



Der Weg zu einer pragmatischen KI-Richtlinie

.....

Unser aktuelles Whitepaper
ist ab sofort abrufbar.

Seite 6



Ihr Weg durch den NIS-2-Dschungel

Flussdiagramm nutzen
und gezielt Maßnahmen planen

Seite 10

Datenschutz trifft digitale Bildung

Die Niedersächsische Bildungscld
für tausende Schulen

Seite 12

1. Norddeutsches KI-Forum

Rückblick auf unsere
Veranstaltung im Februar

Seite 16



Praxistage Datenschutz & Informationssicherheit

in Gesundheits- und Sozialwesen, Kirche & Non-Profits

Freuen Sie sich auf Tage voller spannender Vorträge, praxisnaher Workshops und inspirierender Diskussionen. Die Praxistage sind Ihre Gelegenheit, sich über die neuesten Entwicklungen im Bereich Datenschutz und Informationssicherheit zu informieren und wertvolle Kontakte zu knüpfen. Nach zwei erfolgreichen Veranstaltungen in Paderborn findet die Tagung dieses Mal in Hannover statt.



10.–12.09.2025



Designhotel Wienecke
Hannover

Alle Informationen
finden Sie hier:



Editorial

News
Seite 4

**Der Weg zu
einer pragmatischen
KI-Richtlinie**
Unser aktuelles Whitepaper
Seite 6

**Ihr Weg durch den
NIS-2-Dschungel**
Flussdiagramm nutzen
und gezielt Maßnahmen planen
Seite 10

**Datenschutz trifft
digitale Bildung**
Die Niedersächsische Bildungscloud
für tausende Schulen
Seite 12

Akademie
Seite 15

**1. Norddeutsches
KI-Forum**
Rückblick auf unsere
Veranstaltung im Februar
Seite 16

Liebe Leserin, lieber Leser,

manchmal fühlt sich die digitale Welt an wie ein Dschungel: neue Technologien, neue Vorschriften, neue Chancen – und mittendrin die Frage: Wo fange ich an? Genau deshalb haben wir für diese Ausgabe Themen ausgewählt, die Orientierung geben und Mut machen.

Unser neues Whitepaper „Der Weg zu einer pragmatischen KI-Richtlinie“ bietet Ihnen einen klaren Einstieg in den verantwortungsvollen Umgang mit Künstlicher Intelligenz – praxisnah, realitätsbezogen und ab sofort für Sie verfügbar.

Wie digitale Innovation und Datenschutz Hand in Hand gehen können, zeigt ein besonders gelungenes Beispiel aus Niedersachsen: Die Niedersächsische Bildungscloud ermöglicht zehntausenden Schulen sicheres, offenes und datenschutzkonformes Lernen.

Falls Sie beim Stichwort „NIS-2“ noch Fragezeichen im Kopf haben: Keine Sorge. Unser Artikel „Ihr Weg durch den NIS-2-Dschungel“ nimmt Sie an die Hand. Mit einem klaren Flussdiagramm helfen wir Ihnen, gezielt die nächsten Schritte zu planen – damit Cybersicherheit nicht zur Stolperfalle wird.

Und schließlich blicken wir zurück auf das 1. Norddeutsche KI-Forum in Hannover. Fachleute aus ganz Deutschland diskutierten dort, warum fehlendes Know-how oft der größte Hemmschuh bei der Einführung von Künstlicher Intelligenz ist – und wie wir gemeinsam Lösungen finden können.

Wir wünschen Ihnen viel Freude beim Lesen, beim Entdecken – und beim Loslegen!

Herzliche Grüße



Thomas Althammer & Niels Kill

Darüber wird gesprochen



KLICK/SCAN

Weitere aktuelle Themen sowie die Anmeldemöglichkeit für den Althammer & Kill-Newsletter finden Sie unter: althammer-kill.de/news



Zwei Messen, viele Gespräche, ein Ziel: Digitalisierung sicher gestalten

Im April waren wir gleich doppelt unterwegs: auf der HANNOVER MESSE und der ALTENPFLEGE Messe in Nürnberg. Zwei sehr unterschiedliche Veranstaltungen – mit einer gemeinsamen Erkenntnis: Die Themen Datenschutz, Informationssicherheit und Künstliche Intelligenz stehen bei vielen Organisationen ganz oben auf der Agenda.

In Hannover – auf einer der weltweit wichtigsten Industriemesen – haben wir am Gemeinschaftsstand des Niedersächsischen Ministeriums für Wirtschaft, Verkehr, Bauen und Digitalisierung zahlreiche Gespräche geführt. Vom

Einsatz von KI in der Produktion bis zur Frage, wie sich mittelständische Unternehmen konkret auf die NIS-2-Richtlinie vorbereiten können: Das Interesse war groß,



der Bedarf an praxisnahen Lösungen spürbar.

Ganz andere, aber nicht weniger relevante Fragen bewegten das Fachpublikum auf der ALTENPFLEGE Messe in Nürnberg – der Leitmesse für Pflegewirtschaft, Sozialträger und Dienstleister. Hier lag der Fokus auf Technologien, die den Alltag in der Pflege unterstützen können. Besonders gefragt: Wie lassen sich digitale Anwendungen sinnvoll und sicher in bestehende Strukturen integrieren? Wie gelingt Datenschutz bei begrenzten Ressourcen?

Unser Fazit: Die Digitalisierung ist überall spürbar – in der Industrie wie in der Pflege. Aber sie braucht Orientierung, Wissen und Vertrauen. Genau dafür stehen wir – im direkten Austausch und mit einem klaren Fokus auf machbare Lösungen.

Fast jedes Unternehmen in der Industrie betroffen: Informationssicherheit ganzheitlich über IT und Operational Technology hinweg denken

Mehr als die Hälfte der befragten Unternehmen verzeichnete im letzten Jahr einen Cybervorfall, drei Viertel glauben, davon in den nächsten Monaten betroffen zu sein. Das sollte die Verantwortlichen für Informationssicherheit in Unternehmen hellhörig werden lassen. Schutz und Sicherheit sind nicht nur im Hinblick auf das Internet relevant, sondern ganzheitlich für Information- und auch Operational-Technology. Trotzdem sind aktuell nur zwei Prozent der deutschen Unternehmen bestmöglich auf Angriffe vorbereitet. Warum IT-Sicherheit bei Entscheidungen ganz oben auf der Agenda stehen sollte und weshalb auch der Schutz von Operational Technology immer mehr in den Fokus rückt.



KLICK/SCAN

Künstliche Intelligenz in der Automobilwirtschaft: Im Spannungsfeld zwischen technologischem Fortschritt und Datenschutz



Der Markt für Künstliche Intelligenz (KI) ist einer, der am schnellsten wachsenden. Bis zum Jahr 2030 geht Statista von einem jährlichen Zuwachs in Höhe von rund 29 Prozent und einem Marktvolumen von rund 775 Milliarden Euro aus.

Besonders die Automobilwirtschaft forscht stark an Technologien, die auf Machine Learning basieren, und kann durch den Einsatz von KI erheblich profitieren. Gleichzeitig müssen die Risiken hinsichtlich des Datenschutzes und Cybersicherheit sorgfältig abgewogen werden. In diesem Spannungsfeld gibt Thomas Althammer, Geschäftsführer des Beratungsunternehmens Althammer & Kill, einen Überblick.



KLICK/SCAN

Cyberangriffe auf soziale Organisationen: Wie Angreifende vorgehen – und wie Sie sich besser schützen

Cyberangriffe nehmen weltweit zu. Für soziale Organisationen, die oft sensible Informationen betreuen, stellt dies eine besondere Herausforderung dar. Der Schutz dieser Daten geht weit über IT-Sicherheit hinaus – er



KLICK/SCAN

bewahrt die Würde und Sicherheit von Menschen, die auf Vertrauen angewiesen sind. Doch wie genau gehen Cyberkriminelle vor? Und welche Schutzmaßnahmen sind notwendig?

