

Erfahrungsbericht:

Vom Hack zur Staatsaffäre



Tobias Bolliger | Legal Counsel Xplain AG
tobias.bolliger@xplain.ch

Stephan Bischof | Geschäftsführer Xplain AG
stephan.bischof@xplain.ch

Agenda

Schweizerischer Polizei-Informatik Kongress 2026

00 Über uns

Das Unternehmen, die Produkte und die Kunden

01 Der Angriff

Was passierte im Mai 2023?

02 Krisenmanagement

Die ersten 72 Stunden im Ausnahmezustand

03 Medien & Staatsaffäre

Vom Darknet zum Bundesratsbeschluss

04 Audit & Wiederaufbau

Quellcode-Prüfung, Auslieferungsstopp, Erholung

05 Aufarbeitung 2024

BACS-Analyse, EDÖB, Massnahmen

06 Lessons Learned

Was der Vorfall wirklich lehrt



Über uns

Xplain AG

xplain
digital homeland security

Xplain aus Interlaken entwickelt **seit 2000** mit rund 60 Mitarbeitenden spezialisierte Fachapplikationen für:

- Polizei
 - Staatsanwaltschaften
 - Gerichte
 - Straf- und Massnahmenvollzug
 - Migrationsämter
- auf **Bundes-, Kantons- und Gemeindeebene.**

Xplain betreibt **keine** Kundendaten und hat auch kein Zugriff auf produktive Systeme. Die Software läuft auf Infrastruktur der Kunden.





Der Angriff

Samstagmorgen, Ende Mai 2023 – PLAY Ransomware, Double Extortion

"Wir wurden gehackt – alle Systeme verschlüsselt."

CEO Xplain AG per Telefon an seine engsten Mitarbeiter

PLAY Ransomware

Double Extortion: Verschlüsseln + Leaken drohen
Aktiv seit 2022, zahlreiche Opfer weltweit

907 GB

publiziertes Datenvolumen

14 Tage

Darknet-Timer bis Leak



Krisenmanagement

Die **ersten 72 Stunden** – BCM als Grundlage, Kommunikation als Schlüssel

1

Std. 0–6 | Entdeckung & Isolierung

CEO alarmiert Team. Server offline. Recovery-Plan aktiviert. BCM funktioniert, doch der eigentliche Marathon beginnt erst.

2

Std. 6–24 | OSINT & SOMAS

Tor, GitHub, Leak-Foren durchsucht. PLAY identifiziert. Backups, Recovery Plan etc.

3

Std. 24–48 | Behörden & Versicherung

Strafanzeige bei Kantonspolizei Bern. IT beschlagnahmt. NCSC, fedpol, BAZG, Cyber-Versicherung informiert. Erste Lageberichte.

4

Std. 48–72 | Kommunikation vorbereiten

Kundenbriefe. Medien-Q&A erarbeitet. Narrativ festgelegt: **Kein Lösegeld.**
Volle Transparenz. Fakten statt Spekulation.



Vom Darknet in die Schlagzeilen

Juni 2023 – 1.3 Millionen Dateien öffentlich

Mitte Juni 2023: PLAY lädt 907 GB hoch - operative Dokumente von Bund und Kantonen sind öffentlich zugänglich. Hunderte Medienberichte in zwei Monaten.

Warum die Medien so schnell informiert waren:

Wochen zuvor: Grosses Schweizer Medienhaus selbst Opfer von PLAY. Investigativredaktion überwachte seitdem täglich das Darknet-Leak-Forum der Bande.

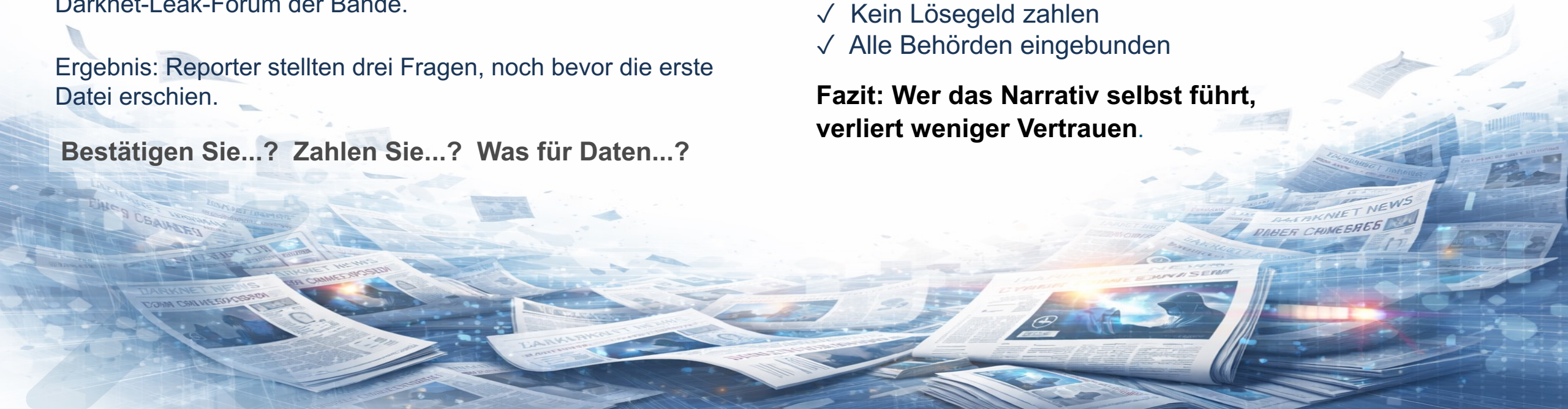
Ergebnis: Reporter stellten drei Fragen, noch bevor die erste Datei erschien.

