

Ransomware bei Ixa Systems: Sicherheitspläne geleakt

Stand 21.10.2026 12:34 · Sendung: – · · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

Wissensstand

■ Wissen 49 % ■ Wahrscheinlich 20 % ■ Nicht bekannt 31 %

Mittel bis gut. Täter, Zeitraum, Datenarten und die Stellungnahmen von Ixa, Kanton und BCV sind über Le Temps (wiedergegeben von AWP/cash.ch, ICTjournal und Netzwoche) übereinstimmend belegt. Offen sind der Einstiegsweg, der genaue Datenumfang, die Aktualität der Zugangsdaten und der Stand der Bereinigung bei den Kunden. Den Originalartikel von Le Temps konnte keine der beiden Recherchen direkt einsehen.

1. Was ist passiert, und warum?

WISSEN

- Ixa Systems SA, Route de Prilly 23 in Crissier, ist seit 02.08.2007 im Handelsregister eingetragen. Laut Firmenzweck plant, liefert, installiert und wartet die Firma Sicherheits-, Telekom- und Netzwerksysteme (bestätigt, Handelsregisterdaten). (100 %)

[<https://www.moneyhouse.ch/en/company/ixa-systems-sa-3767117901>]

- Laut Le Temps (via AWP) hat die Ransomware-Gruppe TheGentlemen Ixa Ende August 2026 angegriffen. Ixa ist auf Videoüberwachung, Zutrittskontrolle und Einbruchschutz spezialisiert (berichtet). (100 %)

[<https://cash.ch/news/presse-hacker-erbeuten-schweizer-sicherheitsdaten-von-gefangnissen-und-banken-974664>]

- ransomware.live führt Ixa als Opfer von TheGentlemen. Der Eintrag auf der Leak-Seite wurde am 30.08.2026 um 09:53 UTC erfasst, als Angriffstag wird der 28.08.2026 geschätzt (berichtet, Aggregator). (100 %) [<https://www.ransomware.live/id/SXhhlFN5c3RIbXNAdGhIZ2VudGxlbWVu>]

- TheGentlemen hat sich Ende August zum Datendiebstahl bekannt, am 25.09.2026 wurden die Dokumente im Darknet zum Verkauf angeboten (berichtet, ICTjournal nach Le Temps). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- Ixa gibt an, kein Lösegeld gezahlt und den Zugriff auf seine Daten nie verloren zu haben (Angabe des Unternehmens, berichtet). (100 %)

[<https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtländer-firma-legt-sensible-sicherheitsdaten-offen>]

- TheGentlemen ist ein Ransomware-as-a-Service-Angebot, aktiv seit 2025, und arbeitet mit Double Extortion: Daten stehlen, Systeme verschlüsseln, mit Veröffentlichung drohen (berichtet). (100 %) [<https://ictk.ch/inhalt/datenleck-bei-ixa-systems-hacker-erbeuten-sensible-schweizer-sicherheitsdaten>]

- Trend Micro hat die Gruppe erstmals im August 2025 beobachtet; in einem untersuchten Fall war ein kompromittierter FortiGate-Server der Einstieg (berichtet, Analyse, kein Bezug zu Ixa). (100 %) [<https://trendmicro.com/en/research/25/i/unmasking-the-gentlemen-ransomware.html>]

- Laut Check Point dringt die Gruppe fast ausschließlich über ungepatchte Edge Devices (VPN, Appliances), über Zugänge von Initial Access Brokern oder über Zugangsdaten aus Infostealer-Logs ein; genannt werden u. a. CVE-2024-55591 und CVE-2025-32433. Sekundärquellen erwähnen auch SSL-VPN und exponiertes RDP (berichtet, Analyse, kein Bezug zum Fall Ixa belegt). (100 %) [<https://blog.checkpoint.com/research/when-the-ransomware-gang-gets-hacked-what-the-gentlemen-leak-reveals-about-modern-ransomware-risk/>]

- Check Point Research hat im April 2026 einen DFIR-Bericht zu TheGentlemen veröffentlicht (berichtet, Analyse). (100 %) [<https://research.checkpoint.com/2026/dfir-report-the-gentlemen/>]

