Cybersicherheit am Arbeitsplatz

IT Security Day

01. Oktober 2026, Castrop-Rauxel

Bundesamt
für Sicherheit in der
Informationstechnik

Michael Krauß, Referat W 25 „Cybersicherheit bei KMU“
Bundesamt für Sicherheit in der Informationstechnik

Bild: © AdobeStock/Nirut

Unsere Stakeholder

- Staat
- Wirtschaft
- Gesellschaft
- Wissenschaft

Prävention

Detektion

Reaktion

- Übernahme technischer Schutzmaßnahmen
- Nationales IT-Lagezentrum
- Technische Unterstützung und Dienstleistungen
- CERT-Bund und MIRTs
- Beratung und Service-Center
- Kooperation
- Allianz für Cybersicherheit
- UP KRITIS
- Begleitung in der Aus- und Fortbildung
- Technische Richtlinien
- Zertifizierung
- IT-Sicherheitskennzeichen

Bundesamt für Sicherheit in der Informationstechnik

Gründung

01. Januar 1991

Bundesministerium des Innern und für Heimat

Bundesamt für Sicherheit in der Informationstechnik

Stellen 2026

~1.800

379 Mio. Euro

Haushalt 2026

36 %* **Frauen**

64 % **Männer**

*Anteil in Leitungsfunktion: 28 %

Stand: 31.12.2025

Neue Technologien – neue Unsicherheiten

KI als Werkzeug der Angreifer

KI-assistierte Ransomware-Angriffe

- KI-Programmierassistenten
  - **beschleunigen** Erstellung von Schadcode
  - verringern benötigtes Vorwissen
- KI **beschleunigt** die Analyse und Ausnutzung von Schwachstellen
- KI ermöglicht **skalierbare** Verteilung von Schadsoftware durch hochwertiges & individualisiertes Social Engineering
- KI **beschleunigt** Auswertung exfiltrierter Daten
- KI „unterstützt“ Betroffene bei Bezahlung des Lösegelds in Kryptowährung
- KI-Agenten (OpenClaw) attraktives Ziel für Identitätsdiebstahl

Kein Zukunftsthema: Angreifer nutzen KI bereits heute
-> KI ermöglicht **höhere Produktivität** (Geschwindigkeit von Angreifern)
-> KI ermöglicht **skalierbare Angriffe** (über Sprachbarrieren hinweg)

Cybersicherheit muss Top-Priorität sein
KI-Produktivitätsgewinn auch für Verteidigung nutzen

Geschwindigkeit

Skalierung

Die Lage der IT-Sicherheit in Deutschland 2025

Die IT-Sicherheitslage in Deutschland 2025 ist weiterhin auf einem angespannten Niveau

- Angriffsflächen noch immer zu schlecht geschützt
- Insbesondere KMU sowie Institutionen des (vor)politischen Raums betroffen
- Trotz Erfolgen internationaler Strafverfolgungsbehörden gegen Cybercrime-Angreifergruppen:
  - zunehmende Ausnutzung von Schwachstellen (Exploitation)
  - mehr Exfiltration und Veröffentlichung von Daten (Datenleaks)
- Zunahme der APT-Aktivitäten im Kontext geopolitischer Konflikte

