COMPLIANCE
konkret

**Das Kundenmagazin**
**von Althammer & Kill**
Ausgabe 1/2024

# Noch Fragen zum Hinweisgeberschutzgesetz?

Wir haben die Antworten.
*Seite 6*

**Künstliche Intelligenz im Alltag**
Vom Hype zu konkretem Nutzen
*Seite 10*

**Aufbau eines Informations-sicherheitsmanagementsystems**
Worum geht es konkret?
*Seite 12*

**Künstliche Intelligenz und Cybercrime**
Neuartige Hacking-Angriffe
*Seite 16*

# Editorial

Liebe Leserin, lieber Leser,

die Verpflichtung zur Einrichtung eines Hinweisgebersystems ist seit Dezember vergangenen Jahres für Organisationen ab 50 Mitarbeitenden Pflicht. Dennoch stellen sich im Zusammenhang mit dem Hinweisgeberschutzgesetz Fragen: von der korrekten Umsetzung bis hin zu Vor- und Nachteilen einzelner Lösungen. Wir haben einen unserer Experten befragt, um Unsicherheiten zu klären.

Dass künstliche Intelligenz längst keine Science-Fiction mehr ist, steht außer Frage. Doch dass sie bereits in vielen Bereichen (womöglich unbemerkt?) Einzug gehalten hat, mag den einen oder anderen überraschen. Vor allem, da der ethische und datenschutzkonforme Einsatz der Technologie nicht abschließend geklärt ist. Denn ChatGPT und Co. können nicht nur zum Kürzen von Texten, dem Schreiben von Abschlussarbeiten oder für Brainstorming genutzt werden, sondern können auch ein wertvolles Werkzeug bei Hacking-Angriffen sein. Wir gehen darauf ein, wie sich Cybercrime verändert und worauf Sie achten müssen.

Nachhaltige Informationssicherheit im Unternehmen ist kein Zufall. Der Aufbau eines Informationssicherheitsmanagementsystems ist ein wichtiger Schritt, um wichtige Daten zu schützen. Wir beschreiben Herangehensweisen und zeigen in unserem Beileger, wie das im konkreten Anwendungsfall aussehen kann.

Schon jetzt ist das Jahr 2024 für viele Unternehmen und Organisationen mit Veränderungen und Herausforderungen verbunden – wir halten Sie auf dem neuesten Stand und unterstützen Sie weiterhin bei Fragen rund um die Digitalisierung.

Wir wünschen Ihnen viel Spaß beim Lesen

**Thomas Althammer & Niels Kill**

# Darüber wird gesprochen

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

### KI soll beherrschbar bleiben

Nicht zuletzt das große Interesse an der Veröffentlichung von ChatGPT hat künstliche Intelligenz (KI) zum Lieblingsthema der Marketingabteilungen vieler Tech-Unternehmen gemacht. Für viele User wurde KI und ihre schon jetzt beeindruckenden Fähigkeiten erstmals erfahrbar. Und klar ist auch, dass wir uns erst am Anfang einer Entwicklung befinden, die unser Leben wahrscheinlich umfassend beeinflussen wird.

### Zertifizierung und Standards im Compliance-Bereich?

Wer sich mit Informationssicherheit oder Qualitätsmanagement beschäftigt, kennt die Normen ISO 27001 und ISO 9001. Aber auch im Bereich Compliance legt die Internationale Organisation für Normung (kurz ISO) Standards fest. Welche gibt es überhaupt? Und für wen ist diese Zertifizierung notwendig und wo kann man sie durchführen?

### Informationssicherheit – ja, aber wie? Der BSI-Grundschutz als Baukastensystem

Wer kennt das nicht – im Unternehmen soll die Informationssicherheit aufgebaut werden und schon steht man vor einem großen Fragezeichen. Welcher Standard ist der richtige? Soll eine Zertifizierung angestrebt werden? Und wie wählt man die richtigen Maßnahmen aus und setzt sie effizient um? Die Antwort kann Ihnen der „BSI-Grundschutz“ des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geben.

### Was ist ein Datenschutzmanagementsystem (DSMS)?

Was beinhaltet ein DSMS? Wann sollte ich den Aufbau eines DSMS in Angriff nehmen, welche Inhalte müssen bedacht werden und was muss ich beim Betrieb beachten?

### Datenklassifizierung – ein Schritt zur Datensicherheit

Datenklassifizierung ist ein wichtiger Prozess, um die Sicherheit sensibler Informationen zu gewährleisten. Durch die Klassifizierung können Unternehmen ihre Daten entsprechend ihrem Schutzbedarf einordnen und angemessene Sicherheitsmaßnahmen ergreifen. Diese Einordnung in die Datensicherheit ermöglicht es, potenzielle Risiken zu identifizieren und präventive Maßnahmen zu treffen.

Mit dem Top Company-Siegel werden jene Unternehmen ausgezeichnet, die auf kununu besonders gut bewertet wurden. Mit einem kununu Score von 4,3 und einer Weiterempfehlungsrate von 100 % freuen wir uns, dass wir auch 2024 zu den Top Companies gehören und nicht nur als Beratungshaus, sondern auch als Arbeitgeber überzeugen.





### Das A&K Rechtsupdate

Welche Urteile und Gesetzesvorgaben gab es im Jahr 2023 und welche Auswirkungen haben diese für Ihre Organisation/Ihr Unternehmen?
In diesem Online-Seminar werden wir in einem Rechtsupdate eine Auswahl relevanter Urteile und Gesetzesvorgaben behandeln und ein Augenmerk auf deren Auswirkungen legen. Wo gibt es Handlungsbedarf und wo gibt es Haftungsrisiken?
Melden Sie sich jetzt für das Seminar am 19. März 2024 an und wir bringen Sie auf den neuesten Stand!

ALTHAMMER & KILL AKADEMIE

**Zahl des Monats**

# 50

Die NIS-2 Richtlinie, die für mehr Informationssicherheit in Organisationen und Unternehmen sorgen soll, ist die Erweiterung ihres Vorgängers NIS-1. Durch die Aktualisierung der Richtlinie sind nun deutlich mehr Unternehmen in der Pflicht, Vorkehrungen zu treffen, da die Schwellenwerte aktualisiert wurden. Unternehmen, die von herausragender Bedeutung für die Aufrechterhaltung der Gesellschaft sind, wie beispielsweise kritische Infrastrukturen (Kritis), fallen unter die NIS-2-Richtlinie, wenn sie einen Jahresumsatz von über 10 Millionen Euro und mehr als 50 Mitarbeitende haben.