Zahl des Monats

700

So viele Datenpunkte analysiert KI im Schnitt über eine Person – pro Anfrage. Moderne KI-Modelle ziehen bei der Beantwortung von Fragen oft hunderte Datenpunkte heran: Standort, Sprache, Surfverhalten, Geräteinformationen und mehr. Das macht sie effektiv – aber auch datenhungrig.

Veranstaltungen

10. September 2025, Hannover

KI Deep Dive: Künstliche Intelligenz verstehen und anwenden



Am 10. September 2025 starten wir die Praxistage mit einem intensiven Workshop-Tag zum Thema Künstliche Intelligenz. Der KI Deep Dive bietet praxisnahe Einblicke in die Funktionsweise von KI, ihren Einsatz im Umgang mit personenbezogenen Daten und die Anforderungen der KI-Verordnung. In interaktiven Workshops erarbeiten die Teilnehmenden konkrete Vorgehensmodelle und erhalten Best Practices aus realen KI-Projekten im Gesundheits- und Sozialwesen. Ein idealer Einstieg für alle, die KI nicht nur verstehen, sondern verantwortungsvoll einsetzen möchten.



KLICK/SCAN

Der Weg zu einer pragmatischen KI-Richtlinie – Unser aktuelles Whitepaper ist ab sofort abrufbar.

Verantwortliche müssen jetzt entscheiden, wie KI in den Organisationen eingeführt werden soll. Anderenfalls wird sie vielerorts als sogenannte Schatten-IT durch die Hintertür Einzug halten.

Von Jessica Henning und Dr. Martin Mühlpfordt



„Künstliche Intelligenz (KI) ist die Fähigkeit einer Maschine, menschliche Fähigkeiten wie logisches Denken, Lernen, Planen und Kreativität zu imitieren. KI ermöglicht es technischen Systemen, ihre Umwelt wahrzunehmen, mit dem Wahrgenommenen umzugehen und Probleme zu lösen, um ein bestimmtes Ziel zu erreichen.“

So definiert es das Europäische Parlament. Generative KI hält inzwischen Einzug in vielen Unternehmen und Organisationen. Einer aktuellen IBM-Studie zufolge werden deutsche Unternehmen ihre Investitionen in KI im laufenden Jahr weiter ausbauen. 80 Prozent der Befragten berichten von Fortschritten bei der Umsetzung der KI-Strategie. Es ist absolut wichtig, sich mit dem Thema KI auseinanderzusetzen. Anderenfalls öffnen Unternehmen Tür und Tor für die Einführung von KI-Anwendungen als sogenannte Schatten-IT. Also Software, die ohne Wissen der IT-Verantwortlichen installiert und betrieben wird.

KI generiert typisches Beispiel für Einführung von Schatten-IT

Ein Mitarbeiter in der Marketingabteilung nutzt eigenständig eine generative KI wie ChatGPT oder Google Gemini, um schneller kreative Texte für Kampagnen zu erstellen. Die offizielle Unternehmenssoftware bietet keine vergleichbaren Funktionen oder ist zu umständlich. Der Mitarbeiter lädt sensible Kundendaten in die KI-Anwendung hoch, um personalisierte Vorschläge zu erhalten. Dabei umgeht er die IT-Abteilung, da der Genehmigungsprozess zu lange dauert oder die Nutzung solcher Tools offiziell nicht erlaubt ist. Dieses Verhalten birgt mehrere Risiken:

- Datenschutzverletzungen: Kundendaten könnten in Länder mit unzureichendem Datenschutzstandard übertragen werden.
- Sicherheitslücken: Die KI-Anwendung könnte ein Einfallstor für Cyberangriffe sein.

- Compliance-Verstöße: Die Nutzung der KI verstößt möglicherweise gegen interne Richtlinien oder gesetzliche Vorgaben, z. B. den EU AI-Act.
- Verlust von Geschäftsgeheimnissen: Sensible Informationen könnten ungewollt offengelegt werden.

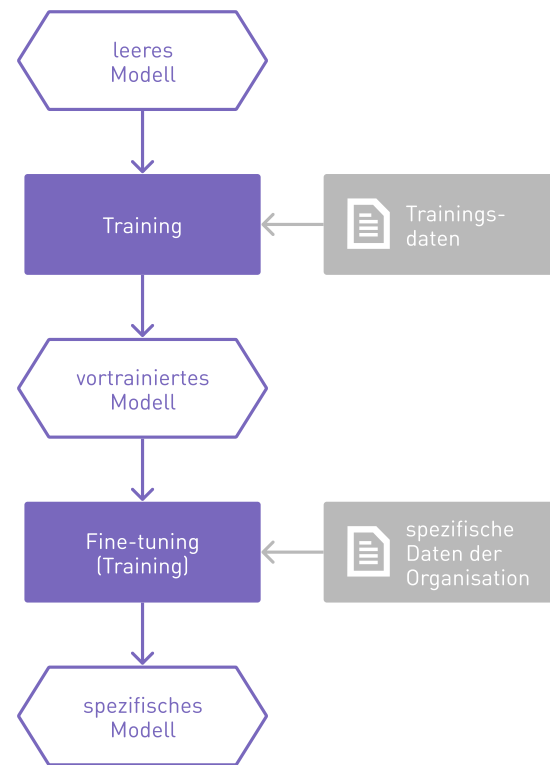
Dieses Szenario hat die KI „Perplexity.ai“ zur Frage nach einem Beispiel für die Einführung von KI-Schatten-IT in Unternehmen erstellt. Die Situationsbeschreibung deckt sich mit unseren Praxiserfahrungen und wir können sagen, dass dieses Szenario realistisch ist und so oder so ähnlich permanent in Unternehmen und Organisationen auftritt. Auf der anderen Seite sind die aufgeführten Risiken nur zum Teil korrekt. Richtig wäre bei Datenschutzverletzungen beispielsweise, dass personenbezogene Daten vom KI-Betreiber ohne Rechtsgrundlage (durch einen Auftragsverarbeitungsvertrag) übermittelt werden. Das geschieht z. B., wenn man ChatGPT mit privatem Account nutzt und dabei personenbezogene Daten eingibt. Dabei können die Daten in Ländern mit unzureichendem Datenschutzstandard übertragen werden und/oder Daten an Dritte gelangen.

Das Beispiel von Perplexity.ai im Umgang mit KI zeigt anschaulich, dass Ergebnisse, die KI liefert, immer auf Richtigkeit geprüft werden müssen. Das erzeugte KI-Ergebnis ist fast, aber nicht vollständig richtig, es klingt plausibel, muss aber überarbeitet werden. Die fehlende Nachvollziehbarkeit der Ergebnisse ist einer der Gründe für den zögerlichen Umgang von Unternehmen mit dem komplexen Thema KI. Nicht umsonst nennen Befragte einer Studie in der Sozialwirtschaft fehlendes Know-how zu KI als das größte Hindernis bei der Einführung von KI. Weitere Hemmnisse sind Datenschutzbedenken und weitere rechtliche Unsicherheiten, fehlende Leitlinien oder unklare Einsatzszenarien.

Das ab sofort kostenfreie downloadbare Whitepaper von Althammer & Kill zur Erstellung einer KI-Richtlinie bietet eine fundierte Handreichung. Es informiert über den Einsatz von KI-Systemen und KI-Methoden – sei es die Nutzung durch Mitarbeitende, die Integration in Produkte oder bei der Eigenentwicklung. Organisationen finden hier praktische Hinweise, wie sie den Vorschriften der Datenschutz-Grundverordnung (DSGVO) oder entsprechender kirchlicher Datenschutzgesetze sowie der KI-Verordnung (KI-VO) gerecht werden können.

