:data[re]port

_ABER SICHER!

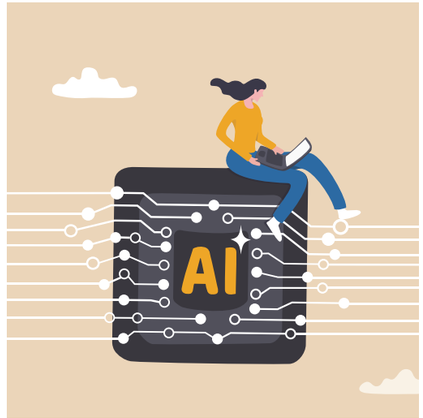
Künstliche Intelligenz hilft Cyberkriminellen: Angriffe werden immer perfekter und sind kaum noch durchschaubar. Die Verwaltung weiß sich zu wehren.

HEREINSPAZIERT

Die älteste Kirche Schleswig-Holsteins lädt ein zum virtuellen Rundgang

INS KLEINSTE

Rückt der praktische Einsatz von Quantencomputern näher?



Liebe Leserinnen, liebe Leser,

„KI ist das Weltraumrennen unserer Zeit“, so formulierte es unser Vorstand Torsten Koß vor kurzem in einem Vortrag. Die Entwicklung verläuft extrem rasant, die Hoffnungen auf den Nutzen von KI sind gewaltig. Wie immer gibt es eine Schattenseite. Deep Fakes generiert von KI verhelfen Cyberkriminellen zu durchschlagendem Erfolg. Sie steigern die Effizienz und machen Techniker ratlos (S. 6).

Auch Verwaltungen sehen sich mit der Tatsache konfrontiert, dass Cyber-Attacken dank künstlicher Intelligenz immer effizienter werden. Doch in dem Maße, wie sich Angriffstechniken verbessern, werden Abwehrtechniken weiterentwickelt und optimiert, wie es Andreas Reichel im Interview betont (S. 9). Ein Unternehmen wie Dataport investiert dafür 60 bis 70 Millionen Euro pro Jahr.

Natürlich werfen wir auch einen Blick auf die technischen Entwicklungen, die zu unser aller Nutzen eingesetzt werden. Digitale Zwillinge von Brücken etwa, die sowohl bei der Planung als auch bei der Instandhaltung wichtige Hilfestellung geben (S. 18).

Und ganz wichtig: Bitte nehmen Sie sich etwas Zeit und helfen uns, den Datareport weiterzuentwickeln. Sie tun sogar etwas für die Umwelt. Mehr dazu auf Seite 21.

Ihre

Britta Heinrich
(Leiterin Öffentlichkeitsarbeit)

DATAPORT ERHÄLT HAMBURGER VERGABEPREIS

Wenn Dataport Aufträge an externe Dienstleister vergibt, dann macht das eine einzige Abteilung im Haus. Auf diese Weise sollen auch große Vergaben rechtssicher, effizient und ohne externe Unterstützung durchgeführt werden. Für diese Praxis hat Dataport den Hamburger Vergabepreis 2024 erhalten. Die rund 40 Fachleute der Abteilung „Strategisches Vergabemanagement und Lizenzvertragsmanagement“ führen und verantworten den gesamten Vergabeprozess, von der Ausschreibung bis zum Vertragsabschluss. Diese Aufstellung hat die Jury des Vergabepreises überzeugt. <

MEHR: https://dataport.de

GEMEINSAM NACHHALTIG: REMARKETING-BASIS GESTARTET

Ausgediente Handys oder Laptops landen bei Dataport nicht auf dem Müll. Sie werden wiederverwertet. Dafür haben Dataport und der Dienstleister Bechtle gemeinsam ein Konzept erarbeitet. Seit Anfang 2024 werden Geräte von Kunden in Hamburg und Bremen nach ihrer fünfjährigen Nutzungsdauer gesammelt, wenn nötig repariert und dann wieder vermarktet. Erster Erfolg des Projekts ist der Verkauf von 700 Smartphones aus Hamburg. Das Projekt Remarketing-BASIS ist ein weiterer Meilenstein auf dem Weg zum nachhaltigen IT-Kreislauf bei Dataport. <

MEHR: https://dataport.de

DIGITAL-INDEX ZEIGT GESPALTENE GESELLSCHAFT

In Deutschland kann ein Großteil der Bevölkerung die digitale Welt selbstbestimmt für sich nutzen. Gleichzeitig sinkt jedoch die Fähigkeit, mit dem digitalen Wandel Schritt zu halten. Das sind die Ergebnisse einer repräsentativen Studie, die Anfang 2024 auf die zunehmende digitale Spaltung der Gesellschaft verweist. (Quelle: „D21-Digital-Index 2023/24“ der Initiative D21 e. V.) <

KI IN UNTERNEHMEN

Das vom BMAS geförderte Projekt KI-ULTRA steht vor dem Abschluss. Herausgekommen sind praxisnahe Leitfäden und ein Evaluation Toolkit – sie sollen in Zukunft Unternehmen dabei unterstützen, künstliche Intelligenz (KI) in ihre Arbeitsprozesse besser zu integrieren. Zusammen mit 29 deutschen Unternehmen hat das Fraunhofer Institut drei Jahre lang Erfahrungen aus der Praxis zusammengetragen. Die Ergebnisse werden nicht nur deutschen Unternehmen zur Verfügung gestellt, sondern auch auf internationaler Ebene in der Arbeitsgruppe „Future of Work“ weiter diskutiert. <

MEHR: https://hci.iao.fraunhofer.de

KÜNSTLICHE INTELLIGENZ: GLOBALE KOOPERATION

Einen Leitfaden zur Nutzung von künstlicher Intelligenz (KI) haben das Bundesamt für Sicherheit in der Informationstechnik (BSI) und zehn internationale Partnerbehörden erstellt. Dieser soll Unternehmen und Regierungen helfen, sich mit Sicherheitsrisiken von KI auseinanderzusetzen. <

OZG IM VERMITTLUNGSAUSSCHUSS

Nach der Ablehnung des Onlinezugangsgesetzes (OZG) im Bundesrat hat die Bundesregierung inzwischen den Vermittlungsausschuss angerufen. Bund und Länder müssen nun in dem gemeinsamen Gremium klären, wie es mit den Standards von Verwaltungsdienstleistungen weitergeht. <

CYBERSICHERHEIT FÜR KOMMUNEN

Angesichts zunehmender Cyberangriffe bietet das Bundesamt für Sicherheit in der Informationstechnik BSI einen niederschwelligen Einstieg in den IT-Grundschutz an. Der „Weg in die Basis-Absicherung (WiBA) besteht aus Checklisten, die mittels Prüffragen den Aufbau von kommunalen Sicherheitssystemen unterstützen sollen. <

FEHLENDE KONZEPTE: DIGITALREPORT 2024 FORDERT DIGITALAGENDA

Deutschland ist nach Ansicht der Bevölkerung bei der Digitalisierung zu langsam. Das ist das Ergebnis einer repräsentativen Befragung des Allensbach-Instituts im Auftrag des European Center for Digital Competitiveness der ESCP Business School. Die Studie hält die Lage im Bereich digitaler Zukunftstechnologie für schwierig und fordert eine Digitalagenda 2026. Vor allem die Bundesregierung sei in der Pflicht: „Strategische Defizite, die Zersplitterung von Zuständigkeiten und unzureichende Investitionen werden als Hauptursachen für den fehlenden Fortschritt benannt“, bemängeln die Meinungsforscher. <

MEHR: https://digital-competitiveness.eu/digitalreport

KRIMINELLE INTELLIGENZ

TEXT: Jürgen Gressel-Hichert

KÜNSTLICHE INTELLIGENZ GIBT CYBER-KRIMINELLEN NEUE METHODEN AN DIE HAND. VOR ALLEM ABER PERFEKTIONIERT SIE BEKANNTE ANGRIFFSSZENARIEN SO, DASS DIESE NUR NOCH SCHWER ZU DURCHSCHAUEN SIND.

