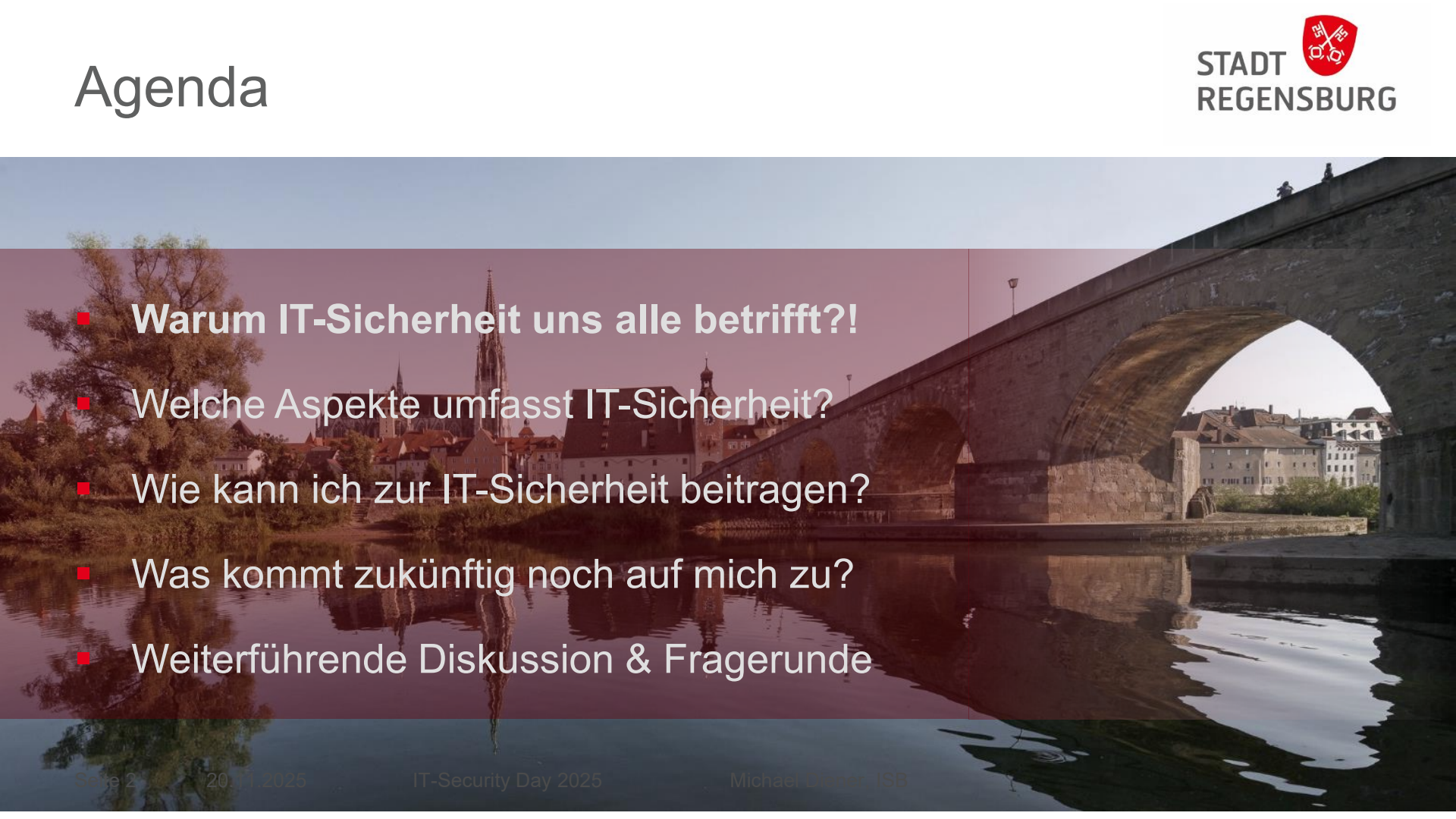


Kleines 1x1 der IT-Sicherheit

IT-Security Day // 20. November 2025

Michael Diener
Informationssicherheitsbeauftragter

Agenda

- 
- **Warum IT-Sicherheit uns alle betrifft?!**
 - Welche Aspekte umfasst IT-Sicherheit?
 - Wie kann ich zur IT-Sicherheit beitragen?
 - Was kommt zukünftig noch auf mich zu?
 - Weiterführende Diskussion & Fragerunde

Die Zahl der Cyberangriffe steigt seit Jahren an.

Westfälische Nachrichten

Dienstag, 18.11.2025

MÜNSTER MÜNSTERLAND SCP WELT SPORT

Fachhochschule lahmgelegt

FH Münster von großem Cyberangriff betroffen

Münster - Die Fachhochschule in Münster ist aktuell von einem Cyberangriff betroffen. Große Teile der IT sind lahmgelegt. Aktuell ist nicht absehbar, wann Studierende und Mitarbeiter wieder Zugriff auf wichtige Programme haben. Von Jonas Wiening

Mittwoch, 22.06.2022, 14:35 Uhr aktualisiert: 24.06.2022, 12:25 Uhr



Golem

MÜNCHEN

Cyberangriff trifft Universität der Bundeswehr

Angreifer sind wohl über geleakte Zugangsdaten in den Besitz persönlicher Daten von Soldaten und zukünftigen Offizieren der Bundeswehr gelangt.

14. Februar 2025 um 09:09 Uhr / Marc Stöckel

4 News folgen Teilen



Blick auf eine dunkle Tastatur (Symbolbild)

<https://www.wn.de/muenster/fachhochschule-fh-muenster-cyberangriff-system-2589252>

<https://www.golem.de/news/muenchen-cyberangriff-trifft-universitaet-der-bundeswehr-2502-193337.html>

Auch Behörden werden massiv angegriffen ...

Aufgrund von Auffälligkeiten im Datennetz der Stadtverwaltung wurden die Systeme am 6. November 2025 vorsichtshalber vom Netz genommen. Die Stadtverwaltung ist per Telefon und E-Mail nicht erreichbar. Anwendungen wie die Online- Dienstleistungen und die Online-Terminvergabe auf dieser Seite sind noch nicht verfügbar. Auch einige andere städtische Internetseiten sind noch nicht wieder im Netz. Wie lange der Ausfall dauert, steht derzeit nicht fest. Die Stadtverwaltung arbeitet mit Hochdruck an einer Lösung.

Die Stadtverwaltung bedauert die Unannehmlichkeiten, die sich daraus für viele Menschen ergeben. Vielen Dank für Ihr Verständnis.

Aktuelle Informationen gibt es [hier](#) → (Stand 18. November 2025)



Stadtverwaltung

Bürgerservice

Verwaltung & Politik

Standort mit Zukunft

Soziales & Gesellschaft

Leben



← Verwaltung & Politik

🏠 > Verwaltung & Politik > Auffälligkeiten im Datennetz

Auffälligkeiten im Datennetz

Oberbürgermeister*innenwahl 2025 →

Landtagswahl 2026 →

Amtsblatt

Auffälligkeiten im Datennetz

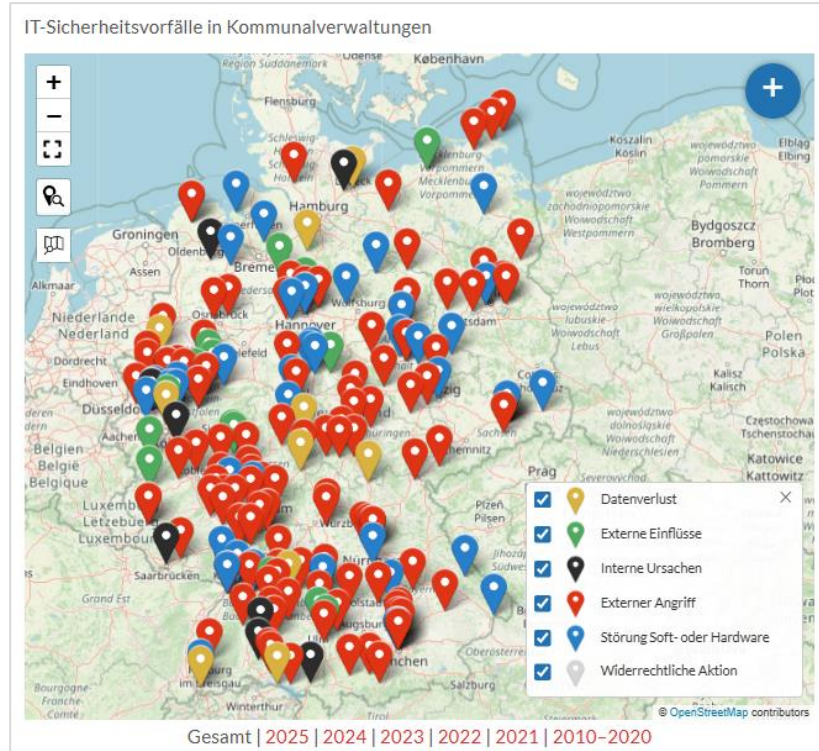
Aufgrund von Auffälligkeiten im Datennetz der Stadtverwaltung wurden die Systeme am 6. November 2025 vorsichtshalber vom Netz genommen. Die Stadtverwaltung ist per Telefon und E-Mail nicht erreichbar. Anwendungen wie die Online- Dienstleistungen und die Online-

Reisepass?

Kfz-Wechsel?

OZG-Services?

Kommunaler Notbetrieb: Das Lagebild, das es nicht gibt.



<https://kommunaler-notbetrieb.de/zeitleiste/>

Zeitleiste



Deutschlands erste Cyberkatastrophe: der Hackerangriff auf den Landkreis Anhalt-Bitterfeld im Juli 2021.


