

01100
0011100011011010
10101011001011110
001110101101100101011
110101101010110000111
0101111001101101010
010 0110 0111100011100010101110110001
10111000010101011000101101011011000
01110001 1010111001100110011010
1101010110101100011
110111000

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Herzlich willkommen!

Eine Initiative von:



Cyber-Sicherheit im Fokus

10:00 – 10:05

Begrüßung – Holger Schmitz, Sprecher IT-Security-Expertsgroup
Laneexpert GmbH

10:05 – 10:35

Impulsvorträge:

- ✓ NIS II, Lieferkette & Datenschutz
(Dr.iur. Ludwig Notsch, Unternehmensberater, Internetjurist)
- ✓ Cyber-Angriff Notfallplan – Was tun, wenn es passiert?
(Mag. Angelika Höber, FH CAMPUS 02)

10:35 – 10:45

Vorstellung DIH SÜD & Leistungen

10:45 – 11:30

Thementische:

- ✓ Austausch mit den Expert*innen und Zusammenfassung der Ergebnisse

11:30

Veranstaltungsende & Ausklang

```
01100
0011100011011010
10101011101011110
0011101011011001101011
111010110101011000111
010111001101101101010
010 0110 0111100011100010101110110001
101110001101010110001011101011011000
01110001 1010111001100110011010
11010101101011000111
110111000
```

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Mitwirkende:



Business Frühstück

Holger Schmitz, Sprecher IT-Security-Expertsgroup
Laneexpert GmbH



01100
0011100011011010
10101011001011110
0011101011011001101011
111010110101011000111
0101111001101101101010
010 0110 0111100011100010101110110001
101110001101010110001011101011011000
01110001 1010111001100110011010
11010101101011000111
110111000

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Eine Initiative von:



Die Angebote der Wirtschaftskammer Kärnten

- ✓ Beratungen, Digital Consultant
- ✓ KMU DIGITAL & GREEN
- ✓ Beratungsangebot NIS 2
- ✓ Cyber Security Hotline 0800 888 133
- ✓ www.it-Safe.at
- ✓ wko.at/ki NEU: KI-Guidelines 2. Fassung



ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Business Frühstück

01100
0011100011011010
10101011001011110
00111010110110010101
11101010101011000111
01011100110110101010
010 0110 0111100011100010101110110001
10111000110101011000101101011011000
01110001 1010111001100110011010
110101010101100011
110111000

Impulsvortrag 1: NIS 2, Lieferkette & Datenschutz

Dr. Ludwig Notsch, Unternehmensberater, Internetjurist



KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Eine Initiative von:





„Erfolgreiche“ Cyberkriminalität ist das Ergebnis von *fehlendem* Datenschutz



SURINAME ✕

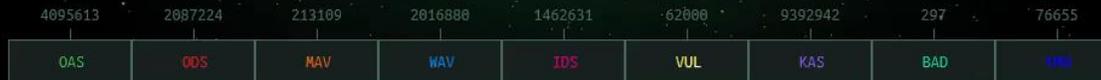
193 HÄUFIGST ANGEGRIFFENE LÄNDER

OAS	31
ODS	24
MAV	9
WAV	17
IDS	9
VUL	9
KAS	5
BAD	9
IRN	9

Ermittelte Ekennungen seit 00:00 GMT

[Mehr Details](#)

Daten teilen





Platz 52 Österreich 2024

von gesamt aktuell 195 Ländern

#01

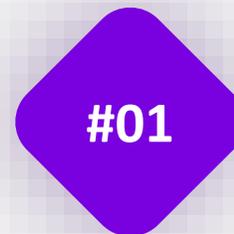




Platz 38
Österreich

2025

von gesamt aktuell 195 Ländern



CYBERBEDROHUNGEN LIVE-KARTE  DE

KARTE STATISTIK DATENQUELLEN BUZZ WIDGET

 **ÖSTERREICH** 

38 HÄUFIGST ANGEGRIFFENE LÄNDER

OAS	5373
ODS	3871
MAV	273
WAV	13908
IDS	3420
VUL	307
KAS	3895
BAD	0
RPW	10

Ermittelte Ekennungen seit 00:00 GMT

[Mehr Details](#)

