AEGYS DATALYTICS

MITTELSTANDS-REALITÄTS-CHECK · MAI 2026

Die ungleiche Mathematik 2026

Ein Mittelständler verteidigt sich mit einem Mitarbeiter. Der Gegner greift an mit einem Algorithmus.

Cyberangriffe werden 2026 nicht häufiger — sie werden anders. Erst dokumentiert: KI-entwickelte Zero-Day-Exploits. Autonome Malware. Eine Asymmetrie, die der typische deutsche Mittelstand mit Bordmitteln verteidigen soll. Acht Fragen, die jeder Geschäftsführer für sich beantworten sollte.

> Erstellt von der AEGYS DATALYTICS AG. Basierend auf Bitkom Wirtschaftsschutzstudie 2025, BSI-Lagebericht 2025, Google Threat Intelligence Report Mai 2026, sowie der praktischen Erfahrung aus Einsätzen bei mittelständischen Unternehmen seit 2023 (Energie, Maschinenbau, Finanzdienstleister, IT-Service, Fahrzeughandel).

INHALT

In diesem Leitfaden

Vorwort

Dieser Realitäts-Check ist kein Schreckens-Katalog. Er ist eine strukturierte Diagnose. Wenn Sie die acht Fragen ehrlich beantworten, haben Sie eine klare Sicht auf den Stand Ihrer Cyberabwehr — und auf die Lücken, die strukturell entstehen, wenn ein Mittelständler mit Bordmitteln gegen industrialisierte Angreifer steht.

Die Antworten sind nicht für uns gedacht. Sie sind für Sie. Falls einzelne Punkte unklar bleiben, sprechen wir gerne 15 Minuten darüber — kein Sales-Call.

Gerald Hahn
Mitgründer, AEGYS DATALYTICS AG

WARUM JETZT

Warum dieser Realitäts-Check existiert

Drei Zahlen, die 2026 ein neues Bild zeichnen — und die Sie kennen sollten, bevor Sie Ihre Cyberabwehr planen:

289,2
Mrd. €

Gesamtschaden für die deutsche Wirtschaft 2024/2025

Laut Bitkom Wirtschaftsschutzstudie 2025 — Anstieg um 22,6 Mrd. EUR gegenüber dem Vorjahr. Rund 70 Prozent (202,4 Mrd. EUR) sind direkt auf Cyberangriffe zurückzuführen.[1]

149.000
Stellen vakant

Unbesetzte IT-Stellen in Deutschland

Laut Bitkom-Studie (Februar 2025) fehlen 149.000 IT-Fachkräfte. Eine offene IT-Stelle bleibt durchschnittlich 7,7 Monate vakant — Tendenz steigend.[2]

Mai 2026
Erstmals dokumentiert

KI-entwickelter Zero-Day-Exploit

Google Threat Intelligence Group (Mandiant) dokumentiert einen Zero-Day-Exploit, der mit KI-Hilfe von einer kriminellen Gruppe entwickelt wurde — geplant für Mass-Exploitation.[3]

[1] Bitkom e.V., Wirtschaftsschutzstudie 2025 [2] Bitkom e.V., IT-Fachkräftemangel 2025 [3] Google Threat Intelligence Group, Mai 2026

Wer hinter diesem Leitfaden steht

Aufsichtsrat AEGYS DATALYTICS AG: Dr. Rasso Graber (Falch & Partner München), Candid Wüest (Threat Research, ehemals Acronis und Symantec, RSA- und BlackHat-Sprecher), Jörg Eschweiler (NATO Digital Capability, ehemals IBM, Airbus Defense, Atos), Prof. Dr. Jivka Ovtcharova (KIT-Professorin, FZI-Direktorin, KI-Expertin für industrielle Sicherheit), Markus Geier (Cyber-Krisenmanagement seit 1985, CEO ComCode).

