

KI-basierte Lernplattform der nächsten Generation für mehr Cybersicherheit und IT-Awareness:

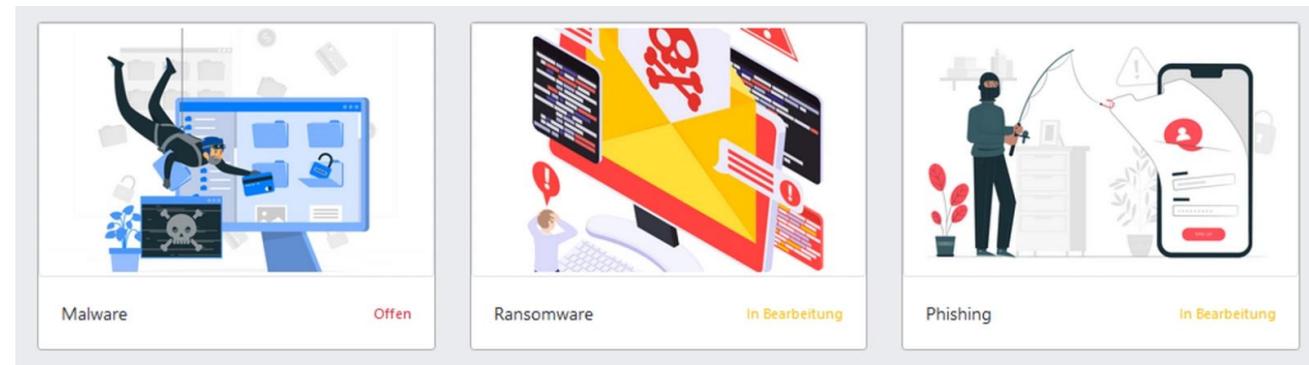
Können adaptive Lernumgebungen und mehr Personalisierung die Lernerfolge im IT-Awareness-Training steigern?

Ringvorlesung Cybersicherheit 2024

05.12.2024

Prof. Dr. Michael Massoth

Hochschule Darmstadt / EUT+ und ATHENE



h_da

hochschule
darmstadt
informatik

member of
eut+
EUROPEAN UNIVERSITY
OF TECHNOLOGY



digitales.hessen
DISTR@L



ATHENE
Nationales Forschungszentrum
für angewandte Cybersicherheit

Agenda

Die aktuelle Sicherheitslage **12/2024** in Deutschland

Das **NIS2-Umsetzungsgesetz** kommt **2025**

Der **Faktor Mensch** in der Cybersicherheit

KI-basierte Lernplattform der **nächsten Generation**

Personalisierung und **adaptive Lernumgebungen**

Gamification und die **HEXAD-Spielertypen**

Lokale Large Language Modells als Lernchatbots

Datenschutz (DSGVO), Security- und Privacy-by-Design

Demonstrator, Wirksamkeitsstudien und **Ergebnisse**



Umgang im Netz

Offen



Datenschutz im Netz

Fertig



Ausspähen von Daten

Offen

Aktuelle Bedrohungslage IT-Sicherheit **2024** in Deutschland

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

| Schaden durch... | Schadenssummen in Mrd. Euro (2024) | Schadenssummen in Mrd. Euro (2023) | Schadenssummen in Mrd. Euro (2022) |
|--|------------------------------------|------------------------------------|------------------------------------|
| Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen | 54,5 | 35,0 | 41,5 |
| Kosten für Rechtsstreitigkeiten | 53,1 | 29,8 | 16,2 |
| Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate | 39,2 | 15,3 | 21,1 |
| Kosten für Ermittlungen und Ersatzmaßnahmen | 32,2 | 25,2 | 10,1 |
| Datenschutzrechtliche Maßnahmen, z.B. durch Behörden | 27,2 | 12,4 | 18,3 |
| Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung | 20,2 | 35,3 | 23,6 |
| Patentrechtsverletzungen, auch vor Anmeldung | 14,8 | 10,4 | 18,8 |
| Erpressung mit gestohlenen Daten | 13,4 | 16,1 | 10,7 |
| Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen | 11,2 | 21,5 | 41,5 |
| Geldabfluss durch Betrugsversuche | 0,8 | 3,9 | - |
| Sonstige Schäden | 0 | 1,1 | 0,9 |
| Gesamtschaden pro Jahr | 266,6 | 205,9 | 202,7 |

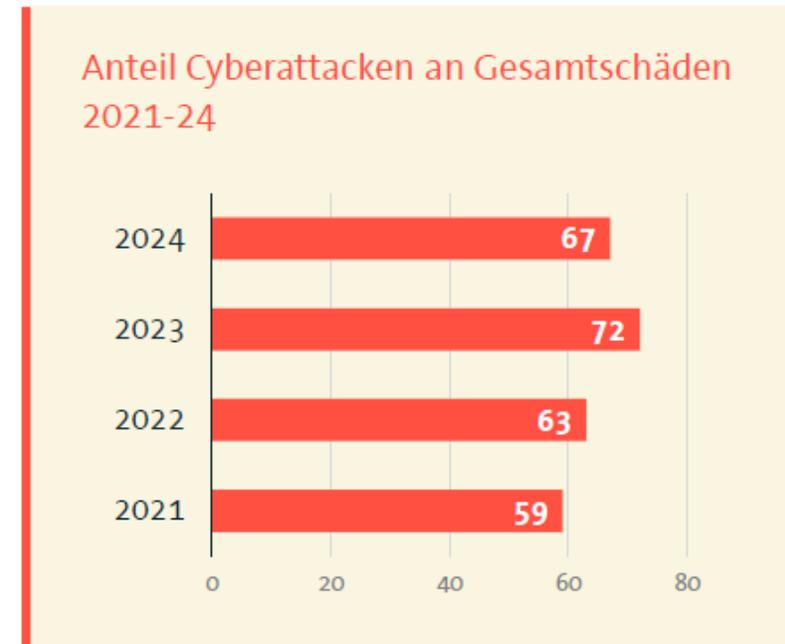
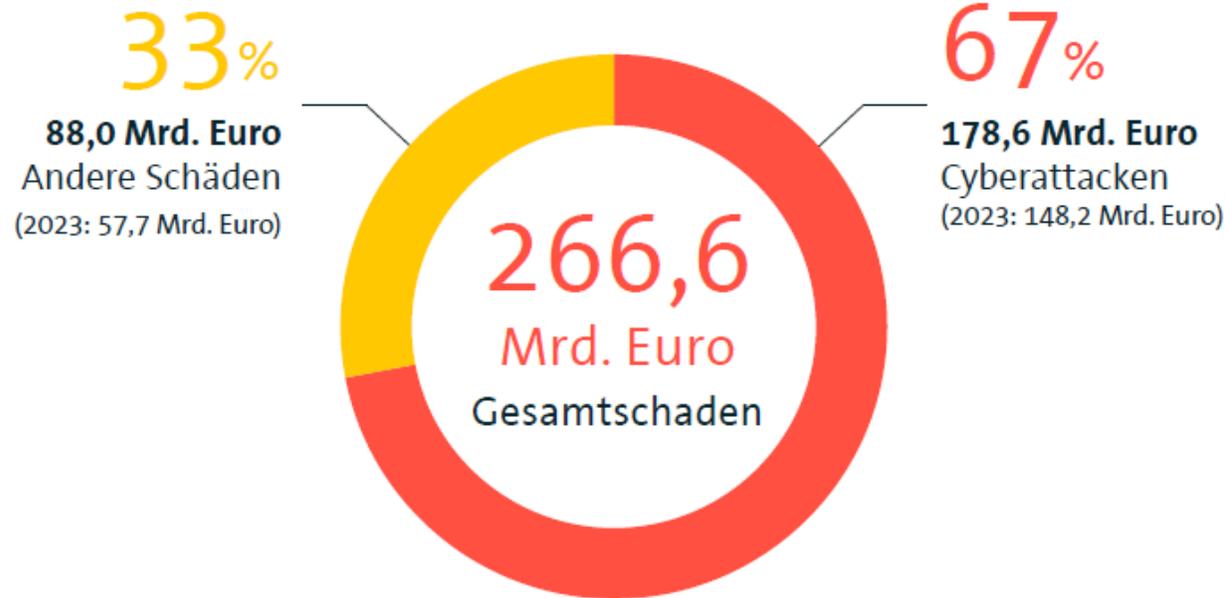
Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

[Bitkom 28.08.2024]

Aktuelle Bedrohungslage IT-Sicherheit **2024** in Deutschland

Cyberattacken verursachen zwei Drittel der Schäden

Wie hoch ist der prozentuale Anteil des entstandenen Gesamtschadens, der auf Cyberattacken zurückgeführt werden kann?