Bestätigen Sie...? Zahlen Sie...? Was für Daten...?

Unsere Kommunikationsstrategie:

- ✓ Angriff bestätigen, keine Spekulation
- ✓ Systemwiederherstellung transparent kommunizieren
- ✓ Kein Lösegeld zahlen
- ✓ Alle Behörden eingebunden

Fazit: Wer das Narrativ selbst führt, verliert weniger Vertrauen.



Die Staatsaffäre

28. Juni 2023 – Bundesrat bildet Krisenstab PSK-D

Erstmals in der Schweizer Geschichte: Politisch-strategischer Krisenstab
Datenabfluss (**PSK-D**) unter Leitung des Finanzdepartements.

Sofortmassnahmen Bund

Bundesinterne Notfall-Protokolle aktiviert.
Betroffene Systeme isoliert.

Kommunikationslinien

Einheitliche Linien für Bund, Kantone und alle
IT-Lieferanten.

Vertragsprüfung

Überprüfung sämtlicher IT-
Lieferantenverträge des Bundes.

Source-Code-Audit

NCSC versiegelt Xplain-Quellcode.
Vollständige Prüfung jeder Commit-Historie.

Auslieferungsstopp

Kein Release bis externer Audit «keine
Hintertüren» bestätigt.

Finanzielle Folgen

Kunden frieren Rechnungen ein.
Liquiditätsdruck bis November 2023.



Audit & Wiederaufbau

Sommer bis November 2023 – unter den Augen von Bund und NCSC

Jede Commit-Historie, jedes Jenkins-Script, jeder Build-Artefakt forensisch untersucht.
Erst das Siegel «keine Hintertüren» gab den Weg frei.

Juni/Juli 2023

Forensische Prüfung

Interne und externe Auditoren. Jede Commit-Historie, Jenkins-Scripts, Artefakte.

Aug. 2023

Administrativuntersuchung

Bundesrat ordnet vollständige Aufarbeitung aller Umstände an.

Nov. 2023

Schlussbericht & Freigabe

Urteil: Infrastruktur neu aufgebaut, Prozesse nachvollziehbar.
Auslieferungsstopp aufgehoben.

**8. Februar 2024: Erwartetes Jahresergebnis 2023. Kein Konkurs.
Keine ungewollten Mitarbeitenden-Abgänge.**



Aufarbeitung 2024

BACS-Analyse, EDÖB & Administrativuntersuchung

7. März 2024: BACS legt Zahlen vor. 2. Mai 2024: EDÖB und Administrativuntersuchung veröffentlicht.

1'300'000

gestohlene Dateien gesamt

65'000

aus Bundesbehörden (5%)

Kritikpunkte (EDÖB / Admin-Untersuchung):

- * Unklare Vertragsformulierungen beim Bund
- * Ungenügende Löschroutinen bei Xplain
- * Keine Need-to-know-Freigaben durchgesetzt

Medientitel: Fehlerkette bei Bund und Lieferant

Massnahmen (alle vor Bericht umgesetzt):

- ✓ Need-to-know-Freigaben in allen Support-Prozessen
- ✓ Verbindliche Purge-Policies eingeführt
- ✓ Datenschutz-Schulung für alle Mitarbeitenden
- ✓ Compliance-Checks extern auditiert



**Strafuntersuchungen noch nicht
abgeschlossen**

Neues Reifegrad-Niveau

Zero Trust, Auditierbarkeit & Transparenz als DNA

Handlungsfeld	Was umgesetzt wurde
Zero-Trust-Architektur	MFA, Least-Privilege, segmentierte Netze, kontinuierliches Monitoring
Auditierbare Prozesse	Jährliche SOC 2 Type II, automatisierte CIS-Benchmark-Checks
Finanzielle Resilienz	Kredit-Fallback, Cyber-Versicherung, Release-Freeze-Szenario in Liquiditätsplanung
Vertrauensgarantie	Strenge Datenklassifikation, Need-to-know, Purge-Policies



2024: Chapters Group übernimmt Xplain.

Lessons Learned

Vier Erkenntnisse – direkt aus der Praxis

1

BCM ist nur Phase 1

IT-Wiederherstellung startet erst den Marathon aus Recht, Aufsicht und Kommunikation.

→ Eigenes Kapitel After-Action und Legal Track im BCM-Handbuch anlegen.

2

Transparenz schützt Reputation

Offene Lageberichte halten das Narrativ unter eigener Kontrolle. Proaktive Kommunikation = signifikant weniger Kundenverluste.

→ Kommunikationsleitfaden mit Eskalationsstufen vorbereiten.

3

Finanzielle und strukturelle Resilienz braucht Vorarbeit

Cash-Drain folgt oft erst Wochen nach dem Angriff – Kunden frieren Rechnungen ein.

→ Kredit-Fallback, Cyber-Versicherung und Liquiditätsplanung heute einrichten.

4

Mitarbeitende sind der Schlüsselfaktor

Psychische Belastung dauert länger als das Incident-Ticket.

→ Vertrauensperson definieren, ehrlich kommunizieren.

Resilience-Programme: bis -30% Fluktuation.



Security ist kein Zustand -
es ist ein Prozess.

Wer ihn durchlaufen hat -
ist xperienced.



Stephan Bischof | Xplain AG
stephan.bischof@xplain.ch

Tobias Bolliger | Xplain AG
tobias.bolliger@xplain.ch