STADT REGENSBURG

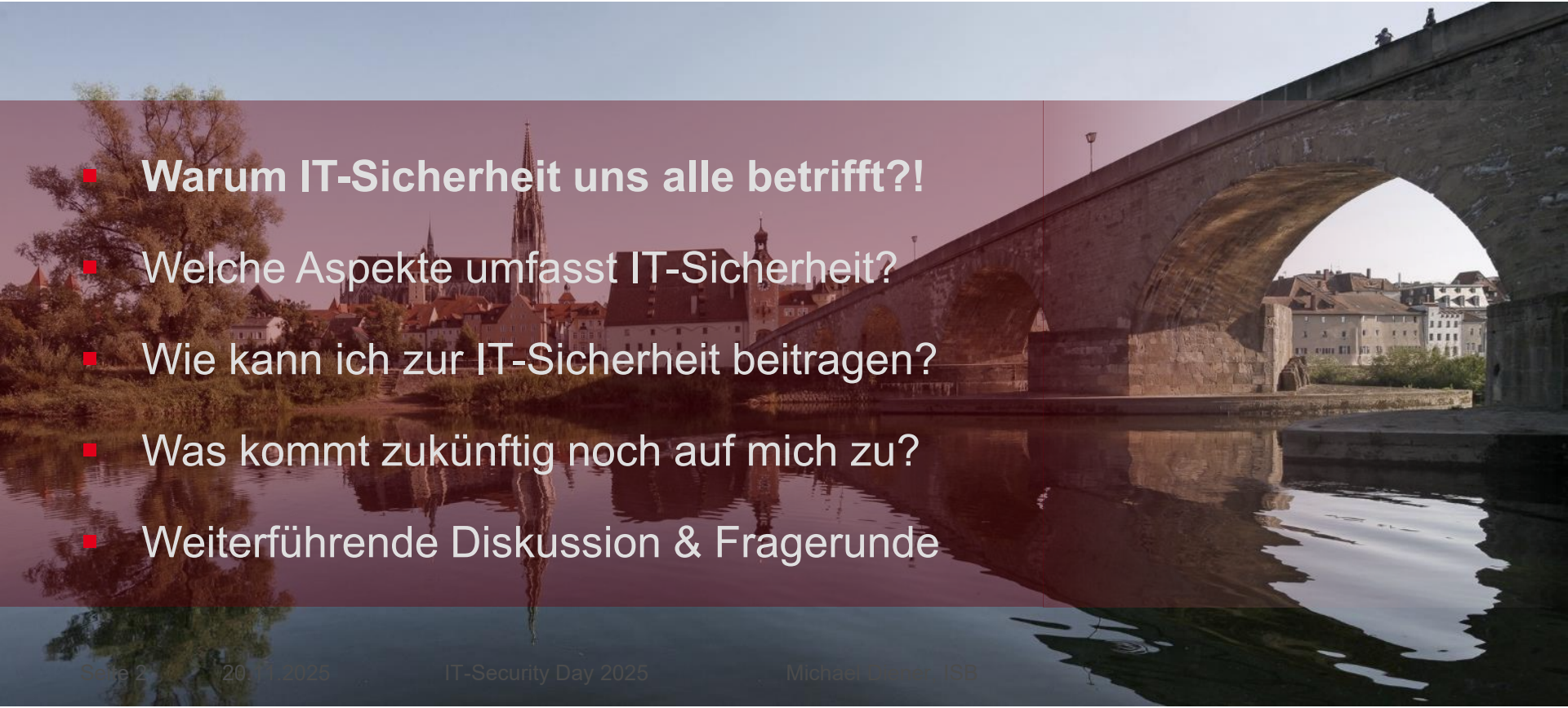
Kleines 1x1 der IT-Sicherheit

IT-Security Day // 20. November 2025

Michael Diener
Informationssicherheitsbeauftragter

Agenda

STADT REGENSBURG



- **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.

Anzeige aufgeben ePaper Abo

Dienstag, 18.11.2025

Westfälische Nachrichten

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 Abo testen Anmelden

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.

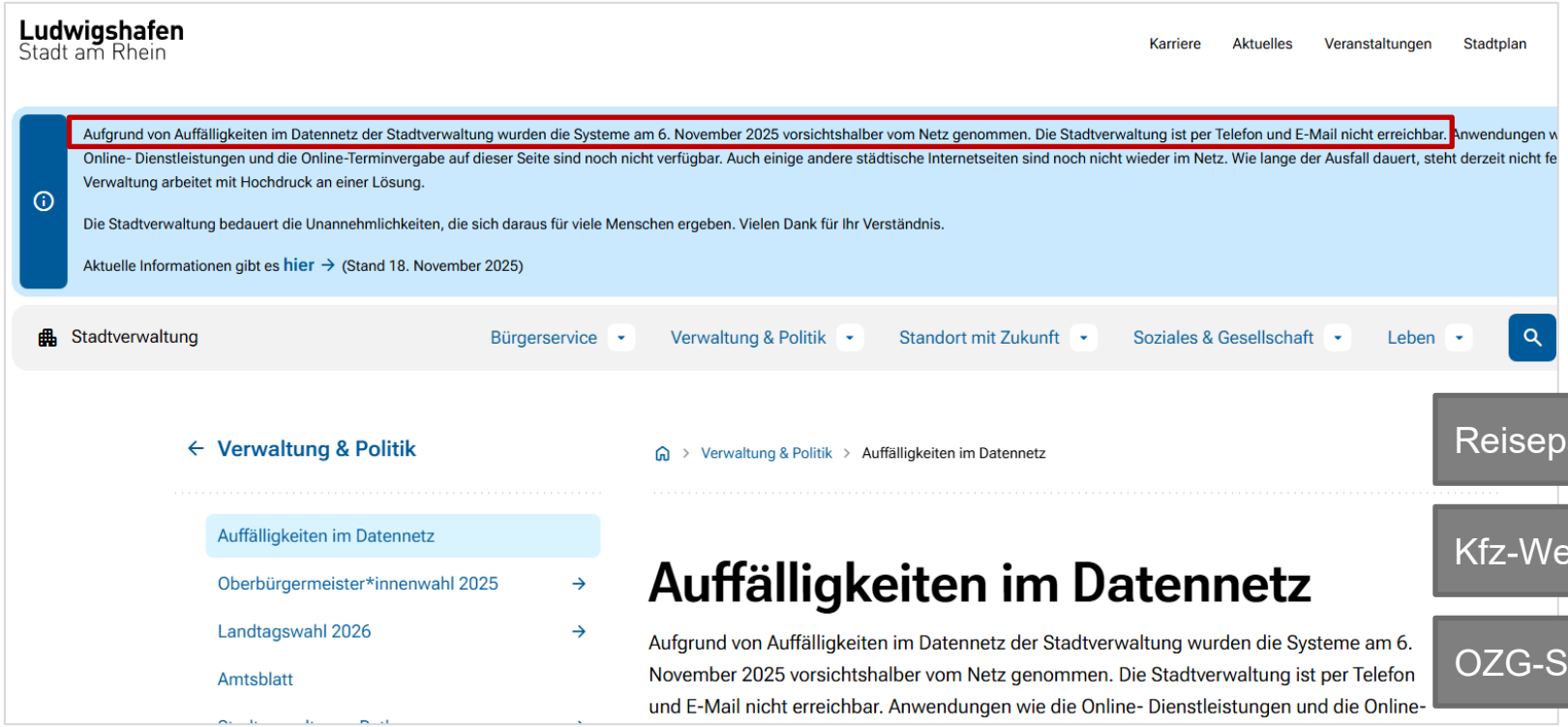
14. Februar 2025 um 09:09 Uhr / Marc Stöckel

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 …



Reisepass?

Kfz-Wechsel?

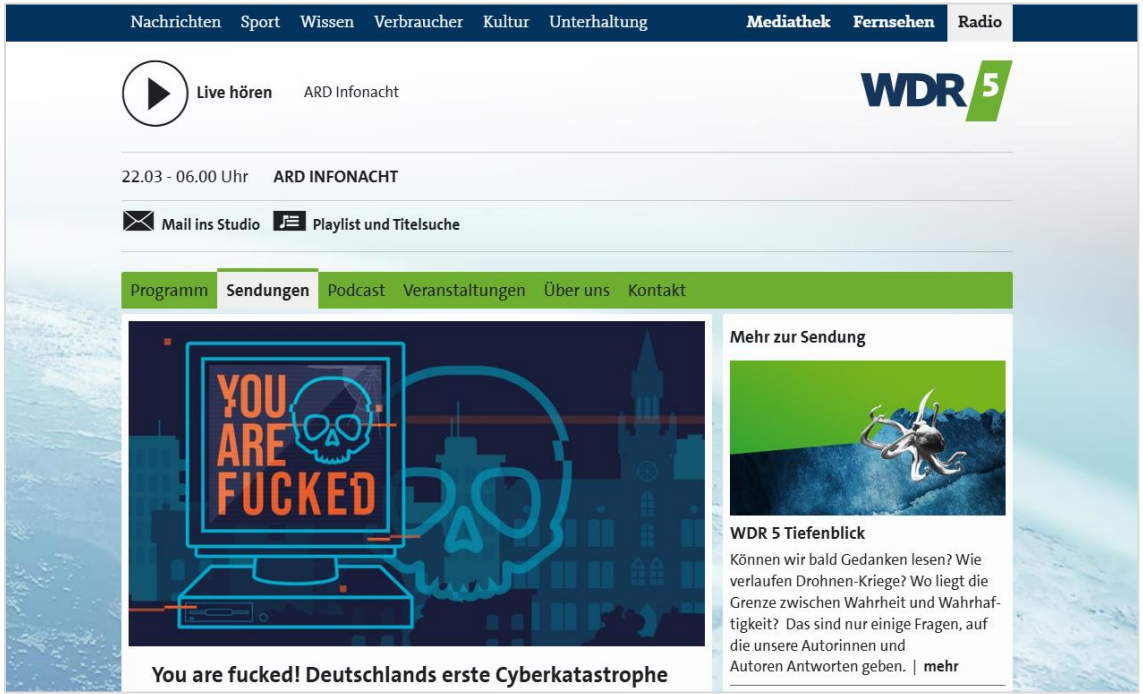
OZG-Services?

https://ludwigshafen.de/verwaltung-politik/datennetz

Kommunaler Notbetrieb: Das Lagebild, das es nicht gibt.

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

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



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.