# Veranstaltungen

22.–26.04.2024, Hannover
**Hannover Messe 2024**
Wir freuen uns, auf der Hannover Messe mit dabei zu sein. In Halle 16 auf dem Gemeinschaftsstand Niedersachsen „Digitalisierung“ (F11) freuen wir uns auf Ihren Besuch, interessante Gespräche und neue Einblicke. Weitere Informationen: *https://www.hannovermesse.de/de/themen/*

04.–06.09.2024, Paderborn
**Praxistage Datenschutz und Informationssicherheit in Gesundheits- und Sozialwesen, Kirche & Non-Profits**
Wir möchten Sie ganz herzlich zu unseren exklusiven Praxistagen einladen! IT-Recht, KI & NIS-2 in der Praxis wirksam zu gestalten ist eine große Herausforderung. Unsere Praxistage in Paderborn bieten die ideale Möglichkeit zum Diskutieren, Mitwirken und voneinander Lernen. Die Anmeldung ist ab dem 18.03.2024 möglich. Sie möchten das Programm aktiv mitgestalten? Dann äußern Sie jetzt Ihre Themenwünsche:
*https://www.althammer-kill.de/praxistage-datenschutz-informationssicherheit*

### KI in der Sozialwirtschaft

Die Nutzung von KI in der Sozialwirtschaft steht in den Startlöchern, es ist jedoch noch unklar, wie Potenziale und Risiken erkannt werden können. Dies nahmen wir zum Anlass, gemeinsam mit der Arbeitsstelle für Sozialinformatik an der Katholischen Universität Eichstätt-Ingolstadt, die Anwendung von Künstlicher Intelligenz (KI) in der Sozialwirtschaft zu erforschen.
Eingeleitet wird die Studie mit einer explorativen Expertenbefragung, zusätzlich werden auch die Software-Anbieter für die Sozialwirtschaft nach bereits vorhandenen bzw. in Entwicklung befindlichen KI-Anwendungen sowie nach künftigen Potenzialen befragt. Erste Forschungsergebnisse werden im Sommer diesen Jahres erwartet, wir halten Sie selbstverständlich auf dem Laufenden.

# Noch Fragen offen zum Hinweisgeberschutzgesetz?

Auch wenn klar ist, dass das Hinweisgeberschutzgesetz Veränderungen in Organisationen nach sich ziehen muss, wirft es häufig Fragen auf. Wir haben bei Christian Klande, Berater bei Althammer & Kill und Compliance-Experte, nachgefragt.




*Warum sollte eine interne Meldestelle eingerichtet werden?*

**Christian Klande:** Bekannterweise gibt es eine gesetzliche Verpflichtung zur Einrichtung von internen Meldestellen, gefordert vom deutschen Hinweisgeberschutzgesetz (HinSchG). Diese gilt in der Regel für alle Beschäftigungsgebenden mit mindestens 50 Mitarbeitenden. Das HinSchG ist die nationale Umsetzung der EU-Richtlinie 2019/1937, oft auch „Whistleblower-Richtline" genannt. Sie dient, einfach formuliert, dem Schutz Hinweisgebender vor Repressalien des Beschäftigungsgebender und damit der vereinfachten Aufdeckung von Verstößen im beruflichen Umfeld. Eine Nichteinrichtung ist bußgeldbewehrt. Insofern könnte man an dieser Stelle einen Haken machen – Gesetz fordert, Organisation hält Gesetze ein – also kommt es zur Einrichtung.

Es gibt aber noch weitere Gründe dafür. Die Rechtsprechung hat in den letzten Jahren und Jahrzehnten eine Art Pflichtenkatalog für die Organisationsleitung formuliert, allem voran die sog. Legalitätspflicht. Diese besagt grob, dass die Leitung dafür zu sorgen hat, dass gesetzliche Regelungen umgesetzt werden müssen. Tut Sie das nicht im erforderlichen Maß, kann es zu einer persönlichen Haftung der Leitung kommen. Werden bestimmte Maßnahmen umgesetzt, vor allem die Implementierung eines wirksamen Compliance-Management-Systems, kann dies haftungsmindernd wirken. Ein internes Hinweisgebersystem bzw. eine interne Meldestelle ist ein elementarer Bestandteil eines solchen Systems. Es wirkt somit der persönlichen Haftung entgegen.

*Warum sollte die interne Meldestelle sorgsam und glaubwürdig eingerichtet werden?*

**Christian Klande:** Das HinSchG schützt alle Personen, die potenziell Kenntnis von einem Verstoß im beruflichen Umfeld erlangt haben können. Dazu zählen neben Beschäftigten unter anderem auch Bewerbende, ehemalige Mitarbeitende, Praktikanten, Gesellschafterinnen und Gesellschafter, Mitglieder, Lieferantinnen und Lieferanten, Kundinnen und Kunden, Mandantinnen und Mandanten sowie Klientinnen und Klienten. Der Anwendungsbereich ist vom Gesetzgeber bewusst weit gewählt worden. Alle diese natürlichen Personen haben ein Wahlrecht zwischen einer externen und einer internen Meldestelle. Die externen Meldestellen werden von staatlichen Stellen betrieben, z. B. dem Bundesjustizamt als Sammel- und Auffangstelle. Wenn die interne Meldestelle über keine ausreichende Reputation und Glaubwürdigkeit zur vertraulichen und objektiven Nachverfolgung von Hinweisen verfügt, wird ein Melder extern melden oder gar keine Meldung abgeben.
Beides sollte vermieden werden, da zum einen die Kontrolle über das Verfahren verloren geht und erfahrungsgemäß externe Stellen einen erhöhten Aufwand an Ressourcen bedeuten. Zum anderen sind nicht gemeldete Verstöße ein teilweise erheblicher Nachteil für die Arbeit der Organisation. Sie schwächt direkt, aber auch indirekt über demotivierte und ggf. zynisch agierende Mitarbeitende. Jede Organisation sollte dankbar für Hinweise sein, zumal diese in der Regel von motivierten Mitarbeitenden erfolgt, die ein Interesse an der gemeinsamen Zukunft haben. Eine nicht regeleinhaltende Organisation dürfte es auch zukünftig schwerer haben, die passenden Mitarbeitenden zu finden.

*Welche Möglichkeiten der Implementierung gibt es?*

**Christian Klande:** Die Implementierung kann komplett intern gelöst werden. Hierzu bedarf es entsprechend gesetzlich geforderter Meldekanäle und geeigneten Personals. Oftmals wird als Kommunikationskanal eine E-Mail-Adresse angeboten. Eine sichere Kommunikation darüber ist jedoch nur unter bestimmten Voraussetzungen möglich. Zudem haben auch Administrierende Zugriff, die mit der eigentlichen Bearbeitung zunächst nichts zu tun haben. Da jede eingehende Nachricht bearbeitet werden muss, ist der Einsatz von Spamfiltern separat zu prüfen. Dieses Einfallstor könnten sich auch Cyber-Angreifende zu Nutze machen.

Eine andere Möglichkeit wäre es, ein externes Hinweisgeberportal bereitzustellen, auf denen sicher und geschützt jederzeit Hinweise eingehen können und mit dessen Hilfe auch eine anonyme Kommunikation mit den Hinweisgebenden sichergestellt werden kann. Ein entsprechender Auftragsverarbeitungsvertrag wäre zu schließen. Ein Teil der Angebote, so auch das von Althammer & Kill, bietet parallel dazu einen telefonischen Meldekanal an. Gerade für unsichere Meldende ist das vertrauliche, persönliche Gespräch Grundvoraussetzung für eine Meldung.

