Business Frühstück

Cyber-Sicherheit im Fokus

Rechtlicher Rahmen und Handlungsempfehlungen bei Cyber-Angriffen

Impulsvorträge & Austausch mit den Expert*innen

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Termin: **6. März 2025, 10:00 – 11:30 Uhr**

Ort: **Wirtschaftskammer Klagenfurt**
Europaplatz 1, 9020 Klagenfurt
WIFI Haupthaus, Erdgeschoss (Raum C001)

Jetzt anmelden!

Eine Initiative von: DIHSÜD Digital Innovation Hub | WKO Wirtschaftskammer Kärnten

Business Frühstück

Programm:

10:00 – 10:05 **Begrüßung**

10:05 – 10:35 **Impulsvorträge:**

- ✓NIS II, Lieferkette & Datenschutz
  (Dr. Ludwig Notsch, Wirtschaftskammer Kärnten)

- ✓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**

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Mitwirkende:

DIH SÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

Business Frühstück

Begrüßung

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Eine Initiative von:

DIHSÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

Business Frühstück

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Impulsvortrag 1: NIS 2, Lieferkette & Datenschutz

Dr. Ludwig Notsch, Wirtschaftskammer Kärnten

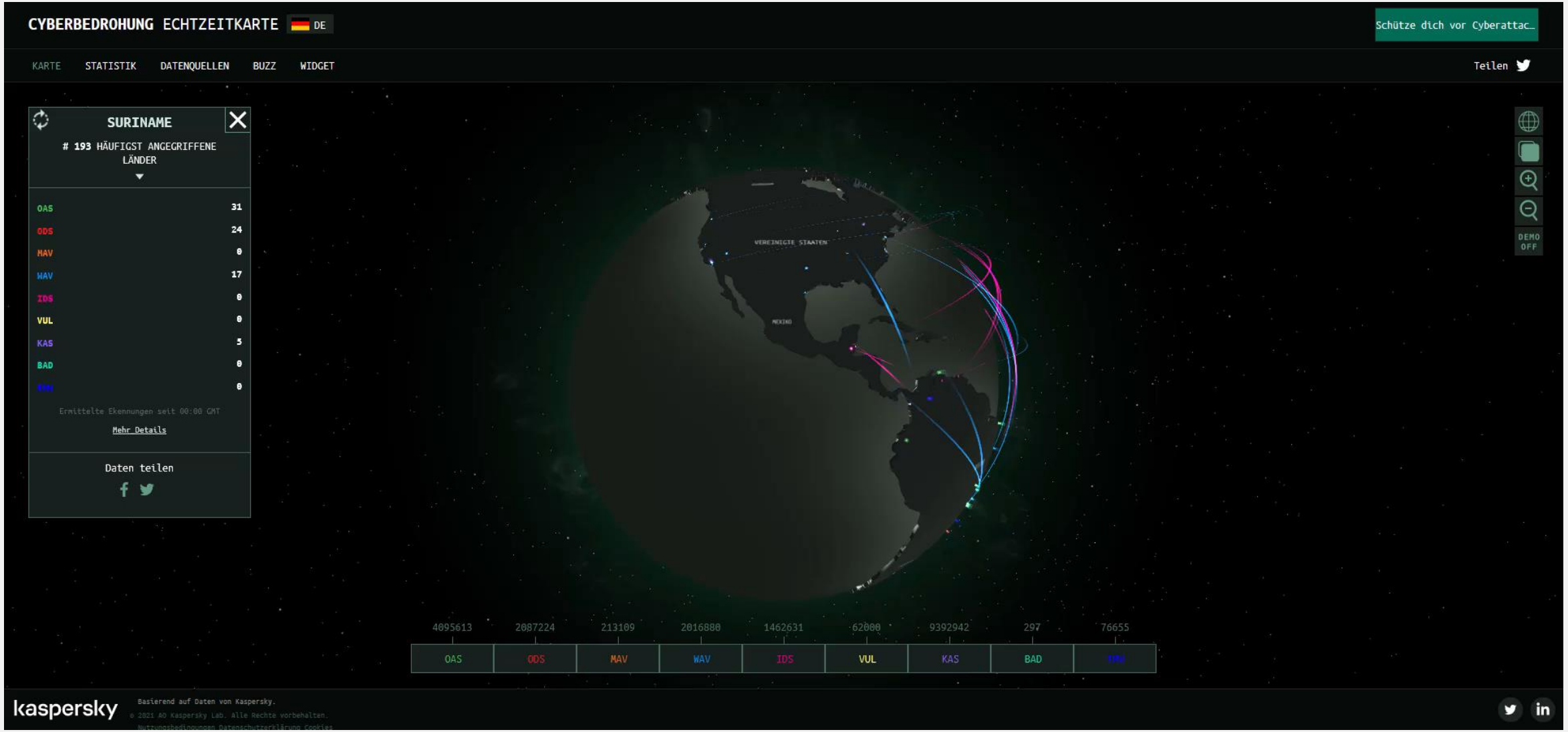
Eine Initiative von:

DIHSÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

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

Das passiert im Internet in EINER Minute https://www.youtube.com/watch?v=_JU7U1uuNxo



INTERNETJURIST.AT

Cyberbedrohungen in Echtzeit https://cybermap.kaspersky.com/de

Platz 52 Österreich 2024

von gesamt aktuell 195 Ländern

Platz 38
Österreich

2025

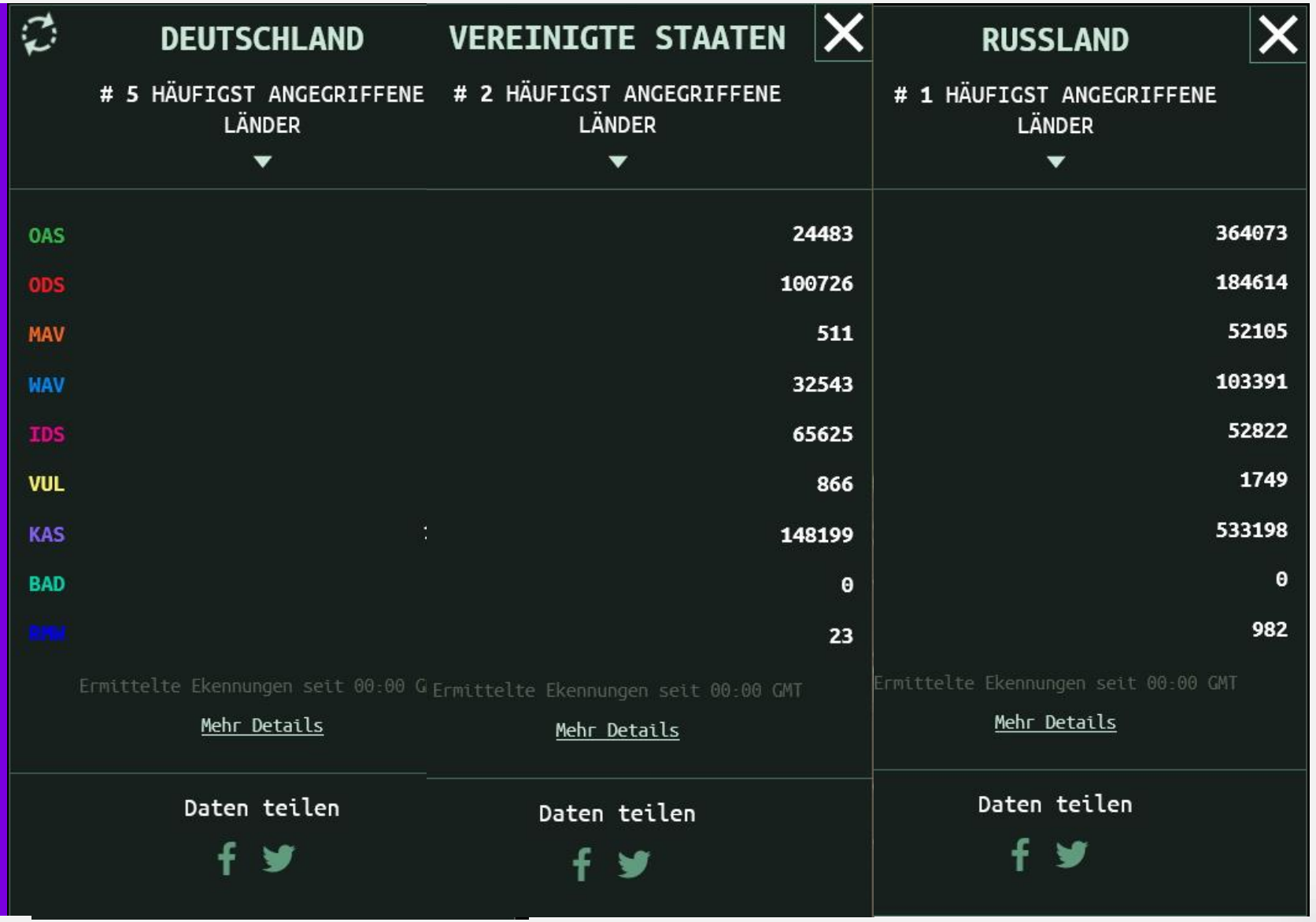
#01

von gesamt aktuell 195 Ländern

Platz 5 Deutschland

Platz 2 USA

Platz 1 Russland



#01

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

NIS 2

Datenschutz

Lieferkette

INTERNETJURIST.AT

01

NIS 2

NIS 2 >

NIS

= Netzwerk- und InformationsSicherheit

NIS 2

Ziel:

Gemeinsames, hohes Sicherheitsniveau in der EU

01

Anwendungs-bereich?

Direkt angesprochen >

Zwei Hauptprüfkriterien

1. In einem sog. **einschlägigen Sektor** tätig?

2. **Größenschwellen** überschritten? (= Size-Cap)

01

