BRANDEFENSE COUNTRY REPORT · SWITZERLAND 2026

Brandefense Schweiz Bericht zur Cyberbedrohungslage 2026

Identitätsmissbrauch, Vorfälle bei Dienstleistern und Wiederherstellung in verbundenen Diensten

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

49 von 250
Organisationen mit zum Prüfzeitpunkt angebotenen Zugangsdaten

5
Fallstudien, die angebotene Daten von verifizierten Vorfällen trennen

97000
Bewilligungsdatensätze, keine Personenzahl

41
Gruppenbezeichnungen in der Schweizer Ransomware-Momentaufnahme

INHALT

Inhalt

Translated with AI

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

01	Zusammenfassung	04
	Berichtsübersicht	09
	Inhalt und Lesewege	10
02	Der digitale Kontext und die Bedrohungslage der Schweiz	11
03	Nationale Exposition: die ausgewählte Organisationsgrundgesamtheit	17
04	Darkweb-Angebote und die Grenzen ihrer Belege	25
05	Beispiele für Zielauswahl nach Sektor	41
06	Hacktivismus und DDoS	57
07	Bedrohungsakteure und belegte Beziehungen	62
08	Die Betrugsökonomie: Identität, Vertrauen und Zahlung	74
09	Vertiefung zum Bankwesen	79
10	Regulatorische und nationale Reaktion	83
11	Ausblick	89
12	Massnahmenplan	94
	Anhänge	100
A	Anhang A. Umfang, Quellen und Vertrauensgrad	101
B	Anhang B. Belegregister	104
C	Anhang C. Quellen	106
D	Anhang D. Glossar	111
	Über diesen Bericht	113

Verwaltungsrat und CISO	01 05 11 12
SOC und Vorfallbehandlung	04 06 07 12
Identität und Infrastruktur	03 05 07 12
Betrugsbekämpfung und Bankwesen	08 09 12
Recht und Beschaffung	05 10 12

Über diese Ausgabe

Mit KI übersetzt. Bei Abweichungen ist die englische Fassung massgeblich.

KI-gestützte Recherche und Redaktion. Kriminelle Behauptungen, offizielle Darstellungen und analytische Einordnungen bleiben getrennt. Anhang A erläutert Umfang und Vertrauensgrad.

Die Schweizer Befunde sprechen für gemeinsame Investitionen in Identitätskontrollen, Meldungen von Dienstleistern und erprobte Wiederherstellung. Dabei bleiben Untergrundangebote von bestätigten Vorfällen getrennt.

122

Schweizer Ransomware-Listungen im Berichtszeitraum

250

ausgewählte Organisationskandidaten aus dreizehn Sektoren

48 / 100

nationale Atlas-Kennzahl für 247 geprüfte Organisationskandidaten; höhere Werte bedeuten eine stärkere beobachtete Exposition

4

Entscheidungen mit benannten Verantwortlichen und Abschlussnachweisen

KAPITEL 01

Zusammenfassung

01

DIESES KAPITEL BEANTWORTET

Welche Sicherheitsentscheidungen stützen die Schweizer Belege?

4

Entscheidungen mit klarer Verantwortung und Abschlussnachweisen

Vier Entscheidungen für Führungskräfte 07

Das Jahr in Zahlen 07

KAPITEL 01

Zusammenfassung

KURZFASSUNG

Die Schweizer Belege verbinden Identitätsmissbrauch, Dienstleistervorfälle und Wiederherstellungsrisiken. Ransompedia erfasst 122 Schweizer Listungen im Berichtszeitraum. Zugangsdaten mit Bezug zu 49 von 250 ausgewählten Organisationen wurden zum Prüfzeitpunkt angeboten. Die nationale Atlas-Kennzahl beträgt 48 von 100 für 247 geprüfte Kandidaten. Offizielle Meldungen behalten Unsicherheiten zu Dienstfolgen und Daten bei. Priorität haben Kontoprüfung, Dienstleistermeldungen, unabhängige Wiederherstellung und Kommunikation auf Grundlage gesicherter Fakten.

Dieser Bericht verbindet Beitragsbelege aus Brandefense Blackhole, Ransompedia-Listungen, Atlas-Expositionsbeobachtungen und passive Prüfungen mit quellengeprüften öffentlichen Berichten. Jede Grundgesamtheit beantwortet eine andere Frage. Beiträge und Listungen zählen keine bestätigten Einbrüche. Die ausgewählten Organisationen bilden keine landesweite Verbreitung ab [S1][S2][S3].

1. Erpressungslistungen unterstützen die sektorübergreifende Kontinuitätsplanung. Für die Schweiz liegen 122 Listungen im angegebenen Zeitraum 2026 vor, gegenüber 50 im gesamten Jahr 2025. Die Zeiträume sind unterschiedlich lang. Der Vergleich misst keine Angriffsrate. Auf AKIRA entfallen 13 Listungen, auf The Gentlemen und Qilin jeweils 9. Die übrigen Listungen verteilen sich auf zahlreiche andere Gruppenbezeichnungen. Eine Listung belegt für sich weder Verschlüsselung noch Datendiebstahl oder Zahlung [S2].

Die regionale Momentaufnahme erfasst 457 Listungen für Deutschland, 295 für Frankreich, 286 für Italien und 61 für Österreich. Diese grösseren und kleineren Grundgesamtheiten unterscheiden sich in Offenlegung und Beobachtungsabdeckung. Sie liefern Kontext für die Wiederherstellungsplanung und keine Rangliste nationaler Sicherheit [S2].

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

2. Offizielle Berichte stellen Identitätsmissbrauch neben Ransomware. Das Bundesamt für Cybersicherheit meldet 27128 freiwillige Meldungen und 200 Pflichtmeldungen im ersten Halbjahr 2026, gegenüber 29006 freiwilligen Meldungen und 145 Pflichtmeldungen im zweiten Halbjahr 2025 [S5][S107]. Der Bericht zum ersten Halbjahr 2025 wies insgesamt 35727 Cybervorfallmeldungen und 57 Ransomware-Meldungen aus, während für das erste Halbjahr 2026 insgesamt 79 gemeldete und beobachtete Ransomware-Fälle ausgewiesen wurden [S5][S108]. Diese behördlichen Grundgesamtheiten nutzen zeitraumspezifische Definitionen und dürfen nicht zu Beitrags- oder Listungszahlen dieses Berichts addiert werden [S5][S107][S108].

Das Amt hebt Phishing gegen Cloud-Konten sowie die Identitätsvortäuschung von Führungskräften oder Helpdesks hervor. Eine realistische Nachricht kann Menschen dazu bringen, Passwörter preiszugeben, Anmeldungen zu genehmigen oder Software zu installieren. Die praktische Kontrolle ist die Prüfung der Berechtigung über einen getrennten, vertrauenswürdigen Kanal. Bei Missbrauchsverdacht sind anschliessend Sitzungen und Wiederherstellungseinstellungen zu untersuchen [S5].

3. Vorfälle bei Dienstleistern erfordern technische Entscheidungen und Meldeentscheidungen. Eine Organisation kann für Vorsorge-, Gesundheits-, Medien-, Kunden- oder Personalprozesse von einem Auftragsbearbeiter abhängen. Die erste verlässliche Information kann deshalb von einem Anbieter kommen. Die verantwortliche Organisation muss dennoch ihre eigenen Daten, betroffenen Prozesse und Meldepflichten bestimmen. Kapitel 5 bewahrt die Unsicherheit jeder offiziellen Meldung darüber, worauf zugegriffen oder was entwendet wurde.

Die Untersuchung eines Anbieters sollte die erste Risikobeurteilung seines Kunden nicht verzögern. Ebenso sollte eine Angreiferanzeige nicht zur öffentlichen Darstellung der Organisation werden. Sichern Sie die Meldung, bestimmen Sie den betroffenen Dienst und halten Sie fest, welche Belege jede Datenaussage tragen.

4. Die jüngste kantonale Offenlegung unterscheidet Datensätze von Personen. Die Meldung vom 20. November beschreibt ungefähr 97 000 Datensätze in einer Verwaltungsanwendung. Wiederholte Bewilligungen oder Verlängerungen bedeuten, dass die Datensatzzahl nicht der Zahl betroffener Personen entspricht. Dieselbe Meldung beschreibt die Isolation der Plattform und die weitere Bearbeitung über alternative Formulare. Es geht um Dienste und Datenverwaltung. Daraus lässt sich keine weitergehende Zahl betroffener Einwohnerinnen und Einwohner ableiten [S16].

5. Externe Identitätsbeobachtungen erfordern Kontoprüfung. Das geprüfte Portfolio erfasst mindestens 172 240 Gerätezuordnungen und 11 072 599 historische Zugangsdatenzuordnungen. Zugangsdaten mit Bezug zu 49 von 250 ausgewählten Organisationen wurden zum Prüfzeitpunkt angeboten. Beobachtungen liegen für 247 Kandidaten vor; für 3 fehlen Expositionsergebnisse. Keine dieser Grundgesamtheiten zählt bestätigte Einbrüche oder eindeutige Personen. Prüfen Sie aktuelle Konten, relevante Aktivität und frühere Bereinigung vor einschneidenden Massnahmen [S3].

6. Meldefristen benötigen einen vorbereiteten Entscheidungsbaum. Meldungen kritischer Infrastrukturen, Datenschutzmeldungen und Finanzaufsicht haben unterschiedliche Auslöser und Fristen. Eine allgemeine Meldecheckliste kann diese Unterschiede übersehen. Rechts- und Vorfallteams sollten vor einem tatsächlichen Ereignis klären, welche Pflichten parallel laufen können [S6][S7][S8].

Vier Entscheidungen für Führungskräfte

1. **Identitätssignale mit tatsächlicher Aktivität abgleichen.** Beauftragen Sie den Identitätsbetrieb, neue Angebote und Phishing-Warnungen mit aktiven Konten, Sitzungen und geänderten Wiederherstellungseinstellungen abzugleichen. Sichern Sie Belege vor dem Zurücksetzen von Zugängen. Eskalieren Sie belegte unberechtigte Nutzung über den Vorfallprozess.

1. **Meldungen mit wesentlichen Dienstleistern üben.** Beschaffung, Dienstverantwortliche und Rechtsabteilung sollten eine erste Anbieterwarnung durchspielen. Klären Sie, welche Daten und Abläufe vom Anbieter abhängen, wer Aufzeichnungen sichern kann und wer jede Meldeprüfung beginnt.

1. **Einen wesentlichen Dienst unabhängig wiederherstellen.** Beauftragen Sie Kontinuitäts- und Infrastrukturteams mit einem Wiederherstellungstest aus geschützten Sicherungen und mit getrennten Wiederherstellungszugängen. Verlangen Sie neben dem technischen Ergebnis eine fachliche Prüfung des wiederhergestellten Dienstes und seiner Daten.

1. **Behauptungsprüfung und öffentliche Vorfallkommunikation trennen.** Benennen Sie eine Kommunikationsleitung, eine verantwortliche Person für Belege und einen alternativen Dienststatuskanal. Erfassen Sie Behauptungen, beobachtete Dienstauswirkungen und gesicherte Aussagen der Organisation zu Daten.

Das Jahr in Zahlen

Die Zahlen beschreiben getrennte Grundgesamtheiten. Eine nicht verfügbare Messgrösse ist keine Null.

122

Schweizer Ransomware-Listungen im Berichtszeitraum [S2]

WAS SIE NICHT BESCHREIBT

Verifizierte Einbrüche, einzelne Opfer oder landesweite Verbreitung

50

Schweizer Listungen aus dem gesamten Jahr 2025 in derselben Momentaufnahme [S2]

WAS SIE NICHT BESCHREIBT

Eine Vergleichsbasis gleicher Dauer

250

Ausgewählte Organisationskandidaten in dreizehn Sektorzellen [S3]

WAS SIE NICHT BESCHREIBT

Eine offizielle Rangliste oder repräsentative Landesstichprobe

49 von 250

Organisationen mit zum Prüfzeitpunkt angebotenen Zugangsdaten [S3]

WAS SIE NICHT BESCHREIBT

Geprüfte Konten, abgeschlossene Verkäufe oder bestätigte Einbrüche

48 / 100

Nationale Atlas-Kennzahl für 247 geprüfte Kandidaten [S3]

WAS SIE NICHT BESCHREIBT

Nationale Verbreitung oder Sektorbewertung

60 475

Unterschiedliche aufbewahrte Beiträge dieser Ausgabe [S1]

WAS SIE NICHT BESCHREIBT

Die Gesamtheit Schweizer Cyberkriminalität oder einzelner Vorfälle

27 128

Freiwillige Meldungen beim Bundesamt für Cybersicherheit im ersten Halbjahr 2026 [S5]

WAS SIE NICHT BESCHREIBT

Bestätigte Angriffe oder eine mit Untergrundbeiträgen vergleichbare Grösse

200

Pflichtmeldungen im Halbjahresbericht dieser Behörde [S5]

WAS SIE NICHT BESCHREIBT

Eine vollständige Zahl sämtlicher Schweizer Cybervorfälle

79

Schweizer Ransomware-Fälle aus Meldungen und Beobachtungen der Behörde im ersten Halbjahr [S5]

WAS SIE NICHT BESCHREIBT

Eine direkt mit den 122 Listungen abgleichbare Teilmenge

97 000

Ungefähre Anwendungsdatensätze in der kantonalen Novembermeldung [S16]

WAS SIE NICHT BESCHREIBT

Einzelne Personen oder bestätigter Diebstahl sämtlicher Anhänge

KERNAUSSAGEN

01

Führen Sie Anzeigen, Listungen und offizielle Offenlegungen in getrennten Entscheidungswegen.

02

Prüfen Sie Identitäts- und Dienstleisterbelege, bevor Sie den Umfang eines Vorfalls beschreiben.

03

Verlangen Sie nachgewiesene Wiederherstellung und einen erprobten Entscheidungsbaum für Meldungen.

Berichtsübersicht

Beginnen Sie bei Ihrer Entscheidung und folgen Sie den zugehörigen Belegen und dem Abschlussnachweis.

Verwaltungsrat und CISO	Welche Risiken rechtfertigen jetzt Investitionen?	01 05 11 12
SOC und Vorfallbehandlung	Wann erfordert eine externe Behauptung eine Untersuchung?	04 06 07 12
Identität und Infrastruktur	Welche Zugangswege und Abhängigkeiten sind zu prüfen?	03 05 07 12
Betrugsbekämpfung und Bankwesen	Welche persönlichen Angaben dürfen niemals eine Transaktion autorisieren?	08 09 12
Recht und Beschaffung	Wer muss wen auf welcher Grundlage informieren?	05 10 12

Belegart	Beantwortete Frage	Grenze
Untergrundbeiträge	Was Menschen anbieten, suchen oder ankündigen	Echtheit und Ergebnisse benötigen getrennte Nachweise
Ransomware-Listungen	Was in der aufbewahrten Momentaufnahme erscheint	Listungsdaten können vom Einbruchsdatum abweichen
Passive Beobachtungen	Was öffentlich sichtbare Konfigurationen zeigen	Kein Nachweis eines Einbruchs oder der Wirksamkeit von Kontrollen
Offizielle Offenlegungen	Was eine Organisation oder Behörde meldet	Schätzungen und Untersuchungen können sich ändern
Offizielle Bedrohungsanalysen	Welche Bedrohungen eine Behörde einschätzt	Zuschreibungen bleiben ihre eigene Einschätzung

Inhalt und Lesewege

Der Bericht führt von Entscheidungen über die Belege zu klar verantworteten Aufgaben. Beachten Sie bei jeder Zahl und jedem Fall die Grenzen der Belege.

Kapitel	Frage	Erste Zielgruppe
1 Zusammenfassung	Welche Entscheidungen folgen aus den Belegen?	Leitung
2 Digitaler und sicherheitspolitischer Kontext	Welche Abhängigkeiten prägen das Schweizer Bild?	Leitung
3 Exposition von Organisationen	Was lässt sich aus der ausgewählten Grundgesamtheit ableiten?	Infrastruktur
4 Darkweb-Belege	Was wird angeboten, und was bleibt ungeprüft?	Bedrohungsanalyse
5 Vorfälle nach Sektor	Was haben Organisationen und Behörden offengelegt?	Sektorverantwortliche
6 Hacktivismus und DDoS	Was unterscheidet Ankündigungen von Dienstunterbrechungen?	Betrieb
7 Bedrohungsakteure	Welche Beziehungen und Zuschreibungen sind belegt?	Bedrohungsanalyse
8 Betrugsökonomie	Wie werden Identitäten und Vertrauen für Betrug genutzt?	Betrugsteams
9 Bankwesen	Welche Kontrollen benötigen gemeinsame Verantwortung von Finanz- und Sicherheitsteams?	Bankwesen und Identität
10 Regulatorische Reaktion	Welche Meldepflichten gelten für welche Ereignisse?	Recht und Compliance
11 Ausblick	Welche Signale würden die Einschätzung verändern?	Leitung
12 Massnahmenplan	Wer handelt, und was weist den Abschluss nach?	Alle Verantwortlichen

Leseweg für die Leitung: Kapitel 1, 5, 10–12. **Leseweg für den Betrieb:** Kapitel 4, 6–7 und 12. **Leseweg für Identität und Betrug:** Kapitel 3, 8–9 und 12.

Beobachtet bedeutet, dass das Material oder die Messung vorliegt. **Behauptet** bedeutet, dass ein Beitrag oder eine Listung etwas geltend macht. **Offiziell gemeldet** bedeutet, dass eine Organisation oder Behörde es im angegebenen Umfang offengelegt hat.

Eine analytische Einordnung verbindet Belege mit einer Entscheidung. Sie ersetzt keine fehlenden Nachweise zu Zugriff, Zuschreibung, betroffenen Personen oder Verlusten.

KAPITEL 02

Der digitale Kontext und die Bedrohungslage der Schweiz

02

DIESES KAPITEL BEANTWORTET

Welche Merkmale der Schweiz prägen die Bedrohungen, auf die Führungskräfte vorbereitet sein sollten?

3

unterschiedliche Bereiche: sensible Informationen, gemeinsame Dienste und öffentliche Anlässe

2.1 Der Informationswert zählt mehr als ein Länderbezug 12
2.2 Spionageeinschätzungen brauchen einen benannten Urheber 13
2.3 Gemeinsame Dienste können sonst getrennte Vorfälle verbinden 14
2.4 Der Hostingstandort belegt keine Nationalität des Betreibers 14
2.5 Internationale Anlässe geben Kontext für Kontinuitätsplanung 15
2.6 Meldepflichten verändern die zählbaren Grundgesamtheiten 15

KAPITEL 02

Der digitale Kontext und die Bedrohungslage der Schweiz

KURZFASSUNG

Die Schweiz vereint internationale Organisationen, Forschung, Finanzdienste und gemeinsam genutzte digitale Infrastruktur. Der Nachrichtendienst des Bundes nennt diese Bereiche als Nachrichtendienstziele. Cybermeldepflichten gelten für bestimmte kritische Dienste. Internationale Anlässe bieten zudem Gelegenheiten für Behauptungen über Verfügbarkeitsangriffe. Diese Probleme erfordern unterschiedliche Belege. Bestimmen Sie die relevanten Informations-, Dienstleister- und Dienstabhängigkeiten Ihrer Organisation, bevor Sie Kontrollen auswählen.

2.1 Der Informationswert zählt mehr als ein Länderbezug

Das nationale Umfeld schafft mehrere unterschiedliche Gründe für eine Zielauswahl. Der Nachrichtendienst des Bundes nennt in seiner Lagebeurteilung 2026 staatliche Stellen, internationale Organisationen, diplomatische Einrichtungen und international tätige Unternehmen als Nachrichtendienstziele. Dazu kommen Hochschulen und Forschungsinstitute [S9]. Dies ist die Einschätzung des NDB. Sie besagt nicht, dass jede Organisation dieser Kategorien im Berichtszeitraum einen Vorfall erlitt.

Für Sicherheitsverantwortliche ist entscheidend, welche Informationen nach einem Zugriffsverlust wertvoll blieben. Verhandlungspositionen, Forschungsergebnisse, Kundenbeziehungen und betriebliche Entwürfe können unterschiedlichen Schutz benötigen. Eine allgemeine Länderwarnung beantwortet diese Frage nicht. Die Informationsverantwortlichen müssen sensible Tätigkeiten und zugriffsberechtigte Personen bestimmen.

Der NDB beschreibt besonderes Interesse an Aussen-, Handels- und Sicherheitspolitik, militärischen Fähigkeiten, Rüstungsindustrie und fortgeschrittener Forschung [S9]. Seine Liste betrifft nachrichtendienstliche Prioritäten. Eine Verkaufsanzeige für Kundendaten ist ein anderer Sachverhalt, auch wenn derselbe Sektor vorkommt. Keine dieser Grundgesamtheiten erlaubt eine Schätzung der anderen.

Diese Unterscheidung verändert die Reaktion. Eine Kundendatenbehauptung erfordert Belegsicherung, Datensatzprüfung und Betrugsvorbereitung. Vermuteter Zugriff auf sensible Forschung erfordert zusätzlich die Prüfung von Zusammenarbeitskonten, Projektablagen und externer Freigabe. Beide erfordern die Verifizierung des betroffenen Systems und Zugriffszeitraums. Der Länderbezug allein belegt keines von beidem.

Die Tabelle verbindet den nationalen Kontext mit internen Fragen. Sie vergibt keine sektoralen Bedrohungswerte.

Umfeld	Quelleneinschätzung	Interne Frage	Verantwortliche
Staat und Diplomatie	Der NDB nennt politische Informationen als nachrichtendienstliches Ziel [S9]	Wer kann sensible Briefings aus der Ferne lesen?	Informationsverantwortliche und Identitätsteam
Hochschulen und Forschung	Der NDB nennt wissenschaftliche Einrichtungen und Spitzentechnologie [S9]	Welche externen Partner behalten nach Projektende Zugriff?	Forschungsleitung und IT
Internationale Unternehmen	Der NDB zählt international tätige Unternehmen zu Nachrichtendienstzielen [S9]	Welche Geschäftsentscheidungen hängen von vertraulichen Informationen ab?	Geschäftsleitung und Sicherheit
Gemeinsame digitale Dienste	Der NDB nennt Telekommunikations- und IT-Anbieter als mögliche Zugangswege [S9]	Welcher Dienstleister erreicht mehrere kritische Dienste?	Beschaffung und Dienstverantwortliche

2.2 Spionageeinschätzungen brauchen einen benannten Urheber

Die Zusammenfassung der Lagebeurteilung 2026 des Bundes nennt russische und chinesische Nachrichtendienste als Hauptbedrohung durch Spionage in der Schweiz, neben vom NDB beschriebenen staatlichen Cyberbedrohungen aus Russland, China, Iran und Nordkorea [S9][S110]. In dieser offiziellen Einschätzung wird russische Aktivität mit Druck auf Politik, Diplomatie und kritische Infrastrukturen verbunden, chinesische Aktivität zusätzlich mit Technologie-, Wirtschafts- und Forschungsaufklärung [S9][S110]. Diese Zuschreibungen stammen von den Bundesbehörden; dieser Bericht weist ungeprüften Datenangeboten oder Websiteunterbrechungen kein Herkunftsland zu.

Die Einschätzung nennt mehrere Zugangsmuster: Ausnutzung öffentlich erreichbarer Netzwerkgeräte, gezieltes Phishing und Kontakt über Messaging-Anwendungen [S9]. Bekannte Schwachstellen veralteter Software würden häufiger genutzt als bisher unbekannte Schwachstellen. Das spricht für klare Anlagenverantwortung, unterstützte Software und rasche Behebung. Es bestimmt keinen Zugangsweg eines einzelnen Schweizer Vorfalls.

Forschung und Entwicklung verdienen besondere Aufmerksamkeit, weil die Informationen lange wertvoll bleiben können. Der NDB bezieht akademische und privatwirtschaftliche Forschung ein [S9]. Reaktionspläne sollten deshalb dauerhaften Zugriff und unangemessene Freigaben ebenso abdecken wie offensichtliche Dienstausfälle.

Eine praktische Prüfung beginnt bei Systemen, die sensible Tätigkeiten über Organisationsgrenzen hinweg ermöglichen. Benennen Sie Verantwortliche für Fernzugriff, externe Identitäten, gemeinsame Ablagen und Supportkanäle von Dienstleistern. Verlangen Sie Nachweise, dass Zugriffe mit dem Ende der Geschäftsbeziehung enden. Dies ist eine Kontrollprüfung und keine Behauptung eines Angriffs auf diese Systeme.

2.3 Gemeinsame Dienste können sonst getrennte Vorfälle verbinden

Dienstleisterabhängigkeiten verbinden Geschäftsprozesse, die im Organigramm getrennt erscheinen. Der NDB nennt IT-Dienstleister als wichtige Zugangswege. Telekommunikationsanbieter beschreibt er als Nachrichtendienstziele und mögliche Wege zu Kunden [S9]. Auch FINMA betont institutsspezifische Cyberszenarien und Abhängigkeiten von Dritten [S61].

Ein Dienstleistervorfall kann mehrere Folgen zugleich haben. Mitarbeitende verlieren möglicherweise einen Dienstzugang, während Kundeninformationen anderswo verfügbar bleiben. Die Wiederherstellung kann vom Identitätsdienst, Supportpersonal oder Unterauftragnehmer des Anbieters abhängen. Ob auf Daten zugegriffen wurde, bleibt eine andere Frage als ein Dienstausfall.

Das Dienstinventar sollte deshalb mehr als den Anbieternamen erfassen. Es sollte den Dienst mit Geschäftsprozess, sensiblen Informationen, Ausweichverfahren und Vorfallkontakt verbinden. Der Abschlussnachweis ist eine erprobte Abhängigkeitsdokumentation. Eine vertragliche Aussage zur Sicherheitsverantwortung des Anbieters belegt keine Wiederherstellbarkeit.

Bei Finanzinstituten bleibt die Verantwortung ebenfalls beim beaufsichtigten Institut. Laut FINMA kann die Verantwortung für aufsichtsrechtliche Anforderungen nicht auf einen Dienstleister übertragen werden [S8]. Kapitel 10 erklärt, wie eine Meldefrist bereits mit der Feststellung beim beauftragten Anbieter beginnen kann.

2.4 Der Hostingstandort belegt keine Nationalität des Betreibers

Der NDB beschreibt die Nutzung Schweizer Serverinfrastruktur über Wiederverkäufer und Zwischenhändler für Operationen gegen Ziele im Ausland [S9]. Akteure wechselten zudem Infrastruktur und nutzten mehrere Zwischensysteme. Ein Schweizer Serverstandort belegt deshalb weder Schweizer Betreiber noch Schweizer Opfer oder staatliche Beteiligung der Schweiz.

Für Hosting- und Cloud-Anbieter ist die Entscheidung operativ. Sichern Sie Mandanten- und Verwaltungsaufzeichnungen, wenn ein glaubwürdiger Vorfall eine Untersuchung erfordert. Der Dienst muss die relevante Kundenbeziehung feststellen und über bestehende Rechts- und Sicherheitskanäle reagieren können. Behandeln Sie nicht sämtliche Kunden gemeinsamer Infrastruktur als mit der Aktivität verbunden.

Für andere Organisationen betrifft die Lehre die Zuschreibung. Der Netzwerkstandort kann Untersuchungen unterstützen, belegt aber nicht, wer eine Operation steuerte. Sprache, Hostingland oder behauptetes politisches Motiv sollten getrennt gekennzeichnete Beobachtungen bleiben. Eine Akteursbeziehung benötigt Belege für diese Beziehung und nicht bloss einen gemeinsamen Länderbezug.

2.5 Internationale Anlässe geben Kontext für Kontinuitätsplanung

Der Ukraine-Friedensgipfel im Juni 2024 ist relevanter historischer Kontext ausserhalb des Vorfallszeitraums dieses Berichts. In seiner ersten Bilanz schrieb das NCSC DDoS-Aktivität rund um den Gipfel NoName057(16) zu [S42]. Es meldete geringe Infrastrukturstörungen. Systeme und Daten des Gipfels und seiner Organisatoren seien nicht bedroht gewesen.

Die Quelle unterscheidet mehrere Erscheinungen. Sie meldete versuchte digitale Einbrüche und Phishing getrennt von DDoS. Übertragungsprobleme und ein Stromausfall seien keine Cybervorfälle gewesen [S42]. Diese Unterscheidung zählt bei technischen Störungen während öffentlich stark beachteter Anlässe.

Die historische Darstellung unterstützt die Vorbereitung auf Unterbrechungen öffentlicher Dienste bei Grossanlässen. Sie belegt keine ähnliche Kampagne im Jahr 2026. Der NDB schätzt Überlastungsangriffe rund um internationale Konferenzen und Grossanlässe gesondert als sehr wahrscheinlich ein [S9]. Das ist eine Quellenbewertung, keine eigene Prognose dieses Berichts oder Position zum Anlass.

Nutzen Sie den Veranstaltungskalender, um Dienstkontinuität, Anbietereskalation und öffentliche Aussagen zu üben. Eine Aussage sollte Akteursbehauptung, beobachtete Dienstauswirkung und verbleibende Ungewissheit unterscheiden. Leiten Sie aus einem Websiteausfall keinen Datenzugriff ab. Leiten Sie aus dem Zeitpunkt allein keine politische Ursache ab.

2.6 Meldepflichten verändern die zählbaren Grundgesamtheiten

Die Meldepflicht für kritische Infrastrukturen begann am 1. April 2025 [S60]. In seinen Halbjahresberichten erfasste das BACS im ersten Halbjahr 2025 insgesamt 35 727 Cybervorfallmeldungen [S108]. Danach erfasste es getrennt 29 006 freiwillige und 145 Pflichtmeldungen im zweiten Halbjahr 2025 sowie 27 128 und 200 im ersten Halbjahr 2026 [S5][S107]. Ein Jahresvergleich muss diesen Begriffswechsel und den Start der Meldepflicht im April 2025 bereinigen, bevor er eine Trendaussage ableitet [S60][S107][S108]. Solche Meldungen lassen sich nicht mit Darkweb-Beiträgen, Ransomware-Listungen oder sämtlichen Vorfällen Schweizer Organisationen gleichsetzen.

Die getrennten Belegpopulationen dieses Berichts sollten Entscheidungen unterstützen, ohne zu einer nationalen Gesamtzahl verbunden zu werden. Öffentliche Warnungen können ein Kampagnenmuster zeigen. Eine Erpressungslistung dokumentiert eine Behauptung. Expositionszuordnungen und passive Konfigurationen beschreiben unterschiedliche Beobachtungen. Jede benötigt eigene Prüfung und Verantwortliche.

Aussagen über Bankgeheimnis oder Aussenbeziehungen sind für eine kausale Deutung dieser Beobachtungen nicht erforderlich. Entscheidend sind betroffene Informationen, Dienste und die Aussagekraft der Belege. Kapitel 10 überführt unterschiedliche Meldepflichten in eine Entscheidungsdokumentation für Vorfälle.

KERNAUSSAGEN

01

Schreiben Sie nationale Nachrichtendiensteinschätzungen dem NDB zu und trennen Sie sie von einzelnen Vorfallsbehauptungen.

02

Gemeinsame Dienste verbinden Geschäftsauswirkungen, Wiederherstellung und Meldepflichten. Prüfen Sie diese Abhängigkeiten mit dem Anbieter.

03

Der Gipfelbericht 2024 ist historischer Kontext. Zeitpunkt und Websiteunterbrechung belegen keinen Datenzugriff.

KAPITEL 03

Nationale Exposition: die ausgewählte Organisationsgrundgesamtheit

DIESES KAPITEL BEANTWORTET

Welche Identitätsbeobachtungen erfordern Prüfung bei den ausgewählten Organisationen?

49 von 250

Organisationen mit zum Prüfzeitpunkt angebotenen Zugangsdaten

3.1 Karte der Grundgesamtheit 18

3.2 Passive Beobachtungen und ihre Grenzen 20

3.3 Aktuelle Listungen und die nationale Atlas-Kennzahl 21

3.4 Beobachtungen zu Geräten, Zugangsdaten und Dokumenten 22

3.5 Externe Signale in vertretbare Entscheidungen überführen 24

KAPITEL 03

Nationale Exposition: die ausgewählte Organisationsgrundgesamtheit

KURZFASSUNG

Bei 49 von 250 ausgewählten Organisationen wurden zum Prüfzeitpunkt Zugangsdaten angeboten. Expositionsbeobachtungen liegen für 247 Kandidaten vor; 3 bleiben ungeprüft. Die nationale Atlas-Kennzahl beträgt 48 von 100 für dieses geprüfte Portfolio. Geräte- und historische Zugangsdatenzuordnungen können Kunden, Mitarbeitende oder älteres Material betreffen. Passive Konfiguration hat einen getrennten Nenner. Prüfen Sie aktuelle Listungen, untersuchen Sie relevante Mitarbeitendengeräte-Belege und kontrollieren Sie beabsichtigte Mail- und Webschutzmassnahmen.

