White Paper

# Systeme zur Angriffserkennung

## Einleitung

Cybercrime ist längst keine Modeerscheinung mehr. Es hat sich zu einem lukrativen und vor allem professionellen Geschäftsmodell entwickelt. Cyberkriminelle handeln extrem dynamisch und passen sich flexibel an technische Entwicklungen und gesellschaftliche Trends an. Erfolgreiche Cyberangriffe bedrohen nicht nur die Existenz von Wirtschaftsunternehmen. Angriffe auf kritische Infrastrukturen (KRITIS) und Organisationen der öffentlichen Verwaltung können die Bevölkerung destabilisieren, wenn zentrale Dienste nicht oder nur noch eingeschränkt zur Verfügung stehen.

Die Medienpräsenz erfolgreicher Cyberangriffe trägt dazu bei, dass die Themen Cybercrime und IT-Sicherheit nicht mehr ausschließlich in der IT-Abteilung diskutiert werden, sondern organisations-und unternehmensweit Priorität erhalten. Viele Unternehmen, kritische Infrastrukturen und Organisationen der öffentlichen Verwaltung sind trotzdem nicht ausreichend vor Cyberkriminellen geschützt. Das liegt vor allem daran, dass nicht nur herkömmliche Malware für einen Cyberangriff genutzt wird. In den meisten Fällen werden legitime Software und IT-Werkzeuge, die direkt im Bestriebssystem enthalten sind oder von Drittanbiertern bereitgestellt werden, missbraucht, um einen Angriff durchzuführen.

Da die Ausführung einer legitimen Software oder die Benutzung eines IT-Werkzeuges an sich keinen Missbrauch darstellt, braucht es zusätzliche Komponenten (Personal, Prozesse, Technologie), um einen Cyberangriff zu erkennen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) fasst erforderliche Maßnahmen als „System zur Angriffserkennung" zusammen und beschreibt den technischen und organisatorischen Aufbau eines solchen Systems in einer entsprechenden Orientierungshilfe.

In diesem Whitepaper sind die wesentlichen Anforderungen an ein System zur Angriffserkennung im Kontext der Orientierungshilfe des BSI zusammengefasst. Sie erhalten außerdem eine Übersicht über Lösungen von Trend Micro, mit denen Sie erforderliche Maßnahmen schnell und einfach umsetzen können.

## Was ist ein System zur Angriffserkennung?

Zielgerichtete Cyberangriffe (Advanced Persistent Threats – APTs) verfolgen keine stringenten Abläufe, da sie in der Regel von Individuen ausgeführt werden. Es gibt also keine Checklisten oder Ablaufpläne, gemäß derer Cyberkriminelle vorgehen, um das Opfer zu kompromittieren. Trotzdem lassen sich wiederkehrende Taktiken, Techniken und Prozeduren bestimmen, die von Tätern genutzt werden.

Innerhalb eines Systems zur Angriffserkennung werden Telemetriedaten von IT- und OT-Systemen gesammelt und gespeichert, die Indikatoren für einen Cyberangriff sein können. Zu diesen Daten zählen beispielsweise Zugriffe auf kritische Bereiche des Betriebssystems oder auf potenziell gefährliche Internetseiten, Datei-Downloads und die Ausführung legitimer Werkzeuge mit dem Ziel, neue Benutzerkonten zu erstellen oder Kennwörter von Benutzerkonten zu ermitteln.

Die gesammelten Daten werden normalisiert, aggregiert und korreliert, damit verschiedene Aktionen innerhalb eines IT- oder OT- Systems oder übergreifend über mehrere IT- oder OT-Systeme in Zusammenhang gebracht werden können. Dadurch ergibt sich ein vollständiges Bild der ausgeführten Aktionen. Innerhalb des Systems zur Angriffserkennung folgt manuell oder (teil-) automatisiert die Identifizierung von sicherheitsrelevanten Ereignissen und die Reaktion darauf.

