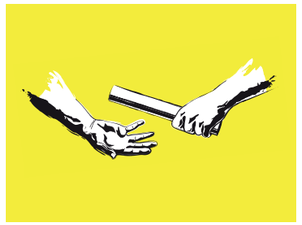
ExperSite

Das Magazin für Digitalisierung, Informationssicherheit und Datenschutz

Ausgabe 01 | 2022

DIGITALISIERUNG GEMEINSAM LEBEN

Cybersecurity-Kompetenz – Angriffe aus der Wolke 4



Joint Controllership 14

Interview: Sicherheitskultur durch Human Factors schaffen 23

ExperSite ist das Magazin der DR. JÄSCHKE-Gruppe für Digitalisierung, Informationssicherheit und Datenschutz

Zur DR. JÄSCHKE-Gruppe gehören die Unternehmen:

DR. JÄSCHKE DIGITALISIERUNG

www.dr-jaeschke.ag

Wir leben es einfach nicht.

Firmennetzwerk per Ikea-Einrichtungs-Assistent ihre Wohnung einrichten, sich schnell per Whatsapp über den Patienten Müller austauschen und das leckende Wasserrohr über dem Serverschrank mit einem Eimer vom einzigen IT-Mitarbeiter des Krankenhauses gerettet wird.

„Ganz schön unverschämt, die Frau Kill", denken Sie sich vermutlich gerade. Ich bin keine Freundin von geschönten Worten, eingepackt in viel rosa Watte, aber ich bin auch eine Freundin von Lösungen.

Und ich wünsche mir, dass Sie gemeinsam mit Ihrem Team alles dafür tun, um Prozesse zu optimieren, Risiken zu identifizieren und Probleme zu beheben – denn die Digitalisierung ist eine enorme Chance, die Sie mit den richtigen Tools, der richtigen Management-Attention und dem richtigen Personal gestemmt bekommen.

Und jetzt lassen Sie uns miteinander reden und uns gemeinsam die Hände schmutzig machen.

Viel Spaß bei der Lektüre.

Ihre Nina Kill
(Redaktionsleitung)

Wir sprechen von Digitalisierung. Wir sprechen von den unendlichen Möglichkeiten, die von technologischen Entwicklungen ausgehen, um unsere Gesellschaft zu einem besseren und lebbareren Ort zu machen, um die medizinische Entwicklung voranzutreiben und ressourcensparsamer agieren zu können. Worüber wir jedoch am liebsten nicht sprechen, sind die damit einhergehende Verantwortung, die Gefahren, die davon ausgehen und die Abhängigkeiten, in die wir uns damit begeben.

„Uns passiert schon nichts."

Manchmal kommt es mir vor, als ob sich Verantwortliche mit geschlossenen Augen in eine Ecke setzen, beide Hände auf die Ohren drücken und laut rufen: „Uns passiert schon nichts." Und das alles während gerade Mitarbeiter:innen im

- CYBERSECURITY-KOMPETENZ -

Angriffe aus der Wolke

Text: Thomas Jäschke

Die fortschreitende digitale Transformation bringt auch im Gesundheitswesen neue Herausforderungen mit sich. Das Interesse an digitalen Daten ist groß – nicht nur für diejenigen, die die Daten erheben, verarbeiten und kommunizieren, weil es für eine Vertragserfüllung notwendig ist oder einen wirtschaftlichen Mehrwert bieten kann. Sie sind die Voraussetzung zur Optimierung von Prozessen im Gesundheitswesen.

Die Forderung nach sektorenübergreifender Kooperation führt zu einer steigenden Kommunikation sensibler Daten. Große Datensammlungen sind Voraussetzung, insbesondere für die medizinische Forschung, aus der sich neue Diagnostikverfahren ableiten lassen. Ebenso können Behandlungsleitlinien verbessert werden und durch KI-Verfahren Zusammenhänge identifiziert werden, die ohne Anwendung von Big Data wegen der großen Komplexität nicht erkannt werden würden.

Aber wo Licht ist, ist auch Schatten. Die besondere Bedeutung dieser Daten lockt auch Kriminelle auf den Plan. Umfangreiche Dokumentationen wurden in der Medizin schon immer erstellt. Doch erst durch die Digitalisierung und die Vernetzung ist es Angreifer:innen möglich, aus allen Teilen der Welt auf diese Informationen zuzugreifen und diese je nach Ziel zu verändern, zu löschen oder zu kopieren.

„Gerade, wenn es um Menschenleben geht, wird deutlich, wie wichtig die Informationssicherheit als Voraussetzung einer erfolgreichen Digitalisierung ist."

(BSI 2020, S. 79)

Die vorstehende Aussage ist dem Fazit des BSI-Lageberichts zur IT-Sicherheit 2020 entnommen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist die Cyber-Sicherheitsbehörde des Bundes.

Der BSI-Lagebericht spiegelt in Zahlen einen ersten Eindruck der Quantität von Cyber-Angriffen wider. Die Angriffe erfolgen auf Basis unterschiedlicher Motivation. Deren Folgen für den Staat, die Unternehmen, Behörden und an allererster Stelle für die betroffenen Personen müssen im Einzelfall bewertet werden.

Die Vorfälle sind stark branchenabhängig

Voraussetzung für eine Interpretation der Zahlen ist das Wissen um die Zusammenhänge der Digitalisierung und den Folgen sowie ein tiefes Verständnis für die Geschäftsvorfälle in einer konkreten Branche, hier konkret im Gesundheitswesen. Allein die Geschäftsvorfälle im Gesundheitswesen unterscheiden sich stark in den verschiedenen Sektoren. Dazu kommen die steigenden Anforderungen an die intersektorale Kommunikation und damit einhergehend der elektronische Austausch zwischen den Leistungserbringern, den Kostenträgern und anderen Teilnehmer:innen des Marktes. Je nach Anforderungen an die Sicherheit müssen unterschiedliche technische und organisatorische Maßnahmen getroffen werden.

Zunächst geht es darum, den Schutzbedarf der betroffenen Daten zu ermitteln. Um diesen Schutzbedarf genau zu bewerten, bedarf es eines umfangreichen Branchen- und Prozesswissens.

Auf der anderen Seite stehen die Anforderungen im Fokus, mögliche Bedrohungen zu identifizieren. Dies kann wiederum nur mit der notwendigen Kompetenz im Bereich der informationstechnischen Systeme gelingen. Wie die Komplexität der verschiedenen Disziplinen in der Medizin in der Vergangenheit immer weiter zugenommen hat, so wird diese durch den weiter steigenden Einsatz der Medizininformatik auch zukünftig zunehmen.

Die erfolgte Bedrohungsanalyse ist zusammen mit der Abschätzung des potenziellen Schadens die Grundlage für eine Risikobewertung. Auf Basis der gesammelten Informationen zur Bewertung können anschließend Maßnahmen identifiziert werden, um das Risiko zu minimieren. Eine Eliminierung aller Risiken ist in der Regel nicht möglich, sodass auch an dieser Stelle auf Basis einer Wirtschaftlichkeitsbetrachtung ein optimales Gleichgewicht zwischen Kosten und Sicherheit erzielt werden muss.

Die zentrale Aussage lautet:

> **Eine 100-prozentige Sicherheit gibt es nicht.**

Das vorhandene Restrisiko muss also akzeptiert werden. Gut, wenn dieses bekannt ist. Denn in vielen Fällen wurden die vorstehenden Schritte gar nicht erst begonnen und die Verantwortlichen haben einfach nur ein schlechtes Bauchgefühl und hoffen, dass nichts passiert. Wenn dann doch etwas passiert, kann der Schaden, ohne Vorkehrungen getroffen zu haben, jedoch sehr hoch werden. Er kann am Ende Menschenleben kosten.

Die Anforderungen an die Cyber-Sicherheit zu erfüllen leitet sich in großen Teilen, insbesondere im Gesundheitswesen, aus gesetzlichen Vorgaben ab. Darüber hinaus sind sicherlich auch weitere Informationen schützenswert und so Teil der internen Compliance, die sich nicht aus Gesetzen ableiten. Am Ende geht es darum, verschiedenste Kategorien von Informationen zu schützen, wie beispielsweise Bilanzdaten, Qualitätsdaten, Diagnosedaten sowie Forschungsergebnisse.