NICHT BEKANNT

- Wie die Angreifer bei Ixa eingedrungen sind

- Ob Systeme bei Ixa verschlüsselt wurden oder nur Daten abgeflossen sind
- Wie viele Daten insgesamt abgeflossen sind
- Ob die Daten inzwischen verkauft oder frei veröffentlicht sind
- Ob eine Strafanzeige gestellt oder das BACS informiert wurde

WAHRSCHEINLICH (Einschätzung)

- Der Angriff war finanziell motiviert und opportunistisch und richtete sich nicht gezielt gegen Gefängnisse oder Banken. (70 %) – TheGentlemen arbeitet als RaaS mit mehreren hundert Opfern quer durch alle Branchen, Ixa ist ein kleiner Betrieb ohne erkennbares politisches Profil. Das Interesse an den Kundendaten kann aber nachträglich wachsen.
- Der Einstieg erfolgte über ein Edge-Gerät oder über gültige Zugangsdaten (VPN, Remote Access, Cloud-Konten). (55 %) – Laut Check Point und Trend Micro ist das das dokumentierte Hauptmuster der Gruppe. Für Ixa selbst gibt es keinen Beleg.

2. Was ist die Auswirkung?

WISSEN

- Laut einer Expertenanalyse, die Le Temps einsehen konnte, umfassen die Daten Infrastrukturpläne, Kamerastandorte, Angaben zur Videoüberwachung und in einigen Fällen Benutzernamen oder Passwörter (berichtet). (100 %)

[<https://cash.ch/news/presse-hacker-erbeuten-schweizer-sicherheitsdaten-von-gefangnissen-und-banken-974664>]

- Bei manchen Kunden liegen nur Ausschreibungsunterlagen vor, bei anderen Kamerastandorte und die Anordnung von Alarmknöpfen (berichtet). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- Betroffen sind laut Le Temps unter anderem die Etablissements de la plaine de l'Orbe, Räume der Gendarmerie, mehrere Banken (darunter die BCV) und mehrere Dutzend Unternehmen (berichtet). (100 %)

[<https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtländer-firma-legt-sensible-sicherheitsdaten-offen>]

- ictk.ch nennt zusätzlich kryptografische Schlüssel und Gebäude-Sicherheitspläne. Die anderen Berichte erwähnen kryptografische Schlüssel nicht (berichtet, nur eine Quelle). (100 %)

[<https://ictk.ch/inhalt/datenleck-bei-ixa-systems-hacker-erbeuten-sensible-schweizer-sicherheitsdaten>]

- Laut Ixa gelangten die Angreifer nicht direkt an Kamerabilder; die Firma hat mehrere Kunden informiert (Angabe des Unternehmens, berichtet). (100 %)

[<https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtländer-firma-legt-sensible-sicherheitsdaten-offen>]

- Der kantonale Cybersicherheitsdelegierte Marc Barbezat sagt, die bisherigen Prüfungen hätten keine Informationen ergeben, die die Sicherheit der Einrichtungen gefährden oder Zugang zur IT des Kantons geben (bestätigt, Behörde, via Le Temps). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- Die BCV meldet nach vertieften Analysen kein besonderes Sicherheitsproblem (Angabe der Betroffenen, via Le Temps). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

NICHT BEKANNT

- Wie viele Kunden insgesamt betroffen sind und welche ausserhalb der Waadt
- Ob die Passwörter noch gültig waren und wie aktuell die Pläne sind
- Ob kryptografische Schlüssel tatsächlich dabei sind
- Ob Kunden Zugangsdaten und Schlüssel bereits getauscht haben
- Ob jemand die Daten gekauft hat

WAHRSCHEINLICH (Einschätzung)

- Betroffene Kunden prüfen ihre Zugangsdaten zu Video- und Zutrittssystemen und tauschen sie, wo nötig. (60 %) – Bei abgeflossenen Passwörtern ist das Standard in der Incident Response. Öffentlich bestätigt ist es nicht, und Kanton und BCV sehen kein akutes Problem.
- Das Hauptrisiko ist mittelfristig und physisch (Kenntnis von Kamerastandorten und Alarmknöpfen), eine akute Betriebsstörung bei den Kunden ist nicht zu erwarten. (60 %) – Es gibt

keine Berichte über Ausfälle, Ixa meldet keinen Kamerazugriff, der Kanton relativiert die Gefahr. Die Pläne bleiben aber im Umlauf. (A schätzte 55, B 65.)