Ein System zur Angriffserkennung besteht also aus technischen und organisatorischen Maßnahmen, die zur Erkennung von Cyberangriffen und zur Reaktion darauf erforderlich sind. Diese Systeme sollten unabhängig von gesetzlichen Vorgaben und der Branche einer Organisation eingesetzt werden, um einen möglichst wirksamen Schutz gegen Cyberangriffe und einen hohen Grad an Erkennung zu bieten.

## Systeme zur Angriffserkennung gemäß BSIG

***„Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten."***
(§ 2 Absatz 9b BSIG)

Weiterhin muss ein System zur Angriffserkennung ***„geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten“*** können. (§ 8a Absatz 1a BSIG)

Das BSI spezifiziert für die Gesetzesvorgabe drei wesentliche Aufgabenbereiche: Protokollierung, Detektion und Reaktion, und es definiert spezielle Anforderungen in der ***„Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“***, um die gesetzlichen Vorgaben zu erfüllen.

## Was wird für ein System zur Angriffserkennung benötigt?

Ein System zur Angriffserkennung erfolgreich einzusetzen und effizient zu betreiben, erfordert verschiedene technische und organisatorische Maßnahmen. Dabei können die Maßnahmen zur Erfüllung der Anforderungen in Kooperation mit externen Dienstleistern umgesetzt werden.

Spezialisierte Partner können vor allem dabei unterstützen, die folgenden Voraussetzungen und Rahmenbedingungen umzusetzen:

- Einführung und Betrieb eines (Informations-) Sicherheitsmanagementsystems (ISMS)
- Erstellung oder Aktualisierung einer vollständigen IT- und OT-Dokumentation
- Durchführung einer Risikoanalyse
- Definition von Netzen, Systemen und Prozessen, die kritisch für die Aufrechterhaltung der primären Dienstleistungen / des primären Geschäftsbetriebes sind
- Erstellung oder Aktualisierung von Prozessen für den erfolgreichen Betrieb des Systems zur Angriffserkennung (etwa Ablaufpläne, Notfallpläne und Meldewege)
- kontinuierliche Bewertung von Cyberbedrohungen für die IT- und OT-Infrastruktur der Organisation

Insgesamt definiert das BSI zum aktuellen Zeitpunkt (Februar 2023) 89 Anforderungen für Systeme zur Angriffserkennung in den speziellen Aufgabenbereichen Protokollierung, Detektion und Reaktion. Diese sind unterteilt in (6) **KANN-**, (19) **SOLL-** und (64) **MUSS-**Kriterien. Dabei können mehrere MUSS-Kriterien ausschließlich innerhalb der Organisation erfüllt werden, etwa folgende:

- Bereitstellung ausreichender finanzieller Ressourcen zur Umsetzung des Projektes
- Meldung und Eskalation von Risiken, die für die IT- und OT-Infrastruktur des Kunden auf Basis von externen Quellen ermittelt wurden
- Abruf von Meldungen zu Hard- und Softwareschwachstellen von Herstellern, Behörden, Medien und weiteren Stellen
- Dokumentation des Ausschlusses von Netzen oder Netzsegmenten aus dem Bereich der automatischen Reaktion
- Meldung sicherheitsrelevanter Ereignisse und Vorfälle an zuständige Behörden

## Welche Anforderungen können Trend Micro Lösungen erfüllen?

Trend Micro bietet Produkte und Dienstleistungen an, die in Systemen zur Angriffserkennung erforderlich sind. Dadurch kann Trend Micro zielführend und schnell dabei unterstützen, folgenden Abdeckungsgrad gemäß der BSI-Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung zu erreichen:

- **MUSS** Anforderungen: 85,94% (55 von 64 Kriterien)
- **SOLL** Anforderungen: 89,47% (17 von 19 Kriterien)
- **KANN** Anforderungen: 100% (6 von 6 Kriterien)