Einheitliche Begrifflichkeiten bilden die Basis

Es besteht noch eine große Unschärfe bei der Benutzung von Fachwörtern rund um das Thema „Cybersecurity" – vielmehr lässt sich eine Art „Begriffswolke" zeichnen. Meist hat man schnell eine eigene Interpretation von Begriffen, welche zwar in die richtige Richtung geht. Wo Unterschiede gegeben sind, ist aber die sichere Verwendung wichtig.

Gern wird in Diskussionen die Kombination aus Datenschutz und Datensicherheit oder ebenso gern Anonymisierung versus Pseudonymisierung verwendet. In der konkreten Umsetzung oder gar im Hinblick auf gesetzliche Anforderungen gibt es hier große Unterschiede. In vielen Fällen wird dann im Verlauf des weiteren Gesprächs deutlich, dass Vielen die Unterschiede nicht klar sind und so falsche Schlüsse gezogen werden. Insbesondere der Datenschutz wird oftmals fehlinterpretiert und als Störfaktor gesehen.

Bekannteste Floskel ist sicher:

> **Das geht aus Datenschutzgründen nicht.**

Um die umgangssprachlichen Probleme mit den Begriffen Datenschutz und Datensicherheit zu eliminieren, kann eine Abgrenzung der Begriffe hilfreich sein.

Datensicherheit ist dabei eher ein Oberbegriff. Es scheint also darum zu gehen, dass Daten sicher gehalten werden sollen. Einzelne Zeichen und daraus zusammengesetzte Daten haben aber für sich stehend oftmals noch keinen Wert, sondern werden erst wertvoll, wenn verschiedene Daten in einen Zusammenhang gebracht und so zu Informationen werden. Zum Beispiel ist eine Liste mit ansonsten öffentlich zugänglichen Adressdaten nicht besonders schützenswert. Wird diese Liste jedoch so benannt, dass es sich um eine Teilnehmergruppe zu einer Nachsorge eines konkreten Krankheitsbildes handelt, so erhöht sich die Schutzbedürftigkeit und es werden Daten einer besonderen Kategorie erhoben, gespeichert und übermittelt. Aus einfachen Daten werden Informationen.

Da Informationen einen höheren Wert als Daten haben, wurde statt des Begriffs Datensicherheit der Begriff **Informationssicherheit** eingeführt. In Unternehmen und Institutionen heißt die Rolle daher nicht Datensicherheitsbeauftragter, sondern Informationssicherheitsbeauftragter. In obigem Beispiel liegt aber auch eine Besonderheit: Die Daten sind personenbezogene Daten im Sinne des Art. 9 der Europäischen Datenschutzgrundverordnung (EU-DSGVO) und unterliegen dem Datenschutz. Dafür ist in einer Institution eine weitere Rolle verantwortlich: **der Datenschutzbeauftragte.**

Datenschutz ist somit ein Teil der Informationssicherheit, der allerdings durch gesetzliche Rahmenbedingungen geregelt ist.

Die IT-Sicherheit hingegen, ebenfalls Teil der Informationssicherheit, stellt die technischen Maßnahmen zum Schutz der Informationen dar. Eine Firewall allein macht aber noch kein Netzwerk oder Server sicherer. Zuvor müssen die eingangs erläuterten Schritte erfolgen. Die IT-Sicherheit folgt daher den Vorgaben der Informationssicherheit. Cyber-Sicherheit kann im Prinzip als erweiterte IT-Sicherheit betrachtet werden, da diese den Fokus auf die Kommunikation und die verwendeten Verfahren über das öffentliche Netz, das Internet, einschließt.

Der gemeinsame Erfolg steht und fällt mit einem gemeinsamen Verständnis – nicht nur über die Notwendigkeit, sondern auch in der Begriffswelt. Es werden zwingend Vermittler zwischen den Welten benötigt, die durch ihre interdisziplinären Kenntnisse eine umfängliche Sicht auf den Themenkreis Informationssicherheit, Datenschutz, IT-Sicherheit und Cyber-Sicherheit bekommen können.

Cybersecurity – Kein Thema für Nerds

Es werden also Expert:innen benötigt, welche in den beiden Branchen Gesundheitswesen und Informatik zu Hause sind. Dazu kommen die Fachkompetenzen mit Blick auf die Medizin, als einen Bereich, der mit besonders sensiblen Daten betraut ist und die Perspektive der Informationssicherheit.

Eingebettet in das Thema Informationssicherheit ist Cybersecurity aber sicher kein Thema für Nerds. Schon gar nicht, wenn man ihnen, nach allgemeiner Meinung, die fehlenden Kompetenzen im Bereich der Soft Skills abspricht, die zweifelsohne über die reine Fachlichkeit hinaus notwendig sind. Keine Frage, in den Tiefen der Cyber-Abwehr muss man jedes Bit beim Vornamen kennen. Aber funktionierende Cyber-Abwehr ist viel mehr.

> Cybersecurity muss als Teamwork par excellence gesehen werden, um erfolgreich zu sein.

Das Thema beginnt auf der Managementebene, geht über das Security Engineering bis hinunter auf die System- und Netzwerkebene. Die benötigten Soft Skills sind daher höchst umfangreich. So muss die Fähigkeit zum Perspektivenwechsel vorhanden sein. Das Verständnis für die Anforderungen und Prioritäten aus Sicht der Organisation muss ebenso selbstverständlich sein, wie die Sicht des Angreifers, seiner Ziele und Bemühungen sowie nicht zuletzt der Betrachtungswinkel der Mitarbeiter:innen, dessen sich die Angreifer oftmals durch verschiedene Angriffsmethoden bedienen.

Ohne die notwendige Fach- und die Methodenkompetenz geht es selbstverständlich nicht. Aber diese muss zwingend durch eine umfangreiche soziale Kompetenz ergänzt werden. Die Anforderungen schließen Authentizität und Empathie ein, die mit der Beratungskompetenz und dazugehörigem Durchsetzungsvermögen zusammen die Voraussetzung bilden. Die Kandidat:innen müssen ausgeprägte konfliktfähige Moderationstalente sein, die durch analytisches Denken und Handeln das erwartete Qualitätsbewusstsein mitbringen.

Prof. Dr. Thomas Jäschke

Thomas Jäschke ist als Medizin- und Wirtschaftsinformatiker tätig und Vorstand der DR. JÄSCHKE AG und der DATATREE AG. Hier berät und unterstützt er Unternehmen in den Bereichen Digitalisierung, Compliance, Informationssicherheit, Datenschutz und IT-Sicherheit. Thomas Jäschke legt bei seiner Arbeit besonderen Fokus auf die Themen Intersektorale Vernetzung und die entsprechenden Sicherheitsaspekte und hat maßgeblich an der Erfindung und Markteinführung der Zuweiserportale mitgewirkt. Als Lehrbeauftragter der FOM Hochschule für Oekonomie und Management gGmbH im Studiengang Wirtschaftsinformatik legt er den Schwerpunkt auf IT-Security, Mobile Computing und Informationsmanagement.

Dieser Beitrag ist ein Auszug aus dem Buch:

Future Skills in Medizin und Gesundheit Kompetenzen. Stärken. Menschen.

ISBN: 978-3-95466-594-5
www.mwv-berlin.de

Das Praxisbuch will mit vielen Anekdoten, harten Fakten und Beispielen Inspiration geben für Ärztinnen und Ärzte, Führungskräfte sowie Gründerinnen und Gründer im Gesundheitswesen. Es geht um einen Paradigmen- und Kulturwechsel – hin zu Technik und Humanitas.

Literatur

Bundesamt für Sicherheit in der Informationstechnik (BSI) (2020) Die Lage der IT-Sicherheit in Deutschland 2020. *URL: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html*
(abgerufen am 26.01.2021)

Der Mensch steht im Mittelpunkt der Digitalisierung

Text: Thomas Jäschke

Ich bin überzeugt, dass Menschen im Mittelpunkt der Digitalisierung stehen. Das ist noch keine Selbstverständlichkeit: Digitalisierung ist nur sinnvoll, wenn sie den Menschen dienlich ist. Dieser Punkt ist auch entscheidend für den Erfolg Ihrer Organisation, denn die holistische Sicht ist entscheidender Erfolgsfaktor und geht weit über die klassische IT-Perspektive hinaus. Sie muss alle Beteiligten, intern wie extern, in der Digitalen Transformation mitnehmen und einbinden.

