Wir beraten Unternehmen und versorgen sie mit

- Internet & Glasfaser
- Standortvernetzung & SD-WAN
- Cloud & Rechenzentrum
- Cyber Security
- Telefonie, Mobilfunk & Kommunikation

lancon

LANCON WHITEPAPER

Cyberbedrohungslage 2025/2026

Was internationale Lageberichte für deutsche Unternehmen bedeuten

Einordnung statt Alarmismus

Dieses Whitepaper führt Erkenntnisse von BSI, ENISA, Verizon, Mandiant, Microsoft, CrowdStrike, IBM, Sophos, Acronis, Gartner, NIST, CISA und Heise/iX zusammen. Es trennt unterschiedliche Datengrundlagen, ordnet widersprüchlich wirkende Zahlen ein und leitet daraus konkrete Prioritäten für digitale Infrastruktur ab.

August 2026

lancon GmbH

EXECUTIVE SUMMARY

Die Lage in sechs Aussagen

1. Externe Systeme und Identitäten sind parallele Angriffsflächen.

Schwachstellen in öffentlich erreichbaren Anwendungen, VPNs und Edge-Systemen bleiben ein zentraler Einstieg. Gleichzeitig verlagern sich Angriffe auf gültige Konten, Tokens, Supportprozesse und maschinelle Identitäten. [3–5, 7, 8]

2. Der Angriff sieht immer häufiger wie reguläre Administration aus.

Gültige Zugangsdaten, PowerShell, SaaS-Integrationen, Fernwartung und native Systemwerkzeuge reduzieren die Sichtbarkeit. „Malwarefrei“ bedeutet nicht harmlos, sondern schwerer zu unterscheiden. [6, 9, 17]

3. Ransomware greift die Wiederherstellungsfähigkeit an.

Verschlüsselung bleibt relevant, wird aber durch Datenabfluss, Identitätsübernahme und gezielte Angriffe auf Backup-, Virtualisierungs- und Managementsysteme ergänzt. [3, 4, 8, 16]

4. Dienstleister und zentrale Plattformen vervielfachen die Reichweite.

RMM, SaaS-Integrationen, CI/CD, Identitätsprovider und andere Steuerungsebenen verbinden viele Systeme und Mandanten. Genau diese Effizienz macht sie zu strategischen Zielen. [3, 7, 9, 12, 18–21]

5. Geschwindigkeit wird zum organisatorischen Problem.

Zwischen Erstzugriff, Übergabe und lateraler Bewegung bleiben teilweise nur Sekunden oder Minuten. Lange Meldewege und rein manuelle Reaktion reichen dann nicht aus. [4, 6]

6. KI beschleunigt bekannte Angriffe und schafft neue Governance-Aufgaben.

KI verbessert Recherche, Täuschung, Skripterstellung und Datenanalyse. Zugleich werden KI-Konten, Agenten, Konnektoren und Prompt-Schnittstellen selbst Teil der Angriffsfläche. [3, 5–7, 9, 11, 12]

Die zentrale Schlussfolgerung

Cybersicherheit lässt sich nicht mehr sinnvoll als Sammlung einzelner Produkte steuern. Entscheidend ist, ob ein Unternehmen seine externen Systeme, Identitäten, Verwaltungszugänge, Dienstleisterabhängigkeiten und Wiederherstellungswege als zusammenhängende Infrastruktur kennt und kontrolliert.

Zahlen auf einen Blick – mit unterschiedlicher Bedeutung

Die Werte stammen aus verschiedenen Grundgesamtheiten. Sie dürfen nicht zu einer einzigen globalen Quote verrechnet werden. Ihre Stärke liegt darin, unterschiedliche Seiten derselben Entwicklung sichtbar zu machen.

Wert	Aussage	Datenbasis
31 %	Anteil der bestätigten Datenpannen, die laut Verizon 2026 mit Schwachstellenausnutzung begannen.	Bestätigte Breaches; Verizon DBIR [3]
32 %	Anteil der von Mandiant untersuchten Intrusionen mit Exploits als initialem Vektor.	Incident Response 2025; M-Trends [4]
28 %	Phishing oder Social Engineering als Einstieg in Microsofts Incident-Response-Untersuchungen.	Microsoft IR; MDDR [5]
82 %	Anteil malwarefreier CrowdStrike-Erkennungen 2025.	Herstellertelemetrie; CrowdStrike [6]
48 %	Anteil der Verizon-Breaches mit Ransomware-Bezug.	Bestätigte Breaches; Verizon [3]
22 Sek.	Mandiant beobachtete 2025 im Median nur 22 Sekunden zwischen initialem Zugang und der Übergabe an eine zweite Tätergruppe. Die Kennzahl beschreibt die arbeitsteilige Übergabe, nicht die gesamte Angriffsdauer.	Mandiant-Fallanalyse; nicht gesamte Angriffsdauer [4]
79 %	Anteil identitätsbezogener Ursprünge in der Sophos-Ransomware-Befragung.	Befragung betroffener Organisationen [8]
15 %	15 Prozent der im DBIR betrachteten Angriffstechniken zeigten eine Unterstützung durch generative KI.	DBIR-Technikanalyse [3]