KI-Kompetenz als Basis

Die technologischen Grundlagen Künstlicher Intelligenz sind nicht neu. Innovativ sind vor allem die Verfügbarkeit



Trainingsphase von KI-Modellen

riesiger Datenmengen und Rechenkapazitäten, die das Training sehr großer künstlicher neuronaler Netze möglich machen. Diese sind zu verblüffenden Leistungen bei der Erstellung von Texten, Bildern und Videos in der Lage. Verblüffend deshalb, weil sie ein tieferes Verständnis über den erzeugten Inhalt suggerieren. Beim verantwortungsvollen Umgang mit KI muss sich immer wieder bewusst gemacht werden, welche Ergebnisse ein KI-Verfahren liefern kann und wo dem System überzogene Fähigkeiten zugesprochen werden. Im Whitepaper werden deshalb grundlegende Begriffe wie künstliche neuronale Netze und Verfahren des maschinellen Lernens erklärt.

Wie funktioniert KI und wie wird sie reguliert?

Um die europäische KI-Verordnung (KI-VO) korrekt anwenden zu können, muss zunächst unterschieden werden, ob die einzuführende KI lediglich betrieben oder entwickelt werden soll. Denn die KI-Verordnung unterscheidet zwischen Anbietern, die als natürliche oder juristische Person, Behörde oder Einrichtung ein KI-System entwickelt, entwickeln lässt oder ein solches System in Verkehr bringt.

Betreiber sind dagegen natürliche oder juristische Personen, die ein KI-System in eigener Verantwortung

geschäftlich oder beruflich verwendet. Diese Unterscheidung zieht unterschiedliche Pflichten nach sich.

Last, not least muss klassifiziert werden, zu welcher Risikoklasse das KI-System gehört. Anwendungen, die gegen europäische Werte und Grundrechte verstoßen, sind in der EU verbotene Praktiken. Dabei geht es um Technologie, die verdeckt manipuliert, oder Menschen aufgrund ihres sozialen Status, Herkunft, Religion o. ä. bewertet (Social Scoring).

Anwendungen mit hohem Risiko sind solche, deren Ergebnisse Auswirkungen auf den Menschen haben. Man denke nur an KI-gestützte medizinische Geräte. Hier gelten strenge Transparenz- und Risikomanagementauflagen. Chatbots zur direkten Interaktion mit Menschen oder KI-Tools zur Erzeugung von Inhalten wie Text oder Bilder haben ein mittleres Risiko und unterliegen spezifischen Transparenzpflichten. Der Einsatz vieler anderer KI-Werkzeuge wie Rechtschreibprüfungen oder Empfehlungsalgorithmen sind jedoch nur mit einem minimalen oder keinem Risiko verbunden. Aber auch hier verlangt die KI-Verordnung beim Einsatz ausreichende Kompetenz seitens der Mitarbeitenden.

Jede KI ist nur so gut wie die zugrundeliegenden Daten

Soll die KI mit unternehmenseigenen Daten trainiert werden, müssen die Rechtsgrundlage und die datenschutzrechtlichen Pflichten beachtet werden. Jede Verarbeitung personenbezogener Daten bedarf einer Rechtsgrundlage. Das Training von KI-Modellen wird in aller Regel eine neue Verarbeitung sein, deren Rechtsgrundlage zu klären ist. Das Gleiche gilt, wenn die personenbezogenen Daten für das Training anonymisiert werden. Dann ist diese Anonymisierung eine neue Verarbeitung.

Die Einführung von KI-Systemen sollte – wie jede Einführung eines neuen IT-Verfahrens – gut geplant und der Umgang mit den neuen Möglichkeiten und auch Risiken geregelt werden. Darüber hinaus empfiehlt es sich, mit Pilotprojekten zu starten und den Kompetenzaufbau bei Mitarbeitenden direkt zu integrieren.

Welche Bausteine braucht eine KI-Richtlinie?

Es gibt also einiges zu beachten auf dem Weg in automatisierte und oder effiziente Prozesse über KI-Anwendungen.

Eine KI-Richtlinie gibt den Mitarbeitenden Sicherheit durch klare Regelungen und Leitplanken im Umgang mit KI. Das Whitepaper von Althammer & Kill stellt u. a. detailliert folgende Bausteine für eine Richtlinie vor:

- Ziele, Geltungs- und Anwendungsbereiche
- Compliance-Anforderungen
- Vorgaben für das Training von KI-Modellen
- Nutzungsregeln für KI-Systeme
- Nutzung externer KI-Systeme wie z. B. ChatGPT
- Einführungs- und Freigaberegungen
- Verantwortlichkeiten und Ansprechperson

Eine KI-Richtlinie ist ein Baustein auf dem Weg zu einer systematischen und ganzheitlichen Implementierung von KI-Anwendungen in Organisationen, Praxissschulungen über Pilotprojekte ein weiterer. Der bereits genannten IBM-Studie zufolge plant ein Drittel der befragten Unternehmen, im laufenden Jahr mehr als 20 KI-Pilotprojekte zu starten. Das ist eine Steigerung von 21 Prozent im Vergleich zum Vorjahr. Schwierigkeiten bei der Integration neuer KI-Lösungen in bestehende Systeme sehen dabei 44 Prozent der Studienteilnehmenden.

Das Whitepaper von Althammer & Kill bietet Informationen für die Erstellung einer umfassenden KI-Richtlinie. Darüber hinaus bietet das Unternehmen Schulungen und Workshops, KI-Kompetenz-Nachweise gemäß KI-VO, Bestandsaufnahmen für Organisationen zu KI (sog. KI-Readiness-Checks), Begleitung bei der Implementierung von KI und deren Entwicklung oder dem KI-Risikomanagement an. &



Jetzt das Whitepaper herunterladen



Das Whitepaper „Der Weg zu einer pragmatischen KI-Richtlinie“ ist ab sofort auf unserer Homepage zum kostenlosen Download abrufbar.

Ihr Weg durch den NIS-2-Dschungel

Flussdiagramm nutzen und gezielt Maßnahmen planen.