Basis: Unternehmen, die in den letzten 12 Monaten von Datendiebstahl, Industriespionage oder Sabotage betroffen waren (n=812) | Quelle: Bitkom Research 2024

[Bitkom 28.08.2024]

Das nationale IT-Lagezentrum vom BSI

- 24/7 Überwachung der deutschen Cybersicherheitslage
- Ziel ist ein verlässliches Bild der aktuellen IT-Sicherheitslage in Deutschland, um Handlungsbedarf und -optionen einschätzen zu können
- Standort, an dem verschiedene Meldestellen (sowohl gesetzlich festgelegt als auch freiwillige) zusammenlaufen
- Bei schweren Cyber-Sicherheitsvorfällen und IT-Krisen entsteht das Nationale IT-Krisenreaktionszentrum
- Im IT-Lagezentrum werden Bedrohungen analysiert und Gegenmaßnahmen entwickelt
- Informationsaustausch mit nationalen und internationalen Partnern

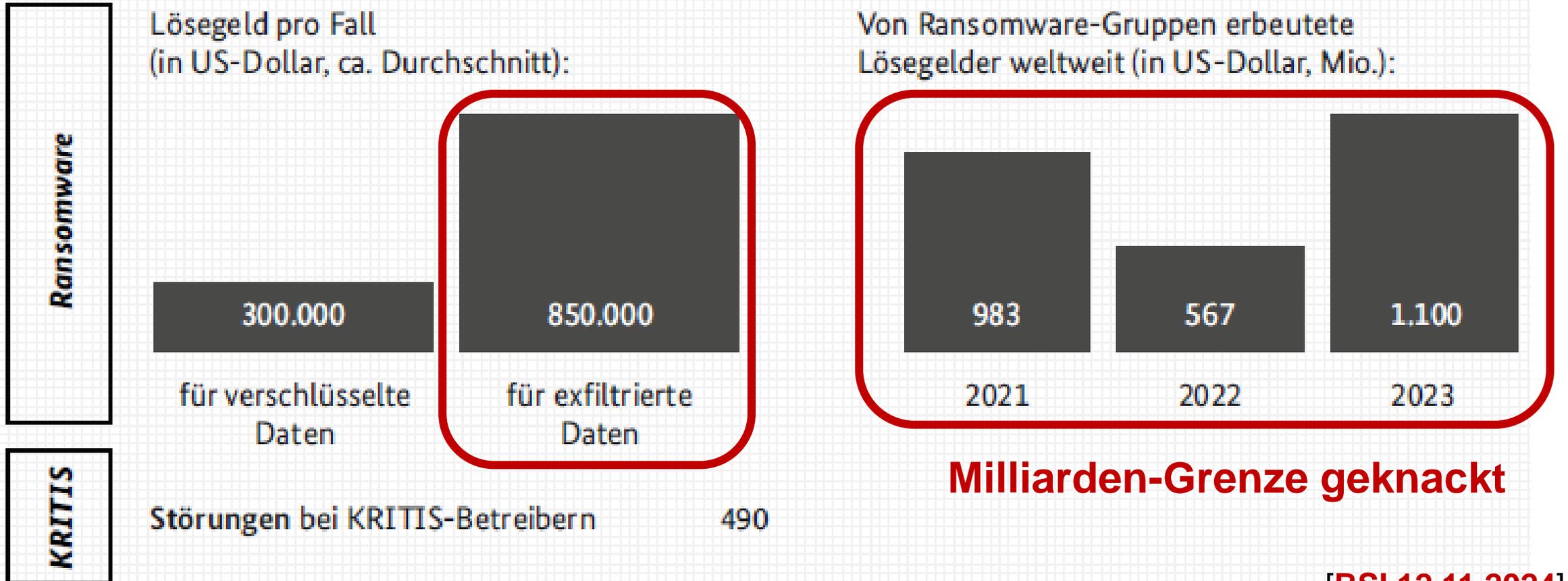


Seit Februar 2024

<https://www.bsi.bund.de/dok/Nationales-IT-Lagezentrum>

Aktuelle Bedrohungslage IT-Sicherheit **2024** in Deutschland

Schadwirkung/Impact



[BSI 12.11.2024]

Aktuelle Bedrohungslage IT-Sicherheit 2024 in Deutschland

Beispiele

Ransomware-Angriff auf kommunalen IT-Dienstleister im Oktober 2023

Betroffene Kommunen: 72
Betroffene Arbeitsplätze: rund 20.000
Betroff. Einwohnerinnen und Einwohner: rund 1,7 Mio.

Geschätzter Schaden durch Systemausfälle eines fehlerhaftes Update in der Software CrowdStrike Falcon:
> 8,5 Mio. Geräte > 5 Milliarden Dollar

VerbraucherInnen

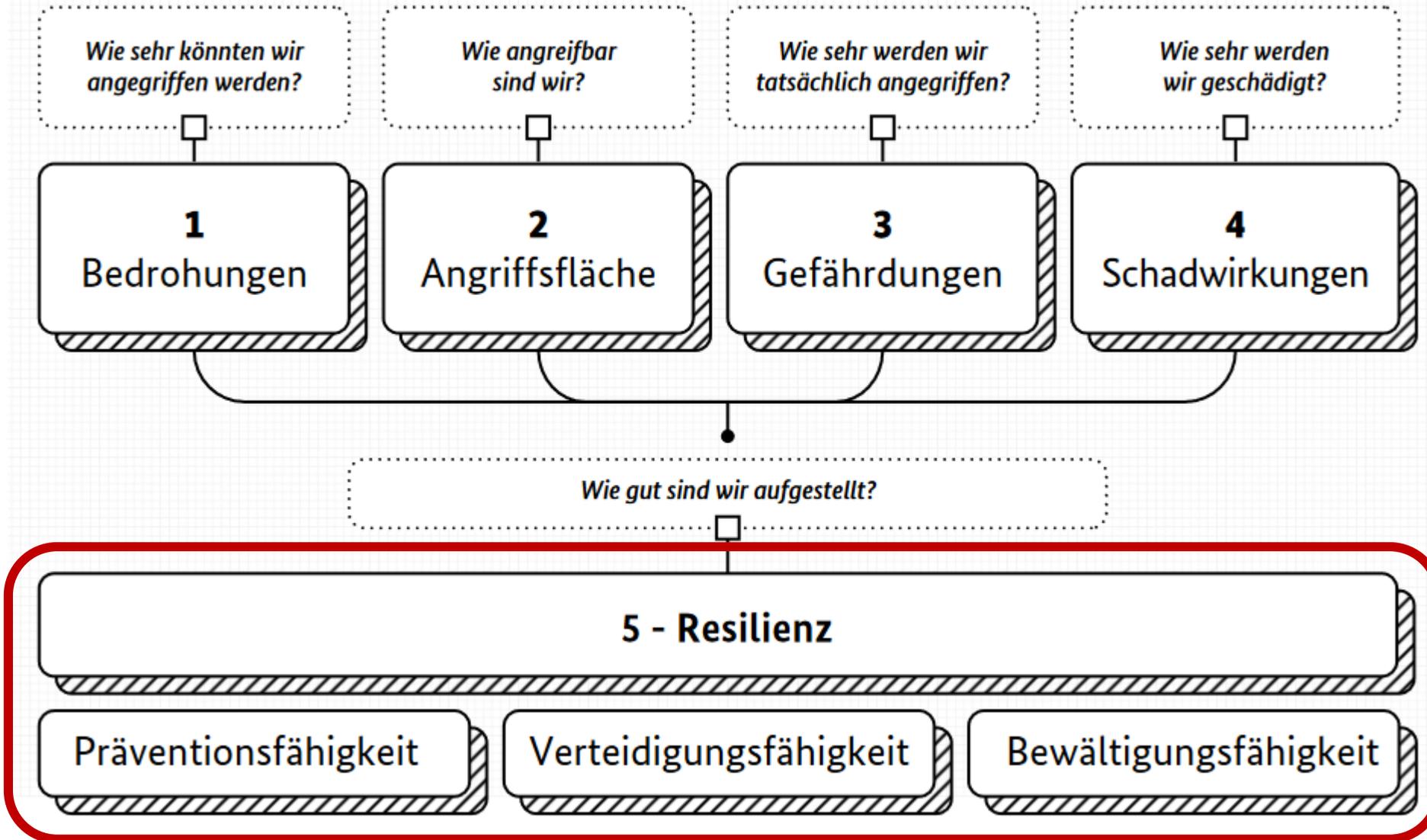
Top-3-Schäden für Verbraucherinnen und Verbraucher bei IT-Sicherheitsvorfällen und Cybercrime (%)

Vertrauensverlust in den Onlinedienst 30
Finanzieller Schaden 26
Zeitlicher Schaden 24

- Exfiltrierte Daten wesentlich mehr wert als verschlüsselte → Fähigkeit zur Prävention muss gestärkt werden
- Schäden im Milliardenbereich, unvorhergesehene Ereignisse, menschliches Versagen → Fähigkeit zur Vorfallsbewältigung muss gestärkt werden

[BSI 12.11.2024]

Aktuelle Bedrohungslage IT-Sicherheit 2024 in Deutschland



[BSI 12.11.2024]

Aktuelle Bedrohungslage IT-Sicherheit am **01.12.2024** in D

Bei schweren Cyberangriffen aus **Russland** Innenministerin Faeser hält Nato-Bündnisfall für möglich



Die hybride Bedrohungslage nehme klar zu, sagt die SPD-Politikerin. [**Tagesspiegel 01.12.2024**]



Kritische Infrastrukturen und NIS2

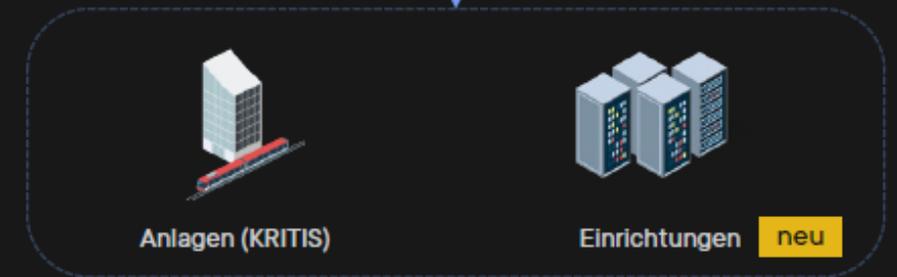


Kritische Infrastrukturen sind von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

§ 2 Absatz 10, BSI-Gesetz, Stand 2021

- Energie
- Informationstechnik
Telekommunikation,
- Transport/Verkehr
- Wasser
- Gesundheit
- Ernährung
- Finanzen und
Versicherungen
- Entsorgung

BSI-Gesetz und BSI-KRITIS-Verordnung, Stand 2021



Schutz der IT

[<https://www.openkritis.de/>]

Das NIS2-Umsetzungsgesetz kommt 2025

[Network and Information Security Directive]



NIS2UmsuCG

Ziele

Cyber Security

Umsetzung NIS 2

Große Teile der Wirtschaft

6. Entwurf Juni 2024



Betroffenheit

- Mittlere Unternehmen: ≥ 50 MA oder > 10 Mio. EUR
- Große: ≥ 250 MA oder > 50 Mio. Umsatz und > 43 Mio. Bilanz
- Sonderfälle