METHODIK

Warum die Zahlen nicht direkt vergleichbar sind

Der Verizon DBIR untersucht bestätigte Datenpannen aus vielen beteiligten Organisationen. Mandiant und Microsoft werten konkrete Incident-Response-Fälle aus. CrowdStrike und Acronis sehen, was ihre Sensoren in geschützten Umgebungen erkennen. Sophos befragt Unternehmen, die tatsächlich von Ransomware betroffen waren. ENISA arbeitet überwiegend mit offenen Quellen und freiwillig bereitgestellten Informationen. Gartner liefert strategische Prioritäten, aber keine globale Vorfallstatistik. Heise/iX ergänzt die Lageberichte durch unabhängige technische Einordnungen und dokumentierte Fallbeispiele aus der Praxis. [2–12, 17–21]

Quellentyp	Beispiele	Was wird gemessen?	Grenzen
Behörden / Agenturen	BSI, ENISA	Nationale und europäische Lage, regulatorischer Kontext, offene und gemeldete Vorfälle	Breite Einordnung; nicht vollständig und durch Meldeverhalten geprägt
Bestätigte Datenpannen	Verizon DBIR	Breaches aus zahlreichen Partnerquellen	Starke Vergleichsbasis; Fokus auf bestätigte Vorfälle
Incident Response	Mandiant, Microsoft, IBM	Forensisch untersuchte reale Einbrüche	Technisch tief; Auswahl durch Kunden- und Mandatsstruktur
Herstellertelemetrie	CrowdStrike, Acronis	Erkennungsereignisse aus geschützten Endpunkten und Plattformen	Hohe operative Nähe; keine repräsentative Weltstichprobe
Befragung	Sophos	Antworten betroffener IT- und Security-Verantwortlicher	Organisatorische und wirtschaftliche Folgen; Selbstauskunft
Analystenperspektive	Gartner	Befragungen, Marktbeobachtung und strategische Einordnung	Governance und Prioritäten; keine Incident-Datenbank
Technikjournalismus	Heise / iX	Redaktionelle Prüfung, technische Fachbeiträge, konkrete Vorfälle	Unabhängige Plausibilisierung; keine globale Statistik
Rahmenwerke	NIST, CISA	Normative Orientierung und operative Handlungsempfehlungen	Struktur für Maßnahmen; keine Aussage über Häufigkeiten

Leseregel

Prozentwerte werden in diesem Whitepaper nur mit ihrer jeweiligen Datenbasis verwendet. Aus „82 Prozent malwarefreie Erkennungen“ folgt beispielsweise nicht, dass 82 Prozent aller Cyberangriffe ohne Malware erfolgen. Ebenso beschreibt der hohe DDoS-Anteil in ENISAs offenem Vorfalldatensatz nicht den Anteil von DDoS an allen erfolgreichen Unternehmenseinbrüchen.

01

Externe Angriffsfläche und Schwachstellen

Verizon sieht die Ausnutzung von Software-Schwachstellen 2026 bei 31 Prozent der bestätigten Datenpannen als häufigsten bekannten Einstieg. Mandiant kommt in seinen 2025 untersuchten Intrusionen auf 32 Prozent und damit im sechsten Jahr in Folge auf denselben führenden Vektor. IBM meldet gegenüber dem Vorjahr einen Anstieg der Ausnutzung öffentlich erreichbarer Anwendungen um 44 Prozent; 56 Prozent der ausgewerteten veröffentlichten Schwachstellen erforderten keine vorherige Authentifizierung. [3, 4, 7]

Damit wird eine operative Schwäche sichtbar: Viele Organisationen patchen nach Kalender, Angreifer handeln nach Gelegenheit. Besonders kritisch sind Internetdienste, VPNs, Firewalls, Webanwendungen, Remote-Access-Systeme, RMM-Plattformen, Identitätsdienste und administrative Schnittstellen. Eine Schwachstelle in einer Steuerungsebene ist nicht nur ein einzelnes technisches Problem – sie kann zur Eintrittstür für ganze Flotten oder Mandanten werden. [3, 7, 18–20]

