Opfer ohne Stimme

Der Cyberangriff auf die Xplain AG 2023 und die Wanderung der Verantwortung zum Bund

Othmar Baeriswyl

KMK-Fallstudie · Entwurf 2 vom 21. November 2026, bereinigt am 22. November 2026

Zusammenfassung

Im Mai 2023 wurde die Xplain AG, ein kleiner Softwareanbieter aus Interlaken für Polizei-, Justiz- und Migrationsbehörden, Opfer eines Ransomware-Angriffs. Die Täter veröffentlichten die erbeuteten Daten im Darknet, und darunter befanden sich auch operative Daten von Bundesstellen und Kantonen. Damit wurde aus der Krise eines Lieferanten eine Krise seiner Auftraggeber. Die Fallstudie fragt, ob die Schweizer Medien das Opfer des Angriffs als mitschuldig rahmen, an wen sie die Verantwortung richten und welche Kommunikationsstrategie daraus für die Organisation folgt.

Grundlage ist das Analysesystem KMK, ein Framework, das sich auf Theorien der Krisenkommunikation (Situational Crisis Communication Theory, Image-Repair-Theorie) und auf Erkenntnisse zur Wirkung von Botschaften stützt; sein Kern ist eine Framing-Analyse, die deskriptive, normative und emotionale Frame-Elemente getrennt erfasst. Untersucht wurden 74 Ursprungsbeiträge aus allen drei Sprachregionen der Schweiz (23.05.–30.06.2023). Die Analyse wurde zu einem simulierten Zeitpunkt am Ende dieses Fensters erstellt, ohne Zugriff auf eine bestehende Fallstudie zum selben Fall, die erst danach zum Vergleich geöffnet wurde.

Bis Ende Juni 2023 wird Xplain in keinem codierten Beitrag ein Schuldurteil zugewiesen. Rund 70 % der Beiträge setzen keine eigene Rahmung; wo sie es tun, erscheint die Firma fast ausnahmslos als Opfer. Das normative Urteil trifft die Bundesstellen, die die Daten beim Lieferanten liessen, und die einzige ausgedrückte Emotion ist Besorgnis. Zugleich verliert Xplain rasch die eigene Stimme: Die Deutung übernimmt der Bund. Das System leitet daraus eine zurückhaltende Strategie der kooperativen Aufklärung ab, die ausdrücklich reversibel geführt wird, weil eine Prüfung der Sicherheitsvorgaben bei Xplain angekündigt war.

Der Verlauf bis Ende 2024, erhoben aus Trefferzahlen und Titeln, stützt die Kernaussage, dass die Verantwortung zu den Auftraggebern wandert: Die Untersuchungsberichte vom Mai 2024 sahen den Bund als mitverantwortlich. Die geringe Zuschreibung an Xplain hielt dagegen nur für die Frühphase. Schon am letzten Tag des Untersuchungsfensters schrieb ein Leitmedium der Firma ein Versäumnis zu, und die Untersuchungsberichte belasteten auch sie. Der Bund hielt an der Firma fest, ein Kanton kündigte im Februar 2024. Weil das Sprachmodell den späteren Verlauf kennen konnte, der Verlauf nicht codiert ist und zwei Leitmedienbeiträge im Korpus fehlen, sind die Befunde als orientierend zu lesen.

Résumé

© 2026 mediata sa, Villars-sur-Glâne

En mai 2023, Xplain AG, petit éditeur de logiciels d'Interlaken travaillant pour des autorités de police, de justice et de migration, a été victime d'une attaque par rançongiciel. Les auteurs ont publié les données dérobées sur le darknet, parmi lesquelles figuraient aussi des données opérationnelles d'offices fédéraux et de cantons. La crise d'un fournisseur est ainsi devenue celle de ses mandants. L'étude de cas examine si les médias suisses présentent la victime de l'attaque comme coresponsable, à qui ils attribuent la responsabilité et quelle stratégie de communication en découle pour l'organisation.

L'analyse repose sur le système KMK, un cadre qui s'appuie sur des théories de la communication de crise (Situational Crisis Communication Theory, théorie de la réparation d'image) et sur des acquis relatifs à l'effet des messages ; son noyau est une analyse de cadrage qui saisit séparément les éléments descriptifs, normatifs et émotionnels. Le corpus comprend 74 articles originaux issus des trois régions linguistiques de Suisse (23.05–30.06.2023). L'analyse a été conduite à une date simulée en fin de période, sans accès à une étude de cas existante sur la même affaire, ouverte seulement ensuite à des fins de comparaison.

Jusqu'à fin juin 2023, aucun article codé n'attribue de faute à Xplain. Environ 70 % des articles ne proposent pas de cadrage propre ; lorsqu'ils le font, l'entreprise apparaît presque toujours comme victime. Le jugement normatif vise les offices fédéraux qui avaient laissé les données chez le fournisseur, et la seule émotion exprimée est l'inquiétude. En même temps, Xplain perd rapidement la parole : l'interprétation passe à la Confédération. Le système en déduit une stratégie réservée de clarification coopérative, conduite de manière explicitement réversible, puisqu'un examen du respect des prescriptions de sécurité par Xplain avait été annoncé.

L'évolution jusqu'à fin 2024, relevée à partir du nombre de résultats et des titres, confirme le constat central : la responsabilité se déplace vers les mandants ; les rapports d'enquête de mai 2024 ont jugé la Confédération coresponsable. La faible attribution à Xplain ne s'est en revanche vérifiée que pour la phase initiale. Dès le dernier jour de la période étudiée, un média de référence reprochait une négligence à l'entreprise, et les rapports d'enquête l'ont également mise en cause. La Confédération a maintenu sa collaboration avec l'entreprise, tandis qu'un canton a résilié son contrat en février 2024. Le modèle de langage pouvant connaître la suite des événements, l'évolution n'étant pas codée et deux articles de médias de référence manquant au corpus, les résultats ont une valeur indicative.

Riassunto

Nel maggio 2023 Xplain AG, piccola azienda di software di Interlaken attiva per autorità di polizia, giustizia e migrazione, è stata vittima di un attacco ransomware. Gli autori hanno pubblicato nel darknet i dati sottratti, tra cui anche dati operativi di uffici federali e cantoni. La crisi di un fornitore è così diventata la crisi dei suoi committenti. Lo studio di caso indaga se i media svizzeri presentino la vittima dell'attacco come corresponsabile, a chi attribuiscano la responsabilità e quale strategia di comunicazione ne derivi per l'organizzazione.

L'analisi si basa sul sistema KMK, un framework che si fonda su teorie della comunicazione di crisi (Situational Crisis Communication Theory, teoria della riparazione dell'immagine) e su conoscenze relative all'effetto dei messaggi; il suo nucleo è un'analisi del framing che rileva separatamente gli elementi descrittivi, normativi ed emotivi. Il corpus comprende 74 contributi originali delle tre regioni linguistiche svizzere (23.05–30.06.2023). L'analisi è stata svolta a una data simulata alla fine del periodo, senza accesso a uno studio di caso esistente sulla stessa vicenda, aperto solo in seguito per il confronto.

Fino alla fine di giugno 2023 nessun contributo codificato attribuisce una colpa a Xplain. Circa il 70 % dei contributi non propone un proprio inquadramento; quando lo fa, l'azienda appare quasi sempre come vittima. Il giudizio normativo colpisce gli uffici federali che avevano lasciato i dati presso il fornitore, e l'unica emozione espressa è la preoccupazione. Al tempo stesso Xplain perde rapidamente la parola: l'interpretazione passa alla Confederazione. Il sistema ne ricava una strategia riservata di chiarimento cooperativo, condotta in modo esplicitamente reversibile, poiché era stata annunciata una verifica del rispetto delle prescrizioni di sicurezza da parte di Xplain.

L’evoluzione fino alla fine del 2024, rilevata dal numero di risultati e dai titoli, conferma il risultato centrale: la responsabilità si sposta verso i committenti; i rapporti d’inchiesta del maggio 2024 hanno ritenuto corresponsabile la Confederazione. La debole attribuzione a Xplain ha invece retto solo nella fase iniziale. Già l’ultimo giorno del periodo esaminato un media di riferimento rimproverava all’azienda una negligenza, e i rapporti d’inchiesta hanno chiamato in causa anche lei. La Confederazione ha mantenuto la collaborazione con l’azienda, mentre un cantone ha disdetto il contratto nel febbraio 2024. Poiché il modello linguistico poteva conoscere il seguito, l’evoluzione non è codificata e due articoli di media di riferimento mancano nel corpus, i risultati hanno valore orientativo.

Abstract

In May 2023, Xplain AG, a small software company in Interlaken serving police, justice and migration authorities, fell victim to a ransomware attack. The attackers published the stolen data on the darknet, including operational data belonging to federal offices and cantons. The crisis of a supplier thus became a crisis of its clients. This case study asks whether Swiss media frame the victim of the attack as complicit, to whom they attribute responsibility, and which communication strategy follows for the organisation.

The analysis draws on the KMK system, a framework grounded in theories of crisis communication (Situational Crisis Communication Theory, image repair theory) and in findings on how messages take effect; its core is a framing analysis that records descriptive, normative and emotional frame elements separately. The corpus comprises 74 original articles from all three Swiss language regions (23 May–30 June 2023). The analysis was carried out at a simulated date at the end of this window, without access to an existing case study of the same case, which was opened only afterwards for comparison.

Up to the end of June 2023, no coded article assigns blame to Xplain. Around 70 % of the articles set no framing of their own; where they do, the company appears almost without exception as a victim. The normative judgement falls on the federal offices that had left their data with the supplier, and the only emotion expressed is concern. At the same time, Xplain quickly loses its own voice: interpretation passes to the federal government. From this, the system derives a restrained strategy of cooperative clarification, explicitly designed to be reversible because a review of Xplain’s compliance with federal security requirements had been announced.