STADT REGENSBURG

Vertraulichkeit

Unberechtigte haben Zugangsdaten erbeutet und Daten eingesehen

Verfügbarkeit

Dateien und Server wurden verschlüsselt mittels Ransomeware

Integrität

Unberechtigte konnten (unbemerkt) Dateien manipulieren

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

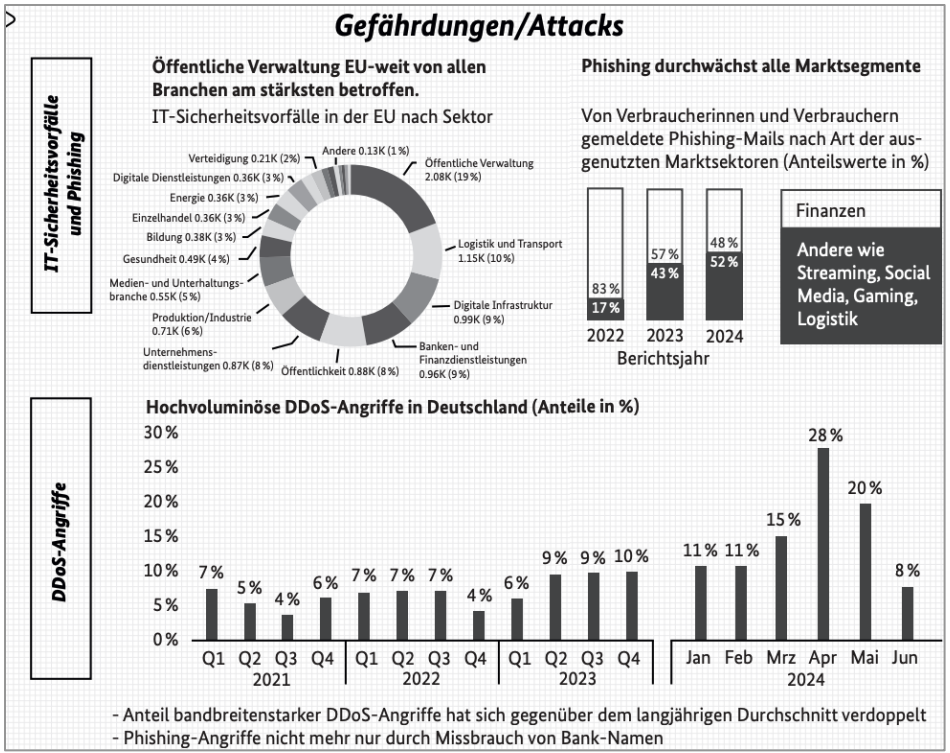
Die Ursachen von Cyberangriffen sind vielfältig.

STADT REGENSBURG

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?“

BSI-Lagebild 2024

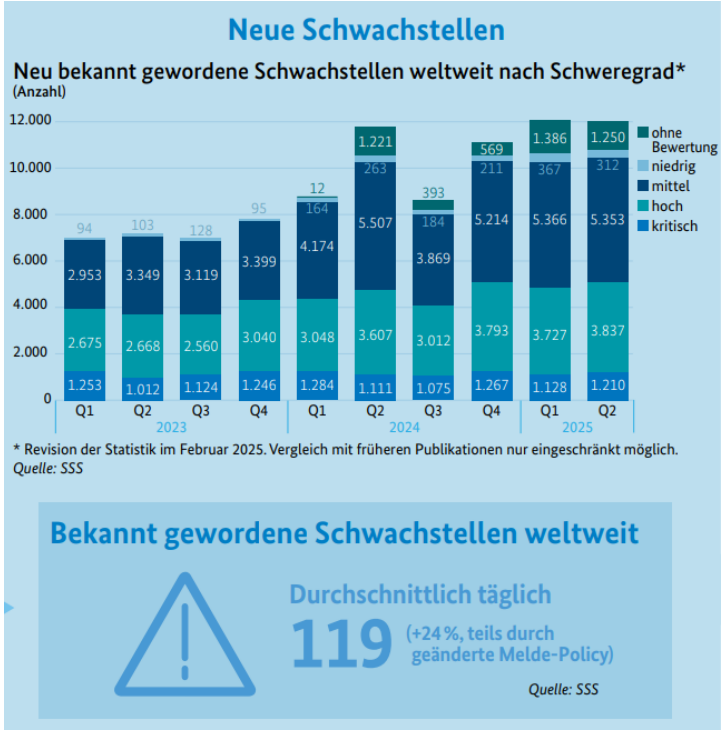


Top-Gefährdungen:

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

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024-Doppelseite.pdf?__blob=publicationFile&v=4

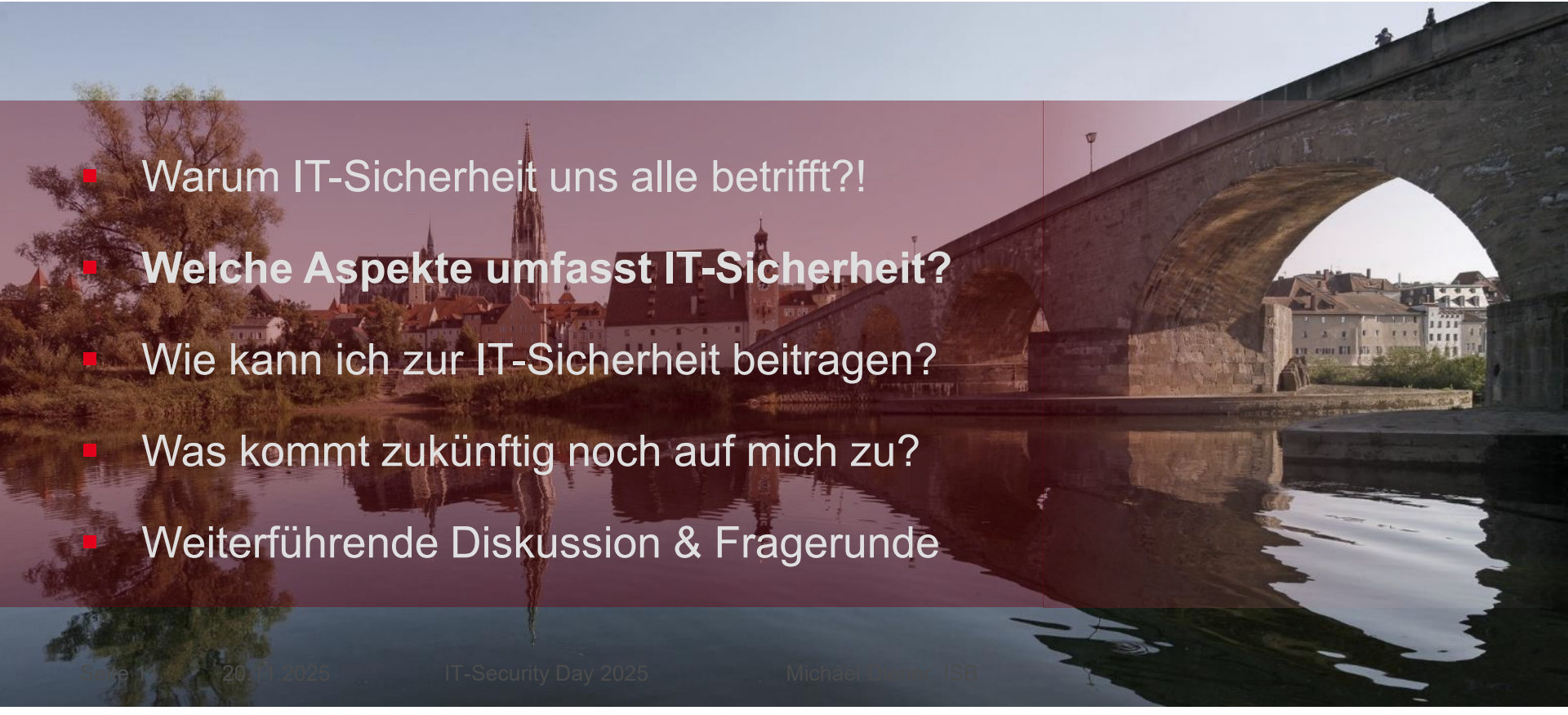
BSI-Lagebild 2025 / Cybersicherheit in Bayern 2025



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

Agenda

STADT REGENSBURG

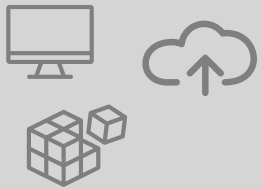


- Warum IT-Sicherheit uns alle betrifft?!
- **Welche Aspekte umfasst IT-Sicherheit?**
- Wie kann ich zur IT-Sicherheit beitragen?
- Was kommt zukünftig noch auf mich zu?
- Weiterführende Diskussion & Fragerunde

Was umfasst Informationssicherheit?

STADT REGENSBURG

- 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.)
- …

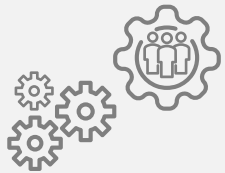
Daten-Sicherheit

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

Infrastruktur-Sicherheit

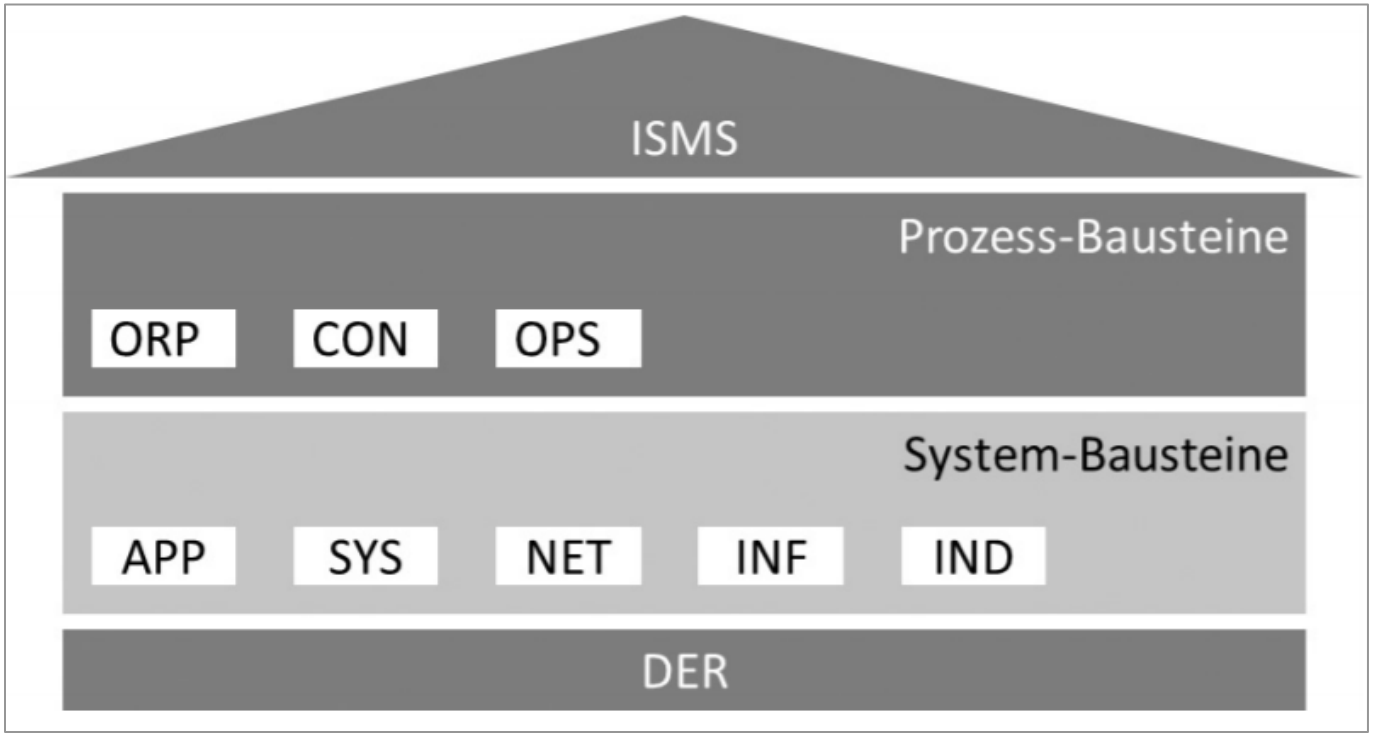
- Vorgaben bzgl. der Aktualität von IT-Dokumentationen,
- Koordination Awareness-Schulungen,
- Schwachstellenmanagement,
- Prozessaudits / Penetrationstests, …