3.1 Karte der Grundgesamtheit

Auswahl und Messung sind getrennt. Die Aufnahme benennt einen Prüfungskandidaten. Sie belegt weder Exposition noch einen aktuellen Vorfall oder eine unabhängig betriebene Unternehmensgruppe [S3].

Merkmal	Definition
Ausgewählte Grundgesamtheit	250 Organisationskandidaten mit einer primären öffentlichen Domain
Auswahlgrundlage	Behörden, offizielle Finanz- und Bildungsverzeichnisse sowie bedeutende Sektororganisationen
Zweck	Ausgewählte externe Signale beschreiben und Fragen für Dienstverantwortliche unterstützen
Abdeckung	Dreizehn Sektorzellen
Organisationsgrenze	Manche getrennt betriebenen Tochtergesellschaften haben dieselbe Muttergesellschaft
Zeitbezug	Exposition gelesen am 21. und 22. November 2026; passive Beobachtungen haben ihr eigenes Aufnahmedatum
Öffentliche Ergebnisse	Sektorale Signalzahlen und nationale Atlas-Kennzahl; einzelne Organisationen bleiben verborgen
Aussagegrenze	Keine nationale Verbreitungsschätzung, Sicherheitsrangliste oder Zertifizierung einzelner Kontrollen

Die Sektortabelle beschreibt die Auswahl. Diese analytischen Gruppen bestimmen nicht, ob eine Organisation gesetzlich als kritische Infrastruktur meldepflichtig ist.

Sektor	Kandidaten	Sicherheitsfrage
Banken und Finanzen	40	Können Identitäts-, Betrugs- und Zahlungsteams dasselbe Ereignis prüfen?
Öffentliche Verwaltung	35	Kann ein Dienst während der Isolation einer Anwendung weiterlaufen?
Bildung und Forschung	25	Wer kann Forschungs- oder Identitätsdaten über gemeinsame Dienste exportieren?
Gesundheitswesen	20	Können klinische Abläufe während der Wiederherstellung weiterlaufen?
Energie und Versorgung	20	Welche Geschäftsabhängigkeiten können wesentliche Betriebsabläufe beeinträchtigen?
Transport und Logistik	20	Lassen sich Kunden- und Betriebsabläufe getrennt wiederherstellen?
Industrie und Bau	21	Sind Dienstleisterzugriffe und Produktionsabhängigkeiten bekannt?
Telekommunikation und Technologie	15	Wer kann Identitäten zurücksetzen oder vertrauenswürdige Mitteilungen veröffentlichen?
Life Sciences und Chemie	15	Welche Partner bearbeiten Forschungs- und Personaldaten?
Handel, Lebensmittel und Landwirtschaft	15	Welche Kunden- und Lieferantenkonten autorisieren Transaktionen?
Konsumentenmedien und Immobilien	9	Welche ausgelagerten Plattformen speichern Kundeninformationen?
Handel und Unternehmensdienste	5	Welche gemeinsamen Dienste unterstützen kritische Transaktionen?
Versicherungen	10	Lassen sich Schaden- und Vorsorgedaten jedem Auftragsbearbeiter zuordnen?
Gesamt	250	Eine gezielte Auswahl mit unterschiedlichen institutionellen Grenzen

3.2 Passive Beobachtungen und ihre Grenzen

Die passive Momentaufnahme umfasst 246 der 250 ausgewählten Kandidatendomains und lässt je einen Kandidaten in Banken und Finanzen, öffentlicher Verwaltung, Bildung und Forschung sowie Gesundheitswesen aus. Diese vier Auslassungen überschneiden sich nicht mit den drei ungeprüften Kandidaten der 247 Organisationen umfassenden Expositionsgrundgesamtheit, sodass 243 Kandidaten in beiden Prüfungen enthalten sind. Nicht eindeutige Antworten gelten nicht als Kontrollversagen [S3].

Beobachtung	Anzahl	Nenner
Geprüfte Kandidatendomains	246	246
DMARC-Richtlinie reject oder quarantine beobachtet	164	246
SPF beobachtet	233	246
DKIM-Einträge beobachtet	168	246
DNSSEC-Delegationseintrag beobachtet	69	246
TLS-Zertifikatsprüfung gültig	243	246
TLS-Zertifikatsvalidierung erfolglos	2	246
TLS-Prüfung ungeklärt	1	246
Antwort erfasst	216	246
HSTS beobachtet	182	216

Die E-Mail-Beobachtung erfasst eine veröffentlichte Richtlinie. Sie misst nicht die Abweisung jeder betrügerischen Nachricht. Ein DKIM-Eintrag belegt keine Signierung sämtlicher legitimer E-Mail-Ströme. HSTS-Befunde verwenden den Nenner der erfassten Antworten.

Eine Richtlinienbeobachtung ist eine Frage an die Dienstverantwortlichen. Eine rein beobachtende E-Mail-Richtlinie kann während der Prüfung legitimer Absender beabsichtigt sein. Eine fehlende Beobachtung kann auch auf eine uneindeutige Antwort zurückgehen. Keines von beidem belegt eine Nutzung dieses Zustands durch Angreifer.

Bei E-Mail-Authentisierung zählt operativ, ob legitime Dienste ausgerichtete Nachrichten senden und Empfänger die beabsichtigte Richtlinie durchsetzen können. Eine veröffentlichte Richtlinie allein belegt diese Ergebnisse nicht. Verantwortliche sollten Zustellberichte und genehmigte Versanddienste prüfen, bevor sie die Durchsetzung ändern.

Eine DNS-Delegationsbeobachtung beschreibt die sichtbaren Vertrauensinformationen dieser Domain. Sie prüft nicht jeden Resolver, jeden Eintrag oder den internen Namensdienst. Ebenso belegt ein gültiges TLS-Zertifikat nur eine begrenzte Beobachtung zur Transportsicherheit. Es bewertet weder Anwendungsberechtigungen noch Wiederherstellungskontrollen oder den Schutz gespeicherter Kundendaten.

Headerbeobachtungen haben einen noch engeren Umfang. Ein Header einer Antwort kann sich von anderen Anwendungen, Hostnamen oder Pfaden unterscheiden. Prüfen Sie deshalb die Richtlinienkonsistenz über relevante Dienste hinweg. Validieren Sie nach einer Änderung auch die Nutzungserfahrung.

Passive Beobachtungen beschreiben Konfigurationen mit ausdrücklich genannten Sektornennern

	DMARC	SPF	DKIM	DNSSEC	TLS	HSTS
Banken und Finanzen	25/39	38/39	19/39	21/39	39/39	34/35
Öffentliche Verwaltung	20/34	30/34	12/34	6/34	33/34	24/30
Bildung und Forschung	9/24	23/24	21/24	11/24	24/24	16/23
Gesundheitswesen	11/19	17/19	11/19	3/19	19/19	14/19
Energie und Versorgung	15/20	19/20	18/20	0/20	20/20	17/19
Transport und Logistik	13/20	19/20	15/20	9/20	19/20	15/17
Telekommunikation und Technologie	15/15	15/15	11/15	4/15	15/15	11/14
Life Sciences und Chemie	10/15	14/15	13/15	2/15	15/15	9/13
Industrie und Bau	17/21	21/21	16/21	5/21	21/21	16/18
Versicherungen	8/10	10/10	7/10	3/10	10/10	8/8
Handel, Lebensmittel und Landwirtschaft	12/15	14/15	13/15	2/15	14/15	9/10
Unternehmens- und Verbraucherdienste	9/14	13/14	12/14	3/14	14/14	9/10

Quelle: passive Beobachtungen, 22. November 2026. Jede Zelle zeigt beobachtete/geprüfte Domains; HSTS verwendet erfasste Antworten. Veröffentlichte Richtlinien belegen keine Durchsetzung für jede Nachricht [S3].

3.3 Aktuelle Listungen und die nationale Atlas-Kennzahl

Bei 49 von 250 ausgewählten Organisationen wurden zum Prüfzeitpunkt Zugangsdaten zum Verkauf angeboten. Expositionsbeobachtungen liegen für 247 Kandidaten vor; die 3 ungeprüften Kandidaten (je einer in Energie und Versorgung, Transport und Logistik sowie Unternehmens- und Verbraucherdiensten) sind alle in der passiven Momentaufnahme über 246 Domains enthalten. Die nationale Atlas-Kennzahl beträgt 48 von 100 für das bewertete Portfolio [S3].

Höhere Atlas-Werte bedeuten eine stärkere beobachtete Exposition. Die Kennzahl beschreibt das ausgewählte Portfolio, weder die nationale Verbreitung noch bestätigte Vorfälle. Dieser Bericht veröffentlicht ausschliesslich diese nationale Atlas-Zahl. Die Sektortabelle zeigt Signalzahlen mit den jeweiligen geprüften Grundgesamtheiten.

Die Expositions- und Passivtabellen fassen Unternehmens- und Verbraucherdienste zusammen. Die Karte der Grundgesamtheit behält die ursprünglichen Auswahlsektoren bei.

Sektor	Geprüft	Aktuelle Listungen	Mitarbeitendengeräte: Organisationen	Dokumente: Organisationen	Geräte: Organisationen
Banken und Finanzen	40	7	15	19	36
Öffentliche Verwaltung	35	4	20	26	29
Bildung und Forschung	25	6	23	24	25
Gesundheitswesen	20	0	10	6	14
Energie und Versorgung	19	1	10	8	15
Transport und Logistik	19	7	14	10	17
Telekommunikation und Technologie	15	6	13	13	15
Biowissenschaften und Chemie	15	2	12	10	12
Industrie und Bau	21	4	16	16	18
Versicherungen	10	3	7	8	10
Handel, Lebensmittel und Landwirtschaft	15	6	10	9	14
Unternehmens- und Verbraucherdienste	13	3	8	9	10
Alle geprüften	247	49	158	158	215

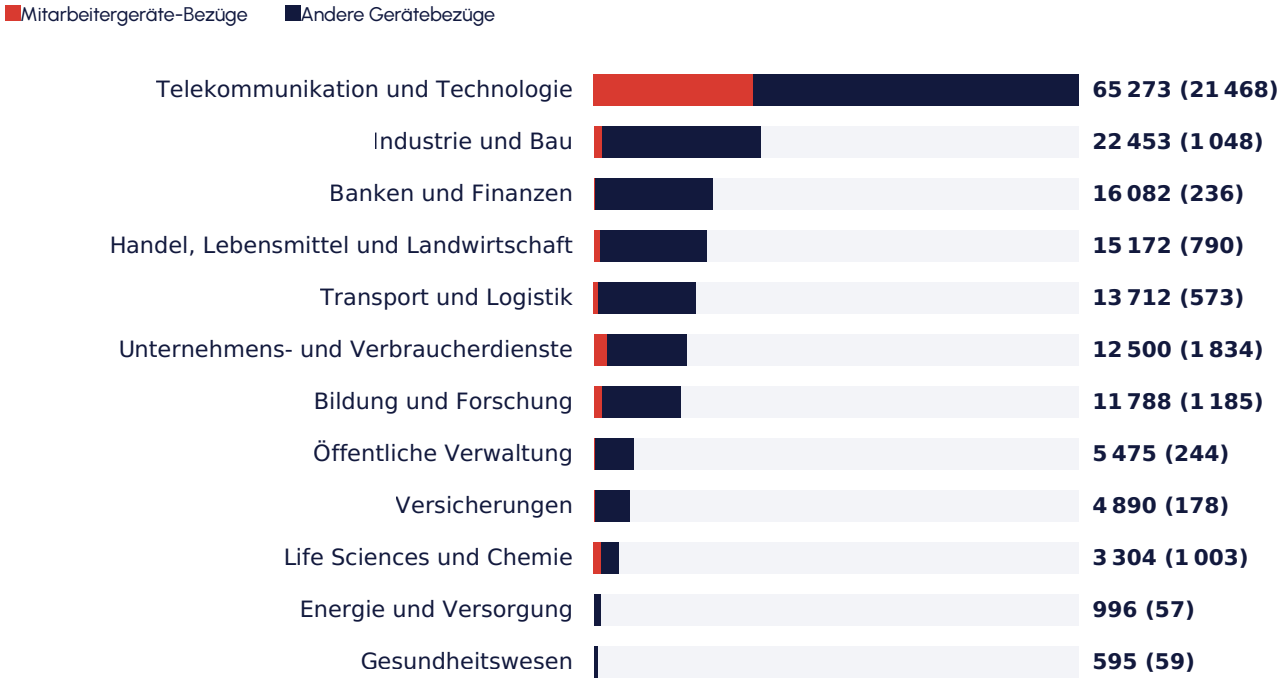
Eine aktuelle Listung bedeutet, dass Zugangsdaten mit Bezug zur Domain zum Prüfzeitpunkt angeboten wurden. Sie belegt weder gültige Konten noch einen abgeschlossenen Verkauf oder Zugriff auf interne Systeme. Sichern Sie das Angebot und prüfen Sie das Konto anhand autorisierter Organisationsunterlagen.

3.4 Beobachtungen zu Geräten, Zugangsdaten und Dokumenten

Die Expositionsaufnahme wurde am 21. und 22. November 2026 gelesen. Geräte- und Zugangsdatenzahlen beschreiben damals vorhandene Datensätze, einschliesslich älteren Materials. Erwähnungen beziehen sich auf die vorangegangenen 365 Tage; ähnliche Domains auf 30 Tage [S3].

Beobachtung	Anzahl	Geprüfte Organisationen
Gerätezuordnungen, mindestens	172 240	247
Mitarbeitendengeräte-Zuordnungen	28 675	247
Weitere Gerätezuordnungen	143 565	247
Historische Zugangsdatenzuordnungen	11 072 599	247
Datensätze aus Datenleckbeständen	4 102 097	247
Zeilen aus Stealer-Protokollen	2 216 250	247
Combolist-Einträge	4 754 252	247
Beobachtungen ähnlicher Domains	109 410	247
Dokumentbeobachtungen	2 696	247

Geräte- und Zugangsdatenzuordnungen in den geprüften Sektorgrundgesamtheiten



Quelle: Expositionsbeobachtungen für 247 geprüfte Organisationskandidaten, 21.–22. November 2026. Kumulative Bezüge, keine verifizierten Einbrüche [S3].

Einige Gerätezahlen sind Mindestwerte. Es sind Zuordnungen zu ausgewählten Domains, keine eindeutigen Schweizer Personen oder Beschäftigten. Ein Gerät oder Zugangsdaten können mehreren Organisationen zugeordnet sein. Datensätze können wiederholt, veraltet oder bereits bereinigt sein.

Als Mitarbeitendengeräte klassifizierte Zuordnungen erfordern die Prüfung aktueller Konten und verwalteter Geräte. Andere Zuordnungen belegen nicht, wem das Gerät gehört. Bildungs- und Kundendienstdomains können Studierende, Kunden und weitere berechtigte Nutzende einschliessen.

Ähnliche Domainnamen belegen für sich weder Phishing noch böswillige Absicht. Dokumentbeobachtungen erfordern eine getrennte Prüfung von Eigentum, Zugänglichkeit und Sensibilität. Trennen Sie diese Prüfung von der Kontoeindämmung.

3.5 Externe Signale in vertretbare Entscheidungen überführen

Identitätsverantwortliche sollten prüfen, ob Konto oder Dienst zur Organisation gehören, noch aktiv sind und dieselben Belege bereits bereinigt wurden. Threat Intelligence sollte Anzeigen getrennt von internen Befunden sichern.

Prüfen Sie relevante Aktivität wie Sitzungen, Wiederherstellungsänderungen, Anwendungsfreigaben und Postfachregeln. Beschreiben Sie fehlende passende Telemetrie mit ihren Aufbewahrungs- und Abdeckungsgrenzen. Ein abgelöstes historisches Passwort kann einen Abschluss rechtfertigen; eine unbefugte Sitzung kann Widerruf und Vorfalleskalation erfordern.

Eine Bankdomain-Zuordnung kann Kunden, Mitarbeitende, Dienstleister oder historische Datensätze betreffen. Kapitel 9 trennt die gesamte Bankenzelle von der mit Kartenherausgebern abgeglichenen Teilmenge. Keine Grundgesamtheit ergibt eine Kompromittierungsrate des Bankwesens.

Dokumentieren Sie Verantwortliche, Beobachtungen, Unsicherheit, Massnahmen und Wiederaufnahmebedingungen. Lassen Sie Geschäftsverantwortliche Kontinuität bei isoliertem Dienst demonstrieren. Kontoprüfung, Konfigurationsprüfung und Wiederherstellung benötigen jeweils eigene Abschlussbelege.

KERNAUSSAGEN

01

Prüfen Sie aktuelle Listungen gegen aktive Konten und relevantes Verhalten.

02

Trennen Sie kumulative Zuordnungen von Personen und aktuellen Vorfällen.

03

Lesen Sie Expositions- und passive Ergebnisse mit ihren unterschiedlichen geprüften Nennern.

KAPITEL 04

Darkweb-Angebote und die Grenzen ihrer Belege

DIESES KAPITEL BEANTWORTET

Was belegen Untergrundangebote mit Schweizer Bezug, und wo sollten Sicherheitsverantwortliche Bestätigung suchen?

5

Fallstudien, die angebotene Daten von verifizierten Vorfällen trennen

4.1 Die Beobachtungsgrundgesamtheit 26

4.2 Unterschiedliche Produkte erfordern unterschiedliche Reaktionen 29

4.3 Fünf Fälle zur Prüfung 30

4.4 Zugangsdaten, Kontakte und Nachfrage 36

4.5 Jüngste Aktivität: 9.–22. November 39

4.6 Belege mit einer klar verantworteten Entscheidung verbinden 40

KAPITEL 04

Darkweb-Angebote und die Grenzen ihrer Belege

KURZFASSUNG

Beiträge mit Schweizer Bezug bieten Versicherungsdaten, Kundeninformationen, Kontaktlisten und Kontozugänge an. Manche beschreiben älteres Material. Andere sind Kaufgesuche oder Antworten mit zitierten Behauptungen. Ein Angebot zu Dienstleisterdaten erweitert die Prüfung auf physische Sicherheit. Keine dieser Anzeigen belegt allein einen Einbruch, abgeschlossenen Verkauf oder aktuellen Zugang. Prüfen Sie Quelle, Datum, Konto und Geschäftsprozess vor Eindämmungsmassnahmen oder der Kommunikation einer Zahl betroffener Personen.

4.1 Die Beobachtungsgrundgesamtheit

Eine Länderkennzeichnung belegt kein Schweizer Opfer. Odin by Brandefense zählte 59 956 der Schweiz zugeordnete, ländermarkierte Beiträge im angegebenen Zeitraum. Das vereinte aufbewahrte Material umfasst 60 475 unterschiedliche Beiträge über die Quellengruppen des Berichts hinweg. Diese Zahlen beschreiben Beiträge, keine Vorfälle, Personen oder erfolgreichen Transaktionen. [S1]

Die Quellengruppen überschneiden sich. Die vereinte Gesamtzahl ist eine eigene Grundgesamtheit. Deshalb dürfen diese Zeilen nicht addiert werden. Wo Quellenmaterial fehlte, ist die aufbewahrte Abdeckung unvollständig.

Grundgesamtheit	Beiträge	Bedeutung
Ländermarkierte Zahl	59 956	Gemeldete Beitragsgrundgesamtheit im angegebenen Zeitraum
Aufbewahrtes ländermarkiertes Material	59 953	Für diese Ausgabe verfügbares Material
Aufbewahrtes Forenmaterial	1 409	Aufbewahrtes Forenmaterial mit Bezug zur Schweiz
Aufbewahrtes jüngstes Material	1 595	Beiträge vom 9.–22. November
Vereintes aufbewahrtes Material	60 475	Unterschiedliche Beiträge über die Quellengruppen hinweg

Die Plattformzahlen ländermarkierter Beiträge beschreiben den Erscheinungsort. Sie zählen keine einzelnen Personen, kriminellen Gruppen oder erfolgreichen Transaktionen [S1].

Plattform	Beiträge	Grenze
Telegram	58 805	Beitragsgrundgesamtheit, keine einzelnen Teilnehmenden
Forum	887	Beitragsgrundgesamtheit, keine einzelnen Teilnehmenden
Discord	240	Beitragsgrundgesamtheit, keine einzelnen Teilnehmenden
Paste	24	Beitragsgrundgesamtheit, keine einzelnen Teilnehmenden
Tor	0	Beitragsgrundgesamtheit, keine einzelnen Teilnehmenden

Sprachkennzeichnungen beschreiben das Material. Sie belegen weder Staatsangehörigkeit der Verfassenden noch Standort eines Käufers oder Identität eines Angreifers. Ein Beitrag kann mehrere Kennzeichnungen haben [S1].

Sprache	Markierte Beiträge	Einordnung
Englisch	35 077	Sprachbeobachtung ohne Zuschreibung
Deutsch	585	Sprachbeobachtung ohne Zuschreibung
Französisch	492	Sprachbeobachtung ohne Zuschreibung
Italienisch	95	Sprachbeobachtung ohne Zuschreibung
Russisch	5 835	Sprachbeobachtung ohne Zuschreibung
Türkisch	2 039	Sprachbeobachtung ohne Zuschreibung

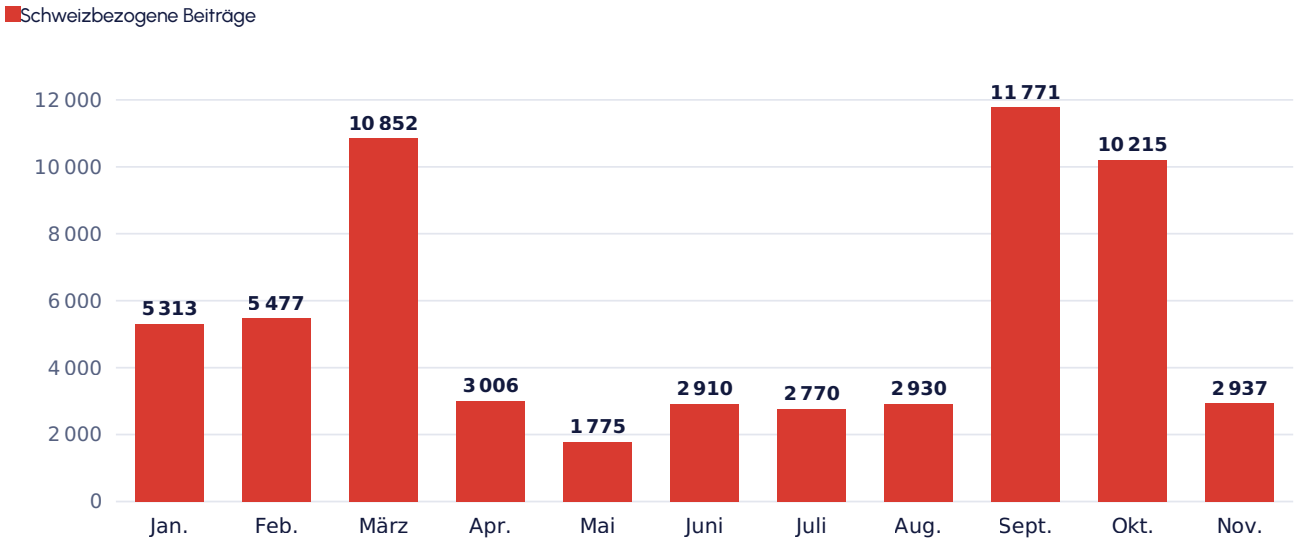
Das Monatsdiagramm behält Beiträge als Einheit. Automatisierte Werbung und wiederholtes Material können das Volumen beeinflussen. Das Diagramm unterstützt deshalb die Belegprüfung und keine Schlussfolgerung über Angriffswachstum.

Die Unterscheidung zählt, weil die Schweiz in verschiedenen Materialarten erscheint. Verkäufer können das Land in globale Bestandslisten aufnehmen. Käufer können Schweizer Informationen suchen, ohne selbst etwas anzubieten. Forenantworten können frühere Vorwürfe wiederholen. Beiträge können auch andernorts ansässige Dienste oder frühere Vorfälle international tätiger Schweizer Marken beschreiben.

Die Fallstudien beginnen deshalb mit der Aussage, die jeder Beitrag tatsächlich stützt. Eine Anzeige belegt ein beobachtetes Angebot. Ein Zitat in einer Antwort belegt die Wiederholung einer Behauptung. Ein Mustergesuch belegt eine offene Verifizierungsfrage. Keines liefert forensische Belege von der Opferseite.

Auch Aktualitätsangaben erfordern Zurückhaltung. Verkaufsbegriffe wie «frisch» können ein neu verpacktes Produkt, eine aktuelle Anzeige oder eine Behauptung über die Datensätze bezeichnen. Sie belegen weder Diebstahldatum noch aktuelle Kontogültigkeit. Für die Abwehr zählt, ob das Material zu weiterhin genutzten Konten, Prozessen oder Datensätzen passt.

Das Volumen von Beiträgen mit Schweizer Bezug schwankt, ohne die Vorfallhäufigkeit zu messen



Quelle: aufbewahrtes schweizbezogenes Beitragsmaterial, 1. Januar–22. November 2026 bis 07:20 UTC; November unvollständig. Themen können sich überschneiden; Beiträge sind keine bestätigten Vorfälle [S1].

Themenzahlen sind überlappende Beschreibungen aufbewahrten Materials. Kartenbezogene Beiträge messen weder Karten noch Verluste. Nutzen Sie die Abbildung zur Zuweisung von Prüfverantwortung, ohne einen nationalen Betrugsmarkt abzuleiten [S1].

Kartenbezogene Themen sind im aufbewahrten Beitragsmaterial häufig



Quelle: aufbewahrtes schweizbezogenes Beitragsmaterial, 1. Januar–22. November 2026 bis 07:20 UTC; November unvollständig. Themen können sich überschneiden; Beiträge sind keine bestätigten Vorfälle [S1].

4.2 Unterschiedliche Produkte erfordern unterschiedliche Reaktionen

Die Tabelle gruppiert ausgewählte Belege nach unterstützter Reaktionsentscheidung. Ihre Zeilen sind Beispiele und keine überschneidungsfreien nationalen Kriminalitätszahlen. [S1]

Material	Beobachtung	Hauptgrenze	Erste Entscheidung
Versicherungsexporte	Ein Angebot beschrieb vertragsbezogene Zeilen und zwei Dateien	Zeilen sind keine einzelnen Versicherten; Herkunft bleibt ungeprüft	Vertragsfelder und genehmigte Exporte abgleichen
Telekommunikationsdaten	Antworten bewahrten eine umfangreiche Kundendatenbehauptung	Zitierter Vorwurf und Beleggesuche bestätigen keinen Vorfall	Anbieterbelege suchen, bevor die Angebotszahl genutzt wird
Dienstleisterinformationen	Ein Angebot beschrieb Betriebs- und Gebäudeinformationen	Funktionierende Zutrittsdaten und aktueller Zugang waren nicht belegt	Dienstleister-, Cyber- und physische Sicherheitsprüfung verbinden
Personalverwaltung im Pflegesektor	Ein Angebot beschrieb Personal- und Verwaltungsdaten	Patientendaten, Echtheit und aktueller Zugang ungeprüft	Personal- und Verwaltungssysteme getrennt validieren
Geschäftsdaten im Transportsektor	Ein Angebot beschrieb Kunden-, Lohn- und Finanzunterlagen	Herkunft, Alter und aktueller Zugang ungeprüft	Geschäftsunterlagen und frühere Bereinigung prüfen
Historisches Handelsmaterial	Ein späterer Beitrag beschrieb ein früheres Ransomware-Ereignis	Beitragszeit ist keine Einbruchszeit	Frühere Bereinigung mit dem Material abgleichen
Exporte gehosteter Websites	Ein Angebot behauptete eine gemeinsame Ursache mehrerer Sites	Gemeinsame technische Ursache wurde behauptet, nicht nachgewiesen	Anbieter und Mandanten sollen eigene Systeme prüfen
Zugangsdatenkombinationen	Als schweizerisch markierte E-Mail- und Passwortdaten wurden angeboten	Länderkennung und «frisch» belegen keine aktuelle Gültigkeit	Konten über autorisierte Identitätsprozesse prüfen
Kontaktinformationen	Beiträge boten schweizerisch markierte Telefon- oder Verzeichnisabschnitte an	Ursprung, Alter und einzelne Personen bleiben ungeklärt	Personal auf überzeugende kontaktgestützte Identitätsvortäuschung vorbereiten
Kaufgesuche	Beiträge suchten Datenbanken, Postfächer oder Konten	Nachfrage ist kein Besitz oder abgeschlossener Handel	Nachfrage als Kontext für Kontoschutz nutzen

Die angemessene Reaktion kann selbst bei überlappenden Angebotsfeldern unterschiedlich sein. Versicherungsinformationen erfordern Vertrags- und Kundenserviceprüfung. Gebäudebezogene Informationen bringen physische Sicherheitsverantwortliche hinzu. Historische Zugangsdaten erfordern den Abgleich mit früheren Bereinigungen, bevor eine neue Rücksetzaktion erwogen wird.

4.3 Fünf Fälle zur Prüfung

FALL A

A

Als schweizerisch angebotene Versicherungsdaten

Belegkarte B01 | 4 Mai 2026 | Datenteilungsforum | Versicherungen

Ungeprüfte Datenteilungsbehauptung

BEHAUPTUNG	Ein Beitrag vom 4. Mai beschrieb zwei Dateien als Schweizer Versicherungsinformationen. Eine Datei enthalte 4 260 757 strukturierte Zeilen zu Verträgen, Versicherten, Fahrzeugen, Vermittlern und Finanzangaben. [S1]
CHRONOLOGIE	Derselbe Alias erschien am 4. Mai in zwei aufbewahrten Beiträgen mit sehr ähnlichem Text. Das stützt wiederholte Werbesprache und keine zwei unabhängig festgestellten Vorfälle.
VORLIEGEND	Der Text beschreibt Vertragsfelder und bietet hier ausgelassene Links an. Die behauptete Einheit ist eine Dateizeile. Sie ist keine verifizierte Zahl von Versicherten oder einzelnen Verträgen.
ALTERNATIVEN	Vertragsversionen, wiederholte Versichertendetails und zusammengeführte Verwaltungsexporte könnten wiederholte Zeilen erklären. Ebenso möglich bleiben neu verpackte historische Informationen, falsche Kennzeichnung oder ein unzutreffendes Angebot. Der Beitrag allein erlaubt keine Auswahl zwischen diesen Erklärungen.
GRENZEN	Dieser Bericht belegt weder Inhalt noch Herkunft, Alter oder Echtheit der Dateien. Er bestätigt weder einen Einbruch beim Versicherer noch aktuellen Zugang oder einen abgeschlossenen Transfer.
REAKTION	Sicherheits-, Datenschutz- und Betriebsteams sollten autorisierte Warnungen mit eigenen Exportschemata und Aufbewahrungsaufzeichnungen vergleichen. Bestimmen Sie den betroffenen Geschäftsprozess, bevor Sie Personenzahlen veröffentlichen oder Kundenauthentisierung ändern.

Fazit

Prüfen Sie Herkunft und Vertragsumfang, bevor Sie angebotene Zeilenzahlen als betroffene Personen behandeln.

Eine glaubwürdig wirkende Feldbeschreibung hilft, eine Untersuchung zuzuweisen. Sie authentisiert nicht die gesamte Datei. Die Prüfung sollte Ursprungssystem, abgedeckte Zeiträume und wiederholte Personen oder Policen feststellen.

Belegkarte B01 4 Mai 2026

NormalLeVrai Datenteilungsforum Forum Englisch

ORIGINAL

contains 4,260,757 complete lines of structured insurance data [...] information for a contract [...] related to insurance contracts (policies)

ÜBERSETZUNG

enthält 4 260 757 vollständige Zeilen strukturierter Versicherungsdaten [...] Informationen für einen Vertrag [...] bezogen auf Versicherungsverträge (Policen)

Belegt
Ein Angebot beschreibt zwei Dateien als Schweizer Versicherungsinformationen, mit behaupteter Zeilenzahl und Feldbeschreibungen.

Nicht festgestellt
Dateien, Zeilenzahl, Herkunft, einzelne Personen, aktuelle Gültigkeit, Einbruchsdatum oder abgeschlossener Transfer.