REALITÄTS-CHECK 1 VON 8

1 Wer in Ihrem Unternehmen erkennt einen Cyberangriff?

KONTEXT

Die meisten Mittelständler glauben, dass ihr Antivirus oder ihre Firewall einen Angriff erkennen würde. Das stimmt 2026 nicht mehr. Ein Großteil moderner Malware ist polymorph — sie verändert ihre Signatur kontinuierlich, um signaturbasierte Erkennung zu umgehen.

DIE ZAHL, DIE ZÄHLT

80% aller Cyberangriffe nutzen menschliches Versagen als Einfallstor (Phishing, Social Engineering). Klassische Schutzmaßnahmen erkennen den eigentlichen Eindringling oft nicht, sondern erst die Folgen.

Quelle: BSI Lagebericht zur IT-Sicherheit in Deutschland 2025

✓ EINE GUTE ANTWORT

„Wir haben aktive Detection, die ungewöhnliches Netzwerk-Verhalten erkennt — nicht nur bekannte Signaturen."

× ROTE FLAGGE

„Unser IT-Mensch oder externer Dienstleister würde es schon merken."

IHRE ANTWORT

REALITÄTS-CHECK 2 VON 8

2 Wie lange würde ein Angreifer in Ihrem Netzwerk unbemerkt agieren können?

KONTEXT

Die durchschnittliche Dwell Time eines Angreifers im Netzwerk lag 2024-2025 bei 11-21 Tagen. In dieser Zeit bewegen sich Angreifer lateral, sammeln Zugangsdaten und bauen Persistenz auf — bevor sie zuschlagen. Die wirkliche Frage ist nicht, ob jemand reinkommt, sondern wie schnell Sie es merken.

DIE ZAHL, DIE ZÄHLT

Mean Time to Detect bei Unternehmen ohne dedizierte Network Detection: typisch Wochen bis Monate. Mit moderner NDR/XDR-Lösung und automatisierter Korrelation: Stunden bis wenige Tage.

Quelle: Google Threat Intelligence Group, Mandiant 2026

✓ EINE GUTE ANTWORT

„Maximal 24-72 Stunden. Wir haben kontinuierliche Sicht auf den Netzwerkverkehr und automatische Alerts bei Anomalien."

× ROTE FLAGGE

„Keine Ahnung. Wahrscheinlich würden wir es merken, wenn etwas Größeres passiert."

IHRE ANTWORT

REALITÄTS-CHECK 3 VON 8

3 Wie viele Personen in Ihrem Unternehmen arbeiten dediziert an Cybersecurity?

KONTEXT

Ein professionelles 24/7-SOC benötigt 5-8 Personen (drei Schichten plus Reserve). Senior SOC Analysten verdienen 80-120k EUR pro Jahr. Selbst ein minimales Setup kostet 400-600k EUR Personalkosten jährlich — ohne Tools, ohne Onboarding-Zeit, ohne Fluktuationsrisiko.

DIE ZAHL, DIE ZÄHLT

99,3% aller deutschen Unternehmen sind KMU. Die meisten haben null bis eine Person für Cybersecurity — typischerweise dieselbe Person, die auch IT-Betrieb, Backups und DSGVO verantwortet.

Quelle: Statistisches Bundesamt + Bitkom Wirtschaftsschutz 2025

✓ EINE GUTE ANTWORT

„Wir haben dedizierte Cybersecurity-Kapazität — entweder intern oder über einen spezialisierten externen Partner."

× ROTE FLAGGE

„Macht unser IT-Mensch nebenbei."

IHRE ANTWORT

REALITÄTS-CHECK 4 VON 8

4 Wann haben Sie zuletzt nachweislich getestet, ob Angreifer in Ihr Netzwerk eindringen könnten?

KONTEXT

Penetrationstests, die nur im Compliance-Kontext einmal jährlich gemacht werden, geben eine Momentaufnahme. Moderne autonome Pentest-Plattformen liefern kontinuierliche Bewertung der tatsächlichen Angriffsfläche. Der Unterschied: Sie wissen heute, was morgen ein Einfallstor wäre.

