100. KI-Business Frühstück

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

KI & Cyber-Sicherheit im Fokus

Notfallpläne, IT-Sicherheit und Datensouveränität, AI Act und NIS2

Impulsvorträge & Austausch mit den Expert*innen

Herzlich willkommen!

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

DIHSÜD Digital Innovation Hub

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

100. KI-Business Frühstück

Begrüßung
Martin Zandonella
Fachgruppenobmann UBIT

Eine Initiative von:

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

175 JAHRE WKO
WIRTSCHAFTSKAMMER KÄRNTEN

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

100. Veranstaltung von KI Österreich

Eine Initiative von:

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

175 JAHRE WKO
WIRTSCHAFTSKAMMER KÄRNTEN

KI Österreich

KI Österreich ist im Jahr 2022 durch die Initiative der WK Österreich als Kooperationsprojekt der WK Kärnten, WK Steiermark und WK Burgenland mit dem DIH SÜD gestartet.

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Formate:

Impulse in form von KI-Business-Frühstücken

Workshops und Weiterbildungen

Umsetzungsbegleitung

100 Veranstaltungen in vier Jahren mit rund 4.000 Teilnehmer:innen

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

DIHSÜD Digital Innovation Hub

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

Einlass: 08:30

09:00 – 09:10 **Begrüßung**

09:10 – 09:55 **Impulsvorträge:**

- ✓Cyber-Angriff Notfallplan: Was tun, wenn es passiert? (Mag.a Angelika Höber, FH CAMPUS 02)
- ✓Zero Trust im Microsoft-365-Umfeld: Sicherheit beginnt beim Konto (Ing. Wolfgang Stauder, Lanexpert GmbH)
- ✓Passwörter sind tot – und KI braucht Regeln: Was AI Act & NIS2 jetzt von Unternehmen verlangen (Lukas Stattmann MSc & Nikolas Kachelmaier, MA, Coding School Wörthersee)

09:55 – 10:15 **Aktivitäten UBIT, Wirtschaftskammer Kärnten, DIH SÜD & Förderungen KWF**

10:15 – 11:30 **Matching mit den Expert*innen**

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

11:40 **Veranstaltungsende & Ausklang**

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

DIHSÜD Digital Innovation Hub

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

CAMPUS 02 GRAZ FACHHOCHSCHULE DER WIRTSCHAFT

CODING. SCHOOL WÖRTHERSEE

KWF

100. KI-Business Frühstück

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

Mag.a Angelika Höber
FH CAMPUS 02

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

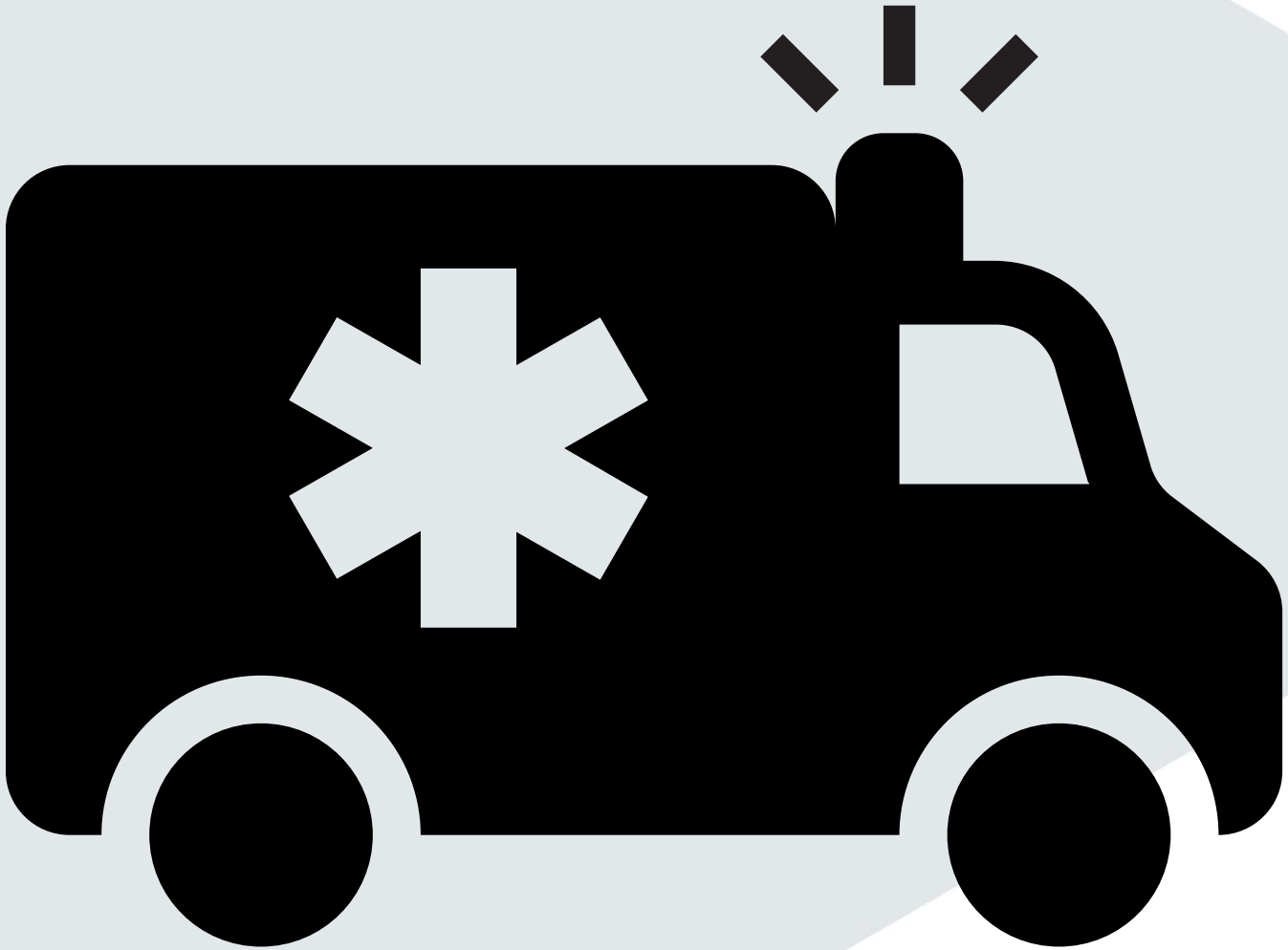
DIHSÜD Digital Innovation Hub

175 JAHRE 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



CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Geschäftsprozesse

Was muss täglich laufen?

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

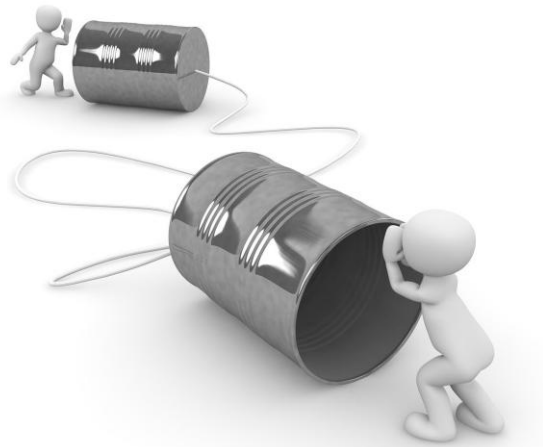
Dokumentation

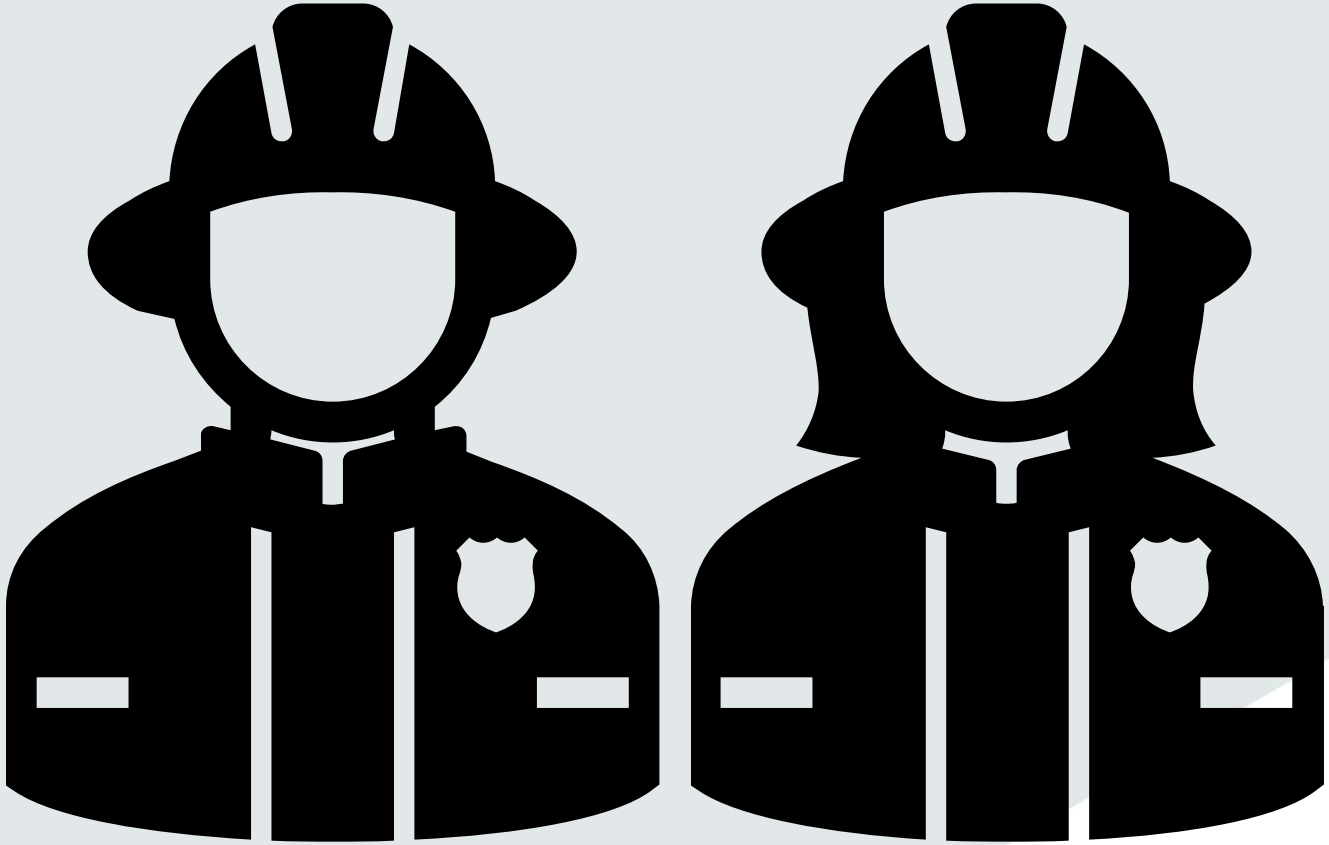
Auf welche Dokumente muss immer zugegriffen werden können?

