



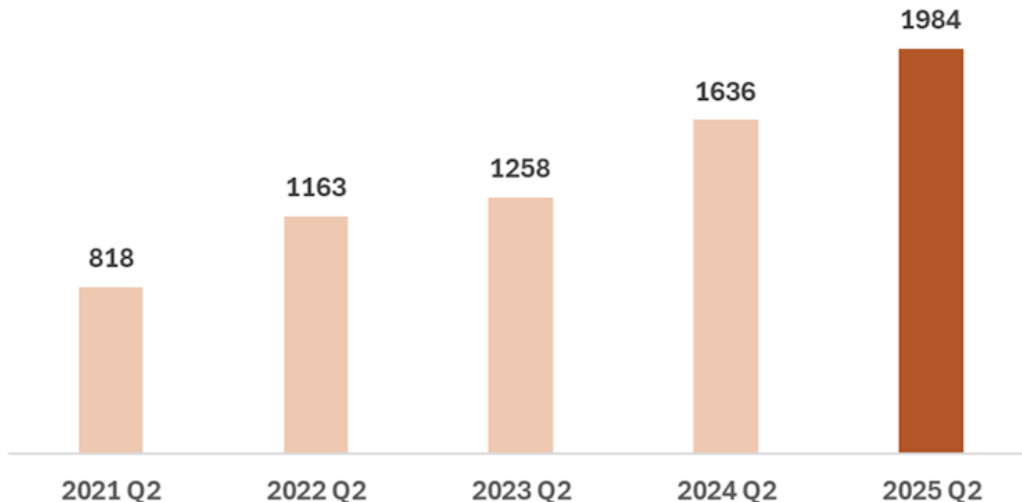
KI IN DER CYBERTHREAT INTELLIGENCE

Cybersecurity Region Stuttgart Meetup bei IHK Stuttgart

Dramatischer weltweiter Anstieg von Cyberangriffen um 21 % im zweiten Quartal 2025

Europa meldet das höchste Wachstum, Steigerung im Vergleich zum Vorjahr um 22 %

Avg. Weekly Cyber Attacks per Organization in Q2
(2021 - 2025)



NIS2 Directive verpflichtet Unternehmen zur Implementierung risikobasierter Cybersicherheitsmaßnahmen und zur Reaktion auf Sicherheitsvorfälle für kritische Netzwerke und Systeme.

Herausforderungen der CTI-Berichterstattung

- KMU fehlt der klare Überblick über die Cybersicherheitslandschaft.
- Die Berichterstattung über Cyberbedrohungen (CTI) ist manuell und zeitaufwändig.
- Die Nutzung mehrerer CTI-Quellen birgt Herausforderungen:
 - Unstrukturierte und inkonsistente Informationen.
 - Stark schwankende Datenmengen.
 - Verschiedene Formate (PDF, JSON, XML).
 - Unterschiedliche Übermittlungskanäle (E-Mail, Newsletter, Abonnements).
- Der Kontext der Bedrohungsdaten fehlt oft.
- Die gewonnenen Erkenntnisse sind häufig nicht umsetzbar, was ihren praktischen Nutzen einschränkt.



CTI-Berichtsphasen



- **Datenerfassung**
 - Rohdaten aus verschiedenen Quellen
- **Normalisierung**
 - Datenbereinigung, -strukturierung und -anreicherung
- **Korrelation**
 - Datenverknüpfung, Mustererkennung, Bedrohungsanalyse
- **Berichterstattung**
 - Weitergabe von handlungsrelevanten Informationen an Stakeholder

Phase 1: Datenerfassung

- API-basierte Datenerfassung (REST, GraphQL, gRPC)
- Abonnement-Endpunkte/Feeds
- E-Mail-Erfassung
- Scrapping Open-Source Intelligence (OSINT)
- Kommerzielle Bedrohungsfeeds (STIX/TAXII, MISP)
- Darknet-/Underground-Quellen
- Bedrohungs-Sharing-Communities



Phase 2: Normalisierung

- Standardisierung von Datenformaten (STIX, TAXII, JSON, CSV)
- Entfernung von Duplikaten und redundanten Einträgen
- Validierung von Indikatoren für eine Kompromittierung (IOCs)
- Anreicherung von Daten mit Kontextinformationen (Geolokalisierung, Informationen zu Bedrohungsakteuren, Malware-Familien)
- Standardisierung von Zeitstempeln und Ereignisreihenfolge
- Kennzeichnung und Kategorisierung von Daten nach Typ, Schweregrad und Quelle



