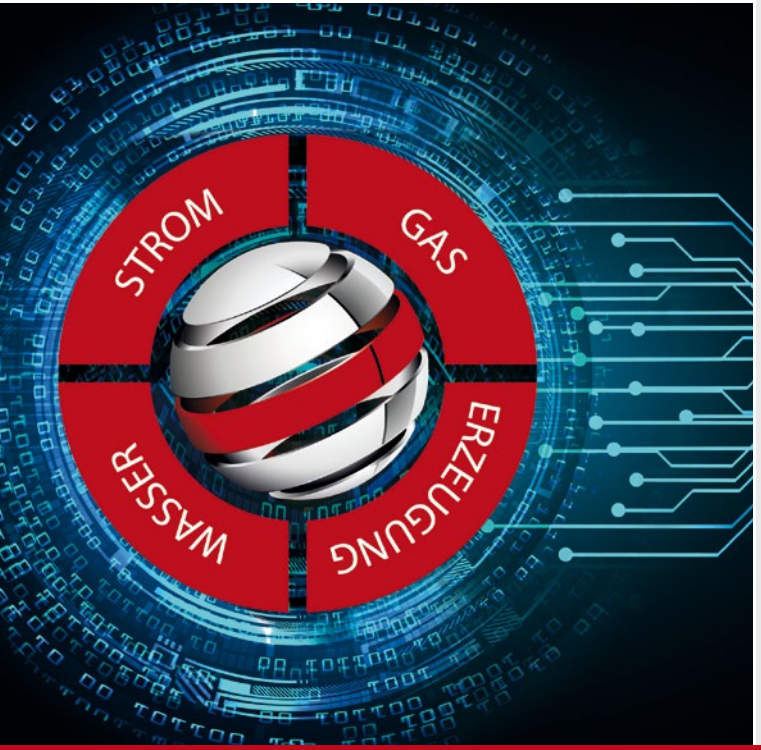
KRITIS Defender.

# KRITIS Defender
## Intrusion Detection System für Leittechnik

**Detektion von meldepflichtigen Angriffen**




www.ausecus.com

## KRITIS DEFENDER – IHRE VORTEILE

- Der **KRITIS** Defender agiert rein passiv im Netzwerk
- Frühzeitige Erkennung von Ereignissen und Sicherheitsvorfällen – echte Verbesserung für Ihre IT-Sicherheit
- Absolute Verlässlichkeit in der Erkennung, minimalste Quote von falsch-positiven Ereignissen durch einen regelsatzbasierten Ansatz
- Fernwartung nach Stand der Technik und nur nach expliziter Freigabe von Ihrer Seite
- Tiefgreifende fachliche Unterstützung bei der Aufklärung von Sicherheitsvorfällen durch unsere erfahrenen Netzwerksicherheitsexperten
- Konformität zur Meldepflicht (§8 BSIG) und zum IT-Sicherheitskatalog (EnWG)
- Nachweise der kontinuierlichen Verbesserung Ihres ISMS
- Langjähriges Know-How von ausecus aus der Praxis bei KRITIS Betreibern, Stadtwerken, EVUs, Kraftwerken und Wasser-/Abwasserunternehmen
- Herstellerunabhängige IT-Security – Made in Germany

## KONTAKT

### Erfahrung aus der Praxis

Unsere Mitarbeiter bringen langjährige Erfahrung mit ISMS und aus der IT-Sicherheit Leittechnik bei Stadtwerken, Energieversorgern, Kraftwerken, Wasser- ver- und Entsorgungsunternehmen sowie aus der Industrie mit.

Mit dem **KRITIS** Defender steht Ihnen eine effiziente Lösung zur Verfügung, die selbst die fortschrittlichsten Angriffe detektieren kann, ohne in die Verfügbarkeit Ihres Leitsystems einzugreifen.

Zudem schaffen Sie einen wesentlichen Sicherheitsfaktor, der für den Angreifer unerkannt bleibt und selbst dann noch funktioniert, wenn Firewall oder Virenscanner bereits umgangen wurden.

**ausecus GmbH**
Werner-von-Siemens-Straße 6
D-86159 Augsburg
Tel. +49 / 821 / 20 70 97 - 0
Fax +49 / 821 / 20 70 97 - 99

