#CybersicherheitJETZT

Bevor es zu spät ist

Ein Vorschlag der Wolfram Consult GmbH & Co. KG, die Cybersicherheit in Deutschland durch Sensibilisierung, Basisschutz und klare Verantwortung messbar zu verbessern

Berlin, Oktober 2026

Unsere Kernbotschaft

Das Wissen ist meist vorhanden. Es fehlt die Aufmerksamkeit, bevor etwas passiert.

Beobachtung

Interesse an IT-Sicherheit entsteht in vielen Betrieben erst nach dem Vorfall, wenn der Schaden schon da ist.

Folge

Gesetze, Förderangebote und Warnungen existieren, erreichen aber nicht die Menschen, die handeln müssten.

Vorschlag

Sensibilisierung muss zur Routine werden, wie Brandschutz: regelmäßig, verständlich, verpflichtend.

Die Lage: Angriffe sind zum Normalfall geworden

58 %

der Unternehmen erlitten in den letzten 12 Monaten einen Schaden durch Cyberangriffe

Bitkom 2026

160–206 Mrd. €

Schaden allein durch Cyberangriffe in der deutschen Wirtschaft (Korridor 2026)

Bitkom 2026

~80 %

der gemeldeten Ransomware-Angriffe treffen kleine und mittlere Unternehmen

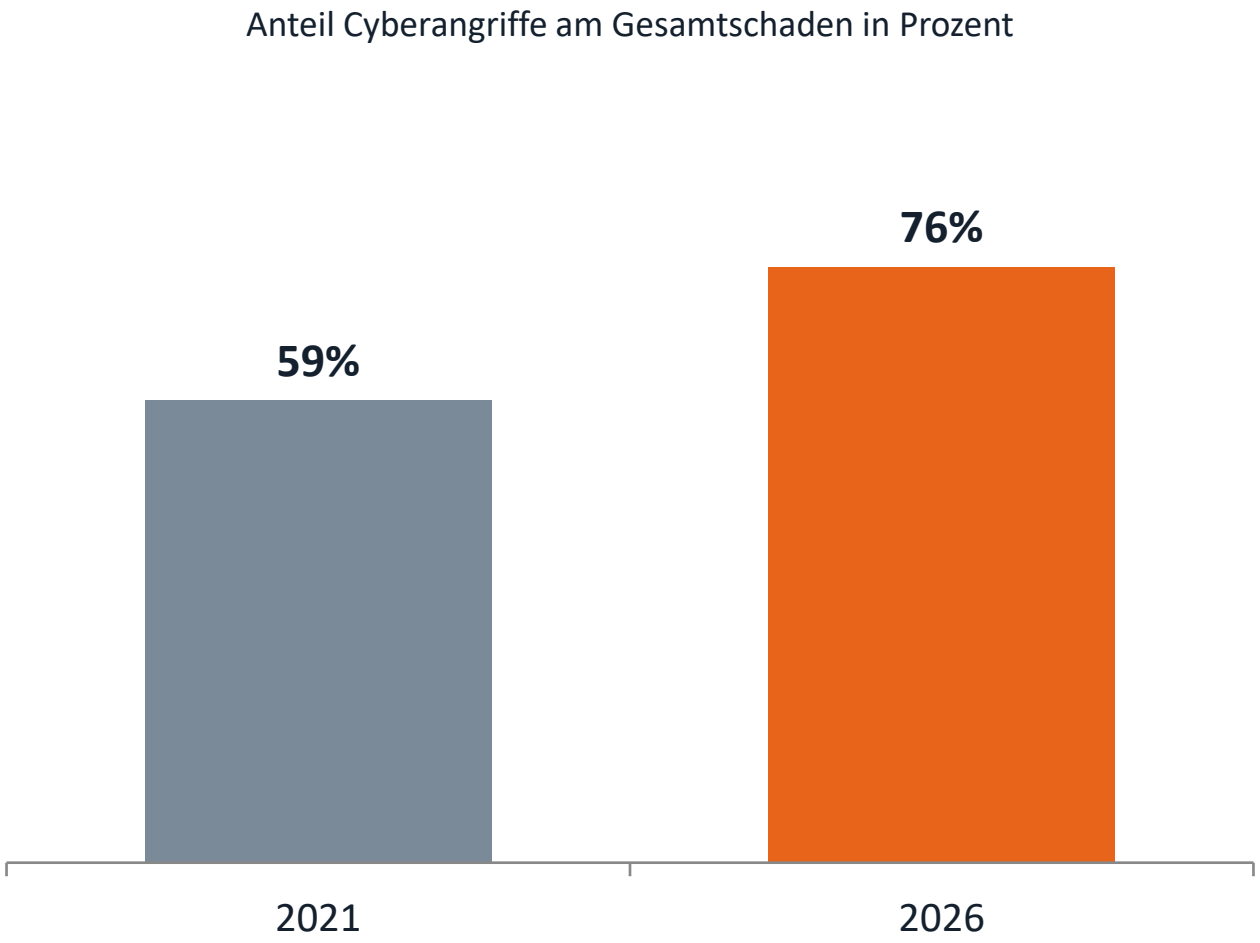
BKA, zit. n. BSI-Lagebericht 2025

0 %

der befragten Unternehmen rechnen mit einem Rückgang; 69 % erwarten eine Zunahme

Bitkom 2026

Der Cyberanteil am Wirtschaftsschaden wächst



Was das bedeutet

Diebstahl, Spionage und Sabotage finden immer häufiger digital statt. Der Schutz von Servern, Konten und Daten ist damit zum Kern des Wirtschaftsschutzes geworden.

Auch im Korridor 2026 bewegt sich der Gesamtschaden im dreistelligen Milliardenbereich.

Quelle: Bitkom, Wirtschaftsschutz 2026

PHP2Shell: Zwei Jahre Vorlauf, ein Tag Alarm

2024

