VORFALL-LAGEBILD

Safepay veröffentlicht Daten der ARA-Region Lyss-Limpachtal (BE) und der Gemeinde Manno (TI)

Stand 10.11.2026 14:00 · Sendung: – · · Belegstärke: bestätigt · berichtet · vermutet · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach bisherigem Stand ging es um Daten und Erpressung; ein Ausfall der Abwasserreinigung ist nicht bekannt.

2. Safepay kommt laut FBI und CISA vor allem über schwache Zugänge, VPN und ungepatchte Edge-Geräte, das lässt sich auch in kleinen Betrieben absichern.

3. Manno zeigt, dass getrennte Backups und ein Notfallplan aus einem Angriff einen Ausfall von Stunden machen statt von Wochen.

Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Safepay hat laut inside-it.ch Daten einer Tessiner Gemeinde und einer Berner Abwasserreinigungsanlage veröffentlicht, nach Darstellung des Mediums darunter hochsensible Informationen.	100 %	100 %	bestätigt
Ransomware.live führt ara-lyss.ch seit dem 15.09.2026 (19:29 UTC) als Safepay-Opfer.	100 %	100 %	bestätigt
Manno bestätigt: Anfang August wurde ein Teil der Gemeindeserver angegriffen und verschlüsselt. Die Gemeinde hat Meldung erstattet und Strafanzeige gegen Unbekannt eingereicht.	100 %	95 %	präzisiert
Safepay betreibt laut CISA/FBI Double Extortion, also Datendiebstahl und Verschlüsselung. Die Gruppe kommt vor allem über gestohlene oder erratene Zugangsdaten, VPN-Zugänge und Schwachstellen in Edge-Geräten herein.	100 %	100 %	bestätigt
Bei der ARA gab es tatsächlich einen Einbruch in die IT mit Datenabfluss.	75 %	75 %	offen
Das Motiv ist finanziell (Erpressung) und nicht Sabotage.	85 %	85 %	offen
In Manno waren Daten und Betrieb dank Backups innerhalb von Stunden wiederhergestellt. Die Gemeinde warnt die Bevölkerung vor betrügerischen Zahlungsaufforderungen.	100 %	95 %	bestätigt
Die ARA Lyss ist auf 85 000 Einwohnerwerte ausgelegt und reinigt Abwasser aus Gemeinden der Kantone Bern und Solothurn.	100 %	40 %	präzisiert
Die Abwasserreinigung lief ohne Unterbruch weiter.	70 %	70 %	offen

Frühere Aussage	vorher	jetzt	Status
Die Hauptauswirkung ist der Datenabfluss, also Folgerisiken wie Phishing oder Betrug mit den veröffentlichten Daten.	65 %	65 %	offen
Manno hat den Betrieb mit vorhandenen Backups innerhalb von Stunden wiederhergestellt.	100 %	95 %	bestätigt
Die IT der ARA läuft sechs Wochen nach dem Leak-Eintrag wieder normal.	70 %	70 %	offen
Mechanische oder verfahrenstechnische Schäden an der Anlage sind entstanden.	10 %	8 %	offen
Systeme wie die Leitstellen-PCs waren vorübergehend betroffen.	25 %	25 %	offen
Safepay bekennt sich seit dem 15.09. zu acht Angriffen in der Schweiz, darunter Bio-Strath und DD Automation.	100 %	100 %	bestätigt
Laut CISA/FBI hat Safepay seit August 2024 mindestens 600 Organisationen in mehreren KRITIS-Sektoren angegriffen.	100 %	100 %	bestätigt
Das BACS hat einen eigenen IKT-Minimalstandard für Abwasser veröffentlicht. Er behandelt unter anderem Ransomware-Befall und Manipulation von Prozessdaten.	100 %	75 %	präzisiert
Viele kleine ARA mit wenigen Mitarbeitenden haben keine eigene IT-Sicherheit und hängen an einem externen IT-Dienstleister.	70 %	70 %	offen
CISA/FBI empfehlen MFA, eingeschränkte Admin-Rechte gegen Lateral Movement und schnelles Patchen von VPNs, Firewalls und anderen Edge-Geräten.	100 %	100 %	bestätigt
Bei einer simulierten Social-Engineering-Attacke auf eine Zürcher ARA kam der Tester an Prozessleitsystem und Server heran. Entdeckt wurde das erst nach zehn Tagen.	100 %	100 %	bestätigt
Weitere Schweizer Gemeinden oder Versorger tauchen in den nächsten Wochen bei Safepay oder anderen Gruppen auf.	75 %	75 %	offen

Neu seit dem letzten Stand

• Manno: Gemeinde warnt laut inside-it.ch vor unerwarteten Briefen/E-Mails mit Zahlungsaufforderungen (jetzt belegt).