Events up to the end of 2024, traced through hit counts and headlines, support the core finding that responsibility migrates to the clients: the investigation reports of May 2024 held the federal government jointly responsible. The low attribution to Xplain, however, held only for the early phase. On the last day of the study window a leading newspaper already accused the company of negligence, and the investigation reports implicated it as well. The federal government stayed with the company, while one canton terminated its contract in February 2024. Because the language model may have known how events unfolded, the later course is not coded and two articles from leading media are missing from the corpus, the findings should be read as indicative.

Schlüsselwörter: Krisenkommunikation · Framing · Verantwortungszuschreibung · Cyberangriff · Lieferkette · Opferrolle · SCCT · Image Repair · Xplain

1 Problem- und Fragestellung

Ein Cyberangriff hat zunächst ein klares Opfer. Wer angegriffen wird, gilt in der Regel nicht als Verursacher, sondern als Geschädigter einer Straftat. Die Situational Crisis Communication Theory (SCCT) ordnet solche Ereignisse deshalb dem Opfercluster zu, in dem einer Organisation nur minimale Verantwortung zugeschrieben wird; als Antwort genügen Information und Anteilnahme, eine Verantwortungsübernahme ist nicht gefordert (Coombs, 2007). Diese Zuordnung setzt allerdings voraus, dass die Ursache

tatsächlich ausserhalb der Organisation liegt. Wird bekannt, dass eine Schwachstelle hätte geschlossen werden können, rückt dieselbe Krise in die Nähe der vermeidbaren Krisen, und die Zuschreibung steigt.

Bei einem Lieferanten kommt eine zweite Unsicherheit hinzu. Gehören die abgeflossenen Daten nicht der angegriffenen Firma, sondern ihren Kunden, so stellt sich die Frage nach der Verantwortung auch an diese: Warum lagen die Daten beim Lieferanten, und wer hätte dessen Sicherheit prüfen müssen? Sind die Kunden Behörden, die selbst öffentlich rechenschaftspflichtig sind, entsteht eine Krise mit mehreren Adressaten. Ob die Verantwortung dann beim Angreifer, beim Lieferanten oder beim Auftraggeber verortet wird, entscheidet darüber, welche Kommunikationsstrategie für das Opfer angemessen ist.

Der Angriff auf die Xplain AG im Mai 2023 zeigt diese Konstellation in exemplarischer Form. Ein wenig bekannter Anbieter von Behördensoftware wird von einer kriminellen Gruppe erpresst; die erbeuteten Daten erweisen sich in den folgenden Wochen als Daten des Bundesamts für Polizei, des Zolls und mehrerer Kantone. Ende Juni setzt die Landesregierung einen Krisenstab ein und kündigt zugleich an zu prüfen, ob die Firma die Sicherheitsvorgaben des Bundes eingehalten hat.

Im Zentrum steht deshalb die Frage, **ob das Opfer eines Cyberangriffs im Mediendiskurs als mitschuldig gerahmt wird und was daraus für seine Krisenkommunikation folgt.** Sie gliedert sich in vier Teilfragen:

1. **Ausgangslage:** Mit welcher Fallhöhe und welchen strukturellen Risiken tritt ein wenig bekannter Lieferant in die Krise?
2. **Framing:** Wie rahmen die Medien den Fall deskriptiv, normativ und emotional, und an wen richtet sich die Zuschreibung?
3. **Strategie:** Welche Kommunikationsstrategie leitet das System aus diesen Befunden ab?
4. **Bewährung:** Wie verhalten sich Prognose und Strategie zum Verlauf nach Ende Juni 2023?

Der Fall nimmt unter den KMK-Fallstudien eine besondere Stellung ein. Er wurde zu einem simulierten Zeitpunkt analysiert, während eine bestehende Fallstudie zum selben Fall bis zum Abschluss der Strategie verschlossen blieb (Abschnitt 3). Die Fallstudie dient der Lehre und der Prüfung des Analysesystems. Sie gibt die Befunde einer abgeschlossenen Analyse wieder und ist keine Beratung zur heutigen Lage der Organisation.

2 Fall und Chronologie

Die Xplain AG ist eine privat gehaltene Aktiengesellschaft mit Sitz in Interlaken, im Handelsregister seit 2000 (Moneyhouse, 2026). Sie entwickelt Software «für Behörden und Organisationen mit Sicherheits-, Migrations-, Arbeits- oder Wirtschafts-, Strafverfolgungs- und Strafvollzugsaufgaben» (zitiert nach Schurter, 2023a). Zu ihrer Kundschaft gehörten 2023 Stellen des Bundes, darunter das Bundesamt für Polizei (fedpol) und das Bundesamt für Zoll und Grenzsicherheit (BAZG), sowie kantonale Polizei-, Justiz- und Migrationsbehörden (Schurter, 2023b). Vor dem Angriff war die

Firma in der Öffentlichkeit kaum bekannt; ein Regionalradio stellte sie im Mai 2023 als «Interlakner Software-Unternehmen» vor (Radio BeO, 2023). Ihre Grösse ist für 2023 nicht genau belegt; die Analyse führte sie als kleines bis mittleres Unternehmen (KMK, 2026a).

Auf Seiten des Bundes treten mehrere Akteure auf. Das Nationale Zentrum für Cybersicherheit (NCSC) war 2023 die Fachstelle des Bundes für Cyberrisiken und dem Eidgenössischen Finanzdepartement (EFD) angegliedert, dem Finanzministerium. Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) ist die unabhängige Datenschutzaufsicht des Bundes. Die politische Verantwortung liegt beim Bundesrat, der siebenköpfigen Landesregierung. Tabelle 1 zeigt die Chronologie bis zum Ende des Untersuchungsfensters.

Tabelle 1: Chronologie bis zum Ende des Untersuchungsfensters. Quellen: KMK (2026a), Abschnitt 2.2; KMK (2026b), Blatt «Korpus»; KMK (2026c), Abschnitt 3; Inside IT (2023a, 2023b); NCSC (2023); 20 Minuten (2023); Kleinreport (2023).

Datum	Ereignis
23.05.2023	Erste Berichte: Xplain bestätigt einen Ransomware-Angriff der Gruppe «Play»; die Angreifer geben 907 GB erbeutete Daten an. Xplain erklärt, man speichere «keine Personen- und Fall-Daten aus Kundensystemen»
01.06.2023	«Play» veröffentlicht Daten im Darknet; Xplain lehnt Verhandlungen und Lösegeld ab, die Kantonspolizei Bern ermittelt
03.06.2023	Erste Meldungen, dass Daten von fedpol und Zoll betroffen sind
08.06.2023	NCSC und EFD: Auch operative Daten der Bundesverwaltung könnten betroffen sein
um den 14.06.2023	Im veröffentlichten Datensatz werden Personen- und Polizeidaten berichtet; auch der Kanton Aargau ist betroffen (Datum geschätzt)
21.06.2023	Der EDÖB eröffnet eine Untersuchung gegen fedpol und BAZG wegen möglicher Verstösse gegen den Datenschutz
28.06.2023	Der Bundesrat setzt den politisch-strategischen Krisenstab «Datenabfluss» ein und kündigt eine Prüfung an, ob Xplain die Sicherheitsvorgaben des Bundes mangelhaft umgesetzt hat
29.06.2023	Ankündigung einer Administrativuntersuchung; die Zusammenarbeit mit Xplain soll weitergeführt werden, weil die Systeme betreut werden müssen

Für die Kommunikation der Firma ist die erste Stellungnahme vom 23. Mai bedeutsam. Xplain gab an, den Angriff «sofort bemerkt» zu haben, und hielt fest, Personen- und Falldaten aus Kundensystemen würden nicht gespeichert (Schurter, 2023a). Zugleich räumte die Firma ein, trotz Notfallplan vom Aufwand der Kommunikation «überwältigt» worden zu sein (Inside IT, 2023a). Die Meldungen des Bundes ab dem 8. Juni standen zu dieser Zusage in einem Spannungsverhältnis, das die Berichterstattung über die folgenden Wochen begleitete. Der Verlauf nach dem 30. Juni folgt in Abschnitt 5.2.

© 2026 mediata sa, Villars-sur-Glâne

3 Methode und Datengrundlage

Die Analyse folgt dem KMK-System in der Fassung 2.0. Theoretische Grundlagen, Codiersysteme und Gütekriterien sind im wissenschaftlichen Projektbeschrieb dargestellt, Architektur und Verfahrensschritte der Module in der Technischen Systemdokumentation (Baeriswyl, 2026a, 2026b). Hier wird nur das festgehalten, was zum Verständnis der Befunde nötig ist.

Das System verbindet die Framing-Theorie (Entman, 1993), die Attributionstheorie in ihrer krisenkommunikativen Weiterentwicklung (Schwarz, 2008), die SCCT (Coombs, 2007) und die Image-Repair-Theorie (Benoit, 1997). Für den vorliegenden Fall ist der Ausgangspunkt der SCCT zentral: Sie unterscheidet Krisen, in denen die Organisation selbst Opfer ist, von Unfällen und von vermeidbaren Krisen, und knüpft an diese Zuordnung die Stärke der erwarteten Verantwortungszuschreibung (Coombs, 2007). Für die Rezeption stützt sich das System zusätzlich auf wahrnehmungspsychologische Ansätze. Nach der Theorie der kognitiven Dissonanz und der Forschung zur selektiven Wahrnehmung werden neue Informationen bevorzugt so aufgenommen, dass sie zu bestehenden Einstellungen und Erwartungen passen (Festinger & Möntmann, 2020; Schenk, 2007). Emotionen führt das System als eigene Dimension. Nach der attributionalen Emotionstheorie folgt Ärger auf die Wahrnehmung, dass ein Akteur einen Schaden hätte verhindern können (Weiner, 2006). Daraus lässt sich ableiten, dass Ärger ausbleibt, solange ein Schaden als von aussen verursacht gilt; die Emotion richtet sich dann eher auf die Bedrohung als auf einen Verantwortlichen.