Was in der Praxis zählt

- Eine vollständige und laufend aktualisierte Sicht auf alle extern erreichbaren Systeme, Domains, Zertifikate, Cloud-Dienste und administrativen Portale.
- Risikobasierte Patch-Fristen: aktiv ausgenutzte und internetnahe Schwachstellen erhalten Vorrang vor reinem CVSS-Sortieren.
- Abgleich mit dem CISA-Katalog bekannter aktiv ausgenutzter Schwachstellen und mit herstellerseitigen Sicherheitsmeldungen.[15]
- Klare Eigentümerschaft: Für jedes exponierte System muss feststehen, wer patcht, überwacht und im Notfall abschaltet.
- Reduktion unnötiger Dienste und Fernzugänge statt dauerhafter Absicherung historisch gewachsener Exposition.

Einordnung für den Mittelstand

Nicht fehlendes Fachwissen ist häufig das Kernproblem, sondern fehlende Transparenz: Ein Altserver, ein vergessenes Kundenportal, eine Testinstanz oder ein nicht mehr betreuter VPN-Zugang kann außerhalb regulärer Patch- und Monitoringprozesse weiterlaufen.

02

Identität und Vertrauen als Sicherheitsperimeter

Microsoft ordnet in seinen Incident-Response-Untersuchungen 28 Prozent der Einstiege Phishing oder Social Engineering zu, 18 Prozent ungepatchten Websystemen und 12 Prozent exponierten Remote-Diensten. Sophos berichtet in seiner Befragung betroffener Organisationen, dass 79 Prozent der Ransomware-Angriffe mit einem identitätsbezogenen Ansatz begannen. Bei 97 Prozent der Fälle, in denen kompromittierte Zugangsdaten die Ursache waren, existierte MFA grundsätzlich – die Abdeckung war jedoch häufig lückenhaft. [5, 8]

MFA bleibt deshalb unverzichtbar, aber nicht ausreichend. Microsoft bewertet phishingresistente MFA als Goldstandard und nennt für MFA insgesamt eine Blockierwirkung von mehr als 99 Prozent gegen unautorisierte Zugriffsversuche. Gleichzeitig verlagert sich das Risiko auf Session-Cookies, OAuth-Tokens, Servicekonten, API-Schlüssel, Workload-Identitäten und privilegierte technische Konten, für die klassische Benutzer-MFA nicht greift. [5, 10, 11]

Identität umfasst heute mehr als Benutzerkonten

- Menschliche Identitäten: Beschäftigte, Administratoren, externe Dienstleister und Notfallkonten.
- Maschinelle Identitäten: Dienste, Workloads, Zertifikate, Bots, Automatisierungen und API-Clients.
- Delegierte Identitäten: OAuth-Anwendungen, SaaS-Integrationen, Tokens und verbundene Drittanbieter.
- Neue Identitäten: KI-Agenten, die eigenständig Werkzeuge aufrufen, Daten verarbeiten und Aktionen auslösen. [10, 11]

Die zentrale Kontrollfrage

Welche Identität darf von welchem Gerät, aus welchem Kontext, für welchen Zeitraum und mit welcher Reichweite auf ein kritisches System zugreifen – und wie wird ein Missbrauch erkannt?

03

Legitime Werkzeuge und kanalübergreifendes Social Engineering

CrowdStrike berichtet, dass 82 Prozent seiner Erkennungen 2025 malwarefrei waren. Gemeint ist nicht, dass Schadsoftware bedeutungslos geworden ist. Angreifer nutzten gültige Zugangsdaten, vertrauenswürdige Identitätsflüsse, freigegebene SaaS-Integrationen und native Systemwerkzeuge. Acronis identifiziert PowerShell über alle beobachteten Monate hinweg als am häufigsten missbrauchte legitime Anwendung. Heise/iX bestätigt die technische Entwicklung unter dem Begriff „Living off the Land“: Angreifer verwenden Bordmittel des Systems, um sich in normale Administration einzufügen. [6, 9, 17]

Gleichzeitig wird Social Engineering interaktiver. Mandiant sah Voice-Phishing 2025 bei 11 Prozent der untersuchten Intrusionen und damit an zweiter Stelle, während klassisches E-Mail-Phishing auf 6 Prozent sank. Verizon beobachtet in Simulationen bei mobilen Kanälen wie Sprache und Textnachrichten rund 40 Prozent höhere Klickraten als bei E-Mail. Acronis sieht E-Mail weiterhin als skalierbaren Erstkontakt. Zugleich stieg der Anteil technisch fortgeschrittener Angriffe auf Kollaborationsplattformen von 12 Prozent im Jahr 2024 auf 31 Prozent im Jahr 2025. [3, 4, 9]