Nachrichten Sport Wissen Verbraucher Kultur Unterhaltung Mediathek Fernsehen Radio

Live hören ARD Infonacht WDR 5

22.03 - 06.00 Uhr ARD INFONACHT


Mail ins Studio Playlist und Titelsuche

Programm Sendungen Podcast Veranstaltungen Über uns Kontakt



You are fucked! Deutschlands erste Cyberkatastrophe

Mehr zur Sendung



WDR 5 Tiefenblick
Können wir bald Gedanken lesen? Wie verlaufen Drohnen-Kriege? Wo liegt die Grenze zwischen Wahrheit und Wahrhaftigkeit? Das sind nur einige Fragen, auf die unsere Autorinnen und Autoren Antworten geben. | [mehr](#)

<https://www1.wdr.de/radio/wdr5/sendungen/tiefenblick/tiefenblick-you-are-fucked-100.html>

Die Folgen von Cyberangriffen sind gravierend und bedrohen mehrere **IT-Grundschutzziele**.



Vertraulichkeit

Unberechtigte haben
Zugangsdaten erbeutet
und Daten eingesehen



Verfügbarkeit

Dateien und Server
wurden verschlüsselt
mittels Ransomware



Integrität

Unberechtigte konnten
(unbemerkt) Dateien
manipulieren

Quelle: IT-Grundschutz-Kompendium (Edition 2023). Bundesamt für Sicherheit in der Informationstechnik (eigene Darstellung).

Die **Ursachen** von Cyberangriffen sind vielfältig.

Komplexität von IT-
Umgebungen

Technische
Schwachstellen

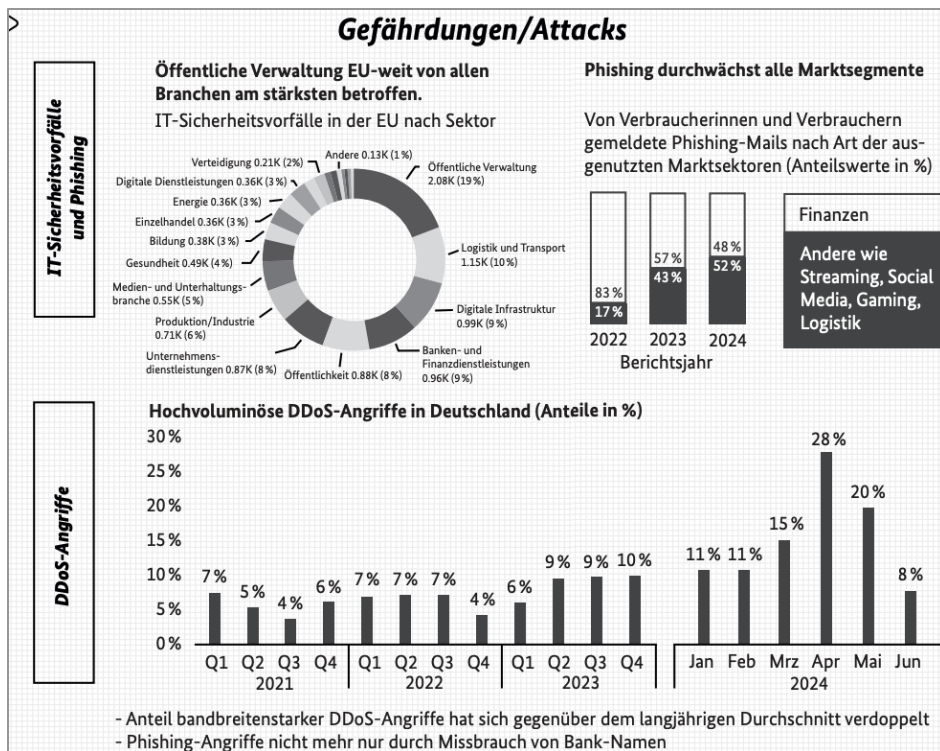
Faktor
„Mensch“

Fehlende/Lückenhafte
IT-Sicherheitskultur

Wirtschaftliche
Anreize

Möglichkeiten des
Internets & AI

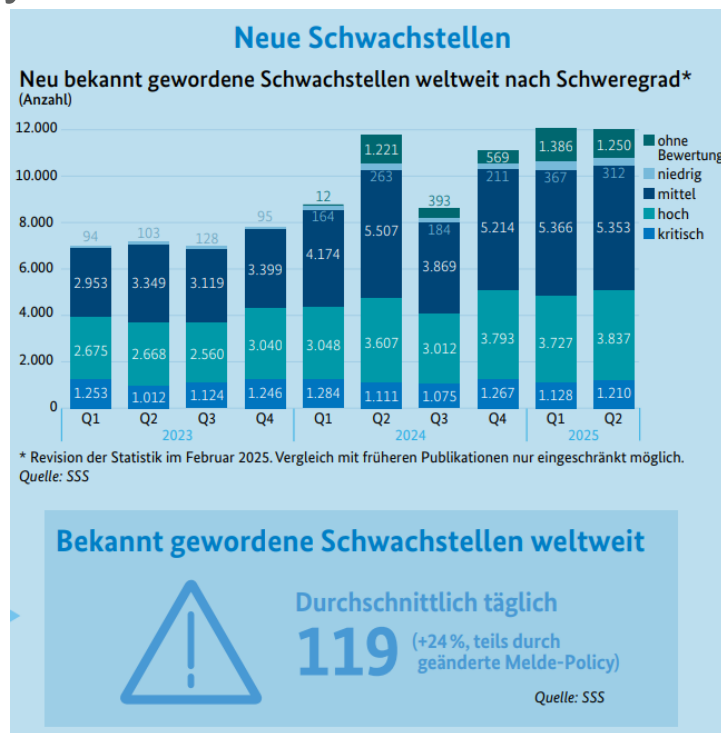
Quelle: ChatGPT.com // Prompt: „Warum sind Cyberangriffe möglich?“



Top-Gefährdungen:

- Phishing / Spear-Phishing
- DDoS-Angriffe
- Malware
- ...
- „Mensch-Maschine-Schnittstelle“

BSI-Lagebild 2025 / Cybersicherheit in Bayern 2025



<https://bsi.bund.de/lagebericht>

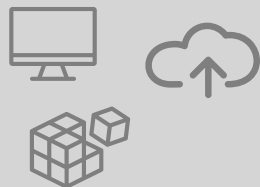
https://www.stmfh.bayern.de/digitalisierung/it_sicherheit/BerichtCybersicherheit2025.pdf

Agenda

- 
- Warum IT-Sicherheit uns alle betrifft?!
 - **Welche Aspekte umfasst IT-Sicherheit?**
 - Wie kann ich zur IT-Sicherheit beitragen?
 - Was kommt zukünftig noch auf mich zu?
 - Weiterführende Diskussion & Fragerunde

Was umfasst Informationssicherheit?

- Desktop-PC, Notebook, Tablet, Handy, IoT, ...
- Programme (Fachverfahren), Apps, ...
- Webanwendungen
- Public Clouds
- ...



IT-Sicherheit



- Zutrittsmittel (Chip, Schlüssel)
- Zugangsdaten (PW, PIN, 2FA, ...)
- Zugriffsrechte (Rollen, Rechte, etc.)
- ...

Daten-Sicherheit

- RZ / Technikräume
- Gebäude, Büros, ...
- Home-Office / Mobile Arbeit
- ...



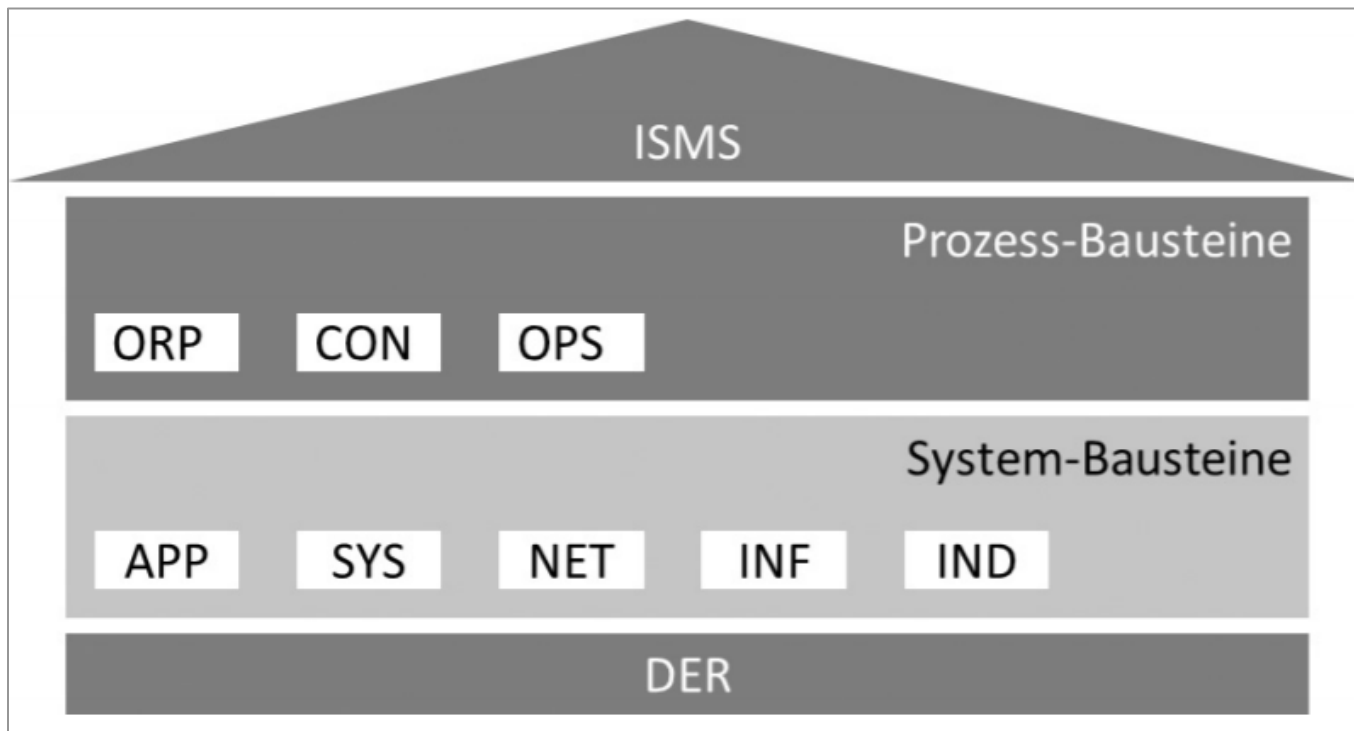
Infrastruktur-Sicherheit

- Vorgaben bzgl. der Aktualität von IT-Dokumentationen,
- Koordination Awareness-Schulungen,
- Schwachstellenmanagement,
- Prozessaudits / Penetrationstests, ...