DIE ZAHL, DIE ZÄHLT

Nur 31% der Mittelständler in Deutschland führen regelmäßig Penetrationstests durch. Die Mehrheit verlässt sich auf Tools, die im Ernstfall nicht zeigen, was Angreifer wirklich erreichen könnten.

Quelle: Bitkom Wirtschaftsschutz 2025

✓ EINE GUTE ANTWORT

„Innerhalb der letzten 6 Monate. Idealerweise mit autonomer Wiederholbarkeit, sodass Veränderungen sichtbar werden."

× ROTE FLAGGE

„Noch nie. Oder: Vor mehr als 24 Monaten."

IHRE ANTWORT

REALITÄTS-CHECK 5 VON 8

5 Erfüllen Sie die Mindeststandards Ihrer Cyberversicherung?

KONTEXT

Cyberversicherer prüfen 2026 deutlich strenger. Die häufigsten Mindeststandards: Multi-Faktor-Authentifizierung (MFA) für alle Konten, regelmäßige Backup-Tests, dokumentierte Vorfallsreaktion, Endpoint Protection, Mitarbeiterschulungen, kontinuierliches Patching. Im Schadensfall werden diese Punkte konkret abgefragt.

DIE ZAHL, DIE ZÄHLT

Zwischen 27 und 31 Prozent der Cyber-Schadensfälle werden 2026 ganz oder teilweise abgelehnt — der MRTK Cyber-Monitor 2025 spricht von 31 Prozent abgelehnten Anträgen. Hauptgrund: nicht erfüllte Mindeststandards.

Quelle: CyberDirekt Marktanalyse 2024 + MRTK Cyber-Monitor 2025

✓ EINE GUTE ANTWORT

„Ja, wir können das in unter 5 Minuten dokumentiert nachweisen — inklusive aktueller Auditierbarkeit."

× ROTE FLAGGE

„Wir haben den Antrag mal ausgefüllt, aber wer weiß, ob das alles noch stimmt."

IHRE ANTWORT

REALITÄTS-CHECK 6 VON 8

6 Was passiert, wenn morgen früh Ihre Server verschlüsselt sind?

KONTEXT

Ransomware ist mit 34% Betroffenheit die häufigste Cyberangriffsform in deutschen Unternehmen 2025. Durchschnittliche Wiederherstellungszeit ohne getesteten Notfallplan: 2-6 Wochen Betriebsausfall. Der Schaden geht weit über das Lösegeld hinaus — Vertrauensverlust, Vertragsstrafen, Existenzbedrohung.

DIE ZAHL, DIE ZÄHLT

Nur 11% der Ransomware-Opfer konnten 2025 ihre Daten vollständig wiederherstellen — auch nach gezahltem Lösegeld. Backups allein reichen nicht; sie müssen segmentiert, getestet und außerhalb des kompromittierten Netzwerks sein.

Quelle: Bitkom Wirtschaftsschutz 2025 + Ponemon/Illumio 2025

✓ EINE GUTE ANTWORT

„Wir haben einen geprobten Notfallplan. Backups sind segmentiert, getestet und außerhalb des produktiven Netzwerks."

× ROTE FLAGGE

„Wir würden den IT-Menschen anrufen und hoffen, dass die Backups laufen."

IHRE ANTWORT

REALITÄTS-CHECK 7 VON 8

7 Kennen Sie Ihren Angriffsflächen-Stand?

KONTEXT

Das BSI fordert 2026 ein Jahr des Angriffsflächen-Managements. Gemeint sind: alle digital erreichbaren Systeme, Schnittstellen, Schatten-IT, Cloud-Dienste ohne offizielle Freigabe. Die meisten Mittelständler haben mehr Angriffsfläche, als sie wissen.

DIE ZAHL, DIE ZÄHLT

BSI Lagebericht 2025: 119 neue Schwachstellen pro Tag — ein Anstieg um 24% gegenüber dem Vorjahr. Eine unbekannte Schwachstelle in einem vergessenen Cloud-Service ist 2026 das häufigste Einfallstor.

Quelle: BSI Lagebericht 2025

✓ EINE GUTE ANTWORT

„Wir haben einen kontinuierlichen Überblick — extern erreichbare Dienste, Cloud-Bestand, Patch-Status sind dokumentiert."