• Leak-Eintrag manno.ch erst am 28.09.2026, Angriff laut Gemeinde schon Anfang August.

• Betreiberangaben ARA: 42 000 Einwohner, 60 000 Einwohnergleichwerte; die Zahl 85 000 EW ist nicht belegt.

• Manno war bereits 2019 Ransomware-Opfer.

• Advisory AA26-293A: Mitautor LKA Rheinland-Pfalz; Safepay setzt NAS mit Backups auf Werkseinstellungen zurück.

Wissensstand



■ Wissen 44 % ■ Wahrscheinlich 24 % ■ Nicht bekannt 32 %

Für Manno belastbar (Gemeindemitteilung, wiedergegeben von inside-it.ch), für die ARA nur Leak-Eintrag und Medienbericht ohne Bestätigung durch Betreiber oder Behörden.

1. Was ist passiert, und warum?

WISSEN

• inside-it.ch (27.10.2026, 07:55, Philipp Anz): Safepay hat Daten der Gemeinde Manno und der ARA-Region Lyss-Limpachtal veröffentlicht, laut Teaser darunter hochsensible Informationen; beide werden als kritische Infrastrukturen bezeichnet. (100 %)
[https://www.inside-it.ch/kritische-schweizer-infrastrukturen-attackiert-20261027]

• Ransomware.live führt ara-lyss.ch seit 15.09.2026, 19:29 UTC als Safepay-Opfer; der Eintrag beschreibt Hauptsitz und zentrale Kläranlage in Lyss sowie die ARA Messen. (100 %)
[https://www.ransomware.live/id/YXJhLWx5c3MuY2hAc2FmZXBheQ==]

• Ransomware.live führt manno.ch seit 28.09.2026, 08:34 UTC als Safepay-Opfer. (100 %)
[https://www.ransomware.live/id/bWFubm8uY2hAc2FmZXBheQ==]

• Laut Mitteilung der Gemeinde Manno (wiedergegeben von inside-it.ch, 29.09.2026) wurde ein Teil der gemeindeeigenen Server Anfang August angegriffen und verschlüsselt; der Vorfall wurde gemeldet und Anzeige gegen Unbekannt erstattet. (100 %)
[https://www.inside-it.ch/tessiner-gemeinde-wird-opfer-von-cyberkriminellen-20260929]

• Joint Advisory AA26-293A (20.10.2026, FBI, CISA, USSS, LKA Rheinland-Pfalz, NCA, North West ROCU): Safepay erlangt Zugang über gestohlene oder erratene Passwörter, Brute Force, VPN-Zugänge, Phishing und bekannte Schwachstellen in Edge-Geräten, exfiltriert Daten und verschlüsselt danach. (100 %) [https://www.ic3.gov/CSA/2026/261020.pdf]

NICHT BEKANNT

• Ob die ARA einen Angriff bestätigt und wann er stattfand.

• Welche Daten der ARA veröffentlicht wurden (Volltext inside-it.ch hinter Bezahlschranke).

• Wie die Täter hereinkamen, bei ARA wie bei Manno.

• Ob es eine Lösegeldforderung oder Verhandlung gab.

WAHRSCHEINLICH (Einschätzung)

• Bei der ARA gab es tatsächlich einen Einbruch in die IT mit Datenabfluss. (75 %) – Leak-Eintrag seit 15.09. und laut inside-it.ch veröffentlichte Daten; Safepay arbeitet laut Advisory immer mit Exfiltration. Keine Bestätigung des Betreibers.

• Das Motiv ist finanziell (Erpressung), Sabotage war nicht das Ziel. (85 %) – Safepay verlangt laut Advisory Lösegeld in Kryptowährung und veröffentlicht Daten bei Nichtzahlung; kein Hinweis auf politische Motive.