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Kommunikation

Wie wird kommuniziert?
Was wird kommuniziert?
Mit wem?

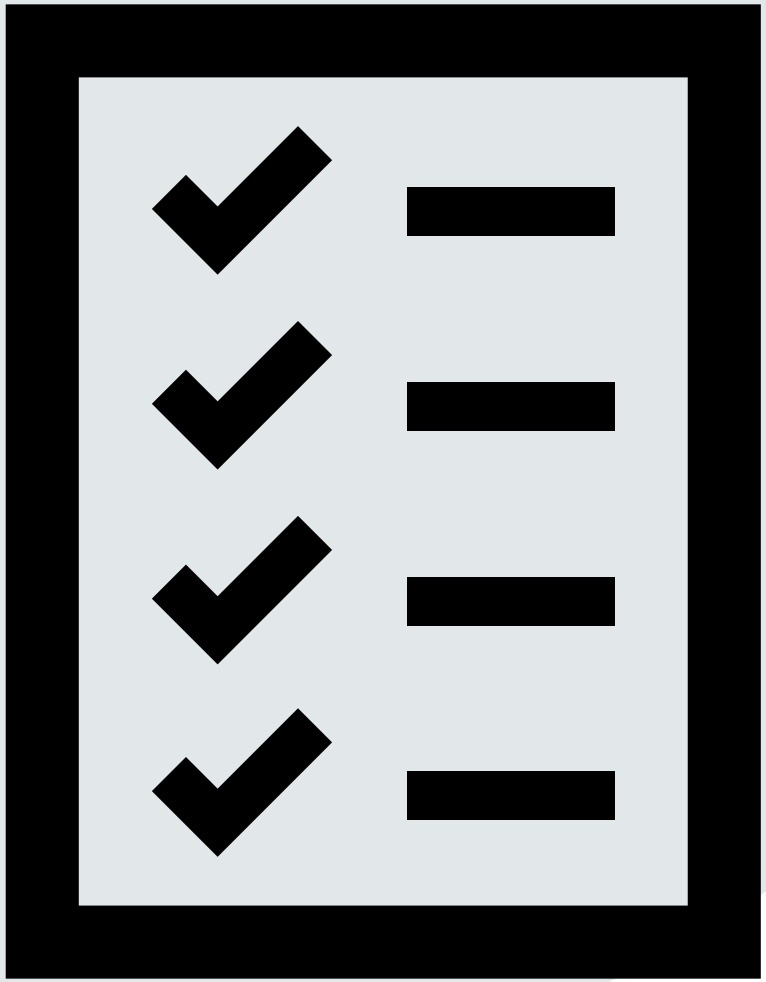




CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Notfallteam

Wer wird kontaktiert?
Wer koordiniert?
Wer entscheidet?

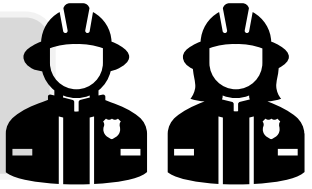


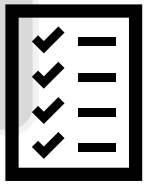
CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

Vorgehensplan

CYBERANGRIFF NOTFALLPLAN für Ihr Unternehmen

- Geschäftsprozesse
- Dokumentation
- Kommunikation
- Notfallteam
- Vorgehensplan





Ziel: handlungsfähig bleiben

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

Vielen Dank für Ihre Aufmerksamkeit!

Weitere Weiterbildungen

https://www.campus02.at/wirtschaftsinformatik/weiterbildung/

KURZPROGRAMME

- Requirements Engineering →
- DevOps →
- IT-Projektmanagement →
- AI-Fundamentals →
- Advanced Digital Management & Leadership →

100. KI-Business Frühstück

Impulsvortrag:
Zero Trust im Microsoft-365-Umfeld: Sicherheit beginnt beim Konto

Holger Schmitz, Lanexpert GmbH

Eine Initiative von:

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

175 JAHRE WKO
WIRTSCHAFTSKAMMER KÄRNTEN

Microsoft 365 - Fest im Griff

Holger Schmitz

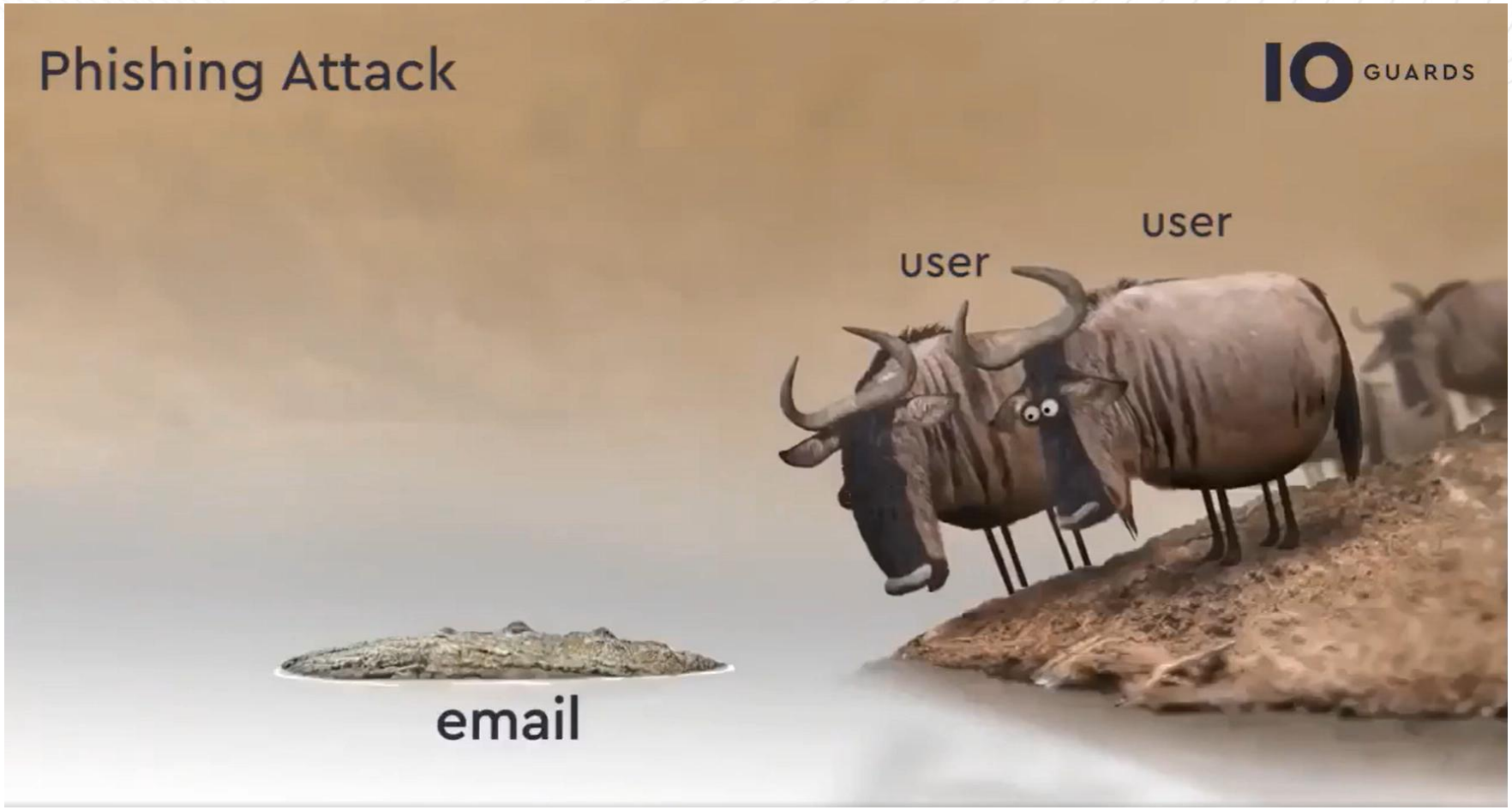
WKO WIRTSCHAFTSKAMMER KÄRNTEN

Microsoft 365 ist nicht „einfach“ sicher

UBIT ExpertsGroups

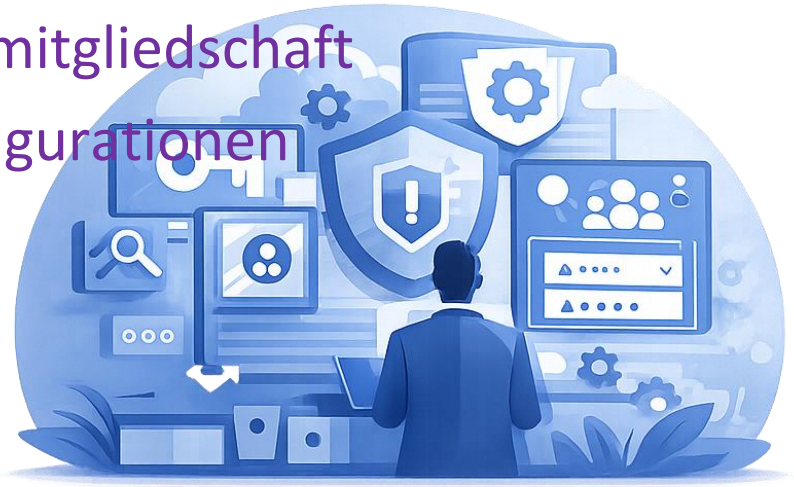
- Die meisten erfolgreichen Angriffe auf Microsoft 365 nutzen keine Exploits, sondern Fehlkonfigurationen.
- **Typische Schwachstellen:** fehlendes MFA, Legacy Auth, lange Token-Laufzeiten.
- **Ziel:** Risiken erkennen und Konfigurationen gezielt härten.

Angriff auf Microsoft 365



Unsichere Defaults – was sollte man ändern

- Standardkonfigurationen des Benutzers
- Gaststandards
- Einwilligung & Berechtigungen für Benutzeranwendungen
- Sichere Entra ID-Rollen
- Schutz der privilegierten Rollenmitgliedschaft
- Rollenzuweisbare Gruppenkonfigurationen
- Bedingte Zugriffsrichtlinien (Conditional Access)



Standardkonfigurationen für User

- Benutzer können Anwendungen registrieren und standardmäßig neue Tenants erstellen.