Einschlägige Sektoren >

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

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 Kritikaliität)	Anhang II (= Sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/ Kälte, Öl, Gas, Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schiffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräten)	Verarbeitendes/ Herstellendes Gewerbe (Medizinprodukte; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD,Cloud-Computing, Rechenzentren, CDN, TSP und Anieter von öffentlichen elektronischen Kommunikationsnetzen und-diensten)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	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

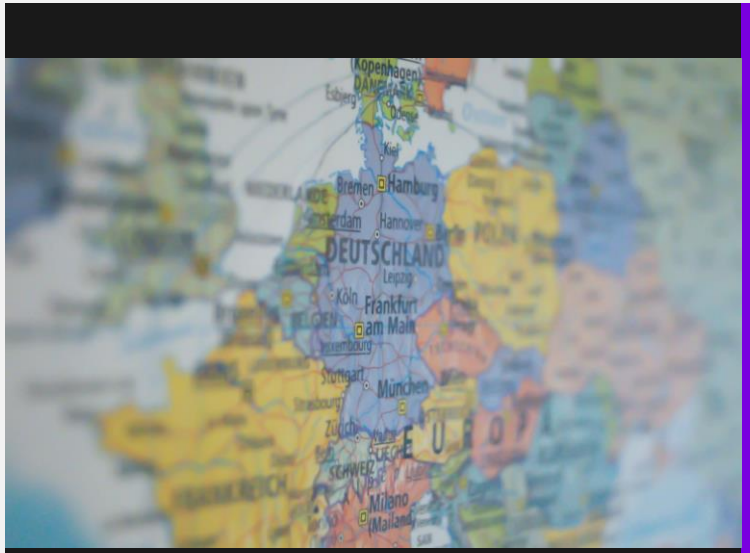
Wie ist NIS 2 Anwendung konkret zu Prüfen?

Prüfmodus.

EU.

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

#001.



Sektor.

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

#002.

Größe.