- Es gab bereits konkreten physischen Missbrauch der Daten (Einbruch, Ausbruch). (3 %) – Dafür gibt es keinerlei Hinweis in Medien oder Behördenaussagen, der Kanton sagt das Gegenteil.

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

WISSEN

- Ixa gibt an, den Zugriff auf seine Daten nie verloren zu haben (Angabe des Unternehmens, berichtet). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- Der Kanton wurde am Tag des Angriffs informiert, sein Security Operations Center (SOC) arbeitet mit dem Unternehmen zusammen; Analyse und Risikobewertung laufen weiter (berichtet). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- ransomware.live beschreibt Ixa als familiengeführten Kleinbetrieb mit etwa 9 bis 10 Mitarbeitenden und rund CHF 3,5 Mio. Umsatz (Aggregator, nicht unabhängig verifiziert). (100 %)

[<https://www.ransomware.live/id/SXhhlFN5c3RlbXNAdGhlZ2VudGxlbWVud>]

NICHT BEKANNT

- Ob und wie lange der Betrieb bei Ixa eingeschränkt war
- Wann die Analyse des Kantons abgeschlossen ist
- Wie weit die Bereinigung bei den Kunden ist

WAHRSCHEINLICH (Einschätzung)

- Die eigene IT von Ixa läuft wieder weitgehend normal (widersprüchlich: A 85 % / B 70 %). (70 %) – Ixa meldet keinen Datenverlust, ein Ausfall wurde nirgends berichtet, seit dem Angriff sind über sieben Wochen vergangen. Belegt ist das nur durch die Angabe des Unternehmens selbst, deshalb der niedrigere Wert.

- Die Bereinigung bei den Kunden (Passwörter, Schlüssel, Pläne, eventuell Anpassungen am Sicherheitskonzept) zieht sich über Wochen bis Monate. (55 %) – Viele Standorte, unterschiedlich stark betroffen; bauliche oder organisatorische Änderungen gehen langsamer als ein Passworttausch. Der Kanton sieht bisher wenig Kritisches, das relativiert den Aufwand. (A schätzte 50, B 60.)

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

WISSEN

- Laut Ixa gab es keinen direkten Zugriff der Angreifer auf Kamerabilder (Angabe des Unternehmens, berichtet). (100 %)

[<https://www.netzwoche.ch/news/2026-10-08/cyberangriff-auf-waadtländer-firma-legt-sensible-sicherheitsdaten-offen>]

- Laut Kanton ergaben die Prüfungen keinen Zugang zur IT-Umgebung des Staates (bestätigt, Behörde, via Le Temps). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

- Barbezat sagt, die Kenntnis der Kameramodelle reiche nicht aus, um eine Schwachstelle auszunutzen; die Angreifer müssten die Geräte auch erreichen können. Er verweist auf die Segmentierung der Systeme (bestätigt, Behörde, via Le Temps). (100 %)

[<https://www.ictjournal.ch/news/2026-10-07/une-cyberattaque-expose-des-donnees-de-securite-de-sites-vaudois>]

NICHT BEKANNT

- Ob Ixa Remote Access oder Fernwartung auf Kundenanlagen hat und ob diese Zugänge betroffen waren, geprüft oder geändert wurden
- Ob irgendwo Hardware getauscht werden muss

WAHRSCHEINLICH (Einschätzung)

- An den Kundenanlagen ist physisch nichts beschädigt; es geht um Informationen, nicht um zerstörte Technik. (85 %) – Alle Berichte sprechen nur von Datenabfluss, weder Ixa noch Kanton noch BCV melden Ausfälle, Ixa schließt direkten Zugriff auf Kamerabilder aus. (A schätzte 90, B

85.)

- Einzelne Kunden passen Teile ihrer Sicherheitskonzepte an (Kamerapositionen, Alarmabläufe). (35 %) – Bei Gefängnissen als Vorsicht üblich, aber öffentlich nicht berichtet und nur bei detaillierten, aktuellen Plänen nötig; bei vielen Kunden lagen laut Bericht nur Ausschreibungen vor.