B

FALL B

Ein Telekommunikationsvorwurf in einer Antwort (B02, B03)

Telekommunikation

In Antworten zitierte Behauptung

BEHAUPTUNG	Eine Antwort vom 10. März zitierte ein Niphra zugeschriebenes Angebot. Das Zitat behauptete einen Vorfall bei einem Telekommunikationsanbieter im Januar 2026 und bot mehr als 6 Millionen Kundendetails an. [S1]
CHRONOLOGIE	Eine weitere Person verlangte am selben Tag Muster. Die Diskussion bewahrte den Vorwurf und das Gesuch um Belege. Die Daten belegen die beobachtete Diskussion, nicht den behaupteten Einbruch.
VORLIEGEND	Die gezeigten Belege sind ein Zitat innerhalb einer Antwort und eine folgende kritische Nachfrage. Das ist schwächer als ein authentisiertes Originalangebot, ein geprüftes Datenmuster oder eine Organisationsaussage.
ALTERNATIVEN	Die Person könnte ein echtes Angebot wiederholen, einen unbelegten Vorwurf kopieren oder falsch bezeichnetes Material diskutieren. Das Beleggesuch zeigt nicht, dass die Behauptung falsch ist.
GRENZEN	Angebotszahl, Datenfelder, Herkunft und Datum bleiben ungeprüft. Die Diskussion belegt weder aktuellen Zugang noch einen offiziell bestätigten Vorfall. Sie darf nicht zu den bestätigten Fällen in Kapitel 5 addiert werden.
REAKTION	Leiten Sie die Behauptung über etablierte Kanäle an Sicherheits- und Datenschutzkontakte des Anbieters. Fragen Sie nach bestätigtem Umfang und Kun-

denhinweisen. Interne Briefings müssen die Herkunft von Forenangaben deutlich machen.

Fazit

Ein Mustergesuch bewahrt eine offene Beleglücke. Es bestätigt oder widerlegt das Angebot nicht.

Eine skeptische Antwort belegt Zweifel und kein abschliessendes Urteil. Ein Mustergesuch als Widerlegung zu behandeln wäre ebenso unbegründet wie das zitierte Angebot als Bestätigung. Bewahren Sie die offene Frage und prüfen Sie Belege der verantwortlichen Organisation.

Belegkarte B02 10 März 2026

john2samira, quoting Niphra | Forenantwort mit Angebotszitat | Forum | Englisch

ORIGINAL

Date of breach: January 2026. [...] [telecommunications provider] [...] 6M+ Customer Details [...] please post some rows

ÜBERSETZUNG

Datum des Vorfalls: Januar 2026. [...] [Telekommunikationsanbieter] [...] 6M+ Kundendetails [...] bitte einige Zeilen veröffentlichen

Belegt
Eine Antwort bewahrt eine angebotene Kundendatenbehauptung und verlangt Musterzeilen.

Nicht festgestellt
Authentisierte ursprüngliche Verkäuferaussage, verifizierte Kundenzahl, Dateieigentum, aktueller Zugang oder vom Anbieter bestätigter Vorfall.

Belegkarte B03 10 März 2026

jb75 | Forendiskussion | Forum | Englisch

ORIGINAL

Please add a sample. [...] no one can take your word for it if they can't verify the data.

ÜBERSETZUNG

Bitte ein Muster ergänzen. [...] Niemand kann Ihnen einfach glauben, wenn die Daten nicht geprüft werden können.

Belegt
Eine teilnehmende Person hinterfragte die Belege zur Telekommunikationsbehauptung.

Nicht festgestellt
Nachweis einer falschen Behauptung, technische Validierung der angeblichen Daten oder unabhängige Verkäuferbestätigung.

FALL C

C ■ Dienstleisterinformationen und Fragen zur physischen Sicherheit

Ungeprüftes Dienstleisterdatenangebot

Belegkarte B04 | 5 Nov. 2026 | Datenverkaufsforum | Unternehmensdienste

BEHAUPTUNG	Eine Anzeige vom 5. November beschrieb eine Datenbank eines Schweizer Unternehmensdienstleisters. Sie behauptete 980 093 strukturierte Zeilen und beschrieb Gebäude-, Abhol-, Logistik- und Standortinformationen. [S1]
CHRONOLOGIE	Der beobachtete Beitrag warb für eine exklusive Käufervereinbarung. Zugleich erklärte der Anbieter, nicht jede Zeile geprüft zu haben. Beides belegt keine Kontrolle über einen vollständigen oder aktuellen Datensatz.

VORLIEGEND	Die Anzeige verbindet Dienstleisterinformationen mit mehreren Arten von Kundeneinrichtungen. Der Beitragstext wird privat aufbewahrt. Identifizierende Beschreibungen, Kontaktdaten und angebliche Zutrittsinformationen fehlen in der öffentlichen Karte.
ALTERNATIVEN	Das Material könnte veraltete Anweisungen, doppelte Betriebsaufzeichnungen, gewöhnliche Lieferinformationen oder falsch eingeordnete Felder enthalten. Auch ein echter Verwaltungsexport erfordert eine getrennte Beurteilung seiner aktuellen Sicherheitsbedeutung.
GRENZEN	Der Bericht bestätigt weder Zeilenzahl noch funktionierende Zutrittsdaten, erfolgreichen Zutritt, aktuellen Dienstleistervorfall oder Verkauf. Beschreibungen sensibler Kunden belegen deren Beteiligung nicht unabhängig.
REAKTION	Das Dienstleistermanagement sollte die beim Auftragnehmer vorhandenen Handhabungsanweisungen bestimmen. Die physische Sicherheit sollte passende Betriebsdetails anhand eigener Aufzeichnungen prüfen. Ersetzen Sie betroffene Anweisungen, wenn Echtheit und weitere Nutzung feststehen.

Fazit

Verbinden Sie Cyber- und physische Sicherheitsprüfung, ohne funktionierende angebotene Zutrittsinformationen anzunehmen.

Die Reaktion sollte die Verantwortlichen des physischen Prozesses einbeziehen. Ein Cyberteam erkennt möglicherweise einen Kundenexport, übersieht aber die Pflege der Betriebsfelder durch Gebäudepersonal. Ebenso darf eine dramatische Verkaufsbeschreibung keinen erfolgreichen Zutritt zu Räumlichkeiten unterstellen.

Belegkarte B04 5 Nov. 2026

pfavre Datenverkaufsforum Forum Englisch

ORIGINAL

Complete database from a [business-services provider]. [...] 980,093 structured rows [...] we have not manually verified every single row.

ÜBERSETZUNG

Vollständige Datenbank eines [Unternehmensdienstleisters]. [...] 980 093 strukturierte Zeilen [...] wir haben nicht jede einzelne Zeile manuell geprüft.

Belegt

Eine Anzeige behauptet einen Dienstleisterdatensatz mit betrieblichen Gebäudeinformationen und einer Zeilenzahl.

Nicht festgestellt

Datei, aktueller physischer Zugang, funktionierende Zutrittsdaten, behauptete Zeilenzahl oder erfolgreicher Verkauf.

FALL D

D

Älteres Handelsmaterial wird im Zeitraum erneut angeboten

Belegkarte B05 | 11 Okt. 2026 | Datenteilungsforum | Handel

Älteres Material erneut angeboten

BEHAUPTUNG	Ein Beitrag vom 11. Oktober bot Informationen zu einem Outdoorhändler an. Der Beitrag selbst beschrieb ein Ransomware-Ereignis 2025 und ein früher geschätztes Vorfallsdatum. Seine historischen Aussagen bleiben die Darstellung des Verfassers. [S1]
CHRONOLOGIE	Ähnliches Beschreibungsmaterial erschien im aufbewahrten Februar-Beitrag unter anderem Alias. Der Oktoberbeitrag ist deshalb eine neue Werbebeobachtung. Er belegt keinen neuen Einbruch im Oktober.
VORLIEGEND	Die Beiträge beschreiben ähnliche Inhalte und verweisen auf früheres Material. Übereinstimmende Beschreibungen verbinden die Angebotsdarstellungen. Sie belegen weder identische Dateien noch Transfers zwischen Aliasen oder einen gemeinsamen Betreiber.
ALTERNATIVEN	Jemand könnte eine Beschreibung kopiert, ältere Informationen neu verpackt oder Material unabhängig beschafft haben. Der Text klärt dies nicht und authentisiert keine behauptete historische Zuschreibung.
GRENZEN	Der Bericht bestätigt weder Inhalt noch Vollständigkeit oder historische Vorfallsbehauptungen. Er belegt keine weiterhin nutzbaren Zugangsdaten. Wiederholung macht aus einem Beitrag 2026 keinen bestätigten Ransomware-Vorfall 2026.
REAKTION	Gleichen Sie passendes Material mit früheren Vorfall- und Bereinigungsaufzeichnungen der Organisation ab. Prüfen Sie die weitere Relevanz alter Konten, Geheimnisse, Dienstleisterzugänge und aufbewahrter Exporte. Öffnen Sie Kontrollfragen bei rechtfertigenden aktuellen Belegen erneut.

Fazit

Ein Beitragsdatum 2026 kann älteres Material beschreiben und belegt keinen neuen Einbruch.

Historische Informationen können weiterhin eine heutige Schutzaufgabe schaffen. Ihr Abwehrwert hängt von verbleibender Gültigkeit ab und nicht vom jüngsten Anzeigendatum. Der Abschlussvermerk sollte bereinigtes Material von neu geprüften Problemen unterscheiden.

Belegkarte B05 — 11 Okt. 2026

updap | Datenteilungsforum | Forum | Englisch

ORIGINAL

Today I've uploaded [outdoor retailer] [...] DataCarry attack (2025): [...] The estimated compromise date [...] remains unconfirmed by [outdoor retailer].

ÜBERSETZUNG

Heute habe ich [Outdoorhändler] hochgeladen [...] DataCarry-Angriff (2025): [...] Das geschätzte Vorfallsdatum [...] bleibt von [Outdoorhändler] unbestätigt.

Belegt
Eine Neuveröffentlichung verbindet das angebotene Material ausdrücklich mit einem früheren Vorfall.

Nicht festgestellt
Neuer Einbruch 2026, behauptete historische Zuschreibung, Alter oder Vollständigkeit der Dateien oder unveränderte Zugangsdaten-Gültigkeit.

FALL E

E

Exporte gehosteter Sites und eine behauptete gemeinsame Ursache

Belegkarte B10 | 30 Jan. 2026 | Datenteilungsforum | Gehostete Dienste

Ungeprüfte gemeinsame Hostingbehauptung

BEHAUPTUNG	Ein Beitrag vom 30. Januar behauptete eine gemeinsame Datenbankzugangskonfiguration mehrerer Schweizer Sites. Er bot 92 SQL-Dateien und ein als 45 MB beschriebenes Paket an. Eine getrennte Forenantwort wiederholte die Behauptung. [S1]
CHRONOLOGIE	Die aufbewahrten Beobachtungen datieren Angebot und Wiederholung innerhalb des Berichtszeitraums. Sie datieren keinen zugrunde liegenden Einbruch unabhängig und bestimmen nicht die Dateierstellung.
VORLIEGEND	Der Text verbindet mehrere Sites mit einer behaupteten gemeinsamen technischen Erklärung. Die öffentliche Karte lässt Sites, Dateinamen und behauptete Zugangsdaten aus. Die Dateizahl ist keine verifizierte Organisationszahl.
ALTERNATIVEN	Die Anzeige könnte unverbundene Exporte, historische Sicherungen oder irreführende Sitezuordnungen vereinen. Gemeinsames Hosting kann eine Beziehung erklären, ohne denselben Fehler oder denselben Zugang bei jedem Mandanten zu belegen.
GRENZEN	Dieser Bericht authentisiert weder Dateien noch technische Ursachenbehauptung. Er bestätigt weder die Betroffenheit jeder aufgeführten Site noch weiteren Datenbankzugang oder einen gemeinsamen Ursprung des Materials.

REAKTION

Hostinganbieter und Mandantenverantwortliche sollten eigene Zugriffsaufzeichnungen, Verwaltungsschnittstellen und Exporthistorien prüfen. Halten Sie Mandantenbefunde getrennt, bis Belege eine gemeinsame Ursache stützen.

Fazit

Eine gemeinsame Ursache benötigt Anbieter- und Mandantenbelege statt übereinstimmender Anzeigentexte.

Eine Hypothese zu gemeinsamen Diensten kann die Zuweisung verbessern, ohne zur verifizierten Ursache zu werden. Der Anbieter kann die Verwaltungsplattform verantworten, der Kunde Anwendungskonfiguration und Daten. Die Untersuchung braucht beidseitig benannte Verantwortliche und eine gemeinsame Dokumentation gesicherter Fakten.

Belegkarte B10 30 Jan. 2026

hexvior Datenteilungsforum Forum Englisch

ORIGINAL

Multiple Swiss Sites [...] Total Package Size: 45 MB [...] 92 .sql files

ÜBERSETZUNG

Mehrere Schweizer Sites [...] Gesamtpaketgrösse: 45 MB [...] 92 .sql-Dateien

Belegt

Eine Behauptung verbindet mehrere gehostete Sites mit angebotenen Datenbankexporten; eine getrennte Antwort wiederholte sie.

Nicht festgestellt

Erfolgreicher Einbruch, gemeinsame technische Ursache, Dateigleichheit, Zahl betroffener Organisationen oder aktueller Datenbankzugang.

4.4 Zugangsdaten, Kontakte und Nachfrage

Kaufgesuche belegen keine erfolgreichen Käufe. Ein Kaufgesuch im Januar suchte aktuelle Kryptowährungsdatenbanken aus der Schweiz, Deutschland und Österreich. Es verlangte Altersnachweise und Musterzeilen. Es belegt einen geäusserten Kaufwunsch und keinen identifizierten Vorfall einer Schweizer Börse. [S1]

Eine andere Aprilanzeige suchte Postfach- oder Kontomaterial mit Schweizer Bezug und nannte eine Zahlung je geprüftem Konto. Russische und englische Passagen beschreiben das gesuchte Material nicht ganz gleich. Das begrenzt die präzise Einordnung des vorgeschlagenen Geschäfts. Weder Zahlung noch Kontokontrolle wurden verifiziert. [S1]

Belegkarte B06 6 Jan. 2026

xmrlover76 | Kaufgesuch im Forum | Forum | Englisch

ORIGINAL

interested in purchasing [...] Switzerland Crypto DBs [...] must contain minimum 5k+ lines [...] must be able to provide proof

ÜBERSETZUNG

am Kauf interessiert [...] Schweizer Krypto-Datenbanken [...] müssen mindestens 5k+ Zeilen enthalten [...] Nachweis muss möglich sein

Belegt
Ein Kaufgesuch nennt die Schweiz neben anderen Ländern und verlangt Belege zum Datenalter.

Nicht festgestellt
Angebotener Datensatz, erfolgreicher Kauf, betroffene Börse oder aktueller Schweizer Einbruch.

Belegkarte B11 17 Apr. 2026

kleinanzeige | Kontokaufforum | Forum | Russisch und Englisch

ORIGINAL

Почты на других швейцарских доменах и корпы также принимаются ОПЛАТА - 8$ ЗА 1 ВАЛИДНЫЙ АККАУНТ

ÜBERSETZUNG

Postfächer auf anderen Schweizer Domains und Firmenkonten werden ebenfalls akzeptiert. ZAHLUNG: $8 für ein gültiges Konto.

Belegt
Ein Kaufgesuch sucht Postfach- oder Kontomaterial mit Schweizer Bezug und nennt einen Preis.

Nicht festgestellt
Abgeschlossene Transaktion, aktuelle Kontokontrolle, verlässliche Auszahlung oder Übereinstimmung russischer und englischer Passagen des vollständigen Beitrags.

Beiträge zu Zugangsdatenkombinationen zeigen ein weiteres Einheitenproblem. Eine Januar-Anzeige bezeichnete eine Datei als «Switzerland» und behauptete mehr als 24 Tausend E-Mail- und Passwortzeilen. Zeilen können Duplikate, inaktive Konten, wiederverwendete Passwörter oder falsche Länderzuordnungen enthalten. Das Aktualitätsversprechen des Verkäufers ist kein unabhängiges Kontoprüfergebnis. [S1]

Die Abwehr sollte beim autorisierten Identitätsprozess der Organisation beginnen. Prüfen Sie, ob ein Konto besteht, frühere Bereinigung das Material abdeckte und aktuell ein Anmeldeproblem vorliegt. Einschneidende Massnahmen sollten geprüftem Risiko und keiner beworbenen Dateigrösse folgen.

Belegkarte B07 27 Jan. 2026

thejackal101 Zugangsdatenforum Forum Englisch

ORIGINAL

Database: Switzerland [...] Email : Password [...] [24 K++]
Line Status: FRESH | HQ

ÜBERSETZUNG

Datenbank: Schweiz [...] E-Mail : Passwort [...] [24 K++]
Zeilenstatus: FRISCH | HQ

Belegt
Eine als schweizerisch markierte Zugangsdatenanzeige mit behaupteter Zeilenzahl und Aktualitätskennzeichnung des Verkäufers.

Nicht festgestellt
Einzelne Konten, nutzbare Passwörter, Schweizer Wohnsitz, Diebstahldatum oder neu betroffene Organisation.

Belegkarte B09 18 Jan. 2026

Cod3xx Datenteilungsforum Forum Englisch

ORIGINAL

Country : Switzerland Format : csv [...]

ÜBERSETZUNG

Land : Schweiz Format : csv [...]

Belegt
Ein Beitrag bietet einen als schweizerisch markierten Kontaktexport an und beschreibt seine Struktur.

Nicht festgestellt
Beschaffungsweise, Einbruch in private Systeme, vollständige Datensätze, aktueller Zugang oder Zahl betroffener Personen.

Telefon- und Verzeichnismaterial kann überzeugende Identitätsvortäuschung unterstützen, ohne internen Netzwerkzugang zu belegen. Eine Anzeige vom 7. November bezeichnete einen Abschnitt als «Switzerland-600k». Sie beschrieb Material aus 2024–2026 und vielen Ländern. Die Behauptung erschien unter verschiedenen Aliasen. Übereinstimmender Text belegt weder identische Dateien noch gemeinsame Betreiber. [S1]

Wer Arbeitgeber, Funktion oder Vertragsdetails einer Kontaktperson kennt, kann glaubwürdig wirken. Kundenservice- und Finanzteams sollten Kontoänderungen, Zahlungen und Dokumentgesuche dennoch unabhängig prüfen. Eine angebotene Kontaktliste bestätigt nicht die Nutzung dieser Daten für Betrug.

Belegkarte B08 7 Nov. 2026

RummRif Datenverkaufsforum Forum Englisch

ORIGINAL

Year: 2024-2026 Country: [...] *Switzerland-600k [...] & from more 70+ Country.

ÜBERSETZUNG

Jahr: 2024-2026 Land: [...] *Switzerland-600k [...] & aus mehr als 70+ Ländern.

Belegt
Eine länderübergreifende Telefondatenanzeige kennzeichnet einen Abschnitt als schweizerisch und datiert das Material über mehrere Jahre.

Nicht festgestellt
Einzelne Schweizer Personen, verlässliche Zuordnung jeder Nummer, Einwilligungsstatus, Diebstahldatum 2026 oder vollendeter Betrug.

4.5 Jüngste Aktivität: 9.–22. November

Das jüngste Aktivitätsfenster beobachtet Beiträge. Es zählt keine getrennte Gruppe neu betroffener Organisationen. Wiedererscheinendes älteres Material bleibt älter, solange neue Belege keinen anderen Vorfall feststellen.

Eine angekündigte Veröffentlichung ist kein abgeschlossenes Datenleck. Ein Beitrag vom 19. November behauptete, ein ehemaliger Mitarbeiter werde am 30. November Bankinformationen veröffentlichen. Das versprochene Datum liegt nach dem Berichtsstichtag. Der Beitrag belegt weder Beschäftigung noch Dateibesitz oder aktuellen Zugang. [S1]

Die behauptete Insidergeschichte und angekündigten Inhalte bleiben Aussagen des Verfassers. Dieser Bericht authentisiert sie nicht und nennt die Bank nicht. Die Ankündigung darf in Zusammenfassung, Zeitleiste oder Bankenzahlen weder bestätigter Vorfall noch abgeschlossene Veröffentlichung werden.

Angemessen ist, die Ankündigung zu sichern und über etablierte Sicherheitsprozesse der Organisation zu prüfen. Vergleichen Sie unabhängig erlangte Belege mit autorisiertem Zugriff und Austrittsaufzeichnungen. Entscheiden Sie anhand aktueller Belege über Eskalation und schützen Sie die Vertraulichkeit der Prüfung.

Belegkarte B12 — 19 Nov. 2026

Jlkrumholz01 | Forenankündigung | Forum | Englisch

ORIGINAL

On November 30th I will release a PDF list containing all this information. [...] Wait until November 30th. [...] Account Holder Info.

ÜBERSETZUNG

Am 30 November werde ich eine PDF-Liste mit allen diesen Informationen veröffentlichen. [...] Warten Sie bis 30 November. [...] Kontoinhaberinformationen.

Belegt
Ein Beitrag vom 19 November kündigte eine künftige Bankdatenveröffentlichung nach dem Berichtsstichtag an.

Nicht festgestellt
Behauptete Beschäftigung, Dateibesitz, aktueller Zugang, Datenechtheit, betroffene Personen oder abgeschlossene Veröffentlichung.

Eine weitere Dienstanzeige vom 19. November nannte die Schweiz als eines ihrer Sprach- und Nachrichtenziele. Sie behauptete geringe Identitätsprüfungen und die Beibehaltung von Anruferinformationen. Verwandter Text erschien später erneut. Die Anzeige verifiziert diese Fähigkeiten nicht und demonstriert keine Zustellung in ein Schweizer Netz. [S1]

Die Dienstanzeige kann eine Abwehrübung unterstützen, ohne ein verifizierter Schweizer Vorfall zu werden. Prüfen Sie, ob Mitarbeitende bei sensiblen Gesuchen der angezeigten Rufnummer vertrauen. Testen Sie unabhängige Rückrufe mit bereits vertrauenswürdigen Kontaktdaten.

Das Dienstleisterangebot vom 5. November und die Telefonanzeige vom 7. November bieten nahen Kontext, liegen aber ausserhalb des jüngsten Aktivitätsfensters. Sie dürfen zur Betonung nicht dorthin verschoben werden. Ihre getrennten Prüffragen bleiben nach dem ursprünglichen Beitragsdatum relevant.

4.6 Belege mit einer klar verantworteten Entscheidung verbinden

Der Sicherheitsbetrieb sollte Quellenaussage und Prüfergebnis intern dokumentieren. Ein Beitrag kann eine Untersuchung rechtfertigen, ohne eine öffentliche Vorfallaussage zu rechtfertigen. Erfassen Sie aktuelle Konten, Systeme, Dienstleisterdatensätze oder Prozesse, die bei Echtheit des Vorwurfs betroffen wären.

Datenschutzteams sollten Dateizeilen von einzelnen Personen und Organisationsverantwortung von Datenbesitz trennen. Ein Dienstleister kann Kundeninformationen besitzen, ohne Zugang zu dessen Produktionssystemen zu haben. Bestimmen Sie Verantwortlichen- und Auftragsbearbeiterrollen anhand der tatsächlichen Beziehung.

Dienstleisterverantwortliche sollten das Inventar geteilter Informationen pflegen. Neben offensichtlichen Kundendaten gehören Betriebsanweisungen und Supportdaten hinein. Bei einer Behauptungsprüfung ermöglicht dies den Abgleich angebotener Felder mit genehmigten Geschäftsabläufen.

Kommunikationsteams sollten Akteursvorwurf, eigenen Organisationsbefund und offene Fragen auseinanderhalten. Wiederholen Sie nur für Schutzmassnahmen nötige Details. Sensible Feldbeschreibungen oder dramatische Behauptungen können die Unsicherheit vergrössern, ohne das Handeln zu erleichtern.

KERNAUSSAGEN

01

Behandeln Sie Angebot, Antwort, Kaufgesuch und bestätigten Vorfall als getrennte Belegarten

02

Prüfen Sie Alter, Eigentum und aktuelle Relevanz angebotener Informationen vor einschneidenden Massnahmen

03

Beziehen Sie physische Sicherheits- und Dienstleisterverantwortliche ein, wenn betriebliche Handhabungsinformationen betroffen sein könnten

KAPITEL 05

Beispiele für Zielauswahl nach Sektor

05

DIESES KAPITEL BEANTWORTET

Wie verändern bestätigte Vorfälle die Kontrollprioritäten verschiedener Sektoren?

97 000

Bewilligungsdatensätze, keine Personenzahl

5.1 Fälle anhand ihrer Beleggrenzen lesen 42

5.2 Kampagnen verbinden sonst getrennte Sektoren 51

5.3 Jüngste Aktivität: 9.–22. November 52

5.4 Weitere öffentliche Berichte und engere Einordnungen 53

5.5 Weitere kantonale Vorfälle und Betrugskampagnen 55

KAPITEL 05

Beispiele für Zielauswahl nach Sektor

KURZFASSUNG

Bestätigte Schweizer Fälle verbinden Informationsdiebstahl, Dienstunterbrechung und nachfolgenden Betrug. Eine kantonale Bewilligungsdatenbank, ein Vorsorgesoftwareanbieter und ein Versorgungsdienstleister zeigen unterschiedliche Abhängigkeitsrisiken. Gesundheits- und Medienfälle erfordern getrennte Beschreibungen betroffener Daten und betrieblicher Folgen. Jüngste Warnungen betreffen auch Kühlungssteuerungen. Weisen Sie jede Reaktion den Dienstverantwortlichen zu. Prüfen Sie danach betroffene Systeme, Daten und Wiederherstellungsbelege.

5.1 Fälle anhand ihrer Beleggrenzen lesen

Ein Dienstleistervorfall und ein Einbruch in ein Kundensystem sind unterschiedliche Ereignisse. Betroffene Datensätze können bei einem Auftragnehmer liegen, während eigene Produktionssysteme weiterlaufen. Ebenso kann eine Organisation Dienste wiederherstellen, während die Folgen entwendeter Informationen ungeklärt bleiben. Diese Unterschiede bestimmen Verantwortliche, Mitteilungen und Abschlusskriterien im Vorfallplan.

Die Fälle wurden nach ihrem Entscheidungswert ausgewählt. Sie sind weder eine Rangliste von Sektorrisiken noch ein Verzeichnis sämtlicher Schweizer Einbrüche. Daten bezeichnen entsprechend ihrer Kennzeichnung den Vorfall oder das öffentliche Update. Datensatzzahlen bleiben ihrer ursprünglichen Grundgesamtheit zugeordnet. Öffentliche Ankündigungen geben diesem Bericht keinen forensischen Zugang auf Opferseite.

Die Tabelle trennt zentrale Kontrollfragen, bevor die Fallkarten Details liefern.

Sektor	Berichteter Sachverhalt	Beleggrenze	Erste Entscheidung
Kantonale Dienste	Datendiebstahl aus einer Bewilligungsdatenbank	Eine Person kann mehrfach vorkommen	Antragstellende und Arbeitgeberkontakte schützen
Gesundheitswesen	Ransomware unterbrach den Zugriff auf Bildgebungsinformationen	Diebstahl medizinischer Daten bleibt ungeklärt	Klinische Ausweichabläufe und Abruf testen
Vorsorge	Datendiebstahl beim Anbieter löste Untersuchungen aus	Dienstleisterereignis belegt keinen Einbruch in Produktionssysteme	Inventar übertragener Daten feststellen
Medien	Historische Personalkontaktdaten betroffen	Keine gemeldeten Hinweise auf Offenlegung von Quellen oder Recherchematerial	Mitarbeitende unterstützen und Aufbewahrung prüfen
Energie	Adress- und Zählerinformationen beim Auftragnehmer entwendet	Laut Versorger blieben Systeme und Versorgung unberührt	Dienstleisterdatensätze abgleichen
Handel und Gebäudebetrieb	Kühlungseinstellungen manipuliert	Öffentliche Darstellung belegt keinen benannten Akteur	Temperatur und unabhängige Alarme prüfen

FALL F

F

Kantonale Bewilligungsdaten und nachfolgendes Identitätsrisiko (O01)

Öffentliche Verwaltung

Offizielle Offenlegung; Datensätze sind keine Personen

DARSTELLUNG	Basel-Landschaft bestätigte am 20. November 2026 Datendiebstahl aus seiner Datenbank für Grenzgängerbewilligungen. Die Ankündigung nannte 97 000 Datensätze mit persönlichen Informationen und Arbeitgeberkontakten. [S17]
CHRONOLOGIE	Ein Update vom 18. November beschrieb Auswirkungen auf ungefähr 20 Anwendungen. Die Erklärung vom 20. November bestätigte Datendiebstahl. Das Bewilligungssystem war seit dem 28. November 2016 in Betrieb. [S47][S17]
FESTGESTELLT	Der Kanton nannte unter anderem Namen, Adressen, Geburtsdaten, Berufsangaben und Migrationssystemkennungen. Die betroffene Onlineplattform wurde abgeschaltet. Gesuche konnten weiterhin über alternative Verfahren eingereicht werden. [S16][S17]
GRENZEN	Der Kanton unterscheidet ausdrücklich Datensätze von Personen. Verlängerungen, Adress- und Beschäftigungswechsel können wiederholte Einträge erzeugen. Die FAQ bestätigen keinen Diebstahl hochgeladener Ausweisdokumente oder Arbeitsverträge. [S16]
ALTERNATIVEN	Historische Einträge können einen Teil des Datenvolumens erklären. Die Gesamtzahl lässt sich nicht in aktuelle Bewilligungsinhaber, einzelne Personen oder bestätigte Identitätsbetrugsopfer umrechnen. [S16]
REAKTION	Öffentliche Dienste und Personalabteilungen sollten betroffene Abläufe bestimmen, die offizielle Warnung sichern und ungewöhnliche Gesuche unabhängig prüfen. Richtige persönliche Angaben dürfen Authentisierung nicht ersetzen.

Fazit

Prüfen Sie Abläufe von Antragstellenden und Arbeitgebern. Nutzen Sie danach vertrauenswürdige Kontaktwege.

Der begründbare Befund ist bestätigter datenbankbezogener Datendiebstahl mit ungeklärtem Personenumfang. Es handelt sich nicht um 97 000 Personen. Die unmittelbare Schutzaufgabe schliesst Arbeitgeber ein, weil ihre Verwaltungskontakte ebenfalls in den betroffenen Informationen erscheinen. [S16]

FALL G

G ■ Radiologiekontinuität und getrennte Fragen zu entwendeten Daten (O02)

Gesundheitswesen

Ransomware gemeldet; medizinischer Datendiebstahl ungeklärt

DARSTELLUNG	Groupe 3R nennt einen Ransomware-Angriff vom 30. April 2026. Die Gruppe meldet Verschlüsselung und Diebstahl administrativer Informationen, darunter Angaben zu aktuellen und ehemaligen Mitarbeitenden. [S18]
CHRONOLOGIE	Die Patientenversorgung war am 1 und 2. Mai besonders beeinträchtigt. Laut Betreiber verfügten die Zentren ab 26. Juni über eine neu aufgebaute Infrastruktur. Seine öffentliche Informationsseite enthält einen Lagebericht vom 22. September. [S18]
FESTGESTELLT	Medizinische Untersuchungsergebnisse wurden verschlüsselt und waren dadurch eingeschränkt verfügbar. Laut Betreiber blieben die Zentren offen. Manche Untersuchungen wurden verzögert, verschoben oder umgeleitet. Wichtige Systeme und Teleradiologie wurden anschliessend wiederhergestellt. [S18]
GRENZEN	Der Betreiber konnte nicht sicher feststellen, ob auch medizinische Patientendaten entwendet wurden. Eine fehlende bestätigte Veröffentlichung dieser Dateien klärt diese Frage nicht. [S18][S19]
ALTERNATIVEN	Dienstwiederherstellung und Datenvertraulichkeit erfordern getrennte Abschlussentscheidungen. Laut Betreiber steht das Ereignis 2026 nicht mit seinem Vorfall 2025 in Verbindung. Der frühere Angriff darf nicht erneut als Fall 2026 gezählt werden. [S18]
REAKTION	Der klinische Betrieb sollte den Abruf von Untersuchungsergebnissen, Überweisungsalternativen und Terminbestätigungen testen. Sicherheits- und Datenschutzteams sollten Datendiebstahl und möglichen späteren Patientenbetrug getrennt beurteilen.

Fazit

Testen Sie klinische Abläufe. Beurteilen Sie Vertraulichkeit getrennt von Wiederherstellung.

ICTjournal berichtet, der Betreiber habe den Angriff unter Verweis auf Befunde spezialisierter Partner Akira zugeschrieben. Dies ist die von der Publikation wiedergegebene Betreiberzuschreibung. Dieser Bericht besitzt keine unabhängigen technischen Belege zur Verbindung eines Akteurs mit dem Vorfall. [S19]

Ein erfolgreicher Wiederherstellungstest sollte im Gesundheitswesen den gesamten klinischen Ablauf umfassen. Ein wiederhergestellter Server zeigt nicht, dass Fachpersonen Bilder abrufen, Untersuchungen beurteilen und mit zuweisenden Praxen kommunizieren können.