• Die ARA wurde eher zufällig getroffen, als Teil breiter Angriffe auf erreichbare Zugänge, und nicht gezielt als Abwasserbetrieb ausgewählt. (60 %) – Advisory beschreibt automatisierte Skripte gegen internetexponierte Systeme; Opferspektrum in der Schweiz reicht von Firmen bis Gemeinden.

2. Was ist die Auswirkung?

WISSEN

• Manno konnte laut Gemeinde Daten und Betrieb dank Backups innerhalb von Stunden wiederherstellen und warnt die Bevölkerung vor unerwarteten Briefen oder E-Mails mit Zahlungsaufforderungen oder Abfragen persönlicher Daten. (100 %)
[https://www.inside-it.ch/tessiner-gemeinde-wird-opfer-von-cyberkriminellen-20260929]

• Im Einzugsgebiet der ARA (Anlagen Lyss und Messen) leben laut Betreiber 42 000 Einwohner, mit Grossindustrie 60 000 Einwohnergleichwerte. (100 %) [https://ara-lyss.ch/einzugsgebiet/]

• Der Gemeindeverband umfasst bernische Gemeinden sowie die solothurnischen Gemeinden Messen und Unterramsern (Stand RRB 2014: 13 bernische plus 2 solothurnische). (100 %)
[https://rrb.so.ch/beschlussnummer/2014_1289/download/34e84ab03b73446ea0ba517473cb1b06]

• Die ARA erzeugt rund 870 000 m³ Biogas pro Jahr und Strom mit drei Blockheizkraftwerken. (100 %) [https://ara-lyss.ch/anlagen/]

NICHT BEKANNT

• Ob die Abwasserreinigung je beeinträchtigt war.

• Welche Personen- oder Betriebsdaten der ARA offenliegen.

• Ob Bevölkerung, Mitarbeitende oder Verbandsgemeinden informiert wurden.

WAHRSCHEINLICH (Einschätzung)

• Die Abwasserreinigung lief ohne Unterbruch weiter. (70 %) – Keine Berichte über Störungen oder Gewässerbelastung; Webseite online; Kläranlagen lassen sich notfalls lokal fahren. Aber keine Aussage des Betreibers.

• Die Hauptauswirkung ist der Datenabfluss mit Folgerisiken wie Phishing oder Betrug. (65 %) – Schema bei Safepay laut Advisory; Manno warnt genau davor. Für die ARA fehlen Angaben zu Daten und Betrieb.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

• Manno: Daten und Betrieb laut Gemeinde mit vorhandenen Backups innerhalb von Stunden wiederhergestellt. (100 %) [https://www.inside-it.ch/tessiner-gemeinde-wird-opfer-von-cyberkriminellen-20260929]

• Safepay stoppt laut Advisory den Volume Shadow Copy Service und setzt NAS-Speicher mit Backup-Daten auf Werkseinstellungen zurück, um Wiederherstellung zu verhindern. (100 %) [https://www.ic3.gov/CSA/2026/261020.pdf]

NICHT BEKANNT

• Ob bei der ARA überhaupt verschlüsselt wurde.

• Wie lange eine allfällige IT-Wiederherstellung bei der ARA dauerte.

WAHRSCHEINLICH (Einschätzung)

• Die IT der ARA läuft rund acht Wochen nach dem Leak-Eintrag wieder normal. (70 %) – Webseite erreichbar, keine Störungsmeldung; aber kein Beleg zum Zustand der internen IT.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

• Das Advisory nennt OT-Betreiber ausdrücklich als Zielgruppe, beschreibt aber keine Manipulation von Steuerungen durch Safepay; das Vorgehen zielt auf Windows-Netze, Dateifreigaben und Backups. (100 %) [https://www.ic3.gov/CSA/2026/261020.pdf]

NICHT BEKANNT

• Ob Leittechnik, Prozessleitsystem oder Fernwirktechnik der ARA berührt wurden.

• Wie IT und OT bei der ARA getrennt sind.

WAHRSCHEINLICH (Einschätzung)

• Mechanische oder verfahrenstechnische Schäden an der Anlage sind entstanden. (8 %) – Keinerlei Hinweis; Safepay sabotiert laut Advisory keine Prozesse; Kläranlagen haben lokale Handebene.

• Windows-Rechner der Leitstelle (Bedien- oder Visualisierungs-PCs) waren vorübergehend betroffen. (25 %) – In kleinen Anlagen sind Büro-IT und Leitstelle oft schlecht getrennt; konkreter Beleg fehlt völlig.