Sein Kern ist eine regelgeleitete Inhaltsanalyse, die drei Dimensionen getrennt erfasst: **deskriptive** Frame-Elemente (Problemdefinition, Ursache, Krisentyp), **normative** Frame-Elemente (Verantwortung, Rollen, Forderungen) und **emotionale** Frame-Elemente (ausgedrückte Emotionen und ihre Intensität). Vier Module arbeiten nacheinander: ADAM erhebt den Kontext, SCHNUFFI recherchiert die Berichterstattung, FRAMI analysiert das Framing, und EVI leitet daraus eine Strategie ab. Für die Lesart der Befunde ist ein Ebenenmodell massgeblich. Der *Befund* beschreibt, was manifest im Text steht; die *Deutung* erschliesst, was der Text latent nahelegt; die *Prognose* schliesst, wie Anspruchsgruppen voraussichtlich reagieren. Die Prognose ist eine theoriegeleitete Inferenz und wird mit Regel, Evidenzgrad, Konfidenz und Falsifikator geführt (Baeriswyl, 2026a).

Analyse zu einem simulierten Zeitpunkt. Der Fall wurde im September 2026 als Systemtest analysiert, jedoch so, als stünde man am 30. Juni 2023. Der Stichtag schliesst die Ausweitung vom Vorfall bei einem Lieferanten bis zum Krisenstab der Landesregierung ein, liegt aber vor späteren Untersuchungsergebnissen (KMK, 2026a). Als Vergleichsmassstab diente eine bereits publizierte Fallstudie zum selben Fall, die ein längeres Zeitfenster bis November 2023 untersucht (Dalic et al., 2025). Sie blieb gesperrt, bis die Strategie vorlag, und wurde erst danach geöffnet (KMK, 2026e). Blind war die Analyse damit gegenüber dieser Vergleichsstudie, nicht aber gegenüber dem Wissen des Sprachmodells: Der Stichtag liegt lange vor dessen Trainingsstand, und es ist anzunehmen, dass das Modell den späteren Verlauf kannte. Die Analyse hat dies in einem Kontaminationsprotokoll festgehalten. Inhalte nach dem Stichtag, die bei der Recherche sichtbar wurden, sind dort verzeichnet und gingen nicht in die Codierung ein (KMK, 2026a, 2026b). Ein unbemerkter Einfluss auf Codierentscheide lässt sich

© 2026 mediata sa, Villars-sur-Glâne

gleichwohl nicht ausschliessen. Übereinstimmungen mit dem späteren Verlauf sind deshalb vorsichtiger zu werten als Abweichungen.

Korpus. Erhoben wurde die Berichterstattung vom 23. Mai bis 30. Juni 2023 in Deutsch, Französisch und Italienisch, mit einem Vorlauf ab dem 15. Mai. Die Recherche in fünf Strängen ergab 74 Ursprungsbeiträge; 65 davon waren abrufbar und codierbar, neun scheiterten an einer Bezahlschranke oder an gesperrten Seiten (KMK, 2026b). Befundbasis sind 56 codierbare Beiträge aus Presse, öffentlich-rechtlichen Sendern, Boulevard- und Online-Medien; Beiträge in sozialen Medien und Kommentarspalten dienten nur der Beobachtung der Publikumsreaktion. 32 Beiträge wurden zusätzlich auf der Deutungsebene codiert (Tabelle 2).

Tabelle 2: Korpus. Quelle: KMK (2026b), Blatt «Korpusbefund»; KMK (2026c), Abschnitt 2.3.

Merkmal	Verteilung
Ursprungsbeiträge	74; codierbar 65; Befundbasis 56
Sprache (alle 74)	Deutsch 56 · Französisch 10 · Italienisch 8
Medientyp (alle 74)	Qualitätspresse und öffentlich-rechtliche Sender 23 · Boulevard 13 · Online- und Fachmedien 24 · soziale Medien 14 (nur Beobachtung)
Zeitlicher Verlauf	22.–28.05.: 3 · 29.05.–04.06.: 8 · 05.–11.06.: 19 · 12.–18.06.: 17 · 19.–25.06.: 12 · 26.–30.06.: 13 · ohne exaktes Datum: 2
Codiertiefe	Befundebene 56 · Deutungsebene 32

Codiert hat ein Sprachmodell (claude-opus-5, Anthropic) in sechs Durchgängen mit identischem Auftrag; eine zweite, unabhängige Codierinstanz fehlt. Die Werte sind deshalb orientierend. Die Volltexte kamen über ein Abrufwerkzeug, das Seiten über ein Zwischenmodell wiedergibt; eine Stichprobe von vier Zitaten bestätigte den Wortlaut am Original (KMK, 2026b, 2026c).

4 Befunde

4.1 Ausgangslage: Fallhöhe, Attributionsverstärker und Risikofallen

Die *Reputations-Fallhöhe* bezeichnet im KMK-System, wie schwer eine Verantwortungszuschreibung für eine Organisation wiegt. Sie setzt sich aus neun Faktoren zusammen, darunter Branche, Marktstellung, Transparenzerwartung und Bekanntheit, und reicht von −8 bis +14. Für Xplain ergibt sich ein Wert von +1 (Tabelle 3). Acht der neun Faktoren beruhen ganz oder teilweise auf Schätzungen, weil über die Firma vor dem Angriff wenig publiziert war. Werden die geschätzten Faktoren innerhalb des Vertretbaren nach oben verschoben, erreicht der Wert +5 und damit das hohe Band. Die Fallhöhe ist deshalb als Spanne «mittel bis hoch» zu lesen (KMK, 2026f).

Tabelle 3: Kontextkennwerte. Quellen: KMK (2026a), Abschnitte 5, 7 und 8; KMK (2026f).

Grösse	Wert	Lesart
Reputations-Fallhöhe	+1 (Spanne mittel bis hoch; Grenzfall +5)	Behördensoftware mit sensiblen Daten, strenge Sicherheitsauflagen; zugleich geringe Bekanntheit und keine belegten Vorfälle
Krisenhistorie	0 (geschätzt)	kein ähnlicher Vorfall in den 24 Monaten vor dem Angriff belegt
Vorreputation	1 (geschätzt)	neutral; keine belegte Vorbewertung
Attributionsverstärker	1	allein aus neutraler Vorreputation; löst keine Verstärkung aus
Risikofallen	3 von 5 angelegt	Heuchelei, Kompetenz, Allianz; Krisenhistorie und Machtgefälle nicht angelegt

Bemerkenswert ist, woraus die Fallhöhe entsteht. Sie kommt nicht aus der Firma selbst, die klein und kaum bekannt ist, sondern aus ihrer Stellung: Xplain verarbeitet sensible Daten im Auftrag mächtiger Kunden, die hohe Erwartungen an Sicherheit und Diskretion stellen. Die geringe Bekanntheit senkt den Wert; die Branche, die Sicherheitsauflagen und die Transparenzerwartung, die aus öffentlichen Aufträgen folgt, heben ihn (KMK, 2026a).

Die *Krisenhistorie* erfasst, ob eine Organisation früher ähnliche Krisen erlebt hat und wie schwer diese wogen; die *Vorreputation* beschreibt ihr Ansehen vor der Krise. Nach der SCCT verstärken eine belastete Krisengeschichte und eine schlechte Vorreputation die Verantwortung, die einer Organisation in einer neuen Krise zugeschrieben wird (Coombs, 2007). Das KMK-System fasst beide als *Attributionsverstärker* zusammen. Bei Xplain ist kein früherer Vorfall belegt, und die Vorreputation ist neutral. Der Nulltreffer ist allerdings ein schwacher Beleg: Bei einer Firma, über die vor dem Angriff kaum berichtet wurde, zeigt eine erfolglose Suche nur, dass nichts öffentlich wurde, nicht, dass nichts geschah (KMK, 2026a).

Die *Risikofallen* bezeichnen strukturelle Konstellationen, die bestimmte belastende Frames verfügbar machen. Angelegt sind drei von fünf. Die Heuchelei-Falle ergibt sich aus dem Gegensatz zwischen dem Versprechen, für Sicherheitsbehörden zu arbeiten, und dem Abfluss sensibler Behördendaten; verschärft wird sie durch die Zusage vom 23. Mai, keine Personen- und Falldaten aus Kundensystemen zu speichern. Die Kompetenzfalle folgt daraus, dass die Kernleistung, sichere Software für Sicherheitsbehörden, auf einen erfolgreichen Angriff trifft. Die Allianzfalle schliesslich ergibt sich aus der Nähe zur Informatik und IT-Beschaffung des Bundes, die durch frühere Fälle bereits belastet war (KMK, 2026a). Ob die Medien diese Fallen tatsächlich aktivieren, ist eine Frage an das Korpus.

© 2026 mediata sa, Villars-sur-Glâne

4.2 Framing: Opfer ohne Schuld, Verantwortung beim Bund

Deskriptives Framing. Die Berichterstattung stellt das Ereignis fast durchgehend als Tat Dritter mit Schaden bei Dritten dar. In 49 der 56 Beiträge wird die Ursache extern verortet, in sechs intern und extern zugleich. 44 Beiträge benennen die Angreifer als Verursacher. Die ausgenutzte Schwachstelle auf den Servern von Xplain wird in einzelnen Beiträgen erwähnt, aber nicht als Versäumnis gewertet (KMK, 2026c).

Für die Einordnung nach der SCCT unterscheidet das System zwei Perspektiven. Die *textnahe Einordnung* hält fest, welchen Krisentyp ein Beitrag selbst setzt; die *rekonstruierte Einordnung* erschliesst ihn aus dem Gesamtzusammenhang der Codierungen. Textnah setzen 39 der 56 Beiträge (69,6 %) keine eigene Rahmung; sie referieren Fakten und Behördenangaben. Von den 17 Beiträgen, die rahmen, stellen 16 die Firma als Opfer dar (94,1 %), einer als Unfall; keiner rahmt die Krise als vermeidbar. Typisch ist die Formel, Xplain sei «Opfer einer Ransomware-Attacke» geworden. Rekonstruiert ergibt sich ebenfalls ein deutliches Bild: 94,6 % der Beiträge fallen in den Opfercluster (KMK, 2026c).