Die Wertschätzung dieser Beteiligten liegt mir und meinem Team der DR. JÄSCHKE-Gruppe am Herzen, weil nur so die Wirksamkeit und Optimierung der Wertschöpfung gewährleistet ist. Damit komme ich nun zu einem weiteren Aspekt: Partnerschaften. Partnerschaften sind der Schlüssel des Gelingens in Zeiten knapper Ressourcen und insbesondere knapper Zeit. Die dadurch notwendige Effizienz erfordert die Definition neuer Rollen und Mitarbeiterprofile, um den Anforderungen gerecht zu werden. Ergänzend dazu befähigen wir Ihre Mitarbeiter:innen durch die Akademieangebote der Dr. Jäschke-Gruppe.

Entscheidend ist die professionelle Steuerung der Projekt-Teilnehmer:innen, intern sowie extern. Mit der DR-JÄSCHKE-Gruppe an Ihrer Seite verfügen Sie sogleich über die erforderliche Expertise und die notwendigen Ressourcen auf allen Organisationsebenen, inklusive C-Level.

Willkommen zu unserem wöchentlichen KHZG-Roundtable.

Auch, wenn Digitalisierung bereits ein Thema der 90er Jahre ist, bringen Themen wie der Krankenhausstrukturfonds, das IT-Sicherheitsgesetz 2.0, die Telematik Infrastruktur und nicht zuletzt das Krankenhauszukunftsgesetz immer wieder neuen Diskussionsbedarf.

Gemeinsam mit Gleichgesinnten über die Herausforderungen und Themen des Krankenhauszukunftsgesetz (KHZG) sprechen, sich Hilfestellung für die eigenen Projekte geben und aus der eigenen Praxis berichten: Hier trifft man sich wöchentlich, um genau diesen wertvollen Austausch zu pflegen.

Die einen verfluchen es, die anderen sehen es als Chance, denn für die einen ist das KHZG die Fördermöglichkeit von Projekten, die in den nächsten Jahren sowieso umgesetzt werden sollten, für die anderen ist es enormer Druck, der bei der Nichtumsetzung zu Strafen in Form von Abschlägen führen kann. Es bietet sich hier die Gelegenheit, Defizite in Krankenhäusern durch Analysen zu identifizieren und diese durch die bereitgestellte Förderung auszugleichen.

Der erste Impuls ist gesetzt. Die interne Überlegung der Krankenhäuser über erforderlichen Bedarf und Modernisierung. So werden unterschiedliche Akteure aus verschiedenen Abteilungen an einen Tisch gebracht, um gemeinsam Probleme zu erörtern und Projekte zu definieren. Der Austausch mit Gleichgesinnten ist hier von elementarer Bedeutung. Nicht nur das ist der Grund, weshalb der von Herrn Prof. Dr. Thomas Jäschke initiierte Roundtable zum KHZG regen Anklang findet. Eine feste Agenda gibt es selten – und das ist auch gut so.

Unklarheiten über die Vertragsvergabe, die Projektskizzen und die zu stellenden Anträge werden thematisiert.

Jede Woche bringen die Krankenhausvertreter:innen und Softwareanbieter:innen ihre Fragen mit, diskutieren diese untereinander und finden Lösungen und neue Ansatzpunkte rund um die Antragsstellung zum KHZG.

> „Man ist sich einig: das KHZG ist ein Meilenstein, um die Digitalisierung in den Krankenhäusern voranzutreiben.

Für die Kliniken ist es eine große Herausforderung, die richtigen Lösungen zu kombinieren. Einerseits bestehet die Abhängigkeit der etablierten Primärsystemanbieter, andererseits drängen immer mehr Lösungsanbieter für Nischen- und Spezialprodukte in den Markt. Auch die Thematik, dass Digitalisierung häufig von Geschäftsführer:innen ausschließlich von der Kostenseite betrachtet wird, macht es den Verantwortlichen nicht leichter. Insbesondere auch deshalb, weil der Gesetzgeber offenlässt, wie die Häuser mit den laufenden Kosten nach der Förderphase innerhalb des KHZG umgehen müssen.

Die Geschäftsführung muss die Digitalisierung im Sinne der ganzheitlichen Unternehmensstrategie verstehen und kommunizieren. Nur dann können die Projekte erfolgreich umgesetzt werden und die Digitale Transformation im Gesundheitswesen nachhaltig zu den dringend notwendigen Verbesserungen führen.

Der von Professor Dr. Thomas Jäschke initiierte wöchentliche Roundtable ist für alle Interessierten geöffnet. Die einzige Voraussetzungen: Werbung von IT-Unternehmen sind hier fehl am Platz. Es geht ausschließlich um den fachlich-fundierten Austausch.

Werden Sie Teil unserer KHZG-Community unter:
https://www.linkedin.com/groups/9020042/

How-To: (Digitales) Management von Datenschutz im Unternehmen

Text: Alexander Vogel

Die Komplexität des Datenschutzes und die u.a. damit verbundenen Dokumentationen werden immer vielfältiger. Zudem nimmt die Digitalisierung der Industrie, des Gesundheitswesens und vieler weiterer Branchen immer mehr Fahrt auf. Warum also nicht auch das Management des Datenschutzes im Unternehmen digitalisieren?

Wenn vom Datenschutz-Management die Rede ist, meint dies nicht nur die unterschiedlichen Arbeitsanweisungen, Richtlinien und Regelungen zum Datenschutz im Unternehmen - hierzu würde für die Digitalisierung auch ein Dokumentenmanagementsystem oder Intranet ausreichen. Es geht vielmehr um die Digitalisierung der Prozesse zum Datenschutz.

Als anschauliches Beispiel für die Digitalisierung von Datenschutz-Prozessen ist die Meldung von Datenschutzverletzungen prädestiniert: In vielen Unternehmen erfolgt die Meldung telefonisch direkt an die Datenschutzbeauftragte:n. Falls dieser nicht erreichbar ist, wird die Datenschutzverletzung per E-Mail gemeldet oder ggf. später per Telefon - manchmal wird dies im Laufe des Arbeitstages auch vergessen. Und hier wird schon wertvolle Zeit verloren, da im Fall einer Meldung an die Aufsichtsbehörde die 72-Stunden-Frist gilt (lesen Sie hierzu unsere ExperSite-Ausgabe 01/2020). Erfolgt dann noch eine verspätete Meldung an die Aufsichtsbehörde, unterstellt Ihnen diese Organisationsverschulden.

Im besten Fall funktioniert die erste telefonische Aufnahme direkt und die Datenschutz-Verletzung wird irgendwie - meist unstrukturiert - dokumentiert und nach bestem Wissen und Gewissen einer Risikoabschätzung unterzogen. Dann erfolgt die Meldung an die Aufsichtsbehörde - falls notwendig - und die Datenschutz-Verletzung wird in irgendeiner Word- oder Excel-Datei dokumentiert. Fertig!

Schauen wir uns einmal an, wie hier die Digitalisierung helfen kann:

Ihr Datenschutz-Managementtool besitzt eine integrierte Meldeplattform für Datenschutzverletzungen, welche für alle Mitarbeitenden - auch anonym - genutzt werden kann. Die wichtigsten Angaben zur Datenschutzverletzung werden in einem strukturierten Formular erfasst und an das System übertragen. Das System informiert direkt die zuständigen Personen (z.B. Datenschutzbeauftragte, Datenschutz-Koordinator:innen, Informationssicherheitsbeauftragte etc.) und aktiviert den 72-Stunden-Countdown.