5. Wie viele solcher Ziele gibt es?

WISSEN

• Safepay bekennt sich laut inside-it.ch seit 15.09.2026 zu acht Angriffen in der Schweiz, darunter Bio-Strath und DD Automation. (100 %) [https://www.inside-it.ch/kritische-schweizer-infrastrukturen-attackiert-20261027]

• Laut Advisory hat Safepay seit August 2024 mindestens 600 Opfer aus mehreren KRITIS-Sektoren in Nordamerika, Südamerika, Europa und Australien getroffen. (100 %) [https://www.ic3.gov/CSA/2026/261020.pdf]

• Für Abwasserbetriebe gibt es den IKT-Minimalstandard Abwasser (Erstausgabe 2019, aktualisiert März 2021), herausgegeben von BWL und VSA, abrufbar über das BACS. (100 %)
[https://www.bwl.admin.ch/bwl/en/home/bereiche/ikt/ikt_minimalstandard/ikt_branchenstandards/abwasser.html]

• Die im Social-Engineering-Test 2022 geprüfte Zürcher ARA hatte fünf Mitarbeitende bei 45 000 Einwohnerwerten. (100 %)
[https://www.aquaetgas.ch/wasser/abwasser/20220829_ag9_simulierter-cyberangriff-auf-ara/]

• Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Schweiz: 48129 gesamt (DNP3 14246, ProConOS 13564, EtherNet/IP 13515, Modbus 1920, Siemens S7 559, OPC UA 368) (100 %)

NICHT BEKANNT

• Wie viele Schweizer ARA aktuell Fernwartungs- oder VPN-Zugänge ins Internet exponieren.

• Wie viele ARA den Minimalstandard umgesetzt haben.

WAHRSCHEINLICH (Einschätzung)

• Viele kleine ARA mit wenigen Mitarbeitenden haben keine eigene IT-Sicherheit und stützen sich auf einen externen IT-Dienstleister. (70 %) – Personalbestand im Zürcher Testfall; Manno arbeitet laut eigenen Angaben (2019) ebenfalls mit externer Informatikfirma. Keine Branchenstatistik gefunden.

6. Kann das wieder passieren?

WISSEN

• Advisory-Empfehlungen: Firewalls und Edge-Geräte zeitnah patchen, Zero Trust, Admin-Werkzeuge und Rechte einschränken, MFA und Identitätsmanagement. (100 %)
[https://www.ic3.gov/CSA/2026/261020.pdf]

• Bei einem Social-Engineering-Test an einer Zürcher ARA gelangte der Tester per Vorwand an Betriebsgebäude, Prozessleitsystem und Server; der Zugriff fiel erst zehn Tage später zufällig in der Kaffeepause auf. (100 %)
[https://www.aquaetgas.ch/wasser/abwasser/20220829_ag9_simulierter-cyberangriff-auf-ara/]

• Manno war bereits 2019 Opfer von Ransomware (laut damaligem Gemeindepräsidenten ein Arbeitstag verloren, kein Lösegeld). (100 %)
[https://www.ticinonews.ch/ticino/hackerato-anche-il-comune-di-manno-321782]

NICHT BEKANNT

• Welche Massnahmen die ARA seither getroffen hat.

WAHRSCHEINLICH (Einschätzung)

• Weitere Schweizer Gemeinden oder Versorger tauchen in den nächsten Wochen bei Safepay oder anderen Gruppen auf. (75 %) – Acht Schweizer Opfer in sechs Wochen; Advisory nennt Safepay unter den aktivsten Gruppen 2026.

Lage

Die Ransomware-Gruppe Safepay hat laut inside-it.ch Daten der Berner ARA-Region Lyss-Limpachtal und der Tessiner Gemeinde Manno veröffentlicht. Manno hat einen Angriff Anfang August mit Verschlüsselung von Servern bestätigt und laut Bericht den Betrieb mit Backups innerhalb von Stunden wiederhergestellt. Von der ARA gibt es weiterhin keine öffentliche Stellungnahme; ob Leittechnik oder Betrieb betroffen waren, ist offen.

