

„Update Verfügbar – ein Podcast des BSI“

Transkription für Folge 33, 31.07.2023:

Künstliche Intelligenz – Was es ist, was es kann und wo es hingeht

Moderation: Ute Lange, Michael Münz

Gast: Christian Temath

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)



Ute Lange AI: Hallo und herzlich willkommen zu einer neuen Folge von Update Verfügbar, dem Podcast für Sicherheit im digitalen Alltag. Mein Name ist Ute lange.

Michael Münz AI: Und ich bin Michael Münz, und in dieser Folge gehts um ein Thema, das gerade intensiv diskutiert wird. Ich bin schon sehr neugierig. Es gibt viel zu besprechen und bin sicher, das wird ein weiteres erkenntnisreiches Gespräch.

Ute Lange: Das klang aber komisch, Michael, oder?

Michael Münz: Ja, das klang komisch, das klang irgendwie nach uns, aber irgendwie auch nicht.

Ute Lange: Ja, damit hast du das, was wir jetzt alle gerade gehört haben, ganz gut beschrieben, denn das war eine Computerstimme, die zuvor mit Sprachbeispielen von uns beiden gefüttert worden ist.

Michael Münz: Vielleicht, liebe Hörerinnen und Hörer, erinnert ihr euch noch an die Deep Fake Folge aus dem Juli 2022, da waren gerade die Fake-Videocalls von Vitali Klitschko Thema, und da hatten wir Markus Ullmann vom BSI in der Folge, der uns das Thema Deep Fakes eingeordnet hat, und bei dem Gespräch mit Marcus entstand auch die Idee, dass Markus und sein Team Ute und mich künstlich nachbauen könnten.

Ute Lange: Ja, und das haben sie stimmtechnisch auch gemacht, denn das Ergebnis habt ihr gerade gehört. Markus und seine Kolleginnen haben einer Software beigebracht, so zu klingen wie wir. Dann haben sie das ganze aber noch mit einem Update versehen und haben die Stimmen auch noch getauscht.

Michael Münz: Und haben mich beeindruckt und erschüttert, zugleich also beeindruckt, weil ich schon finde, dass es nach uns klingt und dass ja auch noch so die Charakteristiken unserer Sprachen mit drin sind. Und gleichzeitig bin ich erschüttert, weil mich dieser Stimmtausch verwirrt, und wenn ich mir dann noch vorstelle, der Enkeltrick oder der CEO Fraud werden damit noch besser, dann kriege ich schon so ein bisschen so ein mulmiges Gefühl.

Ute Lange: Ja, und genau über diese neuen Dimensionen wollen wir heute sprechen. Was kann man mit künstlicher Intelligenz, kurz KI, schon alles machen? Wozu kann man dann diese Methoden nutzen, und damit starten wir jetzt so wie sonst ganz gewohnt. Hallo und herzlich willkommen zu dieser Folge von Update Verfügbar, dem Podcast für Sicherheit im digitalen Alltag von und mit der einzig wahren Ute.

Michael Münz: Und dem einzig wahren Michael und einem Experten, der uns erklärt, wo wir schon überall künstliche Intelligenz begegnen, was die so macht, und auch, wie wir vielleicht erkennen, dass wir mit künstlicher Intelligenz zu tun haben.

Ute Lange: Ja, und natürlich wollen wir auch wissen, wo im digitalen Alltag Gefahren durch künstliche Intelligenz, auf uns lauern und wie genau diese künstliche Intelligenz uns vielleicht auch davor schützen kann. Deswegen freuen wir uns sehr, dass heute bei uns ist, Christian Temath, Geschäftsführer von der zentralen Kompetenzplattform für künstliche Intelligenz in Nordrhein-Westfalen.

Christian Temath: Hallo.

Michael Münz: Hallo Christian, schön, dass du da bist und dir Zeit für unsere Fragen nimmst, und ich bin mir sicher, wir stellen die heute auch wieder stellvertretend für unsere Hörerinnen und Hörer, die sicherlich auch viele Nachfragen haben zum Thema künstliche Intelligenz. Da reden ja gerade sehr viele Menschen darüber. Bevor wir aber starten, erkläre es doch noch einmal kurz, was KI-NRW ist und was genau deine Aufgabe dort ist.

Christian Temath: Ja, lieber Michael, liebe Ute, vielen Dank, dass ich dabei sein darf. Wie ihr schon gesagt habt, ich bin Christian Temath, Geschäftsführer bei KI-NRW, das ist die vom Land NRW geförderte Kompetenzplattform für künstliche Intelligenz in Nordrhein-Westfalen, und wir sind angesiedelt am Fraunhofer IAIS in St. Augustin, was eins der größten Forschungsinstitute für angewandte künstliche Intelligenz ist in Europa, und das bringt uns auch relativ schnell zu unserem Ziel von KI-NRW. Wir wollen mit Nordrhein-Westfalen, in der Champions-League für angewandte künstliche Intelligenz spielen. Was heißt das dann konkret für uns? Wir wollen auf der einen Seite Sichtbarkeit schaffen, Sichtbarkeit für Technologie Themen im Bereich der KI, wo sie wirtschaftlich und gesellschaftlich relevante Themen besetzt und in Anwendung gebracht wird. Dazu paar Projekte, dazu kommen wir vielleicht später auch noch mal, und ansonsten bieten wir ganz dedizierte Angebote auch für kleinere mittelständische Unternehmen, um ihre KI-Reise zu begleiten, durch Informationsangebote, durch Workshopformate, durch Sprechstunden und so weiter. In Summe wollen wir einfach das gesamte KI- Ökosystem in Nordrhein-Westfalen gemeinsam stärken.