FALL H

H ■ Vorsorgedaten beim Dienstleister und Untersuchungsumfang (O03)

Vorsorge

Dienstleisterverfall; Untersuchung läuft weiter

DARSTELLUNG	Publica bestätigte ein Datenleck nach einem Angriff, den ein externer Softwareanbieter Ende September festgestellt hatte. Der Anbieter informierte Publica, weitere Kunden und zuständige Bundesbehörden. [S21]
CHRONOLOGIE	Publica verschickte am 8. Oktober eine erste Versichertenmitteilung. Der EDÖB erhielt am selben Tag die Anbietermeldung. Er begann am 14. Oktober Vorabklärungen zu Publica und eröffnete am 22. Oktober eine Anbieteruntersuchung. [S21][S15]
FESTGESTELLT	Laut EDÖB wurden Daten mehrerer Vorsorgeeinrichtungen entwendet. Seine Untersuchung soll übermittelte Personendaten, rechtliche Übermittlungsgrundlagen und den Umfang verlorener Informationen klären. [S15]
GRENZEN	Ein bestätigtes Dienstleisterdatenleck bestimmt nicht jede betroffene Person, jedes Feld oder den Betriebszustand jedes Kundensystems. Die Untersuchung war in der zitierten Ankündigung noch offen. [S15]
ALTERNATIVEN	Ein Arbeitsdatensatz beim Anbieter und eine produktive Vorsorgedatenbank haben unterschiedliche Rollen. Die öffentliche Darstellung darf nicht zu unbelegten Aussagen über Zugriff auf Letztere erweitert werden.
REAKTION	Vorsorgeverantwortliche sollten beim Anbieter aufbewahrte Daten mit Vertragszwecken und Aufbewahrungspflichten abgleichen. Versichertenservices sollten die Identität unabhängig prüfen, wenn Anrufende persönliche oder finanzielle Details bereits kennen.

Fazit

Gleichen Sie Anbieterinformationen mit Vertragszwecken und Versichertenschutz ab.

Der Fall schafft zwei getrennte Arbeitsstränge. Der erste klärt, welche Informationen der Anbieter hielt und was entwendet wurde. Der zweite schützt Versicherte vor überzeugenden Kontaktversuchen mit diesen Angaben. Die Kundenkommunikation sollte die Beziehung zwischen beiden Strängen ausdrücklich erläutern.

Cybercrimepolice warnt zudem vor Anlageangeboten nach einem Datenleck bei einem Vorsorgedienstleister. Die Darstellung betrifft möglichen Missbrauch von Lohn- und Vorsorgeinformationen. Die Warnung unterstützt die Betrugsvorbereitung. Sie ist keine verifizierte Liste sämtlicher bei diesem Anbieter entwendeten Felder. [S45]

Am 19. November kündigte Publica eine externe Untersuchung zu Beschaffung, Personendatenbearbeitung, Sicherheitskontrollen und Governance an. Sie nannte die Testumgebung des Anbieters als betroffenen Bereich. Publicas Produktionssysteme seien unberührt. Technische Abklärungen zu betroffenen Personen und Daten waren noch nicht abgeschlossen. [S55]

FALL I

Historische Medienpersonaldaten und Grenzen einer breiteren Deutung (O04)

Medien

Historische Personalinformationen gemeldet

DARSTELLUNG	SRG meldete am 28. September einen Cybervorfall mit Kontakt- und Organisationsinformationen aus 2020 zu ungefähr 340 aktuellen und ehemaligen SRF-Mitarbeitenden. [S20]
CHRONOLOGIE	Laut SRG wurde der betroffene Zugang deaktiviert. Zusätzliche Sicherheitsmassnahmen wurden ergriffen, Behörden benachrichtigt und Betroffene informiert. Bei der Ankündigung lief die Untersuchung weiter. [S20]
FESTGESTELLT	Die Angaben umfassten Namen, Funktionen und geschäftliche Kontaktdaten sowie teilweise private Kontakte. SRG beschrieb die betroffene Personengruppe und unterstützte die Betroffenen. [S20]
GRENZEN	SRG meldete keine Hinweise auf betroffene Passwörter, Finanzinformationen, journalistische Quellen, Recherchematerial oder Kommunikationsinhalte. Ebenso gab es damals keine Hinweise auf Veröffentlichung oder Missbrauch. [S20]
ALTERNATIVEN	Historische Mitarbeiterinformationen können ihren Wert für Social Engineering behalten. Ihr Vorliegen belegt keine Einmischung in Berichterstattung, redaktionelle Entscheidungen oder Sendebetrieb.
REAKTION	Sicherheit und Personal sollten prüfen, weshalb historische Kontaktdatensätze zugänglich bleiben. Mitarbeiterunterstützung sollte Identitätsvortäuschung und verdächtige Kontaktversuche abdecken, ohne ungeprüfte Folgen als festgestellten Schaden darzustellen.

Fazit

Prüfen Sie Aufbewahrung und Zugang. Unterstützen Sie Mitarbeitende gegen Identitätsvortäuschung.

Die Kontrolllehre betrifft aufbewahrte Informationen und Zugriffsverwaltung. Die Rolle einer Medienorganisation rechtfertigt keine Zuschreibung eines politischen Motivs. Die zitierte Darstellung bietet dafür keine Grundlage. Der Bericht trennt deshalb Datenkategorie und ungeklärte Ursache. [S20]

FALL J

J

Versorgerdaten beim Auftragnehmer ohne Energieversorgungsvorfall (O05)

Energie und Versorgung

Dienstleisterdaten: Versorgungssysteme laut Meldung unberührt

DARSTELLUNG	IWB teilte am 15. Juli mit, Angreifer hätten ungefähr 40 000 Adressdatensätze bei einem Dienstleister entwendet. Dazu gehörten technische Angaben zu Energiezählern. [S40]
CHRONOLOGIE	Der Anbieter informierte IWB nach Feststellung des Angriffs. IWB prüfte Zugriffe, begrenzte den Austausch mit diesem Anbieter und schrieb betroffene Kunden an. [S40]
FESTGESTELLT	Der Versorger nannte Namen, Adressen, Zählernummern und Installationsmerkmale. Seine Systeme und die Sicherheit der Energieversorgung seien unberührt. [S40]
GRENZEN	Laut IWB enthielt der entwendete Datensatz keine E-Mail-Adressen, Telefonnummern, Verbrauchs-, Bank- oder Zahlungsdaten. Zum damaligen Zeitpunkt lagen keine Missbrauchshinweise vor. [S40]
ALTERNATIVEN	Ein versorgerbezogener Datensatz belegt keinen Angreiferzugriff auf Betriebssteuerungen. Adress- und Zählerinformationen sollten nicht als vollständiges finanzielles Kundenprofil beschrieben werden.
REAKTION	Dienstleisterverantwortliche sollten das mit Auftragnehmern geteilte Inventar prüfen. Kundenservices sollten sich auf Kontaktversuche vorbereiten, die eine echte Adresse oder Zählernummer mit dringenden Zahlungs- oder Auskunftsforderungen verbinden.

Fazit

Gleichen Sie Dienstleisterinformationen ab. Bereiten Sie Kundenservices auf überzeugende Gesuche vor.

Laut IWB bewertete die kantonale Datenschutzbehörde das Missbrauchsrisiko als niedrig. Diese Bewertung gehört zu den beschriebenen Informationen und Umständen. Sie darf nicht zur allgemeinen Aussage werden, Datendiebstahl bei Auftragnehmern sei harmlos. [S40]

FALL K

K ■ Kühlungssteuerung und unabhängige Prüfung des physischen Prozesses (O06)

Handel und Gebäudebetrieb

Offizielle Warnung: Akteur nicht zugeordnet

DARSTELLUNG	Das BACS warnte am 10. November vor Kühlungssteuerungsangriffen auch in der Schweiz. Eine Polizeimeldung vom 12. November beschreibt manipulierte Einstellungen bei einem Schweizer Betrieb. Deutliche Temperaturabweichungen führten zur vorübergehenden Filialschliessung. [S53][S41]
CHRONOLOGIE	Die Meldungen gehören zum jüngsten Aktivitätsfenster. Sie behandeln aus den vorausgehenden Wochen bekannte Angriffe. Für den einzelnen Betrieb nennen sie kein verifiziertes Datum des Erstzugriffs. [S53][S41]
FESTGESTELLT	Die Polizei beschreibt veränderbare Temperaturen, Abtauzyklen und Alarmeinstellungen über ungenügend geschützte Verwaltungsschnittstellen. Sie empfiehlt die Prüfung tatsächlicher Temperaturen mit einem unabhängigen Messgerät. [S41]
GRENZEN	Die verfügbaren Darstellungen belegen weder benannten Akteur noch politisches Motiv. Die technische Warnung umfasst mehrere Produktfamilien. Sie identifiziert nicht das von einem bestimmten Opfer betriebene System. [S53]
ALTERNATIVEN	Eine stille Alarmanzeige belegt keinen gesunden physischen Prozess, wenn Alarme veränderbar sind. Gerätefehler und unberechtigte Änderungen erfordern unterschiedliche Untersuchungen, aber beide benötigen unabhängige Sicherheitsprüfungen.
REAKTION	Gebäudebetrieb, Kühlungsdienstleister und IT sollten Fernzugriff, unterstützte Software und Alarmzustellung gemeinsam prüfen. Schützen Sie notwendige Fernwartung. Bestätigen Sie vor Normalbetrieb die tatsächlichen Temperaturen.

Fazit

Prüfen Sie physische Temperatur unabhängig und kontrollieren Sie Fernverwaltungszugang.

Der Fall begrenzt auch die Interpretation älterer nationaler Einschätzungen. Das BACS nannte im Halbjahresüberblick keine bekannte gezielte Cybersabotage in der Schweiz. Ein späterer Betriebstechnikvorfall ist nach eigenen Fakten zu beurteilen, ohne ihn in staatliche Sabotage umzudeuten. [S5][S41]

FALL L

L ■ Bundeszugang zur Zusammenarbeit und betroffene Konten (O07)

Öffentliche Verwaltung

Offizielle Darstellung: ungefähr 200 Konten

DARSTELLUNG	Das Bundesamt für Informatik teilte am 4. August mit, ungefähr 200 Benutzer- und technische Konten seien von einem Angriff auf seine SharePoint-Server betroffen. [S54]
CHRONOLOGIE	Fachleute erkannten am 28. Juli ungewöhnliche Aktivität. Die Analyse identifizierte am 31. Juli betroffene Kontozugangsdaten. Das Amt setzte Passwörter zurück, sperrte externen Internetzugang und begann den Serverneuaufbau. [S54]
FESTGESTELLT	Die Amtsdarstellung trennt betroffene Zugangsdaten von anderen Informationen. Die bis zur Veröffentlichung vorliegende Analyse enthielt keine Hinweise auf zusätzlichen Datendiebstahl. Interne Nutzer behielten Dokumentenzugriff und alternative Austauschmöglichkeiten. [S54]
GRENZEN	Fehlende Hinweise sind keine abgeschlossene forensische Feststellung. Die Meldung nennt keinen Akteur. Sie rechtfertigt weder eine Motivzuschreibung noch die Ausweitung der betroffenen Grundgesamtheit über die beschriebenen Konten hinaus. [S54]
REAKTION	Verantwortliche für Zusammenarbeitsdienste sollten Zugangswiderruf und alternativen Dokumentaustausch testen. Trennen Sie die Freigabe externen Zugangs von den Belegen zum Abschluss der Datendiebstahluntersuchung.

Fazit

Prüfen Sie Kontoumfang und betroffene Dienste, ohne eine grössere Grundgesamtheit abzuleiten.

FALL M

M ■ Bildungssupporttickets und gezielte Helpdesk-Vortäuschung (O08)

Bildung

Offizielle Offenlegung: schulische Kontaktinformationen

DARSTELLUNG	Waadt meldete unberechtigte Kopien von Namen und schulischen E-Mail-Adressen von ungefähr 3500 Lehrpersonen und 38000 Lernenden. Inhalte von Supportanfragen wurden ebenfalls kopiert. [S59]
CHRONOLOGIE	Der Kanton erkannte den unberechtigten Zugriff am 26. Oktober. Er trennte die Supportplattform, sicherte sie mit seinem Sicherheitsbetriebszentrum und informierte die Nutzenden direkt. [S59]

FESTGESTELLT	Der Dienst bearbeitete IT-Supportanfragen der nachobligatorischen Bildung. Laut Kanton waren dort keine Kontopasswörter gespeichert. Schulunterlagen wie Noten und Schülerdossiers waren nicht betroffen. [S59]
GRENZEN	Tickettext und Bildungsdatenbank sind unterschiedliche Grundgesamtheiten. Der Fall belegt nicht, dass Angreifer sämtliche Passwörter oder Schulunterlagen erlangten. [S59]
REAKTION	Die Bildungs-IT sollte vor vorgetäuschten Schul- oder Helpdesknachrichten warnen. Verlangen Sie verifizierte Supportanfragen. Prüfen Sie, ob Anhänge oder Freitexttickets mehr Informationen als betrieblich nötig aufbewahren.

Fazit

Schützen Sie betroffene Bildungsidentitäten. Prüfen Sie ungewöhnliche Kontakte über vertrauenswürdige Wege.

N

FALL N

Erwachsenenbildung und eine veränderte Datenfolgenbewertung (O09)

Bildung

Offizieller Vorfall; Umfang später korrigiert

DARSTELLUNG	Laut Ifage führte ein Angriff am 11.–12. April zu Datendiebstahl. Die Erkennung folgte am 13. April. Eine spätere Meldung erklärt, die Veröffentlichung am 23. Juli habe auch betroffene Lernenden- und Kundendaten belegt. [S58]
FESTGESTELLT	Die Einrichtung nennt Kursverwaltung, Kontaktdaten und Prüfungsdokumente. Manche Dateien enthielten Ausweise, Bewerbungsunterlagen oder Abwesenheitsbegründungen. Die betriebliche Kontinuität sei gewahrt geblieben. [S58]
GRENZEN	Die Meldung nennt keine verifizierte Zahl betroffener Personen. Eine spätere Klärung erweitert den bekannten Umfang eines Vorfalls. Sie schafft keinen zweiten Einbruch. [S58]
ALTERNATIVEN	Eine erste Ankündigung kann eine unvollständige Untersuchung korrekt wiedergeben. Lesende sollten veränderte Erkenntnisse von einem neuen Angriff oder verifiziertem anhaltendem Zugriff unterscheiden.
REAKTION	Bildungs- und Datenschutzteams sollten ein versioniertes Datenfolgenregister führen. Aktualisieren Sie direkte Mitteilungen bei neu festgestellten Kategorien. Bewahren Sie Datum und Grundlage früherer Bewertungen.

Fazit

Halten Sie die korrigierte Datenbeurteilung von früherer Dienstwiederherstellung getrennt.

FALL O

Universitäre Onlineformulare im jüngsten Aktivitätsfenster (O10)

Bildung

Offizielle Offenlegung: Onlineformularinformationen

DARSTELLUNG	USI kündigte am 19. November an, unberechtigte Dritte hätten zwischen 9 und 17. November über ein verwundbares Onlineformularsystem auf Informationen zugegriffen. [S80]
FESTGESTELLT	Die Anwendung unterstützte manche Stellenbewerbungen, Stipendiengesuche und Umfragen. Formularantworten und Anhänge lagen auf dem Server. Die Universität sicherte ihn und informierte Behörden sowie potenziell Betroffene. [S80]
GRENZEN	USI klärte nach eigener Aussage Umfang, Sensibilität und Risiken der Informationen weiter ab. Die Ankündigung nannte keine verifizierte Personenzahl und belegte nicht das Kopieren jedes Anhangs. [S80]
ALTERNATIVEN	Unterschiedliche Formulare sammeln unterschiedliche Informationen. Stellenbewerbende, Stipendienbewerbende und Umfrageteilnehmende sollten keine einheitliche Datenrisikogruppe bilden.
REAKTION	Anwendungsverantwortliche sollten Zwecke und Aufbewahrungszeiten betroffener Formulare bestimmen. Empfänger sollten unerwartete Dokument-, Bank- und Zahlungsgesuche über etablierte Universitätskanäle prüfen.

Fazit

Bestimmen Sie betroffene Formulare, sichern Sie die Meldung und prüfen Sie Folgegesuche unabhängig.

5.2 Kampagnen verbinden sonst getrennte Sektoren

Mehrere offizielle Warnungen beschreiben einen gemeinsamen Mechanismus statt eines benannten Opfers. Sie sind relevant, weil Dienstleisterkunden, Mitarbeitende und Haushalte verbundenen Betrugsstufen begegnen können. Die Abfolge belegt keinen gemeinsamen Betreiber sämtlicher Stufen.

Die Kampagnentabelle bewahrt die Quelleneinheit und nennt eine angemessene Kontrollreaktion.

Meldedatum	Kampagnendarstellung	Verbleibende Unsicherheit	Abwehrentscheidung
2026-02-03	Echte SharePoint-Freigaben führten zu späterem Echtzeitphishing [S24]	Die Meldung zählt nicht alle betroffenen Organisationen	Gesamten Linkverlauf und Sitzungsexposition prüfen

Meldedatum	Kampagnendarstellung	Verbleibende Unsicherheit	Abwehrentscheidung
2026-02-10	Abonnementbombardierung verdeckte wichtige Kontonachrichten [S25]	Ein überfülltes Postfach allein belegt keine betrügerische Zahlung	Konto-, Bestell- und Zahlungsänderungen suchen
2026-02-24	ClickFix-Köder verleiteten zur Ausführung schädlicher Befehle [S26]	Nutzerhandlung zeigt nicht den gesamten Einbruchsweg	Falsche Reparaturen zum Helpdesk leiten und Endpunktbelege prüfen
2026-04-14	Falsches Bankpersonal verlang-te Fernwartungssoftware [S27]	Bankmarken im Gespräch belegen keinen Bankeinbruch	Anrufe unabhängig prüfen und unaufgeforderten Fernsupport begrenzen
2026-05-05	Paketphishing folgte ein falscher Bankanruf [S28]	Kampagnenumfang und Betreiberidentität sind nicht festgestellt	Kunden die tatsächliche Autorisierung einer Zahlungsbestätigung erklären
2026-06-09	Stellensuchende trafen auf Interviewphishing, Zahlungsforderungen und Schadsoftwareköder [S30]	Die Meldung beschreibt unterschiedliche Maschen	Rekrutierungs- und Zahlungsabläufe trennen
2026-09-01	Eine Essenslieferwebsite diente versuchtem Zahlungsdatendiebstahl [S32]	Die Quelle identifiziert nicht jede betroffene Transaktion	Änderungen der Zahlungsseite und Drittinhalte überwachen
2026-10-20	Hotelbuchungsköder zielten zunehmend auf Mobilzahlung und Bankzugang [S34]	Buchungswissen belegt nicht jede vorgelagerte Ursache	Ungewöhnliche Gesuche über den gebuchten Anbieter bestätigen

5.3 Jüngste Aktivität: 9.–22. November

Richtige persönliche Angaben belegen kein vertrauenswürdiges Gesuch mehr. Die BACS-Meldung vom 17. November verbindet ein früheres Datenleck eines Haushaltsdienstleisters mit gezieltem Phishing. Nachrichten nutzten Namen, Adressen und Sozialversicherungsnummern. Die Meldung beschreibt zudem Phishing unter dem Vorwand eines PHP-Sicherheitsupdates. [S14]

Die Polizeimeldung derselben Woche beschreibt Ferienbuchungsnachrichten mit echten Unterkunftsangaben und Buchungsreferenzen. Angreifer verlangten angebliche Reservationsbestätigung und danach Zahlungskartendaten. Dieser Bericht behält die Dienstleisterrolle bei, weil die Voraussetzungen einer Namensnennung nicht vollständig belegt sind. [S43]

Die Polizeiwarnung vom 18. November ergänzt eine physische Zahlungsstufe. Anrufende gaben sich als Bankpersonal aus. Sie nutzten ein gefälschtes Zentralbankschreiben, um Bargeld für ein angebliches Sicherungskonto zu fordern. Die behauptete Autorität gehört zur Betrugsgeschichte und belegt keine Zentralbankbeteiligung. [S44]

Das Update von Basel-Landschaft vom 20. November macht die Verbindung zwischen Daten und Betrug unmittelbar relevant. Personalabteilungen sollten Kontaktversuche mit echten Beschäftigungs- oder Bewilligungsangaben erwarten. Die Erklärung stützt erhöhte Wachsamkeit. Sie belegt nicht, dass jede betroffene Person bereits eine betrügerische Nachricht erhielt. [S16][S17]

USIs Meldung vom 19. November ergänzt Onlineformulare und Anhänge auf der unmittelbaren Aufgabenliste. Publicas Update desselben Tages betrifft eine externe Governance-Prüfung ihres bestehenden Dienstleistervorfalls. Dies sind unterschiedliche Entwicklungen: ein neu offengelegter Universitätsvorfall und eine spätere Reaktion auf ein früheres Vorsorgedatenereignis. [S80][S55]

Diese Updates stützen eine praktische Novemberübung. Geben Sie Kundenservice und Helpdesk ein unerwartetes Gesuch mit richtigen persönlichen Angaben. Verlangen Sie unabhängige Prüfung, Nachrichtensicherung und Entscheidungsdokumentation. Messen Sie, ob das Team trotz überzeugender Angaben dem vertrauenswürdigen Prozess folgt.

5.4 Weitere öffentliche Berichte und engere Einordnungen

Die folgenden Punkte erweitern die Sektorabdeckung, ohne ungeprüfte Akteursdarstellungen zu übernehmen. Wo keine direkte öffentliche Bestätigung aufbewahrt wurde, bleibt die Organisation als Rolle beschrieben. Die verlinkte Publikation ist Quelle der wiedergegebenen Organisationsdarstellung.

Datum	Rolle	Berichtete Darstellung	Einordnung
2026-01-23	Radio- und Veranstaltungsbetreiber	Externe Veranstaltungsdatenbank betroffen; Passwörter und Zahlungsdaten laut Bericht ausgenommen [S56]	Beispiel für Dienstleisterdatenoffenlegung
2026-03-04	Unternehmenssoftwareanbieter	Unternehmen bestätigte Vorfall mit begrenzten Betriebsfolgen; gesondert angebotenes Datenvolumen bleibt Behauptung [S50]	Behauptung und Auswirkung getrennt
2026-03-25	Ingenieurdienstleister	Auf Februarvorfall folgten vorsorgliche Trennung und gemeldete Wiederherstellung [S48]	Unerwartete Lieferantenrechnungen prüfen
2026-04-14	Medizinproduktehersteller	Unternehmensdarstellung nannte älteres internes System und ältere interne Dokumente [S49]	Beispiel für Aufbewahrung in Altsystemen
2026-08-26	Wirtschaftshochschule	Externer Anbietervorfall betraf Studierenden- und Alumnidaten; laut Hochschule lief lokaler Betrieb weiter [S57]	Anbieter- und lokale Systeme unterschieden
2026-07-09	Wohn- und Betreuungsanbieter	Ransomware störte Systeme; Oktoberupdate beschrieb teilweisen Neuaufbau und fortgesetzte Betreuung [S81]	Längere Kommunikations- und Betreuungsausweichverfahren testen

Datum	Rolle	Berichtete Darstellung	Einordnung
2026-03-14	Gemeindeverwaltung	Teilverschlüsselung mit anschliessender Wiederherstellung; Gemeinde meldete keine Datendiebstahlhinweise [S86]	Wiederherstellung und Datendiebstahlbefunde trennen
2026-07	Industrieunternehmen	Kantonaler Überblick beschrieb Zugriff auf Dienstleister-Austauschplattform und gesonderte Erpressungsforderung [S84]	Umfang gemeinsamer Plattformen bestätigen
2026-07	Treuhanddienste	Kantonaler Überblick beschrieb veröffentlichte Kundendateien nach einem Vorfall [S84]	Steuer- und Kundendokumente bei Beratern inventarisieren
2026-09	Spitallaborpartner	Kantonaler Überblick beschrieb betroffene Patienteninformationen bei einem externen Labor [S85]	Laborübermittlungen und Patientenkontakte abgleichen
2026-10-26	Sportverwaltungsplattform	Verband bestätigte unberechtigten Kontozugriff und folgendes Forenangebot; Passwörter unberührt [S88]	Kontoberechtigungen prüfen und Teilnehmende warnen
2026-10-31	Sportlizenzplattform	Verband bestätigte Personendatenvorfall, hatte vollständigen Umfang aber noch nicht geklärt [S87]	Angebotszeilen nicht als Personen behandeln
2026-11-16	Streamingwebsite	Sicherheitsforscher meldete schädliche Drittanbieterskripte bei einem Schweizer Streamingdienst [S89]	Browserseitige Abhängigkeiten und Anbieterhinweise prüfen

Das Oktoberupdate des Betreuungsanbieters ging weiter von einem Datenleck aus, ohne dessen Umfang festzustellen. Grundpflege, medizinische Unterstützung und Sicherheit der Bewohnenden seien gewährleistet geblieben. Erwarteter Normalbetrieb bis Ende November war eine Prognose und kein bestätigtes Wiederherstellungsdatum. [S81]

Offizielle Meldungen unterscheiden zudem Schutzmassnahmen von Einbrüchen. Eine Behörde berichtete über vorübergehende Diensteinschränkungen zur Behebung von PHP-Schwachstellen im Oktober, ohne einen entsprechenden Angriff festgestellt zu haben. Die Aprilwarnung des EDÖB betraf dessen Identitätsvortäuschung und keinen Zugriff auf seine Systeme. [S83][S82]

Diese Beispiele dürfen den Fallkartenzahlen nicht als neue Belegkarten zugeschlagen werden. Es sind Vorfallserwähnungen. Der Unterschied ist eine Darstellungsentscheidung und keine Behauptung geringerer Geschäftsauswirkungen.

5.5 Weitere kantonale Vorfälle und Betrugskampagnen

Trennen Sie unberechtigten Zugriff von vorsorglichen Dienstbeschränkungen. Eine kantonale Behörde meldete am 5. August einen SharePoint-Vorfall. Ihre vorläufige Analyse zeigte keine Hinweise auf betroffene Konten oder Datendiebstahl. Ein abendliches Sicherheitsupdate sollte die öffentliche Website vorübergehend unterbrechen. Andere Anwendungen blieben verfügbar. Die Meldung beschreibt einen anderen Vorfall als den Zusammenarbeitsfall des Bundes. [S90]

Auch öffentliche Informationen können überzeugenden Betrug unterstützen. Eine gemeinsame Meldung vom 28. August beschrieb automatisierte Sammlung öffentlich zugänglicher Fahrzeughalterinformationen aus fünf Kantonen. Gesperrte Einträge waren nicht betroffen. Die Meldung beschrieb zudem Erpressungsversuche und warnte vor Zahlungsforderungen mit diesen Angaben. Sie belegt keinen Diebstahl geschützter Fahrzeugdatensätze. [S91]

Die folgenden Polizeimeldungen ergänzen das jahresweite Identitätsvortäuschungsmuster um lokale Belege. Sie betreffen unterschiedliche Zeiträume und Grundgesamtheiten. Ihre Zahlen dürfen nicht zu einer nationalen Vorfalls- oder Verlustzahl addiert werden.

Meldung	Polizeidarstellung	Umfangsgrenze	Massnahme
2026-01	Waadt erfasste in der Woche des 12. Januar 24 Fälle falscher Bank- oder Polizeikontakte, darunter 12 Versuche [S92]	Eine kantonale Woche	Kundenpersonal für dringende Bargeldforderungen schulen
2026-02-10	St.Gallen beschrieb Fernzugriffsbetrug mit Einzelverlust über CHF 500 000 Ende Januar [S93]	Verlust einer gemeldeten Person	Unaufgeforderte Supportanrufe vor Fernzugriff prüfen
2026-04-24	Tessin beschrieb versuchten Familiennotfallbetrug, nach rascher Meldung unterbrochen [S94]	Polizeilich gemeldeter Versuch, kein abgeschlossener Verlust	Vertrauenswürdigen familiären Prüfweg einrichten
2026-06-10	Bern warnte vor Fernzugriffsbetrug mit hohen Verlusten [S95]	Verlustzeitraum November 2025 bis April 2026	Gesamtbetrag nicht vollständig 2026 zuweisen
2026-09-24	Zwei mutmassliche Kuriere berichteten von angenommenen Onlinejobangeboten [S96]	Ihre Darstellung identifiziert kein ganzes Netzwerk	Bezahlte Umschlagabholungen prüfen
2026-10-13	Nachrichten führten zu Anrufen und Abholung von Karten mit intakten Chips [S97]	Mehrere Untersuchungen und Beobachtungen	Kartenabholgesuche eskalieren

Meldung	Polizeidarstellung	Umfangsgrenze	Massnahme
2026-10-29	Neuenburg meldete bis dahin 160 festgestellte Fälle 2026 mit geschätzten Verlusten um CHF 950 000 [S98]	Kantonale Meldungen bis zum Meldedatum	Zeitraum in Führungsbriefings bewahren
2026-11-10	Wallis beschrieb rund 40 Meldungen seit Mitte Oktober, mit Versuchen und vollendetem Betrug [S99]	Versuche sind keine abgeschlossenen Verlustvorfälle	Ergebnis und Vorgehen erfassen
2026-11-19	Zug beschrieb zwei Kurieruntersuchungen und eine durch Bankpersonal angestossene Intervention [S100]	Zwei unabhängige Fälle; Ermittlungen liefen weiter	Eskalationsweg bei ungewöhnlichen Bargeldbezügen pflegen

Diese Meldungen stützen eine Kontrolle über Bankwesen, Kundenservice und Familienunterstützung hinweg. Überzeugende Anrufende können bekannte Institutionen, echte persönliche Angaben und dringende Forderungen verbinden. Ein nachfolgender Kurier schafft eine physische Abschlussstufe. Prüfen Sie vor Geldtransfer, Kartenübergabe oder Fernzugriff über einen bekannten Kanal. [S92][S93][S97][S100]

Die Schaffhauser Darstellung verbindet auch Jobangebotsprüfung und Betrugsprävention. Sie belegt nicht, dass jeder Kurier den Abholzweck versteht. Arbeitgeber, Plattformen und Bewerbende sollten ungewöhnlich einfache bezahlte Aufgaben mit Bargeld oder versiegelten Umschlägen prüfen. Sie sollten nicht sämtliche Anzeigen einem Akteur zuordnen. [S96]

Die Novembermeldungen stärken die jüngste Aktivitätsbeurteilung, ohne nationales Wachstum zu belegen. Lokale Fallzahlen hängen von ihren angegebenen Zeiträumen und Meldepopulationen ab. Warnungen oder Festnahmen belegen einen aktiven Mechanismus. Sie messen keine landesweite Verbreitung. [S99][S100]

KERNAUSSAGEN

01

Führen Sie Dienstwiederherstellung und Datendiebstahlbeurteilung als getrennte Entscheidungen

02

Behandeln Sie Datensätze, Personen und Organisationen als unterschiedliche Grundgesamtheiten

03

Prüfen Sie unerwartete Gesuche auch bei richtigen persönlichen Angaben

KAPITEL 06

Hacktivismus und DDoS

06

DIESES KAPITEL BEANTWORTET

Was können Verfügbarkeitsvorfälle zu Auswirkungen, Zuschreibung und Motiv belegen?

40 Minuten

Gemeldeter Salt-Internetausfall

6.1 Die offizielle Darstellung 2026 58

6.2 Behauptung und Berichterstattung 58

6.3 Datierter historischer Vergleich: der Gipfel 2024 59

6.4 Zeitleiste und Reaktionsentscheidungen 59

6.5 Verfügbarkeit von Messaging-Diensten und ein unabhängiger Statuskanal 60

KAPITEL 06

Hacktivismus und DDoS

KURZFASSUNG

Verfügbarkeitsangriffe benötigen eine Auswirkungsdokumentation getrennt von Akteurswerbung. Das BACS beschreibt begrenzte Schweizer DDoS-Störungen im ersten Halbjahr 2026 und nennt einen spürbaren Telekommunikationsausfall. Historische Gipfelangriffe bleiben nützliche Vorbereitungsbeispiele, gehören aber zu 2024. Weder länderbezogene Rhetorik noch erfolgreiche Websiteunterbrechung belegen Zugriff auf interne Daten. Erfassen Sie betroffenen Dienst, Kundenfolgen, Quellenzuschreibung und Wiederherstellungsbelege vor der Eskalationsentscheidung.