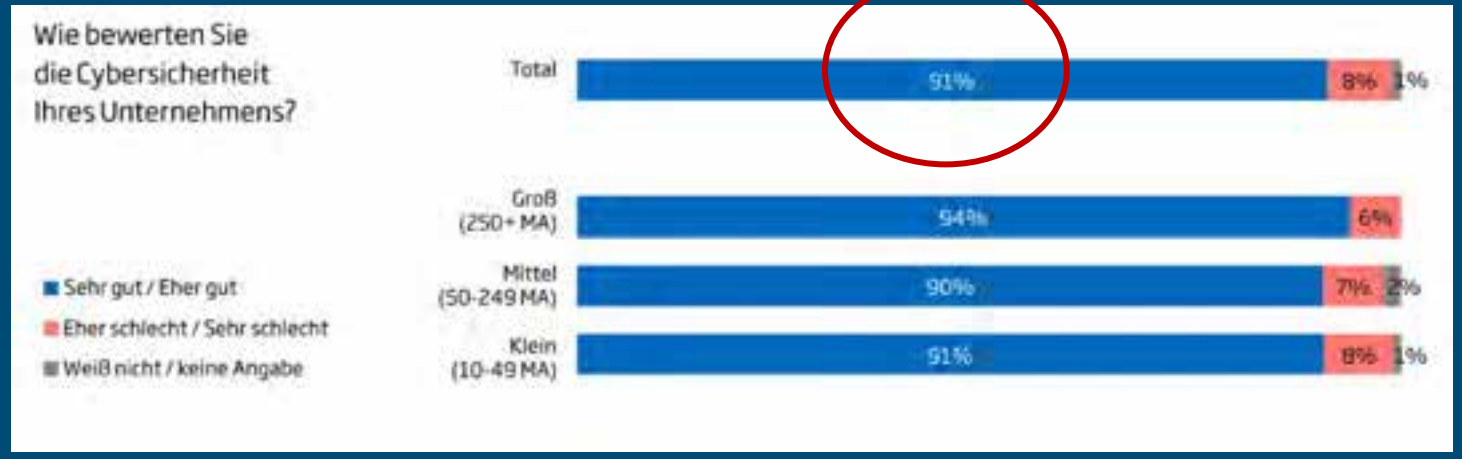
Bedrohungslage - weitere Studien

TÜV Cybersecurity Studie 2025

Cyberbedrohungen wachsen, aber viele Unternehmen hinken beim Schutz hinterher. Die TÜV Cybersecurity Studie 2025 zeigt: KI-gestützte Angriffe nehmen zu, doch nur wenige Betriebe setzen KI zur Verteidigung ein. Die Studie liefert alarmierende Zahlen – und klare Handlungsempfehlungen für Politik und Wirtschaft.

#studie #safety&security #cybersecurity #ki

- IT-Sicherheitsvorfälle nehmen zu: 15 Prozent der Unternehmen sind 2024 Opfer eines Cyberangriffs geworden – das ist ein Anstieg um 4 Prozentpunkte im Vergleich zur → TÜV Cybersecurity Studie 2023. Besonders häufig: Phishing (84 Prozent).



Bundesamt für Sicherheit in der Informationstechnik

Befragung zur Cybersicherheit 2025

CyMon
Der Cybersicherheitsmonitor

Kurzbericht zur Studie der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Welche der folgenden Schutzmaßnahmen vor Gefahren im Internet verwenden Sie?

Regel Nr. 1:

Jeder wird angegriffen, es gibt keine Ausnahmen!

Bild: © AdobeStock/ The Little Hut

Regel Nr. 1:

Jeder wird angegriffen, es gibt keine Ausnahmen!

- Identifizieren Sie Risikoprofil u. Kronjuwelen
- Sensibilisieren Sie Ihre Mitarbeiter
- Sichern Sie Ihre Systeme möglichst gut ab

Bild: © AdobeStock/ The Little Hut

Regel Nr. 2:

Früher oder später werden Ihre Schutzmaßnahmen versagen!

Bild: © AdobeStock/ The Little Hut

Regel Nr. 2:

Früher oder später werden Ihre Schutzmaßnahmen versagen!

- Erarbeiten Sie ein Notfallkonzept/Notfallplan
- Befolgen Sie Ihre Backup-Strategie !!!!!!
- Bereiten Sie die Einholung externer Hilfe vor
- Üben Sie den Ernstfall !!
- Schließen Sie ggf. eine Cyber-Versicherung ab