Betreiber

- Betreiber kritischer Anlagen (ex-KRITIS)
- Besonders wichtige Einrichtungen
- Wichtige Einrichtungen

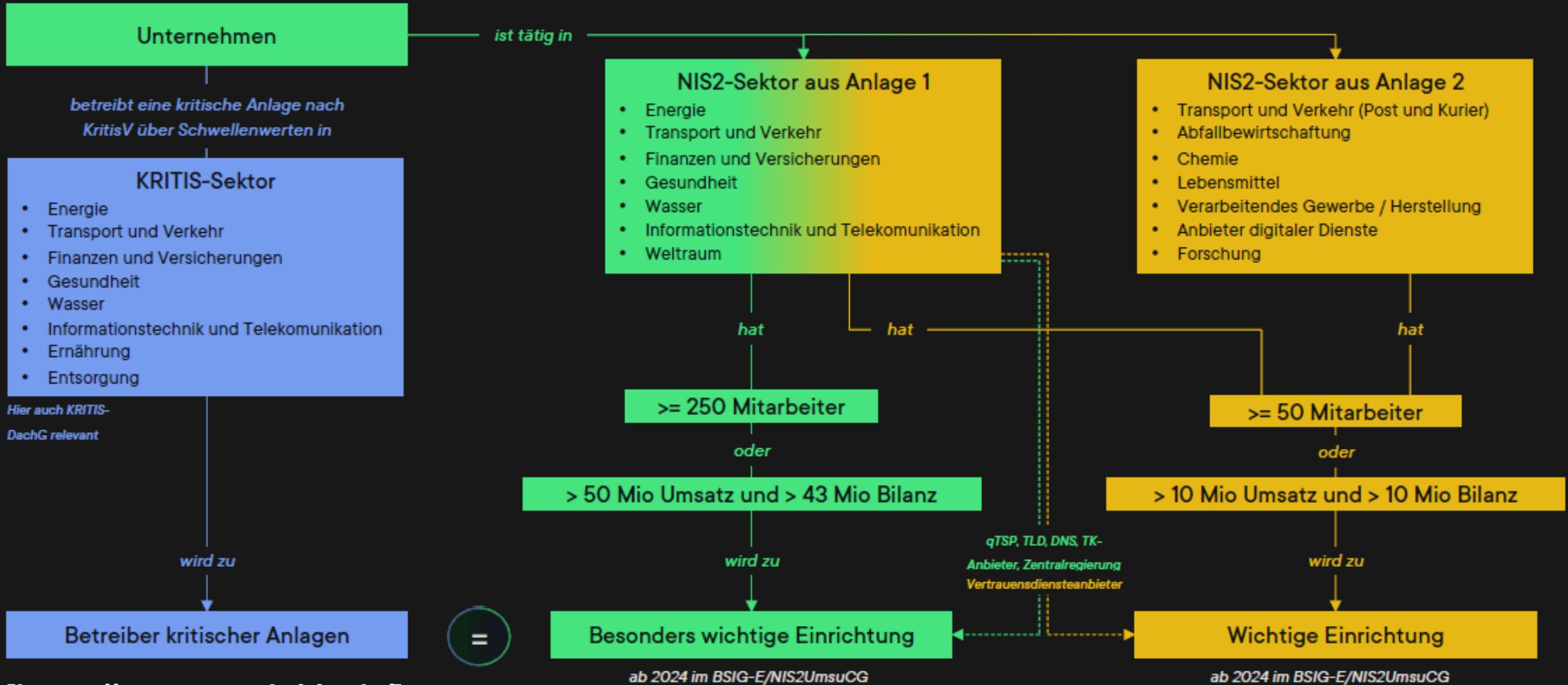


Regulierung

- Aufsicht durch das BSI (+ andere)
- BSI als zentrale Meldestelle (+ andere)

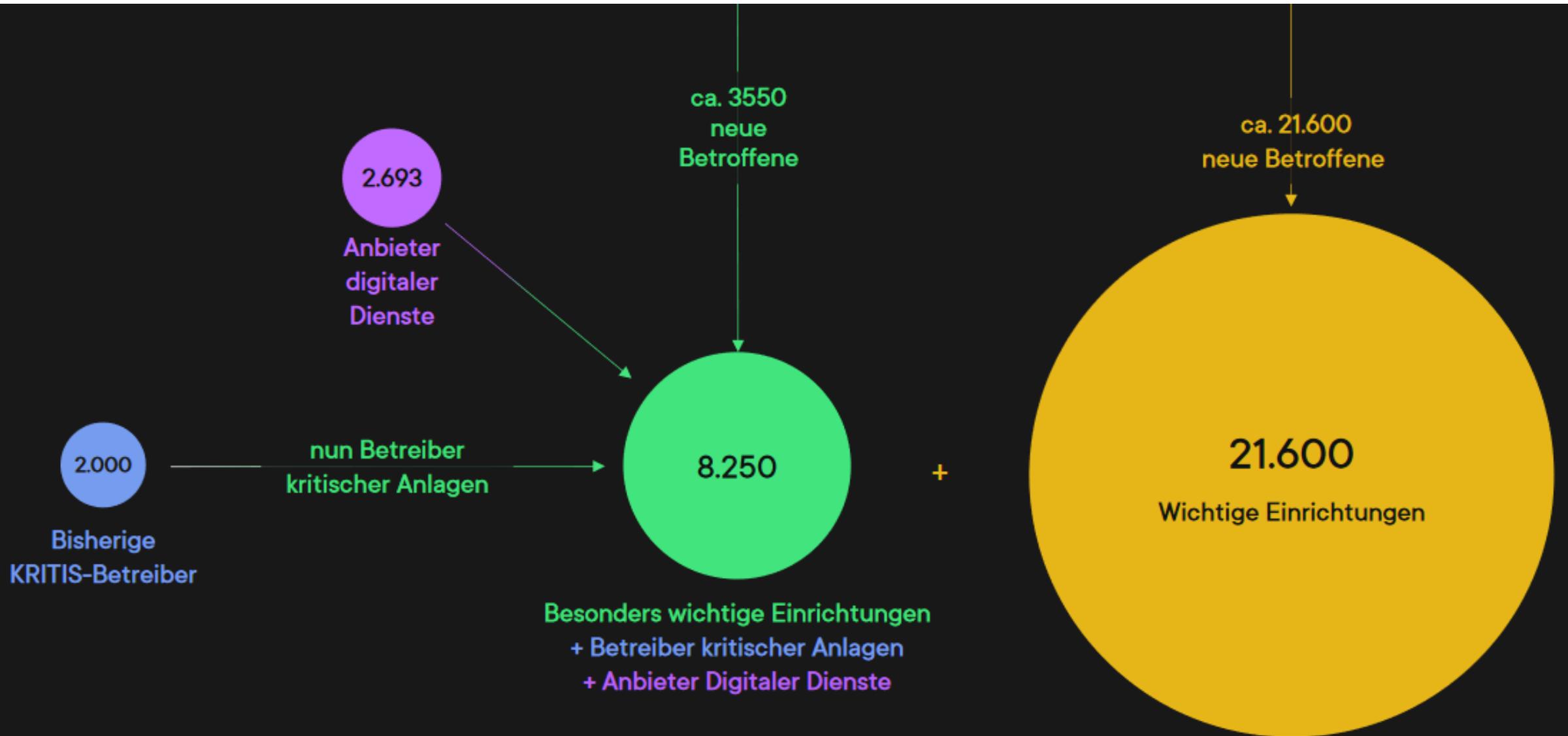
[<https://www.openkritis.de/>]

NIS2-Betroffenheitsanalyse (1)



[<https://www.openkritis.de/>]

NIS2-Betroffenheit in Zahlen (2)