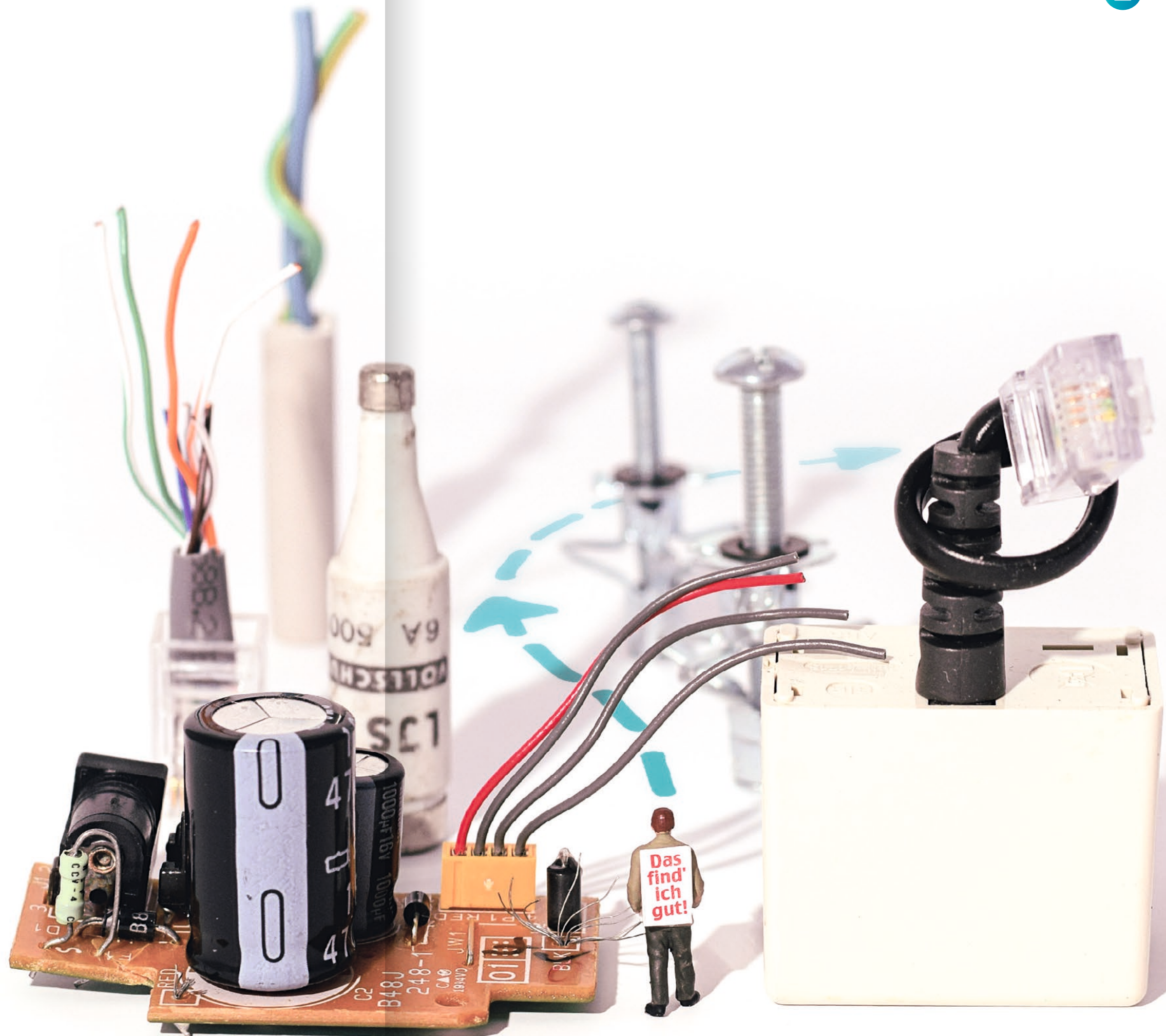
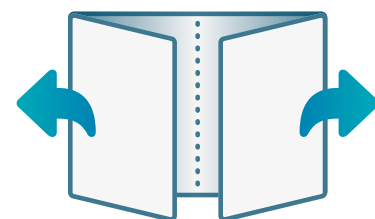
Von Winona Wenning und Wulf Bolte

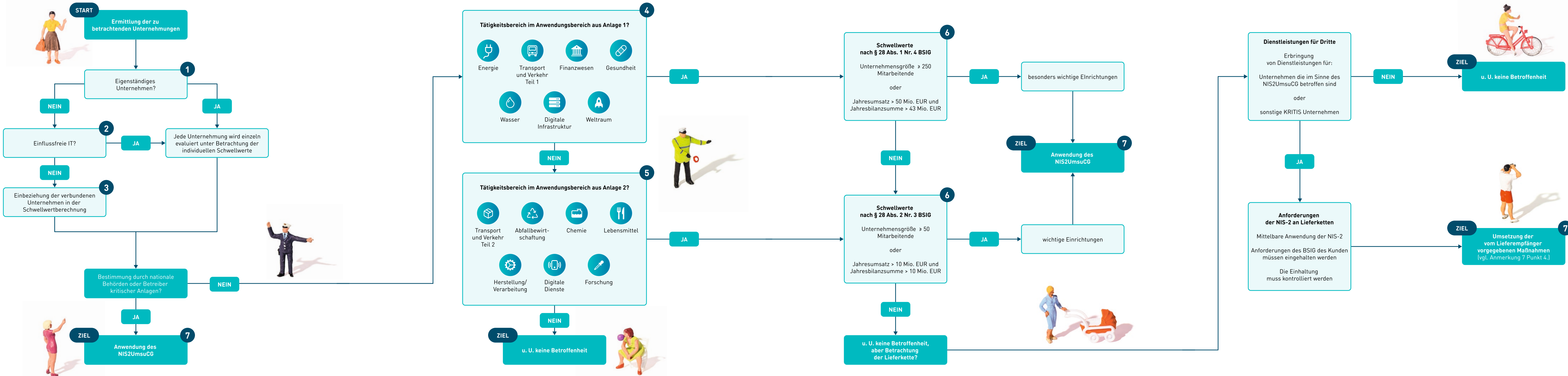
Mit der NIS-2-Richtlinie hat die EU die Messlatte für die Cybersicherheit in Unternehmen deutlich angehoben – und das auch für Unternehmen, die bisher nicht betroffen waren. Auch wenn die Überführung in deutsches Recht noch aussteht, sollten Unternehmen ihre Betroffenheit bereits jetzt bewerten.

Neben der NIS-2-Richtlinie selbst kann hierzu der Regierungsentwurf zum sogenannten NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) herangezogen werden. Kernstück des Gesetzentwurfs ist die geplante Neufassung des BSI-Gesetzes (BSIG), indem neben den konkreten Anforderungen an adressierte Unternehmen auch geregelt wird, wen die neuen Pflichten betreffen.

Neben den bereits durch KRITIS betroffenen sollen nun abhängig von Branche, Tätigkeit und Größe weitere Unternehmen als wichtige oder besonders wichtige Einrichtungen gelten, und damit unter das neue Cybersicherheitsregime fallen.

Damit Sie sich im Dickicht der Regelungen zu betroffenen Sektoren und Schwellwerten besser zurechtfinden, haben wir ein Flussdiagramm entwickelt, das Schritt für Schritt durch die Anwendbarkeitsprüfung auf Basis des aktuellen Gesetzentwurfs führt. Mit dieser Prüfung können Sie Orientierung schaffen, um rechtzeitig die richtigen Maßnahmen planen und ergreifen zu können. &





1

Arten von Unternehmen

Eigenständige Unternehmen sind völlig unabhängig. Sie halten nur Minderheitsbeteiligungen (< 25 %) und kein anderes Unternehmen ist an ihnen selbst beteiligt.

Partnerunternehmen haben eine Beteiligung an einem anderen Unternehmen, welche größer als 25 % ist, aber 50 % nicht überschreiten.

Verbundene Unternehmen übersteigen bei der Beteiligung die Grenze von 50 %.

2

Einflussfreie IT?

Eine IT ist einflussfrei, wenn das Unternehmen Entscheidungen bzgl. der IT-Systeme und Prozesse eigenständig trifft, insb. der Beauftragung von Dienstleistern.

Eine unselbstständige IT liegt vor, wenn Systeme und Prozesse vollständig von der Konzernmutter betrieben werden und Tochterunternehmen keinen Einfluss nehmen.

Im Zweifel kommt es auf die Selbstständigkeit der IT an, welche für den NIS-2-relevanten Tätigkeitsbereich notwendig ist, z. B. das KIS in Kliniken.

3

Einbeziehung im Verbund

Verbundene Unternehmen gehen zu 100 % in die Betrachtung der Schwellwerte ein.

Partnerunternehmen werden anteilig gemäß des Beteiligungsumfanges eingerechnet.

4

Ermittlung NACE Code als Ausgangspunkt?

Soweit bekannt, kann Ihnen der NACE Code Ihres Unternehmens einen Anhaltspunkt für die Einordnung in die Tätigkeitsbereiche, welche in den Anwendungsbereich des NIS2UmsuCG fallen, bieten.