Ein Zusatzbefund verschiebt den Blick. Erhebt man die Rahmung getrennt für die Bundesstellen, rahmen elf Beiträge (19,6 %) das Ereignis für den Bund als vermeidbar, gestützt vor allem auf die Aussage, die Daten hätten nicht bei der Firma sein dürfen. Alle elf liegen zwischen dem 21. und 29. Juni, also nach Eröffnung der Untersuchung durch den EDÖB (KMK, 2026c).

Normatives Framing. Hier liegt der Kernbefund der Studie. Kein codierter Beitrag spricht Xplain ein Schuldurteil zu. Ein Heuchelei-Vorwurf fehlt ebenso wie Kritik an der Kommunikation der Firma. Die Verantwortung wird stattdessen Dritten zugewiesen, und zwar in 14 Beiträgen (25,0 %) den Bundesbehörden, wegen ihrer Datenhaltung, des Datenschutzes und der Kontrolle ihrer Lieferanten; die Angreifer werden in fünf Beiträgen normativ verantwortlich gemacht. Auch der Vorwurf, mit zweierlei Mass zu messen, trifft nur den Bund: Vier Beiträge kritisieren die anfängliche Beschwichtigung, die Reaktionszeit oder fehlende Angaben der Bundesstellen. Als moralische Instanz tritt vor allem die Datenschutzaufsicht auf (EDÖB in sechs Beiträgen), daneben Medien und Politik. Die neun codierten Forderungen stammen alle aus Mitteilungen und Aussagen des Bundes; sie zielen auf Strukturen (Anforderungen im Beschaffungsprozess, Überprüfung der Verträge) und auf die technische Sicherheit der Dienstleister. Wiedergutmachung, Sanktionen oder personelle Konsequenzen werden nicht verlangt (KMK, 2026c).

Im codierten Korpus erscheint eine Mitschuld von Xplain nur als Frage, nie als Urteil; zu einem fehlenden Beitrag vom 30. Juni siehe Abschnitt 7. Ein Experte fragt am 3. Juni, weshalb die Kundenliste der Firma öffentlich einsehbar war; ein Journalist fragt am 29. Juni «nach der erheblichen Sicherheitslücke»; und der Bundesrat kündigt am 28. Juni an zu prüfen, «ob, wo und weshalb von Xplain die Sicherheitsvorgaben des Bundes mangelhaft umgesetzt worden sind» (KMK, 2026c, Abschnitt 3.2). Die Bundesstellen tragen dagegen die belastenden Rollen: mitschuldig in vier, schuldig und versagend in je einem Beitrag, als Kontrolleure in fünf.

Emotionales Framing. Die Berichterstattung bleibt emotional zurückhaltend. Codiert ist ausschliesslich Angst beziehungsweise Besorgnis, in sieben Beiträgen mit einer

© 2026 mediata sa, Villars-sur-Glâne

mittleren Intensität von 3,4 auf einer Fünferskala; Wut, Trauer und Sarkasmus fehlen. Die Besorgnis wird überwiegend vom Bund geäussert oder ihm zugeschrieben, etwa wenn die Vorsteherin des EFD die Lage als «beunruhigend» bezeichnet oder ein Beitrag festhält, in Bundesbern «schrillen die Alarmglocken» (KMK, 2026c). Das Profil passt zur attributionalen Emotionstheorie: Ärger setzt die Wahrnehmung voraus, dass jemand den Schaden hätte verhindern können (Weiner, 2006). Solange die Ursache bei Dritten liegt und die Folgen offen sind, bleibt die Emotion auf die Bedrohung gerichtet, nicht auf einen Schuldigen.

Frames und ihr Verlauf. Die Codierung ergibt sieben Frame-Familien (Tabelle 4). Leitframe ist die *Ausweitung und Bedrohung*: Die Betroffenheit und die Art der Daten erweitern sich schrittweise, die Ursache bleibt extern, die Folgen offen. Seine Dominanz ist mässig; er ist in 51,9 % der Beiträge mit Frame enthalten und macht 34,6 % aller Frames aus. Ein Skandalframe, der Vermeidbarkeit, Verantwortung der Organisation und Wut verbindet, fehlt vollständig (KMK, 2026c).

Tabelle 4: Frame-Familien. Quelle: KMK (2026c), Abschnitt 3.6.

Frame-Familie	Frames	Beiträge mit Frame (n = 54)
Ausweitung und Bedrohung (Leitframe)	28	28 (51,9 %)
Bewältigung und Schadensbegrenzung	20	16 (29,6 %)
Opfer Xplain, Täter «Play»	14	12 (22,2 %)
Verantwortung von Bund und Auftraggebern	11	10 (18,5 %)
Beschwichtigung durch Behörden	4	4 (7,4 %)
Kommunikationskritik an Behörden	2	2 (3,7 %)
Nebenstrang Datenschutz im Zoll	2	2 (3,7 %)

© 2026 mediata sa, Villars-sur-Glâne

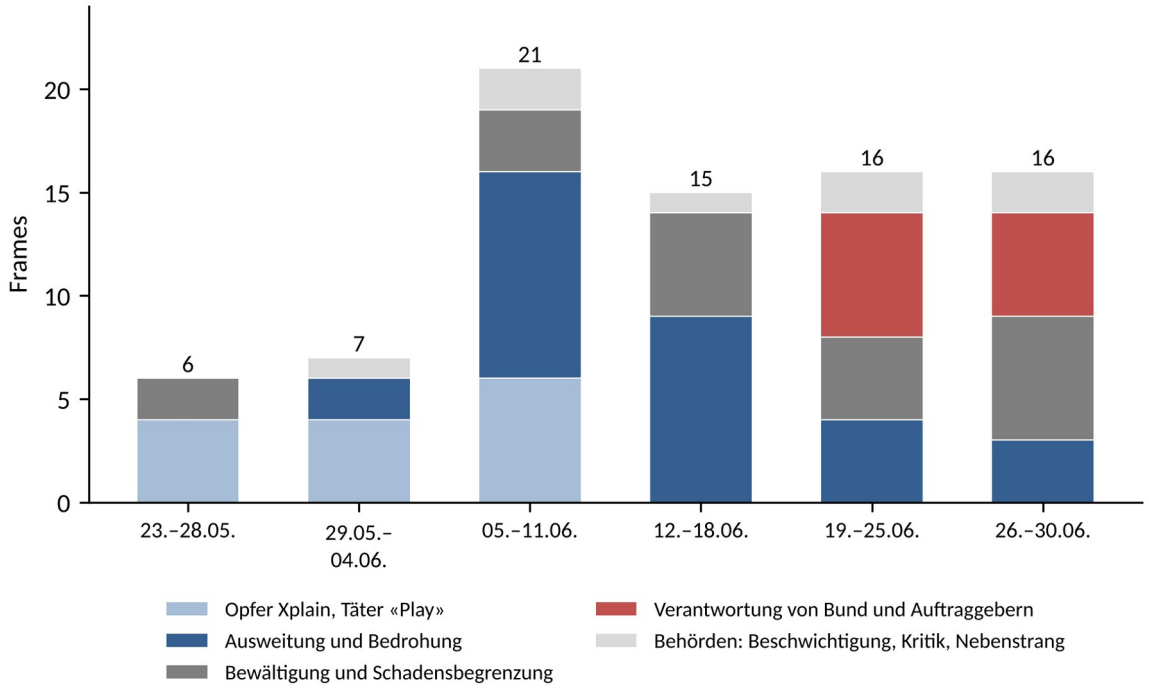


Abbildung 1: Frames je Kalenderwoche, 23. Mai bis 30. Juni 2023, nach Frame-Familien. Quelle: KMK (2026c), Abschnitt 3.5.

Abbildung 1 zeigt, wie sich die Frames über die sechs Wochen verschieben. In einer ersten *Opferphase* (Ende Mai bis Anfang Juni) dominiert die Erzählung vom angegriffenen Unternehmen und seinen Tätern, und Xplain spricht selbst. In der *Ausweitungsphase* (Mitte Juni) wächst die Zahl der Betroffenen, und die anfängliche Beschwichtigung der Bundesstellen wird revidiert. In der *Verantwortungsphase* (letzte zwei Juniwochen) treten die Datenhaltung der Bundesämter und die Kontrolle der Lieferanten in den Vordergrund; die Opferrahmung von Xplain verschwindet fast vollständig, weil die Beiträge die Firma kaum noch rahmen, nicht weil sie sie belasten (KMK, 2026c).

Deutungsebene. Auf der Ebene der latenten Bedeutung treten drei Muster hervor. Das erste ist die *Definitionsmacht beim Bund*: In der grossen Mehrheit der tiefer codierten Beiträge kommen ausschliesslich Stimmen des Bundes oder der Kunden zu Wort, oft im Verhältnis von drei bis zehn zu null. Xplain erscheint als Objekt, als «ditta terza» oder «private Firma», und spricht nur in 13 der 56 Beiträge selbst, fast ausschliesslich in der Frühphase. Das zweite Muster ist die *Ausblendung des Einfallstors*: Frühe Beiträge und die Berichte zur Untersuchung des EDÖB nennen die ausgenutzte Schwachstelle nicht und richten die Verantwortungsfrage an die Bundesämter; diese Auslassung wirkt für Xplain entlastend. Das dritte Muster, eine *latente Belastung der Lieferantenseite*, setzt in der letzten Juniwoche ein. Neue Schutzstandards für Lieferanten stehen unmittelbar neben der Nennung von Xplain, die Wortwahl verschärft sich («Affäre», «an die Kandare nehmen», «Xplain-Desaster», «Daten-Supergau»), und die Frage nach der Datenhaltung beim Anbieter wird gestellt, ohne dass dieser antwortet (KMK, 2026c, Abschnitt 3.4).