6.1 Die offizielle Darstellung 2026

Verfügbarkeitsfolgen und Öffentlichkeitswirkung sind unterschiedliche Messgrössen. Laut BACS-Halbjahresbericht blieb DDoS-Aktivität für Schweizer Organisationen beherrschbar. Gegen Grossanlässe wie WEF oder Olympische Winterspiele habe es praktisch keine hacktivistischen Angriffe gegeben. Er beschreibt auch Versuche gegen DNS-Infrastruktur und einzelne Bankdienste ohne erhebliche Ausfälle. [S5]

Diese Aussagen betreffen Berichtszeitraum und Behördensicht. Sie belegen weder das Ausbleiben sämtlicher Versuche noch vollständige Meldung oder dasselbe Muster bis November. Eine spätere Akteursankündigung ist deshalb als neuer Beleg zu beurteilen.

Der Bericht nennt einen Salt-Vorfall als weithin spürbare DDoS-Auswirkung des Zeitraums. Laut Netzwoche verloren Festnetzkunden am 15. Mai ungefähr 40 Minuten Internetzugang. Das Mobilnetz funktionierte weiter. Der Publikation zufolge blieben Akteur, Motiv und mögliche Lösegeldforderung unklar. [S5][S22]

Machen Sie aus einer Telekommunikationsunterbrechung keine unbelegte Behauptung entwendeter Kundendaten. Ebenso belegt eine unterbrochene öffentliche Website keine Beeinträchtigung des internen Netzes. Die Reaktion braucht getrennte Verantwortliche für Verfügbarkeit, Einbruchsanalyse und Kundenkommunikation.

6.2 Behauptung und Berichterstattung

Das folgende Panel trennt die Messgrössen bewusst. Es lässt die Akteursdarstellung ungeklärt, statt die Lücke mit einem plausiblen Namen zu füllen.

Punkt	Akteursbehauptung	Offizielle Darstellung	Öffentliche Berichterstattung
Telekommunikationsfolge 2026	Keine authentisierte Akteursaussage belegt hier Verantwortung	BACS nennt spürbaren Salt-DDoS-Ausfall im Halbjahresbericht [S5]	Ungefähr 40 Minuten Festnetz-Internetunterbrechung am 15. Mai [S22]
Netzumfang	Keine verifizierte Behauptung belegt weitergehenden Zugang	Die Behördendarstellung betrifft Verfügbarkeit [S5]	Laut zitiertem Bericht funktionierte das Mobilnetz weiter [S22]
Motiv	Kein unabhängig gestütztes Motiv	Die nationale Darstellung weist diesem Vorfall keinen politischen Zweck zu [S5]	Akteursidentität und Motiv waren in der Publikation unklar [S22]
Interne Daten	Dienstunterbrechung liefert keinen Datendiebstahlbeleg	Die zitierte Verfügbarkeitsdarstellung stellt dies nicht fest [S5]	Bericht beschreibt Ausfallfolgen und keinen bestätigten internen Datenvorfall [S22]

Das Panel dient disziplinierter Reaktion. Laute Behauptungen können mit geringer Störung einhergehen. Ein unbenannter Angriff kann erhebliche Kundenfolgen haben. Ein zahlenmässiges Behauptungs-Auswirkungsverhältnis benötigt Messungen desselben Ereignisses mit derselben Einheit.

6.3 Datierter historischer Vergleich: der Gipfel 2024

Der Ukraine-Friedensgipfel fand am 15.–16. Juni 2024 statt. In seiner Bilanz vom 20. Juni schrieb das NCSC zugehörige DDoS-Angriffe NoName057(16) zu. Die Behörde beschrieb geringe Störungen. IT-Systeme und Daten des Gipfels seien nicht bedroht gewesen. Dies sind Befunde des NCSC. [S42]

Dieselbe Bilanz trennt weitere Vorfälle von der DDoS-Aktivität. Sie beschreibt Einbruchsversuche gegen kantonale Systeme und Phishing gegen Mitarbeitende von Notrufzentralen. Technische Probleme der Liveübertragung und ein regionaler Stromausfall seien keine Cybervorfälle gewesen. Das verhindert die Aufnahme unverbundener Störungen in eine Angriffsdarstellung. [S42]

Der historische Vergleich ist keine Vorfallszahl 2026. Er belegt weder Verantwortung für den Telekommunikationsangriff 2026 noch eine aktuelle Kampagne gegen jede an internationalen Anlässen beteiligte Organisation. Der Bericht nimmt keine Position zu Gipfel, Sanktionen, EU-Beziehungen oder Regierungspolitik ein.

Die übertragbare Lehre betrifft Vorbereitung. Das NCSC beschreibt einen öffentlich-privaten Lageverbund, frühe Vorbereitung und koordinierte Reaktion. Veranstalter können damit Kommunikationskontakte zuweisen, öffentliche Dienste schützen und Störungsmessung vereinbaren. [S42]

6.4 Zeitleiste und Reaktionsentscheidungen

Die Zeitleiste unterscheidet historischen Hintergrund, ein Vorfallsdatum 2026 und spätere Veröffentlichungsdaten.

20 Juni 2024 **NCSC**
Historische Bilanz schrieb Gipfel-DDoS mit geringen Störungen NoName057(16) zu [S42]

15 Mai 2026	**Öffentliche Berichterstattung** Salt-Festnetzausfall später als DDoS-Vorfall beschrieben [S22]
24 Aug. 2026	**BACS** Halbjahresbericht beschrieb beherrschbare DDoS-Folgen und Telekommunikationsausfall [S5]
18 Nov. 2026	**Kantonsverwaltung** Laut Basel-Landschaft blieben Notruf- und Rettungssysteme beim getrennten IT-Vorfall betriebsfähig [S47]

Das kantonale Novemberupdate dient hier als Kommunikationslehre und nicht als DDoS-Zuschreibung. Eine frühe Warnung vor möglichen Störungen darf nicht als beobachtetes Notfalldienstversagen erscheinen. Laut Kanton waren die relevanten Notruf- und Rettungs-IT-Systeme niemals betroffen. [S47]

Im Sicherheitsbetrieb sollte Eskalation von beobachteter Dienstverschlechterung und dokumentierten Geschäftsfolgen abhängen. Bewahren Sie Beginn, Wiederherstellungszeit, betroffene Funktion und eigene Dienstmessungen auf. Ein Bildschirmfoto Dritter ist ein Hinweis und keine vollständige Auswirkungsdokumentation.

Kommunikationsteams sollten öffentliche Site, Kundenanmeldung, Kommunikationsnetz und interne Systeme unterscheiden. Updates sollten nutzbare Kundenfunktionen und verfügbare Alternativwege erklären. Vermeiden Sie Akteursslogans und die Darstellung behaupteter politischer Motive als gesicherte Fakten.

Dienstverantwortliche sollten den Punkt üben, an dem Schutzmassnahmen Funktionen einschränken. Vereinbaren Sie Genehmigung, Erklärung und Wiederherstellungsprüfung. Die Aufzeichnung sollte vorsorgliche Eindämmung von Angreiferschaden unterscheiden lassen.

6.5 Verfügbarkeit von Messaging-Diensten und ein unabhängiger Statuskanal

Threemas Darstellung vom 14 August 2026 beschreibt DDoS-Störungen am 11–12 August. Das Unternehmen meldete am Dienstag Nichtverfügbarkeit zwischen 19:30 und 23:30 CEST. Am Mittwochmorgen folgten zeitweilige Unterbrechungen. Laut Unternehmen war der Normalbetrieb am Mittwoch um 12:23 wiederhergestellt. Das Ereignis gehört zum zweiten Halbjahr 2026. [S101]

Das Unternehmen beschrieb Angriffe auf seinen Dienst und einen Colocation-Partner. Ob Threema das Hauptziel oder eines von mehreren Zielen war, konnte es nicht feststellen. Kunden mit Threema OnPrem auf eigener Infrastruktur waren laut Unternehmen unberührt. Die Verfügbarkeitsdarstellung rechtfertigt weder die Zuweisung eines staatlichen Akteurs noch die Annahme eines Zugriffs auf interne Nachrichten. [S101][S102]

Ein unabhängiges technisches Problem verhinderte zunächst die Aktualisierung der Statusseite. Threema nahm diese vorübergehend offline. Laut Update vom 14 August war zusätzlicher DDoS-Schutz aktiviert worden. Geplant waren zudem ein Vorfallsverlauf und ein unabhängiger Benachrichtigungsfeed. Das sind datierte Reaktionsaussagen des Unternehmens und keine Bewertung heutiger Kontrollwirksamkeit. [S101]

Der Fall unterstützt den Test eines alternativen Kommunikationswegs neben Verfügbarkeitsschutzmassnahmen. Dienstverantwortliche sollten sicherstellen, dass Kunden einen nicht verfügbaren Dienst von einer nicht verfügbaren Statusseite unterscheiden können. Dokumentieren Sie Unterbrechungs- und Wiederherstellungszeiten jeder Funktion getrennt.

KERNAUSSAGEN

01

Schreiben Sie Akteursverantwortung nur der belegenden Quelle zu

02

Halten Sie den Gipfel 2024 aus den Vorfallszahlen 2026 heraus

03

Messen Sie Dienstfolgen und Wiederherstellung, bevor Sie Akteursdarstellungen verbreiten

KAPITEL 07

Bedrohungsakteure und belegte Beziehungen

07

DIESES KAPITEL BEANTWORTET

Welche Akteursbeschreibungen helfen der Abwehr, ohne Zuschreibung zu überdehnen?

41

Gruppenbezeichnungen in der Schweizer Ransomware-Momentaufnahme

7.1 Ransomware-Marken beschreiben Listungen und keine vollständigen Einbruchshistorien 63
7.2 Regionaler Kontext ohne Länderrangliste 66
7.3 Personas und Beziehungen in den aufbewahrten Beiträgen 67
7.4 Staatsbezogene Aktivität nach Einschätzung des NDB 69
7.5 Technikmatrix für Kontrollplanung 69
7.6 Patchbereitschaft: die PHP-Warnung im Oktober 70
7.7 Politisch gerahmte Akteure 71
7.8 Was eine Akteursbeurteilung stärken würde 71
7.9 Kurze Manipulationsfenster bei Updates und rückblickende Belege 72

KAPITEL 07

Bedrohungsakteure und belegte Beziehungen

KURZFASSUNG

Die Belege stützen getrennte Akteurssichten: Ransomware-Listungsmarken, anbietende Personas, politisch gerahmte Verfügbarkeitsbehauptungen und offizielle Spionageeinschätzungen. Sie bilden kein nachgewiesenes gemeinsames Netzwerk. AKIRA hat die höchste Schweizer Listungszahl dieser Momentaufnahme. Andere Marken bilden zusammen die Mehrheit. Nationale und staatsbezogene Zuschreibungen bleiben diejenigen der zitierten Behörde. Nutzen Sie Akteursinformationen zur Auswahl von Untersuchungsfragen und Wiederherstellungsszenarien.

7.1 Ransomware-Marken beschreiben Listungen und keine vollständigen Einbruchshistorien

Ransompedia erfasst im Berichtszeitraum 122 Schweizer Listungen unter 41 Gruppenbezeichnungen. AKIRA trägt 13 bei, The Gentlemen (in der Rohaufnahme als Thegentlemen geführt) und Qilin jeweils 9. Zusammen ergeben diese drei 31 Listungen oder 25.4% der Schweizer Gesamtzahl. Die übrigen 91 Listungen ergeben 74.6% [S2].

Diese Verteilung spricht gegen eine auf eine einzige Marke ausgerichtete Kontinuitätsplanung. Bezeichnungen können wechseln, Organisationen mehrfach erscheinen. Eine öffentliche Erpressungsbehauptung belegt keine ausgeführte Software. Wiederherstellungsplanung sollte auch bei ungeklärtem Betreiber oder Zugangsweg nützlich bleiben.

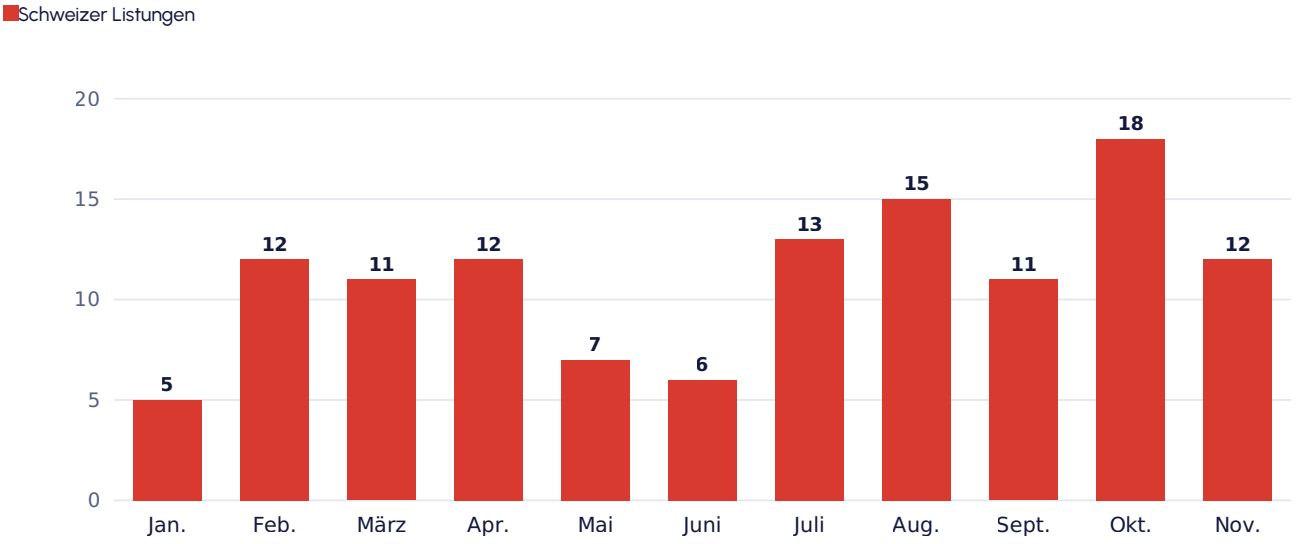
Die Tabelle bewahrt die Messeinheit. Sie zählt Listungen der Momentaufnahme und keine unabhängig verifizierten Vorfälle.

Gruppenbezeichnung	Listungen	Anteil	Beleggrenze
AKIRA	13	10.7%	Listungsbezeichnung; einzelne Ergebnisse benötigen Bestätigung
The Gentlemen	9	7.4%	In der Momentaufnahme als Thegentlemen geführt; kein gemeinsamer Betreiber mit anderen Marken abgeleitet
Qilin	9	7.4%	Listungsbezeichnung; Zahl belegt keinen Erstzugang
Bravox	8	6.6%	Listungsbezeichnung; Behauptungen bleiben Behauptungen
Safepay	7	5.7%	Listungsbezeichnung; Zahlung und Datenumfang ungeklärt

Gruppenbezeichnung	Listungen	Anteil	Beleggrenze
Andere Bezeichnungen	76	62.3%	Übrige Bezeichnungen zusammengefasst; kein Bündnis unterstellt
Gesamt	122	100.0%	Getrennt von der behördlichen Ransomware-Grundgesamtheit

Die gerundeten Gruppenanteile weichen geringfügig vom Gesamtwert ab. Der Gesamtwert nutzt die zugrunde liegenden Listungszahlen.

Schweizer Erpressungslistungen erscheinen im gesamten Berichtszeitraum



Quelle: aufbewahrte länderbezogene Ransompedia-Listungen, erfasst am 22. November 2026. Listungsdaten sind keine Vorfallsdaten [S2].

AKIRA

Ransomware-Listungsmarke | Erpressungsbehauptungen; Identität einzelner Betreiber ungeklärt

VORLIEGENDE BELEGE

1 Januar–22 November

13 Schweizer Listungen in der aufbewahrten Momentaufnahme [S2]

LISTUNGSUMFANG

Organisationsbezeichnungen in der Schweizer Listungsmomentaufnahme

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] 13 von 122 Schweizer Listungen; eine Listung ist eine kriminelle Behauptung.

UNSERE EINSCHÄTZUNG

Die Listungszahl unterstützt Kontinuitätsplanung. Sie belegt weder Verschlüsselung noch Datendiebstahl, Zahlung oder Zugangsweg jeder Organisation.

VERTRAUENSGRAD
Hoch für die aufbewahrte Listungszahl; einzelne Vorfallsergebnisse benötigen Bestätigung.

Qilin

Ransomware-Listungsmarke | Erpressungsbehauptungen; Identität einzelner Betreiber ungeklärt

VORLIEGENDE BELEGE

1 Januar–22 November
9 Schweizer Listungen in der aufbewahrten Momentaufnahme [S2]

LISTUNGSUMFANG

Organisationsbezeichnungen in der Schweizer Listungsmomentaufnahme

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] 9 von 122 Schweizer Listungen; eine Listung ist eine kriminelle Behauptung.

UNSERE EINSCHÄTZUNG

Die Listungszahl unterstützt Kontinuitätsplanung. Sie belegt weder Verschlüsselung noch Datendiebstahl, Zahlung oder Zugangsweg jeder Organisation.

VERTRAUENSGRAD
Hoch für die aufbewahrte Listungszahl; einzelne Vorfallsergebnisse benötigen Bestätigung.

The Gentlemen

Thegentlemen (Listungsbezeichnung)

Ransomware-Listungsmarke | Erpressungsbehauptungen; Identität einzelner Betreiber ungeklärt

VORLIEGENDE BELEGE

1 Januar–22 November
9 Schweizer Listungen in der aufbewahrten Momentaufnahme [S2]

LISTUNGSUMFANG

Organisationsbezeichnungen in der Schweizer Listungsmomentaufnahme

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S2] 9 von 122 Schweizer Listungen; eine Listung ist eine kriminelle Behauptung.

UNSERE EINSCHÄTZUNG

Die Listungszahl unterstützt Kontinuitätsplanung. Sie belegt weder Verschlüsselung noch Datendiebstahl, Zahlung oder Zugangsweg jeder Organisation.

VERTRAUENSGRAD
Hoch für die aufbewahrte Listungszahl; einzelne Vorfallsergebnisse benötigen Bestätigung.

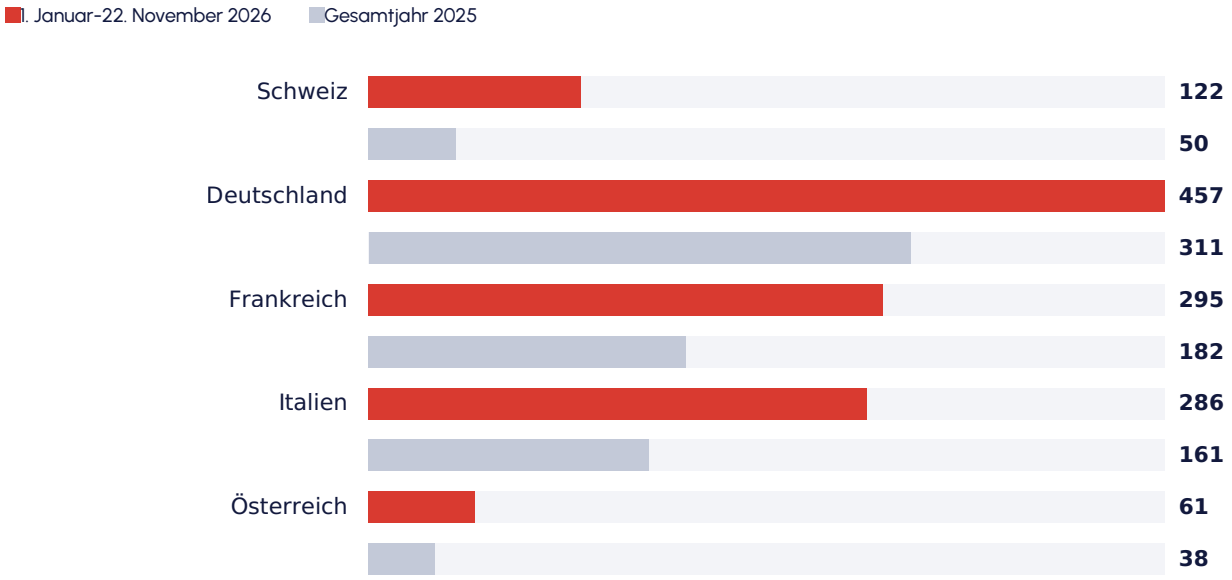
7.2 Regionaler Kontext ohne Länderrangliste

Die Vergleichsländer teilen Grenzen oder sprachliche und geschäftliche Verbindungen mit der Schweiz. Ihre Listungszahlen sind Deutschland 457, Frankreich 295, Italien 286 und Österreich 61. Dieselbe Momentaufnahme enthält für das Gesamtjahr 2025 jeweils 311, 182, 161 und 38. Die Schweizer Gesamtzahl 2025 ist 50 [S2].

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

Bei jedem Vergleichsland übersteigt der Teiljahreswert 2026 in dieser Momentaufnahme den Gesamtjahreswert 2025. Dies ist ein beschreibender Listungsvergleich. Unterschiedliche Zeiträume, Beobachtungsabdeckung, Offenlegung und Länderzuordnung verhindern direkte Aussagen zur Angriffsrate. Er belegt keinen höheren Schutz von Einwohnern oder Unternehmen in einem Land.

Jedes Vergleichsland hat mehr Listungen als im gesamten Vorjahr



Ungleiche Zeiträume; keine nationale Risikorangliste. Quelle: aufbewahrte länderbezogene Ransompedia-Listungen, erfasst am 22. November 2026. Listungsdaten sind keine Vorfallsdaten [S2].

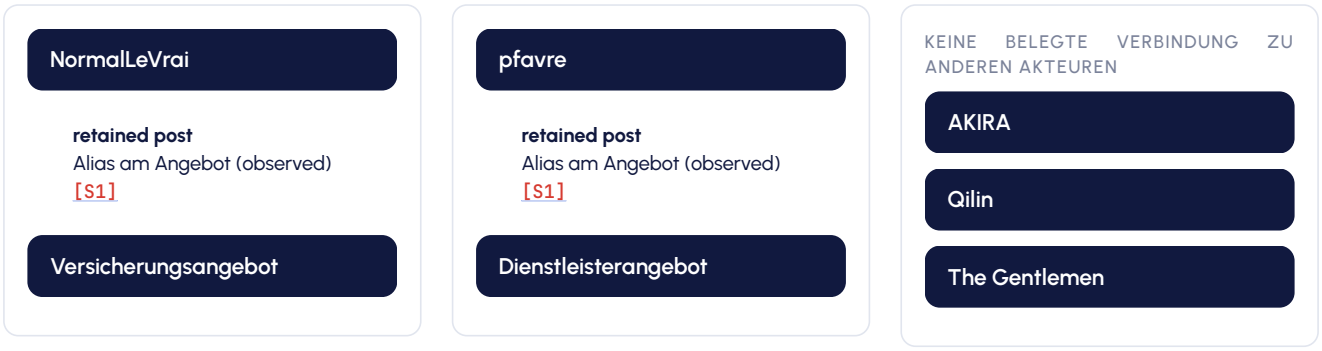
Für internationale Unternehmen liegt der Nutzen im Test eines gemeinsamen Wiederherstellungsszenarios über regionale Betriebe hinweg. Gemeinsame Dienste oder Anbieter können grenzüberschreitende Abhängigkeiten schaffen, selbst wenn die Listung nur eine lokale Einheit nennt. Vorfallverantwortliche müssen den tatsächlichen Umfang feststellen, statt die Länderkennzeichnung zu übernehmen.

7.3 Personas und Beziehungen in den aufbewahrten Beiträgen

Eine Persona ist der einem Beitrag zugeordnete Alias. Sie ist keine verifizierte Person, Firma, Nationalität oder beständiger Betreiber. Die Belegkarten bewahren nur zum Verständnis der Behauptung nötige Informationen. Kontakte, Opferkennungen und Personendaten bleiben zurückgehalten [S1].

Ein wiederholter Alias kann eine Beziehung zwischen Anzeigen stützen. Er belegt weder denselben menschlichen Verfasser noch identische Dateien oder einen Verkauf unabhängig. Ähnliche Titel oder Datensatzzahlen können auch durch kopierte Werbung entstehen.

Die Beziehungssicht hält Anzeigen, Personas und Listungsmarken deshalb als getrennte Knoten. Eine quellenbelegte Verbindung beschreibt, was zwei Knoten verbindet; der gezeigte Graph enthält nur zwei beobachtete Persona-zu-Beitrag-Verbindungen (NormalLeVrai zu B01 und pfavre zu B04), während die drei Listungsmarken unverbunden bleiben. Die folgende Tabelle fasst mögliche Belegbeziehungen im Bericht zusammen.



Unverbundene Knoten haben keine festgestellte Beziehung. Gemeinsamer Betreiber oder Bündnis werden nicht abgeleitet.

Mögliche Belegbeziehung	Stützender Beleg	Nicht belegt
Persona zu Beitrag	Alias am aufbewahrten Material [S1]	Rechtliche Identität, Nationalität oder Kontrolle jedes Kontos mit diesem Alias
Beitrag zu behauptetem Datensatz	Angebotsbeschreibung [S1]	Echtheit, Ursprung, Alter oder Zahl einzelner Personen
Marke zu Listung	Aufbewahrter Listungsdatensatz [S2]	Verschlüsselung, Diebstahl, Affiliate-Identität oder abgeschlossene Zahlung
Behörde zu Zuschreibung	Veröffentlichte Behördeneinschätzung [S9][S42]	Unabhängige Zuschreibung einer unverbundenen Schweizer Anzeige

NormalLeVrai

Forenpersona | Werberolle beobachtet; rechtliche Identität ungeklärt

BELEGE UND ÖFFENTLICHE BESTÄTIGUNG

2026-05-04
Anzeige in B01 gezeigt [S1]

BEHAUPTETES THEMA

Als Versicherungsinformationen bezeichnetes Material

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S1] Der aufbewahrte Beitrag belegt die Anzeige. Unabhängige Bestätigung der zugrunde liegenden Behauptung ist hier nicht festgestellt.

UNSERE EINSCHÄTZUNG

Ein Angebotsalias belegt weder verifizierte Person noch Nationalität, aktuellen Zugang oder abgeschlossene Transaktion.

VERTRAUENSGRAD
Hoch für die Materialbeobachtung; angebotene Informationen bleiben ungeprüft.

pfavre

Forenpersona | Werberolle beobachtet; rechtliche Identität ungeklärt

BELEGE UND ÖFFENTLICHE BESTÄTIGUNG

2026-11-05
Anzeige in B04 gezeigt [S1]

BEHAUPTETES THEMA

Unternehmensdienstleisterinformationen

IN ÖFFENTLICHER BERICHTERSTATTUNG

[S1] Der aufbewahrte Beitrag belegt die Anzeige. Unabhängige Bestätigung der zugrunde liegenden Behauptung ist hier nicht festgestellt.

UNSERE EINSCHÄTZUNG

Ein Angebotsalias belegt weder verifizierte Person noch Nationalität, aktuellen Zugang oder abgeschlossene Transaktion.

VERTRAUENSGRAD
Hoch für die Materialbeobachtung; angebotene Informationen bleiben ungeprüft.

Eine Abfolge von Identitätsinformationen über Identitätsvortäuschung und Kontomissbrauch zu Erpressung kann als **analytisches Modell** nützlich sein. Sie ist eine Planungsabfolge und kein Befund der Zusammenarbeit berichteter Personas und Marken.

7.4 Staatsbezogene Aktivität nach Einschätzung des NDB

Der Lagebericht 2026 des NDB und die Bundeszusammenfassung nennen russische und chinesische Dienste als Hauptbedrohung durch Spionage in der Schweiz, neben staatlichen Cyberbedrohungen aus Russland, China, Iran und Nordkorea [S9][S110]. Die offizielle Einschätzung unterscheidet Ziele in Politik, Diplomatie und kritischer Infrastruktur von Informationssammlung gegen Forschungseinrichtungen, Hochschulen und Technologieunternehmen [S9][S110]. Diese Zuschreibungen stammen von den Schweizer Behörden; dieser Bericht weist unbenannte Verkäufer oder ungeprüfte Listungen keinem Staat zu.

Der NDB beschreibt Phishing, Ausnutzung bekannter Netzwerkausrüstungsschwachstellen und Zugang über IT- oder Telekommunikationsanbieter. Dies sind strategische Muster einer offiziellen Einschätzung. Sie bestimmen keinen Zugangsweg der in Kapitel 5 beschriebenen Gesundheits-, Dienstleister- oder Verwaltungsvorfälle.

Nutzen Sie die Einschätzung zur Bestimmung sensibler Informationen und dauerhafter Zugangswege. Forschungseinrichtungen müssen möglicherweise externe Zusammenarbeitskonten prüfen. Internationale Unternehmen müssen möglicherweise Fernzugriff auf sensible Geschäftsinformationen untersuchen. Anbieter müssen möglicherweise feststellen, welche Kundenumgebungen ihre Supportidentitäten erreichen.

Quellengestützter Schwerpunkt	Offizielle Einschätzung [S9][S110]	Entscheidungspriorität für CISOs
Hauptpriorität Spionageabwehr	Der NDB nennt russische und chinesische Nachrichtendienste als wichtigste Spionagebedrohung in der Schweiz	Dauerhafte Zugänge, diplomatische oder politische Arbeitsbereiche und externe Zusammenarbeitskonten prüfen
Spitzentechnologie und Forschung	Der NDB hebt Informationssammlung gegen Hochschulen, Forschungsinstitute und Technologieunternehmen hervor	Berechtigungen für Projektablagen, Austritte von Gastforschenden und Datenaustausch mit Partnern kontrollieren
Kritische Infrastrukturen und Dienstleister	Der NDB nennt staatliche Cyberaktivität gegen kritische Infrastrukturen, IT-Anbieter und Telekommunikation	Öffentlich erreichbare Netzwerkgeräte, Behebung bekannter Schwachstellen und Supportwege von Anbietern validieren

7.5 Technikmatrix für Kontrollplanung

Die Matrix ordnet quellenbeschriebenes Verhalten standardisierten ATT&CK-Begriffen zu. Dies ist eine analytische Planungseinordnung. Sie behauptet weder eine vollständige Angriffskette noch bestätigte Ausführung in jedem Schweizer Fall [S9].

Quellenverhalten	ATT&CK-Begriff	Planungsfrage	Grenze
Gezieltes Phishing	T1566, Phishing [S70]	Können Nutzende Absender über einen vertrauenswürdigen Weg prüfen?	NDB beschreibt das Muster; Zustellung im Einzelfall bleibt getrennt
Ausnutzung exponierter Geräte	T1190, Exploit Public-Facing Application [S71]	Hat der Dienst Verantwortliche, Unterstützung und behobene Schwachstellen?	Verwundbares Produkt belegt keine Ausnutzung
Nutzung eines erlangten Kontos	T1078, Valid Accounts [S72]	Werden Sitzungen, Rechte und Wiederherstellungseinstellungen geprüft?	Kontobesitz und Nutzung benötigen eigene Belege

ANALYTISCHE ZUORDNUNG FÜR KONTROLLPLANUNG

T1566
Phishing

Quellenbeschriebenes NDB-Muster; Planungseinordnung [S9] [S70]

T1190
Ausnutzung öffentlich erreichbarer Anwendung (Exploit Public-Facing Application)

Quellenbeschriebenes NDB-Muster; Planungseinordnung [S9] [S71]

T1078
Gültige Konten (Valid Accounts)

Planungseinordnung mit erforderlichen fallspezifischen Belegen [S72]

Die Begriffe helfen, Beleganforderungen zu ordnen. Sie sollten keine dekorative Checkliste nie beobachteter Techniken werden. Ein Vorfallteam sollte Techniken nur bei stützenden eigenen Belegen oder zitierten Fallquellen als festgestellt markieren.

7.6 Patchbereitschaft: die PHP-Warnung im Oktober

Das BACS veröffentlichte am 21. Oktober 2026 eine dringende PHP-Warnung zu CVE-2026-109618 und CVE-2026-109619. Die Warnung belegt eine offizielle Behebungskampagne. Sie belegt keine Ausnutzung bei einer Schweizer Organisation [S62].

NVD-Einträge beschreiben Speicherkorruptions- und Anfragezustandsschwächen. Sie enthalten den CVSS 4.0-Wert 9.2 der PHP Group und keine unabhängige NVD-Bewertung. Herstellerhinweise nennen betroffene und korrigierte Zweigversionen [S63][S64][S65][S66].

PHP-Zweig	Betroffene Zweigversionen	Korrigierte Version
8.2	Vor 8.2.35	8.2.35
8.3	Vor 8.3.36	8.3.36
8.4	Vor 8.4.27	8.4.27
8.5	Vor 8.5.12	8.5.12

Die Tabelle nennt vier Zweige aus der zitierten Releaseankündigung. Sie belegt nicht, dass ältere Versionen unbetroffen sind.