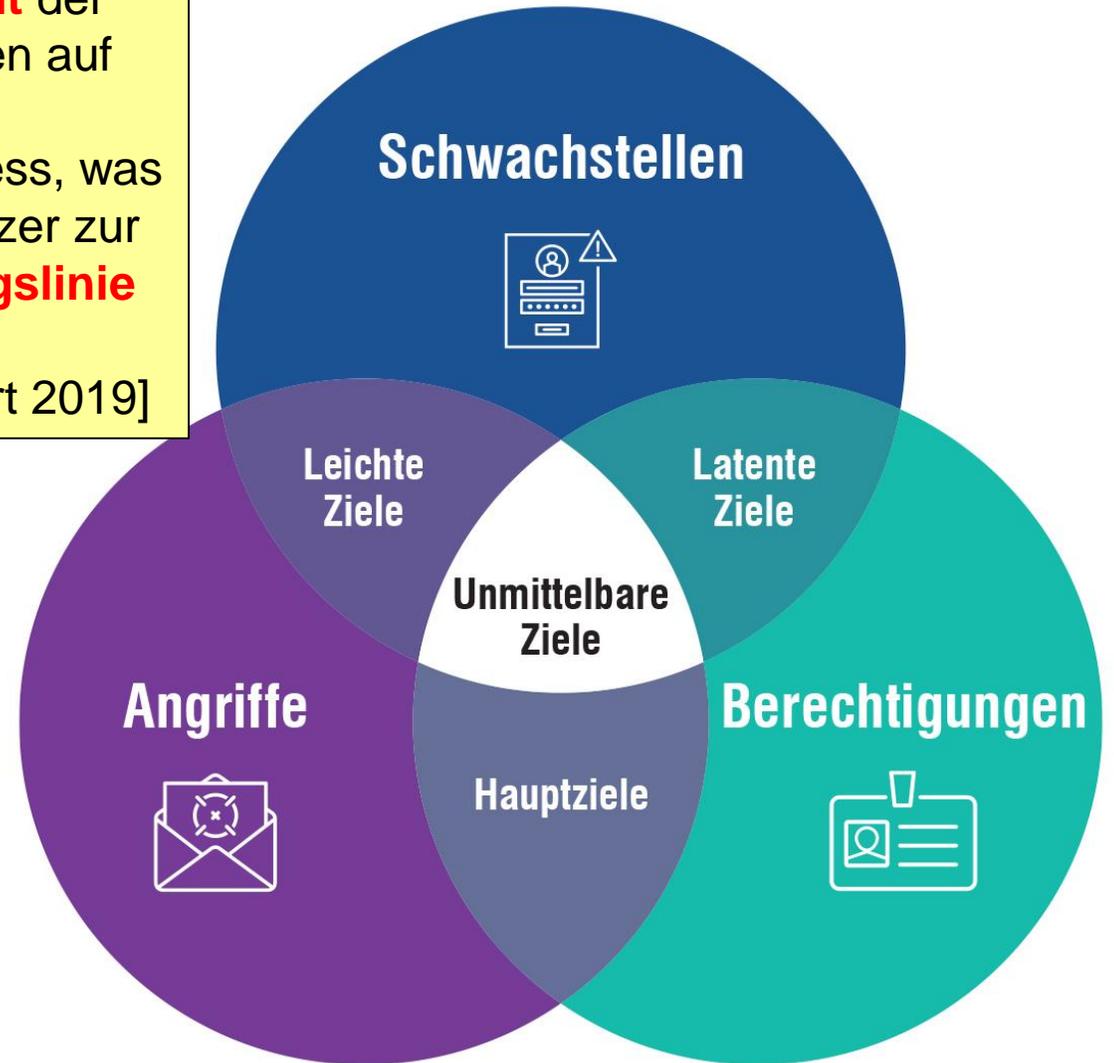
Faktor Mensch in der Cybersicherheit

„**Mehr als 99 Prozent** der Cyberangriffe beruhen auf einer **menschlichen Interaktion** im Prozess, was den einzelnen Benutzer zur **letzten Verteidigungslinie** macht.“ [Proofpoint, Human Factor Report 2019]

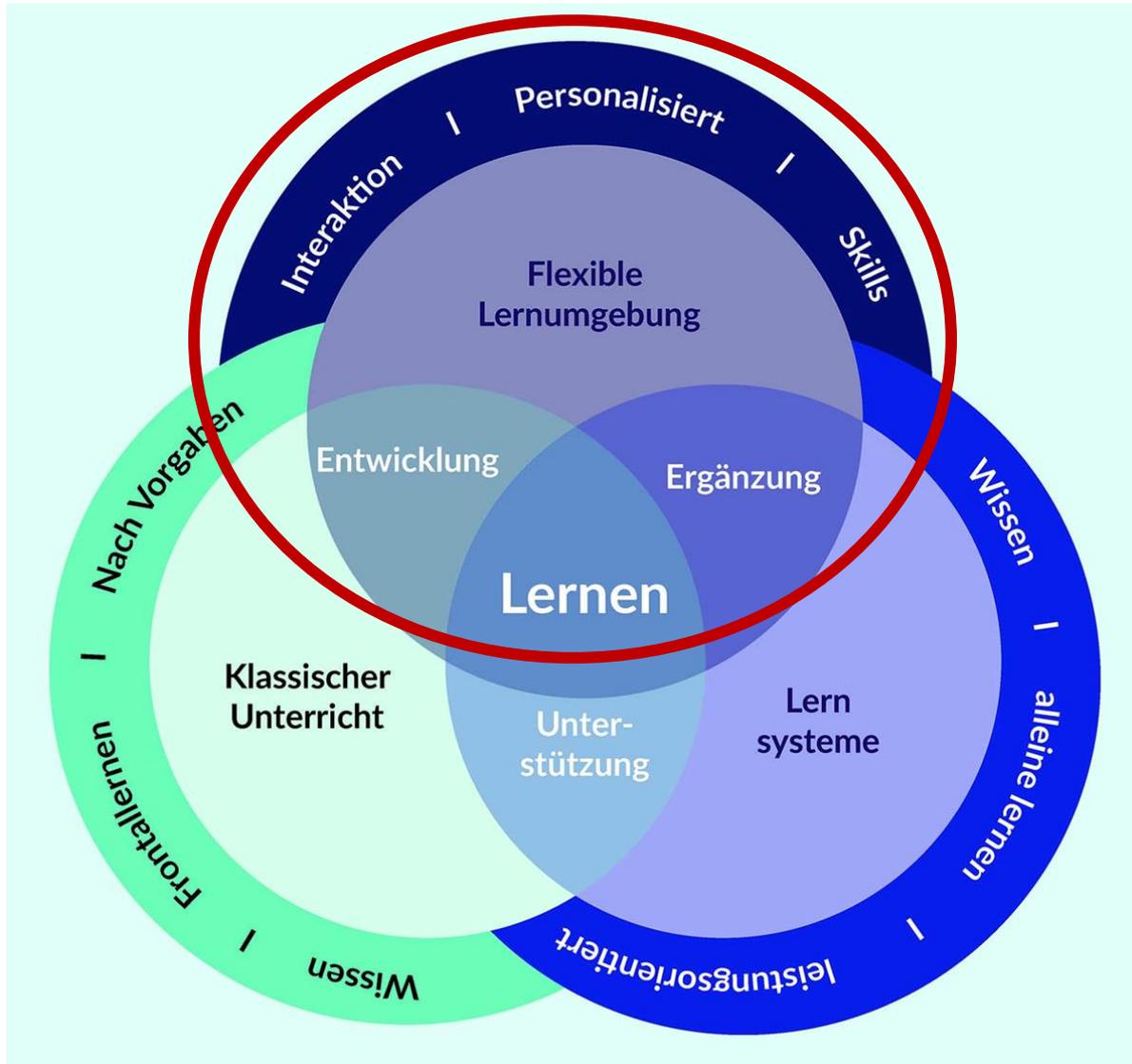
„**Cyberangreifer** nehmen gezielt Menschen ins Visier und nutzen deren Schwächen aus. Letztlich handeln Menschen einfach nur menschlich. Und deshalb sind sie – und nicht die Technologie – die **wichtigste Variable bei aktuellen Cyberbedrohungen.**“

[Proofpoint, Threat Report: Der Faktor Mensch 2023]

[Bildquelle (oben): IT-Talents; Bildquelle (rechts): IT-Markt]



Probleme und **Mängel** traditioneller Schulungen



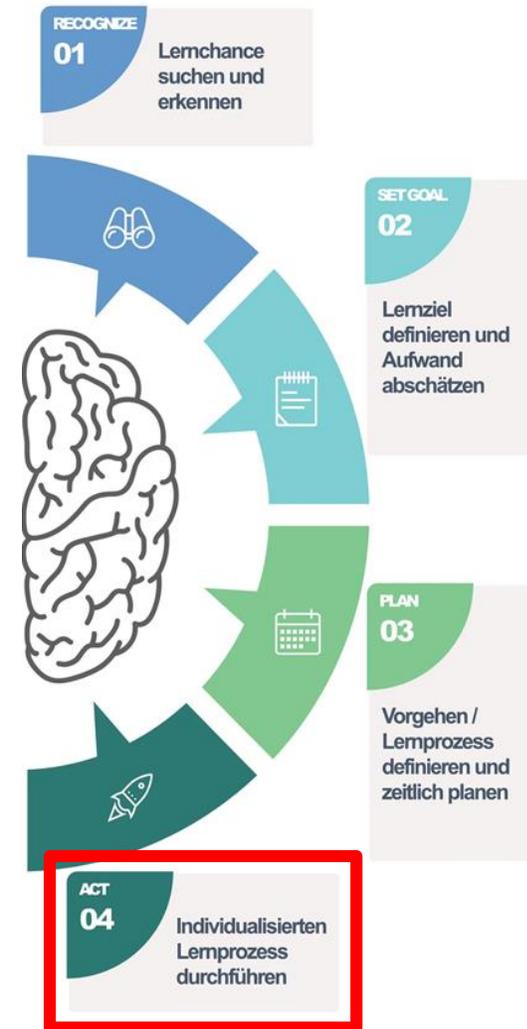
Nur PowerPoint-Schulungen, Lernvideos, standardisierte Tests, Multiple-Choice-Quizze und passiv rezeptive Lernformate, erweisen sich zunehmend als **unzureichend!**

[Bildquelle: **Co:Lab**,
<https://colab-digital.de/initiativen/koki/bildung/>]

KI-basierte Lernplattformen der nächsten Generation

Revolutionieren die Cybersicherheits- und IT-Awareness-Ausbildung durch **adaptive Lernumgebungen** und **personalisiertes Lernen**, das sich besser auf die **individuellen Lernbedürfnisse, -stile** und **-geschwindigkeiten** der Nutzer einstellen kann.

Durch **personalisiertes Lernen** in **adaptiven digitalen Lernumgebungen** haben die Anwender signifikant **bessere Lernerlebnisse (Motivation/UX/Spaßfaktor)** und **höhere Lernerfolge**.