Daten teilen



	DEUTSCHLAND	VEREINIGTE STAATEN	RUSSLAND
	# 5 HÄUFIGST ANGEGRIFFENE LÄNDER	# 2 HÄUFIGST ANGEGRIFFENE LÄNDER	# 1 HÄUFIGST ANGEGRIFFENE LÄNDER
Platz 5 Deutschland			
	OAS 24483	24483	364073
	ODS 100726	100726	184614
	MAV 511	511	52105
Platz 2 USA	WAV 32543	32543	103391
	IDS 65625	65625	52822
	VUL 866	866	1749
	KAS 148199	148199	533198
	BAD 0	0	0
	BMW 23	23	982
Platz 1 Russland	Ermittelte Ekennungen seit 00:00 GMT	Ermittelte Ekennungen seit 00:00 GMT	Ermittelte Ekennungen seit 00:00 GMT
	Mehr Details	Mehr Details	Mehr Details
	Daten teilen	Daten teilen	Daten teilen



#01

Was hat das mit **JUS** zu tun?

NIS 2

Datenschutz

Lieferkette



01

NIS 2



► NIS 2 >

NIS

= **N**etzwerk- und **I**nformations**S**icherheit

NIS 2

Ziel:

Gemeinsames, hohes Sicherheitsniveau
in der EU



01

Anwendungsbereich?



► Direkt angesprochen >



Zwei Hauptprüfkriterien

1. In einem sog. **einschlägigen Sektor** tätig?
2. **Größenschwellen** überschritten?
(= Size-Cap)

01

Anhang 1 + 2

Essential Entities
(Wesentliche Einrichtungen)
Sektoren mit hoher Kritikalität

Anhang I

- **Energie**
- **Luft-, Schienen-, Straßen- und Schiffsverkehr**
- **Bankwesen/ Finanzwesen**
- **Gesundheit**
- **Wasser**
- **Digitale Infrastruktur und IT-Dienste**
- **Öffentliche Verwaltung**
- **Raumfahrt**

► Einschlägige Sektoren >

Important Entities
(Wichtige Einrichtungen)
Sonstige kritische Sektoren

Anhang II

- **Anbieter von Post- und Kurierdiensten**
- **Abfallwirtschaft**
- **Chemische Erzeugnisse**
- **Lebensmittel**
- **Hersteller**
- **Digitale Anbieter**
- **Forschungseinrichtungen**

Anhang I (= Sektoren mit hoher Kritikalität)

Energie (Elektrizität, **Fernwärme/ Kälte**, Öl, Gas, **Wasserstoff**)

Verkehr (Luft, Schiene, Schifffahrt, Straße)

Bankwesen

Finanzmarktinfrastrukturen

Gesundheitswesen
(Gesundheitsdienstleister, **EU-Referenzlaboratorien**, **Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräten**)

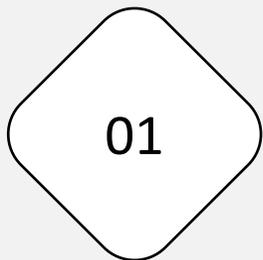
Trinkwasser

AbwasserDigitale Infrastruktur
(IXP, DNS, TLD, Cloud-Computing, **Rechenzentren**, **CDN**, **TSP** und **Anbieter von öffentlichen elektronischen Kommunikationsnetzen und-diensten**)**Verwaltung von IKT-Diensten (B2B)****Öffentliche Verwaltung****Weltraum**

Anhang II (= Sonstige kritische Sektoren)

Post- und Kurierdienste**Abfallbewirtschaftung****Chemie (Herstellung und Handel)****Lebensmittel (Produktion, Verarbeitung, Vertrieb)****Verarbeitendes/ Herstellendes Gewerbe**
(**Medizinprodukte**; **Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen**; **Maschinenbau**; **Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau**)**Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)****Forschung**

rot = Neuerungen gegenüber NIS 1



01

Jus.

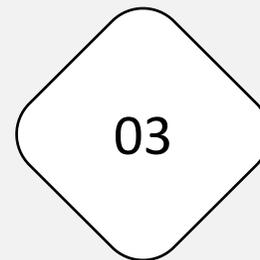
Einschlägiger Sektor.



02

Schwellenwert.

Ja oder nein.



03

Handlung.

NIS 2 Pflichten.