Ein typischer mehrstufiger Ablauf

1	**Kontakt**	Eine Nachricht, ein Anruf oder eine externe Chat-Anfrage erzeugt einen plausiblen Anlass.
2	**Vertrauen**	Der Angreifer imitiert IT-Support, Führungskraft, Lieferant oder internen Kollegen.
3	**Aktion**	Das Opfer bestätigt eine MFA-Anfrage, installiert Fernwartung oder führt einen kopierten Befehl aus.
4	**Legitime Werkzeuge**	PowerShell, WMI, RMM oder Cloud-Funktionen werden für Ausführung und Bewegung genutzt.
5	**Ausweitung**	Der Angriff wechselt in interne Chats, Filesharing, SaaS und administrative Systeme.

Konsequenz

E-Mail-Security, Endpoint-Schutz und Awareness dürfen nicht getrennt betrachtet werden. Kritische Vorgänge wie Passwort-Reset, MFA-Neuregistrierung, Zahlungsänderung, Rechtevergabe oder Fernwartungsfreigabe benötigen kanalunabhängige Verifikationsregeln.

04

Ransomware und Wiederherstellungsfähigkeit

Verizon ordnet Ransomware 48 Prozent der bestätigten Datenpannen seines 2026er Datensatzes zu. Sophos berichtet aus einer Befragung von 2.158 betroffenen Organisationen: Bei 56 Prozent wurden Daten verschlüsselt, der Median der gezahlten Lösegelder lag bei 769.000 US-Dollar und die durchschnittlichen Wiederherstellungskosten bei 1,7 Millionen US-Dollar. 66 Prozent der Organisationen mit verschlüsselten Daten nutzten Backups für die Wiederherstellung. [3, 8]

Mandiant beschreibt zugleich „Recovery Denial“: Angreifer zielen auf Identitätsdienste, Virtualisierungsmanagement, Backup-Infrastruktur und andere Tier-0-Systeme, um Wiederherstellungspunkte zu löschen, Notfallkonten unbrauchbar zu machen oder den Zugriff auf Recovery-Werkzeuge zu verhindern. CISA empfiehlt deshalb getestete, isolierte und unveränderbare Backups sowie einen dokumentierten und geübten Reaktionsplan. [4, 16]

Die Wiederherstellungsfrage muss weiter gefasst werden

- Sind Datenkopien unveränderbar oder offline und von Produktionsidentitäten getrennt?
- Können Active Directory, Entra ID, DNS, Zertifikate und andere Identitätsgrundlagen wiederhergestellt werden?
- Sind Hypervisor, Backup-Kataloge, Managementplattformen und Netzkonfigurationen separat abgesichert?
- Existieren saubere Notfallkonten und administrative Arbeitsplätze außerhalb der kompromittierbaren Produktionsumgebung?
- Wurde die Wiederherstellung bis zur tatsächlich betriebsfähigen Anwendung getestet – nicht nur bis zur erfolgreichen Rücksicherung einer Datei?
- Kann das Unternehmen kommunizieren und entscheiden, wenn E-Mail, Kollaboration oder zentrale Identitäten ausfallen? [4, 16]

Belastbare Formulierung

Ein Backup ist eine Datenkopie. Resilienz ist die nachgewiesene Fähigkeit, unter kompromittierten Bedingungen wieder einen kontrollierten Geschäftsbetrieb herzustellen.

05

Dienstleister, Control Planes und Lieferketten

Verizon berichtet, dass die Beteiligung Dritter an bestätigten Datenpannen gegenüber dem Vorjahresdatensatz um 60 Prozent zunahm und 48 Prozent der Breaches erreichte. IBM sieht große Lieferkettenvorfälle über fünf Jahre nahezu vervierfacht und nennt kompromittierte Entwickleridentitäten, CI/CD-Plattformen, SaaS-Integrationen und nachgelagerte Vertrauensbeziehungen als wiederkehrende Hebel. [3, 7]

Acronis betrachtet speziell MSPs, Telekommunikationsanbieter und RMM-Plattformen. Im eigenen Datensatz waren Phishing und ungepatchte Schwachstellen die wichtigsten dokumentierten Einstiegspunkte. Heise berichtete 2025 über Angriffe auf SimpleHelp, aktiv ausgenutzte Schwachstellen in N-able N-central sowie Spear-Phishing gegen ScreenConnect-Administratoren. Diese Fälle zeigen, dass legitime Managementsoftware sowohl als Eintrittstor als auch als Verteiler missbraucht werden kann. [9, 18–20]

