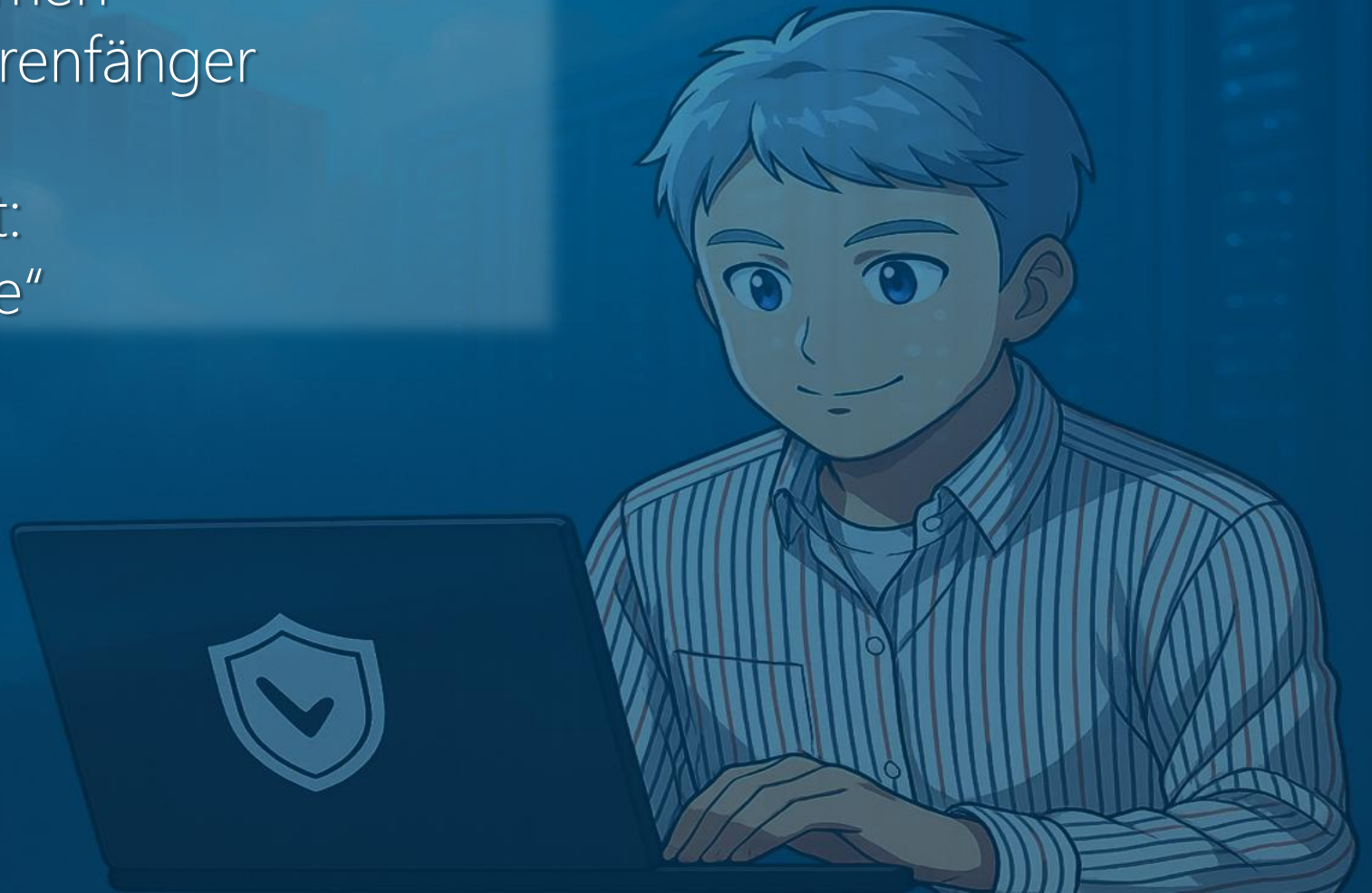


IT-Sicherheitscheck nach BSI-Standards

Unverzichtbar für Unternehmen
Webcast 2025-11, Patrick Bärenfänger

alle Abbildungen erstellt mit:
„Microsoft Copilot Enterprise“



Lage

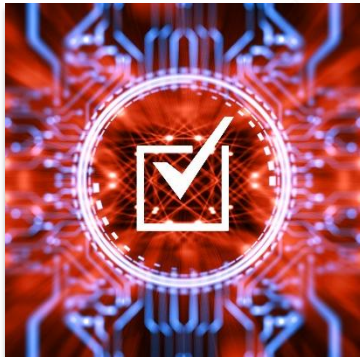
- Die Bedrohungslage durch Cyberangriffe wächst stetig
- Viele Unternehmen sind ungenügend vorbereitet
- Fragestellung: Warum ist ein IT-Sicherheitscheck nach BSI so wichtig?





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 ab 1.1.2026 und verschärft die gesetzlichen Vorgaben zur IT-Sicherheit.



Erhöhte Schutzanforderungen

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

- Die Zahl der Cyberangriffe auf Unternehmen steigt drastisch an.