Der Hersteller veröffentlichte diese Sicherheitsversionen am 21. Oktober. Dienstverantwortliche sollten eingebettete und gehostete Installationen inventarisieren. Prüfen Sie nach Neustart oder Neuverteilung die laufende Komponente. Ein dokumentierter Anbieter-Backport kann eine gesonderte Paketprüfung erfordern [S67].

Beziehen Sie Updates über den etablierten Herstellerkanal, unabhängig von unaufgeforderten Nachrichten.

Ein Versionsbefund sollte zu einer Behebungsentscheidung führen und keiner Datendiebstahlschlussfolgerung. Bei Ausnutzungsverdacht sichern Sie relevante Belege und untersuchen den Dienst. Schutzfilter können helfen, ersetzen aber keine Prüfung korrigierter Software.

7.7 Politisch gerahmte Akteure

Historische DDoS-Berichte helfen bei Verfügbarkeitsübungen, bleiben aber ausserhalb der Vorfallszahl 2026. Die NCSC-Bilanz zum Gipfel im Juni 2024 schrieb DDoS NoName057(16) zu. Sie beschrieb begrenzte Störung und trennte unverbundene technische Probleme von Cybervorfällen [S42].

Eine politische Gruppenbeschreibung belegt keine staatliche Steuerung. Eine Ankündigung zeitnah zu Sanktionen, internationalem Treffen oder politischer Entscheidung belegt den Vorfallsgrund nicht unabhängig. Die operative Reaktion sollte auf Dienstbelegen und etablierten Vorfallverantwortlichkeiten beruhen.

7.8 Was eine Akteursbeurteilung stärken würde

Bei Anzeigen würden stärkere Belege ein authentisches Muster mit relevantem System und Zeitraum verbinden. Bei Zugangsbehauptungen würden sie bestehendes Konto, Rechte und unberechtigte Aktivität feststellen. Bei Listungen käme die eigene Organisationsdarstellung zu Dienst- und Datenfolgen hinzu.

Bei Zuschreibungen würden stärkere Belege Infrastruktur, Konten, Werkzeuge oder Operationen über eine verantwortliche Quelle mit einem benannten Betreiber verbinden. Gemeinsame Sprache oder Geografie reichen nicht. Jeder neue Fakt sollte eine bestimmte Aussage stärken, statt einer gesamten Persona pauschal Vertrauen zu geben.

7.9 Kurze Manipulationsfenster bei Updates und rückblickende Belege

P

FALL P

Updatekampagne für Sicherungssoftware mit gemeldeten Auswirkungen in der Schweiz (R01)

Softwarelieferkette

Vom Anbieter bestätigter Vorfall; Schweizer Betroffene ungenannt

DARSTELLUNG	Google Threat Intelligence Group und Mandiant berichten über eine Kampagne gegen AOMEI Technologys Updateinfrastruktur zwischen April und Juli 2026. Ihre Darstellung zählt die Schweiz zu Ländern mit betroffenen Organisationen. AOMEI bestätigt den Updateservervorfall in einer eigenen Stellungnahme. [S103][S105]
CHRONOLOGIE	Die Herstellerstellungnahme erschien am 19. Oktober und wurde am 30. Oktober 2026 aktualisiert. Sie beschreibt Serverhärtung bis 29. Juli, Migration am 5. August und Veröffentlichung von Backupper 8.5.1 am 19. Oktober. Dies sind datierte Reaktionsaussagen des Herstellers. [S105]
FESTGESTELLT	Die Forschenden beschreiben Konfigurationsänderungen von fünf bis zehn Minuten, bevor wieder legitime Inhalte bereitgestellt wurden. Sie führen die Aktivität als UNC7017 und beschreiben Schadsoftware namens CROSSROAD und SHINYROAD. Die Darstellung stützt eine Untersuchung der Dienstleisterupdates. Sie belegt keine Beziehung zu den Werbepersonas oder Ransomware-Marken dieses Berichts. [S103]
GRENZEN	Schweizer Organisationen werden nicht genannt. Die Sektorliste der gesamten Kampagne bestimmt keine betroffenen Schweizer Sektoren. Dieser Bericht besitzt weder Zugang zu betroffenen Systemen noch Belege einer Verbindung zur Organisationsauswahl. Weder Forschung noch Herstellerstellungnahme belegen einen staatlichen Auftraggeber. [S103][S105]
ALTERNATIVEN	Die Forschenden beschreiben opportunistische Auslieferung während kurzer Manipulationsfenster. Die Länderliste belegt keine schweizspezifische Zielauswahl. Eine später beobachtete legitime Updateantwort klärt nicht den früheren Empfang eines Endpunkts. Laut AOMEI läuft die Beurteilung potenziell betroffener Nutzender weiter. [S103][S105]
REAKTION	Software- und Endpunktverantwortliche sollten Produktnutzung feststellen, historische Update- und Endpunktaufzeichnungen sichern und den in der Quelle beschriebenen Zeitraum beurteilen. Folgen Sie aktuellen Vorfallhinweisen des Herstellers. Eine Produktaktualisierung allein ersetzt keine Untersuchung möglicher früherer Exposition. [S105]

Fazit

Prüfen Sie frühere Auslieferung und Endpunktaktivität getrennt von der heutigen Updateantwort des Anbieters.

Die Kontrolllehre ist, Belege über Anbieter- und Kundensysteme hinweg zu sichern. AOMEIs Stellungnahme unterscheidet ausdrücklich zwischen Backupper-Aktualisierung und Prüfung betroffener Geräte. Der Abschluss sollte historische Auslieferung, Endpunktaktivität und relevante Kontoexposition deshalb getrennt behandeln. Aus diesen Quellen lässt sich keine Zahl Schweizer Opfer ableiten. [S105]

KERNAUSSAGEN

01

Behandeln Sie Ransomware-Marken, Personas und offizielle Zuschreibungen als unterschiedliche Belegpopulationen.

02

Nutzen Sie Technikzuordnungen für Beleganforderungen und Kontrolltests, ohne Angriffsketten zu erfinden.

03

Lassen Sie unbelegte Akteursbeziehungen unverbunden. Binden Sie politische Zuschreibungen an ihre Quellen.

KAPITEL 08

Die Betrugsökonomie: Identität, Vertrauen und Zahlung

08

DIESES KAPITEL BEANTWORTET

Wie können offengelegte Informationen ein späteres Betrugsgesuch überzeugender machen?

3

getrennte Entscheidungen: Identität, Berechtigung und Zahlung

8.1 Persönliche Informationen sind Kontext und keine Berechtigung 75

8.2 Buchungs- und Lieferungsanlässe machen Kontext dringlich 75

8.3 Falsche Bankautorität und die physische Zahlungsstufe 76

8.4 Was Untergrundangebote belegen 76

8.5 Zahlungskartenmaterial im engen Umfang 77

8.6 Die Abfolge an mehreren Stellen unterbrechen 78

KAPITEL 08

Die Betrugsökonomie: Identität, Vertrauen und Zahlung

KURZFASSUNG

Offizielle Warnungen zeigen, wie echte persönliche Angaben oder Buchungsdetails falsche Gesuche stärken. Angreifer müssen Empfänger weiterhin zum Vertrauen, zur Zugangsänderung oder Zahlungsfreigabe bewegen. Untergrundangebote beschreiben mögliche Ausgangsmaterialien dieses Prozesses und keinen vollendeten Betrug. Halten Sie Zahlungskartenbeobachtungen eng begrenzt und von Verlustzahlen getrennt. Verlangen Sie unabhängige Prüfung, wenn unerwartete Gesuche richtige Angaben enthalten.

8.1 Persönliche Informationen sind Kontext und keine Berechtigung

Die BACS-Meldung vom 17. November beschreibt gezieltes Phishing nach einem Dienstleisterdatenleck. Die Nachrichten nutzten echte persönliche Angaben einschliesslich Sozialversicherungskennungen. Ihre Richtigkeit machte den Kontakt überzeugender, ohne eine Berechtigung des Absenders zu belegen [S14].

Dies verändert die Frage des Supportteams. Wiederholt ein Anrufer eine Adresse oder andere offengelegte Angaben, bestätigt das möglicherweise seinen Informationsbesitz. Es belegt nicht seine Identität als betroffene Person. Ein stärkerer Ablauf prüft Gesuche über bestehende vertrauenswürdige Kanäle. Änderungen dieses Kanals gelten als eigene sensible Handlung.

Drei Aussagen bleiben getrennt: Die Daten können echt sein. Der Absender kann trotzdem betrügen. Die gewünschte Handlung kann einen neuen Verlust schaffen, selbst wenn der ursprüngliche Vorfall eingedämmt ist. Eine gemeinsame Schlussfolgerung kann Folgerisiken unterschätzen.

Der Vorsorgedienstleisterfall liefert ein dienstspezifisches Beispiel. Eine offizielle Polizeiwarnung behandelt Anlagekontaktversuche nach einem Vorsorgedienstleisterleck. Die Nennung von Lohn- und Vorsorgeinformationen unterstützt die Vorbereitung auf gezielte Ansprache. Sie belegt nicht die exakten entwendeten Felder jedes Dienstleisterkunden [S45].

Bereiten Sie Versichertenservices auf überzeugende Angaben vor. Geben Sie ihnen einen sicheren Prüfweg für echte Anliegen und einen klaren Weg zur Sicherung betrügerischer Kontaktversuche. Lassen Sie Betroffene sensible Angaben nicht in Gesprächen wiederholen, die über unerwartete Kanäle begannen.

8.2 Buchungs- und Lieferungsanlässe machen Kontext dringlich

Die Polizeiwarnung im November beschreibt Nachrichten mit Kenntnis von Unterkunftsdetails und Buchungsreferenzen. Sie verlangten Reservationsbestätigung und anschliessend Zahlungskartendaten. Wissen über eine echte Buchung belegte keinen Ursprung beim gebuchten Anbieter [S43].

Dasselbe gilt für scheinbare Liefernachrichten an Kunden, die ein Paket erwarten. Passendes Timing kann einen überzeugenden Vorwand liefern. Das BACS-Update vom 10. November behandelt betrügerische Shops und Paketphishing. Es stützt Verkäufer- und Nachrichtenprüfung, statt jede verspätete Lieferung als böswillig anzusehen [S13].

Reise-, Hotel- und Handelsorganisationen sollten klären, wie Kunden unerwartete Gesuche ohne deren Link oder Telefonnummer prüfen können. Die Antwort sollte vor einem Vorfall sichtbar sein. Ein konsistentes Portal, Buchungsdatensatz und Supportweg helfen bei sicherer Klärung.

Anbieter sollten auch Konten schützen, die echte Nachrichten versenden. Ein überzeugendes Gesuch kann von einer Betrugsdomain, einem missbrauchten Konto oder einem anderen Kommunikationsweg kommen. Die Nachricht allein bestimmt keine vorgelagerte Ursache. Bewahren Sie diese Unterscheidung während der Untersuchung.

8.3 Falsche Bankautorität und die physische Zahlungsstufe

Die Polizeiwarnung vom 18. November beschreibt falsches Bankpersonal und ein gefälschtes Zentralbankschreiben. Der Betrug forderte Bargeld für ein angebliches Sicherungskonto. Die behauptete Zentralbankbeteiligung war Teil der Täuschung und keine festgestellte Beziehung [S44].

Das Beispiel zeigt, warum Betrugsreaktion über die Onlineanmeldung hinausgehen muss. Kunden können zu Bargeldbezug, Vermögensverschiebung oder Softwareinstallation bewegt werden. Technische Websitekontrollen ersetzen weder vertrauenswürdige Kundenprüfung noch einen Eskalationsweg für ungewöhnliche Gesuche.

Die Quelle begrenzt auch die Schlussfolgerung. Eine Warnung belegt die beschriebene Methode und Sorge der Behörde. Sie liefert weder nationale Verlustschätzung noch Nachweis, dass alle Empfänger folgten. Der Bericht leitet dies nicht aus der Veröffentlichung ab.

Banken und andere Organisationen sollten Supportteams klare Formulierungen zum Unterbrechen der Geschichte geben. Kunden können unerwartete Gespräche beenden und die Organisation über ihren etablierten Weg kontaktieren. Mitarbeitende sollten behauptete Autorität nicht anhand verdächtiger Nachrichtenangaben bestätigen.

8.4 Was Untergrundangebote belegen

Das aufbewahrte Material enthält Anzeigen zu Konten, Identitäten, Zugang und Daten. Sie können kriminelles Interesse an einem Produkt anzeigen. Sie belegen weder abgeschlossenen Handel noch verifizierten Schweizer Herausgeber oder spätere Käuferverwendung [S1].

Das Kontokaufgesuch B11 nannte $8 für ein vom Inserenten als gültig bezeichnetes Konto. Das ist eine vorgeschlagene Zahlung, keine beobachtete Transaktion oder ein Marktdurchschnitt [S1].

Beispiel	Angebotener Betrag	Einheit	Grenze
Kontokaufgesuch, B11	$8	Ein als gültig bezeichnetes Konto	Zahlung und Kontokontrolle ungeprüft
Versicherungsmarkiertes Angebot, B01	Im ausgewählten Ausschnitt nicht genannt	Dateien und vertragsbezogene Zeilen	Kein vergleichbarer Transaktionspreis festgestellt
Dienstleisterangebot, B04	Im ausgewählten Ausschnitt nicht genannt	Behaupteter Datensatz	Exklusivitätsbehauptung belegt keinen abgeschlossenen Verkauf

Ein geforderter Preis ist eine Werbebedingung. Er kann mit Alter, Umfang, behaupteter Exklusivität, Prüfung und Verkäuferreputation variieren. Ohne Belege abgeschlossener Transaktionen und vergleichbarer Produkte darf er keine Verlustschätzung oder ein Marktdurchschnitt werden.

Dasselbe gilt für Konto- und Identitätsbeschreibungen. Verkäufer können vollständig verifizierte Konten, Dokumentensätze oder Wiederherstellungsdienste beschreiben. Der Text belegt das Angebot. Er belegt weder Kontobestand noch rechtmässige Verifizierung oder erlangte Käuferkontrolle.

Für die Abwehr zählt zuerst, ob die Behauptung ein eigenes Konto, einen Kunden oder Dienst betrifft. Danach ist bestätigende Aktivität zu prüfen. Erst dann lässt sich die Verhältnismässigkeit von Kontoeingriff, Betrugskontrolle, Kundenunterstützung oder breiterer Vorfallreaktion beurteilen.

8.5 Zahlungskartenmaterial im engen Umfang

UMFANG DER KARTENANGABEN

Diese Beobachtungen umfassen nur Zahlungskarten, die im aufbewahrten Darkweb-Beitragsmaterial dieses Berichts im Klartext erschienen. Brandefense erkennt gestohlene Karten auch mit anderen Methoden ausserhalb dieses Abschnitts. Diese Beobachtungen messen weder Kartendiebstahl noch aktive Karten, Betrugsverluste oder die gesamte Brandefense-Abdeckung.

Die aufbewahrte Grundgesamtheit enthält 164 unterschiedliche, der Schweiz zugeordnete Klartextkarten in 165 Beiträgen. Dies ist die oben beschriebene enge Grundgesamtheit [S4].

Ein Beitrag kann eine Karte als funktionierend bezeichnen oder eine scheinbare Prüferantwort zeigen. Dies bleibt eine Darstellung des Verfassers. Es ist kein vom Herausgeber autorisierter Test und belegt keine abgeschlossene Belastung. Der Bericht veröffentlicht weder persönliche Angaben noch Kartennummern oder nutzbares Kartenmaterial.

Ein Herausgeber sollte relevante externe Signale über etablierte interne Prozesse prüfen. Kundenkontakt, Kontobeschränkung oder Kartenersatz hängen von seinen Belegen ab. Eine kleine aufbewahrte Beitragsgrundgesamtheit belegt weder hohe noch geringe nationale Finanzverluste durch Karten.

8.6 Die Abfolge an mehreren Stellen unterbrechen

Die folgende Abfolge ist ein **analytisches Modell** zur Kontrollplanung. Sie belegt keinen gemeinsamen Betreiber hinter den zitierten Warnungen oder aufbewahrten Anzeigen.

Stufe	Möglicher Missbrauch	Entscheidungspunkt	Verantwortliche
Information	Echte persönliche oder Buchungsdetails erscheinen in einer Nachricht	Absenderberechtigung getrennt prüfen	Kundenservice
Überzeugung	Dringlichkeit oder vertrauenswürdige Institutionsrolle wird behauptet	Unerwarteten Kontakt beenden und etablierten Weg nutzen	Empfänger und Support
Identität	Anrufende verlangen Rücksetzung oder neue Wiederherstellungsdaten	Sensible Änderung unabhängig prüfen	Identitätsbetrieb
Zahlung	Neuer Begünstigter, Bargeldbezug oder Kartenhandlung wird verlangt	Transaktions- und Betrugsprüfung des Instituts anwenden	Betrugsbetrieb
Nachbetreuung	Empfänger melden versuchten oder vollendeten Betrug	Belege sichern und weitere Exposition beurteilen	Vorfall- und Kundenteams

Das Modell schafft mehrere Handlungsmöglichkeiten. Jemand hat möglicherweise Informationen preisgegeben, kann aber eine Zahlung noch stoppen. Ein Anbieter hat möglicherweise Systeme wiederhergestellt, muss Kunden aber weiter auf gezielte Nachrichten vorbereiten. Technischer Vorfallabschluss sollte deshalb nicht das Ende der Betrugsunterstützung bedeuten.

KERNAUSSAGEN

01

Prüfen Sie Berechtigung getrennt von der Richtigkeit persönlicher Angaben oder Buchungsdetails.

02

Behandeln Sie Angebotspreise und Prüfkennzeichnungen als Behauptungen, ohne Verkäufe oder Verluste abzuleiten.

03

Geben Sie Kunden und Support einen vertrauenswürdigen Weg unabhängig von der verdächtigen Nachricht.

KAPITEL 09

Vertiefung zum Bankwesen

09

DIESES KAPITEL BEANTWORTET

Welche Bankentscheidungen verbinden Identität, Betrug, Dienstleister und Aufsicht?

40

Bank- und Finanzkandidaten in der ausgewählten Grundgesamtheit

9.1 Gemessene Banken- und Herausgebergrundgesamtheiten 80

9.2 Bankgeheimnis ist keine Cyberrisikoableitung 81

9.3 Identitäts- und Betrugsbelege verbinden, ohne Fälle zu vermischen 81

9.4 Dienstleistererkennung kann die Aufsichtsprüfung auslösen 81

9.5 Eine Bankenübung auf Grundlage der Warnungen 82

KAPITEL 09

Vertiefung zum Bankwesen

KURZFASSUNG

Die 40 ausgewählten Bank- und Finanzorganisationen erfassen mindestens 16 082 Gerätezuordnungen und 1 055 051 historische Zugangsdatenzuordnungen. Zugangsdaten mit Bezug zu 7 wurden zum Prüfzeitpunkt angeboten. Das sind Beobachtungen, keine Zahlen betroffener Kunden oder bestätigten Bankeinbrüche. Herausgeberteilmenge und enge Kartengrundgesamtheit beantworten getrennte Fragen. Beauftragen Sie Identitäts-, Endgeräte- und Betrugsteams, jedes relevante Signal anhand autorisierter Unterlagen zu prüfen.

9.1 Gemessene Banken- und Herausgebergrundgesamtheiten

Die Auswahl enthält 40 Bank- und Finanzkandidaten. Diese gezielte Zelle ist weder vollständige Liste zugelassener Banken noch repräsentative Stichprobe. Primäre Domains definieren nicht jede Tochtergesellschaft, jedes Kundenportal oder jede ausgelagerte Funktion [S3].

Beobachtung	Anzahl
Geprüfte Bank- und Finanzorganisationen	40
Organisationen mit aktuellen Listungen	7
Gerätezuordnungen, mindestens	16 082
Mitarbeitendengeräte-Zuordnungen	236
Historische Zugangsdatenzuordnungen	1 055 051

Die mit Kartenherausgebern abgeglichene Teilmenge enthält 6 Organisationen dieser Bankenzelle. Sie erfasst 4 mit aktuellen Zugangsdatenlistungen, 5 mit Mitarbeitendengeräte-Zuordnungen und 6 mit Zuordnungen ausserhalb dieser Klassifikation [S3][S4].

Diese Teilmenge enthält 208 Mitarbeitendengeräte-Zuordnungen und 12 924 weitere Gerätezuordnungen. Die erhaltene Beitragsgrundgesamtheit ordnet diesen Herausgebern 7 unterschiedliche Klartextkartenbeobachtungen zu. Es sind überlappende Grundgesamtheiten mit unterschiedlicher Bedeutung, keine Zahlen betroffener Kunden oder Betrugsverluste.

Eine Kartenbeobachtung belegt keinen Einbruch beim Herausgeber. Eine Gerätezuordnung belegt weder Eigentum noch aktuelle Infektion oder ein weiterhin aktives Bankkonto. Prüfen Sie jedes Signal über autorisierte Identitäts-, Endgeräte- und Betrugsprozesse des Herausgebers.

Offizielle Betrugswarnungen bleiben quellenspezifische Beispiele [S14][S44][S45]. Testen Sie damit vertrauenswürdige Prüfung und Transaktionseskalation. Trennen Sie passive Konfigurationsprüfungen von der nationalen Atlas-Kennzahl und Kontountersuchungen.

9.2 Bankgeheimnis ist keine Cyberrisikoableitung

Der Bericht nimmt keine Position zu Bankgeheimnis oder Regierungspolitik ein. Er leitet weder Sicherheitslage noch Angreiferinteresse oder Vorfallsursache aus einer rechtlichen oder politischen Beschreibung des Finanzsektors ab. Die Belege betreffen konkrete Behauptungen, offizielle Warnungen und ausgewählte Kontrollbeobachtungen.

Für Banken zählt, welche Informationen Zugriff oder Transaktionen autorisieren dürfen. Kenntnis von Kundenadresse, Vorsorgehistorie oder anderen privaten Details sollte Berechtigung nicht automatisch belegen. Die Warnungen zeigen, weshalb richtiger Kontext und betrügerische Anweisung zusammen auftreten können [S14] [S44][S45].

Mitarbeitende benötigen einen nutzbaren Prüfweg unabhängig von Anruferangaben. Der Prozess sollte dringende Kundenhandlungen, vermeintliche Führungskräfte mit Ausnahmegesuchen und angebliche Dienstleistermeldungen umfassen. Jeder Fall braucht einen anderen Bestätigungsweg und klare Verantwortung.

9.3 Identitäts- und Betrugsbelege verbinden, ohne Fälle zu vermischen

Eine Identitätswarnung kann verdächtige Anmeldung belegen, ohne einen betrügerischen Transfer zu zeigen. Eine Zahlungswarnung kann ungewöhnliche Transaktion belegen, ohne Nutzung des Onlinekontos zu zeigen. Ein Informationsleck kann Anrufe überzeugender machen, ohne Zugang zu Banksystemen zu liefern.

Eine gemeinsame Vorfalldokumentation sollte diese Unterschiede bewahren. Der Identitätsbetrieb kann Sitzungen, Wiederherstellungsänderungen und Anwendungszugriff erfassen. Der Betrugsbetrieb kann Begünstigte, Genehmigungsweg und Transaktionsstatus dokumentieren. Der Kundenservice kann Kommunikation sichern und Kontaktweise erklären.

Die gemeinsame Sicht hilft bei angemessener Reaktion. Sitzungswiderruf betrifft einen Zugangsweg, die Prüfung neuer Begünstigter einen anderen. Die Unterstützung bei Nachrichtenprüfung betrifft einen dritten. Keine einzelne Massnahme belegt vollständige Problemlösung.

9.4 Dienstleistererkennung kann die Aufsichtsprüfung auslösen

FINMA bezieht ausgelagerte Funktionen in die Vorfallverantwortung des Instituts ein. Für die beschriebene Meldepflicht kann die Frist mit Angriffsfeststellung durch Institut oder Anbieter beginnen. Das Institut darf nicht seine spätere Leitungssitzung als Fristbeginn annehmen [S8].

Der FINMA-Risikomonitor 2025 hält fest, dass Meldungen zu Angriffen auf Dritte im angegebenen Zeitraum rund 47% der bei der FINMA gemeldeten Cybervorfälle ausmachten [S109]. Dieser Aufsichtsrichtwert erklärt die Bedeutung von Auslagerungsübungen im Finanzsektor, ohne eine Dienstleistervorfallsrate für die 40 ausgewählten Bank- und Finanzkandidaten abzuleiten [S3][S109].

Testen Sie die erste Dienstleistermeldung praktisch. Sie sollte betroffene Funktion, Entdeckungszeit, bekannte Folgen, Unsicherheit und einen auskunftsfähigen Kontakt nennen. Compliance- und Vorfallteams sollten die Meldepflicht während laufender technischer Untersuchung beurteilen können.

Das Institut sollte seine Aufsichtsmeldung auch von anderen Pflichten trennen. Personendatenrisiko und kritische Infrastruktur haben eigene Auslöser. Ein über einen Kanal weitergeleitetes Formular erfüllt nicht automatisch alle Meldungen. Kapitel 10 beschreibt die Unterschiede [S6][S7][S8].

9.5 Eine Bankenübung auf Grundlage der Warnungen

Nutzen Sie einen Anruf mit Bezug auf echten Dienstleistervorfall und richtigen persönlichen Angaben. Gefordert wird dringender Schutztransfer oder Bargeldbewegung. Die Übung sollte Support-, Betrugs- und Identitätsteams gemeinsam testen [S14][S44][S45].

Der Abschlussnachweis des Kundenservice ist ein unabhängig verifizierter Kontaktweg. Das Betrugsteam dokumentiert die Transaktionsentscheidung. Das Identitätsteam beurteilt Kontozugriff und Wiederherstellungsänderungen. Die Kommunikation erklärt klar, was das Institut weiss.

Ein zweites Szenario kann mit einer Cyberwarnung eines Auslagerungsanbieters beginnen. Dienstverantwortliche müssen betroffene Bankfunktion und Kontinuitätslösung bestimmen. Compliance dokumentiert geltende Meldepflichten. Die Infrastruktur weist Wiederherstellung unabhängig vom Produktionszugang des betroffenen Anbieters nach.

Das Ergebnis sollte aus nachgewiesenen Entscheidungen bestehen und keiner Sicherheitserklärung der Bank. Eine Übung kann fehlenden Kontakt, unklaren Auslöser oder nicht verfügbares Wiederherstellungskonto zeigen. Dies sind bearbeitbare Befunde mit Verantwortlichen und Abschlussbelegen.

KERNAUSSAGEN

01

Halten Sie Identitäts-, Transaktions- und Datenoffenlegungsbefunde in einer gemeinsamen Fallakte getrennt.

02

Testen Sie die erste Dienstleistermeldung gegen eigene Meldeverantwortlichkeiten des Instituts.

03

Nutzen Sie vertrauenswürdige Prüfung und unabhängige Wiederherstellung als nachweisbare Bankkontrollen.

KAPITEL 10

Regulatorische und nationale Reaktion

10

DIESES KAPITEL BEANTWORTET

Welche Schweizer Meldepflichten gelten, wann beginnen Fristen und was sollten Organisationen vorbereiten?

24 h

Erstmeldung kritischer Infrastruktur nach Entdeckung, sofern die Pflicht gilt

10.1 Drei Pflichten können für einen Vorfall gelten 84
10.2 Kritische Infrastrukturen: Geltung vor einem Vorfall klären 85
10.3 Personendaten: Schaden für Menschen beurteilen 85
10.4 Finanzinstitute: Dienstleistererkennung bei der Frist berücksichtigen 86
10.5 Ein geplantes Cybersicherheitsgesetz ist keine geltende Pflicht 87
10.6 Eine Belegdokumentation und mehrere Entscheidungen vorbereiten 87

KAPITEL 10

Regulatorische und nationale Reaktion

KURZFASSUNG

Die Schweiz hat getrennte Meldepflichten für kritische Infrastrukturen, Personendaten und beaufsichtigte Finanzinstitute. Umfang, Fristen und Abschlussanforderungen unterscheiden sich. Die Pflicht für kritische Infrastrukturen ist bereits in Kraft. Das geplante Cybersicherheitsgesetz ist künftige Gesetzgebung; ein Vernehmlassungsentwurf ist für Juni 2027 beauftragt. Erstellen Sie eine Vorfalldokumentation für alle geltenden Pflichten. Bestimmen Sie Verantwortliche für rechtzeitige Erstmeldungen bei unvollständigen Fakten.

10.1 Drei Pflichten können für einen Vorfall gelten

Ein technischer Vorfall kann mehrere rechtliche Prüfungen erfordern. Das Informationssicherheitsgesetz betrifft Cyberangriffe auf erfasste kritische Infrastrukturen. Artikel 24 des Datenschutzgesetzes betrifft Datensicherheitsverletzungen und Personenrisiken. FINMA-Hinweise betreffen wesentliche Cybervorfälle beaufsichtigter Institute [S6][S7][S8].

Diese Pflichten haben unterschiedliche Auslöser. Sie sollten eine Dokumentation teilen, ohne austauschbar zu werden. Rechtsverantwortliche müssen Geltung, Nichtgeltung oder noch nötige Fakten dokumentieren. Dieses Kapitel fasst offizielle Hinweise zusammen und ist keine Rechtsberatung.

Die Tabelle trennt den Beginn jedes Arbeitsstrangs von seiner zentralen Meldeanforderung.

Regelwerk	Geltungsentscheidung	Erstanforderung	Weitere Anforderung
Informationssicherheitsgesetz und Cybersicherheitsverordnung	Erfasste kritische Infrastruktur und meldepflichtiger Cyberangriff	BACS-Meldung innerhalb 24 Stunden nach Entdeckung [S6]	Meldung innerhalb 14 Tagen vervollständigen; Kalendertage [S12]
Datenschutzgesetz, Artikel 24	Zuerst anwendbares Recht und zuständige Aufsichtsbehörde klären [S106]. Bei EDÖB-Zuständigkeit eine Datensicherheitsverletzung mit voraussichtlich hohem Risiko für Persönlichkeit oder Grundrechte Betroffener beurteilen	Verantwortlicher meldet dem EDÖB so rasch als möglich [S7]	Betroffene informieren, wenn zu ihrem Schutz erforderlich oder vom EDÖB verlangt [S7]
FINMA-Aufsichtsmitteilung 05/2020, präzisiert durch 03/2024	Beaufsichtigtes Institut und Vorfall gemäss Meldekriterien	Erstmeldung innerhalb 24 Stunden [S8]	Vollständige Meldung innerhalb 72 Stunden über FINMA-Plattform, gemäss Fristregeln der Mitteilung [S8]

Die Finanzsektorfrist erfordert besondere Aufmerksamkeit. FINMA zählt die 24- und 72-Stunden-Fristen in offiziellen Bankwerktagen. Schwere Angriffe bilden eine Ausnahme: Erstmeldung innerhalb 24 Stunden auch ausserhalb der Bankwerktage [S8]. Eine vereinfachte Einheitsfrist im Vorfallhandbuch würde den Unterschied übersehen.

10.2 Kritische Infrastrukturen: Geltung vor einem Vorfall klären

Das BACS nennt Informationssicherheitsgesetz und Cybersicherheitsverordnung als Rechtsgrundlage der Meldepflicht [S6]. Sie erfasst bestimmte Behörden und Organisationen, etwa Energie, Trinkwasser, Transport sowie Kantons- oder Gemeindeverwaltungen. Die Verordnung enthält Ausnahmen [S6]. Sektorzugehörigkeit allein klärt deshalb nicht den Status jeder Organisation.

Laut BACS kann es die Unterstellung interessierter Behörden oder Organisationen feststellen. Bei Unklarheit kann eine Verfügung beantragt werden [S12]. Das ist eine konkrete Vorbereitungsaufgabe für Rechts- und Kontinuitätsverantwortliche. Dokumentieren Sie Antwort, geprüfte Dienste und Zuständigkeit für erneute Beurteilung.

Auch das meldepflichtige Ereignis ist zu beurteilen. Offizielle Hinweise nennen Angriffe auf die Funktionsfähigkeit kritischer Infrastrukturen, Informationsmanipulation oder -offenlegung, länger unentdeckte Angriffe sowie Erpressung, Drohung oder Nötigung [S12]. Ein IT-Angriff ist nicht allein deshalb ausgenommen, weil Betriebstechnik weiterläuft.

Umgekehrt schafft DDoS gegen eine unkritische Anwendung laut BACS nicht automatisch eine Meldepflicht. Entscheidend ist die Gefährdung der Betriebsfähigkeit kritischer Infrastruktur [S12]. Die Dokumentation sollte deshalb betroffene Geschäftsfunktion statt nur technischer Symptome nennen.

