

DsiN Magazin

06/2024 Jahresbericht 2023

IT-SICHERHEIT IN BERUF UND AUSBILDUNG

Cybersicherheit und Politik

Seite 56

ONLINEBANKING

Ein Gespräch mit Frau Dr. Strack- Zimmermann

Seite 74

KI & AUSBLICK

Drei Fragen an den Beirat

Seite 88

FOKUSTHEMA

DsiN-Jahreskongress 2023 Desinformationen entgegenwirken

Seite 22

Schirmherrschaft:



Bundesministerium
des Innern
und für Heimat



Deutschland
sicher im Netz

**Liebe Mitglieder von
Deutschland sicher im Netz,
liebe Partner und Engagierte
für IT-Sicherheit und sichere
digitale Teilhabe im Netz,**

im vergangenen Jahr wurde erneut deutlich, wie wichtig es ist, IT-Sicherheit zu stärken und Desinformation entgegenzuwirken. Denn die Angriffe auf die Sicherheit unserer digitalen Infrastrukturen haben massiv zugenommen. Auch die Zahl der Desinformationskampagnen in Form von Falschmeldungen, Deep Fakes, Propaganda und anderen Methoden hat 2023 einen neuen Höchststand erreicht. Kriminelle Hacker:innen, aber auch staatliche Akteure versuchen so, das Vertrauen in den Staat und seine Institutionen zu untergraben.

Als Bundesregierung haben wir deshalb unsere Fähigkeiten zur Analyse und Abwehr von hybriden Bedrohungen wie Desinformation deutlich ausgebaut. Wir haben unsere Instrumente und Regelungen gestärkt, um Missbrauch und Schaden abzuwenden. Mithilfe des künftigen europäischen Cyber Resilience Acts dürfen beispielsweise nur noch Produkte mit digitalen Elementen auf den europäischen Markt kommen, die hohe IT-Sicherheitsstandards erfüllen. Auch die Umsetzung der EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS2) wird das Sicherheitsniveau steigern und damit das Risiko für Unternehmen senken, Opfer von Cyberangriffen zu werden.

Damit diese neuen Regelungen gut greifen können, braucht es kompetente Nutzer:innen. Gerade im außerschulischen Bildungsbereich engagieren sich Deutschland sicher im Netz, seine Mitglieder und Partner in der Vermittlung von Basiskompetenzen. Sie leisten dabei vorbildliche Arbeit: mit Initiativen wie dem Bundesnetzwerk Digitale Nachbarschaft, dem Digital-Kompass, dem Digitalen Engel sowie PolisiN – Politiker:innen sicher im Netz. Jeden Tag erreichen sie damit zahlreiche Menschen.



Als Schirmherrin freut es mich sehr, dass DsiN mit dem geplanten FitNIS2-Navigator zukünftig auch kleinere und mittlere Unternehmen auf dem Weg zur Cybersicherheits-Compliance unterstützt. Sie leisten damit einen wichtigen Beitrag, damit die EU-Richtlinie flächendeckend umgesetzt werden kann.

Es ist gut, dass diese wichtige Bildungsarbeit immer mehr Aufmerksamkeit erhält. Ganz besonders möchte ich dabei auf die noch wenig ausgebaute außerschulische Bildung und Ansprache im non-formalen Bildungsbereich hinweisen. Hier sprechen wir von über 70 Millionen Menschen, die außerhalb des formalen Bildungssystems Unterstützung brauchen, um den digitalen Alltag sicher und selbstbestimmt zu gestalten. Gerade hier ist Bildungsarbeit wichtig, denn alle Menschen müssen die Chance haben, sich sicher und kompetent im digitalen Alltag zu bewegen.

Die Herausforderungen wachsen stetig. Die Arbeit von DsiN ist und bleibt deshalb wichtig. Machen Sie genauso engagiert weiter, wie es das vielfältige Engagement aus 2023 zeigt, das in diesem Jahresbericht vorgestellt wird.

Ihre Nancy Faeser

*Bundesministerin des Innern und für Heimat
Schirmherrin von Deutschland sicher im Netz*

Drei Fragen an ...

Lieber Herr Tschersich, lieber Herr Schulte. Was ist für Sie beide das Besondere an Deutschland sicher im Netz?

Thomas Tschersich: Der Verein wurde gegründet, um Menschen zu Fragen rund um digitale Alltagsthemen aufzuklären. Dabei geht es vor allem darum, Chancen im Alltag aufzuzeigen, die einen echten Mehrwert bieten. Gleichzeitig geben wir praktische Tipps, wie mit oftmals kleinen Routinen im Alltag die eigene Sicherheit im Netz deutlich erhöht werden kann. Dabei bauen wir Ängste ab, ohne sie zu verharmlosen. Zudem ist einmalig bei DsiN, dass hier alle Akteure an einem Tisch sitzen: also große wie auch kleine Unternehmen, Vertreter der öffentlichen Hand, der Zivilgesellschaft und der Wissenschaft. Ein gutes IT-Sicherheitsniveau erreicht niemand alleine.

Joachim Schulte: Dabei arbeiten wir Hand in Hand mit Kooperationspartnern, die nahe an den Menschen sind, die wir erreichen wollen. Oftmals haben sie den besten Zugang zu ihnen und genießen deren Vertrauen. Wir gehen dabei auch in ländliche Regionen, in Schulen, in Senioreneinrichtungen und in Vereine sowie in Unternehmen. Es geht bei DsiN immer darum, praktisches Wissen zu Digitalthemen zu erlangen und dieses dann auch im Alltag anwenden zu können – wichtig: nicht zu müssen. Bei uns wird niemand gezwungen, einen Dienst zu nutzen oder ein Produkt zu kaufen. Ganz wichtig ist mir noch zu betonen, dass wir immer zuerst darauf schauen, um wen es genau

geht: Über welches Vorwissen verfügt die Person? Welche Form der Ansprache und der Wissensvermittlung passt am besten? Bei DsiN gibt es keine Angebote von der Stange, sondern passende für jede Zielgruppe.

Was waren Ihre Highlights im Jahr 2023?

Tschersich: Viele. Ganz klar gehört der DsiN-Digitalführerschein dazu. Ein gefördertes Angebot aus dem Hause unserer Schirmherrin im Bundesinnenministerium, mit dem wir bei DsiN über 170.000 absolvierte Einzelprüfungen erreicht haben. Eindrucksvoll ist nicht nur die schiere Zahl, sondern auch, dass wir wirklich alle Altersgruppen gezielt angesprochen haben. Zudem haben wir zwischen der privaten und beruflichen Nutzung in Unternehmen und Verwaltung unterschieden.

Schulte: Ich bin sehr froh, dass es uns gelungen ist, Initiativen wie die Digitale Nachbarschaft und den Digitalen Engel von der Bundesebene auf die regionale Ebene zu übertragen und Landesregierungen zu überzeugen, in diesen Strukturen mitzuwirken, anstatt das sprichwörtliche Rad neu zu erfinden. Dadurch verstärken wir unsere Präsenz vor Ort und knüpfen zugleich an die Erfolge auf Bundesebene an. Beispielhaft dafür stehen die Projekte im Netzwerk der Digitalen Nachbarschaft: Engagement Digital in Sachsen-Anhalt und digital verein(t) in Bayern, sowie ganz neu der Digitale Engel in Thüringen.



Thomas Tschersich

DsiN-Vorstandsvorsitzender

Was kommt 2024?

Tschersich: 2024 wird ein Jahr des Aufbruchs, aber sicher auch der Veränderung. Im Zeichen einer angespannten Haushaltslage suchen wir Wege, die Förderung von Digitalkompetenzen neu zu denken: Wir werden stärker arbeitsteilig denken müssen – und die Kooperationen mit vielfältigsten Partnern aus Zivilgesellschaft und Unternehmen weiter ausbauen. Zudem sehe ich einen enormen Bedarf, zum Thema Künstliche Intelligenz aufzuklären: Hier gibt es nahezu täglich Veränderungen und da fällt es auch IT-Profis schwer immer auf dem Laufenden zu bleiben.

Ist auch für Sie KI das Thema des Jahres?

Schulte: Künstliche Intelligenz ist natürlich das Thema, das alles überlagert. Es bietet so unfassbar viele Chancen zur Erleichterung des Alltags für Menschen jeden Alters und für unterschiedlichste Anwendungsfälle – vom Beruf bis zum Ehrenamt. Es durchdringt somit eine Vielzahl von Themen. Gleichzeitig besteht bei vielen Menschen eine hohe und zugleich diffuse Verunsicherung: Werden wir bald von KI gesteuert? Was „weiß“ die KI über mich und wie verwendet sie dieses „Wissen“? Hier müssen



Joachim Schulte

DsiN-Geschäftsführer

wir zunächst ansetzen, damit wir möglichst alle Menschen in die digitale Welt von morgen mitnehmen.

Herr Schulte, was wird anders werden bei DsiN unter Ihrer Leitung?

Zunächst einmal freue ich mich enorm über das Vertrauen, das mir der DsiN-Vorstand schenkt. Ich werde nun – gemeinsam mit meinen vertrauten Kolleg:innen und den vielfältigen Partnern und Mitgliedsunternehmen – Ideen umsetzen, um Lernangebote zu schaffen, die einen echten Mehrwert für Verbraucher:innen sowie KMUs bieten.

Sicherlich wird sich vieles ändern, aber nicht alles und vor allem nicht sofort. Der Verein steht weiterhin zu seinen getroffenen Zusagen und Versprechen. Gleichzeitig habe ich auch richtig Lust, neue Projekte zu initiieren, die Menschen helfen, die Orientierung im Netz zu behalten. Besonders gerne möchte ich Angebote schaffen, die sich an junge und sehr junge Menschen richten: Sie sind die Zukunft unserer Gesellschaft und sollten sich sicher im Netz bewegen. Für dieses Thema gibt es bereits einige gute Angebote, aber ich habe den Eindruck, dass wir hier – gemeinsam mit unseren Partnern – mehr machen müssen und noch Luft nach oben haben.

Inhalt

DESINFORMATION ENTGEGENWIRKEN

- 8 DsiN-Sicherheitsindex 2023
- 12 Alt und Jung: Gemeinsam für ein besseres Internet
- 14 Digitale Teilhabe
- 16 Im Fokus: Desinformationen und Verschwörungserzählungen im Netz
- 18 DsiN-Digitalführerschein
- 20 Digitale Unterstützung für Vereine – ist doch Ehrensache
- 22 DsiN Jahreskongress 2023
- 32 Facts Against Fakes
- 34 Lokal, persönlich und konkret
- 38 Schutz vor Online-Betrug
- 42 Tag der offenen Tür der Bundesregierung

IT-SICHERHEIT IN BERUF UND AUSBILDUNG

- 50 Drei Jahre TISiM: Ein Erfolgsmodell für den Mittelstand
- 52 Neue Workshopformate im Projekt „MIT Sicherheit ausbilden“
- 54 PolisiN mit fraktionsübergreifender Schirmherrschaft im Deutschen Bundestag
- 56 Cybersicherheit und Politik



22 DsiN Jahreskongress 2023



14 Digitale Teilhabe für Menschen mit Sehbehinderung, Hörbeeinträchtigung oder Mobilitätseinschränkung



50 Drei Jahre TISiM: Ein Erfolgsmodell für den Mittelstand



Zwischen Information und Manipulation: Gespräch mit Marie-Agnes Strack-Zimmermann



62 DsiN-Talk „Sicherer Login“



88 Drei Fragen an den Beirat

ONLINEBANKING

- 62 DsiN-Talk „Sicherer Login“
- 66 Onlinebanking – aber sicher!
- 68 DsiN-Talk zum neuen DiFü-Fokusmodul „Sicheres Onlinebanking“
- 72 Kann ich nachts beim Onlinebanking überfallen werden?
- 74 Zwischen Information und Manipulation: Gespräch mit Marie-Agnes Strack-Zimmermann

KI & AUSBLICK

- 80 Jahresrückblick im Zeichen von KI
- 84 2023 – ein Jahr ChatGPT
- 88 Drei Fragen an den Beirat
- 92 Ausblick & Perspektiven auf das neue Jahr 2024

- 1 Vorwort
- 2 3 Fragen an ...
- 46 Infografik KPIs DsiN
- 95 Impressum

Die Illustration entstand mit dem Text-zu-Bild-Generator DreamStudio.
Prompt: oil painting of data streams only with green colors

Fokusthema
**Desinformation
entgegenwirken**

DsiN-Sicherheitsindex 2023

Die digitale Sicherheitslage ist auf dem Tiefstand

Am 14. Juni 2023 war es so weit und die Ergebnisse zur digitalen Sicherheitslage der Verbraucher:innen in Deutschland konnten im DsiN-Sicherheitsindex vorgestellt werden. Seit 2014 erhebt DsiN mit Studienpartner Kantar (ehemals TNS Infratest) diese Studie durch, welche die Sicherheitslage auf einer Skala von 0 bis 100 zuordnet. Hierzu wird nach Sicher-

cher:innen über 16 Jahre werden hierfür in Zusammenarbeit mit dem Markt- und Meinungsforschungs-institut KANTAR befragt.

Mit 57,2 Punkten fällt dieser Index im Jahre 2023 auf den tiefsten Wert seit seiner ersten Erhebung vor zehn Jahren. Maßgeblich dafür ist der starke Anstieg von IT-Sicherheitsvorfällen um 11,2 Indexpunkte im Vergleich zum Vorjahr, das heißt ein Anstieg um 20 Prozent.

Allgemein zum Index

Index auf dem tiefsten gemessenen Wert von

57,2 ↓

PUNKTEN

Rückgang in diesem Jahr

2023

2,6 Punkte ↓

Rückgang im letzten Jahr

2022

2,9 Punkte ↓

Sicherheitslage der Internetnutzer:innen in Deutschland erreicht **niedrigstes Niveau** seit Beginn der Erhebung 2014.

heitsfaktoren unterschieden: Erlebte Sicherheitsvorfälle sowie das Verunsicherungsgefühl der Verbraucher:innen beschreiben die Bedrohungslage. Das Sicherheitswissen und Sicherheitsverhalten von Verbraucher:innen ergeben das Schutzniveau. Etwa 2.000 Verbrau-

Zugleich halten die Schutzkompetenzen der Menschen im Netz mit den wachsenden Risiken im digitalen Raum nicht stand. Rund 56 Prozent der Personen im Netz benötigen zusätzliche Hilfestellungen.

+5,9% ↑

Sicherheitsvorfälle

Phishing-Versuche per SMS oder Messenger (betrügerische Nachrichten mit unbekanntem Link oder Aufforderung zur Eingabe von sensiblen Daten) haben um **5,9%** zugenommen.



Sicherheitsvorfälle auf neuem Höchststand

Die Zunahme der erlebten Sicherheitsvorfälle erstreckt sich auf das gesamte Umfeld digitaler Dienste und Technologien. Die Reihenfolge der häufigsten fünf Bedrohungen hat sich auch 2023 dabei nicht verändert. Am stärksten gestiegen sind im Vergleich zu 2022 Phishing-Versuche per SMS oder Messenger um 5,9 Prozent, der Erhalt von Malware, also infizierter E-Mails, Anhänge oder Web-links um 4,3 Prozent, sowie Datenlecks bei Anbietern digitaler Dienste um 4,2 Prozent.

„Die Zunahme von IT-Sicherheitsvorfällen zeigt, wie wichtig es ist, die IT-Sicherheit weiter zu stärken. Hier sind der Staat, Unternehmen und Nutzer:innen gleichermaßen gefordert. Der geplante

„Die Zunahme von IT-Sicherheitsvorfällen zeigt, wie wichtig es ist, die IT-Sicherheit weiter zu stärken.“

Dr. Christiane Rohleder

EU-Cyber-Resilience-Act wird die Cybersicherheit deutlich verbessern, indem zum ersten Mal europaweit geltende Anforderungen an die Cybersicherheit von vernetzten Produkten gestellt werden. Aber auch die Förderung digitaler

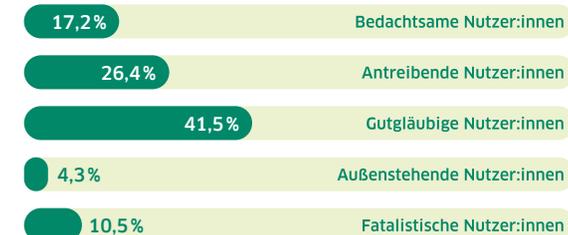
Kompetenzen in der Gesellschaft ist ein wesentlicher Faktor,“ erklärte Verbraucherstaatssekretärin Dr. Christiane Rohleder zur Vorstellung der Studie am Mittwoch. „Dabei müssen sich die Hilfestellungen im Umgang mit digitalen Risiken an den Bedürfnissen der Nutzenden orientieren. Der Einzug von Künstlicher Intelligenz in den Alltag vieler Menschen wird den Bedarf an solchen Angeboten weiter erhöhen.“

Digitale Verunsicherung rückläufig – Sicherheitsgefälle wächst

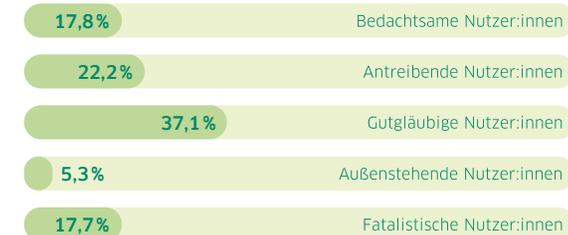
Auf den ersten Blick überraschend ist die Reaktion der Verbraucher:innen auf die erhöhte Bedrohungslage mit digitaler Sorglosigkeit. So ist das Verunsicherungsgefühl auf einen neuen Tiefstand von 21,5 Indexpunkten gesunken (- 24 Prozent). Der Anteil der „Gutgläubigen“ im Netz ist um 4,4 Prozentpunkte auf 41,5 Prozent gewachsen und baut seine Stellung als größte digitale Verbrauchergruppe

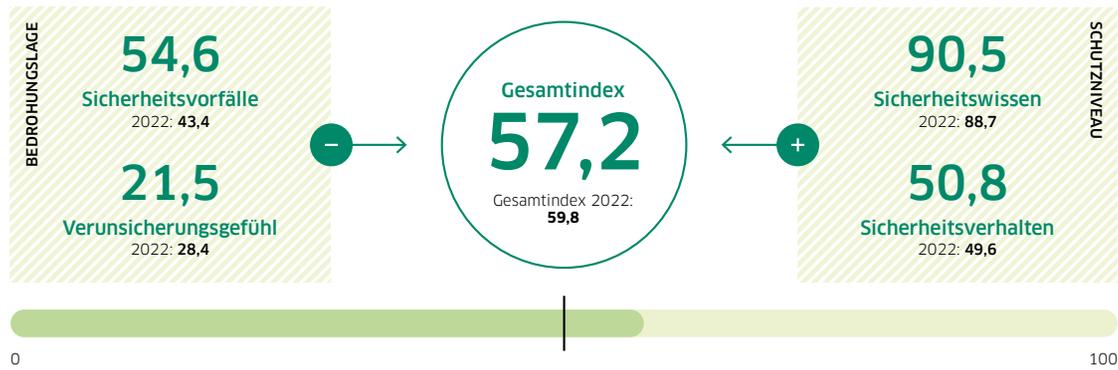
Verteilung der Anteile nach Nutzertypen an Gesamtheit der Internetnutzer:innen

2023



2022





aus. Gemeinsam mit den „Außenstehenden“ und „Fatalisten“ machen sie 56,4 Prozent der Onliner aus, deren Sicherheitslage deutlich unterdurchschnittlich ausfällt.

„Der Index zeigt ein IT-Sicherheitsgefälle zwischen den unterschiedlichen Verbrauchergruppen. Um dem entgegenzuwirken, setzen wir auf digitale Kompetenzförderung, die alle Menschen erreicht und zur Selbsthilfe befähigt“ bekräftigt DsiN-Geschäftsführer Dr. Michael Littger. Tatsächlich verbesserte sich das Sicherheitswissen der Verbraucher:innen um 1,8 Indexpunkte sowie auch das Sicherheitsverhalten um 1,2 Indexpunkte. Dieser Anstieg kann mit den wachsenden Risiken im Netz aber nicht Schritt halten.

„Der Index zeigt ein IT-Sicherheitsgefälle zwischen den unterschiedlichen Verbrauchergruppen. Um dem entgegenzuwirken, setzen wir auf digitale Kompetenzförderung, die alle Menschen erreicht und zur Selbsthilfe befähigt“

Dr. Michael Littger

Fokus Soziale Medien: Desinformation größte Herausforderung

Nach der Sondererhebung des DsiN-Sicherheitsindex 2023 zum Fokusthema „Soziale Medien“ nutzen 57,9 Prozent aller

befragten Personen soziale Netzwerke in ihrem Alltag. Der überwiegende Teil nutzt die sozialen Netzwerke zur Kommunikation mit Freund:innen und Familie (61,3 Prozent) und zur Unterhaltung (54,2 Prozent). Jede:r Dritte zur Information über das Tagesgeschehen (36,6 Prozent) und mehr als jede:r Achte zu politischen

„Wir brauchen ein Zusammenwirken aller Akteure, die sich für ein sicheres Netz engagieren.“

Paul Heimann

Fragestellungen (13,3 Prozent). Negative Erfahrungen mit sozialen Medien machten ein Viertel der Nutzer:innen (26,1 Prozent). Hier stehen Falschinformationen ganz vorn mit 50,8 Prozent, gefolgt von unerwünschten Nachrichten mit 49,5 Prozent und Cybermobbing mit 35,2 Prozent.

„Wir brauchen ein Zusammenwirken aller Akteure, die sich für ein sicheres Netz engagieren. Mit der neuen Initiative „Sicher handeln“ möchten wir Nutzer:innen über Risiken im Onlinehandel aufklären und ihnen universelles Anwendungswissen vermitteln, sodass sie sich wirksam gegen Betrug schützen können“, erklärte Paul Heimann, Geschäftsführer von Kleinanzeigen, DsiN-Mitglied und Partner des Fokusthemas „Soziale Medien“ im Sicherheitsindex 2023.

Fokusthema: Soziale Medien

- 57,9% aller Befragten nutzen soziale Netzwerke (2022: 54,3%).
- 36,6% nutzen soziale Medien, um sich über das Tagesgeschehen zu informieren, 13,3% diskutieren zum politischen Geschehen.
- 61,3% halten über soziale Medien Kontakt zu Freund:innen und Familie.
- 37,7% betrachten soziale Medien als zuverlässige Informationsquelle.
- 26,1% haben negative Erfahrungen gemacht, davon gut die Hälfte (50,8%) mit Falsch- oder Desinformation.

Vulnerable Verbraucher:innen und Ehrenamt als weitere Zielgruppen

Als Reaktion auf die erhöhten digitalen Aufklärungsbedarfe wird DsiN mit Unterstützung des Verbraucherschutzministeriums die Hilfestellungen für seh- und hörbbeeinträchtigte Menschen im Netz und Menschen mit Mobilitätseinschränkungen mit dem bundesweiten Angebot Digital-Kompass intensivieren und auch den Zugang zum DsiN-Digitalführerschein erleichtern. Darüber hinaus wird im Bundesnetzwerk Digitale Nachbarschaft das bayerische Landesprojekt Digital Verein(t) die Unterstützung von ehrenamtlichem Engagement in der Fläche weiter ausbauen und neue Standorte gründen. Die SiBa-App wird als zentrales Angebot über aktuelle Sicherheitsvorfälle im Verbund mit Kleinanzeigen und PayPal sowie Sicherheitsbehörden weiter ausgebaut und die Anzahl der heute bereits rund 100.000 Nutzer:innen weiter erhöht.

Sie können die aktuelle Studie als PDF herunterladen



Paul Heimann, CEO Kleinanzeigen, Mitglied bei DsiN und Partner der Studie

Alt und Jung: Gemeinsam für ein besseres Internet

SAFER INTERNET DAY 2023

Together for a better Internet – unter diesem Motto beteiligte sich DsiN mit zahlreichen Initiativen am jährlichen Safer Internet Day.

Auf dem zentralen SID-Event des Bundesverbraucherschutzministeriums am 14. Februar in Berlin sprachen Joachim Schulte (DsiN) und Katharina Braun (BAGSO) über die Erfahrungen im Projekt Digital-Kompass bei der Überwindung von struktureller Ungleichheit im digitalen Raum mit Blick auf ältere Benutzergruppen. Bereits zuvor fanden Aktionen der Projekte DigiBitS -Digitale Bildung trifft Schule und dem Digitalen Engel statt:

Darf man im Internet alles sagen? Grenzen der Meinungsfreiheit.

Am 07. Februar 2023 richtete das Team DigiBitS einen Workshop an einer Schule in Riesa in Sachsen im Rahmen des Safer Internet Days aus. Unter dem Motto „Darf man im Internet alles sagen? Grenzen der Meinungsfreiheit“ wurden Schüler:innen der Klassenstufen 7 bis 9 fit gegen Hate Speech gemacht. Der Workshop klärte über Formen und Auswirkungen von Hassrede auf und machte klar: Hate Speech kann strafbar sein und zur Anzeige gebracht werden. Die Schüler:innen kamen auch zu der Erkenntnis, dass es sich in zahlreichen Fällen lohnt, im Sinne einer wehrhaften Demokratie bewährte Reaktionsstrategien zu nutzen, Haltung gegenüber Hater:innen zu zeigen, Grenzen der Meinungsfreiheit zu setzen und beispielsweise Falschbehauptungen und Fake News mit Fakten und Argumenten zu widerlegen. So wurden die Teilneh-

mer:innen dafür sensibilisiert, Opfern von Hass und Hetze zu helfen und ihnen Unterstützung anzubieten. Die anwesenden Lehrkräfte beobachteten den Workshop und reflektierten ihre Beobachtungen, um Ansätze und Ideen für ihren eigenen Unterricht in weiteren Klassen zu implementieren. Das Konzept dahinter nennt sich „Unterricht im Unterricht“ und ist in Dänemark fester Bestandteil der Lehrkräfteaus- und Weiterbildung. Auch aus der Politik haben sich mehrere begeisterte Fürsprecher:innen gefunden, die die Relevanz der Initiative „Schule gegen Hate Speech – Für mehr Fairness im Netz“ für den Zusammenhalt unterstreichen.

Digitaler Engel: Datenschutz und Datensicherheit fit im Alter

Auch das DsiN-Projekt Digitaler Engel veranstaltete anlässlich des Safer Internet Days eine Schulung für Senior:innen. In dieser Veranstaltung wurden den Teilnehmer:innen die wichtigsten Begriffe zum Datenschutz sowie zur Datensicherheit wie Cookies, Updates, Backups, Phishing, Doxing oder Scam erklärt. Zudem werden bei den Workshops des Digitalen Engels Empfehlungen gegeben, wie Gefahren im Internet erkannt werden können und welche wichtigsten Einstellungen vorgenommen werden sollten, um auch im Alter sicher im Internet unterwegs zu sein.



Margit Stumpp, MdB a.D., ehemalige Sprecherin für Medien- und Bildungspolitik, Bundestagsfraktion Bündnis 90/ Die Grünen

„Wir brauchen eine Humanisierung des digitalen sprachlichen Miteinanders. Auch in der digitalen Kommunikation ist das Gegenüber kein Feind und Worte und Bilder sind keine Waffen. Langfristig ist die Investition in Medienkompetenz die wirksamste Präventivmaßnahme gegen Hassrede. Zur digitalen Bildung gehört vielerlei: die Fähigkeit, digitale Anwendungen zu nutzen, das technische Wissen um die Funktionsweisen digitaler Technologien sowie die Reflektion darüber, welche Auswirkungen digitale Technologien z. B. auf Alltag, Gesundheit und Gesellschaft haben. Je kompetenter junge Menschen mit digitalen Medien umgehen, desto sicherer und souveräner bewegen sie sich im Netz.“



Impressionen zur DigiBitS-Initiative „Schule gegen Hate Speech – Für mehr Fairness im Netz“

In Partnerschaft mit:



Gefördert vom:



Bundesministerium für Familie, Senioren, Frauen und Jugend



„Ich freue mich, dass wir mit den Projektpartnern und Engagierten gemeinsam an dem Ziel arbeiten, noch mehr Menschen den Weg in die digitale Welt zu ebnen.“

Steffi Lemke, Bundesministerin für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz

Empfänger: **BAGSO Service Gesellschaft und Deutschland sicher im Netz**

Betrag in Worten: eine Million achthunderteintausendneuhundert-einundneunzig

Betrag, Euro: **1.801.991,00***

Anlass: **Digital Kompass: Digitale Teilhabe für Menschen mit besonderen Aufklärungsbedarfen**

Digitale Teilhabe

FÜR MENSCHEN MIT SEHBEHINDERUNG, HÖRBEEINTRÄCHTIGUNG ODER MOBILITÄTSEINSCHRÄNKUNG

Am 22. Februar 2023 lud das DsiN-Projekt Digital-Kompass zur Auftaktveranstaltung mit Bundesverbraucherschutzministerin Steffi Lemke ein. Mit der neuen Ausrichtung des Projekts werden Menschen mit Hörbeeinträchtigung, Sehbehinderung und Mobilitätseinschränkung über die nächsten drei Jahre über konkrete Hilfestellungen im digitalen Alltag unterstützt. Adressiert werden dabei meist ältere Menschen. Dafür steht auch der offizielle Name des Projekt: „Digitale Teilhabe für Menschen mit besonderen Aufklärungsbedarfen“.

In der Umsetzung werden ehrenamtlich Engagierte in Zusammenarbeit mit dem

Deutschen Blinden- und Sehbehindertenverband e. V., dem Deutschen Schwerhörigenbund e. V., der Verbraucher Initiative e. V. und der Universität Vechta im Projekt befähigt, Menschen mit Einschränkungen im sicheren Zugang zu digitalen Anwendungen zu unterstützen.

Zum Startschuss überreichte Bundesverbraucherschutzministerin Steffi Lemke in Wittstock den Verbundpartnern, der Bundesarbeitsgemeinschaft der Seniorenorganisationen e. V. (BAGSO) und Deutschland sicher im Netz e. V. (DsiN), die Zuwendungsbescheide und betonte: „Menschen mit Sehbehinderung, Hörbeeinträchtigung und Mobilitätseinschränkung

v.l.n.r.: Sebastian Wegner, Bundesarbeitsgemeinschaft der Seniorenorganisationen e.V. (BAGSO), Marie-Christin Schoeffel, Referentin Digital-Kompass, Steffi Lemke, Bundesministerin für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz, Dr. Barbara Keck, Geschäftsführerin Bundesarbeitsgemeinschaft der Seniorenorganisationen e.V. (BAGSO), Dr. Michael Littger, Geschäftsführer Deutschland sicher im Netz e.V.

wollen an digitalen Themen teilhaben und mitwirken, das ist ihnen aber nicht immer uneingeschränkt möglich. Ich freue mich, dass wir mit den Projektpartnern und Engagierten gemeinsam an dem Ziel arbeiten, noch mehr Menschen den Weg in die digitale Welt zu ebnen.“

te: „Wir möchten, dass die Chancen des Internets gerade auch von Menschen sicher genutzt werden, die im Alltag mit körperlichen Einschränkungen leben und Bildungsangebote vor Ort nur schwer oder gar nicht aufsuchen können.“

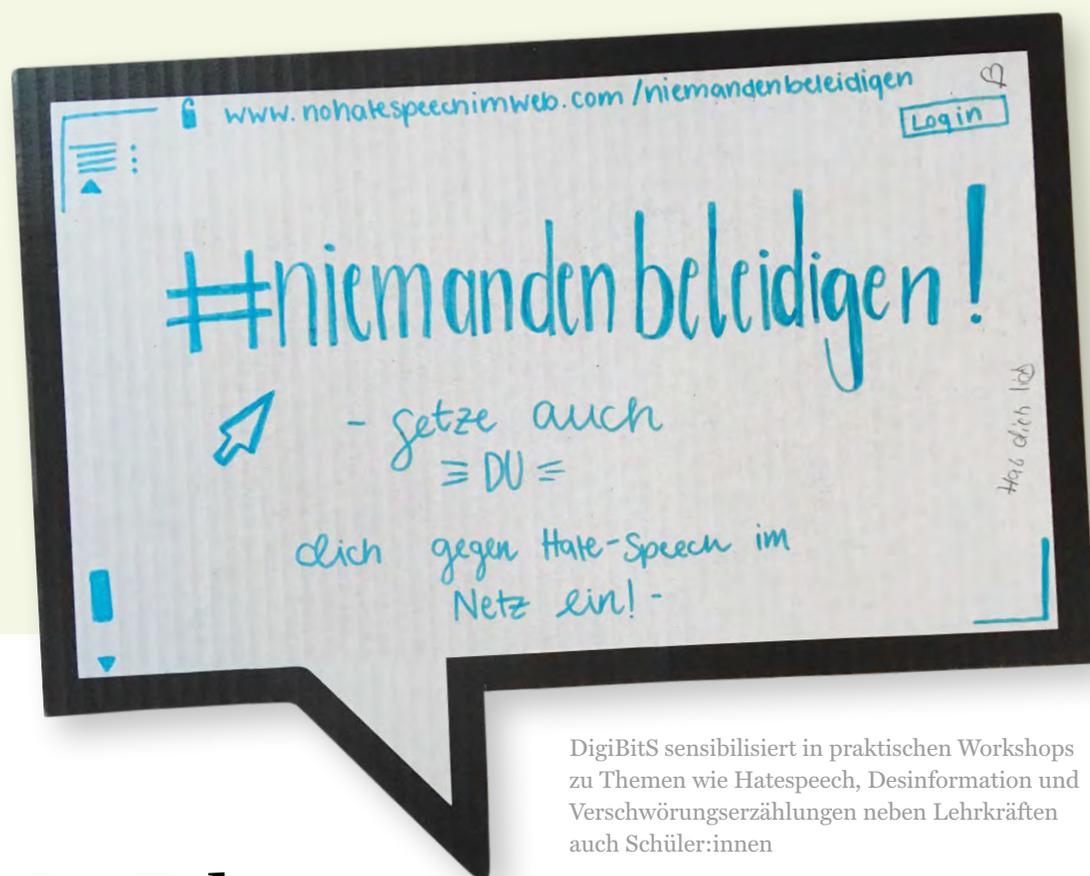
Die Angebote des Digital-Kompasses bringen auch Studierende und mobilitätseingeschränkte ältere Menschen in Lern-Tandems zusammen. In diesen Lern-Tandems werden digitale Grundkenntnisse anhand anschaulicher Materialien vermittelt. Der Austausch erfolgt in den eigenen vier Wänden oder nach individuellen Wünschen, beispielsweise über Telefon, Chat, E-Mail oder Videoanruf. Joachim Schulte, stellvertretender Geschäftsführer von DsiN und DiKo-Projektleiter, ergänz-

Das Projekt wird gefördert vom:



DigiBits

Digitale Bildung trifft Schule



DigiBitS sensibilisiert in praktischen Workshops zu Themen wie Hatespeech, Desinformation und Verschwörungserzählungen neben Lehrkräften auch Schüler:innen

Im Fokus: Desinformationen und Verschwörungserzählungen im Netz

DigiBitS hat 2023 im Verbund mit den Partnerprojekten weitklick und Medien in die Schule des Vereins FSM e. V. sowie der Suchmaschine für Kinder fragFINN die Initiative „Schule gegen Fake News – Medienkompetenz statt Desinformation“ gestartet. Denn Kinder und Jugendliche sind vor allem in sozialen Netzwerken wie YouTube, Instagram oder TikTok unterwegs. Dort treffen sie tagtäglich auf Fake News, die sie verwirren und irritieren, gar wütend oder Angst machen. Mit Folgen: Ihr Vertrauen in die Demokratie, in die Welt der Erwachsenen, die ihnen Sicherheit und Gewissheit geben soll, wird erschüttert. Eine Frage drängt sich auf: Was tun?

Zum Angebot gehören Workshops, Fachtage und Unterrichtsmaterialien. Zum Aktionstagen der Thüringer Landesmedienanstalt gegen Desinformation, Fake News und Verschwörungstheorien veranstaltete DigiBitS einen Workshop an der Erfurter Schule Otto Lilienthal.

DiFü für Lehrkräfte

Bildung braucht Digitalisierung – und Digitalisierung braucht Bildung. Denn iPads, Smartboards und digitale Tools sind nur dann sinnvoll, wenn Lehrkräfte sie sicher und souverän einsetzen. Das passende Know-how vermittelt der kostenlose Digitalführerschein für Lehrkräfte:

- Praxistipps zum digitalen Unterricht
- Cybersicherheit
- Daten- und Jugendmedienschutz
- Gefahren für Kinder und Jugendliche im Netz
- Hatespeech, Cybermobbing und Fake News
- Urheberrecht in der Schule

Hol dir dein Zertifikat!
www.difue.de/lehrkraefte

Mehr Informationen zur Initiative finden Sie hier:



Mit Medienkompetenz gegen Desinformation

Zum DigiBitS-Angebot gehörten 2023 neben Workshops auch Unterrichtsmaterialien, die in Zusammenarbeit mit dem Projekt weitklick des DsiN-Partners FSM entwickelt und an Fortbildungsinstituten in Thüringen und Sachsen sowie vor Ort in Berlin mit insgesamt mehr als 50 Lehrkräften erfolgreich durchgeführt wurden. Der Fokus lag auf dem Ziel, Kinder und Jugendliche zu befähigen, zwischen glaubwürdigen und unglaubwürdigen Aussagen unterscheiden zu können.

Außerdem müssen Schüler:innen mit zunehmendem Alter lernen, die Seriosität ihrer Quellen zu erkennen (Informationskompetenz). Sie ist ein Aspekt von Medienkompetenz, die in allen Lehrplänen bundesweit verankert ist, leider immer noch zu wenig im Unterricht gefördert wird.

Mitglieder DigiBitS



FSM





(von links nach rechts) Elisabeth Wisniewski, DsiN Projektleiterin; Florian Eiben, Bürgermeister der Stadt Norden; Johann Saathoff, Parlamentarischer Staatssekretär im Bundesministerium des Innern und für Heimat

DsiN-Digitalführerschein

STAATSEKRETÄR JOHANN SAATHOFF MDB VERLEIHT DSiN-DIGITALFÜHRERSCHEIN AN BÜRGERMEISTER EIBEN

Seit Frühjahr 2022 bietet der DiFü allen Bürger:innen kostenfrei die Möglichkeit, ihre digitalen Kompetenzen zu erweitern und darüber hinaus ein persönliches Zertifikat zu erwerben.

Zu den Absolvent:innen des DiFüs gehört nun auch Florian Eiben, Bürgermeister der Stadt Norden, der im April 2023 sein DiFü-Zertifikat von Johann Saathoff, Parlamentarischer Staatssekretär im Bundesministerium des Innern und für Heimat, überreicht bekam.

Er sagte: „Die Nachfrage zum Digitalführerschein zeigt, dass Bürger:innen zur Förderung ihrer Digitalkompetenz ermuntert werden können. Hier wollen wir ansetzen und noch mehr Menschen vom DiFü-Zertifikat überzeugen.“

Um das Angebot auch als berufsförderndes Zertifikat noch bekannter zu machen, wird der DiFü nun auch verstärkt in Vereinen, Betrieben sowie öffentlichen Verwaltungen beworben. Zu den neuen DiFü-Teilnehmenden gehört auch die Verwaltung der Stadt Norden in Niedersachsen.

Florian Eiben, Bürgermeister der Stadt und DiFü-Absolvent, ist überzeugt: „Der DiFü ist unkompliziert nutzbar und vermittelt Medienkompetenz auf spielerische Weise.“

Viel einfacher dürfte sich eine Weiterbildungsmaßnahme nicht in Vereinen oder Betrieben integrieren lassen können. Auch Schulen und Lehrkräfte könnten besonders davon profitieren.“

Den Termin nutzte DsiN zum Anlass, auch einen Workshop im Rahmen seines Projekts Digitale Nachbarschaft für Ehrenamtsträger:innen der Stadt Norden auszurichten und stellte den DsiN-Digitalführerschein als Weiterbildungsmaßnahme vor.

Gefördert durch:



Bundesministerium
des Innern
und für Heimat

aufgrund eines Beschlusses
des Deutschen Bundestages

Partner DiFü:



Digitale Unterstützung für Vereine – ist doch Ehrensache



Unser gesellschaftlicher Zusammenhalt ist auf das ehrenamtliche Engagement von engagierten Menschen angewiesen: Derzeit setzen sich ca. 29 Mio. Menschen in Deutschland für das Wohl anderer ein.

Digitale Dienste, neue Tools und Social Media verändern die Formen der Zusammenarbeit, der Kommunikation und sogar des Engagements. Wie in kaum einem anderen Bereich sind die technischen Voraussetzungen und das Vorwissen zu digitalen Alltagsschancen jedoch so unterschiedlich wie bei Ehrenamtlichen: vom Jugendlichen bis zum Ruheständler, vom digital hoch Affinen bis

zum Offliner, vom extrovertierten Netzwerker bis zum ruhigen Schatzmeister.

Die Bildungsangebote müssen deshalb vorab besonders gut mit den Teilnehmer:innen abgestimmt werden. Im Freistaat Bayern führt DsiN in enger Kooperation mit der Landesarbeitsgemeinschaft der Freiwilligenorganisationen e.V. (lagfa)

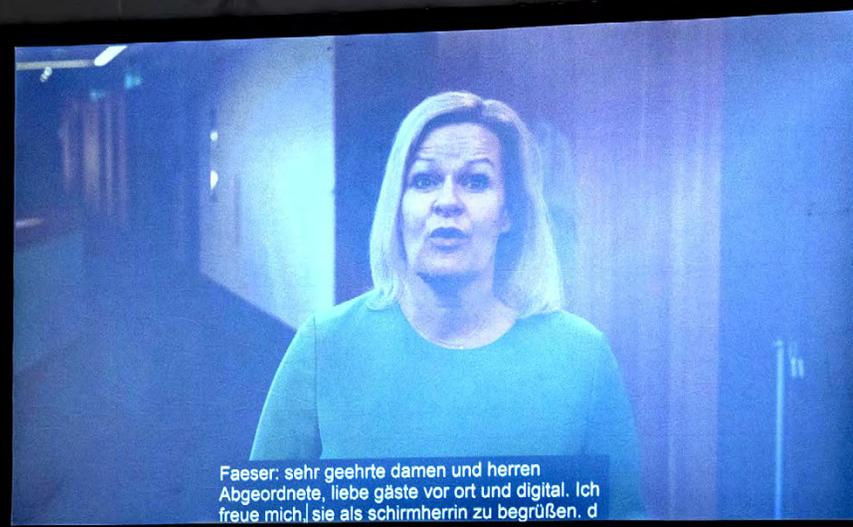
das Projekt digital verein(t) durch. Es ist somit Teil des Bundesnetzwerks Digitale Nachbarschaft und bietet ein buntes Portfolio zu allen Digitalthemen, die für das organisierte Ehrenamt wichtig sind: Von der sinnvollen Nutzung von Social Media über rechtliche Fragen beispielsweise zur Verwendung von Fotos bis hin zu digitalen Formen der Mitgliederverwaltung und Finanzfragen. An 28 Standorten landesweit finden Workshops mit Engagierten in Präsenz oder online statt. Die mobilen Referent:innen reisen mit dem projekteigenen Infomobil an und bringen Informationsmaterialien und Schulungsunterlagen mit. In 56 Workshops wurden 1.900 Engagierte erreicht.

Auch in Sachsen-Anhalt hat das Bundesnetzwerk Digitale Nachbarschaft Engagierte in Vereinen unterstützt: Gemeinsam mit der lagfa Sachsen-Anhalt hat DsiN das Projekt >Engagement Digital – Netzwerke stärken< durchgeführt und Workshops durchgeführt.

Kooperationspartner:

lagfa bayern

DSiN
JAHRES
KONGRESS
2023



Faeser: sehr geehrte damen und herren
Abgeordnete, liebe gäste vor ort und digital. Ich
freue mich, sie als schirmherrin zu begrüßen. d

DSiN
JAHRES
KONGRESS
2023

merksamkeit. (Bertan)
wobbe: vielen dank für die einle
Einiges wurde genannt, worum
erwerb digitaler Kompetenzen. D
schirmherrschaft des bundesinn
Jetzt freuen wir uns auf das gruf
ministerin faeser.
Faeser: sehr geehrte damen und
Abgeordnete, liebe gäste vor ort
freue mich, sie als schirmherrin z

„Deutschland sicher im Netz
trägt mit seinen konkreten
Hilfestellungen und Tipps
ganz praktisch zur Förderung
von Digitalkompetenzen in
der Breite der Gesellschaft
bei – und das schon seit
Jahren und mit großem
Erfolg – denn Cyberresilienz
ist eine Aufgabe für uns alle.“

Eröffnungsrede zum DsiN-Jahreskongress 2023, Nancy Faeser, DsiN-
Schirmherrin, Bundesministerin des Inneren und für Heimat

DSIN JAHRES KONGRESS 2023

Cyberresilienz für Demokratie & Sicherheit Desinformation entgegenwirken

Am 14. Juni 2023 lud DsiN unter dem Leitthema „Cyberresilienz für Demokratie und Sicherheit – Desinformation entgegenwirken“ zum Jahreskongress ins Hotel Oderberger in Berlin Prenzlauer Berg ein.

Im Austausch mit 35 Referent:innen in acht Panels standen Strategien und Maßnahmen für die digitale Kompetenzförderung in der Breite der Gesellschaft im Fokus. Auf den Ausstellungsflächen des Kongresses veranschaulichten zahlreiche Projekte von DsiN und seiner Mitglieder, wie Digitalkompetenz als Baustein für Cyberresilienz und digitale Teilhabe vermittelt wird.

Forderung nach Stärkung der digitalen Kompetenzförderung

Zusätzliche Aufmerksamkeit gewann der Kongress durch die aktuellen Herausforderungen von Desinformationen und Fake News, die durch den Einsatz von Künstlicher Intelligenz zuletzt deutlich zugenommen hatten.

DsiN-Schirmherrin Nancy Faeser sprach sich zu Beginn des Kongresses im Grußwort für eine deutliche Stärkung der digitalen Aufklärungsarbeit aus: „Je mehr

Menschen sich mit Cybersicherheit beschäftigen, desto mehr selbstbestimmte digitale Teilhabe gibt es.“

Dass an einer Stärkung der digitalen Kompetenzförderung kein Weg vorbeiführt, betonte Thomas Tschersich, DsiN-Vorstandsvorsitzender: „Cyberresilienz braucht Digitalkompetenz, im privaten Umfeld sowie für unternehmerische Entscheidungen.“ Sie gehöre zu den zentralen Herausforderungen, um Sicherheit und Vertrauen in Zeiten wachsender Bedrohungslagen sowie Desinformation und Hetze zu stärken.

Bedeutung von Transfernetzwerken und öffentlicher Förderung

Um eine „Zeitenwende“ für mehr digitale Basiskompetenzen zu erreichen, verwies Dr. Robert Reinermann, Vorsitzender der VdS Schadenverhütung und Mitglied im DsiN-Vorstand, im Eröffnungspanel auf



Eröffnungsrede von Andreas Könen, DsiN-Beiratsvorsitzender
Abteilungsleiter für Cyber- und Informationssicherheit, BMI

„Mit wachsenden Cyberbedrohungen und Desinformationen gewinnen Digitalkompetenzen an Bedeutung.“

Zitat & Foto: Thomas Tschersich, DsiN-Vorstandsvorsitzender Chief Security Officer (CSO), Deutsche Telekom AG

bereits vorhandene Lösungskompetenzen in Deutschland hin. Wirtschaft und Zivilgesellschaft hätten mit Unterstützung der Bundesregierung bereits frühzeitig in Strukturen der nonformalen Fortbildung und Kompetenzförderung investiert. Beispiele dafür seien die Initiativen „Digitale Nachbarschaft“ und „Bottom-Up für Berufsschulen“, so Reiner Mann. Hier müsse gewährleistet werden, dass solche Transfernetzwerke nachhaltig gestärkt und in den Sicherheitsstrategien von Bund und Ländern verankert werden.

In ihrem Statement zum Fachpanel über Desinformation beschrieb Marie-Agnes Strack-Zimmermann, dass sie täglich rund 250 Taten zur Anzeige bringe. Aus Sicht der Politikerin übersteigen Angriffe, denen Personen des öffentlichen Lebens schon heute im Netz ausgesetzt seien, ein demokratiegefährdendes Ausmaß. Dass die Herausforderung durch Fake News und Verleumdungen mit der Verbreitung von Künstlicher Intelligenz an Schärfe zunehmen, waren sich die Teilnehmer:innen des Fachpanels einig. Notwendig seien klare Vorgaben auch auf europäischer Ebene, wo der Digital Service Act eine Chance böte, sowie lebenslange Kompetenzförderung.

Chancen der KI im Kampf gegen Cyberangriffe?

Zum Einzug von Künstlicher Intelligenz wurden auch die Chancen benannt, die im Kampf gegen Cyberangriffe und Bedro-

hungen möglich sind. Sie müssten in Betracht gezogen und diskutiert werden, so die Botschaft des Kongresspanels zu KI mit Vertreter:innen des Bundesinnenministeriums, des Einstein Centers, Google Deutschland und des DsiN-Digitalführerscheins, das mit einem Impuls von Ayad Al-Ani eröffnet wurde. Dabei gehe es um wirksamere Strafverfolgung und -vermeidung sowie die Erkennung von rechtswidrigen Inhalten im Netz. Jedoch erforderten die neuen Möglichkeiten eine Debatte über rechtliche und ethische Grenzen, über diese aufgeklärt werden muss und die für Bürger:innen nachvollziehbar sein muss.

Nachholbedarf auch in Betrieben und Ausbildung

Erheblichen Nachholbedarf in puncto digitale Kompetenzförderung machten die Teilnehmer des Fachpanels #IT-Sicherheit in kleineren Betrieben sowie der Berufsausbildung aus. Fast die Hälfte aller Unternehmen (44 Prozent) verzichteten laut des aktuellen DsiN-Praxisreports auf jede Art der Kompetenzförderung, wobei auch weitergehende Maßnahmen der Prävention und Abwehr von Sicherheitsangriffen längst nicht ausreichend etabliert seien. Ursächlich seien fehlende Ressourcen in den Betrieben und Berufsschulen für Fortbildungs- und Ausbildungsangebote sowie Nachholbedarf in der zielgruppengerechten Bündelung von vorhandenen Angeboten. Aus dem Bundeswirtschaftsministerium verwies



Das Video zum DsiN-Jahreskongress.
Hier reinschauen!

Eröffnungspanel mit Tobias Wobbe, Dr. Eva Flecken, Dr. Robert Reinermann,
Katharina Kunze, Sven Ursinus, Ariane Fäscher (v. l. n. r.)



Abteilungsleiterin Frau Dr. Brönstrup auf die Initiative TISiM – Transferstelle IT-Sicherheit im Mittelstand, die ab Sommer mit zusätzlichem Fokus auf junge Unternehmen sowie Angriffserkennung unter CyberSicher neu aufgestellt würde.

Dr. Christiane Rohleder, Staatssekretärin im Bundesverbraucherschutzministerium, bekräftigte die Bedeutung digitaler Kompetenzen in der Breite der Gesellschaft, um Cyberresilienz für mehr Sicherheit und ein demokratisches Miteinander zu fördern. Sie betonte, dass hier sowohl der Staat als auch Unternehmen und die Nutzer:innen gefordert seien. Auch der Vorsitzende des Brandenburgischen Berufsschullehrerverbandes, Thomas Pehle, bekräftigte den Zusammenhang zwischen IT-Sicherheit und Bildungsarbeit: „Wir müssen zeigen, welchen wichtigen Beitrag Initiativen wie Bottom Up für Berufsschulen und mIT Sicherheit schon heute leisten, aber auch, welche zusätzlichen Anreize erforderlich sind, um diese Initiativen nachhaltig aufzustellen.“

Angebote für alle Alters- und Berufsgruppen

Für den Innenpolitiker Manuel Höferlin gelten die Anforderungen der Kompetenzförderung für alle Bevölkerungsteile und Berufsgruppen – auch Politiker: innen. „Politiker:innen, auch ehrenamtliche, stehen immer wieder im Fokus von Cyberangriffen und Doxing. Mit Initiativen wie PolisiN-Politiker:innen sicher im Netz ist es schon heute möglich, IT-Sicherheit im politischen Alltag vorzuleben und Desinformationskampagnen entgegenzuwirken, um Vorbild für andere zu sein“. Hier müsse man ansetzen, so Höferlin, denn Cybersicherheit ist und bleibe die Achillesferse der modernen Informationsgesellschaft.



Der Jahreskongress wurde von den DsiN-Mitgliedern unterstützt, insbesondere von



Ausstellungsflächen auf dem DsiN-Jahreskongress 2023



Auf dem Abschlusspanel: Tabea Rößner, Manuel Höferlin, Thomas Jarzombek, Dr. Michael Littger (v. l. n. r.)

FACTS AGAINST FAKES

Preisverleihung myDigitalWorld 2023

Die aktuelle Ausschreibung des Jahres 2022/2023 unter Schirmherrschaft von Bundesdigitalminister Dr. Volker Wissing stand unter dem Motto „Facts Against Fakes“ mit der Fragestellung, wie Verschwörungstheorien, Fake News und Desinformation im Netz durch Medienkompetenz begegnet werden kann. Dabei standen die Aufgaben vor dem Hintergrund der Entwicklungen in der Corona-Pandemie und dem Angriff auf die Ukraine.

Hauptpreisträger aus Berlin: 11. Klasse des Droste-Hülshoff-Gymnasiums

Der Politikwissenschaften-Leistungskurs der 11. Stufe des Droste-Hülshoff-Gymnasiums in Berlin überzeugte die Jury in diesem Jahr mit einem Video-Beitrag, der fundiert und zugleich unterhaltsam die unterschiedlichen Facetten von Fake News aufzeigt und technisch überzeugend vermittelt.

Die Preisverleihung erfolgte im Rahmen des DsiN-Jahreskongresses als Abendveranstaltung. Schirmherr Bundesminister Dr. Volker Wissing hielt die Laudatio und würdigte die Einreichungen als fundamentalen Beitrag für eine digital aufgeklärte Gesellschaft. Als besondere Überraschung wurden die 1. Gewinner zur Mitwirkung im Jugendrat der Medienanstalt Berlin-Brandenburg eingeladen, wie deren Direktorin Dr. Eva Flecken übermittelte.

Außerdem wurden alle Schüler:innen des Droste-Hülshoff-Gymnasiums in das Bundesministerium für Digitales und Verkehr eingeladen, wo sie mit Vertreter:innen des Ministeriums über ihre Erfahrungen im Umgang mit Fake News sprechen konnten.

2. Platz und 3. Platz gehen nach Hamburg und Nürnberg

Der Kurs „Politik, Wirtschaft & Geschichte“ der 11. Klasse der Stadtteilschule Süderelbe in Hamburg reichte eine vertonte Präsentation ein, die sich gut strukturiert und inhaltlich fundiert mit dem Wettbewerbsthema befasste. Besonders positiv würdigte die Jury, dass sich der Beitrag auch mit Erfahrungen im eigenen Umfeld beschäftigte.

Die Schüler:innen des Informatikkurses der 7. Klasse am Hans-Sachs-Gymnasium in Nürnberg reichten einen Videobeitrag ein, der unterhaltsam in Form kleiner „Sketches“ verschiedene Arten von Fake News thematisierte und einordnete, um am Ende zehn Empfehlungen und konkrete Tipps zum Umgang mit Falschnachrichten auszusprechen.



Seit 2014 würdigt DsiN im Jugendwettbewerb myDigitalWorld junge Menschen, die sich für einen sicheren und selbstbestimmten Umgang mit dem Internet engagieren.

Aufruf zur Teilnahme 2023/24: Ist das Kunst oder kann das KI?

Zum neuen Start für das Schuljahr 2023/2024 rief Bundesminister Dr. Volker Wissing Schüler:innen in ganz Deutschland zur Teilnahme am Wettbewerb unter dem Motto „Ist das Kunst oder kann das KI?“ auf: „Spätestens mit dem Start von ChatGPT ist allen klar geworden: KI ist ein Gamechanger und gekommen, um zu bleiben. Wir können innerhalb weniger Minuten Inhalte erstellen, für die wir sonst Stunden brauchen. Es ist wichtig, dass junge Leute lernen, damit umzugehen. Jedoch bringt KI auch Herausforderungen mit sich und verlangt ein hohes Maß an Medienkompetenz, beispielsweise um KI-generierte Inhalte zu erkennen. Daher ist es wichtig, junge Menschen im sicheren Umgang mit digitalen Technologien zu fördern.“

In Partnerschaft mit:



Der Kinderschutzbund
Bundesverband



Google Safety Engineering Center



Lokal, persönlich und konkret

Auch 2023 zeigen die Maßnahmen des Projekts großen Erfolg - sei es durch zahlreiche Schulungen für Personen im Umfeld älterer Menschen oder durch direkte Beratung vor Ort. Die Sichtbarkeit des Digitalen Engels konnte nochmals gesteigert werden: Das zeigen über 900 Presseberichterstattungen und über ein Dutzend Ausstrahlungen im regionalen und überregionalen Fernsehen.

Digitale Dienste bieten vielfältige Chancen für eine selbstbestimmte Gestaltung, Bereicherung und Erleichterung des Alltags älterer Menschen. Ihre „digitale Teilhabe“ umfasst mehr soziale Kontakte zu Familie und Freunden, Onlineterminen mit Gesundheitsdiensten oder Behörden, eine kompetente Informationsrecherche sowie die Vermeidung von konkreten Risiken und digitalen Gefahren im Netz. Um diese Vorteile zu nutzen und Vorbehalten sowie Risiken zu begegnen, fördert das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) das Projekt Digitaler Engel. Es richtet sich an ältere Menschen, die digitale Kompetenzen erwerben wollen, um in der Online-Welt sicher zu agieren, und unterstützt Wissensvermittler:innen dabei, ein nachhaltiges und vertrauenswürdige Angebot vor Ort zu schaffen. Das Projekt Digitaler Engel ist Bestandteil

der Umsetzungsstrategie der Bundesregierung zur Gestaltung des digitalen Wandels und unter dem Dach des Digitalpakts Alter eine konkrete Maßnahme zur Förderung der digitalen Teilhabe älterer Menschen.

Online-Schulungen: ein Angebot für Wissensvermittelnde

Das Jahr 2023 startete mit dem neuen Maßnahmenpaket für Menschen aus dem Umfeld älterer Menschen, die Interesse daran haben, ihr Digitalwissen weiterzugeben. In 60 Online-Schulungen zu sieben didaktischen und fachlichen Lerneinheiten wurden über 600 Interessierte geschult, die ein Digitalangebot in ihrem Seniorentreff initiieren möchten. Zur Unterstützung der Akteure der Seniorenbildungsarbeit wurde zudem ein Methodenkoffer entwickelt und produ-



Ein Digitaler Engel berät ältere Menschen im Bürgerhaus in Unterföhring

ziert. Er beinhaltet Lernhefte für die zielgruppengerechte Vermittlung aktueller digitaler Themen, praktische Anleitungen und ein Train-the-Trainer-Schulungskonzept zum DsiN-Digitalführerschein. Durch passende Online-Schulungen der Digitaler Engel wurde das Wissen vertieft und weiterführende Fragen beantwortet.

In 60 Online-Schulungen zu sieben didaktischen und fachlichen Lerneinheiten wurden über 600 Interessierte geschult, die ein Digitalangebot in ihrem Seniorentreff initiieren möchten.

Mit dieser Maßnahme wurden nun auch die Partner aus der lokalen Seniorenarbeit in ihrer Arbeit für ältere Men-

schen unterstützt und zum Beispiel dazu angeleitet, wie ein Smartphone-Café aufgebaut werden könnte.

Digitaler Engel vor Ort: ein Angebot für Freiwillige aus den Freiwilligendiensten FSJ & BFD

Die Bedeutung von Senioreneinrichtungen dabei, ältere Menschen an digitale Technik heranzuführen und im Prozess des Wissens- und Kompetenzerwerbs zu begleiten, nimmt zu. Mobilitätseingeschränkte und hochaltrige Menschen können über ein Bildungs- oder Freizeitangebot in ihrer Wohn- und Pflegeeinrichtung erreicht werden und sich darüber hinaus gegenseitig unterstützen, ermutigen und über Neuerungen austauschen. Um auch diese Menschen in Einrichtungen der Altenhilfe nachhaltig zu erreichen, startete im Herbst 2023 die



Digitale Engel am Infomobil mit älteren Menschen in Bad Kreuznach



Ein Digitaler Engel berät ältere Menschen im MehrGenerationenHaus in Bad Salzungen (Bild: Elvira Fischer, Seniorenbüro Wartburgkreis)

Maßnahme "Digitaler Engel vor Ort", in der junge Freiwillige aus den Freiwilligendiensten FSJ und BFD qualifiziert werden, an ihrer Einsatzstelle ein Angebot für Ältere durchzuführen. Mit fünf Einsatzstellen bundesweit startete die Maßnahme mit den Qualifizierungen der Freiwilligen als kompetente Ansprechpartner:innen an ihrer Einsatzstelle. Diese Qualifizierung beinhaltet neben der Vermittlung relevanter digitaler Inhalte besonders auch didaktische Hinweise zur gezielten Vermittlung von Kompetenzen an Ältere. Mit dieser

Maßnahme wird auch in Einrichtungen der Altenhilfe ein nachhaltiges Angebot für die digitale Teilhabe älterer Menschen geschaffen und gleichzeitig der generationenübergreifende Ansatz, voneinander zu lernen, gefördert.

Infomobile: ein bundesweites Angebot für ältere Menschen

Der Digitale Engel hat mit seinem aufsuchenden Ansatz und der konkreten Ansprache im persönlichen Umfeld älterer Menschen eine bundesweite

Projekt Digitaler Engel: Hilfe für Senior:innen im Umgang mit Technik

Apps auf dem Smartphone installieren, ein W-LAN einrichten, online Geld überweisen: Was für viele selbsterklärend ist, stellt insbesondere ältere Menschen oft vor Herausforderungen. Das Projekt Digitaler Engel will ihnen dabei helfen. Ein Expertenteam fährt dafür durch alle 16 Bundesländer und zeigt Senior:innen, wie sich technische Geräte einrichten und nutzen lassen.

Das geschieht bei Seniorentreffs, auf Marktplätzen oder in Online-Veranstaltungen. Der Verein Deutschland sicher im Netz, Träger des Projekts, wird dafür vom Bundesministerium für Familie, Senioren, Frauen und Jugend finanziell gefördert.



Termine der geplanten Veranstaltungen sowie Schulungsvideos stehen auf der Website digitaler-engel.org.

Strahlkraft. Durch die Alltagsnähe der Themen und die individuelle Beratung vor Ort erreicht der Digitale Engel die Menschen direkt in ihrem Lebensumfeld und schafft dadurch einen Zugang mit nachhaltiger Wirkung. In knapp 300 Veranstaltungen vor Ort wurden im persönlichen Gespräch individuelle Bedarfe und Herausforderungen identifiziert und Lösungen angeboten. Auch Menschen mit wenig oder gar keinen Erfahrungen im Internet wurden durch die Digitalen Engel über Mehrwerte digitaler Angebote informiert. Zudem wurden bei allen 297 Stationen lokale Anlaufstellen für ältere Menschen durch den Verweis auf deren Bildungsangebote bekannt gemacht.

Der Digitale Engel zeigt, wie wichtig es ist, auf die Menschen zuzugehen und ihnen aktiv Unterstützung bei einer sicheren Nutzung des Internets anzubieten.

Durch diese Herangehensweise ist der Digitale Engel ein Vorbild für weitere Angebote und Landesprojekte im Bereich der digitalen Bildung und Unterstützung geworden. Als Best Practice wurde der Digitale Engel im Konzept der Seniorenmedienbildung des Landes Thüringen berücksichtigt und wird nun im nächsten Jahr mit einem landeseigenen Infomobil in Thüringen unterwegs sein. Dieses Vorhaben wird vom Thüringer Ministerium für Arbeit, Soziales, Gesundheit, Frauen und Familie gefördert.





Schutz vor Online-Betrug

DIE „INITIATIVE SICHER HANDELN – ISH“ KLÄRT AUF

Online-Betrug beeinträchtigt das Einkaufserlebnis und kann zu erheblichen Schäden führen – ein Problem, das die „Initiative Sicher Handeln – ISH“ neu bekämpft. Sie klärt Verbraucher:innen über Schutzmaßnahmen gegen Identitätsdiebstahl und Warenbetrug auf. Doch wie effektiv sind ihre Maßnahmen – und wie erreichen sie Menschen?

Die nun seit einem Jahr aktive „Initiative Sicher Handeln – ISH“, zielt darauf ab, Verbraucher:innen über Risiken und Präventionsmaßnahmen im Onlinehandel aufzuklären. DsiN unterstützt als Bindeglied die ISH, welche vom DsiN-Mitglied Kleinanzeigen und weiteren Partnern getragen wird. Dazu zählen die Polizeiliche Kriminalprävention der Länder und des Bundes (ProPK), die Stiftung Deutsches Forum für Kriminalprävention (DFK), das Bundesamt für Sicherheit in der Informationstechnik (BSI), aber eben auch die Unternehmen RISK IDENT sowie Deloitte .

Online-Betrug ist ein weit verbreitetes Phänomen, das von Identitätsdiebstahl über Warenbetrug bis hin zu Phishing reicht. Besonders häufig werden Verbraucher:innen beim Online-Kauf über kleine Online-Shops oder auf Social-Media-Plattformen getäuscht. Die ISH spricht dazu über Themen wie Passwortsicherheit, Fake Shops, aber auch neueste Betrugsmaschen per SMS (Smishing) oder Messenger-Diensten wie WhatsApp. Auf diese Weise hat sie im ersten Quartal 2024 den Fokus auf das Thema digitale Identität gerichtet.



Ein Schneewittchen-Kampagnenmotiv der Initiative Sicher Handeln:
Die Kampagne soll auch jüngere Menschen ansprechen.

Themenschwerpunkt „Digitale Identität“ | Planung für 2024

Die Zunahme von Online-Transaktionen und die stetige Präsenz in digitalen Medien haben dazu geführt, dass die digitale Identität eines Einzelnen sowohl eine wertvolle Ressource als auch ein potenzielles Ziel für kriminelle Aktivitäten geworden ist.

- Eine digitale Identität umfasst alle persönlichen Daten und digitalen Fußabdrücke, die eine Person im Internet hinterlässt. Dazu gehören Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern, Bankinformationen und vieles mehr. Diese Informationen ermöglichen es Individuen, online zu interagieren, Dienstleistungen zu nutzen und Geschäfte zu tätigen.

- Identitätsdiebstahl tritt auf, wenn jemand unbefugt persönliche Informationen einer anderen Person verwendet, um Betrug zu begehen. Dies kann das Eröffnen von Konten, das Erhalten von Krediten oder das Tätigen von Einkäufen im Namen des Opfers umfassen. Die Folgen können von finanziellen Verlusten bis hin zu langfristigen Schäden an der Kreditwürdigkeit reichen.

Online-Shopping-Betrug ist oft direkt mit Identitätsdiebstahl verbunden. Betrüger nutzen gestohlene Identitätsdaten, um Waren oder Dienstleistungen online zu erwerben. Sie können auch gefälschte Online-Shops einrichten, um Kreditkartendaten ahnungsloser Käufer zu sammeln. Solche Aktivitäten schaden nicht nur den unmittelbaren Opfern, sondern untergraben auch das Vertrauen in die digitale Wirtschaft.



Ein ISH-Kampagnenmotiv, das ein Kondom zeigt.

Überraschend: Besonders junge Menschen häufig Opfer von Betrug

Die ISH hat herausgefunden, dass Identitätsdiebstahl in Deutschland besonders junge Erwachsene trifft. Eine Umfrage ergab, dass viele junge Leute riskante Online-Praktiken anwenden wie die Nutzung gleicher Passwörter für verschiedene Konten oder das Versenden persönlicher Dokumente an Unbekannte. Zudem nutzen Kriminelle verstärkt „Künstliche Intelligenz“ (KI), um Betrug zu automatisieren, insbesondere auf Wohnungsmärkten und durch „Money

Muling“, was die Geldwäsche erleichtert. Es sei vor allem die Sorglosigkeit junger Menschen, welche die Akteur der ISH besorge, hieß es in einer dazugehörigen Pressemitteilung, die deutschlandweit in nahezu allen nennenswerten Medien Verbreitung fand.

Die Aktivitäten der ISH sollen dabei die Öffentlichkeit über sichere Online-Praktiken aufklären, Ressourcen zum Schutz der digitalen Identität zur Verfügung stellen und Opfern von Identitätsdiebstahl und Online-Betrug konkrete Ansprechpartner aufzeigen. Durch die Stärkung der digitalen Bildung und die Förderung sicherer

Im Kern steht die „SHS-Regel“. Sie gliedert sich in drei Schritte der jeweiligen Anfangsbuchstaben: Stoppen, Hinterfragen und Schützen.

Online-Verhaltensweisen helfen solche Initiativen, die Risiken im Zusammenhang mit digitalen Identitäten und Online-Transaktionen zu mindern.

Im Kern steht die „SHS-Regel“. Sie gliedert sich in drei Schritte der jeweiligen Anfangsbuchstaben: Stoppen, Hinterfragen und Schützen. Nutzer:innen sollen demnach im Falle vor dem Kauf pausieren und kritisch bewerten, ob es sich um seriöse Anbieter handelt. Im zweiten Schritt wird geraten, Angebote zu hinterfragen, etwa bei besonders attraktiven Preisen wie bspw. ein ungewöhnlich günstiges Smartphone. Schließlich sollten verdächtige Aktivitäten an Plattformen

Aufmerksamkeit im Alltag erlangt. Dies ermöglicht es ihr, effektive Strategien zur Prävention von Online-Betrug zu entwickeln und umzusetzen, die direkt auf die Bedürfnisse der Verbraucher abgestimmt sind. Durch Bildung, Prävention und direkte Unterstützung stärkt sie die Widerstandsfähigkeit der Gesellschaft gegenüber Cyberkriminalität.

Durch Bildung, Prävention und direkte Unterstützung stärkt die Initiative die Widerstandsfähigkeit der Gesellschaft gegenüber Cyberkriminalität.

gemeldet und gegebenenfalls bei der Polizei angezeigt werden, um sich und andere zu schützen. Hier bieten sich auch die Portale der „Internetwachen“ an, da Anzeigen hier zügig zu darauf spezialisierten Kriminalbeamten weitergeleitet werden.

Die Unterstützung der ISH durch Polizeibehörden sowie den Projekten von DsiN gewährleistet, dass die ISH zusätzliche

Besucher:innen beim Tag der offenen Tür im Bundesinnenministerium

Tag der offenen Tür der Bundesregierung



DSIN-PROJEKTANGEBOTE STARK NACHGEFRAGT

Am 19. und 20. August 2023 öffnete die Bundesregierung unter dem Motto „Die Regierung lädt ein“ ihre Tore, um Bürger:innen Einblick in ihre Arbeit zu gewähren.

Als Partner der Ministerien ist DsiN seit seiner Gründung 2006 regelmäßig mit seinen Projekten vor Ort vertreten. Im Jahre wurden interessierten Besucher:innen der DsiN-Digitalführerschein im Bundesinnenministerium (BMI) vorgestellt, der Digitale Engel im Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) sowie der Digital-Kompass im Bundesministerium für Umwelt und Verbraucherschutz (BMUV).

Die DsiN-Projektstände stießen auf großes Interesse: „Ich bin beeindruckt vom regen Interesse der Besucher:innen. Die verstärkte Nachfrage nach Hilfsangeboten

„Ich bin beeindruckt vom regen Interesse der Besucher:innen.“

Dr. Michael Littger

zum sicheren Umgang im Netz macht sich auch hier beim Tag der offenen Tür der Bundesregierung bemerkbar“, sagte Dr. Michael Littger, DsiN-Geschäftsführer.

Als Neuigkeit des DsiN-Digitalführerscheins (DiFü) wurde im BMI auch über die Projekterweiterungen des Lehrkräfte-moduls informiert. Besucher:innen



Bundesministerin Nancy Faeser besucht den Stand des Digitalführerscheins beim Tag der offenen Tür.

nutzten die Gelegenheit, an den DiFü-Tablets die eigene Digitalkompetenz zu testen und das Lernangebot auszuprobieren. DsiN-Schirmherrin und Bundesinnenministerin Nancy Faeser sowie Staatssekretär Dr. Markus Richter informierten sich ausführlich über die Fortschritte des Angebots, die sie in der Verbreitung bis

und Klein dazu ein, digitales Wissen anhand ausgewählter Fragen zu testen und zu erweitern. Häufige Fragen der Senior:innen drehten sich um künstliche Intelligenz und ihre Vor- und Nachteile. „Die Nachfrage nach Unterstützung steigt enorm, auch bei älteren Verbraucher:innen“, bestätigt Katharina Kunze, Projektleiterin des Digitalen Engels.

„Die Nachfrage nach Unterstützung steigt enorm, auch bei älteren Verbraucher:innen.“

Katharina Kunze

dato von 85.000 Prüfungen bestätigten [Bis Redaktionsschluss im März 2024 erreichte die Verbreitung über 150.000 erfolgreiche Einzelprüfungen].

Das Projekt Digitaler Engel baute seinen Stand „Nie zu alt fürs Internet“ gemeinsam mit der BAGSO – der Bundesarbeitsgemeinschaft der Seniorenorganisationen im BMFSFJ auf. Ein Glücksrad lud Groß

Auch der Digital-Kompass (DiKo) zeigte neue Informationsmaterialien zum Thema Barrierefreiheit im Internet, mit einer Simulationsbrille für Seherkrankungen und einem Quiz standen Projektmitarbeiter:innen Interessierten für ihre Fragen zur Verfügung. Staatssekretärin Dr. Christine Rohleder zeigte sich davon überzeugt, dass das Projekt einen wachsenden Bedarf in der Gesellschaft nach nonformaler Bildung aufgreife und würdigte den neuen DiKo-Podcast als Angebot, das Alltagsfragen der Digitalisierung einfach erkläre.



Interessierte erkundigen sich beim Stand des Digitalen Engels.

28 4.400

Kooperationspartner:innen

Presseberichte

30

Partner-Einrichtungen



3.053

Social Media-Follower:innen

92.487

Homepage-Besucher:innen

3.225

Downloads

238

Partner-Einrichtungen

58

Kooperationspartner:innen

DigiBits
Digitale Bildung trifft Schule

175

ausgebildete Multiplikator:innen

56.870

Homepage-Besucher:innen

314

ausgebildete Multiplikator:innen

32

absolvierte Prüfungen

246

Partner-Einrichtungen



908

Presseberichte

265

Veranstaltungen

4 970

Schirmherr:innen im Bundestag

Homepage-Besucher:innen

474

TN Zahlen



PolisiN
Politiker:innen sicher im Netz

7

absolvierte Prüfungen

12

Veranstaltungen

101 32

ausgebildete Multiplikator:innen

Kooperationspartner:innen

286

Presseberichte

DiF

123.305

absolvierte Prüfungen

25.131

TN Zahlen

130

ausgebildete Multiplikator:innen

78

Standorte



5.000

Tools/Übungen

130

Standorte

123

absolvierte Prüfungen



3.450

ausgebildete Multiplikator:innen

Die Illustration entstand mit dem Text-zu-Bild-Generator DreamStudio.
Prompt: oil painting on a white surface of data streams with different blue colors

IT-Sicherheit in Beruf und Ausbildung

DREI JAHRE TISIM: Ein Erfolgsmodell für den Mittelstand



Ausgangssituation

Kleine und mittlere Unternehmen (KMU), Freiberufler:innen und das Handwerk stehen oft vor der Herausforderung, ihre IT-Sicherheit gewährleisten zu müssen, ohne dafür eigene IT-Abteilungen zu haben. Hier setzte TISiM – die Transferstelle IT-Sicherheit im Mittelstand – an. Mit maßgeschneiderten Lösungen wie dem Sec-O-Mat und einem deutschlandweiten Netzwerk von Regionalstellen hat TISiM seit 2020 bis 2023 auf diese dringenden Bedürfnisse reagiert.

Mission

Das Hauptziel von TISiM war es, die IT-Sicherheitskompetenzen von KMU zu stärken und somit die Digitalisierung sicher zu gestalten. Dies sollte durch praxisnahe Unterstützung und konkrete Umsetzungshilfen erreicht werden. Ein weiteres Ziel war die Schaffung eines umfangreichen Netzwerks von TISiM-Regionalstellen und mobilen Teams, um auch in ländlichen Regionen präsent zu sein und vor Ort Unterstützung bieten zu können.

Von der Planung zur Realisierung

Die Umsetzung begann mit einer erfolgreichen Pilotphase, in der der Sec-O-Mat entwickelt und getestet wurde. Dieses digitale Tool liefert individuelle Aktionspläne für Unternehmen, basierend auf spezifischen Bedürfnissen und Gefahrenlagen. Unterstützt wird der Sec-O-Mat von einem flächendeckenden Netzwerk: Bis Ende 2021 wurden bundesweit TISiM-Regionalstellen und das TISiM-Mobil eingerichtet, um vor Ort Hilfe zu leisten und den Wissenstransfer zu fördern.

Erfolge

In den vergangenen drei Jahren hat TISiM beeindruckende Erfolge erzielt. Über 5.000 TISiM-Aktionspläne wurden erstellt, mehr als 130 TISiM-Trainer:innen geschult und 78 regionale Anlaufstellen eingerichtet. Diese Zahlen zeigen die breite Akzeptanz und die erfolgreiche Verankerung der Initiative in der deutschen Unternehmenslandschaft.

Im Rückblick ...

... waren drei Jahre TISiM ein voller Erfolg! Mit gezielten Maßnahmen und einem starken Netzwerk hat TISiM einen wichtigen Beitrag zur IT-Sicherheit im Mittelstand geleistet. Durch die kontinuierliche Unterstützung und Schulung konnten viele Unternehmen ihre IT-Sicherheit erheblich verbessern und sich besser gegen Cyberbedrohungen wappnen. TISiM zeigt eindrucksvoll, wie erfolgreiche Digitalisierung im Mittelstand aussehen kann – sicher, unterstützend und praxisnah.

Fortsetzung als Transferstelle Cybersicherheit

Nach drei erfolgreichen Jahren hat sich TISiM weiterentwickelt und ist nun als Transferstelle Cybersicherheit aktiv. Diese neue Phase baut auf den Errungenschaften von TISiM auf und erweitert das Angebot, um noch umfassender auf die wachsenden Herausforderungen der digitalen Welt zu reagieren. Unter der neuen Marke wird das bewährte Konzept fortgeführt und weiter ausgebaut, um noch mehr Unternehmen zu erreichen und die Cybersicherheit im Mittelstand nachhaltig zu stärken. Besuchen Sie transferstelle-cybersicherheit.de, um mehr über die aktuellen Angebote und Unterstützungsmaßnahmen zu erfahren.

Neue Workshopformate im Projekt „mIT Sicherheit ausbilden“

EIN FRISCHER WIND FÜR MEHR IT-SICHERHEIT

Das Projekt „mIT Sicherheit ausbilden“ geht mit einem neuen Workshop-Konzept an den Start und bringt frischen Wind in die IT-Sicherheitslandschaft. Hier eine Übersicht über die spannenden Neuerungen:

Kompakte und flexible Workshops

Früher mussten Teilnehmer:innen zwei volle Tage für die Basisworkshops einplanen, was oft eine große Hürde darstellte. Jetzt wird der Workshop auf einen Tag komprimiert. Das spart Zeit und macht die Teilnahme einfacher. Als Bonus gibt es ein optionales gemeinsames Vorabendprogramm – die perfekte Gelegenheit zum Netzwerken in entspannter Atmosphäre.

Starterpaket „Online TTT“

Das neue Online Train-the-Trainer-Programm wird modular aufgebaut und mindestens einmal im Monat eine Veranstaltung angeboten. Der Fokus liegt auf der Nutzung der Lernplattform und der Didaktik-Trainings, angepasst an die Bedürfnisse der Teilnehmenden. Neben dem kompakten Präsenz-Workshop bieten diese fortlaufend neue Inhalte und ermöglichen eine flexible und kontinuierliche Weiterbildung.

Aktive Community

In der Teams-Gruppe der Trainer:innen gibt es wöchentlichen Input mit Zusatz-

materialien, Links und Tipps. Die regelmäßige Abfrage gewünschter Themenschwerpunkte sorgt dafür, dass die Online-Workshops immer relevant und aktuell bleiben.

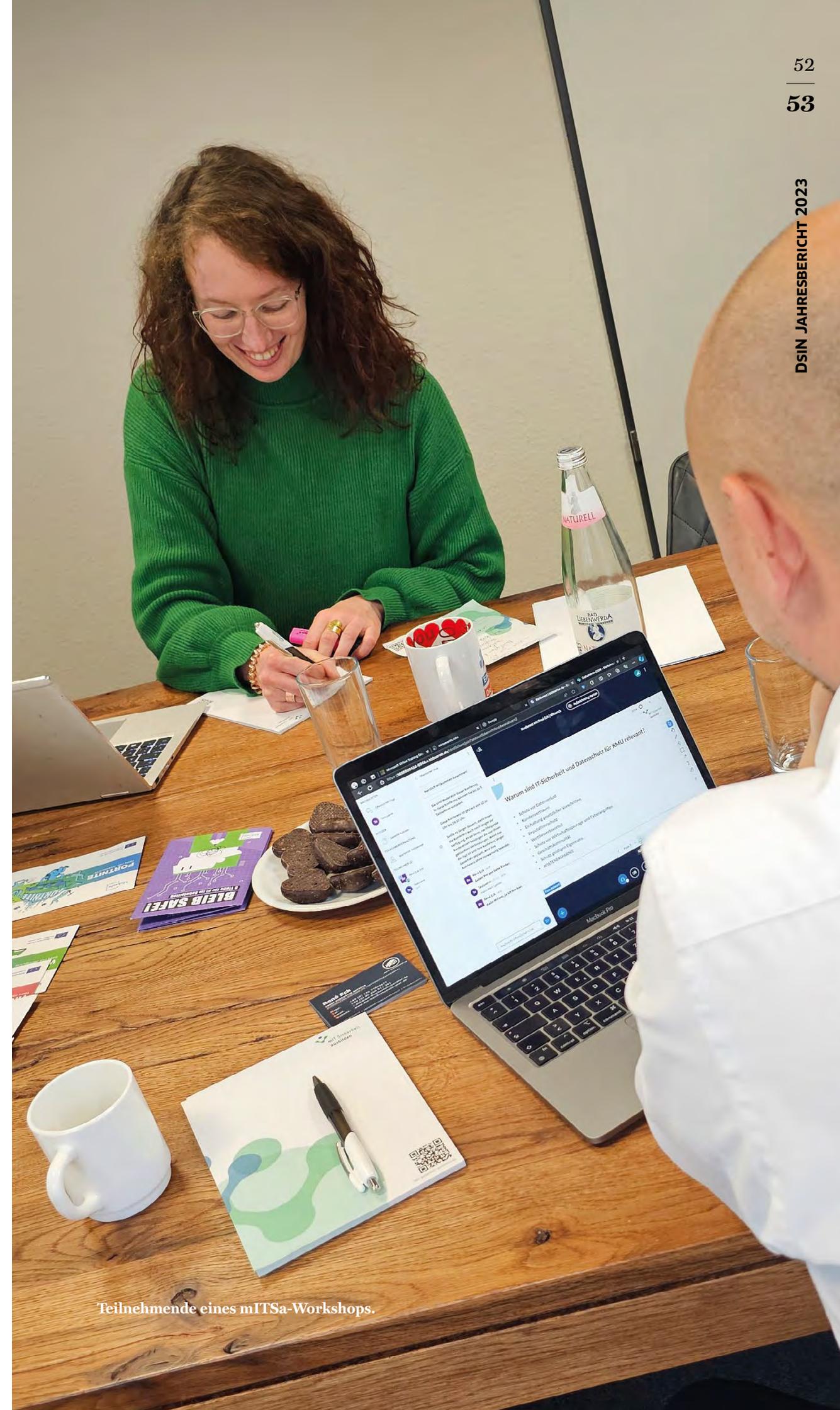
Interaktive Lernplattform

Die Lernplattform wird kontinuierlich überarbeitet und mit mehr interaktiven Inhalten ausgestattet, welche die Trainer:innen direkt in ihren Workshops nutzen können. So wird die Plattform zum zentralen Werkzeug für die Vermittlung und Vertiefung der Inhalte.

Immer aktuell

Um unsere Qualität fortwährend zu verbessern, wird regelmäßig Feedback der Teilnehmer:innen und Trainer:innen eingeholt. Diese Rückmeldungen fließen direkt in die Weiterentwicklung des Programms ein.

Das neue Konzept von „mIT Sicherheit ausbilden“ macht die Teilnahme einfacher, flexibler und praxisnäher. Es motiviert durch interaktive und kompakte Formate und fördert den kontinuierlichen Austausch unter den Teilnehmer:innen. Ein echter Gewinn für alle, die sich im Bereich IT-Sicherheit weiterbilden möchten!



Teilnehmende eines mITSa-Workshops.

PolisiN mit fraktionsübergreifender Schirmherrschaft im Deutschen Bundestag

Das DsiN-Projekt „Politiker:innen sicher im Netz – PolisiN“ ist als Unterstützungsangebot auf kommunaler, Landes- und Bundesebene aktiv. Seit dem vergangenen Jahr zählt dazu auch eine Schirmherrschaft im Deutschen Bundestag, die Vertreter:innen von CDU/CSU, SPD, GRÜNE sowie FDP umfasst und sich gemeinsam für mehr IT-Sicherheit und sichere Möglichkeiten der Digitalisierung einsetzt.

Das Signal soll dafür sensibilisieren, dass Cyberkriminalität jeden treffen kann, auch die Abgeordneten des Deutschen Bundestags und ihre Büros im Bundestag und im Wahlkreis: „Hackerangriffe, Datenklau, Identitätsdiebstahl – je mehr wir im Netz tun, desto mehr setzen wir uns den wachsenden Cyberbedrohungen aus“, berichtet Tabea Rößner MdB, Schirmherrin für die GRÜNEN. Sie ist Vorsitzende des Ausschusses für Digitales im Deutschen Bundestag und hat langjährige Erfahrungen auf dem Gebiet. Gemeinsam mit PolisiN hat sie zu Veranstaltungen für die Bundestagsfraktion der GRÜNEN eingeladen. Aber auch bei Schulungen von ehrenamtlich Tätigen sowie dem DsiN-Jahreskongress 2023 unterstützte Rößner mit Ihrer Präsenz und Aufrufen zur Teilnahme.

Gemeinsam engagieren sich die Schirmherren und -frauen, die erworbenen Kompetenzen an Bürger:innen weiterzugeben. Zu den PolisiN-Themen gehören

Kontensicherheit, verschlüsselte Kommunikation oder auch Hass und Hetze im Netz. „Passwort 12345 - Die Liste mit den meistgenutzten Passwörtern in Deutschland jagt mir jedes Mal einen Schauer über den Rücken!“, berichtet Anna Kassautzki MdB, Schirmherrin für die SPD und stellvertretende Vorsitzende des Digitalausschusses im Bundestag. In intensiven Beratungen – unter anderem mit ihrem Büro – konnte grundlegend darüber gesprochen werden, wie mehr Bewusstsein für Fragen von IT-Sicherheit und Digitalisierung geschaffen werden kann.

Viele Abgeordnete oder Mitarbeiter:innen des Bundestages besetzen weitere politische Ämter, etwa in ihren Parteien, in lokalen Parlamenten oder auch in Vereinen. Hier laufen oftmals viele verschiedene Informationen und Kontakte zusammen. PolisiN trägt dazu bei, dass auch an dieser Stelle digitale Kompetenzen in den Alltag integriert werden.



Tabea Rößner MdB,
Schirmherrin für die GRÜNEN



Anna Kassautzki MdB,
Schirmherrin für die SPD



Marc Henrichmann MdB,
Schirmherr für die CDU/CSU



Manuel Höferlin MdB,
Schirmherr für die FDP

„Wir müssen insgesamt schneller werden in Fragen der IT-Sicherheit, gerade auch bei den Digitalkompetenzen im beruflichen Alltag.“

Marc Henrichmann

Innen-Experte Marc Henrichmann MdB (CDU/CSU) und Manuel Höferlin MdB (FDP) verbinden mit ihrer Schirmherrschaft für PolisiN zentrale Themenfelder. „Wir müssen insgesamt schneller werden in Fragen der IT-Sicherheit, gerade auch bei den Digitalkompetenzen im beruflichen Alltag“, berichtet Henrichmann dazu auch von Erfahrungen aus seinem Wahl-

kreis. „Der aktuelle DsiN-Sicherheitsindex zeigt, dass die Kompetenzen in der gesamten Bevölkerung zunehmen müssen – da sind wir Politiker:innen natürlich auch in einer Vorbildfunktion“, ergänzt Höferlin.

Beide engagieren sich für PolisiN, insbesondere in ihren Bundestagsfraktionen. Das geschieht auch in Absprache mit der Bundestagsverwaltung. Die entsprechenden Referate der IT-Sicherheit stehen ebenso im Austausch mit PolisiN und unterstützten bereits mit gemeinsamen Veranstaltungen.

Cybersicherheit und Politik

WARUM SICH GERADE PARLAMENTE UND PARTEIEN SCHÜTZEN MÜSSEN – UND WIE

Cyberbedrohungen und die Sicherheit von Politiker:innen – in einer Welt, in der digitale Angriffe zunehmen, stehen politische Akteure besonders im Fokus. Wie können sie sich effektiv schützen, wenn ihre Arbeit Transparenz und Offenheit erfordert? PolisiN bietet hierzu Workshops an, die von Grundlagen der Digitalisierung bis zu fortgeschrittenen Techniken unter Nutzung künstlicher Intelligenz im politischen Alltag reichen.

Die Cybersicherheitsbedrohungen, denen sich Deutschland ausgesetzt sieht, sind vielfältig und komplex. Nach Angaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist die Bedrohungslage im Cyberraum höher denn je, mit einer zunehmenden Zahl von Cyberangriffen, die sich gegen kleine und mittlere Unternehmen sowie staatliche Einrichtungen richten. Ransomware, also das Verschlüsseln von Daten im Austausch gegen Lösegeld (Englisch: Ransom), bleibe dabei eine der größten Bedrohungen, wobei Angreifende zunehmend professionell und vernetzt operieren.

Die Bundesregierung hat auf diese Herausforderungen mit einer umfassenden Cybersicherheitsstrategie reagiert.

Die Cybersicherheitsagenda, die von Bundesinnenministerin Nancy Faeser vorgestellt wurde, umfasst eine Vielzahl von Maßnahmen zur Stärkung der Resilienz gegenüber Cyberangriffen. Das Projekt „Politiker:innen sicher im Netz – PolisiN“ von DsiN unterstützt die Bemühungen der Bundesregierung und ist Teil der umfassenderen Anstrengungen, die digitale Resilienz in Deutschland zu stärken. Dies beinhaltet eine Kombination aus technologischen, regulatorischen und bildungsorientierten Ansätzen, um die Sicherheit in einer digital vernetzten Welt langfristig zu gewährleisten.

Das Projekt entstand auf Initiative von DsiN-Mitgliedern, allen voran das Google Safety Engineering Center um dessen langjährigen Leiter sowie DsiN-

Ein wesentliches Problem, das die Cybersicherheit in politischen Kreisen einzigartig macht, ist die Offenheit und Zugänglichkeit, die demokratische Prozesse erfordern.

Vorstandsmitglied Michael Guntsch und seinen Nachfolger, Dr. Jochen Eisinger. Auch das DsiN-Mitglied yubico hat mit kostenfreien „YubiKeys“, ihren bekannten Multifaktor-Sicherheitssticks, Teilnehmer:innen der PolisiN-Workshops von Anfang an unterstützt. Seit Ende 2023 ist Governikus hinzugekommen – die 100% Tochter des Bundeslands Bremen, die vielen durch die „AusweisApp“ des Bundes bekannt ist, hilft dem Projekt, der wachsenden Anfrage, gerade auf kommunaler Ebene, nachzukommen.

Politik muss sich anders zu helfen wissen

Politiker:innen stehen wegen ihrer öffentlichen Rollen und Verantwortlichkeiten zunehmend im Fokus von Cyberbedrohungen. Diese reichen von gezielten Phishing-Angriffen und Ransomware bis hin zu Desinformationskampagnen, die darauf abzielen, politische Prozesse zu manipulieren oder zu stören. PolisiN bietet hierbei wesentliche Unterstützung, indem es durch Workshops sowie Beratungen politischen Akteuren hilft, sich gegen solche Bedrohungen zu schützen.

Ein wesentliches Problem, das die Cybersicherheit in politischen Kreisen einzigartig macht, ist die Offenheit und

Zugänglichkeit, die demokratische Prozesse erfordern. So muss beispielsweise eine Landtagsfraktion mit Parteien, Verbänden, aber auch Journalist:innen oder interessierten Bürger:innen kommunizieren und teils wichtige sowie schützenswerte Informationen austauschen. Das macht es schwierig, geschlossene Systeme zu implementieren, die in anderen Sektoren zum Schutz vor Cyberangriffen eingesetzt werden könnten.

Zudem sind politisch Aktive, besonders auf kommunaler oder ehrenamtlicher Ebene, oft mit begrenzten Ressourcen ausgestattet.

Zudem sind politisch Aktive, besonders auf kommunaler oder ehrenamtlicher Ebene, oft mit begrenzten Ressourcen ausgestattet. Dies bedeutet, dass sie möglicherweise nicht auf die fortschrittlichsten Sicherheitstools oder größere Server-Infrastrukturen zugreifen können, die unter anderem in kommerziellen Organisationen zur Verfügung stehen. Hier setzt PolisiN an. Es werden kostenlose Schulungen und Ressourcen angeboten, die speziell darauf ausgerichtet sind, politische Akteure über sichere Praktiken

im Internet aufzuklären und ihnen Werkzeuge an die Hand zu geben, um sich selbst zu schützen.

Ein weiteres Problem liegt in der Natur der politischen Daten selbst. Politiker:innen verarbeiten oft sensible Informationen, die sowohl für Cyberkriminelle als auch für staatlich gesponserte Akteure von großem Interesse sein können. Dies erhöht das Risiko von Cyberangriffen, die darauf abzielen, Daten zu stehlen oder zu manipulieren. Ohne geschlossene Systeme bleibt aber am Ende nur, dass sich politisch Aktive ganz individuell um ihre Cybersicherheit kümmern.

Politisch Aktive müssen schlichtweg gut informiert, sensibilisiert und wachsam sein – etwas, was im hektischen Betrieb der Politik keine Leichtigkeit ist.

Sie müssen schlichtweg gut informiert, sensibilisiert und wachsam sein – was im hektischen Betrieb der Politik keine Leichtigkeit ist.

Angebote für die praktische Umsetzung und Begleitung

Die Workshopreihe, das zentrale Element von PolisiN, deckt dabei verschiedene Aspekte der digitalen Sicherheit für politische Akteure ab. In den Grundlagen-Workshops werden Teilnehmer:innen über die Digitalisierung von Abgeordnetenbüros und Parteiverbänden sowie über sicheren Umgang mit sozialen Medien unterrichtet. Aufbau-

Workshops vertiefen Themen wie Datenschutz gemäß den neuesten EU-Regelungen und die sichere Nutzung von Clouddiensten.

In spezialisierten Vertiefungs-Workshops lernen Teilnehmer:innen, wie man die private Identität online schützt und sichere Kommunikationsmittel effektiv einsetzt. Zusätzlich werden moderne Technologien wie Künstliche Intelligenz und deren Anwendung im politischen Kontext behandelt, um den Teilnehmer:innen zu helfen, technologisch auf dem neuesten Stand zu bleiben.

Diese umfassenden Schulungen zielen darauf ab, die digitale Resilienz von Politiker:innen zu stärken und sie vor den vielfältigen Cyberbedrohungen zu schützen, die im politischen Alltag auftreten können. Sie bieten wertvolle Ressourcen für Politiker:innen, die ihre digitalen Fähigkeiten erweitern und ihre Arbeitssicherheit verbessern möchten.

Politik muss digitaler werden und – sicherer

PolisiN trägt zur Cybersicherheit bei, indem politisch Aktive in den alltagsrelevanten Praktiken der IT-Sicherheit geschult werden, um auf allen Ebenen der Politik sicherer zu agieren und gleichzeitig die Offenheit und Transparenz beizubehalten, die für demokratische Prozesse erforderlich sind.

PolisiN hilft damit konkret, politische Akteure zu schützen, es stärkt das Vertrauen in die Sicherheit und Integrität politischer Prozesse. Allerdings zeigt sich

auch in der Praxis: Oft wird die Einführung von Software und Endgeräten mit Digitalisierung gleichgesetzt. De facto wird dadurch aber in vielen Fällen eine Überforderung ausgelöst, wenn nicht parallel Strukturen, Prozesse und auch Hierarchien entstehen. PolisiN arbeitet hier konkret mit Parteien und Fraktionen an Lösungen.

Dabei wird es immer wichtiger, dass die Politik ihre Prozesse digitalisiert, um die Effizienz zu steigern und die öffentliche Teilnahme zu vereinfachen.

Dabei wird es immer wichtiger, dass die Politik Prozesse digitalisiert, um ihre Effizienz zu steigern und die öffentliche Teilnahme zu vereinfachen. Anders ausgedrückt: Politik muss vor allem Zeit

und Ressourcen gewinnen, bevor sie digitalisiert. Die Implementierung digitaler Werkzeuge kann dazu beitragen, administrative Vorgänge zu beschleunigen, die Kommunikation zwischen den Beteiligten zu verbessern und politische Entscheidungen transparenter zu machen. Dies erfordert fortlaufende Investitionen in Technologie und Bildung – dazu leistet PolisiN einen Beitrag.

Partner:

Google Safety Engineering Center

GOVERNIKUS

yubico

Die Illustration entstand mit dem Text-zu-Bild-Generator DreamStudio.
Prompt: oil painting on a white surface of data streams only with dark green colors

**Online-
banking**



DsiN-Talk „Sicherer Login“

„Das sichere Internet ist gewachsen, das unsichere aber auch.“

Patrick Schnell, Senior Channel Manager
DACH & BeNeLux & CEE bei Yubico

Wie können sich Nutzer:innen gegen Phishingangriffe wehren und sich vor Identitätsdiebstahl schützen? Welchen Herausforderungen stehen sie gegenüber und wo gibt es Anlaufstellen zur Aufklärung? Diesen und weiteren Fragen widmete sich der diesjährige DsiN-Talk „Sicherer Login“ am 29. März.

Zum Thema „Sicherer Login: Wie Nutzer:innen ihre Benutzerkonten sicher verwalten und sich vor Phishingangriffen und Identitätsdiebstahl schützen“ luden wir in das DsiN-Forum Digitale Aufklärung ein. Gemeinsam mit Expert:innen aus Politik, Wirtschaft und Gesellschaft diskutierten wir über aktuelle Gefahren und mögliche Schutzmaßnahmen.

Gastgeber und Moderator Dr. Michael Littger begrüßte Martin Stein vom Deutschen Sparkassen- und Giroverband e.V. (DSGV), Sven Kindervater vom Projekt

PolisiN – Politiker:innen sicher im Netz und die Bundestagsabgeordnete Anna Kassautzki vom Ausschuss Digitales. Ebenfalls zum Thema auf dem Panel vertreten war Patrick Schnell, Senior Channel Manager DACH & BeNeLux & CEE bei Yubico, der die Diskussion mit einem Impulsvortrag zum Thema „Sicherheit von Benutzerkonten durch die Zwei-Faktor-Authentifizierung: Methoden und Vorteile“ eröffnete.

Die Gesprächsgäste waren sich über den Nachholbedarf an digitaler Aufklärung

eing und diskutierten darüber, wie Risiken eliminiert und das Bewusstsein der Nutzer:innen gegen Datenklau gestärkt werden können. Bereits zum „Sicheren Login Tag“ am 1. Februar veröffentlichte DsiN gemeinsam mit dem Authentifizierungsexperten Yubico einen Verbraucherratgeber „Benutzerkonten sichern – einfach einloggen“ mit Tipps und Hilfestellungen zum Schutz von Onlinekonten.

Phishing-Angriffe nehmen zu

Gleich zu Beginn betonte MdB Anna Kassautzki, wie wichtig es sei, Aufmerksamkeit für das Thema sichere Onlinekonten und Login zu erhalten, denn: „Das sichere Internet ist gewachsen, das unsichere aber auch.“ Auch Patrick Schnell bestätigte, dass Phishing-Angriffe zunehmen. Auf diesen Anstieg müsse man mit Lösungen reagieren, die für Verbraucher:innen alltagstauglich seien, so Sven Kindervater.

Tatsächlich ist jeder dritte IT-Sicherheitsvorfall inzwischen eine Phishing-Angriffe (30,5 Prozent), was aus dem DsiN-Sicherheitsindex 2023 hervorgeht.

Jeder dritte IT-Sicherheitsvorfall ist inzwischen eine Phishing-Angriffe (30,5 Prozent).

DsiN-Sicherheitsindex 2023

Ob man im Internet kommuniziert, soziale Medien nutzt, Streaming-Dienste oder Onlinebanking in Anspruch nimmt – all diese Anwendungen stützen sich auf die eindeutige Identifizierung durch ein Login. Deshalb ist Aufklärung über die Chancen und Risiken im Umgang mit Onlinekonten das zentrale Element für die digitale Souveränität. Denn durch schwache Passwörter oder schlecht geschützte Onlinekonten gelingt es Kriminellen, digitale Identitäten zu



stehlen oder an sensible Daten zu gelangen. Benutzerkonten sind deshalb besonders schutzbedürftig. Das hoben auch die Expert:innen aus Politik, Wirtschaft und Zivilgesellschaft während des DsiN-Talks hervor.

Aufklärung und Präventionsmaßnahmen

Die Diskussionsteilnehmer:innen waren sich einig: Es muss Anlaufstellen und Angebote für Aufklärung und Präven-

tionsmaßnahmen geben. Herr Stein berichtete von seinen persönlichen Erfahrungen mit Phishing-Angriffen und machte deutlich, dass jede:r Opfer von Betrug werden kann. Denn Betrugsmaschinen sind so intelligent platziert und gestaltet, dass Verbraucher:innen sie oft nur schwer als Betrug enttarnen können.

Es muss Anlaufstellen und Angebote für Aufklärung und Präventionsmaßnahmen geben.



Anna Kassautzki machte auf die vielen Projekte aufmerksam, die Verbraucher:innen nutzen können, um sich Tipps für den Alltag einzuholen. Die Transferleistung muss hierbei von Vereinen und Projekten wie DsiN geleistet werden, forderte Patrick Schnell. Die Alltagslösungen, die Nutzer:innen benötigen, um sich vor Angriffen schützen zu können, müssen für jede Person nachvollziehbar kommuniziert werden. Eine Empfehlung, die der DSGVO an die eigenen Kund:innen kommuniziert, ist, die Digitalisierung in die „reale Welt“ zu übertragen. So würde man den Haustürschlüssel auch nicht einer dritten, fremden Person überlassen, verdeutlichte Stein.

Insgesamt spielt die Sensibilisierung für das Thema eine wesentliche Rolle. Die Gesellschaft muss über diese Betrugsmaschinen aufgeklärt sein und digitale Kompetenzen erlangen, um sich sicher im Netz bewegen zu können. Hier bietet der DsiN-Digitalführerschein eine Möglichkeit, digitale Kompetenzen zu erlangen und zu testen, so Dr. Michael Littger, Geschäftsführer DsiN e.V.

Sicherer Login in der Zukunft

Mit Blick auf die Zukunft sahen die Talk-Teilnehmenden einen Trend in neuen KI-Techniken, die Betrugsmaschinen verstärken und vereinfachen. Deswegen sei das Thema Awareness auch in fünf Jahren aktuell und der Bedarf an Aufklärungsarbeit und der dazugehörigen

Technik groß. Im Gespräch wurde zudem deutlich, dass Multiplikator:innen eine wesentliche Rolle spielen. Jede Person sei Multiplikator:in, indem sie ihr Wissen zum Thema Internetsicherheit an ihr Umfeld weitergibt.

Die Gesellschaft muss über diese Betrugsmaschinen aufgeklärt sein und digitale Kompetenzen erlangen, um sich sicher im Netz bewegen zu können.

Abschließend waren sich alle Teilnehmer:innen des Panels einig, dass die Zwei-Faktor-Authentifizierung eine gute Lösung ist, um sich sicher in persönliche Onlinekonten einzuloggen. Die dafür notwendige Hardware sollte in Zukunft selbstverständlicher Teil unseres Alltags sein, so die Talk-Gäste. Folgend können Sie sich die Aufzeichnung des DsiN-Talks ansehen.

In Partnerschaft mit:



Onlinebanking – aber sicher!

Der DsiN-Digitalführerschein hat 2023 Zuwachs bekommen: Im neuen Fokusmodul „Sicheres Onlinebanking“ werden bestehende Inhalte zu digitalen Bankgeschäften vertieft. Anhand echter Phishing-Mails lässt sich erlernen, wie Social Engineering funktioniert, wie man Betrugsversuche abwehrt und gleichzeitig zur Kriminalitätsprävention beiträgt.

Überweisungen, Lastschriften, Daueraufträge – immer mehr Bankgeschäfte werden heute online abgewickelt. Doch viele Menschen fürchten sich vor Cyberkriminalität, auch in der digitalen Bankfiliale. Deshalb hat der **DsiN-Digitalführerschein** gemeinsam mit dem Deutschen Sparkassen- und Giroverband (DSGV) ein spezielles Lernangebot entwickelt: das **Fokusmodul „Sicheres Onlinebanking“**.

Wer die vier Lerneinheiten des Fokusmoduls absolviert, erfährt alles über PIN, TAN, 2FA und Co. Dabei werden grundlegende **Sicherheitsmaßnahmen** fürs Onlinebanking vorgestellt. Neben der Absicherung von Geräten und Software bedeutet das vor allem starke Passwörter und die Vertraulichkeit des gesamten Ablaufs. Auch ausgewählte Einstellungen im Onlinebanking erhöhen die Sicherheit.

Anschließend lässt sich erlernen, wie man Warnsignale in zweifelhaften E-Mails deutet und Betrugsversuche rund ums Onlinebanking verhindert. Dabei kommen **echte Phishing-Mails** als Anschauungsmaterial zum Einsatz. Denn das sogenannte **Social Engineering** wird zwar immer ausgefeilter, setzt aber stets auf die gleichen Ängste und Unachtsamkeiten.

„Vor 10-15 Jahren war Schadsoftware, mit denen Kriminelle Geräte infiziert haben, der Hauptschadenstreiber. Mittlerweile sind technische Angriffe so aufwendig geworden, dass sie fast nur noch auf Social Engineering setzen.“

Sebastian Garbe, Geschäftsführer Sparkassen-Finanzportal

Und falls doch einmal etwas passiert ist? Dann lohnt ein Blick in den Abschnitt „Erste Hilfe“. Hier werden die nächsten Schritte im Betrugsfall zusammengefasst, genauso wie Anlaufstellen, bei denen sich **Phishing-Versuche** unkompliziert melden lassen. So können alle ihren Teil zur Kriminalitätsprävention beitragen.

2. Reingefallen – was nun?

Du bist Opfer von Phishing geworden, zu Hause oder im Büro? Das ist keine Schande, denn die Methoden werden immer raffinierter. Am besten gehst du offen damit um und informierst dein Umfeld. So gehst du vor:

1. Karten und Zugänge sperren

Ist dir klar geworden, dass deine Zugangsdaten zum Onlinebanking oder sogar deine Kreditkartendaten bei Kriminellen gelandet sind, veranlasse sofort eine Sperrung über die Notfall-Rufnummer 116 116. Die Nummer ist kostenfrei rund um die Uhr erreichbar, 365 Tage im Jahr.

Das Onlinebanking kannst du noch schneller sperren: Gib einfach dreimal das falsche Passwort bzw. die falsche PIN ein, per App oder im Browser.

Deine Kredit-, EC- oder Debitkarte kannst du in einem ersten Schritt auch direkt im Online-Banking bzw. in der Banking-App sperren lassen. Je schneller du bist, desto höher ist deine Chance, dass die Kriminellen mit deiner Karte bzw. mit deinen Kartendaten nichts mehr anfangen können.

2. Bank informieren

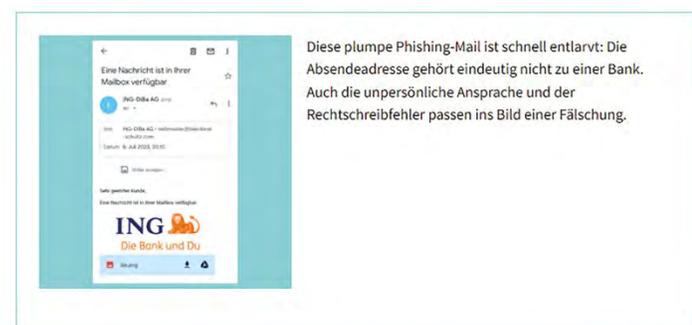
3. Anzeige erstatten

4. Geräte auf Schadsoftware prüfen

5. Meldepflichten für Unternehmen beachten

3. Schau hin! Dein Phishing-Training

Wirf einen Blick auf die folgenden 12 E-Mails. Viele Adressen und Links sind absichtlich verpixelt, denn jede dieser Nachrichten ist eine echte Phishing-Mail. Das heißt auch: Sie enthält konkrete Anhaltspunkte für einen Betrugsversuch. Entdeckst du alle Hinweise?



Eine besonders fiese Masche ist übrigens die IBAN-Manipulation bei Rechnungen. Technisch versierte Kriminelle schaffen es, in den Datenverkehr einzugreifen und E-Mails zu sich selbst umzuleiten. Dort können sie in einer angehängten Rechnung eine andere IBAN hinterlegen und die manipulierte Mail anschließend zustellen.

Ein Ausschnitt aus dem Fokusmodul „Sicheres Onlinebanking“



Fokusmodul

Das Fokusmodul „Sicheres Onlinebanking“ ist seit dem 16. November 2023 gratis verfügbar auf www.difue.de.



Dr. Michael Littger im Gespräch mit Staatssekretär Dr. Markus Richter

DsiN-Talk zum neuen DiFü-Fokusmodul „Sicheres Onlinebanking“

Am 16. November 2023 lud Deutschland sicher im Netz e.V. (DsiN) zur Podiumsdiskussion „Mein Geld geht online – aber sicher!“ mit Staatssekretär Dr. Markus Richter aus dem Bundesinnenministerium, Sebastian Garbe vom DSGVO und Elisabeth Wisniewski vom DsiN-Digitalführerschein (DiFü) DiFü im DsiN-Forum ein. Anlass war die Veröffentlichung des neuen DiFü-Fokusmoduls „Sicheres Onlinebanking“.

Allein rund 30 Millionen Kund:innen der Sparkassen nutzen derzeit in Deutschland die Möglichkeit des Onlinebankings. Trotz hoher technischer Sicherheitsstandards im digitalen Finanzsektor sind viele Nutzer:innen verunsichert und fürchten Cyberbetrug. Um dem entgegenzuwirken, hat der DsiN-Digitalführerschein (DiFü) in Kooperation mit dem Deutschen

Sparkassen- und Giroverband (DSGV) ein Lernangebot rund um das Thema Onlinebanking entwickelt. Das neue Fokusmodul „Sicheres Onlinebanking“ erklärt die Grundlagen zum digitalen Umgang mit Geld, zeigt konkrete Sicherheitsvorkehrungen auf und sensibilisiert für Phishing und Social Engineering anhand simulierter Betrugs-Mails.



„Die Cyberrisiken im Bereich digitale Finanzdienstleistungen nehmen zu.“

Dr. Markus Richter

Podiumsdiskussion mit BMI-Staatssekretär Dr. Markus Richter

Im Podium standen Strategien und Maßnahmen im Fokus, um die IT-Sicherheit digitaler Bankdienste zu stärken und zugleich ihre Akzeptanz zu erhöhen. Neben technischer IT-Sicherheit und guten Rahmenbedingungen, wies Richter der Förderung digitaler Kompetenz maßgebliche Bedeutung zu: „Die Cyber Risiken im Bereich digitaler Finanzdienstleistungen nehmen zu. Hier hilft der erweiterte DsiN-Digitalführerschein ganz praktisch und konkret, um erforderliche Digitalkompetenzen zu erlernen.“

Mit Kompetenzverstärkung und Kooperation gegen Kriminalität

Sebastian Garbe hob die Gefahrenlage hervor, die sich in den vergangenen Jahren deutlich verändert habe: „Vor 10 bis 15 Jahren war Schadsoftware, mit denen Kriminelle Geräte infizierten, der Hauptschadenstreiber. Mittlerweile sind, auch weil wir aufgerüstet haben, technische Angriffe für Kriminelle so teuer geworden, dass sie heute fast nur noch auf Social Engineering setzen.“

Einer solchen Bedrohungslage könne man nur gemeinsam begegnen, so Elisabeth Wisniewski: „Wir spüren die Verunsicherung auch in der starken Nachfrage beim DiFü. Hier hilft es, unterschiedliche Partner aus der Praxis an unserer Seite zu haben. Wir nutzen ihre Expertise und übersetzen sie im didaktischen Angebot des DiFü, das Spaß und nicht Angst

macht. Damit wollen wir animieren und unsere Nutzer:innen und Unternehmen ermuntern, am DiFü teilzunehmen. Mit dem DiFü empowern wir Menschen, sich Inhalte und Kompetenzen selbst zu erarbeiten.“

Welche Rolle spielt Künstliche Intelligenz?

Beim Thema Künstliche Intelligenz (KI) war sich das Panel einig: Kriminelle werden neue Technologien wie Künstliche Intelligenz einsetzen. Zugleich ist KI schon heute enorm hilfreich, um Angriffe abzuwehren. Transaktionen könnten etwa mit KI-Anwendungen viel sicherer verifiziert werden. „Auch in der Verwaltung werde KI zunehmend zum Einsatz kommen. Da sei es nur noch eine Frage der Zeit, bis auch der DiFü die KI nutzen werde, um Teilnehmer:innen beim passgenauen Kompetenzerwerb zu unterstützen,“ so Dr. Michael Littger, der durch die Veranstaltung führte.



Elisabeth Wisniewski spricht während der Podiumsdiskussion über die starke Nachfrage nach Aufklärungsangeboten.



Dr. Richter weist im Gespräch auf die Bedeutung von Förderangeboten für digitale Kompetenzen hin.



V. l. n. r.: Sebastian Garbe (DSGV), Dr. Markus Richter (BMI), Elisabeth Wisniewski (DiFü), Dr. Michael Littger (DsiN)



Kann ich nachts beim Online-Banking überfallen werden?

Informationskampagne des DsiN-Digitalführerscheins (DiFü)

Pünktlich zur Osterreisezeit startete der DsiN-Digitalführerschein (DiFü) im März 2023 eine bundesweite Informationskampagne mit rund 2.400 Plakaten an zentralen Bahnhöfen. Mit der Aufforderung „Quizz dich zum Zertifikat“ griff die Kampagne den spielerischen Lernansatz des Digitalführerscheins auf.

„Der DsiN-Digitalführerschein ist ein wichtiger Baustein, um Digitalkompetenzen für Teilhabe und Cyber-Resilienz in der Bevölkerung konkret zu stärken“, erklärte Dr. Markus Richter, Staatssekretär im Bundesministerium des Innern und für Heimat (BMI) und CIO des Bundes. „Die bundesweite Plakatkampagne trägt dazu bei, mehr Menschen auf das kostenfreie Angebot aufmerksam zu machen und auch Menschen im Berufsleben von den Vorteilen eines Digitalzertifikats zu überzeugen.“

Zum Startschuss der Plakat-Aktion am 30.03.2023 enthüllte Richter das Leitmotiv der Kampagne auf einer digitalen Säule im Foyer des Berliner Hauptbahnhofs. Begleitet wurden die Plakate online unter #klickdichsicher und mit Gratispostkarten in der Gastronomie.



Launch der Informationskampagne am Berliner Hauptbahnhof mit DsiN-Geschäftsführer Dr. Michael Littger, DiFü-Projektleiterin Elisabeth Wisniewski und dem parlamentarischen Staatssekretär Dr. Markus Richter (v.l.n.r.).

Zwischen Information und Manipulation

Dr. Marie-Agnes Strack-Zimmermann und Eveline Metzen, Google Deutschland, über den Kampf gegen Desinformation und Hatespeech

Desinformation und Hate Speech nehmen zu – ein Problem, das auch Dr. Marie-Agnes Strack-Zimmermann (FDP), Vorsitzende des Verteidigungsausschusses im Bundestag, persönlich kennt. Sie erlebt täglich, wie Hassbotschaften versuchen, Debatten zu vergiften. Doch wie wirksam sind politische und rechtliche Gegenstrategien?

In einer Zeit, in der Falschinformationen und Hatespeech das Potenzial haben, Gesellschaften zu spalten und demokratische Prozesse zu untergraben, wird die Notwendigkeit einer fundierten Diskussion über diese Phänomene immer dringlicher. Die Politikerin Dr. Marie-Agnes Strack-Zimmermann steht selbst oft im Zentrum intensiver Debatten. In einer der meistgehörten Ausgaben unseres Podcasts „D wie Digital“ vom DsiN-Digitalführerschein spricht sie über ihre Erfahrungen. Der Podcast selbst zielt darauf ab, Bürger:innen ohne Vorkenntnisse Einblicke in komplexe Themen zu bieten und Lösungsansätze aufzuzeigen.

Ganz persönlich getroffen: Im Kreuzfeuer von Hatespeech

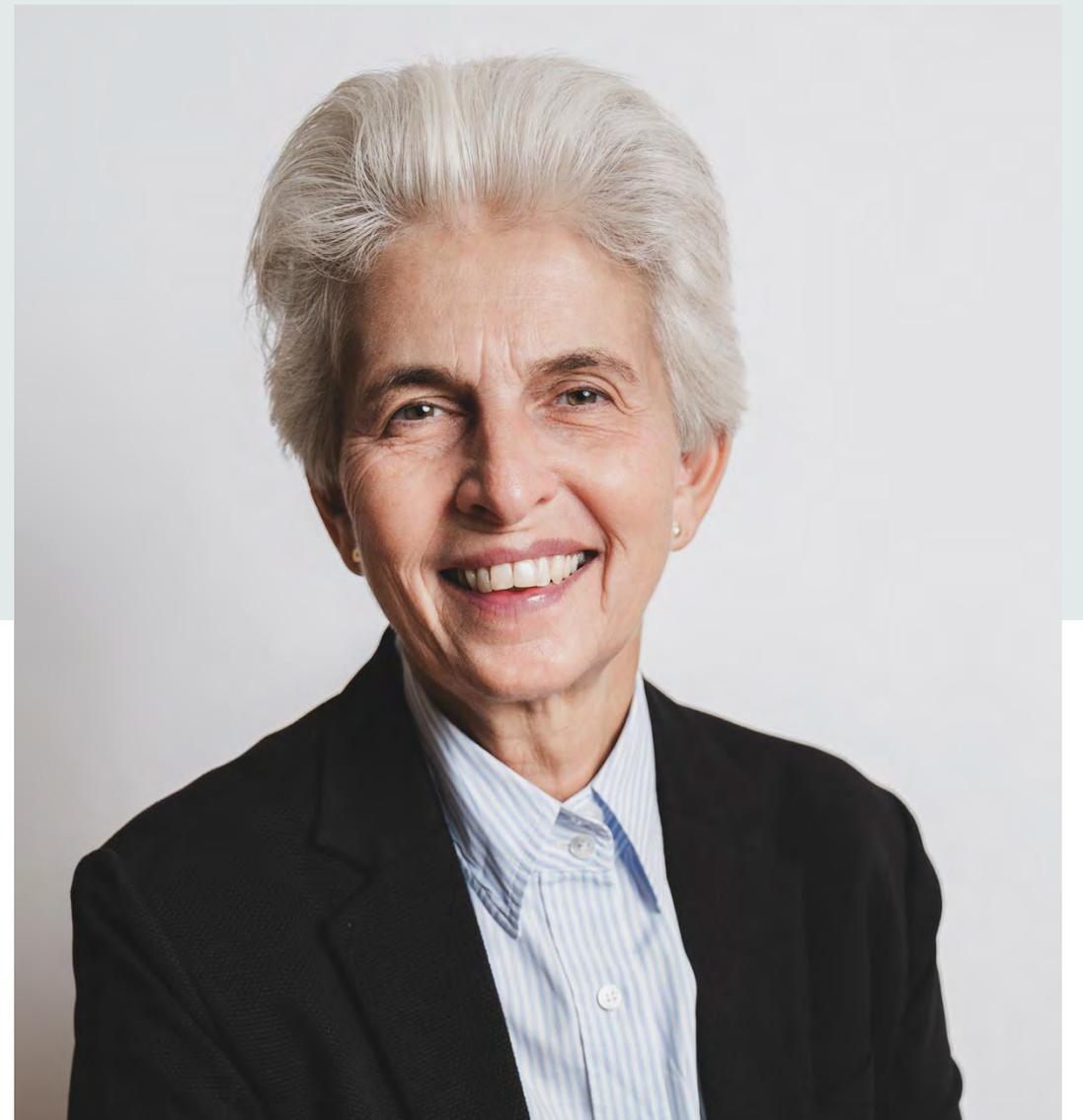
Strack-Zimmermann beschreibt zunächst eindringlich ihre eigene Konfrontation mit Hatespeech, eine Erfahrung, die sie

mit vielen Politiker:innen teilt: „Von morgens bis abends erlebe ich Hatespeech, was mir allerdings am Allerwertesten vorbeigeht“. Sie signalisiert eine beachtliche Resilienz, die sicher nicht für alle in der Politik gelten kann oder gar gelten sollte.

„Von morgens bis abends erlebe ich Hatespeech, was mir allerdings am Allerwertesten vorbeigeht.“

Dr. Marie-Agnes Strack-Zimmermann

Tatsächlich zeigt sich, dass immer mehr politisch Aktive die Kraft und innere Überzeugung verlieren, sich für unsere Demokratie einzusetzen. Unser Projekt „Politiker:innen sicher im Netz – PolisiN“ weiß von vielen Fällen zu berichten, bei denen Teilnehmer:innen der Workshops von Überforderung, Angst und fehlendem Rahmen für gute Entscheidungen



Dr. Marie-Agnes Strack-Zimmermann (FDP), Vorsitzende des Verteidigungsausschusses im Bundestag

berichten. „Eine repräsentative Demokratie braucht auch die leisen Töne, die Fragesteller:innen, die Kompromissorientierten – die werden dieser Tage mitunter totgeschrien“, berichtet PolisiN-Referent Sven Kindervater, der das Interview mit Strack-Zimmermann führte. Dazu, so Kindervater weiter, kämen die kräfteraubenden Scheidebatten anhand von Desinformation.

Wenn Desinformation den Diskurs erschwert

Desinformation, die absichtliche Verbreitung irreführender Informationen, hat historische Wurzeln, die so alt sind wie

„Eine repräsentative Demokratie braucht auch die leisen Töne, die Fragesteller:innen, die Kompromissorientierten – die werden dieser Tage mitunter totgeschrien.“

Sven Kindervater

die Medien selbst – diese Erkenntnis illustriert Strack-Zimmermann sogleich anhand aktueller Beispiele: „Wir erleben das seit dem russischen Angriff auf die Ukraine. Wir erleben es jetzt massiv, nachdem die Hamas Israel angegriffen hat.“ Diese Ereignisse verdeutlichen, wie staatlich gesponserte und individuelle



Mehr zum Thema in den DiFü-News
(DsiN-Digitalführerschein)

Akteure Desinformation nutzen, um geopolitische Ziele zu verfolgen und öffentliche Meinungen zu manipulieren.

Desinformation beeinträchtigt dabei nicht nur die politische Landschaft, sondern hat auch tiefgreifende soziale Auswirkungen. Strack-Zimmermann erörtert weiter, wie Desinformation dazu beiträgt, Misstrauen in die Medien und Regierungen zu säen und das soziale Gefüge zu destabilisieren. Sie fordert eine verstärkte Aufklärungsarbeit, um die Öffentlichkeit darüber zu informieren, wie Falschinformationen erkannt und bekämpft werden können.

Marie-Agnes Strack-Zimmermann fordert eine verstärkte Aufklärungsarbeit, um die Öffentlichkeit über die Erkennung und Bekämpfung von Falschinformationen zu informieren.

Im Ergebnis erlebten politisch Aktive nämlich, wie sie immer mehr Zeit – ob nun hauptamtlich im Bundestag oder kommunalpolitisch vor Ort – dafür verwenden müssen, sich neben anderen Argumenten und Kompromissen auch noch zunehmend mit Falschaussagen

auseinanderzusetzen. Und während Strack-Zimmermann hier berichtet, wie ihr Team sie dabei unterstützt, sind die fast 200.000 ehrenamtlichen Gemeinderatsmitglieder und Stadtverordnete meist gänzlich auf sich alleingestellt.

Technologische Abwehrstrategien und Bildungs-Offensive

In der Diskussion betont Strack-Zimmermann zudem die Bedeutung technologischer Sicherheitsmaßnahmen. Die Entwicklung und Implementierung fortschrittlicher Cybersecurity-Technologien sei entscheidend, um sensible Informationen zu schützen und die Integrität von Informationssystemen zu gewährleisten. Eveline Metzen von Google Deutschland ergänzt: „Ich komme aus dem Rheinland, ich bin mal grundsätzlich positiv eingestellt und muss dennoch sagen – ich halte die Situation, in der wir gerade sind, für unvorstellbar dramatisch, und deswegen muss sich jeder angesprochen fühlen, vom Mitglied des berühmten Karnickelvereins bis eben hin zu großen Unternehmen wie Google.“ Sie verdeutlicht, wie IT-Unternehmen täglich an ihrer Sicherheitsinfrastruktur arbeiten, um unter anderem Nutzer:innen vor Desinformation und Cyberangriffen zu schützen.

“

„Ich komme aus dem Rheinland, ich bin mal grundsätzlich positiv eingestellt und muss dennoch sagen – ich halte die Situation, in der wir gerade sind, für unvorstellbar dramatisch, und deswegen muss sich jeder angesprochen fühlen, vom Mitglied des berühmten Karnickelvereins bis eben hin zu großen Unternehmen wie Google.“

Dr. Marie-Agnes Strack-Zimmermann

“

Ein wiederkehrendes Thema sei zudem die Rolle der Bildung. Strack-Zimmermann argumentiert, dass Medienkompetenz in den Bildungscurricula verankert werden muss, um kommende Generationen auf die Herausforderungen der Informationsgesellschaft vorzubereiten. Projekte wie der Digitalführerschein von DsiN sind Beispiele für Initiativen, die darauf abzielen, Bürger:innen in die Lage zu versetzen, Falschinformationen kritisch zu hinterfragen und sicher im digitalen Raum zu navigieren.

Zusammenarbeit als Schlüssel zum Erfolg

Die Notwendigkeit einer umfassenden Zusammenarbeit zwischen verschiedenen Sektoren, einschließlich Regierung, Privatwirtschaft und Zivilgesellschaft, sei wichtig. Strack-Zimmermann spricht sich für eine verstärkte Kooperation aus, um effektive Strategien gegen Desinformation und Hatespeech zu entwickeln. „Jeder darf sich dann freuen, wenn er Post von der Staatsanwaltschaft bekommt“, unterstreicht sie die Bedeutung rechtlicher Maßnahmen im Kampf gegen schwere Fälle von Online-Hass.

So fasst es der Publizist und Politikberater Mads Pankow, der im Podcast die Sicht der Zivilgesellschaft einnahm, zusammen: „Wir müssen uns daran gewöhnen, dass wir nicht mehr in einer medialen Gesellschaft leben, in der andere für uns den

„Wir müssen uns daran gewöhnen, dass wir nicht mehr in einer medialen Gesellschaft leben, wo andere für uns den Job machen.“

Mads Pankow

Job machen.“ Frau Strack-Zimmermann, könne sich nicht allein wehren, auch wenn sie sehr wirkmächtig sei. „Aber am Ende brauchen wir alle, müssen uns zusammentun, und die Leute, die die Kompetenz haben, müssen auch für andere eintreten“, so Pankow weiter. Es ginge um eine Kombination aus Regulation, Bildung und persönlichem Einsatz von Zivilgesellschaft, Politik und Wirtschaft: „Das kann nur zusammen sein.“

Die Illustration entstand mit dem Text-zu-Bild-Generator DreamStudio.
Prompt: oil painting on a white surface of data streams only with magenta and pink colors

Künstliche Intelligenz & Ausblick

Jahresrückblick im Zeichen von KI

„Nur weil man ein Auto immer schneller baut, wird es nicht anfangen zu fliegen.“



Publizist und Politikberater
Mads Pankow

Im DiFü-Podcast „D wie Digital“ sprachen wir mit dem Experten Mads Pankow über die rasante Entwicklung von KI-Technologien. Es ranken sich viele Ängste und Mythen rund um KI; ethische Fragen, die Reproduktion von Stereotypen durch KI, politische Herausforderungen und die Zukunft der Arbeit. Pankow diskutiert, wie KI die menschliche Wahrnehmung von Logik und Ethik herausfordert und welche Auswirkungen sie auf das Rechtssystem haben könnte. Er betrachtet auch die schnelle Entwicklung und Integration von KI in alltägliche Technologien und deren potenziellen Einfluss auf die Arbeitswelt.



Podcast „D wie Digital“:
KI-lling us softly?
Künstliche Intelligenz, ein
Jahresrückblick & Ausblick

Es folgt ein Auszug, die gesamte Folge lässt sich online nachhören.

DiFü-News: Mads, warum denkst du, dass das Thema Künstliche Intelligenz nicht nur faszinierend, sondern für viele auch emotional aufgeladen ist?

Mads Pankow: Ich denke, dass das Thema stark mit Angst besetzt ist. Wenn man sieht, dass Maschinen wöchentlich oder im Monatstakt Dinge können, von denen wir dachten, dass nur wir Menschen das könnten, dann haben viele den Reflex, das

zu skalieren und zu sagen: Dann denken Maschinen bald wie Menschen, und wenn sie wie Menschen denken, dann können sie sich auch selbst verbessern. Und wenn sie das können, dann sind sie bald hyperintelligent und bringen dann plötzlich alle Menschen um? Jeder zweite Science-Fiction-Film handelt davon, dass die Künstliche Intelligenz (ein) Bewusstsein entwickelt und uns Menschen tötet. Diese Angst kann ich verstehen. Ich glaube, dass das vielleicht auch ein Grund dafür war, warum ich mich so detailliert mit dem Thema auseinandersetzen wollte.

DiFü-News: Um vielleicht auch gegen deine eigene Angst anzukommen?

Mads Pankow: Ja vielleicht. Aber eigentlich müsste man eher Angst vor dummer Technik haben. Das ist dann die andere

Hälfte der Science-Fiction-Filme; Maschinen, die ihren Auftrag nicht verstehen. Da gibt es das berühmte Paperclip-Gedankenexperiment (Anmerkung der Redaktion: Paperclip bedeutet Büroklammer): Was passiert, wenn eine KI den Auftrag hat, besonders effizient so viele Büroklammern wie möglich herzustellen? Sie fängt dann irgendwann an, alle Ressourcen auf der Welt dafür zu verbrauchen und die Menschen zu töten, um Büroklammern herzustellen. Eine solche Gefahr, dass eine Maschine stumpf und ohne Rücksicht einen Auftrag ausführt, ist wahrscheinlicher als eine Maschine, die bewusst handelt.

DiFü-News: Das klingt gruselig. Was sind deiner Meinung nach die größten negativ besetzten Mythen rund um KI?

Mads Pankow: Das ist immer schwer zu sagen, weil wir darüber ein begrenztes Wissen haben. Vor drei Jahren habe ich Dinge, die heute möglich sind, noch für unmöglich gehalten.

Um diese Frage zu beantworten, muss ich ganz weit rauszoomen: Ich denke, der größte Mythos ist, dass jede Form von Problemlösungsfähigkeit am Ende mit menschlicher Intelligenz gleichgesetzt wird – oder einer Vorstufe – und man dann anfängt, überall menschliche Intelligenz zu sehen. Der Delfin kann Probleme lösen, also ist er genauso intelligent wie wir, der

muss nur schneller werden, wir sehen, wie intelligent Krähen und Primaten sind. Beim Primaten ist das ja auch ein plausibles Argument, weil wir uns aus dem heraus entwickelt haben. Aber Computern wird immer unterstellt, dass wenn wir sie noch schneller machen, dass sie dann wie Menschen denken können. Früher gab es

„Aber Computern wird immer unterstellt, dass wenn wir sie noch schneller machen, dass sie dann wie Menschen denken können.“

Mads Pankow

beispielsweise die Annahme, dass ein Computer bei 10.000 Terraflops so schnell wie das menschliche Gehirn ist.

Ich denke, das Wichtige ist zu verstehen, dass es erkenntnistheoretisch oder bewusstseinstheoretisch beliebig viele verschiedene Formen gibt, um die Welt zu verarbeiten und Probleme zu lösen. Diese Formen müssen dann aber nicht automatisch auf eine menschliche Intelligenz zustreben. Denn nur weil man ein Auto immer schneller baut, wird es nicht anfangen zu fliegen. Die Art und Weise, wie Menschen verarbeiten, ist im Gegenteil viel schlechter als Computer, bei denen wir immer darauf warten: Wann sind die intelligenter als wir? Taschenrechner

rechnen seit 80 Jahren schneller als jeder Mensch. Sprachmodelle können inzwischen so viel Wissen verarbeiten wie kein Mensch. Ich frage mich, worauf wir warten. Die KI ist in vielerlei Hinsicht längst viel besser als wir, und zwar in den Dingen, die sie gut kann. Und warum müssen wir immer noch mit Gewalt versuchen, ihr auch noch beizubringen, wie wir denken,

„Die KI ist in vielerlei Hinsicht längst viel besser als wir, und zwar in den Dingen, die sie gut kann.“

Mads Pankow

nämlich leider extrem unlogisch, sehr ineffizient. Aber: Wir haben ein Bewusstsein, wir können reflektieren, wir wissen um die Existenz der Welt. Das zeichnet uns Menschen aus und dadurch können wir andere Lösungen finden. Maschinen haben das nicht, sie verarbeiten nur Nullen und Einsen. Wir haben mit Künstlicher Intelligenz sehr viel möglich gemacht, aber die Frage des Bewusstseins, also einer Selbst- und Fremdrelexion, der Weltverarbeitung und das Wissen um die Existenz der Welt – da gibt es überhaupt keinen Fortschritt.

DiFü-News: *Es gibt viele Debatten darüber, dass Künstliche Intelligenz Stereotype reproduziert, weil die Daten für die KI eben von Menschen eingespeist werden. Kannst du etwas dazu sagen, wie KI uns als Gesellschaft vielleicht den Spiegel vorhält?*

Mads Pankow: Das ist eine großartige Frage. Meiner Meinung nach ist die Geschichte der KI und der Algorithmen eine kontinuierliche Kränkung des Menschen. Vorher galt der Mensch als logisch denkendes Wesen als hohes Ideal der Philosophie: Doch rational denken, besser rechnen und logisch denken, das können Computer schon lange viel besser als wir. Außerdem müssen wir uns, genau, wie du gesagt hast, damit auseinandersetzen, dass, wenn ein

Computer von Menschen lernt, er vor allem auch Rassismen, Chauvinismen und Vorurteile lernt.

Dass unsere Kreativität, die wir vorher für einen göttlichen Funken gehalten haben, in verschiedenster Art und Weise durch einen Computer abzubilden ist, ist eine große Enttäuschung. Genauso wie die Annahme, dass wir wissen, was richtig und falsch ist – wenn wir versuchen, das einem Computer beizubringen, stellen wir fest, dass Ethik nicht eindeutig ist. Es gibt viele Graubereiche. Das heißt nicht, dass sie falsch ist, aber das entzaubert das Verständnis von richtig und falsch, bis hin zur gesellschaftlichen Konstruktion. Stellen wir uns vor, dass wir einen Rechtssprechungscomputer bauen, der die Gesellschaft überwacht. Was macht das mit einer Gesellschaft, wenn jedes Vergehen geahndet wird? Unser Rechtssystem basiert zwar auf der Idee, dass wir alle gleich sind und dass wir alle jederzeit geahndet werden müssten. Das passiert dann aber nicht, denn unser Rechtssystem baut darauf, dass es immer Variationen und Interpretationen von Menschen mit Entscheidungsspielräumen gibt. Ich will das Recht nicht lächerlich machen, es ist richtig und gut. Aber es funktioniert anders, als wir uns das vorgestellt haben.

DiFü-News: *Welche Auswirkungen kann das haben?*

Mads Pankow: Es gibt Regionen auf der Welt, in denen man Künstliche Intelligenz weniger kritisch sieht. Es gibt eine chinesische Stadt, in der die Ampeln mit Sprühsystemen ausgestattet sind. Wer bei Rot über die Ampel geht, wird nass gesprüht. Wir müssen uns damit auseinandersetzen, was diese Automatisierung der Ahndung und dieses Nudging der Bevölkerung, hin zu einem erwünschten Verhalten, bedeutet. Im Moment sagen wir hier: Das ist bevorzugend, das trainiert die intrinsische Motivation zu rechtem Verhalten ab, weil man überall überwacht wird. Ja, ist

„**Wir haben mit Künstlicher Intelligenz sehr viel möglich gemacht, aber die Frage des Bewusstseins, also einer Selbst- und Fremdrelexion, der Weltverarbeitung und das Wissen um die Existenz der Welt – da gibt es überhaupt keinen Fortschritt.**“

Mads Pankow

alles richtig. Das ist alles hoch bedenklich, auch wenn man bedenkt, dass möglicherweise eine politische Agenda durchgesetzt wird und eine Gesellschaft so zunehmend überwacht wird. Das könnte aber möglicherweise auch Vorteile haben, dass zum Beispiel Kriminalität fast vollständig ausgerottet ist. Es wird schon jetzt häufig nach China geschaut. Ich stelle mir dann

„Ich glaube, wir müssen uns hier zeitnah Gedanken machen, wie wir unsere Gesellschaft als universalistische, rechtsstaatliche Gesellschaft neu denken, mit künstlicher Intelligenz.“

Mads Pankow

aber vor, wie wir in 40 Jahren solche Systeme importieren müssen. Davon habe ich Angst. Ich glaube, wir müssen uns hier zeitnah Gedanken machen, wie wir unsere Gesellschaft als universalistische, rechtsstaatliche Gesellschaft, mit künstlicher Intelligenz neu denken. Da müssen wir anfangen, so etwas selbst zu bauen. Nur weil es kompliziert und gefährlich ist, können wir uns dem nicht verwehren.

DiFü-News: *Kannst du uns noch kurz einen Rückblick auf das Jahr 2023 geben?*

Mads Pankow: 2022 war die Zeit, in der die ersten wichtigen generativen KIs

veröffentlicht wurden, Bildgeneratoren und Sprachmodelle, die so sprechen und Bilder erstellen konnten, dass wir sie kaum von menschlichen Produkten unterscheiden konnten. 2023 sind wir bereits in dem Jahr, in dem das in der Masse ausgerollt wurde. Das ging sehr schnell für einen technologischen Schub, insbesondere wenn man vergleicht, wie lange es bei E-Mails oder Social Media gebraucht hat, um sich im Internet zu verbreiten. Innerhalb weniger Wochen hat ChatGPT mehr als 100 Millionen Nutzer:innen erreicht. Solche Large Language Models durchdringen jetzt überall unsere Anwendungen: Man kann sich das so vorstellen, dass 2023 der Anfang war, dass generative KI sich wie ein dünner Film über alle Nutzeroberflächen legte.

In einem Jahr kann es sein, dass die meisten Menschen keine E-Mails mehr selbst schreiben, sondern nur noch den Befehl geben: Schreib eine freundliche Absage. Es gibt so viele Bereiche, die davon beeinflusst sind, Programmieren ändert sich gerade rapide. Ich glaube, dass 2023 mit dem Ausrollen dieser wirklich funktionalen Technologien in die Breite, dass das eben nicht mehr ein Nischenprodukt ist, sondern dass man diesen smarten Assistenten nicht mehr entgehen können wird.

2023 – ein Jahr ChatGPT

WIE UMGEHEN MIT DEM KI-HYPE?

Seit der Veröffentlichung von ChatGPT im November 2022 hat das Thema Künstliche Intelligenz ein neues Tempo aufgenommen. Erstmals zeigte sich ein computer-generierter Chat in der Lage, überraschend menschliche und sachbezogen-informative Antworten zu geben. Viel mehr noch: Er verstand, was von ihm verlangt wurde und erledigte die Aufgabe mitunter besser, als es sich der Mensch vor dem Endgerät zutraute. Wo kommt diese Technologie her – und wie damit umgehen?

Eigentlich ging der Hype mancherorts schon vor ChatGPT los: Mit der Bilderzeugungs-KI „Dall-E“ (gesprochen „Dali“, wie der bekannte spanische Maler) entstanden gänzlich neue Grafiken, rein basierend auf der Eingabe per Text. Beide Produkte stammen von der Firma OpenAI, die eine wechselvolle Geschichte hinter sich hat. Im Bewusstsein, welche Möglichkeiten entstehen und vor allem welche Macht KI haben kann, wurde die Firma als Non-Profit-Organisation gegründet mit der festen Absicht, niemals ein florierendes Geschäftsmodell zu entwickeln und eine Marktdominanz zu erreichen.

Einige Zeit später verwarf man sich bereits mit einigen Gründern, darunter Elon Musk (der dann vehement vor der KI warnte und mittlerweile mit „Grok“ seine eigene KI entwickelt hat). Nach einer Milliarden-Förderung an das Unternehmen rund um Gründer Sam Altman steht OpenAI Microsoft so nahe, dass der Windows-Konzern mittlerweile sein gesamtes Geschäftsmodell auf die Möglichkeiten von OpenAI ausrichtet – womit aus Sicht vieler der Non-Profit-Gedanke endgültig ad acta gelegt wurde.

Illustrationen erstellt mit DreamStudio

Prompt: abstract illustration on a white surface of artificial intelligence with light blue, dark blue, light green, dark green, turquoise and a little magenta



Ratgeber & Tools
KInsights! – künstliche
Intelligenz einfach entdecken



KI – bitte was ?

Der Begriff KI (Künstliche Intelligenz) ist kein geschützter Begriff und hat keine einheitliche Definition. Im Grunde muss er seit Jahrzehnten dafür herhalten, wenn vor allem auf einem Bildschirm „Dinge“ passieren, die ein Mensch nicht direkt selbst steuert. So bezeichnen Videospiele:innen die Computergegner:innen schon sehr viel länger als KI. Auch im Bereich des autonomen Fahrens kommt der Begriff seit vielen Jahren vor. Die tagesaktuellen Debatten richten sich dabei vor allem an eine bestimmte Form: die sogenannte „generativen KI“, die Bilder, Texte, Videos und Audios per Eingabe erzeugen kann.

Das Dynamische ist, dass generative KI-Modelle exponentiell lernen. Das bedeutet, dass sich ihre Qualität nach aktueller Kenntnis in einem sich stets steigenden Tempo verbessert. Aktuell basiert beispielsweise ChatGPT – was eigentlich nur als Test gedacht war, nun aber aufgrund seiner Beliebtheit weiter ausgebaut wird – auf der Version GPT 4 sowie als Option zum Vorgänger GPT 3.5, während bereits erste Testversionen von GPT 5 im Umlauf sind. Die Versionssprünge dabei sind eher willkürlich und beruhen vor allem auf größeren Entwicklungssprüngen wie zum Beispiel im Erkennen von Bildern, die zusätzlich zu den Texteingaben hochgeladen werden können.

Auf diesen GPT-Versionen basieren auch die allermeisten anderen Angebote wie der „Bing Chat“ sowie „Copilot“ von Microsoft und viele der wohl täglich über 200 neuen KI-StartUps. Es gibt aber auch andere Modelle, etwa „LLaMa“ von Meta (zuvor Facebook) oder „Gemini“ von Google. Der Suchmaschinen-Primus aus Palo Alto fährt dabei ein sehr breit gefächertes Konzept aus Privat- und Unternehmensanwendungen auf. Das Bildprogramm „Canva“ nutzt mit seiner KI-Funktion „Magic Switch“ bspw. Google-Modelle. Mittlerweile gibt es auch erste Endgeräte wie die Smartphones von Google oder Samsung, die eine sogenannte „NPU“ haben. Eine „Neural Proces-

sing Unit“ – ein Chip, der extra für Rechenleistungen von KI-Modellen eingebaut ist, sodass zum Beispiel einfache KI-Anwendungen auf dem Endgerät ohne Verbindung zum Internet stattfinden können.

Der ChatGPT-Schock stellt eine Branche auf den Kopf

Der „ChatGPT“-Schock im Frühjahr 2023, als sich das Tool seinen Weg in die allgemeine Aufmerksamkeit bahnte und klar wurde, dass es wohl zu mehr als nur zum Üben genutzt werden wurde, äußerte sich aber auch in der Annahme, die seit ca. 20 Jahren stabilisierten Verhältnisse in der digitalen Marktdominanz von Anbietern auf den Kopf zu stellen. Es hat ein neues Wettrüsten begonnen, denn es ist klar: Wenn KI auf alles (scheinbar) eine Antwort hat und vieles selbst erzeugen kann, sind aktuelle Lösungen wie beispielsweise Suchmaschinen obsolet. Doch da gibt es einen Haken: die Kosten.

Eine Eingabe – man spricht hier von „Prompts“ – von einer KI kann das bis zu 100-fache an Strom im Vergleich zu einer Anfrage in einer Suchmaschine kosten. Wer diese Kosten trägt, ist aktuell noch völlig offen. Zwar haben Modelle wie Gemini oder ChatGPT ein mitunter mehrstufiges Bezahlmodell, allerdings zahlen die großen Anbieter aus den USA die meisten Kosten gerade aus der Portokasse, wohl um sich im Wettbewerb zunächst die beste Marktposition zu erkämpfen. Es ist zu erwarten, dass sich der Markt aufteilt, wie schon bei den sozialen Medien: Während es Services gibt, bei denen wir mit unseren Daten „bezahlen“, werden andere auf monetäre Bezahlmodelle setzen. Letztere werden sich dabei scharf nach Datenvolumen staffeln, ähnlich wie beim Cloud-Speicher.

Aktuell überwiegt das Sammeln von Daten. Denn mit jedem „Prompt“ trainieren nun auch wir die LLMs. Das führt immer wieder zu Datenschutzbedenken. Es zeigt sich, dass Menschen sehr viel mehr Intimes über sich oder bspw. ihre Firma eintragen.



Dadurch geben sie fast noch mehr Einblicke in ihr Seelenleben und ihre Ziele preis als zuvor in den sozialen Medien und davor in den Suchmaschinen. Einige große Unternehmen untersagten daraufhin sehr schnell die Nutzung von ChatGPT. Viele Anbieter wiederum reagierten mit speziellen Unternehmens-Produkten, teilweise angeknüpft an bestehende Abo-Modelle wie etwa Google Workspace oder Microsoft 365 Enterprise, die nach einigen Angaben genau nicht „nach Hause telefonieren“.

Aber auch das Urheberrecht meldet sich zu Wort. Da viele KI-Modelle mehr oder weniger nachweislich urheberrechtlich-geschützte Texte aus der Literatur, Journalismus oder Wissenschaften sowie Videos und

Wo hört bei erzeugter Kunst die Inspiration auf und wo fängt das Kopieren an?

Musik kennen, klagen nun einige über die nicht-genehmigte Verwendung und bestehen zudem teilweise auf Lizenzgebühren. Auch steht eine fast schon philosophische Frage im Raum: Wo hört bei erzeugter Kunst die Inspiration auf und wo fängt das Kopieren an? KI-Enthusiasten argumentieren dabei, dass Künstler:innen sich schon immer gegenseitig inspirieren haben und nun inspirieren lassen sich KI eben durch die Werke anderer. Aber wenn ein Song auch immer mehr überzeugend echt an die Lieder der Original-Interpreten herankommt, weil es deren Lebenswerk „studiert“

hat und es nachweislich Nutzenden auf Spotify reichlich egal ist, ob der „neue Song“ von Jay Z tatsächlich nur KI-erzeugt ist, dreht dies ganze Branchen auf den Kopf.

Politik und Regularien für die KI

Es wird daher noch viele Entscheidungen der Rechtsprechung und womöglich auch der Politik geben, denn wie so oft preschen vor allem amerikanische Unternehmen erst einmal vor und ordnen dann eher im Nachgang. So sieht es der deutsche Digitalminister Dr. Volker Wissing (FDP) sehr kritisch, dass OpenAI ausgerechnet jetzt nach gesetzlichen Regulierungen ruft. Hintergrund ist die Tatsache, wie einst bei der im Zuge der Einführung der DSGVO gefürchteten Bürokratie, dass große Firmen diese Regularien spielend bewältigt bekommen, sie kleine Unternehmen hingegen vor große Herausforderungen stellen können. Hier geht es wohl auch um den Schutz deutscher Branchen-Vorreiter wie Aleph Alpha aus Heidelberg. Denn mit zu viel Regulierung zum jetzigen Zeitpunkt würden kleinere deutsche Firmen womöglich zu früh vor dem Aus stehen – und die EU damit erneut in eine Abhängigkeit von Digitaldiensten aus dem Silicon Valley geraten.

Staaten wie China spielen derweil mit dem Gedanken, ihren Bürger:innen die Nutzung von KI im Einzelfall zu erlauben oder zu verbieten. Die Nutzung solle in jedem Fall gekennzeichnet werden. Wie dies allerdings erreicht werden soll, bleibt unbeantwortet. Einige Firmen haben dazu eine bestimmte Form des digitalen Wasserzeichens erfunden, etwa SynthID von Google. Es droht aber eher, dass sich ähnlich wie beim Bundestrojaner echte Cyberkriminelle bestens zu verschleiern wissen, während „der kleine Mann“ mit vergleichsweise geringen Verstößen ins Visier der Ermittler:innen gerät. Inwieweit das als Mittel gegen Urheberrechtsverletzung dienen kann, jedoch sonstige Kriminalität nicht aufhält, bleibt offen.



Martin Groß-Albenhausen

stellv. Hauptgeschäftsführer,
Bundesverband E-Commerce
und Versandhandel Deutsch-
land e. V. (bevh)

DsIN und BEVH arbeiten gut zusammen, weil ...

... beide Organisationen Wege dafür bahnen, die Chancen der Digitalisierung im beruflichen und privaten Umfeld sicher und souverän zu nutzen. Aufgabe des BEVH ist es, für bestehende und neue Formen des Einkaufens und Verkaufens im Internet verlässliche und faire Regeln mitzugestalten. DsIN vermittelt auf allen Ebenen der Zivilgesellschaft die Kompetenz, mit der Entwicklung digitaler Technologien Schritt zu halten und so vom Zuwachs an Angeboten durch das Internet zu profitieren.

Digitale Kompetenzförderung ist wichtig, weil ...

... das Leitbild der mündigen Bürger:innen in einer freiheitlichen Demokratie nur dann Bestand hat, wenn die Menschen in die Lage versetzt werden, jederzeit bewusste und selbstverantwortliche Entscheidungen im digitalen Raum zu treffen.

Cybersicherheit ohne Kooperation ist wie ...

... Hausbau ohne Zusammenarbeit von Bauherrn, Architekten, Bauleitung und Gewerken.

Drei Fragen an den Beirat

DsIN und BfDI arbeiten gut zusammen, weil ...

... wir gemeinsame Interessen und Strategien bei der Förderung digitaler Fähigkeiten zur Stärkung von Sicherheit und Datenschutz im digitalen Raum verfolgen.

Digitale Kompetenzförderung ist wichtig, weil ...

... in einer zunehmend digitalisierten Welt dadurch die notwendige Mündigkeit erreicht wird, um digitale Technologien effektiv nutzen und gleichzeitig Persönlichkeitsrechte und Privatsphäre schützen zu können.

Cybersicherheit ohne Kooperation ist wie ...

... ein Schiff ohne Segel, das keine Fahrt aufnehmen kann. Nur durch Kooperation und Bündelung von Expertise sind die Herausforderungen im Bereich der Cybersicherheit sinnvoll und mit den notwendigen Mitteln zu bewältigen.



Tanja Jost

Abteilungsleitung Technologischer
Datenschutz, Telekommunikation
und Telemedien



„Um die Cybernation Deutschland zu gestalten, brauchen wir ein zielgerichtetes und vor allem schlagkräftiges Engagement für Cybersicherheit“

Claudia Plattner

Claudia Plattner

Präsidentin, Bundesamt für Sicherheit in der Informationstechnik (BSI)

DsiN und BSI arbeiten gut zusammen, weil ...

... wir uns als Partner einig sind: Nur Kooperation gewinnt. Um die Cybernation Deutschland zu gestalten, brauchen wir ein zielgerichtetes und vor allem schlagkräftiges Engagement für Cybersicherheit – und das kann nur gemeinsam gelingen. DsiN vernetzt viele wichtige Partner aus Wirtschaft, Verwaltung und Wissenschaft und setzt mit öffentlichkeitswirksamen Projekten Cybersicherheit auf die Agenda. Dieses Ziel verfolgt auch das BSI.

Digitale Kompetenzförderung ist wichtig, weil ...

... wir die Bürger:innen nicht mit den Herausforderungen unserer Zeit allein lassen dürfen. Die Cyberbedrohungslage ist besorgniserregend. Deshalb müssen wir die Menschen im Netz aktiv schützen – etwa, indem wir sie dabei unterstützen, die richtigen Schutzmaßnahmen zu ergreifen, Gefahren rechtzeitig zu erkennen und Ernstfälle souverän zu überwinden.

Cybersicherheit ohne Kooperation ist wie ...

... Sicherheit ohne Cyber: in einer digital vernetzten Welt einfach nicht möglich.



Patrick von Braumnühl

Leiter Public Affairs,
Bundesdruckerei GmbH

DsiN und Bundesdruckerei arbeiten gut zusammen, weil ...

... sich unsere Kompetenzen hervorragend ergänzen.

Digitale Kompetenzförderung ist wichtig, weil ...

... sie die Voraussetzung dafür ist, sich sicher im Netz zu bewegen.

Cybersicherheit ohne Kooperation ist wie ...

... ein Boot auf hoher See ohne Funkkontakt.

Ausblick & Perspektiven auf das neue Jahr 2024



Insgesamt wird es 2024 darum gehen, die Relevanz von Datenkompetenzen für Cyberresilienz und digitale Teilhabe in Öffentlichkeit und Politik zu verdeutlichen und neue Ansätze zu entwickeln, wie Kompetenzförderung in der Breite der Gesellschaft über neue Strukturen wirkungsvoll gestaltet werden kann.

Wie auch 2023 steht das neue Jahr 2024 unter dem Leitthema der Cyberresilienz für Demokratie und Sicherheit im 21. Jahrhundert - Desinformation entgegenwirken.

Unsere Initiativen für private Nutzer:innen werden wir weiterentwickeln, insbesondere:

- für ältere Generationen mit dem **Digital-Kompass** (Förderung durch BMUV) an mehr als 100 Standorten sowie mit dem **Digitalen Engel** (Förderung durch BMFSFJ) mit einem aufsuchenden Ansatz für sichere digitale Teilhabe im Alltag.
 - im Projekt Digitaler Engel das Engagement im **Bundesland Thüringen** ausweiten, das uns ermöglicht, die Netzwerke im Flächenland auszubauen und zu verdichten.
 - weitere Landesengagements im Rahmen des Bundesnetzwerkes Digitale Nachbarschaft in Bayern mit **Digital Verein(t)** sowie Rheinland-Pfalz voranbringen sowie eine Roadshow zur EU-Wahl im April 2024 an mehreren Standorten in Bayern.
- Für die über 200.000 politisch aktiven Menschen entwickeln wir **PolisiN – Politiker: innen sicher im Netz** weiter: die Initiative wird unter einer fraktionsübergreifenden MdB-Schirmherrschaft zusätzliche Workshops und Schulungen durchführen sowie den Fokus verstärkt auch auf kommunale und ehrenamtliche Politik legen.
- Für unsere Projekte sowie zahlreiche Partnerschaften und Kooperation möchten wir den **DsiN-Digitalführerschein** als Standardtool zum Erwerb und Nachweis digitaler Kompetenz etablieren und insbesondere im beruflichen Umfeld zusätzliche Partner gewinnen. Die Grenzmarke von 200.000 absolvierten Prüfungen soll bis Jahres 2024 erreicht werden.

Für mittelständische Unternehmen stehen die Zeichen ganz auf NIS2:

- Mit einem neuen Angebot, dem **FitNIS2-Navigator** möchten wir im Rahmen der Initiative IT-Sicherheit in der Wirtschaft des BMWK ab dem 4. Quartal ein zentrales Angebot zur Unterstützung und Orientierung betroffener Unternehmen bereitstellen, das den eigenen Grad der Compliance darstellt und passende Maßnahmen vermittelt, um den Anforderungen zu entsprechen.
 - Darüber hinaus werden wir das Angebot für Ausbildungsbetriebe, **mIT Sicherheit ausbilden**, in die Breite tragen und in Zusammenarbeit mit der Transferstelle CYBERsicher insbesondere Ausbildungsverantwortliche zur Förderung von IT-Sicherheitskompetenzen im Betrieb befähigen.
- Zudem steht der **Ausbau der Kooperation** im Fokus unserer Arbeit; in einer neuen Kooperation mit der Bertelsmann Stiftung möchten wir das „**Forum gegen Fakes**“ unterstützen und gemeinsam neue Beteiligungsformen erproben, um im Kampf gegen Desinformation wirksame Strategien und Methoden zu entdecken. Die Übergabe der Empfehlungen an die DsiN-Schirmherrin, Nancy Faeser, ist für Herbst 2024 geplant. In der **Stiftung Warentest** wird DsiN (Dr. Michael Littger) im Kuratorium die Themen Datenschutz und Digitale Gesellschaft vertreten.
- Insgesamt wird es 2024 darum gehen, die Relevanz von Datenkompetenzen für Cyberresilienz und digitale Teilhabe in Öffentlichkeit und Politik zu verdeutlichen und neue Ansätze zu entwickeln, wie Kompetenzförderung in der Breite der Gesellschaft über neue Strukturen wirkungsvoll gestaltet werden kann. In diesem werden wir den **Dat-O-Mat** zur auf den Weg bringen (BMBF), er die Transparenz der Angebotslandschaft erhöht sowie fehlende Angebote (Vakanzen) sowie Doppelungen (Redundanzen) identifiziert. Mit dem **DsiN-Jahreskongress 2024** verdeutlichen wir die Potenziale und Perspektiven der digitalen Kompetenzförderung – auch im öffentlichen und politischen Raum.

Neue Projekte 2024

Transferprojekte und -tools (Beispiele)

Digitaler Engel | Unser Bundesprojekt Digitaler Engel soll auf Landesebene ergänzt werden und dazu ein Projekt im Bundesland Thüringen ein eigenständiges Projekt auf den Weg bringen, das den aufsuchenden Ansatz in ländliche Regionen nachhaltig verdichtet.

Dat-O-Mat | Die Erhebung individueller Kompetenzbedarfe und ihr passgenaues Matching mit vorhandenen Angeboten ist Ziel dieses KI-gestützten Forschungsvorhabens. Im Ergebnis soll eine Orientierungshilfe auch für Anbieter entstehen, die sich über Vakanzen informieren.

FitNIS2-Navigator | Für Unternehmen dürften die NIS2-Regelungen das Thema im neuen Jahr werden. Als Orientierungs- und Umsetzungshilfe möchte DsiN ein Vorhaben in Kooperation mit der Transferstelle CyberSicher auf den Weg bringen, KI-Hilfe inklusive!

Digital-Kompass | Im Projekt für ältere Generationen dreht sich alles um vulnerable Menschen mit Gehör- und Seh- sowie Mobilitätsbeeinträchtigungen. Neue Kooperationsformate mit Universitäten soll die Förderung digitaler Kompetenzen zusätzlich befeuern.

PolisiN – Politiker: innen sicher im Netz | Das Projekt widmet sich verstärkt der Zielgruppe der rund 200.000 politischen Ehrenämter. Sie erfahren oftmals keine Unterstützung im Umgang mit IT. Hinzu kommen Politiker: innen auf Landes- (MdL) und Bundesebene (MdB).

Sicher Handeln | Die neue Initiative zur Aufklärung von Verhaltensweisen zum sicheren Onlineshopping wird 2024 an Fahrt aufnehmen und in Kooperation auch mit Polizeien zusätzliche Verbreitung finden.

Mitglieder & Partner

Mitglieder | DsiN möchte an sein Wachstum der Mitgliederbasis anknüpfen und 5 bis 6 neue engagierte Unternehmen hinzugewinnen, die Cybersicherheit und sichere digitale Teilhabe gemeinsam mit Leben füllen wollen.

Förderpartner | Als Zeichen der Befürwortung und Unterstützung des DsiN-Engagements steht allen Organisationen die Zusage einer Förderpartnerschaft zu. Im Gegenzug werden sie zu Veranstaltungen eingeladen und können ihre Partnerschaft nach außen zeigen.

Impressum

Deutschland sicher im Netz e. V. (DsiN)
Berlin Juli 2024
Verantwortlich (V.i.S.d.P.): Joachim Schulte

Redaktion

Judith Neuling, Can Felix Demirden

Gestaltung

Pia Kolle, Judith Neuling

Druckerei

Europrint Medien GmbH

Bildnachweise

S. 1: Ministerin Nancy Faeser/Peter Jülich

S. 4: Thomas Tschersich/Telekom, Joachim Schulte/Rafalzyk

S. 10: Paul Heimann/Kleinanzeigen

S. 13: Margit Stumpp, Stefan Kaminski

S. 14/15: Gruppenbild/Andi Weiland

S. 22-31: Jahreskongress 2023, Stefanie Loos

S. 32: Preisverleihung/Stefanie Loos

S. 34: Digitaler Engel/Derk van Groningen

S. 42-44: Tag der offenen Tür/Henning Schacht

S. 55: Tabea Rößner/MdB, Anna Kassautzki/MdB

S. 55: Marc Henrichmann/Anja Tiwisina, Manuel Höferlin/Christian Kuhlmann

S. 72-73: Plakatkampagne, SilkeReents

S. 74: Dr. Marie-Agnes Strack-Zimmermann/MdB

S. 80: Mads Pankow/Steven Haberland

S. 88-91: Martin Groß-Albenhausen/bevh, Tanja Jost/BfDI, Claudia Plattner/BSI, Patrick von Braunmühl/Bundesdruckerei GmbH

S. 96 Dr. Michael Littger/Andi Weiland

Umschlag (U4): Andreas Könen/BMI, Prof. Dr. Christian Bär/BMI, Patrick von Braunmühl/Bundesdruckerei GmbH, Prof. Dr. Gabi Dreo Rodosek/Universität der Bundeswehr München, Gesa Förster/BMWK, Martin Groß-Albenhausen/bevh, Dr. Sven Herpig/Stiftung Neue Verantwortung, Tanja Jost/BfDI, Holger Münch/BKA, Claudia Plattner/BSI, Mirja Rasmusson/BMDV, Prof. Dr. Haya Shulman/Frauenhofer SIT, Wolfgang Teves/BMUV

Alle weiteren Bilder: Deutschland sicher im Netz e.V.

Kontakt

Deutschland sicher im Netz e.V. (DsiN)

Albrechtstr. 10 c

10117 Berlin

Telefon +49 (0) 30 767581-500

info@sicher-im-netz.de

sicher-im-netz.de

Geschäftsführung & Teamsprecher:innen



Joachim Schulte
(seit Juni 2024)
Geschäftsführer
Deutschland sicher im Netz e.V. (DsiN)



Dr. Michael Littger
(bis Mai 2024)
Geschäftsführer
Deutschland sicher im Netz e.V. (DsiN)



Aliona Tebidze
Teamsprecherin
Deutschland sicher im Netz e.V.
(DsiN)



Sven Kindervater
Teamsprecher
Deutschland sicher im Netz e.V.
(DsiN)

DsiN-Vorstand



Thomas Tschersich
DsiN-Vorstandsvorsitzender
Chief Security Officer (CSO),
Deutsche Telekom AG



Martin Drechsler
Schatzmeister
Geschäftsführer, Freiwillige
Selbstkontrolle Multimedia-
Diensteanbieter e.V.



Nikolaus Hagl
Stellv. Vorstandsvorsitzender
Leiter Geschäftsbereich
Public & Energy, SAP Deutsch-
land SE & Co. KG



Michael Guntsch
(bis Ende 2023)
Beisitzer
Engineering Director,
Privacy, Safety & Security,
Google Deutschland



Dr. Jochen Eisinger
(seit 2024)
Beisitzer
Director of Engineering for
Chrome Trust & Safety,
Google Deutschland



Dr. Robert Reinermann
Beisitzer
Vorsitzender der Geschäftsfüh-
rung, VdS Schadenverhütung
GmbH

Beirat



Andreas Könen
(bis Ende 2023)

Abteilungsleiter Cyber- und Informationssicherheit, Bundesministerium des Innern und für Heimat (BMI)



Prof. Dr. Christian Bär
(bis Ende 2023)

Technikvorstand, DATEV eG (BMI)



Patrick von Braumnühl

Leiter Public Affairs, Bundesdruckerei GmbH



Prof. Dr. Gabi Dreo Rodosek

Professorin für Kommunikationssysteme und Netzsicherheit, Universität der Bundeswehr München



Gesa Förster

Leiterin der Initiative IT-Sicherheit in der Wirtschaft, Bundesministerium für Wirtschaft und Klimaschutz (BMWK)



Martin Groß-Albenhausen

Stellv. Hauptgeschäftsführer, Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh)



Dr. Sven Herpig

Leiter Internationale Cybersicherheitspolitik, Stiftung Neue Verantwortung



Tanja Jost

Abteilungsleitung Technologischer Datenschutz, Telekommunikation und Telemedien beim Bundesdatenschutzbeauftragten (BfDI)



Holger Münch

Präsident, Bundeskriminalamt (BKA)



Claudia Plattner

Präsidentin, Bundesamt für Sicherheit in der Informationstechnik (BSI)



Mirja Rasmusson

Referatsleiterin, Datenschutz in der digitalen Welt, Cybersicherheit, Vertrauensdienste, Bundesministerium für Digitales und Verkehr (BMDV)



Prof. Dr. Haya Shulman

Direktorin Cybersecurity Analytics and Defences, Fraunhofer SIT



Wolfgang Teves

Referatsleiter, Grundsatzfragen des digitalen Verbraucherschutzes, vertrauenswürdige KI, Cybersicherheit, Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz (BMUV)



Susanne Wein

Referatsleiterin, Bildung für ältere Menschen, Digitalisierung, Bundesministerium für Familien, Senioren, Frauen und Jugend (BMFSFJ)

Mitglieder



