



# WILLKOMMEN BEI NEAM

Informationssicherheit, IT-Services,  
Schulungen & Workshops



# IHR TRAINER

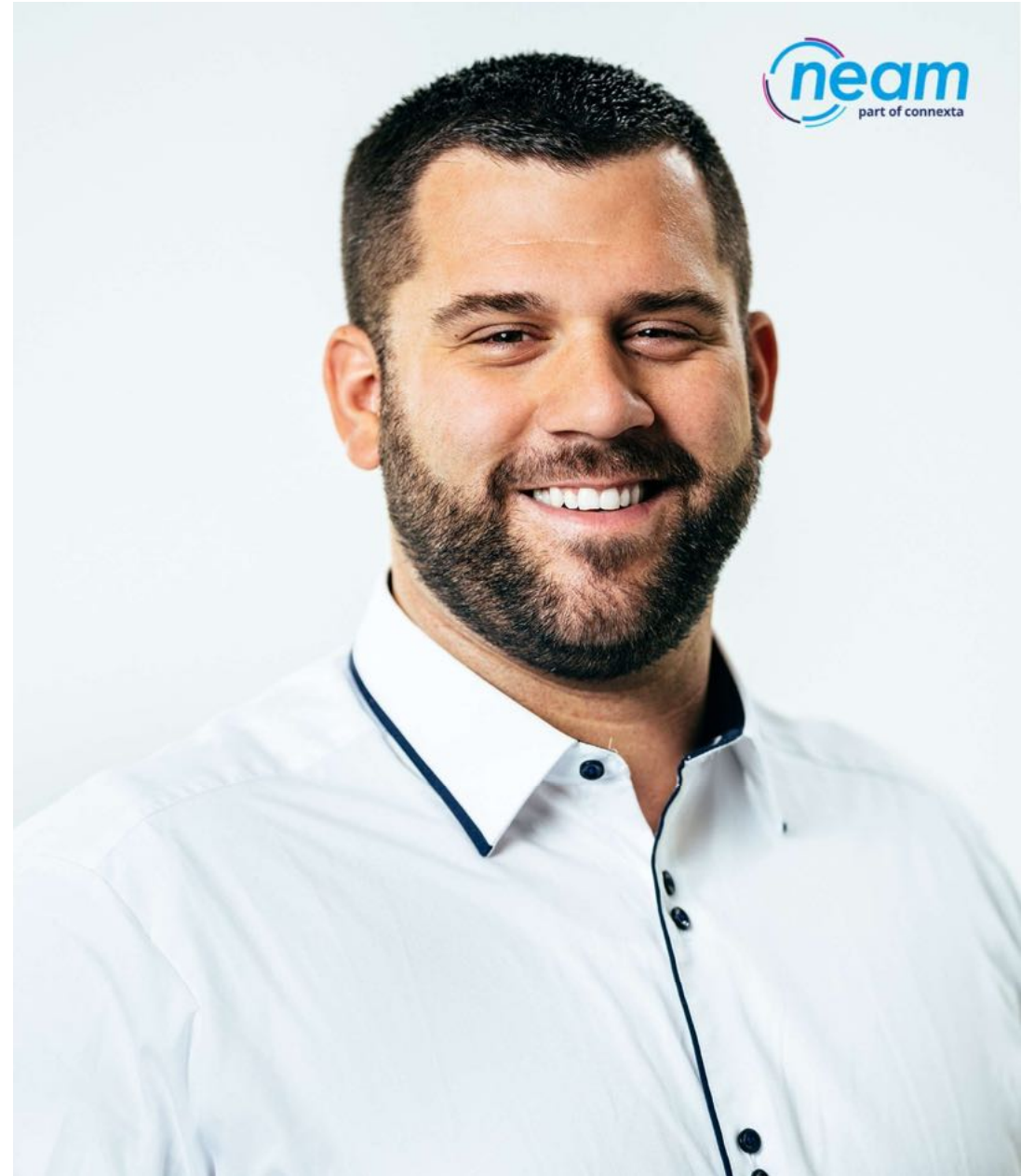
## Sören Risse

Senior Security Consultant  
Leiter Team Sicherheitsberatung

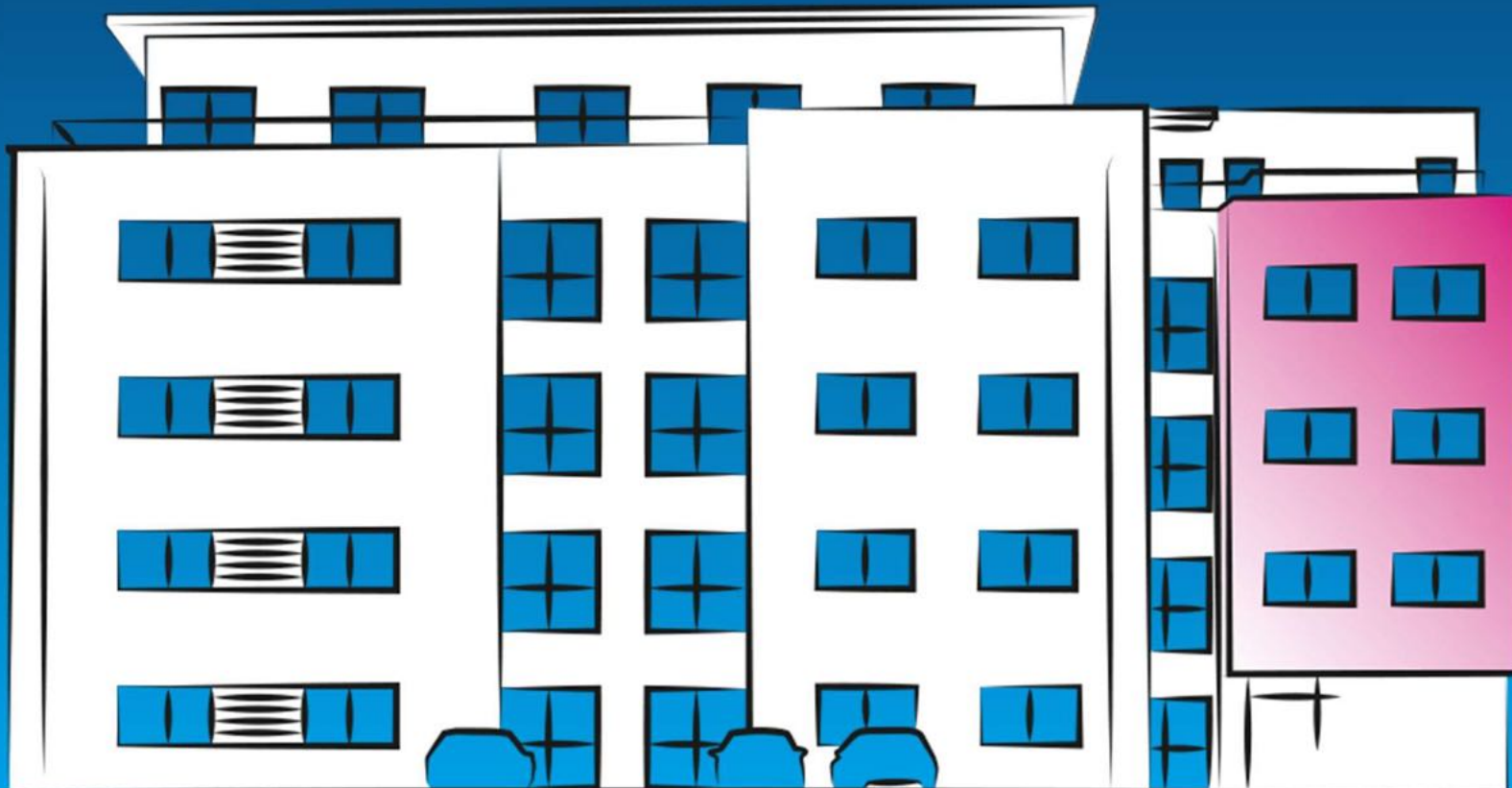
IT-Grundschutz-Berater  
Certified ISO 27001 Lead Auditor  
verinice.EXPERT  
Informationssicherheitsbeauftragte(r) mit TÜV  
Rheinland geprüfter Qualifikation

[Soeren.Risse@neam.de](mailto:Soeren.Risse@neam.de)

+49 (5251) 1652 0



# NEAM IT-SERVICES GMBH



## Warum neam?

**25+**

Seit über 25 Jahren am  
Markt

**IT-Services &  
Informationssicherh  
eit**

**3+**

3 Standorte

**Paderborn,  
Wiesbaden & Berlin**

**100+**

über 100 hochqualifizierte  
Mitarbeiter

**Starkes Team**





# WIBA – WEG IN DIE BASIS-ABSICHERUNG

Toolbasierte Unterstützung





# AGENDA

- 1 Aktuelles
- 2 Die WiBA – „Weg in die Basisabsicherung“
- 3 Vorteile der WiBA
- 4 Abbildung in verinice
- 5 Anschließende Absicherung - Ausblick

16.11.2023

## Cyber-Angriff auf den IT-Dienstleister Südwestfalen-IT (SIT) ■

Informationen für Kommunen, die vom Cyber-Angriff betroffen sind.

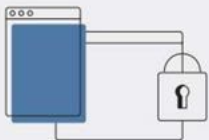
📍 Kommunen, Kreise, öffentliche Einrichtungen

Bekanntermaßen sind derzeit viele Kommunen und Kreise in Nordrhein-Westfalen von dem Cyber-Angriff auf den IT-Dienstleister Südwestfalen-IT (SIT) betroffen.

# Ransomware

ist weiterhin die größte Bedrohung.

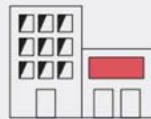
**2** Ransomware-Angriffe auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



**68** erfolgreiche Ransomware-Angriffe auf Unternehmen wurden bekannt.

**15**

davon richteten sich gegen IT-Dienstleister.