- Benutzer können Entra-Geräten beitreten – oft ohne MFA-Anforderung.

Gast-Standards

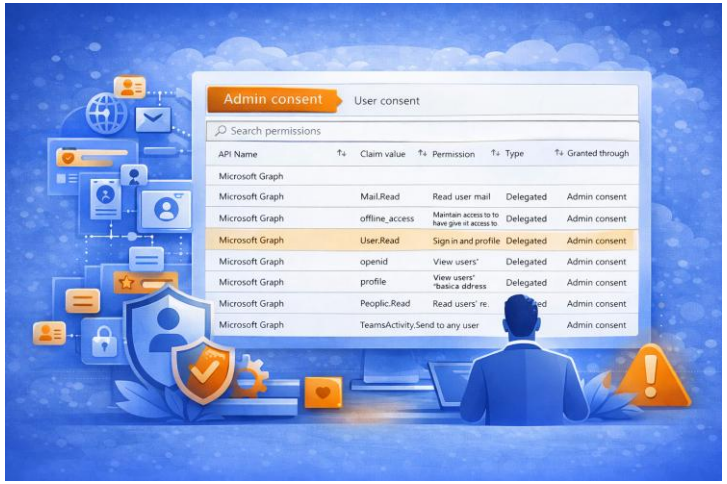
- Gäste haben standardmäßig ähnliche Ansichtsrechte wie interne Benutzer.

- Empfehlung: Gastzugriff auf das Notwendigste beschränken (Least Privilege).

Zustimmung & Berechtigungen für User-Apps

- In vielen Umgebungen dürfen Benutzer weiterhin App-Berechtigungen selbst freigeben.

- Risiko: OAuth-Consent-Phishing und Datenabfluss über Drittanbieter-Apps



Sichere Entra ID-Rollen

- Viele Rollen (Stand Okt. 2025: 117) erschweren den Überblick.

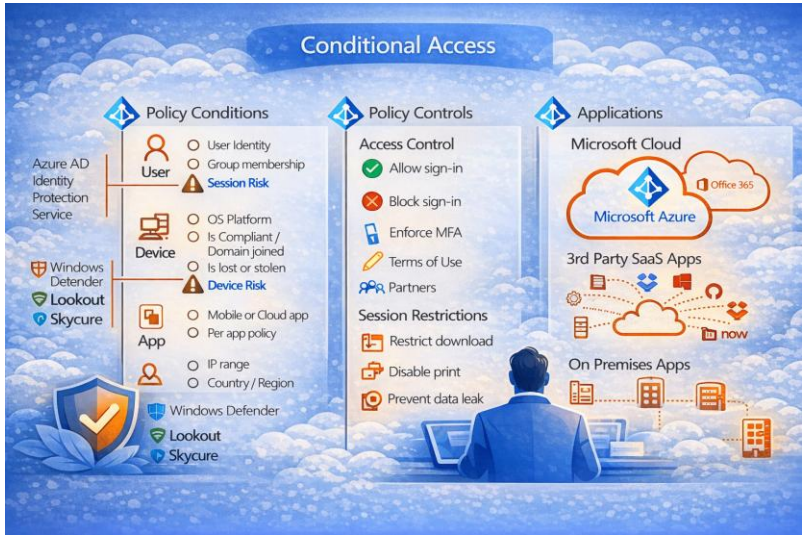
- Besonders kritisch: Tier-0 Rollen wie Global Administrator

Sichere privilegierte Rollenmitgliedschaft

- Keine Standardbenutzerkonten in hochprivilegierten Rollen.
- Rollenmitgliedschaft bevorzugt „eligible“ statt dauerhaft (PIM).
- MFA für privilegierte Aktionen verpflichtend.

Conditional Access

- Für Conditional Access ist mindestens Entra ID P1 erforderlich.
- Glass-Break-Admin nur für Notfälle – danach deaktivieren.
- Fehlkonfiguration kann Admins aussperren → Break-Glass und Tests sind Pflicht.



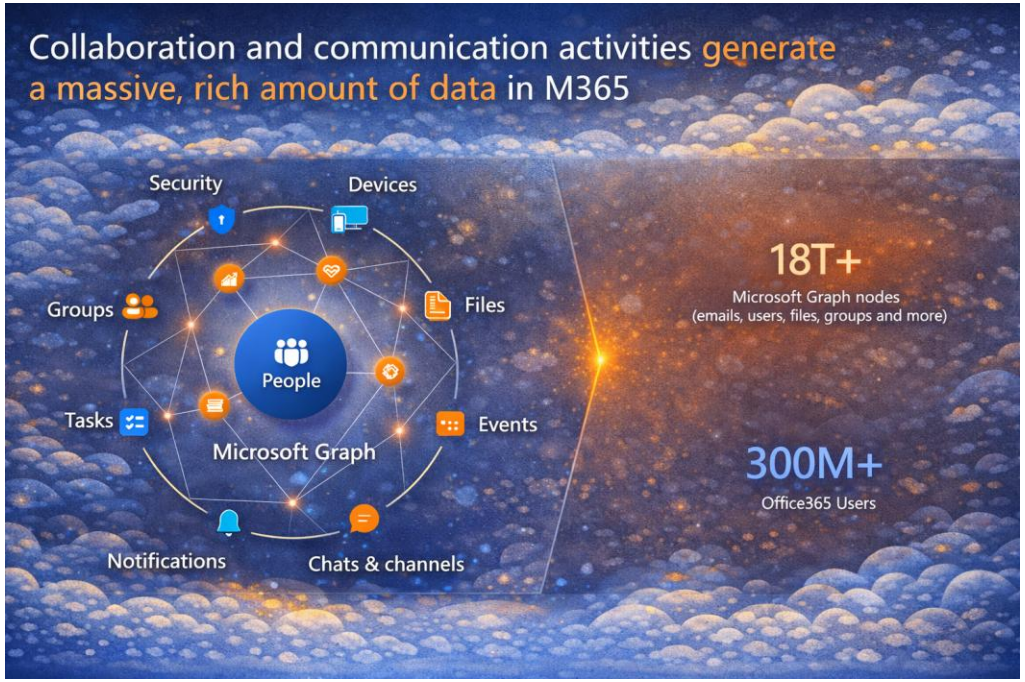
Gefahren: „Diesem Gerät immer vertrauen“

- Gerätevertrauen ohne Compliance-Prüfung ist riskant.
- Geolocation-Blocking kann via Proxy/VPN umgangen werden.

Microsoft 365 - GraphSpy

- Tool kann Userdaten via Microsoft Graph API auslesen.

- Zeigt: Tokens + OAuth-Rechte sind ein attraktives Angriffsziel.



Absicherung (Praxis)

- PCs/Laptops: Hybrid joined oder bekannte Standorte (Public IP).
- Sonst: Anmeldehäufigkeit begrenzen + MFA erzwingen.
- Mobilgeräte: nur konform (Intune registriert) zulassen.

Logging

- Business Basic/Standard:
  30 Tage Logs, nur Basis-Filter.

- Business Premium oder Entra ID P1:
  90 Tage Logs + erweiterte Filter.

Results 13 results found

Filter results

Date	IP address	User	Activity	Item
2017-03-15 23:20:08	40.141.128.246	edmondh@	UserLoggedIn	Unknown
2017-03-15 23:20:07	40.141.128.246	edmondh@	UserLoggedIn	Unknown
2017-03-15 23:20:04	40.141.128.246	edmondh@	UserLoggedIn	00000002-0000-0000-...
2017-03-15 23:16:54	40.141.128.246	edmondh@	Accessed file	
2017-03-15 23:16:51	40.141.128.246	edmondh@	Viewed page	
2017-02-09 11:10:30	64.203.175.98	edmondh@	UserLoggedIn	Unknown
2017-02-09 11:10:12	64.203.175.98	edmondh@	UserLoggedIn	Unknown
2017-02-09 11:10:05	64.203.175.98	edmondh@	UserLoggedIn	Unknown
2017-02-08 15:29:22		edmondh@	Viewed page	
2017-02-08 15:29:15		edmondh@	Viewed page	
2017-02-08 15:28:44		edmondh@	Accessed file	
2017-02-08 15:28:42		edmondh@	Updated user	

Lizenzierung

- Microsoft 365 Standard:
  Entra ID P1 für Conditional Access.

- Mobile Geräte: Business Premium oder separate Intune-Lizenz.

	AAD Free/AAD Office 365	AAD Premium P1	AAD Premium P2
Basic user and group management (inc MFA)	X	X	X
Conditional Access		X	X
Advanced group management		X	X
Password protection		X	X
Self-service password reset (Cloud User)	X	X	X
Self-service password reset (On-Premise User)		X	X
Microsoft Defender for Cloud Apps		X	X
AAD Application Proxy		X	X
Microsoft Identity Manager		X	X
Azure AD Connect	X	X	X
Azure AD Connect Health Monitoring		X	X
Terms of use attestation		X	X
SLA		X	X
Access reviews			X
Privileged Identity Management (PIM)			X
Identity Protection			X

Quellen zur Vertiefung

- adsecurity.org/?p=4825
- youtube.com/watch?v=WUHzpDdauAw
- https://www.microsoft.com/security/blog
- https://www.youtube.com/c/Practical365/search

Abschluss

- Microsoft 365 ist sicher –
  wenn es richtig konfiguriert ist.

- Fokus: MFA, Conditional Access,
  Least Privilege, Logging.

- Regelmäßig prüfen: Rollen, App-Consent, Gastzugriff.

Abschluss

Vielen Dank für Ihre Aufmerksamkeit

Sicherheit ist kein Produkt – sondern ein Prozess.