Angriff	Ransomware mit Datenveröffentlichung (Double Extortion); bei Manno Verschlüsselung bestätigt, bei der ARA nur Leak-Eintrag und Veröffentlichung
Wann / Status	Manno: Anfang August 2026 (Gemeinde); ARA: Leak-Eintrag 15.09.2026, Angriffszeitpunkt unbekannt · unklar
Täter	Safepay – berichtet
Betreiber / Branche	ARA-Region Lyss-Limpachtal (Gemeindeverband) sowie Gemeinde Manno · Abwasserentsorgung / Gemeindeverwaltung

Anlage / Alter	Zwei kommunale Kläranlagen (Lyss, Messen) mit Biogas und drei BHKW ·
Region	Seeland BE / Bucheggberg SO; Manno TI
Auswirkungen	Keine Berichte über Störungen der Abwasserreinigung oder Gewässerbelastung. Hauptrisiko sind veröffentlichte Daten (Betrug, Phishing). Manno warnt die Bevölkerung vor unerwarteten Zahlungsaufforderungen.
Behörden	Manno: zuständige Behörden informiert, Anzeige gegen Unbekannt (Gemeinde laut inside-it.ch). ARA: keine öffentliche Angabe; ob BACS informiert wurde, ist nicht bekannt.
Regulatorik	Seit 1.4.2025 müssen Betreiber kritischer Infrastrukturen Cyberangriffe innert 24 Stunden dem BACS melden (ISG/CSV), Busse bis 100 000 Franken, sanktioniert ab Oktober 2025 (https://www.itreseller.ch/Artikel/102757/Ab_1__April_2025_gilt_Meldepflicht_fuer_Cyberangriffe.html). Ob ARA-Verband und Gemeinde im Einzelfall meldepflichtig sind, nicht geprüft (vermutet ja). Branchenstandard: IKT-Minimalstandard Abwasser, freiwillig. NIS2 und CRA gelten in der Schweiz nicht direkt.

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

• Gestohlene oder erratene Zugangsdaten für VPN oder Remote Access (Fernwartung durch Dienstleister) (hoch): Laut Advisory der bevorzugte Weg von Safepay; kleine Betriebe haben oft externe Fernwartungszugänge ohne MFA.

• Ausnutzung bekannter Schwachstellen in Firewalls/VPN-Gateways oder Backup-Servern (mittel): Advisory nennt automatisierte Ausnutzung bekannter CVEs in Edge- und Backup-Produkten; ob solche Produkte bei der ARA laufen, ist unbekannt.

• Phishing gegen Mitarbeitende (mittel): Advisory nennt Phishing und gephishte Konten; Zürcher ARA-Test zeigte Anfälligkeit für Social Engineering.

• Kompromittierung über einen gemeinsamen IT-Dienstleister (gering): Bei Gemeindeverbänden verbreitete Abhängigkeit; für diesen Fall gibt es keinerlei Hinweis.

Zeitleiste

Sommer 2019 Manno erstmals von Ransomware betroffen – berichtet
[https://www.ticinonews.ch/ticino/hackerato-anche-il-comune-di-manno-321782]

Anfang August 2026 Teil der Server von Manno angegriffen und verschlüsselt, mit Backups in Stunden wiederhergestellt – bestätigt
[https://www.inside-it.ch/tessiner-gemeinde-wird-opfer-von-cyberkriminellen-20260929]

15.09.2026, 19:29 UTC ara-lyss.ch erscheint auf der Safepay-Leak-Seite – berichtet
[https://www.ransomware.live/id/YXJhLWx5c3MuY2hAc2FmZXBheQ==]

28.09.2026, 08:34 UTC manno.ch erscheint auf der Safepay-Leak-Seite – berichtet
[https://www.ransomware.live/id/bWFubm8uY2hAc2FmZXBheQ==]

29.09.2026 inside-it.ch berichtet über Gemeindemitteilung Manno – berichtet
[https://www.inside-it.ch/tessiner-gemeinde-wird-opfer-von-cyberkriminellen-20260929]

20.10.2026 Joint Advisory AA26-293A zu Safepay veröffentlicht, mit LKA Rheinland-Pfalz – bestätigt [https://www.ic3.gov/CSA/2026/261020.pdf]

27.10.2026, 07:55 inside-it.ch: Daten von ARA und Manno veröffentlicht, acht Schweizer Safepay-Opfer seit 15.09. – berichtet
[https://www.inside-it.ch/kritische-schweizer-infrastrukturen-attackiert-20261027]

