



KRITISCHE INFRASTRUKTUREN

SYSTEM ZUR ANGRIFFSERKENNUNG – EINFACH GELÖST

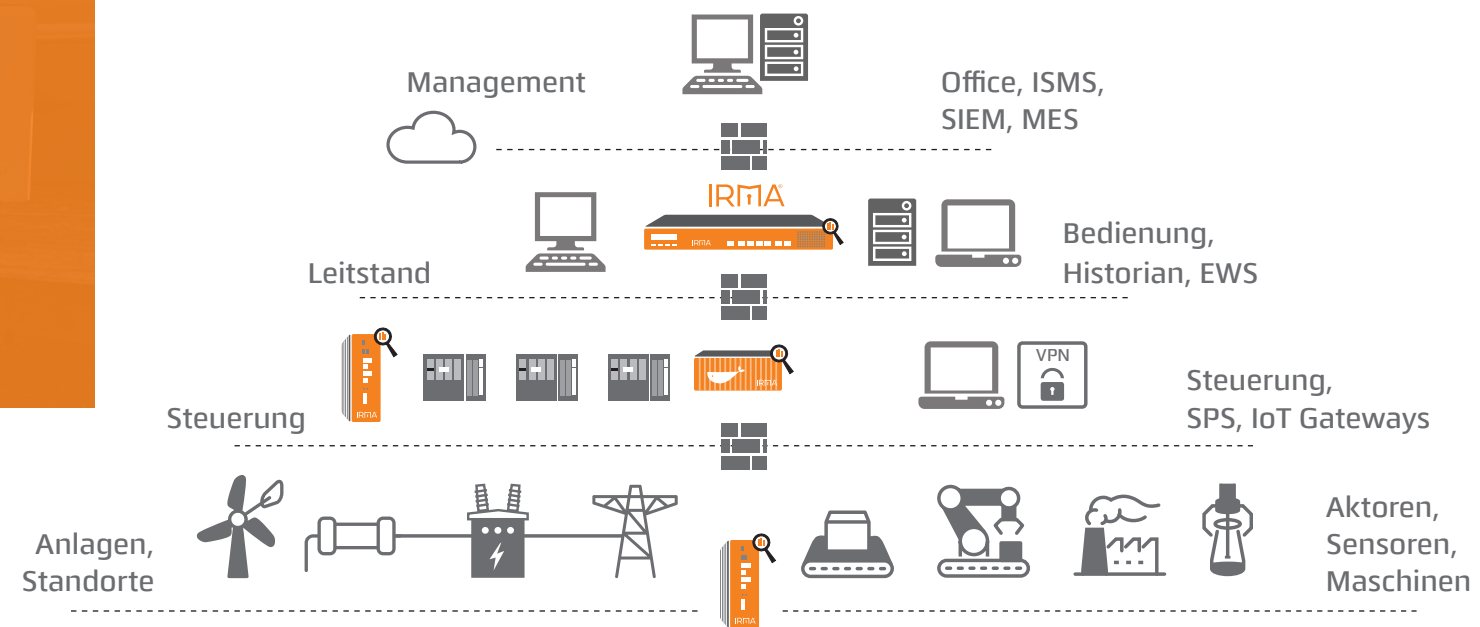


- ITSiG 2.0 / BSI-KritisV / ENWG
- Die richtige Protokollierung, Detektion und Reaktion für die KRITISCHE DIENSTLEISTUNG
- Beratung, Evaluierung, Einführung und langfristige Unterstützung

FÜR ALLE ENERGIEVERSORGER. STROM, GAS, ÖL ODER FERNWÄRME

Das IT-Sicherheitsgesetz 2.0 (ITSiG 2.0) hat konkretisiert, dass Betreiber KRITISCHER INFRASTRUKTUREN verpflichtet sind zum 1. Mai 2023 ein System zur Angriffserkennung (SZA) einzusetzen.

Mit dem IRMA® SYSTEM erreichen Sie Stufe 3 für ihre KRITISCHE DIENSTLEISTUNG, VERNETZTE AUTOMATISIERUNG (OT), NETZLEIT- oder FERNWIRKTECHNIK.



Die Rahmenbedingungen

Für die Umsetzung der organisatorischen und technische Maßnahmen eines Systems zur Angriffserkennung wurden die Maßnahmen in der Orientierungshilfe des BSI konkretisiert. Dabei müssen die Systeme durch fortlaufende Auswertung (Protokollierung) der gesammelten Informationen sicherheitsrelevante Ereignisse (SRE) erkennen (Detektion). Dies kann durch muster- und anomaliebasierte Erkennung durch ein netzbasiertes Detektionssystem erfolgen. Um die Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion), sind weitere Maßnahmen gefordert.

Das Ziel ist die Absicherung der KRITISCHEN DIENSTLEISTUNG

Der Einsatz von SZA muss die informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, abdecken. Dies bezieht sowohl IT als auch OT sowie Rechenzentren oder Embedded Systems und schließt weitere Bereiche mit ein.

Die Lösung: IRMA®

IRMA® ist das technische System zur Angriffserkennung für die KRITISCHE DIENSTLEISTUNG.

- Muster- und anomaliebasierte Erkennung als netzbasiertes Detektionssystem für OT und IT
- Alarmierungsfunktion bei einer Angriffserkennung

Die Funktionen sind einfach zu bedienen, die Parametrierung systemgeführt zu erlernen. IRMA® erkennt das Verhalten von Angreifern und schützt Ihre ungesicherten Geräte und Protokolle unabhängig vom Standort vor Angriffen.

Einfach – sicher – kompetent

VIDEC bietet 30 Jahre Expertise im Bereich Automatisierung gepaart mit umfassendem Erfahrungswissen in Beratung und Umsetzung sowie tiefem Branchen-Knowhow in allen KRITIS Bereichen.

Ob für Energienetzverteiler, Kraftwerksbetreiber oder Stadtwerk, on- bzw. offshore Windanlagen oder Industrieunternehmen verschiedenster Branchen.

Unser Konzept – Ihr Vorteil

ALS PARTNER UNTERSTÜTZEN WIR SIE

- Planung und Betrieb der SzA
- Konzeption und Inbetriebnahme
- Implementierung zur fristgerechten Umsetzung
- Webbased Infomaterial in der Mediathek
- Checklisten aller Anforderungen der Orientierungshilfe verfügbar
- Vielzahl qualifizierter Partner

MIT IRMA[®] ERREICHEN SIE EINFACH UND SICHER DIE ZIELE ZUR UMSETZUNG

- Tiefes Branchen-Knowhow in allen KRITIS Bereichen
- Schneller Einstieg durch Begleitung in der Einführungsphase und angepasste Schulungskonzepte
- Sicherer Betrieb durch technische Unterstützung, Updatekonzepte und gestaffelte Supportpakete
- Telefon- und Mailsupport

Sie wollen weitere Informationen zu OT Security und KRITIS – gerne.



Mit Videos,
Online Seminaren,
Infopapers, Checklisten
Erfahrungsberichten

Besuchen Sie unsere Webseite unter www.videc.de/irma/ oder rufen Sie uns an.



VIDEC Data Engineering GmbH
Contrescarpe 1 · DE-28203 Bremen · Phone +49(0)421 – 33 950-0 · info@videc.de · www.videc.de
Niederlassungen und internationale Vertretungen entnehmen Sie bitte unserer Webseite.

Es gelten die AGB der VIDEC Data Engineering GmbH | IRMA[®] ist ein Produkt der ACHTWERK GmbH & Co KG. Alle Rechte vorbehalten.