Kontaktdaten:
Holger Schmitz
holger.schmitz@lanexpert.at

100. KI-Business Frühstück

Passwörter sind tot – und KI braucht Regeln: Was AI Act & NIS2 jetzt von Unternehmen verlangen

KI ÖSTERREICH
ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Lukas Stattmann, MSc
Coding School Wörthersee

Nikolas Kachelmaier, MA
Coding School Wörthersee

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

DIHSÜD Digital Innovation Hub

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

PASSWÖRTER SIND TOT & KI BRAUCHT REGELN

Was AI Act und NIS II jetzt von Unternehmen verlangen

powered by HoliSec GmbH & JML Coding School GmbH

WER SIND WIR

Niki & Lukas

Holisec | Coding School & Academy Wörthersee

- Zertifikatslehrgänge inkl. ECTS
- Aus- & Weiterbildung für Privatpersonen
- Aus- & Weiterbildung für Unternehmen

NIS 2

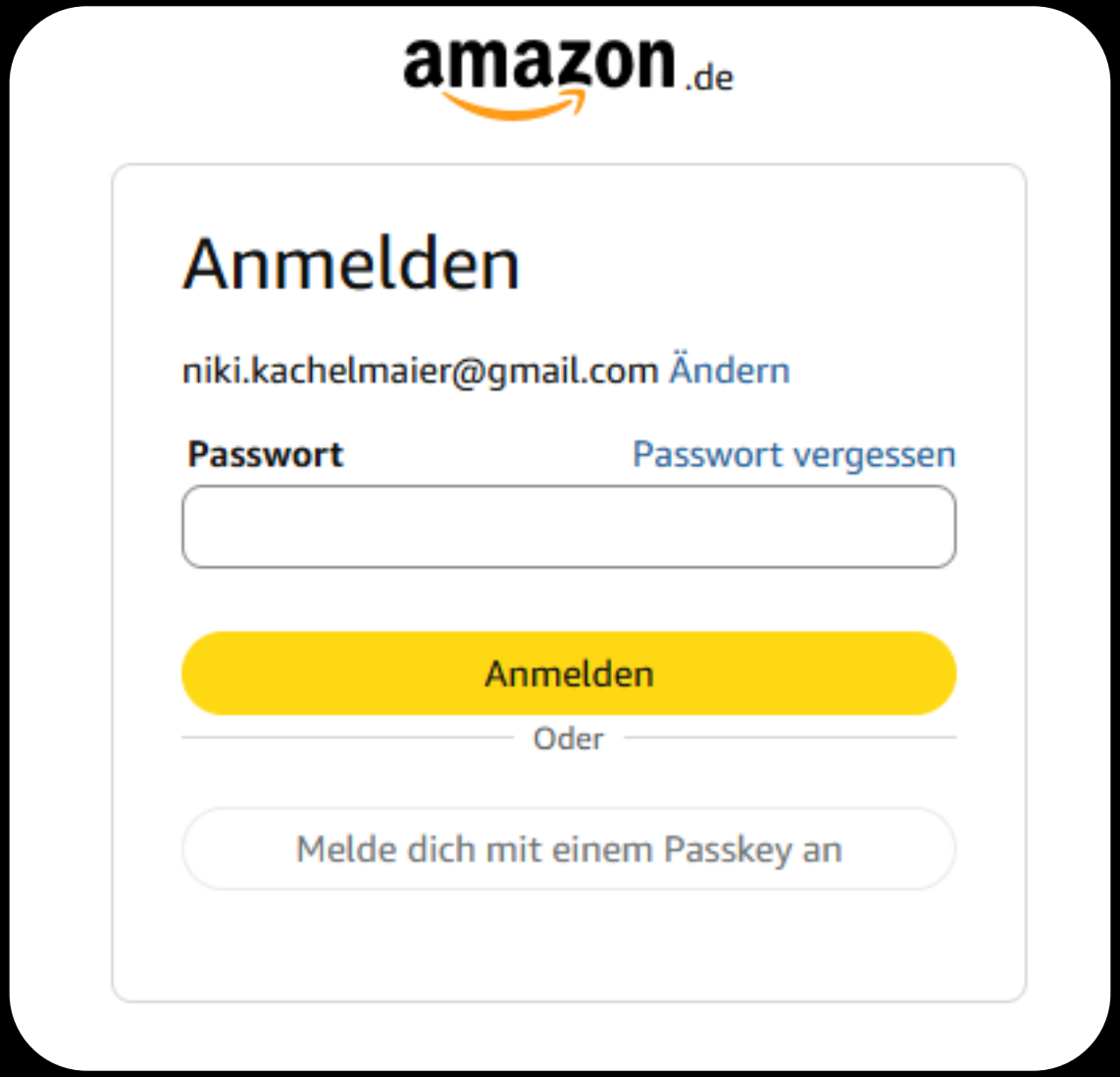
Network and Information Security Directive 2

powered by HoliSec GmbH & JML Coding School GmbH

NIS2 - Identity und Access Management

- IAM = Verwaltung, wer Zugriff auf welche Ressourcen hat
- **NIS2** verlangt:
  - Starke **Authentifizierung**
  - Minimierung von Passwort-Risiken
  - Zentralisierte Kontrolle von **Accounts**


Passwortverwaltung
& Generierung
Teilen von Logins
Vaultwarden
Selbst-gehostet
& DSGVO-konform
Browser-Integration
& Autofill

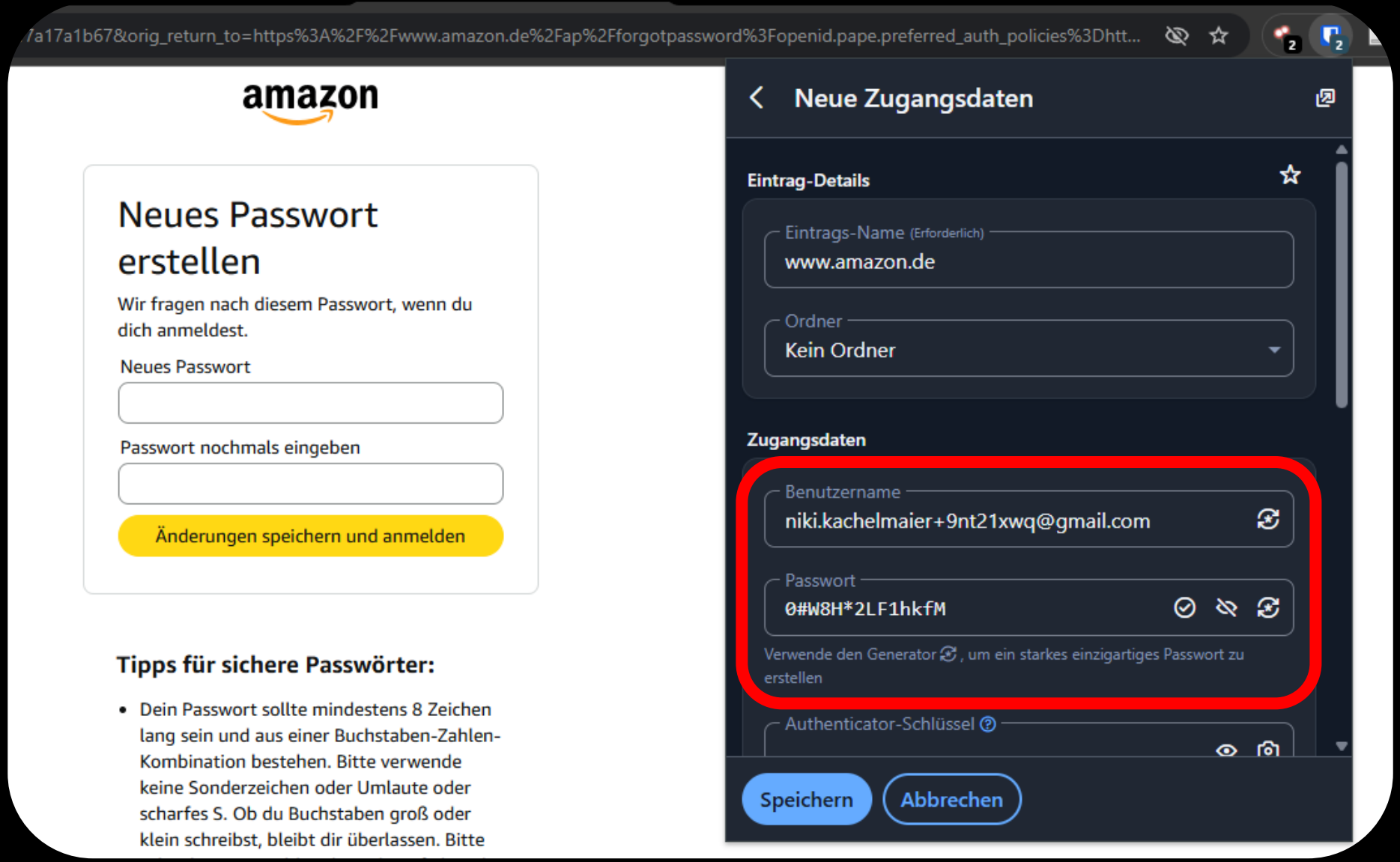

amazon.de
Anmelden
niki.kachelmaier@gmail.com Ändern
Passwort
Passwort vergessen
Anmelden
Oder
Melde dich mit einem Passkey an