Auch Softwarelieferketten bleiben relevant. Heise dokumentierte unter anderem einen großen Angriff auf das Node.js-Ökosystem. Gartner zählt Softwarelieferketten 2026 zu vier Bedrohungsfeldern mit dringendem Verbesserungsbedarf und empfiehlt unter anderem signierte Artefakte, kuratierte Repositories sowie Software- und AI Bills of Materials (AIBOMs). [12, 21]

Control-Plane-Systeme sind wie Tier-0-Systeme zu schützen

- Identitätsprovider, RMM, Backup, Virtualisierung, Netzwerkmanagement, CI/CD und zentrale SaaS-Administration als besonders kritische Systeme klassifizieren.
- Separate Administratoridentitäten, dedizierte Managementnetze und phishingresistente MFA einsetzen.
- Reichweiten begrenzen: Ein Dienstleisterkonto oder eine Automatisierung darf nicht mehr Systeme erreichen als für die konkrete Aufgabe erforderlich.
- Privilegien zeitlich begrenzen und besonders kritische Aktionen zusätzlich bestätigen.
- Protokollierung außerhalb der verwalteten Plattform sichern, damit der Angreifer nicht zugleich Spuren und Beweise entfernen kann.
- Notabschaltung und Entkopplung zentraler Verteilerfunktionen regelmäßig testen. [4, 12, 14]

> **Administrative Lieferkette**
>
> Die entscheidende Frage lautet nicht nur, welche Lieferanten ein Unternehmen hat. Entscheidend ist: Wer kann über welche Plattform, mit welchen Rechten, auf welche Systeme zugreifen – und wie weit reicht dieser Zugriff im Ernstfall?

06

KI als Beschleuniger und neue Angriffsfläche

Verizon sieht generative KI inzwischen unterstützend bei 15 Prozent der untersuchten Angriffstechniken. CrowdStrike beobachtete einen Anstieg der Angriffe durch KI-gestützte Akteure um 89 Prozent. IBM beobachtete 2025 rund 300.000 Zugangsdaten zu KI-Chatbots, die im Darknet

zum Verkauf angeboten wurden. Acronis dokumentiert KI unter anderem bei Ransomware-Verhandlungen, Skripterstellung, Datenanalyse und Zielpriorisierung. [3, 6, 7, 9]

Gleichzeitig entsteht eine neue interne Angriffsfläche. Gartner nennt für 2026 die Governance autonomer KI-Agenten, die Anpassung des Identity and Access Managements an maschinelle Akteure sowie menschliche Kontrolle in KI-gestützten Security Operations. In einer Gartner-Befragung von 175 Beschäftigten verwendeten mehr als 57 Prozent private GenAI-Konten für berufliche Zwecke; 33 Prozent gaben an, sensible Informationen in nicht freigegebene Werkzeuge eingegeben zu haben. Diese Werte sind Befragungsergebnisse, keine gemessenen Datenabflüsse. [11]

Zu den von Gartner hervorgehobenen dringenden Bedrohungen gehören Deepfakes und Identitätsimitation, Kompromittierung von KI-Anwendungen, Prompt Injection und Softwarelieferketten. Microsoft ergänzt technische Risiken wie Datenvergiftung, unkontrollierte Tool-Aufrufe und den Missbrauch von Konnektoren. [5, 12]

Zwei getrennte Aufgaben

Angriffe mit KI

KI unterstützt Recherche, Täuschung, Übersetzung, Skripterstellung, Schwachstellensuche, Datenanalyse und Erpressung. Die Methoden sind meist bekannt; Geschwindigkeit und Skalierung verändern sich.

Angriffe auf KI

Konten, Modelle, Agenten, Prompts, Konnektoren, Datenquellen und API-Schlüssel werden selbst zum Ziel. Besonders kritisch sind eigenständige Aktionen mit weitreichenden Berechtigungen.

