COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 2/2022

IT-Sicherheit in Krankenhäusern wird verpflichtend

Was ist jetzt zu tun?
Seite 6

Privacy Shield 2.0
Licht am Ende des Schrems II-Tunnels?
Seite 10

Risikomanagement in der Cloud
Ein kritischer Blick auf das hochgelobte „Allheilmittel“
Seite 12

Der Compliance-Beauftragte
Rechtstreue und Legalitätspflicht
Seite 14

Editorial

Liebe Leserin, lieber Leser,

von Mai bis Juli 2022 sind wir auf einer Roadshow mit der Firma Microsoft unterwegs. Mit der Keynote „Gordischer Knoten – gelöst?“ gehen wir der Frage nach, wie Microsoft 365 im Einklang mit dem Datenschutz gebracht werden kann.

Sehr viele Organisationen stehen vor einem großen Dilemma: Auf der einen Seite wollen sie datenschutzkonform und im Rahmen der gesetzlichen Vorgaben handeln. Stand Mai 2022 haben ausnahmslos alle Aufsichtsbehörden in Deutschland eine ablehnende Haltung zu Microsoft 365.

Auf der anderen Seite gibt es kaum nennenswerte Alternativen: In Unternehmen führt (fast) kein Weg an Microsoft 365 vorbei. Das mag man verwerflich finden und kritisieren. Microsoft hat aus der „alten“ Office-Suite eine, selbst während Pandemiezeiten, gut funktionierende Plattform gemacht, die von überall genutzt werden kann.

Letztendlich haben wir die Schuld an diesem Quasi-Monopol auch bei uns in Europa zu suchen: In den vergangenen 25 Jahren haben wir es nicht geschafft, eine relevante Rolle in Sachen IT und Digitalisierung zu spielen (wenn man einmal von SAP absieht). Technologie wird in den USA und in Asien gemacht – wir Europäer spielen keine Rolle.

„Wenn wir die Menschen beim Thema Datenschutz nicht verlieren wollen, müssen wir Wege finden, moderne Werkezuge datenschutzkonform einzusetzen.“

Es ist richtig und wichtig, dass Aufsichtsbehörden die DSGVO und europäische Werte verteidigen. Das ist ihre Aufgabe. Internationale IT-Konzerne haben noch lange nicht alle erforderlichen Anstrengungen unternommen, um hiesige Bestimmungen zu erfüllen.

Zugleich dürfen wir die Sorgen und Nöte der Organisationen und Menschen nicht aus dem Blick verlieren. Wenn wir die Menschen beim Thema Datenschutz nicht verlieren wollen, müssen wir Wege finden, moderne Werkezuge datenschutzkonform einzusetzen.

Wir freuen uns auf den weiter konstruktiv-kritischen Dialog mit Ihnen!

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*

Hier klicken oder scannen!

Volles Haus beim ersten Stopp der Microsoft NGO-Tour in Köln

Erleben auch Sie in Ihrer Nähe unsere Keynote „Gordischer Knoten … gelöst? Microsoft 365 im Kontext Datenschutz“ sowie weitere spannende Praxisvorträge zu den Top-Digitalisierungsthemen im Sozialwesen. An einigen Stopps zeigen wir zudem live, wie Security Awareness-Konzepte im Microsoft 365-Umfeld umgesetzt werden können. Melden Sie sich jetzt kostenlos für Stopps in Ihrer Nähe an!

We are „principle agree“ to force a Schrems III

Am 25.03.2022 verkündeten Ursula von der Leyen (EU-Kommissionspräsidentin) und Joe Biden (US-Präsident) eine „grundsätzliche Einigung“ über ein neues Regelwerk, das einen datenschutzkonformen Transfer zwischen den USA und der EU ermöglichen soll. Kritik ließ nicht lange auf sich warten – vor allem von Maximilian Schrems, dem Juristen, Datenschutzaktivisten und Namensgeber der „Schrems-Urteile“.