Ute Lange: Ja, schön, dass du da bist. Wir haben auch eine ganze Reihe von Fragen mitgebracht, auch von Hörern und Hörerinnen, die sich bei uns melden können. Wir haben den Eindruck, dass in der öffentlichen Diskussion gerade so ein paar Begriffe auch durcheinander gehen. Vielleicht können wir anfangs erst nochmal klären, was ist künstliche

Intelligenz und wie grenzt es sich von anderen Begriffen ab, zum Beispiel Deep Learning oder so? Kannst du das nochmal auseinander puzzlen, bevor wir dann einsteigen?

Christian Temath: Ja, sehr gerne, ich glaube, das Thema künstliche Intelligenz, die Begrifflichkeit ist tatsächlich immer so ein bisschen kontrovers und ein bisschen unklar. Es gibt eine Definition, die ich gerne bemühe, die ist von Professor John McCarthy, die er in den 50er-Jahren bemüht hat, und da hat er gesagt, KI ist das science and engineering of making intelligent machines. Das heißt, wir Menschen machen einen Computer, eine Maschine für irgendeine Tätigkeit intelligent, und das fängt dann tatsächlich bei so relativ simplen Sachen an, in dieser weiten Definition, dass man deterministisch sagt, es gibt irgendwelche Regeln, es gibt irgendwie Daten, Input und eine Maschine, ein Algorithmus sagt links oder rechts, wie zum Beispiel eine Ampelschaltung. Das ist in irgendeiner Art und Weise auch schon künstlich intelligent. Wenn man da keine Polizistin oder keine Polizisten hinstellen muss, was in den letzten Jahren deutlich stärker geworden ist, ist das maschinelle Lernen, was in Teilgebieten der künstlichen Intelligenz ist, wo es sehr viel stärker darum geht, das mit sehr, sehr vielen Datenmengen, wo wir dem Computer sagen, das sind irgendwelche Merkmale, zum Beispiel bei Lilien, das ist die Kelchblatt Länge, das ist die Blütenblatt Länge und irgendwelche anderen Merkmale, dass man sagt, daraus kannst du erkennen, dass es genau diese Lilie ist, und dann wird das mit ganz viel Datenmaterial eingelernt, und am Ende des Tages kann dann, wenn man der Machine Learning KI sagt, das sind die Werte von einer Kelchblatt Länge oder Blütenblatt Länge, kann das dann selbst klassifizieren. Ist es diese Lilie oder ist das eine andere Lilie, und was sehr, sehr große Fortschritte gemacht hat, insbesondere jetzt auch im Bereich der Sprachverarbeitung, also Texte generieren, auch Sprache verstehen, ist das Thema Deep Learning, denn da geht es um tiefe neuronale Netze. Die neuronalen Netze sind angelehnt an das menschliche Gehirn, da gibt es dann Neuronen, und die haben dann Verbindungen zu anderen Neuronen. Und diese tiefe neuronalen Netze haben ganz, ganz viele tiefe Schichten, ganz, ganz viele Neuronen, und den hat man ganz viele Daten und ganz viel Trainingsaufwand dann beigebracht. Zum Beispiel, auf diesem Bild ist eine Katze, und auf diesem Bild ist ein Hund, und das faszinierende beim Deep Learning ist, dass wir als Menschen beim Programmieren gar nicht mal gesagt haben, das sind die Merkmale, auf die du achten sollst, sondern dass darin identifiziert für sich selber, was die Merkmale sind, woran sie erkennt, ob auf einem Bild eine Katze oder ein Hund ist, und das macht für uns ein bisschen weniger nachvollziehbar, was da passiert. Aber das macht diese Tools auch so effektiv, weil die dann verbessert für sich verstehen können, wie sie dann diese Bilder interpretieren müssen.

Michael Münz: Das heißt, da passieren gerade Sachen, von denen wir nicht wissen, warum sie passieren. Habe ich dich da richtig verstanden?

Christian Temath: Es ist so, dass wir grundsätzlich technisch schon verstehen, wie diese neuronalen Netze funktionieren. Das sind am Ende ganz große Matrizenmultiplikationen, die am Ende stattfinden. Also wer sich noch an seine Schulzeit zurückerinnert und Matrizenmultiplikation in Mathe, viel mehr als das passiert tatsächlich in seinem neuronalen Netz nicht. Aber weil diese tiefen neuronalen Netze so groß sind und so viele Parameter haben,

bei den großen neuronalen Netzen sprechen wir von über 100 Milliarden Parametern, ist im Einzelfall nicht mehr genau nachvollziehbar, welcher Parameter denn jetzt für welche Entscheidung verantwortlich ist, und das macht es schon schwieriger nachzuvollziehen. Da spricht man auch gerne mal von einer Blackbox.

Michael Münz: Und ist es diese Blackbox, die dazu führt, dass alle gerade über künstliche Intelligenz sprechen? Also diese Ungewissheit? Ist das der Grund, warum wir jetzt auf einmal, seit sechs Monaten gefühlt täglich über neue Entwicklungen bei sprechen?

