Cybercrime-Bedrohungslage und IT-Sicherheitsstrategie nach BSI-Standards

Webcast für unsere Kunden –
Schutzmaßnahmen, Compliance & Angebote
Version: 2026-02-13

GWS

SYSKO ZERTIFIZIERT

Agenda

Wird vom Teams Facilitator benutzt

- 1. Bedrohungslage
  - Ransomware, Datenexfiltration, Phishing – steigende Angriffszahlen & wirtschaftliche Folgen
- 2. Branchenfokus
  - Genossenschaften, Baustoffhandel, Lebensmittelgroßhandel, Technischer Großhandel jeweilige Top-Risiken & NIS2-Relevanz.
- 3. BSI-Grundschutz & NIS2Pflichten
  - Standards 200-1 bis 200-4, Konsequenzen bei Nichterfüllung.
- 4. IT-Sicherheitscheck & Notfallplan und Risiko-Analyse
  - Audit-Nachweise, Risikoanalyse, Wiederherstellung & Compliance.
- 5. Kombipaket & Umsetzung
  - Ganzheitliche Lösung, Unterlagenpakete, jährliche Folgeaudits, praktische Umsetzungstipps.
- 6. Call to Action
  - Audit prüfen/erneuern, Notfallplan erstellen, Workshop/Termine vereinbaren.

Pressespiegel

Sicherheitsvorfälle

BSI Lagebericht

"IT-Sicherheitslage bleibt angespannt; über 70.000 neue Schwachstellen dokumentiert"
Quelle öffnen

Check Point Report

"Weltweite Angriffe +44%; Deutschland Ø 1.200 Attacken pro Woche – insbesondere Mittelstand betroffen"
Quelle öffnen

PRX / The World

"Ransomware legt Krankenhäuser in EU lahm; Diagnostik & OP-Abläufe verzögert"
Quelle öffnen

Hackread

"Zwei Todesfälle nach Ransomware-Angriffen – Patientensicherheit akut gefährdet"
Quelle öffnen

CSIDB

"Centre Hospitalier Stell: kompletter IT-Ausfall, Rückkehr zu Papierbetrieb, Monate Wiederaufbau"
Quelle öffnen

Heise Security

"Dell Data Protection Advisor über unzählige Sicherheitslücken angreifbar"
Quelle öffnen

Cybercrime-Bedrohungslage und Auswirkungen

Überblick

- Angriffe nehmen kontinuierlich zu (Ransomware, Phishing, Datenexfiltration).
- Aktuelle BSI-Berichte melden zehntausende neue Schwachstellen pro Jahr.
- Leistungskürzungen/hohe Selbstbehalte bei Cyber-Versicherungen.
- Kreditvergabe zunehmend abhängig vom IT-Sicherheitsnachweis.
- BSI-Lagebericht: IT-Sicherheitslage weiterhin "angespannt"; >70 Diagramme.
- Check Point: +44 % Angriffe weltweit; in DE Ø 1.200 Angriffe/Woche.
- Europaweite Krankenhaus-Angriffe (PRX): gestörte Versorgung/Diagnostik.
- Ransomware mit Todesfällen (UK Synnovis; DE Düsseldorf).
- FR: Centre Hospitalier Stell – Komplettausfall, Papierbetrieb.
- Security-Insider: fortlaufende Vorfälle in DE (u. a. Radiosender).

Folgen

Details

- direkte Kosten, Reputationsschäden und Betriebsunterbrechungen.
- Versicherer reagieren mit Leistungskürzungen, drastisch erhöhten Selbstbehalten oder Ablehnung von Policen, wenn Nachweise zur IT-Sicherheit fehlen.
- Kreditgeber berücksichtigen den Sicherheitsstatus in der Vergabe.
- Ohne proaktive Maßnahmen drohen operative Ausfälle und Haftungsrisiken der Geschäftsführung.

Branchenanalyse: Raiffeisen und andere Genossenschaften

NIS2-Betroffenheit Getreide, Energie, Chemikalien/Pflanzenschutz

- Hohe Abhängigkeit von Zahlungsverkehr, SB-Filialtechnik und Verbund-IT.
- Top-Risiken: Phishing/CEO-Fraud, Ransomware, Lieferkette (Dienstleister).
- NIS2: Teile der Verbünde gelten als „wichtige Unternehmen“.

Branchenanalyse: Baustoffhandel

NIS2-Betroffenheit durch Handel mit Chemikalien/Lacken (BTU)

- Datenverlust und Stopp der Geschäfts-Prozesse, Betriebsstillstand
- Top-Risiken: Ransomware, ERP-Ausfall, Exfiltration von Preislisten.
- NIS2: Einstufung abhängig von Größe/Marktrelevanz möglich.