Praktische Governance

- Alle freigegebenen und nicht freigegebenen KI-Dienste, Agenten und Konnektoren inventarisieren.
- Datenklassen festlegen und technisch durchsetzen, welche Informationen in welche Dienste übertragen werden dürfen.
- KI-Agenten als maschinelle Identitäten behandeln: eindeutige Identität, minimale Rechte, kurze Laufzeiten und vollständige Protokollierung.
- Tool-Aufrufe, externe Aktionen und irreversible Schritte mit menschlicher Freigabe absichern.
- KI-Anwendungen in Secure Development, Threat Modeling und Incident Response integrieren.
- Awareness auf konkrete Arbeitsabläufe ausrichten statt allgemeiner Verbote und Standardschulungen. [10–12]

07

Was dies für deutsche Unternehmen bedeutet

Das BSI sieht keinen Grund zur Entwarnung und betont die Bedeutung exponierter Angriffsflächen und bestehender Resilienzdefizite. ENISA wertete für seine europäische Lage 4.875 Vorfälle im Zeitraum Juli 2024 bis Juni 2025 aus und weist ausdrücklich darauf hin, dass offene Quellen und

freiwillige Meldungen kein vollständiges Bild ergeben. Diese methodische Einschränkung gilt auch für nationale und europäische Ranglisten. [1, 2]

Kommerzielle Telemetrie zeigt Deutschland in mehreren Bereichen auffällig, darf aber nicht als globale Rangliste interpretiert werden. Acronis verzeichnete innerhalb seiner Kundenbasis hohe Aktivität beim Missbrauch legitimer Werkzeuge und bei Ransomware-Erkennungen. Microsoft führte Deutschland in einer eigenen Auswertung betroffener Kunden im ersten Halbjahr 2025 auf Rang vier. Das sind jeweils herstellerspezifische Beobachtungen, keine Aussage, Deutschland sei weltweit „das am stärksten angegriffene Land“. [5, 9]

Typische strukturelle Risiken

- Historisch gewachsene On-Premises-, Cloud- und Standortarchitekturen mit unterschiedlichen Sicherheitsständen.
- Viele Dienstleister und Verträge, aber keine vollständige Sicht auf delegierte Rechte und technische Abhängigkeiten.
- Kritische Systeme mit langen Wartungsfenstern, Legacy-Komponenten oder hohen Verfügbarkeitsanforderungen.
- Knappe interne Kapazität für kontinuierliche Angriffsflächenanalyse, Patchpriorisierung und 24/7-Reaktion.
- Backups sind vorhanden, aber Wiederherstellung von Identität, Virtualisierung und Gesamtbetrieb wurde nicht realistisch getestet.
- Sicherheitsprodukte arbeiten nebeneinander, ohne dass Signale, Zuständigkeiten und Eskalationen durchgängig verbunden sind.

> **Strategische Konsequenz**
>
> Für deutsche Unternehmen ist nicht die Zahl der eingesetzten Werkzeuge der entscheidende Reifegradindikator. Gartner berichtet, dass große Unternehmen durchschnittlich 45 Cybersecurity-Werkzeuge einsetzen. Der größere Hebel liegt häufig in Konsolidierung, nachgewiesener Wirksamkeit, klaren Zuständigkeiten und belastbaren Wiederherstellungswegen. [10]

08

Prioritäten für die Praxis

GOVERN

Verantwortung und Risiko steuern

- Cyberrisiken mit Geschäftsauswirkungen, Abhängigkeiten und Risikotoleranz verbinden.
- Verantwortung für externe Systeme, Identitäten, Dienstleister und Recovery eindeutig zuweisen.
- KI-, Cloud- und Lieferkettenregeln in Beschaffung, Entwicklung und Betrieb verankern.

IDENTIFY

Sichtbarkeit herstellen

- Externe Angriffsfläche, Assets, Identitäten, Datenflüsse und Control Planes inventarisieren.
- Kritische Geschäftsservices und technische Abhängigkeiten abbilden.
- Schwachstellen nach Exposition, aktiver Ausnutzung und möglicher Reichweite priorisieren.

PROTECT

Vertrauen begrenzen

- Phishingresistente MFA, minimale Rechte und getrennte Administration umsetzen.
- Netze, Mandanten und Managementebenen segmentieren.
- Backups und Recovery-Identitäten isolieren; unnötige Exposition entfernen.

DETECT

Verhalten und Kontext erkennen

- Endpoint-, Identitäts-, Netzwerk-, Cloud-, E-Mail- und SaaS-Telemetrie korrelieren.
- Missbrauch legitimer Werkzeuge und ungewöhnliche administrative Aktionen erkennen.
- Protokolle außerhalb kompromittierbarer Control Planes sichern.

RESPOND

Entscheidungen beschleunigen

- Automatisierte Eindämmung für definierte Hochrisikosignale vorbereiten.
- Eskalationswege, Abschaltbefugnisse und externe Unterstützung vorab klären.
- Tabletop- und technische Übungen mit realistischen Ausfallszenarien durchführen.