Informationssicherheit



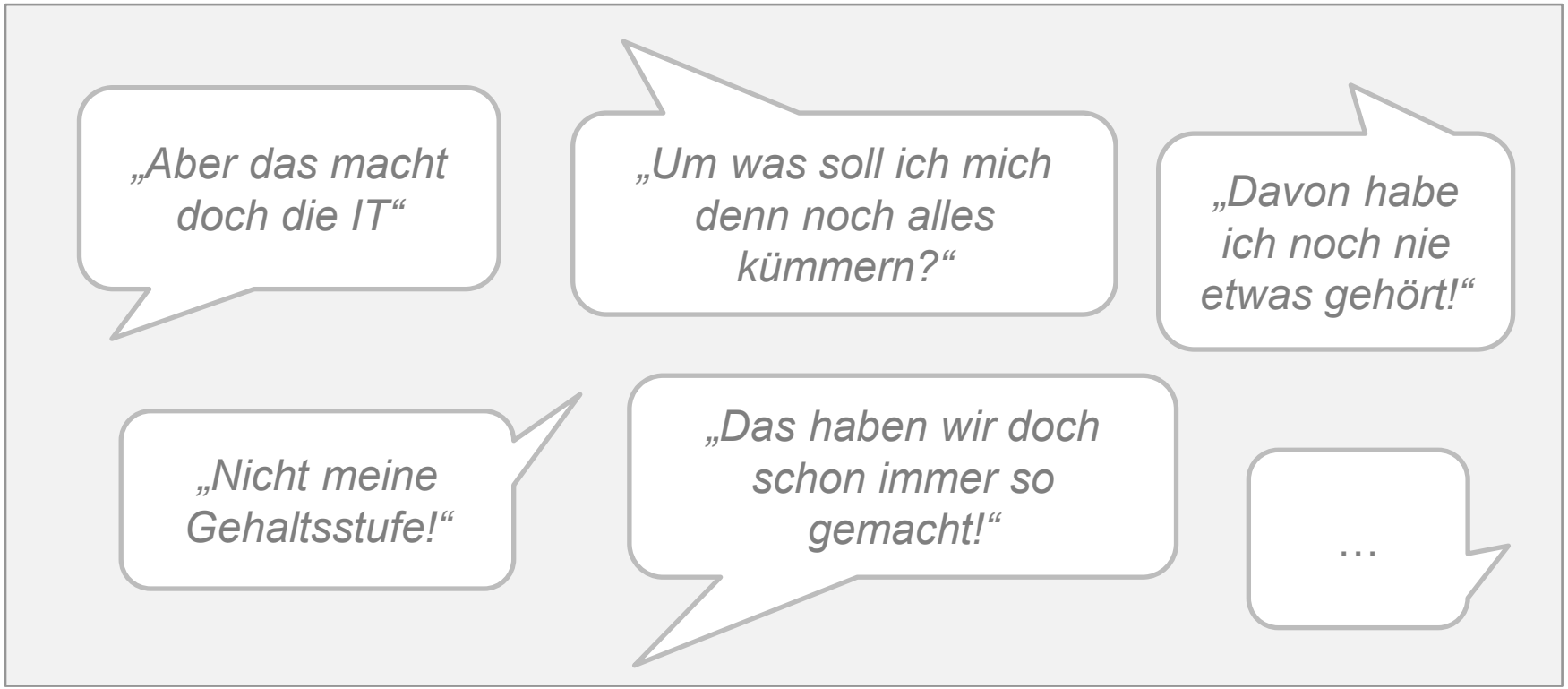
Quelle: eigene Darstellung

Übersicht: BSI IT-Grundschutz-Bausteine



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

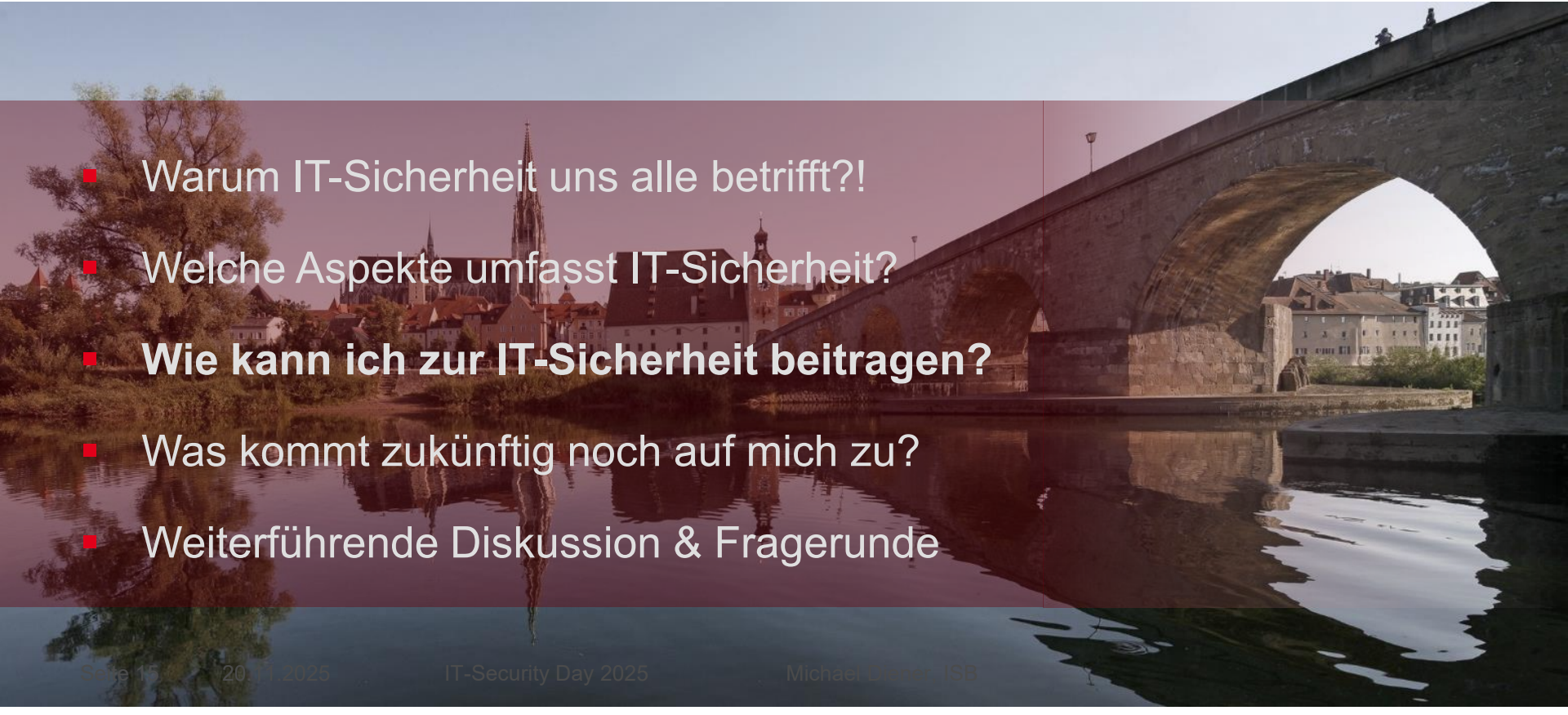
Informationssicherheit betrifft **JEDEN!**



Quelle: eigene Darstellung

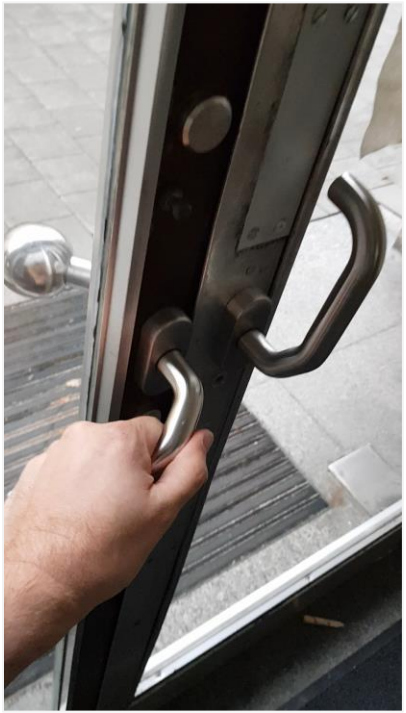
Agenda

STADT REGENSBURG



- 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

Infrastruktur-Sicherheit in Gebäuden und Büros



Quelle: Stadt Regensburg

- 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!

Infrastruktur-Sicherheit in Gebäuden und Büros

STADT REGENSBURG

Quelle: Stadt Regensburg

IT-Sicherheit mit USB-Sticks

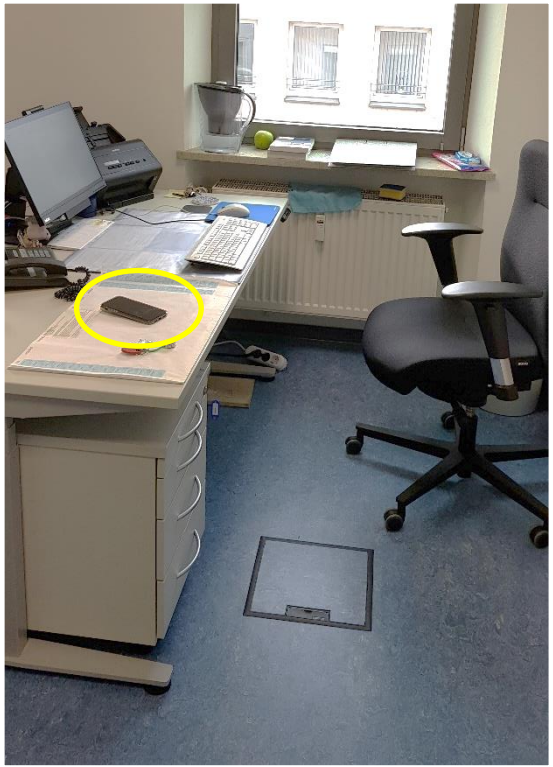
- **Verdächtige USB-Sticks <u>niemals</u>** an ungeschützte IT-Hardware anschließen!
- **IT-Sicherheitsrichtlinien** der Organisation beachten bzgl. Nutzung von USB-Sticks!
- Bei Bedarf auf USB-Sticks eine sichere **Verschlüsselung aktivieren**, z. B. zip-Datei mit Passwort konfigurieren.