5

Mehrere Tätigkeitsbereiche

Bei der Prüfung der Schwellwerte sind alle Unternehmensteile zu berücksichtigen, welche in den durch Anlage 1 und Anlage 2 definierten Tätigkeitsbereich agieren.

Übergeordnete Abteilungen wie Finance oder HR gehen anteilig in die Berechnung der Kennzahlen ein.

6

Berechnungshinweise Mitarbeitende

Mitarbeitende = alle Lohn- und Gehaltsempfänger, Leih- und entliehene Arbeitnehmer sowie Teilzeitkräfte anteilig.

Keine Mitarbeitende = Auszubildende; sowie Mitarbeitende in Mutterschafts- oder Elternurlaub.

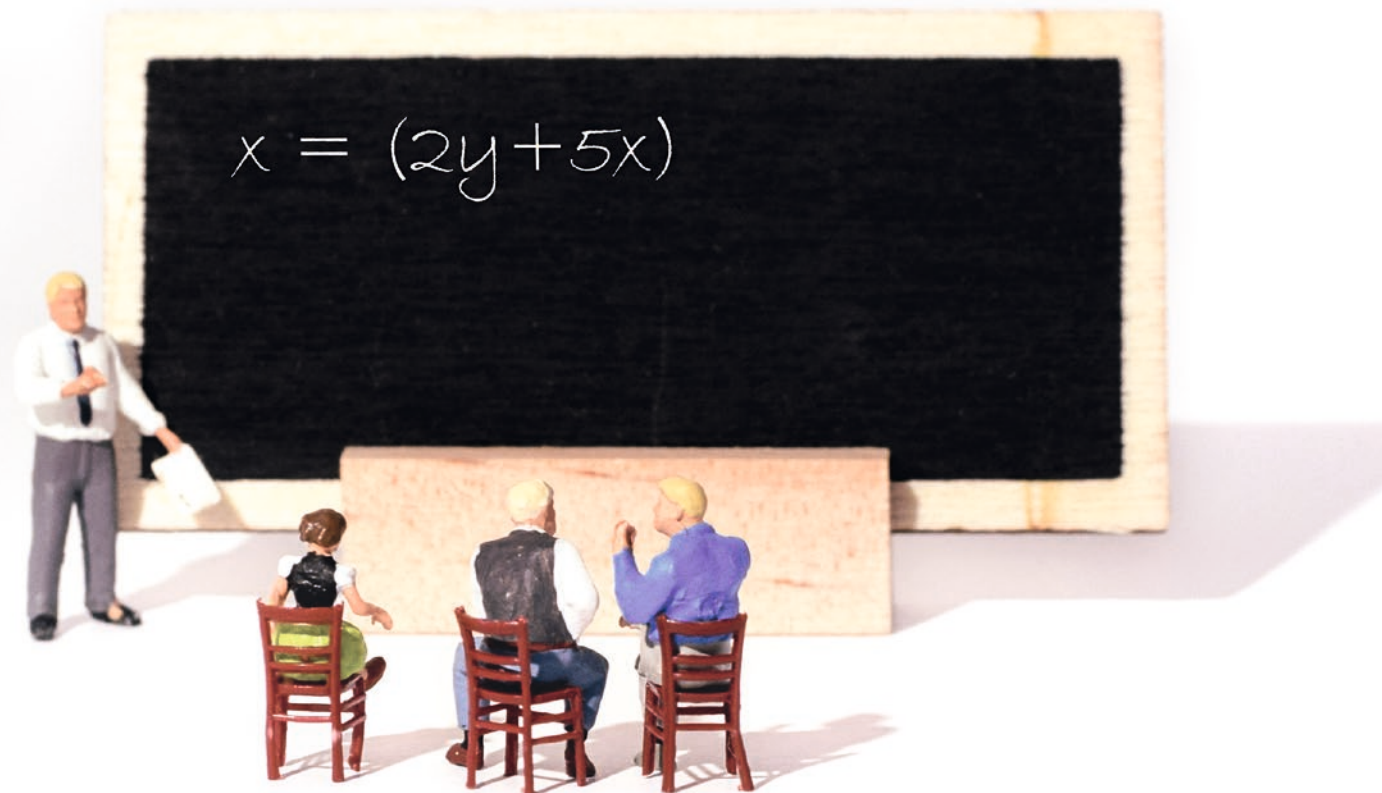
Es gilt die Zahl der Mitarbeitenden zum Abschluss des letzten Geschäftsjahres.

7

Allgemeine Risikomanagementmaßnahmen für besonders wichtige und wichtige Einrichtungen nach dem NIS2UmsuCG

Mindestumfang an Maßnahmen unter Berücksichtigung von „Stand der Technik“:

- Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik
- Bewältigung von Sicherheitsvorfällen
- Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
- Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik
- grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Sicherheit in der Informationstechnik
- Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und für das Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.



Datenschutz trifft digitale Bildung

Die Niedersächsische Bildungscloud ermöglicht digitales Lernen für tausende Schulen – mit höchsten Datenschutzstandards und einer Open-Source-Architektur.

Von Fabian Brandenburger

Wie kann eine digitale Lernplattform flächendeckend für tausende Schulen bereitgestellt werden – und gleichzeitig höchste Datenschutzstandards erfüllen? Diese Frage stand im Mittelpunkt der Entwicklung der Niedersächsischen Bildungscloud (NBC). Die Landesinitiative n-21: Schulen in Niedersachsen online e. V. setzte dabei auf eine enge Zusammenarbeit mit Datenschutz und Open-Source-Technologien, um eine zukunftssichere, datenschutzkonforme Lösung für digitales Lernen zu schaffen.

„Unsere Vision war es, eine flexible, sichere und datenschutzkonforme Plattform zu entwickeln, die Lehrkräfte,

Schülerinnen und Schüler bestmöglich unterstützt“, erklärt Michael Sternberg, Geschäftsführer von n-21. Was nach einer einfachen Anforderung klingt, entpuppt sich als Mammutprojekt – denn Schulen verarbeiten sensible Daten von besonders Schutzbedürftigen, und die technischen sowie organisatorischen Anforderungen sind enorm.

Hintergrund: Ein landesweites Digitalprojekt

Die Niedersächsische Bildungscloud wurde als zentrale Plattform – als das zentrale Lernmanagementsystem des

Landes Niedersachsen - konzipiert, um Schulen einheitliche digitale Werkzeuge bereitzustellen. Während vielerorts digitale Angebote nur lokal oder in einzelnen Schulen genutzt wurden, kann die Bildungscloud den gesamten Schulbetrieb landesweit vernetzen.

Die Plattform wurde von n-21 im Auftrag des Niedersächsischen Kultusministeriums entwickelt. Ihr Ziel ist es, Lehrkräfte, Schülerinnen und Schüler mit digitalen Werkzeugen auszustatten, um orts- und zeitunabhängig zu arbeiten, Unterrichtsmaterialien zu teilen und gemeinsam Projekte umzusetzen. Dabei steht neben der technischen Skalierbarkeit insbesondere der Datenschutz im Fokus.

„Die Herausforderung war es, eine Plattform zu schaffen, die sowohl für kleine Grundschulen als auch für große Schulverbünde funktioniert – ohne Kompromisse bei der Sicherheit“, beschreibt Fabian Brandenburger, Berater für Datenschutz von Althammer & Kill, die Ausgangslage.

Datenschutz als Fundament: Sicherheit von Anfang an

Von Beginn an war klar: Ohne eine solide Datenschutzgrundlage kann die Bildungscloud nicht funktionieren. Die Einhaltung der Datenschutz-Grundverordnung (DSGVO) war nicht nur eine rechtliche Notwendigkeit, sondern auch ein entscheidender Faktor für die Akzeptanz der Plattform.