Die komfortabelste Lösung ist eine „externe" interne Meldestelle, die durch einen geeigneten Dienstleistenden wie Althammer & Kill zur Verfügung gestellt wird. Hier sind verschiedene Faktoren wie geeignete Meldewege, die fachliche Qualifikation, Vertretungsfähigkeit, Unabhängigkeit und das Fehlen von Interessenskonflik-

ten sichergestellt. Datenschutzrechtlich ist keine Datenschutzfolgenabschätzung zu erstellen und die Betroffenenrechte werden sichergestellt.

*Was sind wichtige Vor- und Nachteile der Lösungen?*

**Christian Klande:** In vielen Organisationen gibt es wenig Erfahrungswerte, was den Aufwand der internen Meldestelle betrifft. Daher ist es sinnvoll, zunächst eine Skalierbarkeit sicherzustellen und die Fixkosten gering zu halten. Dieses kann extern über ein aufwandsorientiertes Modell ohne hohe Pauschalen erreicht werden.

Nichtsdestotrotz muss der Meldestellenbeauftragte bzw. die Ombudsperson über umfangreiche Kompetenzen (Fachkunde) verfügen, diese auf einem aktuellen Stand halten und eingehende Meldungen kompetent und fachkundig bearbeiten können. Gleiches gilt auch für die Vertretungsperson. Die Meldestelle muss auch arbeiten können, wenn der Hauptverantwortliche nicht im Dienst ist (Urlaub, Krankheit usw.). Bei einer externen Lösung fallen diese Aufwendungen zur Erlangung und Erhalt nicht an.

*„Wenn die interne Meldestelle über keine ausreichende Reputation und Glaubwürdigkeit verfügt, wird ein Melder extern melden oder gar keine Meldung abgeben."*

Wichtiger jedoch als diese Argumente ist die Unabhängigkeit und Glaubwürdigkeit der jeweiligen Lösung sowie deren Haftungspotential. Eine interne Person kennt man, oftmals werden jedoch Ombudspersonen ausgewählt, die Führungskraft sind oder Personen, die per se der Leitung nahestehen. Die Gefahr von Interessenskonflikten liegt auf der Hand. Bei der externen Lösung ist diese Gefahr deutlich geringer. Die meisten Betriebsräte bzw. Mitarbeitervertretungen begrüßen daher die externe Lösung.

Es muss auch kein eigener Mitarbeitender eine „Bürde" auf sich nehmen. Denn das Haftungsrisiko liegt zum Großteil beim Dienstleister. Verstößt eine (interne) Ombudsperson bewusst oder unbewusst gegen das Vertraulichkeitsgebot, drohen Geldbußen bis zu 50.000 Euro, die nach derzeitigem Stand nicht versicherbar sind und als persönliches Haftungsrisiko drohen. Dem steht gegenüber, dass es keinen besonderen Kündigungsschutz für interne Ombudspersonen gibt. Der Initialaufwand für die interne Lösung dürfte indes umfangreicher sein als der für die externe.

*Für wen sollte die interne Meldestelle geöffnet sein?*

**Christian Klande:** Das Gesetz schützt alle natürlichen Personen umfangreich. Eine interne Meldestelle muss jedoch nur für Beschäftigte eingerichtet werden. Eine Öffnung für andere ist keine Pflicht, wird jedoch empfohlen. Sofern eine „andere" natürliche Person einen Missstand erfährt und melden möchte, aber keine interne Meldestelle zur Verfügung steht, wird sie extern oder gar nicht melden. Beides ist nicht wünschenswert.
Die einfachste Lösung, ein System für alle natürlichen Personen anzubieten, ist es, eine URL mit der entsprechenden Meldestelle auf der Website zur Verfügung zu stellen, z. B. im Footer neben dem Impressum oder der Datenschutzerklärung. Manchmal werden Bedenken geäußert, dass dann ein Ansturm auf die Meldestelle folgt und Dinge gemeldet werden, die eher bei einer Beschwerdestelle richtig aufgehoben sind. Die bisherige Erfahrung auch von Althammer & Kill zeigt jedoch, dass dem nicht so ist. „Verirrt" sich versehentlich jemand bei der internen Meldestelle, bekommt er einen entsprechenden Hinweis, an welche Stelle er sich eigentlich wenden sollte.

*„Warum anonym? Weil dadurch die Hemmschwelle zur Meldung sinkt und auch Personen mit mehr Bedenken melden. Die Statistik spricht – je nach Quelle – von 45–65 % abgegebener anonymer Meldungen."*

*Laut dem Hinweisgeberschutzgesetz muss der Meldekanal nicht anonym sein, oft wird es jedoch empfohlen – warum?*

**Christian Klande:** Das HinSchG empfiehlt die Bearbeitung anonymer Hinweise. Es ist aber tatsächlich kein Muss. Eine anonyme Meldemöglichkeit ist grundsätzlich sehr einfach möglich, z. B. durch einen Briefkasten, der an einer nicht prominenten Stelle aufgehängt ist. Damit ist aber keine Kommunikation mit dem Hinweisgebenden möglich. Das ist daher unglücklich, da selten in der Erstmeldung alle wertvollen Informationen und Hinweise genannt werden, die für die Stichhaltigkeitsprüfung notwendig sind.

Warum anonym? Weil dadurch die Hemmschwelle zur Meldung sinkt und auch Personen mit mehr Bedenken melden. Die Statistik spricht – je nach Quelle – von 45–65 % abgegebener anonymer Meldungen. Diese würden zum Großteil wegfallen, wenn es keine anonyme Meldemöglichkeit gibt. Es gibt Bedenken, dass anonyme Meldungen dazu einladen würden, andere zu Unrecht an den Pranger zu stellen, also zu denunzieren. Diese Befürchtung kann aus Sicht von Althammer & Kill nicht bestätigt werden. Das Zulassen anonymer Hinweise kann man auch als Zeichen des Vertrauens interpretieren. Im Rahmen der gängigen ISO-Normen ist eine anonyme Melde- und Kommunikationsmöglichkeit ein wichtiger und unverzichtbarer Bestandteil eines angemessenen Meldesystems.

Unabhängig davon besteht bereits seit Jahren im Rahmen der Legalitätspflicht für die Leitung die Pflicht, substanzielle Hinweise auf Verstöße – auch wenn sie anonym sind – umgehend und sorgsam zu prüfen. Verstöße sind schnellstens abzustellen, um ein (vermeidbares) Risiko zu verhindern oder zumindest zu reduzieren.

*Was ist noch wichtig für die Implementierung?*

**Christian Klande:** Neben der richtigen Auswahl der Meldekanäle und der Ombudsperson ist Transparenz über das gewählte Verfahren und eine offene und vertrauensvolle Kommunikation an die Mitarbeitenden besonders wichtig. Es empfiehlt sich vorher den Betriebsrat bzw. die Mitarbeitendenvertretung mit ins Boot zu holen, eine entsprechende Richtlinie über die Meldestelle zu besprechen und in Kraft zu setzen und die Führungskräfte vorab zu schulen.

Danach sollte eine Information am besten dauerhaft abrufbar erfolgen, z. B. im Intranet. Je mehr und offener sich eine Leitung zur Einhaltung von Regeln verpflichtet und das aktive Melden begrüßt, desto wirksamer wird der Meldeprozess sein.

**Fragen oder Unklarheiten?**

Sprechen Sie uns gerne an!