amaz
Anmelden
niki.kachelmaier@gmail
Passwort
Anme
Ode
Melde dich mit ei

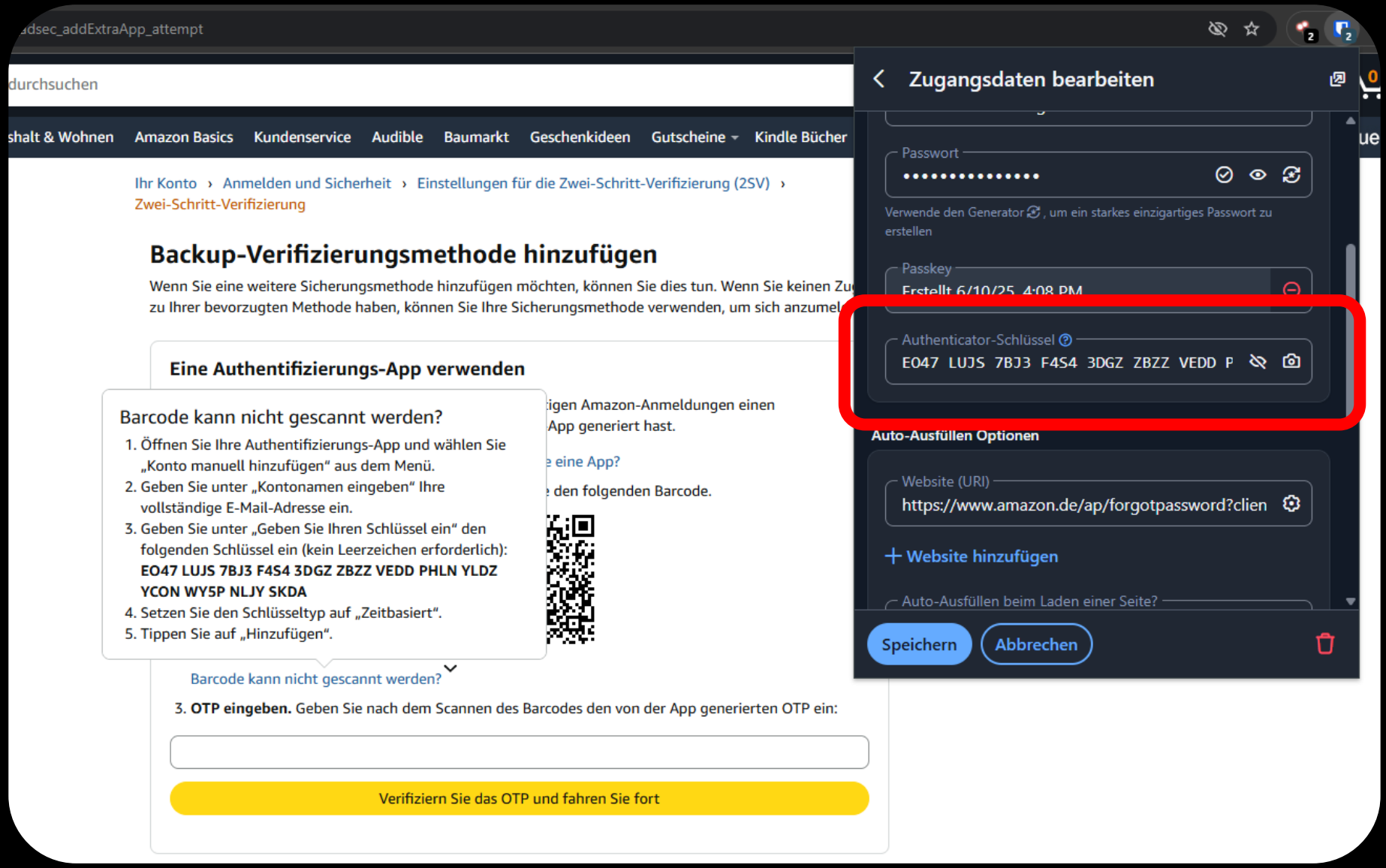

amazon.de
Anmelden
niki.kachelmaier@gmail.com Ändern
Passwort
Passwort vergessen
Anmelden
Oder
Melde dich mit einem Passkey an


amazon
Neues Passwort erstellen
Wir fragen nach diesem Passwort, wenn du dich anmeldest.
Neues Passwort
Passwort nochmals eingeben
Änderungen speichern und anmelden

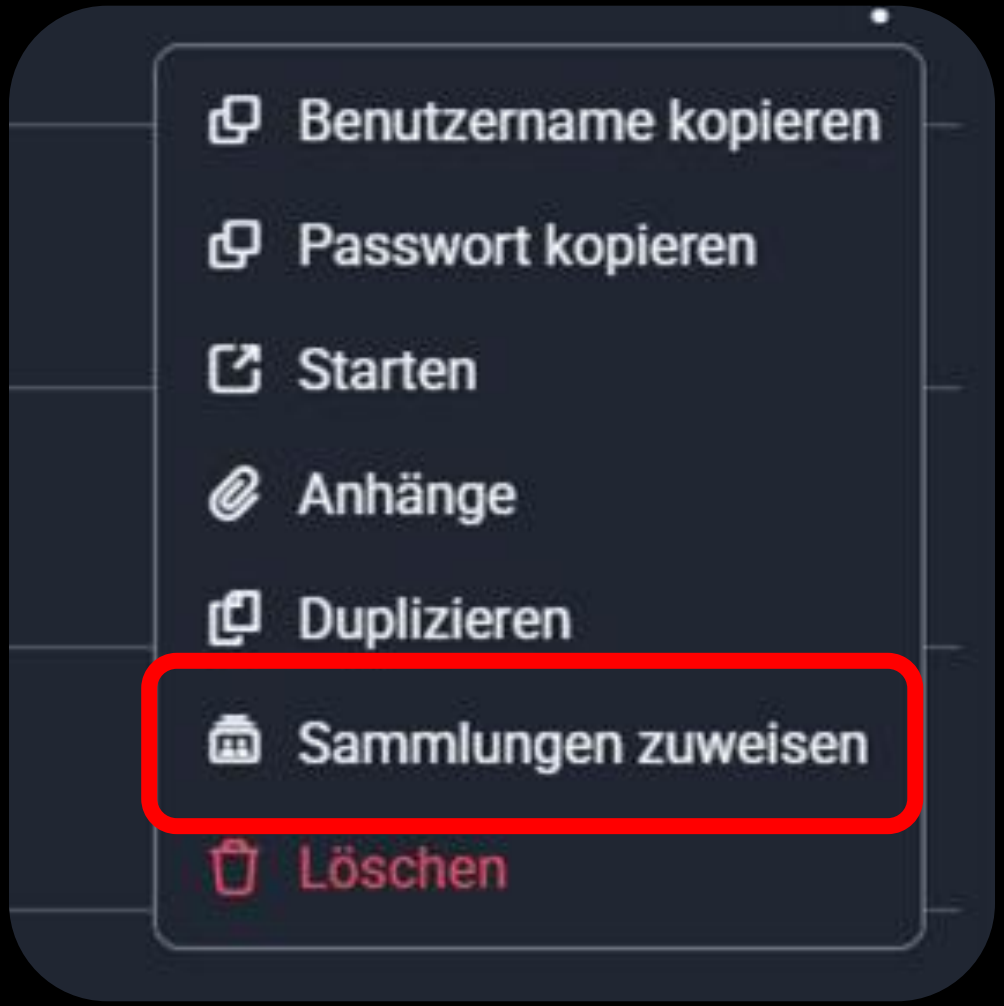
Neuer Zugang



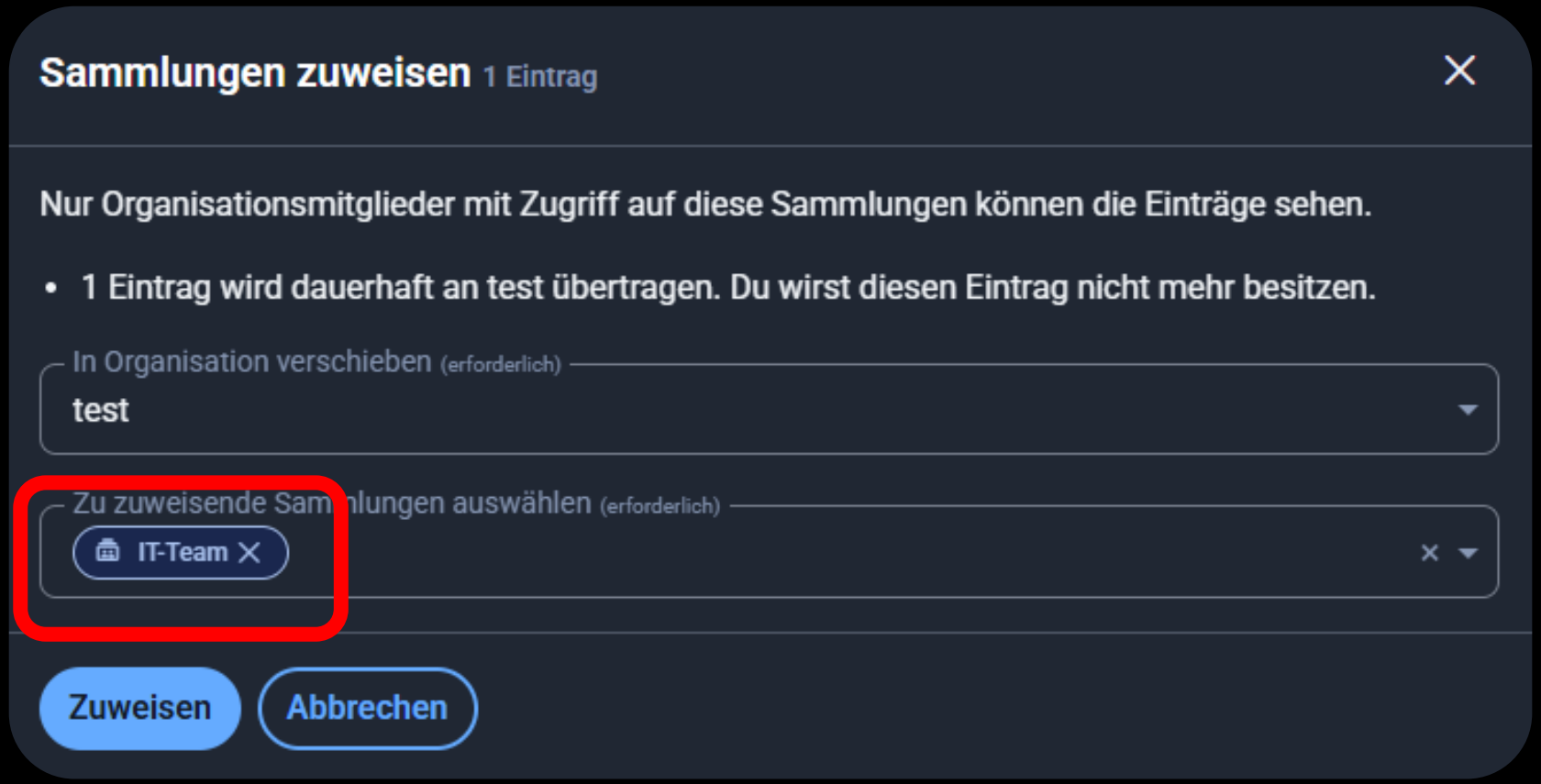
2. Faktor


durchsuchen
shalt & Wohnen
Amazon Basics
Kundenservice
Audible
Baumarkt
Geschenkideen
Gutscheine
Kindle Bücher
Ihr Konto › Anmelden und Sicherheit › Einstellungen für die Zwei-Schritt-Verifizierung (2SV) › Zwei-Schritt-Verifizierung
Backup-Verifizierungsmethode hinzufügen
Wenn Sie eine weitere Sicherungsmethode hinzufügen möchten, können Sie dies tun. Wenn Sie keinen Zu
zu Ihrer bevorzugten Methode haben, können Sie Ihre Sicherungsmethode verwenden, um sich anzumel
Eine Authentifizierungs-App verwenden
igen Amazon-Anmeldungen einen
App generiert hast.
e eine App?
den folgenden Barcode.
Barcode kann nicht gescannt werden?
1. Öffnen Sie Ihre Authentifizierungs-App und wählen Sie „Konto manuell hinzufügen“ aus dem Menü.
2. Geben Sie unter „Kontonamen eingeben“ Ihre vollständige E-Mail-Adresse ein.
3. Geben Sie unter „Geben Sie Ihren Schlüssel ein“ den folgenden Schlüssel ein (kein Leerzeichen erforderlich): EO47 LUJS 7BJ3 F4S4 3DGZ ZBZZ VEDD PHLN YLDZ YCON WY5P NLJY SKDA
4. Setzen Sie den Schlüsseltyp auf „Zeitbasiert“.
5. Tippen Sie auf „Hinzufügen“.
Barcode kann nicht gescannt werden?
3. OTP eingeben. Geben Sie nach dem Scannen des Barcodes den von der App generierten OTP ein:
Verifiziern Sie das OTP und fahren Sie fort
Zugangsdaten bearbeiten
Passwort
Verwende den Generator, um ein starkes einzigartiges Passwort zu erstellen
Passkey
Erstellt 6/10/25, 4:08 PM
Authenticator-Schlüssel
EO47 LUJS 7BJ3 F4S4 3DGZ ZBZZ VEDD P
Auto-Ausfüllen Optionen
Website (URI)
https://www.amazon.de/ap/forgotpassword?clien
+ Website hinzufügen
Auto-Ausfüllen beim Laden einer Seite?
Speichern
Abbrechen

