark-Chat-Nennungen führten bei Handel, Kommunikation und Unternehmensdiensten (8 Domains; 215), Banken und Finanzen (3; 119) sowie Verkehr und Logistik (3; 30). Dark-Web-Nennungen führten bei Hochschulen und Forschung (10 Domains; 116) sowie regionaler Verwaltung (10; 42). Im Zeitraum 1. Januar–22. November 2026 verzeichneten 23 von 250 Domains (9,2%) 221 Beiträge. [S4]

Geräte-, Zugangsdaten-, Dokumenten- und aktuelle Angebotsbeobachtungen bilden eine Momentaufnahme vom 23. November. Beobachtungen ähnlicher Namen umfassen den 19. Oktober–18. November. Rollierende Nachrichtenzuordnungen umfassen 365 Tage bis 22. November; die Teilmenge für 2026 wird gesondert genannt. Keine dieser Ansichten zählt Einbrüche von 2026. [S4]

Ein aktuelles Angebot rechtfertigt eine Kontoprüfung, keine Annahme fortbestehenden nutzbaren Zugangs. Klären Sie Zugehörigkeit, Datenalter, Gültigkeit, Berechtigungen und relevante Sitzungen. Historische Zugangsdaten eines abgelaufenen Kontos brauchen eine andere Reaktion als ein aktuelles privilegiertes Konto mit verdächtiger Aktivität.

Dokumente können öffentlich, historisch oder doppelt vorhanden sein. Ähnliche Namen oder eine Domainnennung allein belegen weder Missbrauch noch Einbruch oder gemeinsame Kontrolle. Lassen Sie den zuständigen Verantwortlichen Dienst oder Datensatz prüfen, bevor Sie Datenverletzung, Kundenauswirkung oder böswillige Domainnutzung feststellen.

3.4 Passive E-Mail- und Webbeobachtungen

Passive Prüfungen liefern eine datierte Ansicht extern sichtbarer E-Mail- und Webkontrollen. Sie testen nicht jeden Versanddienst, Nutzerablauf oder jede Anwendung. Der Nenner jeder Beobachtung muss getrennt erhalten bleiben. [S3]

DMARC, SPF und DKIM unterstützen unterschiedliche Teile der E-Mail-Authentifizierung. Eine Beobachtungsrichtlinie ist keine Durchsetzungsrichtlinie. Ein vorhandener Eintrag belegt weder die korrekte Konfiguration aller berechtigten Absender noch die Ablehnung gefälschter Nachrichten durch alle Empfänger.

Die Kampagne über vertraute Postfächer vom Juli zeigt eine weitere Grenze. Domain-Authentifizierung kann mit täuschenden Inhalten aus einem bereits bekannten Konto zusammenfallen. Authentifizierungskontrollen und Kontoreaktionsverfahren adressieren daher unterschiedliche Teile des Problems. [S10]

Ein gültiges TLS-Zertifikat zeigt eine bestimmte Beobachtung sicherer Übertragung. Es belegt weder Anwendungsberechtigung, sichere Kundenzahlungsanweisungen noch die Abwesenheit unbefugten Zugriffs. Eine fehlende Beobachtung sollte bis zur Prüfung durch den zuständigen Verantwortlichen unbekannt bleiben.

Die öffentliche Kontrolltabelle ist als Arbeitsliste mit gemessenen Nennern zu lesen. Ein Serviceteam sollte unerwartete Ergebnisse erklären, den betroffenen Versand- oder Webdienst bestimmen und die Korrektur vor Abschluss nachweisen.

Die passive Momentaufnahme (abgeschlossen am 23.–27. November 2026) umfasst alle 250 ausgewählten Domains, mit 25 Domains in jeder der zehn Branchengruppen. Positive Beobachtungen stehen neben ihren gemesse-
nen Nennern, ohne ein unbeobachtetes oder nicht verfügbares Ergebnis als fehlende Kontrolle zu werten. [S3]

149 von 250

ausgewählte Domains mit beobachteter DMARC-Durchsetzung in Quarantäne oder Ablehnung (59,6%)

239 von 250

ausgewählte Domains mit beobachtetem SPF-Eintrag (95,6%)

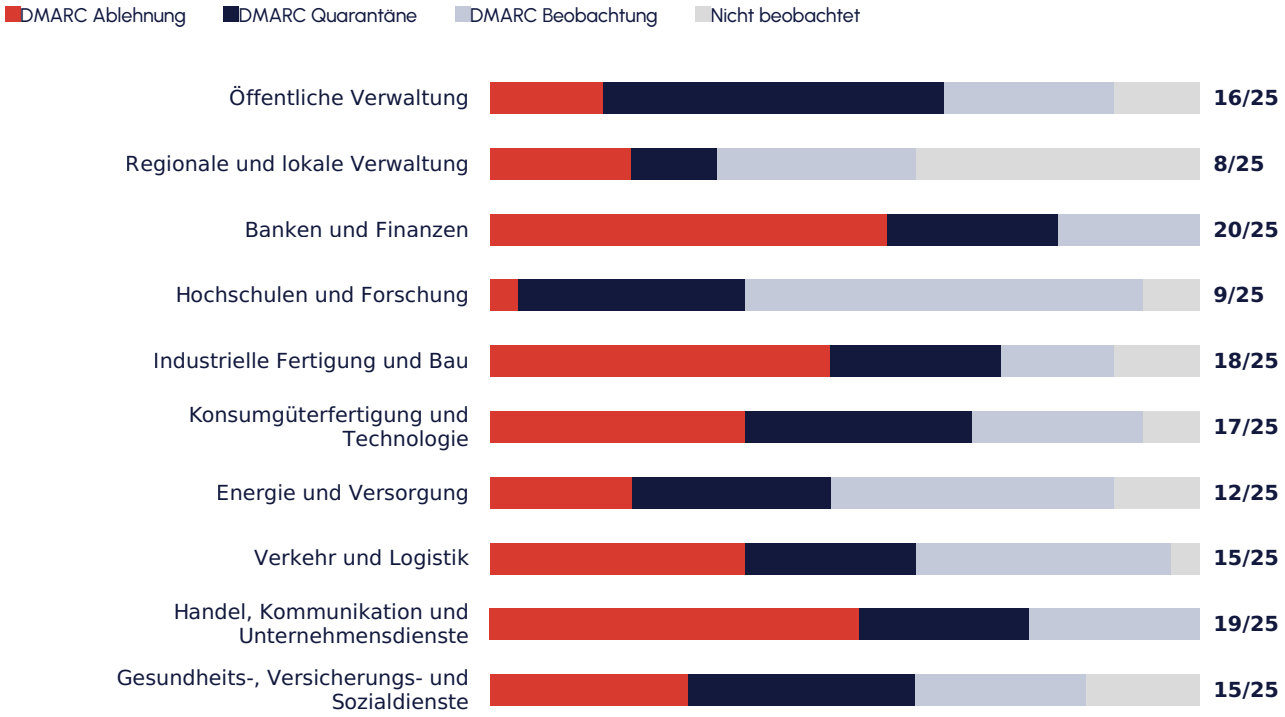
240 von 250

ausgewählte Domains mit gültiger TLS-Beobachtung (6 erfolglos; 4 nicht verfügbar)

184 von 247

Domains mit erfasster HTTP-Antwort und HSTS-Kopfzeile (3 nicht verfügbar)

Banken, Handel und Industrie führen bei beobachteter DMARC-Durchsetzung, während Regionalverwaltung und Hochschulen zurückliegen



Rechte Werte zeigen durchgesetzte Richtlinien (Ablehnung oder Quarantäne) / 25 ausgewählte Domains je Branchengruppe. Quelle: passive DNS- und E-Mail-Richtlinienbeobachtungen für 250 ausgewählte österreichische Domains, Momentaufnahme vom 23.-27. November 2026 [S3]. Veröffentlichte Richtlinien belegen keine Durchsetzung auf Nachrichtenebene für jeden Versanddienst.

Kontrollbeobachtung	Domains	Geprüfte Population
DMARC-Durchsetzung beobachtet (79 Ablehnung; 70 Quarantäne)	149	250 Domains

Kontrollbeobachtung	Domains	Geprüfte Population
DMARC-Beobachtungsrichtlinie beobachtet (`none`)	73	250 Domains
DMARC-Eintrag nicht beobachtet	28	250 Domains
SPF-Eintrag beobachtet	239	250 Domains
DKIM-Schlüssel beobachtet	150	250 Domains
DNSSEC-Delegationseintrag beobachtet	30	250 Domains
CAA-Eintrag beobachtet	48	250 Domains
Gültige TLS-Beobachtung	240	250 Domains
TLS-Prüfung nicht erfolgreich	6	250 Domains
TLS-Beobachtung nicht verfügbar	4	250 Domains
HSTS beobachtet	184	247 Domains mit erfasster HTTP-Antwort (3 nicht verfügbar)

Die folgende Tabelle zeigt die passiven Kontrollzahlen je Branche über alle 250 ausgewählten Domains. Es werden weder Branchen-Hygienewerte noch Rangfolgen veröffentlicht. [S3]

Branchengruppe	Beobachtet	DMARC Ablehnung	DMARC Quarantäne	DMARC Beobachtung	DMARC nicht beobachtet	SPF	DKIM	DNSSEC DS	CAA	Gültiges TLS	HSTS (erfasste HTTP)
Öffentliche Verwaltung	25	4	12	6	3	25	5	5	11	25	18 von 25
Regionale und lokale Verwaltung	25	5	3	7	10	23	10	4	5	25	17 von 25
Banken und Finanzen	25	14	6	5	0	24	17	5	4	25	23 von 25
Hochschulen und Forschung	25	1	8	14	2	22	14	2	7	23	12 von 24

Branchengruppe	Beobachtet	DMARC Ablehnung	DMARC Quarantäne	DMARC Beobachtung	DMARC nicht beobachtet	SPF	DKIM	DNSSEC DS	CAA	Gültiges TLS	HSTS (erfasste HTTP)
Industrielle Fertigung und Bau	25	12	6	4	3	24	20	1	3	23	22 von 25
Konsumgüterfertigung und Technologie	25	9	8	6	2	25	15	4	7	24	17 von 25
Energie und Versorgung	25	5	7	10	3	25	17	1	1	23	19 von 24
Verkehr und Logistik	25	9	6	9	1	24	19	1	1	24	19 von 25
Handel, Kommunikation und Unternehmensdienste	25	13	6	6	0	23	15	6	2	24	20 von 25
Gesundheits-, Versicherungs- und Sozialdienste	25	7	8	6	4	24	18	1	7	24	17 von 24
Gesamt (250 von 250)	250	79	70	73	28	239	150	30	48	240	184 von 247

Aus der vollständigen Momentaufnahme über 250 Domains treten 3 betriebliche Muster hervor [S3]:

- **Die DMARC-Durchsetzung erreicht 149 von 250 Domains (59,6%), während 101 Domains (40,4%) in Beobachtung bleiben oder keinen beobachteten Eintrag zeigen.** Die Durchsetzung umfasst 79 Ablehnungs- (31,6%) und 70 Quarantänerichtlinien (28,0%), neben 73 reinen Beobachtungs- (29,2%) und 28 unbeobachteten Domains (11,2%). Banken und Finanzen (20 von 25; 14 Ablehnung), Handel, Kommunikation und Unternehmensdienste (19; 13 Ablehnung) sowie industrielle Fertigung (18; 12 Ablehnung) zeigen die höchsten Durchsetzungszahlen. Regionale und lokale Verwaltung (8 von 25; 10 unbeobachtet und 7 in Beobachtung) sowie Hochschulen und Forschung (9 von 25; 14 in Beobachtung und 1 Ablehnung) zeigen die größten Lücken. [S3]
- **SPF ist weit verbreitet (239 von 250; 95,6%) und beobachtete DKIM-Schlüssel erscheinen bei 150 Domains (60,0%), auch dort, wo DMARC-Durchsetzung zurückliegt.** Regionale und lokale Verwaltung veröffentlicht SPF bei 23 von 25 Domains, während nur 8 DMARC-Durchsetzung zeigen. Hochschulen und Forschung veröffentlichen SPF bei 22 Domains und beobachtete DKIM-Schlüssel bei 14, doch 14 bleiben im DMARC-Beobachtungsmodus. Energie und Versorgung veröffentlicht SPF bei allen 25 Domains und beobachtete DKIM-Schlüssel bei 17, doch 10 bleiben in Beobachtung und 3 ohne beobachteten DMARC-Eintrag. [S3]
- **Gültiges TLS ist breit vorhanden (240 von 250; 96,0%) und HSTS erscheint bei 184 von 247 erfassten HTTP-Antworten (74,5%), während DNSSEC und CAA konzentriert bleiben.** Sechs Domains lieferten eine erfolglose TLS-Prüfung, und 4 lieferten keine TLS-Beobachtung. Bei 3 Domains blieb eine HTTP-Antwort aus (je 1 bei Hochschulen, Energie und Gesundheitsdiensten), sodass 247 erfasste HTTP-Antworten die Basis für HSTS bilden. DNSSEC-Delegationseinträge erscheinen bei 30 Domains (12,0%), angeführt von Handel (6), öffentlicher Verwaltung (5) und Banken (5). CAA-Einträge erscheinen bei 48 Domains (19,2%), angeführt von öffentlicher Verwaltung (11), Hochschulen (7), Konsumgütertechnologie (7) und Gesundheitsdiensten (7). [S3]

Ein DNSSEC-Delegationseintrag ist eine positive Eintragsbeobachtung, keine vollständige DNS-Vertrauenskettenprüfung. Ein DKIM-Schlüssel belegt nicht die korrekte Signierung jedes Versandablaufs, und ein unbeobachteter Schlüssel belegt nicht das Fehlen jeder Signierung. Nicht verfügbare TLS- oder HTTP-Ergebnisse bleiben unbekannt und gelten nicht als bestätigte Fehlkonfiguration. Die Organisation sollte den relevanten Dienst vor Auswahl einer Korrekturmaßnahme prüfen.

3.5 Ein externes Signal in eine Entscheidung überführen

Der folgende Ablauf ist ein empfohlenes Betriebsmodell. Er behauptet keinen Vorfall bei jeder Portfolioorganisation.

Stufe	Verantwortliche	Abschlussbelege
Relevanz feststellen	Ressourcen- oder Identitätsverantwortliche	Domain, Mandant und Konto gehören zur Organisation oder einem dokumentierten Dienstleister
Zeit feststellen	Vorfallreaktion	Beobachtungsdatum von behauptetem Ereignisdatum und Datenalter getrennt
Zugriff feststellen	Identitäts- und Anwendungsteams	Berechtigungen, Gültigkeit, Sitzungen und Dienstreichweite bewertet
Handlung auswählen	Vorfallleitung und Geschäftsverantwortliche	Eindämmungsentscheidung mit Dienstfolgen und Ersatzablauf
Personen bewerten	Datenschutz und Kundenteams	Datenkategorien, plausibler Schaden und Kommunikationsentscheidung dokumentiert
Abschließen und prüfen	Kontrollverantwortliche	Technische Korrektur überprüft und verbleibende Unsicherheit zugewiesen

Die erste Stufe verhindert unnötige Störung. Historische Zugangsdaten eines abgelaufenen Kontos sollten nicht dieselbe Reaktion erhalten wie ein gültiges privilegiertes Konto mit verdächtigem Zugriff. Beide verdienen ein dokumentiertes Ergebnis, ihre Eindämmungsentscheidungen unterscheiden sich aber.

Gehört das Konto einem Dienstleister, braucht der Kunde dennoch eine dienstspezifische Antwort. Fragen Sie nach erreichbarem Mandanten, Datenkategorien und Funktionen. Eine allgemeine Infrastruktur-Wiederherstellungsaussage beantwortet nicht, ob Kundeninformationen eingesehen wurden.

Halten Sie die Belegbehandlung innerhalb der berechtigten Untersuchung. Der Bericht empfiehlt weder Verkäuferkontakt oder Datensatzkauf noch Tests von Zugangsdaten an fremden Diensten. Die Prüfung sollte Unterlagen und Systeme nutzen, welche die Organisation untersuchen darf.

3.6 Abschluss statt Warnungsmenge messen

Eine hilfreiche betriebliche Kennzahl ist der Anteil relevanter Warnungen mit Verantwortlichem und beleggestütztem Ergebnis. Ihr Nenner sollte die eigene geprüfte Warnungspopulation der Organisation sein. Dieser Bericht nennt weder ein nationales Ziel noch gemessene Wirksamkeit.

Bei einem Kontoproblem kann der Abschluss Sitzungswiderruf, Entfernung einer unbefugten Regel und Prüfung privilegierter Änderungen umfassen. Bei einer E-Mail-Richtlinie kann er ein überprüftes Versanddienstverzeichnis und ein Authentifizierungsergebnis einer berechtigten Testnachricht umfassen.

Dokumentieren Sie Ausnahmen ausdrücklich. Manche berechtigten Abläufe brauchen eine zeitweilige Zulassung oder schrittweise Migration. Der Verantwortliche sollte Dienstfolge, Prüfdatum und ausgleichende Kontrolle nennen. Eine unerklärte Ausnahme lässt sich bei einem späteren Vorfall schwerer bewerten.

KERNAUSSAGEN

01

Lesen Sie das Portfolio als ausgewählte Domains mit möglichen Organisationsüberschneidungen.

02

Erhalten Sie für jede Messung Nenner und unbekannte Ergebnisse.

03

Schließen Sie relevante Signale über verantwortete Konto-, Dienst- und Datenprüfungen ab.

KAPITEL 04

Angebote im Dark Web und die Grenzen ihrer Belege

DIESES KAPITEL BEANTWORTET

Was belegt eine beobachtete Anzeige mit Österreichbezug tatsächlich?

5

Fragen, bevor aus einem Angebot eine Vorfallentscheidung wird

4.1 Datengrundlage auf einen Blick 31
4.2 Produkt und Behauptung trennen 33
4.3 Chronologie lesen, ohne ein Einbruchsdatum zu erfinden 33
4.4 Sechs Fälle von Behauptungen und Nachfrage 33
4.5 Auch die Beschaffung von Zugangsdaten ist eine Nachfragebeobachtung 41
4.6 Aktuelle Untergrundaktivitäten: 8.–22. November 42
4.7 Ein angemessener Prüfauftrag 43
4.8 Beobachtung und Kundenrisiko getrennt abschließen 44

KAPITEL 04

Angebote im Dark Web und die Grenzen ihrer Belege

KURZFASSUNG

Ein beobachteter Beitrag belegt seine Veröffentlichung. Aussagen über Zugänge, Datensätze und Preise müssen weiterhin überprüft werden. Wiederholte Werbung kann die Sichtbarkeit erhöhen, ohne einen neuen Vorfall zu begründen. Ein Länderbezug kann den Absatzmarkt des Verkäufers statt eines bestätigten Ziels beschreiben. Klären Sie Zugehörigkeit, Datenalter, Echtheit, Zugriff und betriebliche Auswirkungen, bevor Sie eine Reaktion auswählen.

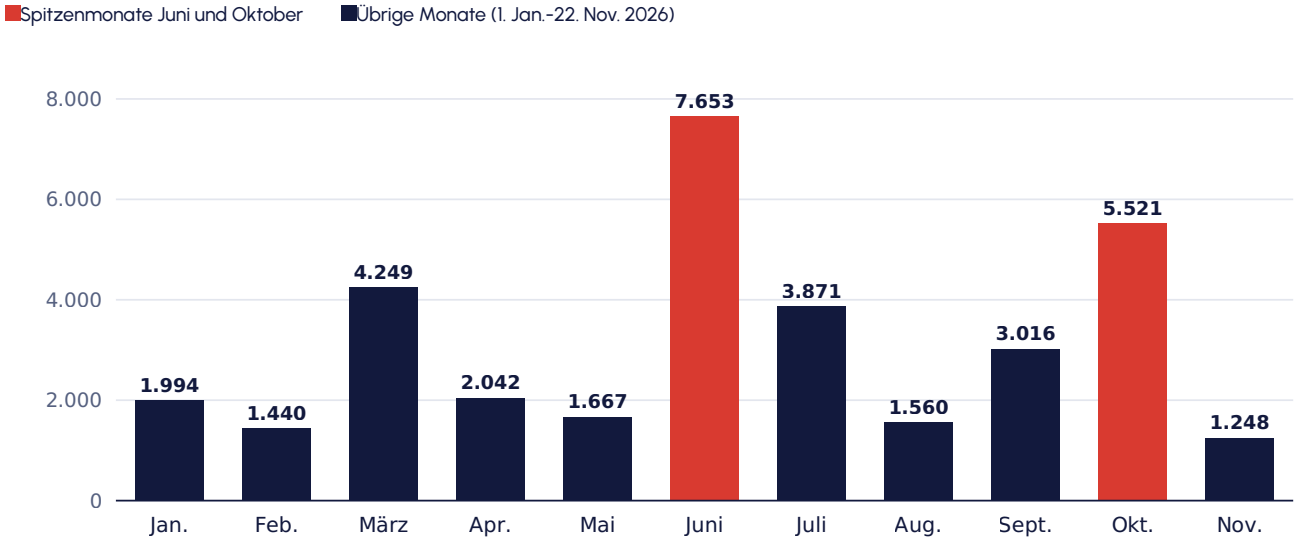
4.1 Datengrundlage auf einen Blick

Die Untergrundpopulation wird durch die gespeicherten Beobachtungen und deren Daten bestimmt. Sie unterscheidet sich von öffentlichen Mitteilungen und Ransompedia-Einträgen. [S1][S2]

Punkt	Bedeutung
Zeitraum	Beiträge vom 1. Januar–22. November 2026
Aktuelle Aktivitäten	Beiträge vom 8.–22. November 2026
Beobachtungseinheit	Veröffentlichter Beitrag; wiederholte Angebote sind nicht automatisch unabhängige Vorfälle
Länderbezug	Mit Österreich verbundene Inhalte; keine bestätigte Zielauswahl oder Nationalität
Marktaussage	Formulierung eines Verkäufers oder Suchenden; keine Bestätigung nutzbarer Zugänge, der Echtheit oder einer Transaktion
Sichtbarkeitsgrenze	Gespeicherte Beobachtungen erfassen nicht sämtliche privaten Austausche oder unveröffentlichten Vorfälle

Vom 1. Januar bis 22. November 2026 erfasste Odin by Brandefense 34.261 Untergrundbeiträge mit Österreichbezug in Monats- wie Plattformansichten. Die Monatsmenge erreichte Spitzen im Juni (7.653) und Oktober (5.521), während November nur den Teilzeitraum bis 22. November umfasst (1.248). Das sind Veröffentlichungszahlen von Nachrichten, keine Daten oder Zahlen von Einbrüchen. [S1]

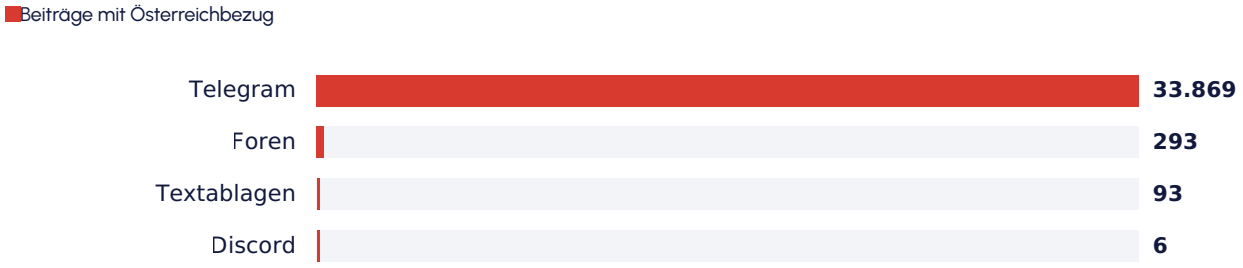
Monatliche Beiträge mit Österreichbezug ergeben 34.261, mit Spitzen im Juni und Oktober



Quelle: Odin by Brandefense, 34.261 Untergrundbeiträge mit Österreichbezug, 1. Januar-22. November 2026; November unvollständig [S1]. Veröffentlichungszahlen sind keine bestätigten Vorfälle.

Von diesen 34.261 Beiträgen entfallen 33.869 auf Telegram (98,9%), 293 auf Foren (0,9%), 93 auf Textablagen (0,3%), 6 auf Discord (unter 0,1%) und 0 auf versteckte Tor-Dienste. Volumenstarke OTC-Handels- und Mehrländer-Werbechats prägen das rohe Telegram-Aufkommen, während sich gezielte Zugangsangebote und Datengesuche auf Foren konzentrieren. Keine Summe zählt unabhängige Vorfälle. [S1]

Auf Telegram entfallen 33.869 von 34.261 Beiträgen mit Österreichbezug, während sich gezielte Angebote auf Foren konzentrieren



Versteckte Tor-Dienste verzeichneten 0 Beiträge in dieser Aufschlüsselung. Quelle: Odin by Brandefense, 34.261 Untergrundbeiträge mit Österreichbezug, 1. Januar-22. November 2026; November unvollständig [S1]. Veröffentlichungszahlen sind keine bestätigten Vorfälle.

Sprachkennzeichnungen über die 34.261 Beiträge können sich überschneiden, wenn eine Nachricht mehrere Schriften oder Sprachen enthält. Die beobachteten Kennzeichnungssummen sind Englisch (22.049), Russisch (11.548), Deutsch (939), Chinesisch (924), Türkisch (512), Ukrainisch (217) und Arabisch (46). Die Sprache einer Nachricht spiegelt Ort oder Zielgruppe wider; sie belegt weder Nationalität noch staatliche Unterstützung eines Betreibers. [S1]

4.2 Produkt und Behauptung trennen

Eine Kontaktliste, ein Zugangsdatenangebot und administrativer Zugriff sind unterschiedliche Aussagen. Die Reaktion sollte vom konkret beschriebenen Material abhängen. Ein großes beworbenes Volumen macht eine Behauptung weder glaubwürdiger noch ihre Datensätze aktueller.

Ein Zugangsdatenangebot verlangt die Prüfung von Kontozugehörigkeit, Gültigkeit und Sitzungen. Eine Dokumentenbehauptung verlangt einen berechtigten Abgleich mit Organisationsunterlagen und früheren Veröffentlichungen. Eine Zugriffsbehauptung braucht Belege für den betroffenen Dienst, die Berechtigung und den Zeitpunkt.

Ein Kaufgesuch belegt Nachfrage, keinen Besitz. Der verlangte Preis belegt eine Preisvorstellung, keinen abgeschlossenen Verkauf oder die Zahlungsbereitschaft eines Käufers. Ein weitergeleiteter Screenshot belegt die Weiterleitung, keine unabhängige Überprüfung.

Diese Unterschiede begrenzen auch die Akteursanalyse. Ähnliche Beschreibungen können durch kopierte Werbung, denselben Datenbestand, einen gemeinsamen Vermittler oder getrennte Personen mit einer vertrauten Vorlage entstehen. Ein gemeinsamer Betreiber braucht einen konkreten Beleg über die Ähnlichkeit hinaus.

4.3 Chronologie lesen, ohne ein Einbruchsdatum zu erfinden

Das Beitragsdatum beschreibt die Veröffentlichung. Das Material kann ein älteres Ereignis, bereits veröffentlichte Informationen oder einen nicht mehr bestehenden Dienst betreffen. Der zuerst beobachtete Beitrag belegt nicht den Zeitpunkt eines Zugriffs oder Diebstahls.

Bei wiederkehrenden ähnlichen Angeboten sollte die Veröffentlichungsfolge erhalten bleiben. Ob es dieselbe Datei ist, bleibt ohne ausreichende Belege offen. Ein wiederkehrender Titel oder Umfang genügt nicht, um den Wechsel derselben Datei zwischen Plattformen zu belegen.

Für den Dienstverantwortlichen ist entscheidend, ob die Behauptung die aktuelle Reaktion verändert. Ein weiterhin gültiges Konto kann andere Eindämmungsmaßnahmen erfordern. Eine weitere Kopie einer bekannten historischen Behauptung kann stattdessen Kundenschutz oder Kommunikation rechtfertigen.

4.4 Sechs Fälle von Behauptungen und Nachfrage

Die folgenden Fälle nutzen gespeicherte Beiträge. Die zugehörigen Belegkarten zeigen die ursprünglichen Formulierungen. Die Daten bezeichnen Veröffentlichungen, keine Zugriffe oder Diebstähle. Weder die Fallauswahl noch die Kartenzahl ergibt eine nationale Vorfallzahl. [S1]

FALL U

U

Nachfrage nach Kontaktdatensätzen und Bankkennungen

Belegkarte B01 | Belegkarte B02 | 8. Jan. 2026 | 27. Jan. 2026 | Forum

Nachfrage nach Personendaten

Gesuche beobachtet

BEOBACHTUNG	Zwei Forumsbeiträge vom Januar suchen personenbezogene Kontaktdaten mit Österreichbezug; einer verlangt zusätzlich IBAN-Informationen. [S1]
CHRONOLOGIE	B01 stammt vom 8. Januar und B02 vom 27. Januar. Ihr ähnliches Thema belegt weder denselben Käufer noch eine abgeschlossene Übertragung.
BELEGT	Das gespeicherte Material belegt Nachfrage nach bestimmten Datenfeldern, keinen Besitz einer authentischen Datenbank.
ALTERNATIVE	Eine gesuchte Kontaktliste könnte aus unterschiedlichen Quellen stammen, darunter ältere oder zusammengestellte Bestände; die Herkunft ist hier ungeklärt.
GRENZE	Ein IBAN-bezogenes Gesuch belegt weder Kontrolle über ein Bankkonto noch gültige Zugangsdaten oder eine Zahlung.
REAKTION	Betrugsabwehr und Datenschutz sollten einen relevanten Datensatzabgleich mit berechtigten Belegen prüfen und eine unabhängige Bestätigung für identitätsbezogene Zahlungsanfragen vorbereiten.

Fazit

Prüfen Sie einen relevanten Hinweis anhand eigener Belege. Eine Anfrage belegt weder Datenbesitz noch Verkauf.

Der Entscheidungswert liegt in der gesuchten Kombination von Kontext und Kennungen. Ein finanzielles Detail kann ein späteres Gespräch glaubwürdiger machen, ohne eine Berechtigung zu erteilen. Der Bericht verbindet diese Gesuche nicht mit den gesonderten polizeilich bestätigten Betrugskampagnen.