Ein externes Sicherheitsaudit findet erste Hinweise auf das Problem im PHP-Kern. Ein konkreter Angriffsweg wird nicht gefunden.

2024–2026

Der Fix stockt monatelang. Die PHP Foundation nennt das später selbst einen „strukturellen Fehler“.

20.10.2026

Details zu den Lücken sickern vorzeitig durch und verbreiten sich online.

21.10.2026

Notfall-Patch. Das BSI warnt auf Stufe 3 / Orange; erste Angriffsversuche werden beobachtet.

Danach

Kommunen, Hochschulen und Kammern nehmen Webportale vorsorglich vom Netz.

Die Fachwelt kannte das Problem seit 2024. Die breite Öffentlichkeit erfuhr davon, als die Angreifer schon unterwegs waren.

Was PHP2Shell über Deutschland verrät

Eine Lücke, ein Großteil des Webs

PHP läuft auf rund 70 % aller Websites mit bekannter Serversprache, darunter WordPress, Typo3, Shops und Portale von Stadtwerken.

Patchen ist der langsame Teil

Exploits entstehen in Stunden. Updates müssen auf jedem einzelnen Server eingespielt werden, und genau dort hakt es.

Veraltete Systeme ohne Fix

Für ältere PHP-Versionen gibt es keine offiziellen Patches. Wer nie aktualisiert hat, steht im Ernstfall ohne Lösung da.

Unterfinanzierte Grundlagen

Die PHP Foundation bittet Unternehmen, Hoster und öffentliche Stellen, ihre Sicherheitsarbeit mitzufinanzieren.

Die Regeln gibt es. Die Umsetzung hinkt hinterher

NIS2-Umsetzungsgesetz

In Kraft seit 6. Dezember 2025, ohne Übergangsfrist. Rund 29.500 Unternehmen in 18 Sektoren betroffen.

18.500

von erwarteten 29.500 Unternehmen hatten sich bis Ende Mai 2026 beim BSI registriert

Umsetzungsstand NIS2

Registrierung ist nicht gleich Sicherheit: Risikomanagement, Meldewege und Lieferkette müssen gelebt werden.