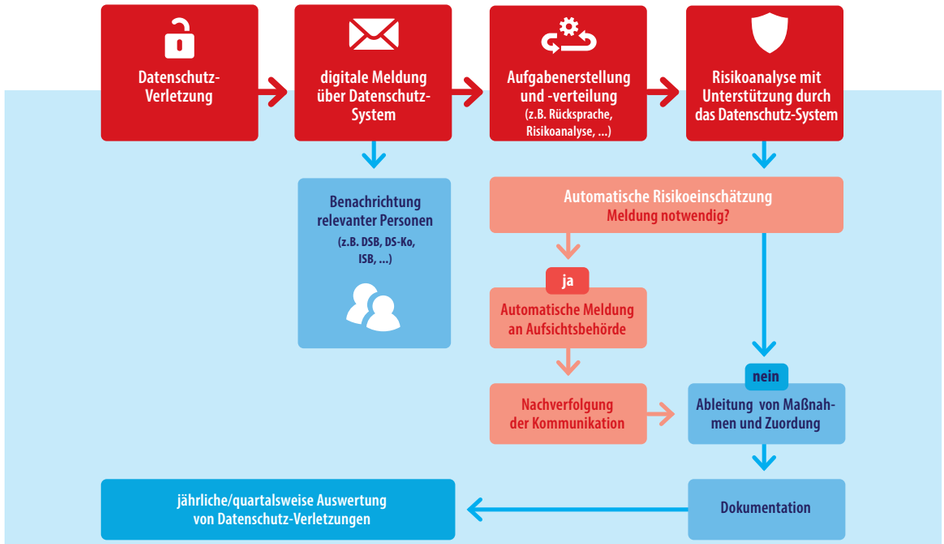
Über ein Aufgaben- und Workflowmanagement verteilt das System direkt die ersten Aufgaben zur Bearbeitung der Datenschutzverletzungen - Kontaktaufnahme zur meldenden Person, Analyse und Risikobewertung der Datenschutzverletzung. Nach der Abarbeitung der verschiedenen Aufgaben folgt zum Abschluss die Übermittlung der Datenschutzverletzung an die zuständige Aufsichtsbehörde (hier müsste jedoch ein deutschlandweit einheitliches digitales Meldeverfahren etabliert werden). Durch die digitale Bearbeitung der Datenschutzverletzung und der Dokumentation der einzelnen Prozessschritte entsteht mit Beendigung der Datenschutzverletzung eine umfangreiche Dokumentation und somit eine ausreichende Erfüllung der Rechenschaftspflicht.

Doch mit der eigentlichen Bearbeitung und Dokumentation der Datenschutzverletzung mit System hört der Nutzen nicht auf - durch die strukturierte Meldung lassen sich Verknüpfungen mit anderen Dokumentationen wie z.B. dem Verzeichnis von Verarbeitungstätigkeiten, Dienstleistern oder Auftragsverarbeitern herstellen. Dies kann für zur Auswertung von Datenschutzverletzungen und damit einer Verbesserung der Geschäftsprozessen hinsichtlich des Datenschutzes genutzt werden. Ein weiterer Vorteil ist die automatische Erstellung von Reportings zum Datenschutz für die Geschäftsführung.

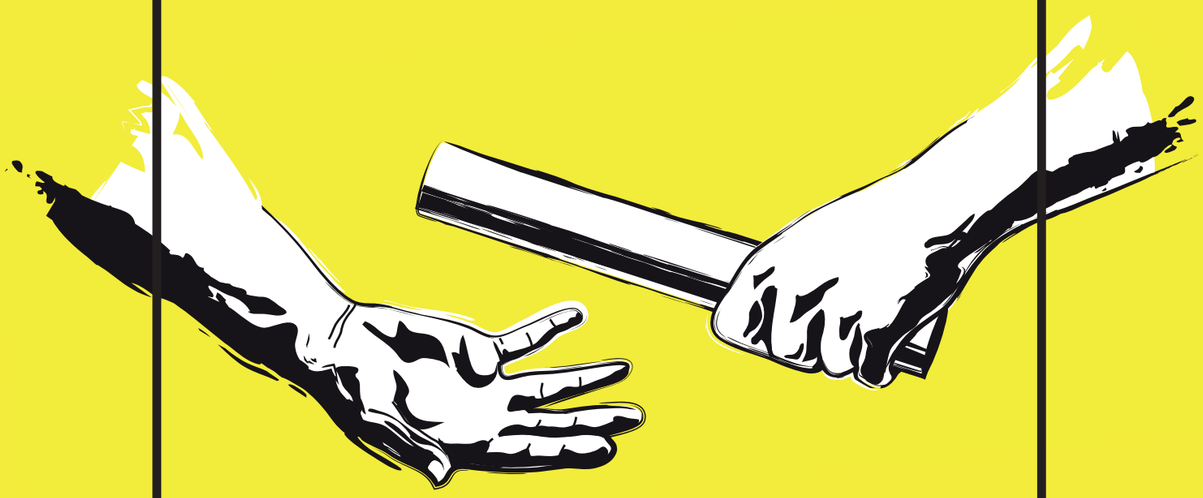
Das Beispiel der Digitalisierung des Melde- und Analyseprozesses von Datenschutzverletzungen zeigt, dass erhebliches Potenzial auch für die Digitalisierung beim Datenschutz-Management besteht. Viele weitere Beispiele wie die digitale kollaborative Erfassung und Verwaltung des Verzeichnisses von Verarbeitungstätigkeiten, Durchführung der Schwellenwertanalyse und Datenschutz-Folgenabschätzung können einen erheblichen Mehrwert für das Management des Datenschutzes darstellen.

Weitere Informationen zu unserem Tool für Ihr Datenschhutz-Management erhalten Sie unter:
www.gaimssoftware.de

Ablauf von Datenschutz- und Sicherheitsvorfällen



JOINT CONTROLLER SHIP



Lohnt sich die Flucht vor dem Joint Controllership!?

Text: Winona Wenning

Die Auftragsverarbeitung sowie die dazugehörige Vereinbarung sind wohl jedem, der mit Datenschutz in Berührung kommt, längst ein Begriff. Jedoch wird vielerseits vor der „Flucht in die Auftragsverarbeitung" gewarnt, weshalb das Konstrukt des Joint Controllership immer mehr Aufmerksamkeit bekommt.

In der Literatur wird oft vor der „Flucht in die Auftragsverarbeitung" (Dochow, Telemedizin und Datenschutz, MedR 2019, 636, 640 f.) gewarnt, welche vornehmlich im Bereich der Telemedizin und Digitalisierung der Gesundheitsbranche um sich greife. Neben der Auftragsverarbeitung kennt die Datenschutzgrundverordnung eine weitere Verarbeitungssituation mit mehreren Akteuren, namentlich die gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO. Das Konstrukt des sog. Joint Controllership bietet eine gemeinsame Datenverarbeitung auf Augenhöhe mit weniger starren Vorgaben. Außerdem kommt es bis jetzt in der Praxis bedeutend seltener zum Einsatz, da die Gestaltungsspielräume mehr Unsicherheiten bergen. Aber muss man vor der gemeinsamen Verantwortlichkeit deswegen wirklich flüchten?

Art. 26 DSGVO eröffnet den Akteuren, die unter Geltung der Datenschutzgrundverordnung mit personenbezogenen Daten zusammenarbeiten wollen, eine weitere Möglichkeit, diese Kooperation auszugestalten. Während die Auftragsverarbeitung gemäß Art. 28 DSGVO eine klare Hierarchie zwischen Auftragnehmer und Auftraggeber verordnet, welche sich in Rechten und Pflichten der Parteien niederschlägt, eröffnet Art. 26 DSGVO große Spielräume: Beide Parteien können „unter sich ausmachen", wie sie die zahlreichen Pflichten, die eine datenverarbeitende Stelle treffen, aufteilen. Einzige Grenze sind dabei Transparenz und die Rechte der betroffenen Person, welche nicht erschwert oder verringert werden dürfen.

Dieser Weg ist vorgesehen, wenn nicht eine Partei weisungsgebunden agiert, sondern eben beide Joint Controller die Zwecke und Mittel der Datenverarbeitung bestimmen. Dies ist zumeist der Fall, wenn auch beide Parteien eigene Interessen mit der Verarbeitung, die über die Erfüllung eines Auftrags hinausgehen, verfolgen. Die gemeinsam Verantwortlichen verhandeln neben der Verarbeitung der Daten auch die Aufteilung der gesetzlichen Verpflichtungen.