Christian Temath: Also, ich glaube, was tatsächlich den ganzen Thema nochmal massiv Schuh verliehen hat, ist das Thema Chat-GPT: In dem ganzen Jahr 2022 war so, dass ganz, ganz viele Berichte über wie kann man aus Texten Bilder generieren passiert sind. Das hat mich eigentlich bis zum November sehr, sehr stark bewegt, das war sehr faszinierend, blieb aber noch ein bisschen auf einem Level. Was so für die Nerds, für die Leute, die sich intensiv mit dem Thema beschäftigen, über war. Chat-GPT hat eine Sache gemacht. Die haben eine extreme Zugänglichkeit zu einem Sprachmodell geschaffen über diese Chat Funktionalität und dadurch, das Chat-GPT tatsächlich in der Lage ist, in richtige Dialoge einzusteigen und richtig eloquent und zugängliche Antworten zu geben, und das war ein schönes Web-Tool, das hat Antworten gegeben, da konnten Leute mit Rumspielen, das war noch umsonst, und das hat dazu geführt, dass innerhalb von fünf Tagen 1 Million Nutzer sich in dem Tool angemeldet haben und unheimlich viel darüber auch berichtet haben. In Social Media wurden dann Dialoge gepostet, das wurde in die Presse aufgenommen und so weiter, und ich glaube, das hat dazu geführt, dass auf einmal das Thema so greifbar wurde, weil auf einmal eine Maschine mit uns auf einem Level gesprochen hat, den wir als sehr, sehr angenehm und sehr, sehr menschlich empfunden haben.

Ute Lange: Du sprichst ein Thema an, was uns natürlich auch beschäftigt. Michael und ich sind ja im Beruf auch Journalist und Journalistin, und wir begegnen natürlich jetzt mit einer gewissen Skepsis den Texten. Sind das tatsächlich von Menschen geschriebene oder sind es von Maschinen? Es gibt aber auch Vorteile, wenn die Maschine einem helfen kann. Erzähl doch mal, wo du dir von KI im Alltag helfen lässt und was für dich Vorteile sind.

Christian Temath: Also, ich nutze tatsächlich KI sehr, sehr stark im, ich sage mal, persönlichen Umfeld. Ein großes Thema, also die Spracherkennung, dass ich tatsächlich meinem Handy oder auch meiner Smartwatch sage, hier ich möchte gerne das Licht ein und ausschalten, und ich weiß jetzt nicht, wie alt die Zuhörerschaft hier ist. Aber ich weiß noch, dass ich früher über den Schulhof gelaufen bin vor 20 Jahren, und ich mit meiner Uhr gesprochen habe. Da gab es ja diese Fernsehserie mit dem Mann, mit der Lederjacke und dem schwarzen Auto, der gerne mit seiner Uhr gesprochen hat. Da haben die Leute über einen gelacht. Heute lacht keiner mehr, wenn jemand mit seiner Smartwatch redet und sagt: Siri, Alexa, wie auch immer, bitte schalte das Licht an oder bitte spiel mir dieses Lied ab. Das mache ich tatsächlich sehr regelmäßig. Ich nutze das zum Beispiel auch in Kontexten wie Bilderkennung, dass ich diese Fotoalben vorsortiert bekomme. Welche Personen sind denn da drauf und so weiter, weil es

mir einfach hilft, natürlich besser zu finden. Wo sind denn dann die relevanten Fotos? Aber tatsächlich sehr, sehr stark im Bereich der persönlichen kleinen Helferlein.

Michael Münz: Und gibt es auch Bereiche, wo du jetzt schon weißt? Da lasse ich die niemals reingucken.

Christian Temath: Ob es Bereiche gibt, wo ich sie niemals reingucken lassen werde, das traue ich mich nicht mehr zu sagen, seitdem die Entwicklung bei einer KI so schnell geworden ist. Was ich sagen kann, ist, ich bin sehr, sehr vorsichtig geworden und schon immer gewesen, wenn es darum geht, Daten, persönliche Daten von mir oder von meinen Kindern freizugeben, preiszugeben, in irgendwelche Systeme einzuspielen. Also ich würde jetzt zum Beispiel niemals auf die Idee kommen, private Daten von mir in Chat-GPT reinzuschreiben, die mir wichtig sind, oder auch Firmendaten reinzumachen oder Bilder von mir hochzuladen, um die anpassen zu lassen, weil, was einmal im Internet ist, klassischerweise auch da und geht nicht mehr weg, und deswegen bin ich da sehr vorsichtig.

Michael Münz: Ich gebe ja zu, dass ich mich an so ein paar Anwendungsfälle schon sehr gewöhnt habe. Übersetzungen zum Beispiel, von einer Sprache in die andere finde ich mittlerweile total komfortabel. Ich kopiere was in der einen Sprache rein, kopiere es aus der anderen Sprache wieder raus, redigiere das noch und habe dadurch einfach sehr viel Zeit gewonnen, die ich dann für andere Dinge nutzen kann. Also das, da kann ich sagen, das ist auf jeden Fall ein Fall, wo ich weiß, da ist eine KI und die hilft mir auch. Gibt es denn auch noch so andere Anwendungsbeispiele, wo wir als Nutzende im Netz künstlicher Intelligenz begegnen, wo es vielleicht noch nicht ganz so offensichtlich ist, dass dahinter so ein System liegt, über das wir gerade sprechen?