8 Maßnahmen, um Cloud-Anwendungen sicher in Ihr Unternehmen einzuführen

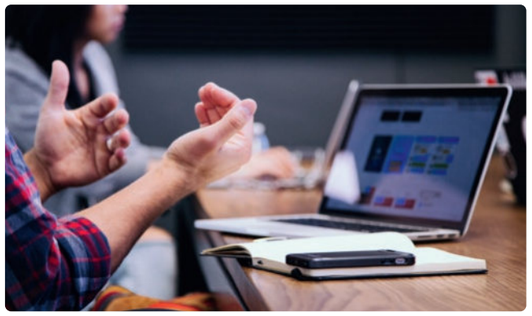
In den letzten Jahren lässt sich ein eindeutiger Trend erkennen: Unternehmen ziehen von selbst betriebenen Servern und lokal gespeicherten Anwendungen zu Cloud-Diensten von großen Tech-Unternehmen. Auch wenn sich die Anwendungen in der Cloud befinden, müssen diese administriert werden. Die Verantwortlichen von Unternehmen unterschätzen häufig, wie aufwendig die Administration von Cloud-Diensten ist und stellen bzw. planen nicht genügend Ressourcen hierfür ein.

Die Multifaktor-Authentifizierung – eine Wunderwaffe gegen Phishing?

Die Corona-Krise hat den Wandel hin zum Cloud-gestützten, dezentralen Arbeitsplatz im Home-Office enorm beschleunigt. Viele Unternehmen sahen sich kurzfristig gezwungen, auf neue Software-as-a-Service-Lösungen umzustellen, um den Betrieb aufrecht zu erhalten.

Bring Your Own Device – ein Risiko für Ihre Compliance?

Immer mehr Unternehmen erlauben ihren Mitarbeitenden die berufliche Nutzung privater Geräte wie Smartphones, Tablets, Laptops oder auch Desktop-PCs. Derartige Bring-Your-Own-Device-Regelungen (BYOD) liegen im Trend und bringen Vorzüge für Arbeitnehmende und Arbeitgebende, aber leider auch datenschutzrechtliche Risiken mit sich.



Theorie und Praxis: Althammer & Kill kooperiert mit Hochschule Hannover

Das interdisziplinäre Referententeam, bestehend aus Lehrenden der Hochschule und Beratenden von Althammer & Kill, vermittelt über ein Semester Wissen in Datenschutz und Change-Management. Teilnehmende können nach erfolgreichem Abschluss, mit dem Hochschulzertifikat im Gepäck, die Stelle eines Datenschutzbeauftragten souverän antreten.

Im Zertifikatskurs, der im Rahmen der Kooperation der Hochschule Hannover und Althammer & Kill Mitte diesen Jahres stattfindet, geben wir Antworten auf verschiedenste datenschutzrechtliche Fragen. Alle Infos zum Kurs, der am 1. September 2022 startet, finden Sie online, wenn Sie dem QR-Code folgen.

Maximale Langeweile

Unser Podcast. Jeden zweiten Donnerstag eine neue Folge auf Spotify, bei Apple Podcast und weiteren gängigen Podcast-Diensten

Zahl des Monats

123456

Kaum zu glauben, doch im Jahr 2021 war „123456“ das am häufigsten gewählte Passwort. Naheliegende Passwörter wie dieses machen es Hackern nur umso leichter, an personenbezogene Daten zu gelangen.