Ist der Größenschwellenwert überschritten?

#003.

Handlung.
NIS 2 Pflichten

#03

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.

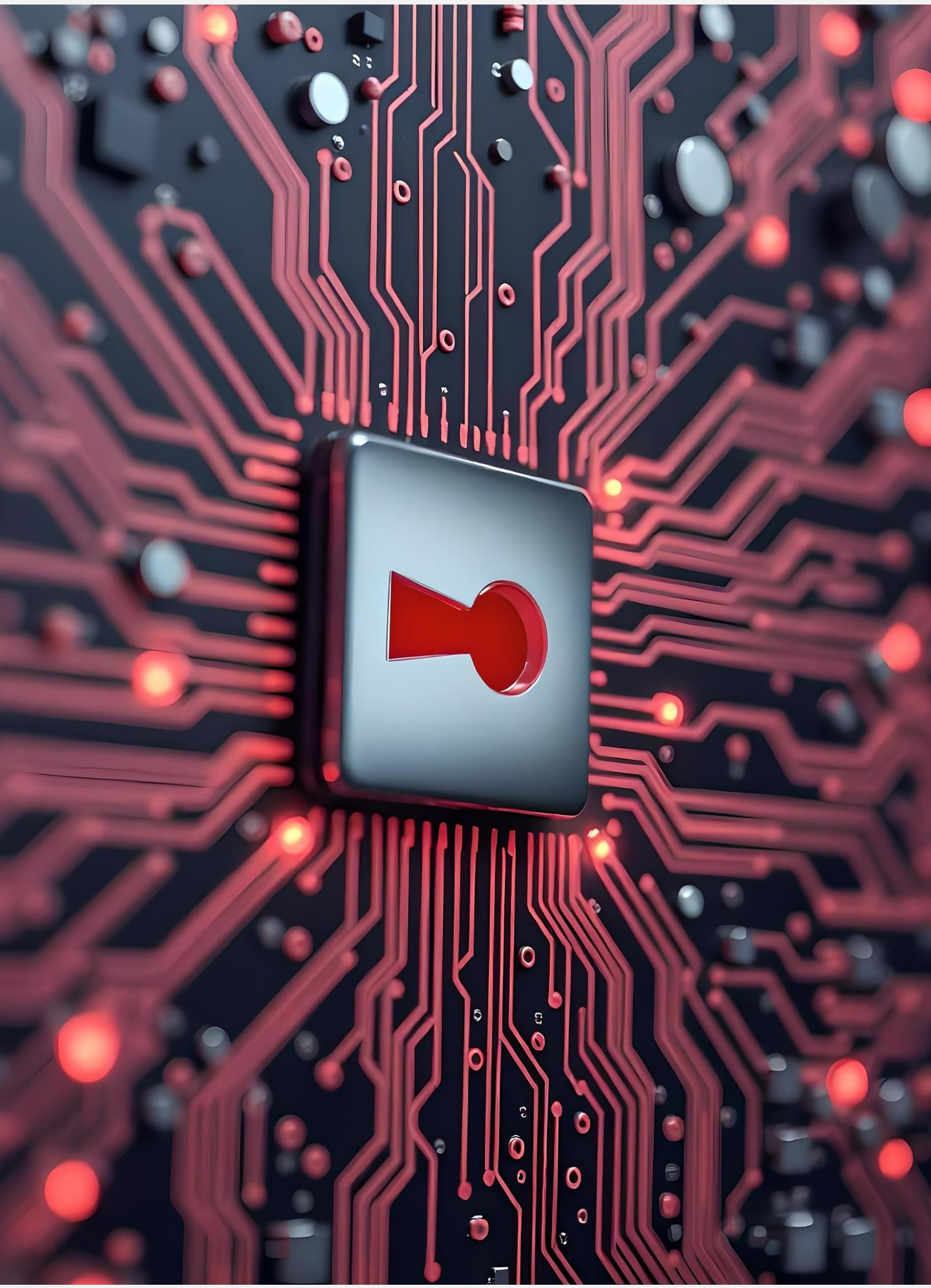
Aktueller Stand kurz zusammengefasst:

Cybersicherheitsrichtlinie NIS 2
in Belgien, Italien, Kroatien und Litauen
umgesetzt

Österreich
Noch nicht absehbar, wann ein „NIS 2
Gesetz“ kommt.