Schulen verarbeiten personenbezogene Daten von Schülerinnen, Schülern, Lehrkräften und Erziehungsberechtigten – darunter Namen, und digitale Kommunikationsinhalte. Diese Informationen zählen zu den besonders schützenswerten Daten gemäß DSGVO.

„Die größte Schwierigkeit lag darin, Datenschutz, Skalierbarkeit und Benutzerfreundlichkeit miteinander in Einklang zu bringen“, erläutert Brandenburger.

Um dieses Ziel zu erreichen, wurde eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt. Sie bewertet potenzielle Risiken für die Betroffenen und legt Maßnahmen fest, um diese zu minimieren. Zusätzlich wurden mehr als 100 technische und organisatorische Maßnahmen umgesetzt, darunter:

„Unsere Vision war es, eine flexible, sichere und datenschutzkonforme Plattform zu entwickeln, die Lehrkräfte, Schülerinnen und Schüler bestmöglich unterstützt.“



Michael Sternberg, Geschäftsführer von n-21

- Verschlüsselte Speicherung und Übertragung von Daten
- Einsatz datenschutzfreundlicher Subdienstleistender
- Pseudonymisierung und Anonymisierung personenbezogener Daten
- Transparente Nutzer-Informationen und Einwilligungsprozesse

Eine besondere Herausforderung war die Abstimmung mit der Datenschutzaufsicht und dem Kultusministerium. „Der Informationsfluss war nicht immer optimal. Viele Abstimmungen waren notwendig, um eine gemeinsame Linie zu finden“, so Brandenburger. Oftmals musste n-21 als Vermittler zwischen den Ministerien und den Entwicklerteams agieren.

Warum Open Source? Eine strategische Entscheidung

Ein entscheidender Faktor für den Erfolg der Bildungscloud war die Wahl von Open-Source-Technologien. Anstelle proprietärer Lösungen setzte n-21 auf frei zugängliche Software, die individuell angepasst und weiterentwickelt werden kann.

„Open Source bedeutet, dass wir keine Blackbox haben – wir wissen genau, wie unsere Daten verarbeitet werden und behalten die Datensouveränität“, so Sternberg.

Die Vorteile dieses Ansatzes:

- Transparenz: Der Quellcode ist einsehbar und überprüfbar.
- Flexibilität: Funktionen können individuell erweitert und angepasst werden.
- Kostenersparnis: Keine Abhängigkeit von teuren Lizenzmodellen.
- Nachhaltigkeit: Schulen und Bildungseinrichtungen können langfristig unabhängig agieren.

Gleichzeitig stellte der Open-Source-Ansatz hohe Anforderungen an die Sicherheit. Da verschiedene Entwickler und Institutionen an der Software mitarbeiten, mussten klare Regeln für Datenschutz, Code-Prüfung und Sicherheitsstandards definiert werden.

„Open Source bringt viele Vorteile, aber es braucht auch ein starkes Sicherheitskonzept, damit die Software langfristig vertrauenswürdig bleibt“, betont Brandenburger.

Herausforderungen bei der technischen Umsetzung

Neben Datenschutzfragen gab es weitere technische Hürden. Eine Plattform, die – bundesweit - von mehr als 4.000 Schulen genutzt wird, muss besonders leistungsfähig und ausfallsicher sein. Zudem mussten bestehende IT-Systeme der Schulen integriert und eine barrierefreie Nutzung gewährleistet werden.

Ein weiteres Thema war die Skalierbarkeit. Während kleine Schulen nur wenige Nutzende haben, arbeiten große Schulverbünde mit mehreren tausend Accounts. Die Infrastruktur musste deshalb so flexibel sein, dass sie mit der Nutzung wachsen kann.

Auch die Zusammenarbeit mit anderen Bundesländern spielte eine Rolle. Neben Niedersachsen nutzen auch Thüringen und Brandenburg die identische Cloud-

Lösung im eigenen Branding und in eigenen Instanzen. Der regelmäßige Austausch im sogenannten Schulcloud-Verbund zwischen den drei Bundesländern half dabei, gemeinsame Standards zu etablieren und Synergieeffekte zu nutzen.

Die Muster-DSFA: Ein wichtiger Baustein im Datenschutzprozess

Ein zentrales Element des Projekts war die Entwicklung einer Muster-Datenschutz-Folgenabschätzung (DSFA), die speziell für die Niedersächsische Bildungscloud konzipiert wurde. Eine DSFA ist ein Verfahren, das potenzielle Risiken für die Rechte und Freiheiten der betroffenen Per-

sonen bei der Verarbeitung personenbezogener Daten bewertet – ein unverzichtbarer Schritt, um sicherzustellen, dass alle datenschutzrechtlichen Anforderungen erfüllt werden.

„Da es sich um eine landesweite Plattform handelt, die von vielen Schulen genutzt wird, war es entscheidend, eine standardisierte Methode zur Risikobewertung zu entwickeln“, erklärt Michael Sternberg. Die Muster-DSFA sollte den Schulen helfen, ihre spezifischen Datenschutzerfordernisse zu erfüllen, ohne jede Institution einzeln die gesamte Analyse durchführen zu lassen.

Die Muster-DSFA wurde von n-21 und den beteiligten Ministerien so konzipiert, dass sie für alle Schulen im Land einsetzbar ist. Sie entlastet die Schulen, indem sie eine vorgefertigte Vorlage zur Verfügung stellt, die lediglich angepasst und gepflegt werden muss. Der Prozess der DSFA umfasst eine gründliche Analyse der verschiedenen Verarbeitungstätigkeiten und die Auswahl geeigneter Sicherheitsmaßnahmen.

„Wir wollten sicherstellen, dass die Schulen in der Lage sind, die DSFA ohne großen Aufwand zu implementieren und dabei die notwendigen datenschutzrechtlichen Anforderungen zu erfüllen“, so Fabian Brandenburger. Die Muster-DSFA gibt den Schulen nicht nur eine klare Struktur an die Hand, sondern sorgt auch dafür, dass alle Anforderungen der DSGVO eingehalten werden.

Diese standardisierte Herangehensweise ist besonders wichtig, da die Schulen in Niedersachsen gemäß der DSGVO selbst für die Verarbeitung personenbezogener Daten verantwortlich sind. Sie müssen prüfen, ob eine DSFA notwendig ist, und diese dann ordnungsgemäß durchführen. Die Muster-DSFA erleichtert diesen Prozess erheblich und stellt sicher, dass die Schulen die Datenschutzvorgaben effizient und korrekt umsetzen können.

Erfahrungen aus der Praxis: So nutzen Schulen die Bildungscloud

Nach mehreren Jahren Entwicklungsarbeit ist die Niedersächsische Bildungscloud heute fester Bestandteil vieler Schulen. Insbesondere während der Pandemie erwies sich die Plattform als unverzichtbar: Unterricht konnte nahtlos digital fortgeführt werden, Lehrkräfte konnten Arbeitsmaterialien teilen und Schülerinnen und Schüler hatten einen einheitlichen Zugang zu digitalen Werkzeugen.

Doch auch über die Pandemie hinaus zeigt sich: Die NBC erleichtert den Schulalltag. Lehrkräfte können digitale Klassenräume erstellen, Gruppenarbeiten organisieren und individualisierte Lerninhalte bereitstellen.

„Die Cloud ermöglicht eine ganz neue Form der Zusammenarbeit. Kolleginnen und Kollegen können Unterrichtsmaterialien teilen und gemeinsam weiterentwickeln“, berichtet eine Lehrkraft aus Hannover. Gleichzeitig gibt es noch Optimierungsbedarf. Rückmeldungen aus den Schulen zeigen, dass die Benutzerfreundlichkeit weiter verbessert werden kann – insbesondere in der mobilen Nutzung. Auch die Integration weiterer Tools und Anwendungen steht auf der Agenda der Entwickler.