Diese Freiheit des Joint Controller ist auch gleichzeitig seine Schwierigkeit: Die Aufgaben müssen individuell und mit Blick auf eine sachgerechte Verteilung zugewiesen werden. Häufig werden bilaterale Abstimmungen notwendig, wenn Betroffenenrechte umgesetzt werden oder eine Datenschutzpanne bewertet werden muss. Auch gilt es den Überblick zu behalten: Wurden alle Pflichten verteilt?

Auch die Partei, welche eine Aufgabe nicht übernimmt, hat gegebenenfalls Anpassungsbedarf: Für Betroffenenanfragen und Datenschutzpannen müssen Benachrichtigungsprozesse implementiert werden, die die vertraglich vereinbarten Fristen einhalten, um dem zuständigen Partner genug Zeit zur Bearbeitung zu lassen. Denn auch für Joint Controller gelten die strengen Fristen aus Art. 33 Abs. 1 und Art. 12 Abs. 3 DSGVO. Ebenso müssen bereits bestehende Prozesse zu den Grundpflichten der Verantwortlichen darauf hin überprüft werden, ob sie den vertraglichen Zusicherungen entsprechen.

!!!

Aber: Eine „falsche" Auftragsverarbeitung ist nicht nur ein bußgeldbewehrter Verstoß (Art. 83 Abs.4 lit. a DSGVO) gegen die Datenschutzgrundverordnung, sie schränkt auch die Rechte der Betroffenen im Ernstfall ein.

Wann handelt es sich typischerweise um eine Situation des Joint Controllers?

Aufsehen erregte der EuGH am 05.06.2018 mit der Entscheidung, die Betreiber von Facebook-Fanpages in gemeinsame Verantwortung mit Facebook selbst für die Verarbeitung der personenbezogenen Daten der Seitenbesucher zu stellen. Auch durch die Einbindung eines „Gefällt mir"-Button des sozialen Netzwerkes auf der eigenen Website begeben sich die Website-Betreiber:innen in die gemeinsame Verantwortung mit Facebook, urteilte der EuGH im Juli 2019. Selbst der Betrieb einer Unternehmenspräzens auf anderen Social Media Plattformen, die die Möglichkeit bieten, personenbezogener Daten der Endnutzer :innen zu erheben, kann zu einer gemeinsamen Verantwortlichkeit führen, da der EuGH seine Urteile entsprechend weit fasste. Twitter, XING oder Instagram werfen mit vergleichbaren Auswertungsmöglichkeiten datenschutzrechtliche Fragen auf, standen aber bisher nicht im Fokus der Diskussion.

Was sind Joint Controller?

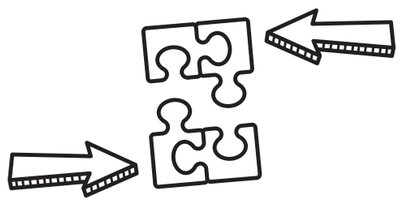
Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und Mittel zur Verarbeitung fest, sind sie nach der Datenschutz-Grundverordnung (DSGVO) gemeinsam Verantwortliche. Sie werden auch Joint Controller genannt.

In den folgenden Fällen sollten die datenverarbeitenden Stellen eine Vereinbarung gem. Art. 26 DSGVO abschließen:
Neben dieser eher unfreiwilligen Zusammenarbeit ist eine typische Situation des Art. 26 DSGVO die gemeinsame Stammdatenverwaltung durch ein CRM innerhalb eines Konzerns. Auch die Nutzung der Adressbestände eines Lettershops für Werbung ist nach Einschätzung der Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.) ein Anwendungsfall der gemeinsamen Verantwortung. Auch im Bereich klinischer Studien kann es notwendig werden, dass Studienzentren und Sponsoren eine Art. 26 Vereinbarung schließen. Auch der kooperative Betrieb einer Buchungsplattform für Reisen durch ein Reisebüro mit einer Hotelkette ist eine gemeinsame Verantwortlichkeit. Eine umfangreiche Whitelist findet sich im Working Paper 169 der Art.-29-Datenschutzgruppe.

!!!

Immer sollte an Art. 26 DSGVO gedacht werden, wenn gemeinsam eine Infrastruktur errichtet wird, die es mehreren Beteiligiten ermöglicht, ihre individiuellen Zwecke zu verfolgen.

Die Grenzziehung, wann es sich um die im Gesetz geforderte gemeinsame Festlegung von Zwecken und Mitteln der Verarbeitung handelt, fällt im Einzelfall schwer. Trifft dies zu, bieten die nur minimalen gesetzlichen Grenzen den Freiraum, den es für eine sachgerechte Vereinbarung braucht. Eine vermeintliche Auftragsverarbeitung kann den komplexen Verarbeitungssituationen nicht gerecht werden. An dieser Stelle stehen wir gerne beratend zur Seite, und erarbeiten mit unseren Kund:innen eine im Einzelfall angemessene Lösung.



Eine Flucht vor dem Joint Controllership ist mit der richtigen Beratung also gar nicht nötig.

Kompetenzentwicklung ist kein Zufall

Text: Angelica Morina

All diese Formulierungen sind nur kleine Auszüge aus diversen Stellenanzeigen, die im Grundtenor nur eines aussagen: Qualifiziertes Personal zu finden, ist für den Großteil von kleinen und mittelständischen Unternehmen (KMU) eine Herkulesaufgabe.

Es existieren weder große Budgets für Marketingkampagnen, sodass geeignete Bewerber:innen maximal durch Zufall auf die Stellenausschreibung aufmerksam werden, noch existiert ein großer Pool an Menschen, die fachlich bereits so gut in den Bereichen Digitalisierung, Informationssicherheit, IT-Sicherheit oder Datenschutz im Gesundheitswesen ausgebildet sind, dass sie geeignete Kandidat:innen für eine entsprechende Stellenbesetzung sind. Als Unternehmensgruppe, die sich genau diesen Themen verschrieben hat, haben wir bereits früh erkannt, dass es notwendig ist, für unsere Berufsfelder eigene Kompetenzen für Nachwuchskräfte zu entwickeln. Für Berufs- und Quereinsteiger:innen bietet das einmalige Chancen.

Das müssen Sie als Arbeitgeber tun:

Schaffen Sie Möglichkeiten!

Individualität und Kundenorientierung

Jede Person, die eine Position in der Unternehmensgruppe der DR. JÄSCHKE-Gruppe inne hat, trägt eine essenzielle Schlüsselfunktion für den Unternehmenserfolg. Egal, ob im Marketing, in der IT oder direkt in der Beratung, jegliche Aktivitäten orientieren sich direkt an und für unseren Kund:innen – immer. Um dies auch in einem einheitlichen Auftreten dem Kundenstamm gegenüber gewährleisten zu können, haben wir Entwicklungspläne erstellt, die sich, je nach Kompetenzprofil der Stelle und Voraussetzungen einzelner Mitarbeiter:innen , unterschiedlich ausgestalten.

Wissen generieren

Neue Denk- und Verhaltensroutinen passieren nicht von heute auf morgen. Eine Entwicklung muss aktiv gestaltet werden und zuerst in den Köpfen, Herzen und Händen der Beteiligten beginnen. Wir vermitteln unseren Mitarbeitenden Zuversicht und Sicherheit und bieten unseren (angehenden) Fachkräften die Möglichkeit eines berufsbegleitenden Studiums und Seminare. Zusätzlich bieten wir Trainings on/along the Job, aber auch Seminare an unserer hauseigenen Akademie an. So können alle Mitarbeitenden, genau die Themen absolvieren, die sie für ihre Weiterentwicklung benötigen.