Christian Temath: Ja, also grundsätzlich im Leben begegnet uns natürlich KI an vielen Stellen, jetzt im Netz sicherlich auch bei Empfehlungsalgorithmen. Da wird ja auch sehr, sehr viel Datenmengen gearbeitet und welche Serien Leuten gut gefallen haben und so weiter. Also die ganzen Streaming Dienste, Netflix und so weiter arbeiten sehr, sehr stark mit basierten Empfehlung, Systematiken. Wir haben auch sehr, sehr gute Beispiele, die sich jetzt im Bereich der Produktion beschäftigen: Touren-Optimierung, also wenn ich jetzt mir Pakete ausliefern lassen, auch da werden sicherlich im Hintergrund KI-basierte Optimierungsalgorithmen laufen um dann die Tourenwege zu verkürzen, um in idealer Weise natürlich auch Sprit zu sparen dabei. Diese Themen finden aus meiner Sicht sehr, sehr häufig noch im Hintergrund statt. Auf der anderen Seite vielleicht als kleine Anmerkung, wir haben ja die KI-Welten, wir haben auf unserer Webseite, da haben wir ein unheimlich großen Fundus an Themen, wo tatsächlich im Unternehmen oder zu Hause KI schon stattfindet, und es ist erstaunlich, an welchen Stellen überall irgendwo schon KI versteckt ist und uns doch den Alltag leichter macht.

Ute Lange: Du hast mir gerade ein wunderbares Stichwort genannt: die KI-Welten bei euch auf der Webseite. Wir haben natürlich auch ein bisschen geschaut und uns schlau gemacht. An welchen Projekten arbeitet ihr denn bei KI-NRW insgesamt, um KI im Lebensalltag zu

integrieren oder zu prüfen? Sind diese Applikationen vielleicht zukunftsfähig oder schon da? Kannst du uns da ein paar Beispiele nennen, die auch unsere Hörer und Hörerinnen nachvollziehen können und vielleicht für sich dann anwenden wollen.

Christian Temath: Genau wir haben auf der einen Seite, und ich glaube, das ist ein sehr, sehr spannendes Umfeld. Ich spreche davon, dass wir diese KI-NRW Flagship Projekte haben, wo wir zusammen mit Konsortium aus Forschung, Anwendungsunternehmen und Technologieunternehmen schauen, wo können wir KI konkret in die Anwendung bringen? Da gibt es zum Beispiel das eine Thema Datenfabrik NRW, wo geguckt wird, wie können wir eine datenbasierte, eine KI basierte Produktionslogik aufbauen, die dann idealerweise zur Losgröße eins hilft? Bei Glas und zum Beispiel CargoBold, so das sind die Anwendungsunternehmen. Die für mich sehr, sehr spannende Anwendungsfelder sind im Bereich der Medizin. Da haben wir den Innovativ Secure Medical Campus an der Uni Bonn oder das Smart Hospital NRW an dem Uni-Klinikum Essen, wo es wirklich darum geht. Wie kann man eigentlich die Patientinnen-Reise mit KI-Helferlein digitaler und besser gestalten und zum Thema Lebensalltag integrieren? Da finde ich das Zitat von einem der Professoren vom Uni-Klinikum Essen sehr, sehr spannend, der sagte bei der Präsentation der Use Cases, einmal klingt verrückt, aber mit Technologie, mit KI wollen wir die Medizin wieder menschlicher machen, und womit hat er das begründet? Ich bin den ganzen Tag mit irgendwelchen administrativen Sachen beschäftigten, ganz viel Monitoren und so weiter, und ich bin ja Radiologe. Ich möchte ja den Patientinnen helfen, und wenn mir die KI-Helferlein diese Last abnehmen oder reduzieren, dann kann ich mich wieder darum kümmern, wofür ich mal Arzt geworden bin, um die Patientinnen, und das finde ich eigentlich sehr, sehr spannend, diesen Blick darauf zu nehmen. Wie können wir die für uns nutzen, dass wir unser Leben angenehmer machen, oder den Patientinnen und anderen Leuten besser helfen?

Ute Lange: Das heißt also, in dem konkreten medizinischen Fall würde dann die KI den Arztbericht schreiben oder andere Sachen tun, die dem Arzt oder der Ärztin halt Zeit weg von der Patientenbetreuung nehmen.

Christian Temath: Genau also, der Arztbrief ist zum Beispiel einer der Anwendungsfälle. Da muss man ja aus den Diagnosen und verschiedenen anderen Berichten und Laborwerten schauen, muss man dann einen Arztbrief generieren, und die KI sorgt dafür, dass die relevanten Informationen dann schon mal vorgefertigt, in einem Dokument zusammengefasst werden, und dann guckt dann der Arzt oder die Ärztin drüber und prüft dann, ob das alles korrekt ist, und stellt dann den finalen Brief. Aber dieses zusammensammeln, diese mühsame Arbeit, teilweise früher Papier basiert, das sind die KI dann einmal.

Michael Münz: So einen vergleichbaren Fall oder vergleichbare Anwendungsfälle sehe ich zum Beispiel auch bei Journalismus. Also es gibt ja Nachrichtentypen, die relativ standardisiert sind, Sport oder Wetter zum Beispiel, wo es ja eigentlich auch nur darum geht, bestimmte Variablen für ein A oder B Ergebnis Tabellenplatz vorher, nachher ein und so weiter und so fort, oder auch beim Wetter: Temperatur ist höher oder niedriger als am Vortag. Das könnte man ja auch

alles von Maschinen schreiben lassen, die man mit den entsprechenden Daten und auch den Baustein füttert, ich frage mich dann an der Stelle, ob es dann für Journalistinnen und Journalisten oder auch für Medizinerinnen und Mediziner dann eigentlich auch geboten wäre, zu signalisieren, dass das kein Mensch mehr gemacht hat oder dass Menschen mitgeholfen haben. Wie transparent sollten wir sein bei der Anwendung von künstlicher Intelligenz?