02

Größenschwellen „Size-Cap“



- ▶ Anwendungsbereich durch Größenschwellenwert >

Kleines Unternehmen:
weniger als 50 Personen beschäftigt

und

Jahresumsatz bzw. Jahresbilanz
unter 10 Mio. EUR

02

Größenschwellen „Size-Cap“

Kleines Unternehmen:
weniger als 50 Personen beschäftigt

und

Jahresumsatz bzw. Jahresbilanz
unter 10 Mio. EUR

▶ Anwendungsbereich durch
Größenschwellenwert >

Mittleres Unternehmen:
ab 50 bis 249 Mitarbeiter

oder

Jahresumsatz
über 10 Mio. EUR bis 50 Mio. EUR

bzw. Jahresbilanz
über 10 Mio. EUR bis 43 Mio. EUR

02

Größenschwellen „Size-Cap“

Mittleres Unternehmen:
ab 50 bis 249 Mitarbeiter

oder

Jahresumsatz
über 10 Mio. EUR bis 50 Mio. EUR

bzw. Jahresbilanz
über 10 Mio. EUR bis 43 Mio. EUR

▶ Anwendungsbereich durch
Größenschwellenwert >

Großes Unternehmen:
ab 250 Mitarbeiter

oder

Jahresumsatz
über 50 Mio. EUR

bzw. Jahresbilanz
über 43 Mio. EUR



02

Wie ist NIS 2
Anwendung
konkret zu
Prüfen?



Prüfmodus.

EU.

Erbringt das Unternehmen seine Dienstleistungen in der EU oder übt seine Tätigkeiten in der EU aus?



Sektor.

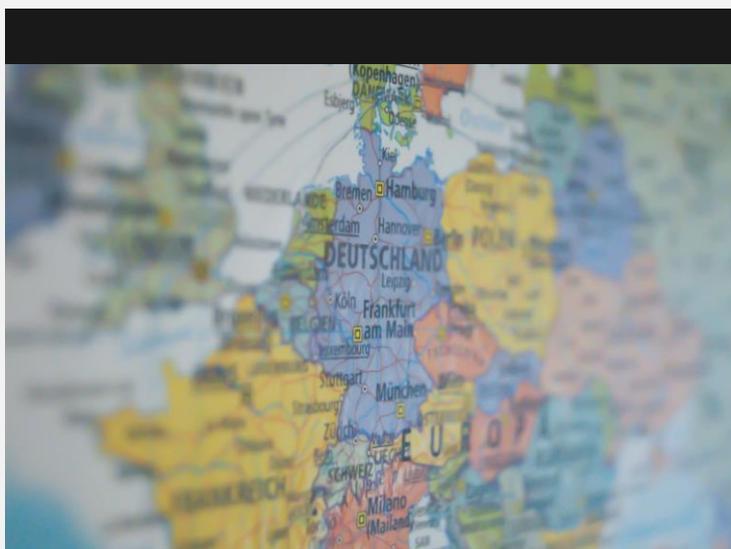
Ist das Unternehmen in einem einschlägigen Sektor (Anhang I und II NIS 2 Richtlinie) tätig?



Größe.

Ist der Größenschwellenwert überschritten?

#001.



#002.



#003.





Handlung. NIS 2 Pflichten



Pflichten.





Pflichten #001.

Risikomanagementmaßnahmen



Unternehmen müssen Maßnahmen ergreifen, um die **Risiken für die Sicherheit ihrer Netz-und Informationssysteme** zu beherrschen und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder möglichst gering zu halten



Pflichten #001.

Risikomanagementmaßnahmen



Unternehmen müssen Maßnahmen ergreifen, um die **Risiken für die Sicherheit ihrer Netz-und Informationssysteme** zu beherrschen

und die Auswirkungen von Sicherheitsvorfällen zu verhindern oder

möglichst gering zu halten

Pflichten #002.



Berichtspflichten

Unternehmen müssen erhebliche Sicherheitsvorfälle unverzüglich an das Computer Notfallteam (CERT/CSIRT) **melden**.

Unternehmen müssen gegebenenfalls Empfänger ihrer Dienste über erhebliche Sicherheitsvorfälle und Bedrohungen **informieren**.



RISIKOMANAGEMENT
#001.

- 
- ✓ Risikoanalyse
 - ✓ Bewältigung von Sicherheitsvorfällen
 - ✓ Business Continuity und Krisenmanagement
 - ✓ Lieferkettensicherheit
 - ✓ Schulungen zur Cybersicherheit
 - ✓ Zugriffskontrolle



Mittelbare „Betroffenheit“ von der NIS 2 Richtlinie

Beispiel Lieferkettensicherheit

Dienstleister und Lieferanten von betroffenen Unternehmen **müssen** Sicherheitsvorkehrungen treffen.