Quelle: Stadt Regensburg

IT-Sicherheit von mobilen Endgeräten

STADT REGENSBURG

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



Quelle: Stadt Regensburg

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

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

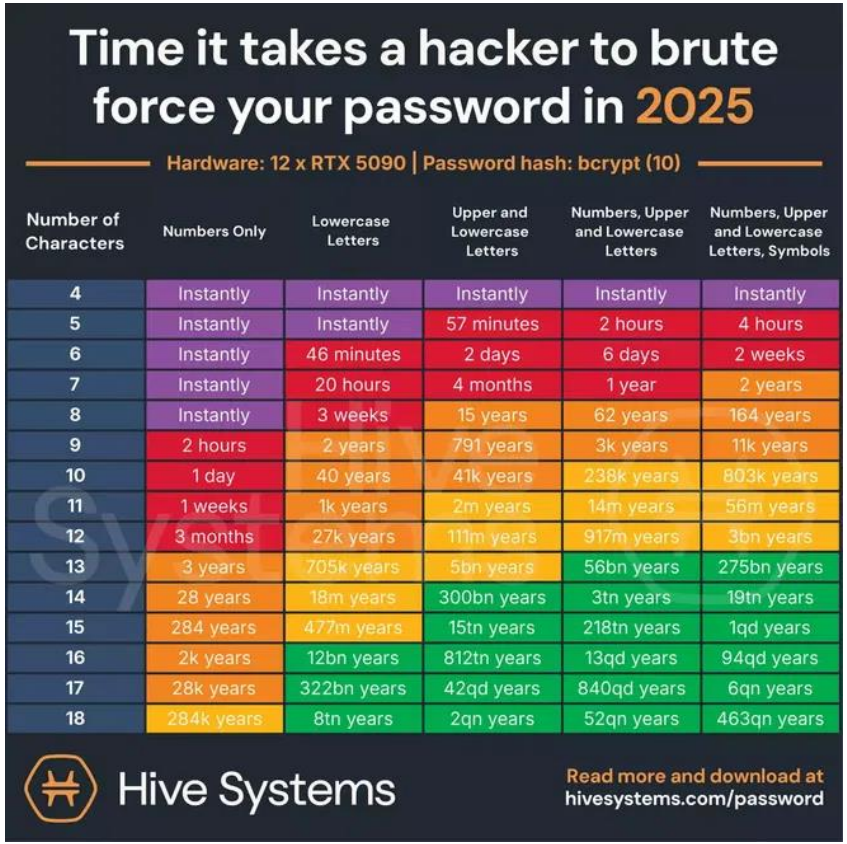
Was sehen starke Passwörter aus?

STADT REGENSBURG

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.

PDF 54 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

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/2VV5hmgHlVs

Merkhilfe: starke Passwörter ■□□

STADT REGENSBURG

- **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 □■□

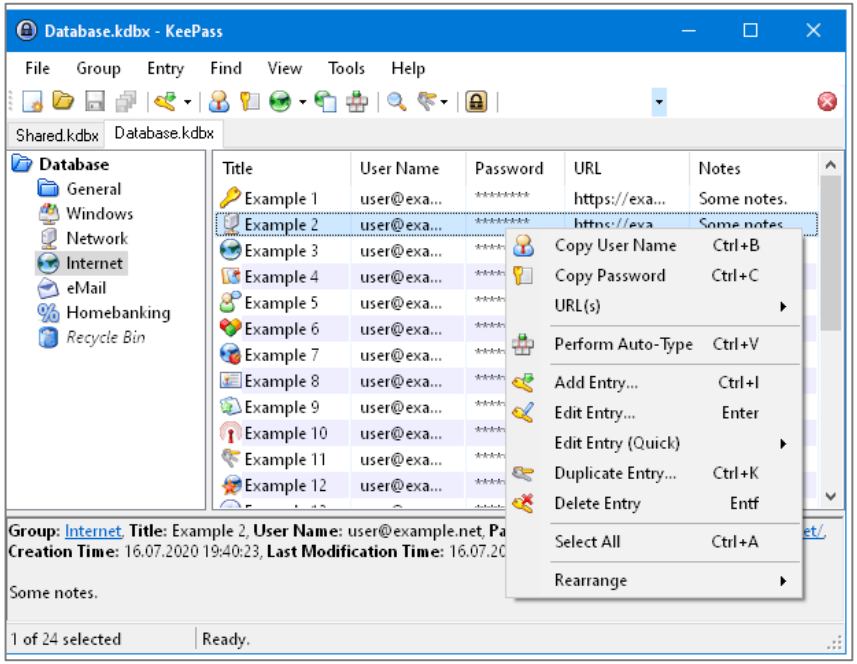
- **Methode II: Ganze Merksätze verwenden**
  1. Einen guten Merksatz ausdenken

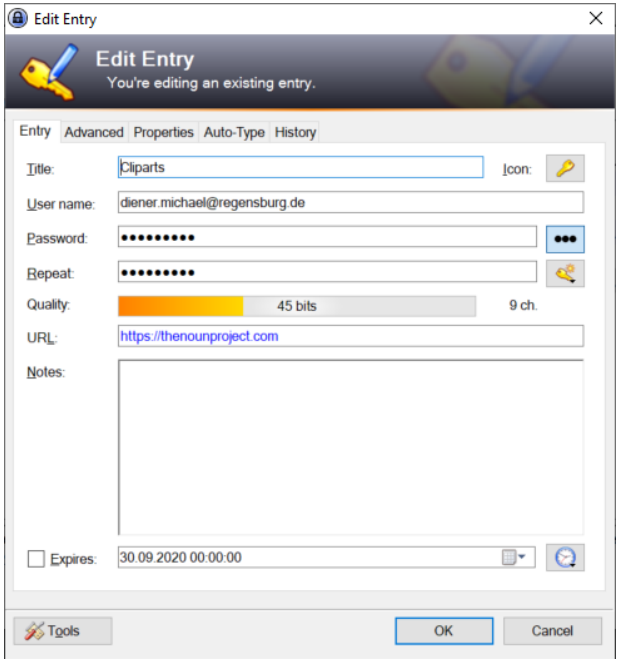
     „Ich jogge gerne um 18 Uhr an der Donau.“

```
Ich jogge gerne um 18 Uhr an der Donau.
```

Merkhilfe: starke Passwörter □□■

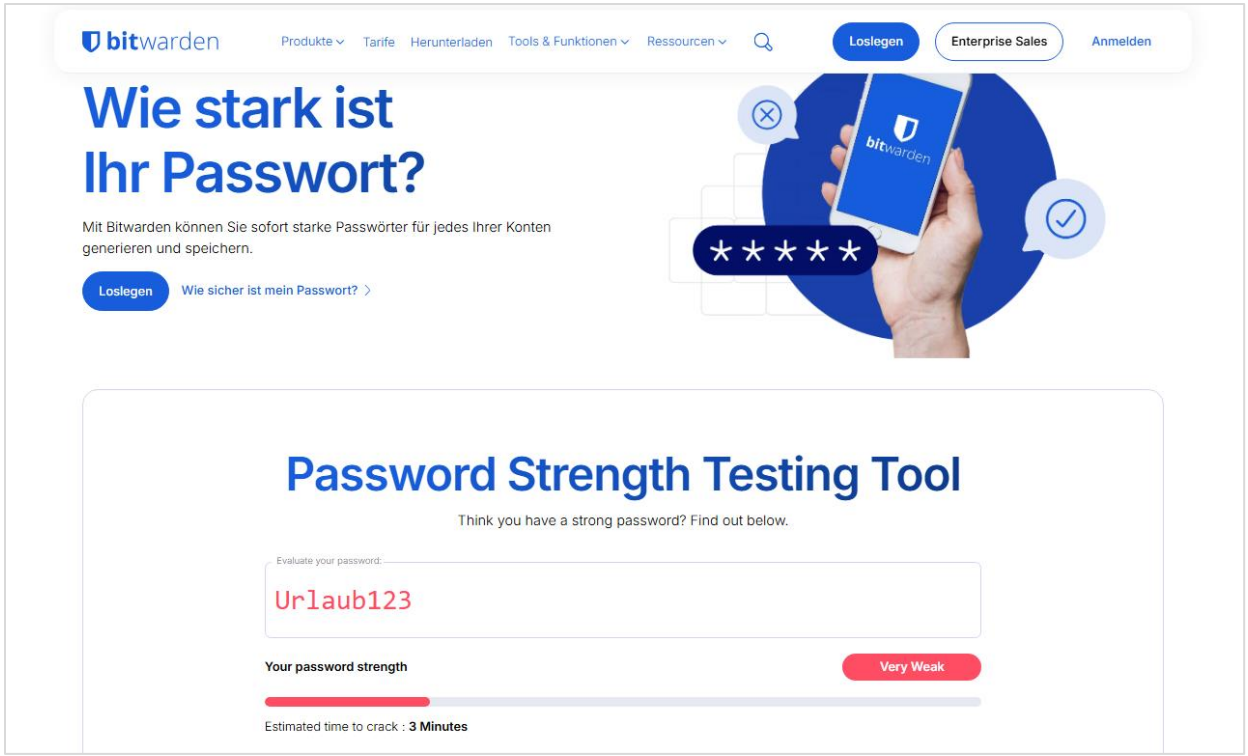
- **Methode III: Passwort-Manager-Tool**





https://keepass.info/

Überprüfung der Passwort-Qualität



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)

STADT REGENSBURG

SMS-Code / Anruf

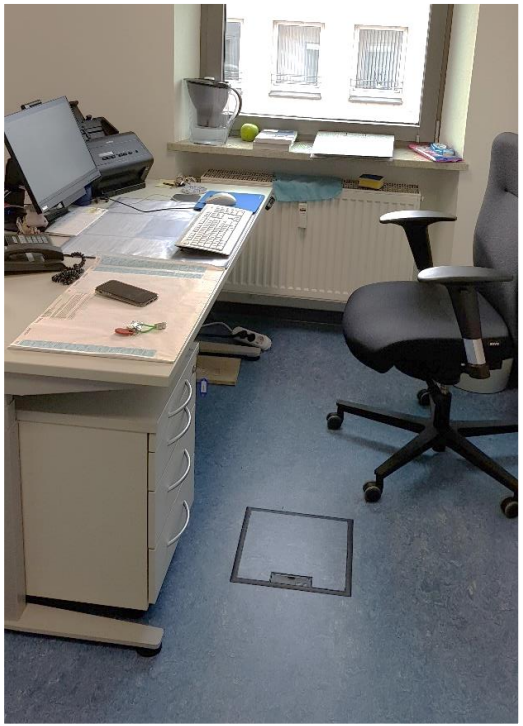
E-Mail-Link

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!

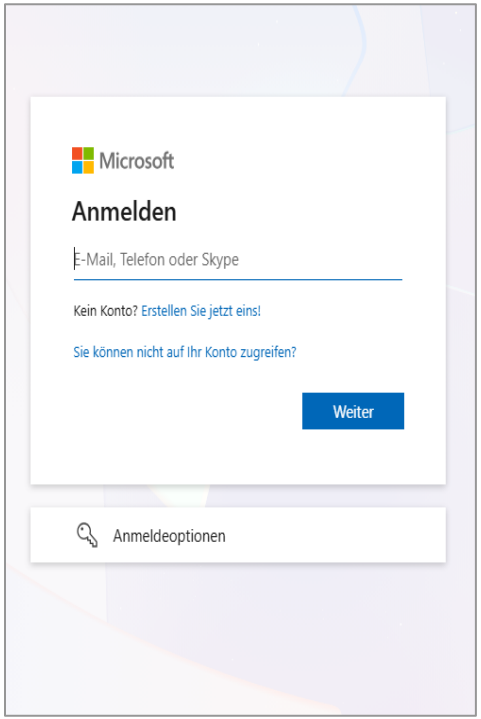
2FA-Token sorgsam nutzen.