Christian Temath: Ich glaube, du sprichst ein ganz, ganz wichtiges Thema an, und das ist das ganze Thema Vertrauenswürdigkeit oder Vertrauen in die Technologie, und wir sehen natürlich auch in den Diskussionen, die wir aktuell haben, dass viele Leute sehr, sehr begeistert und fasziniert von den technologischen Möglichkeiten sind. Aber auf der anderen Seite, und das habt ihr am Anfang ja sehr, sehr klar gesagt, auch ein bisschen Sorge haben, ein bisschen sorgenvoll drauf schauen. Was kann denn so eine KI schon, und ist das wirklich gut, was hier passiert. Und vor dem Hintergrund sind wir auch sehr, sehr froh, dass wir in Nordrhein-Westfalen schon seit Jahren an dem Thema zertifizierte KI-Arbeiten. Also wie kann man vertrauenswürdige KI Systeme aufbauen, wie kann man die auch prüfen entsprechender Kategorien? Da wurde jetzt ein Prüfkatalog mal veröffentlicht, wir arbeiten jetzt an Prüfwerkzeugen im entsprechenden Projekt, wo dann wirklich geschaut wird, wie können wir auch nachweisen gegenüber der Öffentlichkeit und der Gesellschaft, diese KI Systeme haben eine Vertrauenswürdigkeit, und ich glaube, das ist ein Thema, was sehr, sehr wichtig ist und was, glaube ich, auch die Leute dazu bewegen wird, das Thema KI mit einer positiven Grundeinstellung anzunehmen. Das Thema Kennzeichnung ist ja eine der Themen, was auch bei dem EU AI Act sehr intensiv diskutiert wird, dass KI generierte Inhalte gekennzeichnet werden sollen. Das, glaube ich, wird sehr, sehr wichtig sein, dass dem so ist. Was mich persönlich sehr, sehr erfreut hat, war. Ich war kürzlich auf einer Webseite, und dann war in Klammern unten hinter dem Artikel das Kürzel von dem Autor, und da stand KI, da habe ich mal geguckt, und da war es tatsächlich so, dass die Redaktion sich selber einen Leitfaden gegeben hatte, wie sie mit KI generierten Inhalten umgeht, und da steht ganz klar drin, wenn die KI genutzt worden ist, um bei der Generierung zu unterstützen, wird das mit KI gekennzeichnet. Es ist auch gleichzeitig so, dass die generellen Inhalte noch einmal oder zweimal von Redakteurinnen oder Redakteure gegengelesen werden und dann freigegeben werden, und das finde ich insofern gut und wichtig, dass das auch selber passiert, dass das nicht irgendwas ist, was vorgeben muss, dass Leute auch im Journalismus sagen oder in anderen Bereichen. Uns ist wichtig, dass wir unsere Systeme entsprechend kennzeichnen und wie wir damit umgehen.

Michael Münz: Jetzt haben Ute und ich ja zu Beginn schon ein bisschen eingeläutet das Thema digitale Sicherheit und so ein paar der Methoden, die wir auch im Podcast immer mal wieder besprechen. Also, der CEO Fraud ist ja so ein Ding. Man kriegt halt eine Mail. Da steht drin, lieber Kollege, überweisen sie mir 10000 € aufs Konto. Vielen dank bis Montag! Wir haben wir jetzt ja alle gelernt. Ich guck noch mal, ob die E-Mail, die er hat stimmt, und kann das überhaupt sein, dass der Chef geschrieben hat? Wenn ich jetzt aber einen Anruf kriege und ich

die Stimme höre, die von so einer KI gemacht worden ist, macht das die Welt nicht auch ein bisschen unsicherer?

Christian Temath: Das macht sicherlich die Welt an der Stelle unsicherer, und das ist ein Thema, wo wir, glaube ich, in Summe noch viel mehr sensibilisiert werden müssen, welche Möglichkeiten tatsächlich in der KI stecken. Also dieses Beispiel, was du gerade beschreibst, wurde mir tatsächlich vor einem Jahr schon zugespielt. Da waren da ganze Hype um Chat-GPT noch gar nicht da, dass jetzt ein Anruf passiert und gesagt wird, hier, du musst mir jetzt Geld überweisen. Ich bin gerade am Flughafen und dann wirklich abgestimmt, 30 Sekunden später die E-Mail dann im Posteingang ist, und wenn man nicht darauf vorbereitet ist, zu sagen, ich gucke jetzt in der E-Mail nach dem Fehler, sondern da haben wir ja auch noch einen Anruf, ich gehe in die Finanzabteilung und sage, aber, der hat mich ja angerufen, der war ja da, dann ist das natürlich ein Thema, was natürlich eine ganz andere Dynamik entwickelt und natürlich ein ganz anderes Gefährdungspotenzial hat. Also von daher glaube ich, damit werden wir uns beschäftigen müssen, und ich glaube, da müssen wir sehr, sehr intensiv auch Aufklärungsarbeit leisten, wie ihr das auch getan habt, dass es sehr, sehr leicht ist, Stimmen zu imitieren, und es ist aus meiner Sicht auch für Leute, wie du und ich gar nicht so einfach rauszukriegen, ist das jetzt falsch, oder ist das echt?

Ute Lange: Wie würdest du denn in so einem Fall vorgehen? Also du bist ja ein bisschen sensibilisierter als vielleicht Michael und ich und viele unserer Hörer und Hörerinnen, wenn jetzt jemand dir mit einer sehr realistischen Stimme diesen Auftrag gäbe, und dann bekämst du noch eine E-Mail. Also was wären so Merkmale, worauf würdest du achten, und was kannst du den Menschen da draußen mitgeben, damit sie eben nicht darauf reinfallen?