Branchenanalyse: Technischer Großhandel, Sanitärgroßhandel (auch BTU)

NIS2-Betroffenheit seltener als bei anderen Branchen

- Angriffsrisiken aber ähnlich hoch – auch ohne NIS2-Betroffenheit

- Top-Risiken:
  - Verkaufsstillstand
  - kein Online-Handel
  - Keine Zahlungseingänge/Faktura
  - Reputations- und Image Schaden

Branchenanalyse: Lebensmittelgroßhandel / BÄKO (LGH)

NIS2-Betroffenheit hoch bis KRITIS (je nach Größe wegen Lebensmitteln)

- Kühlkette/Telematik, Rezeptur- & Chargenplanung, HACCP-Dokumentation.
- Top-Risiken: OT/IoT, Unterbrechung Kühlketten-Tracking, ERP/Kommissionierung.
- NIS2: Relevanz der Versorgung → Meldepflicht bei erheblichen IT-Störungen.

Cybercrime-Bedrohungslage (SOC-Realität)

Alle Branchen, alle Unternehmen

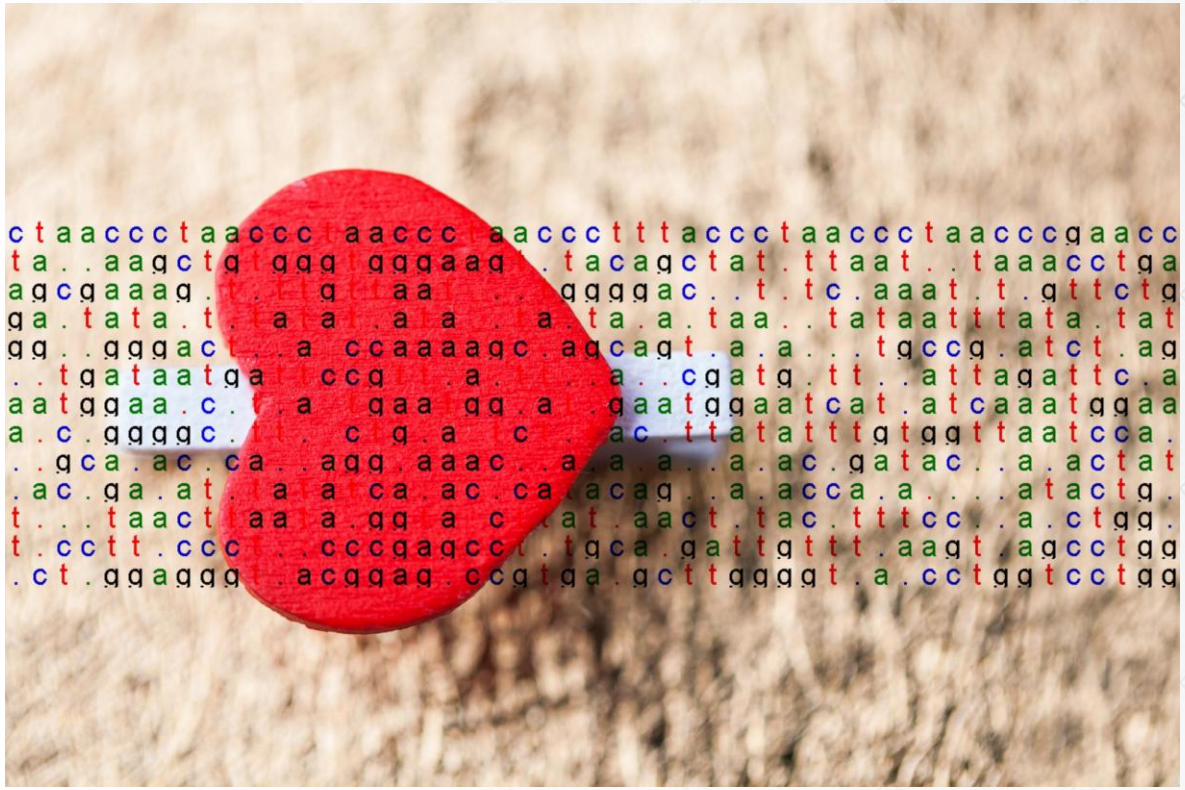
- Ransomware/Phishing/Datenexfiltration: reale SOC-Lage mit 24/7-Monitoring.
- Maßnahmen: MFA/PAM, Patchen, Backup-Härtung, Netzwerksegmentierung.
- Nachweisfähigkeit: BSI 200-1/200-2 + Notfallmanagement 200-4.