**Ihr Vertriebsteam**
vertrieb@althammer-kill.de
Tel. +49 511 330603-0

**Impressum**

**Redaktion/V. i. S. d. P.:**
Marie Plautz, Danny Sellmann,
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

# Künstliche Intelligenz im Alltag – Vom Hype zu konkretem Nutzen

Nach dem Start des KI-Dienstes ChatGPT im November 2022 hat das Angebot innerhalb von nur zwei Monaten mehr als 100 Millionen Menschen erreicht. Die jüngsten Entwicklungen rund um „KI“ verändern unser Berufs- und Privatleben.

*Von Thomas Althammer*

Die Übersetzung ist ein wenig irreführend und tatsächlich trifft „Machine Learning“ die Funktionsweise von KI deutlich besser. KI kann Texte erzeugen, Bilder malen, Musik komponieren und vieles weiteres - in beeindruckender Qualität. KI funktioniert durch Wiedergabe von wahrscheinlichen Verknüpfungen auf Grundlage erlernter Daten. Zum Durchbruch von ChatGPT und anderen Diensten haben die jetzt verfügbare Rechenleistung und die Menge an trainierten Daten geführt.

Der Satz „Die Zukunft Deutschlands“ kann auf verschiedene Weise sinnvoll vollendet werden, z. B. mit „… ist rosig“ oder „… hängt vom Klimawandel ab“. KI wählt die wahrscheinlichste Abfolge an Worten aus. Aufgrund großer Mengen erlernter Texte aus Wikipedia, Webseiten und anderer Quellen kann ein sogenanntes „Sprachmodell“ im Kontext der gestellten Frage sehr eloquent und überzeugend Texte zusammenstellen.

## Signifikante Produktivitätsverbesserung

Die KI-basierten Textgeneratoren verstehen die selbst erzeugten Texte nicht – sie kombinieren nur Wortfolgewahrscheinlichkeiten und erzeugen eine Antwort, die auf uns sehr überzeugend wirkt, aber nicht zwingend richtig sein muss. Wenn die Quellen von schlechter Qualität sind oder die Fragestellung missverständlich ausgedrückt wird, produziert ChatGPT Falschaussagen, ohne rot zu werden. Es braucht weiterhin einen Menschen zur Formulierung der Frage („Prompt“) und zur Interpretation/Weiternutzung der Antwort. Auf viele Berufsgruppen wird KI in den nächsten Jahren einen großen Einfluss haben. Das kann für manche Erleichterungen mit sich bringen, einige Berufe werden jedoch verdrängt. Studien haben gezeigt, dass Menschen dank KI deutlich produktiver arbeiten können.

## Künstlerisch tätig

Auch bei der Erkennung und Erzeugung von Bildern gab es in den vergangenen Monaten große Fortschritte. So können hochaufgelöste Bilder in beeindruckender Qualität mit wenigen Befehlen durch KI-basierte Dienste wie DALL-E oder Midjourney erzeugt werden. Die erforderlichen „Prompts“ werden in natürlicher Sprache formuliert, ergänzt um einige Anweisungen (z. B. “im Stil von van Gogh” oder “als Weitwinkel-Motiv“). KI-erzeugte Kunst ist dabei frei von Urheberrechten. Die Auswirkungen auf Fotografinnen und Fotografen, Künstlerinnen und Küstler sowie andere kreative Berufsgruppen werden erheblich sein. Gleichzeitig





entstehen neue Aufgabenfelder, weil sich Menschen auf das Formulieren von Prompts für die Erzeugung von Bildern spezialisieren.

## Künstliche Intelligenz – schon längst da?

*„Auf viele Berufsgruppen wird KI in den nächsten Jahren einen großen Einfluss haben.“*

Der Einsatz von Algorithmen und Technologien, die wir dem Themenfeld „KI“ zuordnen, ist heute schon weit verbreitet. Im Büroalltag, im Gesundheitswesen oder im Straßenverkehr sind u. a. diese Funktionen bereits im Einsatz:

- Büroalltag: Rechtschreibprüfung und Schreibvorschläge beim Tippen, OCR (Texterkennung) beim Scannen von Unterlagen, automatische Erkennung und Zuordnung von Belegen
- Kommunikation: Spracherkennung und Sprachwiedergabe, z. B. mit smarten Lautsprechern wie Alexa oder mit Übersetzungs-Apps wie z. B. Google Translate; Systeme für sprachgestützte Dokumentation in Industrie und in medizinischen Bereichen
- Kollaboration: Nutzung von KI-Funktionen in ChatBots, Lern- und Wissensplattformen, Funktionen fassen zentrale Aussagen längerer Texte zusammen
- Straßenverkehr: Erkennung von Verkehrszeichen, Routenplanung, KI-gestützte Tourenplanung bis hin zur automatisierten Steuerung von Sammeltaxis bei Buchung und Fahrgastplanung
- Diagnostik: Radiologie mit CT und MRT oder auch Bildbasiertes Hautkrebs-Screening

## IT-Sicherheit und KI

Während Funktionen und Technik rund um Künstliche Intelligenz weiter in unser Leben und den Arbeitsalltag einziehen werden, ist der missbräuchliche Einsatz dieser neuen Technologien nicht ausgeschlossen. Es ist absehbar, dass KI für Cyber-Attacken genutzt wird und dass damit die Erkennung von Bedrohungen deutlich erschwert wird.

Angriffe auf die IT-Sicherheit werden meist aus dem Ausland gesteuert. Die verbesserte Qualität von Übersetzungshilfen steht auch Angreifenden zur Verfügung. Sogenannte „Deep Fakes“ könnten Videos entstehen lassen, in denen beispielsweise einer Geschäftsführerin eine Botschaft in den Mund gelegt wird, die sie so nie gesagt hat. Schon heute ist der Schaden durch den „Enkel-Trick“ oder „CEO Fraud“ immens. In Zukunft wird es schwieriger werden, Originale von Fälschungen zu unterscheiden.

## Ausprobieren erlaubt

Ob wir diese schöne neue KI-Welt mögen oder nicht – sie wird nicht mehr verschwinden und ein elementarer Bestandteil unseres Lebens werden. Umso wichtiger ist es, Kolleginnen und Kollegen aller Altersstufen mitzunehmen und auf diese neue Welt vorzubereiten. Wir brauchen ein kollektives Verständnis dafür, dass KI Grenzen hat und wir die Vorteile von KI zu unserem Wohle nutzen sollten.

## Nutzung verantwortungsvoll gestalten

KI-Systeme werden von Menschen trainiert und genutzt. So ist beim Trainieren von KI-Modellen genauso Umsicht geboten, wie auch bei der Nutzung von KI-gestützten Ergebnissen. Studien haben gezeigt, dass Autos mit Unfallfrüherkennung und Selbstbremsfunktionen auf Menschen mit heller Hautfarbe deutlich besser reagieren als auf Menschen mit dunkler Hautfarbe – weil sie einseitig trainiert wurden.