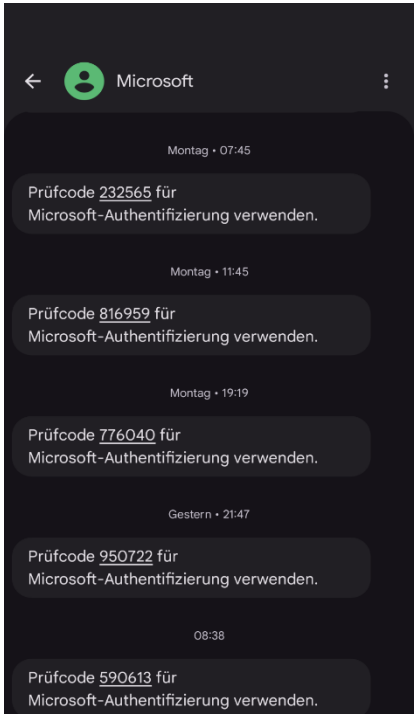


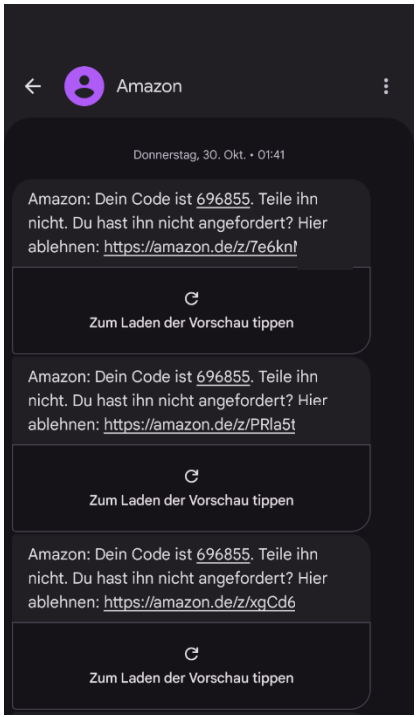
- Chipkarten nicht über Nacht im Lesegerät stecken lassen!

Quelle: Stadt Regensburg

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



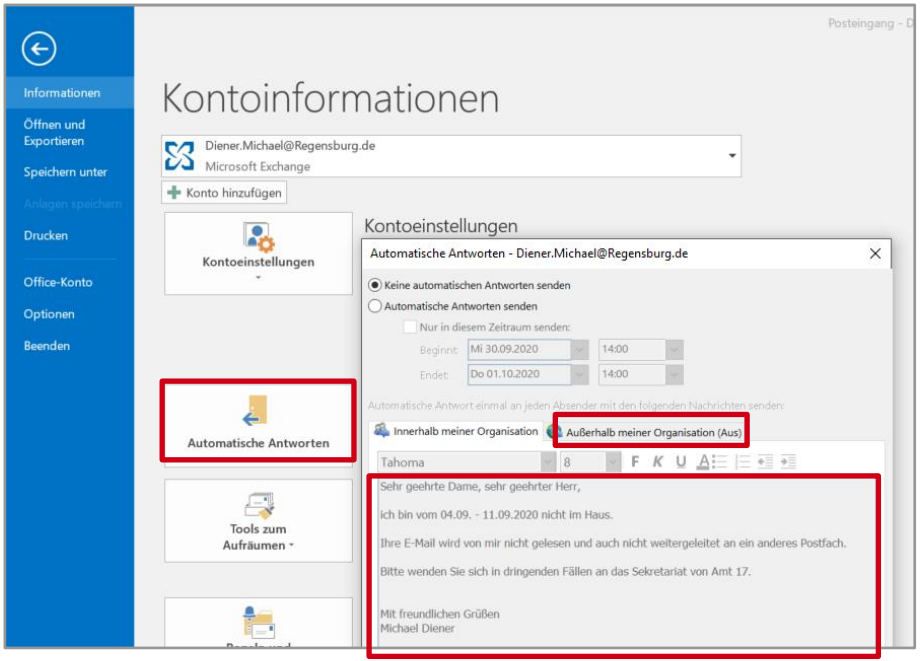




- Keine Panik!
- Nicht überhastet Links klicken!
- URL prüfen!!!
- Passwort ggf. ändern im Web-Service!

Quelle: Stadt Regensburg, Privat.

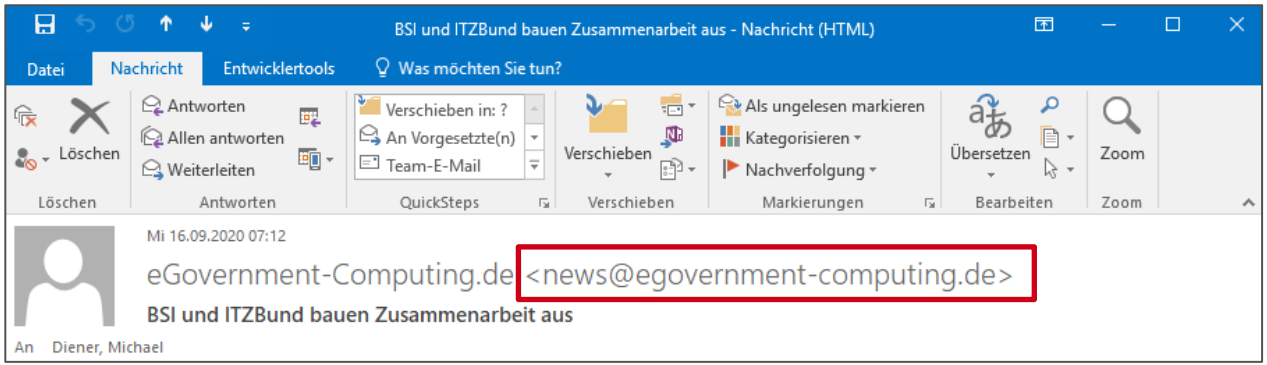
E-Mail Sicherheit ■□



- 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.).

Quelle: Stadt Regensburg

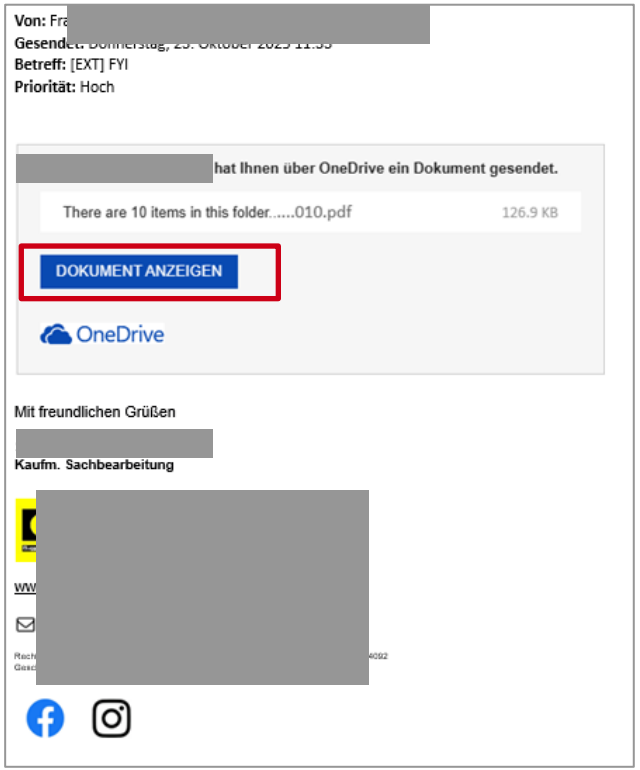
E-Mail Sicherheit



- 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

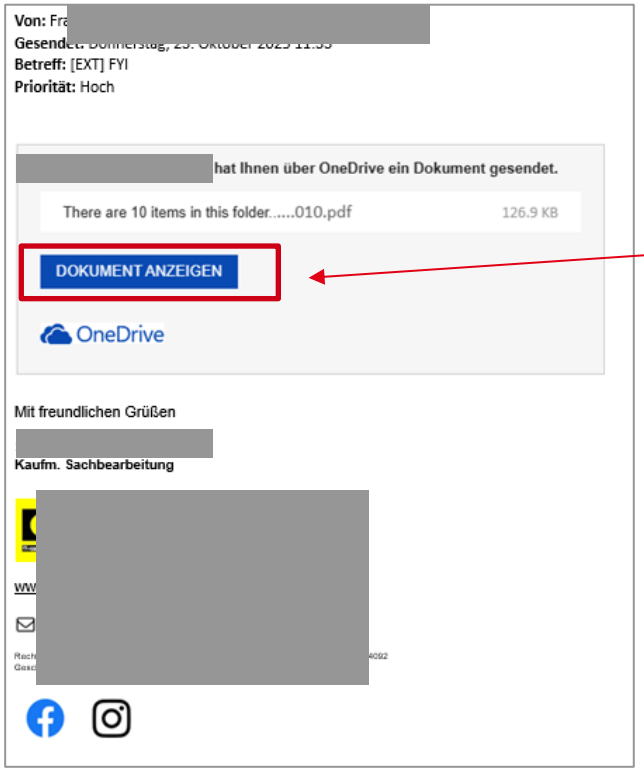
E-Mail Sicherheit: Gefährliche Links



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



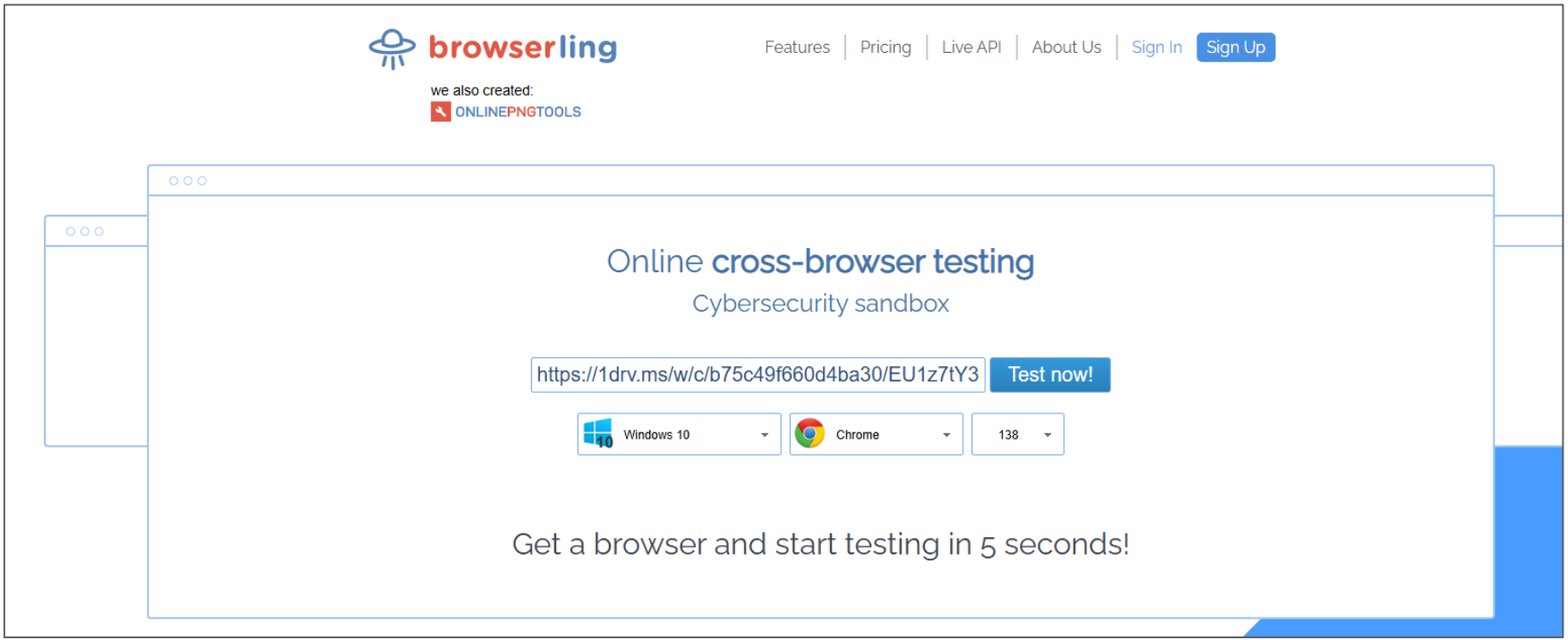
https://1drv.ms/w/c/b75c49f660d4ba30/EU1z7tY3xBJGjyUlX0GDrOMBloi6eJy9-E0WxPHbKm9q5g?e=xlwNCP&CT=1763549991371&OR=Outlook-Body&CID=DD170253-377F-4933-92F6-B62C3C0A4ED9&wdLOR=cACED81C5-93D8-4F07-8474
Klicken oder Tippen Sie, um den Link zu folgen