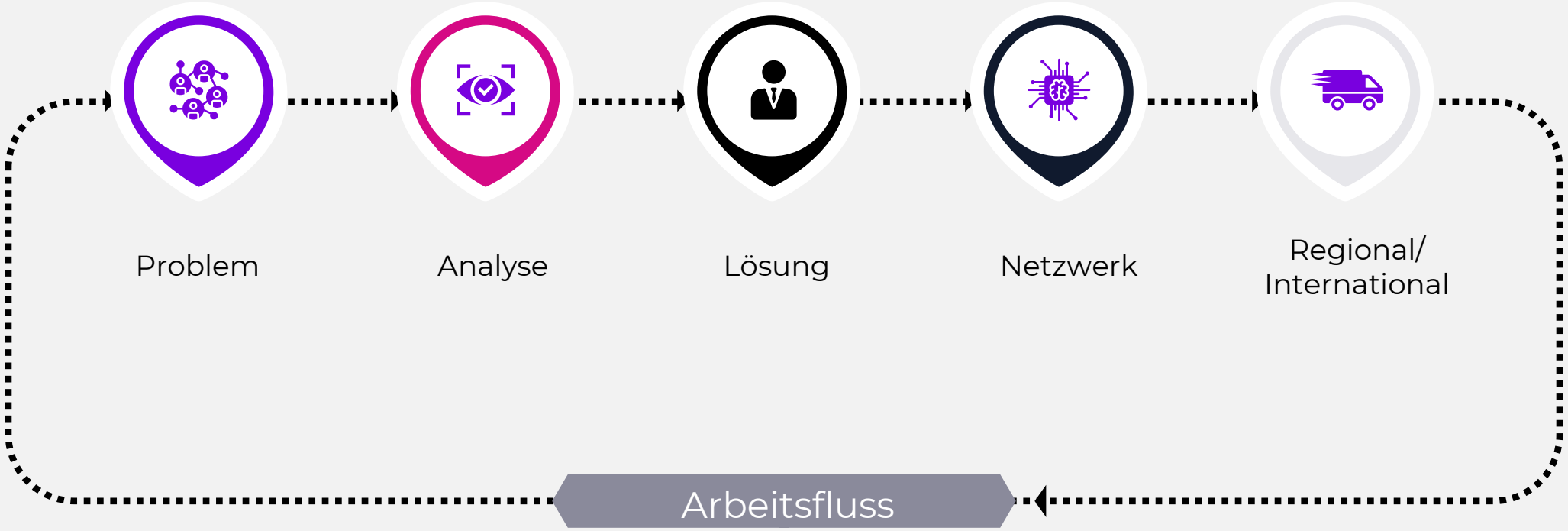
NIS 2 Compliance
Wird verlangt bzw. verlangt werden

Verlieren Sie keine Zeit!