Algorithmen sorgen aktuell dafür, dass Stellenanzeigen auf Facebook sehr gender-bezogen ausgespielt werden: Jobs für Erzieherinnen und Erzieher bekommen fast ausschließlich Frauen zu Gesicht, während Stellen für Kraftwagenfahrende fast ausschließlich bei männlichen Profilen angezeigt werden, wie die Organisation AlgorithmWatch gezeigt hat. Ethik und Datenschutz spielen bei der Entwicklung und Nutzung von KI eine zentrale Rolle. &

Stichwort
**Regulierung und Künstliche Intelligenz – der AI Act**

Für die Entwicklung und den Einsatz von KI-Diensten soll es eine einheitliche gesetzliche Grundlage in der EU geben. Der sogenannte „AI Act“ befindet sich in der Abstimmung. Eine zu große Offenheit könnte den missbräuchlichen Einsatz von KI fördern und Persönlichkeitsrechte untergraben. Kritikerinnen und Kritiker befürchten zu viel Regulierung, was von Seiten der Wirtschaft abgelehnt wird. Im Laufe des Jahres 2024 sollte konkret bekannt werden, wann und in welcher Form der AI Act kommen wird.

# Aufbau eines Informationssicherheits-managementsystems – kurz: ISMS

Ein Informationssicherheitsmanagementsystem ist doch nur was für Software-Unternehmen und Tech-Giganten – oder?

*Von Rodney Wiedemann und Christian Pinnecke*

Die IT- und Cyber-Sicherheit sind Teilaspekte der Informationssicherheit. Während die IT-Sicherheit sich auf den Schutz von technischen Systemen bezieht, geht es in der Informationssicherheit allgemein um den Schutz von Informationen. Diese können auch in nicht-technischen Systemen vorliegen, zum Beispiel auf Papier. So weit so gut – Informationssicherheit kümmert sich also um diverse Themen, doch was bedeutet nun der Begriff „Managementsystem“? In der Literatur gibt es eine Vielzahl von Erklärungen. Für die Autoren ist ein Managementsystem ein Werkzeug, um die komplexen Herausforderungen im Kontext der Informationssicherheit zu bewältigen. Es hilft dabei, die notwendigen Ziele zu setzen, Handlungen und Maßnahmen aus den Zielen abzuleiten und Aufgaben durch klare Abläufe und Verantwortlichkeiten zuverlässig zu erledigen. Dabei wird ein ISMS immer spezifisch auf das jeweilige Unternehmen/die Organisation angepasst.

## Ziele des ISMS

Das Ziel der genannten ISMS ist der dreifache Schutz der Unternehmensinformationen und somit, die Leistungsfähigkeit eines Unternehmens zu gewährleisten. Bei dem dreifachen Schutz aller Unternehmensinformationen geht es um die Schutzziele

- Vertraulichkeit (confidentiality): Informationen werden vor unbefugter Preisgabe geschützt,
- Verfügbarkeit (availability): die Daten stehen dem befugten User zum geforderten Zeitpunkt zur Verfügung, und
- Integrität (integrity): die Daten sind vollständig und unverändert.

Man spricht dabei auch von der „CIA-Triade“. Die beschriebenen Schutzziele vereint alle ISMS.

## Unterschiede in den konzeptionellen Ansätzen

Die Unterschiede der ISMS liegen vor allem bei den konzeptionellen Herangehensweisen. Beim IT-Grundschutz beispielsweise ist der Ansatz Bottom-UP – von der Technik zu den Geschäftsprozessen. Die DIN EN/ISO IEC 27001 hingegen hat den Top-Down Ansatz – von den Geschäftsprozessen zu der Technik. Die Bottom-Up Methode mit konkreten Handlungsempfehlungen der vorhandenen IT-Systeme ist insofern sehr gut, dass keine Managementaufgaben sowie Risikoanalysen vorangestellt sind.

Zudem unterscheiden sich die ISMS in Anzahl und Auswirkung der jeweiligen Anforderungen. Kleinere und schlankere Informations-Sicherheits-Management-Systeme sind z. B. VdS 10000 oder CISIS12. Umfassende, ISMS sind z. B. die DIN EN/ISO IEC 27001 oder der IT-Grundschutz vom BSI.

## Was sind die Gründe für ein ISMS?

Die Gründe für die Implementierung eines ISMS sind vielfältig. Das Motiv, der Schutz der Informationen, ist zwar immer wichtig, aber nicht immer der entscheidende Treiber der Unternehmen zur Entscheidung für die Implementierung eines ISMS.

Zunächst ist zu beobachten, dass die Anforderungen der Kundinnen und Kunden innerhalb der Lieferketten immer anspruchsvoller werden. Selbstverständlich gehört dazu auch die Sicherheit von Informationen.

Hinzu kommt der nicht zu unterschätzende Wettbewerbsvorteil bspw. bei der Beteiligung an Ausschreibungen und somit ein wichtiger Faktor, um am Markt zu bestehen. Die Autoren werden häufig mit der unmissverständlichen Formulierung konfrontiert, dass man „ohne ein Zertifikat keine Chance am Markt hat“.

## Wie finde ich das „richtige“ ISMS?

Welches ISMS für welches Unternehmen, welche Organisation das richtige ist, ist von diversen Faktoren abhängig. Diese können gesetzliche, rechtliche oder gesellschaftliche Anforderungen, Unternehmens- oder Organisationsgröße, aber auch die spezifischen Geschäftsprozesse sein.

Ein wichtiger Faktor ist aber auch die Branche, in der sich das Unternehmen oder die Organisation befindet. Demnach können Unternehmen oder Organisationen für den Aufbau und die kontinuierliche Weiterentwicklung eines ISMS gesetzlich verpflichtet werden, dies gilt bspw. für Unternehmen kritischer Infrastruktur (Kritis).

*„Das Ziel der genannten ISMS ist der dreifache Schutz der Unternehmensinformationen und somit, die Leistungsfähigkeit eines Unternehmens zu gewährleisten.“*

Neben den national/international gültigen ISMS oder branchenspezifischen Sicherheitsstandards gibt es weitere Branchenstandards, wie z.B. der VDA ISA Katalog. Der VDA ISA Katalog ist ein Branchenstandard aus der Automobilindustrie, der in vielen Ländern der Informationssicherheitsstandard ist.

## Wie ist ein ISMS aufgebaut?

Im Grunde sind die ISMS ähnlich aufgebaut. Den PDCA-Zyklus (**P**lan – **D**o – **C**heck – **A**ct) gibt es in allen ISMS.

In der ersten Phase werden die Tätigkeiten des ISMS geplant – also die Umsetzungsplanung der Anforderungen aus den ISMS. Dabei werden Themen wie z. B. Unternehmenspolitik, Rollen- und Verantwortlichkeiten oder auch technische und nicht technische Maßnahmen definiert. Es werden Richtlinien, Organisationsanweisungen, Arbeitsanweisungen oder Prozessbeschreibungen erstellt, um die Anforderungen aus dem ISMS innerhalb des Unternehmens oder der Organisation konkret umzusetzen. Außerdem werden bestehende Prozesse, Verfahren und Dokumente geprüft, analysiert oder, wenn noch keine vorhanden sind, neu definiert, um die Schutzziele der Informationssicherheit, zur Gewährleistung der Geschäftsprozesse, zu erzielen.