September 2023. Die deutsche Hotelkette Motel One erklärt öffentlich, dass ihre IT gehackt wurde. Millionen Gäste-Daten wurden im Darknet veröffentlicht, darunter fast 200 Kreditkarteninformationen. Februar 2024. In Frankreich werden die Gesundheitsdaten von mehr als 33 Millionen Menschen von Cyberkriminellen gestohlen. Der bisher größte Datendiebstahl im Nachbarland betrifft Patienten, Fachpersonal und Apotheken. Die Nationale Kommission für Informatik und Freiheiten CNIL fürchtet den Missbrauch der Daten bei sogenannten Phishing-Kampagnen. Dabei werden von Hackern absolut echt wirkende Mails von vermeintlichen Behörden verschickt, die weitere Daten abgreifen sollen. Mit diesen können Cyberdiebe dann Konten leerräumen oder gestohlene Identitäten für weitere Straftaten verwenden.

//AUCH DIE VERWALTUNG IST ZIEL

Europa ist im Fadenkreuz der Cyberkriminellen. Mehr als 800 Unternehmen und Institutionen in Deutschland waren 2023 von ihren Angriffen betroffen – zunehmend aus dem Ausland. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt deshalb in seinem aktuellen Jahresbericht: „Die Bedrohung im Cyberraum ist so hoch wie nie zuvor." Und das Problem hat sich verschärft: „Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen."

Zu den folgenreichsten Attacken gehören die sogenannten Ransomware-Angriffe. Dabei gelangen die Hacker in die Firmensoftware und verschlüsseln sie. Das ist vergleichbar mit einem Einbruch, bei dem die Räuber in einem Haus alle Schlösser austauschen. Die Schlüssel erhält, wer Lösegeld zahlt. Wer das tatsächlich macht, kann allerdings vor weiteren Übergriffen nicht sicher sein. Wer sich weigert, braucht oft Monate, um die Systeme wiederherzustellen. Ein Blick in die BSI-Jahresberichte macht deutlich, dass die bisherigen Sicherheitsvorkehrungen einfach nicht reichen.

Denn mithilfe von künstlicher Intelligenz (KI) hat sich die Effizienz von derartigen Angriffen enorm gesteigert. Das macht selbst professionelle Sicherheitstechniker oft ratlos.

//„EIN KLEINES SPIELZEUG"

Vermehrt werden Deep Fakes in Form von gefälschten Mails, täuschend echt wirkenden Hilfe-Anrufen oder ganzen Filmsequenzen eingesetzt, die durch eine entsprechende KI verändert wurden. Eine generative KI wie ChatGPT kann zum Beispiel aus wenigen Sprach-, Bild- oder Videoschnipseln eines Menschen eine nahezu perfekte „Kopie" erstellen. So geschehen im November 2023, als ein Video des Künstlerkollektivs „Zentrum für politische Schönheit" eine echt wirkende Ansprache von Bundeskanzler Olaf Scholz in die Medien brachte. Systemgefährdend wird es, wenn sich solche „kriminelle Intelligenz" in Unternehmen oder Behörden „umsehen" darf. Mit einfachen Tools wie Mimikatz oder Bloodhound können Cyberkriminelle zunächst nach Einfallstüren in Programmcodes fahnden, um unerkannt hinter die Firewalls von Unternehmen zu gelangen und sich dann selbst mit möglichst weitgehenden Administrationsrechten zu versorgen.

Ein Programm wie Mimikatz ist frei im Internet zugänglich und wirbt mit dem Slogan: „A little tool to play with Windows security". Wer will, kann mit „dem kleinen Spielzeug" nicht nur Schwachstellen im eigenen System finden, sondern auch Türen in andere Systeme öffnen.

„DIE BEDROHUNG IM CYBERRAUM IST SO HOCH WIE NIE ZUVOR."

//ALTE SICHERHEITSARCHITEKTUR ÜBERDENKEN

Bis vor wenigen Jahren wurden Sicherheitssysteme beim Aufbau einer neuen Informationstechnologie (IT) von vornherein mitgedacht – man nannte das System „Security by Design“. Firewalls und ein Zugangssystem wurden eingerichtet, Mitarbeitende mussten sich mit Zwei-Faktor-Identifizierung ins System einloggen, Passwörter wurden immer länger. Das war lästig, aber bis zu einem gewissen Grad sicher.

Seitdem KI auch in viele Unternehmen Einzug gehalten hat und dort Routine-Arbeiten übernimmt, ist ein neues Zeitalter für Sicherheitsarchitekturen angebrochen. Software-Entwickler nutzen etwa ChatGPT, um Programme für Mail-Antworten, Abrechnungen oder Archiv-Ablagen zu schreiben. Je umfangreicher diese sind und je mehr Prozesse sie im Unternehmen übernehmen, desto weniger Kontrolle hat der einzelne Programmierer. Denn eine KI lernt selbstständig und sammelt Informationen aus allen Bereichen, zu denen sie Zugang hat. Wer einen Angriff auf eine Firma plant, muss also über das Internet „nur“ spezielle präparierte Codes vorbereiten, auf die eine entsprechende KI beim Lernen zugreifen würde. Solche Codes können auch in Bildern versteckt sein und somit Zugriffe ermöglichen, die nicht ohne Weiteres entdeckt werden. Das heißt, das bisherige Sicherheits-System „Security by Design“ funktioniert nicht mehr richtig, denn eine KI organisiert ihr Design selber. Die „gute, alte“ Antivirensoftware hilft also nicht, wenn die Anfragen an die KI es einfach notwendig machen, im gesamten Internet nach Antworten zu suchen. Die Lösung dafür? Keine, so das BSI.

//MIT KI GEGEN KI

Oder vielleicht gibt es doch Lösungen? Denk- und erste Handlungsansätze beruhen darauf, eine KI zur Abwehr von Cyberangriffen nicht mehr statisch und zentral mit Daten zu füttern. Im Gegenteil: Sie soll beim Unternehmen vor Ort die Informationsflüsse beobachten und bei Abweichungen vom Normalfall alarmieren. Denn das kann eine KI besonders gut: Muster erkennen und Veränderungen protokollieren. Die KI erkennt Abweichungen von normalen Abläufen sofort und meldet sie an die Zuständigen oder – je nach Konfiguration – wehrt sie eigenständig ab.

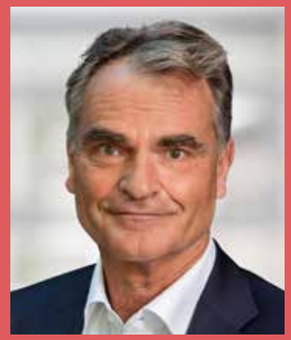
Dass so etwas funktionieren kann, hat beispielsweise die britische Cyber-Security-Firma Darktrace schon mehrfach vorgeführt. Angriffe von unbekannten Servern mit ausführbaren Programmen wurden in Echtzeit gestoppt und an die Sicherheitsabteilungen der betroffenen Firmen gemeldet. Ähnlich funktioniert es, wenn beispielsweise eine KI im Online-Banking arbeitet. Wird plötzlich von einem Konto an einem üblicherweise nicht genutzten Terminal viel Geld abgehoben, fragt die Bank nach und sperrt vorsichtshalber das Konto.

KI eröffnet also Cyberkriminellen neue Wege. Andererseits nutzt die Technik auch im Kampf dagegen. Ob sie in Zukunft proaktiv eingesetzt wird, ist politisch umstritten. Ein Zurück-Hacken, ein sogenannter Hackback, um eine kriminelle Struktur zu zerstören, ist bisher politisch nicht gewollt und technisch auch nur begrenzt sinnvoll. Denn Cyberkriminelle spielen über Bande und sind schon weg, wenn man endlich ihre IP-Adresse hat. Das Fazit vieler Diskussionsrunden zum Thema Cybersicherheit lautet denn auch: Wir müssen lernen, uns besser zu verteidigen. <

Seitdem KI auch in viele Unternehmen Einzug gehalten hat und dort Routine-Arbeiten übernimmt, ist ein neues Zeitalter für Sicherheitsarchitekturen angebrochen.