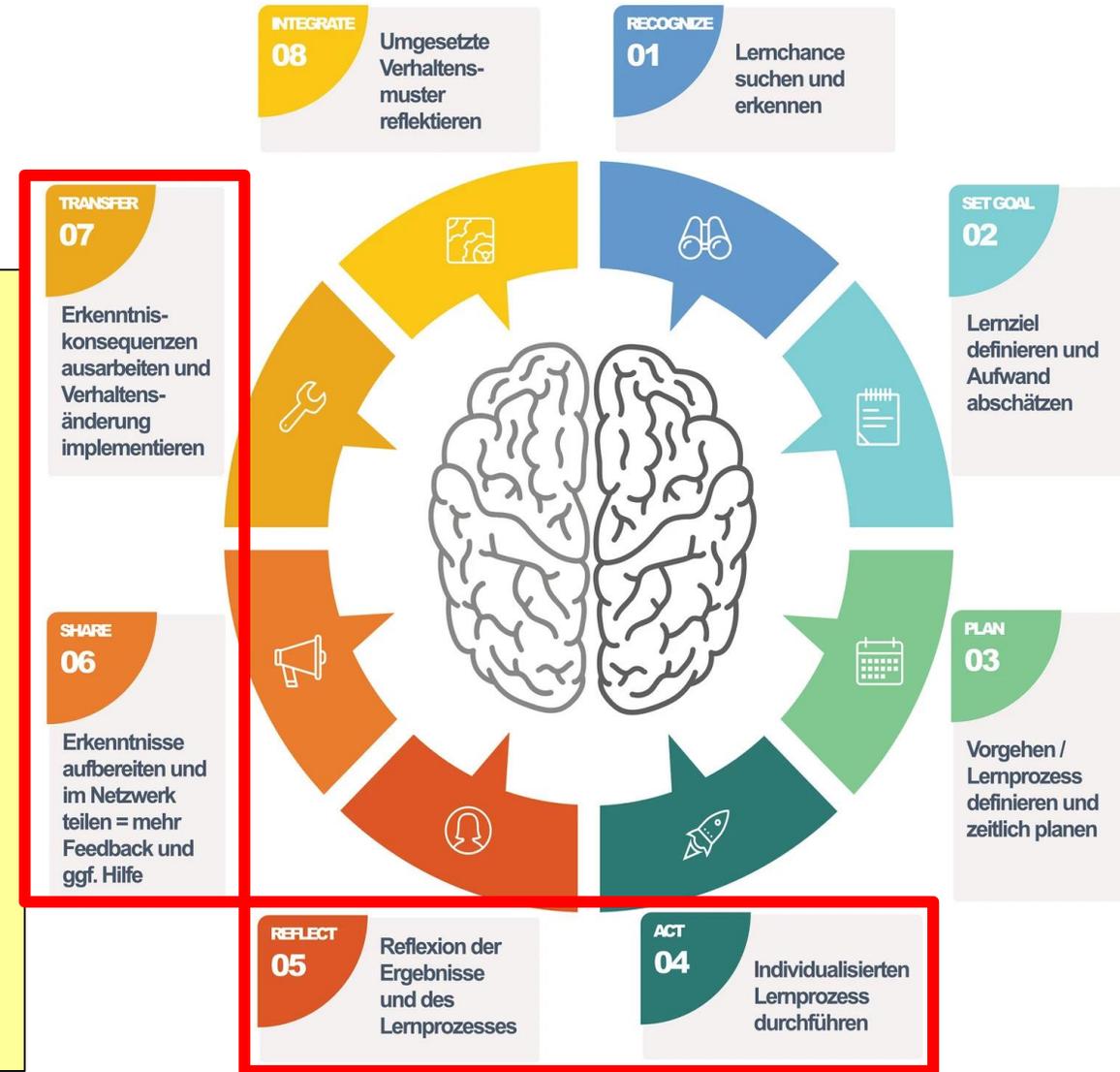


[Bildquelle: Foelsing, J., Schmitz, A. (2021). New Learning – Fokusveränderung im Lernen. Springer]

Personalisierung und adaptive Lernumgebungen

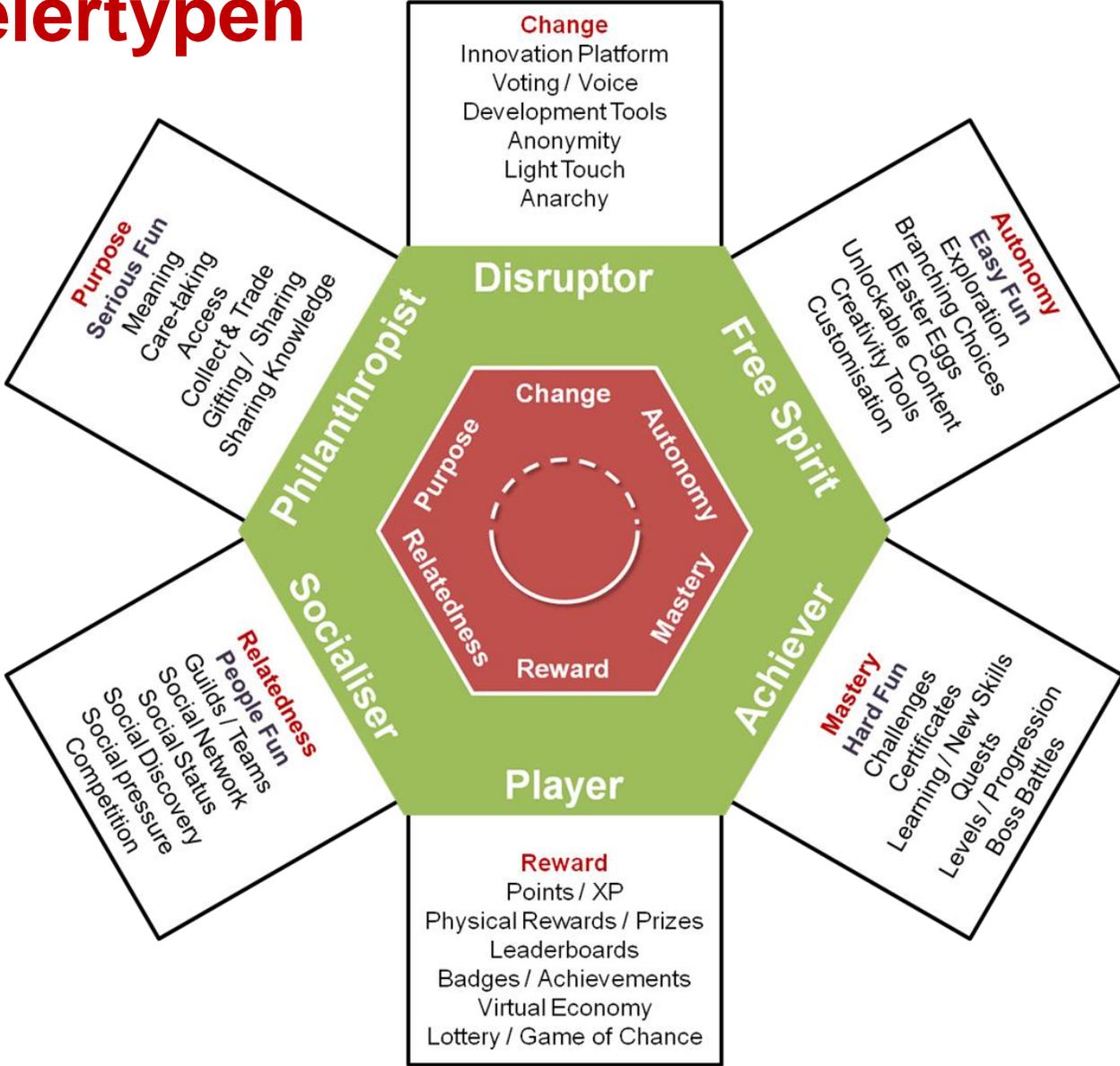
Die digitale Lernumgebung kann sowohl auf **Makro-Ebene** (z.B. Lern-/**Spielertyp**) als auch auf **Mikro-Ebene** (Lernaufgaben, Challenges, **Gamification-Elemente**) **individuell** an den Nutzer angepasst werden und ermöglicht so **maximale Lernerfolge**.

Supervised-Machine-Learning-Algorithmen errechnen Vorhersagen (Empfehlungen) über die **erfolgreichsten Lernpfade** einer bestimmten Nutzergruppe.



[Bildquelle: Foelsing, J., Schmitz, A. (2021). New Learning – Fokusveränderung im Lernen. SPRINGER]

Gamification und HEXAD-Spielertypen



HEXAD-Spielertypen und Persönlichkeit



basiert auf intrinsischen und
extrinsischen **Motivationsfaktoren**

Philanthropists sind durch **Ziele** motiviert. Sie sind altruistisch und bereit zu geben, ohne eine Belohnung zu erwarten.

Socialiser sind durch **Beziehungen** motiviert. Sie wollen mit anderen interagieren und soziale Verbindungen schaffen.

Free Spirits sind durch **Autonomie** motiviert, d. h. durch die Freiheit, sich auszudrücken und ohne äußere Kontrolle zu handeln. Sie schaffen und erforschen gerne innerhalb eines Systems.

Achiever sind durch (neue) **Kompetenz(en)** motiviert. Sie versuchen, innerhalb eines Systems voranzukommen, indem sie Aufgaben erledigen oder sich selbst beweisen, indem sie schwierige Herausforderungen angehen.

Disruptors sind motiviert durch das **Auslösen von Veränderungen**. Sie neigen dazu, das System entweder direkt oder durch andere zu stören, um negative oder positive Veränderungen zu erzwingen. Sie testen gerne die Grenzen des Systems aus und versuchen, darüber hinauszugehen.

Player sind durch **extrinsische Belohnungen** motiviert. Sie werden alles tun, um eine Belohnung innerhalb eines Systems zu erhalten, unabhängig der Art der Aktivität.