Zunehmende Cybercrime-Bedrohungen

wirtschaftliche Folgen

Risiko	Folgen	Finanzielle Auswirkung
Ransomware-Angriff	Systemausfall, Datenverlust	500.000 € – 5 Mio. €
Datenexfiltration	Reputationsschaden, DSGVO-Bußgelder	100.000 € – 2 Mio. €
Versicherungsablehnung	Kein Schutz bei Vorfällen	Unbegrenztes Risiko
Kreditverweigerung	Liquiditätsengpässe	Projektstopps, Insolvenzgefahr

Risiken bei fehlendem BSI Grundschutz



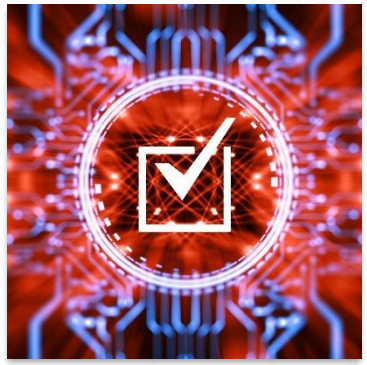
- Erhöhtes Risiko für Cyberangriffe
  - Ohne BSI-Grundschutz steigt die Wahrscheinlichkeit von Cyberangriffen und Datenverlusten in Unternehmen deutlich an.
- Rechtliche Konsequenzen
  - Fehlender Grundschutz kann zu straf- und zivilrechtlichen Folgen durch Verstöße gegen Datenschutzgesetze führen.
- Verlust von Vertrauen und Ruf
  - Reputationsschäden beeinträchtigen das Vertrauen von Kunden und Partnern erheblich und können langfristige Folgen haben.

BSI-Grundschutz: Damals: Empfehlung, heute: Pflicht

Zeitenwandel und mehr Risiken

Pflicht statt Empfehlung

Der BSI-Grundschutz ist mittlerweile für Unternehmen verpflichtend. Unternehmen müssen verbindliche IT-Sicherheitsmaßnahmen umsetzen.



NIS2UmsuCG und neue Standards

Das NIS2UmsuCG betrifft viele Unternehmen seit 15.12.2025 und verschärft die gesetzlichen Vorgaben zur IT-Sicherheit.

Erhöhte Schutzanforderungen

Die Regelungen fordern umfassende Schutzmaßnahmen und höheren Aufwand für den Schutz der Unternehmensdaten.

Warum BSI-Grundschutz auch ohne NIS2 unverzichtbar ist

NIS2 regelt, wer melden muss – Cyberangriffe treffen alle.

- Cyberangriffe unterscheiden nicht nach Unternehmensgröße oder Gesetzesstatus
- Geschäftsführung haftet auch ohne NIS2 für angemessene IT-Sicherheitsmaßnahmen
- Cyber-Versicherer & Banken verlangen nachweisbare Sicherheitsstandards
- Kunden, Verbünde & Lieferketten fordern ISMS & Notfallkonzepte
- Ein Audit älter als 12 Monate verliert seine Anerkennung
- BSI-Grundschutz reduziert Ausfallzeiten, Kosten und Chaos im Ernstfal

BSI-Grundschutz ist kein Gesetzesthema – sondern unternehmerische Pflicht.

BSI-Grundschutz: Pflicht vs. faktische Realität

Folgen und Risiken im Vergleich

Thema	Ohne NIS2-Pflicht	Mit BSI-Grundschutz
Cyberangriffe	Volles Risiko	Risiko reduziert
Haftung Geschäftsleitung	Persönlich bei Fahrlässigkeit	Nachweis „angemessener Maßnahmen“
Cyber-Versicherung	Ablehnung / hoher Selbstbehalt	Versicherbarkeit verbessert
Kreditvergabe	Sicherheitsstatus kritisch	Positiver Prüfpunkt
Kunden & Verbünde	Rückfragen / Ausschluss	Akzeptierter Standard
Notfälle	Improvisation & Stillstand	Strukturierte Wiederherstellung

Strategie: IT-Sicherheitscheck nach BSI-Standards

BSI 200-1/200-2 (ISMS & Sicherheitskonzept).
BSI 200-3 und -4 Risiko-Management
Regelmäßige Folgeaudits (≤12 Monate)