MEHR INPUT

Weitere Infos auf unserer Homepage
https://dataport.de/bsi-zertifizierung



ANDREAS REICHEL ist Vorstand Technik bei Dataport.

WIE SICHER IST DATAPORT? DREI FRAGEN AN ANDREAS REICHEL

Inwiefern haben denn KI-gesteuerte Cyber-Angriffe auf das Rechenzentrum von Dataport schon stattgefunden?
Es finden keine KI-gestützten Angriffe auf unser Rechenzentrum statt. Wir bemerken zwar, dass Phishing Mails durch KI immer perfekter werden. Unsere Mitarbeiterinnen und Kunden sind aber gewarnt und werden geschult. Und etwa 60 Prozent unserer eingehenden Mails sortiert das System sowieso schon als Spam aus.

Die Sicherheit seiner IT kostet Dataport bestimmt einiges?
Wir geben hier insgesamt 60 bis 70 Millionen Euro im Jahr für Security aus. Das ist ein gigantischer Betrag. Und unsere Rechenzentren, Infrastrukturen und Prozesse sind vollumfänglich durch das BSI zertifiziert. Da sind wir einer der ganz wenigen in Deutschland. Und wenn wir etwas neu konzipieren in der IT, dann sitzen, anders als früher, die Sicherheitsexperten gleich mit am Tisch.

Wie sieht die Strategie von Dataport gegen Cyberattacken aus?
Auf der Basis der BSI-zertifizierten Plattformen, wie Patch-Management oder Netztrennung, betreiben wir vier Säulen: Erstens: Prävention. Wir erkennen Schwachstellen, bevor sie gefährlich werden. Die zweite Säule heißt „Detektion.“ Wir erkennen laufende Angriffe. In diesen beiden Bereichen haben wir mächtige Werkzeuge im Einsatz, die vor allen Dingen Anomalien feststellen sollen. Die dritte Säule heißt „Reaktion“. Wir haben ein Cyber Security Operations Center mit etwa 20 Spezialisten. Da sind auch zertifizierte - also ethische - Hacker dabei. Die sind einmal im Monat im Alarmeinsatz, wenn irgendetwas Verdächtiges auftaucht und reagieren dann entsprechend schnell. Und in der vierten Säule beschäftigen wir uns mit dem Wiederanlauf nach einer erfolgreichen Attacke. Im gleichen Maße, wie die Angriffskapazitäten sich verbessern, werden wir auch unsere Abwehrtechniken verbessern. Deswegen sind wir wachsam, aber nicht ängstlich. <

TEXT: Jürgen Gressel-Hichert

WENN NICHTS MEHR GEHT

CYBERANGRIFFE AUF KOMMUNEN UND LANDKREISE NEHMEN ZU. DAS IST TEUER UND GEFÄHRLICH. EIN PROJEKT IN SCHLESWIG-HOLSTEIN BESCHÄFTIGT SICH MIT DIGITALER RESILIENZ UND BIETET EINEN LEITFADEN AN.

Den 6. Juli 2021 werden die Menschen in Anhalt-Bitterfeld so schnell nicht vergessen. Damals legten Hacker fast sämtliche Computer des Landkreises lahm. Die Angreifer hatten mithilfe einer Ransomware das gesamte Netz verschlüsselt und forderten ein Lösegeld.

Der Landkreis lehnte eine solche Geldzahlung ab und rief den Katastrophenfall aus – zum ersten Mal in der Geschichte der Bundesrepublik wegen eines Cyberangriffes. Erst Monate später wurde der Katastrophenstatus wieder aufgehoben. Bislang kostete der Angriff auf den Landkreis mehr als 2,5 Millionen Euro und jede Menge Nerven.

Spezialisten der Bundeswehr, von Dataport (CERT Nord) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) halfen der Verwaltung in dieser Notlage, obwohl das BSI sich eigentlich nur um die Bundes-IT zu kümmern hat und lediglich Ratschläge an Bürgerinnen und Verwaltungen gibt. Im Katastrophenfall ist das BSI nach eigenen Angaben auch nur insoweit zuständig, „das Opfer in eine stabile Seitenlage zu bringen."

Seit 2023 gibt es zwar eine verstärkte und vertraglich vereinbarte Kooperation zwischen Sachsen-Anhalt und dem BSI, aber das Bundesamt kann – außer in akuter Notlage – auf kommunaler Ebene nicht agieren. Und da sehe es „eher besorgniserregend" aus. Das hat der Landesrechnungshof von Sachsen-Anhalt festgestellt, der einen Blick auf die Kosten hat und haben muss. Die meisten Kommunen haben kein IT-Sicherheitskonzept, bemängeln die Kämmerer. Nur weniger als die Hälfte haben überhaupt einen Plan für eineminimale Datensicherung.

//BASISABSICHERUNG

Diese Einschätzung trifft allerdings auch auf Kommunen anderer Bundesländer zu. Das Land Schleswig-Holstein hat deshalb schon vor etwa zehn Jahren ein Projekt aufgelegt. Es bietet eine Basisabsicherung für Kommunen und somit einen Einstieg in den Grundschutzstandard des Amtes BSI an: SiKoSH – Sicherheit für Kommunen in Schleswig-Holstein.

Im Mittelpunkt steht ein gut 50 Seiten starkes „Kochbuch" für die Kommunen, erklärt Frank Weidemann. Er ist von Anfang an dabei und hat das Kochbuch, also die Handreichung „Einführung und Betrieb eines Informations-Sicherheits-Management-Systems (ISMS)" zusammen mit Praktikern aus den Kommunen, vom Land und von Dataport erarbeitet.

„Es gibt keine Meldepflicht für Vorkommnisse in der kommunalen Kernverwaltung", sagt er. „Tatsächlich hat niemand einen Überblick über die Informations-Sicherheitslage in kommunalen Einrichtungen."

Deswegen versteht er die Arbeit mit SiKoSH als Hilfe zur Selbsthilfe. Etwas anderes ist auch kaum möglich, denn die Anforderungen sind von Kommune zu Kommune sehr unterschiedlich.

//LIVE-PHISHING-TRAINING

IT-Sicherheit muss ganzheitlich gedacht werden und vor allem diejenigen einbeziehen, die in der Verwaltung arbeiten. Aber wie bringt man Verwaltungsmitarbeiterinnen dazu, sich mit Cybersicherheit auseinanderzusetzen? „Indem man sie mal in Versuchung bringt und für das Thema sensibilisiert", erklärt Frank Weidemann. In Kooperation mit der Ludwig-Maximilians-Universität München hat er 2018 in der Landeshauptstadt Kiel erstmals ein Live-Phishing-Training durchgeführt. In mehreren Wellen wurden ausgesuchte Abteilungen mit Phishing-Mails konfrontiert. Fast 25 Prozent der vergifteten Mails wurden tatsächlich geöffnet.

Wer so achtlos mit den Phishing-Mails umging, wurde anonymisiert informiert, wie er sich in Zukunft richtig zu verhalten habe. Danach waren viele Mitarbeiter motiviert, sich erstmals mit dem Thema auseinanderzusetzen. Sie waren auch zu Schulungen bereit.

//WER SCHREIBT, DER BLEIBT

SiKoSH hat dazu in seiner Handreichung den Weg vorgezeichnet: Erste lokale Arbeitsgruppen sollen den Ist-Zustand dokumentieren. Jemand muss für die Informationssicherheit beauftragt werden. Die Behördenleitungen sollten mit ins Boot genommen werden. Zusammen wird ein Leitfaden speziell für die Kommune erarbeitet und für alle dokumentiert.

Und dann muss das Ganze natürlich praktisch umgesetzt werden. Denn das Projekt SiKoSH steht nur mit Rat und seinem „Kochbuch" zur Verfügung, aber Rezepte erstellen und umsetzen, das passiert vor Ort. Denn im Falle eines Falles muss ja die Kommune auch selbst schnell agieren können, wenn etwas schiefläuft.