Fazit: Datenschutz und digitale Bildung vereint

Die Niedersächsische Bildungscloud zeigt, dass digitale Bildung und Datenschutz kein Widerspruch sind. Durch die enge Zusammenarbeit zwischen Datenschutzexperten, Entwicklern und Bildungseinrichtungen wurde eine Plattform geschaffen, die nicht nur sicher, sondern auch zukunftsfähig ist.

Ob das Modell noch auf weitere Bundesländer übertragen wird, bleibt abzuwarten. Klar ist: Datenschutz muss von Anfang an mitgedacht werden – dann kann digitale Bildung ihr volles Potenzial entfalten. ☯

Althammer & Kill Akademie

11. Juni 2025 – kostenloses Webinar

NIS-2: Was bedeutet die Richtlinie für mein Unternehmen?

Wie können Sie prüfen, ob Sie ein Informationssicherheitsmanagement in ihrer Organisation bzw. in Ihrem Unternehmen implementieren müssen?

3. Juli 2025 – Online Seminar

KI-VO – Rechtliche Rahmenbedingungen und Vorgehensweisen bei der Einführung

Nutzen Sie dieses Seminar, um sich rechtzeitig mit den Anforderungen des EU AI Acts vertraut zu machen.

9. Juli 2025 – kostenloses Webinar

Wie arbeite ich datenschutzkonform mit KI?

Lernen Sie künstliche Intelligenz besser zu verstehen, verantwortungsvoll damit umzugehen und erhalten wertvolles Wissen zum Schutz der Privatsphäre.

23. Juli 2025 – kostenloses Webinar

Datenschutz-Folgenabschätzung

Das ist die Vorgehensweise und mögliche Methodik einer Datenschutz-Folgenabschätzung.

24.-25. September 2025 – Online Seminar

Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Mit dem essenziellen Grundlagenwissen zum kompetenten Ansprechperson in Datenschutzfragen.



Mehr Informationen, weitere Termine und Anmelde-möglichkeiten finden Sie unter: althammer-kill.de/akademie

Ihre Ansprechpartnerin:



Nina Hoffmann

veranstaltung@althammer-kill.de

Tel. +49 511 330603-0

1. Norddeutsches KI-Forum in Hannover

„Fehlendes Know-how ist der wichtigste Grund für die zögerliche Einführung von KI-Anwendungen“

Von Thomas Althammer

Produktivitätssteigerung, höherer Digitalisierungsgrad, positive Effekte im Fachkräftemangel – das sind Vorteile für die öffentliche Verwaltung beim Einsatz von Künstlicher Intelligenz (KI). Die Studie des IW Consult im Auftrag des Tech-Konzerns Google rechnete zum Jahreswechsel vor, dass eine Produktivitätssteigerung im öffentlichen Sektor in Höhe von fast 24 Milliarden Euro möglich sei. Die im europäischen Vergleich niedrige Digitalisierung ist demnach weiterhin ein Hemmschuh, weshalb sich der Einsatz von KI für Behörden, Ämter & Co. mit 82 Prozent sogar mehr auszahlen könnte als für die Wirtschaft (70 Prozent).

Welche Herausforderungen auf dem Weg dorthin zu bewältigen sind, beleuchtete im Februar das erste Norddeutsche KI-Forum, welches in Kooperation der kommunalen Hochschule für Verwaltung in Niedersachsen (HSVN) mit Althammer & Kill in Hannover organisiert wurde.

Risiken einschätzen, Potenziale und Chancen nutzen

Denis Lehmkemper, Landesbeauftragter für den Datenschutz Niedersachsen, eröffnete die Fachvorträge mit einer kritischen Auseinandersetzung der neuen Technologie mit dem Datenschutz. Er forderte, dass die Europäische Union den Schutz personenbezogener Daten, insbesondere bei internationalen IT-Entwicklern und -Anbietern von Künstlicher Intelligenz, einfordere. „Die Entwicklung datenschutzkonformer und vertrauenswürdiger KI-Modelle muss weiter voranschreiten, ebenso wie die KI-angepasste Rechtsentwicklung“, sagte Lehmkemper. Der technologische Fortschritt schreitet rasend schnell voran, weshalb es essenziell sei, über die Zukunftstechnologie aufzuklären, Risiken richtig einzuschätzen und die Potenziale und Chancen zu nutzen.



Die Organisatoren des 1. Norddeutschen KI-Forums

„Viele Unternehmen (87 Prozent) geben an, dass fehlendes Know-how der wichtigste Grund für die zögerliche Einführung von KI-Anwendungen ist. Das ist Motivation und Antrieb gewesen, das KI-Forum ins Leben zu rufen“, sagte Thomas Althammer, Geschäftsführer des Beratungsunternehmens Althammer & Kill und Mitorganisator, zum Auftakt des Forums.

Das Interesse an KI und dem Forum war enorm, die Veranstaltung mit rund 230 Teilnehmenden schnell ausverkauft gewesen. Dies zeige deutlich, dass der Umgang mit KI für Unternehmen, Organisationen, Behörden und Kommunen ein wichtiges Thema sei, welches den Arbeitsalltag stark verändern werde, so Althammer weiter. Aufgrund der Komplexität der Technologie sowie den regulatorischen Anforderungen nahmen die Akteure aktuell aber noch eine beobachtende Rolle ein. Jetzt gelte es, sich aktiv mit der Technologie auseinanderzusetzen.

Microsoft Copilot im Kontext Datenschutz

Dass der Einsatz von Microsoft Copilot und Co. im Kontext Datenschutz möglich ist, zeigte Althammer anhand konkreter Lösungsmöglichkeiten für den Einsatz von KI in Verbindung mit personenbezogenen Daten auf: „Durch Nutzung von Technologien wie Retrieval-Augmented-Generation (RAG) ist der Einsatz von KI in Verbindung mit personenbezogenen Daten möglich. Halluzinationen können begrenzt und die Verwendung bestehender Daten-

quellen im Unternehmen unter Beachtung der Vorgaben der DSGVO integriert werden.“ Dass eine klare europäische Haltung vonnöten ist, wurde auch beim Panel-Talk zum Thema Bildung deutlich. Das Bildungssystem vermittele aktuell nicht die Kompetenzen, die später im Beruf gebraucht würden, sagte Michael Sternberg, Geschäftsführer der Landesinitiative n-21: Schulen in Niedersachsen. „Dabei bietet KI an Schulen durchaus Vorteile, wenn sie beispielsweise kompetenzorientiert ein-

gesetzt wird, um Schülerinnen und Schüler unterschiedlicher Leistungsstände individuell zu fördern“ sagte er. Denn die Berufsbilder verändern sich aktuell stark. Fähigkeiten, die einmal gelernt wurden und dann die nächsten 20 Jahre anwendbar blieben, werde es dem Professor für Digitalisierungsmanagement an der HSVN zufolge, Peter Daiser, in vielen Bereichen künftig so nicht mehr geben. Eine stetige Anpassung und Weiterentwicklung seien die Folgen.

Europa muss selbstständiger werden

Die Münchner Sicherheitskonferenz habe nochmals deutlich gemacht, dass Europa selbstständiger werden müsse, nicht nur in der Verteidigung, sondern auch in der Digitalisierung, war sich Benedikt Hüppe, Hauptgeschäftsführer der Unternehmensverbände Niedersachsen, sicher. Es gehe darum, Standards zu setzen, Dinge mitzuentwickeln und sich zu fragen, was Europa den Tech-Riesen aus den USA und Asien entgegensetzen habe, um wettbewerbsfähig zu bleiben.