GWS

SYSKO ZERTIFIZIERT

Warum ein IT-Sicherheitscheck unverzichtbar ist

Zuordnung der Themenkreise

BSI-Standard	Zweck	Nutzen
200-1	ISMS-Aufbau	Strukturierte Sicherheitsorganisation
200-2	Sicherheitskonzeption	Klare Maßnahmen und Prozesse
200-3	Risikoanalyse	Risiken identifizieren & bewerten
200-4	Notfallmanagement	Schnelle Wiederherstellung im Ernstfall

IT-Sicherheitscheck, Notfallplan und ggf. NIS2

Details

- IT-Sicherheitscheck nach BSI-Standards deckt technische, organisatorische und personelle Schwachstellen auf und liefert konkrete Maßnahmen.
- BSI 200-1 und 200-2 bilden das Fundament für ISMS und Sicherheitskonzeption.
- Audit, älter als 12 Monate = kein ausreichender Schutz – Folgeaudits aktuell.
- Vertrauen bei Kunden, Partnern, Versicherern und Aufsichtsbehörden.
- Ziel 80+ % BSI-Grundschutz (200-1/200-2).
- Notfallplan & Risikoanalyse gemäß 200-3/200-4 erforderlich.
- (optional NIS2): Meldepflichten & Bußgelder für (besonders) wichtige Unternehmen.

Erfüllung von BSI-Grundschutz und NIS2-Pflichten

Folgen sind auch für Unternehmen OHNE NIS2 Meldepflicht identisch

Anforderung	Standard	Konsequenz bei Nichterfüllung
ISMS-Nachweis	BSI 200-1	Versicherungsablehnung
Sicherheitskonzept	BSI 200-2	Erhöhte Selbstbehalte
Notfallplan	BSI 200-3/200-4	Bußgelder, Betriebsunterbrechung
Meldepflicht (wichtige und besonders wichtige Unternehmen)	NIS2	Strafen bis in Millionenhöhe

Compliance besonders wichtig

Details

- Unternehmen müssen nachweislich mindestens 80 % der relevanten Themen des BSI-Grundschutzes erfüllen.
- Ein Notfallplan mit Risikoanalyse gemäß BSI 200-3 und 200-4 ist erforderlich.
- Fehlende Nachweise führen zu Versicherungsablehnungen oder sehr hohen Selbstbehalten.
- NIS2 bringt zusätzliche Meldepflichten und Bußgelder für wichtige und besonders wichtige Unternehmen.
- Compliance-Überprüfungen erfolgen unter anderem durch Wirtschaftsprüfer wie AWADO oder externe Wirtschaftsprüfer.

Lösung nach BSI-Standards: IT-Sicherheitscheck und Notfallplan

IT-Dokumentation, GAP-Analyse und Feststellung Mängel

- Kombinierte Lösung: Analyse + Resilienzaufbau.
- Bericht/Testat als Nachweis gegenüber Versicherern & Wirtschaftsprüfer.
- Unterlagenpakete, Checklisten, Mustervorlagen inklusive.
- Mehr Infos: IT-Sicherheitscheck | Notfallplan & Risikoanalyse
  - IT-Sicherheitscheck | Notfallplan & Risikoanalyse

Produkt	Leistungsumfang	Nutzen
IT-Sicherheitscheck	Analyse, Soll-Ist-Vergleich, Prüfbericht	BSI-Erfüllung, Versicherungsnachweis
Notfallplan	Risikoanalyse, Maßnahmenkatalog, Schulung	Schnelle Wiederherstellung, Compliance
Kombipaket	Beide Leistungen integriert	Ganzheitliche Sicherheitsstrategie

Kombipaket

Details

- IT-Sicherheitscheck analysiert die aktuelle Lage, identifiziert Schwachstellen und liefert einen Prüfbericht als Nachweis.
- Notfallplan mit Risikoanalyse definiert Maßnahmen zur Bewältigung von IT-Notfällen und stellt die schnelle Wiederherstellung sicher.
- Das **Kombipaket ist praxisorientiert**, beinhaltet Unterlagenpakete, Checklisten und Muster.
- Jährliche Folgeaudits sichern Kontinuität

- Die Umsetzung stärkt Resilienz, erfüllt regulatorische Vorgaben und erhöht das Vertrauen von Kunden und Partnern.

Tipps für erfolgreiche Umsetzung

- Klare Verantwortlichkeiten & Projektleitung
- Gute Dokumentation & Nachverfolgbarkeit
- Einbindung aller Stakeholder
- Priorisierung nach Risiko
- Budget & Ressourcen früh einplanen
- Kontinuierliche Verbesserung & Monitoring

Fallbeispiel: Vorher – Nachher

Vorgehensweise

- Das Audit ermittelt das Delta. Ein Dienstleister oder die Syskos müssen die Mängel abstellen!

