

Erhöhtes Risiko in 2026 für

DEUTSCHE Mittelstands UNTERNEHMEN



TEAL
ALWAYS CHALLENGING IT

DIE BEDEUTUNG VON CYBER SECURITY

GEFAHREN UND BEDROHUNGEN FÜR UNTERNEHMEN LAUERN ÜBERALL



Im Jahr 2026 gehört Cyber Security nicht mehr in die Schublade „IT-Thema“. Sie ist längst zu einer zentralen Managementaufgabe geworden, vergleichbar mit Finanzplanung oder Personalstrategie. Die Zahl der Angriffe wächst stetig, die Professionalität der Täter steigt, und die Schäden für Unternehmen sind enorm.

WICHTIG FÜR DEN MITTELSTAND

Viele Mittelständler gelten als „leichte Beute“, weil sie oft weniger Schutzmaßnahmen implementiert haben als internationale Wettbewerber. Während früher vor allem große Konzerne im Fokus standen, geraten heute zunehmend auch mittelständische Unternehmen ins Visier. Cyber Security ist kein Nice to Have, sondern ein Muss. Angreifer bleiben oft anonym oder ungefasst und hinterlassen riesige Schäden.

WELCHE ZIELE HABEN DIE ANGREIFER?

In Deutschland sind wir zwar technologisch stark, doch beim Thema Cyber-Sicherheit zeigt der internationale Vergleich eine deutliche Lücke. Länder wie die USA oder skandinavische Nationen sind uns voraus.

- ✓ Lieferketten werden blockiert
- ✓ Sensible Daten werden gestohlen
- ✓ Der Geschäftsbetrieb kann nicht fortfahren



CYBER ANGRIFFE AUS DEM JAHR 2025

DEUTSCHLAND UND SEINE SWEETSPOTS FÜR HACKER

Branchenübergreifend stellen wir fest, dass Deutsche Unternehmen großflächig Angriffsziele für Cyber-Kriminelle bieten. Kosten in Milliardenhöhe fallen jährlich für Vorfälle wie Datendiebstahl und Betriebsausfälle an.

Internationale Spannungen machen die Situation noch bedrohlicher. Vor allem Unternehmen die eine Rolle für die Infrastruktur des Landes spielen, werden in hybriden Konfliktsituationen häufig Opfer von professionellen Angreifern. Wer hier nicht die Anforderungen erfüllt, muss mit Strafen rechnen.



CEO Fabian Böhm reist regelmäßig zu Unternehmen im DACH Raum um im Bereich Cyber Security aufzuklären

PRODUKTION

Deutsche Maschinenbauer wurde Opfer einer Ransomware-Attacke. Produktionen standen Still – Zweistellige Millionenkosten

GESUNDHEITSWESEN

Krankenhausnetzwerke wurde gehackt. IT Systeme mussten heruntergefahren werden und Patientendaten wurden durchsucht.

VERWALTUNGEN

Im Sommer traf es eine deutsche Großstadtverwaltung. Bürgerdienste waren für Tage Handlungsunfähig.

DER INTERNATIONALE VERGLEICH

DEUTSCHLAND ALS KRITISCH EINZUSCHÄTZEN

Zwar ist das Bewusstsein für Cyber-Gefahren gestiegen, doch in der Umsetzung hinken viele Unternehmen hinterher. Im internationalen Vergleich zeigt sich: Während die Investitionen in den USA und Israel systematisch steigen, sind deutsche Unternehmen noch zurückhaltend, oft aus Kostengründen oder fehlendem Know-how

WER IST ZUSTÄNDIG IM UNTERNEHMEN?

Ein zentraler Unterschied: In vielen Ländern gilt Cyber Security bereits als Chefsache. Dort wird nicht gefragt, ob man investiert, sondern wie viel. In Deutschland hingegen werden Budgets oft nur nach einem Vorfall freigegeben. Dieses reaktive Verhalten führt zu einer gefährlichen Lücke im Schutz.

REIFEGRAD IM INTERNATIONALEN VERGLEICH

Land	Indikativer Reifegrad 1-5	Konfidenz	Quelle
Israel	5	Hoch	GCI, Branchenreport
USA	4	Hoch	Cisco Readiness
Skandinavien	4	Hoch	EU-/Nationalreports
Deutschland	2-3	Mittel	GCI, PwC, Statista
Südeuropa	2	Niedrig	IT Marktanalysen

Wichtig: Werte sind indikativ und basieren auf einer Kombination öffentlicher Indizes, Branchenstudien und TEAL-Expertenbewertung. Für belastbare Länder- oder Branchenbenchmarks empfehlen wir gezielte Erhebungen und Primärdaten.

UNSERE **HANDLUNGSEMPFEHLUNG**

DEUTSCHLAND ALS KRITISCH EINZUSCHÄTZEN

Was bedeutet das für dich als Geschäftsführer? Die Fakten sind klar: Viele Deutsche Unternehmen sind angreifbar. Die Kosten für Erpressungsgelder und Strafen von Audits sorgen regelmäßig für 6-Stellige Verluste. Delegiere nicht ausschließlich an die IT sondern mach Sicherheitsentscheidungen zur Chefsache.

WAS IST MEIN ERSTER SCHRITT ALS GESCHÄFTSFÜHRER?

Viele Unternehmen wissen gar nicht, wie angreifbar sie sind. Ein Reifegrad-Check ist der erste Schritt, um Transparenz zu schaffen. Sicherheit ist kein Einmalprojekt. Es geht um kontinuierliche Anpassung, technologisch und organisatorisch. Lass von einem Experten einschätzen, welche "Türen" sofort geschlossen werden müssen und wo es langfristig Bedarfe gibt.

MIT TEAL IN DIE UMSETZUNG STARTEN

Genau hier unterstützt TEAL Consulting. Wir sind ein spezialisiertes Cyber-Security-Beratungsunternehmen mit Fokus auf Microsoft-Umgebungen. Unser Ansatz: pragmatisch, messbar und individuell auf Ihr Geschäftsmodell zugeschnitten. Gemeinsam entwickeln wir eine Sicherheitsstrategie, die realistisch umsetzbar ist und sofort Wirkung zeigt. Von der Analyse über den Maßnahmenplan bis zur Schulung der zuständigen Mitarbeiter.

KOSTENFREIE UND INDIVIDUELLE BERATUNG

Du möchtest mit uns über deine individuelle Situation im Unternehmen sprechen?

JETZT KOSTENLOSEN CALL BUCHEN