- 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

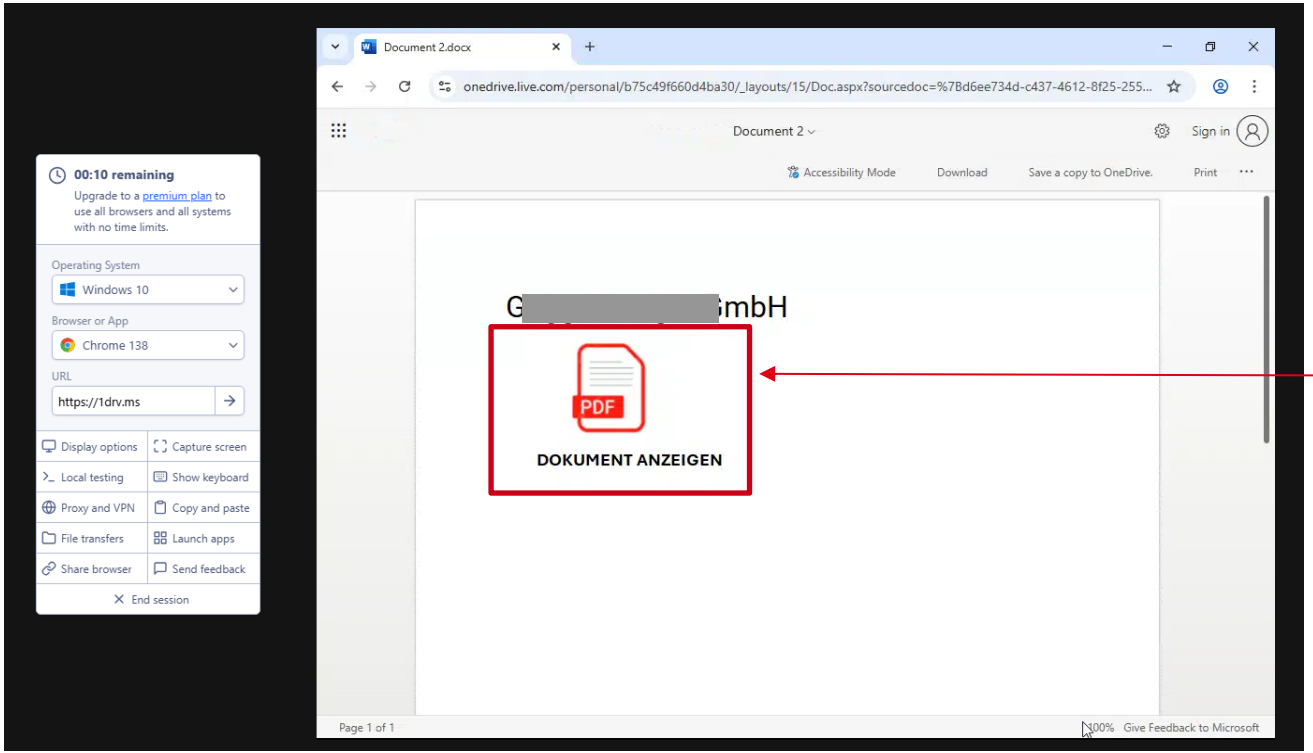
Sandbox-Browser: Verdächtige Links untersuchen

STADT REGENSBURG



https://www.browserling.com/

Sandbox-Browser: Verdächtige Links untersuchen



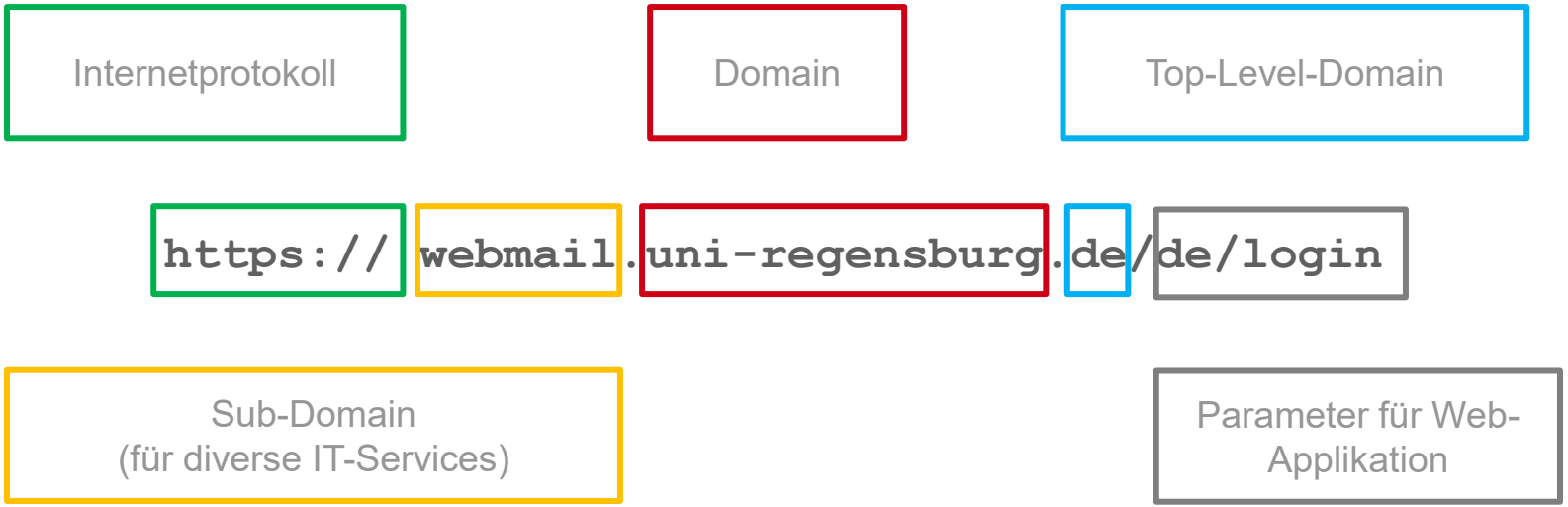
Dieser Fall ist klar!!!

Ein PDF-Dokument im Word-Dokument!

→ **E-Mail löschen!**

https://www.browserling.com/

EXKURS: URLs / Hyperlinks „lesen und verstehen“



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

Übung: Falsche Hyperlinks erkennen

STADT REGENSBURG

`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

STADT REGENSBURG

https://www.regensburg.**net**

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

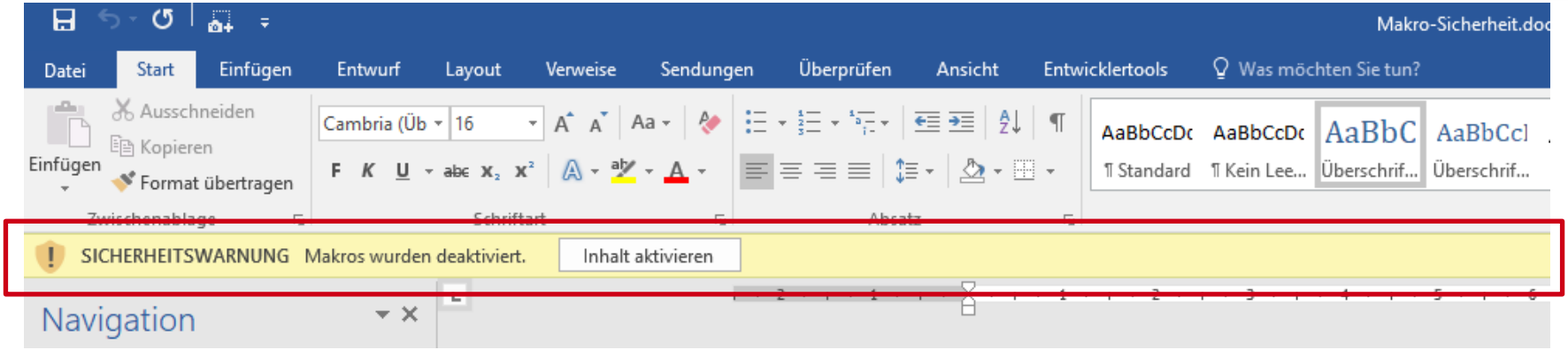
https://www.regensb**e**rg.de

https://www.regensburg.de/itportal

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

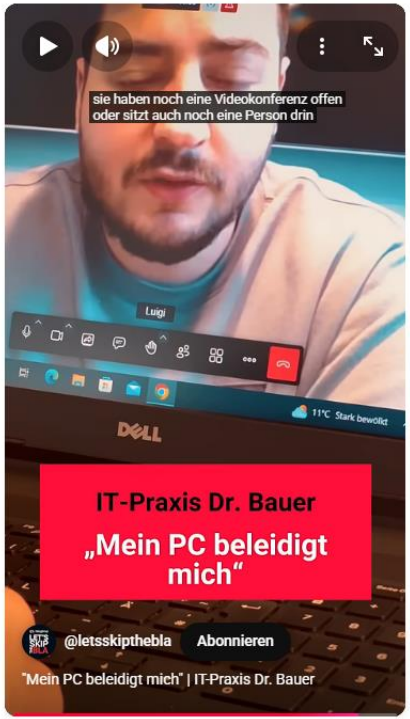
https://srv40.regensburg.de

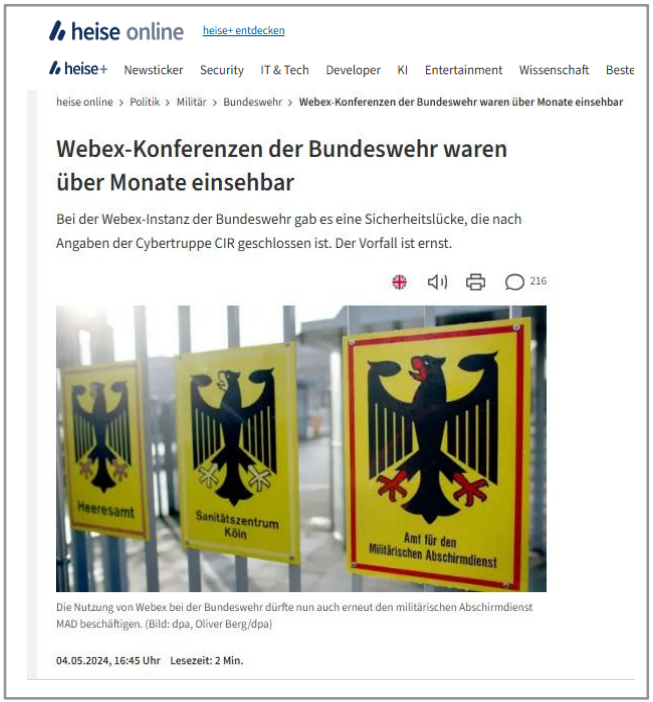
VBA-Makros in Microsoft Office-Dateien



- Achtung: VBA-Makros können schadhaften 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





heise online heise+ entdecken

heise+ Newsticker Security IT & Tech Developer KI Entertainment Wissenschaft Beste

heise online > Politik > Militär > Bundeswehr > Webex-Konferenzen der Bundeswehr waren über Monate einsehbar

Webex-Konferenzen der Bundeswehr waren über Monate einsehbar

Bei der Webex-Instanz der Bundeswehr gab es eine Sicherheitslücke, die nach Angaben der Cybertruppe CIR geschlossen ist. Der Vorfall ist ernst.

