secunet monitor KRITIS Angriffserkennung gemäß IT-Sicherheitsgesetz 2.0

Frederic R. Hermann

Head of Products

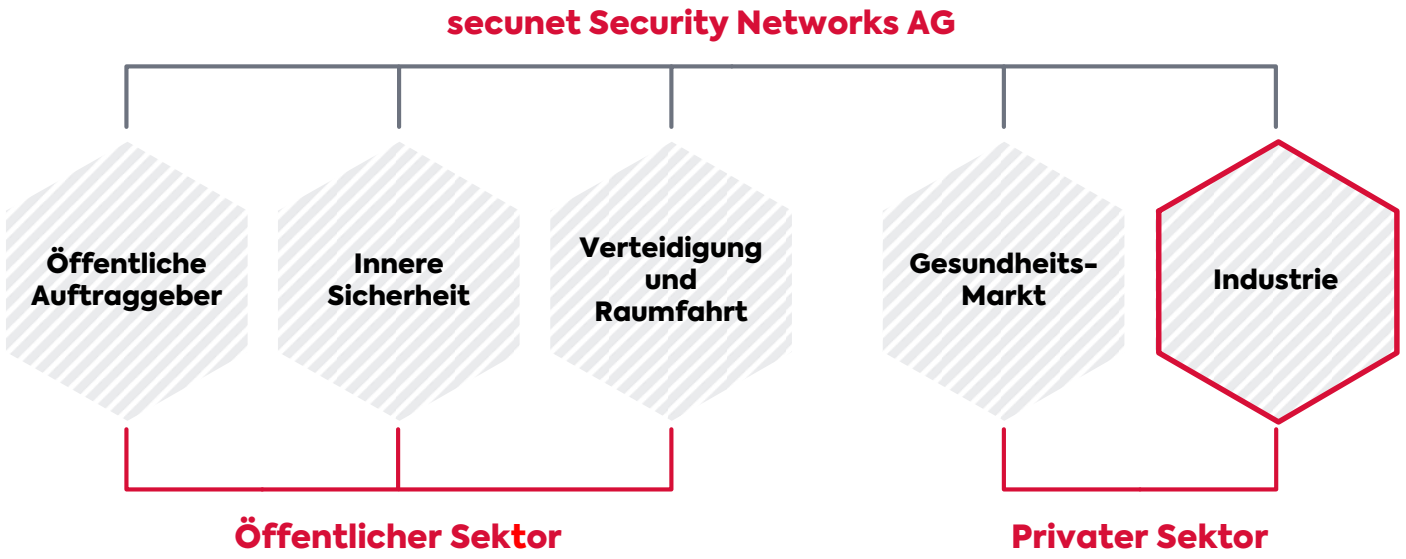
Paul Pflugradt

Team Lead Customer Project Management

Ivanka Stefanova-Achter

Manager Business Enablement

secunet auf einen Blick – 25 Jahre Erfahrung!

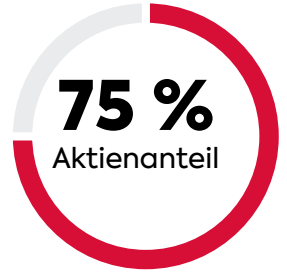


Division Industry Fokus

- **KRITIS-Betreiber**
- **Digitale Infrastrukturen**
- **Industrielle Anlagen**
- **Automotive & Mobilität**