Überbinden von Informationssicherheitsmaßnahmen auf **Dienstleister** und **Lieferanten** durch **direkt** betroffene Unternehmen.



Risikoeinschätzung mittels Risikomatrix.

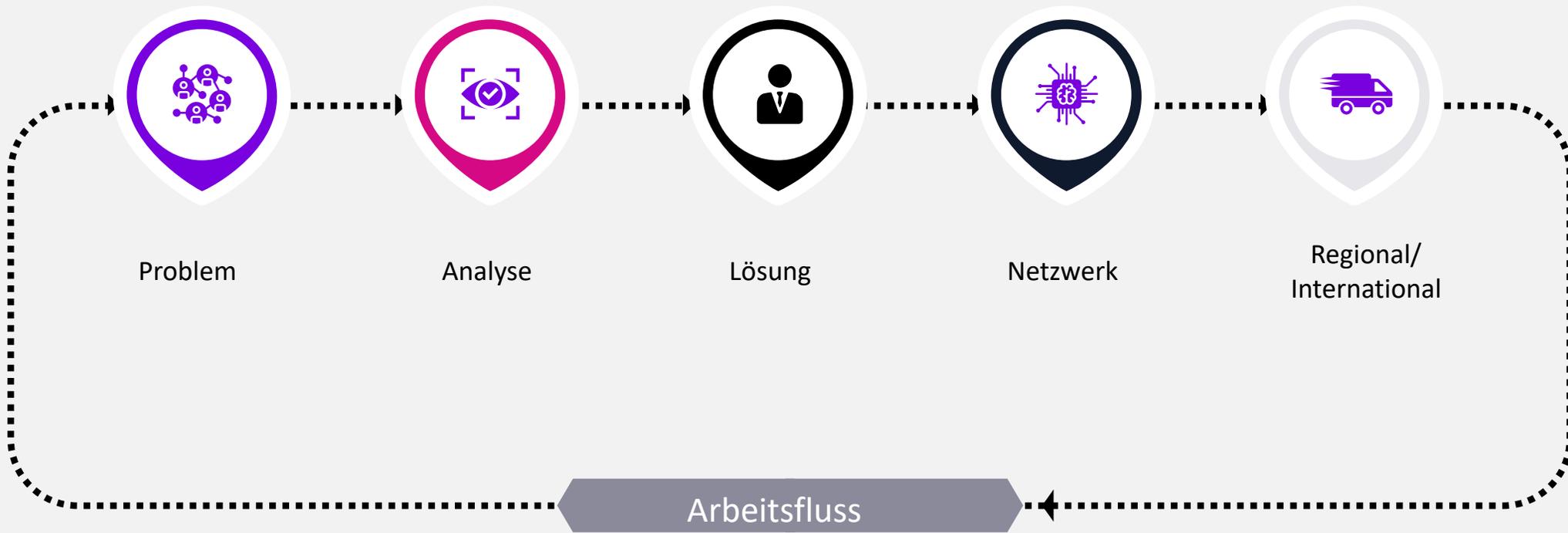






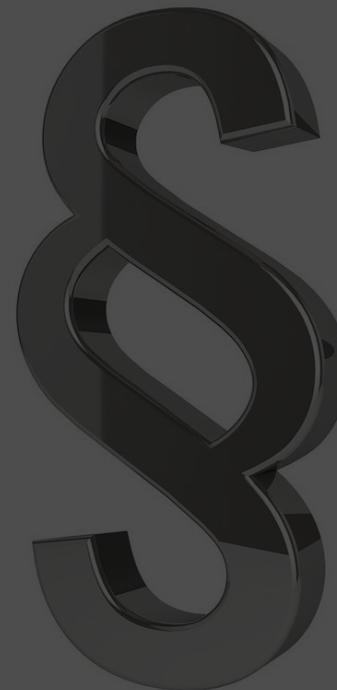
Dr.iur. Ludwig Notsch

INTERNETJURIST & DATENSCHUTZJURIST





LIKE & FOLLOW FOR MORE





Danke
für Ihre geschätzte
Aufmerksamkeit



Disclaimer:

Alle Informationen in diesem Vortrag sind nach bestem Wissen und Gewissen zusammengestellt.