Belegkarte B01 8. Jan. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Hallo, ich suche eine österreichische Datenbank. Österreichische Daten: Name, Telefonnummer, Adresse, Postleitzahl, Geburtsdatum.

Belegt
Ein Käufer fragt nach österreichischen personenbezogenen Datenfeldern. Die Anfrage belegt Nachfrage.

Nicht festgestellt
Datenbesitz, Echtheit, Kauf, Lieferung oder ein neuer Systemzugriff.

Belegkarte B02 27. Jan. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Gesucht werden Datenbankkontakte aus Österreich und Deutschland [...] IBAN.

Belegt
Ein Käufer sucht österreichische und deutsche Kontaktdaten mit IBAN-Angaben.

Nicht festgestellt
Kontozugang, Zahlungsberechtigung, echte Datensätze oder eine Transaktion.

FALL V

V

Zugang zu professionellen Dienstleistungen wird ohne bestätigten Zugriff beworben

Angabe unbestätigt

Belegkarte B03 | 1. Feb. 2026 | Forum | Unternehmensdienste

BEOBACHTUNG	Ein Beitrag vom 1. Februar bewirbt Zugang zu österreichischen professionellen Dienstleistungen mit einer Branchenbezeichnung für Rechtsdienstleistungen. [S1]
CHRONOLOGIE	Das Datum belegt die Veröffentlichung der Anzeige. Beginn, Überprüfung oder Verkauf eines Zugangs sind zeitlich nicht belegt.
BELEGT	Der gespeicherte Beitrag existiert und behauptet Zugang. Er belegt weder einen Preis noch die bestätigte Identität einer Zielorganisation.
ALTERNATIVE	Eine Anzeige kann veralteten, begrenzten oder unbrauchbaren Zugang beschreiben; Organisation und tatsächliche Berechtigungen bleiben ungeklärt.
GRENZE	Die technische Formulierung belegt weder eine Schwachstelle noch einen Ausnutzungsweg oder eine Verbindung zu einem gesonderten Produkthinweis.

REAKTION	Eine möglicherweise betroffene Organisation sollte Kontozugehörigkeit, Berechtigungen und Sitzungsbelege vor der Eindämmung prüfen. Der Dienstverantwortliche bewertet die betrieblichen Auswirkungen.

Fazit

Prüfen Sie Kontozuordnung, Rechte und aktuelle Zugriffe, bevor Sie die Eindämmung festlegen.

Das empfangende Team sollte das relevante Konto und den Dienst intern bestimmen. Hier werden weder ein Opfername noch ein funktionierender Zugangsweg veröffentlicht. Die Anzeige belegt keine Transaktion.

Belegkarte B03 — 1. Feb. 2026

[Alias zurückgehalten] | Forum | Forum | Russisch und Englisch

ORIGINAL

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

ÜBERSETZUNG

Zugang Österreich […] Anwaltskanzleien und Rechtsdienstleistungen forti Domänenbenutzer

Belegt
Eine Anzeige beschreibt Zugang bei einem österreichischen Dienstleister. Ein Verkaufspreis ist nicht belegt.

Nicht festgestellt
Nutzbarer Zugang, Identität eines Betroffenen, Verkaufspreis, Schwachstelle oder abgeschlossener Verkauf.

W

FALL W

Ein verzeichnisähnliches Angebot belegt keinen Einbruch

Belegkarte B04 | 2. Feb. 2026 | Forum | Verzeichnisdaten

Herkunft ungeklärt

BEOBACHTUNG	Eine Anzeige vom 2. Februar beschreibt einen regionalen Verzeichnisdatenbestand mit angeblich 21 Attributen. [S1]
CHRONOLOGIE	Das Veröffentlichungsdatum belegt weder den Erhebungszeitpunkt noch, ob die Datensätze bereits öffentlich waren.
BELEGT	Die Anzeige nennt kontaktbezogene Felder und bezeichnet E-Mail-Adressen als überprüft; diese Überprüfung bleibt eine Behauptung des Verkäufers.
ALTERNATIVE	Zusammengestellte öffentliche Verzeichnisse, ältere Geschäftskontakte oder wiederverwendetes Material könnten ähnliche Beschreibungen ohne neuen Einbruch ergeben.
GRENZE	Echtheit der Datei, Herkunft, Aktualität, Berechtigungen und beworbene Attribute wurden nicht unabhängig überprüft.

REAKTION	Ein zuständiger Datenverantwortlicher sollte berechtigte Beispiele mit öffentlichen und früher veröffentlichten Datensätzen vergleichen. Vor einer Vorfallbeschreibung ist plausibler Missbrauch zu bewerten.

Fazit

Vergleichen Sie die Felder mit öffentlichen Verzeichnissen und autorisierten Unterlagen, bevor Sie einen neuen Systemzugriff annehmen.

Ein Verzeichnisthema kann für Identitätstäuschung relevant sein, auch wenn kein Einbruch belegt ist. Die Organisation sollte die tatsächlichen Informationen und eine glaubhafte Verwendung prüfen. Eine Feldzahl darf nicht zur Zahl betroffener Personen werden.

Belegkarte B04 2. Feb. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Der Datensatz enthält 21 Merkmale, insbesondere Titel, Anschriften, Telefonnummern und bestätigte E-Mail-Adressen.

Belegt

Ein Verkäufer beschreibt einen verzeichnisartigen Datensatz mit 21 Merkmalen. Bestätigt ist die Formulierung des Verkäufers.

Nicht festgestellt

Aktualität, rechtmäßige Herkunft, Richtigkeit, neuer Systemzugriff oder Zahl betroffener Personen.

X

FALL X

Kontakte mit Finanzinteresse enthalten einen älteren Datumshinweis

Angabe unbestätigt

Belegkarte B06 | 18. Apr. 2026 | Forum | Finanzwerbung

BEOBACHTUNG	Ein Beitrag vom 18. April bewirbt Forex- und Kryptowährungskontakte mit Österreichkennzeichnung und behauptet 13.967 Zeilen. [S1]
CHRONOLOGIE	Das gezeigte Material enthält einen Datumshinweis aus 2024. Die Veröffentlichung 2026 belegt daher keinen neuen Diebstahl im Jahr 2026.
BELEGT	Der gespeicherte Beitrag behauptet die Länderkennzeichnung und Zeilenzahl; beides belegt weder eindeutige Personen noch authentische Datensätze.
ALTERNATIVE	Älteres Kontaktmaterial, Zusammenstellung und wiederholte Werbung bleiben plausible Erklärungen der Beschreibung.

GRENZE	Aktueller Kontozugriff, abgeschlossener Verkauf, Anlageverlust oder die Ursache eines späteren Betrugs sind nicht belegt.
REAKTION	Betrugsteams sollten einen relevanten Treffer als Kontext für gezielte Täuschung behandeln. Datenalter und Echtheit sind anhand berechtigter Unterlagen zu prüfen.

Fazit

Halten Sie behauptetes Datum und Dateneinheit fest. Setzen Sie Zeilen nicht mit Personen oder neuem Diebstahl gleich.

Der Vergleich mit amtlichen Berichten über Anlagebetrug betrifft die Funktion der Daten, keine nachgewiesene Lieferkette. Kontaktdaten können eine glaubhafte Ansprache unterstützen. Es gibt hier aber keinen Beleg, dass dieser Anbieter die untersuchten Callcenter belieferte. [S19]

Belegkarte B06 — 18. Apr. 2026

[Alias zurückgehalten] · Forum · Forum · Englisch

ORIGINAL

Country :Austria Quantity :13967

ÜBERSETZUNG

Land: Österreich Anzahl: 13967

Belegt
Ein Beitrag bietet angeblich 13.967 Österreich zugeordnete Kontakte für Devisen- oder Kryptogeschäfte an.

Nicht festgestellt
Unterschiedliche Personen, neuer Datendiebstahl, echte Datensätze oder abgeschlossener Betrug.

FALL Y

Y

Nachfrage nach Haushaltskontakten beschreibt eine Zielgruppe, keine Nationalität

Gesuche beobachtet

Belegkarte B07 · Belegkarte B08 · 22. Sept. 2026 · 15. Okt. 2026 · Forum · Private Kontaktdaten

BEOBACHTUNG	Gesuche vom September und Oktober suchen private Telefonkontakte; eines nennt russischsprachige Menschen ab 45 Jahren. [S1]
CHRONOLOGIE	B07 stammt vom 22. September und B08 vom 15. Oktober. Wiederholte Themen belegen keinen gemeinsamen Betreiber.
BELEGT	Die Beiträge zeigen gesuchte Zielgruppenmerkmale, keinen Listenbesitz oder bereits erfolgten Kontakt mit diesen Menschen.

ALTERNATIVE	Demografische und sprachliche Kriterien können die gewünschte Zielgruppe eines Käufers beschreiben, ohne Datenquelle oder geplante Verwendung zu bestimmen.
GRENZE	Der Wunsch nach russischer Sprache belegt weder Nationalität noch staatliche Unterstützung oder eine Verbindung zu russlandbezogenen politischen Aktivitäten.
REAKTION	Kundenschutzteams sollten einen unabhängig überprüfbaren Hilfsweg anbieten und relevanten vermuteten Missbrauch prüfen, ohne der Zielgruppe eine Schuld zuzuschreiben.

Fazit

Bereiten Sie verständliche Betrugswarnungen vor. Die gewünschte Sprache belegt keine Nationalität des Akteurs.

Der Bericht leitet keine gemessene Betrugsrate für diese Alters- oder Sprachgruppe ab. Eine gesuchte Zielgruppe ist eine Nachfragebeobachtung. Jede Behauptung über eine konkrete Kampagne bräuchte gesonderte Kommunikations-, Zahlungs- und Opferbelege.

Belegkarte B07 — 22. Sept. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

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

ÜBERSETZUNG

Festnetznummern aus Telefonverzeichnissen werden bevorzugt. Gibt es eine solche Datenbank?

Belegt
Ein Käufer bevorzugt private Festnetznummern aus Verzeichnissen.

Nicht festgestellt
Besitz einer Datenbank, abgeschlossener Kauf oder späterer Betrug.

Belegkarte B08 — 15. Okt. 2026

[Alias zurückgehalten] | Forum | Forum | Englisch

ORIGINAL

Home phone numbers of RUSSIAN-speaking individuals aged 45+

ÜBERSETZUNG

Festnetznummern RUSSISCH-sprachiger Personen im Alter von 45+

Belegt
Ein Käufer sucht nach älteren russischsprachigen Personen als Zielgruppe.

Nicht festgestellt
Nationalität, staatliche Steuerung, Datenbesitz oder abgeschlossener Betrug.

FALL Z

Z

Wiederholte Werbung für ein Phishing-Panel behauptet Unterstützung von Anmeldeverfahren

Belegkarte B09 | Belegkarte B10 | 20. Nov. 2026 | 22. Nov. 2026 | Forum | Finanzkundendienste

Angabe unbestätigt

BEOBACHTUNG	Beiträge vom 20. und 22. November bewerben ein Phishing-Panel. Sie behaupten Unterstützung für Einmalpasswörter (OTP), Transaktionsnummern (TAN), Zwei-Faktor-Authentifizierung, QR-Codes und PhotoTAN. [S1]
CHRONOLOGIE	Der spätere Beitrag wiederholt das Produkt und nennt Österreich unter mehreren Ländern; er ist kein zweiter nachgewiesener Einbruch.
BELEGT	Das gespeicherte Material belegt beworbene Fähigkeiten und behauptete Marktabdeckung.
ALTERNATIVE	Eine Produktbeschreibung kann Funktionen übertreiben oder einen ungetesteten Dienst betreffen; Werbung allein belegt keine Wirksamkeit.
GRENZE	Eine erfolgreiche Umgehung der Authentifizierung, Zugang zu Banksystemen, eine Opferzahl oder ein abgeschlossener Verkauf sind nicht nachgewiesen.
REAKTION	Identitäts- und Betrugsverantwortliche sollten den tatsächlichen Kundenablauf und vertrauenswürdige Bestätigungswege prüfen. Kontospezifische Belege sind vor der Auswahl von Eindämmungsmaßnahmen zu überprüfen.

Fazit

Prüfen Sie Schutz vor Kundentäuschung und unerlaubten Zahlungen. Eine Anzeige belegt keine umgangene Anmeldung.

Die Aussage, ein Werkzeug unterstütze ein Anmeldeverfahren, belegt kein Versagen jeder Umsetzung dieses Verfahrens. Die Abwehrprüfung sollte den tatsächlichen Dienst, die Nutzerhandlung und verfügbare Telemetrie berücksichtigen. Sie sollte keine Verkäuferbehauptung als Testergebnis übernehmen.

Belegkarte B09 20. Nov. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Unterstützung für OTP/TAN/2FA einschließlich QR-Codes und PhotoTAN-Verfahren.

Belegt
Eine Anzeige für eine Phishing-Oberfläche behauptet Unterstützung für OTP, TAN, QR und PhotoTAN.

Nicht festgestellt
Nachgewiesene Wirksamkeit, erfolgreiche Umgehung der Anmeldung oder Zugriff auf Banksysteme.

Belegkarte B10 22. Nov. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Das Paket richtet sich an mehrere Länder, darunter Irland, die Niederlande, Finnland, Österreich, Deutschland, Frankreich, Belgien, Griechenland, Luxemburg und Italien.

Belegt
Eine spätere Anzeige nennt Österreich erneut unter mehreren Zielmärkten.

Nicht festgestellt
Ein zweiter Vorfall, gemeinsame Betreiber, Verkäufe, funktionierende Software oder Zugriff auf Banksysteme.

4.5 Auch die Beschaffung von Zugangsdaten ist eine Nachfragebeobachtung

Ein gesonderter Beitrag vom 11. April sucht dauerhafte Lieferanten mit Bezug zu Deutschland, Österreich und der Schweiz. Der gespeicherte Auszug belegt Beschaffungsinteresse. Er belegt weder eine Lieferung noch getestete Zugangsdaten oder eine vereinbarte Geschäftsbeziehung. [S1]

Die Folgerung für die Abwehr ist bedingt: Tauchen relevante Zugangsdaten auf, prüfen Sie das eigene Konto und seine Vorgeschichte. Ein allgemeines Gesuch rechtfertigt weder umfassende Zurücksetzungen noch die Behauptung eines Eindringens in Organisationen der beworbenen Länder.

Belegkarte B05 — 11. Apr. 2026

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

Wir suchen Lieferanten aus Deutschland, Österreich und der Schweiz.

Belegt
Ein Beitrag sucht regelmäßige Lieferanten und nennt Österreich als einen Zielmarkt.

Nicht festgestellt
Besitz von Zugangsdaten, nutzbare Konten, Lieferung oder abgeschlossene Transaktion.

Eine weitere Anzeige behauptet webbasierten Fernzugriff auf Desktop-Systeme mit Bezug zu einem Telekommunikationsanbieter und administrative Berechtigungen. Ihr genaues Veröffentlichungsdatum innerhalb des Berichtszeitraums ist ungewiss und liegt außerhalb des jüngsten Zeitfensters. Aktueller Zugriff, betroffene Daten, eine Transaktion oder eine Verbindung zu einem amtlich beschriebenen Vorfall sind nicht belegt. [S1]

Belegkarte B19 — 2026 (Datum ungeklärt)

[Alias zurückgehalten] Forum Forum Englisch

ORIGINAL

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

ÜBERSETZUNG

RDWeb-Zugang zu einem Telekommunikationsunternehmen in Österreich. Cloud-Administratorrechte (Eigentümer)

Hinweis. Veröffentlichungsdatum im Berichtszeitraum ungeklärt; außerhalb des jüngsten Zeitfensters.

Belegt
Eine Anzeige behauptet RDWeb-Zugang und Cloud-Eigentümerrechte bei einer Österreich zugeordneten Telekommunikationsorganisation.

Nicht festgestellt
Nutzbarer Zugang, Identität des Ziels, aktuelle Rechte, abgeschlossener Verkauf oder geklärtes Veröffentlichungsdatum.

4.6 Aktuelle Untergrundaktivitäten: 8.–22. November

Die Panel-Anzeigen vom 20. und 22. November gehören aufgrund ihrer Veröffentlichungsdaten in das abschließende Zeitfenster. Die Wiederholung belegt fortgesetzte Werbung, keinen gemessenen Anstieg erfolgreicher Angriffe. [S1]

Eine Anzeige vom 18. November beschreibt außerdem Kontaktdaten und zeigt die Menge „115k". Das ist eine ungeprüfte Werbeangabe, keine bestätigte Zahl von Datensätzen oder eindeutigen Personen. Herkunft, Datenalter, Genauigkeit und ein möglicher Geschäftsabschluss bleiben ungeklärt. [S1]

Belegkarte B20 — 18. Nov. 2026

[Alias zurückgehalten] | Chat-Nachricht | Telegram | Englisch

ORIGINAL

People DB
Qty: 115k

ÜBERSETZUNG

Personendatenbank
Anzahl: 115k

Belegt
Eine Nachricht bietet einen Österreich zugeordneten Kontaktdatensatz mit angeblich 115.000 Einträgen an. Die Menge ist unbestätigt.

Nicht festgestellt
Echte Dateien, eindeutige Personen, Aktualität, neuer Diebstahl oder ein Eindringen in eine Organisation.

Ein Orts- oder Firmenbezug im Beispielkontext belegt keinen Zugriff auf eine Organisation. Der Bericht verbindet diese Anzeige nicht mit den gesondert offiziell beschriebenen Vorfällen.

Die amtlichen Novemberhinweise und die beworbenen Panel-Fähigkeiten bleiben getrennte Belege. Zeitliche Nähe zeigt nicht, dass der Verkäufer eine benannte Schwachstelle nutzte, einen Akteur eines amtlich beschriebenen Falls belieferte oder einen Bankvorfall verursachte.

Leiten Sie passende Dienst- oder Kontobeobachtungen an die Verantwortlichen weiter. Halten Sie Produktbehauptung, tatsächliche Zugriffsbelege und das Zahlungsereignis des Kunden getrennt, bis eine konkrete Verbindung ihre Zusammenführung trägt.

4.7 Ein angemessener Prüfauftrag

Ein Eskalationsvermerk sollte dem empfangenden Team sagen, welche Entscheidung sich durch die Beobachtung ändern könnte. Er sollte die Unsicherheit der Behauptung erhalten und personenbezogene Datensätze nicht weiter als nötig verbreiten.

Frage	Gesuchte Belege	Unterstützte Entscheidung
Ist es relevant?	Berechtigter Abgleich mit Domain, Mandant, Datensatz oder Konto	Richtige Verantwortung zuweisen
Ist es aktuell?	Datenalter, Kontostatus und frühere Behebung	Dringlichkeit und Umfang wählen
Ist es authentisch?	Vergleich mit Datensätzen, welche die Organisation rechtmäßig prüfen darf	Relevanz des Materials bestätigen oder verwerfen
Wurde Zugang genutzt?	Zugriffs-, Sitzungs- und Anwendungsbelege	Eindämmung und Untersuchung auswählen
Wem könnte Schaden entstehen?	Bestätigte Datenkategorien und glaubhafter Missbrauch	Datenschutz- und Kundenschutzentscheidungen treffen

Der erste Prüfschritt sollte weder der Erwerb kriminellen Materials noch das Testen fremder Konten sein. Arbeiten Sie mit berechtigten Unterlagen, vorhandenen Belegen und dokumentierten Verantwortlichkeiten. Eskalieren Sie Unsicherheit, statt sie als Zusicherung zu behandeln.

4.8 Beobachtung und Kundenrisiko getrennt abschließen

Eine Kontountersuchung kann abgeschlossen sein, während eine Person weiterhin durch Identitätstäuschung mit bereits veröffentlichten Informationen gefährdet ist. Umgekehrt kann eine verdächtige Nachricht betrügerisch sein, ohne einen Informationsverlust bei der Organisation des Empfängers zu belegen.

Dokumentieren Sie diese Ergebnisse getrennt. Technisch Verantwortliche sollten die Zugriffsergebnisse festhalten. Kundenbetreuung oder Datenschutz sollten plausiblen Schaden und Empfehlungen benennen. Die Kommunikation sollte das bestätigte Ergebnis beschreiben, ohne die weitergehende Verkäuferdarstellung zu übernehmen.

KERNAUSSAGEN

01

Ein veröffentlichtes Angebot und seine inhaltliche Behauptung sind getrennte Aussagen.

02

Behandeln Sie Beitragsdaten als Veröffentlichungsdaten und prüfen Sie das Datenalter gesondert.

03

Weisen Sie Überprüfung und Kundenschutz klar Verantwortlichen zu.

KAPITEL 05

Beispiele für Zielauswahl nach Sektor

05

DIESES KAPITEL BEANTWORTET

Was belegen die in ihren Quellen gelesenen österreichischen Fälle zu Zugriff, Auswirkungen und Reaktion?

17

ausführliche amtliche oder quellenbasiert berichtete Falldarstellungen

5.1 Die Grenzen der Belege bestimmen die Lesart 46

5.2 Identitäten und institutionelle Wiederherstellung 47

5.3 Vertrauensbasierter Betrug gegen Kunden und Beschäftigte 49

5.4 Dienstleister und Geschäftskorrespondenz 51

5.5 Geschäftliche und gehostete Dienstleistervorfälle im späteren Jahresverlauf 55

5.6 Weitere amtliche Hinweise und ausdrückliche Ausschlüsse 60

5.7 Aktuelle Aktivitäten: 8.–22. November 2026 61

KAPITEL 05

Beispiele für Zielauswahl nach Sektor

KURZFASSUNG

Die öffentlichen Fälle umfassen Identitätszugriffe, Bewerbungsköder, Betrug gegen Kunden und Vorfälle bei gehosteten Diensten. Ihre Bestätigungsgrade unterscheiden sich. Kampagnenhinweise können Aktivitäten in Österreich belegen, ohne eine Opferzahl zu nennen. Eine Organisation kann ein begrenztes Datenereignis bestätigen, während die Zuschreibung offenbleibt. Testen Sie anhand der Fälle den passenden Geschäftsprozess und bewahren Sie die Quellengrenzen in Ihrer eigenen Reaktion.

5.1 Die Grenzen der Belege bestimmen die Lesart

Diese Falldarstellungen wurden nach ihrem Nutzen für die Reaktion ausgewählt. Sie sind keine überschneidungsfreie nationale Vorfallerhebung. Ein Kampagnenhinweis kann mehrere Ereignisse beschreiben; eine spätere Aktualisierung kann einen bereits berichteten Fall erneut behandeln. Eine vorläufige Behördenerklärung zu einer laufenden Untersuchung belegt keinen bestätigten Einbruch und keine Kundenauswirkung.

Sektor oder Funktion	Beobachtetes Problem	Grenze der Belege	Schwerpunkt der Reaktion
Bildung	Administrativer Verzeichniszugriff; begrenzter Ransomware-Umfang	Von der Quelle bestätigte Mitteilungen; ungeklärter vollständiger Datenumfang erhalten	Identitätswiederherstellung, Isolation und eingegrenzte Prüfung
Industrie und Personalbeschaffung	Längere Bewerbungskorrespondenz und schädliches Archiv	CERT bestätigt österreichische Fälle; keine öffentliche Gesamtzahl	Untersuchung von Kontaktformular, E-Mail und Endgeräten
Baunahe KMU	Phishing über echte geschäftliche Postfächer	CERT-Kampagnenwarnung; Umfang nicht beziffert	Sitzungen, verbundene Zugänge und Partnerwarnung
Dienstbetreiber	Historische Postfachdokumente im Netz	Enge Bestätigung eines Sprechers unterscheidet sich von weitergehender Behauptung	Umfang von Postfach- und Dokumentenzugriffen
Beherbergung und gehostete Dienste	Täuschung mit Buchungskontext und dienstleistergehostete Systeme	Getrennte Kampagnen- und Vorfallpopulationen	Zahlungsbestätigung und Umfang beim Dienstleister
Öffentliche Verwaltung	Dienstliche Mitarbeiterkontakte oder erweiterter Datenkategorienumfang	Amtliche Darstellungen in der Presse wiedergegeben; Akteur unbenannt	Dienstleisterzugriff, Datenschutzaktualisierungen und Vorsorge gegen Imitation
Bankkunden	SMS, falscher Telefonsupport und Zahlungsmanipulation	Kundenbetrug; Einbruch in Banksysteme nicht belegt	Unabhängiger Kontakt und Reaktion auf Transaktionen

Die Fallbuchstaben kennzeichnen Darstellungen. Sie sind keine Vertrauensskala. Jede nachfolgende Handlung ist eine angemessene Empfehlung für eine Organisation mit vergleichbaren Belegen.

5.2 Identitäten und institutionelle Wiederherstellung

A

FALL A

Administrativer Zugriff verlangt eine eingegrenzte Wiederherstellungsentscheidung (O01)

Bildung

Amtliche Mitteilung

BEOBACHTUNG	Eine österreichische Bildungseinrichtung bestätigte Anfang 2026 administrativen Verzeichniszugriff und eine Kontozurücksetzung. [S25]
CHRONOLOGIE	Die Einrichtung erkannte den Vorfall, datierte den Zugriff auf kurz vor der Erkennung, führte eine Kontozurücksetzung durch und veröffentlichte einige Wochen später eine abschließende Aktualisierung.
BELEGT	Die abschließende Darstellung fand keine Hinweise auf umfangreichen Zugriff oder Verfälschung, schloss einen gewissen Datenzugriff aber nicht aus.
ALTERNATIVE	Administrative Reichweite und zugängliche Datenkategorien belegen keine vollständige Ausleitung.
GRENZE	Die öffentliche Mitteilung klärt nicht die Gefährdung jedes Kontos und weist hier keinem Akteur die Verantwortung zu.
REAKTION	Prüfen Sie administrative Änderungen, stellen Sie Konten über vertrauenswürdige Wege wieder her und dokumentieren Sie offene Fragen zum Datenzugriff.

Fazit

Prüfen Sie administrative Änderungen und vertrauenswürdige Wiederherstellung vor dem Vorfallabschluss.

Die übertragbare Entscheidung betrifft die Freigabe der Identitätswiederherstellung. Eine Zurücksetzung kann viele berechtigte Nutzer beeinträchtigen. Die Organisation braucht daher Kapazitäten für Ausnahmen und Menschen ohne Zugang zum normalen Weg. Die Überprüfung darf nicht auf einer Nachricht über das betroffene Konto beruhen.

Beschäftigte für Ausnahmefälle sollten wissen, welche Belege sie verlangen dürfen und wie Unsicherheit eskaliert wird. Der Vorfallakt sollte ein für berechtigte Nutzung wiederhergestelltes Konto von einem Konto mit vollständig geprüfter historischer Aktivität unterscheiden.

FALL B

B ■ Die Mitteilung einer Bildungseinrichtung präzisiert den Ransomware-Umfang (O02)

Bildung

Primärmitteilung

BEOBACHTUNG	Eine Mitteilung einer Bildungseinrichtung von Anfang 2026 bestätigt einen Ransomware-Vorfall in einem begrenzten Teil ihrer IT-Umgebung. [S58]
CHRONOLOGIE	Erste Eindämmung und Wiederherstellung gingen der formellen Mitteilung voraus, die den hier verwendeten personenbezogenen Datenumfang beschreibt.
BELEGT	Die Einrichtung beschreibt unbefugten Konto- und Netzwerkzugriff sowie entwendete personenbezogene Informationen aus einigen Nutzerkonten; der genaue Informationsumfang bleibt ungeklärt.
ALTERNATIVE	Ein begrenztes System und fortgesetzter Unterricht belegen nicht, dass keine personenbezogenen Informationen eingesehen wurden.
GRENZE	Die Primärmitteilung hält Unsicherheit über Serverzugriff und vollständigen Datenumfang fest. Sie nennt keinen verantwortlichen Akteur.
REAKTION	Prüfen Sie betroffene Identitäten, isolieren Sie Systeme und überprüfen Sie die Wiederherstellung. Bewerten Sie den personenbezogenen Datenumfang, bevor Sie die Wiederherstellung als abgeschlossen beschreiben.

Fazit

Prüfen Sie Identitäten und Wiederherstellung und erhalten Sie die Primäraussage zum personenbezogenen Datenumfang.

Die formelle Primärmitteilung bestimmt den Umfang dieser Darstellung statt früherer enger Entwarnungen. Eine Bezeichnung aus einer Täterbehauptung wird nicht als amtlich festgestellter Betreiber übernommen. Folgen für Unterricht und Datenschutz bleiben getrennte Fragen.

5.3 Vertrauensbasierter Betrug gegen Kunden und Beschäftigte

C

FALL C

Aus einer SMS mit Bankbezug wird eine telefonische Zahlungsanweisung (O03)

Bankkunden

Amtliche Warnung

BEOBACHTUNG	Am 1. April warnte das Bundeskriminalamt vor massenhaften SMS an österreichische Nummern unter der Identität einer deutschen Bank. [S18]
CHRONOLOGIE	Die Nachricht führte zu einem falschen telefonischen Supportweg, anschließend zu einer betrügerischen Bankseite und einer verlangten Überweisung.
BELEGT	Die Polizei berichtete tatsächliche Schäden bei einer ungefähr im hohen zweistelligen Bereich liegenden Opferzahl.
ALTERNATIVE	Die Täuschung der Kunden belegt keinen Zugriff auf die Systeme der imitierten Bank.
GRENZE	Ungefähre polizeiliche Beschreibungen rechtfertigen keine genaue Opferzahl oder nationale Schadenssumme.
REAKTION	Lehnen Sie Anweisungen ab, Geld auf ein angeblich sicheres Konto zu verschieben, und kontaktieren Sie die Bank über einen bekannten Kanal.

Fazit

Nutzen Sie einen bekannten Bankkontakt und prüfen Sie die tatsächliche Transaktion.

Ein Betrugsteam sollte den Moment üben, in dem ein besorgter Kunde den Anrufer als Beschützer wahrnimmt. Eine technisch gültige Zahlungsfreigabe kann dennoch auf Täuschung beruhen. Der Eskalationsprozess sollte Beschäftigten ermöglichen, innezuhalten, den Vorwand zu erklären und den Kunden sicher zu erreichen.