Im zweiten Schritt werden die geplanten Maßnahmen umgesetzt. Der Umsetzungszeitraum kann sich über mehrere Monate erstrecken. Nach der Umsetzung werden im dritten Schritt die Maßnahmen unter anderem auf Anforderungskonformität und Wirksamkeit geprüft. Bei nicht ausreichend wirksamen Maßnahmen wird im vierten Schritt auf erforderliche Änderungen reagiert und der PDCA-Zyklus beginnt von vorne. Dadurch entsteht der kontinuierliche Verbesserungsprozess (KVP), um das Informationssicherheitsmanagementsystem kontinuierlich zu verbessern, zur bestmöglichen Wahrung der Schutzziele in der Informationssicherheit.

## Was sind die Vorteile eines ISMS?

Durch die Implementierung und den Betrieb eines ISMS können Risiken in der Informationssicherheit reduziert werden. Des Weiteren kann das Sicherheitsniveau weiter gesteigert werden und eine verbesserte Außenwirkung erzielt werden. Weitere Vorteile sind:

- Erhöhung der Transparenz der Geschäftsprozesse und IT-Systeme
- Optimierung interner Prozesse
- Geordneter, effektiver IT-Betrieb
- Mittelfristige Kosteneinsparung
- Standardisierter Prozess in Bezug auf die Informationssicherheit
- Messbares Sicherheitsniveau
- Erhöhte Attraktivität für Kunden und Geschäftspartner mit hohen Sicherheitsanforderungen (bei Zertifizierungen)
- Implementierung und Weiterentwicklung eines einheitlichen Sicherheitsverständnis im Unternehmen

Im Zuge der Implementierung eines ISMS werden Prozesse optimiert und/oder zum Teil digitalisiert. Das ISMS kann damit durchaus eine Brücke zu anderen Anforderungen bspw. aus dem Qualitätsmanagement bilden. &

Die Menschen hinter Althammer & Kill:

# Wulf Bolte

*Ja hallo, wer bist du denn?*

**Wulf:** Moin, ich bin Wulf. Ich habe nach meinem Studium der technischen Informatik und dem Diplom in Kommunikationsdesign meine Wahlheimat in Hannover gefunden. Ich habe eine Zeit in der Werbung gearbeitet, um zu sehen, wie dort mit Daten umgegangen wird und mich dann für die gute Seite entschieden: Daten lieber zu schützen als Sie zu verwerten.

*Wieso hast du dich bei Althammer & Kill beworben?*

**Wulf:** Es gibt nicht viele Anbieter, die es schaffen, so trockene Themen wie Datenschutz und Informationssicherheit interessant und verständlich zu kommunizieren. Deswegen bin ich früh auf Althammer & Kill aufmerksam geworden. Da ich mich nur dann mit Herzblut in eine Unternehmung einbringen kann, wenn ich das Gefühl habe, etwas Sinnvolles zu tun, stand Althammer & Kill bei mir ganz oben auf der Liste.

*Wie lange arbeitest du schon bei Althammer & Kill?*

**Wulf:** Ich bin jetzt seit knapp einem Jahr bei Althammer & Kill – abgesehen von einer unfallbedingten Verzögerung gleich zu Beginn.

*Was verstehst du unter Produktmanagement?*

**Wulf:** Das ist an sich ein sehr bewegliches Ziel. Vor Althammer & Kill war für mich Produktmanagement fast gleich Produktentwicklung, das ist hier aufgrund der vielen bereits etablierten Produkte anders.

Produktmanagement bezieht sich für mich auf die Organisation rund um die Dienstleistung – damit Kunden und Beratende ein gemeinsames Ziel vor Augen haben, das erreicht werden muss.

*Was genau sind deine Aufgaben als Produktmanager?*

**Wulf:** Das Produktmanagement gestaltet sich bei Dienstleistungen anders als das von z. B. einer Software.

Bei Althammer & Kill geht es also viel darum, Dinge zu standardisieren und Prozesse zu vereinfachen oder zu harmonisieren.

Gleichzeitig wird nach innovativen Lösungsansätzen gesucht, die dem Kunden helfen, immer neuen Herausforderungen gerecht werden zu können.

*Wie sieht dein Alltag aus (was machst du so den ganzen Tag)?*

**Wulf:** Hauptsächlich werden Anforderungen von Althammer & Kill Mitarbeitenden und von Kundinnen und Kunden aufgenommen, um zu evaluieren, was davon in die jeweilige Produkt Roadmap passt und somit allen einen Mehrwert bietet.

Darüber hinaus werden mögliche Themenfelder bearbeitet, die die Kunden noch gar nicht auf dem Schirm haben– hier arbeiten wir kollaborativ an den Produkten und Dienstleistungen von morgen.

*Was gefällt dir an der Arbeit hier?*

**Wulf:** Ich mag den kundenzentrierten Ansatz bei dem kontinuierlich nach Lösungen gesucht wird, die in dem Bermuda-Dreieck aus Datenschutz, Informationssicherheit und Compliance eine produktive Arbeit zu ermöglichen.

Daraus ergibt sich ein Arbeitsumfeld, das sich sehr sinnvoll anfühlt – also einen echten Mehrwert für unsere Kundinnen und Kunden oder die Gesellschaft im Allgemeinen zur Folge hat.

*Wann, würdest du sagen, war deine Arbeit erfolgreich?*

**Wulf:** Wenn ein Kunde durch unsere Arbeit die mannigfaltigen Anforderungen aus Datenschutz und Co. nicht mehr als Hemmschuh oder Einschränkung erfährt, sondern Vorteile daraus ziehen kann. „It's not a bug – it's a feature".

*Welchem Produkt misst du besondere Bedeutung für das Jahr 2024 bei?*

**Wulf:** Momentan geht es z. B. viel darum, dass neue Richtlinien wie die NIS-2 beim Kunden begleitet werden können, ohne neue Bereiche wie KI-gestütztes Arbeiten aus dem Fokus zu verlieren. Das alles geschieht im Dialog mit den Kunden – das ist ja eines unserer Alleistellungsmerkmale, dass wir MIT den Kunden arbeiten – und nicht gegen… &





# Althammer & Kill Akademie

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

*26. April 2024 – Online-Seminar*

**Hinweisgeberschutz – Meldestellenkoordinator/in Modul 1**

Die Umsetzung der EU-Whistleblower-Richtlinie in deutsches Recht ist in Form des Gesetzes für einen besseren Schutz hinweisgebender Personen (Hinweisgeberschutzgesetz – HinSchG) erfolgt.
Unsere modulare Ausbildung liefert mit Modul 1 eine Grundlagenausbildung für alle Ansprechpartner von internen Meldestellen sowie interessierten weiteren Personen wie Führungskräfte oder Mitarbeitervertreter.

*27. April 2024 – Online-Seminar*

**Hinweisgeberschutz– Meldestellenbeauftragte/r oder Ombudsperson Modul 2**

Ein Hinweisgebersystem wird intern betrieben? Mit unserem Seminar erhalten Sie die notwendige Fachkunde. Durch die erfolgreiche Teilnahme an Modul 1 und Modul 2 wird ein Nachweis über die Fachkunde dokumentiert erbracht.
Die Anmeldung zu Modul 2 setzt die vorherige Teilnahme zu Modul 1 voraus.