Die wichtigste Erkenntnis von Frank Weidemann und seinem Team: „Man ist nie fertig" und – auch das haben Kommunen in Norddeutschland schon selbst erfahren – „am besten ist es, alle Regeln, wie man die IT betreibt, aufzuschreiben. Nur dann ist man fit für den Notfall".

//ZUM NACHAHMEN EMPFOHLEN

SiKoSH ist für das nördlichste Bundesland längst kein Pilotprojekt mehr, sondern Teil der schleswig-holsteinischen IT-Strategie. „Digitale Resilienz" ist das ausdrückliche Ziel der Landespolitik – also fit und stark werden gegenüber Cyber-Angriffen und anderen IT-Unglücken. Die Pläne des Landes sollen Schleswig-Holstein zu einem Musterland in Sachen Digitalisierung machen. SiKoSH hat bereits jetzt mehrere Nachahmer in anderen Bundesländern. Man will Vorbild sein. Auch für andere, die noch überlegen. <

MEHR INPUT

Projekt Sicherheit für Kommunen des ITVSH
https://itvsh.de/sikosh

Informationen zur Cybersicherheit in Kommunen
https://www.dataport-kommunal.de/it-sicherheit

KÜNSTLICHE INTELLIGENZ KANN UNS ARBEIT ABNEHMEN. IHR EINSATZ MUSS ABER GUT GEPLANT UND ORGANISIERT WERDEN, SAGT SOZIALWISSENSCHAFTLER MARKUS HERTWIG.

_FACHKRÄFTEMANGEL: KI IST KEINE WUNDERWAFFE!

KOMMENTAR: Markus Hertwig

Alle Technologien haben das Potenzial, menschliche Arbeitskraft zu ersetzen. Auf künstliche Intelligenz (KI) trifft das in einem besonderen Ausmaß zu. Ihr wird zugetraut, viele automatisierbare Tätigkeiten übernehmen zu können. Im Hinblick auf den Fachkräftemangel wird KI als Lösung breit diskutiert.

KI allein löst das Problem jedoch nicht, im Gegenteil: Man läuft paradoxerweise Gefahr, den Fachkräftemangel zu befeuern, betrachtet man KI als Heilsbringer. Denn was auf jede neue Technologie zutrifft, gilt auch für KI: Es ist nicht damit getan, eine App oder Computerhardware zu installieren. Um die Potenziale der KI auszuschöpfen, sind weitreichende Umstrukturierungen der Arbeitsorganisation erforderlich. Dies betrifft beispielsweise die Frage, wie die Arbeitsteilung zwischen KI und Fachkräften gestaltet werden soll: Welche Aufgaben kann die KI sinnvollerweise übernehmen? Wie verändern sich dadurch die Tätigkeiten der Beschäftigten? Planerische Höchstleistungen sind hier gefragt, die versierte Fachkräfte mit breiten Kenntnissen erfordern.

Stichwort Qualifikation: KI benötigt eine Flut von Daten. Firmen mit effizienter Datenwirtschaft sind im Vorteil. Allerdings setzt dies zunächst eine besondere Fachkompetenz voraus. Genau die fehlt aber in vielen Unternehmen. Sie suchen händeringend jene Fachkräfte, die KI eigentlich ersetzen soll.

KI kann in bestimmten Bereichen Prozesse automatisieren, reproduziert aber einen erneuten Fachkräftemangel. Technikl ösungen erfordern folglich immer auch nichttechnische, also soziale und arbeitsorganisatorische Antworten auf die Probleme, die Technik hervorbringt.

Setzen Unternehmen auf die Potenziale von KI, um dem Fachkräftemangel zu begegnen, sollten sie frühzeitig in eigene Weiterbildung investieren. Sind Fachkräfte auf dem Arbeitsmarkt rar, so liegt es auf der Hand, die vorhandenen Beschäftigten entsprechend der eigenen Bedarfe weiterzuentwickeln. Unternehmen schauen hier allerdings zu stark auf den Arbeitsmarkt, das Bildungssystem und die Politik. Sie haben es aber selbst in der Hand, in die Qualifikation zu investieren, die sie brauchen. Dies sollte unter Beteiligung von Beschäftigten und Personalräten im Rahmen einer klaren Change-Strategie geschehen. In einem Aktionsplan für Fachkräfte kann KI ein Element sein. Deren Grenzen sollten aber nüchtern analysiert werden. <

MARKUS HERTWIG ist Professor und Lehrstuhlinhaber an der Ruhr Universität Bochum. Er erforscht die Ursachen und Auswirkungen der digitalen Transformation von Arbeit und Organisationen.

MEHR INPUT

Ruhr-Universität Bochum, Lehrstuhl für Soziologie der digitalen Transformation
https://www.sdt.ruhr-uni-bochum.de

Werden digitale Technologien Ihren Job verändern? Test mit dem „Job Futuromat“
https://job-futuromat.iab.de

HOHE SICHERHEIT IST ZWINGEND TEIL EINER ZUKUNFTSFÄHIGEN IT. EIN GESPRÄCH MIT MARTIN MEINTS, IT-SICHERHEITSBEAUFTRAGTER BEI DATAPORT, ÜBER “ZERO TRUST“ IM RAHMEN VON CYBERSECURITY.

_TRAU, SCHAU, WEM!

INTERVIEW: Fabian Baumheuer

HERR MEINTS, IN DER IT-WELT WIE AUCH BEI DATAPORT WIRD DAS SICHERHEITSKONZEPT „ZERO TRUST“ – ZU DEUTSCH „NULL-VERTRAUEN“ – DISKUTIERT, WEIL DIE ANZAHL UND RAFFINESSE VON CYBERANGRIFFEN STETIG ZUNIMMT UND HERKÖMMLICHE SICHERHEITSANSÄTZE ZUNEHMEND AN EFFEKTIVITÄT VERLIEREN. WAS IST DAS FÜR EIN KONZEPT UND WAS VERSPRICHT MAN SICH DAVON?

Wenn Sie sich heute irgendwo anmelden, in einem Netzwerk oder einer bestimmten Anwendung, dann wird im Wesentlichen geprüft, ob Sie als Person vertrauenswürdig sind. Also, haben Sie die richtigen Anmeldedaten? Sind Sie registriert? Haben Sie für das, was Sie da tun wollen, die erforderlichen Rechte? Bei Zero Trust wird zusätzlich geprüft, ob Ihr Gerät bestimmte Sicherheitsstandards erfüllt. Ihr Gerät übermittelt seinen Sicherheitsstatus, damit es als vertrauenswürdig eingestuft werden kann. Erst dann können Sie beispielsweise auf Ihr Bürgerkonto zugreifen oder ein Verfahren bei Dataport nutzen oder bestimmte Informationen abrufen.

UND DER REST DER ANMELDEPROZEDUR BLEIBT WIE GEHABT?

Ja, die klassische Authentifizierung von Personen bleibt. Bei den Anwenderinnen und Anwendern ändert sich erst einmal mit ihren Rollen und Rechten gar nichts.

WARUM SCHÜTZT AUSGERECHNET DIES DANN BESSER VOR HACKERANGRIFFEN?

Ich kann der Person, die authentifiziert wird, ja nicht ansehen, ob sie ein Hacker ist. Aber anhand des Endgeräts und dem, was darauf so an Software läuft, kann ich schon sehr viel besser einschätzen, ob das jemand von den „evil guys“ ist.

WIE KOMMT MAN DENN AN DIE ENTSPRECHENDEN INFORMATIONEN ÜBER DAS EINGESETZTE GERÄT?

Das ist genau der Punkt, warum Zero Trust aktuell in der Breite der Anwendungen noch nicht stattfinden kann. Sie brauchen im Betriebssystem oder auch in der Hardware des Nutzenden einen so genannten Zero-Trust-Agenten.