- Hacker nutzen modernste Methoden zur Kompromittierung von Netzwerken, Systemen und Datenbanken.
- Ein veralteter Sicherheitsstatus ist ein Hauptangriffsziel.
- Zunahme von Ransomware, Zero-Days, Social Engineering
- Systeme und Infrastruktur verändern sich kontinuierlich
- Neue Anforderungen und Standards entstehen



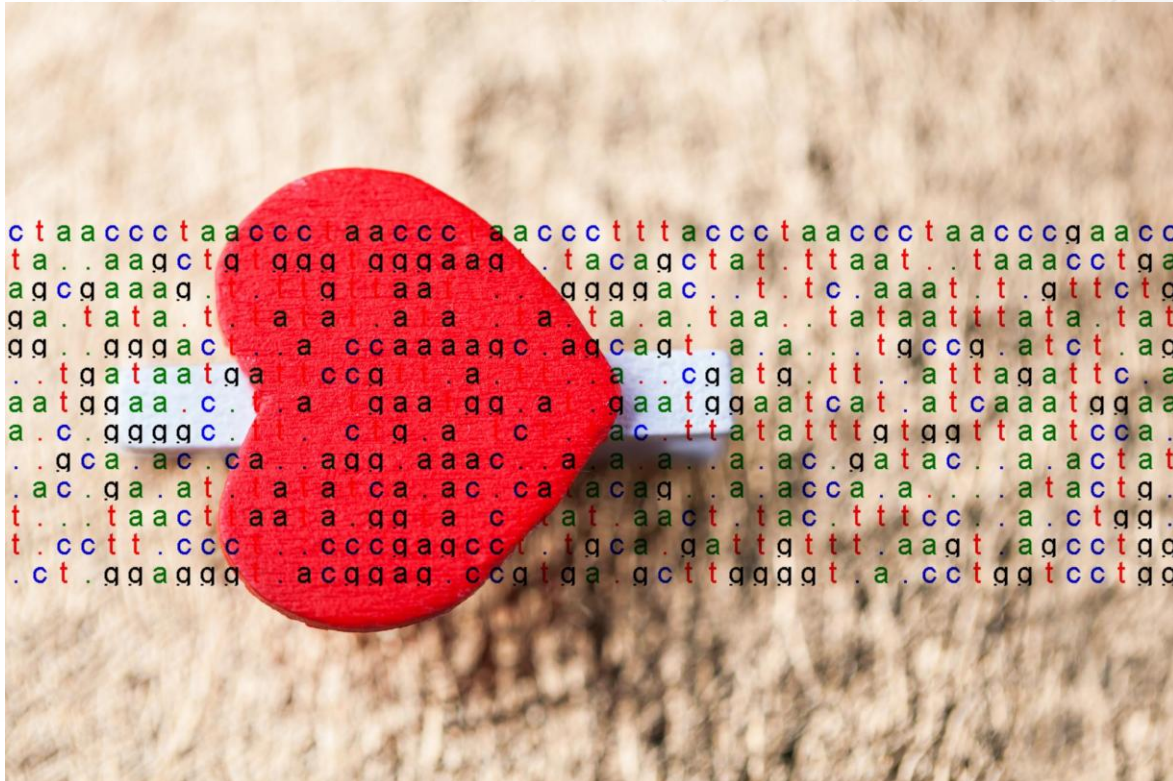
- Sicherheitslücken schließen: Wir decken Schwachstellen auf, die für Sie oft unsichtbar bleiben.
- Compliance sicherstellen: Einhaltung regulatorischer Vorgaben (z.B. NIS2, DSGVO) für rechtliche Sicherheit.
- Kosten sparen: Ein Audit kostet nur einen Bruchteil der Schäden, die ein erfolgreicher Angriff verursacht (Millionenhöhe).
- Vertrauen stärken: Offizieller Nachweis an Kunden, Partner und Behörden, dass IT-Sicherheit oberste Priorität hat.