*20. März 2024 – kostenloses Webinar*

**Datenschutz-Folgenabschätzung – eine Einführung in die „hohe Kunst" des Datenschutzes**

Die Datenschutz-Folgenabschätzung (kurz: DSFA) ist eines der wichtigsten Elemente der Datenschutz-Grundverordnung. Sie soll den Schutz von personenbezogenen Daten betroffener Personen sicherstellen. Was unter Datenschützenden oft als „Hohe Kunst" des Datenschutzes bezeichnet wird, ist weit weniger kompliziert als es scheint. Wir geben Ihnen einen Einblick in die praktische Umsetzung der Datenschutz-Folgenabschätzung und zeigen, dass das Verfahren gradliniger ist, als man denkt.

*3. April 2024 – kostenloses Webinar*

**Souverän reagieren auf IT-Notfälle und Datenschutzpannen**

IT-Sicherheit ist zentral für eine erfolgreiche Digitalisierung. Die Pandemie hat gezeigt, wie wichtig die Digitalisierung der Unternehmen ist. Gleichzeitig sehen wir täglich, wie leicht schwach gesicherte Systeme Kollateralschäden erleiden können.
Umso mehr drängen sich folgende Fragen auf: Wie sicher ist sicher genug? Was ist der richtige Ansatz? Was sind etablierte Lösungen und Standards? Wir erklären den professionellen Umgang mit Notfällen im IT- und Datenschutzbereich.

*03.–04. Juni 2024 – 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.

**Ihr Ansprechpartnerin:**

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

# Künstliche Intelligenz und Cybercrime

Künstliche Intelligenz (KI) hat sich in den letzten Jahren zu einer der am meist diskutierten neuen Technologien entwickelt. Sie hat das Potential, sich auf alle Bereiche unseres Lebens auszuwirken, von der Verbesserung medizinischer Diagnoseverfahren bis hin zur Automatisierung komplexer industrieller Prozesse. Damit verbunden sind jedoch auch Potenziale für neuartige Hacking-Angriffe.

*Von Maximilian Klose und David Armbrust*

In den letzten Jahren hat KI den Weg in die Masse abseits von Forschung und Computer-Nerds geschafft. Heute haben die meisten schon einmal mit einer Text-KI kommuniziert oder ein Bild von einer Text-zu-Image-KI generieren lassen. Viele Unternehmen versuchen gerade Möglichkeiten auszuloten, um künstliche Intelligenz in Prozesse einzubinden und gleichzeitig Datenschutz und Informationssicherheit zu wahren. Allerdings ist es gerade der enorme Fortschritt, den KI in den letzten Jahren gemacht hat, der zunehmend von Cyberkriminellen ausgenutzt wird.

Die Fähigkeit von KI, große Datenmengen zu analysieren und Muster zu erkennen, ermöglicht es Hackerinnen und Hackern, effektivere Angriffe durchzuführen. Daher ist unumgänglich anzuerkennen, dass Cyberkriminelle die gleichen technologischen Fortschritte nutzen wie wir alle – aber auf eine illegale Art und Weise. Es gibt unterschiedlichste Formen von Spezialisierungen und Geschäftsmodellen.

## Phishing

Um ein Unternehmen erfolgreich angreifen zu können ist der einfachste Weg häufig der über die Mitarbeitenden. Social-Engineering ist hierfür das Stichwort, was in diesem Kontext so viel bedeutet, wie einen Menschen durch gezieltes Fragen oder das Vorspielen falscher Tatsachen dazu zu bringen, Informationen preiszugeben oder Dinge zu tun, die einem Hacker oder einer Hackerin nutzen können. Diese Art des Schauspiels kann auf den unterschiedlichsten Ebenen stattfinden. Persönliche Gespräche, Postkarten, die einen dazu bringen sollen, einen QR-Code zu scannen oder auch E-Mails oder Nachrichten in sozialen Netzwerken wie LinkedIn.

Doch wie kann hier eine KI den Kriminellen die Arbeit erleichtern? Der wohl offensichtlichste Vorteil für Kriminelle ist die Fähigkeit, fehlerfrei in fast allen Sprachen zu kommunizieren. Übersetzungssoftware gibt es schon





lange, künstliche Intelligenz passt die Übersetzung jedoch ebenfalls grammatikalisch an und kann unterschiedliche Formulierungen liefern, je nachdem in welchem Kontext ein Text verfasst ist.

Neben dem fehlerfreien Verfassen von Phishing-Mails sind die aktuellen Sprachmodelle in der Lage, HTML-Code zu schreiben. Somit lassen sich nicht nur plausible Texte verfassen, die E-Mails können auch einfach in das beliebige Design eines Unternehmens übertragen werden.

Bei wirklich ausgefeilten Angriffen werden KI-Chatbots sogar für die Kommunikation eingesetzt, um bei der angegriffenen Person das Gefühl zu erzeugen, mit einem Menschen zu kommunizieren.

## Malware

Für die Entwicklung von Malware bedarf es eines sehr hohen technischen Wissenstandes. Sprachmodelle sind jedoch in der Lage, bei der Programmierung von Software zu unterstützen oder diese in Teilen selbst zu schreiben. Hier beschleunigt sich also das ewige Rennen zwischen Anti-Viren-Software und den Entwicklern von Malware um ein Vielfaches.

## Botnetz-Attacken

Auch Botnetz-Attacken können durch KI-Unterstützung leichter vonstattengehen. Hierbei werden eine Vielzahl von Computern infiziert, um sie in ein Botnetz zu verwandeln, welches dann von Cyberkriminellen zur Durchführung von Angriffen genutzt werden kann. KI wird dann dazu verwendet, diese Botnetze zu optimieren und gezielte Angriffe auf spezifische Ziele durchzuführen.

Darüber hinaus werden KIs dazu verwendet, Schwachstellen in Systemen zu finden und zu nutzen. Cyberkriminelle entwickeln hierfür Algorithmen, die automatisiert Schwachstellen in Systemen erkennen und ausnutzen. Dies kann zu erheblichen Schäden führen, wenn sensible Daten gestohlen oder Systeme lahmgelegt werden.

## Wie oft kommen Cyber-Attacken vor?

Laut Bundeslagebild Cybercrime für das Jahr 2021 haben sich allein die bekannt gewordenen Phishing-Attacken seit Dezember 2018 versechsfacht – Tendenz steigend.

Es darf davon ausgegangen werden, dass durch den Einsatz von KI-unterstützten Systemen diese und andere Attacken in einem absehbaren Zeitraum exponentiell ansteigen, da die Erstellung von Angriffen deutlich weniger Zeit und Arbeit in Anspruch nehmen dürften. Durch den Einsatz von KI kann sich auch die Branche relativ leicht weiter ausbauen, ohne weitreichende Fachkenntnis im Bereich des Hacking haben zu müssen, da viel Programmierarbeit durch künstliche Intelligenzen übernommen wird.