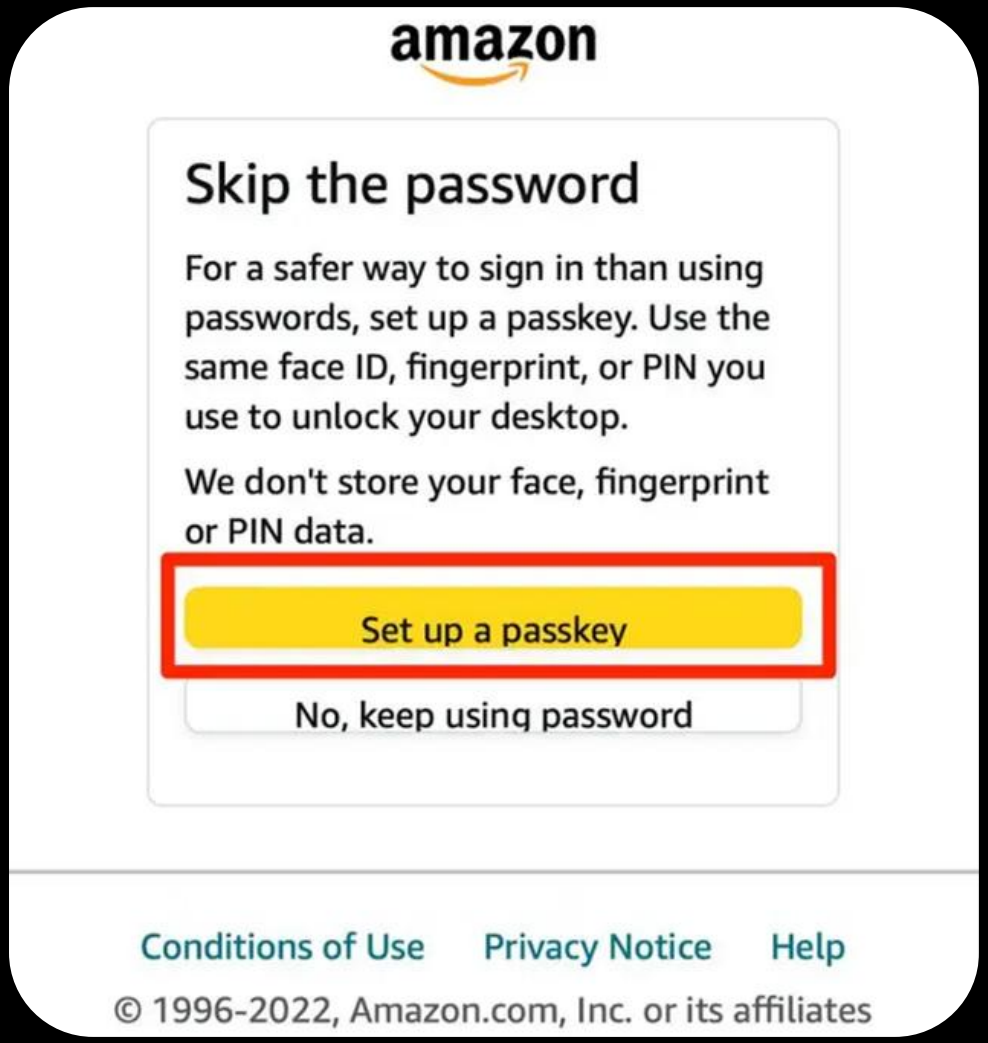
Zugänge teilen



Zugänge teilen



Passwörter sind tod ?


amazon
Skip the password
For a safer way to sign in than using passwords, set up a passkey. Use the same face ID, fingerprint, or PIN you use to unlock your desktop.
We don't store your face, fingerprint or PIN data.
Set up a passkey
No, keep using password
Conditions of Use
Privacy Notice
Help
© 1996-2022, Amazon.com, Inc. or its affiliates

Passkey

Teilst du dieses Konto mit jemandem, der sich mit einem Schlüsselbund anmelden möchte? Diese Person muss sich ihren eigenen einrichten.

1 Passkey bei amazon.de

Windows Hello
Einrichten: 22.09.2025

Passkey hinzufügen

Wenn du einen Passkey hinzufügen möchtest, verwende ein anderes Cloud-Service-Konto (Beispiel: Apple iCloud Keychain oder Google Password Manager).

Weitere Informationen zu Passkeys

- Verwende den Passkey auf verschiedenen Geräten, einschließlich Computer
- Passkeys mit Freunden und Familie teilen
- Verwende Passkeys mit 2-Schritte-Verifizierung
- Überlegungen zum Datenschutz

Bitwarden

Passkey speichern | + Neu

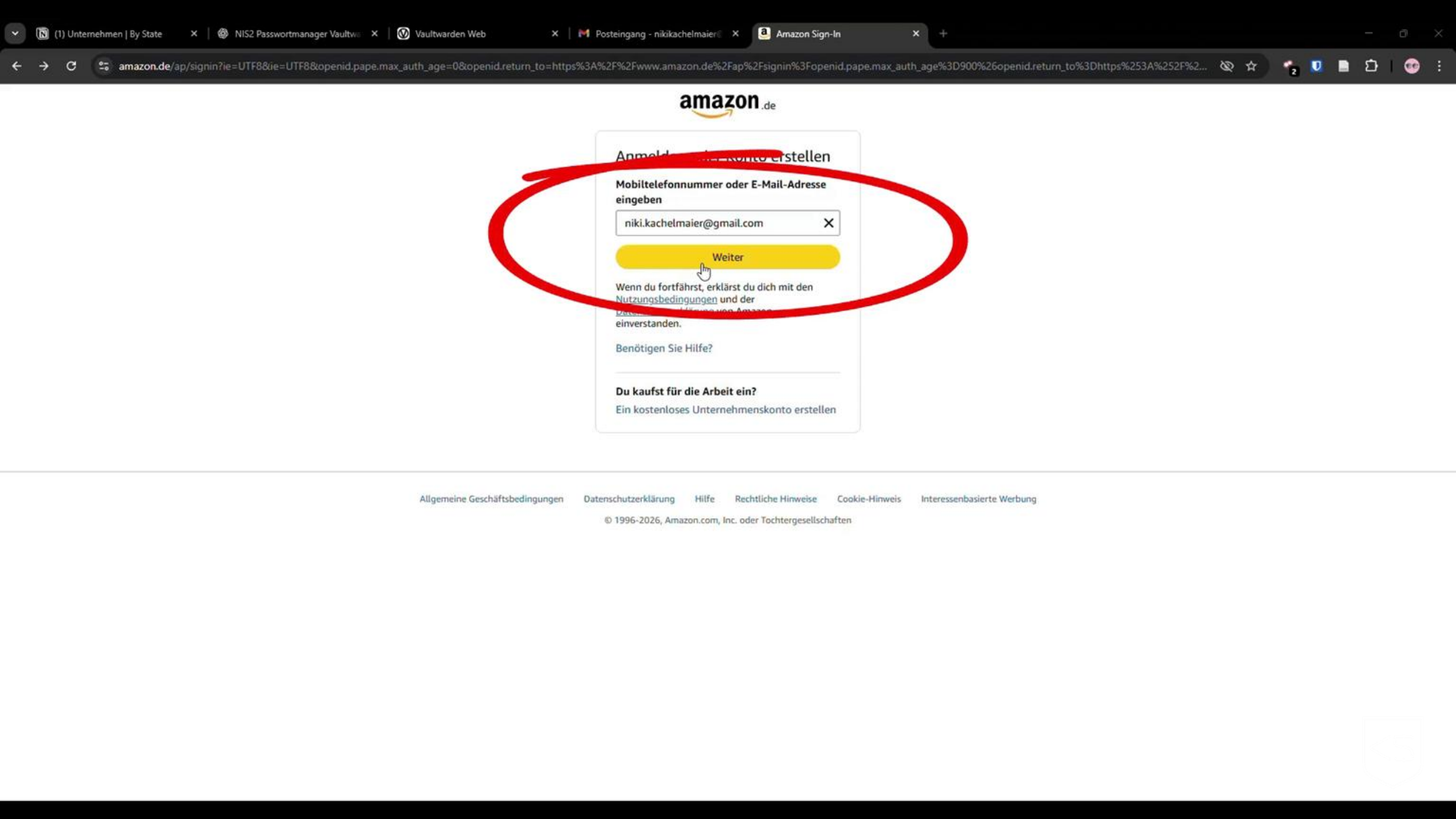
Tresor durchsuchen

Wähle die Zugangsdaten aus, in die dieser Passkey gespeichert werden soll

office - www.amazon.de
office@holisec.com

www.amazon.de
amazon.de
niki.kachelmaier@gmail.com

Gerät oder Hardware-Schlüssel verwenden


(1) Unternehmen | By State
NIS2 Passwortmanager Vaultw
Vaultwarden Web
Posteingang - nikikachelmaier
Amazon Sign-In
amazon.de/ap/signin?ie=UTF8&ie=UTF8&openid.pape.max_auth_age=0&openid.return_to=https%3A%2F%2Fwww.amazon.de%2Fap%2Fsignin%3Fopenid.pape.max_auth_age%3D900%26openid.return_to%3Dhttps%253A%252F%2...
amazon.de
Anmeld konto erstellen
Mobiltelefonnummer oder E-Mail-Adresse eingeben
niki.kachelmaier@gmail.com
Weiter
Wenn du fortfährst, erklärst du dich mit den Nutzungsbedingungen und der
einverstanden.
Benötigen Sie Hilfe?
Du kaufst für die Arbeit ein?
Ein kostenloses Unternehmenskonto erstellen
Allgemeine Geschäftsbedingungen
Datenschutzerklärung
Hilfe
Rechtliche Hinweise
Cookie-Hinweis
Interessenbasierte Werbung
© 1996-2026, Amazon.com, Inc. oder Tochtergesellschaften

Warum sind Passkeys sicherer als Passwörter?