× ROTE FLAGGE

„Wir wissen, was wir bewusst nutzen. Schatten-IT? Schwer zu sagen."

IHRE ANTWORT

REALITÄTS-CHECK 8 VON 8

8 Wie würden Sie heute einen IT-Sicherheits-Auditor empfangen?

KONTEXT

NIS2, DSGVO-Vorfälle, Cyberversicherer, der Wirtschaftsprüfer, Kunden im Ausschreibungsprozess — die Wahrscheinlichkeit steigt, dass Sie 2026 oder 2027 jemandem nachweisen müssen, dass Sie Cybersecurity strukturiert betreiben.

DIE ZAHL, DIE ZÄHLT

65% der von Cyberangriffen betroffenen Unternehmen fühlen sich in ihrer Existenz bedroht. Wer keine strukturierte Dokumentation vorweisen kann, hat im Schadensfall doppelt verloren — operativ und juristisch.

Quelle: Bitkom Wirtschaftsschutz 2025

✓ EINE GUTE ANTWORT

„Wir können einen aktuellen, strukturierten Stand der Cybersecurity-Maßnahmen vorlegen — Dokumentation jederzeit abrufbar."

× ROTE FLAGGE

„Wir würden anfangen, Sachen zusammenzusuchen."

IHRE ANTWORT

AUSWERTUNG

Was die Antworten bedeuten

Zählen Sie die roten Flaggen, die in Ihren Antworten sichtbar wurden. Hier eine ehrliche Einordnung — keine Verkaufs-Inszenierung:

0–2
ROTE FLAGGEN

Sie sind gut aufgestellt

Was noch fehlt, ist meist Dokumentation und Wiederholbarkeit. Sie haben strukturell die richtigen Antworten — der nächste Schritt ist, das auch im Schadensfall nachweisen zu können.

3–5
ROTE FLAGGEN

Strukturelle Lücken

Eine professionelle Detection-Lösung würde mehrere dieser Lücken auf einmal schließen. Sie sind nicht alleine — das ist die häufigste Position deutscher Mittelständler 2026.

6–8
ROTE FLAGGEN

Akuter Handlungsbedarf

Nicht weil Sie schlecht arbeiten — sondern weil Cybersecurity als Add-On zur normalen IT-Arbeit strukturell nicht funktioniert. Die Antwort ist andere Architektur, nicht mehr Aufwand.

Eine ehrliche Beobachtung

Die meisten Mittelständler haben 4-6 rote Flaggen. Das ist kein Versagen — es ist die mathematische Konsequenz, wenn 1-2 Personen die gesamte IT verantworten. Die Antwort ist nicht "mehr Personal" (es gibt keines), sondern "andere Architektur".

DIE LÖSUNG

Was AEGYS liefert

Zwei Produkte. Beide auf der Stellar-Cyber-Plattform. Beide mit deutscher Auswertung. Beide ohne wochenlanges Implementierungs-Projekt.

BEOBACHTEN

AEGYS Monitor

Eine Appliance. Vor Ort. Plug-and-Play. Der Monitor wird per TAP- oder SPAN-Port ans Netzwerk angebunden — passiv, ohne Rückwirkung. Keine Agenten auf Endgeräten, keine Konfiguration auf Ihren Systemen.

Auswertung in Deutschland. Keine Übermittlung in Drittstaaten, keine Hyperscaler-Cloud, keine Auslagerung in andere Rechtsräume. AVV nach Art. 28 DSGVO im Standard.

Erkennt, was Tools übersehen. Aktive Verbindungen, ungewöhnliche Kommunikationsmuster, externe Ziele — mit MITRE-ATT&CK-Mapping. Funktioniert auch in segmentierten und OT-Netzwerken.

Datensparsamkeit by design. Konfigurierbare Erfassungstiefe — auf Wunsch ausschließlich Metadaten, keine Payload-Erfassung.