Informationssicherheit



Übersicht: BSI IT-Grundschutz-Bausteine



Quelle: BSI-Standard 200-2. IT-Grundschutz-Methodik. S. 132ff. Version 1.0. BSI. // <https://bsi.bund.de/grundschutz>

Informationssicherheit betrifft JEDEN!

*„Aber das macht
doch die IT“*

*„Um was soll ich mich
denn noch alles
kümmern?“*


*„Davon habe
ich noch nie
etwas gehört!“*

*„Nicht meine
Gehaltsstufe!“*

*„Das haben wir doch
schon immer so
gemacht!“*

...

Agenda

- 
- Warum IT-Sicherheit uns alle betrifft?!
 - Welche Aspekte umfasst IT-Sicherheit?
 - **Wie kann ich zur IT-Sicherheit beitragen?**
 - Was kommt zukünftig noch auf mich zu?
 - Weiterführende Diskussion & Fragerunde



- Meldung von **defekten Türschlössern** sofort und pragmatisch dem Hausmeister!
- Jährlicher Self-Check: Wie viele Schlüssel gibt es, die an der Türe sperren und wer hat eigentlich einen?
- **Schlüsselkästen** im Büro nicht im direkten Sichtfeld von Publikumsverkehr positionieren!
- Büro-Schränke absperren, Schlüssel aber abziehen am Ende des Tages!



Was ist passiert?

Wie hätte man das verhindern können?

IT-Sicherheit mit **USB-Sticks**

- **Verdächtige USB-Sticks niemals** an ungeschützte IT-Hardware anschließen!
- **IT-Sicherheitsrichtlinien** der Organisation beachten bzgl. Nutzung von USB-Sticks!
- Bei Bedarf auf USB-Sticks eine sichere **Verschlüsselung aktivieren**, z. B. zip-Datei mit Passwort konfigurieren.



IT-Sicherheit von **mobilen Endgeräten**

- Notebooks, Tablets und Smartphones **niemals ungesichert und unbeaufsichtigt** lassen!
- **Displaysperre** aktivieren: ganz schnell am PC mit dem Shortcut [Strg-Taste] + [L] bzw. PIN / Wischmuster auf Smartphones!
- Unterwegs im Zug, in der Hotel-Lobby etc. ggf. **Sichtschutzfolien** am Bildschirm anbringen.



Daten-Sicherheit: **Passwörter**

HOME TICKER PODCAST NEWSLETTER **GOLEM PLUS** FORUM E-PAPER-SHOP **Mehr lesen mit Golem Plus** 🔍 👤

KARRIEREWELT JOBS IT-FACHTRAININGS COACHINGS SPRACHKURSE KARRIERESERVICES | GOLEM-PC TECHNIK-RATGEBER DEALS

FORSCHER MACHEN DEN TEST

59 Prozent aller Passwörter in unter 60 Minuten knackbar

Forscher haben per **Brute-Force-Methode** mit einer **Nvidia** Geforce RTX 4090 Millionen von **Passwörtern** aus dem Darknet geknackt.

📌 in Pocket speichern 📌 merken 📌 21. Juni 2024, 13:30 Uhr, Marc Stöckel



(Bild: pixabay.com / geralt)

<https://www.golem.de/news/forscher-machen-den-test-59-prozent-aller-passwoerter-in-unter-60-minuten-knackbar-2406-186329.html>

Was sehen **starke Passwörter** aus?

RTX 5090 knackt Passwörter in Minuten: So schützen sich Nutzer

Wie schnell knackt moderne Hardware Passwörter? Neue Simulationen mit der RTX 5090 liefern alarmierende Ergebnisse. Gleichzeitig zeigen die Berechnungen auch, welche Fehler Nutzer bei der Passwortwahl unbedingt vermeiden sollten.



Felix Krauth 16.05.2025 16:11 Uhr

- Laut der Hive-Untersuchung befindet sich man im grünen Bereich, wenn das Passwort ...
 - **mindestens 13 Zeichen umfasst**
 - **und Zahlen enthält**
 - **und Groß- und Kleinbuchstaben**
- **VORSICHT: „Wörterbuch-Angriffe“ sind eine Alternative zu Brute-Force und sehr effektiv!!**

<https://winfuture.de/news,150969.html>

Time it takes a hacker to brute force your password in 2025

Hardware: 12 x RTX 5090 | Password hash: bcrypt (10)

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

Hive Systems

Read more and download at hivesystems.com/password

Faktor „Mensch“ vs. **Passwörter**



- Keine Wort-Muster-Kombinationen verwenden, z. B. ~~#Winter2025#~~
- Unterschiedliche Passwörter für private und dienstliche Accounts nutzen!
- Passwort-Zettel nicht unter Schreibtischablagen, Tastaturen bzw. in Laptoptaschen etc. aufbewahren!

<https://www.youtube.com/shorts/2VV5hmgHIVs>

Merkhilfe: starke Passwörter ■□□

■ Methode I: Merksätze bilden

1. Einen guten Merksatz ausdenken

„Ich fahre 20 Minuten zur Arbeit und stehe im Tunnel im Stau!“

2. Einzelne Zeichen ersetzen

z. B. „und“ durch „&“, ein großes „I“ durch eine „1“

„1ch fahre 20 Minuten zur Arbeit & stehe im Tunnel im Stau!“

3. Anfangsbuchstaben und ersetzte Zeichen kombinieren

1f20MzA&siTiS!

Merkhilfe: starke Passwörter ☐☒☐

- **Methode II: Ganze Merksätze verwenden**

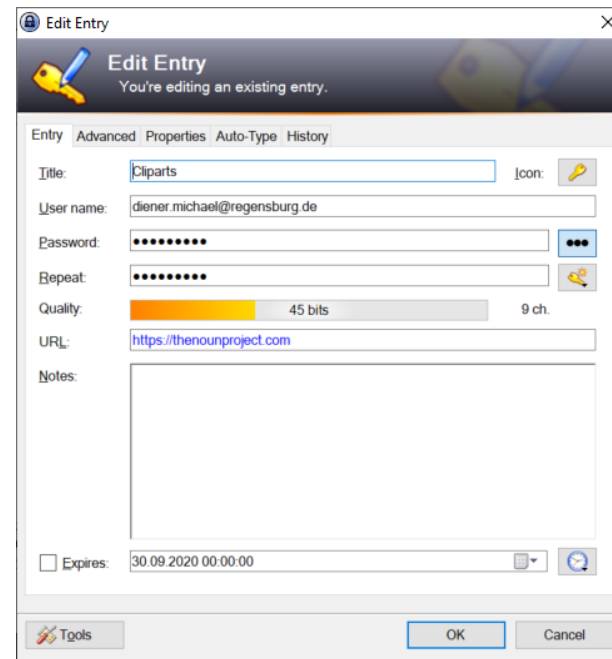
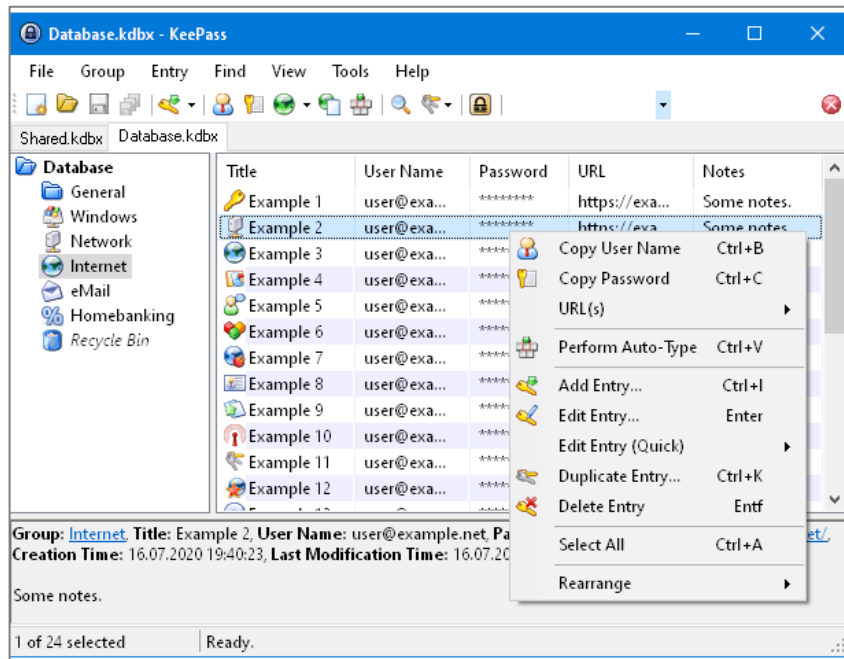
1. Einen guten Merksatz ausdenken

„Ich jogge gerne um 18 Uhr an der Donau.“

Ich jogge gerne um 18 Uhr an der Donau.