DAS KLINGT JA EIN BISSCHEN NACH SPIONAGE …

Ach, wegen „Agent“ … Nein, das ist ein IT-Fachbegriff für eine spezielle Softwarekomponente, die auf einem Endgerät oder in einem Netzwerk installiert ist. Dieses kleine Programm sammelt und übermittelt die Informationen über das verwendete Gerät. Damit kann ich prüfen, ob es auch meinen Sicherheitsansprüchen genügt.

SCHWER VORSTELLBAR, DASS DIE BÜRGERINNEN UND BÜRGER SICH DAVON ÜBERZEUGEN LASSEN, SO EINEN ZERO-TRUST-AGENTEN AUF IHREN ENDGERÄTEN ZU INSTALLIEREN.

Genau, das ist der Knackpunkt. Im Augenblick sind wir vom Goodwill der Anwendenden abhängig.

DAS KLINGT JETZT NICHT DANACH, ALS HÄTTE ZERO TRUST EINE BLÜHENDE ZUKUNFT.

Ich setze da sehr auf die visionäre Kraft der Industrie angesichts der Notwendigkeit, bessere Sicherheitsstandards zu ermöglichen. Irgendwann werden Zero-Trust-Agenten in den Betriebssystemen schon drin sein oder in der Hardware stecken.

DAS HEISST: HOFFEN UND WARTEN?

Nein, Zero Trust funktioniert schon gut in internen Infrastrukturen, also überall, wo ich die Umgebung kontrollieren und die Agenten installieren kann und die Nutzenden kenne.

ZUM BEISPIEL …?

Zum Beispiel bei der Kommunikation innerhalb von Landesverwaltungen oder zwischen den Landesverwaltungen oder zwischen Landesverwaltung und Bundesverwaltung, wo Maschinenzertifikate als Vorläufertechnologie zu Zero Trust ja schon im Einsatz sind. Doch sobald ich es mit Infrastruktur und Benutzenden zu tun habe, die ich nicht kenne, denen ich also grundsätzlich nicht vertrauen kann, funktionieren aktuell Zero-Trust-Absicherungsmechanismen noch nicht.

SIE SIND IT-SICHERHEITSBEAUFTRAGTER VON DATAPORT. HOFFEN SIE MIT BLICK AUF DIE GERADE FÜR DIE ÖFFENTLICHE VERWALTUNG BESONDEREN SICHERHEITSANFORDERUNGEN, DASS SICH ZERO TRUST MEHR UND MEHR DURCHSETZT?

Wir machen schon mehr, als nur zu hoffen. Wie immer brauchen solche technologischen Entwicklungen eine gewisse Reifezeit, auch bei der Qualität der Agenten. Das wollen wir aber nicht abwarten, sondern sondieren genau, wo wir unsere Sicherheit bereits mit Zero-Trust-Konzepten erhöhen können, und was sich am Markt so tun. Das ist es, was wir mit „Zero-Trust-Readyness“ meinen. Wir wollen umsetzen, was schon umsetzbar ist und bereit sein, wenn mehr geht.

ZERO TRUST

„Zero Trust“ in der Cybersecurity gewinnt als IT-Sicherheitskonzept an Bedeutung. Es besagt, dass keinem Akteur im Netzwerk grundsätzlich vertraut wird. Jeder Datenzugriff wird dynamisch und risikobasiert überprüft. Dies ermöglicht eine flexible Cybersecurity, die sich an Geschäftsprioritäten ausrichtet. Dabei werden auch die verwendeten Endgeräte auf Sicherheitsstandards geprüft.

Für Fachleute:
Begriffsdefinition des National Institute of Standards and Technology (U.S. Department of Commerce): https://csrc.nist.gov/pubs/sp/800/207/final

VERSETZEN WIR UNS GEDANKLICH IN EINE ZUKUNFT, IN DER ZERO TRUST ETABLIERT IST, WIRD „NULL-VERTRAUEN“ AUCH AUSWIRKUNGEN AUF DIE UNTERNEHMENSKULTUR, AUF DAS MITEINANDER HABEN?

Ach, das wird vom Begriff her negativ getriggert. Ich sehe eher positive Auswirkungen auf die Betriebskultur. Es geht bei Zero Trust nicht darum, eine Misstrauenskultur, beispielsweise gegenüber den Mitarbeitenden, zu etablieren, sondern gegenüber unbekannter und nicht gemanagter Hard- oder Software. Möglicherweise wird Zero Trust sogar mehr Freiheiten bringen. Denken Sie an das Verbot privater Hard- und Software im dienstlichen Kontext. Das könnte dann flexibler gehandhabt werden. Deshalb sehe ich auch Potenziale und Chancen für die Flexibilisierung und Individualisierung des Arbeitsumfelds.

NIEMAND AUF DER SEITE DER GUTEN MUSS SICH ALSO SORGEN MACHEN ÜBER ZERO TRUST?

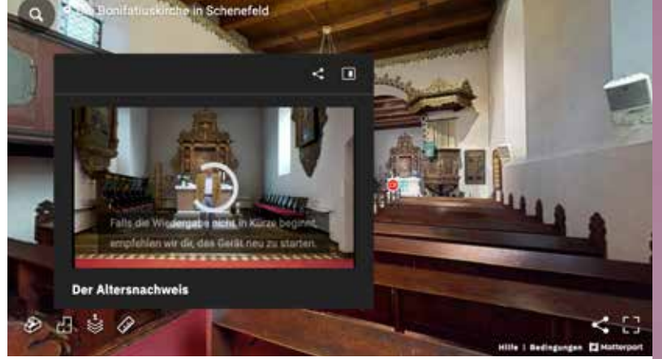
Richtig. Gegenüber Mitarbeiterinnen und Mitarbeitern bleiben aus Unternehmenssicht die Anker des Vertrauens wie sie sind: Qualifikationsnachweise, Sicherheitsüberprüfung und vertragliche Vereinbarungen. Auch Arbeitnehmerrechte bleiben unberührt. <

MARTIN MEINTS

ist seit 2009 IT-Sicherheitsbeauftragter bei Dataport. Der studierte Chemiker wandte sich schon früh der IT zu, war unter anderem IT-Leiter, Netzwerkplaner und Prüfer beim Unabhängigen Landeszentrum für Datenschutz in Schleswig-Holstein.

MEHR INPUT

IT-Sicherheit bei Dataport
https://dataport.de/it-sicherheit



DIE ÄLTESTE KIRCHE SCHLESWIG-HOLSTEINS KANN MAN VIRTUELL BESUCHEN.

_BONIFATIUS IN BITS UND BYTES

TEXT: Jürgen Gressel-Hichert

Sie steht mitten im Dorf, die Bonifatius-Kirche in Schenefeld. Große Feldsteine im unteren Bereich des Gotteshauses lassen schon auf den ersten Blick eine lange Geschichte erahnen. Und in der Tat ist die Schenefelder Dorfkirche ein geschichtsträchtiges Juwel. Ihre Ursprünge reichen bis ins Jahr 811.

Ein solcher Schatz muss für die Nachwelt erhalten werden, dachte sich die Gemeinde vor ein paar Jahren. Deshalb hat sie zusammen mit der regionalen Stiftung Krinkberg überlegt, die Kirche vollständig digital zu dokumentieren und dabei auch deren Geschichte zu erzählen. Das gehört zur „digitalen Daseinsvorsorge“ für die Bürger der Kommune und ihre Besucherinnen. Alle sollen teilhaben am kulturellen Reichtum der Region.

Der Rundgang beginnt mit einem Videogruß von der Pastorin Katharina Schunck: „Herzlich willkommen in Schenefeld!“ Kleine, auf den Boden projizierte Kreise weisen den Weg durch das Kirchenschiff. Von dort kann man sich in alle Richtungen und über zwei Etagen bewegen. Dabei lässt sich manches entdecken, was beim „echten“ Besuch nicht sofort ins Auge springt: Inschriften aus dem 17. Jahrhundert beispielsweise oder Details am spätbarocken Altar. Auch der Glockenturm ist geöffnet. Eine schmale Stiege führt nach oben – ganz ohne schweißtreibenden Aufstieg.