Asset-basierte Subscription. Oder punktueller Reality-Check. Im Einsatz seit 2023.

ANGREIFEN

AEGYS Pentest

Bewiesene Angriffspfade. Autonomer Penetrationstest mit echten Angriffspfaden — ohne Skripte, ohne Disruption Ihres Tagesgeschäfts.

Was Angreifer wirklich erreichen könnten. Nicht nur eine Schwachstellen-Liste, sondern dokumentierte Pfade durch Ihr Netzwerk. Belastbare Aussage statt theoretischer Bewertung.

Vor einem Audit oder als Subscription. NIS2- und Wirtschaftsprüfungs-Audits brauchen belastbare Aussagen — wir liefern sie autonom, ohne mehrwöchige Pentester-Engagements.

Priorisierte Empfehlungen. Konkrete Maßnahmen nach tatsächlichem Risiko sortiert — kein Bericht, der unbearbeitet im Regal liegt.

Festpreis. Klar kalkulierbar. Auf Anfrage.

Technische Basis u.a.: Stellar Cyber Open XDR (Multi-Layer-AI-Plattform, weltweit bei über 14.000 Organisationen im Einsatz). Integration, Konfiguration, Appliance-Bündelung und Auswertung in Deutschland

durch AEGYS DATALYTICS.

15-MINUTEN-ERSTGESPRÄCH

Sehen, was passiert.
Und was passieren könnte.

Ein 15-minütiges Erstgespräch genügt, um zu klären, was zu Ihrer Situation passt. Wenn wir helfen können, gehen wir den nächsten Schritt gemeinsam. Wenn nicht, sagen wir das ehrlich.

Erstgespräch vereinbaren →

hallo@aegysdata.com

QUELLEN

Quellen und weiterführende Informationen

Alle Zahlen in diesem Realitäts-Check stammen aus offiziellen deutschen Aufsichts- und Branchenquellen sowie aus internationalen Top-Tier-Threat-Intelligence-Reports.

1. Bitkom e.V.
Wirtschaftsschutzstudie 2025
87% Betroffenheit, 289,2 Mrd. EUR Gesamtschaden
www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutz

2. BSI
Die Lage der IT-Sicherheit in Deutschland 2025
Offizieller Lagebericht der Bundesoberbehörde
www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html

3. Bundesamt für Verfassungsschutz
Vorstellung Bitkom-Studie 2025
Erkenntnisse zur Bedrohungslage durch staatliche Akteure
www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2025/2025-09-18-studie-bitkom.html

4. Google Threat Intelligence Group
AI Threat Tracker Mai 2026
Erster KI-generierter Zero-Day-Exploit, PROMPTSPY-Malware
cloud.google.com/blog/topics/threat-intelligence/ai-vulnerability-exploitation-initial-access

5. Bitkom e.V.
IT-Fachkräftemangel 2025
149.000 unbesetzte IT-Stellen in Deutschland
www.bitkom.org/Presse/Presseinformation/Rekord-Fachkraeftemangel-Deutschland-IT-Jobs-unbesetzt

6. CyberDirekt
Cyberversicherung Voraussetzungen 2024
Mindeststandards führender Cyberversicherer
www.cyberdirekt.de/cyberversicherung-voraussetzungen/

7. CyberDirekt
Marktanalyse 2024 Risikofragen
Analyse der IT-Standards von 17 Versicherern
www.cyberdirekt.de/marktanalyse-2024-risikofragen/

8. Statistisches Bundesamt

KMU in Deutschland

99,3% aller deutschen Unternehmen sind KMU

www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/_inhalt.html

9. Stellar Cyber

Open-XDR-Plattform

Technische Basis von AEGYS Monitor und AEGYS Pentest

stellarcyber.ai

KONTAKT

AEGYS DATALYTICS AG
Berg am Starnberger See, Bayern

hallo@aegysdata.com
www.aegysdata.com

WEITERFÜHRENDE PILLAR-ARTIKEL

DATEV-Sicherheit für Steuerkanzleien →

§203 StGB für Steuerberater →

Cyberversicherung 2026 →