VIVAVIS

DECODING THE FUTURE

Starkes Immunsystem für kritische Infrastrukturen mit IRMA® und VIVAVIS: System zur Anomalieerkennung nach IT-SiG 2.0

Hintergrund

Als Netzgesellschaft sind Sie Betreiber kritischer Infrastrukturen (nach EnWG § 11 1d). Damit besteht für Sie nach IT-Sicherheitsgesetz 2.0 folgende Verpflichtung: Die Implementierung eines Systems zur Anomalieerkennung in Ihre Netzleittechnik bis zum 01. Mai 2023.

Diese Systeme müssen kontinuierlich, im laufenden Betrieb und mittels Mustern Bedrohungen erkennen und vermeiden. Damit gelten sie als effektive Maßnahme, um den durch Cyberangriffe entstehenden Schaden frühzeitig zu verhindern.

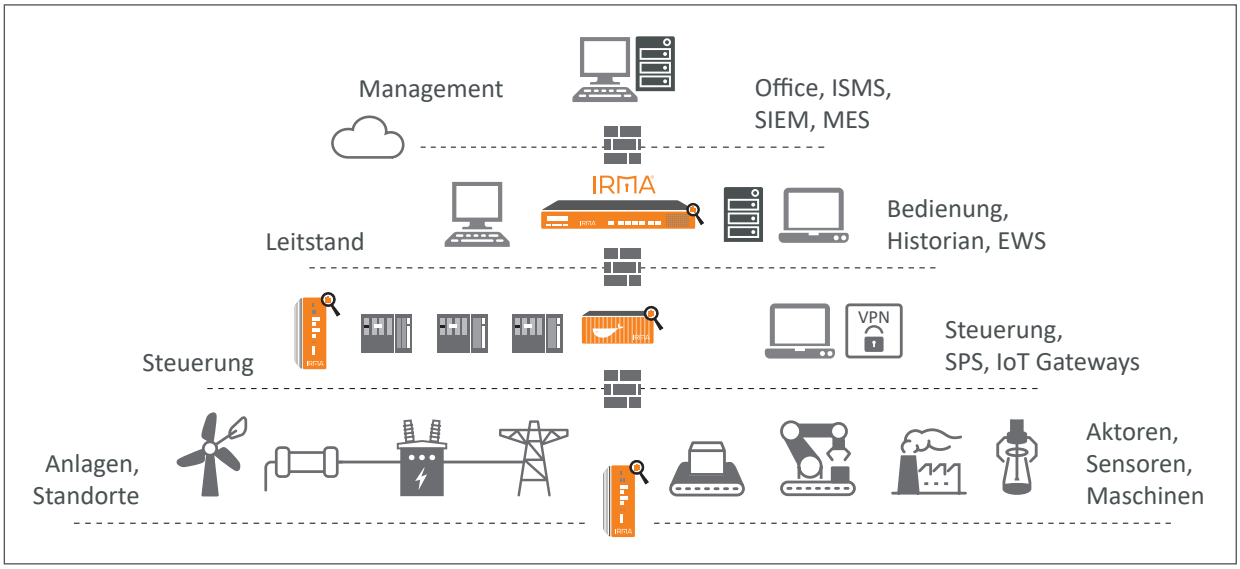
Unsere Lösung

VIVAVIS unterstützt Sie bei der Umsetzung der Anforderungen und setzt dabei auf die Lösung IRMA® (Industrie-Risiko-Management-Automatisierung). Mit IRMA® können Sie auf eine leistungsfähige Lösung zurückgreifen, mit der Cyberangriffe schnell identifiziert und abgewehrt werden können.

Dabei handelt es sich um ein Operation-Technology-Security-Produkt made in Germany. Es entspricht den IT-SiG-Anforderungen für KRITIS-Betreiber und ermöglicht die technisch-organisatorische Einbindung zur Erkennung von Angriffen auf informationstechnische Systeme. IRMA® erfüllt bereits von Anfang an die Empfehlungen des BSI-CS134 für Monitoring und Anomalieerkennung in Netzwerken sowie den BSI-Leitfaden zur Einführung von Intrusion-Detection-Systemen. Die Funktionen bestehen im Wesentlichen aus:

- der Anomalieerkennung im Netzwerk
- einer Alarmierungsfunktion bei einer Angriffserkennung und
- einem integrierten Risikomanagement.

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



Umsetzung

Aus der Orientierungshilfe des BSI ergeben sich seitens der Funktionalität drei wesentliche Aufgabenbereiche: Protokollierung, Detektion und Reaktion. IRMA® erkennt durch fortlaufende Auswertung (Protokollierung) der gesammelten Informationen sicherheitsrelevante Ereignisse (Detektion). Dies erfolgt durch die muster- und anomaliebasierte Erkennung, welche dazu verhilft, Störungen infolge von Angriffen zu verhindern oder auf sie zu reagieren (Reaktion). Somit können Sie durch geeignete Eingriffe eine relevante Beeinträchtigung der kritischen Infrastruktur vermeiden.

Implementierung mit VIVAVIS

Wir verhelfen Ihnen Schritt für Schritt zu einer individuellen Einführung von IRMA® in Ihre kritische Netzwerkumgebung:

- Initial-Workshop zur Klärung der Randbedingungen und Festlegung der System-Konfiguration
- Integration der angebotenen IRMA®-Hardware-Komponenten in das Leit- und FWT-Netzwerk
- Konfiguration des Systems inklusive Erstellung geeigneter Kommunikationsregeln zur Verifizierung von Anomalien
- Schulung für System-Administratoren
- Nach-Verifizierung weiterer Anomalien in enger Abstimmung mit einem unserer VIVAVIS System-Administratoren.

VIVAVIS AG Nobelstraße 18 | 76275 Ettlingen | Deutschland
T +49 7243 218 0 | F +49 7243 218 100 | E info@vivavis.com | W www.vivavis.com

(Stand: 23.01.2023, Änderungen vorbehalten)