Phase 3: Korrelation



- Verknüpfung von Indikatoren aus verschiedenen Quellen
- Erkennen von Mustern und Trends bei Bedrohungen
- Zuordnung von Bedrohungen zu Angreifern oder Kampagnen
- Abgleich mit internen Protokollen und Warnmeldungen
- Priorisierung nach Schweregrad, Relevanz oder Auswirkung
- Kontextualisierung von Ereignissen mit historischen Daten

Phase 4: Berichterstattung

- Maßgeschneiderte Berichte für Führungskräfte (strategischer Überblick)
- Maßgeschneiderte Berichte für SOC/Analysten (taktische/umsetzbare Details)
- Maßgeschneiderte Berichte für IT-Teams (operative Anleitungen)
- Automatisierte Dashboards und Warnmeldungen
- Bedrohungsbewertung und -priorisierung in Berichten
- Inklusive empfohlener Maßnahmen und Gegenmaßnahmen
- Benutzerdefinierte Formate (PDF, HTML, JSON, E-Mail-Benachrichtigungen)



Cyber-Lagebericht – Stadtwerte / Energiesektor

Berichtsdatum: 14. Januar 2026
Gültigkeit: 24 Stunden
Version: 1.0 | Herausgeber: asvin CTI

Aktuelle Cyber-Risikolage für Stadtwerte

Gesamteinschätzung

Bewertung der aktuellen Lage:  **Erhöht**

Trend:  **(unverändert gegenüber dem Vortag)**

Executive Summary

Die aktuelle Cyber-Risikolage für Stadtwerte im Energiesektor ist weiterhin als erhöht einzustufen. Im Fokus stehen anhaltende Ransomware-Aktivitäten sowie gezielte Phishing-Kampagnen, die sich gegen Betreiber kritischer Infrastrukturen richten.

Im Vergleich zum Vortag wurden keine neuen Eskalationen beobachtet. Die Bedrohungslage bleibt jedoch auf einem erhöhten Niveau, insbesondere im Kontext von IT- und OT-nahen Systemen. Für Stadtwerte ergibt sich daraus aktuell kein akuter Handlungsbedarf, jedoch weiterhin ein erhöhter Bedarf an Aufmerksamkeit und Lagebeobachtung.

Einordnung der aktuellen Lage

Was bedeutet das konkret für Stadtwerte?

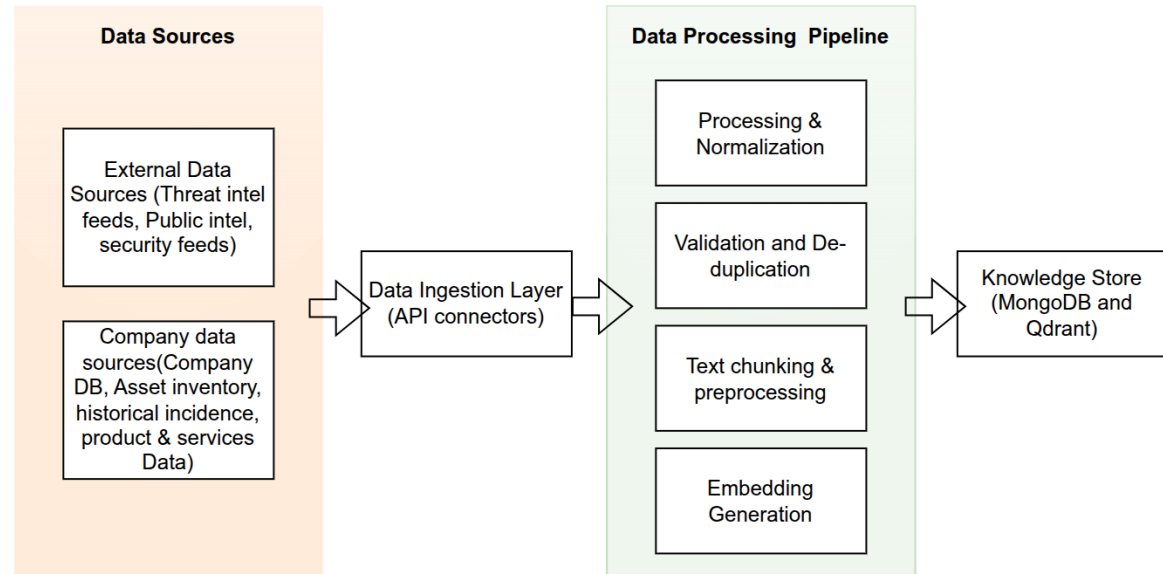
Die beobachteten Aktivitäten zielen vor allem auf Organisationen ab, die eine hohe Betriebsverfügbarkeit sicherstellen müssen und bei denen Ausfälle unmittelbare Auswirkungen auf die Versorgungssicherheit hätten.