D

FALL D

Ein Identitätsverlängerungsköder führt zu Geräte- und Bankzugriff (O04)

Kundenidentität

Amtliche Warnung

BEOBACHTUNG	Der Hinweis des Bundeskriminalamts vom 7. April beschreibt Nachrichten zur Verlängerung digitaler Identitätszertifikate mit anschließendem betrügerischem Supportkontakt. [S17]
CHRONOLOGIE	Das Szenario führt von einer unerbetenen SMS über Bank-Imitation zur Aufforderung, Fernwartungssoftware zu installieren.

BELEGT	Die Warnung betrifft eine reale Betrugskampagne. Auslaufende Zertifikate liefern den Vorwand, keine Zahl betroffener Konten.
ALTERNATIVE	Eine Nachricht mit dem Namen eines Identitätsdienstes zeigt kein Eindringen in diesen Dienst.
GRENZE	Die spätere Darstellung vom Oktober greift diese Frühjahrsgruppe erneut auf. Sie darf nicht als gesonderte Kampagne gezählt werden. [S16]
REAKTION	Prüfen Sie die Verlängerung über den bekannten amtlichen Dienst und lehnen Sie unerbetene Anweisungen zur Gerätesteuerung oder zum Banksupport ab.

Fazit

Beginnen Sie die Verlängerung unabhängig und lehnen Sie unerbetene Fernsteuerung ab.

Die Reaktion muss mehrere Kommunikationskanäle berücksichtigen. Eine Person kann die ursprüngliche Nachricht verlassen und die Täuschung telefonisch fortsetzen. Eine Warnung allein vor schädlichen Links kann die spätere Aufforderung zu Fernsteuerung oder Zahlungsfreigabe übersehen.

FALL E

E

Anlagebetrug setzt sich mit einem falschen Rückholangebot fort (O05)

Finanzkunden

Polizeimeldung

BEOBACHTUNG	Eine polizeiliche Untersuchung vom April beschreibt manipulierte Inhalte mit öffentlichen Personen, falsche Anlageplattformen und spätere Gebührenforderungen für angebliche Geldrückholung. [S19]
CHRONOLOGIE	Die veröffentlichte Darstellung folgte auf koordinierte Maßnahmen vom 17. April gegen Callcenter-Infrastruktur und Wohnobjekte.
BELEGT	Die amtliche Darstellung beschreibt eine grenzüberschreitende Untersuchung mit österreichischen Opfern und mehr als einer Betrugsstufe.
ALTERNATIVE	Eine scheinbare Empfehlung, ein angezeigtes Anlageguthaben oder eine versprochene Rückholung bestätigt eine Anlage nicht unabhängig.
GRENZE	Die Schadensschätzung der gesamten Untersuchung ist weder eine rein österreichische noch eine nur 2026 betreffende nationale Schadenssumme.
REAKTION	Prüfen Sie die Zulassung unabhängig, begrenzen Sie unerbetene Fernsteuerung und warnen Sie betroffene Kunden vor Rückholangeboten als möglicher weiterer Betrugsstufe.

Fazit

Prüfen Sie die Zulassung und schützen Sie vor weiteren Gebührenforderungen für angebliche Rückholung.

Ein Leitfaden für die Kundenbetreuung sollte Schuldzuweisungen vermeiden. Bereits getäuschte Menschen können besonders empfänglich für angebliche Hilfe bei der Rückholung sein. Halten Sie die Schutzhandlung konkret: bekannter Bankkontakt, Sicherung relevanter Kommunikation und unabhängige Bewertung weiterer Anfragen.

5.4 Dienstleister und Geschäftskorrespondenz

FALL F

F

Einer Bewerbungskorrespondenz folgt erpressungsbezogener Zugang (O06)

Industrie und Personalbeschaffung

CERT-Bewertung

BEOBACHTUNG	Im ZipLine-Hinweis vom Mai berichtet CERT.at von bestätigten österreichischen Fällen und Hinweisen auf Zugangsbeschaffung für Qilin-Operationen. [S9]
CHRONOLOGIE	Die beschriebene Ansprache beginnt über öffentliche Kontaktformulare und entwickelt sich über Tage oder Wochen, bevor ein Archiv eintrifft.
BELEGT	CERT.at verbindet seine Kampagnenbewertung mit österreichischen Beobachtungen; eine vollständige österreichische Opferzahl wird nicht veröffentlicht.
ALTERNATIVE	Gewöhnlicher Bewerbungskontakt ist legitim; die spätere Handlung und ihre Belege bestimmen die Untersuchung.
GRENZE	Die beschriebene Zugangsbeziehung belegt nicht denselben Weg für jeden Bewerbungsköder oder Qilin-Eintrag.
REAKTION	Prüfen Sie relevante Korrespondenz, den Umgang mit Anhängen und Endgerätebelege. Dämmen Sie bestätigten Zugriff ein, statt Geschäftskommunikation pauschal zu blockieren.

Fazit

Prüfen Sie relevante Korrespondenz und Endgerätebelege vor der Auswahl von Eindämmungsmaßnahmen.

Beschaffung, Empfang und Personalbeschaffung können die Ansprache zuerst sehen. Ihr Meldeweg sollte die Sicherheit erreichen, ohne eine Schadsoftwarediagnose von ihnen zu verlangen. Der Bericht veröffentlicht weder Köderdomains der Kampagne noch eine Anleitung zur Nachstellung des Angriffs.

FALL G

G

Alte Dokumente im Netz belegen keinen weitergehenden betrieblichen Vorfall (O07)

Dienstbetreiber

Pressebericht

BEOBACHTUNG	Presseberichte aus 2026 zitieren den Sprecher einer österreichischen Organisation zu älteren Dokumenten aus einem Postfach. [S26]
CHRONOLOGIE	Die Berichte betreffen Dokumente aus 2025. Sie belegen kein neues Einbruchsdatum für jedes Dokument.
BELEGT	Die Sprecherdarstellung ist enger als die kriminelle Erzählung. Nach damaligem Kenntnisstand verneint sie einen weitergehenden Vorfall in betrieblichen Systemen.
ALTERNATIVE	Dokumentenoffenlegung und fortgesetzter Betrieb können nebeneinander bestehen; keines widerlegt das andere.
GRENZE	Der Bericht bestätigt weder das vom Urheber der Behauptung genannte Gesamtvolumen noch vollständigen Datenumfang oder Akteursidentität.
REAKTION	Untersuchen Sie Postfach und Dokumentenbestand. Prüfen Sie Auswirkungen auf Kunden und betriebliche Dienste gesondert.

Fazit

Grenzen Sie das Postfach ein und prüfen Sie betriebliche Auswirkungen gesondert.

Die Kommunikation sollte keine einzige Ja-oder-Nein-Formulierung verwenden, die beide Darstellungen vermischt. Sie kann den Dokumentenfund anerkennen, geprüfte Dienstgrenzen nennen und den nächsten Prüfzeitpunkt angeben. Das ist hilfreicher als die Wiederholung einer ungeprüften Behauptung oder eines behaupteten Volumens.

FALL H

H

Ein vertrauter Absender verbreitet einen weiteren Zugangsdatenköder (O08)

Unternehmensdienste

Amtliche Warnung

BEOBACHTUNG	Die CERT.at-Warnung vom 24. Juli beschreibt Phishing über echte österreichische Unternehmenspostfächer, besonders bei baunahen KMU. [S10]
CHRONOLOGIE	Das Muster nutzt einen Köder zum Anzeigen von Dokumenten, erfasst Zugangsdaten und verschickt weitere Nachrichten an bekannte Kontakte.
BELEGT	Die Quelle berichtet eine ungewöhnliche Zunahme dieses Kampagnenmusters; sie nennt keine nationale Opferzahl.

ALTERNATIVE	Domain-Authentifizierung oder ein vertrauter Absender belegen keine berechtigte Anmeldeaufforderung.
GRENZE	Die Warnung nennt nicht jeden verbundenen Dienst und bestätigt nicht, dass jeder Empfänger Zugangsdaten eingegeben hat.
REAKTION	Setzen Sie betroffene Konten zurück, beenden Sie relevante Sitzungen, prüfen Sie verbundene Zugänge und warnen Sie Geschäftskontakte über einen vertrauenswürdigen Weg.

Fazit

Prüfen Sie Sitzungen und verbundene Zugänge und warnen Sie Partner anschließend über einen sicheren Weg.

Die Partnerwarnung sollte die unsichere Handlung erklären. Sie sollte Empfänger nicht um eine Antwort im verdächtigen Gespräch bitten, um sich zu vergewissern. Sicherheits- und Geschäftsverantwortliche sollten festlegen, welche Kontakte gewarnt werden müssen und wie diese die Echtheit prüfen können.

FALL I

Richtige Buchungsdetails bestätigen keine Zahlungsforderung (O09)

Amtliche Warnung

Tourismuskunden

BEOBACHTUNG	Der CERT.at-Hinweis vom 14. August beschreibt Betrug mit glaubhaften Reisebuchungsdaten und täuschenden Zahlungsaufforderungen. [S11]
CHRONOLOGIE	Eine Person erhält nach einer echten Buchung eine Aufforderung oder stößt auf eine falsche Anzeige oder einen imitierten Supportweg.
BELEGT	Der Hinweis unterscheidet mehrere Mechanismen; er ordnet sie nicht einem gemeinsamen Datenereignis oder Betreiber zu.
ALTERNATIVE	Richtige Details können aus Kontomissbrauch oder anderer Informationsoffenlegung stammen, ohne einen plattformweiten Vorfall zu belegen.
GRENZE	Die Warnung nennt keine österreichische Zahl gestohlener Buchungen oder erfolgreicher Zahlungsumleitungen.
REAKTION	Bestätigen Sie unerwartete Zahlungsaufforderungen unabhängig und bieten Sie Gästen einen bekannten Weg zur Prüfung des tatsächlichen Zahlungsablaufs.

Fazit

Bestätigen Sie die verlangte Zahlung über einen bekannten unabhängigen Weg.

Beherbergungsteams sollten sich auf Gäste vorbereiten, die bereits echte Buchungsdetails in der Nachricht sehen. Der allgemeine Rat, nach Schreibfehlern zu suchen, genügt nicht. Entscheidend ist, ob die verlangte Zahlung zum vereinbarten Ablauf dieser Buchung passt.

J

FALL J

Eine Geschäftskorrespondenz erhält eine unbefugte Zahlungsänderung (O10)

Branchenübergreifende Geschäftsabläufe

Amtliche Warnung

BEOBACHTUNG	Der BEC-Hinweis von CERT.at vom 26. August berichtet vermehrte Versuche gegen österreichische Organisationen. [S12]
CHRONOLOGIE	Die Szenarien umfassen Vorgesetzten-Imitation, geänderte Lieferantenanweisungen, Missbrauch bestehender E-Mail-Austausche und Anfragen nach Mitarbeiterdaten.
BELEGT	Die Quelle beschreibt eine Gruppe von Täuschungsszenarien, keinen einheitlichen technischen Angriff.
ALTERNATIVE	Einige Fälle können ein echtes Postfach nutzen; andere kommen mit Imitation ohne Zugriff auf die imitierte Organisation aus.
GRENZE	Eine verdächtige Rechnung allein belegt nicht, auf welches Postfach gegebenenfalls zugegriffen wurde.
REAKTION	Bestätigen Sie geänderte Anweisungen über einen bereits bekannten Kontakt und trennen Sie Zahlungsfreigabe und Ausführung.

Fazit

Bestätigen Sie geänderte Anweisungen unabhängig und trennen Sie Zahlungsfreigabe und Ausführung.

Die zweite Freigabe sollte unabhängige Belege prüfen, statt einen Kollegen dieselbe überzeugende E-Mail lesen zu lassen. Ist eine Rechnung echt, aber ihre Bankverbindung geändert, braucht die Finanzabteilung eine vertrauenswürdige Lieferantenbestätigung. Die Sicherheit benötigt die zugehörigen E-Mail-Belege.

5.5 Geschäftliche und gehostete Dienstleistervorfälle im späteren Jahresverlauf

K

FALL K

Scheinbare Onlinearbeit wird zur Folge von Einzahlungen (O11)

Verbraucherbetrug

Amtliche Warnung

BEOBACHTUNG	Die Warnung des Bundeskriminalamts vom 29. Oktober beschreibt Stellenangebote in sozialen Medien mit anschließenden Aufgaben und Zahlungsforderungen. [S20]
CHRONOLOGIE	Der Kontakt läuft über Nachrichtendienste. Auf kleine erste Auszahlungen folgen größere Einzahlungen und angeblich höherwertige oder zur Fehlerbehebung nötige Aufgaben.
BELEGT	Die Polizei beschreibt österreichische Schäden ungefähr im niedrigen einstelligen Millionenbereich.
ALTERNATIVE	Eine erste Zahlung an Teilnehmende belegt keinen seriösen Arbeitgeber und garantiert keine spätere Auszahlung.
GRENZE	Die Warnung nennt weder eine genaue nationale Opferzahl noch eine Verbindung zu den Untergrundverkäufern dieses Berichts.
REAKTION	Lehnen Sie Zahlungen für Arbeit oder zur Freigabe von Verdienst ab. Sichern Sie das Gespräch und kontaktieren Sie den Zahlungsanbieter bei vermutetem Schaden umgehend.

Fazit

Stoppen Sie weitere Einzahlungen und kontaktieren Sie bei Betrugsverdacht den Zahlungsanbieter.

Für eine Organisation kann Kundenschutz statt eines internen Einbruchs relevant sein. Banken und kundennahe Dienste sollten Erzählungen mit wiederholten Einzahlungen erkennen und einen sicheren Eskalationsweg anbieten. Eine App oder Gruppe mit vielen Teilnehmenden klärt ihre Seriosität nicht.

L

FALL L

Ein Datenvorfall bei einer Projektorganisation lässt Betriebsfähigkeit als eigene Frage offen (O12)

Projektbasierte Wirtschaft

Pressebericht

BEOBACHTUNG	

Presseberichte aus dem Herbst beschreiben einen vom Unternehmen bestätigten Cybervorfall bei einer österreichischen Organisation mit Projektbetrieb. [S27]

CHRONOLOGIE	Der Vorfall ereignete sich im Herbst 2026; spätere Novemberaktualisierungen begründen keinen zweiten Vorfall.
BELEGT	Die Unternehmensdarstellung unterscheidet das Ereignis im Informationssystem von der fortgesetzten Projektarbeit.
ALTERNATIVE	Die Darstellung des Urhebers der Behauptung kann über die Bestätigung der Organisation hinausgehen.
GRENZE	Der Bericht behandelt die Identität der erpressenden Gruppe nicht als unabhängig festgestellten Betreiber.
REAKTION	Bewerten Sie betroffene Geschäftsunterlagen und Wiederherstellung. Prüfen Sie Projektbetrieb und kritische Dienstleisterzugänge gesondert.

Fazit

Prüfen Sie Datensätze und Projektbetrieb mit getrennten Verantwortlichen.

Der Dienstverantwortliche sollte bei Aussagen zur Betriebsfähigkeit nach den getesteten Funktionen fragen. Ein Projekt kann weiterlaufen, während Verwaltungsdaten, Korrespondenz oder eine Dienstleisterbeziehung noch untersucht werden. Wiederherstellung und Datenschutzbewertung brauchen getrennte Abschlussnachweise.

M

FALL M

Zugriff auf Hosting-Infrastruktur verlangt kundenspezifische Eingrenzung (O13)

Anbietermitteilung

Software- und Hosting-Dienstleister

BEOBACHTUNG	Ein kommerzieller Software- und Hosting-Dienstleister berichtete im November 2026 unbefugten Zugriff auf einen Teil seiner gehosteten Infrastruktur. [S28]
CHRONOLOGIE	Nach seiner Darstellung wurden Behörden und Kunden nach der Erkennung umgehend informiert; Mitte November folgten Aktualisierungen.
BELEGT	Der Dienstleister sagt, seine Onlinesysteme seien verfügbar geblieben. Er berichtet keine bekannten Veränderungen, Löschungen oder Verschlüsselungen.
ALTERNATIVE	Fortgesetzter Betrieb und keine bekannten Veränderungen belegen nicht, dass keine Daten eingesehen wurden.
GRENZE	

Laut Mitteilung blieben Akteur und Motiv unbekannt, während der Dienstleister seinen Dienstumfang von unverbundenen Softwarehinweisen und gesonderten Kundenbuchungsabläufen abgrenzt.

REAKTION	Verlangen Sie eine eingegrenzte Dienstleisterbewertung und erhalten Sie die Kundenschutzbeobachtung aufrecht, ohne eine Verbindung zu unverbundenen Hinweisen oder Betrug zu erfinden.

Fazit

Verlangen Sie kundenspezifischen Umfang, ohne eine Verbindung zu unabhängigen Hinweisen oder Betrug zu erfinden.

Die Aussage eines Dienstleisters über die von ihm verarbeiteten Datenarten ist wichtig. Branchennähe allein rechtfertigt keine Behauptung offengelegter Kundendatensätze. Jeder Kunde sollte seine tatsächlichen Datenkategorien und Funktionen prüfen, bevor er nachgelagerte Warnungen ausgibt.

FALL N

N ■ Mitarbeiterkontakte über eine extern betriebene Website eingesehen (O14)

Öffentliche Verwaltung

Pressebericht

BEOBACHTUNG	Presseberichte vom November gaben die Mitteilung einer österreichischen öffentlichen Stelle zu unbefugt eingesehenen dienstlichen Mitarbeiterkontakten wieder. [S29]
CHRONOLOGIE	Die wiedergegebene Darstellung beschreibt einen kurzen Zugriff im November, der rasch erkannt und unterbunden wurde.
BELEGT	Die beschriebene Website wurde extern betrieben. Die genannten Datensätze betrafen Mitarbeiternamen und dienstliche Kontakte, ohne festgestellten Bürgerdatenbezug.
ALTERNATIVE	Kurz eingesehene dienstliche Kontakte belegen weder ein Kopieren noch den Zugangsweg.
GRENZE	Nach der Darstellung waren personenbezogene Bürgerdaten nicht betroffen; ein Akteur wird nicht genannt. Die Originalaussendung war für diese Prüfung nicht verfügbar.
REAKTION	Prüfen Sie beim Dienstleister gespeicherte Verzeichnisse und Dienstberechtigungen. Bereiten Sie Beschäftigte auf gezielte Imitation mit dienstlichen Kontaktdaten vor.

Fazit

Prüfen Sie Dienstberechtigungen und bereiten Sie sich auf Mitarbeiter-Imitation vor.

Die verfügbare Darstellung nennt keinen Betreiber und trägt keine Zuschreibung. Die bestätigten dienstlichen Kontaktkategorien rechtfertigen eine gezielte Warnung vor Identitätstäuschung, während die technische Untersuchung und Zuschreibung getrennt bleiben.

O

FALL O

Eine Verwaltungsaktualisierung erweitert die genannten Datenkategorien (O15)

Öffentliche Verwaltung

Pressebericht

BEOBACHTUNG	Presseberichte vom November griffen einen früheren Vorfall von 2026 bei einer Stelle der öffentlichen Verwaltung auf und beschrieben einen erweiterten Datenumfang. [S55]
CHRONOLOGIE	Erste Feststellungen betrafen engere Datenkategorien, bevor später im Jahr ein breiterer Umfang erkennbar wurde.
BELEGT	Nach der berichteten Darstellung wurden Betroffene persönlich informiert sowie Polizei und Datenschutzbehörde verständigt.
ALTERNATIVE	Eine spätere Umfangsänderung belegt weder einen zweiten unabhängigen Einbruch noch das Zugriffsdatum jedes Datensatzes.
GRENZE	Eine vollständige Originalmitteilung war für diese Prüfung nicht verfügbar.
REAKTION	Aktualisieren Sie betroffene Kategorien, Risiko und Kommunikation mit der Beleglage. Bewahren Sie dabei Vorfallchronologie und Begründung der Benachrichtigung.

Fazit

Aktualisieren Sie betroffene Datenkategorien und Kommunikationsentscheidungen mit der Beleglage.

Die Lehre betrifft verändertes Wissen. Eine frühe Mitteilung beschreibt den damaligen Kenntnisstand. Eine spätere Bewertung kann die Datenschutzentscheidung verändern, ohne zu zeigen, dass die frühere Mitteilung nach damaligem Kenntnisstand falsch war.

P

FALL P

Auf ein Dienstleisterereignis im Beherbergungsbereich folgt Zahlungstäuschung gegen Gäste (O16)

Gastgewerbe

Pressebericht

BEOBACHTUNG	Presseberichte vom November zitierten die Mitteilung eines Beherbergungsbetreibers zu über einen externen Dienstleister offengelegten Gästeinformationen. [S56]
CHRONOLOGIE	

Die Berichte beschreiben laufende Untersuchungen, ohne ein genaues erstes Zugriffsdatum festzustellen.

BELEGT	Die Unternehmensdarstellung nennt Namen, Kontaktdaten, gebuchte Objekte und Aufenthaltsdaten. Zahlungsdaten seien unbetroffen und Buchungen weiter gültig.
ALTERNATIVE	Das Dienstleisterereignis belegt kein Eindringen in eigene Systeme des Betreibers oder bei allen seinen Anbietern.
GRENZE	Die Berichte beschreiben täuschende Nachrichten mit Anfragen nach Bank- oder Kartendaten. Der genaue Zugangsweg wird noch untersucht.
REAKTION	Bieten Sie Gästen einen vertrauenswürdigen Prüfweg. Erklären Sie, dass echte Buchungsdetails eine unerwartete Anfrage nach Zahlungsdaten nicht legitimieren.

Fazit

Bieten Sie Gästen einen vertrauenswürdigen Prüfweg. Bewahren Sie den genannten Umfang gültiger Buchungen und unbetroffener Zahlungsdaten.

Kundenschutz kann nötig sein, während der technische Weg offenbleibt. Beruhigen Sie Gäste zu Buchungen nur innerhalb des vom Unternehmen genannten Umfangs. Trennen Sie diese Aussage von der Untersuchung offengelegter Informationen und nachfolgender Nachrichten.

Q

FALL Q

Ein Betreiber meldet zwei getrennte Dienstleistervorfälle (017)

Beherbergungsdienste

Betreibermitteilung

BEOBACHTUNG	Eine Mitteilung eines Beherbergungsbetreibers aus dem Herbst 2026 beschreibt getrennte Vorfälle beim Buchungssoftwareanbieter und beim Dienstleister für Gästekommunikation. [S57]
CHRONOLOGIE	Die beiden Dienstleisterereignisse lagen im Herbst 2026 mehrere Wochen auseinander; das spätere Ereignis betraf einen Datenabruf auf Kontoebene.
BELEGT	Laut Mitteilung waren Gäste- und Buchungsinformationen betroffen. Beide Vorfälle wurden der Datenschutzbehörde gemeldet. Auch buchungsbezogene betrügerische Nachrichten an Gäste werden berichtet.
ALTERNATIVE	Zwei Dienstleistermitteilungen belegen weder einen Einbruch in eigene Betreibersysteme noch einen gemeinsamen Akteur hinter beiden Ereignissen.
GRENZE	Die spätere Dienstleisterdarstellung nennt eine vierstellige Zahl von Buchungen und Gästedatensätzen als möglicherweise betroffen. Der tatsächliche Abrufumfang ist ungeklärt; es sind keine bestätigten eindeutigen Personen.

REAKTION

Führen Sie getrennte Dienstleisterchronologien, prüfen Sie die tatsächlichen Datenkategorien des Betreibers und warnen Sie Gäste über einen bekannten Kanal. Erhalten Sie die genannten Dienstleisterausschlüsse.

Fazit

Halten Sie Dienstleisterereignisse getrennt und unterscheiden Sie mögliche Buchungs- oder Gästedatensatzzahlen von bestätigten eindeutigen Personen.

Die aktuellen Dienstleisterdarstellungen schließen Zahlungs- oder Kartendaten, Identitätsdokumente, Zugangsdaten und Zutrittscodes aus. Diese Ausschlüsse widerlegen den berichteten Gästedatenzugriff nicht. Eine möglicherweise betroffene Buchungszahl darf nicht zur bestätigten Gesamtzahl betroffener Personen werden.

5.6 Weitere amtliche Hinweise und ausdrückliche Ausschlüsse

Die folgenden Veröffentlichungen erweitern das Bild der erforderlichen Reaktionen, ohne zusätzliche bestätigte Organisationseinbrüche zu begründen.

Veröffentlichung	In der Quelle gelesenes Thema	Einordnung
15. Januar	Gefälschte Steuerzahlungserinnerungen und amtlich wirkende Mitteilungen [S23]	Kontext einer Betrugskampagne mit Behördenbezug
27. Februar	Steuerbezogene Nachrichten, Anrufe und falsche Dienstwebsites [S24]	Kontext kanalübergreifender Imitation
12. März	Internationale Maßnahmen gegen einen Proxy-Dienst [S22]	Strafverfolgungsreaktion; die frühere österreichische Untersuchungspopulation ist historisch
12. August	Präventionshinweis zu Romance Scam [S51]	Thematischer Präventionshinweis; keine neue Zahl von Datenvorfällen abgeleitet
9. Oktober	Phishing-Prävention, Zahlen 2025–2026 und OeNB-/RTR-Aussagen [S16]	Kontext; die Frühjahrskampagne zur Verlängerung überschneidet sich mit Fall D
12. November	Operation TorNado [S21]	Rückblickende Reaktion; österreichische Maßnahmen erfolgten im Februar
20. November	Saisonale Warnung vor Online-Einkaufsbetrug [S52]	Präventionswarnung ohne Vorfallzahl
Mai 2026	Übung zur Gesundheitslogistik [S53]	Übung, von tatsächlichen Vorfallzahlen ausgeschlossen
19. Juni	Brandbedingte Glasfaserunterbrechung [S13]	Physisches Kontinuitätsereignis, von Cyberangriffszahlen ausgeschlossen

Die Januar- und Februarwarnungen des Finanzministeriums beschreiben kriminellen Missbrauch seiner Identität. Sie belegen keinen Einbruch in das Ministerium. Ein Behördenköder und ein behördlicher Datenvorfall verlangen unterschiedliche Belege und Reaktionsverantwortliche. [S23][S24]

Die Darstellung der Proxy-Operation enthält österreichische Ermittlungsergebnisse aus der Zeit vor 2026. Ihre Veröffentlichung im Berichtszeitraum macht nicht alle betroffenen Netze zu neuen Vorfällen von 2026. Dasselbe gilt für Strafverfolgungssummen über mehrere Länder oder Jahre. [S22]

5.7 Aktuelle Aktivitäten: 8.–22. November 2026

Eine aktuelle Veröffentlichung ist nicht gleichbedeutend mit einem aktuellen Einbruch. Die folgenden Unterschiede leiten die Reaktion am Ende des Berichtszeitraums; Einträge zu zurückgehaltenen Organisationen bleiben auf Monatsebene datiert, um indirekte Identifizierung zu verhindern.

Datum	Gegenstand	Was sich änderte	Angemessene Entscheidung
Herbst 2026 (Novemberaktualisierung)	Mitteilung eines Beherbergungsbetreibers [S57]	Zwei getrennte Dienstleistereignisse und eine Gästewarnung	Dienstleisterakten trennen und den echten Zahlungsablauf prüfen
November 2026	Berichte über eine Projektorganisation [S27]	Weitere Berichte über ein Herbstereignis	Datenumfang und fortgesetzten Betrieb trennen
12. November	TorNado-Veröffentlichung [S21]	Darstellung einer internationalen Operation	Historischen und weltweiten Umfang erhalten
November 2026	Aktualisierung eines gehosteten Dienstleisters [S28]	Weitere Aussage zu einem Novemberereignis in gehosteter Infrastruktur	Kundenspezifischen Umfang erfragen und genannte Ausschlüsse bewahren
18. November	Java-Sicherheitshinweis [S44]	Produkt- und plattformabhängige dringende Behebung	Zutreffende Versionen und Herstellerhinweise prüfen
18. November	NGINX und nationale Warnung [S48]	Kritische Softwarewarnung und koordinierte Reaktion	Relevante Installationen bestimmen und Behebung prüfen
18. November	Dialog im Finanzsektor [S42]	Aufsichtlicher Austausch mit Anbietern von Informations- und Kommunikationstechnologie (IKT)	Meldung und Dienstleistereskalation üben
19. November	PHP-Sicherheitshinweis [S45]	Korrekturen und konfigurationsabhängige Bedingungen	Versionen und relevante Sitzungs- oder Backend-Einstellungen prüfen
November 2026	Bericht über einen Beherbergungsdienstleister [S56]	Gästeinformationen und anschließende Warnung vor Zahlungstäuschung	Vertrauenswürdigen Kundenkontakt anbieten
November 2026	Mitteilung aus dem öffentlichen Bereich [S29]	Öffentliche Darstellung eingesehener dienstlicher Mitarbeiterkontakte	Gehostete Mitarbeiterdaten und gezielte Identitätstäuschung prüfen

Datum	Gegenstand	Was sich änderte	Angemessene Entscheidung
20. November	Einkaufsbetrugswarnung [S52]	Saisonale Präventionshinweise	Händler und Zahlungen unabhängig überprüfen
November 2026	Datenaktualisierung einer Verwaltungsstelle [S55]	Revidierter Umfang eines früheren Vorfalls 2026 und persönliche Benachrichtigungen	Datenrisiko- und Kommunikationsbewertung aktualisieren

Diese Tabelle belegt weder einen gemeinsamen Betreiber noch einen zahlenmäßigen Anstieg Ende November. Ihr Wert liegt in der Zuordnung veränderter Entscheidungen: Aktualisierung, Kundenhilfe, Dienstleisterprüfung oder Einordnung eines früheren Ereignisses.

KERNAUSSAGEN

01

Kampagne, Mitteilung und rückblickende Operation sind unterschiedliche Datensätze.

02

Übertragen Sie den bestätigten Umfang und offene Aussagen jedes Falls in die Reaktion.

03

Behandeln Sie aktuelle Meldungen als Entscheidungsänderungen, ohne Vorfälle zu vervielfachen oder unbelegte Akteure zuzuweisen.