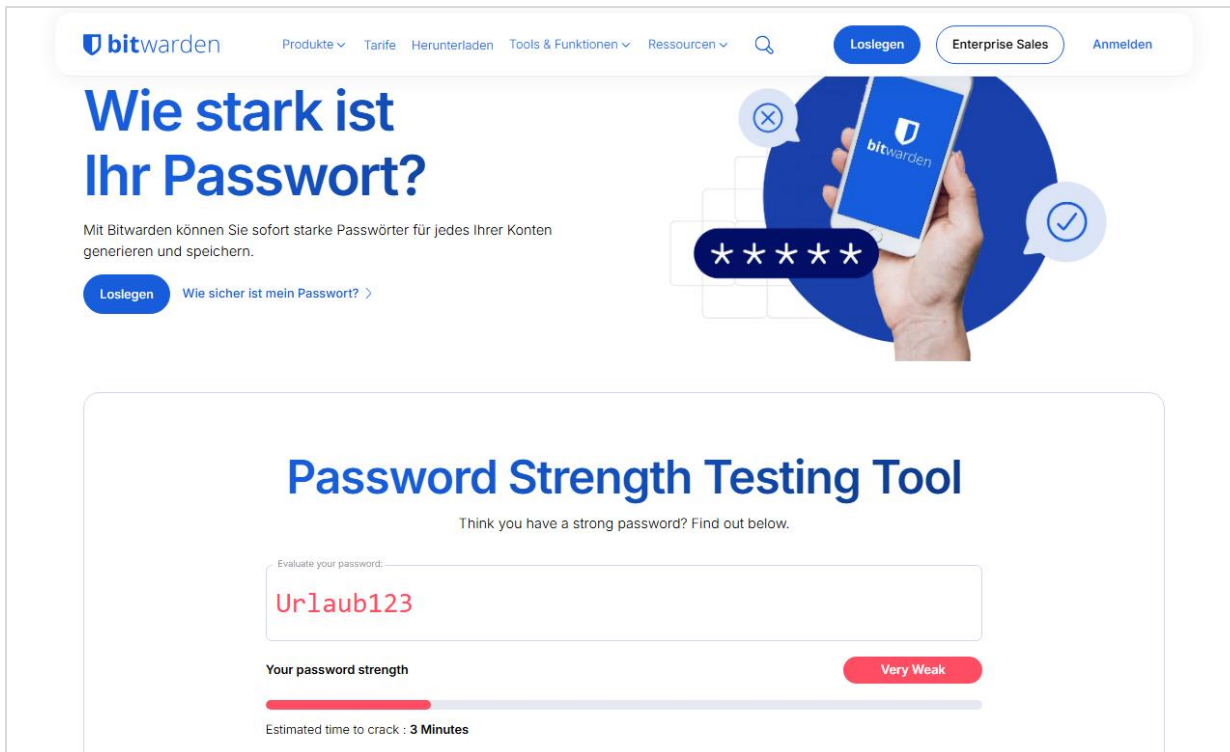
Merkhilfe: starke Passwörter □□■

■ Methode III: Passwort-Manager-Tool



<https://keepass.info/>

Überprüfung der **Password-Qualität**



The screenshot shows the Bitwarden website's password strength testing tool. At the top, the Bitwarden logo and navigation links are visible. The main heading is "Wie stark ist Ihr Passwort?". Below it, a subheading states: "Mit Bitwarden können Sie sofort starke Passwörter für jedes Ihrer Konten generieren und speichern." There are buttons for "Loslegen", "Enterprise Sales", and "Anmelden". A graphic shows a hand holding a smartphone displaying the Bitwarden app, with a speech bubble containing five stars. The tool section is titled "Password Strength Testing Tool" and includes the text "Think you have a strong password? Find out below." A text input field contains the password "Urlaub123". Below the input field, the text "Your password strength" is followed by a progress bar that is mostly red, indicating a weak password. To the right of the progress bar, a red button says "Very Weak". Below the progress bar, the text "Estimated time to crack : 3 Minutes" is displayed.

bitwarden Produkte Tarife Herunterladen Tools & Funktionen Ressourcen Loslegen Enterprise Sales Anmelden

Wie stark ist Ihr Passwort?

Mit Bitwarden können Sie sofort starke Passwörter für jedes Ihrer Konten generieren und speichern.

Loslegen Wie sicher ist mein Passwort? >

Password Strength Testing Tool

Think you have a strong password? Find out below.

Evaluate your password:

Urlaub123

Your password strength

Very Weak

Estimated time to crack : 3 Minutes

<https://bitwarden.com/de-de/password-strength/>

Bitte das zu prüfende
Passwort minimal
abändern!

Nutzung von **Zwei-Faktor-Authentifizierung (2FA)** bzw. Multi-Faktor-Authentifizierung (MFA)



SMS-Code / Anruf



E-Mail-Link



Authenticator-App
(One-Time-Password)



Hardware-Token
(USB-Dongle)

- Beim User-Login muss zusätzlich zum wissensbasierten Faktor (Passwort) ein weiterer **besitzbasierter Faktor** eingegeben werden!
- **2FA in Cloud-Services** muss/sollte abhängig von der Kritikalität der Daten aktiviert werden!

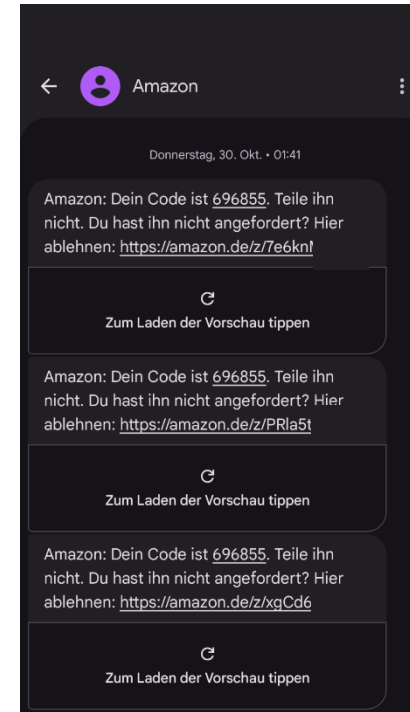
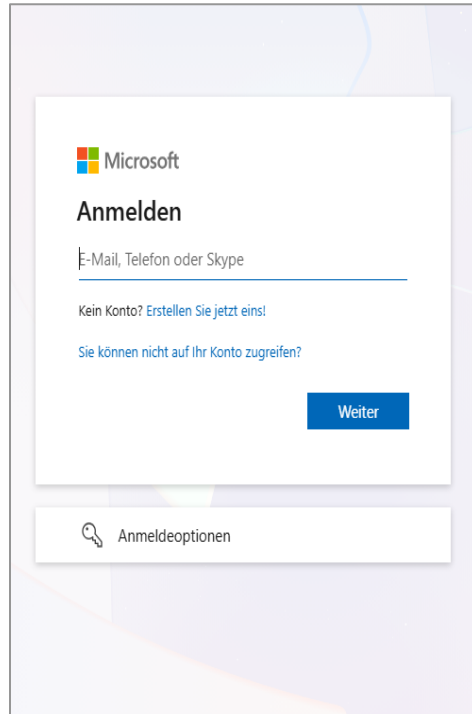
2FA-Token sorgsam nutzen.



- Chipkarten nicht über Nacht im Lesegerät stecken lassen!

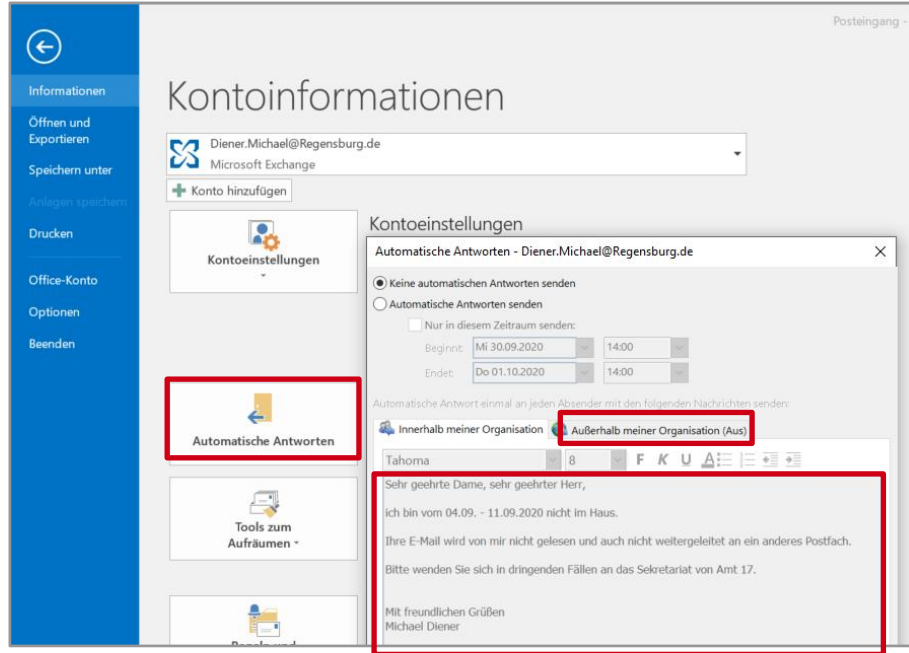
Quelle: Stadt Regensburg

Vorsicht bei unerwarteten 2FA-Tokens (MFA-Bombing) bzw. Passwort-Rücksetz-Links



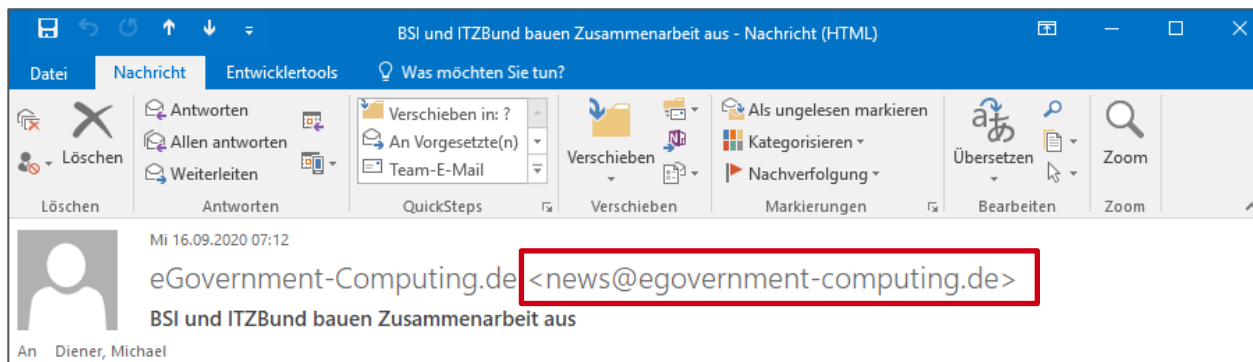
- Keine Panik!
- Nicht überhastet Links klicken!
- URL prüfen!!!
- Passwort ggf. ändern im Web-Service!

