

Herzlich willkommen

Swisscom KMU Zmorge mit der City Vereinigung Luzern
3. November 2026

AI

Cybersecurity für KMU:

Bereit, wenn die Ransomware zuschlägt



Yves Inderbitzin
KMU IT-Berater

Swisscom (Schweiz) AG
Am Mattenhof 12/14, 6010 Kriens

Ransomware

Eine der grössten Cyber-bedrohungen für Unternehmen: Angreifer stehlen Daten und nutzen Malware, um Daten und Systeme zu verschlüsseln.

Ziel: Geschäftsführung aktiv stören oder mit der Offenlegung gestohlener Daten drohen, um Druck zu erzeugen und so möglichst hohes Lösegeld erpressen.

Angreifer sind nicht interessiert an Ihrem Unternehmen oder am Schaden, den sie anrichten. Es geht nur darum, möglichst viel Geld zu erbeuten.

Was ein Ransomware-Angriff für ein KMU bedeutet



Betriebsstillstand

Ohne Zugriff auf Systeme und Daten steht das Tagesgeschäft still — oft über Tage.



Datenverlust

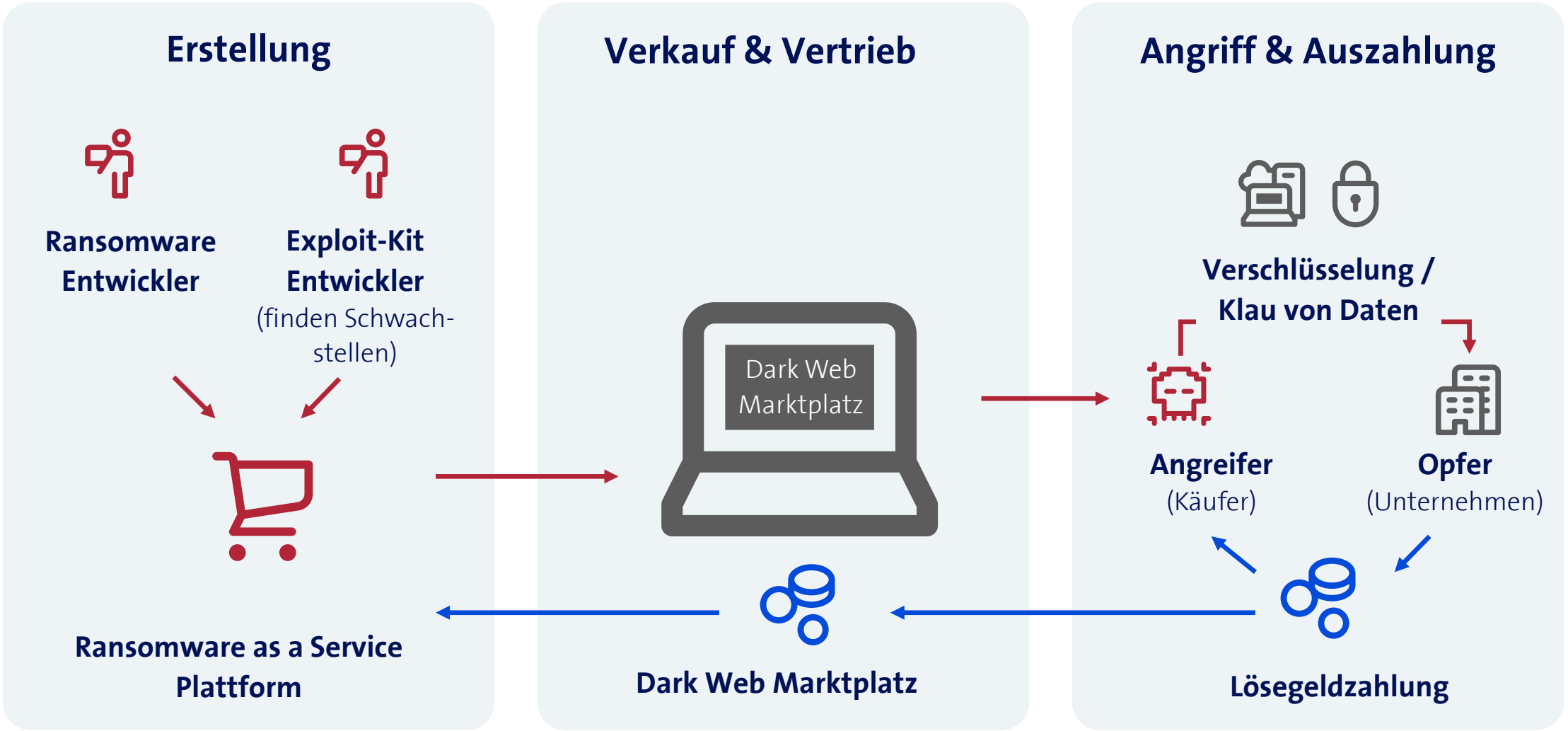
Verschlüsselte oder abgeflossene Daten sind ohne Backup meist unwiederbringlich.