Eine unvollständige Untersuchung setzt die Erstfrist nicht aus. Das BACS verlangt Erstmeldung innerhalb 24 Stunden auch bei fehlender vollständiger Information. Ergänzungen können die Meldung innerhalb 14 Kalendertagen vervollständigen [S12]. Erfassen Sie bestätigte Fakten, Unsicherheit und Verantwortliche des nächsten Updates.

Die Pflicht begann am 1. April 2025. Sanktionsbestimmungen traten am 1. Oktober 2025 in Kraft, mit möglichen Bussen bis CHF 100 000 [S60]. Nicht jede verspätete Meldung führt automatisch zu einer Busse. Die offizielle Darstellung beschreibt Betreiberkontakt, anschliessende Verfügung und mögliche Strafanzeige bei weiterhin ausbleibender Reaktion [S60].

10.3 Personendaten: Schaden für Menschen beurteilen

Klären Sie zuerst das anwendbare Datenschutzrecht und die zuständige Aufsichtsbehörde. Der EDÖB beaufsichtigt private Personen und Bundesorgane. Kantons- und Gemeindebehörden sollten ihre anwendbaren kantonalen Anforderungen und die zuständige Aufsichtsbehörde prüfen [S106].

Die EDÖB-Hinweise definieren Datensicherheitsverletzungen durch unbeabsichtigten oder unrechtmässigen Verlust, Löschung, Vernichtung, Änderung, Offenlegung oder Zugriff auf Personendaten [S7]. Ein öffentliches Leck ist nicht erforderlich. Verfügbarkeit und Integrität können ebenso zählen wie Vertraulichkeit.

Verantwortliche müssen dem EDÖB so rasch als möglich melden, wenn die Verletzung voraussichtlich hohes Risiko für Persönlichkeit oder Grundrechte schafft [S7]. Dies ist keine allgemeine Schweizer 72-Stunden-Frist. Die Beurteilung muss Informationen und Folgen für Betroffene berücksichtigen.

Die Hinweise warnen vor Abwarten bei Zweifeln, wenn hohes Risiko nicht genügend ausgeschlossen werden kann. Geplante Massnahmen beseitigen die Meldefrage nicht. Verantwortliche sollten Wissensstand, Risikogrundlage und bereits belegte Schutzmassnahmen dokumentieren [S7].

Behördenmeldung und Information Betroffener sind getrennte Entscheidungen. Artikel 24 verlangt Personeninformation, wenn sie zum Schutz erforderlich ist oder der EDÖB sie fordert [S7]. Kundenmitteilungen sollten relevante Fakten und Schutzmassnahmen erklären, ohne offengelegte Informationen zu wiederholen.

Dies hilft bei Behauptungen zu alten Kundendaten. Das Anzeigendatum belegt keinen Zugriffszeitpunkt. Die Organisation sollte Echtheit und nötige Schutzmassnahmen bestimmen. Die rechtliche Beurteilung sollte den Belegen und nicht der Verkaufsbeschreibung folgen.

10.4 Finanzinstitute: Dienstleistererkennung bei der Frist berücksichtigen

FINMA erwartet eine erste Kritikalitätsbeurteilung innerhalb der Erstmeldefrist [S8]. Muss das Institut zwischen abgeschlossener Beurteilung und Fristeinhaltung wählen, sollte es die Frist priorisieren. Eine Erstmeldung kann später zurückgezogen werden, wenn die Untersuchung fehlende Meldekriterien zeigt.

Bei ausgelagerten Funktionen beginnt die Frist mit Feststellung des Cybervorfalls beim Institut oder Anbieter [S8]. Vertrag und Eskalationsprozess müssen deshalb die Entdeckungszeit des Anbieters in die Vorfalldokumentation bringen. Warten auf dessen Abschlussbericht kann notwendige Informationen für die eigene Pflicht verzögern.

Die Hinweise behandeln auch Anbieter ohne wesentliche Auslagerungsrolle. Institute müssen Informationen über relevante Anbieter-Cybervorfälle erhalten und die eigene Meldepflicht beurteilen [S8]. Ein auf grösste Verträge begrenztes Register kann Betriebsabhängigkeiten übersehen.

Auch dem Informationssicherheitsgesetz unterstellte Institute können ihre Erstmeldung über das BACS-Formular an FINMA weiterleiten, sofern rechtzeitige Übermittlung gewährleistet ist. Die vollständige 72-Stunden-Meldung muss weiterhin über die FINMA-Erhebungs- und Gesuchsplattform erfolgen [S8]. Bewahren Sie Zustellnachweise jeder erforderlichen Eingabe auf.

Der Meldeprozess sollte gemeinsam mit der Wiederherstellung geübt werden. FINMA verlangt szenariobasierte Cyberübungen und unterscheidet systemrelevante von anderen Instituten [S8]. Ihre Darstellung vom Februar 2026 hebt unvollständige institutsspezifische Szenarien, unklare Zuständigkeiten und ungenügend getestete Reaktionsprozesse hervor [S61].

Eine Bankenübung kann Anbieterausfall, unklaren Kundendatenzugriff und Entdeckung am Wochenende verbinden. Ziel sind notwendige Erstentscheidungen ohne vollständige Forensik. Testen Sie auch die Genehmigung von Kundenkommunikation und den Weiterbetrieb kritischer Dienste.

10.5 Ein geplantes Cybersicherheitsgesetz ist keine geltende Pflicht

Am 25. September 2026 beauftragte der Bundesrat das VBS mit einem Vernehmlassungsentwurf für ein eigenständiges Cybersicherheitsgesetz bis Juni 2027 [S11]. Die Ankündigung betrifft vorgeschlagene Anforderungen an digitale Produkte, wichtige digitale Daten sowie Hosting- oder Cloud-Dienste. Sie sieht auch die Überführung der bestehenden Infrastrukturmeldepflicht vor.

Die Ankündigung beschreibt Gesetzgebung in Entwicklung. Sie belegt keine bereits geltenden vorgeschlagenen Pflichten am Berichtsstichtag. Laut Quelle bleiben bestehende sektorale Regeln in Kraft [S11]. Erfassen Sie das Vorhaben als rechtliches Beobachtungsthema und nicht als bereits geltende Betriebsfrist.

Der Vorschlag nennt den EU Cyber Resilience Act als Vorbild für Produktregeln [S11]. Das macht nicht jede EU-Cyberpflicht zu Schweizer Inlandspflicht. Internationale Gruppen sollten Rechtsträger, Dienste und geltende Zuständigkeiten einzeln prüfen. Der Bericht nimmt keine Position zur politischen Entscheidung oder zu Schweizer EU-Beziehungen ein.

10.6 Eine Belegdokumentation und mehrere Entscheidungen vorbereiten

Die Vorbereitungsaufgaben machen aus getrennten Regelwerken einen Prozess, der bei Unsicherheit funktioniert.

Vorbereitung	Verantwortliche	Abschlussnachweis
Infrastrukturstatus und geltende Ausnahmen klären	Recht und Kontinuitätsleitung	Schriftliche Geltungsbeurteilung mit Überprüfungsdatum
Entdeckung beim Institut und relevanten Anbietern erfassen	Vorfallleitung	Zeitgestempelte Ereignisdokumentation mit erklärter Unsicherheit
Betroffene Menschen und wahrscheinlichen Schaden beurteilen	Datenschutzleitung	Dokumentierte Risikobeurteilung und Meldeentscheidung
Erstmeldungen mit unvollständigen Fakten vorbereiten	Rechts- und Sicherheitsleitung	Getestete Vorlagen und benannte einreichende Person mit Stellvertretung
Meldekanäle und Zustellnachweise bestätigen	Compliance-Leitung	Erprobter Zugang und aufbewahrte Bestätigung
Anbieterausfall mit Geschäftsverantwortlichen üben	Kontinuitätsleitung	Getesteter Alternativprozess, Wiederherstellungsbelege und zugewiesene Verbesserungen

Die Vorfallleitung sollte Beobachtungen von Schlussfolgerungen trennen. Akteursbehauptung, Dienstausfall, bestätigter unberechtigter Zugriff und bestätigte Datenoffenlegung können zu unterschiedlichen Zeiten hinzukommen. Jede kann die Rechtsbeurteilung ändern. Die Dokumentation sollte Entscheidende und tragende Belege zeigen.

KERNAUSSAGEN

01

Die Infrastrukturpflicht gilt bereits. Melden Sie gegebenenfalls innerhalb 24 Stunden und vervollständigen Sie innerhalb 14 Kalendertagen.

02

EDÖB und FINMA haben getrennte Auslöser und Fristen. Anbietererkennung kann die Finanzmeldefrist starten.

03

Das geplante Cybersicherheitsgesetz bleibt ein Beobachtungsthema. Erfüllen Sie heutige Pflichten und verfolgen Sie den Vernehmlassungsentwurf.

KAPITEL 11

Ausblick

11

DIESES KAPITEL BEANTWORTET

Welche Belege sollten die nächste Sicherheitsentscheidung oder diese Einschätzung verändern?

5

bedingte Einschätzungen mit ausdrücklichen Grenzen und Reaktionssignalen

11.1 Zentrale Einschätzungen 90

11.2 Was die Einschätzung verändern würde 91

11.3 Bedingte Szenarien 91

11.4 Entscheidungsbezogener Prüfrhythmus 92

KAPITEL 11

Ausblick

KURZFASSUNG

Planen Sie für Datenerpressung, Identitätsmissbrauch, Dienstleisterstörung und gezielte Informationssammlung. Die Belege liefern keine Angriffswahrscheinlichkeiten einzelner Schweizer Organisationen. Offizielle Einschätzungen und beobachtete Behauptungen erfüllen unterschiedliche Zwecke. Die Szenarien machen daraus Entscheidungen mit Verantwortlichen und planverändernden Belegen. Überprüfen Sie jede Einschätzung bei neuen Organisationsbelegen.

11.1 Zentrale Einschätzungen

Die Einschätzungen betreffen Planungsprioritäten. Der Vertrauensgrad beschreibt die jeweilige Aussage und weder Akteurszuverlässigkeit noch Angriffswahrscheinlichkeit einer Organisation.

Einschätzung	Vertrauensgrad	Grundlage und Grenze	Entscheidungssignal
Erpressung rechtfertigt erprobte Geschäftswiederherstellung	Hoch für Vorbereitungsbedarf	Bericht erfasst Ransomware-Listungen; NDB nennt Ransomware-Risiko kritischer Infrastruktur [S2][S9]. Listungen bestätigen keine Einzelvorfälle	Bestätigter Zugang, beeinträchtigte Wiederherstellung oder relevanter Dienstleistervorfall
Sensible Forschungs- und Politikinformationen benötigen Kontrollen dauerhafter Zugänge	Hoch für Quelleneinschätzung	NDB nennt Informationsziele, Phishing und Netzwerkausrüstungsausnutzung [S9]. Daraus folgt keine Angriffswahrscheinlichkeit	Unerklärter Zugriff, externe Freigabe oder verdächtiger Kontakt zu sensiblen Tätigkeiten
Anbietererkennung muss die Vorfallleitung rasch erreichen	Hoch für Meldeabhängigkeit	FINMA-Frist für ausgelagerte Funktionen kann mit Anbietererkennung beginnen [S8]. Geltung hängt von Institut und Vorfall ab	Anbieter stellt Cybervorfall einer ausgelagerten Funktion fest
Öffentliche Anlässe rechtfertigen Kontinuitätsbereitschaft	Mittel für Planungsszenario	NDB nennt anlassbezogenes Überlastungsrisiko; Gipfel 2024 liefert historischen Kontext [S9][S10]. Keine neue Kampagne festgestellt	Relevante Akteursbehauptungen mit Dienstanomalien oder Anbieterwarnungen
Meldebereitschaft kann vor vollständiger Sachklärung verbessert werden	Hoch für Vorbereitungsbedarf	Offizielle Hinweise erlauben Erstmeldung mit späteren Ergänzungen [S8][S12]. Rechtsauslöser muss trotzdem geprüft werden	Potenziell meldepflichtiger Vorfall mit unvollständigen technischen Fakten

Zuerst zählt, ob die Belege Ihren Dienst betreffen. Eine nationale Warnung kann Bereitschaftsprüfung rechtfertigen. Sie belegt weder ein bestimmtes aktives Konto noch ein echtes Datenangebot oder eigene Datensätze beim betroffenen Anbieter. Dafür sind Organisationsbelege nötig.

Prioritäten unterscheiden sich auch geschäftlich. Eine Forschungseinrichtung kann externe Projektzugänge priorisieren. Ein Zahlungsanbieter kann Kundenkontoschutz und Dritteskalation voranstellen. Ein öffentlicher Betreiber braucht möglicherweise vor einem sichtbaren Anlass einen getesteten manuellen Prozess. Derselbe nationale Kontext kann diese unterschiedlichen Entscheidungen stützen.

11.2 Was die Einschätzung verändern würde

Die Tabelle nennt Belege für eine geänderte Reaktion. Sie nennt auch entlastende Belege, damit ungeprüfte Behauptungen keinen dauerhaften Ausnahmezustand schaffen.

Neue Belege	Reaktionsänderung	Belege zur Eingrenzung	Verantwortliche
Aktuelles gültiges Konto erscheint in relevanten Expositionsbelegen	Konto, Sitzungen und Zugriffshistorie untersuchen; nach Befund eindämmen	Konto bereits deaktiviert, Angaben veraltet oder keine gestützte Organisationsverbindung	Identitäts- und Vorfallteams
Anbieter bestätigt Zugriff auf Mandanten mit Organisationsdaten	Umfang, Meldefristen und Kontinuitätsoptionen bestimmen	Relevanter Mandant, Daten und Verwaltungswege nachweislich unberührt	Anbieter- und Rechtsverantwortliche
Datenmuster entspricht kontrollierten internen Datensätzen	Dokumentierte Untersuchung und Datenschutzrisikoprüfung beginnen	Frühere bereinigte Offenlegung oder öffentliche Information mit geprüftem Restrisiko	Daten- und Datenschutzverantwortliche
Relevante öffentliche Website fällt während Akteurskampagne aus	Dienstfolgen bestätigen und Anbieter eskalieren	Interne und Anbieterbelege zeigen unverbundenen Fehler	Dienst- und Kommunikationsverantwortliche
Ungewöhnliche Aktivität erreicht sensiblen Forschungs- oder Politikarbeitsbereich	Belege sichern und dauerhaften Zugriff sowie Freigaben untersuchen	Informationsverantwortliche und Aufzeichnungen bestätigen autorisierte Aktivität	Informationsverantwortliche und Sicherheitsteam

Keines dieser Signale verlangt sofortige öffentliche Zuschreibung. Stellen Sie zuerst Dienstfolgen, Zugriff und Datenumfang fest. Zuschreibung kann ungeklärt bleiben, während die Organisation Schaden begrenzt und Meldepflichten erfüllt. Kommunikation sollte dieselbe Unsicherheit wie die Untersuchung bewahren.

11.3 Bedingte Szenarien

Erstes bedingtes Szenario: Ein Anbieterdienst fällt während einer Datenerpressungsbehauptung aus. Dies ist eine Planungsannahme. Unterstützt der Anbieter einen kritischen Geschäftsprozess, aktivieren Sie den vereinbarten Kontinuitätsprozess und prüfen Organisationsdatenzugriff. Benennen Sie Geschäftsverantwortliche für Dienstwiederherstellung und getrennte Verantwortliche für die Datenfrage.

Zuerst benötigt werden Entdeckungszeit und vom Anbieter bestätigte betroffene Systeme. Finanzinstitute sollten die Auslagerungsmelderegel ohne abschliessende Anbieteruntersuchung prüfen [S8]. Andere erfasste kritische Dienste sollten Betriebsfähigkeit und Meldeauslöser prüfen [S12]. Die Übung endet bei funktionierendem genehmigtem Alternativprozess und Verantwortlichen für Restrisiken.

Zweites bedingtes Szenario: Ein Akteur nennt ein politisches Thema und einen öffentlichen Dienst. Die Erklärung bleibt seine eigene. Prüfen Sie Anomalien mit Anbieter und Geschäftsverantwortlichen. Sichern Sie die Behauptung, ohne Beschimpfungen zu wiederholen oder Positionen zu übernehmen. Kommunizieren Sie verifizierte Dienstfolgen der Organisation.

Die historische Gipfelbilanz zeigt den Wert getrennter Erklärungen: Das NCSC unterschied DDoS, Einbruchsversuche, Phishing und unverbundene technische Probleme [S42]. Das Szenario sollte diese Trennung testen. Es endet, wenn Dienstverantwortliche Unterbrechung erklären, Wiederherstellung dokumentieren und Ungeprüftes benennen können.

Drittes bedingtes Szenario: Ein sensibles Projekt erhält überzeugenden externen Kontakt. Der NDB nennt gezielte Nachrichten und Messaging-Kontakte als Spionagetechniken [S9]. Betrifft verdächtiger Kontakt ein echtes Forschungs- oder Politikprojekt, prüfen Sie den Absender über einen etablierten Kanal. Untersuchen Sie zugehörige Authentisierungs-, Freigabe- oder Softwareinstallationsbelege.

Informationsverantwortliche sollten zusätzlichen Zugriffsschutz für Projektmaterial bestimmen. Das Sicherheitsteam sollte über die erste Nachricht hinaus nach Zugriff suchen. Das Szenario endet mit geklärtem Kontakt und dokumentierter Einordnung betroffener Konten oder Freigabewege. Eine überzeugende Einladung allein belegt keinen erfolgreichen Einbruch.

Viertes bedingtes Szenario: Ein alter Datensatz wird als neuer Vorfall angeboten. Trennen Sie Anzeigen- und Zugriffsdatum. Vergleichen Sie relevant wirkendes Material über autorisierte Prozesse mit aufbewahrten Vorfallsinformationen. Erklären Sie kundennahen Teams, wie echte alte Angaben überzeugenden Betrug unterstützen.

Die Massnahme ändert sich bei Belegen für neuen Zugriffszeitraum oder neu betroffenes System. Datenschutzverantwortliche sollten Risiken bei neuen Fakten erneut beurteilen. Betrifft das Angebot eine bereinigte Offenlegung, dokumentieren Sie dies und fortbestehende Betrugsvorsorge. Beschreiben Sie Wiederverbreitung nicht als Nachweis eines neuen Vorfalls.

11.4 Entscheidungsbezogener Prüfrhythmus

Benennen Sie Prüfverantwortliche für jede Einschätzung und integrieren Sie sie in bestehende Risikoprozesse. Aktualisieren Sie Zuständigkeiten bei Dienst- oder Anbieterwechseln. Neue Beitrags- oder Listungszahlen sollten eine Belegprüfung auslösen und keine automatische Geschäftsrisikoeskalation.

Die nationale Atlas-Kennzahl beschreibt das geprüfte Portfolio. Sektorale Signalzahlen und passive Beobachtungen unterstützen unterschiedliche Prüfaufgaben. Nutzen Sie dokumentierte Dienst-, Informations- und Anbieterabhängigkeiten zur Arbeitsreihenfolge. Beurteilen Sie Prioritäten neu, wenn Kontogültigkeit, relevante Aktivität oder Dienstfolgen feststehen [S3].

Der nützlichste Fortschrittsnachweis ist der belegte Abschluss. Wiederhergestellte Dienste, entfernte Altzugänge, getestete Meldekanäle oder geklärte Anbieterabhängigkeiten verändern die Handlungsmöglichkeiten im Vorfall. Eine wachsende Warnungsliste belegt keine Verbesserung dieser Ergebnisse.

KERNAUSSAGEN

01

Behandeln Sie den Ausblick als bedingte Planung. Der Bericht schätzt keine Angriffswahrscheinlichkeit Ihrer Organisation.

02

Ändern Sie Reaktionen bei bestätigtem relevantem Zugriff, betroffenen Informationen oder Dienstfolgen. Halten Sie Zuschreibung getrennt.

03

Prüfen Sie Prioritäten mit Verantwortlichen und Abschlussbelegen, besonders bei dienstleisterabhängiger Wiederherstellung.

KAPITEL 12

Massnahmenplan

12

DIESES KAPITEL BEANTWORTET

Wer handelt als Nächstes, und welche Belege weisen den Abschluss nach?

3

Umsetzungszeiträume mit benannten Verantwortlichen

12.1 Aufgaben für den nächsten Planungszyklus 95
12.2 Identität und Vorfallbehandlung 97
12.3 Dienstverantwortliche und Anbieter 97
12.4 Betrugs- und Bankenteams 97
12.5 Recht und Kommunikation 98
12.6 Wie Brandefense helfen kann 98

KAPITEL 12

Massnahmenplan

KURZFASSUNG

Machen Sie aus dem Bericht nachweisbare Arbeit. Beginnen Sie mit Kontoprüfung, Anbieterkontakten und Meldeentscheidungsbaum. Üben Sie danach Isolation, Kommunikation und Wiederherstellung. Testen Sie schliesslich den Geschäftsbetrieb während einer wesentlichen Dienstunterbrechung. Jede Massnahme braucht Verantwortung, Auslösebedingung und Abschlussbeleg. Weisen Sie Verantwortung zu, bevor Sie weitere Warnungsquellen kaufen.

12.1 Aufgaben für den nächsten Planungszyklus

Die Zeiträume sind Planungsziele. Sie ersetzen keine gesetzliche Frist, die während eines Vorfalls bereits laufen kann.

30 Tage

Passt ein neues Zugangsdaten- oder Zugangsangebot zu einem Organisationskonto, Status und jüngste Aktivität prüfen

VERANTWORTLICHE

Identitätsbetrieb

ABSCHLUSSNACHWEIS

Einordnung mit Kontostatus, relevanten Sitzungen, Massnahme und offenen Fakten

Bearbeitet ein wesentlicher Anbieter sensible Daten, Vorfallkontakt und Erstmeldeweg prüfen

VERANTWORTLICHE

Beschaffung und Dienstverantwortliche

ABSCHLUSSNACHWEIS

Kontakttest und Daten-Dienst-Abhängigkeitsdokumentation

Könnte ein Ereignis wesentlichen Betrieb beeinträchtigen, Infrastrukturmeldekriterien prüfen

VERANTWORTLICHE

Vorfallleitung und Recht

ABSCHLUSSNACHWEIS

Auslöserentscheidung, Entdeckungszeit und Meldeverantwortliche

Könnten Personendaten betroffen sein, wahrscheinliches Personenrisiko unabhängig von Dienstfolgen prüfen

VERANTWORTLICHE

Datenschutzbeauftragte

ABSCHLUSSNACHWEIS

Dokumentierte Risikobeurteilung und Meldeentscheidung

Nutzt ein Finanzinstitut Auslagerungen, Beginn der Aufsichtsmeldeprüfung klären

VERANTWORTLICHE

Compliance und Auslagerungsverantwortliche

ABSCHLUSSNACHWEIS

Erprobte Anbietermeldung mit dokumentiertem Timing

260 Tage

Kann Helpdeskpersonal sensible Zugänge zurücksetzen, getrennte Kanalprüfung testen

VERANTWORTLICHE

Identitäts- und Supportleitung

ABSCHLUSSNACHWEIS

Übung mit abgewiesenem oder sicher eskaliertem Täuschungsversuch

Könnte eine Kundenwarnung imitiert werden, vertrauenswürdigen Prüfweg vorbereiten

VERANTWORTLICHE

Betrug und Kommunikation

ABSCHLUSSNACHWEIS

Veröffentlichter Kontaktweg und getesteter Callcentergesprächsleitfaden

Treffen politisch gerahmte Behauptungen einen öffentlichen Dienst, Dienstprüfung und Schutzaktivierung üben

VERANTWORTLICHE

Betrieb und Kommunikation

ABSCHLUSSNACHWEIS

Übungszeitleiste trennt Ankündigung, Verfügbarkeit und verifizierte Folgen

Betrifft ein Auftragsbearbeitervorfall mehrere Bereiche, gemeinsame Beleg- und Entscheidungsakte üben

VERANTWORTLICHE

Datenschutz- und Dienstverantwortliche

ABSCHLUSSNACHWEIS

Planspiel mit getrennter Schlussfolgerung je Datenpopulation

390 Tage

Kann ein wesentlicher Dienst ohne Hauptidentitätsplattform nicht laufen, unabhängige Wiederherstellung testen

VERANTWORTLICHE

Kontinuität und Infrastruktur

ABSCHLUSSNACHWEIS

Fachlich genehmigte Wiederherstellung mit getrennten Wiederherstellungszugängen

Benötigt Wiederherstellung einen Anbieter, dessen Rolle gemeinsam testen

VERANTWORTLICHE

Kontinuität und Beschaffung

ABSCHLUSSNACHWEIS

Gemeinsame Übung zu Zugang, Datenprüfung und Rückgabeverantwortung

Wiederholen sich externe Behauptungen, konsistente Wiederaufnahme abgeschlossener Fälle prüfen

VERANTWORTLICHE

Bedrohungsanalyse und Vorfallbehandlung

ABSCHLUSSNACHWEIS

Stichprobenentscheidungen erklären Abschluss oder Eskalation wiederholter Angebote

12.2 Identität und Vorfallbehandlung

Beginnen Sie mit Identitäten, die andere Identitäten ändern können. Helpdeskpersonal, delegierte Administratoren und Wiederherstellungskonten können den Phishing-Ausgang verändern. Starke Anmeldung verliert Wert, wenn überzeugende Anrufende den Wiederherstellungsfaktor ersetzen können.

Testen Sie den tatsächlichen Supportablauf. Eine autorisierte Übung sollte eine dringende Rücksetzung mit plausibler Führungsidentität und richtigen Organisationsangaben verlangen. Abschlussbeleg ist sichere Ablehnung oder Eskalation über unabhängig verifizierten Kontakt. Eine Erinnerungs-E-Mail ist kein gleichwertiger Beleg.

Bei festgestellter unberechtigter Aktivität sichern Sie Aufzeichnungen, bevor Zugangsänderungen Kontext löschen. Prüfen Sie gegebenenfalls Sitzungen, Anwendungsrechte, Postfachregeln und Wiederherstellungsfaktoren. Passwortänderung allein kann andere Wege offenlassen. Vorfallverantwortliche sollten geprüfte und ausserhalb der Sichtbarkeit verbliebene Wege erfassen.

Analyseteams sollten auch auf schwache Signale klar reagieren. Ein Datensatztitel kann einen historischen Vorfall, öffentliches Verzeichnis oder eine andere ähnlich benannte Organisation betreffen. Dokumentieren Sie die Alternative und zusätzliche Belege für eine Wiederaufnahme.

12.3 Dienstverantwortliche und Anbieter

Ordnen Sie wichtige Geschäftsergebnisse ihren Systemen, Konten und Anbietern zu. Bei öffentlichen Anwendungen gehören alternative Einreichungs- und Prüfverfahren dazu. Im Gesundheitswesen zählen klinischer Zugang und Datenprüfung. Bei Finanzdiensten zählen Zahlungsfreigabe, Kundenservice und Abgleich.

Eine nützliche Anbieterübung beginnt mit unvollständiger Meldung. Der Anbieter weiss von unberechtigtem Zugriff, aber nicht vom Datenabfluss. Dienstverantwortliche sollten betroffene Abläufe bestimmen, ohne die Unsicherheit mit Angreiferbehauptungen zu füllen.

Testen Sie danach die nächste Nachricht. Kann der Anbieter geänderte Belege, betroffene Kundengruppe und bestätigte oder vorläufige Datentypen erklären? Das Kundenvorfallteam sollte seine Bewertung aktualisieren können, ohne die Anbieterschlussfolgerung stillschweigend auszuweiten.

Trennen Sie Wiederherstellungs- von Vertraulichkeitsbelegen. Ein funktionierender Dienst belegt keine gewahrte Vertraulichkeit. Umgekehrt belegt eine ungeprüfte Datenbehauptung keinen Betriebsstillstand. Geschäfts- und Datenschutzverantwortliche brauchen getrennte Fakten und Entscheidungen.

12.4 Betrugs- und Bankenteams

Testen Sie kundennahe Verfahren mit offiziellen Beispielen zu Identitätsvortäuschung und Folgephishing. Wer Adresse, Sozialversicherungskennung oder jüngsten Anbietervorfall kennt, kann trotzdem betrügen. Richtige Personendaten sollten Fälle auffinden helfen und weder Zahlungen noch Authentisierungsänderungen autorisieren.

Kontaktzentren benötigen einen genehmigten Wechsel auf einen vertrauenswürdigen Gesprächsweg. Kunden sollten zur Echtheitsprüfung keiner unerwarteten Nachricht folgen müssen. Konsistente Mitteilungen und eine unabhängig erreichbare Prüfseite erleichtern dies.

Betrugsteams sollten Transaktionspausen und Einbezug der Vorfallbehandlung vereinbaren. Identitätsmissbrauch, Zahlungsbetrug und Personendatenoffenlegung können zusammen auftreten, bleiben aber getrennte Befunde. Die Fallakte sollte die Beleggrundlage jeder Schlussfolgerung bewahren.

Herausgeber sollten externe Kartensignale in eigener kontrollierter Umgebung prüfen. Eine Beitragskennzeichnung oder scheinbare Prüferantwort rechtfertigt weder Kontodetailveröffentlichung noch Kundenverlustmeldung. Ersatz- und Kundenkontaktentscheidungen gehören in etablierte Betrugs- und Vorfallprozesse des Herausgebers.

12.5 Recht und Kommunikation

Bereiten Sie einen Entscheidungsbaum mit dem Auslöser jeder Meldepflicht vor. Erfassen Sie Erstentdeckung, betroffene wesentliche Abläufe, wahrscheinliche Personendatenrisiken und mögliche Aufsichtspflichten. Bewahren Sie die Begründung für Geltung oder Nichtgeltung einer Pflicht.

Geben Sie der Kommunikation dieselben Beleggrenzen wie dem Vorfallteam. Eine erste Stellungnahme kann Dienstproblem, Untersuchung und Kundenalternativen nennen, ohne ungeprüfte Akteursvolumen zu wiederholen. Spätere Aussagen sollten Änderungen und weiter unsichere Fakten erklären.

Politische Formulierungen brauchen dieselbe Disziplin. Nennen Sie behauptete Gruppenmotive nur, wenn sie dem Verständnis dienen. Schreiben Sie sie der Gruppe oder Behörde zu. Vermeiden Sie Slogans oder Regierungstiming als Nachweis einer Förderung.

12.6 Wie Brandefense helfen kann

Brandefense verbindet Cyber Threat Intelligence, Digital Risk Protection und External Attack Surface Management auf derselben Plattform [S73]. Für die Entscheidungen dieses Berichts zählt die Verbindung eines externen Signals mit Organisationsanlagen und einem klar verantworteten Prüfschritt.

Nutzen Sie Bedrohungsanalyse zum Sichern und Beurteilen von Behauptungen. Digitale Risikoarbeit hilft beim Verständnis von Marken- und Kommunikationsmissbrauch. Externe Anlagensichtbarkeit klärt Dienstverantwortung und Prüfzuständigkeit für Konfigurationsbefunde. Nichts davon ersetzt interne Vorfallbelege oder die eigene Meldeprüfung.

Bitten Sie um eine Brandefense-Demonstration anhand einer Berichtsfrage: Wie erreicht eine neue Behauptung die richtigen Verantwortlichen und erhält eine dokumentierte Einordnung? Produktumfang und Dienstvereinbarungen sollten im Gespräch bestätigt werden.

KERNAUSSAGEN

01

Geben Sie jeder Massnahme Verantwortung, Auslösebedingung und nachweisbare Abschlussbelege.

02

Üben Sie Dienstleister, Identitätswiederherstellung und Geschäftswiederanlauf gemeinsam.

03

Binden Sie Rechtsfristen und öffentliche Aussagen an ihre eigenen Auslöser und Fakten.

ANHÄNGE

Anhänge

A–D

DIESES KAPITEL BEANTWORTET

Wie lassen sich Belege einordnen und zur Quelle zurückverfolgen?

4

Anhänge zu Umfang, Belegen, Quellen und Begriffen

Anhang A. Umfang, Quellen und Vertrauensgrad 101

Anhang B. Belegregister 104

Anhang C. Quellen 106

Anhang D. Glossar 111

Anhang A. Umfang, Quellen und Vertrauensgrad

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

A.1 Zeitraum und Zeitstempelbedeutung

Der Berichtszeitraum ist 1. Januar–22. November 2026. Untergrundmaterial wird nach Beitragszeit datiert und nicht nach Entdeckung durch Lesende. Der jüngste Aktivitätsabschnitt umfasst 9.–22. November. Ein älterer Vorfall in einem neuen Beitrag bleibt älter, solange Belege kein neues Ereignis feststellen.

Daten und Quellenlektüre spiegeln die Verfügbarkeit bei der Erhebung. Der Stichtag lief während der Vorbereitung noch. Später an diesem Datum veröffentlichtes Material kann ein Update erfordern. Fehlende Beobachtung wird nicht als fehlende Aktivität gedeutet.