216

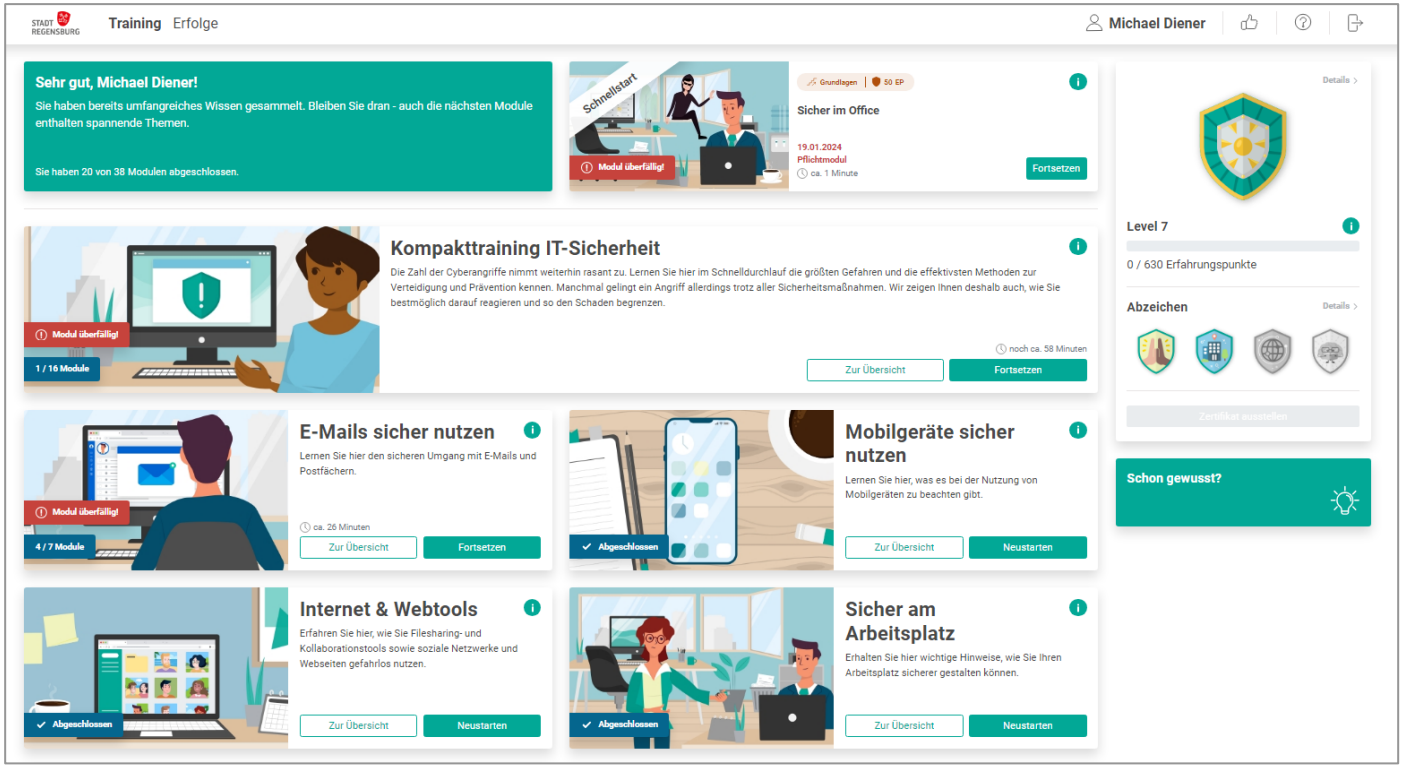
Die Nutzung von Webex bei der Bundeswehr dürfte nun auch erneut den militärischen Abschirmdienst MAD beschäftigen. (Bild: dpa, Oliver Berg/dpa)

04.05.2024, 16:45 Uhr Lesezeit: 2 Min.

- 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/B6GZqcykrgo
https://www.heise.de/news/Webex-Konferenzen-der-Bundeswehr-waren-ueber-Monate-einsehbar-9708307.html

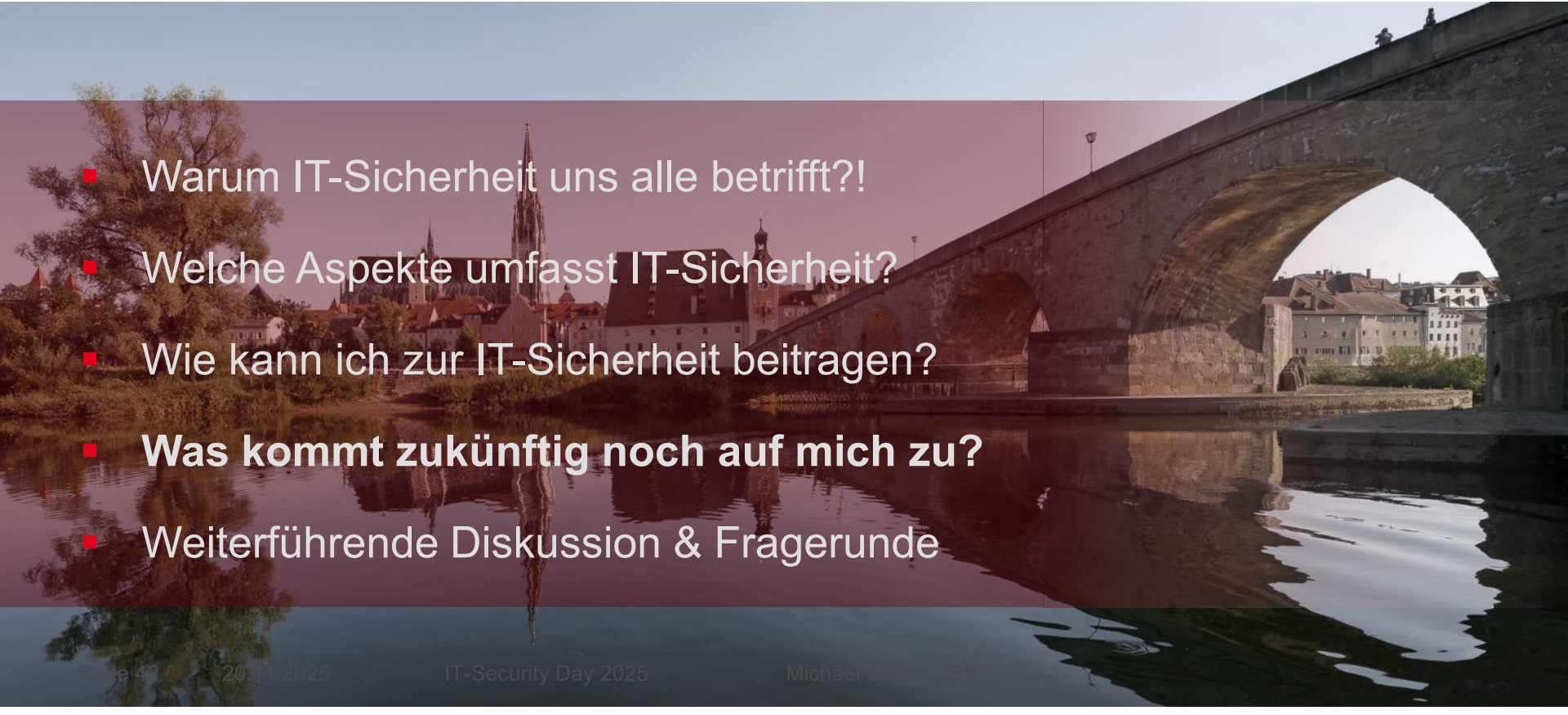
SECURITY-AWARENESS-TRAINING



Quelle: SoSafe E-Learning-Plattform

Agenda

STADT REGENSBURG



- 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

STADT REGENSBURG

Misdirection (Ablenkung)

Time Pressure (Zeitdruck)

Social Proof (Gesellschaftliche Anpassung)

Opportunity (Gelegenheit)

Social Compliance (Respekt vor Autoritäten)

https://humanfirewallconference.com/de/on-demand

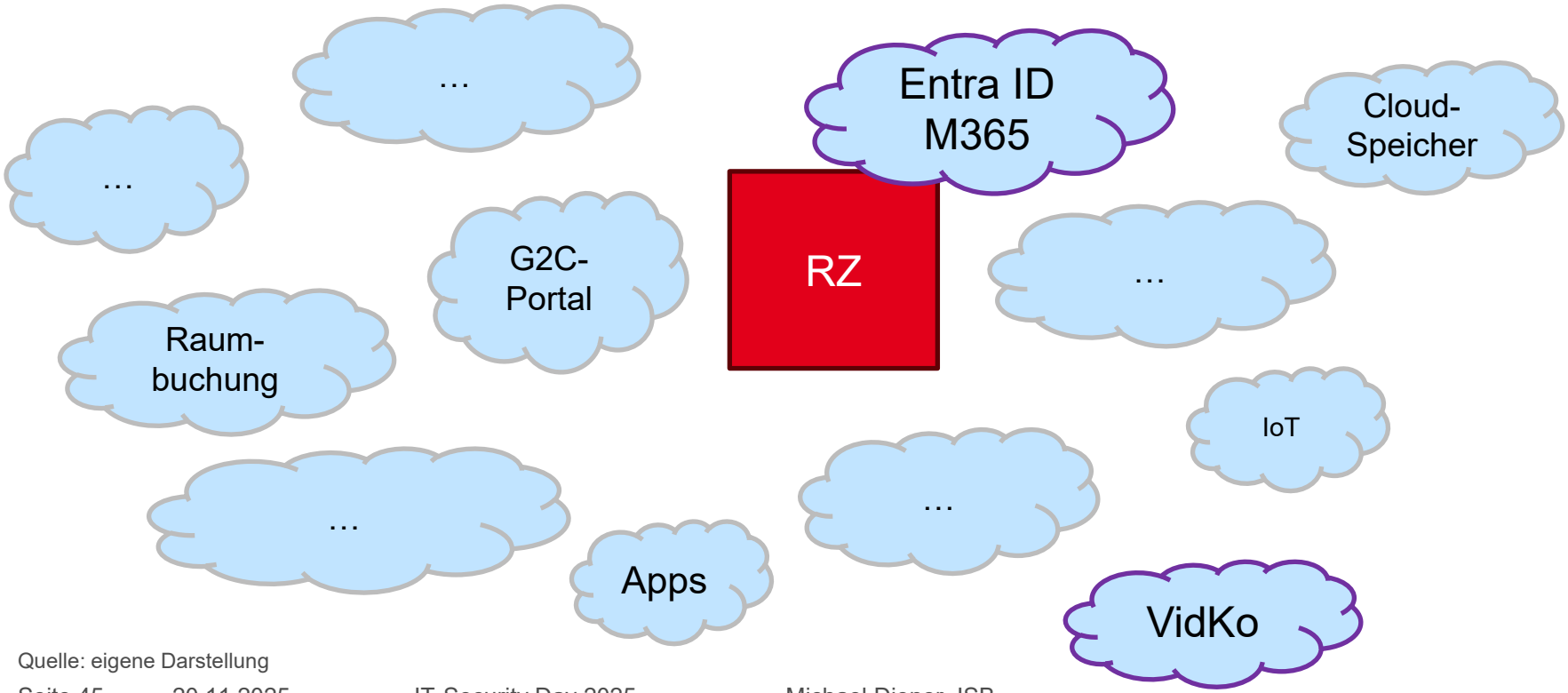
Alexis Conran – Scamproof your life. HufiCon 2025.