NIS2 - Identity und Access Management

	Passwörter	Passkeys
Phishing	❌ anfällig	✅ geschützt
Diebstahl/Leaks	❌ möglich	✅ kein Geheimnis speicherbar
Wiederverwendung	❌ häufig	✅ einzigartig
Brute Force	❌ möglich	✅ unmöglich
Bedienung	😬 merken/eintippen	✅ Face/Fingerprint
Sicherheit gesamt	⭐ ⭐	⭐ ⭐ ⭐ ⭐ ⭐

Warum existieren Passwörter noch?

Kontowiederherstellung

Demo anfordern.

AI ACT ÜBERBLICK

powered by HoliSec GmbH & JML Coding School GmbH

AI ACT

- EU Verordnung
- Inkrafttreten: 1. August 2024
- Verpflichtungen für Anbieter/Betreiber von KI-Systemen
- Kennzeichnungspflicht für KI-generierte Inhalte
- Fristen
  - Umsetzung: Bis 2025
  - Nationale Durchsetzungsmaßnahmen ab 2026
- https://www.digitalaustria.gv.at/Themen/KI/AI-Act.html

RISIKOKLASSEN IM EU AI ACT

1. Inakzeptables (verbotenes) Risiko

- KI-Systeme, die fundamentale Rechte, Sicherheit oder demokratische Prinzipien verletzen (z. B. Echtzeit-Biometrie im öffentlichen Raum, Social Scoring, Emotionserkennung am Arbeitsplatz)
- Status: Komplett verboten ab Februar 2025

2. Hohes Risiko

- KI-Anwendungen mit potenziell gravierenden Auswirkungen: kritische Infrastruktur, HR (z. B. Bewerber-Screening), Strafverfolgung, Migration, Gesundheit, Biometrie außerhalb Echtzeit
- Erfordern umfangreiche Auflagen (Risikomanagement, Dokumentation, Datenqualität, Transparenz…)

RISIKOKLASSEN IM EU AI ACT

3. Begrenztes Risiko

- Systeme, die direkt mit Menschen interagieren (z. B. Chatbots, Deepfakes, Gesichtgenerierung)
- Pflicht: Kennzeichnung & Transparenz gegenüber Nutzenden

4. Minimales oder geringes Risiko

- Alltäglich eingesetzte KI wie Spamfilter, Predictive Maintenance
- Keine speziellen Auflagen, aber Schulungs- und Awareness-Pflicht wird erwartet

PFLICHTEN FÜR UNTERNEHMEN

ANBIETER (PROVIDER / HERSTELLER)

Unternehmen, die KI-Systeme entwickeln oder in Verkehr bringen.

- Risikomanagement-System einführen
- Technische Dokumentation & Konformitätsbewertung erstellen
- Datenqualität sicherstellen (repräsentativ, fehlerfrei, bias-frei)
- Transparenzpflichten: System muss erklärbar sein
- Human Oversight ermöglichen (menschliche Kontrolle)
- Protokollierung & Monitoring (laufende Überwachung)
- Sicherheits-, Genauigkeits- & Robustheitsanforderungen erfüllen
- Registrierung im EU-Datenbankregister (für Hochrisiko-Systeme)

NUTZER (DEPLOYERS / ANWENDER)

Unternehmen, die KI-Systeme verwenden, aber nicht selbst entwickeln.

- System sachgerecht nutzen
- Mitarbeitende schulen, die mit KI-Systemen arbeiten
- Monitoring & Logging sicherstellen
- Vorab prüfen, ob eingesetzte KI in Hochrisiko-Kategorie fällt
- Transparenz gegenüber Betroffenen (z. B. Kennzeichnung, wenn ein Chatbot antwortet)
- Meldung von Vorfällen oder Fehlfunktionen an Behörden / Hersteller

NUTZER (DEPLOYERS / ANWENDER)

Unternehmen, die KI-Systeme verwenden, aber nicht selbst entwickeln.

- **System sachgerecht nutzen**
- **Mitarbeitende schulen, die mit KI-Systemen arbeiten**
- Monitoring & Logging sicherstellen
- **Vorab prüfen, ob eingesetzte KI in Hochrisiko-Kategorie fällt**
- **Transparenz gegenüber Betroffenen (z. B. Kennzeichnung, wenn ein Chatbot antwortet)**
- Meldung von Vorfällen oder Fehlfunktionen an Behörden / Hersteller

KENNZEICHNUNGSPFLICHT

- Anbieter müssen sicherstellen, dass synthetische Inhalte (Text, Bild, Audio, Video) maschinell gekennzeichnet sind und als künstlich erzeugt/ manipuliert erkennbar sind
- Die Kennzeichnung muss maschinell auslesbar sein – etwa durch digitale Wasserzeichen oder Metadaten

Quelle: https://artificialintelligenceact.eu/article/50

KENNZEICHNUNGSPFLICHT

Gekennzeichnet werden muss, wenn …

- … der Text von einer KI erzeugt wurde
- … du den Text öffentlich nutzt oder verbreitest (z. B. Website, Marketing, Kundenkommunikation)
- … die Leser:innen nicht sofort erkennen können, dass er maschinell erstellt wurde

Gekennzeichnet werden muss NICHT, wenn …

- … der Text nur intern verwendet wird (z. B. zur Ideenfindung, Entwurf)
- … menschliche Überarbeitung den Text wesentlich verändert

KENNZEICHNUNGSPFLICHT BEISPIELE

Text

- “Dieser Text wurde mit Hilfe künstlicher Intelligenz erstellt.”
- “Automatisch generierter Entwurf (KI)”

Bilder & Videos

- Sichtbarer Text im Bild oder darunter (z. B. „AI-generated image“)
- Zusätzlich: Metadaten oder Wasserzeichen
- Manche AI Tools kennzeichnen bereits in Metadaten

WAS HEISST DAS FÜR ALLE MITARBEITENDEN?

Bereich	Bedeutung / Mögliche Auswirkungen
HR	KI-gestützte Tools prüfen und dokumentieren; Bewerbertools gelten als Hochrisiko
Marketing	Transparenz bei KI-generierten Inhalten sicherstellen (z. B. Texte, Bilder, Videos)
IT	KI-Systeme inventarisieren; technische Prüfungen und Sicherheitsmaßnahmen mit einplanen
Produktion	Grundverständnis über KI & Risiken entwickeln; Awareness im Umgang mit KI stärken

DATENSCHUTZ & DSGVO

DSGVO

- DSGVO - Datenschutzgrundverordnung
- Zuständig in Österreich: Datenschutzbehörde DSB

Im AI Act selbst ist gemäß Art. 74 Abs. 8 KI-VO (nach aktueller Rechtslage) zudem eine alleinige Zuständigkeit der Datenschutzbehörde als Marktüberwachungsbehörde für KI-Systeme mit hohem Risiko u.a. im Bereich der Strafverfolgung, der Grenzverwaltung, der Justiz und der Demokratie vorgesehen.

WAS SIND PERSONENBEZOGENE DATEN IM KI-KONTEXT?

Definition laut DSGVO: Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Abteilung	Personenbezogene Daten	KI Relevanz
Geschäftsführung	Namen, E-Mails, Berichte mit Personenbezug	Copilot verarbeitet Besprechungsnotizen mit personenbezogenen Infos
HR	Lebensläufe, Krankmeldungen, Bewerberdaten	Hochrisiko: automatische Auswahlprozesse, Bewerberanalyse
Marketing	Kundenverhalten, E-Mail-Adressen, Tracking-IDs	KI-Personalisierung basiert auf personenbezogenen Daten
Vertrieb / CRM	Kundennamen, Gesprächsverläufe, Auftragsdaten	KI nutzt diese Daten für Analysen und Forecasts
IT / Support	IP-Adressen, Login-Informationen, Nutzungsdaten	KI überwacht Systeme, erkennt Anomalien
Produktion	Maschinenzeiten mit Personen-ID (z. B. Zeiterfassung)	KI könnte Arbeitsverhalten analysieren (indirekter Personenbezug)

KANN ICH LEBENSLÄUFE VON BEWERBERINNEN OHNE BEDENKEN IM COPILOT HOCHLADEN?

WIE WÜRDEN SIE ChatGPT LAUT AI ACT EINSTUFEN / WAS WÜRDEN SIE MACHEN?

EINSTUFUNG LAUT EU AI ACT

- ChatGPT ist ein **generatives KI-System** mit **begrenztem Risiko**
- Das Unternehmen ist in diesem Fall **Nutzer** (Deployer), nicht Anbieter
- Daraus entstehen **Transparenz- und Sorgfaltspflichten**
- Zusätzlich gelten **Datenschutzvorgaben** (DSGVO), da potenziell personenbezogene Daten verarbeitet werden

VORGEHEN FÜR UNTERNEHMEN

- KI-Nutzungsrichtlinie erstellen
- Risikobewertung durchführen
- Datenschutz & DSGVO beachten
- Verantwortlichkeiten festlegen
- Mitarbeiterschulung
- Transparenz & Kontrolle
- Dokumentation & Monitoring

🧠 WISSEN | 🛡️ DATENSCHUTZ | 🤝 VERTRAUEN

KI ist kein Risiko, wenn sie bewusst, sicher
und nachvollziehbar eingesetzt wird.