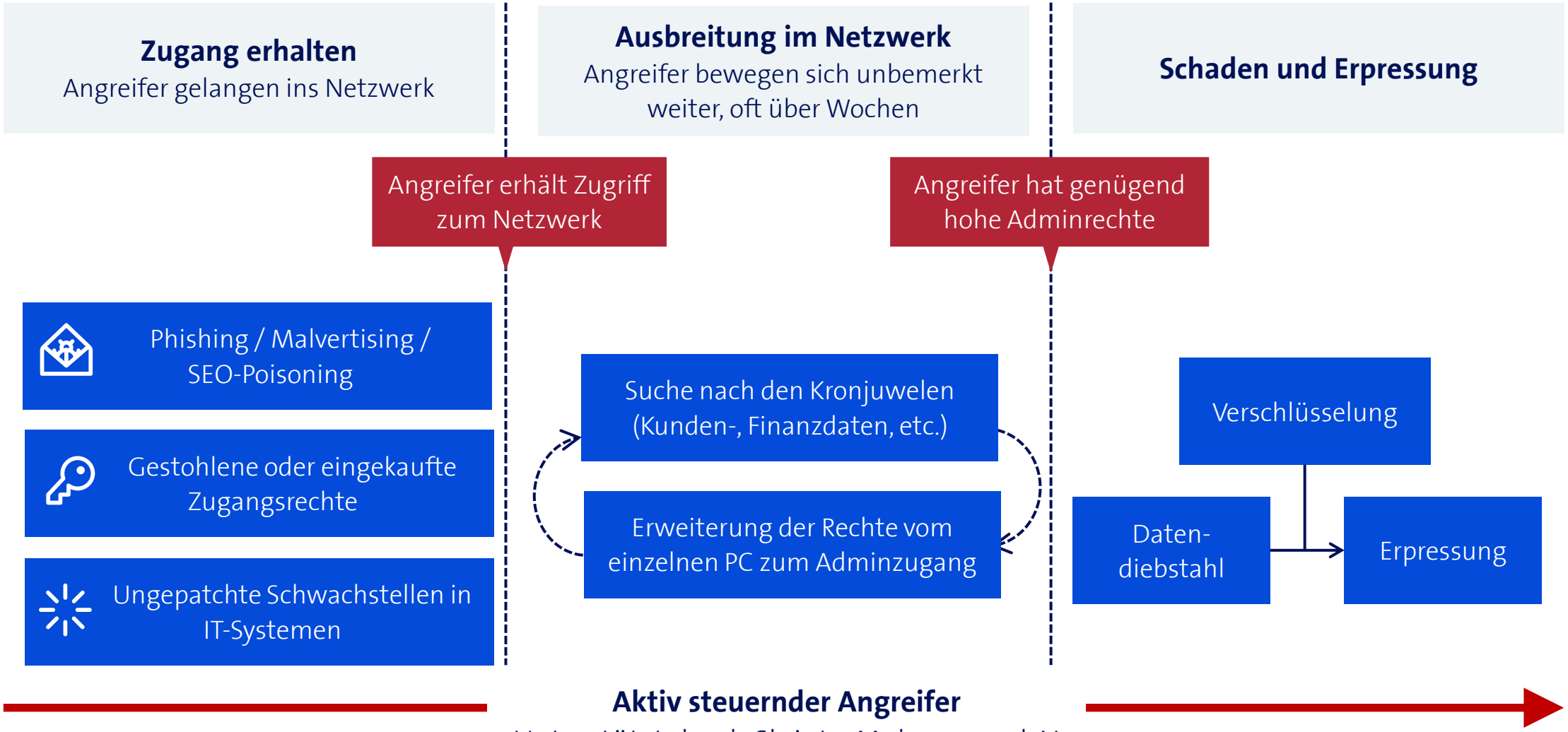
Vertrauensschaden

Kunden, Partner und Behörden erwarten Antworten — die Reputation steht auf dem Spiel.

Hinter den Kulissen – Ransomware as a Service



Ablauf eines Ransomware-Angriffs



Warum Schweizer KMU attraktive Ziele sind

96%

der von Ransomware betroffenen Unternehmen sind KMU.

Das Ziel der Angreifer: möglichst hoher Gewinn bei niedrigem Aufwand.

Was macht Schweizer KMU attraktiv für Angriffe?

Hohe Stillstandskosten
Jede Stunde Ausfall trifft Umsatz, Termine und Vertrauen.

Begrenzte Ressourcen
Security, Backups und Krisen-übungen gehen im Alltag oft unter.

Hohe Zahlungsfähigkeit
Angreifer rechnen eher mit einer Lösegeldzahlung.

Source: 2026 Data Breach Investigations Report, verizon business



Ransomware-Angriff auf einen Dienstleister

50 – 100 Mitarbeitende

Angriffsweg

Angreifer nutzten **schwache Zugangsdaten** für den VPN-Zugang des Unternehmens. Über ein Administratorkonto konnten sie sich im Netzwerk ausbreiten, **Sicherheitsmechanismen deaktivieren und Daten stehlen**.

Y. Inderbitzin, 03.11.26, CVL Zmorge, C2 General

AI

18 Tage Betriebsstillstand

Daten verschlüsselt

Unternehmensdaten wurden gestohlen, verschlüsselt und anschliessend wurden die Systeme mit Ransomware verschlüsselt.

62'000 CHF

Für die Wiederherstellung der IT-Systeme.

Kosten Ransomware-Angriff