KAPITEL 06

Hacktivismus, DDoS und Dienstverfügbarkeit

06

DIESES KAPITEL BEANTWORTET

Welche Belege trennen eine Verfügbarkeitsbehauptung von einer nachgewiesenen Dienstbeeinträchtigung?

3

unabhängige Fragen: Erreichbarkeit, Datenzugriff und Geschäftsfunktion

6.1 Eine Zielliste ist keine Auswirkungsanalyse 64
6.2 Gespeicherte Website- und Zugriffsbehauptungen 64
6.3 Eine weitergegebene Gebäudesteuerungsbehauptung behält ihren Vorbehalt 67
6.4 Behauptung und amtlich genannter Umfang 68
6.5 Zeitleiste unterschiedlicher Belegarten 69
6.6 Für politisch gerahmte Aktivitäten gilt derselbe Belegmaßstab 70
6.7 Verfügbarkeitsübung mit überprüfbarem Abschluss 70
6.8 Physische und technische Abhängigkeiten brauchen getrennte Verantwortliche 71

KAPITEL 06

Hacktivismus, DDoS und Dienstverfügbarkeit

KURZFASSUNG

Ein behaupteter Ausfall, eine unterbrochene Website und ein Vorfall in betrieblichen Systemen sind unterschiedliche Aussagen. Politische Sprache belegt keine technische Ursache. Die zitierten österreichischen Fälle zeigen auch, warum fortgesetzter Betrieb die Datengefährdung nicht klärt. Prüfen Sie die tatsächliche Kundenaufgabe, bewahren Sie die vom Anbieter genannten Grenzen und nutzen Sie einen unabhängigen Statuskanal, bevor Sie Auswirkungen oder Zuschreibung beschreiben.

6.1 Eine Zielliste ist keine Auswirkungsanalyse

Ein Beitrag mit einem Dienstnamen kann das erklärte Interesse oder die Behauptung eines Akteurs belegen. Er belegt weder vollständige Dauer, betroffene Nutzer, Geschäftsfolgen noch verantwortlichen Betreiber. Ein Screenshot zeigt ohne unabhängige Bestätigung, was der Verfasser zeigen wollte. [S1]

Erreichbarkeit kann je nach Dienst, Nutzer, Netzwerk und Zeitpunkt variieren. Eine antwortende Startseite belegt keine funktionierende Anmeldung, Buchung oder Zahlung. Eine fehlgeschlagene Prüfung allein belegt weder böswilligen Datenverkehr noch einen österreichweiten Ausfall.

Das Vorfallteam sollte die Aussagen im Arbeitsakt trennen. Halten Sie fest, welche Funktion ausfiel, wie das festgestellt wurde und welcher Zeitraum belegt ist. Prüfen Sie, ob Dienstverantwortlichenbelege die kriminelle Behauptung stützen. Lassen Sie ungeklärte Ursachen offen.

Bei wesentlichen Abläufen ist ein hilfreicher Maßstab, ob Kunden ihre Aufgabe normal oder über den Ersatzweg abschließen können. Sicherheitstelemetrie kann eine Unterbrechung erklären. Der Dienstverantwortliche muss aber feststellen, ob Menschen die benötigte Leistung erhalten konnten.

6.2 Gespeicherte Website- und Zugriffsbehauptungen

Ein Beitrag vom 26. März aus einer als 313 Team bezeichneten Quelle behauptet die Störung einer Website des öffentlichen Bereichs und kündigt eine Stunde Dauer an. Die Dauer ist ein Plan im Beitrag, kein gemessener Ausfall. Mit der Karte liegt keine fallspezifische amtliche Bestätigung vor. [S1]

Belegkarte B16 — 26. März 2026

313 Team | Chat-Nachricht | Telegram | Arabisch und Englisch

ORIGINAL

The attack is scheduled to last for one hour.

ÜBERSETZUNG

Der Angriff soll eine Stunde dauern.

Belegt
Eine 313 Team zugeordnete Nachricht kündigt eine Aktion gegen eine öffentliche Website mit einer geplanten Dauer von einer Stunde an.

Nicht festgestellt
Ein gemessener einstündiger Ausfall, offizielle Bestätigung, Datenzugriff oder bestätigte Auswirkung auf öffentliche Aufgaben.

Beiträge vom 8. und 17. Mai aus einer als NoName057(16) bezeichneten Quelle behaupten Aktivitäten gegen verkehrsbezogene, Handels-, öffentliche und energiewirtschaftliche Websites. Einige Einträge beschreiben geografische Zugriffsbeschränkungen. Das belegt weder eine erfolgreiche Dienstverweigerung noch Auswirkungen auf berechtigte Nutzer. [S1]

Belegkarte B13 — 8. Mai 2026

NoName057(16) | Chat-Nachricht | Telegram | Englisch

ORIGINAL

"Traveling" through the Austrian internet infrastructure

ÜBERSETZUNG

„Reisen" durch die österreichische Internetinfrastruktur

Belegt
Eine NoName057(16) zugeordnete Nachricht behauptet Angriffe auf verkehrsbezogene, Handels- und öffentliche Websites.

Nicht festgestellt
Gemessene Erreichbarkeit, Dauer, Dienstunterbrechung, Datenzugriff oder Auswirkungen auf den Verkehrsbetrieb.

Belegkarte B14 — 17. Mai 2026

NoName057(16) | Chat-Nachricht | Telegram | Englisch

ORIGINAL

(closed by geolocation)

ÜBERSETZUNG

(durch Geolokalisierung gesperrt)

Belegt
Eine spätere NoName057(16) zugeordnete Nachricht nennt energiebezogene und weitere Websites. Manche beschreibt sie als geografisch gesperrt.

Nicht festgestellt
Erfolgreiche Dienstblockade, Datenzugriff, Unterbrechung der Energieversorgung oder Zugang zu betrieblichen Steuerungssystemen.

Dieselbe bezeichnete Veröffentlichungsquelle enthält außerdem eine Energiebehauptung vom 8. Mai, die im Text Darkstorm zugeschrieben wird. Das ist eine Weitergabe. Es ist weder ein unabhängig vorliegender Darkstorm-Originalbeitrag noch eine amtliche Dienstdarstellung oder ein Beleg gemeinsamer Betreiberkontrolle. [S1]

Belegkarte B15 — 8. Mai 2026

[Alias der Weitergabe zurückgehalten] | Chat-Weitergabe | Telegram | Englisch

ORIGINAL

#DARKSTORM

ÜBERSETZUNG

#DARKSTORM

Belegt
Eine vorliegende Weiterverbreitung ordnet Darkstorm eine Behauptung über eine energiebezogene Website zu. Sie ist kein ursprünglicher Darkstorm-Beitrag.

Nicht festgestellt
Bestätigter Ausfall, betriebliche Auswirkungen, ursprüngliche Urheberschaft, Zusammenarbeit oder gemeinsame Steuerung.

Ein Beitrag vom Mai aus derselben als NoName057(16) bezeichneten Quelle behauptet Zugriff auf die Videoüberwachung eines Einzelhandelsstandorts und beschreibt eine Aufnahme. Aufnahme und Zugriff wurden nicht unabhängig authentifiziert. Die Behauptung belegt weder ein Eindringen in ein übergeordnetes Unternehmensnetz noch eine dauerhafte Verbindung oder offengelegte Kundendatensätze. [S1]

Belegkarte B17 — Mai 2026

NoName057(16) | Chat-Nachricht | Telegram | Englisch

ORIGINAL

We have gained access to the internal video surveillance system

ÜBERSETZUNG

Wir haben Zugang zum internen Videoüberwachungssystem erhalten

Belegt
Eine NoName057(16) zugeordnete Nachricht behauptet Zugang zur Videoüberwachung einer Handelsfiliale.

Nicht festgestellt
Echtheit eines Videos, aktueller Zugang, Standort, Zugangsweg, Datenoffenlegung oder Zugang zu einem übergeordneten Unternehmensnetz.

Die folgende Gegenüberstellung vergleicht Behauptungen mit den dafür vorliegenden Belegen. Eine fehlende amtliche Darstellung begrenzt diese Beleglage; sie ist kein amtliches Dementi.

Punkt	Aussage des Akteurs oder der Weitergabe	Vorliegende amtliche Belege	Schlussfolgerung des Berichts
Dauer	B16 kündigt eine Stunde an [S1]	Keine fallspezifische amtliche Dauer gespeichert	Geplante Dauer ist keine gemessene Ausfallzeit
Verfügbarkeit	B13 und B14 listen Websites oder geografische Beschränkungen [S1]	Keine fallspezifische Bestätigung der Dienstbeeinträchtigung gespeichert	Erreichbarkeit und Nutzerauswirkungen bleiben unbelegt
Energie	B15 gibt eine Darkstorm zugeschriebene Websitebehauptung weiter [S1]	Keine Bestätigung eines energiebetrieblichen Vorfalls gespeichert	Website-Zielauswahl belegt keinen Vorfall im Energieprozess
Überwachung	B17 beschreibt Zugriff auf Einzelhandelskameras [S1]	Kein unabhängig authentifizierter Zugriff oder Aufnahme gespeichert	Weitergehender Netzzugriff und Dauerhaftigkeit bleiben unbelegt

Die entsprechende Abwehraufgabe ist die Prüfung des tatsächlichen Dienstes. Fragen Sie den Websiteverantwortlichen nach Funktion und Zeitraum. Bei einer Kamerabehauptung sollte der berechtigte Eigentümer Gerät, Konto, Herkunft der Aufnahme und Zugriffshistorie feststellen.

Behandeln Sie eine spätere Softwarewarnung oder einen unverbundenen amtlichen Vorfall weder als Bestätigung noch als Widerlegung. Aussage, Dienst und Zeitraum müssen zusammenpassen, bevor zwei Quellen denselben Fall stützen können.

6.3 Eine weitergegebene Gebäudesteuerungsbehauptung behält ihren Vorbehalt

Eine gesonderte Übersicht vom Mai aus einer als NoHeartz bezeichneten Quelle gibt eine NoName057(16) zugeschriebene Zugriffsbehauptung zu einer Gebäudesteuerung weiter. Die Übersicht sagt ausdrücklich, dass der Zugriff auf industrielle Steuerungssysteme (ICS) nicht amtlich bestätigt ist. Dieser Vorbehalt gehört in jede Zusammenfassung der Behauptung. [S1]

Belegkarte B18 Mai 2026

[Alias der Weitergabe zurückgehalten] Chat-Weitergabe Telegram Russisch

ORIGINAL

⚠ ICS-доступ официально не подтверждён.

ÜBERSETZUNG

Der ICS-Zugang ist nicht offiziell bestätigt.

Belegt
Eine Weiterverbreitung beschreibt einen angeblichen Vorfall an einer vernetzten Gebäudesteuerung in Österreich. Sie erklärt ausdrücklich, dass ein ICS-Zugang nicht offiziell bestätigt ist.

Nicht festgestellt
Bestätigter Standort, aktuelle Kontrolle, geänderte Einstellungen, unsicherer Prozess, Zugriff auf Herstellersysteme oder ursprüngliche Urheberschaft.

Das gespeicherte Material authentifiziert Standort, Land, Steuerung oder Aufnahme nicht unabhängig. Es belegt weder eine abgeschlossene Einstellungsänderung noch einen unsicheren physischen Prozess. Auch ein Eindringen in die Infrastruktur des Herstellers ist nicht belegt.

Die Reaktion hängt von einem berechtigten Abgleich ab. Der tatsächliche Anlagenverantwortliche sollte Zugriffsprotokolle, Fernwartungsvereinbarungen und unabhängige Zustandsinformationen prüfen. Der Bericht empfiehlt weder das Testen einer unbekannten Steuerung noch Kontakt mit dem Urheber der Behauptung.

Eine Gebäudesteuerungsbehauptung und eine Behauptung zu einer Energieunternehmenswebsite betreffen unterschiedliche technische Populationen. Ihre Zusammenfassung als ein Betriebstechnikvorfall würde die zentrale Unsicherheit beider Behauptungen beseitigen.

6.4 Behauptung und amtlich genannter Umfang

Der Fall der Postfachdokumente zeigt, wie breitere Werbung und eine enge offizielle Darstellung nebeneinander bestehen können. Der angemessene Vergleich erhält beide Aussagen, ohne Verhältniszahl oder Annahme, dass eine die andere aufhebt. [S26]

Punkt	Kriminelle Darstellung	Offizielle Darstellung	Schlussfolgerung des Berichts
Material	Weitergehende erpressungsbezogene Behauptungen	Sprecher bestätigt ältere Dokumente aus einem Postfach	Dokumentenoffenlegung ist innerhalb dieser Darstellung gestützt
Systeme	Werbung kann ein größeres Ereignis nahelegen	Sprecher verneint nach damaligem Wissen einen weitergehenden Angriff auf betriebliche Systeme	Weitergehender Systemzugriff bleibt hier unbelegt
Zeit	Die Veröffentlichung ist ein sichtbares Behauptungsereignis	Bestätigtes Material stammt aus 2025	Beides belegt keinen frischen Einbruch für jeden veröffentlichten Gegenstand
Auswirkungen	Eine Behauptung kann umfangreiche Störung nahelegen	Quelle verneint Kernbetriebs- und Kundenumfang	Relevante Funktion gesondert überprüfen
Akteur	Behauptungsbezeichnung und Werbeidentität	Kein unabhängig festgestellter Betreiber in diesem Bericht	Behauptung erhalten, ohne Verantwortung zuzuweisen

Die Gegenüberstellung urteilt nicht über die Ehrlichkeit des Urhebers der Behauptung. Sie soll verhindern, dass ein Serviceteam die falsche Frage beantwortet. Dokumentenuntersuchung und betriebliche Absicherung können beide erforderlich sein.

Der Herbstfall einer Projektorganisation verlangt ähnliche Vorsicht. Die Unternehmensdarstellung betrifft ein Informationssystemereignis bei fortgesetzter Projektarbeit. Das ist die vom Unternehmen genannte betriebliche Grenze, keine allgemeine Zusicherung für jede verbundene Organisation. [S27]

6.5 Zeitleiste unterschiedlicher Belegarten

Die Zeitleiste enthält datierte amtliche Hinweise, Kampagnenwarnungen sowie gespeicherte Akteurs- und Weitergabenachrichten. Mitteilungen zu zurückgehaltenen Organisationen verwenden in Kapitel 5 Jahres-, Saison- oder Monatsangaben, um indirekte Identifizierung zu verhindern. Die Abfolge deutet keine gemeinsame Kampagne an.

26. März 2026 — **Als 313 Team bezeichnete Quelle**
Behauptet Websitestörung und kündigt eine Stunde geplante Dauer an. [S1]

8. Mai 2026 — **Als NoName057(16) bezeichnete Quelle**
Veröffentlicht Websitebehauptungen; Dienstbeeinträchtigung nicht unabhängig belegt. [S1]

8. Mai 2026 — **Dieselbe bezeichnete Veröffentlichungsquelle**
Gibt eine Darkstorm zugeschriebene Energie-Websitebehauptung weiter. [S1]

17. Mai 2026 — **Als NoName057(16) bezeichnete Quelle**
Veröffentlicht weitere Websitebehauptungen, darunter geografische Zugriffsbeschreibungen. [S1]

26. Mai 2026	**CERT.at** Die Quelle verbindet eine Bewerbungsköderkampagne mit bestätigten österreichischen Fällen. [S9]
19. Juni 2026	**CERT.at** Brandbedingte Glasfaserunterbrechung; physisches Kontinuitätsereignis. [S13]
24. Juli 2026	**CERT.at** Warnung vor Phishing über echte österreichische Geschäftskonten. [S10]
26. Aug. 2026	**CERT.at** Vermehrte BEC-Versuche gegen österreichische Organisationen. [S12]
9. Okt. 2026	**Bundeskriminalamt, OeNB und RTR** Phishing-Präventionsmitteilung mit Fallkontext 2025–2026 und SMS-Absenderkennungsregeln. [S16]
29. Okt. 2026	**Bundeskriminalamt** Warnung vor Aufgaben- und Stellen-Einzahlungsbetrug über soziale Medien. [S20]
18. Nov. 2026	**CERT.at und BMI** Dringender Java-Hinweis und nationale Koordination zur NGINX-Sicherheitswarnung. [S44][S48]
19. Nov. 2026	**CERT.at** Kritische PHP-Sicherheitskorrekturen und Konfigurationsbedingungen. [S45]

Die Zeilen unterscheiden Erkennung, Akteursaussagen, Weitergaben, Kampagnenwarnungen und spätere Aktualisierungen. Sie sind keine gleichartigen Beobachtungen eines Vorfallbeginns. Die Brandzeile liegt ausdrücklich außerhalb der Cyberangriffszahlen.

6.6 Für politisch gerahmte Aktivitäten gilt derselbe Belegmaßstab

Ein Akteur kann seine Handlungen als Unterstützung eines politischen Anliegens darstellen. Diese Selbstbeschreibung belegt Rhetorik, keine bestätigte Staatsbeziehung, Nationalität oder das Motiv eines anderen Vorfalls. Der Bericht lässt Beleidigungen aus und verstärkt keine ideologischen Parolen.

Wahlnähe oder die Bedeutung einer öffentlichen Stelle belegen für sich keine Einflussoperation. Aussagen über Wahlauswirkungen bräuchten gesonderte Belege. Eine solche Schlussfolgerung wird hier nicht gezogen.

Sicherheitsteams können die Originalnachricht intern sichern und öffentlich betriebliche Fakten kommunizieren. Eine hilfreiche Aktualisierung nennt betroffene Funktion, verfügbare Alternative, bestätigte Datenfolgen und nächsten Aktualisierungszeitpunkt. Dafür ist keine politische Interpretation erforderlich.

Legen Sie denselben Maßstab an Behauptungen an, die sich auf einen Staat oder einen internationalen Konflikt berufen. Kennzeichnen Sie relevante Quellenbewertungen als solche und nennen Sie ihre Grenzen. Übernehmen Sie keinen behaupteten Anlass als eigene Erklärung der Autoren.

6.7 Verfügbarkeitsübung mit überprüfbarem Abschluss

Die folgende Übung ist eine Planungsempfehlung. Sie beschreibt keinen tatsächlichen Angriff.

Geben Sie dem Team eine unerreichbare öffentliche Website, eine umlaufende Behauptung und Unsicherheit über Datenzugriff vor. Der Dienstverantwortliche sollte ausgefallene Kundenfunktionen feststellen. Das technische Team sollte Ursachenuntersuchung und unmittelbare Dienstabsicherung unterscheiden.

Lassen Sie anschließend auch den normalen Statuskanal ausfallen. Die Kommunikation sollte über einen vorher vereinbarten unabhängigen Weg veröffentlichen. Der Kundensupport sollte zeigen, dass Menschen die Alternative ohne Links aus dem Täterbeitrag finden können.

Beenden Sie die Übung erst, wenn der Geschäftsverantwortliche die kritischen Aufgaben überprüft und die Vorfallleitung den ungeklärten Umfang dokumentiert hat. Wiederherstellung allein sollte keine gesonderte Datenzugriffs- oder Meldebewertung abschließen.

6.8 Physische und technische Abhängigkeiten brauchen getrennte Verantwortliche

Der Brückenbrandbericht ist relevant, weil er Kontinuitätsannahmen ohne feindliche Zuschreibung prüft. Der Dienstverantwortliche sollte klären, ob vermeintlich unabhängige Verbindungen dieselbe physische Route, Einrichtung oder Verwaltungsabhängigkeit teilen. [S13]

Dasselbe gilt für logische Ersatzwege. Eine alternative Website mit demselben Identitätsanbieter kann zugleich mit dem Hauptweg ausfallen. Eine nur im ausgefallenen Dienst gespeicherte Notfallkontaktliste hilft während der Störung möglicherweise nicht.

Dokumentieren Sie die Annahmen des Ersatzwegs und testen Sie diese mit dem zuständigen Anbieter. Der Abschlussnachweis sollte die funktionierende Geschäftsaufgabe unter dem angenommenen Ausfall zeigen. Ein zweiter Vertrag oder ein ungeprüftes Diagramm genügt nicht.

KERNAUSSAGEN

01

Prüfen Sie Dienstfunktionen, Datenzugriff und Zuschreibung unabhängig.

02

Nutzen Sie einen unabhängigen Statuskanal und bewahren Sie die betrieblichen Grenzen der Quelle.

03

Üben Sie physische und logische Abhängigkeiten, ohne Ausfälle zu Angriffen umzudeuten.

KAPITEL 07

Bedrohungsakteure und belegte Beziehungen

07

DIESES KAPITEL BEANTWORTET

Welche akteursbezogenen Schlussfolgerungen tragen Einträge und amtliche Berichte?

61

österreichische Ransomware-Einträge im angefragten Zeitraum; kriminelle Behauptungen

7.1 Erpressungsbezeichnungen beschreiben den Eintragsbestand 73
7.2 Regionale Nachbarn liefern Eintragskontext 74
7.3 Eine Zugangsbeziehung braucht eine quellenspezifische Verbindung 76
7.4 Staatlich verbundene Aktivität: die Behördenbewertung erhalten 80
7.5 Personas und Weitergaben bleiben getrennt 80
7.6 Administrationszugänge von Dienstleistern verdienen frühe Aufmerksamkeit 80
7.7 Aktuelle Aktualisierungsbereitschaft: Produkt, Version und Konfiguration abgleichen 81
7.8 Hacktivistische Bezeichnungen und Eintragsweitergaben 83
7.9 Was eine Akteursbewertung stärken würde 85

KAPITEL 07

Bedrohungsakteure und belegte Beziehungen

KURZFASSUNG

Ransompedia erfasst im angefragten Zeitraum 61 österreichische Einträge über 56 eindeutige Namen und 22 Bezeichnungen der behauptenden Gruppen. CERT.at beschreibt gesondert eine bewertete Zugangsbeziehung zwischen ZipLine-Akteuren und Qilin. Diese Beobachtungen haben unterschiedliche Beleggrenzen. Einträge belegen weder Verschlüsselung oder Diebstahl noch einen gemeinsamen Betreiber für jeden Fall. Nutzen Sie belegte Beziehungen für Überprüfung und Wiederherstellung. Erhalten Sie dabei die Quelle jeder Zuschreibung.

7.1 Erpressungsbezeichnungen beschreiben den Eintragsbestand

Den 61 österreichischen Einträgen stehen 38 für das gesamte Jahr 2025 gegenüber. Ein Teiljahreszeitraum steht neben einer Ganzjahressumme; das ist keine Wachstumsrate für gleiche Zeiträume. Vier Einrichtungen erscheinen mehr als einmal (3 zweimal und 1 dreimal, was fünf Wiederholungseinträge ausmacht), sodass 56 eindeutige gelistete Einrichtungsnamen verbleiben. Jeder Eintrag dokumentiert eine kriminelle Aussage, keinen unabhängig bestätigten Einbruch oder eine Zahlung. [S2]

Die führende Dreiergruppe der Bezeichnungen umfasst 28 von 61 Einträgen beziehungsweise 45,9%. Die übrigen 33 Einträge verteilen sich auf weitere Bezeichnungen. Das spricht für Vorbereitung auf mehrere Erpressungsdarstellungen statt einer auf einen Namen zugeschnittenen Reaktion. [S2]

Eintragsbezeichnung	Österreichische Einträge	Einordnung
The Gentlemen	11	Kriminelle Bezeichnung für gelistete Behauptungen
Qilin	9	Kriminelle Bezeichnung; der Zugangsweg wird nicht aus dem Namen abgeleitet
LockBit 5	8	Eintragsbezeichnung, keine bestätigte Betreiberzahl
Weitere Bezeichnungen	33	Übrige Behauptungen im Eintragsbestand
Gesamt	61	Datierte Einträge im angefragten Zeitraum

Die Fertigung umfasst 11 Einträge beziehungsweise 18,0% der österreichischen Population. Beratung und die breite globale Kategorie enthalten je sechs, Einzelhandel und Bildung je fünf. Das sind Branchenbezeichnungen der Einträge, keine nationalen Branchenvorfallraten oder unabhängig überprüften Geschäftsklassifikationen. [S2]

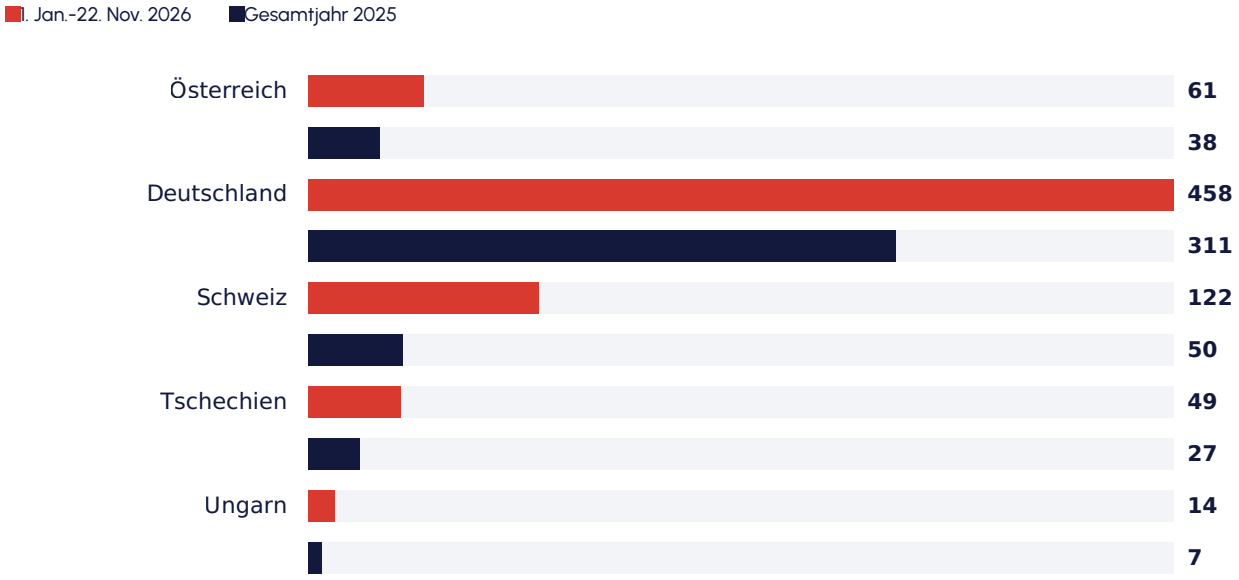
Eine Organisation kann mehrfach erscheinen oder eine komplexe Gruppenstruktur haben. Leser sollten das Eintragsvolumen nicht in eindeutige Opfer umrechnen. Auch die Länderkennzeichnung eines Feeds bestimmt nicht automatisch den betroffenen Rechtsträger.

7.2 Regionale Nachbarn liefern Eintragskontext

Deutschland, die Schweiz, Tschechien und Ungarn bieten benachbarten Wirtschafts-, Dienstleister- und Dienstkontext. Der Vergleich verwendet denselben angefragten Zeitraum und dieselbe Eintragseinheit. Er schätzt nicht die Vorfallwahrscheinlichkeit einer österreichischen Organisation. [S2]

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

Österreich hat 61 Einträge im selben Zeitraum neben unterschiedlichen regionalen Eintragspopulationen



Quelle: Brandefense Ransompedia, länderbezogene Erpressungseinträge, 1. Januar–22. November 2026 gegenüber Gesamtjahr 2025 [S2]. Ungleiche Zeiträume und unterschiedliche Länderpopulationen; keine nationale Risikorangliste.

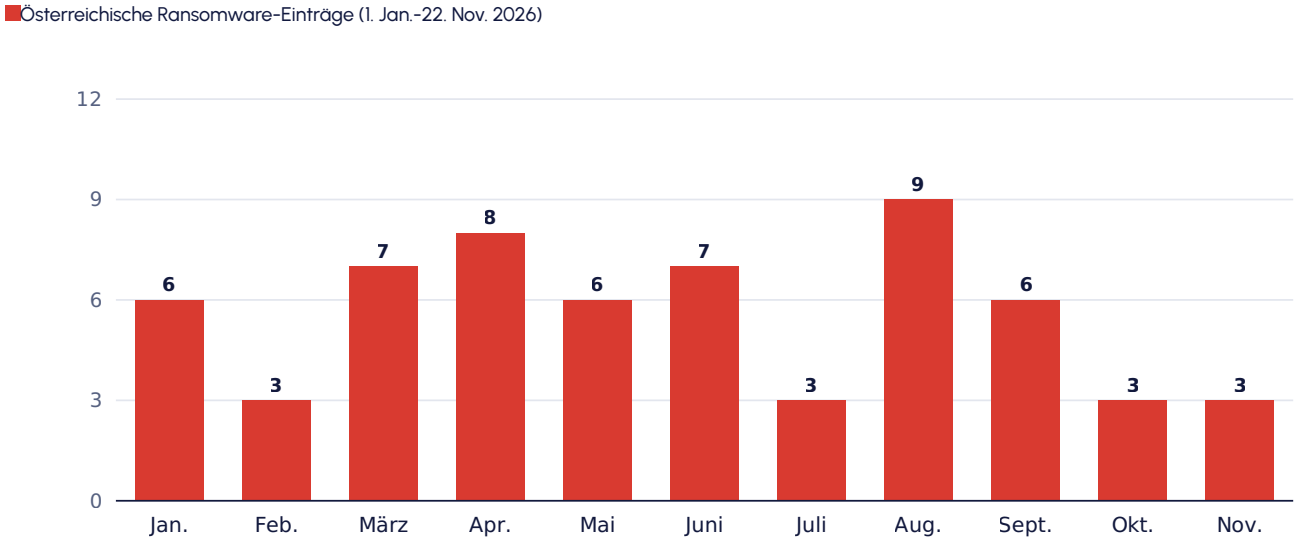
Land	Einträge	Belegte Lesart
Österreich	61	Als österreichisch gekennzeichnete Erpressungsbehauptungen in der beobachteten Population
Deutschland	458	Größere sichtbare Eintragspopulation im selben Zeitraum
Schweiz	122	Gesonderte nationale Eintragspopulation
Tschechien	49	Gesonderte nationale Eintragspopulation
Ungarn	14	Gesonderte nationale Eintragspopulation

Ländergröße, Gruppenzusammensetzung, öffentliche Bekanntgabe und Sichtbarkeit unterscheiden sich. Die Zahlen sind dafür nicht bereinigt. Kein Verhältnis zwischen ihnen wird als vergleichbare Cybersicherheitswirksamkeit oder nationales Risiko dargestellt.