IT-Sicherheitspartner
der Bundesrepublik Deutschland

345m*
Euro Umsatz



Hauptaktionär:
Giesecke & Devrient

*vorläufig, im Jahr 2022

secunet auf einen Blick

12 Standorte
in Deutschland

über 1000
MitarbeiterInnen

secunet.com

Das IT-SiG 2.0 – Das Wichtigste in Kürze

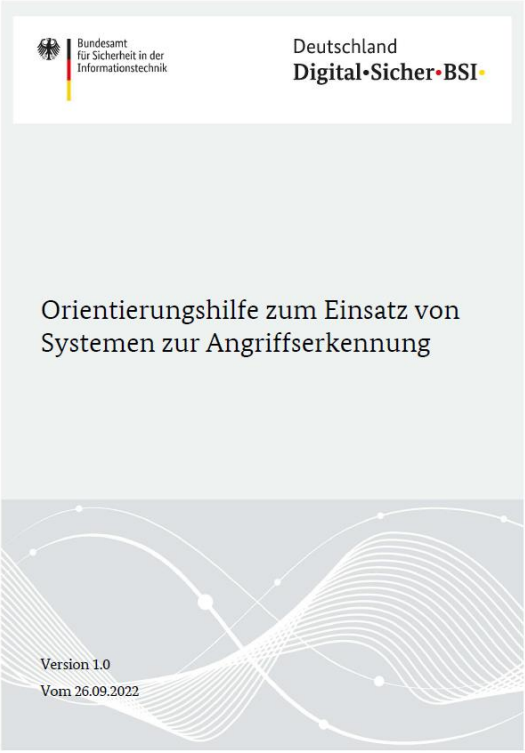
- Verpflichtet alle KRITIS-Unternehmen zum Einsatz eines Systems zur Angriffserkennung
- Ab dem 1. Mai 2023 bei Audits nachzuweisen
- Definition 2021: Systeme zur Angriffserkennung
  - „ […] Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.“
  - „ […] Dabei soll der Stand der Technik eingehalten werden.“

» **Eine Konkretisierung der Anforderungen wurde mit der „Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung “ veröffentlicht**

Die Orientierungshilfe

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterscheidet zwischen MUSS-, SOLL- und KANN-Anforderungen

- Auszug der MUSS-Anforderungen
  - Signaturbasierte Angriffserkennung über IoCs
  - Logdatenfunktionen



» Die Orientierungshilfe dient als Hilfestellung zur Umsetzung der Anforderungen aus dem IT-SiG 2.0 und ist für Auditoren die maßgebliche Grundlage in ihrer Beurteilung.

Orientierungshilfe des BSI – Umsetzungsgradmodell

secunet monitor KRITIS

… erfüllt die Anforderungen

… ist kontinuierlich ausbaufähig für weitere Stufen des Umsetzungs-gradmodells

0	Es sind bisher keine Maßnahmen zur Erfüllung der Anforderungen umgesetzt und es bestehen auch keine Planungen zur Umsetzung von Maßnahmen.
1	Es bestehen Planungen zur Umsetzung von Maßnahmen zur Erfüllung der Anforderungen, jedoch für mindestens einen Bereich noch keine konkreten Umsetzungen.
2	In allen Bereichen wurde mit der Umsetzung von Maßnahmen zur Erfüllung der Anforderungen begonnen. Es sind noch nicht alle MUSS-Anforderungen erfüllt worden.
3	Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Idealerweise wurden SOLLTE-Anforderungen hinsichtlich ihrer Notwendigkeit und Umsetzbarkeit geprüft. Ein kontinuierlicher Verbesserungsprozess wurde etabliert oder ist in Planung.
4	Alle MUSS- Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen wurden erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.
5	Alle MUSS-Anforderungen wurden für alle Bereiche erfüllt. Alle SOLLTE-Anforderungen und KANN-Anforderungen wurden für alle Bereiche erfüllt, außer sie wurden stichhaltig und nachvollziehbar begründet ausgeschlossen. Für alle Bereiche wurden sinnvolle zusätzliche Maßnahmen entsprechend der Risikoanalyse / Schutzbedarfsfeststellung identifiziert und umgesetzt. Ein kontinuierlicher Verbesserungsprozess wurde etabliert.

Zulässig ab 1. Mai 2023

Wissen Sie, was gerade in Ihrem Netzwerk passiert?

Angriffe frühzeitig erkennen

Hier bemerken Sie den Angriff **ohne SzA**

Unsichere Systeme finden und übernehmen

Durch Benutzer-interaktion:
Phising E-Mail
USB Stick
Social Engineering

Hier bemerken Sie den Angriff **mit SzA**

Alles was Sie erpressbar macht:
Kundendaten
Geschäftsemails
Personaldaten
Produktionsgeheimnisse

Mit Drohung Druck aufbauen:
Sensible Daten veröffentlichen
Produktion dauerhaft stilllegen

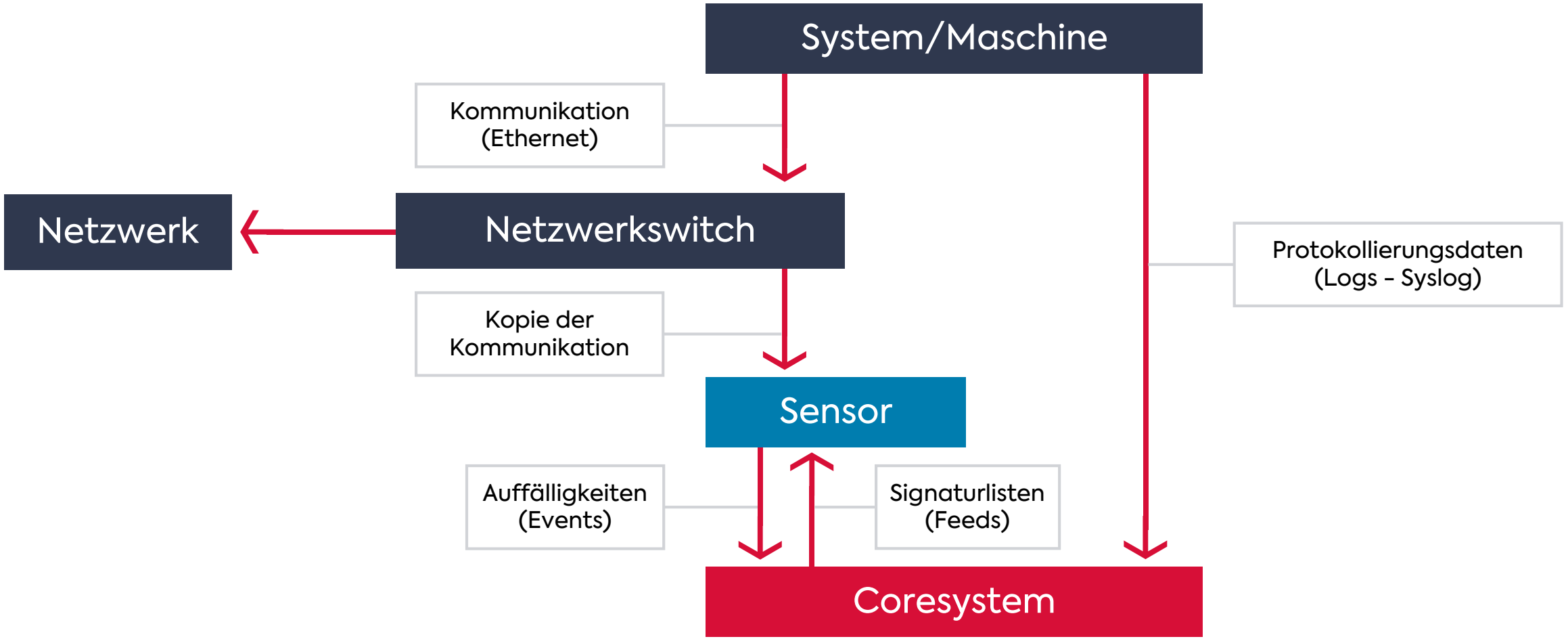
Was wäre eine echte Bedrohung für Sie?

secunet
monitor KRITIS

Die einfache Lösung zur Angriffserkennung optimiert für KRITIS-Betreiber

- ✓ Umsetzung aller technischen MUSS-Anforderungen zum 01.05. der Orientierungshilfe zur Erfüllung des IT-SiG 2.0
- ✓ Signaturbasierte Netzwerkangriffserkennung
- ✓ Logaggregation
- ✓ Flexibel, unkompliziert und kosteneffizient
- ✓ Optimiert für MSS/SOCs sowie für die Selbstverwaltung
- ✓ Unterstützte Meldung von Sicherheitsvorfällen an das BSI
- ✓ Passives und rückwirkungsfreies System für IT & OT
- ✓ Übersichtliches Changelog zur sicheren Dokumentation

Funktionsweise der Komponenten detailliert



Kontakt

Paul Pflugradt

Team Lead Customer Project Management

secunet Security Networks AG

paul.pflugradt@secunet.com

Ivanka Stefanova-Achter

Manager Business Enablement

secunet Security Networks AG

ivanka.stefanova-achter@secunet.com

Save The Date – unsere Industrial Security Webinare

- **Sichere Cloud-Anbindung in der Produktion**

  29. März, 10:00 – 11:00 Uhr

- **Cyberangriff – Notfallplan für den Ernstfall**

  24. April, 15:00 – 16:00 Uhr

- **Vorbereitung auf Cyberangriffe – Üben für den Ernstfall**

  15. Mai, 15:00 – 16:00 Uhr

Informationen und Anmeldung unter:
www.secunet.com/industrie


secunet