Aktuelle Rechtsmaterien sind schnelllebig und kontinuierliche Veränderungen immanent. Die Präsentation stellt die Themen auszugsweise dar und bildet nur mit den mündlichen Ausführungen des Referenten eine entsprechende Einheit. Jede Weitergabe und/ oder Vervielfältigung der Unterlagen ohne Zustimmung des Referenten ist unzulässig!

Der Referent des Vortrags weist darauf hin, dass keine Haftung für die Richtigkeit, Aktualität und Vollständigkeit übernommen wird. Insbesondere ersetzt dieser Vortrag keine rechtliche, organisatorische oder technische Beratung im Einzelfall.

Die Teilnehmer sind sowohl für die Richtigkeit als auch für die Vollständigkeit ihrer Unterlagen und Auskünfte verantwortlich, auch gegenüber den Nutzern der im Vortrag erstellten Unterlagen.

Weiters schließt der Referent des Vortrags jegliche Haftung im Zusammenhang mit der möglichen Dateneinsicht, Datenverwendung und Datenweitergabe der Teilnehmer untereinander, aus.

Der Vortrag behandelt die aktuelle Rechtslage. Für mögliche Interpretationen und Auslegungsvarianten wird eine Haftung gleichermaßen ausgeschlossen wie für eine heute noch nicht absehbare Rechtsprechung. Die Vertragspartner vereinbaren einen wechselseitigen Ausschluss der Haftung.

Datenstand: März 2025

Business Frühstück

01100
0011100011011010
10101011001011110
00111010110110010101
11101010101011000111
01011100110110101010
010 0110 0111100011100010101110110001
10111000110101011000101101011011000
01110001 1010111001100110011010
11010101101011000111
110111000

Impulsvortrag 2: Cyber-Angriff Notfallplan – Was tun, wenn es passiert?

Mag. Angelika Höber, FH CAMPUS 02



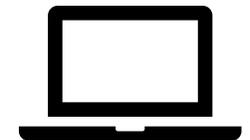
KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Eine Initiative von:



Ein ganz normaler Tag





CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Ziel: handlungsfähig bleiben

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse

Dokumentation

Kommunikation

Notfallteam

Vorgehensplan

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

❖ **Gefördert durch DIH-Süd Kooperation**

- ▶ **Ziel:** Unterstützung von KMUs gegen Cyberkriminalität
- ▶ **Basis:** Interviews mit Expert*innen und Betroffenen

❖ **Disclaimer**

- ▶ Erfordert regelmäßige individuelle Prüfung und Anpassung
- ▶ Dienst als Ergänzung zum techn. Sicherheitskonzept
- ▶ Professionelle Unterstützung im Angriffsfall wird empfohlen

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse

Was muss täglich laufen?



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Dokumentation

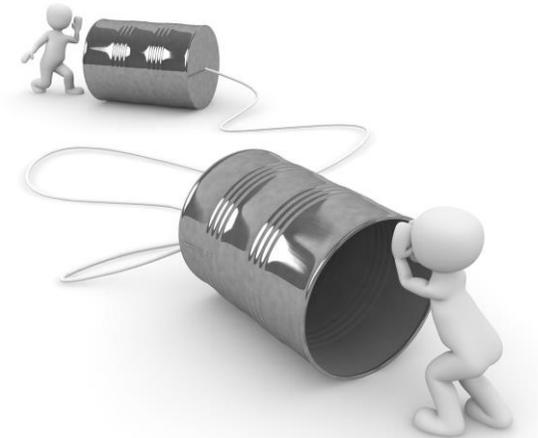
*Auf welche Dokumente muss immer
zugegriffen werden können?*



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Kommunikation

*Wie wird kommuniziert?
Was wird kommuniziert?
Mit wem?*



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Notfallteam

*Wer wird kontaktiert?
Wer koordiniert?
Wer entscheidet?*



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Vorgehensplan



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse



Dokumentation



Kommunikation



Notfallteam



Vorgehensplan



Ziel: handlungsfähig bleiben



Business Frühstück

01100
0011100011011010
10101011001011110
0011101011010010101
1110101101010000111
010111001101101010
010 0110 0111100011100010101110110001
10111000110101011000101101011011000
01110001 1010111001100110011010
1101010110101100011
110111000

DIH SÜD Vorstellung & Leistungen

Martina Eckerstorfer
Geschäftsführerin DIH SÜD

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ



Eine Initiative von:



DIGITALISIERUNG FÜR KMU

MÖGLICH MACHEN

DER DIGITAL INNOVATION HUB SÜD ALS KOSTENLOSES
SERVICE FÜR KMU



UNSERE LEISTUNGEN

Der DIH SÜD
unterstützt KMU in
der Region
Südösterreich bei der
digitalen
Transformation.

