sure[secure]
your security operations center

secure mag

CYBERSECURITY-TRENDS FÜR DEN MITTELSTAND

AI, SOC-Transformation und operative Resilienz

Von Erkenntnis zu Umsetzung

Cybersecurity befindet sich an einem strukturellen Wendepunkt. Während frühere Jahre von neuen Angriffstechniken oder einzelnen Großvorfällen geprägt waren, hat sich 2025 vor allem durch eine nüchterne Erkenntnis ausgezeichnet: Sicherheitsprobleme entstehen selten durch fehlende Technologien, sondern durch fehlende Umsetzungsfähigkeit und das bei weiterhin steigenden Angriffszahlen. Laut BitKom Studie Wirtschaftsschutz 2025 waren 87% aller Unternehmen in den letzten 12 Monaten von mindestens einem Cyberangriff betroffen. Der dadurch entstandene Schaden summiert sich auf 289 Milliarden Euro, was einem Plus von rund 8% gegenüber dem Vorjahr entspricht.[1]

Unternehmen verfügen heute über leistungsfähige Security-Tools, Cloud-Plattformen mit integrierten Schutzmechanismen und einen breiten Markt an Managed Services. Gleichzeitig zeigen Vorfälle, Audits und regulatorische Anforderungen, dass diese Fähigkeiten häufig nicht in belastbare Betriebsmodelle übersetzt sind. Reaktionszeiten sind zu lang, Verantwortlichkeiten unklar und Prozesse nicht auf Geschwindigkeit ausgelegt.

2026 markiert den Übergang von strategischer Einsicht zu operativer Konsequenz. Künstliche Intelligenz, regulatorischer Druck und zunehmende Abhängigkeiten in Lieferketten wirken dabei nicht isoliert, sondern verstärken sich gegenseitig. Für CISOs und IT-Sicherheitsverantwortliche stellt sich weniger die Frage, welche Technologie eingeführt wird, sondern wie Sicherheitsorganisationen strukturell auf ein neues Tempo vorbereitet werden.

1. Quelle: https://www.bitkom.org/sites/main/files/2025-12/bitkom-studienbericht-wirtschaftsschutz-2025_2.pdf

Rückblick 2025:
Die prägenden Linien

Drei Entwicklungen aus 2025 bilden die Ausgangsbasis für 2026.

Erstens hat sich gezeigt, dass Cybersecurity ohne strategische Einbettung zu einem reaktiven Werkzeugkasten verkommt. Sicherheitslösungen werden eingeführt, ohne klar zu definieren, welche Geschäftsprozesse sie schützen sollen und welche Risiken tatsächlich priorisiert sind. Der operative Nutzen bleibt damit hinter den Erwartungen zurück.

Zweitens hat die Diskussion um NIS2 verdeutlicht, dass regulatorische Anforderungen nicht als Compliance-Übung verstanden werden dürfen. Sie zielen explizit auf Reaktionsfähigkeit, Nachweisbarkeit und Managementverantwortung ab und damit auf genau jene Schwächen, die von den Angreifern gerne ausgenutzt werden.

Drittens hat der zunehmende Einsatz von AI auf Angreifer- wie Verteidigerseite eine neue Dynamik erzeugt. Der entscheidende Faktor ist dabei nicht die Intelligenz einzelner Modelle, sondern die Automatisierung ganzer Prozessketten.

Gemeinsam verschieben diese Entwicklungen die Koordinaten moderner Cyberabwehr. Die folgenden Kapitel ordnen die zentralen Trends ein, die 2026 Geschwindigkeit, Klarheit und operative Belastbarkeit prägen werden.

Agentic AI komprimiert Angriffsabläufe

Angriffe folgen zunehmend nicht mehr linearen Mustern. Agentenbasierte AI-Systeme ermöglichen es, Reconnaissance, Privilegienausweitung, laterale Bewegung und Vorbereitung von Schadaktionen parallelisiert und automatisiert auszuführen. Zeitfenster, die früher in Tagen oder Wochen gemessen wurden, schrumpfen auf Stunden oder Minuten.

Diese Entwicklung verändert die Grundannahmen klassischer Sicherheitsarchitekturen. Detektion, die auf periodischer Analyse oder manueller Auswertung basiert, verliert an Wirksamkeit. Entscheidend ist die Fähigkeit, verdächtige Aktivitäten frühzeitig in ihrem Zusammenhang zu erkennen und ohne Verzögerung zu reagieren.