Die österreichische Monatsfolge hilft bei der zeitlichen Einordnung sichtbarer Behauptungen. November ist gegenüber einem vollen Kalendermonat unvollständig, weil der Zeitraum am 22. November endet.

Monat	Österreichische Einträge	Zeitliche Grenze
Januar	6	Vollständiger Kalendermonat
Februar	3	Vollständiger Kalendermonat
März	7	Vollständiger Kalendermonat
April	8	Vollständiger Kalendermonat
Mai	6	Vollständiger Kalendermonat
Juni	7	Vollständiger Kalendermonat
Juli	3	Vollständiger Kalendermonat
August	9	Vollständiger Kalendermonat
September	6	Vollständiger Kalendermonat
Oktober	3	Vollständiger Kalendermonat
November	3	Bis 22. November
Gesamt	61	Angefragter Zeitraum

Die österreichische Eintragsfolge beschreibt Veröffentlichungen von Behauptungen; November endet am 22. November



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

Die Folge belegt weder Einbruchszeitpunkte noch einen zugrunde liegenden nationalen Angriffstrend. Ein gelistetes Ereignis kann älter als seine Veröffentlichung sein. Ein nicht gelisteter Vorfall bleibt außerhalb dieser Population. [S2]

7.3 Eine Zugangsbeziehung braucht eine quellenspezifische Verbindung

CERT.at berichtet Hinweise darauf, dass Qilin Zugänge von mit der ZipLine-Phishingkampagne verbundenen Akteuren erwirbt. Der Hinweis nennt außerdem bestätigte österreichische Fälle. Das stützt die von der Quelle beschriebene Beziehung mit ihrer verbleibenden Unsicherheit. [S9]

Diese Verbindung belegt keinen gemeinsamen Betreiber hinter jedem zugehörigen Beitrag oder Eintrag. Eine Qilin-Bezeichnung rechtfertigt auch nicht, einer einzelnen Firma ohne Fallbelege den Bewerbungsweg zuzuordnen. Das Vorfallteam braucht weiterhin die relevanten Konto- und Endgeräteunterlagen.

Eigener Beitrag Weiterverbreitung Offizielle Mitteilung Öffentliche Berichterstattung Unsere Beobachtung



Die Beziehungskarte sollte eine dreiteilige Unterscheidung vornehmen: beobachtete Beitragszuordnung, Eintragsbezeichnung aus eigenen Daten und bewertete Zugangsbeziehung einer öffentlichen Quelle. Eine Verbindung steht für die beschriftete Aussage, nicht für allgemeine Mitgliedschaft in einer gemeinsamen kriminellen Organisation.

Eine weitergehende Kette aus Identitätsdiebstahl, Zugangsweiterverkauf, Erpressung und Zahlungsbetrug bleibt ein **analytisches Modell**, solange kein konkretes gemeinsames Element die einzelnen Beobachtungen verbindet. Das Modell kann Kontrollverantwortung zuweisen helfen, ohne zur Zuschreibung eines bestimmten Vorfalls zu werden.

Qilin

Bezeichnung im beobachteten Erpressungsbestand

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

BEHAUPTETE ZIELE

Population der Einträge; Identitäten und Branchen zurückgehalten

IN ÖSTERREICH, 2026

2026
9 Österreich zugeordnete Einträge im Berichtszeitraum

Mai 2026
CERT.at berichtet Hinweise auf Zugangskäufe von ZipLine-Akteuren, S9

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 9 Österreich zugeordnete Einträge mit dieser Bezeichnung.

[S9] CERT.at nennt bestätigte österreichische ZipLine-Fälle und Hinweise, dass Qilin Erstzugang von ZipLine-Akteuren erwirbt.

UNSERE EINSCHÄTZUNG

Die Einträge begründen Vorbereitungen auf Wiederherstellung und Kommunikation, während die Mai-Bewertung von CERT.at die Prüfung entsprechender Bewerbungskorrespondenz stützt. Keines von beiden belegt einen gemeinsamen Betreiber aller Qilin-Einträge.

VERTRAUENSGRAD
Hoch für die Zahl der Einträge und die amtliche Meldung; einzelne Einträge bleiben Behauptungen

The Gentlemen

Bezeichnung im beobachteten Erpressungsbestand

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

2026
11 Österreich zugeordnete Einträge im Berichtszeitraum

BEHAUPTETE ZIELE

Population der Einträge; Identitäten und Branchen zurückgehalten

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 11 Österreich zugeordnete Einträge mit dieser Bezeichnung.

UNSERE EINSCHÄTZUNG

Die Einträge begründen Vorbereitungen auf Wiederherstellung und Kommunikation. Sie belegen weder Datendiebstahl noch Verschlüsselung, gemeinsame Betreiber, abgeschlossene Verkäufe oder finanzielle Schäden.

VERTRAUENSGRAD
Hoch für die Zahl der vorliegenden Einträge; ihre Inhalte bleiben Behauptungen

LockBit 5

Bezeichnung im beobachteten Erpressungsbestand

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

2026
8 Österreich zugeordnete Einträge im Berichtszeitraum

BEHAUPTETE ZIELE

Population der Einträge; Identitäten und Branchen zurückgehalten

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 8 Österreich zugeordnete Einträge mit dieser Bezeichnung.

UNSERE EINSCHÄTZUNG

Die Einträge begründen Vorbereitungen auf Wiederherstellung und Kommunikation. Sie belegen weder Datendiebstahl noch Verschlüsselung, gemeinsame Betreiber, abgeschlossene Verkäufe oder finanzielle Schäden.

VERTRAUENSGRAD
Hoch für die Zahl der vorliegenden Einträge; ihre Inhalte bleiben Behauptungen

ZipLine-Kampagnenakteure

Erstzugangs-Kampagne mit Bewerbungsködern (CERT.at)

Phishing-Kampagne für Erstzugang | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

26.–28. Mai 2026
CERT.at nennt bestätigte österreichische Fälle und Bewerbungsköder-Domains im DACH-Raum, S9

BEHAUPTETE ZIELE

Fertigung und exportorientierte KMU laut CERT.at; keine Opfergesamtzahl veröffentlicht

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S9] CERT.at-Update über Bewerbungskorrespondenz über Kontaktformulare, schädliche Archive und Hinweise auf Weiterverwendung von Zugängen durch Qilin.

UNSERE EINSCHÄTZUNG

CERT.at bestätigt österreichische Fälle und nennt Hinweise auf Zugangskäufe durch Qilin. Die Abwehr sollte ungewöhnliche Bewerbungskorrespondenz und Endgerätebelege prüfen, ohne jeden Bewerbungsköder einem Betreiber zuzuordnen.

VERTRAUENSGRAD
Hoch für die amtliche CERT.at-Bewertung; nationale Fallzahl nicht beziffert

7.4 Staatlich verbundene Aktivität: die Behördenbewertung erhalten

Die DSN-Mitteilung zum Bericht für 2025 beschreibt Spionage als anhaltendes Sicherheitsproblem. Dieser behördliche Kontext belegt keine staatliche Beziehung für einen Vorfall oder kriminellen Eintrag dieses Berichts. [S43]

Eine staatliche Zuschreibung braucht eigene Belege und eine Quelle. Eine öffentliche Einrichtung oder ein geopolitisches Thema können relevanter Kontext sein. Für sich identifiziert beides keinen Betreiber.

Der Bericht trennt deshalb kriminelle Behauptungsbezeichnungen, quellenbewertete Beziehungen und ungeklärte Zuschreibung. Er leitet keine Nationalitäten aus Sprache ab. Er überträgt keine Zuschreibung von einem Vorfall auf einen anderen ohne fallspezifische Belege.

Bei einem folgenreichen Fall sollte die Vorfallleitung die Zuschreibungsfrage getrennt von der Eindämmung führen. Eine Organisation kann ein missbrauchtes Konto sperren und Beschäftigte schützen, ohne die Identität des Betreibers zu klären.

7.5 Personas und Weitergaben bleiben getrennt

Eine Persona ist eine öffentlich auftretende Identität im gespeicherten Material. Sie kann geteilt, umbenannt, imitiert oder von mehreren Personen betrieben werden. Ein Plattformkonto ist daher keine bestätigte Zahl menschlicher Betreiber. [S1]

Eine Weitergabe kann die Reichweite einer Behauptung erhöhen, ohne eine zweite unabhängige Quelle zu liefern. Wiederholte Beschreibungen, gleiche Zahlen und kopierte Beispiele verlangen vorsichtige Einordnung. Sie können Werbeähnlichkeit belegen, während Dateiidentität und Übertragung ungeklärt bleiben.

Dieselbe Vorsicht gilt für die Behauptung exklusiven oder aktuellen Materials. Das bleiben Verkäuferangaben, bis die jeweilige Aussage gestützt ist. Vertrauen gehört zur konkreten Aussage, nicht zur gesamten Persona.

7.6 Administrationszugänge von Dienstleistern verdienen frühe Aufmerksamkeit

Die N-central-Warnung von CERT.at vom September beschreibt aktive Ausnutzung und eine Notfallkorrektur. Der NVD-Eintrag nennt betroffene Versionen vor 2026.3.1.14. CERT.at bezeichnet die korrigierte Veröffentlichung als 2026.3 HF4. [S7][S46]

Die unmittelbare Leserfrage lautet, ob die Organisation oder ihr Anbieter eine betroffene Version betreibt. Ein Dienstleister sollte tatsächlichen Administrationsdienst, Aktualisierungsstand und nachgelagerte Zugangsbeziehungen benennen. Der Bericht behauptet keine Zahl betroffener österreichischer Anbieter.

Ein Administrationsdienst kann Berechtigungen für viele Kundensysteme haben. Diese architektonische Möglichkeit belegt keinen Zugriff auf jeden Kunden. Verlangen Sie eine mandantenspezifische Bewertung. Erhalten Sie die Unterscheidung zwischen betroffenem Produkt, nachgewiesener Nutzung und nachgelagerten Auswirkungen.

Für die Betriebsfähigkeit sollte der Kunde wissen, wie privilegierter Dienstleisterzugang bei fortgesetzter wesentlicher Administration ausgesetzt werden kann. Die Übung braucht einen Wiederherstellungs- und erneuten Freigabeweg. Eine Sperre ohne brauchbare Alternative kann ein weiteres Dienstproblem erzeugen.

7.7 Aktuelle Aktualisierungsbereitschaft: Produkt, Version und Konfiguration abgleichen

Die Novemberhinweise begründen eine rasche Bestandsprüfung mit ihren jeweiligen Bedingungen. Sie zählen keine erfolgreichen Ausnutzungen in Österreich. Alle fünf zitierten CVE-Einträge wurden am 27. November 2026 in der NVD neben den zitierten Sicherheitshinweisen überprüft. [S7][S44][S45][S46][S47]

Eintrag	NVD-Status (27. Nov.)	Relevanter betroffener Umfang	Korrigierte Versionen oder Maßnahme
CVE-2026-114938	Analysiert; CVSS 3.1 8,1 Hoch (aktualisiert 24. Nov.)	Bestimmte Oracle-Java- und zugehörige Distributionsversionen; die nachgewiesenen Prozessorbedingungen sind relevant	Korrigierte Oracle-Versionen stehen unten; passenden Hinweis des Distributors prüfen
CVE-2026-129289	Analyse ausstehend; CNA CVSS 4.0 9,2 Kritisch	Relevante PHP-Zweige vor den genannten Korrekturen; der beschriebene Angriff auf den FastCGI Process Manager (FPM) hängt von dauerhaften Backend-Verbindungen und einem Pfad mit ungelesenem Anfrageinhalt ab	8.2.36, 8.3.37, 8.4.28, 8.5.13; 8.6.0 enthält Korrekturen
CVE-2026-115560	Analyse ausstehend; CNA CVSS 4.0 9,2 Kritisch	Relevante PHP-Zweige vor denselben Korrekturen; Upload-Fortschritt für Sitzungen, gemeinsamer Speicher und unterschiedliche Serialisierer schaffen bestimmte Bedingungen	Zweigkorrektur anwenden und ausdrücklich aktivierten Upload-Fortschritt sowie gemeinsame Sitzungskonfiguration prüfen

Eintrag	NVD-Status (27. Nov.)	Relevanter betroffener Umfang	Korrigierte Versionen oder Maßnahme
CVE-2026-86218	Analysiert; NVD CVSS 3.1 9,8 Kritisch	N-central-Versionen vor 2026.3.1.14	2026.3 HF4; installierte Version und Anbieterhinweise prüfen
CVE-2026-41940	Analysiert; CVSS 3.1 9,8 Kritisch	Betroffene cPanel- und WHM-Versionszweige nach 11.40 vor Zweigausschlüssen (Authentifizierungsumgehung)	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 oder 136.0.5 (11.x-Zweigkorrekturen laut NVD); rückblickenden Zugriff prüfen [S7][S47]

Der ausgewählte Java-Hinweis nennt diese korrigierten Oracle-Versionskennungen. Es sind Softwareversionen. [S44]

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

Für Java nennt NVD bestimmte betroffene Oracle-Versionen, darunter 8u511b33-perf, 17.0.21.0.3, 21.0.13.0.3, 25.0.5.0.3 und 27.0.1.0.3 sowie aufgeführte GraalVM-Versionen. Andere Distributionslinien brauchen ihren eigenen passenden Hinweis. Die nachgewiesene Prozessorbedingung ist x86-64 mit AVX-512-VBMI-Unterstützung. [S7] [S44]

Bei PHP-Anfragen ist die Versionsinventur nur der erste Schritt. Beide zitierten PHP-Einträge stehen am 27. November in der NVD weiter auf ausstehender Analyse, mit PHP-CNA-CVSS-4.0-Werten von 9,2 (Kritisch). Das beschriebene FPM-Szenario hängt von wiederverwendeten Backend-Verbindungen und einem relevanten Anfragepfad ab. Standardkonfigurationen mit geschlossener Verbindung nach jeder Anfrage liegen außerhalb des im Hinweis nachgewiesenen FPM-Szenarios. [S7][S45]

Beim Sitzungsproblem stellt eine Aktualisierung allein nicht sicher, dass getrennte Konfigurationen denselben Serialisierer für gemeinsame Sitzungsdaten verwenden. Prüfen Sie ausdrücklich aktivierten Upload-Fortschritt für Sitzungen und die tatsächliche Installation. Leiten Sie allein aus einer vorhandenen Version keine entfernte Codeausführung ab. [S7][S45]

Auch die NGINX-Warnung vom 18. November sollte eine produkt- und konfigurationsspezifische Prüfung auslösen. Die BMI-Mitteilung beschreibt die koordinierte Warnreaktion, keine Zahl österreichischer verwundbarer Server. Nutzen Sie den aktuellen Herstellerhinweis für die installierte Distribution. [S48]

Frühere Hosting-Administrationswarnungen rechtfertigen auch nach einer Korrektur die Sicherung rückblickender Zugriffsbelege. Der CERT.at-Hinweis vom April zu cPanel und WHM (CVE-2026-41940) beschreibt aktive Ausnutzung und Kontakt zu bekannten verwundbaren österreichischen Betreibern. Er beziffert keine erfolgreichen österreichischen Einbrüche. [S7][S47]

7.8 Hacktivistische Bezeichnungen und Eintragsweitergaben

Die akteursbezogenen Karten in Kapitel 6 belegen die Aussagen der bezeichneten Veröffentlichungsquellen. Sie belegen weder Betreiber-Nationalität oder staatliche Steuerung noch erfolgreiche Auswirkungen. Für diese Behauptungen wird hier keine staatliche Zuschreibung vorgenommen. [S1]

NoName057(16)

Bezeichnete Veröffentlichungsquelle

Behauptungen zu Verfügbarkeit und Zugang | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

2026-05-08
Website-Behauptungen, B13

Mai 2026
Behauptung zur Filialüberwachung, B17

2026-05-17
Website- und Geolokalisierungsangaben, B14

BEHAUPTETE ZIELE

Öffentliche, verkehrsbezogene, energiebezogene und Handelsdienste, ausschließlich als breite Rollen beschrieben

IN EIGENEN WORTEN

"(durch Geolokalisierung gesperrt)" B14

IN ÖFFENTLICHER BERICHTERSTATTUNG

UNSERE EINSCHÄTZUNG

Nachrichten aus einer NoName057(16) zugeordneten Quelle belegen veröffentlichte Behauptungen. Sie belegen weder gemessene Ausfälle noch aktuellen Zugang, Betriebsunterbrechung oder staatliche Steuerung. Quelle: S1.

VERTRAUENSGRAD
Hoch für die vorliegende Veröffentlichung; Ergebnis und Zuordnung bleiben unbestätigt

Darkstorm

Zugeschriebene Bezeichnung in Weitergaben

Zuordnung innerhalb einer Weitergabe | Keine staatliche Zuordnung bewertet

BEHAUPTETE ZIELE

Energiebezogene Website; keine Auswirkung auf Energieprozesse belegt

IN ÖSTERREICH, 2026

2026-05-08
Energiebezogene Website-Behauptung in B15 zugeordnet

IN EIGENEN WORTEN

"#DARKSTORM" B15

IN ÖFFENTLICHER BERICHTERSTATTUNG

UNSERE EINSCHÄTZUNG

Der vorliegende Beitrag ist eine Weitergabe, die Darkstorm nennt. Er belegt weder ursprüngliche Urheberschaft noch Zusammenarbeit, gemeinsame Steuerung, bestätigten Ausfall oder eine staatliche Verbindung. Quelle: S1.

VERTRAUENSGRAD
Hoch für die vorliegende Veröffentlichung; Ergebnis und Zuordnung bleiben unbestätigt

313 Team

Bezeichnete Veröffentlichungsquelle

Behauptung zur Verfügbarkeit eines öffentlichen Dienstes | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

2026-03-26
Geplante Aktion und Dauer in B16 angekündigt

BEHAUPTETE ZIELE

Öffentliche Website ohne Identifikator des Betroffenen

IN EIGENEN WORTEN

"soll eine Stunde dauern" B16

IN ÖFFENTLICHER BERICHTERSTATTUNG

UNSERE EINSCHÄTZUNG

Eine Quelle mit dieser Bezeichnung kündigt eine Aktion und eine geplante Dauer an. Die Dauer ist kein gemessener Ausfall. Datenzugriff, Auswirkungen auf öffentliche Aufgaben und Betreiberidentität bleiben unbestätigt. Quelle: S1.

VERTRAUENSGRAD
Hoch für die vorliegende Veröffentlichung; Ergebnis und Zuordnung bleiben unbestätigt

Darkstorms Auftreten über eine andere bezeichnete Quelle ist eine Weitergabebeziehung. Es belegt weder Zusammenarbeit noch gemeinsame Kontrolle. Auch die Zuschreibung einer NoHeartz-Übersicht bleibt deren Aussage; der Vorbehalt zum Steuerungszugriff bleibt erhalten.

Mehrere Feed-Weitergaben wiederholten 2026 einen einzelnen als 0APT bezeichneten österreichischen Eintrag. Das sind Verbreitungsbeobachtungen, keine mehreren unabhängig bestätigten Angriffe oder eine 0APT-Originalveröffentlichung. Zielangaben und Branchenbezeichnungen bleiben zurückgehalten, weil der Eintrag eine unbestätigte Behauptung ist. [S1][S2]

0APT

Bezeichnung im beobachteten Erpressungsbestand

Bezeichnung in Erpressungseinträgen | Keine staatliche Zuordnung bewertet

IN ÖSTERREICH, 2026

2026

1 Österreich zugeordneter Eintrag in Ransompedia (S2), mehrfach durch Weitergaben verbreitet (S1)

BEHAUPTETE ZIELE

Österreich zugeordneter Eintrag; Identität und Branche zurückgehalten

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] Ransompedia verzeichnet 1 Österreich zugeordneten Eintrag mit dieser Bezeichnung.

UNSERE EINSCHÄTZUNG

Mehrere Meldungsweitergaben eines Eintrags ergeben keine getrennten Angriffe, und die Bezeichnung belegt keinen staatlich verbundenen Betreiber. Datendiebstahl, Verschlüsselung und offizielle Bestätigung bleiben unbestätigt. Quellen: S1, S2.

VERTRAUENSGRAD

Hoch für die vorliegende Eintragszahl; Ergebnis und Zuordnung bleiben unbestätigt

Die Bezeichnung 0APT belegt keine staatliche Unterstützung, nur weil ihr Name APT enthält. Auch übereinstimmende Akteursbezeichnungen in einem Feed und einem anderen Datenbestand brauchen fallspezifische Identitätsprüfungen, bevor Datensätze zusammengeführt werden.

7.9 Was eine Akteursbewertung stärken würde

Eine stärkere Bewertung würde Beobachtungen durch ein unabhängig aussagekräftiges gemeinsames Element verbinden. Beispiele sind gestützte Infrastruktur, ein gemeinsames Kampagnenartefakt oder eine von der Quelle bestätigte Zugangsbeziehung. Ähnliche politische Rhetorik oder derselbe Zielsektor genügen nicht.

Halten Sie die Aussage auch bei starker Verbindung eng. Ein gemeinsamer Kontakt kann eine Kontaktbeziehung stützen, während die Betreiberidentität ungeklärt bleibt. Derselbe Datenbestand kann Wiederverwendung belegen, ohne den ursprünglichen Erwerber zu zeigen.

Für die Abwehr entscheidet der Nutzen einer stärkeren Zuschreibung danach, ob sie eine Entscheidung verändert. Sie kann eine gezielte Suche oder Dienstleisterfrage leiten. Sie sollte keine dringende Konto-, Dienst- oder Kundenschutzmaßnahme verzögern, die bereits durch direkte Belege gerechtfertigt ist.

KERNAUSSAGEN

01

Eintragsbezeichnungen beschreiben Behauptungen, keine eindeutigen Betreiber oder erfolgreichen Einbrüche.

02

Erhalten Sie die von CERT.at bewertete Beziehung, ohne sie auf jeden gleich bezeichneten Fall anzuwenden.

03

Passen Sie dringende Behebung an Produkt, Version und Konfiguration an.

KAPITEL 08

Betrugsökonomie: Identität, Kontext und Zahlung

DIESES KAPITEL BEANTWORTET

Wie werden glaubhafte Informationen zu einer unbefugten Finanzanweisung?

3

unterschiedliche Entscheidungen: Identitätsprüfung, Zahlungsfreigabe und Kundenschutz

8.1 Kontext ist keine Berechtigung 88

8.2 Bewerbungen und Arbeitsangebote brauchen unterschiedliche Eskalationswege 88

8.3 Behörden- und Bankidentitäten können Kommunikationskanäle verbinden 89

8.4 Rückholbetrug kann den Schaden verlängern 89

8.5 Konten- und Identitätsdienste im Untergrund bleiben Behauptungen 89

8.6 Zahlungskartenmaterial in Beiträgen: ein enger Ausschnitt 91

8.7 Gemeinsame Reaktion ohne gemeinsame Vorfallsumme 91

KAPITEL 08

Betrugsökonomie: Identität, Kontext und Zahlung

KURZFASSUNG

Österreichische Warnungen beschreiben Betrug über Nachrichten, Anrufe, Websites und Fernwartungssitzungen. Richtiger Kontext kann eine Anfrage überzeugend machen, ohne sie zu legitimieren. Untergrundangebote zeigen Marktaussagen oder Nachfrage; amtliche Hinweise beschreiben tatsächlich berichtete Abläufe. Bestätigen Sie die verlangte Handlung unabhängig, erhalten Sie einen sicheren Kontaktweg und unterstützen Sie Menschen, die bereits gehandelt haben.

8.1 Kontext ist keine Berechtigung

Der Buchungshinweis beschreibt Nachrichten mit richtigen persönlichen Angaben und Reisedetails. Der BEC-Hinweis beschreibt glaubhafte Lieferanten- oder Vorgesetztenanfragen. Beides zeigt, warum die Kenntnis einer echten Information die nächste Handlung nicht autorisiert. [S11][S12]

Eine Organisation sollte den Punkt bestimmen, an dem vertrauter Kontext zu einer neuen Forderung wird: Zahlung, Kontoanmeldung, Anhang, Fernsteuerung oder Mitarbeiterinformationen. Dieser Wechsel ist ein sinnvoller Zeitpunkt für eine unabhängige Prüfung.

Der unabhängige Kanal sollte bereits bekannt sein. Eine Telefonnummer in der umstrittenen Nachricht kann Teil der Täuschung sein. Eine Bestätigung durch Antwort an dasselbe Postfach klärt nicht, ob jemand anderes dieses Postfach kontrolliert.

Dieses Vorgehen verlangt nicht die Annahme, jede unerwartete Nachricht sei kriminell. Es verlangt einen Prozess, der eine legitime Änderung bestätigen kann, ohne allein dem Übermittlungskanal der Änderung zu vertrauen.

8.2 Bewerbungen und Arbeitsangebote brauchen unterschiedliche Eskalationswege

Der Bewerbungsfall und der Aufgabenjob-Fall nutzen beide einen Beschäftigungskontext, verlangen aber unterschiedliche Handlungen. Ersterer betrifft Geschäftskorrespondenz und ein Archiv. Letzterer verlangt Einzahlungen von Einzelpersonen, die Verdienst erwarten. [S9][S20]

Eine betriebliche Schulung sollte beides nicht in einer allgemeinen Warnung zusammenfassen. Empfang und Personalbeschaffung brauchen einen Weg zur Eskalation ungewöhnlicher Korrespondenz oder Dateien. Kundennahe Teams müssen Menschen erkennen, die für Arbeit oder die Freigabe eines Guthabens zahlen sollen.

Sichern Sie im ersten Szenario die Korrespondenz und lassen Sie relevante Endgeräte- und Kontobelege durch die Sicherheit prüfen. Helfen Sie im zweiten, weitere Überweisungen zu stoppen und den Zahlungsanbieter zu kontaktieren. Keine Reaktion erfordert die Annahme eines gemeinsamen Betreibers.

8.3 Behörden- und Bankidentitäten können Kommunikationskanäle verbinden

Die Warnungen des Finanzministeriums unterscheiden seinen echten Zustellprozess von erfundenen Steuerforderungen. Bank-Imitation und Verlängerungsszenarien zeigen, wie eine Nachricht in ein überzeugendes Telefongespräch führen kann. [S23][S24][S17][S18]

Kundenhinweise sollten erklären, wie ein echter Kontakt begonnen wird. Wer selbst die bekannte App öffnet oder einen vorhandenen Kontakt nutzt, ist besser geschützt als jemand, der nur den angezeigten Namen prüft.

Ein Supportleitfaden sollte auch Fernzugriff behandeln. Anrufer können Gerätesteuerung als Sicherheitsmaßnahme darstellen. Beschäftigte sollten den tatsächlichen Supportablauf erklären. Wer bereits Software installiert oder eine Zahlung freigegeben hat, braucht einen zugänglichen Hilfsweg.

Leiten Sie daraus keinen Zugriff auf die imitierte Stelle ab. Markenmissbrauch, ein betroffenes Kundengerät und ein institutioneller Einbruch sind getrennte Aussagen. Der Meldeverantwortliche braucht tatsächliche Fakten, bevor er eine rechtliche oder öffentliche Beschreibung auswählt.

8.4 Rückholbetrug kann den Schaden verlängern

Die Anlageuntersuchung vom April beschreibt eine spätere Ansprache mit dem Versprechen, verlorenes Geld gegen eine weitere Gebühr zurückzuholen. Diese zweite Stufe kann die Kenntnis eines echten früheren Verlusts ausnutzen. Sie bestätigt keine Berechtigung des neuen Kontakts. [S19]

Eine Bank oder Kundenbetreuung sollte deshalb nach weiteren Kontaktaufnahmen fragen, wenn sie nach einem Betrug hilft. Auch eine als Rückhol-, Ermittlungs- oder Rechtsgebühr dargestellte Forderung braucht unabhängige Bestätigung.

Die Schutzbotschaft sollte praktisch und respektvoll sein. Geben Sie einen bekannten Kontakt an, erklären Sie den nächsten berechtigten Schritt und nennen Sie Forderungen, die die Organisation nicht stellen wird. Hilfe sollte keine eigene Diagnose eines kriminellen Netzwerks voraussetzen.

8.5 Konten- und Identitätsdienste im Untergrund bleiben Behauptungen

Eine Anzeige für ein Konto, Identitätsdokument oder einen Finanzdienst belegt ein Angebot. Sie zeigt weder ein nutzbares Konto noch die Zustimmung seines Inhabers oder eine mögliche Umgehung der beschriebenen Überprüfung. [S1]

Preise sind ebenso begrenzt aussagekräftig. Ein verlangter Preis kann Werbestrategie, Paketbeschreibung oder wiederholte Vorlage widerspiegeln. Er ist weder ein Geschäftsabschluss noch eine Schätzung des durch einen Käufer möglichen Schadens.

Eine sinnvolle Eskalation vergleicht die beworbene Kategorie mit dem tatsächlichen Organisationsrisiko. Ein behauptetes Mitarbeiterkonto kann die Identitätsreaktion betreffen. Ein Kundendatensatz kann Betrug und Datenschutz betreffen. Ein allgemeines Dienstangebot kann Beobachtung rechtfertigen, ohne einen organisationsspezifischen Vorfall zu belegen.

Zwei gespeicherte Preisangaben zeigen, warum Einheit und geografischer Umfang wichtig sind. Keine belegt einen österreichischen Bankkontopreis oder eine abgeschlossene Transaktion. [S1]

Karte	Preisangabe	Einheit und Grenze
B11	Käufer bietet USD 100	Je gesuchtem persönlichen Konto; Österreichbezug unbestätigt
B12	Verkäufer verlangt USD 2.000	Vollständiges beworbenes weltweites Telefondatenpaket; kein rein österreichischer Preis

B11 ist die erklärte Zahlungsbereitschaft eines Käufers. B12 ist die Preisforderung eines Verkäufers für ein anderes Produkt. Sie sollten weder gemittelt noch als zwei Beobachtungen desselben Marktes behandelt werden. Gemeinsamer Betreiber oder identischer Datenbestand sind nicht belegt. [S1]

Belegkarte B11 — 21. Juni 2026

[Alias zurückgehalten] · Forum · Forum · Russisch

ORIGINAL

За каждое ЛК готов заплатить 100$

ÜBERSETZUNG

Für jedes persönliche Konto bin ich bereit, 100$ zu zahlen.