Geeignete Gamification-Elemente je HEXAD-Spielertyp

| | |
|-----------------------|--|
| Achiever | Ziele setzen und verfolgen, Fortschrittsanzeigen, Level/Stufen, Bestenlisten/Leaderboards, Statistiken, Zertifikate, Auszeichnungen und Anerkennung |
| Socialiser | Team- und Gruppenarbeit, soziale Funktionen und Entdeckungen, sozialer Status, Diskussionsforen, sowie Peer-Feedback |
| Philanthropist | Kooperative Herausforderungen, Aufgaben im Team, ein Forum zum Austausch von Erfahrungen/Wissen, Schenken, Wissensspenden und administrative Rollen |
| Free Spirit | Nicht-lineare Lernpfade, kreative Herausforderungen, Personalisierungsoptionen und Anpassungsmöglichkeiten, Erkundungsaufgaben und Kreativitäts-Tools |
| Player | Punktesysteme, Ranglisten, Leaderboards, (virtuelle) Belohnungen, Preise und Abzeichen |
| Disruptor | Ihm gezielt neue Ideen/Aufgaben vorstellen, testen und evaluieren lassen, Erkundungsaufgaben, regelmäßige Umfragen, Abstimmungen, Feedback und Entwicklungswerkzeuge |

Tabelle 1: Geeignete **Gamification-Elemente** für jeden HEXAD-Haupt-Spielertyp

Table of Gamification Elements

| | | | | | | | | | | | | |
|----------------------------------|---------------------------------------|------------------------------------|-----------------------------|---|--------------------------------------|--------------------------------------|--------------------------------------|---------------------------------------|------------------------------------|-------------------------------------|--------------------------------|----------------------------------|
| 1 Rr Random Rewards | | | | | | | | | | | 2 Fr Fixed Reward | 3 Td Time Dependent |
| 4 Ob On-boarding | 5 Si Signposting | 6 La Loss Aversion | 7 I Investment |  | | | | 8 Pf Progress / Feedback | 9 T Theme | 10 N Narrative | 11 C Curiosity | |
| 12 Tp Time Pressure | 13 S Scarcity | 14 St Strategy | 15 F Flow | 16 Co Consequences | 17 Gt Guilds / Teams | 18 Sn Social Network | 19 Ss Social Status | 20 Sd Social Discovery | 21 Sp Social Pressure | 22 Cm Competition | | |
| 23 Ch Challenges | 24 Ce Certificates | 25 L Learning | 26 Q Quests | 27 Lp Levels / Progression | 28 Bb Boss Battles | 29 E Exploration | 30 Bc Branching Choices | 31 Ee Easter Eggs | 32 U Unlockables | 33 Ct Creativity Tools | | |
| 34 Cu Customisation | 35 Ap Altruistic Purpose | 36 Cg Care Taking | 37 A Access | 38 Cn Collection | 39 Gs Gifting / Sharing | 40 Ks Knowledge Share | 41 P Points | 42 Pr Prizes | 43 Le Leaderboards | 44 B Badges | | |
| | | 45 Ve Virtual Economy | 46 Lo Lottery | 47 Ip Innovation Platform | 48 V Voting | 49 Dt Development Tools | 50 A Anonymity | 51 Lt Light Touch | 52 An Anarchy | | | |



KI-Lernchatbots zur Steigerung der Personalisierung



Ein **KI-Chatbot** ist ein **Software-Dienst**, der **Künstliche Intelligenz** verwendet, um sich mit Menschen in **natürlicher Sprache** zu unterhalten. Benutzer können Fragen stellen, auf welche das System in **natürlicher Sprache** antwortet. [IBM]



Mensch versus generative Large Language Modells

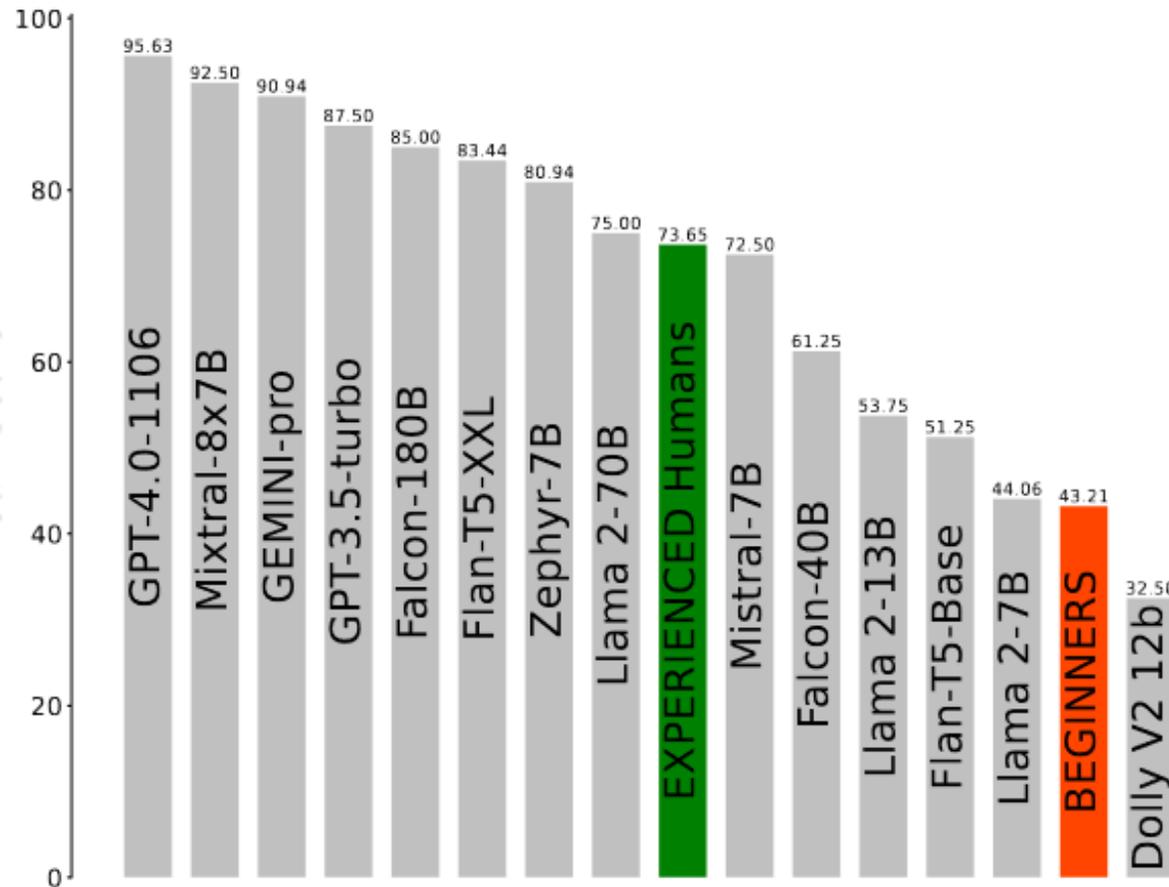


Fig. 4. Human vs Machine in the Cybersecurity

Results for the **CyberMetric-80** survey!

CyberMetric: A Benchmark Dataset for Evaluating Large Language Models Knowledge in Cybersecurity

Norbert Tihanyi, Mohamed Amine Ferrag, Ridhi Jain, Merouane Debbah

[Submitted on 12 Feb 2024]

<https://doi.org/10.48550/arXiv.2402.07688>

Kosten für **Falcon-180B** oder **Mixtral-8x7B**:
Ca. 40-50 Euro/Stunde für Cloud-Instanzen
29.200 - 36.500 Euro/Monat

Haftungsrecht: **Fehlentscheidungen** und **Falschinformationen von KI-Chatbots** aufgrund unzureichender Datenqualität oder algorithmischer Fehler können zu **Haftungsansprüchen** führen.

ChatGPT versus lokale Lernchatbots

Probleme mit ChatGPT:

Datenschutzverletzungen (DSGVO), Halluzinationen, Urheberrechtsverstöße, Produkthaftung, ...

Lösungsmöglichkeiten:

Eigener Intent-Erkennungs-FAQ-Chatbot (100% Kontrolle über Musterlösungen)

Lokales Large Language Modell (100% DSGVO-konform) mit Finetuning gegen Halluzinationen.

Interaktion zwischen Nutzer und lokalen KI-Chatbot ???!



Verwaltungsangestellte
Birgit



Industriekaufmann Peter



Phishing

Trojaner

Ransomware

Skimming

钓鱼网站

Interaktive Mindmaps zur Steigerung der Personalisierung

The screenshot displays the SecureBot learning platform interface. At the top, there is a navigation bar with the logo 'SecureBot' and menu items: DASHBOARD, LERNEN, ERFOLGE, FEEDBACK, STATISTIK, and QUIZ. On the right side, a user profile for 'Max Mustermann' is shown with 'Level 1' and a dropdown arrow.

The main content area is divided into two sections. On the left, an interactive mindmap is displayed. The central node is 'Schutzmaßnahmen gegen Malware-Angriffe', which branches into eight sub-nodes: 'Verwenden einer Antivirensoftware', 'Verwenden von Firewall', 'System- und Anwendungsaktualisierung', 'Schutz vor gefährlichen E-Mail-Anhängen', 'Vermeidung von Software-Downloads aus unbekanntem Quellen', 'Kontosicherheit', 'Erstellen von Backups', and 'Schutz vor gefährlichen Datenträger'. A red box highlights the word 'Mindmap' at the bottom left of this section.

On the right, a chatbot window titled 'Lernplattform Bot' is active. It contains the following text: 'Avast usw. Du kannst dich natürlich auch an die IT-Abteilung wenden und nach einem Antivirenanbieter fragen, der von ihnen empfohlen wird. Du solltest auch darauf achten, dass du deine Antivirensoftware regelmäßig aktualisierst und regelmäßige Scans durchführst. Außerdem empfehle ich dir, den Echtzeitschutz zu aktivieren, der die Ausführung von Programmen in Echtzeit überwacht und gegebenenfalls blockiert.' Below this, a user message asks: 'warum sollte ich meine Anwendungen stetig aktualisieren?'. The chatbot's response explains: 'Systeme und Anwendungen weisen häufig Sicherheitslücken auf, die von den Herstellern nach Bekanntwerden behoben werden. Damit bestehende Sicherheitslücken nicht ausgenutzt werden können, um dir Schaden zuzufügen, solltest du darauf achten, dass du dein System und deine Anwendungen auf dem neuesten Stand hältst. Du kannst automatische Updates für dein Betriebssystem durchführen lassen. Zusätzlich empfehle ich dir, Updates deiner Anwendungen nicht zu ignorieren und selbst in regelmäßigen Abständen nach neuen Versionen zu suchen. Es ist wichtig, nur legitime Quellen für Updates zu verwenden. Die Website des Softwareherstellers ist die sicherste Quelle, um sich über Updates zu informieren.'