Die Idee zur zur virtuellen Dokumentation der Kirche entstand im DigitalHub Hennstedt/Amt Eider von dataport.kommunal. Für Konzeption und Umsetzung wurden die Expertinnen des Dataport Kultur.Kompetenzzentrums hinzugezogen. Mit umfangreichem 3-D-Equipment und spezieller Software haben die IT-Spezialisten von Dataport die Kirche in monatelanger Arbeit mit Grundriss und allen Ebenen dokumentiert.

An mehreren Stellen laden Stoppschilder zu kurzen Videogeschichten ein: Der Lokalhistoriker Reinhard Heesch etwa erzählt, wie er selbst die ältesten Schichten der Kirche bei einer sogenannten Notgrabung freigelegt hat. Er konnte damit beweisen, dass die Grundmauern der heutigen Kirche mehr als 1.200 Jahre alt sind.

„Das Projekt soll uns dabei helfen, hier im Hinterland Stück für Stück einen sanften Tourismus zu entwickeln.“ Für Bürgermeister Johann Hansen war das Digitalisierungsprojekt wichtig für das Standortmarketing von Schenefeld. Und es soll Vorbildcharakter haben – auch für andere noch zu hebende kulturhistorische Schätze. <

MEHR INPUT

Der virtuelle Rundgang durch die Bonifatius-Kirche (auf der Startseite)
https://www.schenefeld-mittelholstein.de

Projekt auf der Homepage von dataport.kommunal
https://dataport-kommunal.de/virtuelle-kirche

"ICH GESTALTE DEN DIGITALEN WANDEL AKTIV MIT."

Von Anfang an Gelerntes praktisch anwenden – das ist für Alperen Sapmaz einer der großen Vorzüge seines Dualen Studiums. Der gelernte Fachinformatiker studiert im 4. Semester Wirtschaftsinformatik an der Dualen Hochschule Schleswig-Holstein (DHSH). Sein Wissen erprobt er täglich bei Dataport.

An welchem Projekt arbeitest du gerade?
Am „Ersti-Kompass“. Dabei handelt es sich um eine interne Webseite der DHSH, auf der wir neuen Studierenden umfassende Informationen über den Start ins Studium anbieten wollen. An diesem gemeinnützigen Projekt sind Product Owner, Scrum Master, ich als Projektleitung und Entwicklerinnen beteiligt. Dataport stellt uns für solche Projekte genügend Zeit während der Hospitationen zur Verfügung, das finde ich großartig.

Dein Lieblingsprojekt bisher?
Im vorigen Sommer war ich in der Praxisphase beim Dataport Consulting. Es ging darum, mit Kunden aus Schleswig-Holstein und Hamburg zu klären: Lohnt es sich, Prozesse aus deren Fachverfahren zu automatisieren? Und wenn ja, bei welchen ist das möglich und vor allem nützlich? Über die Prozessautomatisierung im RPA-Projekt (Robotic Process Automation) habe ich dann eine wissenschaftliche Arbeit geschrieben.

Mit welchem Inhalt?
Ich wollte ermitteln, welche Erfolgsfaktoren es für die Prozessautomatisierung gibt. Deren Ziel ist natürlich, Kosten zu senken, die Anzahl an „stupiden“ und eintönigen Aufgaben für Mitarbeitende zu reduzieren und Fachkräfte da einzusetzen, wo sie wirklich gebraucht werden.

Was begeistert dich an deiner Tätigkeit?
Ich kann in verschiedenen Projekten immer wieder neue Blickwinkel auf die Verwaltungsdigitalisierung einnehmen und mich stetig weiterentwickeln. Mein Ziel ist es, mit meinen fachlichen und sozialen Kompetenzen einen Mehrwert für unsere Gesellschaft zu schaffen. <

KURZPROFIL

Wer: Alperen Sapmaz, 23
Was: Dualer Student, Wirtschaftsinformatik
Woher: Kiel

DIGITALE ZWILLINGE MACHEN BAUWERKE UND STADTPLANUNG EFFIZIENTER UND NACHHALTIGER.

_SMARTE DOPPELGÄNGER

TEXT: Claudia Lohmann

Scheinbar schwerelos schwebt die „Golden Gate Bridge von Hamburg“ an ihren langen Stahlseilen über dem Köhlbrand, einem Seitenarm der Süderelbe. Ihre Tage sind jedoch gezählt. Die marode Brücke ist 50 Jahre alt und soll abgerissen werden. Ein Neubau kann sich hinziehen. Bis dahin hilft ein digitaler Zwilling, die Brücke funktionstüchtig zu halten.

IT- und Bau-Experten haben die alte Brücke zu neuem Leben erweckt – als smartBRIDGE. So heißt der digitale Zwilling der Köhlbrandbrücke, der diese virtuell kopiert. Im Modell gleitet ein Strom von grünen und blauen Lichtern pulsierend über Fahrbahnen, Träger und Seile der smartBRIDGE. Diese verhält sich genauso wie die echte Brücke. So können etwa Abnutzung und Korrosionsschäden am digitalen Zwilling durchgespielt werden, bevor sie weiter fortschreiten. Das spart Zeit und Kosten bei der Instandhaltung und bei Schadensprognosen.

//MODELLPROJEKT AUS HAMBURG

Die Hamburger smartBRIDGE ist ein Pilotprojekt mit dem Ziel, Brücken in ganz Deutschland zukunftsfit zu machen. Digitale Zwillinge sollen sowohl bestehende Bauwerke als auch Neubauten optimieren. Letztere könnten mit Hilfe von digitalen Zwillingen schneller entwickelt und in Betrieb genommen werden.

Das komplexe System sammelt Messdaten in Echtzeit, visualisiert sie und hält Schnittstellen bereit, um die Daten zu pflegen und weiterzuverwenden. Digitale Zwillinge sind aber weit mehr als nur 3D-Modelle, sie sind „so etwas wie das digitale Stethoskop des Bauwerksprüfers der Zukunft“, wie es auf der Homepage des Projektes heißt. Dieses wird von einem Technologie- und Bauingenieur-Konsortium im Auftrag der Hamburg Port Authority durchgeführt und durch das Bundesministerium für Digitales und Verkehr gefördert.

//REVOLUTION FÜR DIE VERKEHRSPLANUNG

Die smarten Doppelgänger können die Verkehrsplanung entscheidend voranbringen und dabei helfen, Schäden erst gar nicht entstehen zu lassen. Digitale Zwillinge simulieren Nutzungs- und Belastungsszenarien virtuell, schon bevor das Bauwerk fertiggestellt ist.

Seit 2021 ist die Köhlbrandbrücke Teil des Bundesfernstraßennetzes. Dieses besteht aus mehr als 50.000 Kilometern Bundesstraßen und Autobahnen sowie fast 40.000 Brücken. Jede vierte Brücke ist sanierungsbedürftig. Ein bundesweites Erhaltungsmanagement soll die Brücken langfristig stabil und verkehrssicher machen. Das smartBRIDGE-Projekt aus Hamburg wird nun Teil davon und unterstützt derzeit die Instandhaltung der Nibelungen-Brücke. Diese verbindet Worms mit den hessischen Städten Lampertheim und Bürstadt.

//MODERNE STADTPLANUNG

Auch Städte lassen sich auf diese Weise mit all ihren Bauwerken und ihrer Infrastruktur abbilden und weiterentwickeln. Stadtplanerinnen benutzen digitale Zwillinge für ihre Smart-City-Strategien. Diese sollen Städte effizienter, nachhaltiger und lebenswerter machen. Hamburg ist seit 2021 zusammen mit Leipzig und München an dem kollaborativen Modellprojekt Connected Urban Twins beteiligt. Dieses wird von der Bundesregierung gefördert. Es geht zum Beispiel um Bahnhöfe, Schulen, Straßen, Radwege, Grünflächen oder um die Wasserversorgung. Die erarbeiteten Lösungen werden auch anderen Städten zur Verfügung gestellt. Der Wissenstransfer und das Teilen von Erkenntnissen sind Kernpunkte des Projekts.