Wissen fördern

Der Personalentwicklungsplan wird zukünftig bereits im Rahmen des Onboardings den neuen Mitarbeiter:innen als Richtungsweiser an die Hand gegeben. Ein zielführender Onboarding-Prozess zeigt den Mitarbeitenden grundsätzliche Erwartungen an ihre Position, bietet die Möglichkeit zum Selbsttest und hilft ihnen in der Folge, ihre Karriere erfolgreich in unsere Gruppe einzubringen. Anhand einer Checkliste können die Mitarbeiter:innen eigenständig überprüfen, welche Anforderungen bereits erfüllt werden und wo ein akuter Nachholbedarf besteht. Mit diesem Wissen und einem vorhandenen Schulungskatalog, wie auch dem persönlichen Engagement versierter Kolleg:innen können Wissenslücken oder fehlende Expertise hinsichtlich bestimmter Fähigkeiten gezielt angegangen und in den Fokus gerückt werden. Diese bewusste Inangriffnahme ist sowohl effektiv wie auch effizient und stärkt nachhaltig die Position des Individuums.

Wissen verteilen

Neben dem Onboarding wird der Entwicklungsplan aber auch für die vorhandene Belegschaft im Rahmen der Personalentwicklung angewendet, um den Kund:innen gegenüber zukünftig einheitliche Maßstäbe garantieren zu können. Hierfür bekommt jeder Mitarbeitende anhand des Plans die Möglichkeit, den eigenen Bedarf zu ermitteln und einzufordern. Der Aufbau eines Mentoring-Programms, um das Know-how erfahrener Mitarbeiter:innen zu nutzen, gehört ebenfalls zum Personalentwicklungsplan. Beispielsweise besitzen unsere langjährigen Berater:innen ein umfassendes Wissen über unser Unternehmen, unsere Produkte sowie Prozesse und geben diese Informationen weiter. Berufs- und Quereinsteiger:innen profitieren langfristig von Wissen, Fähigkeiten und den Erfahrungen der etablierten Mitarbeitenden. Die Praxis zeigt es: Mit dem Wissenstransfer findet die Vermittlung von erfolgskritischem Wissen in einer wesentlich nachhaltigere Form statt, was nicht nur die Einarbeitung im Rahmen des Onboardings neuer Mitarbeiter schneller und effizienter macht. Auch der Wissensverlust bei einem Positionswechsel wird dadurch minimiert.

Coaching als Entwicklungsmotor

Routinen sind das Ergebnis eines langen Prozesses der ständigen Wiederholung und Übung. Durch ständiges Reflektieren und Evaluieren darüber, was und wie man es besser machen kann, erfährt unsere Belegschaft auch durch Coaching ihre eigene Leistung und Handlungskompetenz nachhaltig zu verbessern und zu stärken. Wir sind der Meinung, dass wir durch gezieltes Coaching schlummernde Potenziale erkennen und entwickeln.

Keine Panik vor Fluktuation

Es kann und wird Ihnen auch passieren, dass Mitarbeitende Ihr Unternehmen verlassen. Die Gründe hierzu sind individuell: Mal ist es ein besseres Gehalt, mal ist es der Wunsch nach Veränderung und mal passt die Chemie einfach nicht. Aus diesem Grund nicht in Ihre Mitarbeiter:innen zu investieren wäre jedoch wie Ihre Blumen im Garten in den heißen Sommermonaten sich selbst zu überlassen. Sie haben nämlich nichts davon!

Eines ist uns jedoch klar: In jedem unserer Köpfe steckt ein Schatz voller Kompetenzen und Wissen, welcher weiter gefördert werden will und wird. Als Pioniere der Digitalisierung nutzen wir diese Potenziale, indem wir sie fordern und fördern und verschaffen uns langfristige Wettbewerbsvorteile, um so die Zukunft der Mitarbeitenden und der DR. JÄSCHKE-Gruppe zu sichern.

DIE DREI SÄULEN DER BERATERTÄTIGKEITEN

Die erste Säule
umfasst das notwendige Fachwissens der Berater:innen, welches vorhanden sein muss, um Fragestellungen der hinsichtlich Informationssicherheit mit Expertise erfolgreich bearbeiten zu können.
Hierzu gehören neben der beruflichen Ausbildung bzw. dem Studium der Mitarbeitenden, ebenso fachliche Weiterbildungen/Schulungen sowie Kenntnisse über notwendige Schlüsselqualifikationen am Arbeitsplatz.

Die zweite Säule
der Beratertätigkeit beschäftigt sich mit den konkreten Fähigkeiten, welche zur Ausübung der Tätigkeit notwendig sind. Die Fähigkeiten sind das Handwerkszeug der Berater:innen. Sie spiegeln die Beratertätigkeit wider und geben Aufschluss über konkrete zum Tagesgeschäft gehörende Aufgaben, die es zu beherrschen gilt. Darüber hinaus ermöglichen die Fähigkeiten einen angemessenen Umgang mit Herausforderungen und Problemsituationen hinsichtlich des Konflikts- und Krisenmanagements und lassen die Berater:innen flexibler auf unvorhergesehene Vorkommnisse reagieren.

Die dritte Säule
rundet den Auftritt der Berater:innen ab. Sie behandelt das den Kund:innen und auch Kolleg:innen gegenüber angemessene Auftreten und Gebären.
Hierbei gilt es sowohl Kommunikations- und Verhaltensgrundsätze zu schaffen, um einen respektvollen Umgang zu gewährleisten, wie auch das Auftreten der Person hinsichtlich Umgangsformen, Kleidungswahl und Ausdruck zu prägen.

Alle drei Säulen formen gemeinsam professionelle Berater:innen, die sich im Tätigkeitsfeld voll integrieren, entfalten und kontinuierlich weiterentwickeln können.

- DIGITAL AVANTGARDE AKADEMIE -

Weiterbildungen und Coachings zur Digitalisierung im Krankenhaus

Text: Nina Khan

Die deutsche Wirtschaft verzeichnet seit vielen Jahren ein erfreuliches Wachstum. Grund hierfür ist vor allem die Binnenwanderung in der Europäischen Union. Ohne diese wäre ein ohnehin bestehendes Problem ein noch viel Größeres: Der Fachkräftemangel in Deutschland. Betroffen ist hiervon vor allem die Branche des Gesundheitswesens.

Bedingt durch den jahrelangen Investitionsstau in Kombination mit vielen neuen regulatorischen Vorgaben, ist der Fachkräftemangel in Krankenhäusern ein eklatantes Problem. Weiterhin nimmt nicht zuletzt der demographische Wandel einen entscheidenden Einfluss auf fehlende Expertise bei Mitarbeiter:innen ein. Ein zu hoher Anteil einer alternden Gesellschaft mit einem folglich zu geringen Anteil junger Fachkräfte führt zu personellen Engpässen.

Darüber hinaus verbreitet sich der Megatrend Digitalisierung zunehmend in deutschen Krankenhäusern. Allerdings nennt jede:r zweite Digitalisierungsverantwortliche nicht besetzte Stellen und einen Mangel an Know-How der Mitarbeiter:innen als zwei der größten Hindernisse, um digitales Wachstum in Krankenhäusern voranzutreiben.

Let's Work Together

Um diesem Zustand entgegenzuwirken und die steigenden Anforderungen an Prozess-, Technik- und Methodikwissen zu erfüllen, bietet die Digital Avantgarde Akademie KHZG geförderte Schulungen von ausgewiesenen Expert:innen auf ihrem Gebiet an, beispielsweise für Mitarbeiter:innen von Krankenhäusern oder Gesundheits-IT-Herstellern.

Die Lehrinhalte unterteilen sich in die Themenblöcke „Krankenhaus", „Interoperabilität", „Methodik" und „Gesetze und Regulatorisches". Um auf fehlende Expertise möglichst zielgerichtet zu reagieren, sind aus den Themenblöcken nochmals Schwerpunkte wählbar, wie beispielsweise „Projektmanagement", „Agile Methoden" oder „Software Engineering" aus der Sparte „Methodik".

DIGITAL AVANTGARDE AKADEMIE

Weitere Informationen und eine Demoversion einer Lehreinheit finden Sie auf der Website der Digital Avantgarde Akademie unter www.digital-avantgarde.de

DAS DIGITAL AVANTGARDE AKADEMIE TEAM

Prof. Dr. Christian Wache

Professor der Medizinischen Informatik und den Schwerpunkten „Klinische Informationssysteme", „Medizintechnik", „Datenbanken" und „Telemedizin und eHealth" an der HTWG Konstanz

Prof. Dr. Bernhard Breil

Medizininformatiker mit Professur für Gesundheitsinformatik mit den Schwerpunkten „Klinische IT-Systeme", „Systemintegration und IT-Projektmanagement" an der Hochschule Niederrhein

Prof. Dr. Renato Dambe

Gesundheitsinformatiker mit Professur in Gesundheitsinformatik mit den Schwerpunkten „Medizinische Dokumentation", „Projektmanagement" und „Betrieb von IT-Systemen im Gesundheitswesen" an der HTWG Konstanz

Prof. Dr. Thomas Jäschke

mit Professur an der FOM Hochschule im Studiengang Wirtschaftsinformatik und IT-Management, Digitalisierungsexperte und Datenschützer/Informationssicherheitsbeauftragter

Dr. Matthias Aleff,
Stv. Leiter Verhaltensstandards
EKu.SAFE

Sicherheitskultur durch Human Factors schaffen

Interview: Nina Kill

Wo bis vor kurzem das deutschlandweit einzigartige Training von Fachkräften für Kernkraftwerke stattgefunden hat, trainieren heute Menschen aus unterschiedlichsten Branchen Notfallsituationen. Wir treffen Dr. Matthias Aleff von EKu.SAFE im Kraftwerkssimulatorenzentrum in Essen.

ExperSite *Die Trainingsumgebung in 1:1 Nachbildung eines Kernkraftwerks ist definitiv etwas Neues. Hier finden auch die Human Factors-Schulungen statt?*

Dr. Matthias Aleff: Es gibt eine gesetzliche Verpflichtung für verantwortliches Personal der Kernkraftwerke, zweimal im Jahr am Simulator jeweils für eine Woche zu trainieren. Also finden die Human Factors-Schulungen auch an den 1:1 Simulatoren statt. Das Übungsspektrum richtet sich dabei von einfachen Aufgaben über Störfälle bis hin zu Notfällen. Mit den Schulungen bereiten wir Mitarbeitende auf Szenarien vor, die sie in der Realanlage bisher nicht gesehen haben und, im besten Fall, auch nicht sehen werden. Gleichzeitig geht es uns darum, die strukturierte Zusammenarbeit in der Gruppe zu fördern.

Bis Anfang 2000 wurde am Simulator fast ausschließlich im technischen Bereich geschult. Inzwischen aber wissen wir, dass Fehler nicht nur aufgrund mangelnder Fachkunde des Personals passieren. Ursachen können ebenso im Führungs-, Team- oder Arbeitsverhalten Einzelner liegen. In den Schulungen spielt daher auch die hierarchieübergreifende Kommunikation eine entscheidende Rolle – wir teilen das hier auf in Fachkunde und in Verhalten, jeweils zu 50 Prozent.

Für die Verhaltensthemen haben wir spezielle Trainingsstrecken entwickelt, an denen interdisziplinär und hierarchieübergreifend gearbeitet wird. Inzwischen schulen wir ganze Kraftwerksstandorte – angefangen beim Handwerker, über die Sekretariate bis hin zur Anlagenleitung.

ExperSite *Für wen und was genau sind die erwähnten speziellen Übungsstrecken?*

Dr. M. A.: Mit dem Training an den einzelnen Modulen der Übungsstrecken wenden wir uns an Mitarbeitende unterschiedlicher Branchen. Dazu gehören neben der Kraftwerksindustrie auch Brauereien sowie Krankenhäuser bzw. das gesamte Gesundheitswesen. Die Funktion der Module ist sehr einfach gehalten, fachliche Expertise ist nicht erforderlich. So können sich die Teilnehmenden ausschließlich auf Verhaltensaspekte konzentrieren.

ExperSite *Warum werden Notfallübungen Ihrer Meinung nach heute noch häufig stiefmütterlich gehandhabt?*

Dr. M. A.: Die Notfallschutzplanung in deutschen Kernkraftwerken wird keineswegs stiefmütterlich behandelt, wir haben uns hier den allerhöchsten Ansprüchen verschrieben. In den Kernkraftwerken wird die Notwendigkeit für Übungen sehr klar gesehen. Bestehende Konzepte werden ständig überprüft und ins Verhältnis zu Ereignissen in Kernkraftwerken im In- und Ausland gestellt: Wie hätte die eigene Anlage in diesem Fall das Ereignis gemeistert, wie gut wäre das Personal vorbereitet gewesen? Anschließend kann die Optimierung erfolgen. Es wäre wünschenswert, wenn sich auch andere Branchen so auf Notfälle vorbereiten würden.

>>>

> Wir reden bei Notfällen über sehr seltene Ereignisse. Dennoch, auf Aussagen wie „Uns wird es nicht treffen, weil wir gut aufgestellt sind" oder „Die vorgesehenen Maßnahmen werden wir nie brauchen" kann sich niemand verlassen.
>
> DR. MATTHIAS ALEFF

ExperSite *Was genau beinhalten die Notfallübungen?*

Dr. M. A.: Bei den Übungen wird der Beweis erbracht, dass die Beherrschung von Notfällen durch eine funktionierende Infrastruktur sowie personelle Schulungen möglich ist. Für die Betreiber von Kernkraftwerken in Deutschland sind Notfallübungen kein notwendiges Übel, sondern ein wichtiger Baustein der Notfallschutzplanung. In der Regel ist das Personal auch während der Übungsphasen hochmotiviert. In der Auswertung werden positive Auffälligkeiten verstärkt sowie Optimierungspunkte offen diskutiert und über ein geregeltes Verfahren in die Organisation eingespeist.

Diese Vorgehensweise kommt inzwischen vermehrt auch in anderen Bereichen, wie beispielsweise in Krankenhäusern oder auch in städtischen Strukturen und Gemeinden, zum Einsatz. Stichwörter sind hier Starkregenereignisse oder die Corona-Pandemie. Gerade die letzten zwei Jahre haben gezeigt, wie wichtig eine vorausschauende Notfallplanung ist.

ExperSite *Denken Sie, dass hier ein Umdenken bzw. eine Veränderung stattfinden muss?*

Dr. M. A.: Wir reden bei Notfällen über sehr seltene Ereignisse. Dennoch, auf Aussagen wie „Uns wird es nicht treffen, weil wir gut aufgestellt sind" oder „Die vorgesehenen Maßnahmen werden wir nie brauchen" kann sich niemand verlassen. Jedes Unternehmen sollte jetzt umdenken, seinen Notfallplan regelmäßig trainieren und offen darüber diskutieren.

Untersuchungen haben ergeben, dass häufig menschliche Faktoren bzw. Fehlentscheidungen die Ursache von Unfällen waren. So wurden Fachleute nicht gehört oder Informationen einfach hingenommen, ohne sie kritisch zu hinterfragen. Unsere Trainings setzen daher schon früh an: Wenn gewisse Standards in der Zusammenarbeit und in der Fehlervermeidung von vorneherein gelebt werden, kann darauf auch in brenzligen Situationen zurückgegriffen werden. Mit den Werkzeugen des professionellen Handelns können Fehler schon im Vorfeld verhindert werden.

ExperSite *Was ist neben der Umgebung besonders an Ihren Trainings?*

Dr. M. A.: Die Trainings sind speziell auf die Kund:innen zugeschnitten. Es geht nicht um ein einmaliges Training, wie das bei vielen anderen Anbietern der Fall ist. Wir setzen auf ein gestaffeltes Gesamtkonzept zur nachhaltigen Verbesserung der Sicherheitskultur im Unternehmen. Mit dem Ergebnis, dass weniger Fehler gemacht werden und die Zufriedenheit der Mitarbeitenden steigt.

ExperSite *Verhaltensstandards – was genau beinhaltet das?*

Dr. M. A.: Eine interdisziplinäre Arbeitsgruppe legt Verhaltensweisen fest, die für das Unternehmen gelten sollen. Basierend auf diesen Verhaltensstandards erstellen wir

ein spezielles Training. Dabei profitieren wir auch sehr von Erfahrungen, die wir mit unseren Kund:innen bisher machen durften. Manchmal stellen wir sogar fest, dass schon Standards existieren, nur bisher nicht schriftlich niedergelegt wurden.

Das erste Training richtet sich immer an die Unternehmensleitung sowie an den Personal- und Betriebsrat. Diese sollen schließlich als gutes Beispiel für die Mitarbeitenden vorangehen; mit der Vorbildfunktion steigt die Akzeptanz für sicherheitsgerichtetes Verhalten im Unternehmen. Neben einem Initialtraining für alle Mitarbeitenden empfehlen wir ein abgestimmtes Führungskräfteprogramm bis hin zum gezielten Coaching.

ExperSite *Wie genau läuft ein solches Training ab?*

Dr. M. A.: Die Trainingseinheiten bauen aufeinander auf, durch Wiederholung werden Verhaltensweisen verinnerlicht. Zur Konzeption gehören abwechselnde Theorie- und Praxiseinheiten, wobei die Praxis überwiegt. Auf maximal acht Teilnehmende kommen zwei Trainer:innen, die kleine Gruppengröße macht eine individuelle Betreuung möglich. Nach der Theorie werden zwei Gruppen für Rollenspiele gebildet: Die Teilnehmenden werden zu „Handwerker:innen", nehmen die Position einer „Führungskraft" ein oder fungieren als „externe Beobachter:in". In der Arbeitsvorbesprechung werden die Handwerker:innen angewiesen, eine Tätigkeit an den Trainingsmodulen auszuführen. Hierbei handelt es sich um einfache Aufgaben wie etwa das Stellen von Ventilen.

Der erste Weg führt die Teilnehmenden zur Werkzeugausgabe, um die benötigten Materialien und Werkzeuge sowie eine Schutzausrüstung auszusuchen. Es werden nur die Dinge ausgegeben, die auch verlangt wurden. Anschließend beginnen die Handwerker:innen ihre Aufgabe auszuführen. An der Trainingsstrecke sehen ihnen die Führungskräfte dabei genau über die Schulter, geben Tipps, üben Kritik und halten Ausschau nach organisatorischen Schwächen sowie nach Aspekten, die im Prozess gut laufen.

Damit wird der theoretische Teil der Schulung in die Praxis umgesetzt: Schwerpunkte liegen auf der hierarchieübergreifenden, sicheren Kommunikation und auf dem Arbeitsverhalten. Es folgt eine der wichtigsten Phasen des Trainings, die Arbeitsnachbesprechung. Die Gruppe gibt sich untereinander wertschätzendes Feedback. Ziel ist es, einen Weg zu finden, wie Fehler zukünftig vermieden werden können, ohne Schuldzuweisungen zu machen.

>>>

Arbeitsnachbesprechung: einer der wichtigsten Parts des Trainings: wertschätzendes Feedback innerhalb der Gruppe.

Bei einem akuten Vorfall helfen die Standards, strukturiert zu handeln und nicht blind in Aktionismus zu verfallen.

DR. MATTHIAS ALEFF

ExperSite *Eignet sich das Training auch für andere Berufsgruppen als Kernkraftwerkspersonal?*

Dr. M. A.: Es geht immer um Fehlervermeidung und Zusammenarbeit. Das Verhaltenstraining eignet sich für alle Berufsgruppen, bei denen Menschen zusammenarbeiten. Zu unseren Kund:innen gehören unter anderem die Deutschen Seenotretter, eine große Brauereikette, Kliniken und weitere Hochrisiko-Organisationen.

ExperSite *Können Sie ein Beispiel für Krankenhäuser geben?*

Dr. M. A.: Konservative Schätzungen, wie es in dem „Weißbuch der Patientensicherheit" von Prof. Dr. Schrappe steht, gehen nach wie vor davon aus, dass bei 5-10 % aller Krankenhausbehandlungen ein unerwünschtes Ereignis auftritt, bei 2-4 % der Krankenhausfälle dieses Ereignis vermeidbar wäre und 0,1 % aller Sterbefälle auf Patientensicherheitsprobleme zurückgeführt werden können. In der Vergangenheit wurden beispielsweise zur Verbesserung der Patientensicherheit häufig isoliert wirkende Maßnahmen, etwa OP-Checklisten oder Systeme zur Vermeidung von Patientenverwechslungen, eingeführt. Doch mit diesen singulären, monokausalen Ansätzen konnte keine signifikante Reduktion der vermeidbaren unerwünschten Ereignisse, nachfolgenden Patientenschäden und vermeidbaren Todesfälle erreicht werden.

Die strukturierte Einführung von Verhaltensstandards und das damit verbundene Training kommt der Forderung von Prof. Dr. Schrappe nach komplexen Mehrfachinterventionen gleich.

ExperSite *Wie sollte sich eine Trainingsgruppe bestenfalls zusammensetzen?*

Dr. M. A.: Um den größten Schulungserfolg zu erzielen, sollten die Trainingsgruppen interdisziplinär und hierarchieübergreifend zusammengesetzt sein. Beispielsweise führen Geschäftsführer:innen, Ärzt:innen, Pflegepersonal und Verwaltungsangestellte:innen gemeinsam ein Training durch. Dieses hat einen nachhaltigen Lernerfolg für beide Seiten, Führungskräfte und Mitarbeitende.

ExperSite *Was haben mein Team und ich gelernt, wenn wir das Training abgeschlossen haben?*

Dr. M. A.: Nach einem Training werden Sie auf jeden Fall anders an die Arbeit herangehen. Ein Kernelement ist die kritisch hinterfragende Grundhaltung, die Sie dann verinnerlicht haben. Das heißt, zuerst zu denken, bevor gehandelt wird. Die richtigen Vorteile stellen sich ein, wenn die kritische Masse Ihrer Abteilung, Ihres Unternehmens die Schulung absolviert hat. Anfangs werden Sie die Verhaltenswerkzeuge wie beispielsweise die 3-Wege-Kommunikation noch nicht intuitiv anwenden. Mit der Zeit werden diese aber in Fleisch und Blut übergehen, weil sie dabei helfen, Fehler zu vermeiden. Vielleicht wenden Sie ja auch schon heute manches an, ohne explizit darauf zu achten. Beispielsweise bei der Pizzabestellung am Telefon, bei der Sie noch einmal nachfragen, ob alles richtig notiert wurde.

|||

Sie möchten die ExperSite regelmäßig kostenlos erhalten?

Dann schicken Sie eine Mail mit Ihren Kontaktdaten und dem Betreff „ExperSite" an Ihre Ansprechpartnerin Nina Kill, nina.kill@dr-jaeschke.ag.

Vielen Dank für Ihr Interesse.

Impressum

ExperSite Ausgabe 01 2022 | **ISSN-Print** 2364-5636 | **ISSN-Internet** 2364-5644 | **Herausgeber:** DR. JÄSCHKE AG, Märkische Straße 212-218, 44141 Dortmund, T +49 231 964193-0 office@dr-jaeschke.ag | www.dr-jaeschke.ag | Sitz der Gesellschaft: Dortmund | **Registergericht:** Amtsgericht Dortmund | **Registernummer:** HRB 27509 | **Umsatzsteuer-Identifikationsnummer:** DE300625711 | **Vorstand:** Prof. Dr. Thomas Jäschke, Angelica Morina, B.A. | **Vorsitzende des Aufsichtsrates:** Dr. Anke Diehl | **Inhaltlich Verantwortlicher gemäß § 1 Abs. 4 TMG, § 55 Abs. 1 RStV und § 55 Abs. 2 RStV:** Prof. Dr. Thomas Jäschke | **Redaktionsleitung:** Nina Kill | **Design und Umsetzung:** Silvia Lorenz | **Druck:** www.onlineprinters.de **Auflage:** 5.000 | **Fotos: AdobeStock:** Seite 4 © cottidie, Seite 6 © Graphic Burger, Seite 8 © SmashingStocks | **istockphoto:** Seite 9 © VioletaStoimenova, Seite 12 © sesame, Seite 27 © Sam Edwards | **shutterstock:** Seite 6 © elenabsl, Seite 10 © fizkes, Seite 14 © Mister Duck, Seiten 16-17 © Freud | **Interview:** Seiten 22-26 Fotograf © Christoph Kniel

Exper*Site* ist das Magazin der DR. JÄSCHKE-Gruppe für
Digitalisierung, Informationssicherheit und Datenschutz

www.dr-jaeschke.ag