Belegt
Ein Käufer bietet USD 100 je gewünschtem persönlichem Konto. Der Österreichbezug ist unbestätigt.

Nicht festgestellt
Ein österreichischer Bankkontopreis, nutzbarer Zugang, Kontozuordnung oder abgeschlossene Transaktion.

Belegkarte B12 — 20. Okt. 2026

[Alias zurückgehalten] · Forum · Forum · Englisch

ORIGINAL

Price (full): 2000 $

ÜBERSETZUNG

Preis vollständig: 2000 $

Belegt
Ein Verkäufer verlangt USD 2.000 für ein weltweites Paket zusammengetragener Telefondaten.

Nicht festgestellt
Ein Preis für einen österreichischen Ausschnitt, echte Dateien, neuer Systemzugriff oder abgeschlossener Verkauf.

8.6 Zahlungskartenmaterial in Beiträgen: ein enger Ausschnitt

UMFANG DER KARTENANGABEN

Zahlen in diesem Abschnitt betreffen nur Zahlungskarten, die in den für diesen Bericht gesammelten Dark-Web-Beiträgen im Klartext erschienen. Brandefense erkennt gestohlene Karten auch mit anderen Methoden außerhalb dieses Ausschnitts. Die Zahlen messen weder gesamten Kartendiebstahl noch gültige Karten, abgeschlossene Zahlungen oder Betrugsschäden.

Die nach Ländern gekennzeichnete Nachrichtenpopulation enthält 88 unterschiedliche Zahlungskarten, die in 100 Beiträgen im Klartext erscheinen. Die Länderkennzeichnungen bestätigen weder Ausgabeland noch aktuelle Gültigkeit oder tatsächlichen Missbrauch unabhängig. [S5]

Kartenbeobachtungen aus Beiträgen sind eine enge Population. Sie sollten weder mit polizeilichen Schadenssummen verglichen noch als Zahl betroffener Bankkunden behandelt werden. Eine kriminelle Nachricht kann veraltete Informationen, Wiederholungen oder ungeprüfte Statusbehauptungen enthalten. [S5]

Die Reaktion beginnt mit einer berechtigten Prüfung durch den Kartenherausgeber. Prüfen Sie Zugehörigkeit, Gültigkeit, frühere Behebung und tatsächlichen Missbrauch, bevor Sie eine eingreifende Maßnahme wählen. Ein Beitrag allein sollte keinen automatischen Kartentausch für eine breite Kundengruppe rechtfertigen.

8.7 Gemeinsame Reaktion ohne gemeinsame Vorfallsumme

Betrugs-, Identitäts- und Vorfallteams können relevante Fakten teilen und ihre Entscheidungen getrennt halten. Eine Postfachuntersuchung belegt keinen Zahlungsschaden. Eine betrügerische Zahlung belegt nicht den Erwerbsweg eines Kontos. Ein veröffentlichter Kontaktdatensatz belegt keine Verursachung eines späteren Anrufs.

Nutzen Sie eine Fallakte mit getrennten Feldern für beobachtete Nachricht, bestätigten Zugriff, Zahlungsereignis und Kundenschaden. Erfassen Sie Verbindungen nur bei ausreichenden Belegen. Eine ungeprüfte Verbindung sollte eine Hypothese mit Verantwortlichem und nächstem Prüfschritt bleiben.

Eine erfolgreiche Reaktion kann eine verhinderte Überweisung, ein eingedämmtes Konto und eine gut belegte Kundenmitteilung umfassen. Das sind unterschiedliche Ergebnisse. Getrennte Messung zeigt leichter, welche Kontrolle verbessert werden muss.

KERNAUSSAGEN

01

Richtige Details und vertraute Kanäle autorisieren keine neue Handlung.

02

Bereiten Sie sich auf fortgesetzte Täuschung durch Anrufe, Gerätesteuerung und Rückholangebote vor.

03

Begrenzen Sie Kartenbeobachtungen auf ihren Ausschnitt und prüfen Sie Herausgebermaßnahmen anhand berechtigter Belege.

KAPITEL 09

Banken im Detail

09

DIESES KAPITEL BEANTWORTET

Welche Bankentscheidungen verbinden Identitätsbelege, Zahlungsbetrug und Dienstleisterstörung?

3

getrennt zu haltende Populationen: Domainbeobachtungen, Kartenbeobachtungen und gemeldeter Betrug

9.1 Finanzpopulation vor ihrer Einordnung bestimmen 94

9.2 Kundentäuschung kann von der erwarteten technischen Darstellung abweichen 96

9.3 Finanzdienstleister brauchen eine kundenspezifische Prüfung 96

9.4 Fristen getrennt halten 97

9.5 Eine Bankenübung auf Grundlage der zitierten Warnungen 97

9.6 Praktische Abschlussbelege für Finanzteams 98

KAPITEL 09

Banken im Detail

KURZFASSUNG

Das Bankenbild umfasst kundenbezogene Imitation, ausgewählte Finanzdomainbeobachtungen und einen sektorspezifischen Resilienzrahmen. Keine dieser Ansichten ersetzt die anderen. Gemeldeter Betrug kann ohne Bankeinbruch auftreten; ein Dienstleisterereignis kann eine gesonderte IKT-Prüfung erfordern. Prüfen Sie das relevante Konto oder die Transaktion, bestimmen Sie die tatsächliche Dienstbeeinträchtigung und weisen Sie finanzielle Meldeverantwortung früh zu.

9.1 Finanzpopulation vor ihrer Einordnung bestimmen

Das Portfolio enthält eine Banken- und Finanzgruppe ausgewählter Domains. Sie ist keine überprüfte Liste unabhängiger zugelassener Kartenherausgeber. Gruppenunternehmen, Dienstleister und überlappende Domains können die Einordnungseinheit beeinflussen. [S6]

Finanzdomainpopulation und Kartenbeitragspopulation brauchen daher getrennte Nenner. Eine einem Herausgeber zugeordnete Kartenbeobachtung belegt keine Gefährdung seiner Kernsysteme. Eine Gerätezuordnung steht nicht automatisch für einen Bankbeschäftigten.

Ein Bankenexpositionsergebnis sollte Beobachtungsgegenstand, Zeitpunkt und beschriebene Domain- oder Dienstpopulation benennen. Fehlt die zugrunde liegende Messung, bleibt das Ergebnis unbekannt. Es wird kein Banken- oder Branchenwert abgeleitet.

Die Expositionsmomentaufnahme vom 23. November umfasst alle 25 ausgewählten Finanzdomains. Davon hatten 4 Zugangsdaten im Angebot und 3 frühere Eintragshistorien, da eine Domain ein aktuelles Angebot mit null früheren Einträgen aufweist. Insgesamt tragen 21 Domains Gerätezuordnungen (3.728 gesamt; 47 mitarbeiterbezogene über 11 Domains und 3.681 andere Zuordnungen). Alle 25 Domains tragen Zugangsdatenzuordnungen (53.514), und 12 tragen Dokumentenzuordnungen (53). Das sind überlappende Beobachtungen, keine eindeutigen Beschäftigten, Kunden oder bestätigten Einbrüche. [S4]

Finanzdomainsignal	Beobachtete Menge	Einordnungsgrenze
Domains mit aktuellem Angebot	4 von 25	Nutzbarer Zugang und Transaktion bleiben unbelegt
Domains mit früherer Eintragshistorie	3 von 25	Getrennt vom aktuellen Angebotsstatus; eine Domain hat nur ein aktuelles Angebot
Gerätezuordnungen	3.728	Über 21 Domains; enthält 47 mitarbeiterbezogene (11 Domains) und 3.681 andere Zuordnungen
Zugangsdatenzuordnungen	53.514	Über 25 Domains; keine Gesamtzahl eindeutiger Personen oder aktueller Konten
Dokumentenzuordnungen	53	Über 12 Domains; nicht automatisch eine neue Offenlegung

Das Klartext-Kartenmaterial in §8.6 belegt weder eine überprüfte Zuordnung von Karten zu Banken noch eine Herausgeberrangfolge. [S5]

Die passive Momentaufnahme vom 23.–27. November umfasst alle 25 ausgewählten Finanzdomains. Sie ist eine andere Beobachtungspopulation, keine Erhebung zugelassener Herausgeber. Es wird kein Banken- oder Branchenwert veröffentlicht. [S3][S6]

Kontrollbeobachtung im Bankenbereich	Domains	Geprüfte Population
DMARC-Durchsetzung beobachtet (14 Ablehnung; 6 Quarantäne)	20	25 Domains (5 Beobachtung; 0 nicht beobachtet)
SPF-Eintrag beobachtet	24	25 Domains
DKIM-Schlüssel beobachtet	17	25 Domains
DNSSEC-Delegationseintrag beobachtet	5	25 Domains
CAA-Eintrag beobachtet	4	25 Domains
Gültige TLS-Beobachtung	25	25 Domains
HSTS beobachtet	23	25 Domains mit erfasster HTTP-Antwort

Die Beobachtungen messen nicht jeden E-Mail-Ablauf oder jede Finanzanwendung. Ein unbeobachteter Schlüssel oder Delegationseintrag belegt keine organisationsweit fehlende Kontrolle. Ein gültiges TLS-Ergebnis belegt weder Transaktionsberechtigung noch Anwendungssicherheit. [S3]

9.2 Kundentäuschung kann von der erwarteten technischen Darstellung abweichen

Der SMS-zu-Anruf-Fall vom April beschreibt einen zur Überweisung überredeten Kunden. Das Verlängerungsszenario ergänzt Fernwartungstäuschung. Im Oktober hielt die Oesterreichische Nationalbank (OeNB) fest, dass in Österreich ungefähr 1 von 16.000 Zahlungen von Betrug betroffen ist, bei rund EUR 115 Millionen Vorjahresschäden. Sie ergänzte, dass Täter zunehmend Menschen manipulieren statt technische Systeme zu umgehen. Die RTR-GmbH hob gesondert die Regulierung alphanumerischer SMS-Absenderkennungen gegen Absenderfälschung hervor. Diese Warnungen rechtfertigen Kundenschutzvorsorge, ohne Zugriff auf die Infrastruktur der imitierten Bank zu belegen. [S16][S17][S18]

Betrieblich entscheidet, ob der Support das Muster erkennt, solange die Zahlung noch beeinflussbar ist. Ein Kunde kann einen Sicherheitsnotfall schildern und dem Wissen des Anrufers vertrauen. Die Eskalation sollte Beschäftigte erreichen, die Transaktion und sicheren Kontaktweg prüfen können.

Betrugsteams sollten versuchte Zahlung, berechtigt freigegebene Zahlung unter Täuschung und bestätigten Kontomissbrauch unterscheiden. Das beeinflusst zu sichernde Belege, Kundenerklärung und die über den Zahlungskanal verfügbare Reaktion.

Der Bericht weist diesen Mechanismen keine nationale Schadensschätzung über die amtlichen Zahlen mit ihrem ursprünglichen Umfang hinaus zu. Er leitet auch aus markennennenden Beitragszahlen keine Wirksamkeit einer bestimmten Bank ab.

9.3 Finanzdienstleister brauchen eine kundenspezifische Prüfung

Ein Finanzunternehmen kann von einer gehosteten Plattform, einem verwalteten Dienst oder Kommunikationsanbieter abhängen. Die allgemeine Vorfalldarstellung des Anbieters klärt möglicherweise nicht, ob eine kritische oder wichtige Funktion des Finanzunternehmens betroffen war.

Der Dienstverantwortliche sollte Mandant, Funktion und Informationen bestimmen. Compliance sollte die relevanten DORA-Einstufungs- und Meldebedingungen prüfen. Die Sicherheit sollte dafür erforderliche technische Belege erhalten. [S40]

Warten Sie nicht auf eine vollständig geklärte Darstellung, bevor Sie Verantwortung für die Meldebewertung zuweisen. Bezeichnen Sie ebenso keine gewöhnliche Anbietermitteilung als schwerwiegenden IKT-Vorfall, ohne tatsächliche Kriterien und Umfang anzuwenden.

Der FMA-Dialog mit IKT-Anbietern vom November ist relevanter Aufsichtskontext. Er belegt keine Einbrüche bei teilnehmenden Anbietern oder Banken. Die praktische Reaktion ist, Dienstleistereskalation und Meldeverantwortung bereits nutzbar vorzuhalten. [S42]

9.4 Fristen getrennt halten

Bei einem erfassten DORA-Ereignis verbindet die reguläre Erstmelderegel vier Stunden nach schwerwiegender Einstufung mit vierundzwanzig Stunden nach Kenntnis. Eine Ausnahme für späte Einstufung und eingeschränkte Kalenderbestimmungen gelten ebenfalls; siehe §10.5. [S59]

Eine Prüfung personenbezogener Datenverletzungen kann parallel unter einem anderen Rechtsmaßstab laufen. Das Datenschutzteam sollte Kenntnis und Personenrisiko getrennt dokumentieren. Eine DORA-Meldung klärt nicht automatisch die DSGVO-Entscheidung. [S38]

Der gemeinsame Ereignisakt sollte deshalb Feststellung, Kenntnis, Einstufung, Dienstleisterbenachrichtigung und Meldeübermittlung als getrennte Zeitpunkte erhalten. Ein einziges Feld mit der Bezeichnung Vorfalldatum genügt diesen unterschiedlichen Zwecken nicht.

9.5 Eine Bankenübung auf Grundlage der zitierten Warnungen

Das Folgende ist ein Planungsszenario, kein Bericht über einen gemessenen Bankvorfall.

Ein Kunde erhält eine SMS zur Identitätsverlängerung. Anschließend verlangt ein Anrufer Fernwartung und eine Überweisung zum Schutz des Guthabens. Gleichzeitig meldet ein externer Dienst unklaren Zugriff auf dienstliche Mitarbeiterkontakte.

Das Betrugsteam sollte Kundenkontakt und Transaktion bewerten. Identitätsbeschäftigte prüfen tatsächliche Kontobelege. Der Dienstverantwortliche erfragt den finanzunternehmensspezifischen Umfang beim Anbieter. Compliance und Datenschutz dokumentieren getrennte Meldeentscheidungen.

Geben Sie zusätzlich vor, dass die normale Kontaktperson nicht erreichbar ist. Die Übung sollte eine vertrauenswürdige Alternative zeigen, statt eine Nummer aus dem Anruf oder der umstrittenen Nachricht zu akzeptieren.

Der Abschluss erfordert Belege für einen sicheren Kundenkontaktweg, geprüfte Zahlungsmaßnahmen, bewerteten Dienstleisterumfang und dokumentierte gesetzliche Fristen. Er erfordert nicht die Annahme eines gemeinsamen Betreibers hinter den beiden Beobachtungen.

9.6 Praktische Abschlussbelege für Finanzteams

Arbeitsbereich	Verantwortliche	Abschlussbelege
Kunden-Imitation	Betrugsbetrieb	Kontakt geprüft und Transaktionsergebnis dokumentiert
Mitarbeiterkontosignal	Identitätsreaktion	Kontorolle, Berechtigungen und relevante Sitzungen bewertet
Kartenbeobachtung im Beitrag	Berechtigtes Herausgeberteam	Gültigkeit, frühere Behebung und Missbrauch geprüft
Dienstleistervorfall	IKT-Dienstverantwortliche	Rechtsträgerspezifische Funktion, Mandant und Datenumfang dokumentiert
DORA-Bewertung	Finanz-Compliance	Einstufung, Fristen und erforderliche Übermittlungen dokumentiert
Personenbezogene Datenprüfung	Datenschutzbeauftragte	Risiko- und Meldeentscheidungen mit Gründen

Der Vorstand sollte fragen, ob diese Verantwortlichen bei einem dringenden Ereignis zusammenarbeiten können. Warnungen zu zählen oder eine Richtlinie vorzuhalten ist weniger aussagekräftig als erforderliche Entscheidungen mit unvollständigen Informationen nachzuweisen.

KERNAUSSAGEN

01

Kundenbetrug belegt keinen Einbruch in die Kernsysteme einer Bank.

02

Verlangen Sie finanzunternehmensspezifischen Dienstleisterumfang und dokumentieren Sie Feststellung getrennt von Einstufung.

03

Verbinden Sie Reaktionsteams und erhalten Sie getrennte Transaktions-, IKT- und Datenschutzentscheidungen.

KAPITEL 10

Regulierung und nationale Reaktion

10

DIESES KAPITEL BEANTWORTET

Welche Pflichten gelten, und welches Ereignis startet die jeweilige Meldefrist?

1. Oktober 2026

vollständiges Inkrafttreten des österreichischen NISG 2026

10.1 Zuständigkeiten hängen zusammen, sind aber nicht austauschbar 100
10.2 NISG 2026: aktuelle Pflichten mit rechtsträgerspezifischer Prüfung 101
10.3 NISG-Meldungen: ein dreistufiger Ablauf mit unterschiedlichen Ausgangspunkten 101
10.4 Leitung und Kontrollen brauchen Betriebsnachweise 102
10.5 DORA: Feststellung und Einstufung getrennt festhalten 102
10.6 DSGVO: Personenrisiko und Kenntnis des Verantwortlichen bewerten 103
10.7 Sanktionen: Bestimmung und Kategorie erhalten 103
10.8 Ein Belegakt, mehrere verantwortete Entscheidungen 104

KAPITEL 10

Regulierung und nationale Reaktion

KURZFASSUNG

NISG 2026, DORA und DSGVO haben unterschiedliche Geltungsbereichsprüfungen und Meldeauslöser. Die Registrierungsfrist verschiebt keine NISG-Vorfallpflichten. Finanzmeldungen benötigen Kenntnis- und Einstufungszeitpunkte; Datenschutzmeldungen betreffen Risiken für Personen. Bestimmen Sie den verantwortlichen Rechtsträger und zuständigen Meldeweg. Halten Sie Zeitpunkte getrennt fest und üben Sie eine erste Meldung mit unvollständigen, aber richtigen Informationen.

10.1 Zuständigkeiten hängen zusammen, sind aber nicht austauschbar

Der amtliche Rahmen unterscheidet operative Unterstützung, Strafverfolgung, Datenschutzaufsicht und Finanzaufsicht. Eine Organisation sollte den passenden Weg vor einem dringenden Ereignis bestimmen. Eine einzige Nachricht belegt nicht die Erfüllung sämtlicher geltender Pflichten. [S14][S30][S38][S40]

Die folgende Tabelle fasst den in den Quellen gelesenen Rahmen zusammen. Sie ist eine betriebliche Orientierung, keine rechtsträgerspezifische Rechtsbewertung.

Rahmen	Frage zum Geltungsbereich	Auslöser oder Pflicht	Praktisch Verantwortliche
NISG 2026	Ist die Einrichtung wesentlich, wichtig oder nach einschlägigen Bestimmungen anderweitig erfasst?	Erheblicher Cybervorfall und geltende Sicherheitspflichten	Rechtliche Geltungsbereichsverantwortung und Vorfallreaktion
DORA	Fällt das Finanzunternehmen unter die einschlägigen Kategorien von Artikel 2?	Relevantes IKT-Management und Meldung schwerwiegender Vorfälle	Finanz-Compliance und IKT-Risiko
DSGVO	Liegen eine Verletzung des Schutzes personenbezogener Daten und das entsprechende Personenrisiko vor?	Meldung durch den Verantwortlichen und gegebenenfalls Benachrichtigung Betroffener	Verantwortlicher und Datenschutzbeauftragter
Strafrechtliche Untersuchung	Deuten die Belege auf möglicherweise strafbares Verhalten hin?	Relevante Beweise sichern und Anzeige prüfen	Vorfallleitung und Recht
Dienstleistervertrag	Welche Partei schuldet Informationen, Wiederherstellung oder Unterstützung?	Vertragliche und dienstspezifische Pflichten	Beschaffung und Dienstverantwortung

GovCERT beschreibt eine Zuständigkeit für die öffentliche Verwaltung. Das entbindet eine öffentliche Stelle weder von der gesetzlichen Geltungsbereichsprüfung noch von der Datenschutzentscheidung. Operative Unterstützung, Aufsicht und Strafanzeige erfüllen unterschiedliche Zwecke. [S14]

10.2 NISG 2026: aktuelle Pflichten mit rechtsträgerspezifischer Prüfung

Laut amtlichen Rechts-FAQ trat das NISG 2026 am 1. Oktober 2026 vollständig in Kraft. Das BMI nennt den 1. Januar 2027 als Frist für die erste Registrierung. Der Registrierungszeitraum verschiebt bereits geltende Sicherheits- und Vorfallmeldepflichten nicht. [S30][S54]

§ 24 unterscheidet wesentliche und wichtige Einrichtungen nach Sektor, Größe und bestimmten Kategorien. Ausnahmen umfassen definierte öffentliche Sicherheits- und Strafverfolgungsstellen, Bildungseinrichtungen, Justiz, Gesetzgebung und die Österreichische Nationalbank. Dabei gilt der Vorbehalt der Bestimmung für Vertrauensdienste. [S31]

Einschlägige DORA-Regeln haben für erfasste Einrichtungen Vorrang. Daraus folgt kein pauschaler Ausschluss jedes Finanzunternehmens von sämtlichen NISG-Bestimmungen. Das Gesetz behandelt IKT-Drittdienstleister gesondert. [S31]

Das ausgewählte Domainportfolio ist daher kein Register des rechtlichen Geltungsbereichs. Die Branchenbezeichnung einer Organisation in diesem Bericht klärt nicht die Anwendung einer gesetzlichen Kategorie, Ausnahme oder Größenregel. Dokumentieren Sie den tatsächlichen Rechtsträger und die relevante Bestimmung.

§ 29 verlangt Registrierungsinformationen und spätere Aktualisierungen innerhalb der genannten Fristen. Halten Sie Kontakte und Geltungsbereichsentscheidung nutzbar. Eine Registrierungsbestätigung sollte dem Rechtsträger zugeordnet sein, nicht nur einem Technikteam oder einer informellen Gruppenbezeichnung. [S33]

10.3 NISG-Meldungen: ein dreistufiger Ablauf mit unterschiedlichen Ausgangspunkten

§ 34 verlangt die unverzügliche Meldung erheblicher Vorfälle an das zuständige sektorale CSIRT. Gibt es kein einschlägiges sektorales CSIRT, ist das nationale CSIRT zuständig. Das CSIRT leitet die Meldung an die Behörde weiter. [S32]

Die Reihenfolge ist wichtig.

Schritt	Reguläre Frist	Ausgangspunkt
Frühwarnung	Unverzüglich; spätestens nach 24 Stunden	Kenntnis des erheblichen Vorfalls
Vorfallmeldung	Unverzüglich; spätestens nach 72 Stunden	Kenntnis des erheblichen Vorfalls
Abschlussbericht	Spätestens nach einem Monat	Übermittlung der Vorfallmeldung
Andauernder Vorfall	Fortschrittsbericht zum Fälligkeitszeitpunkt des Abschlussberichts	Abschlussbericht binnen eines Monats nach Ende der Vorfallbehandlung
Vertrauensdienste-Ausnahme	Einschlägige Vorfallmeldung spätestens nach 24 Stunden	Kenntnis eines Vorfalls, der die Vertrauensdiensterbringung beeinträchtigt

Die reguläre 72-Stunden-Meldung und der Abschlussbericht laufen nicht beide ab demselben Zeitpunkt. Auch eine laufende Untersuchung hebt die Pflicht zur geforderten Fortschrittsdarstellung nicht auf. [S32]

Die Meldeleitung sollte Kenntnisgrundlage, Erheblichkeitsentscheidung und vorgesehenen Empfänger dokumentieren. Die erste Meldung kann Unbekanntes benennen. Unsicherheit sollte sichtbar sein; spätere Aktualisierungen folgen den geltenden Anforderungen.

10.4 Leitung und Kontrollen brauchen Betriebsnachweise

§ 31 verpflichtet Leitungsorgane, Risikomaßnahmen sicherzustellen und zu überwachen sowie angepasste Cybersicherheitsschulungen zu besuchen. Beschäftigten sind regelmäßig einschlägige Schulungen anzubieten. § 32 umfasst verhältnismäßige technische, operative und organisatorische Maßnahmen. [S34][S35]

Die Themen umfassen Vorfallbehandlung, Betriebsfähigkeit und Wiederherstellung, Lieferketten, Schwachstellenmanagement, Wirksamkeitsprüfung, Hygiene, Kryptografie, Zugriff und sichere Kommunikation. Daraus sollten zugewiesene Arbeiten mit Belegen für die Funktionsfähigkeit der Kontrolle beim jeweiligen Dienst werden. [S35]

Für die Leitung belegt eine Teilnahmebestätigung allein keinen funktionierenden Dienstleisterersatzweg. Eine Richtlinie allein belegt nicht, dass Beschäftigte eine dringende Zahlungsänderung überprüfen können. Empfohlen wird eine Übung oder berechtigte Kontrollprüfung mit dokumentiertem Ergebnis.

Das ist die praktische Auslegung der Vorbereitung in diesem Bericht. Sie behauptet nicht, jede misslungene Übung sei ein Gesetzesverstoß. Rechts- und Kontrollverantwortliche sollten gefundenen Verbesserungsbedarf von einer Compliance-Schlussfolgerung unterscheiden.

10.5 DORA: Feststellung und Einstufung getrennt festhalten

Laut FMA gilt DORA seit dem 17. Januar 2025 ohne Übergangszeit. Die Anwendung richtet sich nach definierten Finanzunternehmenskategorien. Es gilt keine allgemeine Annahme, dass jedes Unternehmen mit Zahlungsabwicklung erfasst ist. [S50]

Artikel 5 verlangt die reguläre Erstmeldung so früh wie möglich, innerhalb von vier Stunden nach schwerwiegender Einstufung und vierundzwanzig Stunden nach Kenntnis des IKT-Vorfalls. Zwischenmeldungen folgen binnen zweiundsiebzig Stunden nach der Erstmeldung. Der Abschlussbericht folgt binnen eines Monats nach der letzten Zwischenmeldung. [S59]

Erfolgt die schwerwiegende Einstufung später als vierundzwanzig Stunden nach Kenntnis, erlaubt Artikel 5(2) die Erstmeldung binnen vier Stunden nach Einstufung. Kann eine Einrichtung eine Frist nicht einhalten, muss sie die Behörde unverzüglich, spätestens zu dieser Frist, mit Begründung informieren. [S59]

Wochenend- und Feiertagsverlängerungen sind eingeschränkt. Verlängerungen für Erst- und Zwischenmeldungen gelten nicht für Kreditinstitute, zentrale Gegenparteien, Handelsplätze und weitere nach NIS wesentliche oder wichtige Finanzunternehmen. Behörden können andere bedeutende oder systemrelevante Einrichtungen ausnehmen. Für Abschlussberichte gilt eine andere Kalenderbestimmung. [S59]

Das Vorfallteam sollte daher Belege für Feststellung und Einstufung erhalten. Eine Dienstleistermitteilung kann eine Bewertung erfordern, ist aber nicht automatisch die Einstufungsentscheidung. Halten Sie Funktion, Umfang und Begründung dieser Feststellung fest.

Das Meldepaket sollte auch Verantwortung, relevante Belege und Kommunikationsplan bewahren. Eine Übergabe zwischen IKT, Compliance und Dienstleister darf nicht verdecken, wer entscheiden oder die Meldung abgeben kann.

10.6 DSGVO: Personenrisiko und Kenntnis des Verantwortlichen bewerten

Laut Datenschutzbehörde meldet der Verantwortliche eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst binnen 72 Stunden nach Kenntnis, sofern ein Risiko für betroffene Personen nicht unwahrscheinlich ist. Hohes Risiko verlangt unverzügliche Benachrichtigung der Betroffenen. In ihrem Tätigkeitsbericht 2025 verzeichnete die Behörde 1.855 Meldungen von Sicherheitsverletzungen (gegenüber 1.319 im Jahr 2024), darunter 1.704 nationale DSGVO-Meldungen und 83 Telekommunikationsmeldungen nach § 164 TKG 2021. [S38] [S39]

Unvollständige Informationen können ohne unangemessene weitere Verzögerung schrittweise nachgereicht werden. Dokumentieren Sie Risikobewertung und Begründung der Meldeentscheidung. Auch wenige Datensätze können relevant sein, wenn Information oder Missbrauch schweren Schaden erzeugen. [S38]

Eine Auftragsverarbeiter- oder Dienstleistermitteilung sollte dem Verantwortlichen genug zur Bewertung eigener Datensätze und Betroffener sagen. Eine Zusicherung der Systemverfügbarkeit beantwortet die Datenschutzfrage nicht. Umgekehrt belegt eine Sicherheitswarnung nicht automatisch eine Verletzung des Schutzes personenbezogener Daten.

Öffentliche Kommunikation sollte bestätigte von noch geprüften Kategorien unterscheiden. Machen Sie aus einem negativen Befund zu einem Zeitpunkt keine dauerhafte Garantie. Nennen Sie Quelle und Datum der Zusicherung und bieten Sie einen Aktualisierungsweg.

10.7 Sanktionen: Bestimmung und Kategorie erhalten

Für die in § 45 genannten Kernverstöße unterscheiden sich die NISG-Höchstbeträge nach Einrichtungskategorie. Sie sollten nicht pauschal jedem Verfahrensproblem zugeordnet werden. [S37]

Bestimmung	Relevante Kategorie	Genannte Höchstgrenze
§ 45(2)	Wesentliche Einrichtung; genannte Kernverstöße	EUR 10 Millionen oder 2% des weltweiten Vorjahresumsatzes, je nachdem, welcher Betrag höher ist
§ 45(3)	Wichtige Einrichtung; genannte Kernverstöße	EUR 7 Millionen oder 1,4% des weltweiten Vorjahresumsatzes, je nachdem, welcher Betrag höher ist
§ 45(4)	Genannte Registrierungs-, Mitwirkungs- und andere Verfahrensverstöße	EUR 50.000; bei Wiederholung EUR 100.000
DSGVO-Meldehinweis	Meldeverstöße nach Artikeln 33 und 34	Bis zu EUR 10 Millionen oder 2% des weltweiten Vorjahresumsatzes, je nachdem, welcher Betrag höher ist

Quellen: NISG § 44 [S36], NISG § 45 [S37] und Hinweise der Datenschutzbehörde [S38]. Das beschreibt gesetzliche Höchstgrenzen, keine erwarteten Strafen oder eine Risikoberechnung für einen Fall dieses Berichts.