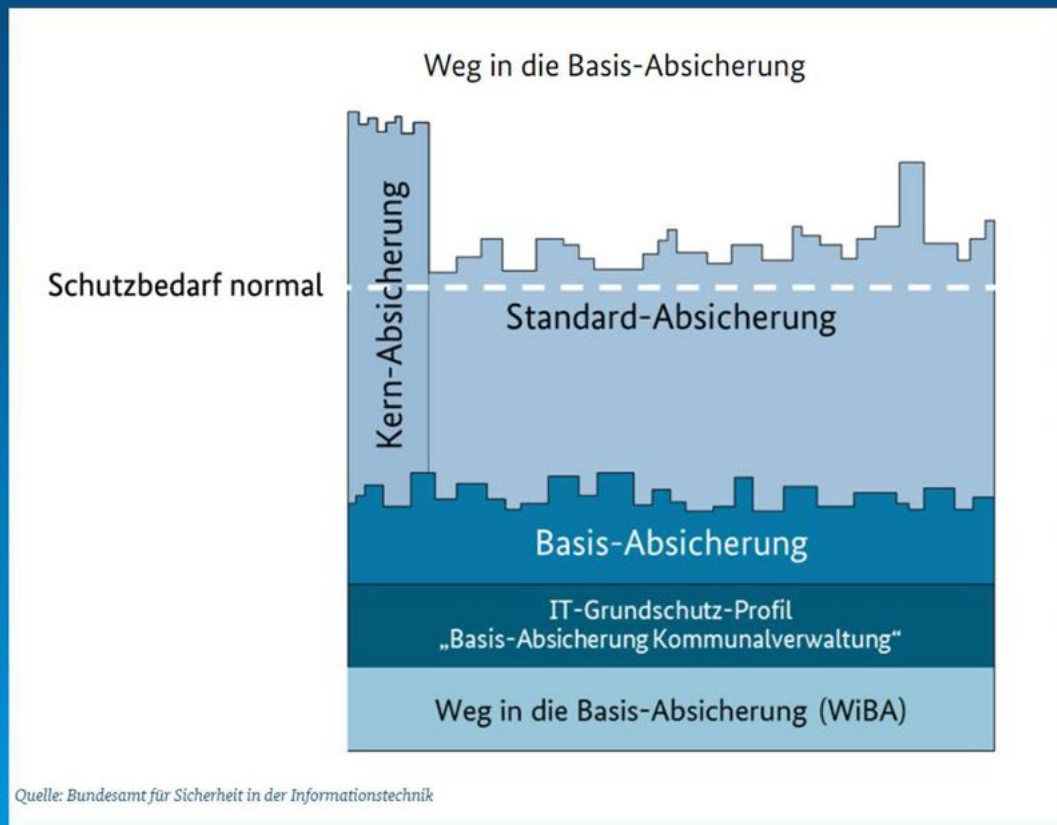


[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?\\_\\_blob=publicationFile&v=7](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.pdf?__blob=publicationFile&v=7)  
<https://www.bra.nrw.de/energie-bergbau/foerderprogramme-fuer-klimaschutz-und-energie-wende/wichtige-und-allgemeine-hinweise-aktuelles/alle-nachrichten-zu-den-foerderprogrammen-fuer-klimaschutz-und-energie-wende/cyber-angriff-auf-den-it-dienstleister-suedwestfalen-it-sit>





# WIBA – WEG IN DIE BASIS-ABSICHERUNG



# ZIEL & ABGRENZUNG



WiBA ist als Einstieg in die Informationssicherheit konzipiert, um die Hürde zur Umsetzung von anerkannten Standards der Informationssicherheit zu verringern.

WiBA selbst ist kein Standard für Informationssicherheit. Die Umsetzung von WiBA ist zum Veröffentlichungszeitpunkt nicht verpflichtend, sondern ein Angebot, um niedrigschwellig in die Informationssicherheit einzusteigen.



# WIBA – AUF EINEN BLICK

Unterstützung bei der ersten Sachstandserhebung  
mittels 19 themenspezifischer Checklisten, z.B.:



Es werden die wesentlichen organisatorischen und technischen Aspekte betrachtet, die bei einer Absicherung im kommunalen Bereich vorrangig sind.

# WiBA – VORTEILE

WiBA ist gezielt für kleine Kommunen erstellt worden

WiBA setzt den Fokus auf das schnelle Erreichen eines höheren Informationssicherheitsniveaus

WiBA kann unabhängig vom Bundesland verwendet werden

WiBA ist eine niedrighschwellige Einstiegsstufe in die Informationssicherheit

WiBA führt mit wenig Aufwand zu einem schnellen Ergebnis

Nicht zwingend Vorkenntnis der Grundschutz Methodik notwendig

# WIBA & VERINICE?



The screenshot displays a software interface for managing IT security profiles. On the left, a tree view shows a hierarchy of profiles under 'Importierte Objekte'. The selected profile is 'WIBA.5.F1 [BASIS] Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?'. The right pane shows the details for this profile, including its identifier, title, and a list of known authentication techniques.