Quelle: Stadt Regensburg, Privat.



- **Abwesenheitsbenachrichtigungen** für externe Empfänger mit nur so vielen Information wie nötig einstellen in Microsoft Outlook.
- Ziel: Reduktion der Gefahr des automatischen Mailversands von sensiblen Informationen (z. B. persönliche Telefonnummer, E-Mail-Adresse(n) Stellvertreter, etc.).

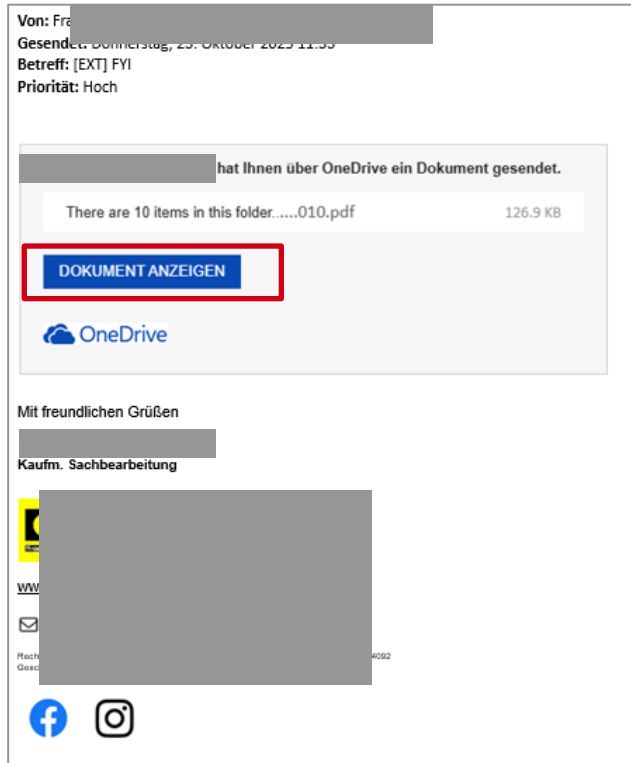
E-Mail Sicherheit



- Bevor Sie eine E-Mail beantworten oder darin einen Link anklicken, prüfen Sie bitte die E-Mail-Adresse (externer Absender) in den **spitzigen Klammern**!
- **Achtung:** Die Absender-Mailadresse kann ggf. von der Antwort-Mailadresse (reply-to) abweichen!
- Ggf. **BCC-Feld** nutzen, um datenschutzkonform senden zu können!

Quelle: Stadt Regensburg

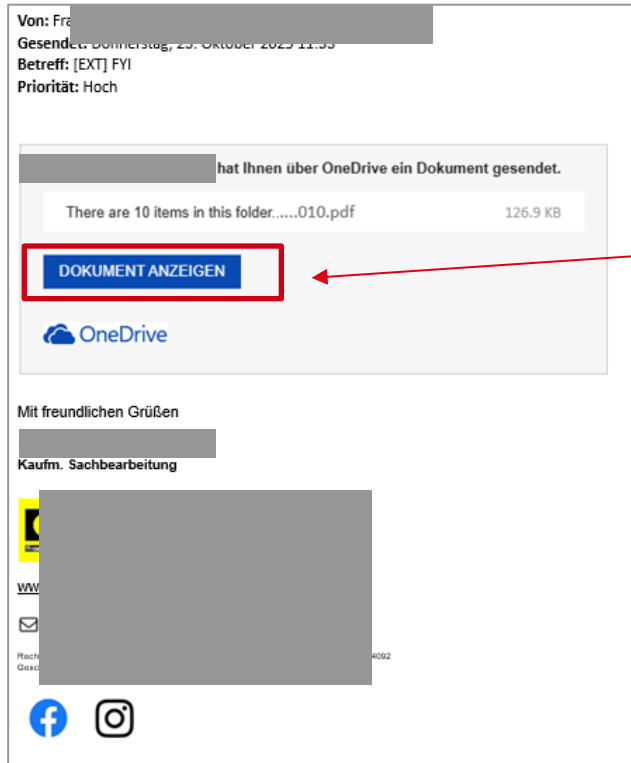
E-Mail Sicherheit: Gefährliche Links



Quelle: Stadt Regensburg

- Problem:
 - Manipulierte E-Mails werden über echte, aber „kompromittierte“ E-Mail-Postfächer versendet!
 - Im Ordner „gesendete Objekte“ finden Angreifer historische E-Mail-Korrespondenz.
 - Empfänger werden mit hoher Wahrscheinlichkeit manipulierte E-Mails lesen und bearbeiten!
 - Schadhafte Links sind auch nicht sofort erkennbar, da diese hinter Bildern platziert werden.
- Lösungsansatz:
 - Im Zweifelsfall Absender via Telefon (bitte nur bekannte Rufnummern aus Historie benutzen!) kontaktieren.
 - Links manuell untersuchen, z. B. mittels Maus-Hover-Effekt oder Hyperlink kopieren (Rechtsklick).

E-Mail Sicherheit: Gefährliche Links



<https://1drv.ms/w/c/b75c49f660d4ba30/EU1z7tY3xBJGjyUIX0GDrOMBloi6eJy9-E0WxPHbKm9q5g?e=xlwNCP&CT=1763549991371&OR=Outlook-Body&CID=DD170253-377F-4933-92F6-B62C3C0A4ED9&wdLOR=cACED81C5-93D8-4F07-8474>
Klicken oder Tippen Sie, um den Link zu folgen

- Lösungsansatz:
 - „Geschultes Auge“: Sehen die Links zu dieser Ziel-URL (OneDrive) immer so aus, oder ist dieser anders?
 - Gefahrlose Untersuchung des Inhalts der Webseite hinter dem Link mit einem sog. Sandbox-Browser (Browser im Browser).

Quelle: Stadt Regensburg

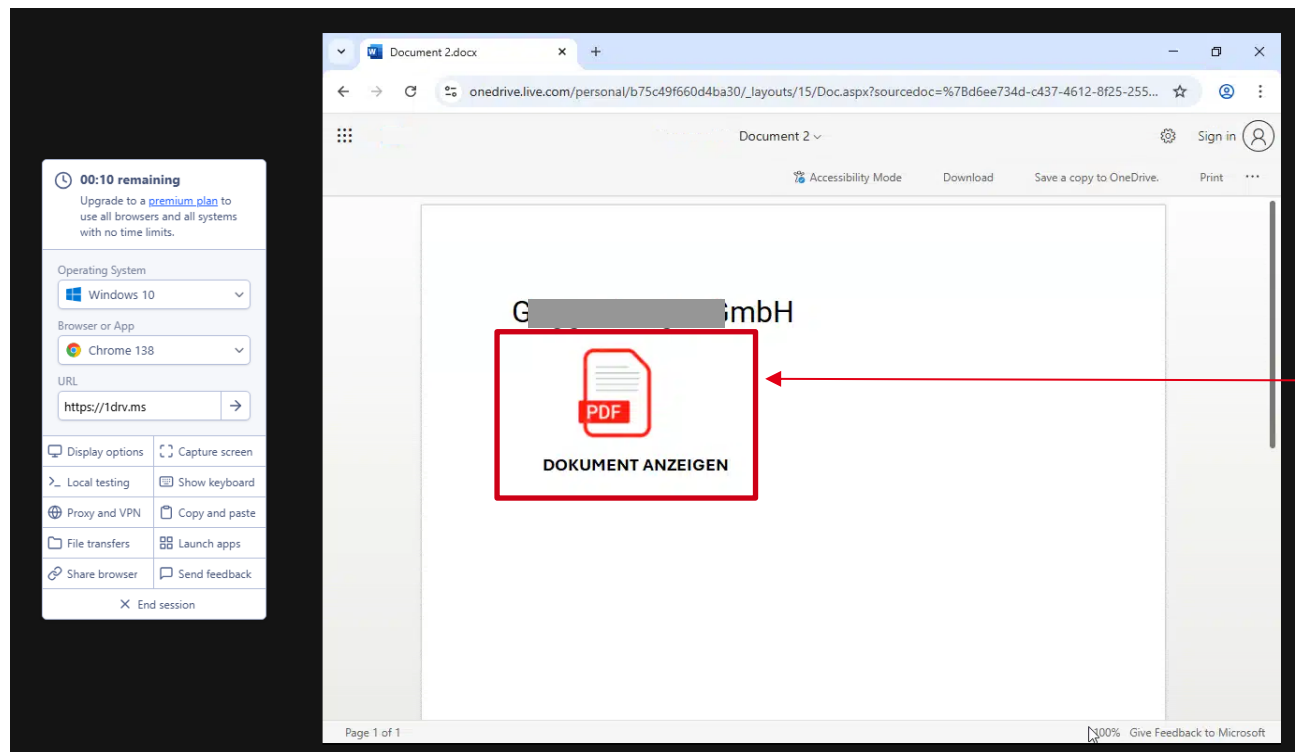
Sandbox-Browser: Verdächtige Links untersuchen



The screenshot shows the Browserling website. At the top left is the Browserling logo (a blue alien head) and the text "browserling". To the right are links for "Features", "Pricing", "Live API", "About Us", "Sign In", and a blue "Sign Up" button. Below the logo, it says "we also created:" followed by a red icon and the text "ONLINEPNGTOOLS". The main content area is a large white box with a blue border. Inside, it says "Online cross-browser testing" and "Cybersecurity sandbox". Below this is a text input field containing the URL "https://1drv.ms/w/c/b75c49f660d4ba30/EU1z7tY3" and a blue "Test now!" button. Underneath the input field are three dropdown menus: "Windows 10" (with a Windows logo), "Chrome" (with a Chrome logo), and "138" (with a dropdown arrow). At the bottom of the white box, it says "Get a browser and start testing in 5 seconds!". The entire interface is set against a light blue background.