Nach NISG § 44(7) darf die Bezirksverwaltungsbehörde für dasselbe zugrunde liegende Verhalten keine NISG-Geldstrafe verhängen, wenn die Datenschutzbehörde bereits eine Geldbuße nach Artikel 58(2)(i) DSGVO verhängt hat. Die oft für andere DSGVO-Verstöße genannte Höchstgrenze sollte nicht an die Stelle der Meldebestimmung treten. Der Bericht addiert auch keine gesetzlichen Maxima verschiedener Regelwerke zu einer erfundenen Gesamtstrafe. [S36][S38]

10.8 Ein Belegakt, mehrere verantwortete Entscheidungen

Nutzen Sie eine gemeinsame Chronologie mit getrennten Entscheidungsunterlagen. Die Chronologie sollte Erstbeobachtung, Feststellung, Kenntnis, schwerwiegende Einstufung, Dienstleistermeldung, Eindämmung und Wiederherstellung unterscheiden. Jeder Meldeverantwortliche sollte Rechtsprüfung und Übermittlungsbeleg festhalten.

Entscheidung	Benötigte Belege	Abschlussnachweis
NISG-Geltungsbereich	Rechtsträger, Tätigkeit und anwendbare Kategorie oder Ausnahme	Freigegebene Geltungsbereichsbegründung
NISG-Vorfallmeldung	Erheblichkeit und Kenntnisgrundlage	Erforderliche Meldungen und Folgezeitplan
DORA-Einstufung	Erfasste Einrichtung, IKT-Auswirkung und Einstufungsgrundlage	Einstufungszeitpunkt und einschlägige Meldungen
DSGVO-Meldung	Personenbezogene Datenverletzung, Kenntnis und Risikobewertung	Meldung oder begründete Nichtmeldung
Kundenkommunikation	Bestätigter Schaden, hilfreiche Handlung und sicherer Kontaktweg	Freigegebene Mitteilung mit Aktualisierungsverantwortung
Strafanzeige	Mögliche Straftat und gesicherte Belege	Entscheidung und gegebenenfalls Anzeigenbestätigung

Eine Übung sollte Vertretung bei Abwesenheit, Wochenenden und Dienstleisterunsicherheit sichtbar machen. Sie sollte mit dem Nachweis enden, dass die Organisation während laufender Untersuchung eine richtige erste Darstellung übermitteln kann.

KERNAUSSAGEN

01

Bestimmen Sie den Geltungsbereich des Rechtsträgers vor Anwendung eines Meldezeitplans.

02

Dokumentieren Sie Kenntnis, Feststellung und schwerwiegende Einstufung als getrennte Ereignisse.

03

Zeigen Sie Melde- und Kontrollverantwortung durch nutzbare Belege und geübte Übergaben.

KAPITEL 11

Ausblick: bedingte Planungsannahmen

11

DIESES KAPITEL BEANTWORTET

Welche plausiblen Entwicklungen sollten die Vorbereitung der Abwehr verändern?

4

Szenarien mit beobachtbaren Auslösern und alternativen Erklärungen

11.1 Zentrale Bewertungen und Vertrauen 107
11.2 Szenario eins: Ein vertrautes Geschäftskonto verlangt eine neue Handlung 107
11.3 Szenario zwei: Ein Dienstleister stellt den Betrieb vor Klärung des Datenumfangs wieder her 108
11.4 Drittes Szenario: Während der Wiederherstellung erscheint eine Erpressungsbehauptung 108
11.5 Szenario vier: Dringende Aktualisierung legt eine Dienstabhängigkeit offen 109
11.6 Signale statt Kalenderprognosen prüfen 109

KAPITEL 11

Ausblick: bedingte Planungsannahmen

KURZFASSUNG

Die Belege rechtfertigen Vorbereitung auf Betrug über vertraute Kanäle, Dienstleisterunsicherheit und erpressungsbezogene Wiederherstellung. Sie tragen keine zahlenmäßige Prognose österreichischer Vorfälle. Die folgenden Szenarien sind bedingte Planungsannahmen. Jedes hat einen Auslöser, eine alternative Erklärung und einen Entscheidungsverantwortlichen. Prüfen Sie die Signale an der eigenen Umgebung und ändern Sie die Reaktion mit der Beleglage.

11.1 Zentrale Bewertungen und Vertrauen

Vertrauen bezieht sich auf jede Aussage und ihre stützende Population. Es ist kein allgemeiner Reputationswert einer Quelle oder eines Akteurs.

Bewertung	Vertrauen	Grundlage	Wichtige Grenze
Die Prüfung vertrauter Kanäle verdient kurzfristige Aufmerksamkeit	Hoch für den zitierten Mechanismus	CERT.at-Hinweise zu Postfächern, Buchungen und BEC [S10][S11][S12]	Keine gemessene nationale Aussage zur Kontrollwirksamkeit
Bewerbungsbezogener Zugang sollte die relevante Industriereaktion informieren	Mittel für die Übertragung auf eine andere Organisation	Von CERT.at bewertete Beziehung und bestätigte österreichische Fälle [S9]	Zugangsweg muss im Einzelfall geprüft werden
Dienstleistervorfälle brauchen kundenspezifische Entscheidungen	Hoch für die Reaktionsanforderung	Unterschiedliche Umfänge der Novemberdarstellungen [S28][S29]	Keine Vorhersage eines Vorfalls bei einem bestimmten Dienstleister
Erpressungsvorsorge sollte mehrere Behauptungsbezeichnungen abdecken	Hoch für die Eintragsverteilung	61 Einträge unter 22 Bezeichnungen [S2]	Behauptungen sind keine bestätigten Ergebnisse oder Betreiberzahlen
Aktuelle Hinweise rechtfertigen bedingte Bestandsprüfung	Hoch für die Hinweise	Überprüfte Einträge und amtliche technische Hinweise [S7] [S44][S45]	Ein betroffenes Produkt belegt keine erfolgreiche Nutzung

Diese Bewertungen unterstützen ein Arbeitsprogramm. Sie schätzen weder Angriffswahrscheinlichkeit oder erwarteten Schaden noch eine aus wiederkehrender Werbung abgeleitete Frist.

11.2 Szenario eins: Ein vertrautes Geschäftskonto verlangt eine neue Handlung

Planungsannahme. Das echte Postfach eines vertrauten Lieferanten sendet einen plausiblen Dokumentenlink oder geänderte Zahlungsanweisungen. Die Organisation erkennt den Absender, hat die Handlung aber nicht unabhängig bestätigt.

Auslöser. Ein abweichender Prozess, eine neue Zugangsdatenabfrage, unerwarteter Kontozugriff oder eine Lieferantenwarnung macht die Anfrage prüfungsrelevant.

Alternative. Der Lieferant kann eine berechtigte Änderung vornehmen. Seine angezeigte Identität kann auch ohne Postfachzugriff imitiert werden. Die Nachricht allein unterscheidet diese Möglichkeiten nicht.

Entscheidung. Das Identitätsteam prüft relevante Zugriffsbelege. Finanzen oder Geschäftsverantwortliche bestätigen die verlangte Handlung über einen bekannten Kanal. Machen Sie das technische Team nicht zur alleinigen Instanz einer Zahlungsentscheidung.

Änderungssignal. Eine bestätigte berechtigte Anweisung beendet die Betrugsfrage, während technische Auffälligkeiten getrennt bewertet bleiben. Bestätigter Missbrauch rechtfertigt eingegrenzte Konto- und Partnermaßnahmen. [S10][S12]

11.3 Szenario zwei: Ein Dienstleister stellt den Betrieb vor Klärung des Datenumfangs wieder her

Planungsannahme. Ein Anbieter meldet einen Vorfall und normalen Betrieb, während er noch prüft, welche Kundendatensätze zugänglich waren.

Auslöser. Ein Kunde nutzt den betroffenen Dienst, Mandanten oder die Informationskategorie. Dieser direkte Bezug verlangt eine zugewiesene Bewertung statt einer pauschalen Aussage fehlender Auswirkungen.

Alternative. Der Vorfall kann Infrastruktur außerhalb des Kundenmandanten oder seiner Daten betreffen. Eine vorläufige Anbietermitteilung belegt nicht die Betroffenheit jedes Kunden.

Entscheidung. Der Dienstverantwortliche verlangt einen rechtsträgerspezifischen Umfang. Datenschutz und Compliance prüfen ihre Auslöser anhand verfügbarer Fakten. Kundenbetreuung bereitet einen sicheren Bestätigungsweg vor, wenn spätere Identitätstäuschung glaubhaft wird.

Änderungssignal. Belege zum Ausschluss des Mandanten begrenzen die Reaktion. Bestätigter Zugriff oder glaubhafter Missbrauch verändert Eindämmung und Kommunikation. Betriebliche Wiederherstellung allein schließt diese gesonderten Entscheidungen nicht ab. [S28][S29]

11.4 Drittes Szenario: Während der Wiederherstellung erscheint eine Erpressungsbehauptung

Planungsannahme. Eine kriminelle Bezeichnung listet die Organisation, während interne Teams einen Dienst wiederherstellen oder verdächtigen Zugriff bewerten.

Auslöser. Ein berechtigter Abgleich zwischen Behauptung und tatsächlichen Datensätzen, Systemen oder einem aktuellen Ereignis der Organisation macht die Aussage relevant.

Alternative. Der Eintrag kann alte Informationen wiederverwenden, einen Rechtsträger verwechseln oder einen unbelegten Umfang behaupten. Sein Vorhandensein genügt nicht zur Bestimmung des Zugangswegs oder vollständigen Umfangs.

Entscheidung. Sichern Sie die Behauptung intern, prüfen Sie ihre relevanten Elemente und setzen Sie die Dienstwiederherstellung fort. Recht und Kommunikation sollten bestätigte Organisationsfakten statt der vorgeschlagenen Täterdarstellung verwenden.

Änderungssignal. Authentische relevante Belege ändern die Datenbewertung. Eine wiederholte alte Behauptung kann stattdessen eine gezielte Kundenwarnung oder Richtigstellung erfordern. Keines der Ergebnisse bestätigt jede gelistete Aussage. [S2]

11.5 Szenario vier: Dringende Aktualisierung legt eine Dienstabhängigkeit offen

Planungsannahme. Ein aktueller Sicherheitshinweis betrifft ein kritisches Produkt. Die Korrektur erfordert aber eine Dienstleisteränderung oder vorübergehende Dienstunterbrechung.

Auslöser. Installierte Version und Konfiguration entsprechen den betroffenen Bedingungen. Allgemeine Markenbekanntheit darf diese Prüfung nicht ersetzen.

Alternative. Der Dienst kann eine korrigierte Distributionsversion oder eine Konfiguration außerhalb der nachgewiesenen Bedingungen betreiben. Das braucht Belege statt einer Annahme allein anhand der Versionsbezeichnung.

Entscheidung. Technik- und Geschäftsverantwortliche vereinbaren Korrektur, Ersatzbetrieb und Zugriffsprüfung. Eine dokumentierte Ausnahme braucht einen Prüfzeitpunkt und eine zur tatsächlichen Gefährdung passende ausgleichende Maßnahme.

Änderungssignal. Eine überprüfte Korrektur ändert den Gefährdungsstatus. Belege früheren unbefugten Zugriffs ändern die Untersuchung. Ein unauffälliger Diensttest belegt die Wiederherstellung dieser Funktion, nicht die Abwesenheit früheren Zugriffs. [S7][S44][S45][S46]

11.6 Signale statt Kalenderprognosen prüfen

Prüfen Sie die Szenarien bei geänderter relevanter Beleglage. Hilfreiche Signale sind ein Treffer zu einem eigenen Konto, revidierter Mandantenumfang des Dienstleisters, ein bestätigtes Zugriffsereignis oder ein aktualisierter Produkthinweis.

Eine veränderte Zahl sichtbarer Beiträge genügt für sich nicht. Sichtbarkeit und wiederholte Veröffentlichung können sich ohne entsprechende Vorfalländerung verändern. Der Analyst sollte erklären, welcher neue Beleg die Bewertung verändert und warum.

Die Leitung sollte nach der folgenden Entscheidung fragen. Ändert eine Beobachtung keine Eindämmungs-, Wiederherstellungs-, Zahlungs- oder Meldewahl, kann sie beobachteter Kontext bleiben. Verändert sie eine folgenschwere Entscheidung, weisen Sie Verantwortung und nächsten Belegprüfzeitpunkt zu.

KERNAUSSAGEN

01

Verwenden Sie Szenarien als Planungsannahmen mit ausdrücklichen Belegauslösern.

02

Dokumentieren Sie Alternativen, welche die Reaktion begrenzen oder umkehren könnten.

03

Ändern Sie Bewertungen mit ihrer Beleggrundlage, statt Sichtbarkeit als Wahrscheinlichkeit zu behandeln.

KAPITEL 12

Maßnahmenplan

12

DIESES KAPITEL BEANTWORTET

Welche Maßnahmen können Teams im nächsten Planungszyklus abschließen und nachweisen?

30 / 60 / 90

Tage für priorisierte Arbeit, vorbehaltlich früherer Vorfall- und Rechtsfristen

12.1 Dreißig, sechzig und neunzig Tage 112
12.2 Identitäten und Vorfallreaktion 114
12.3 Finanzen und Kundenschutz 114
12.4 Dienst- und Dienstleisterverantwortliche 115
12.5 Recht, Datenschutz und Kommunikation 115
12.6 Leitung und Absicherung 115
12.7 Wie Brandefense helfen kann 116

KAPITEL 12

Maßnahmenplan

KURZFASSUNG

Priorisieren Sie relevante Identitätssignale, unabhängige Zahlungsprüfungen und kritische Dienstleisterabhängigkeiten. Zeigen Sie im nächsten Planungszyklus, dass Kontoeindämmung, Ersatzbetrieb und Meldeübergaben zusammen funktionieren. Der Zeitplan verschiebt weder dringende Vorfallmaßnahmen noch gesetzliche Fristen. Weisen Sie jede Maßnahme einem Verantwortlichen zu, dokumentieren Sie ein Ergebnis und schließen Sie verbleibende Unsicherheit ausdrücklich ab.

12.1 Dreißig, sechzig und neunzig Tage

Der Zeitplan ist eine empfohlene Planungsfolge. Beginnen Sie die Vorfallreaktion sofort, wenn aktuelle Belege dies erfordern. Wenden Sie den tatsächlichen Meldezeitplan aus Kapitel 10 an.

30 Tage

Relevante Konto- und Dienstleisterwarnungen mit eigenen Ressourcen abgleichen

VERANTWORTLICHE
Identitätsleitung und Dienstverantwortliche

UMSETZUNGSNACHWEIS
Konto, Mandant, Datum und Ergebnis dokumentiert

Prozess für Bankverbindungsänderungen von Lieferanten prüfen

VERANTWORTLICHE
Finanzbetrieb

UMSETZUNGSNACHWEIS
Unabhängiger Rückruf und getrennte Freigabe nachgewiesen

Vorfall- und Eskalationskontakte kritischer Dienstleister bestätigen

VERANTWORTLICHE
Beschaffung und Dienstverantwortliche

UMSETZUNGSNACHWEIS
Kontakte getestet, Datenrollen und erforderliche Belege bestimmt

NISG-, DORA- und DSGVO-Anwendung für relevante Rechtsträger bestimmen

VERANTWORTLICHE
Recht, Compliance und Datenschutz

UMSETZUNGSNACHWEIS
Geltungsbereichsregister mit benannten Meldeverantwortlichen

Einschlägige dringende Hinweise und Ausnahmen kritischer Dienste prüfen

VERANTWORTLICHE

Infrastruktur- und Anwendungsverantwortliche

UMSETZUNGSNACHWEIS

Korrekte Version oder dokumentierter Behebungs- und Ersatzplan

260 Tage

Betrug über ein echtes Postfach mit Finanzen und Kundensupport üben

VERANTWORTLICHE

CISO und Betrugsleitung

UMSETZUNGSNACHWEIS

Sichere Bestätigung, Eindämmung und Transaktionsentscheidungen nachgewiesen

Kritischen Dienst unter Annahme eines Identitäts- oder Dienstleisterausfalls wiederherstellen

VERANTWORTLICHE

Kontinuitätsmanagement und technische Verantwortung

UMSETZUNGSNACHWEIS

Wesentliche Aufgabe über getesteten Weg abgeschlossen

Dienstleister-Informationsübergaben mit Datenschutz und Compliance testen

VERANTWORTLICHE

Dienstleistermanagement und Meldeleitungen

UMSETZUNGSNACHWEIS

Rechtsträgerspezifischer Umfang und Erstmeldeinformationen erstellt

E-Mail-Regeln, privilegierte Änderungen und Notfall-Kontowiederherstellung prüfen

VERANTWORTLICHE

Identitäts- und E-Mail-Teams

UMSETZUNGSNACHWEIS

Berechtigte Prüfungen, Ausnahmen und Eskalationsweg dokumentiert

390 Tage

Kommunikation bei Erpressung und unklarem Datenumfang üben

VERANTWORTLICHE

Vorfallleitung und Kommunikation

UMSETZUNGSNACHWEIS

Bestätigte Fakten, Unbekanntes, sicherer Kontakt und Aktualisierungszeit freigegeben

Korrekturen erneut testen und dienstabhängige Ausnahmen schließen

VERANTWORTLICHE

Kontroll- und Geschäftsverantwortliche

UMSETZUNGSNACHWEIS

Behebungsnachweis, Restrisiko und nächste Prüfung

Programmergebnisse mit der Leitung prüfen

VERANTWORTLICHE

CISO und verantwortliches Leitungsmitglied

UMSETZUNGSNACHWEIS

Offene Entscheidungen, Abschlussbelege und Ressourcen vereinbart

12.2 Identitäten und Vorfallreaktion

Beginnen Sie mit der Kontoverantwortung. Eine relevante Warnung sollte ein Team erreichen, das Kontoexistenz, Zugriffsrechte und fortbestehende Aktivität feststellen kann. Der Analyst sollte nicht erraten müssen, welcher Administrator den Dienst verantwortet.

Ist Missbrauch belegt, richten Sie die Eindämmung an tatsächlicher Identität und Sitzungen aus. Prüfen Sie gegebenenfalls Berechtigungen, Wiederherstellungsverfahren, Weiterleitungen und verbundene Anwendungen. Dokumentieren Sie abgeschlossene Schritte und weiterhin offene Belegfragen.

Sehen Sie einen sicheren Wiederherstellungsweg für berechtigte Nutzer vor. Eine breite Zurücksetzung ohne nutzbare Wiederherstellung kann unsichere Umgehungslösungen fördern. Der Support sollte eine Ausnahme überprüfen können, ohne allein auf das betroffene Konto zu vertrauen.

Abschluss bedeutet einen geprüften Fall mit Verantwortlichem, Zugriffsfeststellung und dokumentiertem Ergebnis. Eine leere Warnungswarteschlange genügt nicht, wenn betroffener Dienst oder Wiederherstellungsweg ungetestet bleiben.

12.3 Finanzen und Kundenschutz

Die Finanzabteilung sollte unabhängige Bestätigung einer geänderten Zahlungsanweisung nachweisen. Nummer oder Kanal müssen aus einem bereits vorhandenen Datensatz stammen. Eine zweite Freigabe derselben betrügerischen Nachricht ist nicht dieselbe Kontrolle.

Kundenteams sollten die echten Zahlungs- und Supportabläufe der Organisation kennen. Ihre Erklärung muss Menschen mit echten Buchungsdetails, vertrautem Absender oder einem scheinbaren Sicherheitsnotfall helfen.

Bieten Sie Eskalation für Menschen, die bereits Geld überwiesen, Fernsteuerungssoftware installiert oder Zugangsdaten geteilt haben. Der nächste Schritt kann zeitkritisch sein. Der Support sollte das zuständige berechtigte Zahlungs-, Identitäts- oder Vorfallteam erreichen, ohne gefährliches Material sammeln zu lassen.

Eine abgeschlossene Übung sollte die tatsächliche Übergabe und Entscheidung zeigen, auch außerhalb normaler Arbeitszeiten. Sie sollte außerdem zeigen, ob Beschäftigte Rückholgebührenbetrug verstehen und einen sicheren alternativen Kontakt nennen können.

12.4 Dienst- und Dienstleisterverantwortliche

Bestimmen Sie je kritischem Dienst die fortzuführende Funktion, Identitätsabhängigkeit und administrative Reichweite des Anbieters. Dokumentieren Sie Datenkategorien und rechtliche Rollen. Dienstleistername und jährlicher Vertragswert beantworten diese Fragen nicht.

Verlangen Sie dienstrelevante Vorfallbelege: betroffener Mandant, relevanter Zugriffszeitraum, Informationskategorien und Eindämmungsstand. Eine allgemeine Anbieteraktualisierung sollte als dessen Aussage erhalten bleiben. Erweitern Sie sie nicht zu einer eigenen Zusicherung.

Zeigen Sie einen Ersatzablauf unter einem benannten Ausfall. Das Ergebnis sollte belegen, dass Beschäftigte oder Kunden die wesentliche Aufgabe abschließen können. Es sollte auch die Wiederherstellung normaler Zugriffe und die Freigabeverantwortung zeigen.

Ein Abschluss kann eine nicht sofort behebbare Grenze aufdecken. Dokumentieren Sie Geschäftsfolge, Zwischenkontrolle und Prüfverantwortung. Eine ausdrückliche Grenze hilft mehr als eine unbelegt widerstandsfähig genannte Leistung.

12.5 Recht, Datenschutz und Kommunikation

Recht und Compliance sollten den rechtsträgerspezifischen Geltungsbereichsakt pflegen. Er braucht eine verantwortliche Person und Vertretung, nicht nur einen Gesetzeslink. Prüfen Sie ihn erneut, wenn Tätigkeit, Dienstleisterbeziehung oder Rechtskategorie sich ändern.

Dokumentieren Sie während eines Ereignisses die unterschiedlichen fristauslösenden Feststellungen. Entdeckung, Kenntnis und schwerwiegende Einstufung können zeitlich auseinanderfallen. Eine klare Chronologie unterstützt spätere Prüfung und verhindert, dass eine Übergabe frühere Entscheidungen verdeckt.

Die Kommunikation sollte Behauptung, bestätigten Zugriff, eingesehene Informationen und Dienststörung unterscheiden. Sagen Sie Menschen, was sie tun und wie sie die Nachricht überprüfen können. Erhalten Sie Quelle und Datum wiederholter Organisationszusicherungen oder offener Grenzen.

Abschlussbelege sind eine nutzbare erste Darstellung, eine begründete Meldeentscheidung und ein zugewiesener Aktualisierungsplan. Eine vollständig geklärte Zuschreibung ist nicht Voraussetzung für diese Vorbereitungen.

12.6 Leitung und Absicherung

Die Leitung sollte wenige Entscheidungen mit Belegen prüfen. Welche relevanten Konten bleiben ungeklärt? Welcher kritische Dienst hat einen ungetesteten Ersatzweg? Welcher Anbieter liefert keine eingegrenzten Vorfallinformationen? Welche Melderolle hat keine Vertretung?

Diese Fragen helfen mehr als eine aus Beiträgen abgeleitete nationale Risikorangfolge. Sie verbinden die zitierten Mechanismen mit Verantwortlichkeiten, die die Organisation ändern und nachweisen kann.

Das verantwortliche Leitungsmitglied sollte durch Übungen aufgedeckte Ressourcenkonflikte lösen. Die Sicherheit kann den akzeptablen Verlust eines Kundendienstes nicht einseitig bestimmen. Geschäftsverantwortliche sollten auch keine dringende Korrektur ohne Verständnis der Gefährdung erlassen.

12.7 Wie Brandefense helfen kann

Brandefense unterstützt Abläufe für Bedrohungsinformationen, digitale Risiken und externe Angriffsflächen. [S8] Gespeicherte Beiträge, Ransompedia-Einträge und datierte Beobachtungen begründen hier Prüfprioritäten. Sie ersetzen weder eigene Zugriffsbelege der Organisation noch gesetzliche Entscheidungen.

Eine hilfreiche Zusammenarbeit beginnt mit Ressourcen, Diensten und Entscheidungen, welche die Organisation schützen muss. Relevante externe Signale können anschließend Identitäts-, Dienst-, Betrugs- oder Vorfallverantwortlichen mit einer klaren Prüffrage zugewiesen werden.

Besprechen Sie die Ergebnisse dieses Berichts und einen organisationsspezifischen Prüfablauf mit Brandefense: https://brandefense.io/request-a-demo/ . Für die Zusammenarbeit sollten dieselben Beleggrenzen wie für den Bericht gelten.

KERNAUSSAGEN

01

Weisen Sie jede Maßnahme der Stelle zu, die sie überprüfen und abschließen kann.

02

Testen Sie Zahlungs-, Dienstleister- und Meldeübergaben zusammen mit technischer Eindämmung.

03

Schließen Sie Arbeiten mit Dienst- und Belegergebnissen ab und halten Sie Verantwortung für verbleibende Unsicherheit fest.

ANHÄNGE

Anhänge

A–D

DIESES KAPITEL BEANTWORTET

Welche Definitionen und Quellengrenzen stützen die Entscheidungen des Berichts?

4

Anhänge zu Umfang, Belegen, Quellen und Begriffen

Anhang A. Umfang, Quellen und Vertrauen 118

Anhang B. Belegregister 122

Anhang C. Quellen 125

Anhang D. Glossar 128

Anhang A. Umfang, Quellen und Vertrauen

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

A.1 Zeitraum und Bedeutung der Zeitangaben

Der Bericht umfasst Österreich vom 1. Januar bis 22. November 2026. Das jüngste Aktivitätsfenster ist der 8.–22. November. Untergrunddaten bezeichnen Veröffentlichungszeiten. Sie belegen nicht den Beginn eines Zugriffs, den Informationserwerb oder eine Transaktion. [S1]

Ransomware-Einträge verwenden die datierte Eintragspopulation innerhalb dieses angefragten Zeitraums. Die Vergleichsländer nutzen denselben Zeitraum. Ein Eintrag kann ein älteres Ereignis betreffen; sein Datum ist nicht automatisch ein Einbruchsdatum. [S2]

Verlinkte externe Quellen, NVD-Einträge und Behördenhinweise wurden am 27. November 2026 geprüft. Gespeicherte eigene Datenbestände und zurückgehaltene Primärmitteilungen tragen ihr jeweiliges Prüfdatum in Anhang C. Eine Prüfung nach dem 22. November verlängert den Berichtszeitraum nicht über den 22. November hinaus. Ein Jahresbericht über 2025 bleibt eine Population von 2025, auch bei Veröffentlichung im Jahr 2026.

Passive Beobachtungen bilden eine datierte Momentaufnahme vom 23.–27. November 2026. Sie beschreiben nicht jeden Tag des Berichtszeitraums. Der Bericht leitet aus der späteren Beobachtung keinen früheren Kontrollzustand ab. [S3]

A.2 Quellenpopulationen

Der Bericht verbindet die folgenden Belegarten, ohne sie zu einer nationalen Vorfallsumme zu addieren.

Quellenpopulation	Einheit	Wichtige Grenze
Von Odin by Brandefense gesammeltes Untergrundmaterial	Veröffentlichte Beiträge und Anzeigen	Behauptungen, Wiederholungen und Länderbezüge belegen keine unabhängigen Vorfälle
Ransompedia	Datierte Erpressungseinträge	Kriminelle Aussagen; wiederholte Organisationen und unsichere Länderkennzeichnungen sind möglich
Ausgewähltes Domainportfolio	Domain und zugehöriger Dienst	Verbundene Gruppen und ungeklärte rechtliche Eigentümerschaft begrenzen Organisationsinterpretation
Passive DNS- und TLS-Beobachtungen	Datierte Kontrollbeobachtung	Teilansicht eines Dienstes; unbeobachtet bedeutet nicht automatisch fehlend
Amtliche Mitteilungen	Von der Quelle bestätigte Fakten innerhalb einer Aussage	Akteur, Datensatzzahl und vollständiger Umfang können ungeklärt bleiben

Quellenpopulation	Einheit	Wichtige Grenze
Kampagnenhinweise	Von der Behörde beschriebener Ablauf oder Kampagne	Keine vollständige nationale Opferzahl abgeleitet
Polizei- oder Aufsichtsstatistiken	Definierte Meldungen oder Fälle im Quellenzeitraum	Verschiedene Kategorien, Jahre und Überschneidungen verhindern einfache Addition

Die Quellen [S1][S2][S3][S6] definieren die eigenen Datenpopulationen des Berichts. Anhang C nennt die externen Hinweise für Kontext und Falleinordnung.