**Importierte Objekte**

- IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung 3
  - Geschäftsprozesse
  - Anwendungen
    - A01 Internet- Nutzung
    - A02 Benutzer- Authentifizierung
    - A03 Dateiablage
    - A04 Bürokommunikation
    - A05 Office-Produkte
    - Mobile Endgeräte
  - IT-Systeme
  - ICS-Systeme
  - Anderer/IoT-Systeme
  - Kommunikationsverbindungen
  - Infrastruktur (Räume/Gebäude/andere Arbeitsplätze...)
  - Personen
  - ISMS.1 Sicherheitsmanagement
    - ORP.1 Organisation
    - ORP.2 Personal
    - ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
    - ORP.4 Identitäts- und Berechtigungsmanagement
  - CON.3 Datensicherungskonzept
  - CON.6 Löschen und Vernichten
  - CON.9 Informationsaustausch
  - OPS.1.1.2 Ordnungsgemäße IT-Administration
  - OPS.1.1.3 Patch- und Änderungsmanagement
  - OPS.1.1.4 Schutz vor Schadprogrammen
  - OPS.1.1.5 Protokollierung
  - OPS.1.2.4 Telearbeit
  - OPS.1.2.5 Fernwartung
  - OPS.2.1 Outsourcing für Kunden
  - OPS.2.2 Cloud-Nutzung
  - DER.2.1 Behandlung von Sicherheitsvorfällen
  - Zusatz Bausteine nach Kapitel 6.4
  - Elementare Gefährdungen
  - Dokumente
  - Vorfälle
  - Aufzeichnungen
- WiBA Checklisten
  - WiBA Checklisten
    - WiBA.1 Checkliste: Arbeit außerhalb der Institution
    - WiBA.2 Checkliste: Arbeit innerhalb der Institution / Haustechnik
    - WiBA.3 Checkliste: Backup
    - WiBA.4 Checkliste: Bürosoftware
    - WiBA.5 Checkliste: Client
      - WIBA.5.F1 [BASIS] Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?
      - WIBA.5.F2 [BASIS] Wird eine Bildschirmsperre verwendet, wenn ein Client unbeaufsichtigt ist?
      - WIBA.5.F3 [BASIS] Sind Benutzende dazu verpflichtet, sich vom IT-System und in ...
      - WIBA.5.F4 [BASIS] Werden Clients gegen Schadssoftware geschützt?
      - WIBA.5.F5 [BASIS] Ist der Bootvorgang von Clients abgesichert?

WIBA.5.F1 [BASIS] E...

Identifer: WIBA.5.F1

Titel: Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?

Vorgehensweise: BASIS

Aufwand: 1

Beschreibung:

Tags:

Dokument:

Letzte Änderung: 16.01.2024

Release:

Änderungstyp:

Änderungsdetails:

Daten Verknüpfungen Änderungsmetadaten

Objektbrowser

Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?

Nur berechnete Benutzende sollten sich an Clients anmelden können.  
Es gibt verschiedene Techniken, über die die Authentizität von Benutzenden nachgewiesen werden kann.  
Die bekanntesten sind:

- PINs (Persönliche Identifikationsnummern),
- Passwörter,
- Token wie z. B. Zugangskarten sowie
- Biometrie.

# WIBA & VERINICE?

- ✓ WiBA Checklisten
  - ✓ WiBA Checklisten
    - > WiBA.1 Checkliste: Arbeit außerhalb der Institution
    - > WiBA.2 Checkliste: Arbeit innerhalb der Institution / Haustechnik
    - > WiBA.3 Checkliste: Backup
    - > WiBA.4 Checkliste: Bürosoftware
    - ✓ WiBA.5 Checkliste: Client
      - 🔴 WiBA.5.F1 [BASIS] Erfordern Clients eine Authentisierung durch Benutzende, bevo...
      - 🔴 WiBA.5.F2 [BASIS] Wird eine Bildschirmsperre verwendet, wenn ein Client unbeauf...
      - 🔴 WiBA.5.F3 [BASIS] Sind Benutzende dazu verpflichtet, sich vom IT-System und in ...
      - 🔴 WiBA.5.F4 [BASIS] Werden Clients gegen Schadsoftware geschützt?
      - 🔴 WiBA.5.F5 [BASIS] Ist der Bootvorgang von Clients abgesichert?
      - 🔴 WiBA.5.F6 [BASIS] Sind alle nicht benötigten Funktionen in der Firmware von Cli...
      - 🔴 WiBA.5.F7 [BASIS] Sind alle nicht benötigten Cloud- und Online-Funktionen des B...

Daten Verknüpfungen Änderungsmetadaten					
Objektbrowser Verknüpfungen					
Verknüpfung für: WIBA.5.F1 [BASIS] Erfordern Clients eine Authentisierung durch Benutzende, bevor sie verwendet werden können?					
	Verknüpfung		Titel	Scope	Beschreibung
🔴	setzt um	🔴	SYS.2.1.A1 [BASIS] Sichere Benutzerauthentisierung	Basis-Absicher...	
🔴	setzt um	🔴	SYS.2.1.A1 [BASIS] Sichere Benutzerauthentisierung	Basis-Absicher...	

# WIBA & VERINICE - REPORTING

## Checkliste: Arbeit außerhalb der Institution

Zugrundeliegende Bausteine:

- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.11 Allgemeines Fahrzeug
- OPS.1.2.4 Telearbeit

Bearbeitungsinformationen

<b>Anzahl Checkfragen:</b> 10	<b>Davon umgesetzt:</b> 0
<b>Checkliste bearbeitet am:</b> <i>In Bearbeitung</i>	<b>Checkliste bearbeitet von (zuständige Stelle/ Rolle):</b>