<https://www.browserling.com/>

Sandbox-Browser: Verdächtige Links untersuchen

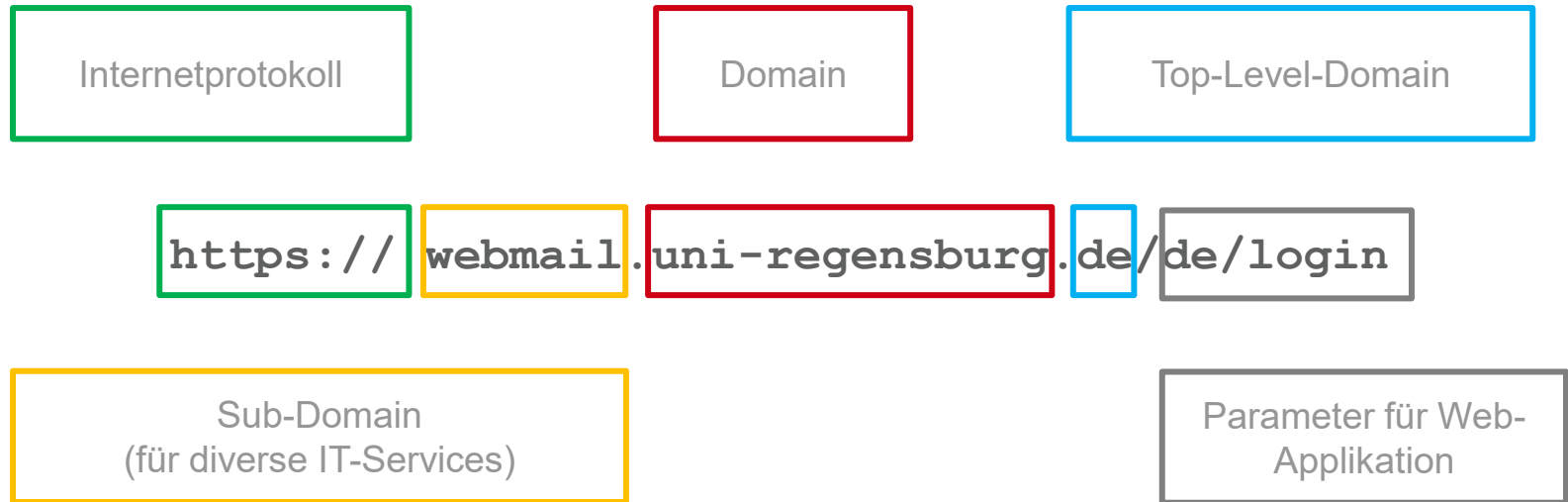


Dieser Fall ist klar!!!

Ein PDF-Dokument im Word-Dokument!

→ E-Mail löschen!

EXKURS: URLs / Hyperlinks „lesen und verstehen“



- Entscheidend ist die korrekte Domain und Top-Level-Domain!

Übung: Falsche Hyperlinks erkennen

`https://www.regensburg.net`

`https://www.regensburg.online.de/intranet`

`https://www.regensberg.de`

`https://www.regensburg.de/itportal`

`https://www.regensburg-stadt.de`

`https://srv40.regensburg.de`

Übung: Falsche Hyperlinks erkennen

`https://www.regensburg.net`

`https://www.regensburg.online.de/intranet`

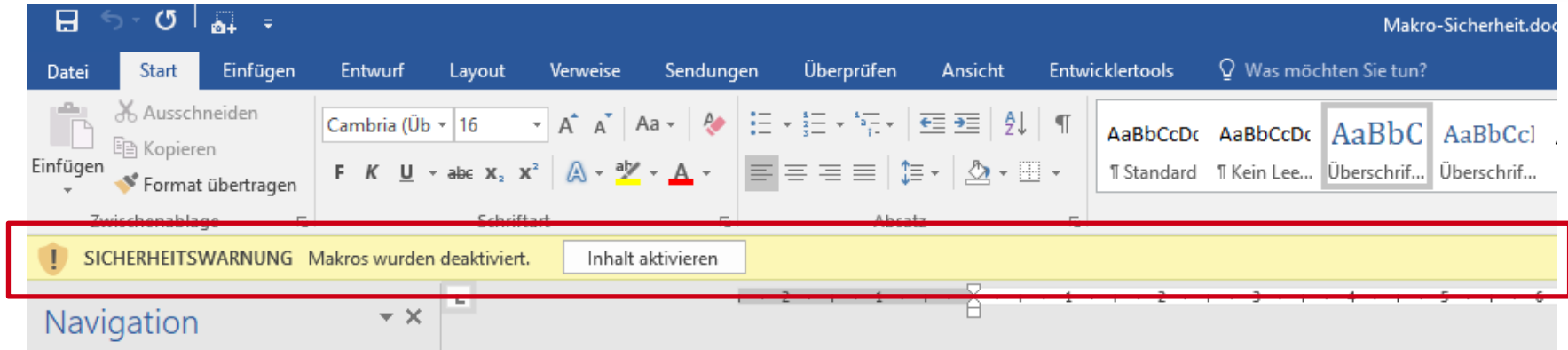
`https://www.regensberg.de`

`https://www.regensburg.de/itportal`

`https://www.regensburg-stadt.de`

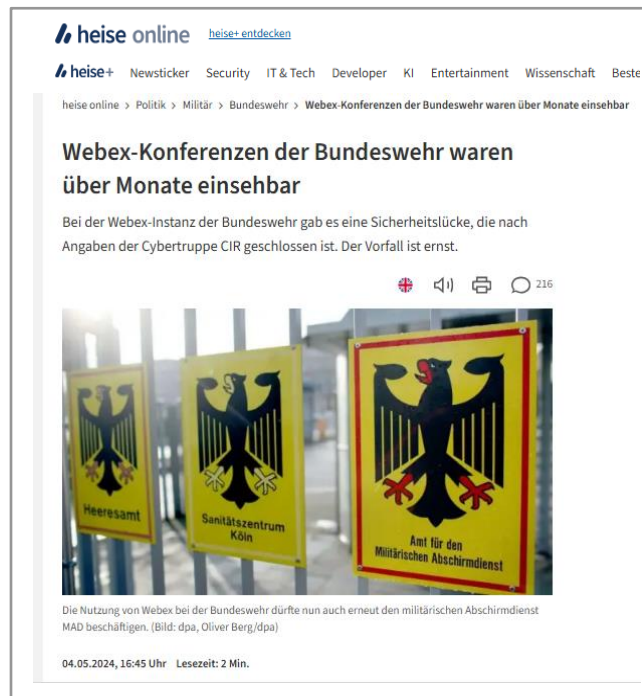
`https://srv40.regensburg.de`

VBA-Makros in Microsoft Office-Dateien



- Achtung: VBA-Makros können schadhafte Code enthalten!
- Vergewissern Sie sich immer, dass eine Office-Datei mit Makro aus einer **vertrauenswürdigen Quelle** stammt. → Wer ist der Urheber?
- Bestätigen Sie die gelbe Sicherheitswarnung erst dann mit einem Klick auf die Schaltfläche „Inhalte aktivieren“, wenn Sie sich absolut sicher sind!

Sichere Nutzung von Videokonferenz-Tools



- Sicherheitseinstellungen setzen: „Warten in Lobby“
- Beachten von vorhandener IT-Sicherheitsrichtlinien
- Hinterfragen, warum der identische Username mehrfach zu sehen ist
- Vorsicht bei Aktivierung der Option „Einwahl per Telefon zulassen“!

<https://youtube.com/shorts/B6GZqcykrqo>

<https://www.heise.de/news/Webex-Konferenzen-der-Bundeswehr-waren-ueber-Monate-einsehbar-9708307.html>

SECURITY-AWARENESS-TRAINING

STADT
REGENSBURG

Training

Erfolge

Michael Diener

Sehr gut, Michael Diener!

Sie haben bereits umfangreiches Wissen gesammelt. Bleiben Sie dran - auch die nächsten Module enthalten spannende Themen.

Sie haben 20 von 38 Modulen abgeschlossen.

Schnellstart

Grundlagen

50 EP

19.01.2024

Pflichtmodul

ca. 1 Minute

Fortsetzen

Kompakttraining IT-Sicherheit

Die Zahl der Cyberangriffe nimmt weiterhin rasant zu. Lernen Sie hier im Schnelldurchlauf die größten Gefahren und die effektivsten Methoden zur Verteidigung und Prävention kennen. Manchmal gelingt ein Angriff allerdings trotz aller Sicherheitsmaßnahmen. Wir zeigen Ihnen deshalb auch, wie Sie bestmöglich darauf reagieren und so den Schaden begrenzen.

Modul überfällig!

1 / 16 Module

Zur Übersicht

Fortsetzen

noch ca. 58 Minuten

E-Mails sicher nutzen

Lernen Sie hier den sicheren Umgang mit E-Mails und Postfächern.

Modul überfällig!

4 / 7 Module

Zur Übersicht

Fortsetzen

ca. 26 Minuten

Mobilgeräte sicher nutzen

Lernen Sie hier, was es bei der Nutzung von Mobilgeräten zu beachten gibt.

Abgeschlossen

Zur Übersicht

Neustarten

Internet & Webtools

Erfahren Sie hier, wie Sie Filesharing- und Kollaborationstools sowie soziale Netzwerke und Webseiten gefahrlos nutzen.

Abgeschlossen

Zur Übersicht

Neustarten

Sicher am Arbeitsplatz

Erhalten Sie hier wichtige Hinweise, wie Sie Ihren Arbeitsplatz sicherer gestalten können.

Abgeschlossen

Zur Übersicht

Neustarten

Level 7

0 / 630 Erfahrungspunkte

Abzeichen

Zertifikat ausstellen

Schon gewusst?