Passive Beobachtungen haben einen eigenen Erhebungszeitbezug. Sie belegen keine durchgehend gleiche Konfiguration im Berichtszeitraum. Auch Ransomware-Listungsdaten belegen kein Einbruchsdatum. Offizielle Meldungen können frühere Ereignisse beschreiben oder erste Schätzungen korrigieren.

Die Beitragszahlen umfassen Material mit Beitragsdatum bis 07:20 UTC am 22. November 2026. Der gewünschte Stichtag ist noch nicht abgeschlossen.

A.2 Quellengrundgesamtheiten

Der Bericht nutzt von Odin by Brandefense erhobene aufbewahrte Darkweb-Beiträge, öffentliche Ransomware-Listungen, passive DNS- und TLS-Beobachtungen, Beobachtungen zur Websicherheit und öffentliche Berichte. Jede Quelle liefert eine andere Belegart [S1][S2][S3].

Ein Beitrag erfasst Anzeige, Gesuch, Ankündigung oder Diskussion. Er belegt weder Datensatzechtheit noch aktuellen Kontozugriff oder Transaktionsabschluss. Wiederholte Angebote können dasselbe behauptete Material beschreiben. Angebotszeilen, Datensätze, Konten und Personen sind unterschiedliche Einheiten.

Eine Ransomware-Listung erfasst eine kriminelle Behauptung mit Organisation und Gruppenbezeichnung. Sie bestätigt weder Verschlüsselung noch Datenentfernung, Zahlung oder einzelnes Opfer unabhängig. Die behördlichen Ransomware-Fälle bilden eine getrennte Grundgesamtheit mit eigener Melde- und Beobachtungsbasis [S2] [S5].

Offizielle Berichte belegen die Offenlegung der genannten Organisation oder Behörde. Sie geben diesem Bericht keinen internen forensischen Zugang. Bei laut Quelle offenen Fragen bewahren Fallkarte und Kernaussage diese Unsicherheit.

A.3 Organisationsauswahl und fehlende Messgrössen

Die Auswahl umfasst 250 Organisationskandidaten in dreizehn Sektorzellen. Sie ist gezielt und enthält teils verwandte Unternehmen und öffentliche Stellen mit gemeinsamer übergeordneter Domain. Sie ist keine nationale Rangliste oder statistisch unabhängige Stichprobe [S3].

Passive Prüfungen umfassen 246 der 250 ausgewählten Kandidaten (ohne je einen Kandidaten in Banken und Finanzen, öffentlicher Verwaltung, Bildung und Forschung sowie Gesundheitswesen) und trennen uneindeutige Beobachtungen von Fehlern.

Expositionsbeobachtungen haben eine getrennte Abdeckung von 247 der 250 ausgewählten Kandidaten, ohne je einen Kandidaten in Energie und Versorgung, Transport und Logistik sowie Unternehmens- und Verbraucherdiensten. Die vier passiven Auslassungen und drei Expositionsauslassungen überschneiden sich nicht, sodass 243 Kandidaten in beiden Grundgesamtheiten erscheinen. Die nationale Atlas-Kennzahl beträgt 48 von 100 für das geprüfte Portfolio. Ausschliesslich die nationale Atlas-Zahl wird veröffentlicht. Geräte- und Zugangsdatenzuordnungen können sich über Organisationen und Daten überlappen. Sie zählen keine eindeutigen Personen oder bestätigten Vorfälle [S3].

A.4 Kartenumfang

Zahlungskartenbeobachtungen umfassen nur Klartextmaterial aufbewahrter Darkweb-Beiträge. Brandefense erkennt gestohlene Karten auch mit anderen Methoden ausserhalb dieses Abschnitts. Die Beobachtungen messen weder Kartendiebstahl noch aktive Karten, Betrugsverluste oder gesamte Brandefense-Abdeckung [S4].

Die Kartengrundgesamtheit darf nicht zu Zugangs-, Geräte- oder Personenzahlen addiert werden. Scheinbare Prüfergebnisse eines Verfassers bleiben Behauptungen. Jeder Kontoeingriff erfordert Prüfung im etablierten Herausgeberprozess.

A.5 Vertrauensgrad und alternative Erklärungen

Vertrauen bezieht sich auf eine Aussage. Der Bericht kann eine Anzeigenbeobachtung sicher feststellen, ohne Echtheit belegen zu können. Er kann eine Organisationsmeldung sicher feststellen, während endgültige Personenpopulation und Datenumfang ungeklärt bleiben.

Ein Akteursalias ist keine verifizierte Person. Gemeinsame Sprache, Hostingland, ähnlicher Titel oder politische Rhetorik belegen keine gemeinsame Kontrolle. Eine Beziehung wird nur auf belegtem Niveau beschrieben. Eine Planungsabfolge ohne festgestellte Betriebsverbindung wird als analytisches Modell bezeichnet.

Bedingte Szenarien in Kapitel 11 sind Planungsannahmen. Sie nennen stärkende und schwächende Belege. Sie sind weder bezifferte Angriffswahrscheinlichkeiten noch Zusagen zur Kontrollwirksamkeit.

A.6 Öffentliche Namensnennung und Neutralität

Organisationen werden in Vorfallsdarstellungen nur bei offizieller Bestätigung und breiterer Berichterstattung genannt. Andere Ziele und Dritte erhalten breite Rollenbezeichnungen. Würde ein Artikellink eines Drittmediums eine zurückgehaltene Organisation offenlegen, nutzt der öffentliche Eintrag die Websitewurzel des Verlags und hält die Artikel-URL zurück. Ist der Herausgeber selbst die zurückgehaltene Organisation oder Behörde, nennt der Eintrag die Herausgeberrolle ohne URL.

Der Bericht nimmt keine Position zu Regierungsentscheidungen, Bankgeheimnis, Sanktionen, EU-Beziehungen oder internationalen Treffen ein. Staats- und Akteurszuschreibungen bleiben diejenigen der Quellen. Akteursslogans und wertende Beschreibungen fehlen.

Anhang B. Belegregister

Das Register verweist auf Kapitelbelege. Karten-IDs bleiben in jeder Ausgabe gleich. Eine Karte belegt aufbewahrtes Material und nicht die Wahrheit seiner Behauptung.

Karte	Datum	Ort	Alias	Sprache	Kapitel
B01	2026-05-04	Datenteilungsforum	NormalLeVrai	Englisch	4
B02	2026-03-10	Forenantwort mit Angebotszitat	john2samira, quoting Niphra	Englisch	4
B03	2026-03-10	Forendiskussion	jb75	Englisch	4
B04	2026-11-05	Datenverkaufsforum	pfavre	Englisch	4
B05	2026-10-11	Datenteilungsforum	updap	Englisch	4
B06	2026-01-06	Kaufgesuch im Forum	xmrlover76	Englisch	4
B07	2026-01-27	Zugangsdatenforum	thejackal101	Englisch	4
B08	2026-11-07	Datenverkaufsforum	RummRif	Englisch	4
B09	2026-01-18	Datenteilungsforum	Cod3xx	Englisch	4
B10	2026-01-30	Datenteilungsforum	hexvior	Englisch	4
B11	2026-04-17	Kontokaufforum	kleinanzeige	Russisch und Englisch	4
B12	2026-11-19	Forenankündigung	Jlkrumholz01	Englisch	4

Das folgende Register führt offizielle Fallkarten getrennt von Untergrundbeitragskarten. Offizielle Offenlegungen und kriminelle Anzeigen dürfen nicht zu einer Vorfallszahl verbunden werden.

Karte	Datum	Thema	Belege	Kapitel
O01 / Fall F	2026-11-20	Kantonale Bewilligungsdaten	Offizielle Darstellung; Grenzen in Fallkarte	5
O02 / Fall G	2026-04-30	Radiologiekontinuität	Offizielle Darstellung; Grenzen in Fallkarte	5

Karte	Datum	Thema	Belege	Kapitel
O03 / Fall H	2026-10-23	Vorsorgesoftwareanbieter	Offizielle Darstellung; Grenzen in Fallkarte	5
O04 / Fall I	2026-09-28	Historische Medienpersonalangaben	Offizielle Darstellung; Grenzen in Fallkarte	5
O05 / Fall J	2026-07-15	Versorgerdaten beim Dienstleister	Offizielle Darstellung; Grenzen in Fallkarte	5
O06 / Fall K	2026-11-12	Kühlungssteuerungen	Offizielle Darstellung; Grenzen in Fallkarte	5
O07 / Fall L	2026-08-04	Zusammenarbeitskonten des Bundes	Offizielle Darstellung; Grenzen in Fallkarte	5
O08 / Fall M	2026-10-26	Bildungs-IT-Supportplattform	Offizielle Darstellung; Grenzen in Fallkarte	5
O09 / Fall N	2026-04-11	Datenumfang Erwachsenenbildung	Offizielle Darstellung; Grenzen in Fallkarte	5
O10 / Fall O	2026-11-19	Universitäre Onlineformulare	Offizielle Darstellung; Grenzen in Fallkarte	5
R01 / Fall P	2026-10-19	Kampagne über Updates einer Sicherungssoftware	Anbietererklärung und Primärforschung; Schweizer Betroffene ungenannt	7

Anhang C. Quellen

Quellennummern, die nicht erscheinen, wurden während der Überprüfung zurückgezogen und werden nicht zitiert. Externe Quellenseiten und die stützenden Passagen wurden während der Erstellung gelesen. Prüfdaten beschreiben diese Lektüre und garantieren nicht, dass eine Seite unverändert bleibt. Eigene Quelleneinträge benennen die in dieser Ausgabe verwendete Grundgesamtheit.

S1: Odin by Brandefense. Odin by Brandefense retained Switzerland-related post material, post window 1 January–22 November 2026 through 07:20 UTC. Own-source population. Verified on 22 November 2026.

S2: Brandefense. Ransompedia listing snapshot for Switzerland and regional peers, collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S3: Odin by Brandefense. Selected organisation universe, Atlas exposure observations read 21–22 November 2026, and passive DNS, TLS and web-security observations collected 22 November 2026. Own-source population. Verified on 22 November 2026.

S4: Brandefense. Clear-text payment-card aggregates from the retained post population. Own-source population. Verified on 22 November 2026.

S5: Federal Office for Cyber Security. First semi-annual cyber report 2026. https://www.bacs.admin.ch/en/hjb-26-1-en. Verified on 22 November 2026.

S6: Federal Office for Cyber Security. Reporting obligation for cyberattacks on critical infrastructure. https://www.bacs.admin.ch/en/reporting-obligation. Verified on 22 November 2026.

S7: FDPIC. Guidelines on reporting data security breaches and informing affected persons under Article 24 FADP. https://www.edoeb.admin.ch/dam/en/sd-web/T64CAUyvAMcF/1_2%20Leitfaden%20des%20ED%C3%96B%20betreffend%20der%20Meldung%20von%20Datensicherheitsverletzungen%20und%20Information%20der%20Betroffenen%20nach%20Art.%2024%20DSG_EN.pdf. Verified on 22 November 2026.

S8: FINMA. FINMA Guidance 03/2024: Cyber risks. https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/4dokumentation/finma-aufsichtsmitteilungen/20160707-finma-aufsichtsmitteilung-03-2024.pdf?sc_lang=en&hash=A1A633E2246BE27B2020897E1A389049. Verified on 22 November 2026.

S9: Federal Intelligence Service. Switzerland's Security 2026. https://www.vbs.admin.ch/dam/en/sd-web/tfhqKbM8ZL5k/VBS-DDPS-NDB-Sicherheit-Schweiz-2026-en.pdf. Verified on 22 November 2026.

S10: Swiss Confederation. First report on the Cyber Situation Network for the Summit on Peace in Ukraine. https://www.europa.eda.admin.ch/en/nsb?id=101528. Verified on 22 November 2026.

S11: Swiss Confederation. Federal Council plans to introduce new Cybersecurity Act. https://www.emek.admin.ch/en/newnsb/zX9oNK8tuI-Z. Verified on 22 November 2026.

S12: Federal Office for Cyber Security. FAQ on the reporting obligation. https://www.bacs.admin.ch/en/faq-reporting-obligation. Verified on 22 November 2026.

S13: Federal Office for Cyber Security. Woche 45: Black Friday wirft seine Schatten voraus – KI-Fakeshops und Paket-Phishing. https://www.bacs.admin.ch/de/26w45-de. Verified on 22 November 2026.

S14: Federal Office for Cyber Security. Woche 46: Personalisiertes Phishing aufgrund von abgeflossenen Daten. https://www.bacs.admin.ch/de/26w46-de. Verified on 22 November 2026.

S15: FDPIC. EDÖB leitete nach Cyberangriff auf Softwarelieferant Abklärungen ein. https://www.edoeb.admin.ch/de/edoeb-leitete-nach-cyberangriff-auf-softwarelieferant-abklaerungen-ein. Verified on 22 November 2026.

S16: Canton of Basel-Landschaft. FAQ-Data - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/direktionen/sicherheitsdirektion/amt_fuer_migration/bewilligungen/faq-data/. Verified on 22 November 2026.

S17: Canton of Basel-Landschaft. Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung führte zu Datenabfluss - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-fuehrte-zu-datenabfluss. Verified on 22 November 2026.

S18: Groupe 3R. Informations sur la cyberattaque d'avril 2026 - 3R - Réseau Radiologique Romand. https://www.groupe3r.ch/fr/informations-importantes/infos-cyberattaque-avril-2026-7268/. Verified on 22 November 2026.

S19: ICTjournal. Données volées, systèmes rétablis: le Groupe 3R fait le point après la cyberattaque (update) | ICTjournal. https://www.ictjournal.ch/news/2026-07-06/donnees-volees-systemes-retablis-le-groupe-3r-fait-le-point-apres-la-cyberattaque. Verified on 22 November 2026.

S20: SRG. SRG von Cybervorfall betroffen | SRG SSR. https://www.srgssr.ch/de/news-medien/news/srg-von-cybervorfall-betroffen. Verified on 22 November 2026.

S21: Publica. Cyber attack on Publica software supplier: data leak confirmed | PUBLICA. https://www.publica.ch/en/about-us/news/cyber-attack-publica-software-supplier-data-leak-confirmed. Verified on 22 November 2026.

S22: Netzwoche. Salt bestätigt Netzwerkausfall durch Cyberangriff | Netzwoche. https://www.netzwoche.ch/news/2026-05-18/salt-bestaetigt-netzwerkausfall-durch-cyberangriff. Verified on 22 November 2026.

S24: Federal Office for Cyber Security. Woche 5: Weltweite «SharePoint»-Phishing-Welle – auch die Schweiz ist betroffen. https://www.bacs.admin.ch/de/26w5-de. Verified on 22 November 2026.

S25: Federal Office for Cyber Security. Woche 6: «Subscription Bombing» – Wenn das E-Mail-Postfach unter Beschuss steht. https://www.bacs.admin.ch/de/26w6-de. Verified on 22 November 2026.

S26: Federal Office for Cyber Security. Woche 8: «ClickFix» – Wenn eine vermeintliche Fehlerbehebung oder Verifikation eine Malware installiert. https://www.bacs.admin.ch/de/26w8-de. Verified on 22 November 2026.

S27: Federal Office for Cyber Security. Woche 15: Falsche Bankmitarbeiter fordern Installation von Fernwartungssoftware. https://www.bacs.admin.ch/de/26w15-de. Verified on 22 November 2026.

S28: Federal Office for Cyber Security. Woche 18: Paket-Phishing mit perfider Fortsetzung – Die Masche des «Double Phishing». https://www.bacs.admin.ch/de/26w18-de. Verified on 22 November 2026.

S30: Federal Office for Cyber Security. Woche 23: Stellensuchende im Visier – Phishing, Betrug und Schadsoftware im Bewerbungsprozess. https://www.bacs.admin.ch/de/26w23-de. Verified on 22 November 2026.

S32: Federal Office for Cyber Security. Woche 35: Skimming bei Essenslieferdienst - Statt einem vollen Magen eine leere Kreditkarte. https://www.bacs.admin.ch/de/26w35-de. Verified on 22 November 2026.

S34: Federal Office for Cyber Security. Woche 42: Neue Variante von Phishing in Zusammenhang mit Hotelbuchungen zielt auf TWINT-Konten. https://www.bacs.admin.ch/de/26w42-de. Verified on 22 November 2026.

S40: IWB. Adressdaten bei Dienstleister von IWB entwendet (15 July 2026). https://www.iwb.ch/ueber-uns/newsroom/medienmitteilungen/artikel~_adressdaten-bei-dienstleister-von-iwb-entwendet~. Verified on 22 November 2026.

S41: Swiss police cybercrime portal. cybercrimepolice.ch | Cyberangriffe auf Kühlanlagen zeigen die.... https://cybercrimepolice.ch/de/faelle/cyberangriffe-auf-kuehlanlagen-zeigen-die-risiken-vernetzter-geraete. Verified on 22 November 2026.

S42: Federal Office for Cyber Security. Summit on Peace in Ukraine: first NCSC report on Cyber Situation Network. https://www.bacs.admin.ch/en/24-kfu-2-en. Verified on 22 November 2026.

S43: Official public source. Official incident or campaign account concerning a withheld organisation. https://cybercrimepolice.ch/ (article URL withheld). Verified on 22 November 2026.

S44: Swiss police cybercrime portal. cybercrimepolice.ch | Falsches Bankpersonal fordert Bargeld für.... https://cybercrimepolice.ch/de/faelle/falsches-bankpersonal-fordert-bargeld-fuer-angebliches-snb-sicherungskonto. Verified on 22 November 2026.

S45: Swiss police cybercrime portal. cybercrimepolice.ch | Betrügerische Investitionsanrufe nach.... https://cybercrimepolice.ch/de/faelle/betrugerische-investitionsanrufe-nach-datenabfluss-bei-pensionskassendienstleister. Verified on 22 November 2026.

S47: Canton of Basel-Landschaft. Update zum Cyberangriff auf die IT-Infrastruktur der kantonalen Verwaltung Basel-Landschaft - Kanton Basel-Landschaft. https://www.baselland.ch/politik-und-behorden/besondere-behoerden/landeskanzlei/medienmitteilungen/update-zum-cyberangriff-auf-die-it-infrastruktur-der-kantonalen-verwaltung-basel-landschaft. Verified on 22 November 2026.

S48: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S49: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S50: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S53: Federal Office for Cyber Security. Kühl- und Kältesteuerungen: Systeme identifizieren, aktualisieren und schützen. https://www.bacs.admin.ch/de/warnung-kuehlanlagen-de. Verified on 22 November 2026.

S54: Swiss Confederation. Cyberangriff auf SharePoint-Server. https://www.admin.ch/de/newnsb/1CjmpBBHQaMV82PjKEpcL. Verified on 22 November 2026.

S55: Swiss Confederation. Cyberangriff auf Softwarelieferanten: Publica lässt Umgang mit Personendaten und Sicherheitskontrollen extern untersuchen. https://www.admin.ch/de/newnsb/A40p0VPerHSv. Verified on 22 November 2026.

S56: IT-Markt. Public reporting on an incident concerning a withheld organisation. https://www.it-markt.ch/ (article URL withheld). Verified on 22 November 2026.

S57: Netzwoche. Public reporting on an incident concerning a withheld organisation. https://www.netzwoche.ch/ (article URL withheld). Verified on 22 November 2026.

S58: Ifage. Information relative à un incident de sécurité impliquant des données personnelles | ifage. https://www.ifage.ch/news/2026/information-relative-a-un-incident-de-securite-impliquant-des-donnees-personnelles/. Verified on 22 November 2026.

S59: Canton of Vaud. La plateforme de support informatique des Gymnases et des Ecoles professionnelles du Canton victime d'un vol de données | État de Vaud. https://www.vd.ch/actualites/communiques-de-presse-de-letat-de-vaud/detail/communique/la-plateforme-de-support-informatique-des-gymnases-et-des-ecoles-professionnelles-du-canton-victime-dun-vol-de-donnees. Verified on 22 November 2026.

S60: Swiss government / NCSC. Six-month reporting obligation for cyberattacks on critical infrastructures. https://www.admin.ch/en/newnsb/gezctyF6KYR7UkCjXBC5s. Verified on 22 November 2026.

S61: FINMA. How FINMA is getting to the bottom of cyber risks in the financial sector. https://www.finma.ch/en/finma-public/article-series,-c-,-finma-at-work/artikelserie/cyberrisiken/. Verified on 22 November 2026.

S62: BACS warning. Kritische Schwachstellen in PHP: Sicherheitsupdates sofort einspielen. https://www.bacs.admin.ch/de/warnung-php-de. Verified on 22 November 2026.

S63: NVD record. NVD CVE-2026-109618. https://nvd.nist.gov/vuln/detail/CVE-2026-109618. Verified on 22 November 2026.

S64: NVD record. NVD CVE-2026-109619. https://nvd.nist.gov/vuln/detail/CVE-2026-109619. Verified on 22 November 2026.

S65: PHP vendor advisory. PHP security advisory: RCE via OOM corruption. https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w. Verified on 22 November 2026.

S66: PHP vendor advisory. PHP security advisory: RCE via stale global state. https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp. Verified on 22 November 2026.

S67: PHP release announcement. PHP security releases of 21 October 2026. https://www.php.net/archive/2026.php#2026-10-21-5. Verified on 22 November 2026.

S70: MITRE ATT&CK. Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1566/. Verified on 22 November 2026.

S71: MITRE ATT&CK. Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1190/. Verified on 22 November 2026.

S72: MITRE ATT&CK. Valid Accounts, Technique T1078 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1078/. Verified on 22 November 2026.

S73: Brandefense. Request a Demo | See AI-Driven Threat Intelligence in Action. https://brandefense.io/request-a-demo/. Verified on 22 November 2026.

S80: Università della Svizzera italiana. Incidente di sicurezza informatica – Informazioni e aggiornamenti | USI. https://www.usi.ch/it/data-breach. Verified on 22 November 2026.

S81: Withheld residential care provider. Public incident notices on the July 2026 ransomware disruption and October 2026 recovery update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S82: FDPIC. Warnung vor betrügerischen E-Mails im Namen des EDÖB. https://www.edoeb.admin.ch/de/warnung-vor-betruegerischen-e-mails-im-namen-des-edoeb. Verified on 22 November 2026.

S83: Withheld Swiss public authority. Public notice on temporary service restrictions during October 2026 PHP vulnerability remediation. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S84: Canton of Vaud. Revue des cybermenaces : Juillet 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26508-revue-des-cybermenaces-juillet-2026. Verified on 22 November 2026.

S85: Canton of Vaud. Revue des cybermenaces : Septembre 2026 | État de Vaud. https://www.vd.ch/actualites/actualite/news/26702-revue-des-cybermenaces-septembre-2026. Verified on 22 November 2026.

S86: Withheld Swiss municipal administration. Public notice of 14 March 2026 on partial encryption and service restoration. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S87: Withheld Swiss sports federation. Public notice of 31 October 2026 on a personal-data incident affecting a licensing platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S88: Withheld Swiss sports federation. Public notice of 26 October 2026 on unauthorised account access affecting an administration platform. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S89: Report URI. Vendor research on an incident concerning a withheld organisation. https://blog.report-uri.com/ (article URL withheld). Verified on 22 November 2026.

S90: Withheld cantonal authority. Public notice of 5 August 2026 on a SharePoint incident and precautionary website update. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S91: Withheld cantonal authorities. Joint public notice of 28 August 2026 on automated collection of public vehicle-holder information across five cantons. Source URL withheld to protect the organisation. Verified on 22 November 2026.

S92: Canton of Vaud. Vaud false-bank and false-police fraud update. https://www.vd.ch/actualites/actualite/news/25944-escroquerie-aux-faux-banquiers-policiers-le-nombre-de-cas-repart-a-la-hausse. Verified on 22 November 2026.

S93: Official or public reporting. St.Gallen remote-access fraud warning. https://www.sg.ch/news/sgch_kantonspolizei/2026/02/kanton-st-gallen--betrugsmasche-richtet-grossen-schaden-an.html. Verified on 22 November 2026.

S94: Official or public reporting. Ticino attempted family-emergency fraud. https://www4.ti.ch/di/pol-new/comunicazioni/comunicati-stampa-1/dettaglio/?user_polizia_pi1%5BnewsId%5D=259127. Verified on 22 November 2026.

S95: Official or public reporting. Bern remote-access fraud warning. https://www.police.be.ch/de/start/themen/news/medienmitteilungen.html?newsID=5cd77d2d-9a47-459f-b91d-60e5b6d54a5b. Verified on 22 November 2026.

S96: Official or public reporting. Schaffhausen suspected courier recruitment. https://www.shpol.ch/CMS/Webseite/Schaffhauser-Polizei-23813465-DE.html. Verified on 22 November 2026.

S97: Official or public reporting. Fribourg false-bank messages and card collection. https://www.fr.ch/dsjs/pol/actualites/escroqueries-aux-faux-banquiers-trois-auteurs-presumes-mis-en-cause. Verified on 22 November 2026.

S98: Official or public reporting. Neuchatel false-police and false-bank prevention. https://www.ne.ch/communiques-de-presse/escroquerie-au-faux-policier-et-faux-banquier-la-police-neuchateloise-la-rencontre-de-la-population-du-2-au-7-novembre-2026. Verified on 22 November 2026.

S99: Official or public reporting. Valais false-police and false-bank fraud. https://www.policevalais.ch/communiques-pour-les-medias/arnaque-aux-faux-policiers-pres-de-deux-tiers-des-escroqueries-dejouees/. Verified on 22 November 2026.

S100: Official or public reporting. Zug two courier investigations. https://zg.ch/de/zuger-polizei-news/2026/November/137-kanton-zug-telefonbetrug-zwei-geldkuriere-festgenommen. Verified on 22 November 2026.

S101: Threema. DDoS Attacks on Threema. https://threema.com/en/blog/outage-august-2026. Verified on 22 November 2026.

S102: SC Media. Encrypted messaging provider Threema hit by large-scale DDoS attacks. https://www.scworld.com/brief/encrypted-messaging-provider-threema-hit-by-large-scale-ddos-attacks. Verified on 22 November 2026.

S103: Google Threat Intelligence Group and Mandiant. Investigating Ephemeral Supply Chain Tampering. https://cloud.google.com/blog/topics/threat-intelligence/investigating-ephemeral-supply-chain-tampering. Verified on 22 November 2026.

S105: AOMEI. Statement on Ephemeral Tampering with the AOMEI Backupper Update Server. https://www.aomeitech.com/company/investigating-ephemeral-tampering.html. Verified on 22 November 2026.

S106: FDPIC. Tasks: data protection. https://www.edoeb.admin.ch/en/tasks-data-protection. Verified on 22 November 2026.

S107: Federal Office for Cyber Security. Semi-Annual Report 2025/2 (30 March 2026). https://www.bacs.admin.ch/en/hjb-25-2-en. Verified on 23 November 2026.

S108: Federal Office for Cyber Security. Semi-Annual Report 2025/1 (18 November 2025). https://www.bacs.admin.ch/en/hjb-25-1-en. Verified on 23 November 2026.

S109: FINMA. FINMA Risk Monitor 2025 (17 November 2025). https://www.finma.ch/en/~/media/finma/dokumente/dokumentencenter/myfinma/finma-publikationen/risikomonitor/20251117-finma-risikomonitor-2025.pdf?hash=6CB0C57B5333208BA29F26542B3B76B8&sc_lang=en. Verified on 23 November 2026.

S110: Swiss Confederation. «Sicherheit Schweiz 2026»: Keine Entwarnung für die Schweiz (25 June 2026). https://www.wbf.admin.ch/de/newnsb/jyRmuld1hBVy. Verified on 23 November 2026.

Anhang D. Glossar

- **BACS / NCSC:** Bundesamt für Cybersicherheit. BACS ist die deutsche Abkürzung; englisches Material verwendet NCSC [S6].
- **FDPIC / EDÖB:** Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter. Die Kürzel bezeichnen dieselbe Bundesbehörde auf Englisch und Deutsch [S7].
- **FINMA:** Eidgenössische Finanzmarktaufsicht mit getrennten Cybermeldeanforderungen für die von ihren Hinweisen erfassten Institute [S8].
- **FADP / DSG:** Datenschutzgesetz, dessen Pflichten bei Datensicherheitsverletzungen von den gesetzlichen Voraussetzungen abhängen [S7].
- **ISA / ISG:** Informationssicherheitsgesetz als Grundlage der hier besprochenen Cybermeldepflicht kritischer Infrastrukturen [S6].
- **CySA:** Geplantes Cybersicherheitsgesetz aus dem Gesetzgebungsauftrag des Bundesrats 2026. Es wird hier nicht als geltendes Recht behandelt [S11].
- **MFA:** Mehrfaktor-Authentisierung. Eine Anmeldung verlangt mehr als eine Nachweisart.
- **Phishing-resistente Authentisierung:** An den vorgesehenen Dienst gebundene Authentisierung. Sie mindert den Nutzen nachgeahmter Anmeldeseiten.
- **DDoS:** Verteilter Denial of Service. Datenverkehr soll legitime Nutzende am Dienstzugriff hindern.
- **DMARC:** E-Mail-Authentisierungsrichtlinie zur Behandlung von Nachrichten, welche relevante Ausrichtungsprüfungen nicht bestehen.
- **SPF / DKIM:** E-Mail-Authentisierungsmechanismen für berechtigten Versand und kryptografische Nachrichtensignatur.
- **DNSSEC:** Signaturen, mit denen validierende Resolver die Echtheit von DNS-Informationen prüfen können.
- **TLS:** Transportverschlüsselung etwa für HTTPS. Eine Zertifikatsprüfung prüft nicht die Anwendung.
- **HSTS:** Websiterichtlinie, die unterstützende Browser zu HTTPS für den angegebenen Host anweist.
- **Zugangsdaten-Datensatz:** Erfasstes kontobezogenes Element. Es kann historisch sein und belegt kein aktuell nutzbares Passwort.
- **Gerätezuordnung:** Verbindung zwischen gerätebezogenem Datensatz und Dienst. Sie belegt weder Eigentum noch aktuelle Infektion unabhängig.
- **Erstzugangsangebot:** Anzeige mit behauptetem Weg in eine Organisationsumgebung, der geprüft werden muss.
- **Stealer:** Schadsoftware zur Sammlung von Zugangsdaten, Sitzungsmaterial oder anderen Geräteinformationen.
- **Ransomware-Listung:** Öffentliche Erpressungsbehauptung mit Gruppenbezeichnung und Organisation.
- **Beitragskarte:** Bereinigte Wiedergabe aufbewahrten Untergrundmaterials mit Datum und ausdrücklichen Beleggrenzen.

- **Dienstleistervorfall:** Vorfall bei einem Anbieter, dessen Informationen oder Dienste eine andere Organisation unterstützen können.
- **Datensatz und Person:** Ein Datensatz ist ein Eintrag. Eine Person kann in mehreren Einträgen erscheinen.
- **TLP:CLEAR:** Weitergabekennzeichnung für uneingeschränkte Verteilung unter Vorbehalt anderer geltender Pflichten.

Über diesen Bericht

Erstellt von Odin by Brandefense für die Reihe Brandefense Country Report. Englischer Master sowie deutsche und französische Ausgabe teilen Quellen-IDs, Karten-IDs, Abbildungen und Zahlenbefunde. Übersetzungen tragen einen sichtbaren KI-Hinweis. Bei Bedeutungsabweichungen gilt die englische Ausgabe.

Dieses Quellenpaket unterstützt Sicherheitsentscheidungen und spätere redaktionelle Prüfung. Es ist weder vollständige Erhebung Schweizer Vorfälle noch Zertifizierung einer Organisation. Empfehlungen beschreiben mögliche Abwehrarbeit. Sie behaupten nicht, dass eine benannte Organisation sie ausgeführt oder unterlassen hat.

© 2026 Brandefense. Alle Rechte vorbehalten.

ABOUT BRANDEFENSE

Attackers See You First. We make sure you do.

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

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

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

GARTNER PEER INSIGHTS
4.7 / 5

COVERAGE
3 pillars
CTI, DRPS, EASM

MONITORING
24 / 7
Open, deep and dark web

REQUEST A DEMO

Request A Demo. See what attackers see.

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

Request a demo →

AWARDS

Recognised Around The World. Technology and trust.

Selected awards recognising Brandefense technology and innovation.



Top InfoSec Innovator

2026



Deloitte Technology Fast 500 EMEA

2024



Global InfoSec Awards

2025



Cybersecurity Excellence Awards

2025

See Brandefense In Action.

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

Request a demo →

BRANDEFENSE

See what attackers see. Before they act.

UNITED STATES

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

TÜRKIYE

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

BRANDEFENSE.IO