5. Wie viele solcher Ziele gibt es?

WISSEN

- ransomware.live zählt für die Schweiz 257 öffentlich auf Leak-Seiten gelistete Ransomware-Opfer (Aggregator, Stand Abruf). (100 %) [<https://www.ransomware.live/country/CHE>]
- Check Point zählt bei TheGentlemen über 400 öffentliche Opfer und nennt sie 2026 die zweitaktivste Ransomware-Gruppe weltweit (Stand 13.05.2026, berichtet). (100 %) [<https://blog.checkpoint.com/research/when-the-ransomware-gang-gets-hacked-what-the-gentlemen-leak-reveals-about-modern-ransomware-risk/>]
- Mit Xplain (2023) wurde schon einmal ein kleiner Schweizer Dienstleister zum Einfallstor für Daten von Bundesbehörden (bestätigt, Bundesamt für Justiz). (100 %) [<https://www.bj.admin.ch/de/information-zum-datenabfluss-bei-xplain>]
- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Schweiz: 51891 gesamt (DNP3 15970, ProConOS 14545, EtherNet/IP 14246, Modbus 1887, Siemens S7 635, OPC UA 409) (100 %)

NICHT BEKANNT

- Wie viele Errichter und Integratoren für Sicherheits- und Gebäudetechnik es in der Schweiz gibt
- Wie viele davon Kundenpläne zentral speichern oder Fernzugriff auf Kundenanlagen haben

WAHRSCHEINLICH (Einschätzung)

- In der Schweiz und in DACH gibt es Hunderte kleine Errichter für Video, Zutritt und Alarm mit ähnlich sensiblen Kundenunterlagen und ohne eigenes Security-Team. (75 %) – Der Markt ist kleinteilig, Ixa selbst hat rund zehn Mitarbeitende; Errichter halten zwangsläufig Pläne, Konfigurationen und oft Fernwartungszugänge. Belastbare Zahlen fehlen.

6. Kann das wieder passieren?

WISSEN

- TheGentlemen gehört 2026 zu den aktivsten Ransomware-Gruppen; Check Point beschreibt die Gruppe als schnell wachsendes RaaS (berichtet). (100 %) [<https://www.darkreading.com/threat-intelligence/gentlemen-rapidly-rise-ransomware>]
- Bei Xplain (2023) flossen über einen Dienstleister rund 65.000 Datenobjekte mit Bezug zur Bundesverwaltung ab, darunter Passwörter und technische Informationen (bestätigt, BACS). (100 %) [<https://www.bacs.admin.ch/en/23xplain-en>]
- Im Oktober 2026 wurde mit PK Softech/Publica erneut ein Zulieferer zum Einfallstor für Daten von Bundesstellen (berichtet). (100 %) [<https://www.20min.ch/fr/story/caisse-de-pension-publica-des-donnees-volees-menacent-les-organes-de-securite-de-la-suisse-103651536>]

NICHT BEKANNT

- Welche Maßnahmen Ixa nach dem Angriff konkret umgesetzt hat

WAHRSCHEINLICH (Einschätzung)

- Ein ähnlicher Angriff auf einen Sicherheits- oder Gebäudetechnik-Dienstleister in DACH passiert innerhalb der nächsten 12 Monate erneut. (80 %) – Zulieferer-Fälle häufen sich (Xplain, PK Softech, Ixa), Ransomware-Gruppen wählen Ziele nach Erreichbarkeit, und kleine Firmen haben selten ein SOC.

Lage

Die Ransomware-Gruppe TheGentlemen hat Ixa Systems SA in Crissier Ende August 2026 angegriffen (geschätzt am 28.08.2026) und die Firma am 30.08.2026 auf ihrer Leak-Seite aufgeführt. Ixa plant, installiert und wartet Videoüberwachung, Zutrittskontrolle und

Einbruchmeldeanlagen. Am 25.09.2026 wurden die Unterlagen im Darknet zum Verkauf angeboten. Laut Le Temps sind darunter Pläne, Kamerastandorte, die Anordnung von Alarmknöpfen und teilweise Benutzernamen oder Passwörter von Kunden, etwa Gefängnissen, Gendarmerie-Gebäuden, Banken und mehreren Dutzend Firmen in der Waadt. Ixa sagt, es habe kein Lösegeld gezahlt, den Zugriff auf seine Daten nie verloren, und die Angreifer seien nicht direkt an Kamerabilder gelangt. Der Cybersicherheitsdelegierte des Kantons Waadt hat nach den bisherigen Prüfungen keine Informationen gefunden, die die Sicherheit der betroffenen Standorte gefährden.