Kosten Audit: Gering

Kosten Vorfall: Hoch

- Neue Bedrohungen und Angriffsmuster entstehen
- Infrastruktur und Prozesse verändern sich
- Regulierung und Standards entwickeln sich weiter
- Haftungs- und Compliance-Risiken bei fehlendem Nachweis

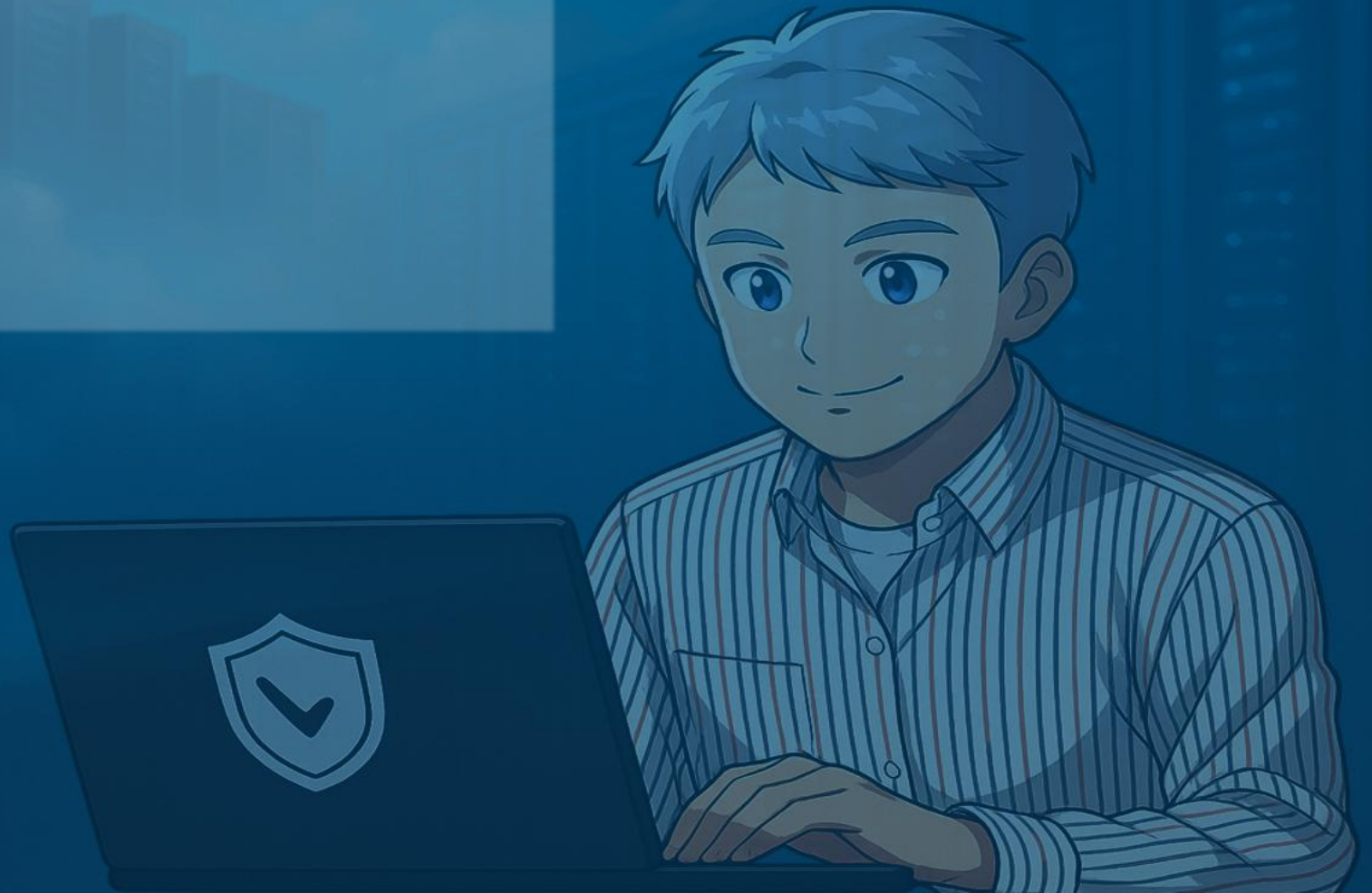




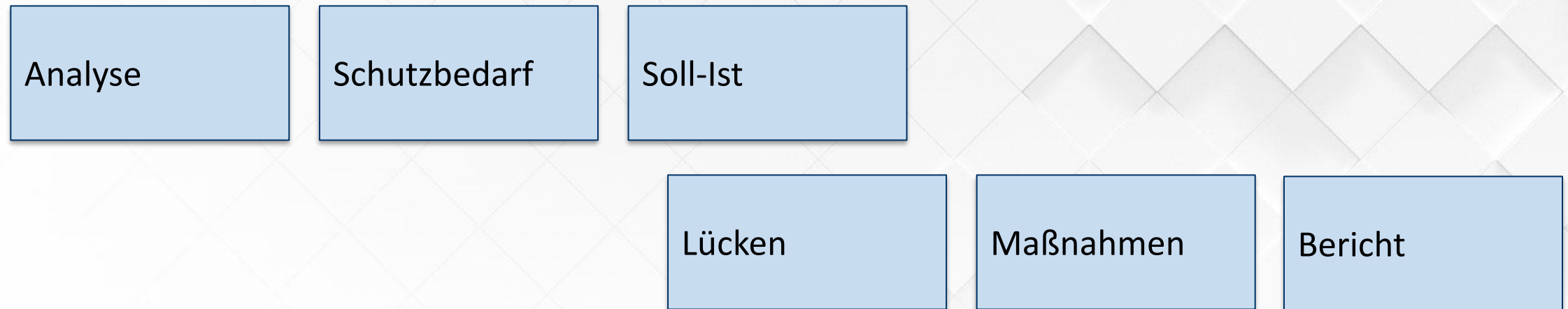
- Erhöhtes Risiko für Cyberangriffe
 - Ohne BSI Grundschutz steigt die Wahrscheinlichkeit von Cyberangriffen und Datenverlusten in Unternehmen deutlich an.
- Rechtliche Konsequenzen
 - Fehlender Grundschutz kann zu straf- und zivilrechtlichen Folgen durch Verstöße gegen Datenschutzgesetze führen.
- Verlust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