Kostenart	%
Lösegeld (falls gezahlt)	15 %
Daten- und Systemwiederherstellung	30 %
Betriebsausfall	30 %
Legal, Bussgelder, Compliance	10 %
Reputationsschaden, Kundenverlust	15 %
Total	**100 %**

- **Kosten schwierig prognostizierbar:** Abhängig von den Auswirkungen auf den Geschäftsbetrieb
- **Erwartbare Erstforderung:** ca. 1–3 % des Jahresumsatzes, mit Verhandlungs -spielraum auf ca. 0,5–1 %
- **Die Kosten, um auf den Angriff zu reagieren,** sind durchschnittlich **5-mal so hoch wie die Lösegeldforderung**

Lösegeld zahlen?

Klare Empfehlung: Nicht zahlen.

Kann aber im Notfall der einzige Ausweg sein, wenn das Bestehen des Unternehmens auf dem Spiel steht.

Unbedingt Spezialisten zuziehen und sich beraten lassen.

Zahlung reduziert Risiken kaum:

- **Meldepflichten** bleiben bestehen
- Trotz Zahlung können **oft nicht alle Daten wiederhergestellt** werden
- Datenlöschung durch den Angreifer ist nicht verifizierbar
- **Erneute Erpressung und Daten-weiterverkauf** kommen trotzdem immer wieder vor

Fazit

Ransomware kann jeden treffen.

Ransomware Banden sind professionell organisiert und versuchen **möglichst viel Geld zu erpressen - mit möglichst geringem Aufwand.**

Je besser man geschützt ist, desto kleiner das Risiko, dass man angegriffen wird

Es geht darum, als Unternehmen resilient gegen Ransomware-Angriffe zu werden.