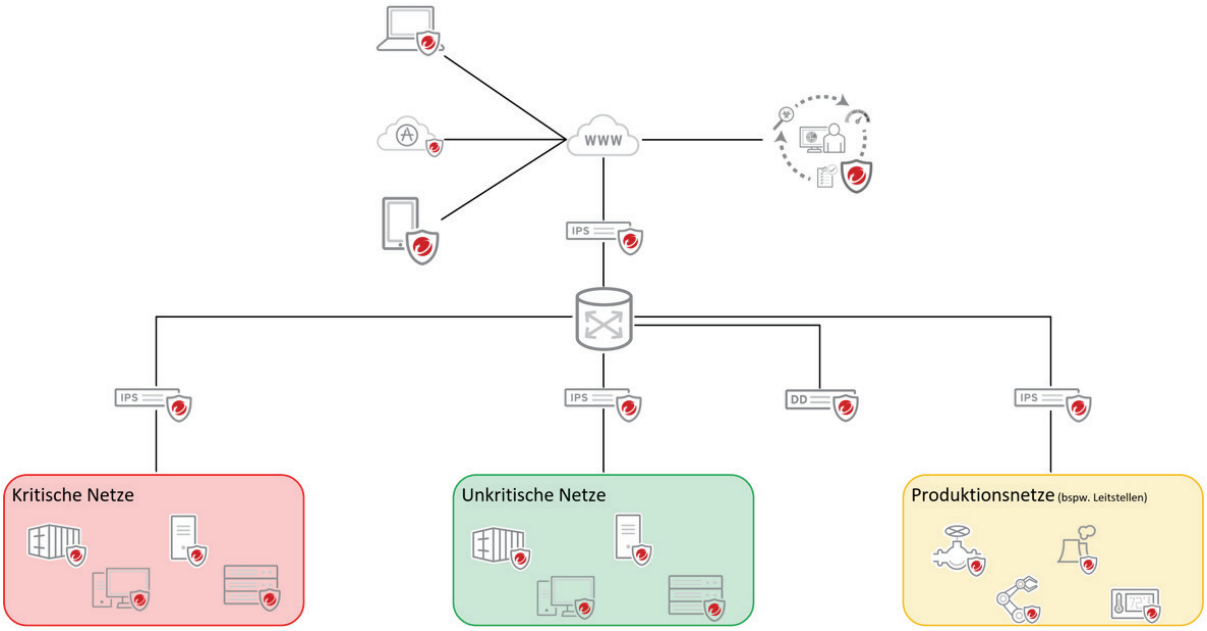
## Trend Micro Referenzarchitektur

Die Trend Micro Referenzarchitektur für ein System zur Angriffserkennung unterteilt sich im Wesentlichen in zwei Kernbereiche: Technologie und Organisation (Dienstleistungen und Prozesse). Technische Lösungen werden dabei vornehmlich in Form von Software-as-a-Service (SaaS) eingesetzt.

Für die aufgeführten SaaS-Lösungen liegt ein Testat gemäß BSI C5 (Cloud Computing Compliance Controls Catalogue) Typ 2 vor.

## Technologie

Der technologische Bereich der Trend Micro Referenzarchitektur für ein System zur Angriffserkennung konzentriert sich auf Sensorik und Schutzfunktionalitäten.