Für Stadtwerte bedeutet dies:

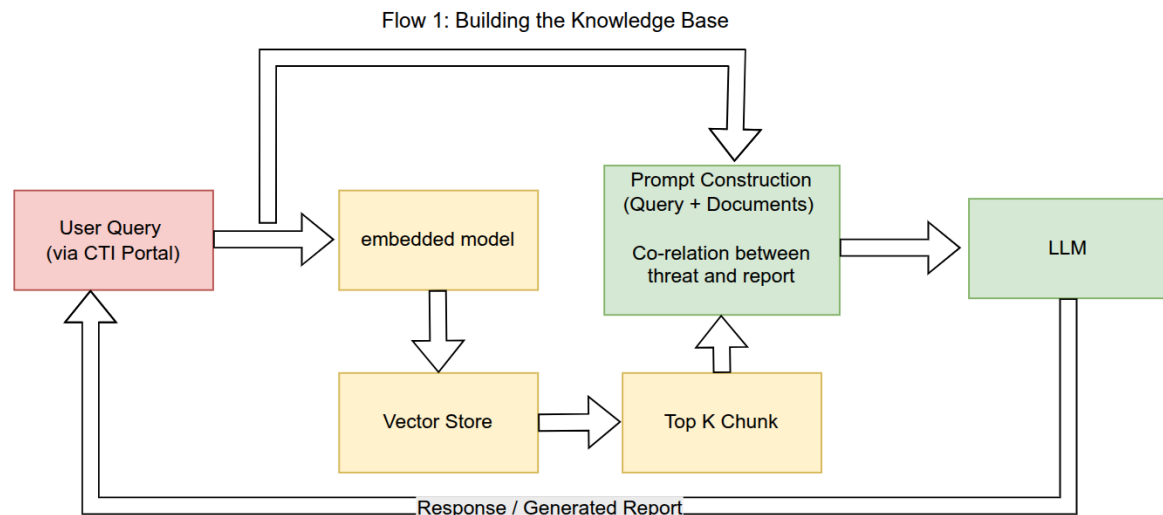
- Cyberangriffe zielen weniger auf Datenabfluss, sondern auf Betriebsunterbrechung
- Angriffe erfolgen häufig indirekt über bekannte, alltägliche Angriffsvektoren
- Die Bedrohungslage ist nicht neu, aber anhaltend präsent

Eine kontinuierliche Einordnung der Lage bleibt daher notwendig, auch bei gleichbleibendem Risikoniveau.

RAG Pipeline



- Wissensdatenbank aufbauen
- Abruf mittels Vektorsuche

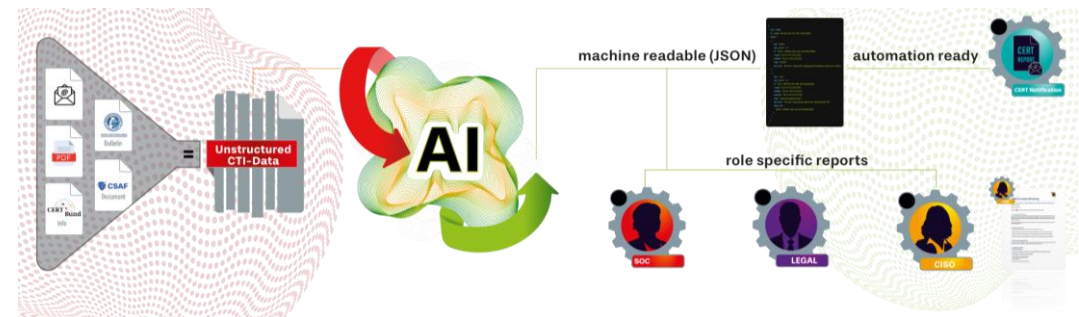


Flow 2: Retrieval from the Knowledge Base

Kontext optimiert Cyber Threat Intelligence (CTI)-Berichte

Die KI-gestützte CTI-Berichterstattung von asvin ermöglicht Automatisierung und Skalierbarkeit für die NIS 2-Konformität in kritischen Infrastrukturen:

- Bedrohungen für die Organisation: z. B. Ransomware- oder Phishing-Angriffe
- Bedrohungen der IT/OT-Infrastruktur durch Schwachstellen
- Bedrohungen durch Lieferanten in der Lieferkette, z. B. Datenlecks



Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026

Gültigkeit: 24 Stunden

Version: 1.0 | Herausgeber: asvin CTI

Aktuelle Cyber-Risikolage für Stadtwerke

Gesamteinschätzung

Bewertung der aktuellen Lage:



Erhöht

Trend:



(unverändert gegenüber
dem Vortag)

Executive Summary

Die aktuelle Cyber-Risikolage für Stadtwerke im Energiesektor ist weiterhin als erhöht einzustufen. Im Fokus stehen anhaltende Ransomware-Aktivitäten sowie gezielte Phishing-Kampagnen, die sich gegen Betreiber kritischer Infrastrukturen richten.