Abgleich mit den Risikofallen. Die erwarteten Signaturen der Heuchelei- und der Kompetenzfalle sind im Korpus nicht nachweisbar: Weder wird der Firma vorgeworfen,

ihre Werte zu verfehlen, noch wird ihre Kommunikation kritisiert. Die Allianzfalle wirkt in der Sache, aber in umgekehrter Richtung. Nicht der vorbelastete Partner belastet Xplain, sondern der Fall belastet den Partner (KMK, 2026c, Abschnitt 4.1). Diese Aussage gilt allerdings nur für den abrufbaren Korpus (Abschnitt 7).

4.3 Prognose

Aus den Befunden leitet das Rezeptionsregelwerk des Systems, eine Sammlung von Wenn-dann-Regeln mit ausgewiesener Konfidenz, Prognosen je Anspruchsgruppe ab. Die Regeln sind im Anhang mit ihren Kennungen zusammengestellt. Bestimmend ist die Regel zur ambigen Verantwortungslage (REZ-R10). Setzen mehr als 40 % der Beiträge keine eigene Rahmung, sinkt die Konfidenz jeder Prognose, und es ist mit einer *sprunghaften* Eskalation zu rechnen: ruhig bis zur Klärung der Faktenlage, danach abrupt. Mit 69,6 % nicht rahmender Beiträge ist die Bedingung deutlich erfüllt. Für die Öffentlichkeit ergibt sich daraus eine minimale Zuschreibung an Xplain, gestützt auf die Grundbeziehung zwischen Opfercluster und minimaler Verantwortung (Coombs, 2007), allerdings nur für die Teilmenge der rahmenden Beiträge und mit niedriger Konfidenz (KMK, 2026c).

Für die Auftraggeber in Bund und Kantonen sagt die Regel zum Opfer eines Dritten (REZ-R18) voraus, dass sie die Zusammenarbeit weiterführen, statt die Firma zu sanktionieren: Wer selbst demselben Risiko ausgesetzt ist, solidarisiert sich eher mit dem Opfer, als dass er es bestraft. Für die Aufsichts- und Strafverfolgungsinstanzen erwartet das System nach der Regel zur institutionellen Durchsetzung (REZ-R19) weitere Verfahrensschritte, unabhängig von der Erregung in den Medien. Für die Betroffenen, deren Daten abgeflossen sind, prognostiziert die Regel zu Angst und offener Gefährdung (REZ-R09) eine zunächst niedrige Zuschreibung, solange die Gefährdung anhält, mit einem Nachholeffekt danach; im Vordergrund steht die Suche nach Information. Diese Komponente ist die operativ wichtigste und zugleich am schwächsten belegte. Eine niedrige Zuschreibung während der Gefährdung ist deshalb keine Entwarnung (KMK, 2026c).

Wie im Fall der RUAG MRO ist auch hier eine Lücke hervorzuheben. Für Bundes- und Kantonsstellen als Auftraggeber trifft das Regelwerk keine Aussage zur Zuschreibung, weil seine Regeln für Behörden als Anspruchsgruppe nicht geprüft sind. Gerade diese Gruppen haben aber die grösste Macht über die Firma: Sie entscheiden über die Fortführung der Verträge. Das System benennt die Lücke, statt sie mit einer Plausibilitätsannahme zu füllen.

5 Strategie und Verlauf

5.1 Die abgeleitete Strategie

Das Strategiemodul EVI verbindet die prognostizierte Zuschreibung mit der Fallhöhe zu einer Alarmstufe. Bei minimaler Zuschreibung ergibt eine mittlere Fallhöhe die Stufe Grün, eine hohe die Stufe Gelb. Da die Fallhöhe als Spanne zwischen beiden Bändern liegt, lässt die Matrix beide Stufen zu. Gewählt wurde Gelb als Arbeitsstufe, und zwar nur aus Angaben, die zum Stichtag bekannt waren: Die Konfidenz der Prognose ist niedrig,

© 2026 mediata sa, Villars-sur-Glâne

für die wichtigsten Anspruchsgruppen liegt keine Zuschreibungsaussage vor, und die Eskalation ist als sprunghaft prognostiziert. Die Einstufung «minimal» stützt sich allein auf die Öffentlichkeit. Bei dieser Datenlage ist die höhere Stufe die vorsichtigere Lesart (KMK, 2026d, 2026f).

Daraus folgt eine Strategie auf der untersten Stufe der Verantwortungsübernahme, einer Basisreaktion im Sinne der SCCT (Coombs, 2007), mit drei Besonderheiten. Erstens gilt ein Basisprotokoll, das allen übrigen Regeln vorgeht: Instruktion vor Reputation, ein Rückfragekanal gleichzeitig mit jeder Information an Betroffene und die Mitarbeitenden zuerst. Bei Xplain stösst dieses Protokoll an eine Grenze, die für Lieferanten typisch ist. Die Firma ist nicht Datenherrin; Betroffene informieren und ihre Auskunftsbegehren bearbeiten können nur die Auftraggeber. Xplain kann deshalb nur zuliefern: vollständige Angaben zu den Datenkategorien an Auftraggeber und NCSC, damit diese rechtzeitig warnen können (KMK, 2026d, Abschnitt 2).

Zweitens empfiehlt das System, die Opferrolle nur flankierend zu nutzen. Die Primärlinie ist die *kooperative Aufklärung als Geschädigte*: überprüfbare Fakten, Mitwirkung an der unabhängigen Untersuchung, technische Massnahmen. Hinzu kommt ein *Betroffenen- und Auftraggeberdienst*. Der Verweis auf die Täter bleibt als Faktenaussage zulässig, wird aber nicht zur Hauptbotschaft. Ausgeschlossen sind eine Schuldverschiebung auf die Bundesstellen, die die wichtigsten Anspruchsgruppen träfe und die Allianzfalle aktivieren würde, ein Rückzug in die Kommunikation allein mit den Auftraggebern, der das Deutungsvakuum vergrössern würde, und die Wiederholung der Zusage vom 23. Mai. Diese soll nicht verteidigt, sondern durch die korrigierte Faktenlage ersetzt werden (KMK, 2026d, Abschnitte 8 und 9).

Drittens zielt die Empfehlung darauf, die verlorene Stimme zurückzugewinnen. Der Befund, dass Xplain nur in 13 von 56 Beiträgen selbst spricht, begründet ein Statement mit eigener Stimme innerhalb einer Woche, gesprochen von einer Sicherheitsfachperson, weil der Sachverhalt fachlich komplex ist. Die Reihenfolge der Botschaften folgt der einzigen ausgedrückten Emotion: Wo Angst vorherrscht, kommen Instruktion und Handlungsmöglichkeiten vor dem Image (KMK, 2026d, Abschnitt 9.3).

Die Strategie ist ausdrücklich als *reversibel* angelegt. Reversibel ist nicht ihre Richtung, denn ein späterer Rückweg zum Bestreiten wäre ausgeschlossen, sondern der Umfang der Verantwortungsübernahme. Den Grund benennt das Strategiemodul selbst: Es hielt die Lage für die Auftraggeber für instabiler, als die Prognose ausdrückt, weil der Bundesrat eine Prüfung der Sicherheitsvorgaben bei Xplain angekündigt hatte. Die Loyalität der Auftraggeber könne in Abwehr umschlagen, sobald diese selbst unter Verdacht geraten (KMK, 2026d, Abschnitt 5). Drei vorab festgelegte Wechselpunkte bestimmen deshalb, wann die Strategie eine Stufe höher geht (Tabelle 5).

Tabelle 5: Wechselpunkte der Strategie. Quelle: KMK (2026d), Abschnitt 9.2.

Wechselpunkt	Auslöser	Folgestrategie
Untersuchungsbe	Untersuchung oder Aufsicht stellen eine mangelhafte Umsetzung der Sicherheitsvorgaben durch Xplain fest	Wiederaufbau: Verantwortungsübernahme, Massnahmen mit Umsetzungsbeleg;

Wechselpunkt	Auslöser	Folgestrategie
fund		Selbstoffenlegung vor der Publikation
Medienentor	Die Folgeberichterstattung rahmt die Krise für Xplain zunehmend als vermeidbar	sofort eskalieren und Wechsel prüfen
Forderungsprofil	Forderungen verschieben sich auf Sanktionen oder personelle Konsequenzen	Strategie neu bewerten

Für den ersten Wechselpunkt sieht das System die Technik des *Stealing Thunder* vor. Arpan und Roskos-Ewoldsen (2005) zeigen experimentell, dass eine Organisation, die belastende Information selbst publik macht, als glaubwürdiger beurteilt wird als eine, über die Dritte berichten. Für Xplain hiesse das, einen festgestellten Mangel selbst offenzulegen, bevor der Untersuchungsbericht oder eine Recherche ihn bekannt macht.

5.2 Verlauf nach dem Stichtag

Der Verlauf nach dem 30. Juni 2023 wurde erst nach Abschluss der Strategie geöffnet. Er ist für die Zeit bis Ende 2024 aus einer Mediendatenbank erhoben, aus der Zahl der Treffer je Monat und aus den Titeln der Beiträge; drei Beiträge wurden gelesen (KMK, 2026g). Codiert wurde nichts. Die folgenden Aussagen beschreiben deshalb, wann und worüber berichtet wurde, nicht, wie die Beiträge rahmen. Ergänzend stützt sich der Abschnitt auf die Vergleichsstudie, die bis November 2023 reicht (Dalic et al., 2025).

Die Aufmerksamkeit verlief in Wellen (Abbildung 2). Im Juli 2023 blieb sie hoch, weil sich der Datenabfluss weiter ausweitete. Berichtet wurde über Angaben zum Schutz von Mitgliedern der Landesregierung und Botschaften, später über Auszüge aus einer Datenbank zu Gewalttätern im Sport, über Daten der Militärpolizei und über Unterlagen aus Strafverfahren (KMK, 2026b, Blatt «Nach Stichtag»). Von Oktober 2023 bis Januar 2024 wurde es ruhig. Neue Spitzen folgten im Februar 2024, als der Chef der Firma öffentlich Selbstkritik übte und der Bund an der Firma festhielt, und im Mai 2024 mit den Untersuchungsberichten. Im Oktober 2024 meldeten die Medien den Verkauf der Firma an eine ausländische Gruppe (KMK, 2026g).