34 %

der Unternehmen haben die NIS2-Vorgaben laut einer Studie vollständig umgesetzt

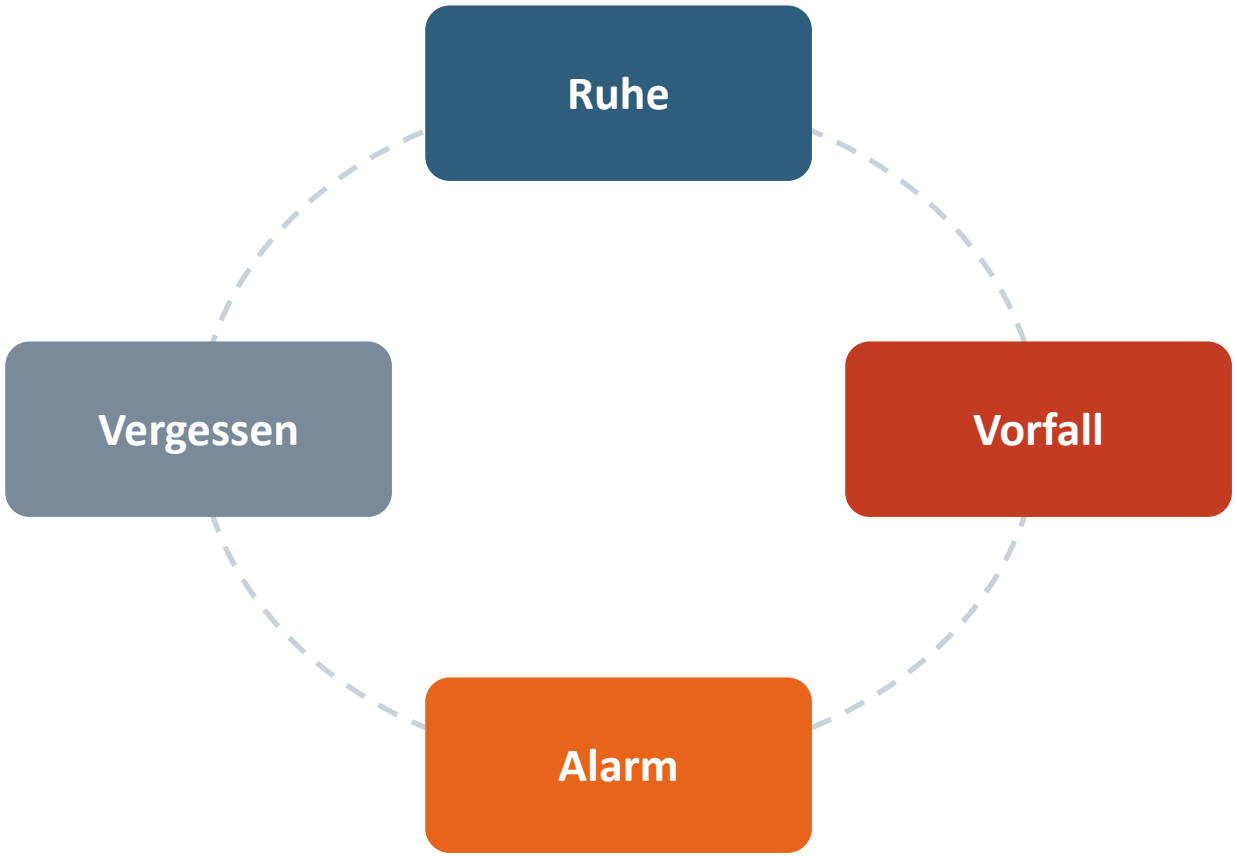
Cyber Resilience Act

Seit 11. September 2026 müssen Hersteller ausgenutzte Schwachstellen binnen 24 Stunden melden.

29 %

der Befragten kannten die Bedeutung des CRA, 28 % war er gänzlich unbekannt

Das Muster, das wir durchbrechen wollen



Die Phasen im Detail

- Ruhe: „Uns trifft es schon nicht.“
- Vorfall: Lücke, Leak oder Angriff
- Alarm: Kurze, hektische Aufmerksamkeit
- Vergessen: Zurück zum Tagesgeschäft

Ziel unseres Vorschlags: Die Aufmerksamkeit dauerhaft in der Phase „Ruhe“ verankern, also dort, wo Vorbeugung noch billig ist.

Unser Vorschlag: sieben Hebel

Sensibilisierung steht im Mittelpunkt. Die übrigen Hebel sorgen dafür, dass aus Aufmerksamkeit tatsächlich Schutz wird.