[...]

_SOLCHE KONZEPTE KOMMEN FÜR DIE ALTE KÖHLBRANDBRÜCKE IN HAMBURG ZU SPÄT, KÖNNTEN FÜR DEN NEUBAU ABER NÜTZLICH SEIN.

//BÜRGER ENTSCHEIDEN MIT

„Neu entwickelte Anwendungen sind open-source-basiert“, betont Marina Brink, verantwortlich für die Öffentlichkeitsarbeit im Projekt Connected Urban Twins. „Um ein gemeinsames Verständnis zu fördern, haben wir außerdem eine DIN-Spezifikation für urbane digitale Zwillinge initiiert.“ Auch innovative Formate der Bürgerbeteiligung spielten eine wichtige Rolle, so Brink. Sie reichen von der Mitsprache bis hin zur Mitentscheidung und können sowohl analog als auch digital durchgeführt werden.

Solche Konzepte kommen für die alte Köhlbrandbrücke in Hamburg zu spät, könnten für den Neubau aber nützlich sein. Über diesen soll der Verkehr ab circa 2042 rollen. Und dann wird die neue Köhlbrandbrücke auch ihren digitalen Zwilling haben und möglicherweise länger leben als die alte. <

MEHR INPUT

Pilotprojekt smartBRIDGE
https://digitalerzwilling.bundesfernstrassen.de

Connected Urban Twins
https://www.connectedurbantwins.de

smartBRIDGE
https://homeport.hamburg

IN VORHERGEHENDEN HEFTEN HABEN WIR ERKLÄRT, WIE QUANTENCOMPUTER FUNKTIONIEREN UND WO SIE EINGESETZT WERDEN KÖNNEN. INZWISCHEN BOOMT DIE FORSCHUNG IN DIESEM BEREICH.

_QUANTENSPRÜNGE NACH VORN

TEXT: Carmen Gräf

Die Bezeichnungen der Rechen- und Speichereinheiten hören sich an wie die Beschreibungen aus einem Science-Fiction-Roman: Gitter aus Laserlicht, neutrale Atome und wundersame Verschränkungen. Quantencomputer sollen Probleme lösen, an denen selbst die leistungsstärksten Supercomputer bisher scheitern.

Der Unterschied zwischen der Leistungsfähigkeit eines Quantencomputers und eines normalen Heim-PCs ist etwa so groß wie der zwischen einem Überschall-Jet und einem Zeppelin. Kein Wunder, dass auch das Deutsche Zentrum für Luft- und Raumfahrt in den weltweiten Wettbewerb um die Entwicklung von Quantencomputern eingestiegen ist. In dessen Auftrag baut das Start-up planqc aus Garching bei München Quantencomputer mit Neutral-Atomen. Normalerweise kommen elektrisch geladene Teilchen zum Einsatz. Neutrale Atome verhalten sich dagegen, wie der Name sagt, neutral. Sie lassen sich mithilfe von speziellen Lasern gut in die Rechenbausteine Qubits umwandeln, die für das Quantencomputing nötig sind.

HEFT NR. 2/2022 BAUSTEINE FÜR EIN GESUNDES LEBEN

Die Quantenwissenschaft wurde im Jahr 2023 mit dem Chemie-Nobelpreis geehrt. Ein Forscherteam aus den USA erhielt die Auszeichnung für die Entdeckung der Quantenpunkte. Diese gelten als zentrale Bausteine für das Quanteninternet. Das muss allerdings noch entwickelt werden und würde dann als besonders sicher gelten. Die entsprechenden Teilchen-Computer versprechen höhere Sicherheitsstandards. Ein Team um den Physiker Marcus Huber vom Wiener Institut für Quantenoptik und Quanteninformation der Österreichischen Akademie für Wissenschaften forscht daran, wie man mithilfe der neuen Technologie Verschlüsselung sicherer gestalten kann.

Auch die Europäische Union setzt auf diese Zukunftstechnologie. 14 Mitgliedsstaaten, darunter Deutschland, haben Ende 2023 die Europäische Deklaration zu Quantentechnologien verabschiedet. Das Ziel: ein europaweites Netzwerk mit einem breiten Spektrum an industriellen und wissenschaftlichen Anwendungen. Damit soll Europa fit werden für den internationalen Wettbewerb. Denn noch in diesem Jahr will ein Anbieter aus Boston/USA den ersten kommerziellen, fehlerkorrigierten Quantencomputer auf den Markt bringen. Diese Fehlerkorrektur beruht auf einer neuartigen technischen Struktur und macht Quantensysteme sehr viel zuverlässiger als bisher. <

WIE FINDEN SIE DEN DATA[RE:]PORT?

Helfen Sie uns, den data[re:]port noch besser zu machen. Das Magazin wird für Sie gemacht und deshalb möchten wir gern erfahren, wie Sie es finden und wie Sie es nutzen. Bitte beantworten Sie uns online ein paar Fragen dazu. Das geht schnell, ist vollkommen anonym und sogar gut für die Umwelt.

Die wenigen Minuten, die Sie dafür benötigen, sorgen für wertvolle Erkenntnisse – und für mehr Biodiversität in Norddeutschland! Denn für jeden ausgefüllten Online-Fragebogen spendet Dataport zwei Euro an den gemeinnützigen Verein blühfläche.de e.V.

Das Geld wird in den Ausbau der Blumenwiesen des Vereins in der Nähe von Bremen investiert. Diese blühen fast das ganze Jahr über und sind ein sicherer Rückzugsort für viele Tiere.

Die Ergebnisse der Umfrage nutzen wir bei Dataport dazu, das Magazinkonzept kritisch zu prüfen und gegebenenfalls Ihren Wünschen und Anforderungen entsprechend anzupassen. <

SO UNTERSTÜTZEN SIE UNS:

- Einfach den **QR-Code scannen *oder***
- auf die Website gehen
www.datareport.online/leserumfrage

- Die Umfrage ist online und vollkommen anonym.
- Personenbezogene Daten werden nicht gespeichert.

Bitte beantworten Sie den Fragebogen bis zum 17.07.24

VIELEN DANK FÜR IHRE UNTERSTÜTZUNG! WIR SIND SEHR GESPANNT AUF IHRE ANTWORTEN.

DER BORKENKÄFER VERNICHTET GANZE WÄLDER. KÜNSTLICHE INTELLIGENZ SOLL HELFEN, DIE SCHÄDLINGE FRÜHZEITIG ZU ENTDECKEN.

_DEN BORKENKÄFER IN SCHACH HALTEN

TEXT: Christina Sartori

Er ist keine zwei Zentimeter groß, aber er kann einen ganzen Wald vernichten: der Borkenkäfer. Im Nationalpark Bayerischer Wald hat die Borkenkäfer-Population deutlich zugenommen, aber auch in anderen Teilen Deutschlands verbreitete sich der Schädling in den vergangenen Jahren stark.

Ein Projekt der österreichischen Forschungsgesellschaft Joanneum Research will mit Hilfe von künstlicher Intelligenz (KI) einen drohenden Borkenkäfer-Befall erkennen und so Forstbesitzern helfen, diesen zu vermeiden oder wenigstens zu begrenzen.

Zunächst trainierte man die KI mit Hilfe von maschinellem Lernen. Als Datengrundlage dienen optische Satellitenbilder der Sentinel-2-Mission der Europäischen Weltraumorganisation, die alle fünf Tage aufgenommen werden, beschreibt Janik Deutscher, Forschungsgruppenleiter Fernerkundung und Geoinformation. „In den bekannten befallenen Beständen versuchen wir, aus den Satellitenbild-Zeitreihen zu erkennen, wie sich das spektrale Signal vor und während eines Befalls verhält.“ Im Ergebnis werden rote Punkte sichtbar, die sich rasch ausdehnen. Im Vergleich mit aktuellen Satellitenaufnahmen lassen sich erkrankte Baumbestände schnell identifizieren.