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
  - …

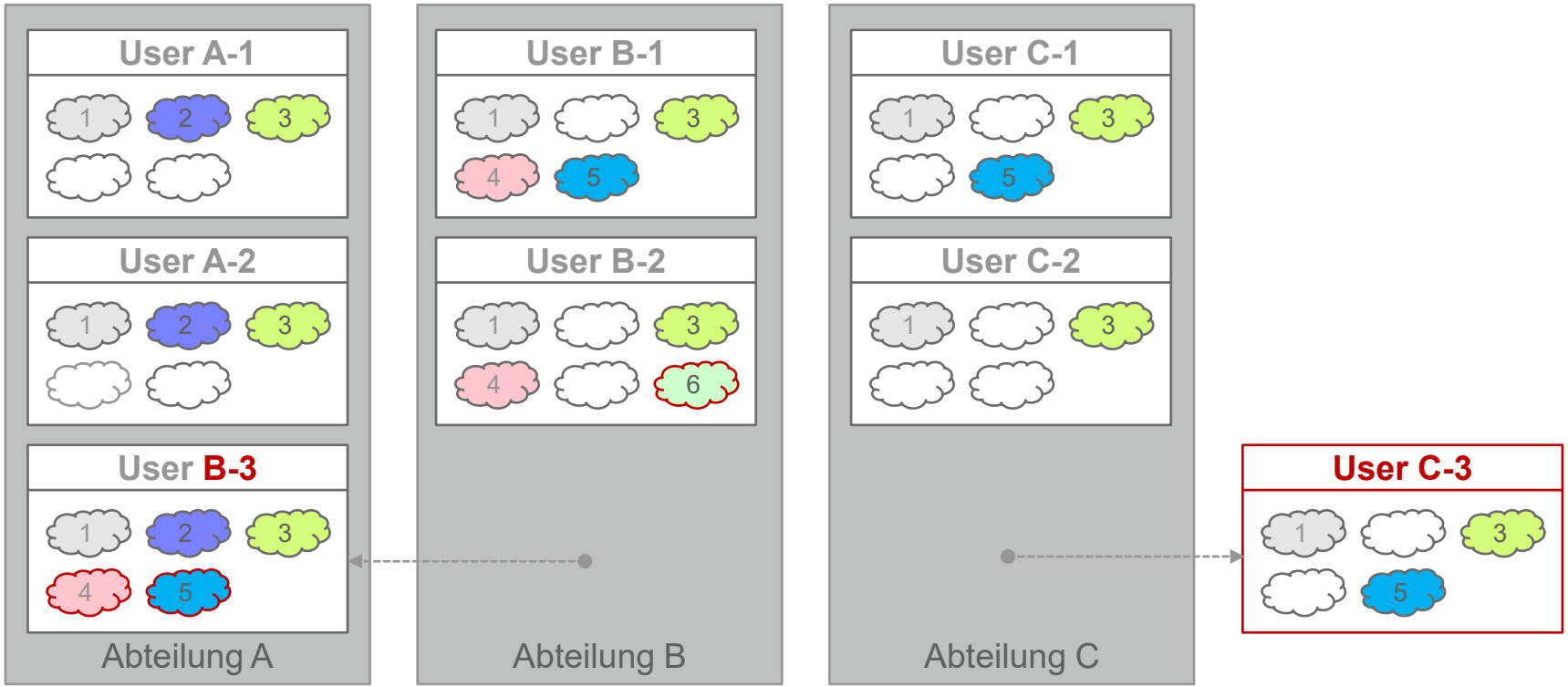
https://www.cloudflare.com/de-de/learning/email-security/business-email-compromise-bec

Zunehmend mehr Public-Cloud-Services in öffentlichen Verwaltungen



Quelle: eigene Darstellung

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



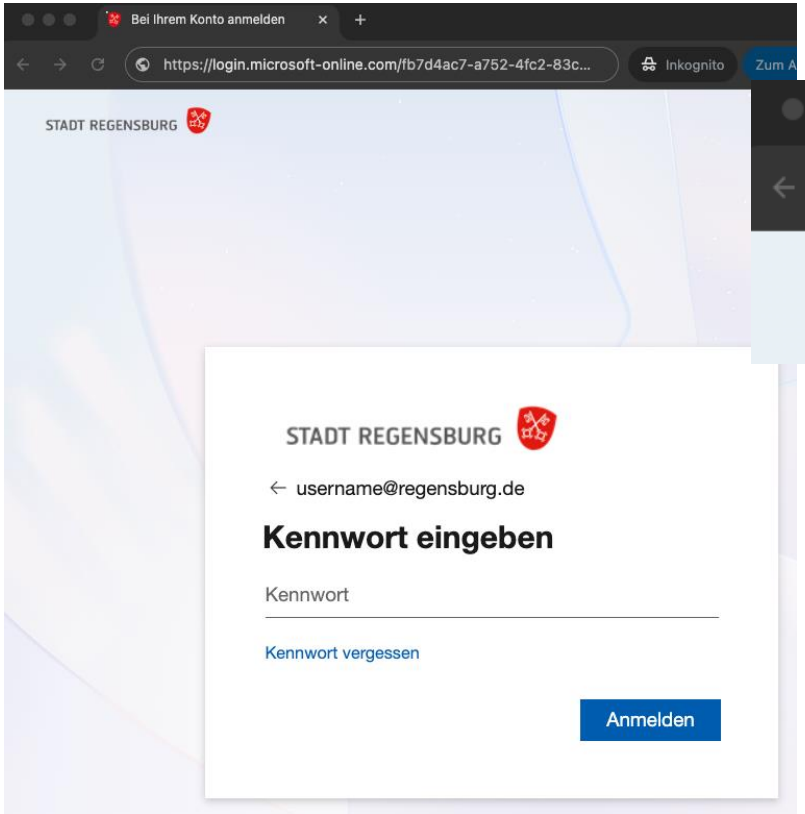
Quelle: eigene Darstellung

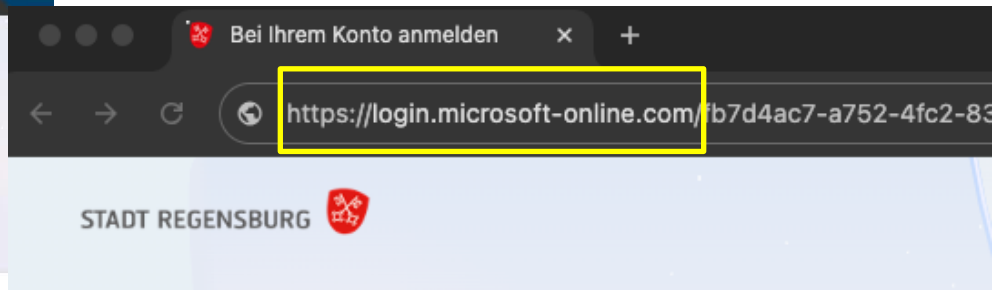
Sichere Bedienung von GenAI-Tools

- 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





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

Sichere Steuerung von IoT- & OT-Systemen


Bundesamt
für Sicherheit in der
Informationstechnik

IND.1 Prozessleit- und Automatisierungstechnik

1. **Beschreibung**

1.1. Einleitung

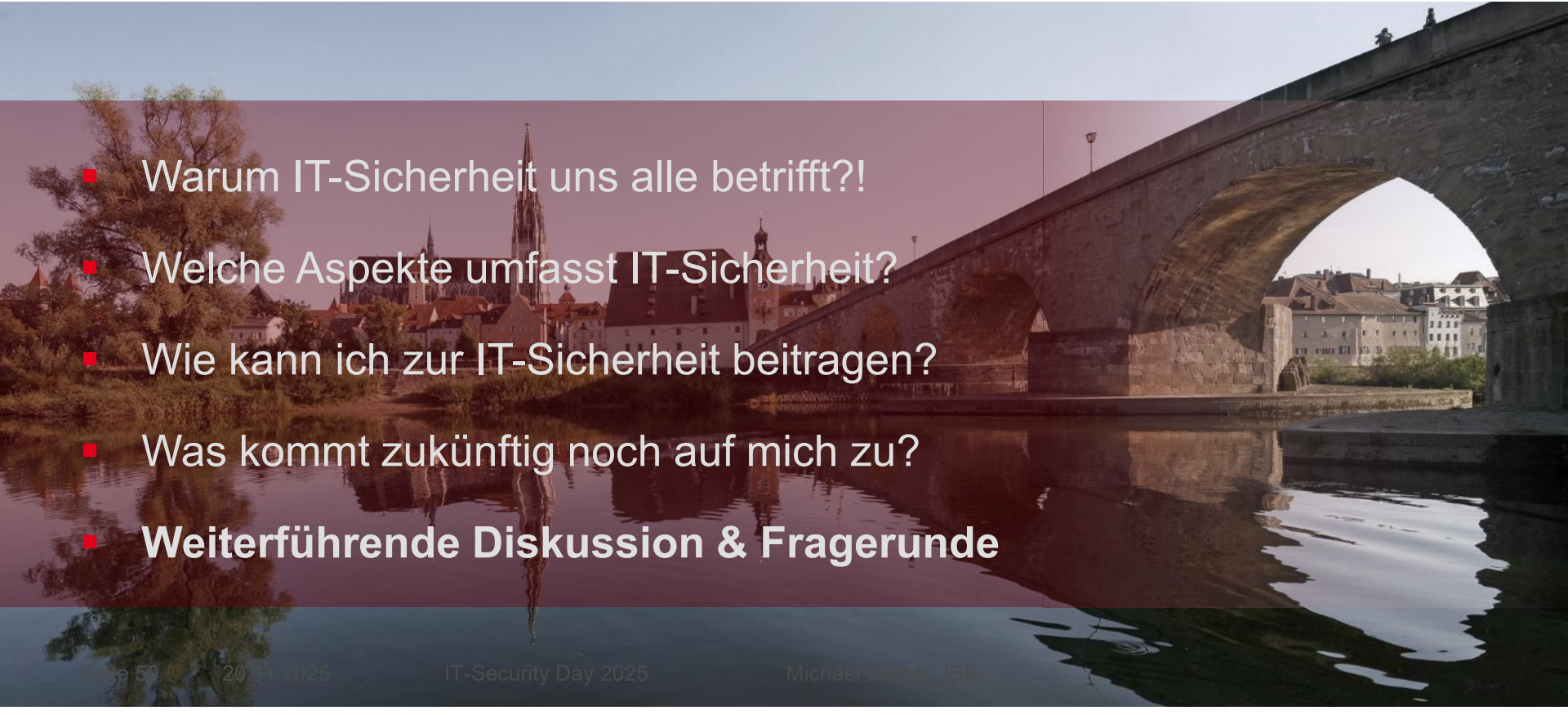
Prozessleit- und Automatisierungstechnik (Operational Technology, OT) ist Hard- und Software, die physische Geräte, Prozesse und Ereignisse in der Institution überwacht und steuert.

- 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/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/08_IND_Industrielle_IT/IND_1_Prozessleit_und_Automatisierungstechnik_Edition_2023.pdf?__blob=publicationFile&v=3#download=1

Agenda

STADT REGENSBURG



- 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

STADT REGENSBURG

- 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