**info@kritis-defender.de**
**www.kritis-defender.de**

**info@ausecus.com**
**www.ausecus.com**

SecurITy made in Germany
Trust Seal www.teletrust.de/itsmig

Quellennachweis: Fotolia, Stadtwerke München, TeleTrusT

## KRITIS Defender als Intrusion Detection System für Ihre Leittechnik

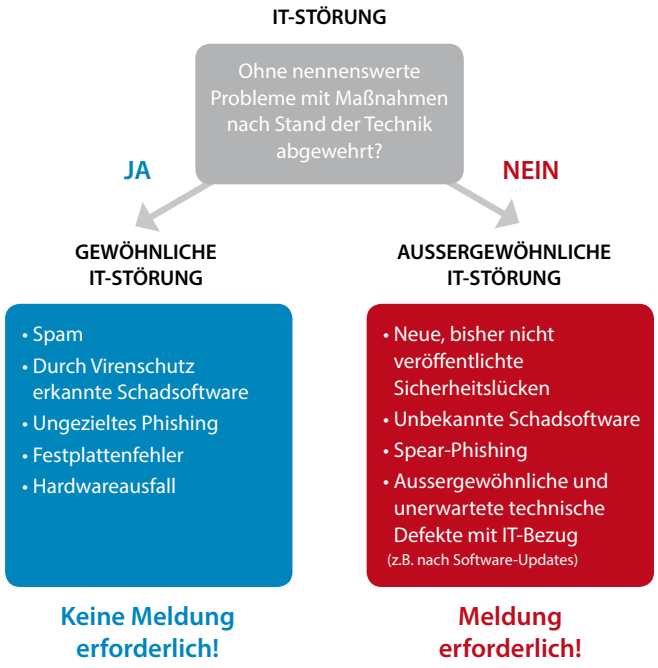
Erfolgreiche Hackerangriffe bleiben zu Beginn unentdeckt, da konservative Detektionsmechanismen nur bereits bekannte Angriffsmuster erkennen können. Moderne Angriffsmuster lassen sich meist mit bestehenden Mechanismen nicht erkennen. Dafür gibt es Intrusion Detection Systeme, die Netzwerkdaten sammeln, analysieren und anormales Verhalten im Netzwerk erkennen.

Der **KRITIS** Defender ist ein Intrusion Detection System für Leittechnik, das spezifisch auf die Bedürfnisse von Kritischen Infrastrukturen wie Stadtwerke, Energieversorger, Kraftwerke, Wasserversorger und Abwasserunternehmen angepasst ist. Protokolle wie IEC-104 werden in der Tiefe analysiert und Sie erkennen dadurch neben Sicherheitsvorfällen im Leitsystem und der DMZ auch Sicherheitsvorfälle in den Prozess- und Fernwirknetzwerken. Zusätzlich zu den Standard-Detektionsregeln sind alle BSI-Meldungen aus den letzten Jahren mit Regelsätzen hinterlegt.

Der **KRITIS** Defender bereitet die erkannten Vorfälle übersichtlich auf und hilft durch die gespeicherten Informationen sowohl bei der Analyse von Ursachen von Vorfällen als auch bei der Entscheidung, ob ein meldepflichtiger Vorfall gegenüber dem BSI vorliegt.

## Meldepflicht von IT-Störungen an BSI

Im IT-Sicherheitsgesetz ist festgelegt, dass IT-Störungen an das BSI zu melden sind, die zu einem Ausfall der Kritischen Infrastruktur geführt haben oder führen könnten. Vom BSI wurde festgelegt, dass aussergewöhnliche IT-Störungen immer zu melden sind, unabhängig ob ein Versorgungsausfall stattgefunden hat oder nicht.




Meldepflichtig sind alle Betreiber Kritischer Infrastrukturen oberhalb der Schwellenwerte. Zudem sind alle Strom- und Gasversorger meldepflichtig, unabhängig von Ihrer Unternehmensgröße.

Außergewöhnliche IT-Störungen können nicht mit Standard-Technologien wie Virenscannern oder Firewalls erkannt werden. Die Melde- und Erkennungspflicht von solchen Störungen bedeutet, dass fortgeschrittene Erkennungstechnologien wie „Intrusion Detection" verwendet werden müssen. Diese entsprechen auch dem „Stand der Technik".

### Wartung und Service

KRITIS Defender.

Der **KRITIS** Defender wird durch die zugehörige Wartung und den damit verbundenen Service gepflegt. Sie erhalten Updates der Regelsätze bei Meldungen von BSI, CERTs, Herstellern und aus einschlägigen Schwachstellendatenbanken.

Bei Änderungen in Ihrem Netzwerk oder Ihrer Infrastruktur werden diese Änderungen durch unsere kompetenten Mitarbeiter in Ihrem **KRITIS** Defender nachgepflegt und für Sie individuell angepasst. Damit ist Ihr **KRITIS** Defender stets auf dem aktuellen Stand.

## IT-SiG 2.0: Einsatzpflicht von Systemen zur Angriffserkennung

In der für 2019 bevorstehenden Überarbeitung des IT-Sicherheitsgesetzes (IT-SiG 2.0) wird vom Gesetzgeber im Entwurfstext der Einsatz von Systemen zur Angriffserkennung für allle Betreiber von Kritischen Infrastrukturen als verpflichtend festgeschrieben.

**Updates** von Regelsätzen nach Meldungen des BSI, von CERTs und Schwachstellen

**Wartung und Service**, Anpassung auf neue Gegebenheiten im Netzwerk, Individualisierung

**Analyse** von Sicherheitsvorfällen und Unterstützung bei der Bewertung von Vorfällen