Die ersten Schritte könnten dabei eine Bewertung von Best Practices sein, Kooperationen mit Spezialistinnen und Spezialisten - auch außerhalb der eigenen Blase - sowie das Starten eigener Pilotprojekte, rieten die Vortragenden.

„Die Basis dieser ersten Schritte liegt in Auf- und Ausbau der eigenen IT-Infrastruktur. Gerade was Datenqualität und Weiterverarbeitungsfähigkeit von Daten angeht,

haben viele Akteure - egal ob Unternehmen oder Verwaltungen – oft noch Hausaufgaben zu erledigen. Erst dann bieten Cloud-Computing, KI & RAG überhaupt echte Chancen! Den geltenden Rechtsrahmen wollen wir natürlich auch nicht vergessen.“ sagte Tim Brockmann, Professor für Zivilrecht und Prodekan an der HSVN. Er führte den hohen Stellenwert von Transparenz und Nachvollziehbarkeit von KI-Entscheidungen aus und warnte vor der Illusion, dass KI gesellschaftliche Herausforderungen wie den Fachkräftemangel oder Akzeptanzprobleme vollständig lösen könne.

Zwischen Empathie und Effizienz: Best Practices aus Verwaltung, Journalismus und Pflege

Wie KI-Anwendungen schon heute in unterschiedlichen Branchen eingesetzt werden, zeigten die Usecases aus der Privatwirtschaft. Michael Klipker stellte den Roboter Navel vor, von dem die Lilienthaler Diakonie zwei von insgesamt 40 Exemplaren deutschlandweit betreibt. Ziel ist es, einerseits Erinnerungsarbeit mit den Klientinnen und Klienten zu leisten (z. B. Tabletteneinnahmen, Unterhalten, Quizen) und andererseits das Personal zu entlasten. Navel spricht nicht nur Menschen an, er kann sich Gesichter merken und knüpft auch an Gespräche vom Vortag an.

Auch Medienschaffende greifen auf generative KI zurück und erreichen damit enorme Effizienzsteigerungen, wie Benjamin Danneberg von Heise berichtete. Anwendungsbeispiele sind Podcasts, die mit KI-Klon-Stimme erzeugt werden, öffentliche und interne Datenbankrecherchen mittels RAG, Transkription von Interviews oder Podcasts



KI-Künstler Kai Lipphardt erklärt Thomas Althammer seine Kunst.

in Text oder die Generierung von Metadaten für Bilddatenbanken. Es gehe dabei darum, Mitarbeitende von repetitiven Arbeiten zu entlasten und Prozesse zu beschleunigen. Die Überprüfung der Ergebnisse verbleibe dabei immer beim Fachpersonal.

Die KI-Pilotprojekte, die bei der Verwaltung der Stadt Braunschweig getestet werden, stellte Justus Engelland vor. Wie KI-gestützte Automatisierung den Verwaltungsalltag des Landkreises Dannenberg entlastet, führten Dr. Andreas Kohne und Sabrina Donner vor. Besonders hervorgehoben wurde die KI-gestützte Robotic Process Automation EMMA, die Anträge prüft und Unterlagen nachfordert. Auch KI-Telefonchatbots wie Wendi sind bereits im Einsatz.

Abgerundet wurde das straffe 2-tägige Tagungsprogramm durch den KI-Künstler Kai Lipphardt.

Ein Auftakt, der Lust auf mehr macht

Das 1. Norddeutsche KI-Forum war für uns als Veranstalter ein besonderes Erlebnis: Verwaltung und Wirtschaft sind hier in einen intensiven Austausch über die Potenziale und Herausforderungen Künstlicher Intelligenz getreten. Genau dieser Dialog war unser Ziel – und wir freuen uns, dass er auf so großes Interesse gestoßen ist. Gemeinsam mit unseren Partnern der Kommunalen Hochschule für Verwaltung in Niedersachsen (HSVN), dem Niedersächsischen Landkreistag (NLT), Heidrich Rechtsanwälte, dem Niedersächsischen Städtetag sowie dem Niedersächsischen Städte- und Gemeindebund konnten wir eine Plattform schaffen, die unterschiedliche Perspektiven zusammengebracht hat.

Unser herzlicher Dank gilt allen Teilnehmenden für ihre Offenheit, ihre Fragen und ihre Bereitschaft, Wissen zu teilen. Die positiven Rückmeldungen zeigen uns: Der Austausch war nicht nur nötig, sondern auch gewünscht. Deshalb denken wir bereits über eine Fortsetzung nach – vielleicht sehen wir uns beim nächsten Mal wieder! ☺

Digitale Souveränität – gemeinsam gestalten

Digitale Souveränität – das klingt groß, abstrakt, vielleicht auch ein bisschen politisch. Aber im Alltag zeigt sich schnell: Es geht um ganz praktische Fragen.

Von Thomas Althammer

Wer entscheidet, welche Software wir einsetzen? Wie unabhängig sind wir von Plattformen oder Herstellern? Können wir erklären, wie KI-basierte Entscheidungen entstehen – und sind wir bereit, sie kritisch zu hinterfragen?

Für uns bedeutet digitale Souveränität vor allem eins: Gestaltungsfreiheit. Die Fähigkeit, in digitalen Räumen bewusst zu handeln – statt nur zu reagieren. Das beginnt bei der Wahl von Open-Source-Technologien. Es zeigt sich in der Entscheidung, Daten verantwortungsvoll zu verarbeiten. Und es endet nicht bei der Technik: Auch Fachwissen, Haltung und eine klare Kommunikation gehören dazu.

In diesem Heft haben wir verschiedene Wege beleuchtet, wie digitale Souveränität heute ganz konkret gelebt werden

kann – ob mit der Niedersächsischen Bildungscloud, einer praxisnahen KI-Richtlinie oder klaren Hilfestellungen für den Umgang mit NIS-2. Uns war wichtig zu zeigen: Auch komplexe Themen lassen sich greifbar machen – wenn man sie gemeinsam denkt.

Wir sind überzeugt: Digitale Souveränität ist kein Zustand, sondern ein Prozess. Und dieser Prozess endet nicht mit dieser Ausgabe. Im Gegenteil. Wir möchten den Dialog weiterführen – und laden Sie herzlich dazu ein, Teil unserer Community zu werden.

Auf LinkedIn teilen wir Fachwissen, Impulse aus der Praxis und neue Perspektiven. Und wir freuen uns über Ihre Gedanken, Fragen und Erfahrungen. Denn die digitale Zukunft gehört denen, die sie gemeinsam gestalten. ☺



Impressum

Redaktion/V. i. S. d. P.:

Fabian Eggers,
Thomas Althammer

Haftung und Nachdruck:

Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Schutzgebühr Print-Ausgabe: 5,- €

Gestaltung:

Designbüro Winternheimer, winternheimer.net

Fotos Mini-Figuren:

Katja Borchhardt, miniansichten.de

Anschrift:

Althammer & Kill GmbH & Co. KG
Roscherstraße 7 · 30161 Hannover
Tel. +49 511 330603-0
althammer-kill.de



Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

Wir sind Digitalisierungskenner, Datenversteher und Vorwärtsdenker –
Ihr Experte für Datenschutz, Informationssicherheit, Künstliche Intelligenz und Compliance.
Unsere 45 Mitarbeitenden bringen Digitalisierung und Datenschutz bundesweit in Einklang.

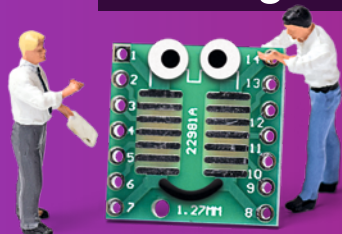
Datenschutz



Informationssicherheit



Künstliche Intelligenz



Compliance