Bild: © AdobeStock/ The Little Hut

Bundesamt für Sicherheit in der Informationstechnik

BSI-Cyber-Sicherheitswarnung

SCHWACHSTELLE

Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken

CSW-Nr. 2020-252417-1151, Version 1.1, 13.10.2020

IT-Bedrohungslage*: 2 Orange

Sachverhalt

Bundesamt für Sicherheit in der Informationstechnik

BSI-IT-Sicherheitswarnung

SCHWACHSTELLE

Mehrere Schwachstellen in MS Exchange

Nr. 2021-197772-1S05, Version 1.1, 08.03.2021

IT-Bedrohungslage*: 3 Rot

Sachverhalt

Bundesamt für Sicherheit in der Informationstechnik

BSI-IT-Sicherheitsinformation

Tausende Microsoft-Exchange-Server in Deutschland weiterhin für kritische Schwachstellen verwundbar

CSW-Nr. 2024-223466-1032, Version 1.0, 26.03.2024

IT-BedrohungsCage*: 2 Orange

TLP:CLEAR: Unbegrenzte Weitergabe

Sachverhalt

Was kann/soll/muss ich tun?

KRITIS?

NIS-2?

TISAX?

<u>Anzustreben:</u>

IT-Sicherheitskonzept nach BSI IT-Grundschutz/Grundschutz++ oder ISO 27001 ff.

Empfehlung für KKU/KMU:
Führen Sie einen CyberRisikoCheck durch!!

nach DIN SPEC 27076

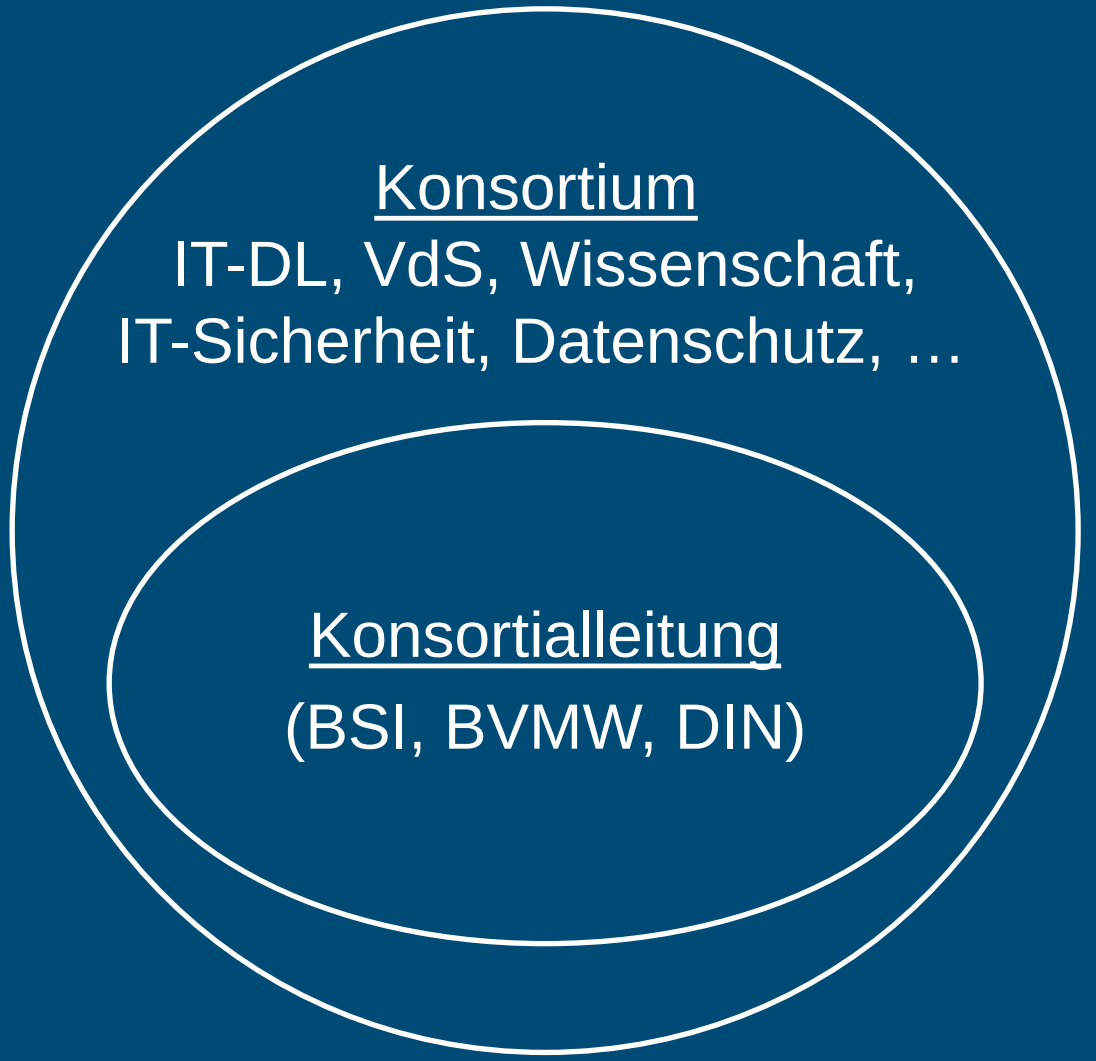
Ermittlung des IST-Zustandes der Informationssicherheit und Sichtbarmachung wichtigster Sicherheitsrisiken bei KKU