Quelle: SoSafe E-Learning-Plattform


Seite 41

20.11.2025

IT-Security Day 2025

Michael Diener, ISB

Agenda

- 
- Warum IT-Sicherheit uns alle betrifft?!
 - Welche Aspekte umfasst IT-Sicherheit?
 - Wie kann ich zur IT-Sicherheit beitragen?
 - **Was kommt zukünftig noch auf mich zu?**
 - Weiterführende Diskussion & Fragerunde

Social Engineering Attacken zielen gezielt auf den Faktor „Mensch“ ab und sind meist schwer erkennbar

Misdirection
(Ablenkung)

Time Pressure
(Zeitdruck)

Opportunity
(Gelegenheit)

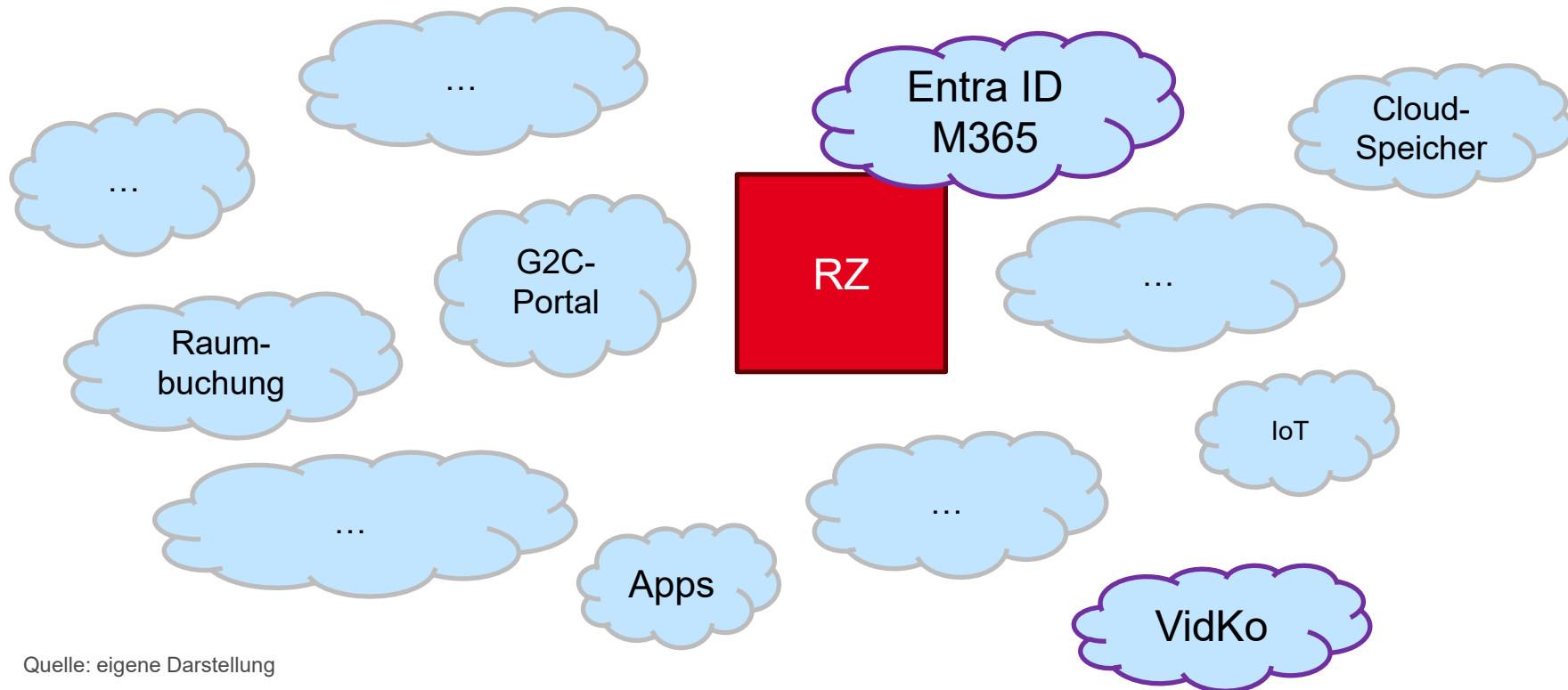
Social Compliance
(Respekt vor
Autoritäten)

Social Proof
(Gesellschaftliche
Anpassung)

Business Email Compromise (BEC-Attacken)

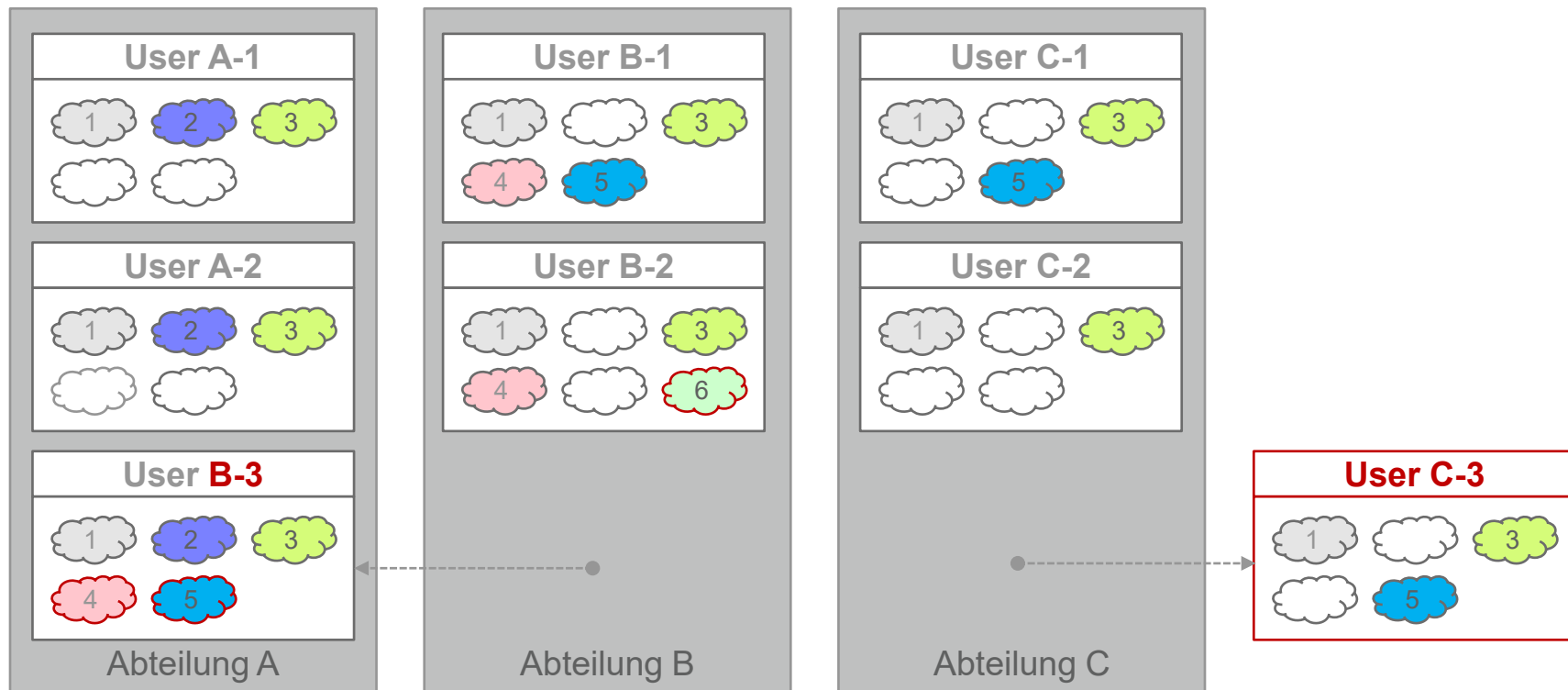
- Sie enthalten keine Schadsoftware, keine böswilligen Links und keine E-Mail-Anhänge
- Sie zielen auf bestimmte Personen innerhalb von Organisationen ab
- Sie sind auf das anvisierte Opfer zugeschnitten und erfordern oft eine vorherige Recherche über die betreffende Organisation
- Beispiele:
 - Aufforderung zur Änderung der IBAN
 - Aufforderung zur Bereitstellung von (vertraulichen) Daten
 - ...