# WIBA & VERINICE - REPORTING

Checkliste: Arbeit außerhalb der Institution

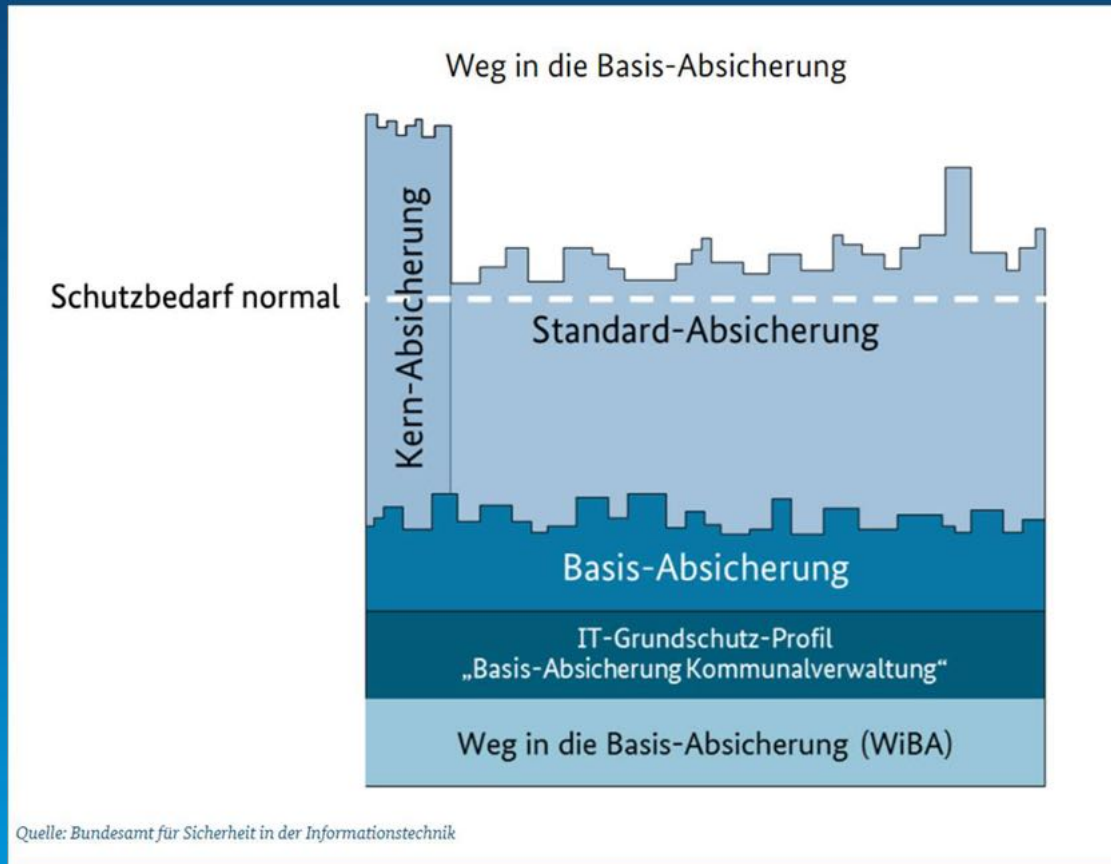
## Prüffragen

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt		
			Ja	Nein	Nicht relevant
1	Ist festgelegt, welche Dokumente und Datenträger außerhalb der Institution transportiert werden dürfen?	2			
	<i>Die Festlegung zielt auf den Transport von physischen Dokumenten und Datenträgern wie bspw. Papierakten oder Festplatten, aber auch auf mobile Geräte mit Speichermedium (bspw. Smartphone, Laptop) ab. „Festgelegt“ meint entweder gelebte Praxis oder schriftliche Fixierung mit Information der relevanten Personenkreise.</i>				
	Notizen				





# WIBA - FORTFÜHRUNG



WiBA?  
IT-Grundschutz?



Know-how  
bringt neam mit.



# FRAGEN





# VIELEN DANK UND AUF BALD

Wir freuen uns auf gute Zusammenarbeit.



BEING  
HUMAN  
AND MAKING IT  
BETTER



**NEAM IT-SERVICES GMBH**

Technologiepark 8  
33100 Paderborn

Tel. +49 5251 1652-0

Fax +49 5251 1652-444

[info@neam.de](mailto:info@neam.de)

[www.neam.de](http://www.neam.de)