Christian Temath: Ich glaube, persönlich ist eine Sache gesunder Menschenverstand. Da gibt's ja mal den schönen Ausspruch, was zu schön klingt, um wahr zu sein, ist wahrscheinlich zu schön, um wahr zu sein. Einfach mal ein Schritt zurückgehen. Selbst wenn mich jetzt jemand angerufen hat, könnte das vielleicht auch irgendwas sein, was irgendwie nicht stimmt. Kann ich hier wirklich 100000 € gewonnen haben? Warum sollte mir jemand 100000€, also dieses kritische hinterfragen und dann auch noch mal gerne gegenchecken? Also bei manchen E-Mails, die man bekommt, wo dann drinsteht, das und das, und das ist passiert, kann man auch einfach mal googeln, ob es da zum Beispiel einen CEO Fraud in der Art und Weise gibt, und wenn das mit den Anrufen passiert, da wird man relativ schnell auch finden auf den relevanten Seiten, das davor gewarnt wird, solche Sachen zu machen, also auch mal nochmal eine zweite oder eine dritte Quelle dazuholen, und das ist, glaube ich, auch wichtig, und vor allen Dingen so offen sein und glaube ich, sich vorstellen zu können, ganz, ganz viele Sachen werden technologisch möglich sein, und dass das dann wirklich auch passieren kann, dass es wirklich ein Fraud ist.

Michael Münz: Dieser Menschenverstand, diese Skepsis betrifft ja nicht nur Anrufe, die ich erhalten könnte, sondern letztendlich ja auch viele Inhalte, denen ich im Netz begegne. Wir haben ja auch die Diskussion gehabt über bekannte Persönlichkeiten in ungewöhnlichen

Klamotten zum Beispiel oder Texte, die einfach maschinell erstellt werden, die dann dafür sorgen, zumindest zeitweise, dass ich bei Suchergebnissen auf dieser Seite landen, also die halt bestimmte Bedürfnisse erfüllen, nach denen ich vielleicht frage. Da ist also ganz viel im Gange, was durch KI erzeugt werden kann. Aber kann man nicht umgekehrt auch dann schon wieder dafür nutzen, so künstliche Inhalte auch zu erkennen? Also kann die uns dann dabei helfen, solche Sachen dann auch leichter ausfindig zu machen oder zu bewerten?

Christian Temath: Ja, das geht, das war ja ganz am Anfang von Chat-GPT, war ja eine der größten Sportaufgaben von Studentinnen, Texte und Aufgaben über eine KI generieren zu lassen. Die Sportaufgabe dann der Forschung, war zu überlegen, an welchen Stellen sehen wir an den generierten Texten, dass wir erkennen können, dies ist ein KI generierter Text, und da ist so ein klassischer Wettlauf losgegangen. Die eine KI generierte Texte, die künstlich generiert sind, und die die andere KI identifiziert, dass es künstlich generiert ist, und ich glaube, diesen Wettkampf, den werden wir auch weiterhin sehen, dass solche Sachen weiter stattfinden. Da wird immer eine Technologie ein Stück weit vorne sein, eine wieder müssen weiter hinten sein. Aber ich glaube, an vielen Stellen wird es tatsächlich wichtig sein, auch tatsächlich KI zu nutzen, um für mehr Sicherheit bei solchen Themen zu sehen.

Ute Lange: Wir haben das ja am Anfang selber schon ein bisschen erwähnt. Es ist auch etwas creepy, was da mit unseren Stimmen gemacht worden ist, und es gibt ja auch eine Diskussion, die mehr so in die Richtung geht, KI ist eine große Bedrohung der Menschheit. Also irgendwann übernehmen die uns also so Science Fiction mäßig. Da gibt es ja auch Filme, die damit spielen. Woher, denkst du, kommt diese Sorge also gerade in Deutschland, weil ich habe so ein bisschen geguckt. In anderen Ländern wird es auch ein bisschen anders konnotiert diskutiert. Da werden häufiger die Chancen in den Vordergrund gestellt. Was, denkst du, steckt dahinter, dass da viele jetzt so den Untergang des Abendlandes erkennen oder zu glauben, diesen zu erkennen?

Christian Temath: Ja zur gesamtulturellen Lage. Ich nehme das auch so wahr, dass wir in Deutschland tendenziell immer ein bisschen skeptischer auf Technologie gucken, am Beispiel Gentechnologie, Biotechnologie, wo sehr, sehr schnell auch in der breiten Öffentlichkeit die Risiken dann platziert wurden und sich auch sehr, sehr stark in den Köpfen verankert haben. Das sehen wir in Teilen jetzt auch schon wieder sehr, sehr deutlich bei der KI, was, glaube ich, zwei Effekte sind, ist das eine natürlich diese Bilder, diese Drohszenarien wie einen Terminator oder auch irgendwie HAL 9000 von 2001, der Computer, der dann entscheidet, die Astronauten sind böse, die wollen mich abschalten, dann schalte ich mal lieber die Astronauten ab und so dieses klassische, die KI will wirklich den Menschen umbringen und töten. Und das ist natürlich ein Bild, was schon ein hohes Maß an, glaube ich, Sorge und auch an einen Kopfkino und Bildern freisetzt. Ich glaube, das andere ist tatsächlich Mystifizierung, die Frage, was glauben wir tatsächlich, was eine KI kann und was sie tatsächlich kann, wenn man sich mal überlegt, dass viele von den Texten, die wir im Internet sehen, zwar eloquent geschrieben sind, aber teilweise total faktenfrei sind, das Bilder, die aktuell generiert werden, aktuell teilweise noch sieben Finger an den Händen haben. Das ist ja nicht so, dass das