Vorher:
- Ungeschützte Systeme
- Veraltete Software
- Keine Nachweise
- Hohes Risiko

Nachher:
- Systeme gehärtet
- Software aktuell
- Audit-Nachweise vorhanden
- Risiko reduziert

Fazit

Zusammenfassung, nächste Schritte

Call to Action: Sichern Sie Ihr Unternehmen

NIS2-Pflicht ≠ Sicherheitsrealität

NIS2-Pflicht bedeutet:

- Gesetzliche Meldepflicht
- Bußgelder bei Verstößen
- Gilt nur für definierte Unternehmen

Faktische Pflicht bedeutet:

- Haftung der Geschäftsführung bei Sicherheitsmängeln
- Ablehnung durch Cyber-Versicherer
- Kritische Rückfragen bei Kreditvergabe
- Anforderungen durch Kunden & Verbünde
- Existenzbedrohende Ausfälle bei fehlendem Notfallplan

Auch ohne NIS2 gilt:
Ohne BSI-Nachweis trägt das Unternehmen das volle Risiko.

Dringender Handlungsbedarf: Die 12-Monats-Frist

oder: es wurde noch nie ein Audit durchgeführt

- **Achtung:** Ist Ihr letztes Audit **älter als 12 Monate**?
- **Standards & Risiken ändern sich:** BSI-Standards werden **regelmäßig aktualisiert**, neue Angriffsmethoden erfordern neue Prüfungen.
- Ein älteres Audit kann Ihr Unternehmen in **falscher Sicherheit** wiegen.
- **Handeln Sie jetzt.**

- **Die Konsequenzen des Nichthandelns**
- Wer nicht handelt, läuft Gefahr:
- **Opfer von Datendiebstahl oder Ransomware** zu werden.
- **Rechtliche Konsequenzen und hohe Bußgelder** zu riskieren.
- Massive **Image- und Vertrauensverluste** zu erleiden.
- **Zentrale Botschaft:** Handeln Sie, bevor es zu spät ist!

Nächste Schritte

Ihr Call to action!

- IT-Sicherheitscheck nach BSI-Standards oder Kombilösung anfragen.
- Notfallkonzept & Risikoanalyse terminieren.
- Folgeaudit in 12 Monaten einplanen.
- Kontakt: TÜV-geprüfter IT-Sicherheitsmanager / Auditor (GWS).

- Tech-Nachrichten: IT-Sicherheitscheck

- Tech-Nachrichten: Notfallkonzept & Risikoanalyse

Quellennachweise

Sysko-Portal der GWS https://tech-nachrichten.de

Mehr Details (und Podcast)

- https://tech-nachrichten.de/warum-ein-it-sicherheitscheck-nach-bsi-standards-unverzichtbar-ist/

Bezug zu NIS-2

- https://tech-nachrichten.de/vorgeh ensweise-zu-it-compliance-mit-nis-2/

Notfallplan:

- Tech-Nachrichten: Notfallkonzept & Risikoanalyse

Erst-Audit:

- https://tech-nachrichten.de/it-sicherheits-check/

Folge-Audit:

- https://tech-nachrichten.de/folgeaudit-itscheck-notfallplan/

Bonus: KI-Aktion

Beteiligen Sie sich aktiv und informieren sich:

KI-Aktion

IT-Sicherheitscheck

Was soll Copilot für Sie übernehmen?

- Praxisnahe Copilot-Use-Cases aus Ihrem Arbeitsalltag
- Entlastung bei wiederkehrenden administrativen Aufgaben
- Automatisierung von Dokumentation & Berichten
- Unterstützung bei Recherche & Informationsaufbereitung
- Standardkommunikation effizienter gestalten
- Ihre Ideen priorisieren wir für konkrete Pilot-Anwendungsfälle

💡 Gestalten Sie mit – nicht theoretisch, sondern praxisnah.

Vielen Dank für Ihre Aufmerksamkeit! Zeit für Ihre Fragen

https://tech-nachrichten.de/feedback?Veranstaltung=webcast-itsicherheit&verandatum=2026-02-27

Ihr Feedback bitte QR-Code scannen:

Patrick Bärenfänger
IT-Security-Manager und Auditor (TÜV)
BSO Business Solutions & Operations - Stabstelle

Tel: +49 (251) 7000-3896
patrick.baerenfaenger@gws.ms

Kennwort für Video und Unterlagen: **Snd-Se-2026 shr-scher?**