Resilienz bedeutet: **Angriffe erschweren und damit verteuern — und im Notfall handlungsfähig bleiben.**

Bereit, wenn die Ransomware zuschlägt

Fundament

Ohne funktionierendes Backup nützt alles andere wenig.

Weniger Angriffsfläche

Macht es Angreifern deutlich schwerer.

Vorbereitet sein

Im Ernstfall zählt, was Sie vorher geregelt haben.

1 · Backup

3-2-1-Regel, Restore üben, Business Continuity planen.

2 · Resilienz

Updates, Least Privilege, Passwort-Manager, Phishing-Training.

3 · Notfallprozess

Krisenstab, Plan auf Papier, Kommunikation vorbereiten.

Y. Inderbitzin, 03.11.26, CVL Zmorge, C2 General

Die 3-2-1-Regel für Backups

3×

Kopien

Drei vollständige Kopien aller wichtigen Daten.

2×

Medientypen

Zwei verschiedene Speichermedien, z. B. Server, Cloud oder externe Festplatte.

1×

Ausser Haus

Mindestens eine Kopie offline und offsite, physisch vom Netz getrennt.

Restore üben

Stellen Sie Ihre Backups mindestens einmal pro Jahr testweise wieder her. Ein nie getestetes Backup ist kein Backup.

Zielzeit und Verantwortung

Definieren Sie, wie schnell Sie wieder arbeitsfähig sein müssen und wer für die Wiederherstellung verantwortlich ist.

Y. Inderbitzin, 03.11.26, CVL Zmorge, C2 General

Zwei Hebel, um die Resilienz zu erhöhen

Technik

Automatische Updates auf Servern und Clients

Virenschutz aktiv und aktuell halten

Berechtigungen nach Least-Privilege vergeben

Passwörter im Passwort-Manager

Mensch

Regelmässiges **Phishing-Training**

Klare **Verant-wortlichkeiten**

Wissen, was im **Ernstfall** zu tun ist

Business Continuity: Wenn die IT ausfällt
(Prozess Backup)



E-Mail

Ausweichlösung für den Mailverkehr, damit die Kommunikation nicht abreisst.



Telefonie

Erreichbarkeit sicherstellen, z. B. über Mobilnummern oder einen alternativen Anbieter.



Messaging

Definierter Kanal für die interne Abstimmung, falls die Hauptsysteme stillstehen.

Ihr Krisenstab: vier Rollen (inkl. Stellvertretung)

Entscheidungsträger

Trifft die geschäftlichen Entscheidungen — Zahlungen, Prioritäten, Freigaben.

Kernaufgabe

Entscheiden und freigeben.

Technik-Verantwortliche/r

Kennt die Systeme, koordiniert Eindämmung und Wiederherstellung intern.

Kernaufgabe

Eindämmen und wiederherstellen.

Ransomware-Experte

Interne oder externe Fachperson für die technische Analyse des Angriffs.

Kernaufgabe

Analysieren und beraten.

Kommunikation

Steuert die Kommunikation nach innen und aussen.

Kernaufgabe

Informieren und beruhigen.

Der Notfallplan muss griffbereit sein

Auf Papier ausdrucken

Digitale Pläne sind im Ernstfall verschlüsselt oder nicht erreichbar. Drucken Sie den Prozess aus.

An einem definierten Ort

Der ausgedruckte Plan liegt an einem festen, allen bekannten Ort.

Dem Krisenstab bekannt

Jedes Krisenstab-Mitglied weiss, wo der Plan zu finden ist.

Aktuell halten: Prüfen Sie den Plan mindestens einmal pro Jahr.

Faustregel: Der beste Plan ist wertlos, wenn ihn im Notfall niemand findet.

Wichtig: Wenn die Systeme stillstehen, nützt ein rein digitaler Plan nichts.

Y. Inderbitzin, 03.11.26, CVL Zmorge, C2 General

Kommunikationsvorlagen vorbereiten

Kunden und Partner

Vorbereitete Botschaft, die erklärt, was passiert ist und was Sie tun.