Vergleichsfälle

• Social-Engineering-Test an einer Zürcher ARA (2022): Mit einem Vorwand kam der Tester an Prozessleitsystem und Server, bemerkt wurde es erst nach zehn Tagen.
[https://www.aquaetgas.ch/wasser/abwasser/20220829_ag9_simulierter-cyberangriff-auf-ara/]

• Manno und Baustoffhändler Taiana (Ransomware) (2019): Dieselbe Gemeinde wurde nach sieben Jahren erneut getroffen; Backups hielten den Schaden beide Male klein.
[https://www.ticinonews.ch/ticino/hackerato-anche-il-comune-di-manno-321782]

• Gemeinde Rolle VD (2021): Veröffentlichte Gemeindedaten beschäftigen Behörden und Bevölkerung noch lange nach der technischen Wiederherstellung.
[https://www.nzz.ch/technologie/cyberangriff-auf-rolle-wie-hacker-die-gemeinde-durchschuettelten-ld.1687856]

Begriffe einfach erklärt

OT: Die Technik, die physische Prozesse steuert, hier Pumpen, Gebläse und Messgeräte der Kläranlage.

Ransomware: Schadsoftware, die Daten verschlüsselt, damit die Täter Lösegeld verlangen können.

Double Extortion: Doppelte Erpressung: Die Täter stehlen zuerst Daten und drohen mit Veröffentlichung, zusätzlich zur Verschlüsselung.

Leak-Seite: Webseite der Täter im Darknet, auf der sie Opfer nennen und gestohlene Daten veröffentlichen.

Edge-Geräte: Geräte am Rand des Netzes wie Firewalls und VPN-Gateways, über die man von aussen hereinkommt.

Einwohnergleichwert: Masseinheit für die Abwasserlast; Industrie wird in vergleichbare Einwohner umgerechnet.

Früherer Stand: Erstmeldung (27.10.2026 13:50)

Wissen 34 % · wahrscheinlich 28 % · nicht bekannt 38 %
Laut inside-it.ch (27.10.2026) hat die Ransomware-Gruppe Safepay Daten der Berner Abwasserreinigung ARA-Region Lyss-Limpachtal und der Tessiner Gemeinde Manno veröffentlicht. Seit dem 15.09. bekennt sie sich zu acht Angriffen in der Schweiz. Manno hat den Angriff bestätigt (Verschlüsselung Anfang August, Wiederherstellung aus Backups in Stunden). Für die ARA gibt es bisher nur den Eintrag auf der Leak-Seite und keine Stellungnahme des Betreibers. Ob die Leittechnik betroffen ist, weiß öffentlich niemand.

Früherer Stand: Nach 24 Stunden (28.10.2026 14:03)

Wissen 39 % · wahrscheinlich 21 % · nicht bekannt 40 %
Die Ransomware-Gruppe Safepay führt die ARA-Region Lyss-Limpachtal seit dem 15.09.2026 auf ihrer Leak-Seite. Laut inside-it.ch vom 27.10.2026 hat sie inzwischen Daten der ARA und der Tessiner Gemeinde Manno veröffentlicht. Die Gemeinde Manno hat einen Angriff Anfang August bestätigt und ihre Systeme innerhalb von Stunden aus Backups wiederhergestellt. Von der ARA selbst oder von Behörden gibt es bis heute (28.10.2026) keine öffentliche Stellungnahme, und ob die Leittechnik betroffen war, ist nicht bekannt.

Früherer Stand: Nach 72 Stunden (30.10.2026 14:08)

Wissen 42 % · wahrscheinlich 24 % · nicht bekannt 34 %
Die Ransomware-Gruppe Safepay führt die ARA-Region Lyss-Limpachtal laut Ransomware.live seit dem 15.09.2026 auf ihrer Leak-Seite, und laut inside-it.ch (27.10.2026) hat sie inzwischen Daten der ARA und der Tessiner Gemeinde Manno veröffentlicht. Manno hat einen Angriff mit Verschlüsselung Anfang August bestätigt und war nach eigenen Angaben dank Backups innerhalb von Stunden wieder im Betrieb. Von der ARA gibt es bis heute keine öffentliche Stellungnahme, und es gibt keinen Hinweis auf eine Störung der Abwasserreinigung oder der Leittechnik.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.