Nicht wirtschaftlich tätiges Kompetenznetzwerk

- Netzwerk aus Digitalzentren, Netzwerkpartnern und Multiplikatoren

Unterstützung von KMU mit Schulungsangeboten

- Information, Qualifizierungsmaßnahmen, Aus- und Weiterbildung

Zugang zu Infrastruktur

- Zugang zu Laboren, Unterstützung bei Prototypenherstellung etc.

UNSERE PARTNER



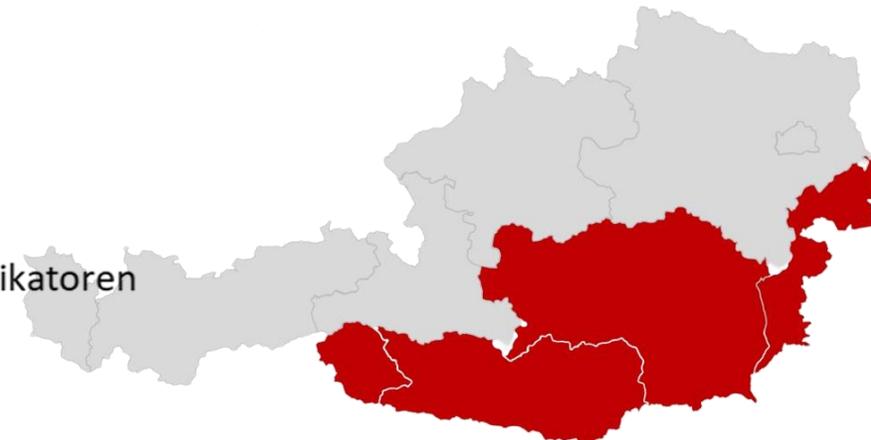
Digitalzentren



Netzwerkpartner



Multiplikatoren



UNSERE THEMEN

 Produktions- &
Fertigungstechnologien



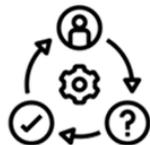
 Sicherheit



 Data Science –
Wissen aus Daten



 Digitale Geschäftsmodelle
& -prozesse



 Logistik



 Humanressourcen



UNSERE AKTIVITÄTEN



IT Security für KMU

- **Basics / Expert / Advanced**
- Security Know-how & Maßnahmen
- Umgang mit Risiken und Entwicklung von Strategien
- Erarbeiten von Security Best Practices für verschiedene IT-Ansätze von KMU
- Sichere Nutzung von Public Cloud Ressourcen
- Cyber Trust Austria Siegel



Penetration Test Trainings

- 3-tägiges Training
- Aufzeigen aktueller Gefahren
- Identifizierung von Schwachstellen eines Unternehmens
- Test von Angriffen und Verteidigungs-Strategien



Cyber Security – Notfallplan

- Einführung Cyber Security
- Vorbereitung auf und Verhalten im Angriffsfall
- Bewusstseinsbildung über aktuelle Bedrohungen
- Vorstellung des Leitfadens / Notfallplans (Maßnahmen vor, während und nach eines Angriffes)
- Erarbeitung von Maßnahmen für KMU



NIS 2 Richtlinie

- Richtlinie zu einem gemeinsamen Sicherheitsniveau von Netz- und Informationssystemen
- Ziele, Anforderungen und Bestimmungen für das eigene Unternehmen

Informieren Sie sich über unser **Angebot**

- Aktivitäten:
<https://www.dih-sued.at/veranstaltungen>
- Newsletter:
<https://www.dih-sued.at/newsletter>



Digitalisierung
ist easy!

Business Frühstück

Thementische – Austausch mit den Expert*innen

01100
0011100011011010
10101011001011110
00111010110110010101
1110101101010000111
010111000101101101010
010 0110 0111100011100010101110110001
10111000010101011000101101011011000
01110001 1010111001100110011010
1101010110101100011
110111000

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Eine Initiative von:



Thementische – Austausch mit den Expert*innen

Thementisch 1:

- **NIS II, LIEFERKETTE UND DATENSCHUTZ**

Thementisch 2:

- **CYBER-SECURITY NOTFALLPLAN**

3 MIN

1 MIN

Vielen Dank für Ihre Aufmerksamkeit!

Eine Initiative von:

