COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 4/2024

NIS-2

Was Unternehmen jetzt wissen müssen

Seite 6

3. Änderung des EKD-Datenschutzgesetzes
Gesetzlich verankerte Überprüfung des Datenschutzgesetzes der EKD
Seite 10

Wie Cyberkriminelle vorgehen
Umfassende Analyse hilft sozialen Organisationen, auf steigende Bedrohungslage zu reagieren
Seite 12

Compliance im Wandel: Die Rolle der Künstlichen Intelligenz in der Arbeitswelt
Interview mit Prof. Sabina Jeschke, CEO des KI Park e. V.
Seite 16

Editorial

Liebe Leserin, lieber Leser,

der Wandel der Arbeitswelt und die fortschreitende Digitalisierung stellen uns vor spannende, aber auch herausfordernde Aufgaben. Um diesen Entwicklungen gemeinsam auf den Grund zu gehen, hatten wir das Vergnügen, Frau Prof. Dr. Sabina Jeschke bei unseren Praxistagen in Paderborn zu begrüßen. Die Expertin für Digitalisierung und Künstliche Intelligenz sprach mit uns über die Veränderungen, die auf Unternehmen zukommen, und erklärte, welche Rolle KI in der Compliance spielen kann. Ein Gespräch, das neue Perspektiven eröffnet und zeigt, wie tiefgreifend Künstliche Intelligenz bereits heute unseren Berufsalltag beeinflusst.

Auch in puncto Cybersicherheit bewegt sich einiges. Die NIS-2-EU-Richtlinie, welche Unternehmen zu höheren Sicherheitsstandards verpflichtet, befindet sich in der Umsetzung in Deutschland. Unser Artikel erklärt, was das konkret bedeutet und wie sich Unternehmen auf die neuen Anforderungen vorbereiten können.

Die neuen Anpassungen im Datenschutzgesetz der Evangelischen Kirche setzen auf mehr Transparenz und Verantwortung – ein Schritt, der auf die Anforderungen der digitalen Gesellschaft reagiert. Im Artikel auf Seite 10 erfahren Sie, welche Neuerungen besonders relevant sind.

In einer Analyse zum Thema Cyberkriminalität zeigen wir auf, wie sich Bedrohungslagen entwickeln und was Organisationen tun können, um sich gegen Angriffe zu wappnen. Gerade soziale Einrichtungen sind oft bevorzugte Ziele, da ihre Ressourcen für Cybersicherheit begrenzter sind. Doch Wissen ist Macht – und die Auseinandersetzung mit typischen Angriffsmustern kann entscheidend sein.

Mit dieser Ausgabe möchten wir nicht nur Impulse für neue Herausforderungen setzen, sondern Sie auch auf die festliche Zeit einstimmen. Wir wünschen Ihnen und Ihren Liebsten ein frohes und besinnliches Weihnachtsfest sowie einen erfolgreichen Start in das neue Jahr 2025. Möge es ein Jahr voller neuer Chancen und positiver Entwicklungen werden!

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*

Rückblick auf unsere Praxistage 2024

Die Praxistage 2024 im Hotel Vivendi in Paderborn, die vom 04. bis 06. September stattfanden, waren ein voller Erfolg. Mehr als 70 Teilnehmende aus verschiedenen Branchen nutzten die Gelegenheit, sich intensiv mit den aktuellen Herausforderungen und Chancen im Bereich Datenschutz und Informationssicherheit auseinanderzusetzen.

Die Veranstaltung begann mit drei beeindruckenden Keynote-Vorträgen. Henning Voß, Referent für Wirtschaftsschutz, sprach über die Bedrohungen durch Spionage, Sabotage und Cyberangriffe und gab praktische Tipps zur Abwehr dieser Gefahren. Manuel Atug, Gründer der AG KRITIS, thematisierte in seinem Vortrag die Sicherheitsanforderungen für kritische Infrastrukturen, während Prof. Dr. Sabina Jeschke die Rolle von Künstlicher Intelligenz in der Compliance und die daraus resultierenden neuen Herausforderungen erörterte.

Im Anschluss an die Keynotes fand eine Podiumsdiskussion zum Thema IT-Sicherheit und Künstliche Intelligenz statt, die den Austausch und die Diskussion unter den Teilnehmenden anregte.

Der Nachmittag bot praxisorientierte Workshops, in denen die Teilnehmenden Lösungen zu spezifischen Themen wie den NIS-2-Vorgaben für das Gesundheitswesen, der Novellierung des DSG-EKD und der Datenschutz-Folgenabschätzung erarbeiteten. Diese Sessions ermöglichten den Teilnehmenden, konkrete Strategien zu entwickeln, die sie direkt in ihren Organisationen anwenden können.

Der zweite Veranstaltungstag beinhaltete weitere spannende Vorträge, darunter von Michael Jakob, der über die datenschutzrechtlichen Herausforderungen von KI in kirchlichen Organisationen sprach, und Prof. Helmut Kreidenweis, der die Ergebnisse seiner Studie zur KI im Sozialwesen vorstellte. Networking spielte an beiden Abenden eine zentrale Rolle, und viele Teilnehmende berichteten von wertvollen Gesprächen und neuen Kooperationen.

Abgerundet wurde das Programm durch einen Erfahrungsbericht von Prof. Dr. Fabian Schmieder, welcher detailliert und aus dem Nähkästchen über den Hackerangriff auf die Hochschule Hannover berichtete und wie die Hochschule diesem begegnete. Wir danken allen Beteiligten für ihre aktive Mitgestaltung und freuen uns bereits auf die nächste Auflage der Praxistage, welche vom 10. bis 12. September 2025 in Hannover stattfinden werden (jetzt schon Datum vormerken).

NIS-2: Neue Anforderungen für die digitale Sicherheit

Der Übergang zu NIS-2 bringt weitreichende Veränderungen im Bereich der IT-Sicherheit. Was das konkret für Ihre Branche bedeutet und wie Sie Ihr Unternehmen optimal vorbereiten, erfahren Sie auf unserer Spezialseite. Hier finden Sie alle wichtigen Informationen, Praxistipps und weiterführende Veranstaltungen rund um das Thema NIS-2.

KLICK/SCAN

Künstliche Intelligenz in der Informationssicherheit

Künstliche Intelligenz revolutioniert auch den Bereich der IT-Sicherheit. Doch mit den Chancen kommen auch neue Risiken. Auf unserer Themenseite sammeln wir aktuelle Trends, praxisnahe Einblicke und spannende Beiträge zu KI in der Informationssicherheit. Entdecken Sie, wie KI Ihre Sicherheitsstrategie verbessern kann und welche Herausforderungen dabei auf Sie zukommen könnten.

KLICK/SCAN

Schon gewusst?

Der Name

Bluetooth

hat überraschenderweise historische Wurzeln und ist eine Hommage an den dänischen Wikingerkönig Harald Blauzahn (Harald „Bluetooth" Gormsson), der im 10. Jahrhundert lebte. König Harald war bekannt dafür, Dänemark und Norwegen zu vereinen und die Kommunikation zwischen verschiedenen Volksgruppen zu fördern.

1996 wählte die Technologieindustrie diesen Namen, weil Bluetooth ebenfalls das Ziel verfolgt: Geräte und Systeme zu verbinden und die Kommunikation zu vereinfachen. Das Bluetooth-Logo, eine Kombination aus den Runen für H und B, erinnert an diese Geschichte und symbolisiert Verbindungen und Zusammenarbeit.

Veranstaltungen

19.–20. Februar 2025, Hannover
Norddeutsches KI-Forum – Der 360°-Blick auf KI in Wirtschaft, Verwaltung & Unternehmen

Das Norddeutsche KI-Forum bietet Ihnen die Möglichkeit, die Chancen und Herausforderungen der Künstlichen Intelligenz aus erster Hand zu erleben. Ob innovative Anwendungsbeispiele, Best-Practice-Vorträge oder praxisnahe Workshops – hier dreht sich alles um die Zukunft der KI in der Wirtschaft und Verwaltung.

Eines der Highlights ist der Vortrag von Denis Lehmkemper, dem Landesbeauftragten für den Datenschutz Niedersachsen, der darüber spricht, wie KI und Datenschutz in Einklang gebracht werden können. Doch er ist nur einer von vielen inspirierenden Köpfen auf der Bühne. Führende Expertinnen und Experten aus Wissenschaft, Wirtschaft und Verwaltung stehen bereit, ihre Perspektiven und Erfahrungen zu teilen. Im Abendprogramm erwarten Sie kreative Höhepunkte: Erleben Sie, wie KI die Kunstwelt beeinflusst, und lassen Sie sich von faszinierenden Kunstwerken inspirieren. Zudem wird Kai Lipphardt mit KI-Musik und -Bildern die Atmosphäre des Abends bereichern und Ihnen einen einzigartigen Einblick in die kreative Kraft der Künstlichen Intelligenz geben.

Nutzen Sie die Gelegenheit, sich in interaktiven Formaten und lebhaften Diskussionen auszutauschen und wertvolle Kontakte zu knüpfen. Das vollständige Programm mit allen Highlights und Details finden Sie im beiliegenden Heft.

KLICK/SCAN

NIS-2: Neue Sicherheitsanforderungen – Was Unternehmen jetzt wissen müssen

Die NIS-2-Richtlinie der Europäischen Union bildet einen aktualisierten Rechtsrahmen, der die Cybersicherheit in den Mitgliedstaaten verbessern und den Herausforderungen der zunehmenden Digitalisierung gerecht werden soll.

Von Julian Lang

Mit der NIS-2-Richtlinie hat die Europäische Union einen neuen rechtlichen Rahmen geschaffen, der die Cybersicherheit in den Mitgliedstaaten stärken und den Anforderungen der fortschreitenden Digitalisierung begegnen soll. NIS-2 ist die Reaktion der Europäischen Union auf die wachsenden Bedrohungen durch Cyberangriffe und zunehmende Professionalisierung der Cyberkriminalität. Angesichts des fortschreitenden Knowhows und nahezu unerschöpflicher Ressourcen der Akteure besteht in der EU ein zunehmendes Risiko auf Cyberangriffe.

Deutschland ist derzeit dabei, diese Richtlinie in nationales Recht umzusetzen, konkret im Rahmen des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG). Die Frist für die nationale Umsetzung endete am 17. Oktober 2024 und wurde dementsprechend nicht eingehalten. Am 4. November 2024 fand eine öffentliche Anhörung zum Entwurf des NIS2UmsuCG im Deutschen Bundestag statt. Der aktuelle Entwurf wird von einigen Stellen stark kritisiert, da dieser die Bundesverwaltung nicht berücksichtigt.

Voraussichtlich soll das Gesetz im Frühjahr 2025 in Kraft treten. Eine Übergangsfrist für Unternehmen wird es nicht geben.

Ziele

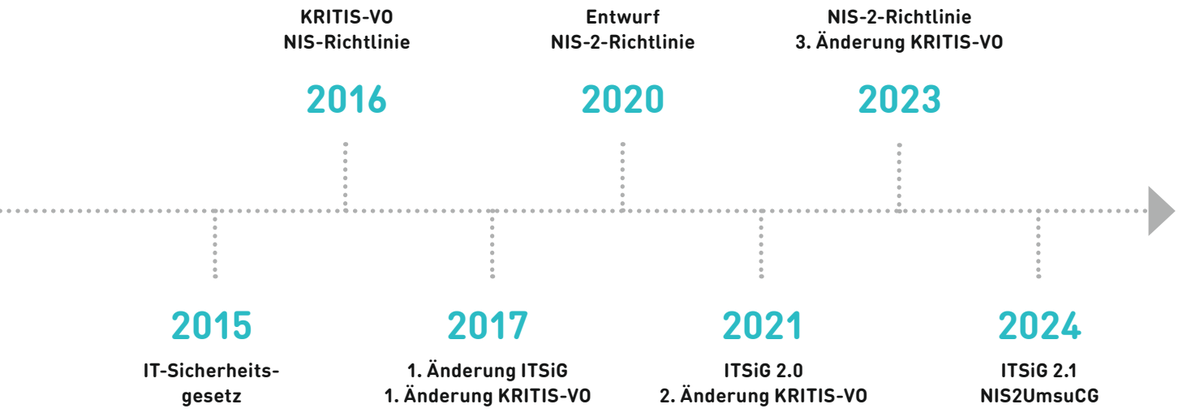
Das NIS2UmsuCG verfolgt das Ziel, das allgemeine Cybersicherheitsniveau zu steigern und die Resilienz kritischer Infrastrukturen sowie Sektoren, die als wichtige oder besonders wichtige Einrichtungen gelten, zu verbessern.

Der Geltungsbereich wird dabei erheblich ausgeweitet: Zusätzlich zu großen Unternehmen könnten nun auch mittelgroße Unternehmen aus verschiedenen Branchen den neuen Vorgaben unterliegen.

Zeitrahmen

Im Jahr 2016 veröffentlichte die Europäische Union (EU) die NIS-1-Richtlinie, die im Mai 2018 in nationales Recht (IT-Sicherheitsgesetz 2.0) überführt wurde und im Mai 2021 in Kraft trat. Im Dezember 2022 folgte die EU mit der neuen NIS-2-Richtlinie, die am 16. Januar 2023 in Kraft trat.

Die Mitgliedsstaaten hatten bis zum 17. Oktober 2024 Zeit, diese Richtlinie in nationales Recht umzusetzen. Das Bundekabinett hat am 24. Juli 2024 den 7. Referentenentwurf für das NIS2UmsuCG beschlossen. Ein Inkrafttreten wird im Frühjahr 2025 erwartet.



Betroffenheit

In Deutschland werden Schätzungen zufolge zwischen 29.000 und 40.000 Unternehmen von dem NIS2UmsuCG betroffen sein. Unternehmen aus 18 festgelegten Sektoren mit mindestens 50 Beschäftigten und einem Umsatz von 10 Millionen Euro fallen unter die Regelung. Dadurch können künftig beispielsweise auch IT-Dienstleister, Online-Marktplätze, Maschinenbauunternehmen, Lebensmittelversorger, Labore, Forschungseinrichtungen und weitere Organisationen betroffen sein, sofern sie die Schwellenwerte überschreiten. Dies bringt eine Vielzahl von Unternehmen in die Verantwortung, die sich bisher kaum mit ihrer Informationssicherheit beschäftigt haben. Die betroffenen Sektoren lassen sich der Anlage 1 und 2 des NIS2UmsuCG entnehmen.

Erbringt ein Unternehmen Dienstleistungen für Dritte, kann ein Sonderfall entstehen: Hier ist unabhängig von den Schwellenwerten zu prüfen, ob die Auftraggeber selbst zur Einhaltung der NIS-2-Anforderungen verpflichtet sind. In solchen Fällen können Anforderungen auch für die Dienstleister entlang der gesamten Lieferkette entstehen.

Umzusetzende Maßnahmen

Von der NIS-2 betroffene Unternehmen sind verpflichtet, erhöhte Sicherheitsanforderungen zu erfüllen. Dazu zählt die Einführung eines umfassenden Risikomanagements, das technische und organisatorische Maßnahmen zur Erkennung und Bewältigung von Cybersicherheitsrisiken umfasst. Im Falle eines schwerwiegenden Sicherheitsvorfalls müssen die zuständigen Behörden unverzüglich informiert werden; eine detaillierte Berichterstattung ist dabei innerhalb von 72 Stunden erforderlich. Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig durch Audits und Bewertungen zu überprüfen.

„Der Stichtag für die nationale Umsetzung der NIS-2-Richtlinie war am 17. Oktober 2024.“

Außerdem müssen Risiken, die durch Geschäftsbeziehungen mit Drittanbietern oder entlang der Lieferkette entstehen, analysiert und gemanagt werden. Schulungen der Mitarbeitenden sind ebenfalls verpflichtend, um das Bewusstsein für Cybersicherheit im Unternehmen zu stärken.

Die zu erfüllenden Verpflichtungen, die sich für betroffene Unternehmen ergeben, lassen sich dem Kapitel 2 des NIS2UmsuCG entnehmen.

Durchführungsbestimmungen

Am 17. Oktober 2024 sind die Durchführungsbestimmungen für die NIS-2-Richtlinie veröffentlicht worden. Diese enthalten spezifische Regelungen zur Umsetzung.

Zum Beispiel Regelungen zur Identifikation und Einstufung von Sicherheitsvorfällen, bei denen Unternehmen

verpflichtet sind, Vorfälle zu protokollieren und zu analysieren, um deren Signifikanz zu bestimmen. Ein Vorfall gilt beispielsweise als signifikant, wenn er eine erhebliche Beeinträchtigung der Dienste, finanzielle Verluste oder materielle bzw. immaterielle Schäden für Personen oder Unternehmen verursachen kann.

Darüber hinaus müssen Unternehmen sicherstellen, dass alle sicherheitsrelevanten Ereignisse systematisch erfasst werden, einschließlich Zugriffsaktivitäten auf Netzwerke und kritische Systeme, und dass für jede Art von Vorfall standardisierte Reaktionsmaßnahmen entwickelt und getestet werden. Die Regelungen legen außerdem fest, dass Unternehmen ihre Reaktionspläne regelmäßig überprüfen und anpassen müssen, insbesondere nach signifikanten Änderungen oder neuen Bedrohungsszenarien.

Mögliche Sanktionen

Die betroffenen Unternehmen sind gefordert, sich eingehend mit ihrer Informationssicherheit zu befassen und erforderliche Maßnahmen umzusetzen. Andernfalls drohen hohe Strafen von bis zu 10 Millionen Euro oder 2 % des gesamten weltweiten Jahresumsatzes.

Nächste Schritte

Es ist ratsam, zeitnah zu prüfen oder ggf. prüfen zu lassen, ob die eigene Organisation in den Geltungsbereich des NIS2UmsuCG fällt. Althammer & Kill bietet hierzu ein NIS-2-Assessment an, das eine Prüfung der Betroffenheit anhand der Schwellenwerte und spezifischen Anwendungsbereiche des NIS2UmsuCG umfasst. Wenn eine Organisation betroffen ist, sollte ein Aktionsplan entwickelt werden, der Zeitrahmen und Zuständigkeiten für die erforderlichen Maßnahmen festlegt. Zusätzlich sollten Prozesse eingeführt werden, um die Cybersicherheitsmaßnahmen regelmäßig zu überprüfen und zu verbessern und so eine kontinuierliche Weiterentwicklung sicherzustellen.

Disclaimer

Der in diesem Artikel genannte Zeitpunkt für das Inkrafttreten des NIS2UmsuCG im Frühjahr 2025 basiert auf derzeitigen Planungen. Der tatsächliche Zeitpunkt hängt von politischen Entscheidungen und dem Fortschritt der Gesetzgebungsverfahren ab. Unabhängig vom genauen Datum wird empfohlen, dass betroffene Organisationen die verbleibende Zeit nutzen, um sich frühzeitig auf die Anforderungen vorzubereiten.

Sie brauchen Unterstützung bei der Umsetzung der NIS-2-Richtlinie?

Auf dem beiliegenden Info-Blatt stellen wir Ihnen unsere Lösungen und Dienstleistungen vor.

Mehr Informationen finden Sie auch auf:
https://www.althammer-kill.de/themen/nis-2-richtlinie

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

3. Änderung des EKD-Datenschutzgesetzes

Die Evangelische Kirche in Deutschland befasst sich mit der gesetzlich verankerten Überprüfung des Datenschutzgesetzes der EKD

Von Sören Hartmann

Bereits im März 2024 kursierte ein Referentenentwurf zur 3. Änderung des EKD-Datenschutzgesetzes (DSG-EKD). Jetzt existiert die Drucksache XIII / 1 „Vorlage des Rates der Evangelischen Kirche in Deutschland gemäß Art. 26 a Absatz 1 GO.EKD - Kirchengesetz zur 3. Änderung des EKD-Datenschutzgesetzes (DSG-EKD)“. Die vorgesehene Novellierung des DSG-EKD knüpft an die grundlegende Überarbeitung des Gesetzes im Jahr 2017 an, die ihrerseits eine Reaktion auf die Einführung der Datenschutz-Grundverordnung (DSGVO) darstellte. Gemäß § 54 Absatz 4 des DSG-EKD war eine Überprüfung des Gesetzes innerhalb von fünf Jahren vorgesehen.

Stichwort
Evangelisches Datenschutzrecht im Einklang mit der DSGVO

Gem. Art. 91 Abs. 1 DSGVO:
„Wendet eine Kirche oder eine religiöse Vereinigung oder Gemeinschaft in einem Mitgliedstaat zum Zeitpunkt des Inkrafttretens dieser Verordnung umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung an, so dürfen diese Regeln weiter angewandt werden, sofern sie mit dieser Verordnung in Einklang gebracht werden.“

Diese Überprüfung begann Ende 2022 und führte zu den nun vorgeschlagenen Änderungen. Die Überarbeitung verfolgt ein Doppelziel: Zum einen soll die Erfüllung des kirchlichen Auftrags weiterhin ermöglicht werden, zum anderen ist sicherzustellen, dass das evangelische Datenschutzrecht im Einklang mit der DSGVO steht.

Wesentliche Änderungen im Gesetz

Die Novellierung enthält mehrere zentrale Änderungen, die sowohl die Anpassung an die DSGVO als auch die Berücksichtigung spezifisch kirchlicher Belange betreffen. Zu den wichtigsten Neuerungen gehören:

Überarbeitung der Rechte der betroffenen Personen: Die Rechte der betroffenen Personen werden gestärkt. So gelten u. a. künftig kürzere Fristen für die verantwortliche Stelle bei den Rechten der Betroffen auf Auskunft, Berichtigung, Löschung etc., die Informationspflicht der betroffenen Person erfolgt künftig zum Zeitpunkt der Verarbeitung und das Recht auf eine Kopie der verarbeiteten personenbezogenen Daten, das in der DSGVO schon immer vorhanden war, wird explizit in das Gesetz aufgenommen. Zudem gibt es Änderungen bei der automatisierten Entscheidungsfindung, beim Recht auf Widerspruch und noch weiteren Punkten der Rechte der betroffenen Personen.

Einwilligung Minderjähriger: § 12 wird dahingehend geändert, dass er sich nicht nur explizit auf elektronische Angebote bezieht, sondern für alle Einwilligungen von Minderjährigen gilt.

Das berechtigte Interesse: § 6, der die Rechtmäßigkeit der Datenverarbeitung regelt, wird an mehreren Stellen überarbeitet. Die wohl wichtigste Änderung ist die Streichung des § 6 Nr. 8 und die damit einhergehende Neuformulierung von Nr. 4, sodass auch das DSG-EKD künftig das berechtigte Interesse der verantwortlichen Stelle vorsieht.

Einführung neuer Paragrafen: Mit § 30a wird eine Regelung für zentrale IT-Verfahren eingeführt, die es ermöglicht, datenschutzrechtliche Aufgaben, Befugnisse und Verantwortlichkeiten zwischen verschiedenen kirchlichen Stellen zu verteilen. Zudem wird mit § 50b eine neue Norm zur Mitgliederkommunikation geschaffen, die die Verarbeitung von Kontaktdaten der Mitglieder regelt.

Bestellung von örtlich Beauftragten: Der Grenzwert zur Verpflichtung der Bestellung von örtlich Beauftragen für den Datenschutz wird auf 20 Personen erhöht, die ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut sind.

Nebenbei erwähnt...

KLICK/SCAN

Vielleicht auch interessant: Der EuGH schafft Klarheit bei dem Begriff „Kopie“ im Rahmen des Auskunftsrechts.

Begriffsbestimmungen: Der Begriff „besondere Kategorien personenbezogener Daten“ wird dahingehend angepasst, dass das Merkmal „rassische Herkunft“ ersatzlos gestrichen wird.

Zweckänderung sowie Offenlegung an kirchliche oder öffentliche Stellen: §§ 7 und 8 werden umfangreich neu formuliert und präzisiert, sodass sie u. a. die anderen gesetzlichen Änderungen berücksichtigen.

Unterwerfungserklärung: Künftig entfällt die Unterwerfung von Auftragsverarbeitern unter die kirchliche Aufsicht gem. § 30 Absatz 5, da diese in der Praxis oft schwer umsetzbar war.

Bußgeld: Der Höchstsatz für Geldbußen wird von bisher 500.000 Euro auf 6 Millionen Euro erhöht.

Erweiterung kirchlicher Spezifika: Neben den Anpassungen an die DSGVO werden auch neue kirchliche Besonderheiten in das Gesetz aufgenommen. So wird in § 50 die Verarbeitung personenbezogener Daten zu Archiv-, Forschungs- und statistischen Zwecken neu geregelt, wobei der Schutz der betroffenen Personen besonders berücksichtigt wird.

Gottesdienste und kirchliche Veranstaltungen: § 53 wird angepasst, sodass auch eine spätere Veröffentlichung einer Aufzeichnung zulässig ist.

Aktuell

Die abschließende Beratung und Beschlussfassung durch die EKD-Synode fand im November statt. Die EKD-Synode hat einstimmig der Novelle des DSG-EKD zugestimmt.

Damit tritt am 1. Mai 2025 die größte Reform des evangelischen Datenschutzrechts seit der Anpassung an die DSGVO in Kraft.

Die Überarbeitung des DSG-EKD zeigt, dass die Evangelische Kirche in Deutschland den Datenschutz als ein dynamisches Feld versteht, das kontinuierlich überprüft und angepasst werden muss.

Die Novellierung trägt sowohl den rechtlichen Anforderungen der DSGVO als auch den spezifischen Bedürfnissen der kirchlichen Arbeit Rechnung und stellt sicher, dass der kirchliche Datenschutz auch in Zukunft den notwendigen rechtlichen Rahmen bietet. &

Wie Cyberkriminelle vorgehen

Umfassende Analyse hilft sozialen Organisationen, auf steigende Bedrohungslage zu reagieren.

Von Wulf Bolte und Maximilian Klose

Cyberkriminalität entwickelt sich stetig weiter. Angreifer nutzen immer ausgeklügeltere Methoden, um in Netzwerke einzudringen, Daten zu stehlen oder Systeme lahmzulegen. Ransomware, Phishing, DDoS-Angriffe und Social-Engineering sind nur einige der Taktiken, die regelmäßig zum Einsatz kommen. Künstliche Intelligenz vereinfacht Cyberangriffe zusätzlich, Rechtschreibung wird korrigiert, Malware kann schnell angepasst werden und Chatbots betreiben das oft aufwendige Social-Engineering. Soziale Organisationen sind besonders gefährdet, da sie oft weniger in Cybersicherheit investieren können als große Unternehmen und daher attraktivere Ziele darstellen.

Nachfolgend wird anhand einer strukturierten Darstellung eines Cyberangriffs durch das Framework "MITRE ATT&CK Frameworks" nachvollzogen, welche Taktiken, Techniken und Verfahren Cyberkriminelle nutzen, sodass soziale Organisationen Angriffsmuster besser verstehen können und Abwehrstrategien entwickeln.

Fallbeispiel eines Cyberangriffes

Im Januar 2022 wurde eines der größten humanitären Netzwerke Opfer eines schwerwiegenden Cyberangriffs. Dabei wurden sensible persönliche Daten von über 515.000 besonders schutzbedürftigen Menschen kompromittiert, darunter Vermisste, ihre Familien und Personen in Haft. Dieser Vorfall zeigt eindrücklich, wie gezielte Cyberangriffe auf soziale Organisationen ablaufen können.

1. Initiale Zugangsgewinnung und Ausführung: Durch Ausnutzung externer Remote-Dienste eines Drittanbieters durch die Angreifer wurde der Zugang zu sensiblen Datenbanken ermöglicht und eine langfristige Präsenz im Netzwerk etabliert.

2. Persistenz: Anschließend wurden Konten mit hohen Privilegien erstellt, um den Zugang aufrechtzuerhalten und nicht aufzufallen.

3. Privilegienerweiterung: Außerdem konnten gültige Accounts aus dem kompromittierten System genutzt werden, um die Zugriffsrechte zu erweitern.

4. Umgehen von Schutzmechanismen: Die Angreifenden deaktivierten Sicherheitssoftware, um die Aktivitäten und die Malware vor Sicherheitsüberwachungen zu verbergen.

5. Zugriff auf Anmeldeinformationen: Tools wie Mimikatz extrahierten Anmeldeinformationen aus dem Speicher und dem Domain-Controller.

6. Laterale Bewegung: Um weitere Systeme anzugreifen, wurden Remote-Dienstprotokolle und andere Protokolle genutzt. Mit gestohlenen Passwort-Hashes authentifizierten sich die Angreifenden auf anderen Systemen.

7. Sammlung von Daten: Die Angreifenden durchsuchten Netzwerkfreigaben nach sensiblen Daten. Sie griffen auf E-Mail-Server zu und extrahierten Nachrichten mit vertraulichen Informationen.

8. Exfiltration von Daten: Um die Übertragung zu beschleunigen und die Entdeckung zu erschweren, wurden Daten vor der Exfiltration komprimiert und verschlüsselt und anschließend über zugelassene Protokolle wie HTTPS aus dem Netzwerk übertragen.

9. Command-and-Control (C2): Die Angreifer kommunizierten über gängige Protokolle, um Befehle zu senden und Daten zu erhalten, wodurch sie weniger auffällig waren und verschleierten die C2-Kommunikation durch Verschlüsselung. Dadurch konnten sie ihre Aktivitäten vor Netzwerküberwachungstools verbergen.

10. Auswirkungen: Es wurden persönliche und sensible Daten von Hunderttausenden von Personen entwendet (exfiltriert).

Folgen des Angriffs

Die Angreifenden konnten große Mengen sensibler Daten entwenden. Die kompromittierten Informationen betrafen besonders schutzbedürftige Gruppen wie Vermisste und Gefangene. Die Cyberattacke gefährdete Personen, denn die Veröffentlichung oder der Missbrauch dieser Daten hätte potenziell schwerwiegende Konsequenzen für die Betroffenen haben können. Der Reputationsschaden für die Organisation war hoch, da das Vertrauen in die Fähigkeit, sensible Daten zu schützen, beeinträchtigt wurde. Last not least führte der Angriff zu Betriebsunterbrechungen. Bestimmte Dienste mussten vorübergehend eingestellt werden, um den Vorfall zu untersuchen und Sicherheitsmaßnahmen zu verstärken.

Der gezielte Angriff auf das soziale Netzwerk über Drittanbietende unterstreicht die Bedeutung von Sicherheitsmaßnahmen entlang der gesamten Lieferkette. Die präzisen Aktionen deuten darauf hin, dass die Angreifenden ein detailliertes Verständnis der internen Netzwerke hatten und ihre Aktivitäten trotz vorhandener Sicherheitslösungen verbergen konnten. Das deutet auf die Nutzung ausgeklügelter Techniken hin.

Reaktion der angegriffenen Organisation

Nach dem Angriff wurden einerseits die betroffenen Systeme isoliert, um eine weitere Kompromittierung zu verhindern. Die Organisation kommunizierte transparent, benachrichtigte die Betroffenen und arbeitete mit Cybersicherheitsexperten und den Strafverfolgungsbehörden zusammen. Auf der anderen Seite wurden die Sicherheitsmaßnahmen verbessert. Es galt, Drittanbietende zu überprüfen und sicherzustellen, dass alle Partner strenge Sicherheitsstandards einhalten. Die Implementierung fortschrittlicher Überwachungs- und Erkennungssysteme erhöhte die Netzwerksicherheit und durch Schulungen für Mitarbeitende wurde das Bewusstsein für Cyberbedrohungen erhöht.

Lehren für die Sozialwirtschaft

Die Herausforderungen sind nicht nur für die eigene Organisation groß – um Risiken aus der Lieferkette zu minimieren, müssen auch die Systeme von Partnern gesichert werden. Anwendungen und Datenbestände sind so zu priorisieren, dass besonders sensible personenbezogene Daten den höchsten Schutz erhalten. Dabei gilt der Zero-Trust-Ansatz. Ohne blindes Vertrauen müssen alle Systeme kontinuierlich überprüft werden.

Das bedeutet, das Cybersicherheit viel stärker in der Ressourcen- und Budgetplanung berücksichtigt werden muss, als dies heute der Fall ist. Kleinere Organisationen, die keine eigene IT-Unit unterhalten, sollten sich extern Unterstützung suchen.

Auch die Anwendung des Frameworks „MITRE ATT&CK" hilft dabei, die Taktiken und Techniken der Angreifenden besser zu verstehen und vermittelt ein besseres Verständnis von Angriffsverläufen und den genutzten Schwachstellen.

Fazit: Cyberangriffe sind eine reale Bedrohung für soziale Organisationen

Angreifende nehmen die Sozialwirtschaft in den Fokus, um an wertvolle und sensible Daten zu gelangen. Durch die detaillierte Analyse des Vorfalls und die Anwendung der notwendigen Mitigationsmaßnahmen können Organisationen effektive Strategien entwickeln, um Netzwerke zu schützen, Bedrohungen frühzeitig zu erkennen und angemessen zu reagieren.

Die Kombination aus fortschrittlichen Angriffstechniken der Täterinnen und Täter und menschlichen Schwachstellen in der Verteidigung macht proaktives Handeln unerlässlich. &

Die Menschen bei Althammer & Kill:

Fabian Eggers

Erzähle uns etwas über deinen beruflichen Werdegang. Wie bist du Marketing-Manager bei Althammer & Kill geworden?

Fabian Eggers: Ich habe zunächst Veranstaltungsmanagement studiert und bin dann als Projektleiter in den öffentlichen Dienst gegangen, später dort sogar als Abteilungsleiter. Doch dabei wollte ich immer schon mehr die verschiedenen Facetten des Marketings verstehen – besonders die Frage, wie Menschen kommunizieren und reagieren. Kommunikation und die richtigen Mittel dafür haben mich einfach fasziniert. Deshalb habe ich noch BWL mit Schwerpunkt Marketing und Vertrieb studiert, um mein Wissen zu vertiefen. Nach spannenden Erfahrungen in der Start-up-Szene und einem Abstecher in die Finanzberatung hat sich schließlich die Chance bei A&K ergeben.

Was hat dich besonders an der Branche Datenschutz und Informationssicherheit fasziniert?

Fabian Eggers: Bis dahin kannte ich Datenschutz und Informationssicherheit nur aus Anwendersicht, und das Thema hat mich neugierig gemacht. Besonders spannend fand ich die Herausforderung, wie man Datenschutz mit Marketing vereinen kann. Beide Bereiche scheinen auf den ersten Blick manchmal gegensätzlich zu sein – das eine verlangte Transparenz und Kreativität, das andere Kontrolle und Sicherheit. Ich wollte wissen, wie sich beides in Einklang bringen lässt und wie man verantwortungsvolles Marketing gestalten kann, das den Schutz der Daten ernst nimmt.

Welche Hauptaufgaben hast du als Marketing-Manager bei A&K?

Fabian Eggers: Als Marketing-Manager bei A&K konzentriere ich mich hauptsächlich auf die Koordinierung von Inhalten. Dazu gehört die Erstellung und Pflege unseres Kundenmagazins sowie das Verfassen von Blogbeiträgen, Broschüren und Beilegern, die unsere Dienstleistungen und Erfolge unterstreichen.

Zusätzlich unterstütze ich das Vertriebsteam, manage Kooperationen und kümmere mich um die interne Kommunikation. Es ist also sehr abwechslungsreich und vielseitig und gibt mir jeden Tag die Möglichkeit, kreativ zu sein und im Team zusammenzuarbeiten.

Was sind die größten Herausforderungen in deiner Position?

Fabian Eggers: Eine der größten Herausforderungen in meiner Position ist sicherlich, den Überblick über die vielen verschiedenen Projekte und Aufgaben zu behalten. Es ist oft ein Jonglieren zwischen den unterschiedlichen Inhalten und Anforderungen. Außerdem erfordert die ständige Anpassung an neue Trends im Marketing und im Datenschutz viel Flexibilität und Kreativität. Manchmal muss ich auch auf unvorhergesehene Ereignisse reagieren. Aber genau diese Dynamik macht meinen Job spannend.

Wie gehst du mit der sich ständig verändernden Marketinglandschaft um?

Fabian Eggers: Da heißt es wachsam bleiben, Augen und Ohren offenhalten und immer wieder neu abwägen. Ich setze auf eine Mischung aus Trends beobachten und mit dem Team gründlich diskutieren, was für A&K wirklich Sinn macht – und was nicht. Wir lassen uns nicht von jedem Trend treiben, sondern setzen auf durchdachte Entscheidungen. Flexibilität ist dabei der Schlüssel, denn so können wir das eine oder andere Experiment wagen, ohne den roten Faden zu verlieren.

Gibt es ein besonderes Projekt oder eine Kampagne, auf die du besonders stolz bist?

Fabian Eggers: Ja, definitiv! Ein Projekt, auf das ich besonders stolz bin, ist die Veröffentlichung meines ersten Kundenmagazins. Obwohl ich noch nicht lange bei A&K bin, war es eine spannende Herausforderung, dieses Magazin von der Idee der Inhalte bis zur Umsetzung zu begleiten.

Was machst du, um nach einem stressigen Arbeitstag abzuschalten?

Fabian Eggers: Ich höre gerne Podcasts, die mich inspirieren, oder lasse mich einfach von einer guten Serie oder einem spannenden Film fesseln. Sich richtig beim Sport auszupowern ist aber genauso gut.

Gibt es Hobbys oder Leidenschaften, die dir im beruflichen Alltag helfen?

Fabian Eggers: Auf jeden Fall! Beim Volleyball und Beachvolleyball lerne ich ständig, wie wichtig Teamwork und klare Kommunikation sind – genau das hilft mir auch im Job enorm. Man muss schnell reagieren, gut abgestimmt sein und als Team gemeinsam Entscheidungen treffen. Und dann gibt es noch meine Leidenschaft für Brettspiele. Die fordern Strategie, Durchhaltevermögen und oft auch Kreativität – Eigenschaften, die im Marketing genauso gefragt sind. Außerdem trainieren sie mein Gespür dafür, wie man Inhalte spannend vermittelt, was ich direkt in meine Arbeit einfließen lasse.

Hast du persönliche Ziele, die du in naher Zukunft erreichen möchtest?

Fabian Eggers: Definitiv! Beruflich möchte ich mich noch stärker im Bereich Content-Strategie weiterentwickeln und Projekte vorantreiben, die A&K langfristig einen echten Mehrwert bieten. Ich finde, sich regelmäßig neue Ziele zu setzen, hält einen nicht nur motiviert, sondern bringt auch jede Menge frische Energie!

Möchtest du dem Lesenden noch etwas mit auf den Weg geben? Vielleicht eine Lebensweisheit oder einen Tipp für den Alltag?

Fabian Eggers: Bleib neugierig und offen für Neues! Oft lohnt es sich, auch mal die Perspektive zu wechseln und Dinge von einer anderen Seite zu betrachten. Im Alltag hilft es, kleine Pausen bewusst zu nutzen – manchmal bringt ein kurzer Spaziergang oder einfach ein paar Minuten Ruhe ganz neue Ideen und Energie. Und am wichtigsten: Nimm dich und die täglichen Herausforderungen nicht zu ernst. Ein bisschen Humor macht das Leben leichter!

Althammer & Kill Akademie

20.–21. Januar 2025 – Online-Seminar

Datenschutzkoordinator/in DSGVO, DSG-EKD & KDG

Auch wenn keine Datenschutzbeauftragten bestellt werden müssen, sind Datenschutzgesetze und -regelungen einzuhalten und umzusetzen. Hier kommt der Datenschutzkoordinator bzw. die Datenschutzkoordinatorin als fachliche Unterstützung der Unternehmensleitung und Mitarbeitenden ins Spiel. Sie haben einen internen oder externen Datenschutzbeauftragten? Mit dem Lehrgang Datenschutzkoordinator/in erwerben Sie das notwendige Grundlagenwissen, um Datenschutzbeauftragte bei deren Arbeit fachgerecht zu unterstützen und kompetenter Ansprechpartner zu sein.

8. Januar 2025 – kostenloses Webinar

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

Fallen Sie unter NIS-2? Ihnen werden Methoden gezeigt, mit denen Sie prüfen können, ob Sie unter die Richtlinie fallen und ein Informationssicherheitsmanagement gem. den Anforderungen der NIS-2-Richtlinie in ihrer Organisation bzw. in Ihrem Unternehmen implementieren müssen.

22. Januar 2025 – kostenloses Webinar

Wie arbeite ich datenschutzkonform mit KI?

In unserem Webinar lernen Sie Künstliche Intelligenz besser zu verstehen, verantwortungsvoll damit umzugehen und erhalten wertvolles Wissen zum Schutz der Privatsphäre. Darüber hinaus können Sie die erworbenen Fähigkeiten direkt in der Praxis anwenden.

KLICK/SCAN

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

Ihre Ansprechpartnerin:

Nina Hoffmann
veranstaltung@althammer-kill.de
Tel. +49 511 330603-0

Compliance im Wandel: Die Rolle der Künstlichen Intelligenz in der Arbeitswelt

Anwendungen, die auf Künstlicher Intelligenz (KI) basieren, sind längst im Alltag angekommen. In der 4. Revolution wird insbesondere intelligente kognitive Arbeit durch KI automatisiert werden.

Welche Auswirkungen dies hat, erläutert Prof. Sabina Jeschke im Interview. Sie forscht auf dem Gebiet der KI unter anderem im Hinblick auf deren Einsatz in der Compliance und ist CEO des KI Park e.V.

Frau Prof. Jeschke, in welchen Bereichen sehen Sie die größten Chancen bei der Nutzung von KI?

Sabina Jeschke: Die größten Chancen liegen in der Analyse großer Datenmengen. Im Gesundheitsbereich wird ein Arzt oder Pflegender schwer in der Lage sein, die Daten eines Patienten über die vergangenen 20 Jahre vollumfänglich zu betrachten. Diese Integration von Daten wäre aber wichtig für die individualisierte Betreuung. In Ländern, in denen der Datenschutz sehr liberal gehandhabt wird, wie z. B. in Schweden, kommen wir auf ein ganz anders Level der individualisierten Medizin und Pflege. Hier sehe ich riesige Chancen.

Ein weiterer positiver Aspekt ist die Entlastung des Fachpersonals von repetitiven oder administrativen Tätigkeiten, wie Dokumentationen. Wenn Projektplanung, Festlegung von Schichtplänen und Administration automatisiert werden können, steht mehr Zeit für die eigentlichen Kernkompetenzen von Fachkräften zur Verfügung.

Mein dritter Punkt betrifft kulturelle Diversität. Wir sind eine bunte Gesellschaft und nicht für jede(n) ist Deutsch die Muttersprache. Der Einsatz von KI ist hier eine hervorragende Möglichkeit für Menschen, die Deutsch nicht gut verstehen oder in kritischen Situationen lieber in ihrer Muttersprache kommunizieren möchten.

„Transformation ist die Adaption von Organisationen an veränderte Lebensweisen und technologische Möglichkeiten“

Der Einsatz von KI-Systemen verhilft also auch zu mehr Individualisierung, mehr Personalisierung und mehr freiwerdenden Kapazität für die Kernaufgaben. Die meisten denken: Wird automatisiert und standardisiert, sinkt die Individualität – in Wirklichkeit ist es umgekehrt.

Wo sehen Sie die größten Risiken beim Einsatz von KI?

Sabina Jeschke: Da ist natürlich das Thema Datenschutz zu nennen. Auf der einen Seite brauchen wir einen Datenschutz, der personenbezogene Daten schützt. Auf der anderen Seite braucht KI aber Daten (anonymisiert und pseudonymisiert), um zu lernen. Es ist noch nicht ausdiskutiert, wo hier der Pfad der Vernunft liegt.

Ein weiteres Risiko, das noch nicht vollständig gelöst ist, betrifft sogenannte Bias. Das ist die Verzerrung von KI-Ergebnissen durch die Technologiesysteme selbst, bzw. durch Trainingsdaten, die einen Bias spiegeln können. Dadurch kann Benachteiligung entstehen. Bias bei KI-Systemen kann im Zweifel aber besser nachgewiesen werden als bei Menschen.

Die dritte Herausforderung bei KI-getriebenen Anwendungen ist die Intransparenz. Die statistischen, generativen und subsymbolischen Verfahren tendieren dazu, als Blackbox zu funktionieren. Der Gegenentwurf ist die erklärbare künstliche Intelligenz (Explainable Artificial Intelligence), aber dort besteht noch riesiger Forschungsbedarf. KIar ist, dass KI über sich Auskunft geben muss, wie sie zu ihren Ergebnissen kommt.

Wenn wir uns den Datenschutz ansehen, wie können Anforderungen wie Transparenz, Datenminimierung und Zweckgebundenheit mit KI vereinbar werden?

Sabina Jeschke: Privacy by Design ist das Zauberwort. Entwicklungen müssen das ganze Konzept bei der Entwicklung mitdenken und nicht hinterher versuchen, Datenschutz in die Prozesse zu integrieren. Damit eng verbunden ist die Transparenz der Prozesse, die klar definieren muss, wie die Prozesse funktionieren sollen und auf welche Daten zurückgegriffen wird.

Bei Datenminimierung ist die Sache anders gelagert. Der Datenschutz unterstellt pauschal, dass Datenminimierung eine gute Idee ist. Das ist ein großer Schwachpunkt der DSGVO, die entstand, als KI noch nicht die heutige Prominenz hatte. Wenn zur Wahl stünde, ob man bei der Privatsphäre kleine Abstriche macht und dafür fünf Jahre länger lebt, können wir uns ausmalen, wie die Menschen sich entscheiden würden.

Solange Datenschutz aber den Anspruch hat, vorher genau zu definieren, wozu Daten hinterher verwendet werden, kommen wir nicht weiter. Oft stellt sich erst später heraus, dass die Nutzung bestimmter Daten sehr sinnvoll wäre, wenn sie denn verwendet werden dürften.

Sie dürfen auch nicht vergessen, dass die Entwicklung von KI-Verfahren alles andere als statisch ist. Ein Auto, das ich heute kaufe, wird in fünf Jahren nicht plötzlich fliegen können. Das ist bei KI komplett anders. Deshalb werden eine ständige Zertifizierung und Auditierung über die Zeit nötig, weil das System sich verändert, während ich es benutze.

Die regulatorischen Herausforderungen bei der Nutzung von KI sind hoch. Welche besonderen Compliance-Anforderungen und ethische Fragestellungen entstehen dabei?

Sabina Jeschke: Auch dabei drehen sich die Fragestellungen um Datenschutz, Bias und Transparenz. In der Sozialwirtschaft sind die Herausforderungen durch KI-Anwendungen vielleicht noch ein bisschen anders gelagert als in anderen Branchen. Beim autonomen Fahren beispielsweise wird über die Fahrerdaten ermittelt, wann sich das Fahrzeug wo befunden hat und welches Bremsverhalten der Fahrer an den Tag gelegt hat. Selbstverständlich möchte niemand, dass diese Daten im Detail auch der eigenen Versicherung vorliegen. Trotzdem ist das etwas anderes, als sehr intime Gesundheitsdaten zu kommunizieren. Es sind einfach zwei unterschiedliche Ebenen personenbezogener Daten.

Prof. Sabina Jeschke, CEO des KI Park e.V.

Viele KI-Systeme funktionieren als Black-Box. Wer kann die Richtigkeit von KI-Ergebnissen im Kontext von Compliance überhaupt kontrollieren?

Sabina Jeschke: Das müssen hybride Teams leisten. Die KI macht Vorschläge (viel schneller als der Mensch es könnte) und der Fachmann oder die Fachfrau entscheidet, was Sinn macht und umgesetzt werden soll. Im Laufe der Zeit aggregieren sich die Daten immer mehr, sodass immer mehr automatisiert werden kann und die Ergebnisse immer richtiger werden.

Darüber hinaus braucht es externe unabhängige Prüfinstanzen, die wirklich bewerten können, wie das KI-System funktioniert und wo die Tücken liegen. Es ist also eine Kombination aus Menschen und Prüfungsinstanzen sowie regulatorischen Behörden.

Sabina Jeschke: *Sie haben in einem Vortrag vom kognitiven Shift hin zu kognitiven Unternehmen gesprochen. Die Durchdringung der Welt mit Sensoren und IT-Systemen ermöglicht die Kontrolle von Organisationen und Unternehmen durch Intelligenzmodelle, die mit biologischen Modellen vergleichbar sind. Welche Anwendungsbeispiele fallen Ihnen ein?*

Organisationen könnten sich selbst überwachen und bei auftretenden Fehlern automatisch eingreifen. Wenn wir an den Gesundheitssektor denken, ist das eins zu eins übertragbar auf Sensoren, die ein Patient möglicherweise am Bett hat, am Körper trägt oder die im Raum vorhanden sind. Diese Sensoren überwachen z. B. die Sättigung von Sauerstoff. Auf Basis automatisierter Parameter können Anpassungen eingeleitet werden, bis hin zu dem Schritt, Personal zu alarmieren. So können Zwischenfälle vermieden werden, die dadurch entstehen, dass Pflegepersonal nicht alle 20 Minuten beim Patienten ist, sondern nur alle zwei bis drei Stunden.

Es gilt, über die Grenzen von Organisationen hinauszuschauen. Wenn

sich jemand einer Operation unterzieht, in Reha geht und auch zu Hause weitere Maßnahmen vollziehen muss und diese einzelnen Bereiche über intelligente Technologien zu einer holistischen Perspektive verknüpft werden, dann haben wir ein verteiltes kognitives System.

Welche Voraussetzungen müssen Unternehmen mitbringen, um sich zu datengetriebenen, selbstwahrnehmenden Organisationen zu entwickeln?

Sabina Jeschke: Das ist ein sehr wichtiger Punkt. Organisationen müssen drei Voraussetzungen erfüllen: Erstens brauchen wir eine höhere Interdisziplinarität in den Unternehmen. In dem Moment, wo KI in Kernkompetenzen und Kernprozesse eingreift, müssen Organisationen Fachexpertise inhouse vorhalten, das kann man nicht outsourcen.

Das zweite Thema ist die Modifikation des Datenschutzes, um Daten und Datenzugang zu schaffen und der dritte Punkt ist der Kulturwandel, der sich vollziehen muss. Es geht darum zu erkennen, dass Unternehmen nur durch Öffnung hin zu Technologie besser werden können. Weil sich dadurch die DNA eines Unternehmens bis zu einem bestimmten Punkt verändert, sind klare Führungskompetenzen und Transformationswillen gefragt.

Eine große Hürde bei der Einführung von KI ist in vielen Branchen fehlendes Expertenwissen. Was wären die ersten Schritte, um hier voranzukommen?

Sabina Jeschke: Mein Rat ist, auf alle Fälle Pilotprojekte zu starten. Ich gebe Ihnen ein Beispiel: Als die ukrainischen Flüchtlinge zu uns kamen, sollten sie zuerst die Sprache lernen und dann in Arbeit gebracht werden. In anderen Ländern wurde es andersherum gemacht und dort zeigte sich, dass die Geflüchteten die Sprache schneller lernten. So ist das auch bei der KI-Einführung. Wenn Schulungen in die Einführung von kleinen Pilotprojekten integriert sind, kommen Sie schneller zum Ziel – learning on the project sozusagen.

Auch Kooperation mit branchenfernen Experten sind sinnvoll, um über den eigenen Tellerrand hinauszudenken und Learnings aus anderen Branchen zu adaptieren. Warum sollte die Überwachung einer Fabrikanlage von VW so viel anders sein als die Überwachung einer Pflegestation?

„Bis die Tinte unter einer neuen Regulierung trocknet, ist die Entwicklung schon wieder ganz woanders."

Außerdem muss die Infrastruktur aufgebaut werden. Große Chance bietet dabei die Cloudifizierung. Dass müssen Organisationen nicht selbst vorhalten, sondern kann gut outgesourct werden.

Welche Use-Cases halten Sie bei Pilotprojekten für besonders vielversprechend?

Sabina Jeschke: Bei der Automatisierung von Dokumentation kann man schnell Effekte heben, wenn man vernünftig digitalisiert ist. Personalplanung ist ein weiteres Feld. Hier frühzeitig Risiken zu erkennen, wenn zum Beispiel Personalengpässe an Feiertagen wegen Urlaub und Krankheit drohen, ist enorm hilfreich. Bei Branchen, die viel beraten, sind Chatbots ein gutes Versuchsfeld. Sie verlängern die Erreichbarkeit über Öffnungszeiten hinaus, sind immer freundlich. Ergebnisse aus Japan zeigen, dass sich Menschen einem Roboter gegenüber weniger schämen und sich viel mehr trauen, so einem System vermeintlich dumme Fragen zu stellen, als einem Mitmenschen gegenüber.

Technologieferne Branchen tun sich oft mit Digitalisierung sehr schwer. Wie kann dort ein Paradigmenwechsel überhaupt herbeigeführt werden?

Sabina Jeschke: Führungskräfte sind die Vorbilder in einer Organisation. Deshalb müssen Unternehmen von der Spitze aus ein klares Bekenntnis zu IT über die Führungsebenen vorleben. Es geht mit ganz trivialen Dingen los, wie zum Beispiel, dass Mitarbeitende nicht ins Büro der Führungskraft zitiert werden, was gerne mit langen Mobilitätszeiten verbunden ist, sondern man sich kurz in einer Videokonferenz bespricht. Das zeigt, dass digitale Kultur gelebt wird.

Transformation funktioniert nur, wenn zuvor Ressource dafür allokiert wurden. Alles andere klappt nicht und führt zu enormer Frustration. Außerdem sollte man Erfolgsgeschichten kreieren und nutzen. Deshalb sind Use-Cases und Pilotprojekte so wichtig, denn hier kommt man schnell zu Erfolgen. Die kommuniziert man nach innen und nach außen. Dann entsteht vielleicht ein kleiner Presseartikel zum Projekt oder man wird eingeladen, seine Learnings auf einer Konferenz vorzustellen. Nichts macht so stolz wie gemeinsamer Erfolg. Hinter allem steht Kulturwandel.

Gibt es in technikfernen Branchen überhaupt genug auswertbare Daten, um KI zu trainieren?

Sabina Jeschke: Man wird gelegentlich noch Unternehmen finden, die Zettelkästen nutzen, aber den meisten werden Daten weitgehend digitalisiert vorliegen. Die Herausforderung für technikferne Unternehmen ist, die Datenintegration und -verfügbarkeit sowie den -zugang zu verbessern.

Auf der anderen Seite ist nur ein Teil der KI-Anwendungen überhaupt datengetrieben. Deterministische KI-Verfahren, also die „symbolischen Verfahren", die vor allem in den 80er und 90er Jahren entwickelt wurden, kann man heute mit ganz anderer Professionalität und Rechnerkapazität betreiben als früher. Die sind belastbar in ihren Aussagen, denn sie halluzinieren nicht, was insbesondere bei medizinischen Daten von Vorteil ist.

Gerade im Hinblick auf die hohen Datenschutzanforderungen ist die Frage zu stellen, welche KI-Algorithmen es insgesamt eigentlich gibt. Ggfs. ist generative KI gar nicht unbedingt das Allheilmittel und andere Verfahren und Kombinationen überwinden das Datenverfügbarkeitsthema.

Der in der Sozialwirtschaft oftmals praktizierte, stark partizipative Führungsstil wirft bei Führungskräften hier immer wieder die Frage auf "Wie nehme ich die Leute mit?" Was empfehlen Sie diesen Führungskräften für eine erfolgreiche und nachhaltige Implementierung und Nutzung von KI in deren Organisationen?

Sabina Jeschke: Es ist zentral, den Widerspruch aufzulösen. „Alle mitnehmen" schiebt die Verantwortung zur Führungskraft. Das ist das Gegenteil von Partizipation und demotivierend, weil alle nur darauf warten, dass sie mitgenommen werden und nicht selbst Verantwortung übernehmen. Es muss aber um aktives Mitwirken, die Moderation des Wandels und Co-Creation gehen. Ich weiß, das sind Buzzwords, trotzdem haben sie nichts von ihrer Richtigkeit verloren.

Was können Führungskräfte aus der Einführung von KI-Systemen in anderen Branchen wie der Autoindustrie lernen?

Sabina Jeschke: Sie können Fehler vermeiden, indem sie die Best Practices übernimmt und so schneller zu Erfolgen kommen können.

Außerdem sind eine Hinwendung zu agilem Arbeiten und zu einer neuen Fehlerkultur entscheidend. Transformation und das Abweichen von bisher gelebten Prozessen fühlen sich bei manchen vielleicht so an, als würde man vermeidliche, bisher gemachte Fehler ausmerzen. Das ist aber nicht notwendigerweise so. Transformation ist eine Adaption an veränderte Lebensweisen und technologische Möglichkeiten. Eine gute Fehlerkultur zu leben ist eine große Herausforderung für viele Unternehmen.

Die rasante technologische Entwicklung läuft der Gesetzgebung und vielen Unternehmen davon. Wie können Organisationen aufschließen?

Sabina Jeschke: KI entwickelt sich so rasant. Bis die Tinte unter einer neuen Regulierung trocknet, ist die Entwicklung schon wieder ganz woanders. Der neue AI-Act bezieht sich in weiten Teilen auf einen Stand von KI, wie wir ihn vor ChatGPT hatten und das sieht man der Regulierung auch an. Sich proaktiv mit den Regulationen auseinandersetzen im Verbund mit Ökosystemen, die dasselbe Problem haben, kann ein Schlüssel sein. Jede Organisation die Experimente zulässt, die Innovationen offen gegenübersteht, die nicht in sich selbst verharrt, tendiert auch dazu, ihr Umfeld hinsichtlich wirtschaftlicher und politischer Veränderungen zu scannen, um reagieren zu können. Es geht darum, disruptive Denkmuster zu fördern. Wer seine Organisation ohnehin auf Veränderung, Agilität und Disruption ausrichtet, wird es auch bei der digitalen Transformation einfacher haben. &

ALTHAMMER & KILL

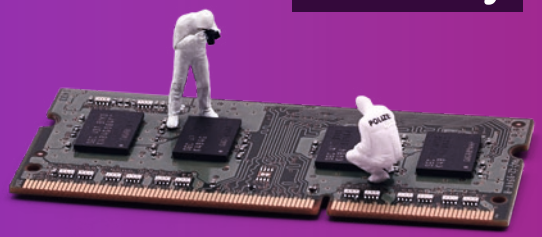
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

Wir sind Digitalisierungskenner, Datenversteher und Vorwärtsdenker –
Ihr Experte für Datenschutz, Informationssicherheit, Cloud- & Cyber-Security und Compliance.
Unsere 45 Mitarbeitenden bringen Digitalisierung und Datenschutz bundesweit in Einklang.

Datenschutz

Informations-sicherheit

Cloud- & Cyber-Security



Compliance

althammer-kill.de

KLICK/SCAN