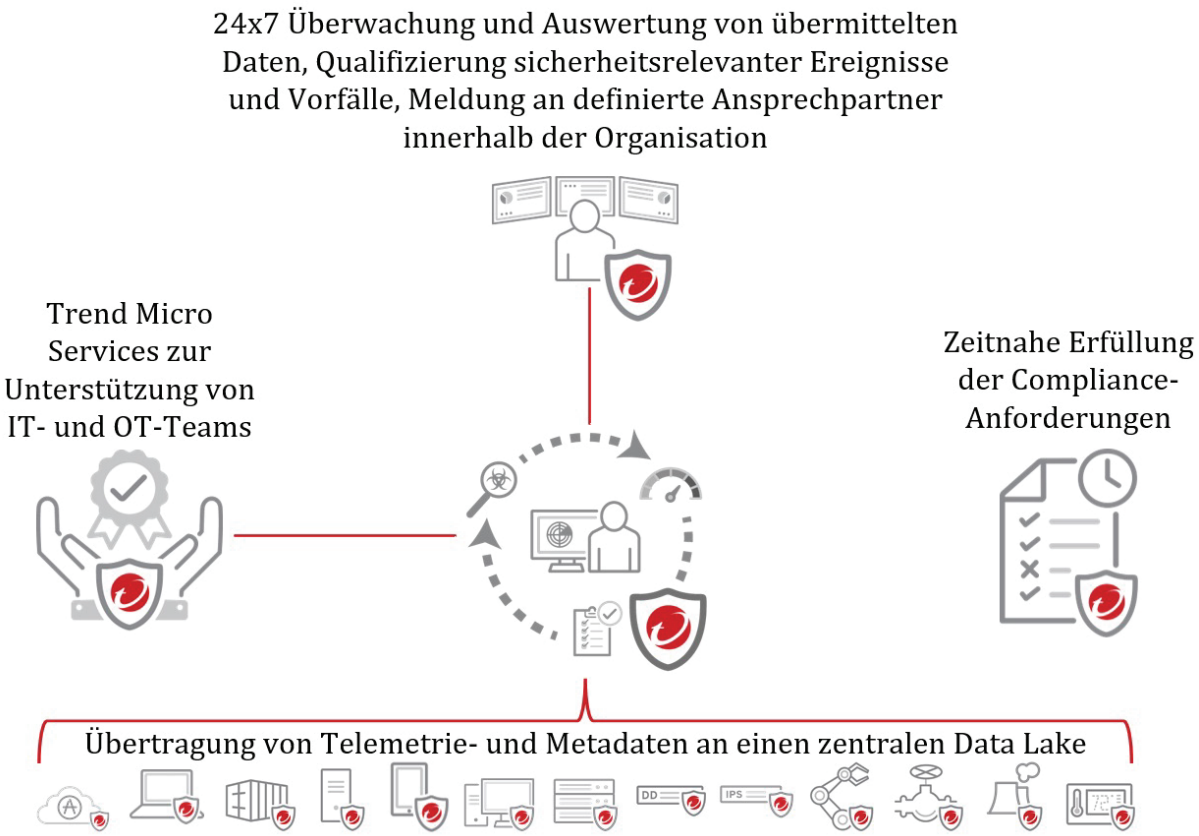


Je nach Einsatzbereich werden die folgenden Produkte (siehe Tabelle) eingesetzt, um vor allem die Anforderungen hinsichtlich Protokollierung und Detektion zu erfüllen. Durch die Kombination mit organisatorischen Komponenten lassen sich auch Anforderungen aus dem Aufgabenbereich Reaktion erfüllen.

| LÖSUNG | EINSATZBEREICH | EINSATZZWECK |
|---|---|---|
| *Deep Discovery Inspector* | *Netzwerküberwachung an Netzübergängen* | *- Anomalie- und Angriffserkennung auf Netzwerkebene* |
| *TippingPoint* | *Netzwerkschutz* | *- Abwehr von Cyberangriffen auf Netzebene durch die Analyse und das Blockieren schädlicher Datenströme* |
| *Cloud One: Endpoint and Workload Security* | *Clients und Server, die mit Software zur Erkennung von Schadcode bestückt werden dürfen* | *- Schutz vor Malware und schädlichen Webseiten<br>- Sensorik zur Erkennung zielgerichteter Angriffe und missbräuchlicher Nutzung legitimer Software* |
| *Cloud One: Container Security* | *Kubernetes Cluster (on Premises und in Form von CSP-Diensten)* | *- Absicherung von Containern gegen Malware und die Ausnutzung von Schwachstellen<br>- Erkennung von Konfigurationsfehlern<br>- Sensorik zur Erkennung zielgerichteter Angriffe* |
| *Cloud App Security* | *SaaS-Anwendungen wie Office 365 oder Google Suite* | *- Schutz vor Malware in SaaS-Anwendungen<br>- Schutz vor Spam und Phishing-Angriffen<br>- Sensorik zur Erkennung zielgerichteter Angriffe* |
| *OT – TxOne EdgeIPS / EdgeIPS Pro* | *OT-Netze und -Systeme* | *- Abwehr von Cyberangriffen auf Netzebene durch die Analyse und das Blockieren schädlicher Datenströme – speziell für OT-Netze und -Systeme* |
| *OT – Stellar* | *OT-Systeme* | *- Schutz vor Malware<br>- Sensorik zur Erkennung zielgerichteter Angriffe und missbräuchlicher Nutzung legitimer Software – speziell für OT-Systeme (agentenbasiert)* |
| *Vision One: Mobile Security* | *mobile Geräte (Android, iOS/iPadOS, ChromeOS)* | *- Schutz vor Malware und schädlichen Webseiten auf mobilen Endgeräten<br>- Konfigurationsprüfung für mobile Endgeräte<br>- Sensorik zur Erkennung zielgerichteter Angriffe* |
| *Vision One* | *Datensammlung und -auswertung* | *- zentrale Datensammlung für die eingesetzte Trend Micro Sensorik<br>- automatische Normalisierung<br>- Aggregation und Korrelation von Ereignissen<br>- automatische Identifizierung sicherheitsrelevanter Ereignisse und Vorfälle<br>- automatische Benachrichtigungen<br>- optional: • automatische Reaktion auf Ereignisse und Vorfälle<br>• Risikobewertung<br>• Schwachstellenidentifizierung<br>• Ermittlung, Aus- und Bewertung von Aktivitätsdaten aus Authentifizierungsdiensten zur Erkennung kompromittierter Benutzerkonten* |

**Organisation**

Der organisatorische Bereich der Trend Micro Referenzarchitektur für ein System zur Angriffserkennung umfasst Dienstleistungen und Prozesse, die auf Technologien von Trend Micro zurückgreifen.




Es gilt, die korrespondierenden Anforderungen der Aufgabenbereiche Protokollierung, Detektion und Reaktion abzudecken und das System zur Angriffserkennung zeitnah in Betrieb zu nehmen. Dafür werden die folgenden Services von Trend Micro eingesetzt.

| SERVICE | EINSATZZWECK |
|---|---|
| *Professional Services* | *- Inbetriebnahme der Trend Micro Technologien unter Berücksichtigung tagesaktueller Best Practices*<br>*- Health Checks für eingesetzte Trend Micro Lösungen* |
| *Training* | *- Schulung und Workshops zur Inbetriebnahme und zum Betrieb von Trend Micro Lösungen* |
| *Service One Complete* | *- dedizierter, deutschsprachiger Ansprech- und Sparringspartner zu den Themen Trend Micro Services, Prozesse und Technologien und Cybersecurity*<br>*- Unterstützung bei der Inbetriebnahme neuer Trend Micro Technologien*<br>*- Unterstützung bei der Aktualisierung von Trend Micro Lösungen*<br>*- regelmäßige Health Checks für eingesetzte Trend Micro Lösungen*<br>*- 24/7-Qualifizierung von sicherheitsrelevanten Ereignissen und Vorfällen durch Fachleute für Cybersecurity und Meldung über definierte Kommunikationskanäle*<br>*- 24/7-Reaktion auf sicherheitsrelevante Ereignisse im Rahmen vorher definierter Zuständigkeitsbereiche und technischer Möglichkeiten*<br>*- 5 Tagessätze Notfallhilfe (Incident Response) bei erfolgreichen Cyberangriffen nach Verbrauch des Kontingentes abgerechnet auf Basis von Tagessätzen*<br>*- Frühwarnsystem zur proaktiven Vorbeugung von Cyberangriffen* |

## Fazit

Trend Micro unterstützt IT- und OT-Teams in Unternehmen und Organisationen durch State-of-the-Art-Technologie, hoch qualifizierte Fachleute in allen Themenbereichen der Cybersecurity und durch bewährte Prozesse. Zusammen mit Trend Micro können Sie effizient und effektiv ein System zur Angriffserkennung einführen und Ihr Unternehmen oder Ihre Organisation dadurch bestmöglich gegen Cyberkriminelle schützen.