RECOVER

Wiederanlauf nachweisen

- Unveränderbare und getrennte Datenkopien regelmäßig testen.
- Identität, Virtualisierung, Netzwerk, Konfiguration und Anwendungen gemeinsam betrachten.
- Recovery-Ziele an Geschäftsbetrieb und nicht nur an Datenrücksicherung messen.

Zero Trust liefert dafür ein wichtiges Architekturprinzip: Vertrauen wird nicht aufgrund von Netzposition oder Herkunft vorausgesetzt, sondern für jede Ressource, Identität und Transaktion fortlaufend bewertet und möglichst eng begrenzt. CISA ergänzt die operative Priorisierung durch den Katalog bekannter aktiv ausgenutzter Schwachstellen und den #StopRansomware-Leitfaden. [13–16]

09

Wie lancon helfen kann

Die Rolle von lancon besteht nicht darin, pauschal weitere Sicherheitsprodukte zu empfehlen. Ausgangspunkt ist die Frage, wo reale Angriffsflächen, unkontrollierte Vertrauensbeziehungen und kritische Abhängigkeiten bestehen – und welche Maßnahmen im jeweiligen Unternehmen den größten Beitrag zur Risikoreduktion leisten.

Sichtbarkeit schaffen

Externe Systeme, Internetdienste, Domains, Zertifikate, Cloud-Ressourcen und öffentlich erkennbare Schwachstellen strukturiert erfassen. Dazu kann ein passives External Attack Surface Assessment gehören, das ausschließlich öffentlich verfügbare Informationen nutzt.

Abhängigkeiten bewerten

Identitäten, administrative Zugänge, Dienstleister, RMM, Backup, Virtualisierung, Netze und Cloud-Plattformen als zusammenhängende Infrastruktur analysieren. Kritische Control Planes und Single Points of Failure sichtbar machen.

Architektur und Maßnahmen priorisieren

Segmentierung, Zero Trust, Identity Security, Exposure Management, Detection, Backup und Recovery nach Geschäftskritikalität, Umsetzbarkeit und Risikowirkung ordnen.

Lösungen und Anbieter einordnen

Bestehende Produkte auf Wirksamkeit, Überschneidungen und Lücken prüfen. Geeignete Anbieter und Betriebsmodelle anbieterneutral auswählen, statt eine vorgegebene Produktlandschaft zu rechtfertigen.

Wiederanlauf und Reaktion erproben

Incident-Response- und Recovery-Szenarien mit Verantwortlichen, Dienstleistern und Technikteams durchspielen. Prüfen, ob Entscheidungen, Kommunikation und Wiederherstellung auch unter kompromittierten Bedingungen funktionieren.

Roadmap und Umsetzung steuern

Aus Befunden eine belastbare Maßnahmenplanung mit Zuständigkeiten, Reihenfolge, Budgetrahmen und überprüfbaren Ergebnissen entwickeln – und die Umsetzung über interne und externe Beteiligte hinweg begleiten.

Positionierung

lancon schafft Orientierung zwischen Bedrohungslage, technischer Infrastruktur, Dienstleistern und konkreten Entscheidungen. Das Ziel ist nicht maximale Komplexität, sondern eine Sicherheitsarchitektur, deren Wirkung, Zuständigkeiten und Wiederherstellungsfähigkeit nachvollziehbar sind.

FAZIT

Bekannte Schwächen werden industriell ausgenutzt

Die wichtigste Verschiebung liegt nicht in einer einzelnen Technologie. Sie liegt darin, dass Angriffe sich in reguläre Prozesse, gültige Identitäten und zentrale Plattformen einfügen. Damit wird die Grenze zwischen IT-Betrieb und Sicherheitsvorfall unschärfer.

Unternehmen benötigen deshalb nicht zwingend mehr Einzellösungen. Sie benötigen eine belastbare Sicht auf ihr Gesamtsystem: externe Angriffsfläche, Identitäten, Rechte, Dienstleister, Control Planes, Erkennung, Reaktion und Wiederherstellung.

Die entscheidende Frage

Kennen und kontrollieren wir unsere externen Systeme, Identitäten, administrativen Abhängigkeiten, Dienstleisterzugänge und Wiederherstellungswege als zusammenhängende digitale Infrastruktur?

