

10. Juli 2026 | 09:30 – 13:00 Uhr

Systeme zur Erkennung von Cyberangriffen für Versorger

Wie erkennen Versorger Cyberangriffe frühzeitig – und wie viel ist regulatorisch tatsächlich erforderlich? Dieses Webinar ordnet die Vorgaben aus dem IT-Sicherheitsgesetz 2.0 ein und zeigt, welche technischen und organisatorischen Ansätze sich in der Praxis bewähren. Sie erhalten eine belastbare Entscheidungsgrundlage für den Aufbau oder die Weiterentwicklung Ihrer Angriffserkennung.

Ihr Nutzen

Die Teilnahme an diesem Webinar unterstützt Sie dabei, Systeme zur Erkennung von Cyberangriffen rechtssicher und praxisnah in Ihrem Unternehmen einzuordnen und weiterzuentwickeln.

Sie erhalten ein klares Verständnis der Anforderungen aus dem IT-Sicherheitsgesetz 2.0, zu den Erfahrungen aus der Praxis sowie der Erwartungen von Aufsicht und Prüfern.

Anhand typischer Einsatzszenarien in IT- und OT-Umgebungen wird aufgezeigt, welche technischen und organisatorischen Lösungsansätze realistisch, verhältnismäßig und wirksam sind. Damit gewinnen Sie eine belastbare Grundlage, um den Reifegrad Ihrer Angriffserkennung fundiert zu bewerten und strategisch sinnvolle Entscheidungen für den Schutz Ihrer kritischen Infrastrukturen zu treffen.

Inhalt

Einordnung und Zielsetzung

- Zunehmende Bedrohungslage durch Cyberangriffe auf Versorgungsunternehmen
- Bedeutung von Angriffserkennung im Kontext des IT-Sicherheitsgesetzes 2.0

Regulatorischer Rahmen: Angriffserkennung nach IT-SiG 2.0

- Gesetzliche Anforderungen an Systeme zur Angriffserkennung (§5c EnWG)
- Vorgaben des BSI und der ISO/IEC 27001
- Umsetzungsfristen

Angriffserkennung in der Praxis von Versorgungsunternehmen

- Phasen eines Hacker-Angriffs
- Bedrohungsszenarien in IT- und OT-Umgebungen
- Technische und Organisatorische Maßnahmen zur Angriffserkennung

Technische Ansätze und Systemarchitekturen

- Implementation der SzA bei Energie- und Wasserversorgern
- Vor- und Nachteile interner, externer und hybrider Betriebsmodelle

Fortsetzung auf Seite 2

Technische Voraussetzung

Das Webinar wird durchgeführt über „Microsoft Teams“. Für die Einwahl zum Webinar erhalten Sie einen Link. Nutzen Sie bitte bevorzugt die Teams-App, insbesondere falls Sie keinen Google-Chrome- bzw. Microsoft-Edge-Browser verwenden. Verwenden Sie nicht den Firefox-Browser. Für gesprochene Beiträge benötigen Sie ein Mikro. Die Einwahl über Telefon ist aber ebenfalls möglich.

Preise und Anmeldung

280,-- Euro zzgl. MwSt. für VBEW/BDEW Mitglieder,
390,-- Euro zzgl. MwSt. für Nichtmitglieder.

Anmeldung bitte bis spätestens 03.07.2026.
Den Link zum Webinar erhalten Sie eine Woche vor der Veranstaltung.
Die Stornobedingungen finden Sie im Anmeldeformular auf unserer Homepage.

Zielgruppe

Das Webinar richtet sich an die Geschäftsleitung sowie an Fach- und Führungskräfte von Versorgungsunternehmen, die für IT- und OT-Sicherheit, Cyberabwehr oder die Umsetzung der Anforderungen aus dem IT-Sicherheitsgesetz 2.0 verantwortlich sind.

Vorkenntnisse sind hilfreich, aber nicht zwingend erforderlich.

Kontakt

Kathrin Knogler
Leiterin Veranstaltungen

Tel. 089 38 01 82-65
Mail vbew-gmbh@vbew.de

Reifegrade, Prüfung und Nachweisführung

- Verständnis und Einordnung von Reifegradmodellen
- Erwartungshaltung von Aufsicht, Prüfern und Behörden
- Praktische Ansätze zur dokumentierten und verhältnismäßigen Umsetzung

Erfahrungen aus der Praxis und Marktüberblick

- Typische Herausforderungen bei Einführung und Betrieb
- Umgang mit begrenzten personellen und finanziellen Ressourcen
- Rolle spezialisierter Dienstleister und Marktteilnehmer

Handlungsempfehlungen und nächste Schritte

- Standortbestimmung im eigenen Unternehmen
- Realistische Zielbilder für unterschiedliche Unternehmensgrößen
- Kurz-, mittel- und langfristige Umsetzungsschritte

Beantwortung von Fragen aus dem Chat

Dozent

Dr. Stefan Kreml ist Berater und freiberuflicher Lead-Auditor für die TÜV Rheinland Cert GmbH. Er ist auf Normen und Anforderungen wie ISO/IEC 27001, IT-Sicherheitskatalog und KRITIS spezialisiert und als zugelassener Fachexperte für Netzbetreiber tätig.

Als Lead-Auditor (ISO/IEC 27001, ISO 9001, ISO 22301), Auditor nach § 8a BSI-G sowie Fachexperte nach § 11 EnWG hat er zahlreiche Projekte für Versorger erfolgreich begleitet. Zudem ist er Datenschutzbeauftragter (IHK) und Datenschutzauditor nach ISO/IEC 27701. Er verbindet fundiertes Normenwissen mit praxisnahen Lösungen und vermittelt Inhalte klar und verständlich – auch in seinen Fachvorträgen.

Ablauf

| | |
|----------------------------|-------------------|
| Technikcheck und Begrüßung | ab 09:00 Uhr |
| Beginn | 09:30 Uhr |
| Pause | 11.00 - 11:15 Uhr |
| Ende | gegen 13:00 Uhr |