Angriff	Ransomware-Angriff mit Datendiebstahl (Double Extortion) auf einen Errichter und Integrator für Video, Zutritt, Einbruchmeldeanlagen und Gebäudeleittechnik. Die Daten wurden auf der Leak-Seite angekündigt und am 25.09.2026 im Darknet zum Verkauf angeboten.
Wann / Status	Ende August 2026 (geschätzt 28.08.2026), Leak-Eintrag 30.08.2026, Verkaufsangebot ab 25.09.2026, Medienberichte ab 07.10.2026 · eingedämmt
Täter	TheGentlemen (Ransomware-as-a-Service) – berichtet
Betreiber / Branche	Ixa Systems SA · Sicherheitstechnik (Planung, Lieferung, Integration, Wartung von Videoüberwachung, Zutrittskontrolle, Einbruchmeldeanlagen; laut Firmenzweck auch Telekom- und Netzwerksysteme)
Anlage / Alter	Integrator/Errichter, kein Anlagenbetreiber. Laut Aggregator auch Gegensprechanlagen, Perimeterschutz, Gebäudeleittechnik und Evakuierungsbeschallung. Kundenanlagen u. a. bei Polizei/Gendarmerie, Justizvollzug, Banken, Spitälern, Schulen · Firma seit 2007 im Handelsregister; Alter der Kundenanlagen unbekannt
Region	Crissier bei Lausanne, Kanton Waadt, Schweiz

Angriffsvektor

Noch nicht bekannt – Hypothesen (Einschätzung):

- HYPOTHESE: Ausgenutzte Schwachstelle in einem Edge Device (Firewall, VPN-Gateway, Appliance), das nicht rechtzeitig gepatcht war. (): Check Point und Trend Micro beschreiben das als häufigsten Einstieg von TheGentlemen (u. a. FortiGate). Für Ixa gibt es keinen Beleg. Zuordnung: CC5 Risk-Based Vulnerability Management.
- HYPOTHESE: Gültige Zugangsdaten für VPN, Remote Access oder Cloud-Konten, gekauft bei einem Initial Access Broker oder aus Infostealer-Logs. (): Laut Check Point der zweite typische Weg der Gruppe; kleine Firmen ohne MFA oder SOC sind dafür anfällig. Kein Beleg für Ixa. Zuordnung: CC4 Secure Remote Access.
- HYPOTHESE: Aus dem Internet erreichbarer Fernzugang (z. B. exponiertes RDP) ohne ausreichende Absicherung. (): Von Sekundärquellen als Einstieg der Gruppe genannt, aber seltener als Edge Devices und Zugangsdaten. Kein Beleg für Ixa. Zuordnung: CC2 Defensible Architecture und CC4 Secure Remote Access.

Früherer Stand: Erstmeldung (07.10.2026 12:08)

Wissen 39 % · wahrscheinlich 26 % · nicht bekannt 35 %

Laut Le Temps (via AWP/cash.ch) hat die Ransomware-Gruppe TheGentlemen Ende August 2026 den Waadtländer Sicherheitstechnik-Errichter Ixa Systems angegriffen und ihn um den 29./30.08.2026 auf ihrer Leak-Site gelistet. Ixa baut Videoüberwachung, Zutrittskontrolle und Einbruchmeldeanlagen. Etwa einen Monat später wurden die erbeuteten Daten im Darknet zum Verkauf angeboten. Darunter sollen Kamerastandorte, Passwörter, kryptografische Schlüssel und Sicherheitspläne von Kunden wie Waadtländer Gefängnissen, Banken, Spitälern und der Polizei sein. Es ist ein Supply-Chain-Fall: Gehackt wurde nicht die Einrichtung selbst, sondern ihr Dienstleister. Zugangsdaten lassen sich tauschen, Gebäudepläne und Kamerastandorte nicht.

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