Lernbereich (1): Übersicht Lernen



Timeline

15.11.2024

Quiz Attempt

Quiz completed with score: 30

15.11.2024

Quiz Attempt

Quiz completed with score: 20

15.11.2024

Grundlagen Malware

In diesem Modul erhältst du eine Einführung in die Welt der Malware. Lerne die grundlegenden Arten von Schadsoftware kennen, wie sie funktioniert, und wie sie deinen Computer oder dein Netzwerk infizieren kann. Entwickle ein Verständnis dafür, wie du Malware erkennen und Infektionen verhindern kannst

15.11.2024

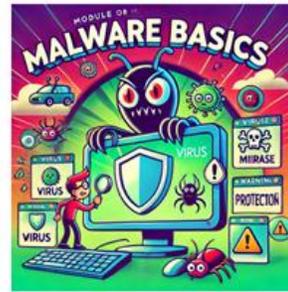
Computerviren

Dieses Modul erklärt, was Computerviren sind, wie sie sich verbreiten und welche Schäden

Fachthemen Auswahl

Gefahren im Umgang mit Malware

Malware, oder Schadsoftware, umfasst Viren, Würmer, Trojaner und andere böartige Programme, die Systeme infiltrieren und schädigen. In diesem Modul erfahren Sie, wie Malware funktioniert, welche Risiken sie birgt und wie Sie sich wirksam davor schützen können. Lerne verdächtige Aktivitäten zu erkennen und geeignete Schutzmaßnahmen zu ergreifen.



100 %



Computerviren

Dieses Modul erklärt, was Computerviren sind, wie sie sich verbreiten und welche Schäden sie anrichten können. Erfahre, wie Viren deinen Computer infizieren und wie du dich durch Antivirenprogramme und sichere Verhaltensweisen effektiv schützen kannst.

Abgeschlossen am: 15.11.2024, 16:23

MEHR ANZEIGEN

Social Engineering

In diesem Modul werden die Grundlagen des Social Engineerings vermittelt, einer Technik, die psychologische Manipulation nutzt, um vertrauliche Informationen zu erlangen oder unbefugte Handlungen zu bewirken. Lerne, wie Angreifer menschliches Verhalten ausnutzen und wie du dich effektiv dagegen schützen kannst.



Grundlagen Social Engineering

In diesem Modul erhältst du eine Einführung in die grundlegenden Konzepte des Social Engineerings. Erfahre, wie Angreifer psychologische Taktiken einsetzen, um Menschen zu beeinflussen, und entwickle ein Verständnis dafür, wie du dich und andere vor diesen Angriffen schützen kannst.

Abgeschlossen am: 15.11.2024, 16:22

MEHR ANZEIGEN

Lernbereich (2): Übersicht Lernaktivitäten



Wähle deine Lernaktivität aus, um mit dem Lernen zu beginnen



Lernvideo



ABBRECHEN

Quiz auf Zeit und Leben

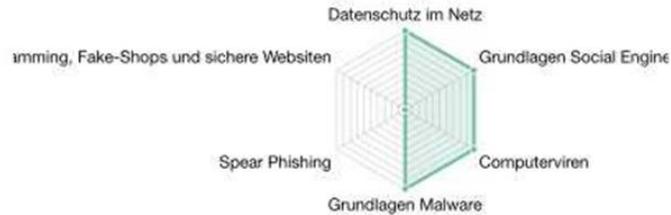


KI-Lernchatbot

Lernbereich (3): Übersicht Statistik

Netzdiagramm

Learning Progress



- 1: Datenschutz im Netz
- 2: Grundlagen Social Engineering
- 3: Computerviren
- 4: Grundlagen Malware
- 5: Spear Phishing
- 6: Scamming, Fake-Shops und sichere Webseiten

20.11.2024

Quiz Attempt

Quiz completed with score: 120

20.11.2024

Datenschutz im Netz

In diesem Modul lernst du, wie du deine persönlichen Daten im Internet schützt. Erfahre, welche Datenschutzrisiken es gibt, wie du deine Privatsphäre in sozialen Netzwerken sicherst und welche Tools dir helfen, deine Daten vor unbefugtem Zugriff zu bewahren.

20.11.2024

Grundlagen Malware

In diesem Modul erhältst du eine Einführung in die Welt der Malware. Lerne die grundlegenden Arten von Schadssoftware kennen, wie sie funktioniert, und wie sie deinen Computer oder dein Netzwerk infizieren kann. Entwickle ein Verständnis dafür, wie du Malware erkennen und Infektionen verhindern kannst.

20.11.2024

Computerviren

Dieses Modul erklärt, was Computerviren sind, wie sie sich verbreiten und welche Schäden sie anrichten können. Erfahre, wie Viren deinen Computer infizieren und wie du dich durch Antivirenprogramme und sichere Verhaltensweisen effektiv schützen kannst.

20.11.2024

Grundlagen Social Engineering

In diesem Modul erhältst du eine Einführung in die grundlegenden Konzepte des Social Engineerings. Erfahre, wie Angreifer psychologische Taktiken einsetzen, um Menschen zu beeinflussen, und entwickle ein Verständnis dafür, wie du dich und andere vor diesen Angriffen schützen kannst.

Leaderboard



| | | |
|----|-------|----|
| 4 | Marta | 98 |
| 5 | Lora | 94 |
| 6 | Mari | 90 |
| 7 | Luca | 82 |
| 8 | Maxi | 81 |
| 9 | Michi | 73 |
| 10 | Fynn | 70 |

Lernbereich (4): Offene Quests und Ideen-Labor

Offene Quests

- Vishing-Experte**
0/100 Fortschritt 
- Smishing-Spezialist**
0/100 Fortschritt 
- Spear Phishing-Meister**
46/100 Fortschritt 
- Quishing-Forscher**
0/100 Fortschritt 
- Malware-Verteidiger**
15/100 Fortschritt 
- Lernfortschritt-Macher**
0/2 Fortschritt 

Ideen Labor

Zero-Day Angriffe
Erklärung und Analyse von Zero-Day Exploits und ihrer Prävention.

JETZT MITWIRKEN!

Wie findest du diese Idee?
 Super  Eher schlecht

Feedbacks Anschauen 

 **Anonymer Nutzer**
Sehr hilfreich, bitte mehr Details zu realen Fällen.

Security- und Privacy-by-Design:

Schutz der Nutzerdaten durch **postquantensichere Verschlüsselung**

Einsatz starker Kryptografie und postquantensichere Verschlüsselung für mehr

- **Datensicherheit und Vertraulichkeit:** Um sicherzustellen, dass sensible Nutzerdaten wie persönliche Informationen und Lernfortschritte vor unbefugtem Zugriff geschützt sind.
- **Integrität:** Um sicherzustellen, dass Nutzerdaten nicht unbemerkt manipuliert oder geändert werden können.
- **Post-Quantum-Sicherheit:** Um sicherzustellen, dass die in unserer Plattform verwendeten Verschlüsselungsalgorithmen resistent gegen Angriffe von Quantencomputern sind => mit AES-256-GCM. (Q3/2025)

KI-basierte Lernplattform als Demonstrator im Testbetrieb

- (1) Registrierung und Bestimmung der **HEXAD-Spielertypen-Ausprägung**
- (2) Auswahl eines Lernmoduls und Einstufungstest
- (3) Verschiedene **personalisierte Lernangebote** und Abschlusstest

Nutzer will lernen und fragt KI-Chatbot:

Dialogbasiertes Lernen mit Mindmap, niedrigschwellig, „in kleinen Häppchen“, mobil und auch „für zwischendurch“.

Nutzer will sein Wissen überprüfen:

KI-Chatbot befragt den Nutzer, geführter Trainingsdialog mit freien Antworten, Quizze und Abschlusstest.

In Zukunft auch
Simulationen und Experimente

Demonstrator und Wirksamkeitsstudien

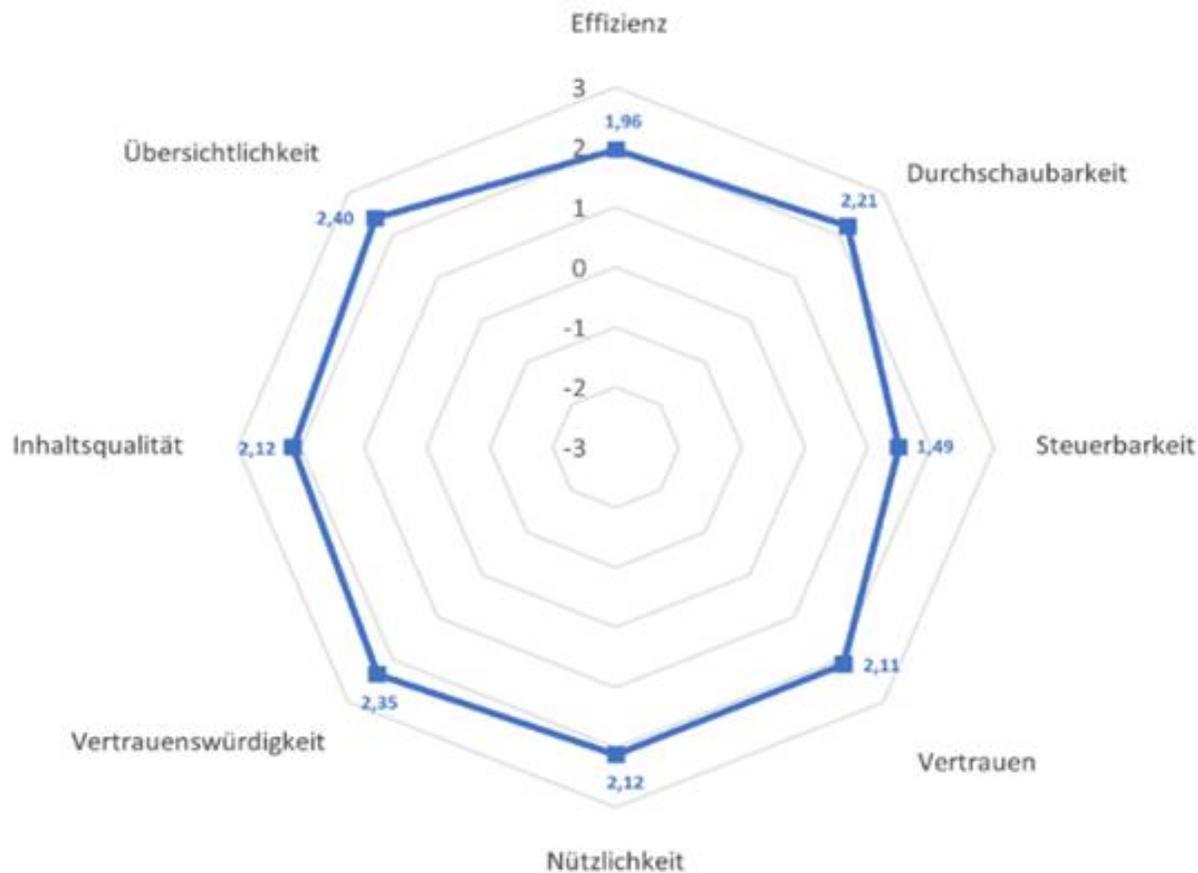


Abb. 6: Auswertung der **8 relevantesten UX-Faktoren** für unsere **KI-basierte Lernplattform** der nächsten Generation für Cybersicherheit und IT-Awareness

(1) Je geringer das vorhandene **Vorwissen** bei den Testpersonen ist, desto höher fällt der relative **Lernzuwachs** innerhalb nur eines Lernzyklus von ≤ 60 Minuten aus.

(2) Bei Testpersonen, mit einem Eingangstest von **unter 50 Prozent (< 50 Punkte)**, lag der relative Lernzuwachs im Durchschnitt bei **51%** innerhalb nur eines Lernzyklus von ≤ 60 Minuten Dauer.

(3) Die **größte Wirksamkeit** erzielt die IT-Awareness-Lernplattform bei Personen, welche keine oder nur wenige Vorkenntnisse im Bereich Cybersicherheit und IT-Awareness haben.

(4) **Jüngere Menschen** befragen den KI-Lernchatbot anders in Bezug auf Grammatik, Pragmatik, Semantik und Syntax als ältere Menschen.

Ergebnisse, **Innovationen** und **Alleinstellungsmerkmale**:

- Die **digitale Lernumgebung** kann sowohl auf **Makro-Ebene** (z.B. Spielertyp) als auch auf **Mikro-Ebene** (Lernaktivitäten, Challenges, Gamification-Elemente) **individuell** an den Nutzer angepasst werden.
- **Mindmaps**: Durch den Einsatz von **interaktiven Mindmaps** und Microcontent können Lerninhalte flexibel in verschiedenen Kontexten genutzt werden, was die **Personalisierung** des Lernprozesses unterstützt.
- **KI-Lernchatbots** können sowohl **Fragen beantworten** als auch **freie Trainings- und Lerngespräche** innerhalb der Lernmodule führen.
- **Supervised-Machine-Learning-Algorithmen** errechnen **Vorhersagen (Empfehlungen)** über die **erfolgreichsten Lernpfade** einer bestimmten Zielgruppe.
- **Postquantensichere Verschlüsselung** der nicht-aktiven Nutzerdaten.
- Ermöglicht dem Nutzer ein **personalisiertes** und **zugeschnittenes Lernerlebnis**.

Danksagung für Förderung und Unterstützung

HESSEN



Hessisches Ministerium für Digitalisierung und Innovation

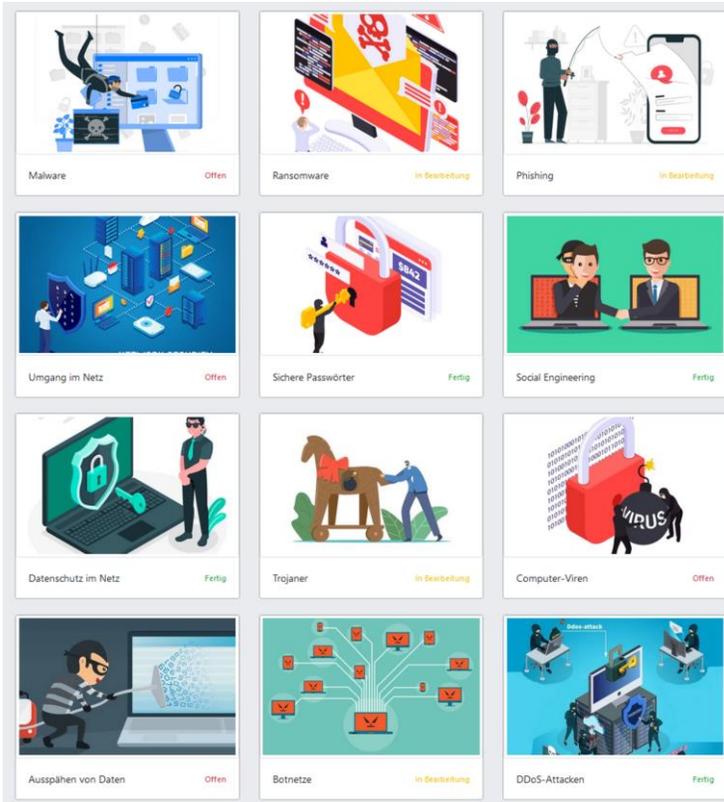


digitales.hessen
DISTR@L

HESSEN



Hessisches Ministerium des Innern, für Sicherheit und Heimatschutz



FORSCHUNGSFÖRDERUNG
CYBERSICHERHEIT

Hessisches Ministerium des Innern,
für Sicherheit und Heimatschutz

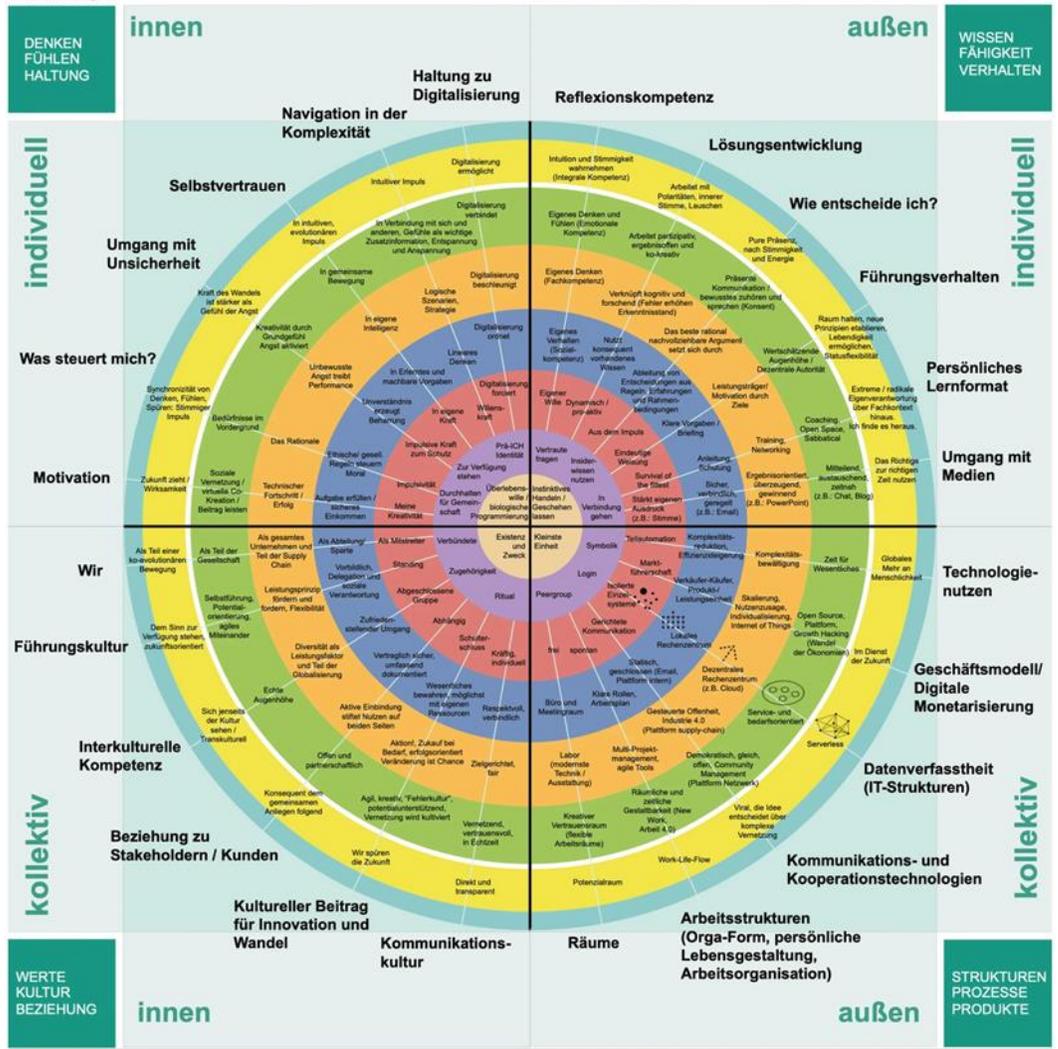
h_da
hochschule
darmstadt
informatik

member of
ewt+
EUROPEAN UNIVERSITY
OF TECHNOLOGY



ATHENE

Nationales Forschungszentrum
für angewandte Cybersicherheit



in Anlehnung an: Spiral Dynamics (Beck/Cowan) sowie Vier-Quadranten-Modell (Wilber)
Ergebnis des Forschungsvorhabens KMUdigital (02P17K024), Stand Januar 2019
imu augsburg in Zusammenarbeit mit 16 Experten aus Wissenschaft und Praxis (www.i-m-u.de/Forschung)

Unsere Zielgruppe

Unsere Zielgruppe sind **alle Menschen, Unternehmen und Organisationen** mit essenziellen IT-Sicherheitsrisiken.

Das **konstante Grundbedürfnis** unserer Zielgruppe besteht darin, ihre **Assets (Daten, Informationen, Geschäftsgeheimnisse)** zu schützen und zu verhindern, dass Angreifende diese ausspähen, manipulieren, kopieren, zerstören oder durch Ransomware unbenutzbar machen können.

Diskussion

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?

Kontakt:

Prof. Dr. Michael Massoth
Hochschule Darmstadt
Fachbereich Informatik
Email: michael.massoth@h-da.de

**Interesse als Beta-Tester, FuE-Partner
und/oder Pilotkunde:**

Nachricht an Herrn Enis Top
Email: enis.top@h-da.de