Sieben Hebel für mehr Cybersicherheit

1

Sensibilisierung als Routine

Verständliche, regelmäßige Lageinformation für Entscheider

2

Notfallübungen wie Brandschutz

Jährliche Übung für Betriebe, mit fertigen Vorlagen

3

Basisschutz-Siegel

Fünf Pflichtpunkte, gekoppelt an Förderung und Vergabe

4

Warnen statt zuschauen

Kostenlose Scans und direkte Warnung an Betreiber

5

Grundlagen finanzieren

Open-Source-Sicherheit stärker öffentlich mittragen

6

Hersteller in die Pflicht

Secure by Default und Updatepflicht konsequent durchsetzen

7

Fachkräfte und Hilfe vor Ort

Regionale Ansprechpartner, Ausbildung, Quereinstieg

Schwerpunkt

Hebel 1 und 2 adressieren direkt die Sensibilisierungslücke.

Hebel 1 und 2: Aufmerksamkeit vor dem Ernstfall

Sensibilisierung als Routine

- Monatlicher „Cyber-Wetterbericht“ in Alltagssprache, über Kammern, Verbände und Hoster verteilt
- Warnungen wie bei PHP2Shell mit klarer Handlungsanweisung: Wer ist betroffen, was ist bis wann zu tun
- Kurzformat für Geschäftsführungen: 30 Minuten pro Quartal, ohne Fachjargon
- Bestehende Angebote wie die Transferstelle Cybersicherheit im Mittelstand sichtbarer machen

Notfallübungen wie Brandschutz

- Jährliche Übung „Tag X“: Was tun wir, wenn morgen die Server verschlüsselt sind?
- Fertige Übungsvorlagen für Betriebe ohne eigene IT-Abteilung
- Prüfen, ob Backups sich tatsächlich zurückspielen lassen
- Notfallnummern und Zuständigkeiten liegen ausgedruckt vor, nicht nur auf dem betroffenen Server

Hebel 3 und 4: Basisschutz und Frühwarnung

Basisschutz-Siegel: fünf Punkte, die die meisten Angriffe verhindern

1. Mehr-Faktor-Anmeldung für alle Zugänge von außen
2. Sicherheitsupdates innerhalb fester Fristen
3. Offline-Backups, regelmäßig zurückgespielt und getestet
4. Keine offen erreichbaren Admin- und Fernwartungszugänge
5. Ein benannter Verantwortlicher und ein Notfallplan

Gekoppelt an Förderprogramme, öffentliche Vergabe und Versicherungsprämien

Warnen statt zuschauen

- Kostenlose, regelmäßige Scans nach verwundbaren, öffentlich erreichbaren Systemen in Deutschland
- Direkte Benachrichtigung der Betreiber über Hoster und Provider, nicht nur ein Eintrag auf einer Website
- Bei Lücken wie PHP2Shell: gezielte Warnung innerhalb von Stunden

Hebel 5 bis 7: Strukturen stärken

Grundlagen finanzieren

Software wie PHP trägt große Teile des Webs, wird aber knapp finanziert. PHP2Shell zeigt die Folgen. Vorschlag: Öffentliche Hand und große Nutzer finanzieren Sicherheitsarbeit kritischer Open-Source-Projekte dauerhaft mit, etwa über bestehende Förderstrukturen wie die Sovereign Tech Agency.

Hersteller in die Pflicht

Der Cyber Resilience Act schafft den Rahmen. Vorschlag: konsequente Marktaufsicht, sichere Werkseinstellungen und verbindliche Mindest-Updatezeiträume, über die Kunden vor dem Kauf informiert werden.

Fachkräfte und Hilfe vor Ort

Kleine Betriebe brauchen erreichbare Ansprechpartner. Vorschlag: regionale Anlaufstellen bei Kammern ausbauen, Quereinstieg in IT-Sicherheit fördern und Dienstleister für den Notfall vorab vermitteln.