Das Projekt AIDForHeRi (AI-driven forest health risk indicator) geht noch einen Schritt weiter: Wie es der Name beschreibt, soll es mit Hilfe von KI vorhersagen, wie groß das Risiko eines zukünftigen Borkenkäfer-Befalles ist. „Die KI wurde dabei trainiert mit Risikomodellen, die Experten auf Basis von bekannten Befallsflächen, dem Fichtenanteil im Wald und täglichen meteorologischen Informationen erarbeitet haben“, erklärt Janik Deutscher.

So erhöhen zum Beispiel lange Dürreperioden, viele Fichten im Wald und nahegelegene befallene Flächen das Risiko. Eine Information, die es Waldbesitzerinnen ermöglicht, größeren Schaden abzuwenden, indem sie beispielsweise altes Holz aus dem Wald entfernen. Erste Versuche mit AIDForHeRi verliefen erfolgreich. Die Prognose könnte sogar noch verbessert werden: Denn abhängig vom Wetter schlüpfen pro Jahr ein bis drei Käfer-Generationen. Viel Arbeit für Waldbesitzer und Forstleute, die anhand der Prognosen aber in Zukunft schneller eingreifen können, um den Wald zu retten. <

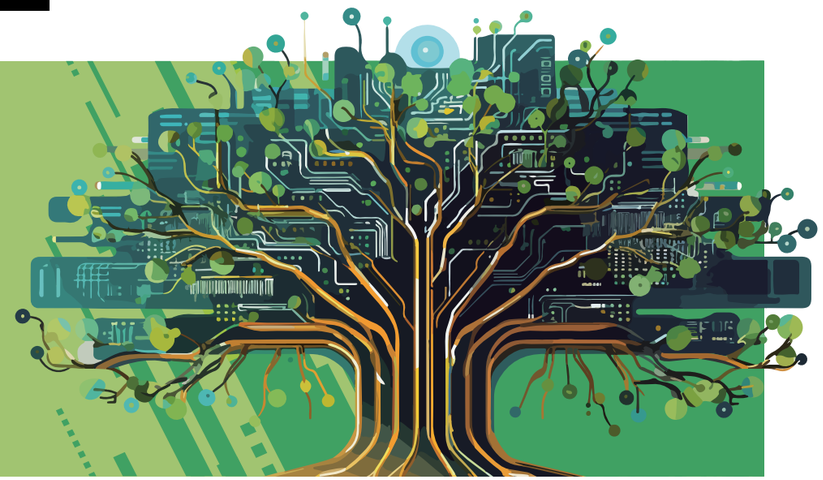
MEHR INPUT

Homepage Joanneum Research (Suchwort: Borkenkäfer)
https://www.joanneum.at

IM DEZEMBER IM NEUEN DATAREPORT

DAS SPECIAL DER NÄCHSTEN AUSGABE

Künstliche Intelligenz (KI) kann für nachhaltigen Umwelt- und Klimaschutz eingesetzt werden. Allerdings sollte KI auch nachhaltig sein, wenn es um Energieverbrauch und CO2-Emissionen geht.



RÜCKBLICK

Binnenschifffahrtskapitäne sitzen künftig in Duisburg – und das Schiff fährt den Rhein alleine hinauf oder herunter.

DIGITAL PRACTICE

Im Erzgebirge gibt es ein digitales Hochgeschwindigkeits-Testfeld für das Bahnfahren der Zukunft. Basis dafür ist ein 5G-Netz.

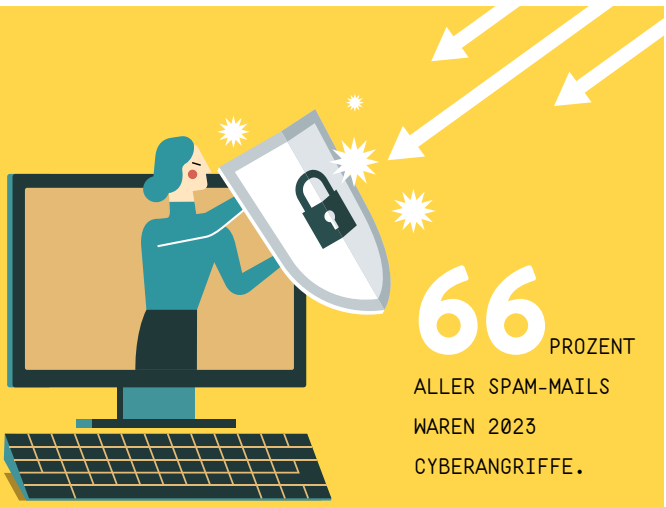
IMPRESSUM
Herausgeber:
Dataport
Anstalt des öffentlichen Rechts
Altenholzer Straße 10-14
24161 Altenholz
Telefon (0431) 3295-0
Telefax (0431) 3295-6410
Internet: www.dataport.de
E-Mail: Redaktion@dataport.de

Redaktionsbeirat: Michael Hauschild, Gerd Schramm
Redaktion: Britta Heinrich (v.i.S.d.P), Andrea Brücken (Redaktionsleitung), Carmen Gräf, Jürgen Gressel-Hichert, Kirsten Wohlfahrt
Autoren: Fabian Baumheuer, Jürgen Gressel-Hichert, Carmen Gräf, Markus Hertwig, Claudia Lohmann, Christina Sartori
Reproduktion: oeding print GmbH
Layout: Melanie Erdmann, Jan Neumann
Konzept: Die Werbegenossen eG
Auflage: 4.000, Ausgabe 2 / Juni 2024

HV8
www.blauer-engel.de/uz195

BILDNACHWEIS
Titel tommy/iStock, S.2 links oben aprott/iStock.com, unten Nuthawut Somsuk/iStock.com, rechts oben © Dataport, rechts mitte freepik.com, rechts unten Henrik_L/iStock.com, S.3 Tristan Vankann, S.4 oben SA 4.0 DEED, unten freepik.com, S.5 oben gorodenkoff/shutterstock, mitte freepik.com, unten Synergee/iStock.com, S. 7 Andrey Popov/adobe.stock.com, S.8 Gorodenkoff/iStock.com, S.9 Andreas-Reichel_(c)Dataport, S.12 © RUB, Marquard, S.14/15 vs148/shutterstock, S. 15 © Dataport, S.16 © Dataport, S.17 © kadriert, S.18/19 Shaumiaa Vector/iStock.com, S.19 ro70_de/stock.adobe.com, S.20 Hurca!/stock.adobe.com, S.21 Tania Anisimova design/shutterstock, freepik.com, S.22 Alexey Protasov/stock.adobe.com, aprott/iStock.com, S.23 oben filo/iStock.com, megan/stock.adobe.com, unten links ceasar/iStock.com, unten rechts smartboy10/iStock.com, S.24 oben links Naddiya/iStock.com, Heena Rajput/iStock.com, oben rechts sorbetto /iStock.com, mitte blocberry/iStock.com, unten links undefined undefined./iStock.com, unten rechts Andrew_Rybalko/iStock.com

6 MONATE BRAUCHEN DEUTSCHE UNTERNEHMEN DURCHSCHNITTLICH, UM EINE STELLE FÜR CYBERSICHERHEIT (MIT EINER QUALIFIZIERTEN MITARBEITERIN) ZU BESETZEN.



66 PROZENT ALLER SPAM-MAILS WAREN 2023 CYBERANGRIFFE.

30 PROZENT DER MITARBEITER VON UNTERNEHMEN SCHÄTZEN IHRE KOMPETENZ BEIM THEMA IT-SICHERHEIT ALS GERING EIN.

203 MILLIARDEN EURO SCHADEN RICHTETEN CYBERATTACKEN 2022 HOCHGERECHNET IN DEUTSCHEN UNTERNEHMEN AN.

775 E-MAILS MIT SCHADPROGRAMMEN WERDEN TÄGLICH IN DEUTSCHEN REGIERUNGSNETZEN ABGEFANGEN.