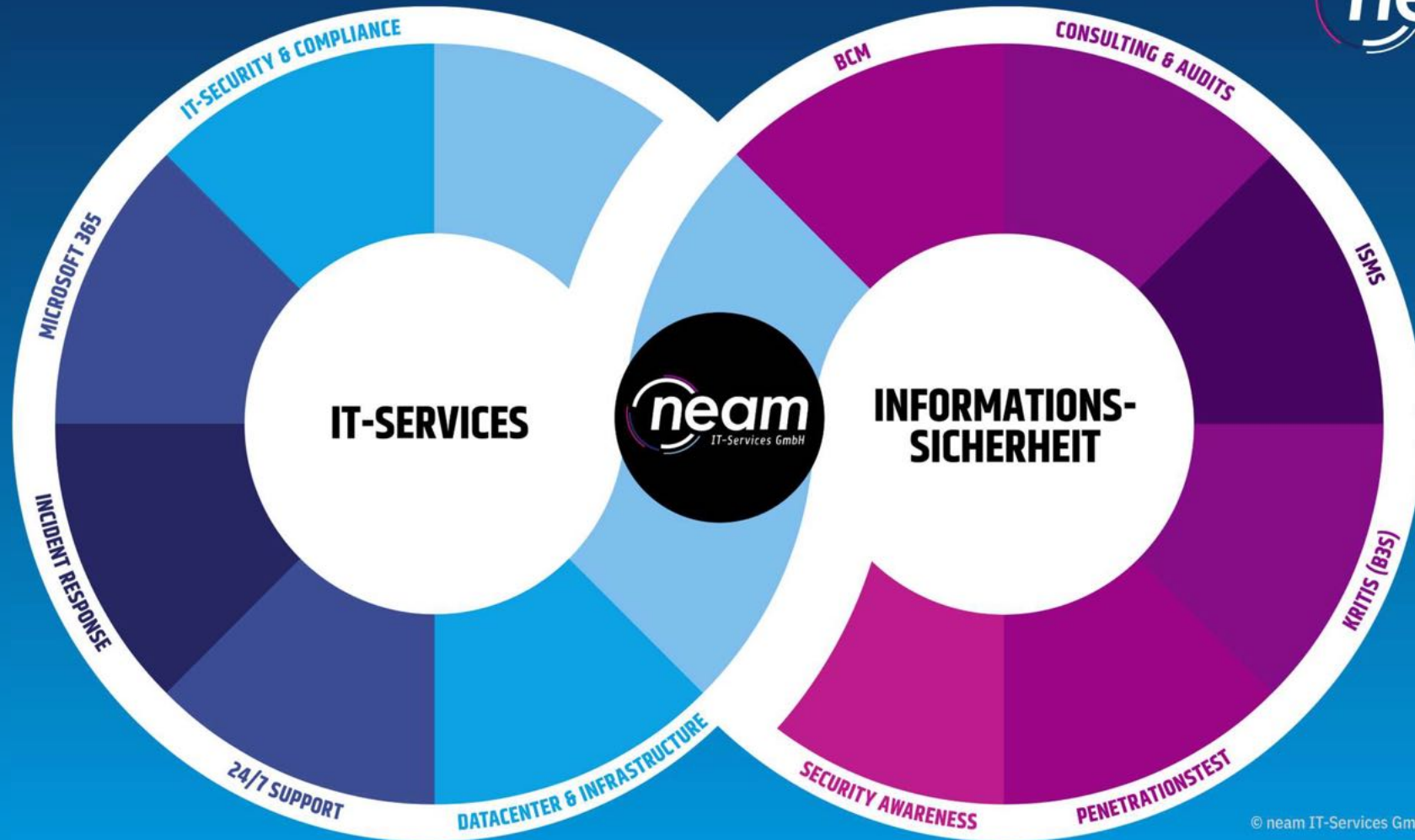
# UNSERE ERFAHRUNG

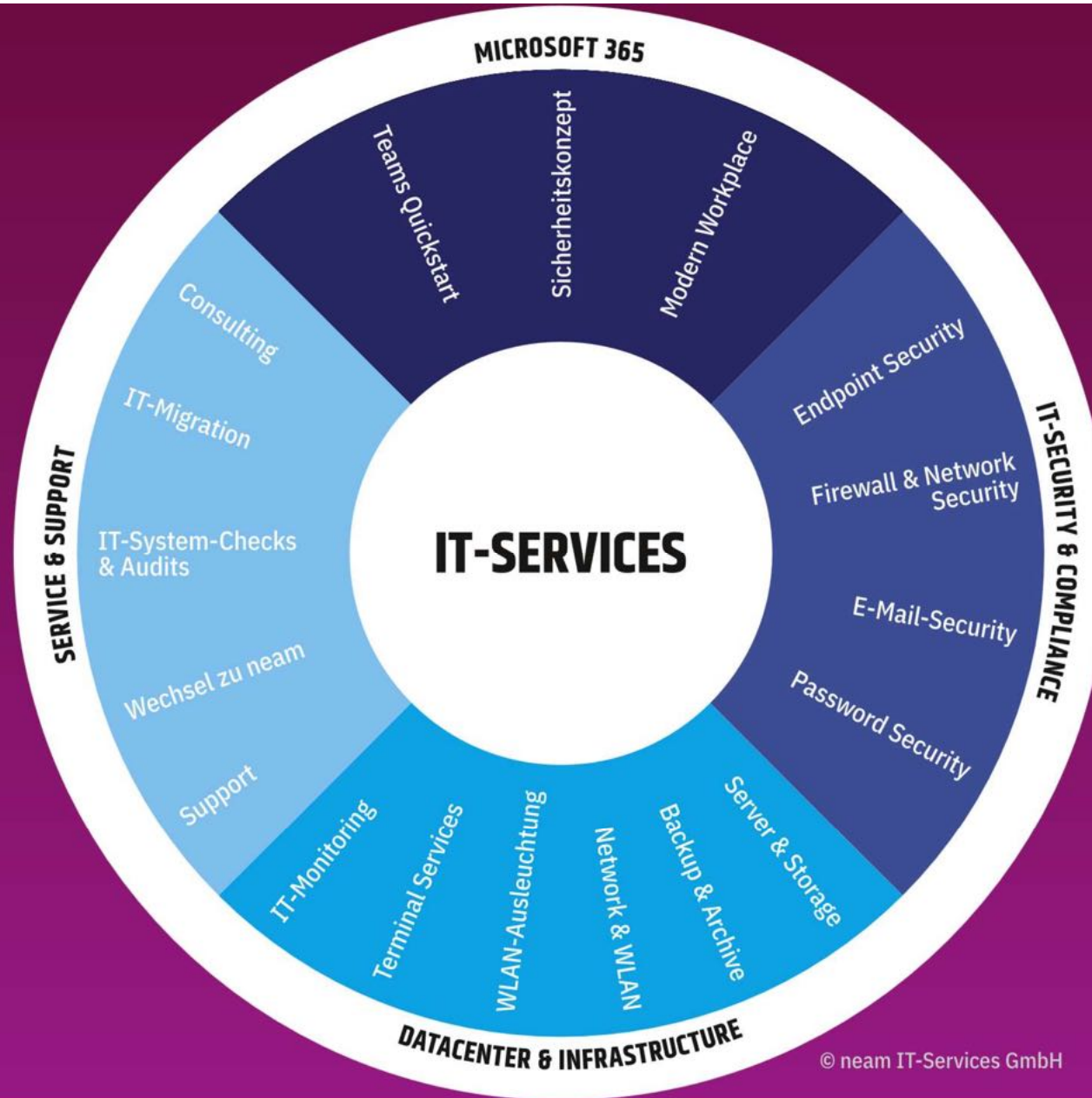
Hohes Service Level

Wir vereinen den Microsoft 365 Modern Workplace, IT-Security-Lösungen, Datacenter- und Netzwerk über