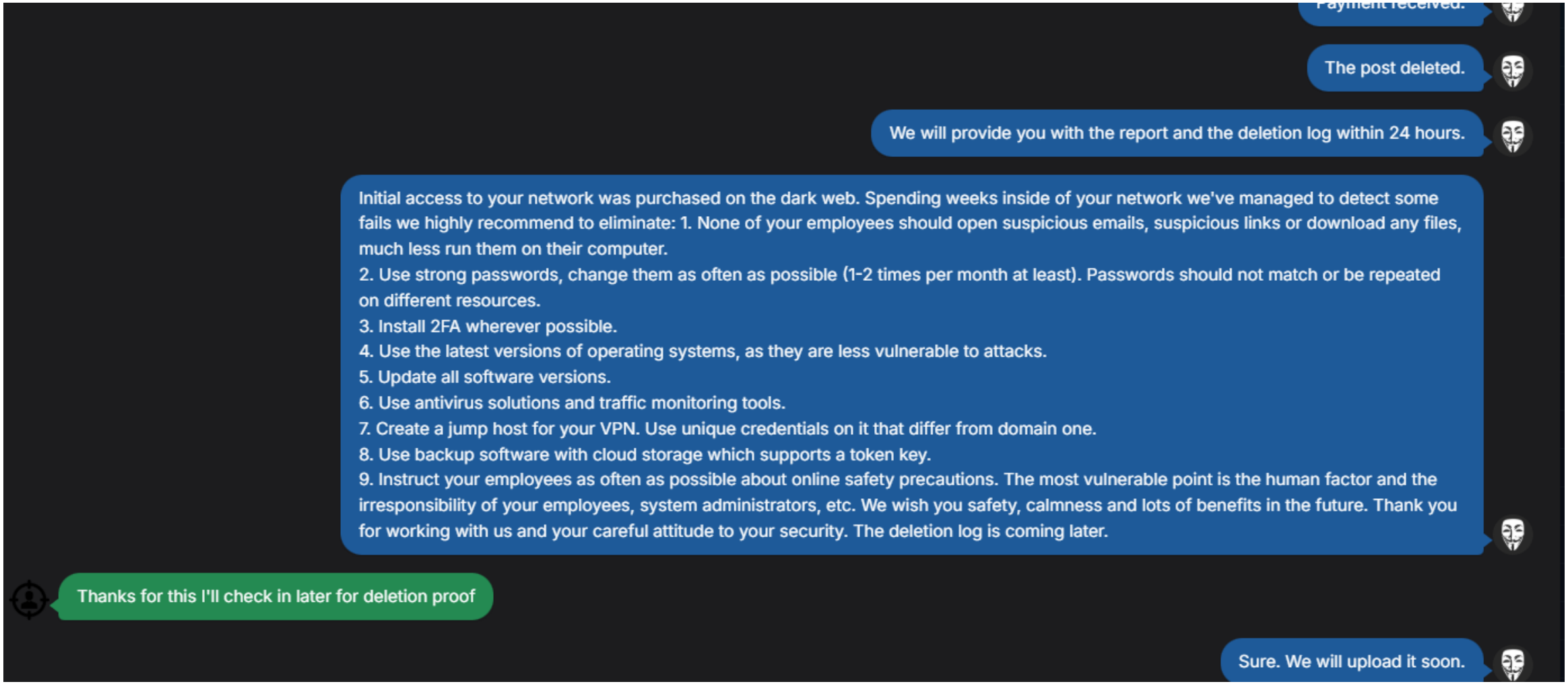
Mitarbeitende

Klare interne Information: was gilt, was zu tun ist, wen man erreicht.

Medien und Behörden

Abgestimmtes Statement für Öffentlichkeit und Meldepflichten.

«Security-Tipps» von Akira



Source: https://ransomware.live/nego/Akira/20230616

Jetzt scannen und anmelden

Videokurs Ransomware

swisscom

Fragen & Antworten

swisscom

Herzlichen Dank!