FRAGEN / DISKUSSION

Lukas Stattmann | JML Coding School GmbH

+ 43 676 843 223 246 | lukas.stattmann@csaw.at

PASSWÖRTER SIND TOT - UND KI BRAUCHT REGELN

Was AI Act und NIS II jetzt von Unternehmen verlangen

powered by HoliSec GmbH & JML Coding School GmbH

100. KI-Business Frühstück

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN
& KÜNSTLICHE INTELLIGENZ

Aktivitäten UBIT, Wirtschaftskammer Kärnten, DIH SÜD & Förderungen KWF

Eine Initiative von:

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

175 JAHRE WKO
WIRTSCHAFTSKAMMER KÄRNTEN

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

KI Day

5. Mai 2026
09:00 – 17:00 Uhr
Lakesidepark Klagenfurt

Keynote: Roger Basler de Roca

JETZT anmelden!

www.ki-day.at

LAND KÄRNTEN
Abt. 7 – Wirtschaftsstandort

iv INDUSTRIELLENVEREINIGUNG KÄRNTEN

BABEG

ki-oesterreich.at

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

WKO WIRTSCHAFTSKAMMER KÄRNTEN

UBIT-Services für Wirtschaftskammer-Mitglieder

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

ubit-kaernten.at
UBIT Kärnten
UBIT Kärnten

• Geförderte Beratungen zu Cyber-Security/NIS

NISG 2026 – verpflichtend ab 1.10.2026
Sicherheits- & Meldepflichten für Unternehmen ab mittlerer Größe

Unser Angebot – 100 % gefördert

- Rechtliche Abklärung (bis 4 Std.)
  Ist Ihr Unternehmen NIS2-pflichtig?
- Technik-Check (bis 3 Std.)
  Erforderliche technische Maßnahmen

- Governance & Organisation (bis 3 Std.)
  Sicherheitsmaßnahmen & Risikomanagement


Die organisatorische Abwicklung erfolgt durch das Team des Servicezentrums.

Beratung durch qualifizierte UBIT-Unternehmensberater & IT-Dienstleister www.ubit-kaernten.at/nis2

UBIT-Services für Wirtschaftskammer-Mitglieder

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

ubit-kaernten.at
UBIT Kärnten
UBIT Kärnten

- **Cyber-Security-Hotline**

Notfallhilfe bei Cyberangriffen

24/7 erreichbar – kostenlos für WK-Mitglieder
☎ 0800 888 133

Wann anrufen?
- Cybercrime & Hackerangriffe
- Ransomware & Verschlüsselung

So wird geholfen:
- Soforthilfe & Erstmaßnahmen
- Koordination zu regionalen UBIT IT-Security-Expert:innen
- Kostenloses Erstgespräch


Die organisatorische Abwicklung erfolgt durch das Team des Servicezentrums.

UBIT-Services für Wirtschaftskammer-Mitglieder

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

ubit-kaernten.at
UBIT Kärnten
UBIT Kärnten

- **KI-Umsetzungsförderung (NEU!)**

Künstliche Intelligenz – der nächste Wachstumsschritt
Von der Idee zur konkreten Anwendung im Betrieb

KI-Umsetzungsförderung – 100 % gefördert:
- Gesamtumfang: 6 Stunden
- Durchführung durch qualifizierte UBIT-Unternehmensberater & IT-Dienstleister

Beratungsinhalte:
- Analyse & Orientierung
  Identifikation geeigneter KI-Anwendungsfälle
- Umsetzungsberatung (Schwerpunkt)
  Konkrete Schritte zur Realisierung einer KI-Lösung

💡 Die organisatorische Abwicklung erfolgt durch das Team des Servicezentrums.

Fokus: Praktische Umsetzung & nutzbares Ergebnis
→ Wählen Sie Ihren UBIT-Berater https://www.wko.at/ktn/digitalisierung/ki-umsetzungsfoerderung

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:

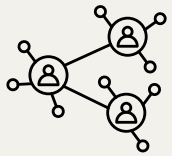
FFG Forschung wirkt.
Das Land Steiermark
LAND KÄRNTEN

DIHSÜD
Digital Innovation Hub

UNSERE LEISTUNGEN

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

Nicht wirtschaftlich tätiges Kompetenznetzwerk



Netzwerk aus Digitalzentren, Netzwerkpartnern und Multiplikatoren

Unterstützung von KMU in der Südregion

Angebote in den Bereichen Information, Qualifikation und Digitale Transformation

Zugang zu Infrastruktur

Zugang zu Laboren, Unterstützung bei Prototypenherstellung etc.

DIHSÜD
Digital Innovation Hub

UNSERE THEMEN

- Produktions- & Fertigungstechnologien 
- Digitale Sicherheit 
- Daten & Künstliche Intelligenz 
- Digitale Geschäftsmodelle & -prozesse 
- Nachhaltigkeit & Kreislaufwirtschaft 
- Arbeit der Zukunft & Humanressourcen 

DIHSÜD
Digital Innovation Hub

Struktur des DIH SÜD: Partnernetzwerk

Digitalzentren

FH JOANNEUM University of Applied Sciences
KÄRNTEN University of Applied Sciences
JOANNEUM RESEARCH
TU Graz
UNIVERSITÄT KLAGENFURT
BABEG Success in Carinthia.

Netzwerk-partner

AEE INTEC
ASMET
build! GRÜNDERZENTRUM KÄRNTEN
CAMPUS 02 FACHHOCHSCHULE DER WIRTSCHAFT
hochschule burgenland Forschung
KNOW Center
Lakeside Labs SELF-ORGANIZING NETWORKED SYSTEMS
Lakeside SCIENCE & TECHNOLOGY PARK
UNI GRAZ
fh st.pölten UNIVERSITY OF APPLIED SCIENCES
Fraunhofer AUSTRIA
innos
mcl
CODING. SCHOOL WÖRTHERSEE
WOOD K PLUS

DIHSÜD
Digital Innovation Hub

Kooperation mit Stakeholdern

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

CODING. SCHOOL WÖRTHERSEE

Penetration Test Training

- 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

CODING. SCHOOL WÖRTHERSEE
TU Graz

DIHSÜD
Digital Innovation Hub

Unser Programm

Objekte finden, verfolgen, verstehen: Computer Vision praktisch
(FH Joanneum, 24.02.2026)

KI-Use Cases planen
(Know-Center, FH Campus 02, 11.02.2026)

Netzwerk Basisschulung
(FH Joanneum, 11.02.2026)

Filamentbasierter 3D-Druck
(FH Kärnten, 13.02.2026)

Python kompakt: Einführung für Einsteiger:innen
(FH Joanneum, 24.02.2026)

Der Digitale Produktpass (DPP) – Chance zur Transformation
(Joanneum Research, 25.02.2026)

GitLab um Source Code selbst (sicher) zu hosten - Einsteigerworkshop
(FH Joanneum, 02.03.2026)

Hands-On Secure Coding – Security für Quereinsteiger:innen
(FH Joanneum, 03.03.2026)

Software-Quality als Basis für Secure Software
(FH Joanneum, 03.03.2026)

Was KMUs aus dem Fall Nokia lernen können. Disruption erkennen – Zukunft sichern.
(Uni Klagenfurt, 17.03.2026)

Business Nachmittag: Zukunft gestalten - Impulse für Tourismusbetriebe durch Digitalisierung und Robotik
(Universität Klagenfurt,

Being like Amazon and Uber - Neue Geschäftslogiken in der digitalen Welt
(Uni Klagenfurt, 21.05.2026)

DIHSÜD
Digital Innovation Hub

UNSERE AKTIVITÄTEN

Wir bieten gemeinsam mit unseren Partnern kostenfreie Veranstaltungen für KMU an. Tauchen Sie ein in unsere informativen Workshops und Weiterbildungen, die Ihnen wertvolle Einblicke in die digitale Welt verschaffen. Unsere erstklassige Partnerstruktur stellt sicher, dass Sie Zugang zu den neuesten Technologien und modernster Infrastruktur erhalten, um Ihre digitale Zukunft im Unternehmensbereich erfolgreich zu gestalten.

DIHSÜD
Digital Innovation Hub

KONTAKT

DIH SÜD GmbH
Leonhardstraße 59
8010 Graz

Mag. Stefan Schafranek
stefan.schafranek@dih-sued.at
+43 316 876-1154

Martina Eckerstorfer
martina.eckerstorfer@dih-sued.at
+43 463 9082 90-25


Passende Förderungen für Ihren Vorsprung
Für den Markt von morgen bereit sein - durch passende Angebote im Heute

Relevante KWF Förderungsangebote

»Eigene« F&E&I vorbereiten und umsetzen

Start.F&E&I

F&E&I Ideen identifizieren, Projekte vorbereiten, Partner finden, Machbarkeiten durchführen, Förderanträge schreiben

Max. 60% Förderquote | EUR 50.000

Personalkosten | Unternehmerlohn
externe Dienstleistungen
Sach- und Materialkosten

Umsetzung.F&E&I

F&E&I Projekte durchführen | bis zur Prototypenenwicklung | Machbarkeiten

Max. 50% Förderquote | EUR 100.000

Personalkosten | Unternehmerlohn
externe Dienstleistungen
Sach- und Materialkosten
Investitionen (anteilige Abschreibung)
25 % Gemeinkostenpauschale

»Externes« Know-How nutzen

Strategie.IMPULS

Vorarbeiten strategischer Projektvorhaben | Konzepterstellung auf organ. und strateg. Ebene | KEINE Implemtierung

Max. 50% Förderquote | EUR 15.000 | 10 Beratungstage

externe Dienstleistungen

Gerne beraten wir Sie persönlich

Cornelia Jann

Forschung, Entwicklung, Technologie

cornelia.jann@kwf.at

M +43.664.839 93 28


KWF
Kärntner
Wirtschaftsförderungs
Fonds

Business Frühstück

KI ÖSTERREICH

ANWENDUNGSZENTRUM FÜR DATEN & KÜNSTLICHE INTELLIGENZ

Matching – Austausch mit den Expert*innen

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

DIHSÜD Digital Innovation Hub

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

Gruppe 1 - Grün:
Expert:innen:

- DIH SÜD
- FH Campus 02 - Mag.a Angelika Höber
- Coding School Wörthersee -Lukas Stattmann MSc
  Nikolas Kachelmaier, MA

Gruppe 2 - Rot:
Expert:innen:

- Fachgruppe UBIT
  Ing. Wolfgang Stauder
- Wirtschaftskammer Kärnten
- Experts Group

Gruppe 3 - Gelb:
Expertin:

- KWF - Mag. Cornelia Jann

Eine Initiative von:

UBIT Unternehmensberatung Buchhaltung IT-Dienstleistung

DIHSÜD Digital Innovation Hub

175 JAHRE WKO WIRTSCHAFTSKAMMER KÄRNTEN

20 MIN

5 MIN

Vielen Dank für Ihre Aufmerksamkeit!

Eine Initiative von:

UBIT
Unternehmensberatung
Buchhaltung
IT-Dienstleistung

DIHSÜD
Digital Innovation Hub

175 JAHRE
WKO
WIRTSCHAFTSKAMMER KÄRNTEN