Konsequenzen für Sicherheitsorganisationen

Sicherheitsmaßnahmen müssen auf Durchgängigkeit ausgelegt sein. Einzelne Tools ohne Integration erzeugen keine Geschwindigkeit. Erst das Zusammenspiel aus Telemetrie, Korrelation und automatisierter Reaktion ermöglicht es, mit der neuen Dynamik Schritt zu halten.

Agentic AI

Agentic AI bezeichnet KI-Systeme, die Abläufe eigenständig steuern und Entscheidungen kontextbasiert vorbereiten. Für Unternehmen verschiebt sich damit der Maßstab von punktueller Sicherheit hin zur Fähigkeit, operative Prozesse dauerhaft und unter Zeitdruck beherrschbar zu halten.

AI im SOC als Stabilisator unter Last

Aktuelle Benchmark-Untersuchungen zeigen, dass AI-gestützte Arbeitsweisen im SOC nicht nur die Bearbeitungszeit reduzieren, sondern vor allem die Ergebnisqualität unter Belastung stabilisieren. Eine praxisnahe Vergleichsstudie der Cloud Security Alliance hat Analysten mit und ohne AI-Unterstützung in realistischen SOC-Szenarien gegenübergestellt. Das Ergebnis: Mit AI arbeiten Teams signifikant schneller und liefern zugleich konsistentere Bewertungen, insbesondere bei hohem Alert-Volumen und zunehmendem Zeitdruck.[1]

Bemerkenswert ist dabei weniger der Effizienzgewinn im Normalbetrieb als die geringere Leistungsvolatilität. Während rein manuelle Arbeitsweisen unter Last deutlich an Genauigkeit verlieren, bleibt die Qualität der Entscheidungen mit AI-Unterstützung deutlich stabiler. Genau dieser Effekt gewinnt in hochvolumigen SOC-Umgebungen strategische Relevanz.

Vor allem unter Stress, Personalmangel und Alert-Flut ist nicht die durchschnittliche Leistung entscheidend, sondern die Verlässlichkeit operativer Entscheidungen.

Einordnung für CISOs

AI wirkt im SOC nicht primär als Ersatz für Fachpersonal, sondern als strukturelles Korrektiv. Sie reduziert die Abhängigkeit von individueller Erfahrung und Tagesform und macht Sicherheitsleistung planbarer. Damit verschiebt sich der Fokus von punktueller Effizienzsteigerung hin zu Resilienz und Skalierbarkeit als Management-Aufgabe.

1. Quelle: https://cloudsecurityalliance.org/artifacts/a-benchmark-study-of-ai-agents-in-the-soc

SOC-Copilots etablieren sich - Governance wird zum Differenzierungsmerkmal

AI-gestützte Assistenzfunktionen im SOC werden 2026 zum Standard. Ihr Einsatz konzentriert sich auf Triage, Kontextanreicherung, Hypothesenbildung und Vorstrukturierung von Incidents. Der Mehrwert entsteht jedoch nur dort, wo klare Leitplanken definiert sind.

Ohne Governance drohen neue Risiken:

- automatisierte Fehlentscheidungen,
- mangelnde Nachvollziehbarkeit und
- unklare Verantwortlichkeiten.

Sicherheitsorganisationen müssen daher präzise festlegen, welche Entscheidungen automatisiert vorbereitet und welche ausschließlich durch Menschen getroffen werden dürfen.

Anforderungen an reife Modelle

Reife SOCs trennen strikt zwischen Empfehlung und Aktion, halten kritische Maßnahmen im Human-in-the-loop und stellen Auditierbarkeit sicher. AI wird damit zum Werkzeug innerhalb klar definierter Prozesse, nicht zu deren Ersatz.

NIS2 verschiebt den Fokus auf operative Nachweise

Mit der Umsetzung von NIS2 rückt die tatsächliche Handlungsfähigkeit von Organisationen in den Mittelpunkt. Gefordert sind keine Tool-Landschaften, sondern funktionierende Prozesse zur Erkennung, Eskalation und Behandlung von Sicherheitsvorfällen.

Für Sicherheitsverantwortliche bedeutet das eine neue Form der Rechenschaft. Reaktionszeiten, Entscheidungswege und Dokumentation werden prüfbar. Cybersecurity wird damit explizit zu einem Management-Thema.

Rolle des SOC

Das SOC wird zur operativen Grundlage regulatorischer Nachweise. Es verbindet technische Erkennung mit organisatorischer Eskalation und strukturiertem Reporting. Ohne diese Klammer bleibt NIS2 ein formales Konstrukt ohne reale Wirkung.