A.3 Ausgewähltes Portfolio und gemessene Abdeckung

Das Portfolio umfasst 250 ausgewählte Domains aus zehn Branchengruppen. Es ist weder Umsatzrangliste, Zufallsstichprobe noch national repräsentative Erhebung. Eine ausgewählte Domain belegt nicht für jeden vertretenen Dienst eine unabhängige rechtliche Identität oder überprüfte Eigentümerschaft. [S6]

Passive Beobachtungen umfassen alle 250 ausgewählten Domains (Momentaufnahme vom 23.–27. November). Insgesamt veröffentlichen 149 Domains (59,6%) durchgesetzte DMARC-Richtlinien und 239 (95,6%) SPF. Gültiges TLS zeigt sich bei 240 Domains (96,0%; 6 erfolglos und 4 nicht verfügbar), und HSTS erscheint bei 184 von 247 erfassten HTTP-Antworten (3 nicht verfügbar). Jede Kontrolle behält ihren gemessenen Nenner, und es werden weder Hygienewerte noch Branchenrangfolgen veröffentlicht. [S3]

Expositionsbeobachtungen umfassen am 23. November 249 von 250 ausgewählten Domains; für eine fehlt ein vollständiger Datensatz. 49 beobachtete Domains (19,7%) haben ein aktuelles Zugangsdatenangebot. Der nationale Atlas-Gesamtwert beträgt 47/100 (B) für das beobachtete ausgewählte Portfolio. Fehlende Mengen bleiben unbekannt; Branchenwerte werden nicht veröffentlicht. [S4]

Beobachtungen ähnlicher Namen umfassen den 19. Oktober–18. November. Rollierende Nachrichtenzuordnungen umfassen 365 Tage bis 22. November über alle 250 ausgewählten Domains, wobei die Teilmenge für 2026 gesondert ausgewiesen wird. Geräte-, Zugangsdaten- und Dokumentenzuordnungen können sich über Domains, Quellen und Personen überschneiden. Ihre Summen messen weder eindeutige Personen oder bestätigte Einbrüche noch nationale Häufigkeit. [S4]

A.4 Ransomware und Vergleichseinordnung

Ransompedia erfasst 61 österreichische Einträge über 56 eindeutige Einrichtungsnamen im angefragten Zeitraum (vier Einrichtungen erscheinen mehr als einmal, was fünf Wiederholungseinträge ausmacht). Die 38 Einträge für das gesamte Jahr 2025 sind ein Ganzjahresrückblick, kein Vergleich gleicher Zeiträume. Gruppen- und Branchenbezeichnungen beschreiben diese Eintragspopulation. [S2]

Die Vergleichswerte beschreiben getrennte nationale Eintrags- und Untergrundbeitragspopulationen. Sie sind nicht für Bevölkerung, Wirtschaftsstruktur, Organisationsgröße oder Sichtbarkeit bereinigt. Daraus werden weder Angriffswahrscheinlichkeit oder politische Bewertung noch eine Rangfolge der Kontrollwirksamkeit abgeleitet.

A.5 Kartenmaterial hat einen eigenen engen Umfang

UMFANG DER KARTENANGABEN

Kartenzahlen betreffen nur Zahlungskarten, die in den für diesen Bericht gesammelten Dark-Web-Beiträgen im Klartext erschienen. Brandefense erkennt gestohlene Karten auch mit anderen Methoden außerhalb dieses Ausschnitts. Die Zahlen messen weder gesamten Diebstahl noch gültige Karten, abgeschlossene Zahlungen oder Betrugsschäden.

Die Population von 88 Karten stammt aus 100 nach Ländern gekennzeichneten Beiträgen und bleibt auf diesen engen Ausschnitt begrenzt. [S5]

Eine Kartenbeobachtung im Beitrag unterscheidet sich von einer Herausgeberbestätigung, einem gültigen Konto und einer betrügerischen Transaktion. Maßnahmen des Herausgebers brauchen eine berechtigte Prüfung von Relevanz, Aktualität, früherer Behebung und tatsächlichem Missbrauch. Der Bericht rechnet dieses Material nicht auf das Land hoch. [S5]

A.6 Öffentliche Berichte und verbleibende Abdeckungsgrenzen

Die amtliche Quellenprüfung berücksichtigt Kampagnenveröffentlichungen ebenso wie Organisationsmitteilungen. Sie unterscheidet aktuelle Ereignisse, rückblickende Statistiken, Präventionswarnungen, Übungen und unverbundene physische Ausfälle. Eine Quelle ohne veröffentlichte Monatsmitteilung belegt keinen vorfallfreien Monat.

Die geprüften Archive von BK, BMI und DSN umfassen das angefragte Kalenderfenster. Amtliche Seiten für NISG-2026-Bestimmungen, BCS-Rechtshinweise, BMI-Registrierungsinformationen, DSB-Meldehinweise und FMA-DORA-Hinweise wurden am 27. November geprüft. Die öffentliche Bekanntmachungsseite der DSB (20. Juli–19. November 2026, geprüft am 27. November) enthält keine Zwischenstatistiken zu Sicherheitsverletzungen für 2026, sodass der Tätigkeitsbericht 2025 die jüngste veröffentlichte Basislinie bleibt. Die FMA veröffentlicht kein chronologisches öffentliches Nachrichtenarchiv; die Abdeckung von FMA-Mitteilungen für Februar–Mai 2026 ist daher unvollständig. Daraus wird keine vollständige nationale Vorfallmeldeerhebung für 2026 abgeleitet. [S30] [S31][S38][S39][S40][S54][S64]

Ein Pressebericht mit amtlicher Aussage wird als solche Belegform gekennzeichnet. War eine Originalaussendung nicht verfügbar, behauptet der Bericht nicht, sie gelesen zu haben. Ein negativer Quellenbefund behält Datum und genannten Umfang.

A.7 Vertrauen und alternative Erklärungen

Belegaussage	Vertrauenssprache	Was getrennt bleibt
Eine gespeicherte Nachricht oder ein Eintrag existiert	Hoch für die Beobachtung	Echtheit und Wahrheit der zugrunde liegenden Aussage
Eine amtliche Mitteilung bestätigt bestimmten Zugriff	Hoch für die genannte Bestätigung	Ungeklärte Datensatzzahlen, Akteur und weitergehende Systemreichweite
Eine Quelle bewertet eine Kampagnen-beziehung	Bewertung und Unsicherheit der Quelle zuordnen	Identität jedes Beteiligten oder Anwend-barkeit auf jeden Fall
Ein Abwehrszenario folgt aus Mechanis-men	Bedingte Planungsannahme	Wahrscheinlichkeit oder vorhergesagter Schaden
Ein Beitrag oder Datenbestand ähnelt einem anderen	Zuordnung mit genannter Grenze	Gemeinsamer Betreiber, identische Datei oder abgeschlossene Übertragung

Alternative Erklärungen sind wichtig, weil sie die Eindämmung verändern können. Historische Datensätze, kopierte Werbung, verbundene Rechtsträger und legitime Dienstnutzung können die Einordnung beeinflussen. Ihre Möglichkeit widerlegt keine Behauptung; sie benennt die noch erforderlichen Belege.

A.8 Namensnennung, technische Details und politische Neutralität

Opfer werden über breite Rollen beschrieben, sofern die Namensanforderungen nicht erfüllt sind. Daten, regionale Herausgeber-Wurzeladressen und enge Beschreibungen werden verallgemeinert, wenn ihre Kombination eine zurückgehaltene Organisation indirekt identifizieren könnte. Quelleinträge lassen die eigene Domain einer zurückgehaltenen Organisation aus. Die nationale Wurzeladresse eines Presse- oder amtlichen Herausgebers kann eine identifizierende Artikeladresse mit Vermerk der Zurückhaltung ersetzen.

Der Bericht veröffentlicht weder Zugangsdaten, personenbezogene Datensätze, Kartennummern, kriminelle Kontaktwege noch operative Angriffsanleitungen. Technische Warnungen unterstützen die defensive Produkt- und Konfigurationsprüfung. Sie geben kein Ausnutzungsverfahren wieder.

Politische Behauptungen bleiben gegebenenfalls ihrer Quelle zugeordnet. Die Autoren beziehen keine Position zu Regierungsentscheidungen, Parteien, Wahlen, Neutralität oder internationalen Konflikten. Sprache, behaupteter Anlass und ein öffentliches Ziel belegen weder Nationalität noch Unterstützung.

Anhang B. Belegregister

Das Register verbindet Falldarstellungen mit ihren öffentlichen Quellenverweisen. Ein Kampagneneintrag zählt keine unabhängigen Opfer. Fälle zurückgehaltener Organisationen verwenden Jahres-, Saison- oder Monatsangaben, um indirekte Identifizierung zu verhindern. Buchstabe und Belegkennung benennen die Darstellung, nicht ihr Vertrauen.

Beleg	Datum	Art	Fall und Abschnitt	Quellen
O01	Anfang 2026	Institutionsmitteilung und Aktualisierungen	A · §5.2	S25
O02	Anfang 2026	Institutionsmitteilung zu Ransomware und Umfang	B · §5.2	S58
O03	2026-04-01	Polizeiliche Kampagnenwarnung	C · §5.3	S18
O04	2026-04-07	Polizeiliche Kampagnenwarnung	D · §5.3	S17, S16
O05	2026-04-29	Polizeiliche Untersuchungsdarstellung	E · §5.3	S19
O06	2026-05-26	CERT-Kampagnenbewertung	F · §5.4	S9
O07	2026	Sprecherdarstellung in der Presse	G · §5.4	S26
O08	2026-07-24	CERT-Kampagnenwarnung	H · §5.4	S10
O09	2026-08-14	CERT-Kampagnenwarnung	I · §5.4	S11
O10	2026-08-26	CERT-Kampagnenwarnung	J · §5.4	S12
O11	2026-10-29	Polizeiliche Kampagnenwarnung	K · §5.5	S20
O12	Herbst 2026	Unternehmensdarstellung in der Presse	L · §5.5	S27
O13	November 2026	Dienstleistermitteilung und Aktualisierungen	M · §5.5	S28
O14	November 2026	Mitteilung einer öffentlichen Stelle in der Presse	N · §5.5	S29

Beleg	Datum	Art	Fall und Abschnitt	Quellen
O15	November 2026	In der Presse zitierte Umfangsaktualisierung	O · §5.5	S55
O16	November 2026	Unternehmensdarstellung in der Presse	P · §5.5	S56
O17	Herbst 2026	Betreibermitteilung zu zwei Dienstleistererereignissen	Q · §5.5	S57

Die Karten gespeicherter Beiträge erhalten geschwärzte Quellenauszüge. Plattformen werden nach Art beschrieben. Private Verkäuferpseudonyme und Kontaktwege werden zurückgehalten; ausgewählte öffentliche Akteursbezeichnungen bleiben erhalten. Die Tabelle identifiziert keine unabhängigen menschlichen Betreiber.

Beleg	Datum	Ort und Sprache	Fall und Abschnitt	Quelle
B01	2026-01-08	Forum; Englisch	U · §4.4	S1
B02	2026-01-27	Forum; Englisch	U · §4.4	S1
B03	2026-02-01	Forum; Russisch und Englisch	V · §4.4	S1
B04	2026-02-02	Forum; Englisch	W · §4.4	S1
B05	2026-04-11	Forum; Englisch	§4.5	S1
B06	2026-04-18	Forum; Englisch	X · §4.4	S1
B07	2026-09-22	Forum; Englisch	Y · §4.4	S1
B08	2026-10-15	Forum; Englisch	Y · §4.4	S1
B09	2026-11-20	Forum; Englisch	Z · §4.4	S1
B10	2026-11-22	Forum; Englisch	Z · §4.4	S1
B11	2026-06-21	Forum; Russisch	§8.5	S1
B12	2026-10-20	Forum; Englisch	§8.5	S1
B13	2026-05-08	Quelle auf einer Chatplattform; Englisch	§6.2	S1
B14	2026-05-17	Quelle auf einer Chatplattform; Englisch	§6.2	S1
B15	2026-05-08	Weitergegebene Behauptung; Englisch	§6.2	S1

Beleg	Datum	Ort und Sprache	Fall und Abschnitt	Quelle
B16	2026-03-26	Quelle auf einer Chat-plattform; Arabisch und Englisch	§6.2	S1
B17	Mai 2026	Quelle auf einer Chat-plattform; Englisch	§6.2	S1
B18	Mai 2026	Übersichtsweitergabe; Russisch	§6.3	S1
B19	2026 (Datum unge-klärt)	Forum; Englisch	§4.5	S1
B20	2026-11-18	Quelle auf einer Chat-plattform; Englisch	§4.6	S1

Anhang C. Quellen

Die folgenden Einträge nennen die für diesen Bericht genutzten Quellen und das jeweilige Prüfdatum. Verlinkte externe Quellen, NVD-Einträge und passive Beobachtungen wurden am 27. November 2026 geprüft. Eine Prüfung nach dem 22. November verlängert den Berichtszeitraum nicht über den 22. November hinaus. Eine zurückgehaltene Artikeladresse oder leere Opferadresse schützt die Organisation, ohne den Belegstatus der Quelle zu ändern.

S1: Odin by Brandefense. Untergrundnachrichten mit Österreichbezug. Gespeicherte eigene Belege; Quellenaufzeichnungen sind privat. Geprüft am 23. November 2026.

S2: Ransompedia. Erpressungseinträge für Österreich und regionale Vergleichsländer. Gespeicherte eigene Belege; Quellenaufzeichnungen sind privat. Geprüft am 23. November 2026.

S3: Odin by Brandefense. Passive Kontrollbeobachtungen über alle 250 ausgewählten Domains (Momentaufnahme vom 23.–27. November 2026). Gespeicherte eigene Belege; Quellenaufzeichnungen sind privat. Geprüft am 27. November 2026.

S4: Brandefense Atlas und Odin by Brandefense. Expositionsbeobachtungen ausgewählter Domains vom 23. November 2026 mit den im Bericht genannten quellenspezifischen Zeiträumen. Gespeicherte eigene Belege; Kennungen bleiben privat. Geprüft am 23. November 2026.

S5: Odin by Brandefense. Nach Ländern gekennzeichnete Zahlungskartenbeobachtungen in Beiträgen. Gespeicherte eigene Belege; Quellenaufzeichnungen sind privat. Geprüft am 23. November 2026.

S6: Odin by Brandefense. Ausgewähltes österreichisches Domainportfolio. Gespeicherte eigene Belege; Quellenaufzeichnungen sind privat. Geprüft am 27. November 2026.

S7: NIST National Vulnerability Database. Ausgewählte Schwachstelleneinträge: CVE-2026-114938; CVE-2026-129289; CVE-2026-115560; CVE-2026-86218; CVE-2026-41940. Geprüft am 27. November 2026.

S8: Brandefense. Fähigkeiten für Bedrohungsinformationen, digitale Risiken und Angriffsflächen. https://brandefense.io/request-a-demo/ Geprüft am 27. November 2026.

S9: CERT.at. Bewerbungsköderkampagne und von der Quelle bewertete Zugangsbeziehung. https://www.cert.at/de/aktuelles/2026/5/zipline-qilin-raas-update. Geprüft am 27. November 2026.

S10: CERT.at. Phishing über berechtigte österreichische Geschäfts-E-Mail-Konten. https://www.cert.at/de/aktuelles/2026/7/vermehrt-phishing-mails-von-legitimen-e-mail-adressen-aus-osterreich. Geprüft am 27. November 2026.

S11: CERT.at. Betrug im Zusammenhang mit Reisebuchungsplattformen. https://www.cert.at/de/aktuelles/2026/8/vermehrt-betrugsversuche-auf-buchungsplattformen-bookingcom. Geprüft am 27. November 2026.

S12: CERT.at. Vermehrte Betrugsversuche über geschäftliche E-Mail-Korrespondenz. https://www.cert.at/de/aktuelles/2026/8/vermehrt-betrugsversuche-durch-business-email-compromise-bec. Geprüft am 27. November 2026.

S13: CERT.at. Brandbedingte Glasfaserunterbrechung. https://www.cert.at/de/aktuelles/2026/6/brand-der-floridsdorfer-brucke-glasfaserausfalle-in-wien. Geprüft am 27. November 2026.

S14: GovCERT. Zuständigkeit für die öffentliche Verwaltung. https://www.govcert.gv.at/en/. Geprüft am 27. November 2026.

S15: Bundeskriminalamt. Cybercrime Report 2025: amtlicher Rückblick. https://www.bundeskriminalamt.at/newsb0e5.html?id=42307473384354634638 6f3d. Geprüft am 27. November 2026.

S16: Bundeskriminalamt. Phishing-Prävention im Oktober, Fallkontext 2025–2026 und OeNB-/RTR-Aussagen. https://www.bundeskriminalamt.at/newsdb49.html?id=654461744b54696b6d66453d. Geprüft am 27. November 2026.

S17: Bundeskriminalamt. Warnung vor Imitation bei der Verlängerung digitaler Identitäten. https://www.bundeskriminalamt.at/news7481.html?id=6f45367243466c735631633d. Geprüft am 27. November 2026.

S18: Bundeskriminalamt. SMS mit Bankbezug und falsche Supportanrufe. https://www.bundeskriminalamt.at/newsea73.html?id=687574376f3455315132733d. Geprüft am 27. November 2026.

S19: Bundeskriminalamt. Untersuchung zu Anlage- und Rückholbetrug. https://www.bundeskriminalamt.at/newsb7b9.html?id=6d4b6c4b525341374c7a633d. Geprüft am 27. November 2026.

S20: Bundeskriminalamt. Aufgaben- und Stellenbetrug über soziale Medien. https://www.bundeskriminalamt.at/newsd00f.html?id=74776d6a304e646536346f3d. Geprüft am 27. November 2026.

S21: Bundeskriminalamt. Rückblick auf Operation TorNado. https://www.bundeskriminalamt.at/news3d42.html?id=446763694e4c42574733383d. Geprüft am 27. November 2026.

S22: Bundeskriminalamt. Internationale Operation gegen einen Proxy-Dienst. https://www.bundeskriminalamt.at/newsb165.html?id=426e%342784932736949683 43d. Geprüft am 27. November 2026.

S23: Bundesministerium für Finanzen. Betrügerische Zahlungserinnerungen und amtlich wirkende Mitteilungen. https://www.bmf.gv.at/presse/pressemeldungen/2026/jaenner-2026/email-phishing.html. Geprüft am 27. November 2026.

S24: Bundesministerium für Finanzen. Betrügerische Nachrichten, Anrufe und imitierte Dienstwebsites. https://www.bmf.gv.at/presse/pressemeldungen/2026/februar-2026/phishing.html. Geprüft am 27. November 2026.

S25: Bildungseinrichtung. Mitteilung zu Verzeichniszugriff und Aktualisierungen (Anfang 2026). URL zum Schutz der Organisation zurückgehalten. Geprüft am 23. November 2026.

S26: Heute. Offenlegung von Postfachdokumenten (2026). https://www.heute.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S27: ORF. Projektorganisation: Cybervorfall im Herbst 2026. https://orf.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S28: Kommerzieller Software- und Hosting-Dienstleister. Aktualisierungen zum Vorfall in gehosteter Infrastruktur (November 2026). URL zum Schutz der Organisation zurückgehalten. Geprüft am 23. November 2026.

S29: ORF. Mitteilung einer öffentlichen Stelle zu einer extern betriebenen Website (November 2026). https://orf.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S30: Bundesamt für Cybersicherheit. Inkrafttreten des NISG 2026 und amtliche Rechts-FAQ. https://www.bundesamt-cybersicherheit.gv.at/faq/gesetzgebung.html. Geprüft am 27. November 2026.

S31: RIS. NISG 2026 § 24: Geltungsbereich und Ausnahmen. https://ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273885/NOR40273885.html. Geprüft am 27. November 2026.

S32: RIS. NISG 2026 § 34: Meldepflichten. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273895/NOR40273895.html. Geprüft am 27. November 2026.

S33: RIS. NISG 2026 § 29: Einrichtungsregister. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273890/NOR40273890.html. Geprüft am 27. November 2026.

S34: RIS. NISG 2026 § 31: Leitungspflichten. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273892/NOR40273892.html. Geprüft am 27. November 2026.

S35: RIS. NISG 2026 § 32: Risikomanagementmaßnahmen. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273893/NOR40273893.html. Geprüft am 27. November 2026.

S36: RIS. NISG 2026 § 44: Allgemeine Strafbestimmungen und kein Kumulieren mit DSGVO-Geldbußen. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273905/NOR40273905.html. Geprüft am 27. November 2026.

S37: RIS. NISG 2026 § 45: Verwaltungsstrafen. https://www.ris.bka.gv.at/Dokumente/Bundesnormen/NOR40273906/NOR40273906.html. Geprüft am 27. November 2026.

S38: Datenschutzbehörde. Hinweise zur Meldung einer Verletzung des Schutzes personenbezogener Daten. https://dsb.gv.at/eingabe-an-die-dsb/-meldung-data-breach. Geprüft am 27. November 2026.

S39: Datenschutzbehörde. Tätigkeitsbericht 2025: Meldungen von Sicherheitsverletzungen. https://dsb.gv.at/sites/site0344/media/downloads/taetigkeitsbericht_2025_v4.pdf. Geprüft am 27. November 2026.

S40: FMA. DORA: IKT-bezogene Vorfälle. https://www.fma.gv.at/querschnittsthemen/dora/dora-ikt-bezogene-vorfaelle/. Geprüft am 27. November 2026.

S41: FMA. Amtlicher Rückblick auf Betrugstrends im Jahr 2025. https://www.fma.gv.at/deepfakes-whatsapp-gruppen-und-ki-bots-waren-die-trends-des-jahres-2025/. Geprüft am 27. November 2026.

S42: FMA. DORA-Aufsichtsaktivitäten. https://www.fma.gv.at/querschnittsthemen/dora/fma-aktivitaeten-zu-dora/. Geprüft am 27. November 2026.

S43: DSN. Mitteilung zur Sicherheitsbewertung für 2025. https://www.dsn.gv.at/news4c8c.html?id=51326d6a3669786c3674773d. Geprüft am 27. November 2026.

S44: CERT.at. Java4Shell-Hinweis und korrigierte Versionen. https://www.cert.at/de/warnungen/2026/11/kritische-sicherheitslucke-in-java-java4shell-updates-verfugbar-cve-2026-114938. Geprüft am 27. November 2026.

S45: CERT.at. PHP-Sicherheitskorrekturen und Konfigurationsbedingungen. https://www.cert.at/de/warnungen/2026/11/kritische-sicherheitslucken-in-php-updates-verfugbar2. Geprüft am 27. November 2026.

S46: CERT.at. Warnung vor aktiver N-central-Ausnutzung. https://www.cert.at/de/aktuelles/2026/9/schwerwiegende-sicherheitslucke-in-n-able-n-central-aktiv-ausgenutzt. Geprüft am 27. November 2026.

S47: CERT.at. Warnung vor aktiver Ausnutzung im Hosting-Management. https://www.cert.at/de/aktuelles/2026/4/aktive-ausnutzung-einer-schwerwiegenden-sicherheitslucke-in-cpanel-und-whm. Geprüft am 27. November 2026.

S48: BMI. Nationale Reaktion auf die NGINX-Warnung. https://www.bmi.gv.at/news9983.html?id=4d506163634349312b716f3d. Geprüft am 27. November 2026.

S49: BMI. Cybersicherheitsbehörde übernimmt veröffentlichte Zuständigkeiten. https://www.bmi.gv.at/news84e1.html?id=766f584a777255376d66513d. Geprüft am 27. November 2026.

S50: FMA. DORA: allgemeine Fragen zur Anwendbarkeit. https://www.fma.gv.at/querschnittsthemen/dora/dora-allgemeine-fragen/. Geprüft am 27. November 2026.

S51: Bundeskriminalamt. Präventionshinweis zu Romance Scam. https://www.bundeskriminalamt.at/newsb89e.html?id=694a5669486857434163383d. Geprüft am 27. November 2026.

S52: Bundeskriminalamt. Saisonale Warnung vor Online-Einkaufsbetrug. https://www.bundeskriminalamt.at/newsbb44.html?id=725a476d7a5342547269553d. Geprüft am 27. November 2026.

S53: ORF. Cyberübung zur Gesundheitslogistik (Mai 2026). https://orf.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S54: BMI. NISG 2026: Rahmen, Registrierung und Meldung. https://www.bmi.gv.at/504/. Geprüft am 27. November 2026.

S55: ORF. Aktualisierung einer Verwaltungsstelle zu einem früheren Datenvorfall 2026. https://orf.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S56: ORF. Dienstleisterereignis bei einem Beherbergungsbetreiber und Warnung vor Zahlungstäuschung gegen Gäste (November 2026). https://orf.at/ (Artikeladresse zurückgehalten). Geprüft am 27. November 2026.

S57: Beherbergungsbetreiber. Mitteilung zu zwei getrennten Dienstleistervorfällen (Herbst 2026). URL zum Schutz der Organisation zurückgehalten. Geprüft am 23. November 2026.

S58: Bildungseinrichtung. Mitteilung zu Ransomware und ungeklärtem Datenumfang (Anfang 2026). URL zum Schutz der Organisation zurückgehalten. Geprüft am 23. November 2026.

S59: Europäische Kommission / EUR-Lex. Delegierte Verordnung 2025/301, Artikel 5: Vorfallmeldefristen. https://eur-lex.europa.eu/eli/reg_del/2025/301/oj/eng. Geprüft am 27. November 2026.

S60: NIST. Begriffe OTP, ICS und ICT sowie Hinweise zur Authentifizierung mit Einmalcodes. 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. Geprüft am 27. November 2026.

S61: PHP. Handbuch zum FastCGI Process Manager. https://www.php.net/manual/en/book.fpm.php. Geprüft am 27. November 2026.

S62: Bundesverband deutscher Banken. Onlinebanking mit PIN und TAN: Auftragsfreigabe. https://bankenverband.de/verbraucher/onlinebanking-sicher-mit-pin-und-tan. Geprüft am 27. November 2026.

S63: DataReportal. Digital 2026: Austria (veröffentlicht am 8. November 2025; Nutzungskontext von Ende 2025). https://datareportal.com/reports/digital-2026-austria. Geprüft am 27. November 2026.

S64: Datenschutzbehörde. Öffentliche Bekanntmachungen der Datenschutzbehörde. https://dsb.gv.at/aktuelles. Geprüft am 27. November 2026.

Anhang D. Glossar

Die Definitionen unterstützen die Einordnung des Berichts. Sie behaupten nicht den Einsatz jeder Technik in einem österreichischen Fall.

Begriff	Einfache Definition
Kontositzung	Fortlaufende authentifizierte Interaktion, die auch nach einer Passwortänderung relevant bleiben kann
Administratives Verzeichnis	Dienst mit Identitäten und Berechtigungen zur systemübergreifenden Zugriffsverwaltung
BEC	Business Email Compromise: Täuschung über geschäftliche Identität oder Korrespondenz zur Erlangung von Geld oder Informationen
CAA	Certification Authority Authorization: DNS-Eintrag, der festlegt, welche Zertifizierungsstellen Zertifikate für eine Domain ausstellen dürfen
Behauptung	Aussage, deren zugrunde liegendes Ereignis nicht allein durch ihre Veröffentlichung belegt ist
Zugangsdatenaufzeichnung	Erfasste Authentifizierungsinformation; ihr Vorhandensein belegt keine aktuelle Gültigkeit
CSIRT	Team zur Koordination oder Unterstützung der Reaktion auf Computersicherheitsvorfälle
DMARC	Domainrichtlinie, die E-Mail-Authentifizierungsergebnisse mit gewünschter Behandlung und Berichterstattung verbindet
DKIM	Verfahren zur Signatur von E-Mails durch einen versendenden Dienst für die Prüfung durch Empfänger
DORA	EU-Rahmen für digitale operationale Resilienz im Finanzsektor mit definiertem Einrichtungsumfang und IKT-Pflichten
DS-Eintrag	DNS-Delegationseintrag im Zusammenhang mit DNSSEC; seine Beobachtung ist keine vollständige Vertrauenskettenprüfung
DDoS	Datenverkehr zur Überlastung der Dienstverfügbarkeit; eine Behauptung braucht eine Auswirkungsprüfung
FPM	FastCGI Process Manager: PHP-Software zur Verwaltung der Prozesse, die Webanfragen über FastCGI bearbeiten [S61]
HSTS	Webrichtlinie, die unterstützte Browser zur sicheren Übertragung für den erfassten Dienst anweist
ICS	Industrial Control System, industrielles Steuerungssystem: System zur Steuerung industrieller Prozesse [S60]

Begriff	Einfache Definition
IKT / ICT	Informations- und Kommunikationstechnologie, englisch Information and Communication Technology: Technik zum Verarbeiten, Speichern und Austauschen von Informationen [S60]
Identitätswiederherstellung	Prozess zur Wiederherstellung berechtigten Kontozugriffs durch vertrauenswürdige Prüfung
Eintrag	Öffentlicher erpressungsbezogener Eintrag; er dokumentiert eine kriminelle Aussage, kein bestätigtes Ergebnis
MFA	Authentifizierung mit mehr als einer Faktorart; Umsetzung und Wiederherstellungswege sind entscheidend
NISG 2026	Österreichisches Netz- und Informationssystemsicherheitsgesetz 2026 mit definierten Sicherheits- und Meldepflichten
OTP	One-Time Password, Einmalpasswort: Authentifizierungscode, der während seiner Gültigkeit nur einmal akzeptiert wird [S60]
Persona	Öffentlich auftretendes Konto oder Pseudonym; nicht zwingend eine unabhängig identifizierte Person
Phishing	Täuschende Kommunikation zur Veranlassung unsicherer Offenlegung oder Handlungen
Ransomware	Mit Erpressung verbundene Schadsoftware, oft durch Störung oder Verschlüsselung; ein Eintrag allein belegt ihren Einsatz nicht
SPF	E-Mail-Domaineintrag zur Kennzeichnung berechtigter Versandinfrastruktur
Dienstleisterumfang	Die in einer Dienstleisterbeziehung konkret betroffenen Dienste, Mandanten, Daten und Zeiträume
TAN	Transaktionsnummer, englisch Transaction Authentication Number: Einmalcode zur Freigabe eines Onlinebanking-Auftrags [S62]
Mandant	Logisch getrennte Kundenumgebung innerhalb eines gemeinsamen Dienstes
TLS	Protokoll zur sicheren Übertragung; eine gültige Beobachtung belegt keine Anwendungsberechtigung

Über diesen Bericht

Dieser Bericht unterstützt Entscheidungen von Sicherheitsleitung, Vorfallreaktion, Infrastruktur, Betrugsabwehr, Datenschutz und Kundenbetreuung. Er ist öffentliche Forschung von Odin by Brandefense mit ausdrücklichen Belegkennzeichnungen und quellenspezifischen Grenzen.

Die ausgewählten Fälle und Beobachtungen erfassen nicht jeden österreichischen Vorfall oder jede betroffene Person. Sichtbare Beiträge und Einträge eines Landes sind kein nationaler Risikowert. Betriebliche und Meldeentscheidungen brauchen eigene Organisationsfakten und fachkundige Beratung.

Die englische Masterfassung ist die Referenzausgabe. Übersetzungen erhalten ihre Zahlen, Belegkennungen, Quellenverweise und Direktiven und tragen einen sichtbaren Hinweis auf KI-Übersetzung.

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