QUELLEN

Vollständiges Quellenverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI). Die Lage der IT-Sicherheit in Deutschland 2025. 11.11.2025. Abruf: 27.07.2026. *Behördlicher Lagebericht; Deutschland.*

[2] European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2025, Version 1.2. 01.10.2025; Revision 09.01.2026. Abruf: 27.07.2026. *4.875 analysierte Vorfälle; überwiegend offene Quellen und freiwillige Meldungen.*

[3] Verizon. 2026 Data Breach Investigations Report (DBIR). 2026. Abruf: 27.07.2026. *Bestätigte Sicherheitsvorfälle und Datenpannen aus zahlreichen Partnerquellen.*

[4] Google Cloud / Mandiant. M-Trends 2026: Executive Edition. 23.03.2026. Abruf: 27.07.2026. *Incident-Response-Erkenntnisse aus mehr als 500.000 Untersuchungsstunden im Jahr 2025.*

[5] Microsoft. Microsoft Digital Defense Report 2025. 2025. Abruf: 27.07.2026. *Globale Plattform-, Identitäts- und Incident-Response-Daten.*

[6] CrowdStrike. 2026 Global Threat Report. 2026. Abruf: 27.07.2026. *Herstellertelemetrie und Threat-Hunting-Erkenntnisse.*

[7] IBM X-Force. X-Force Threat Intelligence Index 2026. 25.02.2026. Abruf: 27.07.2026. *Incident-Response-, Schwachstellen- und Threat-Intelligence-Daten.*

[8] Sophos. The State of Ransomware 2026. 15.07.2026. Abruf: 27.07.2026. *Anbieteragnostische, von Sophos beauftragte Befragung von 2.158 betroffenen Organisationen.*

[9] Acronis Threat Research Unit. Acronis Cyberthreats Report H2 2025: From exploits to malicious AI. 2026. Abruf: 27.07.2026. *Telemetrie von mehr als einer Million Endpunkten sowie öffentliche Ransomware-Daten; Schwerpunkt MSP und Windows.*

[10] Gartner. Gartner Identifies the Top Cybersecurity Trends for 2025. 03.03.2025. Abruf: 27.07.2026. *Strategische Einordnung zu GenAI, maschinellen Identitäten, Konsolidierung und Sicherheitskultur.*

[11] Gartner. Gartner Identifies the Top Cybersecurity Trends for 2026. 05.02.2026. Abruf: 27.07.2026. *Agentic AI, IAM für KI-Agenten, Human-in-the-loop und adaptive Awareness.*

[12] Gartner. Gartner Identifies Four Critical Threats Requiring Urgent Improvements from Cybersecurity Leaders. 02.06.2026. Abruf: 27.07.2026. *Deepfakes, KI-Anwendungen, Prompt Injection und Softwarelieferketten.*

[13] National Institute of Standards and Technology (NIST). NIST-Cybersicherheits-Framework (CSF) 2.0 – deutsche Übersetzung. 26.02.2024 / deutsche Übersetzung 22.11.2024. Abruf: 27.07.2026. *Govern, Identify, Protect, Detect, Respond und Recover.*

[14] National Institute of Standards and Technology (NIST). SP 800-207: Zero Trust Architecture. August 2020. Abruf: 27.07.2026. *Architekturprinzipien für ressourcen- und identitätsbezogene Zugriffskontrolle.*

[15] Cybersecurity and Infrastructure Security Agency (CISA). Known Exploited Vulnerabilities Catalog. laufend aktualisiert. Abruf: 27.07.2026. *Katalog nachweislich aktiv ausgenutzter Schwachstellen.*

[16] Cybersecurity and Infrastructure Security Agency (CISA). #StopRansomware Guide. Version 2023; PDF-Stand 2025. Abruf: 27.07.2026. *Prävention, Erkennung, Reaktion und Wiederherstellung bei Ransomware.*

[17] Heise / iX. Cyberangriffe ohne Malware: Living off the Land. 15.04.2025. Abruf: 27.07.2026. *Unabhängige technische Einordnung zum Missbrauch nativer Systemwerkzeuge.*

[18] Heise online. Cyberangriffe auf SimpleHelp RMM beobachtet. 31.01.2025. Abruf: 27.07.2026. *Konkreter RMM-Fall.*

[19] Heise online. Angriffe auf N-able N-central laufen – mehr als 1000 Systeme ungepatcht. 19.08.2025. Abruf: 27.07.2026. *Aktive Ausnutzung einer MSP-/RMM-Plattform.*

[20] Heise online. ScreenConnect-Admins im Visier von Spear-Phishing-Angriffen. 26.08.2025. Abruf: 27.07.2026. *Identitäts- und RMM-bezogener Angriffsfall.*

[21] Heise online. Großer Angriff auf node.js. 09.09.2025. Abruf: 27.07.2026. *Beispiel für Softwarelieferkettenrisiken.*

[22] Die Zuordnung nennt den jeweils dominierenden Quellentyp. Mehrere Berichte kombinieren Incident-Response-Daten, Herstellertelemetrie, Threat Intelligence und externe Datensätze.