Im Vergleich zum Vortag wurden keine neuen Eskalationen beobachtet. Die Bedrohungslage bleibt jedoch auf einem erhöhten Niveau, insbesondere im Kontext von IT- und OT-nahen Systemen. Für Stadtwerke ergibt sich daraus aktuell kein akuter Handlungsbedarf, jedoch weiterhin ein erhöhter Bedarf an Aufmerksamkeit und Lagebeobachtung.

Einordnung der aktuellen Lage

Was bedeutet das konkret für Stadtwerke?

Die beobachteten Aktivitäten zielen vor allem auf Organisationen ab, die eine hohe Betriebsverfügbarkeit sicherstellen müssen und bei denen Ausfälle unmittelbare Auswirkungen auf die Versorgungssicherheit hätten.

Für Stadtwerke bedeutet dies:

- Cyberangriffe zielen weniger auf Datenabfluss, sondern auf Betriebsunterbrechung
- Angriffe erfolgen häufig indirekt über bekannte, alltägliche Angriffsvektoren
- Die Bedrohungslage ist nicht neu, aber anhaltend präsent

Eine kontinuierliche Einordnung der Lage bleibt daher notwendig, auch bei gleichbleibendem Risikoniveau.

Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026

Gültigkeit: 24 Stunden

Version: 1.0 | Herausgeber: asvin CTI

Zentrale Einflussfaktoren der aktuellen Lage

IT-Systeme	OT / SCADA-nahe Systeme	Lieferketten & Dienstleister
Vermehrte Phishing- und Zugangskampagnen zielen auf Office-IT und VPN-Zugänge ab, um initiale Zugriffe zu erlangen.	Keine Hinweise auf neue, gezielte Angriffe. Dennoch bleibt der Energiesektor im Fokus bekannter Akteure.	Abhängigkeiten von externen IT-Dienstleistern bleiben ein relevanter Risikofaktor, insbesondere bei Fernzugriffen.

Relevante Bedrohungsthemen

Bedrohungsthema	Relevanz für Stadtwerke	Betroffene Bereiche
Ransomware-Kampagnen	● Hoch	IT / OT
Phishing-Aktivitäten	● Mittel	Office-IT
Lieferkettenrisiken	● Mittel	Externe Dienstleister

Kurz-Einordnung der Bedrohungsthemen

Ransomware-Kampagnen

Mehrere bekannte Akteursgruppen richten ihre Aktivitäten weiterhin auf den Energiesektor.

Ziel ist primär die Störung des Betriebs durch Verschlüsselung oder Systemblockaden.

Phishing-Aktivitäten

Aktuelle Kampagnen nutzen thematisch angepasste E-Mails, um Zugangsdaten zu erlangen.

Die Angriffe sind technisch wenig komplex, aber weiterhin effektiv.

Lieferkettenrisiken

Zugriffe über externe Dienstleister und Wartungszugänge stellen weiterhin ein strukturelles Risiko dar.

Cyber-Lagebericht – Stadtwerke / Energiesektor

Berichtsdatum: 14. Januar 2026

Gültigkeit: 24 Stunden

Version: 1.0 | Herausgeber: asvin CTI

Beitrag zur laufenden Risikoanalyse gemäß NIS2

Dieser Bericht unterstützt die laufende Cyber-Risikoanalyse gemäß den Anforderungen der EU-Richtlinie NIS2.

Erfüllte Maßnahmen:

- Regelmäßige Analyse der Bedrohungslage
- Sektorbezogene Bewertung der Relevanz
- Dokumentation der Ergebnisse
- Nachvollziehbare Historisierung

Status: Maßnahme laufend erfüllt | Aktualisierung: täglich

Methodik (Kurzfassung)

Die Bewertung basiert auf der Analyse kuratierter externer Cyber-Threat-Intelligence-Quellen mit Fokus auf den Energiesektor.