Maßnahmen

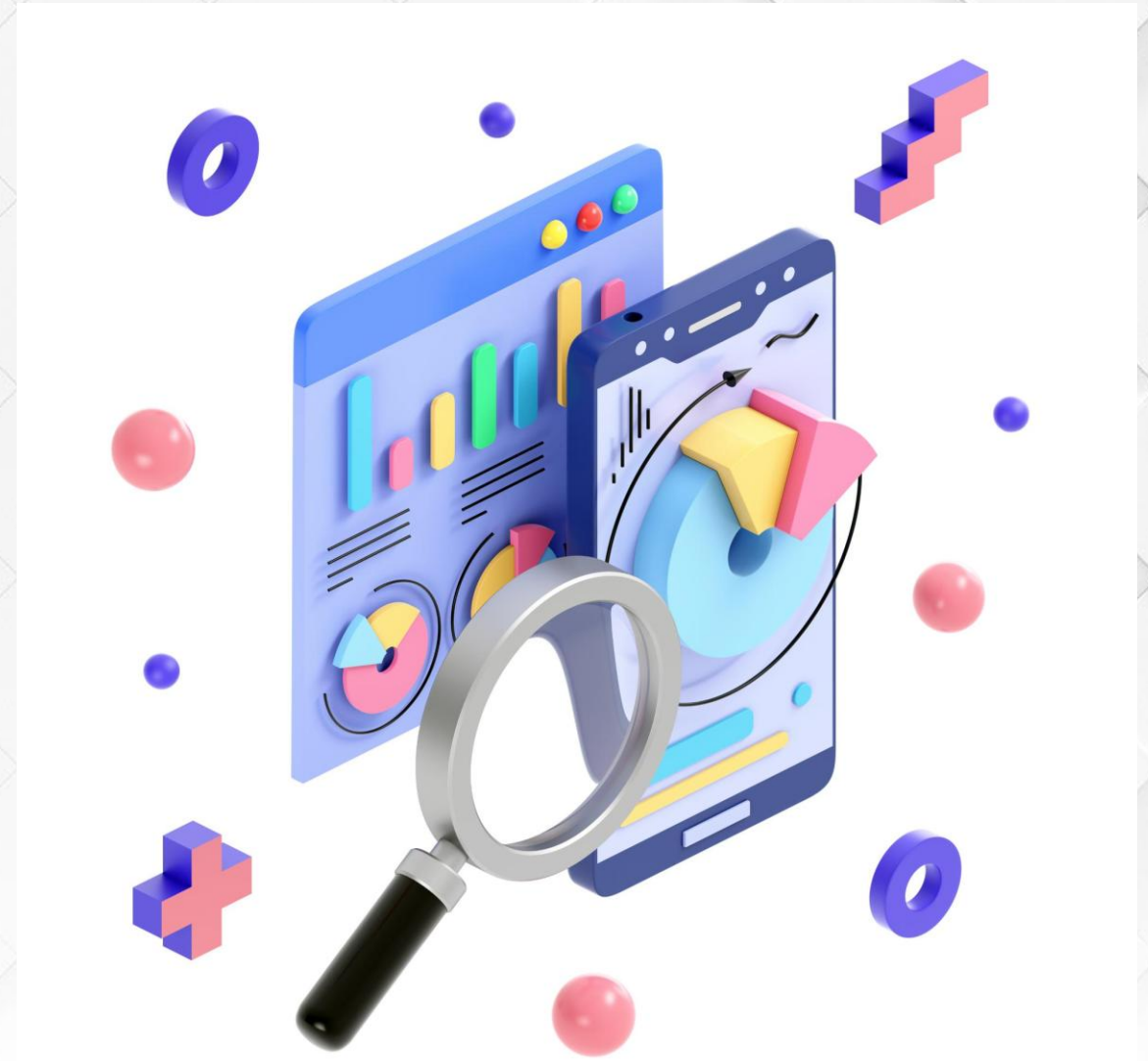
Schutz verbessern



- Analyse des Ist-Zustands
- Schutzbedarfsfeststellung
- Vergleich Soll ↔ Ist
- Identifikation von Sicherheitslücken
- Handlungsempfehlungen & Maßnahmenplan
- Dokumentation & Bericht



- Aktuelle Risikobewertung sicherstellen
- Proaktive Sicherheitsverbesserung
- Erfüllung regulatorischer Anforderungen
- Wettbewerbsvorteil und Vertrauen durch Nachweis
- Empfohlen: jährlich, in kritischen Bereichen häufiger



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



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

Call to Action: Sichern Sie Ihr Unternehmen

Was tun?

Jeder Tag ohne aktuellen Sicherheitscheck **erhöht** Ihr Risiko.

- Ein IT-Sicherheitscheck nach BSI ist essenziell
- Veraltete Checks reichen nicht aus
- Regelmäßige Audits sichern Compliance und Reputation
- Nächster Schritt: Im Sysko-Portal informieren

Beauftragen Sie Ihren aktuellen IT-Sicherheitscheck nach BSI-Standards.



- **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!

Fazit

... und Quellen

Quellennachweise

Im Syskoportal der GWS

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/vorgehensweise-zu-it-compliance-mit-nis-2/>

Erst-Audit:

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

Folge-Audit:

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





SYSKO
ZERTIFIZIERT

GWS

Vielen Dank für Ihre Aufmerksamkeit! Zeit für Ihre Fragen



Patrick Bärenfänger

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

Tel: +49 (251) 7000-3896

patrick.baerenfaenger@gws.ms



Ihr Feedback
bitte QR-Code
scannen:

