.inf 14

DAS INFORMATIK-MAGAZIN
SOMMER 2026

GESELLSCHAFT
FÜR INFORMATIK

The good, the bad and the § 202

Was der Hackerparagraph für White Hats bedeutet

INF.GI.DE ISSN 2940-0694

Systemfehler: Warum viele Frauen der IT den Rücken kehren **SEITE 8**

Nachhaltigkeit ist kein Add-on: Informatik als Teil der Lösung **SEITE 14**

Kanzleramt und Karaokebar: Wie erreichen junge Stimmen die Digitalpolitik? **SEITE 22**

An issue has been detected

Martin Wolf, Präsident der Gesellschaft für Informatik e.V.

Wer hackt, ist nicht gleich kriminell: Viele Forschende versuchen gezielt, die IT-Sicherheitsmaßnahmen von Unternehmen oder Organisationen zu durchbrechen, um ihnen zu helfen, diese besser zu gestalten. Doch für die sogenannten White-Hat-Hacker kann das nach aktueller Gesetzeslage mit einer Anzeige enden. GI-Referentin Marieke Petersen liefert in dieser Ausgabe einen Rundumschlag zum sogenannten Hackerparagraphen – und zahlreiche Stimmen und Argumente, die für seine Abschaffung sprechen. → S. 12

Und gleich noch einen Bug möchte ich Ihnen melden: Während sich mittlerweile zahlreiche Unternehmen um mehr Frauen in der IT bemühen, übersehen viele, dass weibliche Fachkräfte die Branche oft nach nur wenigen Jahren wieder verlassen. Im Interview sprechen Nicola Marsden und Edna Kropp darüber, woran das liegt und welche Maßnahmen wirklich helfen würden. → S. 8

Gerade wenn die Temperaturen steigen, rückt auch die Klimakrise wieder in den Fokus öffentlicher Debatten. Wir als GI sind ganz klar der Meinung, dass Informatik hier Teil der Lösung sein muss, und nicht Teil des Problems. Zusammen mit weiteren Autorinnen aus unterschiedlichen GI-Gremien hat sich meine Vorstandskollegin Ina Schieferdecker mit der Frage auseinandergesetzt, wie das gelingen kann. → S. 20

Dass Politik auch jungen Stimmen zuhört – wenn man sie nur richtig anspricht –, hat das Common Grounds Forum bei seiner Delegationsreise nach Berlin bewiesen. Zwei Vertreter*innen haben für diese Ausgabe ihre wichtigsten Learnings gesammelt. → S. 26

Und ein ganz besonderes Highlight finden Sie ganz hinten im Heft: Junior-Fellow Benjamin Paaßen lädt ein zum Filme-Raten. Und das hat mehr mit Informatik zu tun, als man vermuten würde.

Ich wünsche Ihnen eine anregende Lektüre!
Ihr Martin Wolf

12

Cowboys und Computer

Warum der Hackerparagraph die White Hats in Schwierigkeiten bringt

8

Gekommen, um zu bleiben?

Wie Frauen die IT-Branche erleben und warum sie sie verlassen

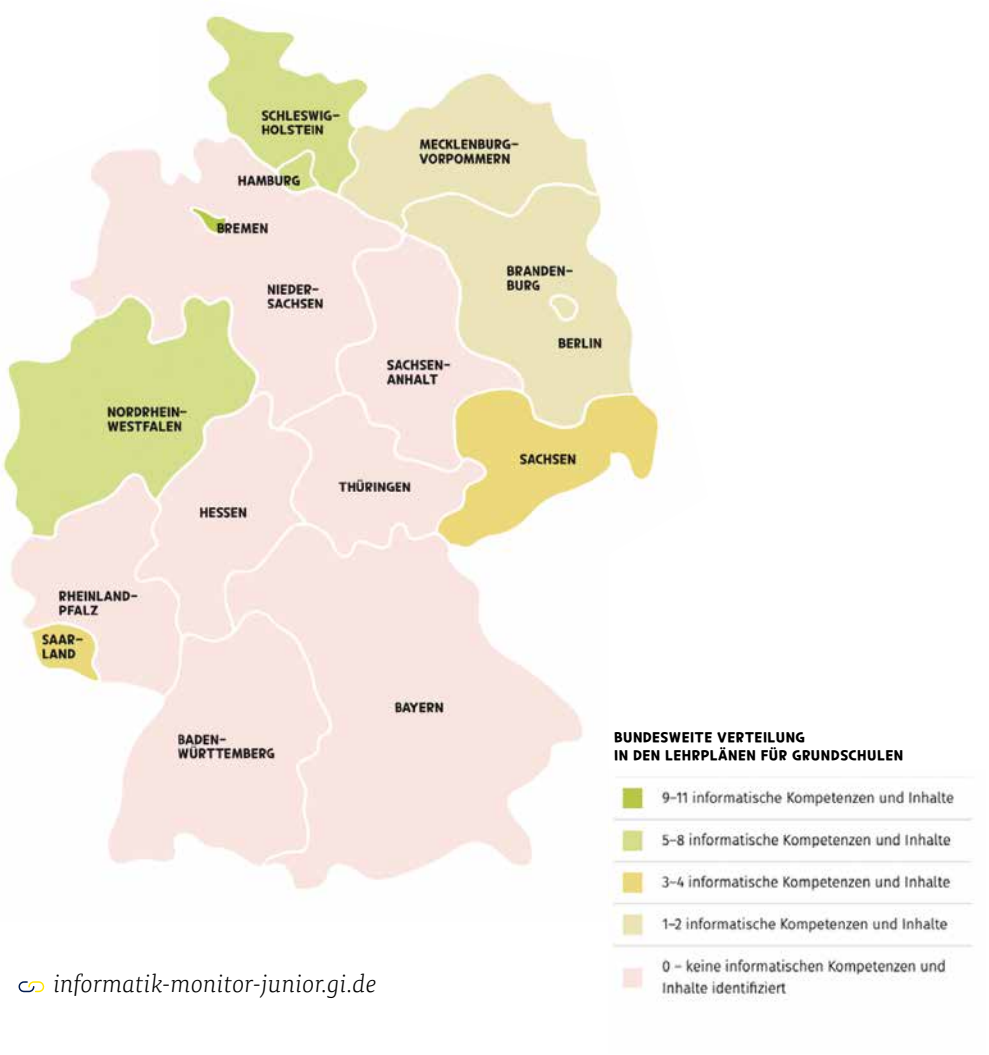
20

Nachhaltigkeit ist kein Add-on

Wie Informatik in Zeiten von KI Teil der Lösung bleibt

LÜCKENHAFTE LEHRPLÄNE

Ob Tablet oder Saugroboter: Kinder kommen heutzutage deutlich früher in Kontakt mit informatischen Systemen. Umso wichtiger ist es, dass sie schon im Grundschulalter beginnen, ein Verständnis für diese Systeme zu entwickeln. Der im Mai veröffentlichte Informatik-Monitor Junior, gefördert von der Klaus Tschira Stiftung, zeigt jedoch große Unterschiede, was informatische Bildung an deutschen Grundschulen angeht: In sieben Bundesländern steht Informatik noch gar nicht auf dem Lehrplan. Und auch dort, wo erste informatische Inhalte empfohlen werden, fehlt es an der nötigen inhaltlichen Breite, um Kinder auf ein selbstbestimmtes Leben in der zunehmend digitalen Welt vorzubereiten. Deswegen werden in der Studie klare Handlungsempfehlungen formuliert, um Informatik deutschlandweit an Grundschulen zu verankern.



informatik-monitor-junior.gi.de

GI-MITGLIEDSCHAFTEN FÜR DREAMTEAMS

Bis zum Jahresende können korporative Mitglieder Gruppenkontingente für ordentliche Mitgliedschaften zu Sonderkonditionen erhalten und somit gleich mehreren Mitarbeitenden Zugang zu den Angeboten der GI ermöglichen. Neben zahlreichen Gelegenheiten zum Netzwerken bedeutet das auch Teilnahme an exklusiven Fachveranstaltungen sowie Rabatte auf Publikationen und Weiterbildungen. Gleichzeitig stärken Unternehmen und Hochschulen durch die GI ihre Sichtbarkeit in der Informatik-Community. Zur Auswahl stehen entweder fünf ordentliche Mitgliedschaften für 485 Euro im Jahr oder bis zu 15 ordentliche Mitgliedschaften zum Preis von 1.450 Euro.

gi.de/mitgliedschaft

DIGITALE BIBLIOTHEK: FRÜH ÜBT SICH

Die Digitale Bibliothek der GI enthält zahlreiche Ressourcen – auch für Lehrkräfte. Drei Beispiele aus der Zeitschrift *Informatische Bildung in Schulen (ibis):*

Expedition in die Tiefsee
Wie Data Science in den informatischen Unterricht einfließen kann, zeigt ein EduBreakout, der zentrale Konzepte wie Clustering und Entscheidungsbäume aufgreift.
inf.gi.de/dl-tiefsee

Das Wollperzeptron
Anhand künstlicher Neuronen (Perzeptron) vermittelt diese Unplugged-Aktivität die grundlegende Funktionsweise von maschinellem Lernen.
inf.gi.de/dl-wollperzeptron

Das Informatikcurriculum der Hector Kinderakademien
Wo an Grundschulen noch keine informatische Bildung angeboten wird, können außerschulische Angebote helfen. Ein Einblick.
inf.gi.de/dl-hector

Alle Beiträge finden Sie in der Digitalen Bibliothek der GI, die allen Mitgliedern kostenlos zur Verfügung steht. Wir laden ein zum Stöbern:
dl.gi.de

KOMMEN SIE, KOMMEN SIE!

Wie jedes Jahr möchten wir Sie auch dieses Jahr zur ordentlichen Mitgliederversammlung der GI einladen: Diese findet am Dienstag, 22. September, ab 16 Uhr im Rahmen unserer Jahrestagung, der INFORMATIK 2026, in Dresden statt. Bei der Versammlung berichten wir über die vergangenen zwölf Monate, stellen Ihnen die Liste für die Präsidiumswahl vor und beantworten gerne Ihre Fragen. Details der Sitzung finden Sie sukzessive unter *meine.gi.de*.
Wir freuen uns auf Sie!

SAVE THE DATES

Für GI-Mitglieder ist der Kalender immer voller Highlights: Drei davon haben wir hier für Sie zusammengestellt.

25. Juli

Sitzung der Jungen GI

Aktive Mitglieder, Hochschulgruppen und Interessierte aus ganz Deutschland kommen zusammen, um sich über aktuelle Themen auszutauschen.

KÖLN

11.–14. August

KI 2026

Die 49. Deutsche Jahrestagung für Künstliche Intelligenz bringt traditionell akademische und industrielle Forschende aus allen Bereichen der KI ins Gespräch.

BREMEN

30. August – 2. September

Mensch und Computer

Unter dem Motto „Transforming Interactions" dreht sich die Fachtagung diesmal um Beziehungen zwischen Gesellschaft und interaktiver Technologie.

DUISBURG

Alle weiteren Infos und Events der GI finden Sie in unserem Veranstaltungskalender: *gi.de/aktuelles/veranstaltungen*

Gekommen, *um zu bleiben?*

INTERVIEW Paul Reinelt

Viele Debatten drehen sich darum, wie sich mehr Frauen für die IT begeistern lassen. Worüber bisher nur wenig gesprochen wird: Sind sie einmal dort angekommen, bleiben sie oftmals nicht lang. Woran das liegt, untersucht Prof. Dr. Nicola Marsden aktuell in einer bundesweiten Befragung. Mit Edna Kropp, Head of Product Management bei einem Anbieter für KI-Kommunikation, und ehemalige Sprecherin der Fachgruppe Frauen und Informatik, hat sie über unsichtbare Hürden, Selbstzweifel und fehlende Vorbilder diskutiert. Und darüber, warum Veränderung nicht allein Aufgabe der Frauen sein kann.

Frau Marsden, Sie forschen schon länger zu der Frage, warum Frauen die IT verlassen. Wie kam es dazu, dass Sie sich überhaupt damit beschäftigen?

NICOLA MARSDEN Ich bin über die Praxis zu dem Thema gekommen. In Unternehmen habe ich immer wieder gesehen, dass Frauen nicht an der Technik scheitern, sondern an den Rahmenbedingungen. Zwar gibt es viele Maßnahmen, um Frauen in die IT zu bringen, aber in den Firmen passiert oft etwas, das dazu führt, dass sie wieder gehen. Unsere Forschung hat gezeigt: Frauen verlassen meist keine Unternehmen, sondern konkrete Teams – dort, wo sie das Gefühl haben, dass ihr Potenzial nicht gesehen wird.

Frau Kropp, was war für Sie der Anstoß, sich mit diesem Thema auseinanderzusetzen?

EDNA KROPP Ich habe Informatik studiert und jetzt, ungefähr 25 Jahre später, hat sich der Frauenanteil noch immer nicht dramatisch erhöht. Ob im Studium, als Berufseinsteigerin oder jetzt in einer Managementposition war mir immer klar: Es gibt wenige Frauen. Ich wollte verstehen, warum das so ist und ob ich etwas verändern

kann. Es kann doch nicht sein, dass wir das Know-how und die Expertise der Hälfte der Bevölkerung nicht nutzen. Als Individuum in einer Firma kann ich nur bedingt etwas erreichen. Deshalb wollte ich, dass wir Frauen uns gemeinsam organisieren, und wurde Sprecherin der Fachgruppe Frauen und Informatik der GI.

Wie geht man die Veränderung eines Systems an?

NM Um Veränderung anzuschieben, braucht es Druck oder Sog. Das Problem ist: In der IT haben diesen Druck hauptsächlich die Frauen. Deshalb sind Verbündete, sogenannte Male Allies, so wichtig. Männer, die darauf hinweisen, wenn jemand unterbrochen wird oder wenn jemandem Kompetenz abgesprochen wird. Denn von allem, was wir aus unserer Reallaborforschung vorschlagen, anregen und austesten, profitieren am Ende auch alle im Team. Wenn Ungerechtigkeiten beseitigt werden, profitieren auch beispielsweise schüchterne Männer oder andere Menschen, die nicht der Norm entsprechen.

Wie kann dieses Handeln als Verbündeter konkret aussehen?

NM Ein wichtiger Punkt ist, sensibel dafür zu sein, dass Frauen in der IT häufig in ihrer Kompetenz hinterfragt werden. Allyship kann schon in kleinen Situationen beginnen: etwa, wenn Frauen in Meetings unterbrochen werden oder ihre Beiträge später anderen zugeschrieben werden. Dann kann man bewusst darauf hinweisen und Frauen den Raum geben, ihre Gedanken auszusprechen. Für Führungskräfte ist das noch mal wichtiger, weil sie Strukturen, Beförderungen und Arbeitsbedingungen mitgestalten. Im Management sollte man darauf achten, Frauen nicht aufgrund von Vorannahmen Entscheidungen abzunehmen, sondern sie selbst zu fragen, wie sie arbeiten möchten. Sobald man für diese Mechanismen sensibilisiert ist, gibt es viele Möglichkeiten, im Alltag unterstützend einzugreifen.

EK Mir fallen dazu zwei Dinge ein. Zum einen wird oft unterschätzt, dass auch Technik selbst nicht neutral ist. Ich habe zum Beispiel erst vor einigen Jahren erfahren, dass viele Konferenztools eher auf Männerstimmen optimiert sind. Frauenstimmen werden teilweise schlechter übertragen oder anders verarbeitet. Das zeigt: Wenn Frauen nicht mitentwickeln, entstehen blinde Flecken – nicht nur bei gesellschaftlichen Fragen, sondern auch ganz konkret technisch. Zum anderen reicht Gleichberechtigung auf dem Papier allein nicht aus. Ich war einmal bei einem Vortrag, nach dem mir jemand stolz erzählte, sein Team sei völlig ausgeglichen, weil dort gleich viele Frauen wie Männer arbeiten. Aber gleiche Zahlen bedeuten noch keine gleichen Bedingungen. Viele Frauen kommen mit einem ganz anderen Druck in den Arbeitsalltag – etwa durch Care-Arbeit oder Teilzeit. Dieser „unsichtbare Rucksack" wird oft übersehen. Deshalb bedeutet Gleichberechtigung nicht nur, Frauen mit am Tisch sitzen zu haben, sondern auch zu verstehen, unter welchen Bedingungen sie dort sitzen.

> ***„Viele Frauen versuchen zunächst, sich anzupassen oder ihre Firma zu verteidigen. Aber sobald man über typische Muster spricht, kommt oft schnell die Antwort: ‚Ja, das ist bei uns genauso.'"***
>
> NICOLA MARSDEN

Frau Marsden, Sie haben im Rahmen Ihrer Forschung viele Gespräche mit Frauen aus der Branche geführt. Was hat Sie in diesen Gesprächen am meisten überrascht?

NM Das war ganz klar die enorme Ähnlichkeit der Erfahrungen – unabhängig von Unternehmen oder Firmengröße. Immer wieder ging es um fehlende Anerkennung, Ausschluss aus informellen Netzwerken oder darum, dass Frauen weniger zugetraut wird und sie seltener befördert werden. Viele Frauen versuchen zunächst, sich anzupassen oder ihre Firma zu verteidigen. Aber sobald man über typische Muster spricht, kommt oft schnell die Antwort: „Ja, das ist bei uns genauso."

In Ihrer Forschung geht es auch um das Thema Altersismus. Ist hier eher die Frau gemeint, die als „zu alt für den Job" gilt – oder die Frau, die als „zu jung" wahrgenommen wird, um auf Augenhöhe zu sein?

NM Beides – und tatsächlich ist der Raum dazwischen oft erstaunlich klein. Junge Frauen werden schnell gefragt, ob sie Kinder planen. Später geht es um Kinderbetreuung und irgendwann um Care-Arbeit für Angehörige. Frauen stehen dadurch dauerhaft unter bestimmten Zuschreibungen. Eigentlich kann man als Frau kein gutes Alter haben. Wenn Organisationen

signalisieren, sie hätten ihre Pflicht getan, sobald eine Frau in die höheren Etagen gelangt, entsteht unter Frauen der Eindruck: Es kann nur eine von uns schaffen. Das ist völlig absurd. Dadurch entsteht Konkurrenz statt Solidarität. Das ist dann aber ein Resultat des Umfelds, keine Eigenschaft der Frauen.

Wenn Frauen sich in solchen Strukturen durchsetzen wollen, wird ihr Verhalten oft anders bewertet als bei Männern. Was hat es damit auf sich?

NM Genau, das ist der sogenannte Backlash-Effekt. Während Männer für ihre Durchsetzungsfähigkeit gelobt werden, gelten Frauen schnell als zu dominant oder sogar aggressiv.

EK Männer lernen außerdem oft schon früher, sich in Gruppen durchzusetzen – etwa über Mannschaftssport oder andere soziale Räume. Viele Frauen machen diese Erfahrungen deutlich seltener. Deshalb braucht es manchmal gezielte Maßnahmen oder geschützte Räume, in denen Frauen nicht ständig das Gefühl haben, sich besonders beweisen zu müssen.

Welche Rolle spielen gemeinsame Hobbys – wie der eben genannte Mannschaftssport?

EK Gemeinsame Interessen entscheiden ja oft darüber, wie gut man in Gruppen ankommt und Netzwerke aufbauen kann. Viele Gespräche drehen sich um Gaming, Science-Fiction oder ähnliche Themen. Wer diese Interessen nicht teilt, bleibt schnell außen vor. Ich selbst interessiere mich zum Beispiel weder besonders für Gaming noch für Science-Fiction, was aber bei vielen männlichen Teammitgliedern oft Verbindung schafft. Dabei sollte es selbstverständlich sein, dass Menschen in der IT ganz unterschiedliche Hobbys haben können.

> ***„Es kann doch nicht sein, dass wir das Know-how und die Expertise der Hälfte der gesamten Bevölkerung nicht nutzen."***
>
> **EDNA KROPP**

NM Genau diese Kultur prägt nicht nur die Zeit nach der Arbeit, sondern auch viele Gespräche während der Arbeit. Wenn Frauen in Teams die Ausnahme sind, werden sie oft nicht mehr als Individuum wahrgenommen, sondern als „die Frau", die stellvertretend für alle Frauen steht. Verhalten oder Fehler werden dadurch viel schneller verallgemeinert. Das kann enormen Druck und Selbstzweifel auslösen.

Druck und Selbstzweifel können letztendlich im Imposter-Syndrom enden. Frau Kropp, kennen Sie das Gefühl?

EK Wenn Dinge nicht funktionieren oder ich Feedback bekomme, hinterfrage ich zuerst mich selbst. Habe ich etwas falsch gemacht? Das kann ich nicht einfach abschalten. Gleichzeitig habe ich gelernt, mich darauf zu stützen, was ich bereits erreicht habe. Trotzdem kommt diese endgültige Bestätigung, wirklich dazuzugehören, oft nicht.

Welche Auswirkungen kann das auf das Berufsleben haben?

NM Gerade wenn Frauen in Teams oder Führungspositionen die Ausnahme sind, ist es häufig so, dass sie sich permanent legitimieren müssen. Viele hinterfragen sich dann selbst und fragen sich, ob sie überhaupt kompetent genug sind oder etwas Wichtiges beizutragen haben.

EK Gleichzeitig treten viele Männer deutlich selbstverständlicher auf, wenn es um Gehalt, Beförderungen oder Führungspositionen geht. Frauen hinterfragen dagegen oft zuerst ihre eigene Leistung.

In Ihrer Forschung zeigt sich, dass in anderen Ländern mehr für Frauen im Berufsleben und somit auch in der IT getan wird. Was läuft dort anders?

NM In Skandinavien, also etwa Finnland und Schweden, sieht man klar andere strukturelle Rahmenbedingungen. Dort gibt es nationale Programme. Vereinbarkeit wird nicht in der Art diskutiert wie hier. Traditionelle Erwartungen an die Mutterrolle sind deutlich schwächer, Elternschaft wird partnerschaftlich gedacht. Karrierewege sind transparenter. Das entlastet die Individuen. Daran sieht man deutlich: Es sind nicht die Frauen das Problem. Wenn die Rahmenbedingungen stimmen, läuft es besser. Die skandinavischen Länder sind bei Gleichstellung stark, aber auch beim Thema Partizipation. Bei technischen Produkten gibt es Vorgaben, dass Partizipation stattfinden muss. Es hängt also nicht alles nur an Entwicklungsteams. Produkte werden stärker gemeinsam mit zukünftigen Nutzerinnen und Nutzern entwickelt.

Nicola Marsden und Edna Kropp sind sich einig: Bessere Bedingungen für Frauen in der IT sind keine reine Frauenthematik. Allyship kann das Arbeitsklima für alle verbessern.

Frau Marsden, wenn Sie basierend auf Erkenntnissen wie diesen nur eine Sache sofort ändern könnten – welche wäre das?

NM Um Gerechtigkeit herzustellen, brauchen wir Transparenz. Daran hängt vieles: gleiche Bedingungen, mehr Fairness in Teams, bessere Sichtbarkeit dessen, wer was macht. In unseren Reallaborinterventionen schauen wir zum Beispiel: Kommen alle gleich viel zu Wort? Oder wird der Gruppendynamik überlassen, wer sprechen darf? Fairness entsteht durch Transparenz, zum Beispiel beim Thema Office Housework versus Glamour Work: Wer macht wie viel wovon? Wollen wir das so haben? Und wenn nicht: Wie können wir es ändern?

Frau Kropp, es scheint, als seien diese Strukturen nicht sofort auf den ersten Blick sichtbar. Wussten Sie, worauf Sie sich einlassen, als Sie in die IT gegangen sind? Oder kam die Erkenntnis erst später?

EK Viele der Strukturen werden einem erst nach und nach bewusst. Im Studium fiel mir auf, wie stark vorausgesetzt wurde, dass man bereits programmiert haben müsse. Viele Mädchen bekommen schon früh das Gefühl, dort nicht dazuzugehören. Das zieht sich später durch alle weiteren Karriereschritte. Ich entscheide mich trotzdem jeden Tag bewusst dafür, hierzubleiben.

Und was würden Sie Frauen raten, die in die Branche gehen wollen?

EK Mein Rat ist, dem eigenen Interesse nachzugehen! Natürlich kann man sich Rat holen und fragen, worin die eigenen Stärken liegen. Aber am Ende ist entscheidend, worauf man selbst wirklich Lust hat. Darauf lässt sich alles andere aufbauen. I

- **Prof. Dr. Nicola Marsden** ist Forschungsprofessorin für Sozioinformatik an der Hochschule Heilbronn. Sie ist Expertin für Gender und IT und als Verbundleitung bei Tech2stay tätig.

- **Edna Kropp** ist in in einem Softwareunternehmen als Head of Product Management tätig. Sie war jahrelang Sprecherin der Fachgruppe Frauen und Informatik und ist Teil des Verwaltungskreises von Tech2stay.

- **Tech2stay** ist ein Forschungs- und Praxisprojekt, das die Rahmenbedingungen für Frauen in der IT untersucht und verbessert. Mit einer groß angelegten Umfrage untersucht das Team, welche Faktoren zum Verbleib oder Weggang von Fachkräften in der IT beitragen. Die Teilnahme ist noch bis 30. Juli 2026 möglich. (Dauer: ca 20 Min)
  inf.gi.de/tech2stay

Cowboys *und Computer*

REDAKTION Marieke Petersen

Eigentlich sollte Forschung nichts mit Wildem Westen zu tun haben. Doch wer sich auf die Suche nach Sicherheitslücken in IT-Systemen macht, läuft Gefahr, sich strafbar zu machen – ganz egal, ob das Hacken mit White Hat oder Black Hat erfolgt. Ein Ritt durch die Geschichte und aktuelle Gesetzeslage rund um den Hackerparagraph.

Computerstrafrecht: Wie schützen wir die, die uns schützen?

Es ist nicht leicht, ein guter Mensch zu sein. Besonders IT-Sicherheitsforschende bewegen sich bei ihrer Arbeit oft in einer legalen Grauzone: Das aktuelle Computerstrafrecht verhindert, dass sie Schwachstellen rechtssicher melden können. Denn wenn sie selbst testen, ob

23.11.2001

Übereinkommen des Europarates zu Cyberkriminalität
Die sogenannte Cybercrime Convention ist das erste internationale Abkommen gegen Computerkriminalität. Es deckt eine Spanne an Straftaten ab: darunter Urheberrechtsverletzungen, Betrug, Kinderpornografie und Hasskriminalität. Dabei wird auch der illegale Zugang adressiert.

24.02.2005

Rahmenbeschluss des Rates der Europäischen Union zu Angriffen auf Informationssysteme
Die Mitgliedstaaten werden verpflichtet, schwere Formen der Cyberkriminalität unter Strafe zu stellen. So sollen die nationalen Strafvorschriften vereinheitlicht werden.

sie über eine solche Schwachstelle Zugriff auf ein System bekommen können, machen sie sich damit strafbar. Dabei wird nicht einmal jede Schwachstelle aktiv „gehackt". Einige fallen durch das bloße Benutzen von Programmen oder Websites auf. Unternehmen setzen längst auf Pen-Tests oder Bug-Bounty-Programme, müssen dafür aber viel bürokratischen Aufwand vornehmen. Solange Sicherheitsforschende nicht wissen, welche Konsequenzen sie erwarten, zögern viele „White Hat Hacker", Schwachstellen zu melden.

Schwarz und Weiß

Bei „Hackern" gibt es drei Gruppen: White, Black und Grey Hats[1]. Die Anlehnung folgt der Logik alter Western: Die Guten haben weiße Hüte, die Bösen tragen Schwarz. Der Begriff „White Hats" bezeichnet „ethische Hacker". Sie suchen nach Sicherheitslücken, um diese betroffenen Anbietern oder Entwicklern zu melden. „Black Hats" hingegen nutzen Schwachstellen zu kriminellen Zwecken aus, etwa Erpressung, Diebstahl oder Löschung von Daten. „Grey Hats" bewegen sich im Feld dazwischen: Sie verfolgen keine kriminelle Absicht, agieren aber oft ohne Wissen der Netzwerkeigentümer oder setzen unethische Methoden ein.

White Hat Hacking, aber wie?

In Deutschland ist jede Art des Hacking offiziell verboten: Die Paragraphen 202 a-c im Strafgesetzbuch (StGB) stellen das Ausspähen und Abfangen von Daten sowie dessen Vorbereitung und den Besitz sogenannter Hackertools unter Strafe. Ethisches Hacken ist damit außen vor. Fällt einer White-Hat-Hackerin eine Schwachstelle auf, so steht sie vor der Wahl: den Hersteller informieren und eine Klage riskieren, oder nichts sagen und das eigene Risiko minimieren. Dadurch bleibt ungenutztes Potenzial auf der Strecke, denn Unternehmen, Privatpersonen und der Staat profitieren davon, dass Lücken geschlossen werden.[2,3] Während andere Länder ethisches Hacken legalisieren, stagniert die Gesetzgebung in Deutschland. ⌶

Simeon Hoffmann
Doktorand am CISPA Helmholtz-Zentrum für Informationssicherheit

Marieke Petersen
Referentin für Politik und Wissenschaft bei der GI

03.07.2007

Kritik der GI an Einführung des § 202 c StGB

Bereits vor dem Inkrafttreten des Hackerparagrafen kritisiert der Arbeitskreis Datenschutz und IT-Sicherheit der GI die Einführung. Prof. Dr. Hartmut Pohl nennt es eine „unzulässige Erweiterung der Cybercrime Convention".

07.08.2007

Inkrafttreten der Strafrechtsänderung zur Bekämpfung der Computerkriminalität

Trotz Kritik tritt die Änderung von § 202 a in Kraft, § 202 b und § 202 c werden hinzugefügt. Damit stellt das deutsche Recht unter anderem die Herstellung und Verbreitung sogenannter Hackertools unter bestimmten Umständen unter Strafe. Die Höchststrafe beträgt ein Jahr.

Drei Perspektiven aus der Praxis

Ich habe gehackt … und es ist gut ausgegangen

Ich habe positive Erfahrungen gemacht: So haben etwa die Firmen hinter den Plattformen KigaRoo und Timeless nach meinen Hinweisen professionell und innerhalb weniger Stunden reagiert und die Lücken geschlossen. Anschließend wurde der Vorfall zum Anlass genommen, ihre Systeme noch mal extern prüfen zu lassen. Schnelle und konstruktive Reaktionen auf Coordinated Vulnerability Disclosure sind wertvoll, denn sie kommen nicht nur den Firmen selbst zugute[4], sondern auch den Nutzenden und der Gesellschaft insgesamt, die dadurch in der digitalen Welt besser geschützt sind. Leider führt die gesetzliche Lage teils dazu, dass Unternehmen eher rechtliche Schritte einleiten, statt kooperativ zu handeln.[5] Zudem hindern zahlreiche Negativbeispiele und die rechtliche Unsicherheit engagierte Sicherheitsforschende daran, sich Systeme genauer anzuschauen.[6] Bessere Gesetze könnten hier bei Unternehmen zu einem Umdenken beitragen und gleichzeitig mehr ethische Hacker*innen zum Hinschauen motivieren – eine klare Win-win-Situation.

Florian Hantke
Doktorand am CISPA Helmholtz-Zentrum für Informationssicherheit

Ich habe gehackt … und wurde verklagt

Als Sicherheitsforscher ist es mein Ziel, Schwachstellen zu finden, bevor Kriminelle sie ausnutzen. Genau dafür geriet ich selbst ins Visier von Ermittlern: Gemeinsam mit meinem Team der Mint Secure GmbH entdeckte ich kritische Sicherheitslücken in Observationssystemen des Herstellers Infodraw. Wir meldeten die Probleme verantwortungsvoll, warteten die übliche 90-Tage-Frist ab und informierten anschließend CERTs und Behörden. In Luxemburg konnte eine Polizeieinheit ihr betroffenes System sogar rechtzeitig offline nehmen. Trotzdem wurde gegen mich ein Ermittlungsverfahren eingeleitet.

Der Fall zeigt ein Grundproblem: In Deutschland und Europa riskieren ethische Hacker*innen noch immer Strafverfolgung, obwohl sie im öffentlichen Interesse handeln. Während Hersteller Sicherheitslücken oft monatelang ignorieren, werden diejenigen kriminalisiert, die Missstände aufdecken. Das schreckt Forschende ab – und gefährdet letztlich die Sicherheit von Behörden, Unternehmen und Bürger*innen.Ein modernes Computerstrafrecht muss Sicherheitsforschung endlich schützen statt bestrafen.

Weitere Infos zur Rechtslage in der EU:
inf.gi.de/cowboysundcomputer

Tim Philipp Schäfers
Gründer von Mint Secure und bloggender White-Hat-Hacker

18.05.2009

Stellungnahme des Bundesverfassungsgerichts nach drei Verfassungsbeschwerden
Aufgrund der rechtlichen Unklarheiten für Sicherheitsforschende reichen drei Personen unabhängig voneinander eine Verfassungsbeschwerde ein. Diese werden im Mai 2009 vom Bundesverfassungsgericht als unzulässig abgelehnt, da die Beschwerdeführenden nicht „selbst, gegenwärtig und unmittelbar" in ihren Grundrechten betroffen wären. Das Gericht sieht kein Risiko für eine strafrechtliche Verfolgung für ihre Tätigkeit bei einer verfassungskonformen Auslegung.

20.11.2015

Änderung des Strafmaßes
2013 wird die EU-Richtlinie über Angriffe auf Informationssysteme geändert und fordert nun eine Mindesthöchststrafe von zwei Jahren. Diese Erhöhung des Strafrahmens wird in 2015 umgesetzt.

Wir melden für Hacker … weil wir müssen

Sicherheitsforschende, die Schwachstellen verantwortungsvoll melden, riskieren in Deutschland Strafverfolgung nach §§ 202 a–c StGB. Nicht wegen verursachter Schäden, sondern wegen des bloßen Zugriffs auf unzureichend gesicherte Systeme. Strafanzeigen sind selten, aber kostspielig genug, um als Abschreckung zu wirken.

Das Ergebnis ist ein kollektives Sicherheitsdefizit: Lücken, die Forschende gern gemeldet hätten, bleiben offen – bis sie ausgenutzt werden. Der CCC fungiert deshalb bei zahlreichen Meldungen als rechtlicher Puffer, wenn Forschende das Risiko nicht tragen wollen oder können.

Kriminelle brauchen keinen solchen Puffer. Sie melden nicht, sie nutzen aus. Das Strafrecht belastet systematisch diejenigen, deren Arbeit Infrastrukturen, Unternehmen und Bürger*innen schützt – und lässt die eigentliche Bedrohung nicht nur unberührt, sondern verschlimmert sie.

Solange Responsible Disclosure rechtlich riskant bleibt, zahlt die Allgemeinheit die Zeche: in Form geleakter Daten und vermeidbarer Angriffe. Die ehrenamtliche Schutzfunktion des CCC wird oft gelobt. Sie sollte aber überflüssig sein.

Linus Neumann
IT-Sicherheitsexperte und Sprecher des Chaos Computer Clubs (CCC)

Standpunkt: Der Hackerparagraph ist irreführend

Cybersicherheit ist der Bundesregierung wichtig: Die zahllosen Akteure visualisiert die Stiftung Neue Verantwortung mit einer interaktiven Grafik.[6] Doch das Cyber-Strafrecht wirkt wie eine Verzweiflungstat. Kann eine Reform Hoffnung machen?

Als Lilith Wittmann eine Wahlkampf-App der CDU, CSU und ÖVP „hackte“[7], kassierte sie von der CDU eine Strafanzeige. Sie habe sich unbefugt Zugang zu Daten verschafft, die dagegen besonders gesichert wären – strafbar nach § 202 a StGB. Doch es fehlte an einer „besonderen Sicherung“. Anders im Fall Modern Solution[8]: Ein IT-Berater fand im kompilierten Programm trivial auslesbare Datenbank-Servernamen und -Zugangsdaten und griff so mit PHPMyAdmin auf Datensätze mehrerer Kund*innen zu. Das sei ein Umgehen „einer besonderen Sicherung“. Konsequenz: 60 Tagessätze.

19.02.2020

GI klärt zu rechtlichen Rahmenbedingungen der IT-Sicherheitsforschung auf
Bei der Veranstaltungsreihe „F5 – Refresh your Knowledge“ dreht sich das Politikfrühstück in der Berliner Außenstelle des FZI Forschungszentrum Informatik um rechtliche Rahmenbedingungen der IT-Sicherheitsforschung. Auch die GI bringt sich mit ihrer Expertise ein.

25.02.2022

Blogbeitrag der GI zu Risiken beim Melden von Datenlecks
Tim Philipp Schäfers und Matthias Marx, Junior-Fellows der GI, klären in ihrem Blogbeitrag über Datenlecks und einen verantwortungsvollen Meldeprozess auf.

Besondere Sicherung ≠ besonders sicher

Für die Rechtsprechung kommt es bei der Sicherung auf den Willen der Sichernden an, nicht auf deren Wirkung. Sie will mangelhaften Schutz nicht zum Freibrief erklären. Anders die Informatik: Selbst Erstsemester denken sofort an Verschlüsselung, Mandantentrennung, individuelle Passwörter – alles bei der inzwischen insolventen[9] Modern Solution nicht zu finden. PHPMyAdmin als Hackertool zu bezeichnen, führt zu Gelächter im gleichen Hörsaal.

Eine Reform muss diese „besondere Sicherung" greifbarer machen. Doch die aufwendige Gesetzgebung mit vielen Rahmenbedingungen von EU-Recht bis Lobbyismus erfordert langlebige, generische Formulierungen, siehe die Definition von Daten in § 202 a Abs 2 StGB, die auch CDs und Qubits mit erfasst.

Üblich sind Verweise etwa auf eine DIN oder – abstrakter – den „Stand der Technik". Denn: Nicht die marktübliche Qualität von Software ist das Maß, sondern das technisch sinnvoll Mögliche. Mehr ist der „Stand der Wissenschaft und Technik"[10].Beides ist für Jurist*innen einzuordnen und macht Personen, die Fehler entdecken, straffrei. Bei Ersterem blieben Entdecker*innen komplexerer Lücken jedoch strafbar.

Ehrliche Finder?

Wer eine Sicherheitslücke beim CERT des BSI abgibt oder direkt dem Hersteller meldet, will Schaden abwenden. Da könnte sogar „Nothilfe" als Abwehr einer unmittelbar drohenden Gefahr ein Rechtfertigungsgrund sein[11]. Doch es wäre deutlich gerechtfertigter, den Straftatverdacht gleich auszuschließen. Ein entsprechender Referentenentwurf der vorigen Bundesregierung nach dem Vorbild anderer europäischer Länder blieb beim Regierungswechsel aber stecken. Statt des schwer prüfbaren Willens jener, die die Lücken entdecken, nutzen einige Nationen eine Mindestschadenhöhe oder nehmen registrierte Sicherheitsforschende von Strafe aus, was jedoch zufällige Entdecker*innen nicht schützt.

Fehlkonzeption

Die Bezeichnung „Hackerparagraph" unter anderem für § 202 a StGB zeigt zwei Denkfehler: Erstens sind die sogenannten Hacker vor allem kreative Problemlöser*innen – quasi digitale MacGyver – und keine Kriminellen. Zweitens sind die Ursachen von Sicherheitslücken Programmierfehler, Sicherheitsforschende entdecken sie nur. Finderlohn statt Strafe wäre besser. Für ordentliche Softwarequalität sorgt ein robuster Regressanspruch gegen den Hersteller.

Weiter schafft der unbeholfene Versuch einer Strafandrohung für „Hackertools" (u.a. § 202 c StGB) ein Paradox, das im analogen Leben schwer nachvollziehbar ist: Während der Besitz eines Vulnerability-Scanners bei entsprechendem Tatvorsatz strafbedroht ist, wäre der einer zum Morden beschafften Axt es nicht.

Prof. Dr. Tobias Eggendorfer
Professor für Cybersicherheit

Dr. Florian Deusch
Fachanwalt für IT-Recht,
RAe Dr. Gretter

09.11.2022

BSI stellt CVD-Leitlinien vor

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlicht seine Richtlinie für Sicherheitsforschende, wie sie mit gemeldeten Schwachstellen umgehen sollten. Die Leitlinie beschreibt den Prozess der Coordinated Vulnerability Disclosure.

07.09.2023

GI hostet ATHENE-Veranstaltungsreihe „Rechtsrahmen der Cybersicherheitsforschung"

In der Veranstaltungsreihe „Rechtsrahmen der Cybersicherheitsforschung" werden Rechtsfragen, die sich IT-Sicherheitsforschende stellen, erörtert. Die Reihe wird von ATHENE-Datenschutzrechts-Expertin Dr. Dr. Annika Selzer und Prof. Dr. Indra Spiecker gen. Döhmann organisiert. Die vierte Ausgabe über Alternativen zum „Hackback" wird auch von der GI gehostet.

In Polen sind Personen, die ausschließlich zum Zweck der Sicherung von Systemen handeln, explizit von der Strafbarkeit ausgenommen. Der polnische Ansatz ist im Vergleich am liberalsten.

In Belgien ist ethisches Hacking unter bestimmten kumulativen Bedingungen gestattet. Dazu zählen eine zeitnahe Meldung an das belgische Cybersicherheitszentrum, das Fehlen einer Schadensabsicht sowie die Einhaltung der Prinzipien von Notwendigkeit und Verhältnismäßigkeit. Zusätzlich unterhält Belgien eine „Hall of Fame", um IT-Sicherheitsforschende für ihren Beitrag zur nationalen Cybersicherheit zu würdigen.

Ethisches Hacking ist in Portugal unter kumulativen Voraussetzungen erlaubt: Die Handlung muss in guter Absicht und ohne finanzielle Motivation erfolgen, darf keine Schäden verursachen und gefundene Schwachstellen sollen zeitnah gemeldet werden.

Rechtlicher Rahmen für ethisches Hacken

- explizit erlaubt
- strafbar; Verfolgung entfällt bei Vorliegen bestimmter Umstände
- verboten
- keine Angabe

04.11.2024

Ampelregierung stellt Referentenentwurf zur Modernisierung des Computerstrafrechts vor
Die Ampelkoalition stellt den Gesetzesentwurf des Bundesjustizministeriums vor, der eine Straffreiheit des White-Hat-Hacking vorsieht. Damit setzt sie ein Vorhaben aus dem Koalitionsvertrag um.

Das sagt die Industrie: Notwendige Anpassung des Computerstrafrechts

Fahrzeughersteller sind gemäß europäischen und deutschen Vorschriften verpflichtet, Cybersicherheitslücken ihrer Produkte durch Penetrationstests zu identifizieren und zu beheben. Für die Typgenehmigung schreibt beispielsweise die UNECE-Regulierung R155 in Verbindung mit der EU-Verordnung 2019/2144 invasive Tests vor. Diese sind unerlässlich, um die Wirksamkeit der Cybersecurity-Maßnahmen zu gewährleisten.

Die derzeitige Strafrechtslage (§§ 202 a–c StGB) stellt Penetrationstests ohne ausdrückliche Zustimmung der Berechtigten unter Strafe. Besonders problematisch ist die oft komplexe Lieferkette in der Automobilindustrie und die Integration von Drittanbietersoftware. Dadurch sind nicht nur unbeauftragte Sicherheitsforschende strafrechtlichen Risiken ausgesetzt. Auch alle, die intern und extern testen, sehen sich schnell mit unübersichtlichen rechtlichen Rahmenbedingungen konfrontiert. Dies benachteiligt ehrliche Sicherheitsforschende und begünstigt kriminelle Hacker (Black Hat Hacker), was die Umsetzung von Fahrzeugsicherheit unnötig erschwert.

Im Rahmen der geplanten Gesetzesnovellierung – die zwar im Koalitionsvertrag verankert, jedoch noch ohne konkreten Entwurf ist – sollte die Strafbarkeit im Computerstrafrecht deshalb nicht allein von der Zustimmung abhängig gemacht werden. Vielmehr muss die Intention der Testenden als zentrales Kriterium berücksichtigt werden. Positive Intentionen zeichnen sich durch verantwortungsvollen Umgang mit Schwachstellen, den Beitrag zur Systemsicherheit sowie durch den Schutz von Herstellern und Nutzenden aus. Negative Absichten wie die Ausnutzung von Sicherheitslücken oder das Streben nach unverhältnismäßigen finanziellen Vorteilen sollen weiterhin sanktioniert werden. Ziel ist eine klare, rechtssichere Regelung, die ethisch motivierte Cybersecurity-Tests ermöglicht, die Cybersicherheit erhöht und zugleich Missbrauch verhindert.

Dr. Kirsten Matheus
Expertin für Digitalisierung und Cybersicherheit beim Verband deutscher Automobilhersteller (VDA)

Das sagt der Verbraucherschutz: Ein strukturelles Dilemma

Angesichts der fortschreitenden Digitalisierung und der damit einhergehenden Erfassung erheblicher Datenmengen ist die Einhaltung des Datenschutzrechts, insbesondere der DSGVO, von zentraler Bedeutung. Zur Aufdeckung möglicher Datenschutzverstöße bestehen im Wesentlichen zwei Ansätze: die Prüfung von Datenschutzhinweisen und die technische Untersuchung des tatsächlichen Datenverkehrs.

Datenschutzhinweise sollen Transparenz schaffen, sind jedoch häufig nur vage formuliert. Verbraucher*innen müssen zudem darauf vertrauen können, dass die tatsächliche Datenverarbeitung den Angaben in den Datenschutzhinweisen entspricht. Hier setzt die technische Analyse an, bei der Datenströme zwischen Gerät und Anbieter-Server untersucht werden.

Ist der Datenverkehr transportverschlüsselt, erfordert seine Analyse regelmäßig die Umgehung dieser Schutzmaßnahme. Dies kann den Tatbestand des § 202 a StGB erfüllen. Damit ist die Analyse von Datenströmen zur Feststellung möglicher Datenschutzverstöße mit einem erheblichen Risiko der Strafbarkeit verbunden. Das gilt insbesondere bei dem Einsatz von Reverse Engineering, das zusätzlich urheberrechtliche Fragen aufwirft.

11.12.2024

Stellungnahme der GI zur geplanten Reform des Computerstrafrechts
Die GI begrüßt den Gesetzesentwurf und das damit erklärte Ende der Rechtsunsicherheit für die IT-Sicherheitsforschung. Trotz offener Fragen zu der praktischen Umsetzung ist es aus Sicht der GI ein Schritt in die richtige Richtung. Mit dem Bruch der Regierung wird dieses Gesetzesvorhaben nicht mehr umgesetzt.

09.04.2025

Reform im Koalitionsvertrag
Die neue Bundesregierung unter Friedrich Merz vereinbart in ihrem Koalitionsvertrag, „Rechtssicherheit für IT-Sicherheitsforschung“ zu schaffen. Seitdem prüft das Bundesjustizministerium die Umsetzung.

05.09.2025

Exkurs zum ethischen Hacken und Computerstrafrecht im GI-Blog
Der Junior-Fellow Tim Philipp Schäfers mahnt, dass das Computerstrafrecht dringend aktualisiert werden muss. In seinem Beitrag geht es zudem um ethisches Hacking.

Im Ergebnis zeigt sich ein strukturelles Dilemma: Anbieter erfüllen durch die Verschlüsselung des Netzwerkverkehrs ihre Schutzpflichten, zugleich wird damit jedoch die Kontrolle datenschutzrechtlicher Vorgaben faktisch erschwert. Nicht selten erfassen Anbieter über das erforderliche Maß hinaus Daten. Eine klarstellende gesetzliche Regelung, die die Analyse von Datenströmen zum Zwecke der Datenschutzkontrolle privilegiert, erscheint daher dringend geboten. Hierzu könnten insbesondere im Verbandsklageregister eingetragene Organisationen in ausgewählten Fällen befugt werden, gemeinsam mit technisch versierten Partnern entsprechende Prüfungen außerhalb einer Strafbarkeit durchzuführen und dadurch zugleich die Datenschutzaufsichtsbehörden zu entlasten.

Dr. Ayten Öksüz
Datenreferentin bei der Verbraucherzentrale NRW

Das sagt das BSI: Hohe Priorität für Rechtssicherheit

Die Cybersicherheitslage ist nach wie vor angespannt: Insbesondere unzureichend geschützte Angriffsflächen machen Deutschland im digitalen Raum verwundbar. Dass es daher notwendig ist, deutsche Bürger*innen, Behörden sowie Unternehmen zu schützen, wird inzwischen von niemandem mehr bestritten. Eine Gesellschaft, die resilient gegen Cyberangriffe werden will, kann sich dabei aber nicht nur auf staatliche Schutzmaßnahmen und kommerzielle Software stützen. Das Engagement und die Erkenntnisse von Forschenden und anderen Personen, die sich beruflich oder privat mit der IT-Sicherheit von Systemen beschäftigen, sind hier äußerst wertvoll und essenziell.

Vor diesem Hintergrund ist eine Reform des Computerstrafrechts von großer Relevanz. Die Sorge davor, sich bei der Untersuchung von IT-Systemen auf Verwundbarkeiten strafbar zu machen oder anderen rechtlichen Konsequenzen auszusetzen, verunsichert die IT-Sicherheits-Community und schränkt Forschungstätigkeiten ein. Rechtsunsicherheit ergibt sich dabei aus dem sehr weiten Anwen-dungsbereich der Computerdelikte im Strafgesetzbuch, andererseits aber auch aus den Vorgaben des Urheber- und des Datenschutzrechts. Auch für das Bundesamt für Sicherheit in der Informationstechnik (BSI) erschwert die aktuelle Rechtslage die Erfüllung seines gesetzlichen Auftrags: Schon allein die Sorge vor rechtlichen Konsequenzen kann Personen von einer Schwachstellenmeldung abhalten. Jede nicht gemeldete und damit nicht geschlossene Schwachstelle stellt ein Risiko für die Cybersicherheit dar und hat zur Folge, dass Betroffenen von Schwachstellen nicht oder erst spät geholfen wird. Auch schränken unterbliebene Meldungen die Erkenntnisse über die Cybersicherheitslage in Deutschland ein.

Das BSI hat im Rahmen seiner CVD-Richtlinie mit Blick auf die Rechtslage auch anonyme Meldewege eingeführt. Anonyme Meldungen können vor Strafverfolgung und anderen rechtlichen Konsequenzen schützen. Sie erschweren aber für das BSI umgekehrt die Bewertung des Sachverhalts und die Kommunikation – denn gerade bei komplexen Sachverhalten ist es oft entscheidend, Rückfragen mit Meldenden besprechen zu können.

Das Bundesjustizministerium hat in der vergangenen Legislaturperiode einen Gesetzesentwurf zur Modernisierung des Computerstrafrechts vorgelegt und plant, das Vorhaben in dieser Legislatur wieder aufzugreifen. Dies sollte mit hoher Priorität geschehen und den Aspekt der Rechtssicherheit für die betroffenen Personenkreise in den Vordergrund stellen – denn Cybersicherheit braucht engagierte, aktive Sicherheitsforschende.

Judith Faust und Tassilo Thieme
Bundesamt für Sicherheit in der Informationstechnik (BSI)

---

[1] *https://www.kaspersky.de/resource-center/definitions/hacker-hat-types*

[2] *https://www.bitkom.org/Presse/Presseinformation/Angriffe-auf-die-deutsche-Wirtschaft-nehmen-zu*

[3] *https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.html*

[4] *https://doi.org/10.1016/j.cose.2022.102936*

[5] *https://doi.org/10.1109/SP54263.2024.00104*

[6] *https://doi.org/10.1145/3133956.3134047*

[7] *https://www.interface-eu.org/publications/deutschlands-staatliche-cybersicherheitsarchitektur*

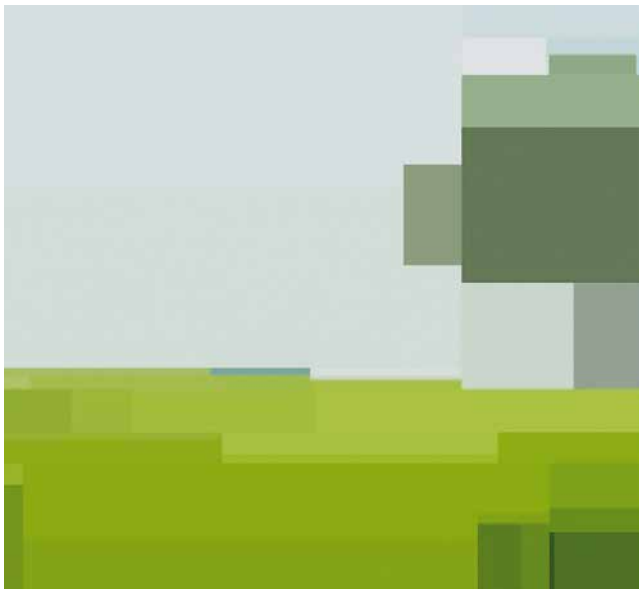
[8] *https://lilithwittmann.medium.com/ wenn-die-cdu-ihren-wahlkampf-digitalisiert-a3e9a0398b4d*

[9] Deusch, Eggendorfer, K&R 2023, 649ff. und K&R 2025, 150ff.

[10] AG Essen, 161 IN 10/26 (vorläufiges Insolvenzverfahren).

[11] Deusch, Eggendorfer, K&R 2018, 223ff., 227f.

[12] Deusch, Eggendorfer, K&R 2023, 649ff.



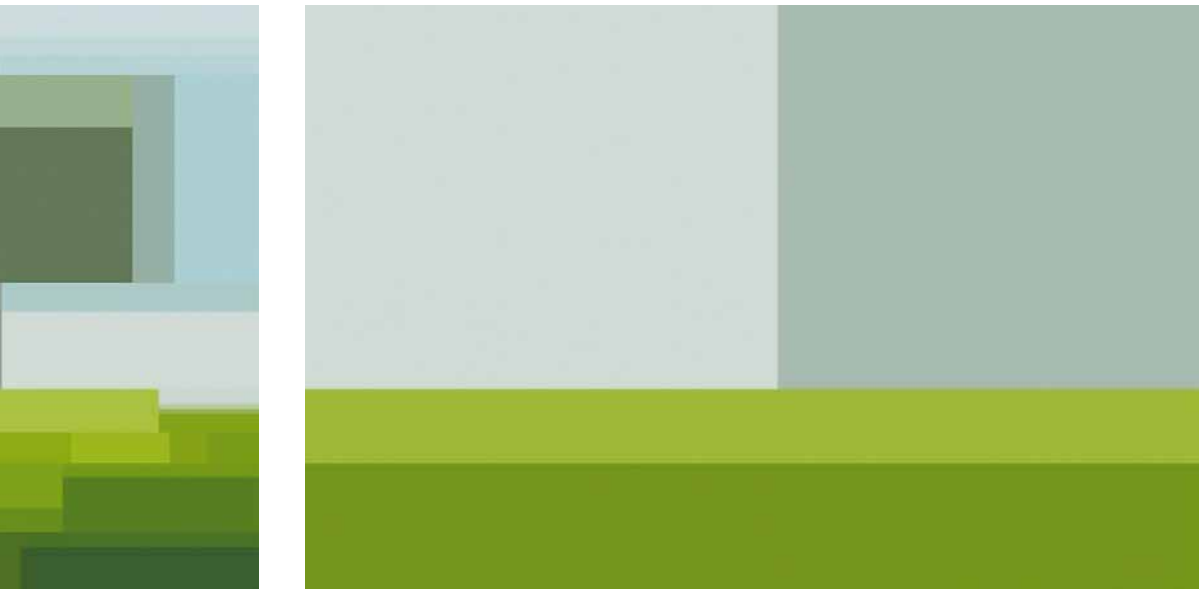
Nachhaltigkeit ist *kein Add-on*

TEXT Christine Hennig, Karolin Kappler,
Ina Schieferdecker, Nicole Wolf

Ob künstliche Intelligenz zur Rettung unseres Klimas beiträgt oder die globale Klimakrise durch ihren massiven Energie- und Ressourcenhunger weiter verschärft, entscheidet sich an ihrer bewussten Gestaltung sowie an der Art, wie wir sie nutzen. Vier Expertinnen beleuchten, warum es an der Informatik liegt, „Sustainability by Design" einzufordern – und warum das weit mehr beinhaltet, als Rechenzentren zu begrünen.

KI[1] ist kein gewöhnliches Werkzeug der Digitalisierung. Sie ist ihr derzeit wirkmächtigstes Versprechen – und womöglich ihr größter Belastungstest. Denn mit KI verschärft sich nicht nur die Frage nach dem exponentiell steigenden Ressourcenverbrauch digitaler Systeme. Neu stellt sich vor allem die Frage nach dem Zweck: Welche Probleme können und sollen mit KI-Anwendungen gelöst werden, damit sie nicht nur der Gewinnmaximierung Einzelner dienen? Unser Ziel sollte es sein, dass wir sie nutzen, um unsere Gesellschaft als Ganzes mit gemeinwohlorientierten Innovationen nachhaltiger zu machen.

Zwischen diesen Polen bewegt sich die Debatte. KI kann dabei unterstützen, Energiesysteme effizienter zu steuern, Forschung zu beschleunigen und knappe Ressourcen effizienter zu nutzen. Andererseits wächst ihr eigener Bedarf an Energie, Frischwasser und Hardware für immer mehr und immer größere Rechenzentren exponentiell. So verschlang der Prozess des Trainings eines Modells wie GPT-4 schätzungsweise 50 Gigawattstunden – genug Strom, um beispielsweise bei 3.000 kWh Jahresverbrauch eines deutschen Haushalts gut



16.000 Haushalte zu versorgen. Bis 2030 könnten Rechenzentren weltweit etwa 945 Terrawattstunden verbrauchen – das wäre eine Verdopplung im Vergleich zum Jahr 2024 und entspräche dem aktuellen kombinierten Strombedarf von Deutschland (ca. 500 TWh/Jahr) und Frankreich (ca. 450 TWh/Jahr).

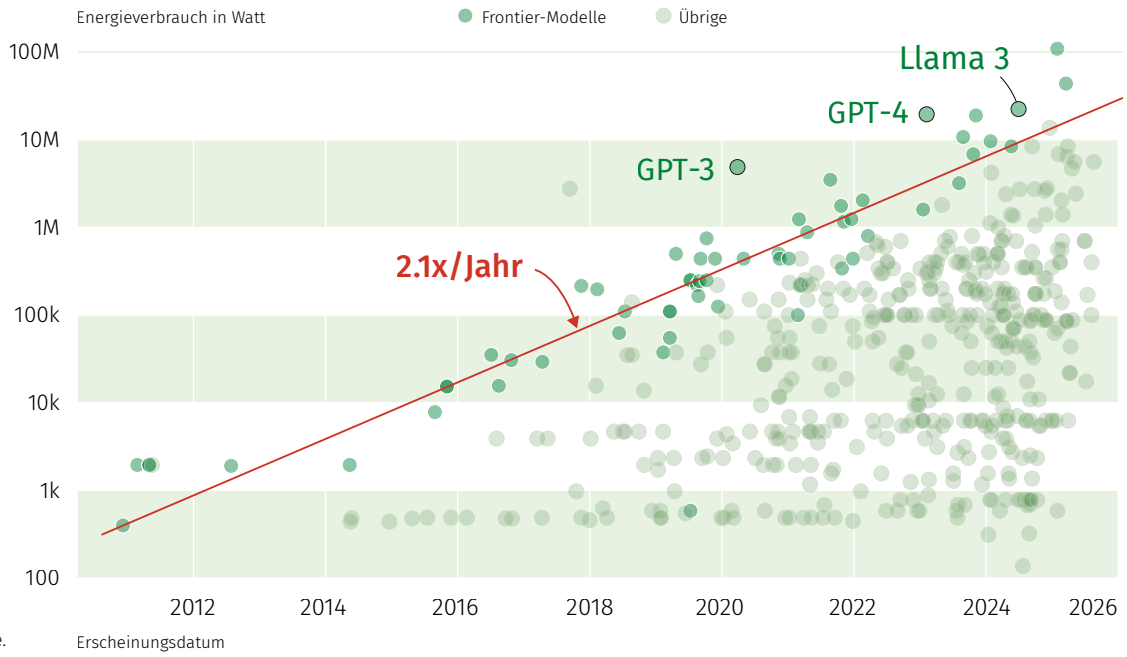
In einer Diskussion zum Beitrag von KI zu nachhaltiger Digitalisierung dürfen nicht nur Klimabilanz, Energieeffizienz oder Wasserverbrauch in den Blick genommen werden. Es muss ebenso um Themen wie soziale Teilhabe, ökonomische Machtverschiebungen, politische Einflussnahme, Arbeitsbedingungen, Grundrechte, globale Gerechtigkeit und Inklusion gehen. Auch darin zeigt sich die Ambivalenz dieser Technologien. KI kann helfen, Klimamodelle zu verfeinern, Kreisläufe zu optimieren und erneuerbare Energiesysteme besser zu steuern. Zugleich erzeugt sie neue Belastungen – für unsere Ökosysteme und Gesellschaft.

Wo KI zum Treiber technischer Erneuerung wird, wächst auch der Bedarf an Daten- und Rechenleistung, werden Innovationszyklen verdichtet, verkürzt sich die Nutzungsdauer von Geräten und Komponenten und verschärft sich die Elektroschrottkrise weiter. Die Nachhaltigkeit von KI-Anwendungen lässt sich daher nicht auf deren Energie- und Ressourceneffizienz reduzieren. Zur Debatte steht: Wie wollen und müssen wir Digitalisierung gestalten, damit alle gleichermaßen davon profitieren?

Nachhaltige Digitalisierung ist mehr als begrünte Rechenzentren

Gerade weil die ökologischen und sozialen Kosten von KI leicht hinter der Faszination des technisch Machbaren und der Innovationsversprechen verschwinden, gehört es zu den zentralen Aufgaben der Informatik, diese Kosten sichtbar zu machen – und der Logik immer kürzerer Software- und Hardware-Zyklen entgegenzuwirken. Nachhaltige Digitalisierung heißt mehr, als Rechenzentren zu begrünen. Sie verlangt ebenso, die sozialen Bedingungen digitaler Wertschöpfung zu gestalten und der prekären Datenarbeit, den ungleichen Verteilungen von Nutzen und Lasten, diskriminierenden Effekten algorithmischer Systeme oder der Zunahme digitaler Gewalt etwas entgegenzusetzen.

Zur Entscheidung steht, ob wir als Informatiker*innen KI-Entwicklungen nur als Hebel und Beschleuniger von technischen Innovationen begreifen oder ob wir auch Verantwortung für deren Richtung übernehmen. Nachhaltige KI entsteht nicht ohne bewusste Gestaltung. Sie erfordert, dass ökologische und soziale Kriterien von Beginn an mitgedacht und nicht nachträglich ergänzt werden.



Die benötigte Compute Power für das Trainieren von LLMs verdoppelt sich alle fünf bis sechs Monate.

Auch technisch zeichnet sich inzwischen ab, dass das alte Skalierungsdogma an Überzeugungskraft verliert. Nicht immer ist das größte Modell auch das sinnvollste. Für viele Anwendungen sind kleinere, spezialisierte Modelle deutlich ressourcenschonender und zugleich hinreichend leistungsfähig oder gar besser. Architekturen wie Mixture-of-Experts verstärken diesen Trend, weil sie nur jene Teile eines Modells aktivieren, die für eine Anfrage tatsächlich benötigt werden. Effizienz wird damit nicht zum Nebenprodukt von Größe, sondern zu einer Frage informierter und suffizienter Systemgestaltung.

Mit Verfahren wie Quantisierung, spezialisierteren Architekturen oder einer der jeweiligen Aufgabe angemessenen Modellauswahl rücken jedoch auch die Grenzen technischer Effizienzgewinne in den Blick, da mehr Ressourceneffizienz keineswegs automatisch zu weniger Ressourcenverbrauch führt. Oft geschieht das Gegenteil: Sinkende Kosten machen KI-Anwendungen attraktiver, verbreiten ihren Einsatz und treiben den Gesamtverbrauch weiter nach oben. Genau diese Rebound-Effekte zeichnen sich bei generativer und agentischer KI bereits ab. Je billiger einzelne Anfragen werden, desto selbstverständlicher wird KI für immer mehr Zwecke eingesetzt – auch dort, wo sie keinen Mehrwert schafft. Nicht selten wird KI zum universellen Workaround, der ineffektive und ineffiziente Prozesse nur überdeckt, statt deren eigentliche Probleme zu lösen. So entstehen neue Individuallösungen, zusätzliche Komplexität und neue Lock-in-Effekte, obwohl für viele Aufgaben längst dedizierte, symbolische oder gar nicht auf KI basierende Verfahren verfügbar wären, die einfacher, robuster und ressourcenschonender sind. KI ist kein Allheilmittel. Nachhaltige Digitalisierung beginnt deshalb nicht mit der Frage, wo sich KI noch einsetzen ließe, sondern welche Lösung für ein Problem tatsächlich die beste ist – und ob KI dafür überhaupt gebraucht wird.

Spätestens hier kommen die Nachhaltigkeitsziele der Vereinten Nationen ins Spiel. Sie sind nicht nur normativer Bezugspunkt, sondern ein Ordnungsrahmen, um digitale Innovation jenseits rein technischer Metriken zu bewerten. Anstelle einer verengten ökonomischen Perspektive ist eine umfassende Wirkungsorientierung bei der Umsetzung von KI-Anwendungen geboten. Sie brauchen „Sustainability by Design“: Prozesse verbessern, statt sie nur mit KI aufzurüsten; gute Lösungen suchen, statt technische Machbarkeit mit Fortschritt zu verwechseln. Nur so kann der nachhaltige Handabdruck von KI größer werden als ihr ökologischer und gesellschaftlicher Fußabdruck.

Die Forschung der vergangenen Jahre hat die frühe KI-Euphorie auf den Boden der Tatsachen zurückgeholt. KI erscheint heute weniger als autonome Problemlöserin denn als Instrumentenkasten, dessen Wirkungen von politischen, ökonomischen und gesellschaftlichen Rahmenbedingungen abhängt. Ihr Potenzial für die Transformation zur Nachhaltigkeit ist damit nicht verschwunden. Ob jedoch KI zu den Nachhaltigkeitszielen beitragen oder bestehende Probleme vertiefen wird, entscheidet sich an ihrer Einbettung in öffentliche Infrastrukturen, Institutionen und Machtverhältnisse.

Leitfragen für die Informatik

Die daraus folgenden Fragen sollten auch für uns Informatiker*innen leitend sein: Wie lässt sich der Beitrag von KI-Anwendungen zu Nachhaltigkeitszielen bewerten, ohne ihre ökologischen und sozialen Folgekosten auszublenden? Wie können wir KI suffizient einsetzen, entwickeln, gestalten und nutzen? Wie kann verhindert werden, dass fehlende digitale Infrastrukturen oder mangelnde lokale Handlungsspielräume bestehende Ungleichheiten weiter verschärfen? Welche Governance-Modelle schaffen Verbindlichkeit, ohne Teilhabe für ressourcenschwächere Akteure zu blockieren? Auf welcher Datenbasis entstehen KI-Applikationen – mit welchen Perspektiven, in wessen Interessen, mit welchen Prioritäten und Ausschlüssen? Diese Fragen adressieren nicht technische Leistungswerte und betreffen Verteilung, Teilhabe, Datenhoheit und die Fähigkeit, KI-Anwendungen an lokale Kontexte und gesellschaftliche Bedürfnisse zu binden.

KI kann uns im Umgang mit globalen Polykrisen unterstützen und Transformationsprozesse wieder ankurbeln, die durch diese Krisen ausgebremst wurden. Voraussetzung hierfür ist eine Innovationskultur, die den Einzelnen, dem Gemeinwohl und dem Planeten dient. Die Dekade bis 2030 ist entscheidend für die Frage, ob die technologische Rendite die globale Wohlfahrt nachhaltig steigert – oder ob sie weiterhin neue Wege hervorbringt, die Menschen ausschließen oder die Umwelt zusätzlich belasten. Für Informatiker*innen ist das keine Randfrage, sondern eine Gestaltungsaufgabe.

- Transparenz und Verantwortungsübernahme
- Nicht-Diskriminierung und Fairness
- Technische Verlässlichkeit und menschliche Aufsicht
- Selbstbestimmung und Datenschutz
- Inklusives und partizipatives Design
- Kulturelle Sensibilität
- Marktvielfalt und Ausschöpfung des Innovationspotenzials
- Verteilungswirkung in Zielmärkten
- Arbeitsbedingungen und Arbeitsplätze
- Energieverbrauch
- CO_2- und Treibhausgasemissionen
- Nachhaltigkeitspotenziale in der Anwendung
- Indirekter Ressourcenverbrauch

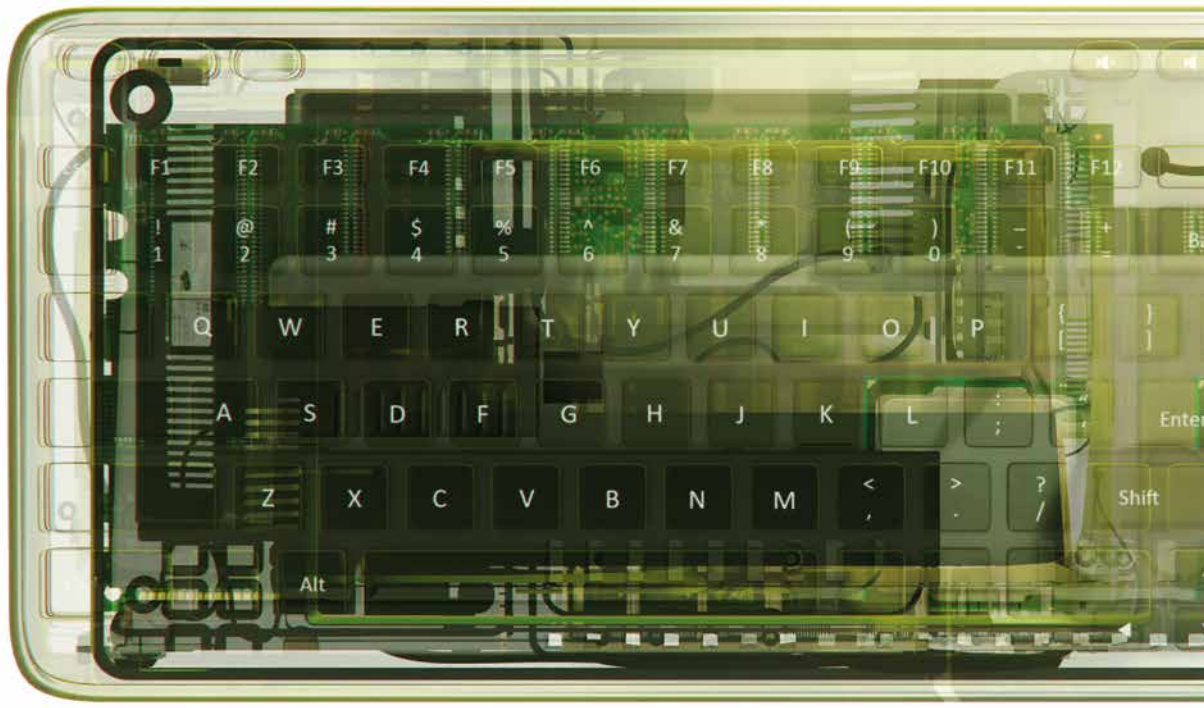
13 Nachhaltigkeitskriterien für KI-Systeme

Unser klarer Aufruf: Die GI sollte diesen Prozess aktiv mitprägen. Gefragt ist ein gemeinsames Nachdenken darüber, was die Informatik konkret zur Entwicklung nachhaltiger KI-Anwendungen beitragen kann: in Forschung und Lehre, in Standards und Bewertungskriterien, in der Praxis digitaler Infrastrukturen und in der öffentlichen Debatte. Wir laden die Mitglieder der GI ein, sich an der Erarbeitung einer Sammlung von Kriterien zu beteiligen, die Positionen bündelt, Leitlinien formuliert und Handlungsfelder sichtbar macht. Nachhaltige KI wird nicht durch Appelle entstehen, sondern durch gemeinsame fachliche Orientierung. Genau dazu kann und soll die GI einen entscheidenden Beitrag leisten. I

[1] Der Begriff KI wird häufig genutzt, um eine Reihe von Verfahren zur Mustererkennung, Entscheidungsdsfindung und Problemlösung zu beschreiben. Wir beziehen uns in diesem Artikel insbesondere auf agentische und generative KI.

Über die Autorinnen
Dieser Beitrag entstand in Zusammenarbeit von Christine Hennig (Sprecherin Fachbereich Informatik und Gesellschaft), Ina Schiefer-decker (Vorstand der GI) sowie Nicole Wolf und Karolin Kappler, die Sprecherinnen der neu gegründeten Fachgruppe Digitalisierung und Nachhaltigkeit sind.

Deep Dive
Quellen, Linktipps und Leseempfehlungen der Autorinnen:
inf.gi.de/kein-add-on



Ressourceneffizienz, **built-in**

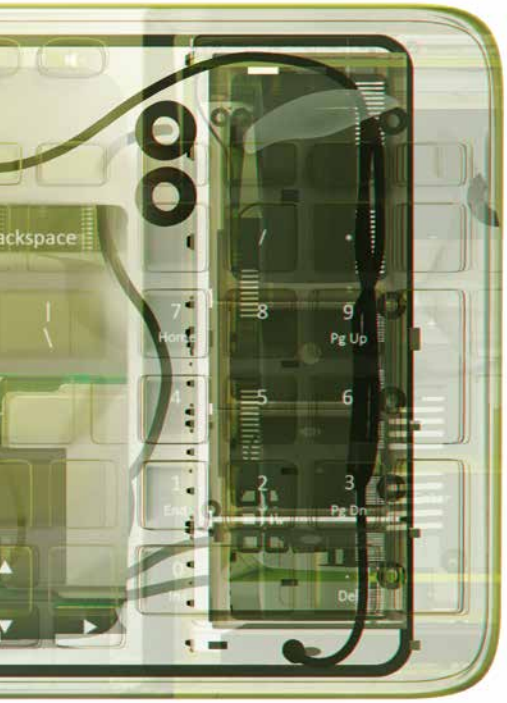
TEXT Stella Drebber, Nikolas Becker

Das Konzept von „Sustainability by Design" klingt erst mal gut. Doch um das einzufordern, braucht es Praktiken in der Softwareentwicklung, die Umweltauswirkungen und Ressourcenverbräuche von der Konzeption an und über den gesamten Software-Lebenszyklus mitdenken. Ein Team der GI befasst sich damit, welche solcher Praktiken bereits existieren und was passieren muss, damit sie großflächig und sinnvoll zum Einsatz kommen.

Die Autorinnen des vorausgegangenen Artikels halten es für eine der zentralen Aufgaben der Informatik, die ökologischen und sozialen Kosten von KI sichtbar zu machen und der Logik von immer kürzeren Software- und Hardware-Zyklen entgegenzuwirken – völlig zu Recht. Gerade die Diskussion um (generative) KI verschiebt den Fokus weg von Rechnern und Rechenzentren hin zu der immateriellen Ebene der Software.

Trotz ihrer offensichtlichen Immaterialität sind digitale Dienste grundlegend von physischer Infrastruktur abhängig und beeinflussen diese wiederum. In den meisten realen Szenarien sind sie auf stark vernetzte Infrastrukturen angewiesen, die zahlreiche Hardwareplattformen, Kommunikationsnetzwerke, Cloud-Umgebungen und Speichersysteme umfassen. Im Wesentlichen bestehen sie aus den Digital Basic Resources (DBRs): Rechenleistung, Speicherleistung, Speicherkapazität und Datenübertragung.[1]

Alle anderen Infrastrukturkomponenten – darunter Kühlsysteme, Gebäude, Back-up-Systeme, Stromverteilung und Netzwerkausrüstung – dienen in erster Linie dazu, diese digitalen Grundressourcen bereitzustellen. Jede Softwareanwendung benötigt daher eine messbare Menge dieser Ressourcen und daran gekoppelt eine tendenziell steigende Menge an Wasser, kritischen Rohstoffen, Flächen und Kühlinfrastruktur über die gesamte digitale Lieferkette hinweg.[2] Software ist somit entscheidende Vermittlerin zwischen digitalem



Bedarf und physischem Ressourcenverbrauch. Denn selbst Anwendungen, die ähnliche Funktionen bereitstellen, können abhängig von Entwicklung, Bereitstellung und Betrieb sehr unterschiedliche ökologische Fußabdrücke haben.[3]

Verschiedene Studien belegen, dass die Umweltauswirkungen digitaler Technologien nicht nur eine Frage der Infrastruktureffizienz sind. Sie hängen auch von der Softwaregestaltung und den Nutzungsmustern ab.[4] Fortran zum Beispiel verbrauchte in einem Use Case weniger Energie als schnellere Programmiersprachen, weil es effizienter mit Systemressourcen umgeht. Java-Programme auf der anderen Seite lieferten deutlich schneller, verbrauchten aber auch mit verbesserter Performance mehr Energie. Grundsätzlich gilt: Schnelligkeit ist kein verlässlicher Indikator auf dem Weg zu Ressourceneffizienz. Während Vorschläge für konkrete Anpassungen in Datenbanksystemen wie MySQL oder dem Open-Source-Webserver Apache web server bestehen, die das Potenzial haben, den Energieverbrauch einer Anwendung um bis zu 25 Prozent zu senken, fehlt es an übergreifenden Handreichungen, die für viele Use Cases relevant sind, und an deren breiter Kommunikation.[5]

Viel ungehobenes Potenzial

An dieser Stelle dockt das Projekt „Unlocking the Potential of Green Coding into Practice" an, das die GI in Kooperation mit der HTW Berlin und dem Umweltcampus Birkenfeld der Hochschule Trier umsetzt. Das Team entwickelt unter anderem eine Policy Roadmap, die Maßnahmen und Interessensgruppen zusammenbringt und Entwicklungen aufzeigt, um Green Coding bis 2035 in der Bildung und als wirtschaftlichen Anreiz zu integrieren. Der Fokus liegt darin auf drei Bereichen: politische und regulatorische Institutionalisierung, Bildung und Kompetenzen sowie auf einem Kulturwandel, der von wirtschaftlichen Anreizen bis hin zu Allgemeinwissen reicht.

Neben der praktischen Umsetzung von Green Coding haben die Maßnahmen das Potenzial, den Wirtschafts- und Wissenschaftsstandort Deutschland nachhaltiger und wettbewerbsfähiger zu gestalten: etwa indem das Thema Green Coding in Curricula aufgenommen und in Unternehmensstrategien verankert wird. Sie sind ein wichtiger Baustein für eine resiliente und unabhängige Energie- und Digitalinfrastruktur und sollten mit diesen Maßnahmen bis 2035 auch genau als solche etabliert sein. I

Green Coding im Visier
Weitere Informationen und die vollständige Policy Roadmap finden Sie unter:
inf.gi.de/greencoding

---

[1] *https://www.oeko.de/fileadmin/oekodoc/Method_sketch_LCA_Software.pdf*

[2] Ebd.

[3] Dauner, M., & Socher, G. (2025). *Energy costs of communicating with AI. Frontiers in Communication, 10. https://doi.org/10.3389/fcomm.2025.1572947*

[4] Pereira, R., Couto, M., & Ribeiro, M. et al. (2017). *Energy efficiency across programming languages: How do energy, time, and memory relate? 10th ACM SIGPLAN International Conference on Software Language Engineering (SLE 2017). https://doi.org/10.1145/3136014.3136031*

[5] Kalu, W. (2025). *Green Coding in Practice: A Developer's Handbook for Energy-Efficient Software Development [Lappeenranta-Lahti University of Technology LUT]. https://lutpub.lut.fi/bitstream/handle/10024/170300/Mastersthesis_Kalu_Wisdom.pdf*

Die Delegierten des Common Grounds Forum trafen im politischen Berlin eine Vielzahl an Akteur*innen. Zu den Gesprächspartner*innen im Bundestag zählten unter anderem Dr. Anna Lührmann und Denise Loop (Bündnis 90/Die Grünen).

Zwischen Kanzleramt und Karaokebar

TEXT Lea Hildermeier, Luca Randecker

Das Common Grounds Forum verschafft jungen Stimmen Gehör: in der Digitalpolitik und darüber hinaus. Bei einer Delegationsreise im Frühling gingen 25 junge Menschen in den Austausch über Positionen, Forderungen und ganz konkrete Tipps für die Lobbyarbeit. Zwei von ihnen haben erarbeitet, was junge Interessenvertretung im politischen Berlin über Digitalpolitik lernen kann.

Wer an Lobbyarbeit denkt, hat oft Bilder von verschlossenen Türen, dunklen Anzügen und etablierten politischen Akteur*innen im Kopf. Ende März 2026 sah das politische Berlin jedoch für einige Tage anders aus. Mit Notizbüchern, vorbereiteten Gesprächsleitfäden und einer langen Liste an Themen reiste eine 25-köpfige Delegation des Common

Gute Interessenvertretung beginnt mit dem Dialog. In zahlreichen Gesprächen brachten die Delegierten des CGFs ihre Perspektiven und Forderungen zu zentralen Fragen der Digitalpolitik ein.

Grounds Forum (CGF) im Alter zwischen 16 und 30 nach Berlin, um über digitale mentale Gesundheit, nachhaltige Software, demokratische Teilhabe und digitale Infrastruktur zu sprechen. Nicht als symbolische Jugendbeteiligung, sondern als Menschen mit konkreten politischen Forderungen und eigenen Perspektiven auf digitale Gesellschaft.

Das CGF bringt seit 2023 junge Stimmen mit unterschiedlichen Perspektiven und Hintergründen zusammen, um Positionen zu Digitalisierung, Bildung, Demokratie und gesellschaftlichem Wandel zu entwickeln. Die Community versteht Digitalisierung nicht als rein technisches Thema, sondern als gesellschaftliche Gestaltungsfrage. Genau das prägte auch die Delegationsreise nach Berlin.

Wie würdest du die Delegationsreise in einem Wort beschreiben?

„Motivierend."

ALINE GIESSLER

Zwischen Gesprächen im Bundestag, Terminen im Bundeskanzleramt und dem Austausch mit zivilgesellschaftlichen Organisationen wie der Gesellschaft für Freiheitsrechte, Wikimedia Deutschland, Bitkom oder der Initiative D21 wurde schnell deutlich: Hinter vielen Debatten über digitale Technologien stehen gesellschaftliche Fragen, die weit über technische Lösungen hinausreichen.

Junge Perspektiven im politischen Berlin

Besonders eindrücklich war bei vielen Delegierten der Moment, plötzlich selbst in diesen politischen Räumen zu sitzen. Was vorher abstrakt wirkte, wurde konkret: „Sehr einprägsam war die Möglichkeit, sich in diesem großen Saal im Kanzleramt auf Augenhöhe mit den operativ tätigen Personen auszutauschen", erinnert sich Moritz Kreinsen, CGF-Vertreter und Experte für Informatikdidaktik.

Für viele war die Reise der erste direkte Kontakt mit politischer Interessenvertretung. Außerordentlich prägend war dabei oft nicht nur der Inhalt der Gespräche, sondern die Erfahrung, überhaupt Teil davon zu sein. „Das war total neu für mich. Dementsprechend war ich auch ein bisschen nervös. Aber ich habe im Gespräch gemerkt, dass es gar nicht so schlimm ist und dass man gut reinkommt, wenn man sich traut", so Aline Geißler, die sich insbesondere für Klimagerechtigkeit einsetzt.

Wie würdest du die Delegationsreise in einem Wort beschreiben?

„Gamechanger."

MORITZ KREINSEN

Gerade darin lag eines der wichtigsten Learnings der Reise: Gute Lobbyarbeit beginnt nicht erst beim fertigen Forderungspapier. Sie beginnt damit, die eigene Perspektive als relevant wahrzunehmen und sie in politische Räume einzubringen. Sarra Lejmi, die sich speziell im Bereich Jugendbeteiligung engagiert, beschreibt die Woche in Berlin als Erfahrung, die weit über einzelne Gespräche hinausging: „Die Reise hat mein Bewusstsein dafür geschärft, wie wichtig demokratische Mitwirkung und gesellschaftliches Engagement für eine lebendige und vielfältige Gesellschaft sind. Die Begegnungen und Gespräche haben mir neue Sichtweisen eröffnet, bestehende Annahmen hinterfragt und mich motiviert, mich auch künftig aktiv in politische und gesellschaftliche Prozesse einzubringen."

Zwischen Forderungen und Dialog

Die Delegationsreise machte auch deutlich, dass erfolgreiche Interessenvertretung weit mehr ist als das möglichst häufige Wiederholen eigener Forderungen. Mehrere Delegierte beschrieben Vorbereitung und echtes Verständnis für das Gegenüber als entscheidend.

„Es ist wichtig, sich genau zu überlegen: Wer sitzt mir gegenüber? Was kann diese Person tatsächlich bewirken?“, bekräftigt Benedikt Kammergruber, einer der Jüngsten der Runde.

Gerade in Gesprächen mit Abgeordneten, Ministeriumsmitarbeitenden oder Verbänden gehe es nicht darum, möglichst viele Themen in kurzer Zeit unterzubringen, sondern sinnvolle Anknüpfungspunkte zu finden. Auch Nils Alznauer, der sich im CGF insbesondere im Bereich digitale Gerechtigkeit engagiert, betont, wie wichtig ein echter Austausch mit Abgeordneten verschiedener Parteien sei, und gibt als Rat mit: „Versuche, das Gespräch aktiv zu strukturieren und in eine sinnvolle Richtung zu lenken. Gleichzeitig ist es wichtig, auf dein Gegenüber einzugehen.“ Lobbyarbeit erschien dadurch weniger als undurchsichtige Hinterzimmerpolitik, sondern vielmehr als kommunikative Übersetzungsarbeit zwischen unterschiedlichen Perspektiven und Erfahrungswelten.

Gerade für die Informatik-Community könnte darin eine wichtige Erkenntnis liegen. Viele Fragen rund um Digitalisierung bewegen sich an der Schnittstelle von Technologie, Politik und Gesellschaft. Wer digitale Zukunft mitgestalten möchte, muss deshalb nicht nur über technische Lösungen sprechen, sondern auch darüber, welche Auswirkungen diese auf unterschiedliche Lebensrealitäten haben und welche Perspektiven in ihre Entwicklung einfließen. Die Gespräche in Berlin machten deutlich, wie wichtig dafür Austausch und Dialog sind. Politische Gestaltung entsteht nicht allein durch Positionen oder Forderungspapiere, sondern auch durch Beziehungen, gegenseitiges Verständnis und die Fähigkeit, unterschiedliche Perspektiven miteinander ins Gespräch zu bringen. Die Themen des CGF spiegeln genau diese Verbindung wider: Nachhaltige Softwareentwicklung, digitale mentale Gesundheit, demokratische Teilhabe oder Alternativen zu monopolisierten Plattformen sind nicht nur technische Fragen, sondern sie betreffen ökologische Verantwortung, digitale Souveränität und gesellschaftliche Machtverhältnisse.

Wie würdest du die Delegationsreise in einem Wort beschreiben?

„Inspirierend.“

BENEDIKT KAMMERGRUBER

Politische Teilhabe braucht Zugänge

Während der Reise wurde aber auch sichtbar, dass politische Beteiligung nicht für alle gleichermaßen zugänglich ist. Moritz Kreinsen beschreibt insbesondere die Bedeutung räumlicher Nähe: „Die Möglichkeit, sich kurzfristig vor Ort mit Stakeholdern und Entscheidungsträger*innen zu treffen, macht einen Unterschied.“ Politische Netzwerke entstehen oft dort, wo Menschen sich regelmäßig begegnen. Gerade deshalb sind Formate wichtig, die jungen Menschen konkrete Zugänge zu politischen Räumen ermöglichen. Auch für Sarra

Bei all den wichtigen Gesprächen darf auch der Spaß nicht zu kurz kommen. Gemeinsame Abende boten Raum für neue Ideen, Perspektiven und Freundschaften.

Leijmi lag die besondere Stärke der Delegationsreise darin, politische Prozesse unmittelbar erleben zu können: „Der direkte Austausch mit politischen Entscheidungsträger*innen sowie engagierten Teilnehmenden aus unterschiedlichen gesellschaftlichen Bereichen hat mein Verständnis für politische Beteiligung vertieft und mich darin bestärkt, eigene Perspektiven aktiv in gesellschaftliche und politische Diskussionen einzubringen."

Mehrfach wurden nicht die offiziellen Termine, sondern die informellen Momente der Reise als besonders bedeutsam beschrieben.

Wie würdest du die Delegationsreise in einem Wort beschreiben?

„(Politische) Relevanz."

NILS ALZNAUER

Bei gemeinsamen Abendessen, spontanen Diskussionen nach langen Tagen oder beim Karaokeabend wurden Gespräche weitergeführt, Eindrücke gemeinsam reflektiert und neue Ideen für die weitere Arbeit entwickelt.

Für Benedikt Kammergruber ergibt sich daraus eine klare Empfehlung: „Nutzt die Reise vor allem, um echte Beziehungen aufzubauen, und nicht nur, um Visitenkarten zu sammeln."

Mit zahlreichen neuen Eindrücken und Erfahrungen im Gepäck kehrten die Delegierten aus Berlin zurück. Geblieben ist vor allem die Erfahrung, dass politische Beteiligung nahbarer sein kann, als sie oft erscheint, und dass junge Perspektiven in diesen Debatten gehört werden wollen müssen.

Das Common Grounds Forum ist eine Community aus jungen Menschen zwischen 14 und 30 Jahren, die digitalpolitische Positionen entwickelt und Forderungen wirksam einbringt.
common-grounds-forum.org

Gut *gemeint*

FALLBEISPIEL Christina B. Class und Gudrun Schiedermeier

Sicherheitslücken frühzeitig erkennen und schließen klingt zunächst nach verantwortungsvoller IT-Sicherheit. Doch was passiert, wenn dabei Kundendaten und Quellcode ungefragt in externe KI-Systeme gelangen? Dieses Fallbeispiel zeigt, wie gut gemeinte Sicherheitsmaßnahmen neue Risiken und Verantwortungsfragen schaffen können.

Susanne und Emmer arbeiten in dem kleinen Start-up „PerfectIT", das sich auf IT-Sicherheit spezialisiert hat. Susanne galt schon während ihrer Studienzeit als respektable Häckse und hat damals bei einem Hochschulwettbewerb den ersten Platz gewonnen. Sie und Emmer kennen sich auch schon aus dieser Zeit. Emmer hatte sich damals aber geweigert, an dem seiner Meinung nach nicht ganz legalen Wettbewerb teilzunehmen. Aber auch er ist ein anerkannter Sicherheitsexperte und kennt sich bestens mit den Schwachstellen verschiedener Betriebssysteme und Browser aus.

Die Firma Bio.Erd.Shop hat in den letzten Jahren ihren Kundenstamm enorm ausgebaut. Ihr bewährtes Kunden-Informationssystem hält aber mit diesem Wachstum nicht mehr Schritt. Die Firmenleitung von Bio.Erd.Shop erteilt deshalb „PerfectIT" den Auftrag, das momentane System auf Aktualisierungsmöglichkeiten zu überprüfen. Lizzy, die Chefin von PerfectIT, ist eine gute Bekannte des Gründers von Bio.Erd.Shop. Sie möchte Bio.Erd.Shop unbedingt als Stammkunden gewinnen, da es sich um eine größere Firma handelt und damit Aufträge über Jahre für ihr kleines Unternehmen gesichert wären. Sie weist Emmer und Susanne daher an, zunächst in der Kunden-Software nach Sicherheitslücken zu suchen und diese zu analysieren. Lissy meint: „In so einer alten Software gibt es bestimmt einiges zu finden und das ist schließlich unser Kerngeschäft." Gleichzeitig sollen sie einen Patch zur Schließung dieser Lücken entwickeln. Selbstverständlich werden dem Kunden diese Schwachstellen in einem ausführlichen Bericht gemeldet und die Patches kostenlos zur Verfügung gestellt, um sich als qualifizierter und attraktiver Partner für Sicherheitsfragen zu präsentieren. Erst in einem zweiten Schritt sollen sie sich um die vom Kunden gewünschten Aktualisierungsmöglichkeiten kümmern, weil eine Erweiterung auf einer unsicheren Grundlage nicht sinnvoll wäre.

Susanne schlägt vor, ein KI-Tool zum Aufspüren von Sicherheitslücken zu verwenden. Ein neues KI-Modell zur Suche nach Schwachstellen hätte ja bei einer anderen Firma erstaunlich viele Sicherheitslücken gefunden, die sogar über Jahrzehnte unentdeckt waren.[1] Emmer ist dagegen skeptisch und weist Susanne darauf hin, dass ihr geplantes Vorgehen nicht den Wünschen des Kunden entspricht. Er hat ja keinen Auftrag erteilt, Schwachstellen in der Software zu finden. Zudem sieht er die Gefahr, dass Sicherheitslücken ausgenutzt werden könnten, sofern sie öffentlich bekannt werden und solange noch keine geeigneten Patches entwickelt und eingespielt wurden. Damit könnten sie die Firma Bio.Erd.Shop erheblich schädigen. Susanne weist die Vorwürfe zurück: „Du bist doch immer noch der gleiche Zauderer wie früher. Wer nicht wagt, der nicht gewinnt. Warum sollten wir kein KI-Tool nutzen? Bisher haben wir doch auch alle möglichen Tools wie Port-Scanner oder NetOrka benutzt und du hattest damit kein Problem. Außerdem sind wir doch fein raus. Uns kann niemand was anhaben. Wir führen doch nur den Auftrag ‚Ihrer Majestät' aus." Diesen Titel hat Susanne Lizzy gegeben, weil sie immer alles kontrollieren will und so erhaben tut.

Trotz seiner zögerlichen Haltung unterstützt Emmer Susanne bei der gestellten Aufgabe. Nachdem sie mit dem lokal betriebenen KI-Tool keine nennenswerten Sicherheitsprobleme finden konnten, verwenden sie ein neu erschienenes, hochgelobtes Tool

eines großen Tech-Konzerns. Mit geschickten, immer weiter verfeinerten Prompts, die Source Code enthalten, werden sie fündig. Sie informieren Lizzy darüber, auch darüber, dass sie noch keine Patches entwickelt haben. Dennoch informieren sie Bio.Erd.Shop in einem vorläufigen Bericht über die gefundenen Sicherheitslücken und kündigen Patches innerhalb der nächsten Wochen an. In dem Bericht sind auch Statistiken des KI-Tools aufgeführt, die das Risiko der Sicherheitslücken mit bekannten Sicherheitslücken vergleichen.

Aber Emmers schlimmste Befürchtungen werden wahr: Kurze Zeit später erhält Bio.Erd.Shop ein Erpresserschreiben, das diese Lücken benennt und sie veröffentlichen will, sollten keine Bitcoins fließen.

Der Kunde ist äußerst verärgert, zumal er keine Sicherheitsprüfung in Auftrag gegeben hat. Da er keinen Zugriff mehr auf sein von den Erpressern verschlüsseltes System hat, fordert er Schadensersatz und droht mit einer Anzeige. Lizzy ist sauer und will Anzeige gegen unbekannt erstatten. Zudem kündigt sie Susanne und Emmer Konsequenzen an, weil sie, gegen besseres Wissen, Source Code an ein externes KI-Unternehmen übermittelt haben. ⌶

[1] *https://www.heise.de/news/Mythos-von-Anthropic-Schwachstellen-KI-wirft-neue-Sicherheitsfragen-auf-11270831.html.*

Die Gewissensbits sind hypothetische, jedoch realistische Fallbeispiele. Mit ihnen will die Fachgruppe Informatik und Ethik einladen, über moralische und ethische Fragen rund um die Informatik nachzudenken und diese mit Freund*innen, Kolleg*innen oder Studierenden zu diskutieren. Meist gibt es auf diese Fragen keine einfachen Antworten – dazu sind die Fallbeispiele, wie auch die Realität, zu komplex. Im gemeinsamen Diskurs lässt sich aber üben, mögliche Probleme zu erkennen und als Gruppe zu einer Lösung zu gelangen: in einem demokratischen Aushandlungsprozess, wie er auch im Alltag erforderlich ist.

FRAGEN

Darf die Chefin ohne Rücksprache mit dem Kunden zuerst nach Sicherheitslücken suchen lassen?

Darf die Chefin Susanne und Emmer mit Konsequenzen drohen, obwohl sie ihnen den Auftrag erteilt hat, zunächst Sicherheitslücken zu finden?

Dürfen Susanne und Emmer ein externes KI-Tool nutzen, ohne die Erlaubnis von Lizzy und dem Kunden einzuholen?

Kann die Chefin selbst Probleme bekommen?

Hätte Emmer noch entschiedener auf die möglichen Gefahren hinweisen sollen?

Wie hätten Emmer und Susanne verhindern können, dass die gefundenen Sicherheitslücken veröffentlicht werden?

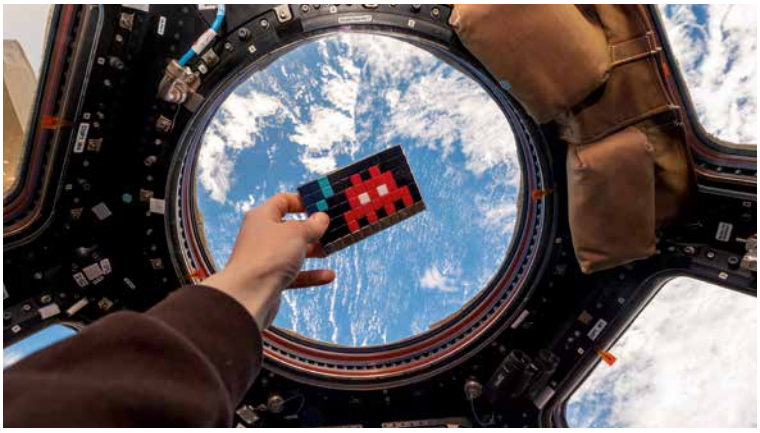
Welche Kriterien verbieten es, firmeninternes Material in ein extern betriebenes KI-Tool zur Analyse hochzuladen?

Welche Rolle spielt in diesem Kontext der sogenannte Hackerparagraph?

Wie würden Sie diese Fragen beantworten? Jetzt mitdiskutieren: *gewissensbits.gi.de*

Neues aus dem Nœrden
Der Nœrdman, ein Webcomic über Technik, Nerds und den Norden, ist fester Bestandteil der .inf-Redaktion. Ab sofort ist er übrigens auch als Bildband verfügbar. noerdman.de

Angriff der 8-Bit-Aliens



REZENSION Torsten Roeder

Aliens sind überall! Sie kleben an Hauswänden, verbergen sich in Straßenecken und beobachten uns aus bunten Pixelaugen. Lässt sich dem wilden Treiben Einhalt gebieten? Mit dem Smartphone können die Streetart-Invasoren eingefangen werden. Unser Autor hat sich auf die Jagd begeben.

Die Weltraummonster erkennt man oft schon von Weitem an ihrer pixeligen Gestalt und ihren tentakeligen Ärmchen und Antennen. Eines davon hat es sogar geschafft, sich in den Unicode-Standard einzuschmuggeln, und ist jetzt als Emoji 👾 auf nahezu allen digitalen Kommunikationsgeräten präsent. Im urbanen Raum jedoch treten sie oft in einen spielerischen Dialog mit ihrer Umgebung, wie etwa in Basel, wo ein riesiges Alien verstohlen zum Spielzeug Welten Museum hinüberlugt. Doch nicht alle sind auf den ersten Blick zu erkennen: Eines in Paris tarnt sich als Pablo Picasso, eines in Tokio als Hello Kitty. „Invader" nennt sich der Streetart-Künstler, der Figuren aus dem Arcade-Spiel „Space Invaders" von Taito aus dem Jahr 1978 als Pixelmosaike an Hauswände bringt. Seit den 1990ern ist Invader als Gehilfe der Außerirdischen aktiv, zunächst in Frankreich, bald international. Mittlerweile sind 4.283 Aliens dokumentiert – mindestens eines davon unter Wasser und eines sogar auf der ISS (angebracht mithilfe der italienischen Astronautin Samantha Cristoforetti). Die Zahl schwankt allerdings: Die Fliesenwerke verschwinden durch Verfall, Renovierung oder sogar Entwendung, wie es zur Kunst im öffentlichen Raum oft dazugehört. Aber Invader liefert stetig nach und mittlerweile gelten weltweit 87 Orte als befallen.

Seit mehr als zehn Jahren hilft die App Flashinvaders bei der Alienjagd, mit der sich Sichtungen ähnlich wie beim Geocaching loggen lassen. Ob es sich um einen echten Invader handelt, wird mittels einer Bilddatenbank und GPS-Koordinaten sichergestellt. Für den ersten Fund in jeder Stadt gibt es einen kleinen Bonus. Invader gamifiziert damit Kunst im urbanen Raum – und verwandelt die Stadt ganz nebenbei in ein global verteiltes Spielfeld. I

Mehr zum Streetart-Künstler „Invader"
inf.gi.de/spaceinvader

Bits, Bytes, *Botcast*

Schätzungsweise gibt es in Deutschland 100.000 aktive Podcasts. Klar, dass man da mal schnell den Überblick verliert. Wir wollten deshalb wissen, welche Podcasts die GI-Community hört. Egal ob True-Cybercrime, Interview-Format oder ein echter Kaffeeklatsch-Podcast – Hauptsache Informatik! Hier sind die besten Tipps für noch mehr Informatik auf die Ohren:

Auslegungssache

- Eingereicht von Uwe Brinkhoff via Mastodon

c't-Datenschutzpodcast

Bit-Rauschen

- Eingereicht von Markus Wamser und Uwe Brinkhoff via Mastodon

Talk über aktuelle Hardware-Themen von der c't

Bits und so

- Eingereicht von Stephan Wagner via Mastodon

Der wöchentliche Mac- und Gadget-Podcast von Timo Hetzel und Team

c't Uplink

- Eingereicht von Uwe Brinkhoff via Mastodon

Talk über aktuelle (Tech-)Themen

CRE: Technik, Kultur und Gesellschaft

- Eingereicht von Ch M[ae][iy]e?r via Mastodon

Interview-Podcast von Tim Pritlove

Die Sicherheits_Lücke

- Eingereicht von Kai Hendrik Wohnert und Marieke Petersen per Mail

„Das ist ein lockerer Podcast über Cybersecurity-Themen mit Interviews, Themenserien und hin und wieder auch Live-Events." – Kai Hendrik Wohnert

„Einblicke in Cybersicherheit, von Experten für alle." – Marieke Petersen

Eigenraum

- Eingereicht via LinkedIn von Dr.-Ing. Lea Schönberger

Der Mathematikpodcast von Prof. Dr. Thomas Kahle von der Uni Magdeburg

Engkiosk

- Eingereicht von Michael Dorner via Mastodon

Wöchentlicher Podcast über Engineering, Tech, Open Source und die Menschen, die sich damit beschäftigen

EPDS On Air – TechSonar

- Eingereicht von Ch M[ae][iy]e?r via Mastodon
  Der offizielle Podcast-Kanal des Europäischen Datenschutzbeauftragten

„Insbesondere die Folge: TechSonar: The 'illusion of education' with a personalised learning"

Haken dran

- Eingereicht von Uwe Brinkhoff via Mastodon

Der Social-Media-Podcast der c't

Informatik für die moderne Hausfrau

- Eingereicht von Denise Schmitz via LinkedIn

Podcast von Dr.-Ing. Lea Schönberger, mit und über Frauen in der Informatik

Internet Explorers

- Eingereicht von dersven.md via Mastodon

Hier wird die unsichtbare Netzinfrastruktur hörbar gemacht.

KI verstehen

- Eingereicht von Sven Lubenau

KI-Podcast vom Deutschlandfunk

Linux-Magazin-Podcast

- Eingereicht von Markus Klie via Mail
  Podcast des Linux-Magazins

Linuxmatters

- Eingereicht von Markus Wamser

Podcast von Alan Pope, Mark Jonson und Martin Wimpress zu allem, was auf Linux läuft

Logbuch: Netzpolitik

- Eingereicht von Oemmes und Klaus via Mastodon, sowie von Marieke Petersen per Mail

„Wahrscheinlich inzwischen ein Klassiker für Netzpolitik. Die beiden Hosts und Moderatoren gehen auf aktuelle politische und gesellschaftliche Entwicklungen in der Cybersicherheit und Digitalpolitik ein." – Marieke Petersen

Passwort

- Eingereicht von Uwe Brinkhoff via Mastodon

IT-Security-Podcast von der c't

Per Anhalter durch den Cyberraum

- Eingereicht von Uwe Brinkhoff via Mastodon

Podcast der Cyberagentur zur Cybersicherheitsforschung

Podcast Software Testing

- Eingereicht von Karin Vosseberg via LinkedIn

„Immer wieder spannende Einblicke in die Welt der Qualitätssicherung" – Karin Vosseberg

Schlüsseltechnologie

- Eingereicht von Markus Wamser via Mastodon

Computertechnik, von Grund auf erklärt

They Talk Tech

- Eingereicht von Uwe Brinkhoff, Markus Wamser und Klaus via Mastodon

Tech-Themen mit Svea Eckert und Eva Wolfnagel und vielseitigen Perspektiven von Frauen aus der Branche.

Update verfügbar

- Eingereicht von Uwe Brinkhoff via Mastodon

Podcast zu Digitalisierung, Cybercrime und Zukunftstechnologien vom BSI

Ohren gespitzt?
Zu hören sind die Podcasts auf den gängigen Plattformen oder gesammelt hier:
inf.gi.de/bitsbytesbotcasts

Ein Film, 20 Fragen

Lust auf eine Challenge bei der nächsten langen Zugfahrt? 1.212.276 Filme verzeichnet das Portal Letterboxd. Mit nur 20 Ja-Nein-Fragen soll es möglich sein, herauszufinden, welcher davon gesucht wird. Ob das wirklich stimmt und was das Ganze mit Informatik zu tun hat, erklärt Benjamin Paaßen, Junior-Fellow der GI.

Die Spielregeln sind schnell erklärt: Ich suche mir einen Film aus, ihr müsst mit maximal 20 Ja-Nein-Fragen herausbekommen, welchen ich im Kopf habe. Mit jeder Frage müsst ihr also möglichst viele falsche Filme ausschließen – bis nur noch der richtige Film übrig bleibt. Wie geht das? Mit Informatik natürlich. Nehmen wir an, gesucht wird der Film „Hackers – im Netz des FBI" (1995). Wenn wir direkt mit einer guten Frage einsteigen, können wir die Anzahl der infrage kommenden Filme schon halbieren. Zum Beispiel: Ist der Film vor 2013 erschienen? Die Antwort wäre in diesem Film „Ja" und wir hätten schon die Hälfte aller möglichen Filme ausgeschlossen. Denn laut der Filmdatenbank IMDb sind ungefähr genauso viele Filme vor 2013 erschienen als danach. Spannend, oder?

Wenn wir mit der nächsten Frage von den verbliebenen Filmen (also denen vor 2013) noch mal die Hälfte ausschließen können, bleibt nur noch ein Viertel der Filme übrig, dann ein Achtel, ein Sechzehntel und so weiter. Nach 20 Fragen landen wir bei nur noch einem 2^{20}-tel, oder anders gesagt einem 1.048.576-tel aller Filme – gerade genug, um mit ziemlicher Sicherheit aus allen möglichen Filmen den richtigen zu finden.

Der Prozess, der hinter diesem Spiel steckt, heißt binäre Suche und ist ungemein effizient – exponentiell effizient, um genau zu sein. Er ist eines der wichtigsten Prinzipien hinter effizienten Suchalgorithmen. Noch etwas nerdiger gesagt: Mit jeder Frage bekomme ich ein Bit an Information (eine 0 bei „Nein", eine 1 bei „Ja"). 20 Fragen sind also 20 Bit oder etwas weniger als drei Byte. Und so wenig Speicherplatz reicht schon, um jeden Film der Welt eindeutig zu kodieren! I

Wer jetzt Informatik nicht zumindest ein bisschen cool findet, der*dem kann ich auch nicht helfen.

Überfragt?
Wie viele Ja-Nein-Fragen habt ihr gebraucht, um zum richtigen Film zu kommen? Und welche waren besonders gut, um die Auswahl zu verkleinern? Eine erste Auswahl findet ihr online: : *inf.gi.de/20fragen*

GESELLSCHAFT
FÜR INFORMATIK

MITGLIEDERMAGAZIN DER
GESELLSCHAFT FÜR INFORMATIK E. V.
NR. 14

HERAUSGABE
Gesellschaft für Informatik e.V. (GI)
Weydingerstraße 14–16, 10178 Berlin
Telefon +49 30 240 09-805

VERANTWORTLICH IM SINNE
DES PRESSERECHTS
Cornelia Winter

REDAKTION
Alexandra Resch (Ltg.), Cornelia Winter,
Michael Koch, Paul Reinelt, Nuri Grenz,
Marieke Petersen, Wiebke Dönnebrink,
Helen Zotz

AUTOR*INNEN
Martin Wolf, Nuri Grenz, Paul Reinelt,
Marieke Petersen, Simeon Hoffmann,
Florian Hantke, Tim Philipp Schäfers,
Linus Neumann, Tobias Eggendorfer,
Florian Deusch, Kirsten Matheus,
Ayten Öksüz, Judith Faust, Tassilo Thieme,
Christine Hennig, Karolin Kappler,
Ina Schieferdecker, Nicole Wolf,
Stella Drebber, Nikolas Becker,
Christina B. Class, Gudrun Schiedermeier,
Lea Hildermeier, Luca Randecker,
Torsten Roeder, Benjamin Paaßen

FACHBEIRAT
Tanja Döring, Oliver Günther,
Dominik Herrmann, Christof Leng,
Friedmann Mattern, Judith Michael,
Andreas Oberweis, Edy Portmann,
Ralf Reussner, Stefanie Rinderle-Ma,
Ute Schmid, Dirk Taubner,
Wolfram Wingerath

GESTALTUNG, SATZ UND GRAFIK
Sven Lubenau (Ltg.), Lucas Crisólogo Oña

LEKTORAT
Dr. phil. Birgit Gottschalk

DRUCK
Klimaneutral gedruckt
auf Recyclingpapier bei
Spreedruck GmbH, Berlin

STAND
Juli 2026

BILDNACHWEISE
Cover, S. 4,12: Sven Lubenau/GenAI, S. 3, 6: Mike Auerbach, S. 5 oben, 11: Kostas Topalidis, Emiliano Vittoriosi, S. 5 mitte, 20: Rens Dimmendaal & Johann Siemens, S. 8: Rawpixel.com/Shutterstock, S. 17: Lucas Crisólogo Oña, S. 22: CC by Epoch.ai, S. 24: Resource Database/Unsplash, S. 26–29: Luca Randecker, S. 32: Jannis Stoppe & Rolf Drechsler, © ESA/NASA, S. 34: Mykhailo Baidala/Shutterstock

ISSN (Print) 2940-0694
ISSN (Online) 2940-0708

KONTAKT
Wir freuen uns immer über Feedback, Anregungen und Ideen: Unter *redaktion@gi.de* können Sie uns diese zukommen lassen und auf Wunsch auch weitere Hefte bestellen.

/mas.to/@informatik
@informatik.bsky.social
/company/gesellschaft-fuer-informatik

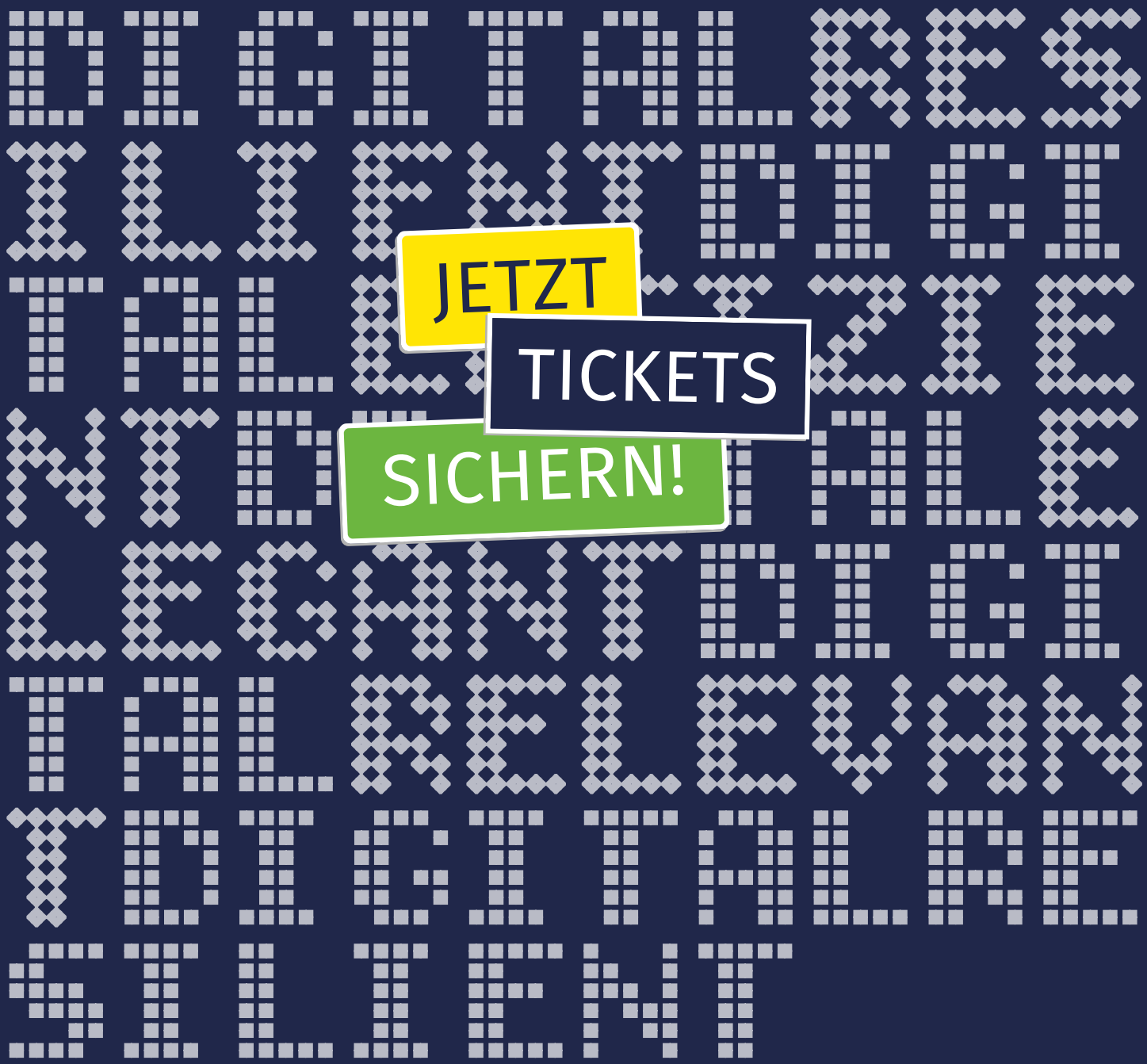
Sie lesen lieber digital?
Alle Ausgaben finden Sie auch frei zugänglich auf *inf.gi.de*.

Ihnen gefällt, was Sie in der Hand haben?
Bestellen Sie die Printversion der .inf im Mitgliederbereich!

56. JAHRESTAGUNG DER GESELLSCHAFT FÜR INFORMATIK

Technische Universität Dresden

GESELLSCHAFT FÜR INFORMATIK



Das INFORMATIK FESTIVAL 2026 bringt die Informatik-Community in Dresden zusammen. In zahlreichen Workshops, Keynotes und Paneldiskussionen geht es um digitale Resilienz und all die Fragen, die sie mit sich bringt. Garantiert genug Gesprächsstoff für das Community Dinner, den Networking-Kaffee zwischendurch oder die GI Festival Night, kuratiert durch die Junge GI.

INFORMATIK FESTIVAL 26

22.—25. SEPTEMBER 2026

INFORMATIK2026.DE