Zunehmend mehr **Public-Cloud-Services** in öffentlichen Verwaltungen



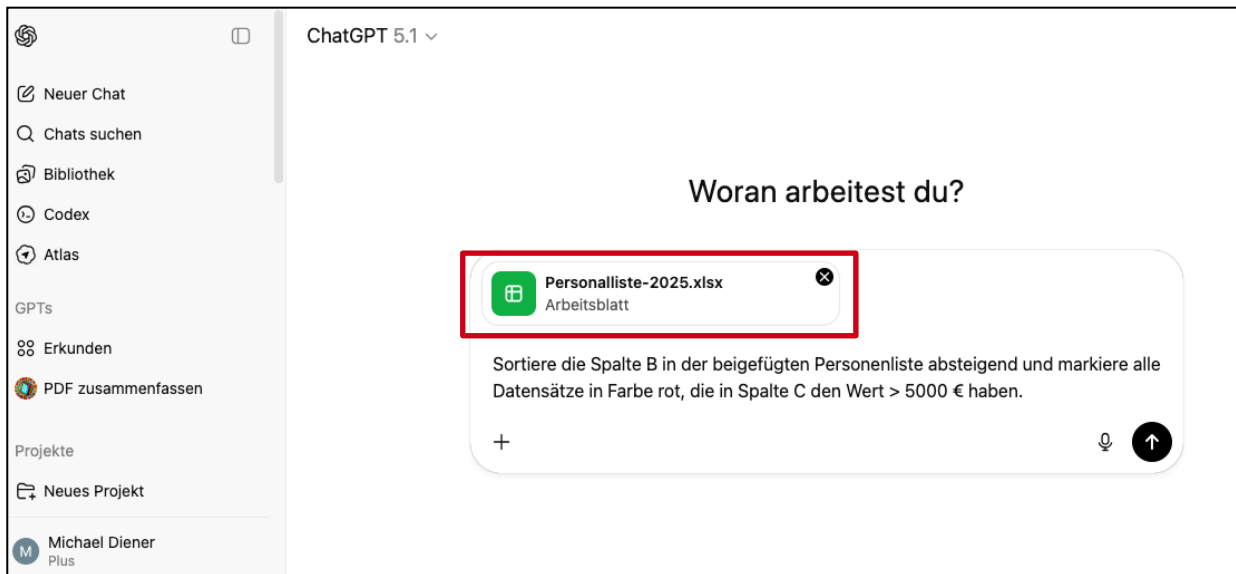
Quelle: eigene Darstellung

Personalwechsel führen zu **User-Inkonsistenzen** in **Public-Cloud-Services**



Quelle: eigene Darstellung

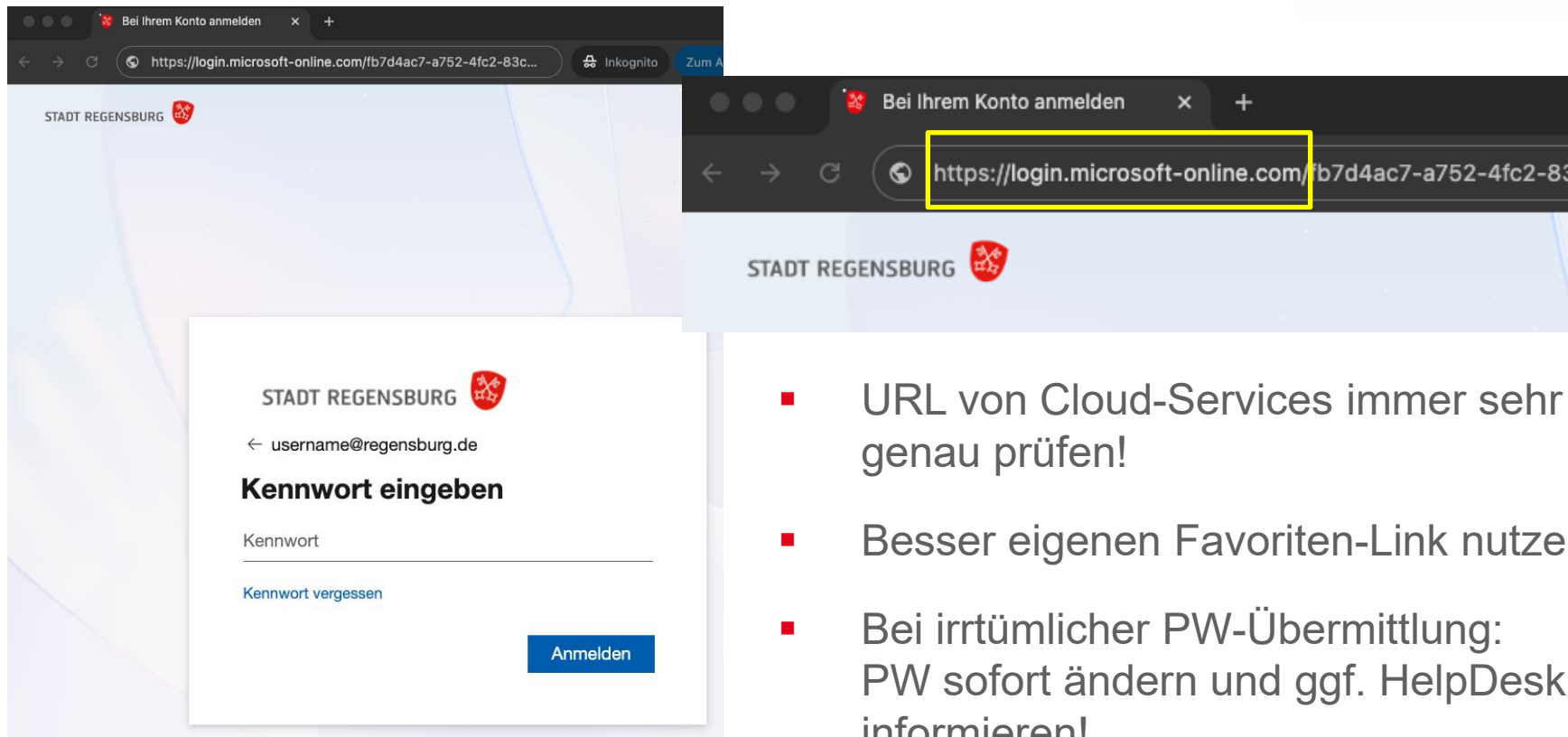
Sichere Bedienung von GenAI-Tools



- Beachtung von Regelungen bzw. IT-Sicherheitsrichtlinien im Umgang mit KI/AI!
- Keine Übermittlung sensibler Dateien an öffentlich zugängliche KI-Modelle!

<https://chatgpt.com>

Sicherer Login in Public-Cloud-Services



STADT REGENSBURG

Bei Ihrem Konto anmelden

← username@regensburg.de

Kennwort eingeben

Kennwort

[Kennwort vergessen](#)

Anmelden

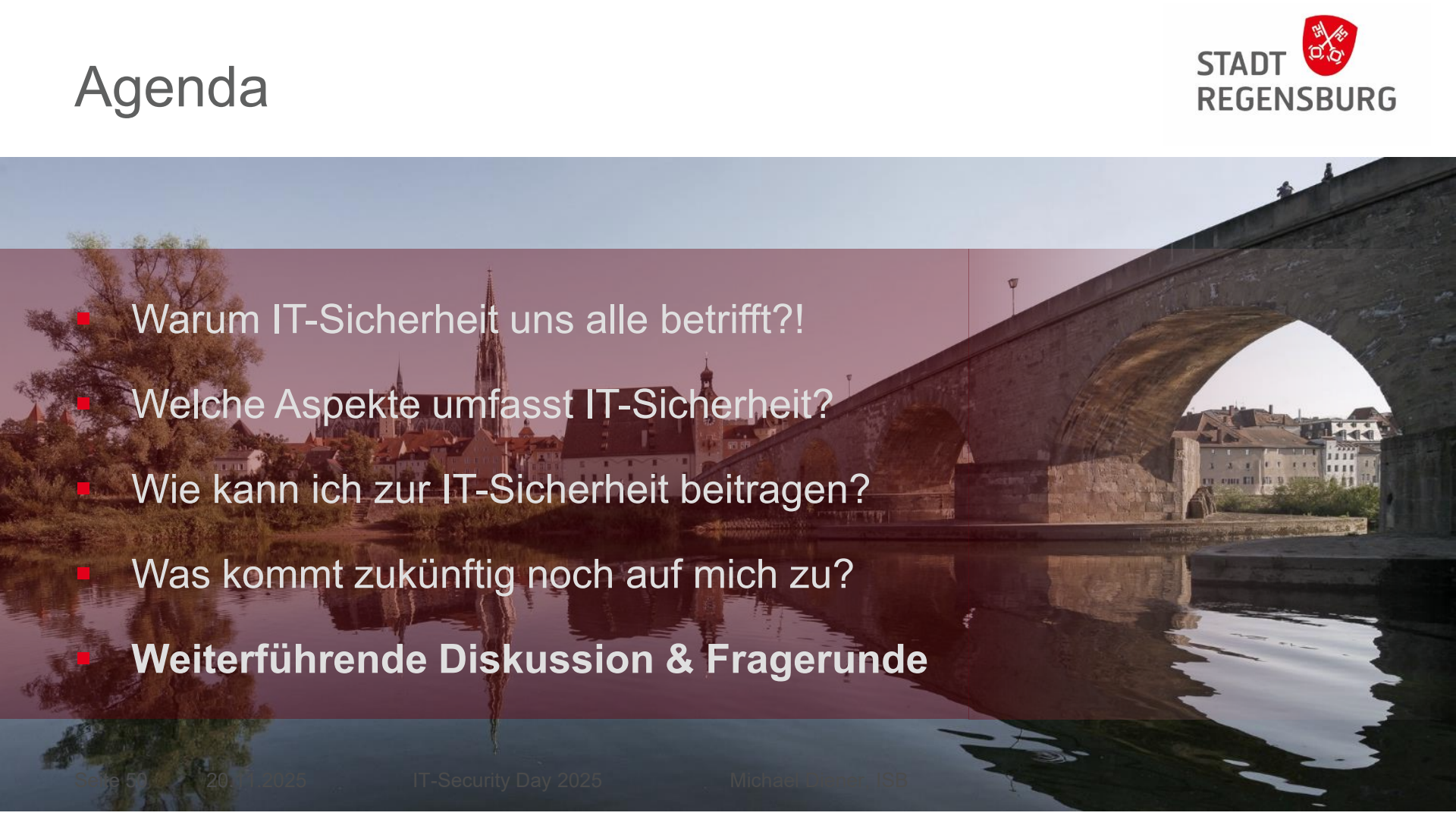
- URL von Cloud-Services immer sehr genau prüfen!
- Besser eigenen Favoriten-Link nutzen!
- Bei irrtümlicher PW-Übermittlung: PW sofort ändern und ggf. HelpDesk informieren!



- ISB frühzeitig einbinden bei IoT-Projekten und OT-Vernetzungen
- IoT- und OT-Netz ggf. abschotten vom regulären IT-Netz
- Neue Verantwortlichkeiten festlegen

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschrift/IT-GS-Kompilium_Einzel_PDFs_2023/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

Agenda

- 
- Warum IT-Sicherheit uns alle betrifft?!
 - Welche Aspekte umfasst IT-Sicherheit?
 - Wie kann ich zur IT-Sicherheit beitragen?
 - Was kommt zukünftig noch auf mich zu?
 - **Weiterführende Diskussion & Fragerunde**



Vielen Dank für Ihre Aufmerksamkeit!

→ Fragen und Diskussionsrunde



Stadt Regensburg

Michael Diener

Informationssicherheitsbeauftragter

Telefon: 0941/507-1172

E-Mail: it-sicherheit@regensburg.de

Security-Check für Web-Accounts



- Wann habe ich mein Passwort für Web-Mail, Amazon, Instagram, etc. zuletzt geändert?
- Wie stark sind meine Passwörter mit Blick auf Zeichenlänge, Zahlen, Groß-/Kleinschreibung und Sonderzeichen?
- Warum habe ich noch keine Zwei-Faktor-Authentifizierung (2FA) aktiviert?
- Welche Passwörter meiner IT-Accounts wurden bereits geleakt?
→ <https://haveibeenpwned.com> oder <https://sec.hpi.de/ilc>