Dr.iur. Ludwig Notsch

INTERNETJURIST & DATENSCHUTZJURIST



Wien – Klagenfurt - Milano

INTERNETJURIST.AT


LIKE & FOLLOW FOR MORE
SCAN ME

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

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

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

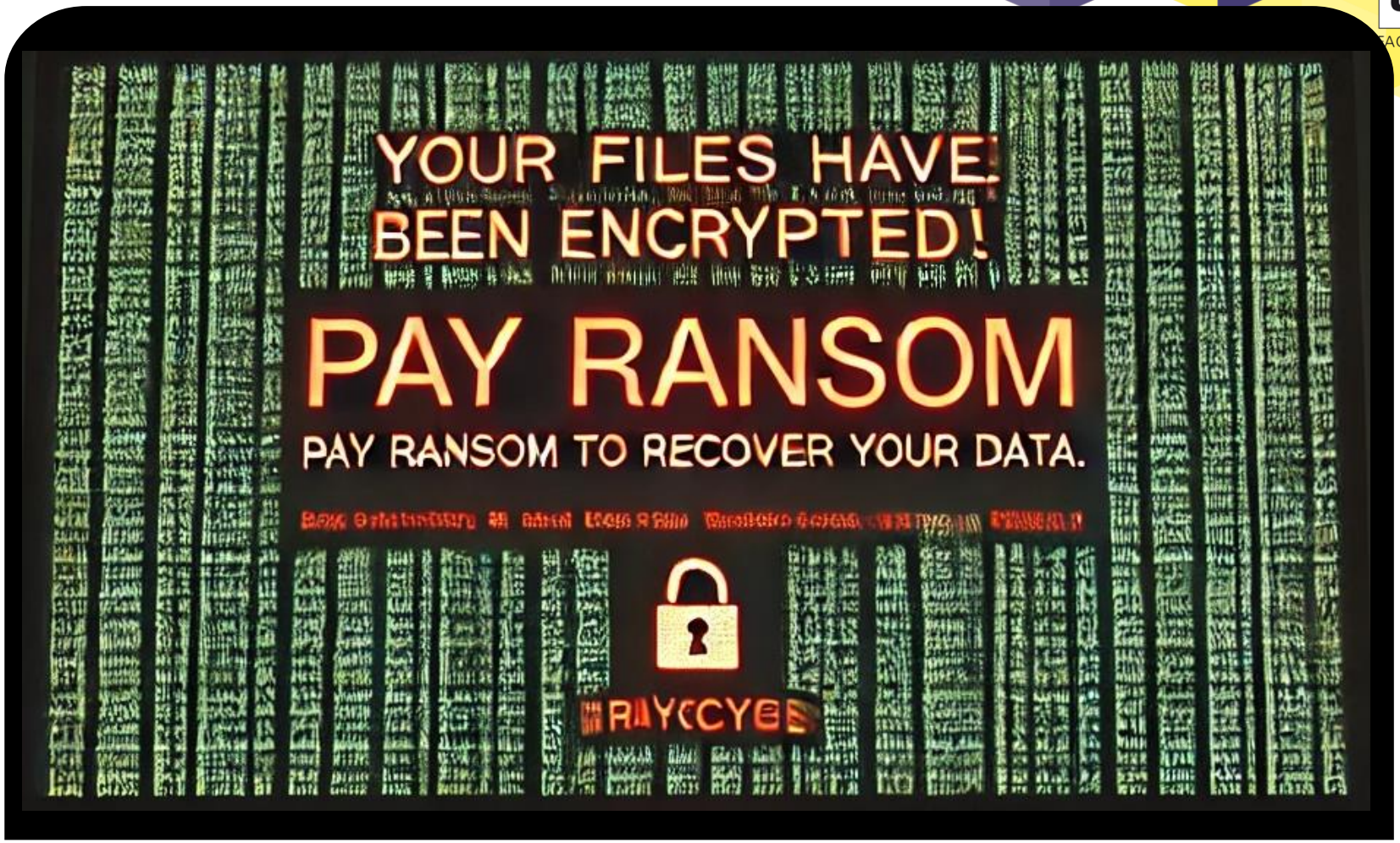
Mag. Angelika Höber, FH CAMPUS 02

Eine Initiative von:

DIHSÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

Ein ganz normaler Tag ….


YOUR FILES HAVE
BEEN ENCRYPTED!
PAY RANSOM
PAY RANSOM TO RECOVER YOUR DATA.