NIS2 - aktueller Kontext

Die NIS2-Richtlinie ist auf EU-Ebene seit 2023 in Kraft, die nationale Umsetzung erfolgt Ende 2025 noch uneinheitlich. Für Unternehmen bedeutet das eine Phase erhöhter Aufmerksamkeit, in der regulatorische Erwartungen bereits greifen, auch wenn Detailregelungen teils noch nachgeschärft werden.

Entscheidend wird damit weniger der formale Stichtag als die Fähigkeit, regulatorische Prüfungen jederzeit operational zu bestehen.

PODCAST

CYBER SECURITY Basement

In unserem Podcast spricht Michael Döhmen über spannende Themen aus dem Bereich Cybersecurity. Dabei legen wir großen Wert auf Objektivität und verzichten auf übertriebenes Marketing oder „Feature-Fucking“. Stattdessen setzen wir auf einen seriösen, authentischen und ehrlichen Austausch zwischen Theorie und Praxis.

Jetzt reinhören

Spotify

Apple Podcast

YouTube Music

amazon music

und noch mehr...

Third-Party Risk verlangt operative Priorisierung

Lieferketten sind weiterhin einer der häufigsten Eintrittspunkte für Sicherheitsvorfälle. Die Herausforderung liegt weniger im Erkennen des Risikos als in dessen Handhabung. Vollständige Bewertungen aller Lieferanten sind weder realistisch noch wirksam.

2026 setzt sich ein priorisierter Ansatz durch. Kritikalität, Exponierung und technische Signale ersetzen pauschale Fragebögen. Risiken werden dort adressiert, wo sie operative Auswirkungen entfalten können.

Bedeutung für das SOC

Third-Party-Risiken müssen in bestehende Detektions- und Reaktionsmodelle integriert werden. Externe Identitäten, Fernzugänge und geteilte Infrastrukturen gehören zu den zentralen Beobachtungsobjekten.

OT-Security rückt ins Zentrum der Resilienz

Produktions- und OT-Umgebungen sind in vielen Unternehmen historisch gewachsen und sicherheitstechnisch unterversorgt. Alte Systeme, eingeschränkte Patchbarkeit und fehlende Transparenz prägen das Bild.

Mit zunehmender Automatisierung von Angriffen steigt die Wahrscheinlichkeit, dass auch OT-Umgebungen gezielt adressiert werden. Was bislang oft verschont blieb, wird damit zu einem realistischen Risiko.

Handlungsperspektive

Der Einstieg in OT-Security erfolgt nicht über vollständige Modernisierung, sondern über Transparenz und abgestufte Überwachung. Passive Monitoring-Ansätze und klare Verantwortlichkeiten bilden die Grundlage für belastbare Reaktionsfähigkeit.

Foto v. Links nach Rechts: Mohamed Abdelfattah (Senior SOC-Analyst), Georg Lauenstein (Senior Detection Engineer) und Halit Cintiriz (SOAR Engineer)

CISO-Takeaways für 2026

1. Geschwindigkeit ist ein Organisationsmerkmal, kein Tool-Feature.
2. AI im SOC stabilisiert Qualität und reduziert operative Volatilität.
3. Regulatorik verlangt nachweisbare Reaktionsfähigkeit, nicht Symbolmaßnahmen.
4. Lieferkettenrisiken müssen priorisiert und technisch integriert werden.
5. OT-Security ist ein integraler Bestandteil unternehmerischer Resilienz.

Schlusswort:

2026 wird nicht durch spektakuläre neue Bedrohungen definiert, sondern durch strukturelle Reife. Unternehmen, die Cybersecurity als Betriebsfähigkeit verstehen und ihre Sicherheitsorganisation auf Geschwindigkeit, Klarheit und Automatisierung ausrichten, verschaffen sich einen nachhaltigen Vorteil.

Das Security Operations Center wird dabei zum Dreh- und Angelpunkt. Nicht als isolierte Einheit, sondern als verbindendes Element zwischen Technologie, Prozessen und Management.

Cybersecurity ist 2026 weniger eine Frage der richtigen Werkzeuge als der richtigen Betriebsmodelle. Wer heute in klare Strukturen, belastbare Prozesse und kontrollierten Einsatz von AI investiert, gewinnt Zeit. Und Zeit ist die entscheidende Ressource moderner Cyberabwehr.

Weitere Informationen zum Thema:

Podcast-Folge:

2025 im Rückblick.
2026 im Ausblick.
KI, NIS2 und die wichtigsten Cybersecurity-Trends

suresecure GmbH
Dreischeibenhaus 1
40211 Düsseldorf

Telefon: +49 (0) 2156 974 90 60

E-Mail: kontakt@suresecure.de
Web: www.suresecure.de