## Wie können Sie sich und Ihr Unternehmen schützen?

Um sich gegen Angriffe durch KI zu schützen, sollten Unternehmen proaktive Maßnahmen ergreifen. Dazu gehören

- die Implementierung von Anti-Malware- und Firewall-Lösungen,
- die regelmäßige Überprüfung auf Schwachstellen und Sicherheitslücken,
- das Patchen und Updaten von Systemen sowie
- die Schulung von Mitarbeitenden in Bezug auf das Sicherheitsbewusstsein und dem Einsatz von neueren Technologien.

Darüber hinaus können Unternehmen auch KI-Technologien selbst nutzen, um ihre Systeme und Daten zu schützen. Die Verwendung von KI-basierten Systemen zur Überwachung und Analyse von Netzwerkaktivitäten, um Angriffe frühzeitig zu erkennen und abzuwehren, ist bereits heute eine weit verbreitete und zuverlässige Maßnahme.

Neben den genannten Empfehlungen hilft zudem, das Wissen der Mitarbeitenden zu fördern. Mitarbeitende müssen sich der Möglichkeit bewusst sein, dass ihnen eine KI gegenübersitzen könnte. Zusätzlich ist es wichtig Prozesse für den Ernstfall zu kennen, sollte ein Versuch, an Daten zu gelangen, doch erfolgreich gewesen sein. Hier ist es von zentraler Bedeutung, dass Notfallpläne existieren, die den Mitarbeitenden bekannt sind, um im Zweifelsfall wenigstens einen Notbetrieb aufrecht erhalten zu können.

Stichwort
**Polymorphe Viren**

Ein Beispiel für die Nutzung von KI bei der Verbreitung von Malware sind sogenannte „Polymorphe Viren". Diese Art von Schadsoftware kann sich selbständig verändern und anpassen, um Erkennung durch Antivirenprogramme zu erschweren.

# Für alle Probleme eine Lösung gefunden

Angefangen als Mitglied des Organisations-Teams hat Nina sich inzwischen zur Projektmanagerin weiterentwickelt. Unter anderem die Umstellung auf ein neues CRM-System hat sie begleitet, wie das ablief, haben wir sie im Interview gefragt.

*Was machst du bei Althammer & Kill?*

**Nina:** Angefangen habe ich 2019 bei Althammer & Kill im Auftragsmanagement und dem Vertriebsinnendienst. Nach drei Jahren habe ich nach einer neuen Herausforderung gesucht, wollte aber gerne bei Althammer & Kill bleiben. Da wir zu der Zeit sowieso über eine interne Projektkoordination nachgedacht haben, passte der Zeitpunkt sehr gut und ich bin mittlerweile als Projektmanagerin für unsere internen Projekte tätig.

*Du bist als Projektmanagerin tätig und hast vor kurzem ein neues CRM-System eingeführt. Was war hier das Ziel?*

**Nina:** Unser damaliges CRM und ERP System war eine maßgeschneiderte und eigens entwickelte





*„Selbstverständlich läuft so ein Projekt niemals reibungslos und ohne jegliche Probleme. So hatten wir mit der Migration, Bugs und allem, was dazu gehört, immer wieder zu kämpfen."*

Lösung, konnte allerdings nicht alles abdecken, sodass wir in zwei Systemen arbeiten mussten. Es wurde entschieden, auf ein professionell angebotenes System umzusteigen, in dem Abrechnung, Auftragsmanagement und der Vertrieb gemeinsam arbeiten können. Nach langer Suche fanden wir „Vertec", eine Software, die unseren Wünschen am nächsten kam.

*Wie bist du an das Projekt herangegangen?*

**Nina:** In die Auswahl der Software war ich zum damaligen Zeitpunkt noch nicht involviert, ich bin also erst im Zuge des Vorprojekts mit eingestiegen. In diesem Vorprojekt haben wir mit unserem heutigen Vertec-Berater geschaut, wie unsere bisherige Software aufgebaut war und was wir für grobe Anforderungen haben. Da sich nach Einschätzung beider Seiten die meisten unserer Wünsche und Ideen von Vertec umsetzen lassen sollten, entschieden wir uns für die Einführung.

Zum Jahreswechsel (2022 auf 2023) sollte als erstes die Abrechnung inklusive des Auftragsmanagements laufen, später dann der Vertrieb umziehen. Wir haben das Projekt im agilen Stil mit einem kleinen Projektteam aufgesetzt. In wöchentlichen Sprints haben wir mit unserem Entwickler, Marian, und unserem Vertec-Berater die Anforderungen umgesetzt. Selbstverständlich läuft so ein Projekt niemals reibungslos und ohne jegliche Probleme. So hatten wir mit der Migration, Bugs und allem, was dazu gehört immer wieder zu kämpfen.

Glücklicherweise hat Marian Nerven aus Stahl, sodass wir für (fast) alle Probleme eine Lösung finden konnten – oder wir mussten uns eben etwas anderes einfallen lassen.

*Wurde das Ziel erreicht? Ist das Projekt abgeschlossen?*

**Nina:** Sowohl die Abrechnung als auch das Auftragsmanagement und der Vertrieb arbeiten heute ausschließlich mit Vertec. Insbesondere unsere Abrechnung kann nun deutlich schneller durchgeführt werden. Da wir aufgrund eines Vertriebsleiter-Wechsels einen neuen Kollegen bekommen sollten, haben wir im Bereich des Vertriebs letzte Anpassungen und Anforderungen in Bearbeitung. Sobald diese abgeschlossen sind, ist die Einführung von Vertec beendet.

*„Nach wie vor gibt es genug zu lernen und zu verbessern, aber wir sind ein tolles Team, unterstützen und hinterfragen uns gegenseitig"*

*Was hast du aus diesem Projekt mitgenommen?*

**Nina:** Die Einführung von Vertec war mein erstes „richtiges" Projekt und dafür nicht gerade klein. Ich organisiere und strukturiere wahnsinnig gerne, weshalb mir das Projektmanagement auch eine Menge Spaß macht. Allerdings musste ich zunächst alles lernen und schauen, wie wir bei Althammer & Kill Projekte eigentlich durchführen wollen. Was ist für uns eine gute Arbeitsweise? Welche Mittel können wir bereitstellen? Wie arbeitet man eigentlich in so einem agilen Projekt? Eine Menge Fragen, die es herauszufinden galt und nach wie vor noch gibt.

Besonders unterstützt hat mich meine Kollegin Daniela, die durch die LearnBase GmbH viel Projekterfahrung mitgebracht hat und mir immer mit Rat und Tat zur Seite stand. Nach wie vor gibt es genug zu lernen und zu verbessern, aber wir sind ein tolles Team, unterstützen und hinterfragen uns gegenseitig – ziehen auch mal eine Notbremse, wenn wir in eine Sackgasse laufen und feststellen-, hm, das war doch keine so gute Idee.

*Welche Projekte stehen als nächstes an? Worauf freust du dich im Jahr 2024?*

**Nina:** Zurzeit sind wir mit der Einführung eines Ticketsystems beschäftigt, damit die Beratung und übergreifende Bereiche ein gutes Tool für Ihre Arbeitsweise untereinander und mit den Kunden bereitgestellt bekommen. Als kleines Highlight steht im Februar unsere 10-jährige Jubiläums-Feier an, bei der wir schon in den letzten Zügen für die Planung sind. &

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