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

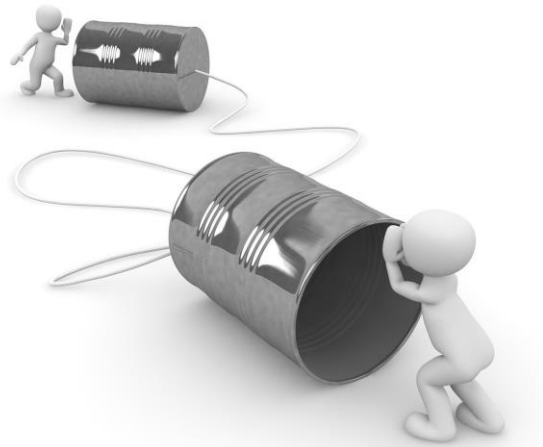
Dokumentation

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

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

DIH SÜD Vorstellung & Leistungen

Martina Eckerstorfer
Geschäftsführerin DIH SÜD

Eine Initiative von:

DIH SÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

DIHSÜD
Digital Innovation Hub

DIGITALISIERUNG FÜR KMU MÖGLICH MACHEN

DER DIGITAL INNOVATION HUB SÜD ALS KOSTENLOSES SERVICE FÜR KMU

Der DIH SÜD
wird unterstützt von:

FFG Forschung wirkt.
Das Land Steiermark
LAND KÄRNTEN

DIHSÜD
Digital Innovation Hub

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.

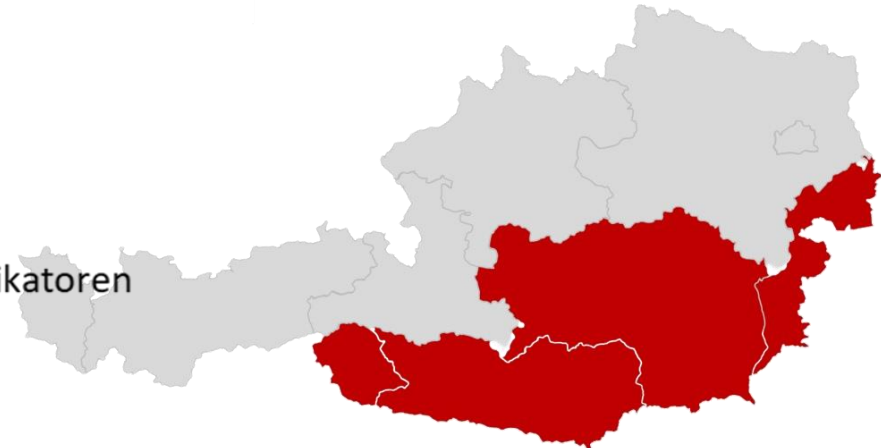
DIHSÜD
Digital Innovation Hub

UNSERE PARTNER

Digitalzentren

Netzwerkpartner

Multiplikatoren



DIHSÜD
Digital Innovation Hub

UNSERE THEMEN

- Produktions- & Fertigungstechnologien 
- Sicherheit 
- Data Science – Wissen aus Daten 
- Digitale Geschäftsmodelle & -prozesse 
- Logistik 
- Humanressourcen 

DIHSÜD
Digital Innovation Hub

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

CODING. SCHOOL WÖRTHERSEE
Lakeside SCIENCE & TECHNOLOGY PARK

Penetration Test Trainings

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

FH JOANNEUM University of Applied Sciences

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

CAMPUS 02 FACHHOCHSCHULE DER WIRTSCHAFT

NIS 2 Richtlinie

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

TU Graz

DIHSÜD
Digital Innovation Hub

Informieren Sie sich über unser Angebot

- Aktivitäten:
  https://www.dih-sued.at/veranstaltungen

- Newsletter:
  https://www.dih-sued.at/newsletter

Business Frühstück

Thementische – Austausch mit den Expert*innen

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Eine Initiative von:

DIHSÜD Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

Thementisch 1:

NIS II, LIEFERKETTE UND DATENSCHUTZ

WIRTSCHAFTSKAMMER KÄRNTEN

Thementisch 2:

CYBER-SECURITY NOTFALLPLAN

CAMPUS 02 GRAZ
FACHHOCHSCHULE DER WIRTSCHAFT

3 MIN

1 MIN