alle Infrastrukturebenen und Sicherheitsanforderungen mit der Informationssicherheit.

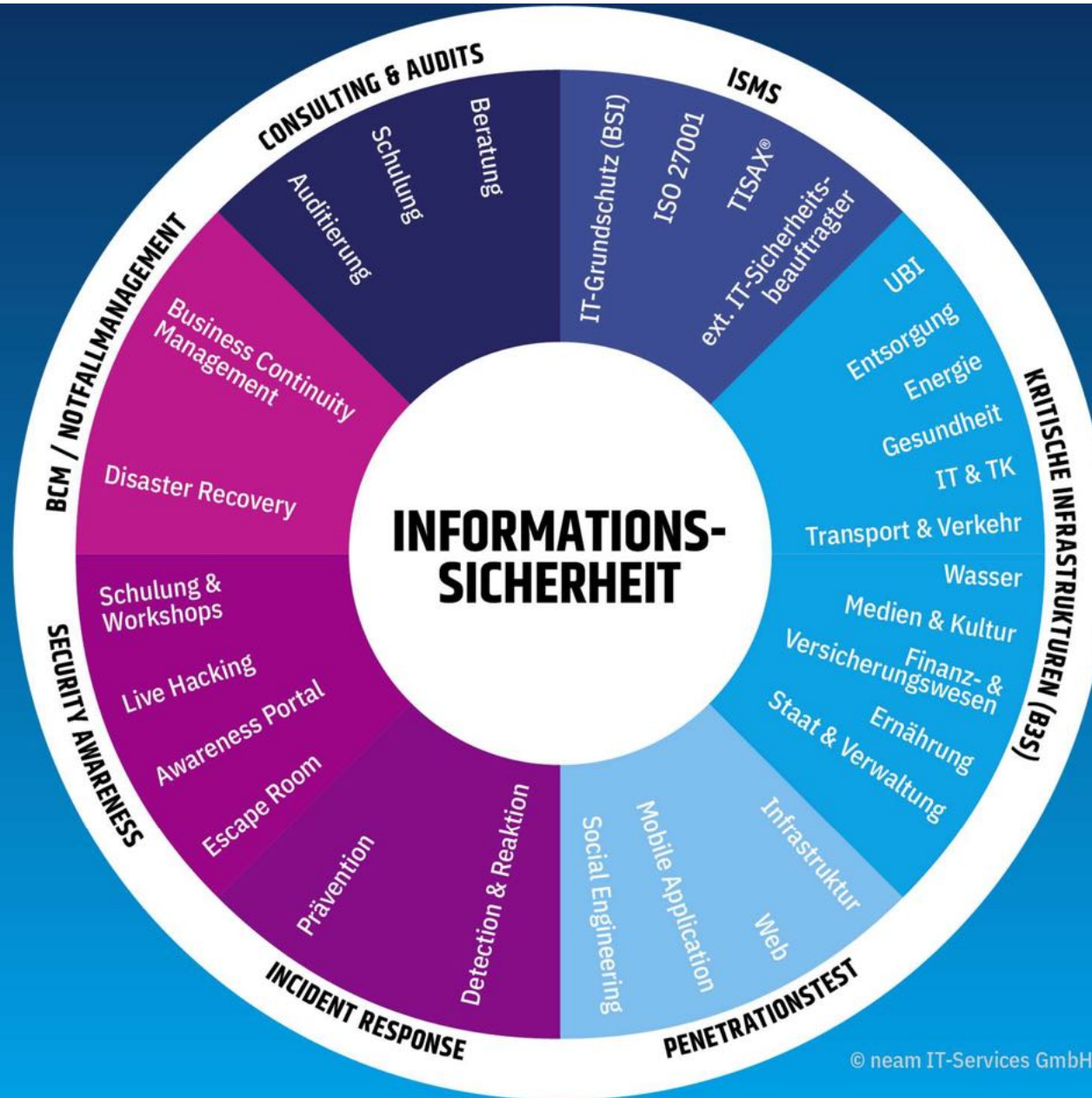
Wir sind ISO 9001 und 27001 zertifiziert und verfügen über tiefgreifende Projekterfahrung.