Die Einordnung erfolgt qualitativ unter Berücksichtigung von:

- beobachteten Aktivitäten
- sektoraler Relevanz
- bekannten Angriffsmustern

Nicht Bestandteil dieser Analyse sind:

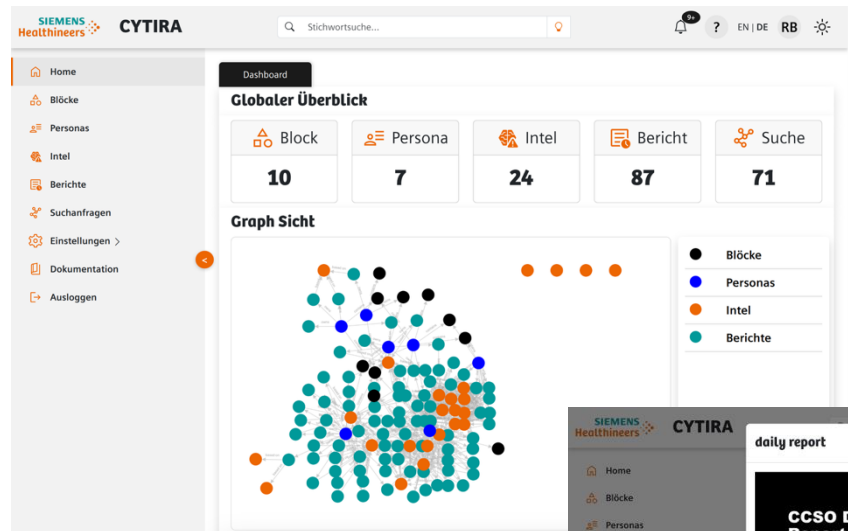
- interne Systemdaten
- individuelle Schwachstellenbewertungen
- operative Sicherheitsmaßnahmen

Transparenz & Zweck des Berichts

Dieser Bericht dient der regelmäßigen Information über die Cyber-Bedrohungslage im Energiesektor und der Unterstützung der organisatorischen Risikoanalyse. Er ersetzt keine operativen Sicherheitsmaßnahmen und stellt keine Handlungsempfehlung im Einzelfall dar.

Referenz-ID: ASV-CTI-ENERGY-2026-01-14
Vertraulichkeit: Intern
© asvin GmbH

SHS Case Study



View Persona

Title: Corporate Cybersecurity Officer

CCSO

Beschreibung: It oversees the protection of corporate digital assets, products, and data across all business units and global offices. It ensures that cybersecurity aligns with corporate governance, compliance, and strategic business operations.

Key Responsibilities:

- Develop and enforce global cybersecurity strategy, policies
- Implementation of targeted awareness and training programs for all employees and specific Cybersecurity roles
- provisioning of a Cybersecurity Management System
- Report cybersecurity state of security resilience and posture Management Board and the Risk Committee

Auswählen Blöcke

Suchen: Anzahl: 10

- Threat Lan...** (2)

The chapter on the threat landscape should provide a clear, structured analysis of a specific threat or campaign. It should have following sections as...
- Geopolitic...**

The Geopolitical Intelligence chapter examines cyber threats driven by nation-state conflict, political tensions, or global instability. It analyzes r...
- Brand Inte...**

The Brand Intelligence chapter focuses on identifying and analyzing threats that exploit or damage an organization's brand across digital channels inc...

daily report

CCSO Daily - Threat Intel Report

daily report

Executive Summary

This report provides an overview of the current cybersecurity landscape, outlining key incidents, emerging threats, and trends relevant to corporate digital assets. The purpose of this report is to inform stakeholders about potential risks and provide actionable insights to enhance our security posture. It covers incidents from February 2025 to November 2025, analyzing events ranging from ransomware attacks to software supply chain compromises and critical vulnerability disclosures.

Recent events demonstrate an escalating sophistication of cyberattacks, including the exploitation of software supply chains and critical vulnerabilities. The Shi-Hulud campaign targeting NPM packages, coupled with the ongoing threat of ransomware groups like Medusa, highlight the need for robust supply chain security and proactive vulnerability management. The incident involving Medusa and Microsoft underscores the potential for significant data breaches.

Schließen Herunterladen

Analysis Summary

document_overview (3)

executive_summary Between February and April 2025, Marks & Spencer (M&S) experienced a prolonged ransomware attack disrupting core retail operations, online services, and internal logistics systems. The incident resulted in extended service outages, significant revenue loss, and reputational damage. The attack highlights the need for continuous monitoring, rapid credential containment, and resilience planning to sustain operations during prolonged cyber incidents.

incident_occurred_at: 2025-02-01T00:00:00Z

source_url: null

target_sector: Retail

finding_register (6)

cve_analysis (0)

remediation_backlog (0)

compliance_mapping (2)

Schließen



THANK YOU FOR YOUR TIME



Rohit Bohara

CTO

r.bohara@asvin.io

asvin GmbH

Stuttgart, Germany

www.asvin.io

contact@asvin.io