© 2026 mediata sa, Villars-sur-Glâne

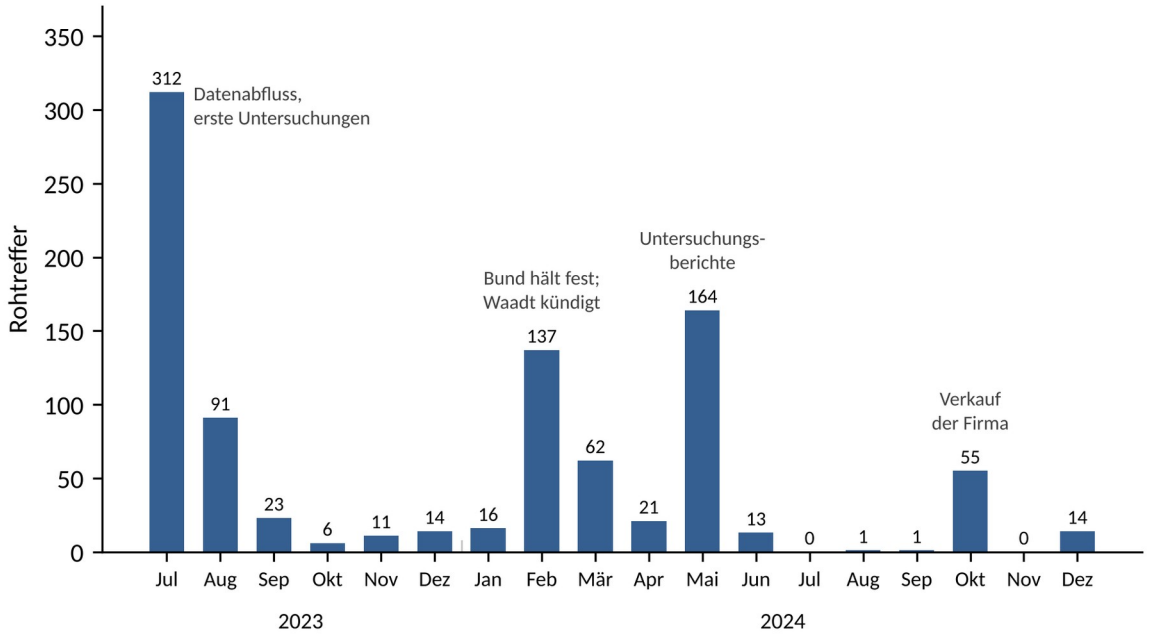


Abbildung 2: Treffer zu «Xplain» je Monat, Juli 2023 bis Dezember 2024. Rohtreffer einschliesslich Duplikaten und Regionalausgaben, nicht codiert. Quelle: KMK (2026g), Abschnitt 1.1.

Zugleich verschob sich die Verantwortungsfrage. Am 1. Juli titelte die Presse «Bund kritisiert IT-Firma Xplain», und Mitte Juli dehnte der EDÖB seine Untersuchung auf die Firma aus. Der Bund benannte Mängel der Firma, bezeichnete sie aber weiterhin als Opfer des Angriffs (KMK, 2026g). Ab Juli stellten Fachleute die Sicherheitspraxis der Firma infrage, und im September berichteten Recherchen, der Bund habe die Sicherheit der Firma in fünfzehn Jahren nie überprüft (Dalic et al., 2025; KMK, 2026g). Die Vergleichsstudie fasst den Befund bis November 2023 so zusammen, dass Xplain eine «doppelte Rolle» als Opfer und Mitschuldige einnehme, während Fachleute vor allem den Bund für die fehlenden Sicherheitsüberprüfungen verantwortlich machten (Dalic et al., 2025). Anfang Mai 2024 lagen die Untersuchungsberichte vor. Die Titel lauteten «Der Bund ist mitverantwortlich», und ein Beitrag hielt fest, das Fazit falle «für den Bund und den Software-Entwickler Xplain» vernichtend aus (KMK, 2026g).

Für die Instanzen bestätigt der Verlauf die Prognose. Ende August 2023 erstattete die Armee Anzeige, und der Bund liess eine Administrativuntersuchung durch eine externe Kanzlei führen; im September übernahm die Bundesanwaltschaft, die Strafverfolgungsbehörde des Bundes, das Verfahren (KMK, 2026b, Blatt «Nach Stichtag»; KMK, 2026g). Die Datenschutzaufsicht dehnte ihre Untersuchung nach zwei Wochen auf die Firma aus und schloss sie nach elf Monaten mit Empfehlungen ab, die Bundesämter und Firma im Juni 2024 annahmen. Die Verfahren wurden also rasch eröffnet, aber erst nach Monaten abgeschlossen (KMK, 2026g).

Für die Auftraggeber ist das Bild geteilt. Der Bund hielt an der Firma fest; im Februar 2024 lauteten die Titel «Bund hält an IT-Firma Xplain fest» und «Bund setzt weiter auf gehackte IT-Firma» (KMK, 2026g). Die Armee setzte das betroffene System unter verstärkter Überwachung weiter ein (Dalic et al., 2025). Der Kanton Waadt dagegen

© 2026 mediata sa, Villars-sur-Glâne

kündigte seinen Vertrag am 8. Februar 2024 mit sofortiger Wirkung, 223 Tage nach dem Stichtag. Er begründete den Schritt mit der Qualität der Produkte und mit Zweifeln an der Leistungsfähigkeit der Firma, um finanzielle und betriebliche Risiken zu begrenzen. Die Presse berichtete darüber unter dem Titel «Erster Kanton kehrt gehackter IT-Firma den Rücken» (KMK, 2026g). Die Kündigung folgte zwei Tage auf die Selbstkritik des Firmenchefs und die Zusage des Bundes. Ob der Angriff oder der Stand des Projekts den Ausschlag gab, lässt sich aus den vorliegenden Beiträgen nicht entscheiden. Tabelle 6 stellt Prognose und Verlauf einander gegenüber.

Tabelle 6: Prognose und Verlauf bis Ende 2024. Verlauf aus Trefferzahlen und Titeln, nicht codiert. Quellen: KMK (2026g), Abschnitt 1.3; KMK (2026e), Abschnitt 5; Dalic et al. (2025).

Gruppe und Grösse	Prognose zum 30.06.2023	Beobachtung bis Ende 2024	Urteil
Bund als Auftraggeber: Verhalten	Weiterführung statt Sanktion	keine Kündigung; «Bund hält an IT-Firma Xplain fest» (Februar 2024)	bestätigt
Kantone als Auftraggeber: Verhalten	Weiterführung mit Schutzmassnahmen	Mehrheit bleibt; der Kanton Waadt kündigt am 08.02.2024	für die Mehrheit gestützt; für einen Kanton nicht eingetreten
Instanzen: Verhalten	Rechtsschritte und institutionelle Durchsetzung	Anzeige der Armee, Administrativuntersuchung, Bundesanwaltschaft; Datenschutzaufsicht eröffnet nach zwei Wochen, schliesst nach elf Monaten	bestätigt; Abschluss erst nach Monaten
Öffentlichkeit: Eskalation	sprunghaft, ruhig bis zur Klärung der Faktenlage	hoch im Juli und August 2023, ruhig von Oktober bis Januar, Sprung bei den Untersuchungsberichten im Mai 2024	teilweise gestützt
Öffentlichkeit: Zuschreibung an Xplain	minimal, Konfidenz niedrig	Mängelkritik des Bundes ab 30.06.2023; «doppelte Rolle»; Untersuchungsberichte belasten Bund und Firma	für die Frühphase knapp gestützt, danach widerlegt
Kernaussage: Verantwortung wandert zum Auftraggeber	Verantwortung beim Bund	Recherche zu fehlenden Überprüfungen (September 2023); «Der Bund ist mitverantwortlich» (Mai 2024)	gestützt

© 2026 mediata sa, Villars-sur-Glâne

Gruppe und Grösse	Prognose zum 30.06.2023	Beobachtung bis Ende 2024	Urteil
Betroffene Personen	Informationssuche, Zuschreibung zunächst niedrig mit Nachholeffekt	nicht erhoben	nicht geprüft
Strategie: Wechselpunkte	Wechsel zum Wiederaufbau bei festgestellten Mängeln	Mängelkritik durch Bund und Fachleute ab Juli 2023; Untersuchungsbefund im Mai 2024	eingetreten, ausgelöst durch Dritte

Die Wechselpunkte der Strategie wurden damit erreicht, aber nicht durch die Firma. Mängel benannten ab Juli 2023 Bundesstellen und Fachleute, und der Untersuchungsbefund vom Mai 2024 traf Bund und Firma gemeinsam. Eine Selbstoffenlegung vor diesen Zeitpunkten ist in den Titeln nicht erkennbar; die öffentliche Selbstkritik des Firmenchefs folgte im Februar 2024, sieben Monate nach dem Stichtag. Wie die Firma im Einzelnen kommunizierte, ist nicht erhoben.

Gestützt wird schliesslich die Vorsicht, mit der das Strategiemodul die Lage der Auftraggeber beurteilt hatte. Es hielt sie für instabiler, als die Prognose ausdrückte, und begründete damit die reversible Anlage der Strategie (Abschnitt 5.1). Die Kündigung eines Kantons zeigt, dass diese Vorsicht berechtigt war. Im Rückblick spricht der Verlauf, der mit dem Verlust eines Kantons und dem Verkauf der Firma endet, eher für eine höhere Alarmstufe als die gewählte; diese Einschätzung ist eine Deutung aus dem Verlauf, keine Prüfung der Regel (KMK, 2026g).