Vertrauen Sie unseren zertifizierten Profis.











# SCHULUNGEN & WORKSHOPS

**Auch Inhouse & Online**

Unsere Trainer sind ausschließlich fest angestellte, projekterfahrene Mitarbeiter/-innen (BSI- oder ISO 27001-Umfeld bzw. im Bereich Penetrationstests).

ISMS nach ISO, IT-Grundschutz, oder technisches Know-how für IT-Lösungen: Lassen Sie sich von unseren projekterfahrenen und zertifizierten Dozenten praxisnah schulen.

# SCHULUNGEN

BSI

ISO

Incident Response

Workshops & Trainings

[www.neam.de/schulungen](http://www.neam.de/schulungen)



# Online buchbar

**21 SEP**

Paderborn

auch als Inhouse-Schulung

ISO | IT-Risikomanagement | Paderborn

**26 - 29 SEP**

Paderborn

auch als Inhouse-Schulung | garantierter Termin  
mit Zertifizierungsprüfung

ISO | 27001 Lead Implementer mit TÜV  
Rheinland geprüfter Qualifikation |  
Paderborn

**26 - 28 SEP**

Online

auch als Inhouse-Schulung | garantierter Termin  
mit Zertifizierungsprüfung

IR | BSI Vorfal-Praktiker | Online

**28 SEP**

Online

auch als Inhouse-Schulung | garantierter Termin

KRITIS | Kompakt | Online

BSI Notfallmanagement

## BSI | IT-Grundschutz-Praktiker | Online

auch als Inhouse-Schulung mit Zertifizierungsprüfung

DATUM	UHRZEIT	PREIS	ORT
07 - 11 Feb 2022 <i>Dauer: 4 Tage inkl. Prüfung</i>	9:00 - 16:00 <i>letzter Tag bis ca. 14 Uhr (Prüfungsdauer: 60 Minuten)</i>	1.690,00€ <i>Preis pro Teilnehmer, zzgl. MwSt. inkl. Prüfungsgebühr</i>	Online

[direkt zur Buchung/Anfrage](#)

### BUCHUNG/ANFRAGE

BSI | IT-Grundschutz-Praktiker | Online

07.02.2022 - 11.02.2022

**Anfrage**

unverbindliche Anfrage

verbindliche Buchung

**Datenschutz**

Ich bin damit einverstanden, dass meine Daten entsprechend [Datenschutzhinweis](#) verarbeitet werden.

[ABSENDEN](#)

# connexa auf einen Blick

- Gruppengesellschaften, Standorte & Facts -

---

Leistungsangebot der Gruppe

## Kurzvorstellung

# Die Gruppe

Die connexta-Gruppe bietet das Beste aus beiden Welten: Die Kraft und Kompetenz eines deutschlandweiten IT-Dienstleisters, bei dem sich die einzelnen Gruppengesellschaften perfekt in ihren fachlichen sowie in ihren regionalen Schwerpunkten ergänzen, und gleichzeitig die persönliche Nähe und Flexibilität eines mittelständischen Unternehmens. Für unsere Kunden und Kundinnen aus dem deutschen Mittelstand sind wir der führende Hybrid-Cloud-Dienstleister.

Mit zwölf Standorten in Ahrensburg, Ansbach, Augsburg, Berlin, Bremen, Kempten, Kötz bei Ulm, München, Oldenburg, Paderborn, Passau und Wiesbaden ist die connexta-Gruppe bereits heute eine der erfolgreichsten IT-Service-Provider-Plattformen in Deutschland und wird durch Mergers & Acquisitions auch anorganisch zum Nutzen der Kunden kontinuierlich weiter wachsen.



# Gruppengesellschaften, Standorte und Facts



- 400+ IT-Experten
- 30+ Jahre Erfahrung in der IT-Branche
- 1.500+ erfolgreich umgesetzte Projekte
- 120 Mio. €+ Umsatz

# Das Leistungsangebot



## Sicherheitsrisiken reduzieren

Schützen Sie Ihre IT und behalten Sie die Kontrolle über Ihre wertvollen Unternehmensdaten.



## Modern, flexibel & effizient arbeiten

Ein moderner, digitaler und sicherer Arbeitsplatz besteht aus mehr als großartiger Technologie.



## Innovativer & schneller werden

Gemeinsam planen und realisieren wir den richtigen Innovations-sprung für Ihre Unternehmens-IT.



## IT-Abteilung entlasten / auslagern

Schaffen Sie wertvolle freie Kapazitäten für die langfristige Weiterentwicklung Ihrer Unternehmens-IT.



## Daten hochverfügbar managen

Daten verdienen die größte Aufmerksamkeit, da sie zum wichtigsten Gut des Unternehmens geworden sind.



## Komplexität reduzieren

Immer komplexere IT-Strukturen führen zu Engpässen, Verzögerungen und unnötigen Kosten.