irgendwann weggehen wird, aber es ist halt so, dass die immer noch grundsätzliche Fehler in sich drin hat, und dieses, die KI wird schon alle unsere Probleme lösen, ist auch so ein bisschen was, was sich in uns verankert hat, und dann kann diese KI uns auch noch irgendwie böse werden und zum Terminator werden. Das macht natürlich dann tendenziell Angst. Und vielleicht mal, um das zu sagen, ich bin ganz, ganz großer Freund, zu sagen, KI ist da, um zu helfen, aber so nur da zu helfen, wo sie assistiert, uns irgendwie unterstützt, Bereiche besser, effizienter, schneller zu machen, und die wir zwar grundsätzlich gut verstanden haben, wo wir wissen, dass eine Maschine das ein bisschen schneller machen kann, weil sie nicht ermüdet, weil sie mit mehr Daten umgehen kann, und so weiter. Aber sie ist nicht besser in solchen kommitativen Themen, jedenfalls stand heute nicht.

Michael Münz: Vielleicht an der Stelle, wo es um die Bilder geht, wer es noch nicht gemacht hat, bei den Zuhörerinnen und Zuhörern, gerade einfach mal die KI bitten Lachs im Wasser darzustellen, das kann ganz interessante Ergebnisse bringen. Also, ich hab es gemacht, das ist super, ich fand es total lustig, und es geht auch ein bisschen, also so, das sieben Finger Syndrom auch, aber auf eine andere Art. Vielleicht nochmal an der Stelle der Hinweis, falls ihr die Minute habt, Christian, wenn jetzt Leute auf dich zukommen und sagen, ja, alles schwierig, und du hast schon gesagt, Terminator und jetzt der neue Tom Cruse Film, da ist auch die KI die böse.

Ute Lange: Ey das war ein Spoiler! Manche wollen den Film vielleicht noch schauen.

Michael Münz: Ich hab's aus einer Vorschau, ich hab den auch noch nicht gesehen. Also, ich weiß es tatsächlich nur aus der Vorschau. Ich glaube das ist allgemein gut. Demnächst, dass wir alle wissen, dass der Bösewicht jetzt nicht mehr aus einem Land kommt oder irgendwie eine Macke hat, sondern tatsächlich eine Maschine ist. Worauf ich hinaus wollte, ist, wie beruhigst du denn jemanden, der sich jetzt gerade Sorgen macht, also welches von von deinen Projekten vielleicht auch kannst du da noch mal hervorziehen und sagen, ja, aber schau mal, dafür ist die KI gut, und nicht für das, wovor du dir gerade sorgen machst.

Christian Temath: Ja, ich glaube verschiedene Aspekte. Das eine ist, wie gesagt, wir haben ja schon an den KI-Welten uns mal kurz entlang gehangelt. Da gibt es jetzt übrigens auch zu dem Bereich Krankenhaus auch neue Welten, wo tatsächlich mal gezeigt wird, wo kann uns KI assistierend helfen, im Alltag ja Erleichterung zu erfahren? Wir haben auf unserer KI-Landkarte 800 Einträge, mehr als 800 Einträge, wo wir zeigen, wo kann KI Unternehmen helfen, effizienter zu sein, mehr zu verkaufen und so weiter. Also viele gute Beispiele, wo das helfen kann. Wenn wir auch zum Beispiel das ganze Thema Fachkräftemangel gucken, auch unter dem Kontext KI ist da um zu helfen, dann sehen wir, dass wir zum Beispiel in den Behörden, in den administrativen Bereichen unendlich viel Handarbeit noch haben, ganz, ganz langwierige Prozesse, und wo jetzt mit dem Ausscheiden ganz vieler Leute aus dem Berufsleben absehbar ist, dass viele von den Sachen gar nicht mehr vernünftig gemacht werden können. Und ich hatte mal eine Veranstaltung mit dem CEO vom Land Nordrhein-Westfalen, und wir müssen das Thema KI in der öffentlichen Verwaltung voranbringen. Und

dann ging so ein bisschen wieder dieser sorgenvolle Blick, oh, jetzt geht es um Arbeitsplatzabbau, jetzt wollen wir hier mal wieder richtig ran, und dann sagte er so, und bevor jetzt irgendwie jemand fragt zum Thema Arbeitsplatzabbau, das ist und kann überhaupt nicht unser Ziel sein. Ich habe jetzt schon soviel offene Stellen, und wir haben schon so viele Probleme, überhaupt noch Leute zu bewegen, bei uns zu arbeiten. Wir haben Online Zugangsgesetz, wo wir sagen, wir wollen unsere Dienstleistungen online verfügbar machen, aber haben hinter dem Vorhang überhaupt nicht die Möglichkeiten, das abzubilden, weil es alles noch manuell und alles händisch ist. Wir müssen Technologie für uns in den Griff bekommen in der assistierenden Funktion, dass wir in der Lage sind, behördliche Aufgaben, die uns zugeschrieben werden, auch wirklich in Zukunft noch erledigen zu können. Und vor dem Hintergrund denke ich, an vielen Stellen gibt es unendlich viele Möglichkeiten, wo eine KI uns helfen kann. Und solange wir als, ich sag mal, KI-Dirigenten diese helfenden Assistenten für uns mit tanzen lassen und nutzbar machen, bin ich da auch total optimistisch, dass das eine gute Sache wird.