6 Diskussion

Wandernde Verantwortung. Der erste Befund betrifft die Adresse der Verantwortung. In der Frühphase entlastet die Verlagerung auf den Auftraggeber das Opfer tatsächlich. Das normative Urteil trifft die Bundesstellen, die die Daten beim Lieferanten liessen, und es trifft sie, während Xplain selbst kaum noch gerahmt wird. Der Vergleich mit der Fallstudie zur RUAG MRO ist aufschlussreich. Dort fügte die Kritik am Eigner der Verantwortung eine zweite Adresse hinzu, ohne das Unternehmen zu entlasten, weil die Krise deskriptiv als vermeidbar gerahmt blieb. Hier fehlt diese deskriptive Belastung, und die Verlagerung wirkt zunächst als Entlastung. Sie hält aber nur, solange die Faktenlage offen ist. Sobald Fachleute und Recherchen die Sicherheitspraxis der Firma thematisieren, wird aus der einen Adresse eine doppelte. Die Untersuchungsberichte vom Mai 2024 haben diese doppelte Adresse bestätigt. Für die Kommunikation folgt daraus, dass ein Lieferant die Kritik an seinen Auftraggebern nicht als Schutz verstehen sollte. Sie ist ein Zeitfenster, kein Freispruch.

Opfer ohne Stimme. Der zweite Befund betrifft die Sprecherrolle. Xplain spricht in der Frühphase selbst, verstummt dann aber, und die Deutung übernimmt der Bund, der zunächst beschwichtigt, dann revidiert und schliesslich selbst unter Verdacht gerät. Für die Firma hat das zwei Seiten. Kurzfristig schützt das Schweigen, weil die Kritik den

© 2026 mediata sa, Villars-sur-Glâne

Sprecher trifft und nicht das Objekt. Mittelfristig überlässt es die Rahmung jenen, deren eigene Verantwortung zur Debatte steht und die ein Interesse haben können, die Last auf den Lieferanten zurückzuschieben. Die Ankündigung des Bundesrats, die Umsetzung der Sicherheitsvorgaben bei Xplain zu prüfen, ist in diesem Sinn bereits ein erster Schritt zurück. Das Reframing-Fenster, also die Möglichkeit, die öffentliche Zuordnung noch zu prägen, war zum Stichtag offen. Nach den Befunden des Korpus wurde es nicht genutzt.

Die Opferrolle als befristeter Schutz. Der dritte Befund betrifft die Reichweite der SCCT-Zuordnung. Das Opfercluster setzt voraus, dass die Ursache ausserhalb der Organisation liegt (Coombs, 2007). Bei Cyberangriffen ist diese Voraussetzung in der Frühphase selten geklärt: Ob eine Schwachstelle vermeidbar war, zeigt sich erst durch Untersuchungen, oft Wochen später. Die Zuordnung zum Opfercluster ist damit vorläufig, und das Muster «ruhig bis zur Faktenklärung, dann abrupt», das die Regel zur ambigen Verantwortungslage beschreibt, trifft im Fall teilweise zu: Auf einen lauten Sommer folgten ruhige Monate, und der grösste Ausschlag kam, als die Untersuchungsberichte die Faktenlage klärten und Bund und Firma gemeinsam belasteten. Ruhig war es aber erst ab Oktober, nicht schon in den Wochen nach dem Stichtag. Bemerkenswert ist, dass die Medien die Schwachstelle in der Frühphase zwar erwähnen, aber nicht werten. Der Grenzfall zwischen Opferrolle und Mitverursachung war also im Material angelegt, bevor er öffentlich entschieden wurde. Für die Praxis spricht das dafür, die Opferrolle nur flankierend zu kommunizieren und einen festgestellten Mangel selbst offenzulegen, bevor Dritte ihn aufdecken. Die Strategie hatte diesen Schritt als Wechselpunkt vorgesehen; im Verlauf wurde er durch Dritte vollzogen.

Die Lieferkette als Krisentyp. Der vierte Befund betrifft die Krisenkonstellation selbst. Xplain ist Auftragsverarbeiterin, nicht Datenherrin. Benachrichtigung der Betroffenen, Bearbeitung ihrer Begehren und die datenschutzrechtliche Verantwortung liegen bei den Auftraggebern, die zugleich die wichtigsten Anspruchsgruppen und mögliche Mitverantwortliche sind. Die Krisenkommunikation der Firma kann in dieser Lage nur unterstützen, und sie muss mit Partnern abgestimmt werden, deren Interessen sich während der Krise verschieben können. Die SCCT ist auf eine Krisenorganisation ausgelegt, die gegenüber ihren Anspruchsgruppen spricht (Coombs, 2007). Krisen in Lieferketten, in denen zwei Organisationen um dieselbe Verantwortung ringen und zugleich voneinander abhängig bleiben, behandelt sie bisher kaum. Der Verlauf zeigt zudem, dass sich die Auftraggeber nicht als Block verhalten. Der Bund hielt an der Firma fest, während ein Kanton nach sieben Monaten kündigte und dies mit der Leistung der Firma begründete. Für einen Lieferanten heisst das, seine Auftraggeber einzeln zu führen und nicht auf eine gemeinsame Loyalität zu bauen.

Abgleich mit der Vergleichsstudie. Im gemeinsamen Zeitfenster bis Ende Juni stimmen beide Analysen in der dominanten Opferrolle von Xplain und der Bundesstellen überein und ebenso darin, dass die Verantwortung zunehmend beim Bund verortet wird. Die Vergleichsstudie kommt zum Befund der «doppelten Rolle» vor allem über Aussagen nach dem Stichtag (Dalic et al., 2025; KMK, 2026e). Umgekehrt erfasst die vorliegende Analyse die französisch- und italienischsprachige Berichterstattung, die frühe Beschwichtigung durch die Bundesstellen und die fehlende eigene Stimme der Firma, die dort nicht untersucht sind.

© 2026 mediata sa, Villars-sur-Glâne

Zusammenfassend lässt sich festhalten, dass das Opfer eines Cyberangriffs in der Frühphase nicht als mitschuldig gerahmt wird, wenn die Daten Dritten gehören und diese Dritten öffentlich rechenschaftspflichtig sind. Die Verantwortung wandert zu den Auftraggebern. Diese Entlastung ist jedoch befristet. Sie endet, sobald die Frage nach der Sicherheit des Lieferanten beantwortet wird, und sie endet zu Lasten derjenigen Organisation, die bis dahin geschwiegen hat. Für die Praxis heisst das, die Opferrolle nicht als Strategie, sondern als Zustand zu behandeln, die eigene Stimme früh zu sichern und den Umfang der Verantwortungsübernahme an vorab definierte Wechselpunkte zu binden. Für die Forschung öffnet der Fall die Frage, wie sich Verantwortung in Lieferketten zwischen Opfer und Auftraggeber verteilt und welche Antwortstrategien in einer solchen Konstellation tragen.

7 Limitationen

Die Befunde sind aus sechs Gründen als orientierend zu lesen.

- **Nicht blind gegenüber dem Modellwissen.** Der simulierte Analysezeitpunkt liegt vor dem Trainingsstand des Sprachmodells. Blind war die Analyse gegenüber der Vergleichsstudie, nicht gegenüber dem, was das Modell über den späteren Verlauf wissen konnte. Übereinstimmungen mit dem Verlauf belegen deshalb nicht die Treffsicherheit der Prognose.
- **Lücke im Korpus.** Zwei Beiträge der Neuen Zürcher Zeitung (NZZ) aus dem Untersuchungsfenster fehlen. Die Recherche hatte sie verworfen, weil ihr Datum beim Abruf nicht bestimmt werden konnte; in der Mediendatenbank sind beide datiert vorhanden (KMK, 2026g). Einer davon erschien online am 30. Juni 2023, am letzten Tag des Fensters, und schreibt der Firma bereits im Titel ein Versäumnis zu: Die Zulieferfirma des fedpol «soll IT-Sicherheit vernachlässigt haben». Zugleich nennt er sie Opfer des Angriffs. Der Befund, Xplain werde bis Ende Juni nicht als mitschuldig gerahmt, gilt deshalb für den letzten Tag des Fensters nicht; er beschreibt den Korpus, wie er bei der Analyse abrufbar war. Die Kennwerte ändern sich erst mit der formalen Nachcodierung beider Beiträge, die noch aussteht.
- **Korpus.** Die französischsprachige Qualitätspresse und das Westschweizer Radio und Fernsehen konnten nicht codiert werden; die Romandie ist vor allem über Agenturmeldungen vertreten. Soziale Medien und Kommentarspalten waren rückwirkend nur lückenhaft erreichbar.
- **Einzelcodierung.** Ein Sprachmodell hat codiert, ohne Prüfung durch eine zweite Codierinstanz; Kennwerte zur Reliabilität liegen nicht vor. In Grenzfällen, besonders bei der Behandlung der ausgenutzten Schwachstelle, entschieden die sechs Codierdurchgänge uneinheitlich.
- **Kontext.** Acht der neun Faktoren der Fallhöhe beruhen ganz oder teilweise auf Schätzungen; die Krisenhistorie stützt sich auf eine Negativrecherche.
- **Verlauf.** Der Verlauf bis Ende 2024 ist aus Trefferzahlen einer Mediendatenbank und aus Titeln erhoben; gelesen wurden drei Beiträge, codiert wurde nichts. Die Zählungen enthalten Duplikate und Regionalausgaben und zeigen die Aufmerksamkeit, nicht die Rahmung. Die Gruppe der Betroffenen ist nicht

© 2026 mediata sa, Villars-sur-Glâne

erhoben. Die Vergleichsstudie arbeitet mit einem anderen Instrument und Zeitfenster; sie ist Massstab, nicht Wahrheit.

8 Literatur und Quellen

Wissenschaftliche Literatur

Arpan, L. M., & Roskos-Ewoldsen, D. R. (2005). Stealing thunder: Analysis of the effects of proactive disclosure of crisis information. *Public Relations Review, 31*(3), 425–433. https://doi.org/10.1016/j.pubrev.2005.05.003

Benoit, W. L. (1997). Image repair discourse and crisis communication. *Public Relations Review, 23*(2), 177–186. https://doi.org/10.1016/S0363-8111(97)90023-0

Coombs, W. T. (2007). Protecting organization reputations during a crisis: The development and application of Situational Crisis Communication Theory. *Corporate Reputation Review, 10*(3), 163–176. https://doi.org/10.1057/palgrave.crr.1550049

Dalic, P., Gretler, N., & Juon, C. (2025). Cyberangriff auf die Firma Xplain. In A. Grynko & O. Baeriswyl (Hrsg.), *Unternehmenskrisen im Informationszeitalter: Fallstudien* (Bd. 5, S. 55–82). mediata.

Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

Festinger, L., & Möntmann, V. (2020). *Theorie der kognitiven Dissonanz* (M. Irle, Hrsg.; 3., unveränderte Aufl., Faksimile-Reprint der deutschsprachigen Erstausgabe von 1978). Hogrefe.

Schenk, M. (2007). *Medienwirkungsforschung* (3. Aufl.). Mohr Siebeck.

Schwarz, A. (2008). Covariation-based causal attributions during organizational crises: Suggestions for extending Situational Crisis Communication Theory (SCCT). *International Journal of Strategic Communication, 2*(1), 31–53. https://doi.org/10.1080/15531180701816601

Weiner, B. (2006). *Social motivation, justice, and the moral emotions: An attributional approach.* Erlbaum.

KMK-Dokumentation und Analyseberichte

Baeriswyl, O. (2026a). *KMK-Projektbeschrieb, wissenschaftlich* (Fassung 0.5). mediata sa. https://krisenkom.ch/dw-content/wissensspeicher/KMK_Projektbeschrieb_wissenschaftlich_v0-5.docx

Baeriswyl, O. (2026b). *KMK – Technische Systemdokumentation* (Fassung 0.5). mediata sa. https://krisenkom.ch/dw-content/wissensspeicher/KMK_Technische_Systemdokumentation_v0-5.docx

KMK. (2026a). *Kontextanalyse: Cyberangriff auf Xplain (2023) (Modul ADAM)* [Unveröffentlichter Analysebericht, Stand 17.09.2026]. mediata sa.

KMK. (2026b). *Medienrecherche: Cyberangriff auf Xplain (2023) (Modul SCHNUFFI)* [Unveröffentlichte Rechercheauswertung, Stand 17.09.2026]. mediata sa.

KMK. (2026c). *Frame-Analyse und Rezeptionsprognose: Cyberangriff auf Xplain (2023) (Modul FRAMI)* [Unveröffentlichter Analysebericht, Stand 17.09.2026]. mediata sa.

KMK. (2026d). *Strategiedokument: Cyberangriff auf Xplain (2023) (Modul EVI)* [Unveröffentlichter Analysebericht, Stand 17.09.2026]. mediata sa.

KMK. (2026e). *Vergleich Tool-Analyse und Fallstudie Band 5: Cyberangriff auf Xplain* [Unveröffentlichte Testauswertung, Stand 17.09.2026]. mediata sa.

KMK. (2026f). *Nachtrag: Reputations-Fallhöhe im Fall Xplain* [Unveröffentlichter Nachtrag zum Analysebericht, Stand 25.09.2026]. mediata sa.

KMK. (2026g). *Verlauf nach dem Stichtag, NZZ-Lücke und Kanton Waadt: Cyberangriff auf Xplain (2023)* [Unveröffentlichter Nachtrag, Stand 21.11.2026]. mediata sa.

Primär- und Medienquellen

20 Minuten. (2023, 8. Juni). *Bundesverwaltung von Ransomware-Angriff betroffen.* https://www.20min.ch/story/bundesverwaltung-von-ransomware-angriff-betroffen-494000619990

Inside IT. (2023a, 23. Mai). *Xplain von Ransomware-Angriff getroffen.* https://www.inside-it.ch/xplain-von-ransomware-angriff-getroffen-20230523

Inside IT. (2023b, 1. Juni). *Ransomware-Bande veröffentlicht Daten von Xplain.* https://www.inside-it.ch/ransomware-bande-veroeffentlicht-daten-von-xplain-20230601

Kleinreport. (2023, 29. Juni). *Xplain-Desaster: «Sie können zu Beginn eines Hackerangriffs nicht ergründen, wie schwerwiegend die Folgen sind».* https://www.kleinreport.ch/news/xplain-krisenbewaltigung-sie-konnen-zu-beginn-eines-hackerangriffs-nicht-ergrunden-wie-schwerwiegend-die-folgen-sind-102150/

Moneyhouse. (2026). *Xplain AG* [Handelsregisterauszug]. https://www.moneyhouse.ch/en/company/xplain-ag-4027493521

National Cyber Security Centre NCSC. (2023, 8. Juni). *Federal Administration also impacted by Xplain hack.* https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2023/xplain.html

Radio BeO. (2023, 23. Mai). *Interlakner Software-Unternehmen gehackt.* https://www.radiobeo.ch/interlakner-software-unternehmen-gehackt/

Schurter, D. (2023a, 23. Mai). *Ransomware-Bande Play hackt Schweizer Anbieterin von Polizei-Software.* watson. https://www.watson.ch/digital/ransomware/671465872-ransomware-bande-play-hackt-schweizer-anbieterin-von-polizei-software

Schurter, D. (2023b, 8. Juni). *Möglicherweise operative Daten des Bundes von Hackern erbeutet.* watson. https://www.watson.ch/digital/ransomware/532052691-moeglicherweise-operative-daten-des-bundes-von-hackern-erbeutet

Anhang: Kennwerte und Regeln

Die Tabelle führt die Kennwerte und Regeln des KMK-Systems auf, die in der Fallstudie vorkommen. Die Kennung verweist auf die Ressource, in der die Grösse oder Regel auf krisenkom.ch definiert ist.

Tabelle A1: Kennwerte und Regeln des KMK-Systems in dieser Fallstudie. Quelle: krisenkom.ch, Stand 21.11.2026.

Bezeichnung im Text	Kennung	Bedeutung	Ressource
Reputations-Fallhöhe	FALLHOEHE	Gewicht einer Verantwortungszuschreibung für die Organisation, aus neun Faktoren (Skala −8 bis +14)	Codiersystem kontextuelle Moderatoren
Krisenhistorie	INT_HIST	frühere ähnliche Vorfälle und ihre Schwere	Codiersystem kontextuelle Moderatoren
Vorreputation	INT_REP	Ansehen der Organisation vor der Krise	Codiersystem kontextuelle Moderatoren
Attributionsverstärker	INT_SUM	Zusammenfassung von Krisenhistorie und Vorreputation	Codiersystem kontextuelle Moderatoren
Risikofallen	TRAP_*	strukturelle Konstellationen, die belastende Frames verfügbar machen (Heuchelei, Krisenhistorie, Kompetenz, Allianz, Machtgefälle)	Risikofallen nichtsituativ
textnahe und rekonstruierte Einordnung	SCCT_TEXT, SCCT_REKON	Krisentyp nach SCCT, wie ihn der Beitrag selbst setzt beziehungsweise wie er sich aus dem Gesamtzusammenhang ergibt	Modul FRAMI – Frame-Analyse
Reframing-Fenster	–	die öffentliche Zuordnung zum Krisentyp ist noch nicht gesetzt und kann geprägt werden	Modul FRAMI – Frame-Analyse
Regel zur ambigen Verantwortungslage	REZ-R10	über 40 % der Beiträge ohne eigene Rahmung → niedrige Konfidenz, sprunghafte Eskalation	Rezeptionsregeln REZ
Regel zu Angst und	REZ-R09	Angst dominant, Folgen	Rezeptionsregel

© 2026 mediata sa, Villars-sur-Glâne

Bezeichnung im Text	Kennung	Bedeutung	Ressource
offener Gefährdung		offen → Informationssuche, Zuschreibung zunächst niedrig mit Nachholeffekt	n REZ
Regel zum Opfer eines Dritten	REZ-R18	Organisation als Opfer eines Dritten gerahmt, Anspruchsgruppe demselben Risiko ausgesetzt → Loyalität statt Sanktion	Rezeptionsregel n REZ
Regel zur institutionellen Durchsetzung	REZ-R19	Normverstoss mit zuständiger Instanz → Verfahrens- und Prüfschritte der Behörden	Rezeptionsregel n REZ
Alarmstufe	STR-R71	Matrix aus prognostizierter Zuschreibung und Fallhöhe (Grün, Gelb, Rot)	Strategieregeln STR
Wechselpunkte	STR-R44	vorab festgelegte Auslöser für eine höhere Stufe der Verantwortungsübernahme bei ambiger Verantwortungslage	Strategieregeln STR

Datengrundlage und Entstehung

Die Fallstudie verdichtet die Analyseberichte der vier KMK-Module ADAM (Kontext), SCHNUFFI (Recherche), FRAMI (Framing) und EVI (Strategie), die Testauswertung zum Vergleich mit der publizierten Fallstudie sowie die datierten Nachträge im Fallordner «xplain_cyberangriff_2023_testfall». Sie übernimmt deren Befunde ohne Neuanalyse. Die ausführlichen Berichte und das für MAXQDA und SPSS aufbereitete Datenmaterial können für Forschungsvorhaben sowie von betroffenen Organisationen angefordert werden bei othmar.baeriswyl@mediata.ch. Volltexte aus Mediendatenbanken sind aus lizenzrechtlichen Gründen davon ausgenommen; die Fallstudie gibt nur Zählungen und kurze Zitate mit Quelle wieder.

Die Analyse wurde mit Claude (claude-opus-5, Anthropic) im System KMK 2.0 erstellt, die Erhebung des Verlaufs vom 21.11.2026 mit Claude (claude-fable-5-2, Anthropic) im selben System. Die Fallstudie entstand mit Unterstützung von Claude (claude-opus-5-5, Anthropic) im Projekt «KMK-Fallstudienbericht», Projektanweisung vom 21.11.2026; Schreibstimme SV-S1 und Belegstandard SV-B1, Version 1.0, Stand 14.08.2026, abgerufen am 21.11.2026.

© 2026 mediata sa, Villars-sur-Glâne