www.CyberRisikoCheck.de

DIN SPEC 27076 „IT-Sicherheitsberatung für Klein- und Kleinstunternehmen“

Wer hat‘s gemacht?

ca. 25 Personen



DIN

Der Mittelstand BVMW e.V. Bundesverband

Bundesamt für Sicherheit in der Informationstechnik

mIT Standard sicher

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages

DIN SPEC 27076 „IT-Sicherheitsberatung für KKUs“ - Inhalt

- Qualifikation der IT-Dienstleister
- Anforderungskatalog mit
  - 6 Themenbereiche (Organisation & Sensibilisierung, Identitäts- und Berechtigungsmanagement, Datensicherung, Patch- und Änderungsmanagement, Schutz vor Schadprogrammen sowie IT-Systeme und Netzwerke)
  - 27 Anforderungen mit insgesamt 54 Fragen
  - 37 Punkte insgesamt erreichbar

- Durchführung der Befragung
  1. Vorgespräch
  2. Gespräch zur Erhebung des **IST-Zustands** anhand des **Anforderungskatalogs**
     => **CyberRisikoCheck** Webanwendung
  3. Präsentation **Ergebnisbericht** mit IST-Stand & **Handlungsempfehlungen**

Kundenbericht

- Enthält alle Informationen für einen Bericht entsprechend der DIN SPEC 27076
- Stammdaten des Kunden
- Scoring-Ergebnis
- Spinnennetzdiagramm zur visualisierten Ergebnisdarstellung
- TOP-Handlungsempfehlungen
- Einfache Handlungsempfehlungen

NIS-2-Betroffenheitsprüfung – Ist mein Unternehmen reguliert? Was tun?

Hilfestellungen des BSI

- **Orientierung**, ob Unternehmen von NIS-2 betroffen ist
- Kurze und präzise Ja/Nein-Fragen
- Grundlage **Eigenangaben**, Ergebnis **nicht rechtlich bindend**

https://www.bsi.bund.de/dok/nis-2

https://www.bsi.bund.de/dok/nis-2-was-tun

https://www.bsi.bund.de/dok/nis-2-betroffenheitspruefung

#nis2know

Direktlink zum Angebot für KMU:

www.bsi.bund.de/kmu

- Informationen zum CyberRisikoCheck
- Tipps und Tricks für die Zielgruppe KMU
- Kontaktmöglichkeit bei Sicherheitsvorfällen
- Abomöglichkeit KMU-Newsletter

Cyber-Sicherheit umgangssprachlich
auf einfachem Niveau erklärt.

Neu:
Mit Informationen zum CyberRisikoCheck
nach DIN SPEC 27076

Vielen Dank für Ihre Aufmerksamkeit!

Michael Krauß

Referat W25 „Cybersicherheit bei kleinen und mittleren Unternehmen (KMU)“

michael.krauss@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Follow us:

Bild: © AdobeStock/Nirut