Ute Lange: Ja, also, ich komme jetzt fast schon wieder zu dem Spruch, den Michael und ich hier auch häufiger sagen, den du vorhin auch gesagt hast. Wenn es zu schön ist, um wahr zu sein, ist es das vielleicht auch, weil wir sind öfter schon an den Schluss hier gekommen, dass der Mensch so ein bisschen der Risikofaktor ist in diesem digitalen Alltag und auch was die Sicherheit betrifft. Das heißt, das nehme ich jetzt auch mit, dass je nachdem, was für Belange ich habe, die KI durchaus sehr nützlich sein kann, dass am Ende aber wir als Menschen, du sagtest das eben so schön, die Dirigenten des Einsatzes bleiben und dadurch vielleicht auch uns entlasten um Aufgaben, du hattest das im medizinischen Bereich kurz angesprochen, die es uns ermöglichen, dass wir uns wieder mehr auf unsere eigentlichen Aufgaben konzentrieren können, zum Beispiel der Medizin oder auch im Journalismus. Da hattest du ja auch Beispiele, dass wir Dinge, die routinemäßig abgearbeitet werden können, Freiräume schaffen, um wieder zu recherchieren oder um vielleicht anders zu informieren, weil wir wieder mehr Zeit dafür haben, und da gibt es bestimmt noch eine ganze Menge andere Beispiele aus anderen Berufsgruppen. Ich fand das sehr Aufschlussreich, also auch ein bisschen noch anders gewendet und belegt als die Diskussion, die ich teilweise so verfolgt habe. Ich hoffe, dass das unseren Höhern und Hörerinnen auch so geht. Michael, was ist bei dir jetzt hängengeblieben?

Michael Münz: Ich mag die Idee, dass wir mit KI abwehren können, was andere mit KI schwierigen Sachen machen, also das vielleicht KI irgendwann helfen kann, Spam-Mails oder diese ganzen schrägen Anforderungen vielleicht auch rauszufiltern, weil die viel besser erkennt, anhand vielleicht auch technischer Details von so einer Mail, dass es sich dabei um eine Fälschung handelt. Also das beruhigt mich sehr. Das ist gut, das zu wissen, und der zweite Punkt ist, mir fällt tatsächlich auf, dass wir immer wieder an den Punkt kommen, wenn es zu schön ist, um wahr zu sein, dann ist es auch als nicht wahr. Ich glaube, ich werde mal so ein Jingle anfordern, den wir immer dann abspielen, wenn es jemand in einer Folge sagt, dann haben wir, glaube ich, unser Ziel erreicht. Mal gucken, ob wir das hinkriegen. Genau, aber ja.

Ute Lange: Also, der gesunde Menschenverstand steckt ja dahinter. Noch mal kritisch bewerten und beleuchten, dafür sind wir ja auch da, und wir haben was ganz schönes fürs nächste mal vor. Erst mal herzlichen Dank Christian, dass du dir die Zeit genommen hast. Ich fand's Aufschlussreich, Michael offensichtlich auch, und ihr da draußen hoffentlich ebenfalls. Wenn ihr uns dann hört, was machen wir denn beim nächsten Mal?

Michael Münz: Beim nächsten Mal kommen wir wieder mit drei vertrauten Stimmen, also deine Stimme gut, meine Stimme und dann die von Felix Rick, den hatten wir auch schon mal im vergangenen Jahr. Da ging es um die Gamescom und Felix ist in der nächsten Folge wieder mit dabei, weil es ist wieder Gamescom, und wir müssen darüber reden.

Ute Lange: Ja, es gibt hier auch Routinen, alle Jahre wieder, nicht Weihnachten, aber Gamescom, und bis dahin hoffen wir, dass ihr einen schönen Sommer habt. Schreibt uns wieder eure Fragen, folgt uns auf den Kanälen. Möchtest du die Kanäle aufsagen?

Michael Münz: Ja, mache ich gleich, und ich wollte noch sagen, schreibt uns nicht nur eure Fragen, sondern schreibt uns auch Antworten auf unsere Fragen, nämlich wo nutzt ihr denn künstliche Intelligenz? Das würden wir nämlich gerne noch wissen. Also seht ihr das auch als hilfreiche Anwendungen, die ihr immer mal wieder einsetzt in eurem Berufsleben, oder last ihr damit Texte schreiben oder Bilder oder Videos generieren? Das würden wir gerne wissen. Schreibt uns das so, und zwar schreibt ihr uns das entweder per E-Mail an Podcast@BSI.Bund.de oder schreibt uns über die Kanäle auf Facebook, instagram, Twitter, Mastodon und YouTube.

Ute Lange: Ja, und bis wir uns wieder hören oder ihr uns, wünschen wir euch einen schönen Sommer und hoffentlich auch einen sicheren Sommer digital, und wir freuen uns, wenn ihr uns bis dahin liket und Update Verfügbar auf euren Podcast Plattformen abonniert, damit ihr uns nicht verpasst oder auch nochmal ältere Folgen anhören könnt. In diesem Sinne: Tschüss!

Michael Münz: Genau Tschüß, mach's gut! Bis nächsten Monat!

Besuchen Sie uns auch auf:

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

<https://www.facebook.com/bsi.fuer.buerger>

https://twitter.com/BSI_Bund

https://www.instagram.com/bsi_bund/

<https://social.bund.de/@bsi>

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI),
Godesberger Allee 185-189, 53133 Bonn