Fahrplan und messbare Ziele

0–6 Monate · Sofort

- Cyber-Wetterbericht starten
- Bestehende Hilfsangebote bündeln und bewerben
- NIS2-Registrierung auf 100 % bringen

6–18 Monate · Aufbau

- Basisschutz-Siegel einführen
- Frühwarnung über Provider etablieren
- Erste landesweite Notfallübung

18–36 Monate · Verankern

- Siegel an Förderung und Vergabe koppeln
- Dauerhafte Open-Source-Förderung
- Jährliche Wirkungsmessung

Woran wir Erfolg messen würden

Weniger Betroffene
Anteil geschädigter Unternehmen (Bitkom) sinkt jährlich

Schneller gepatcht
Zeit bis kritische Lücken auf deutschen Servern geschlossen sind

Mehr Vorbereitung
Anteil Betriebe mit getestetem Notfallplan und Backup

Warum dieser Vorschlag von uns kommt

Wir sind kein Sicherheitskonzern. Wir betreiben selbst Websites, interne Systeme und Kundenprojekte und erleben die Lage aus der Praxis eines Berliner Mittelständlers.

Praxisblick

Wir sehen, wie Warnungen bei Betrieben ankommen, und wo sie untergehen.

Verantwortung

Mit den „Universal Ethical Guidelines for Intelligent Systems“ haben wir 2025 festgehalten: Entscheidend ist das Handeln, nicht die Erklärung (§3). Derselbe Grundsatz trägt diesen Vorschlag.
wolfram-consult.com/ai-ethics

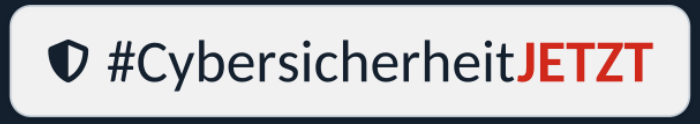
Gesprächsbereitschaft

Wir bringen unsere Erfahrung gern in Arbeitsgruppen, Pilotprojekte oder Anhörungen ein.

Machen Sie mit: #CybersicherheitJETZT

Möchten Sie mithelfen, dem Thema Cybersicherheit mehr Aufmerksamkeit zu geben? Dann laden Sie unseren Web-Button herunter, platzieren Sie ihn gut sichtbar auf Ihrer Website und verweisen Sie damit auf dieses Dokument.

So sieht der Button aus



Mit der Prüfsumme lässt sich kontrollieren, dass die heruntergeladene Datei unverändert ist.

1. **Button herunterladen**

   https://securemaker.de/files/Button-Cybersicherzeit.zip

2. **Auf der eigenen Website einbinden**

   Der fertige HTML-Schnipsel liegt im ZIP bei.

3. **Auf dieses Dokument verlinken**

   https://securemaker.de/Cybersicherheit-Deutschland-Initiative.pdf

SHA-256 der ZIP-Datei: `944a1b650d1a5d419361d2507811c809055b205565beb67f1a366ca47287e28a`

Sicherheit beginnt vor dem Ernstfall

Wolfram Consult GmbH & Co. KG · Berlin · Wir freuen uns auf den Austausch.

Quellen

- BSI: Die Lage der IT-Sicherheit in Deutschland 2025 (11.11.2025) – bsi.bund.de
- Bitkom: Wirtschaftsschutz 2026, Präsentation und Studienbericht (26.08.2026) – bitkom.org
- PHP Foundation, Blogpost zu PHP2Shell (21.10.2026), berichtet u. a. von thenextweb.com und trendingtopics.eu
- SecurityWeek: PHP2Shell – Mass Exploitation Looms (20./21.10.2026)
- ZfK: PHP-Lücke – Kommunen schalten Webportale vorsorglich ab (21.10.2026)
- CybelAngel: What We Know About php2shell (Shodan-Zählung vom 20.10.2026)
- NIS2UmsuCG: secjur.com, ihk.de; Registrierungsstand: boerse-express.com (Juni/Juli 2026)
- Cyber Resilience Act, Meldepflichten ab 11.09.2026: BSI, borncity.com, it-daily.net
- BMWE: Transferstelle Cybersicherheit im Mittelstand, Aktionsmonat Cybersicherheit (01.10.2026)
- Wolfram Consult: Universal Ethical Guidelines for Intelligent Systems (20.04.2025) – wolfram-consult.com/ai-ethics
- Notebookcheck: BKA-Angabe zu Ransomware-Angriffen auf KMU (zum BSI-Lagebericht 2025)