Messen

Lassen Sie uns ins Gespräch kommen auf einer der nächsten Messen oder im Rahmen der Microsoft NGO-Tour:

2.–4. November 2022, München
BeB Fachtagung
https://beb-ev.de/veranstaltung/fachtagung-dienstleistungsmanagement-2022/

15.–17. November 2022, Bielefeld
KommDigitale
https://kommdigitale.de/

7.–8. Dezember 2022, Nürnberg
ConSozial
https://www.consozial.de/

9. Juni 2022, Wiesbaden; Gastgeber: DRK LV Hessen
14. Juni 2022, Berlin; Gastgeber: Stephanus Stiftung
21. Juni 2022, Düsseldorf; Gastgeber: Ev. Christophoruswerk
23. Juni 2022, München; Gastgeber: Ev. Kirche von Bayern
30. Juni 2022, Dortmund; Gastgeber: Ev. Kirche von Westfalen
Microsoft NGO-Tour – mehr Termine online:
https://www.althammer-kill.de/microsoft-roadshow-2022

LearnBase Release: Version 2.7

Wir freuen uns, unser neues LearnBase-Release (Version 2.7) vorzustellen. Das Update ist in der LearnBase-Umgebung verfügbar. Die Neuerungen umfassen unter anderem die Möglichkeit des Imports von Verzeichnissen im .csv-Format sowie die Möglichkeit, Verzeichnisse Organisationen direkt zuzuordnen.

Darüber hinaus ist der Fertigstellungsmodus für einen ganzen Kurs auf einmal einstellbar, Kurse können abgesehen davon von nun an gruppiert werden. Auch die Verlängerung von Kursteilnahmezeiträumen für einzelne Teilnehmende ist inzwischen möglich. Außerdem wurden Layoutanpassungen und Bugfixes vorgenommen sowie die Bedienfreundlichkeit verbessert. Bei Fragen können Sie sich gerne an unser Team wenden unter:
support@learnbase.de

IT-Sicherheit in Krankenhäusern wird verpflichtend – was ist zu tun?

Mit dem Pflegedaten-Schutz-Gesetz wurde auch ein neuer Paragraf im fünften Sozialgesetzbuch geschaffen. Dieser hat erhebliche Auswirkungen auf alle Nicht-KRITIS Krankenhäuser.

Mit dem neu geschaffenen § 75c SGB V werden alle Krankenhäuser verpflichtet angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

Die informationstechnischen Systeme sind spätestens alle zwei Jahre an den aktuellen Stand der Technik anzupassen. In Absatz 2 verweist der Paragraf auf den branchenspezifischen Sicherheitsstandard (B3S) für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus (B3S Krankenhaus). Mit der Umsetzung des B3S Krankenhaus können Krankenhäuser die Verpflichtung erfüllen.

Mit den folgenden Schritten gelingt die praktische Umsetzung des B3S Krankenhaus.

1. Rahmenbedingungen schaffen

- Der Aufbau eines Managementsystems muss durch die Organisationsleitung unterstützt werden. Dies verhält sich beim B3S Krankenhaus nicht anders. Ohne die Unterstützung der Organisationsleitung ist die Implementierung des B3S im Krankenhaus nicht möglich.
- Alle Mitarbeitende sind angemessen zu informieren, um ein einheitliches Verständnis für Sicherheitsmaßnahmen und Regeln zu schaffen.
- Viele Sicherheitsmaßnahmen sind bereits in den Fachabteilungen integriert. Vorhandene Maßnahmen sind daher bei Einbringung neuer Maßnahmen zu berücksichtigen.

Stichwort
B3S Krankenhaus

Die Einführung eines Informationssicherheits-Managementsystems (ISMS) bildet die Grundlage des B3S Krankenhaus. Dabei orientiert sich der Sicherheitsstandard an internationalen Normen der ISO 27001, der ISO 27799 und selbstverständlich an den Vorgaben des BSI. Die bekannten Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität werden um die Schutzziele Patientensicherheit und Behandlungseffektivität ergänzt.

2. Stellung des Informationssicherheitsbeauftragten

Informationssicherheitsbeauftragte (ISB) unterstützen die Organisationsleitung in Bezug auf die IT-Sicherheit im Krankenhaus. Er ist Dreh- und Angelpunkt und fungiert als Verbindungsstelle zwischen Geschäftsführung und der medizinischen Abteilungen (z. B. IT, Medizin- und Haustechnik und Datenschutz). Der ISB ist verantwortlich für die IT-Sicherheitsstruktur und entwickelt mit den Abteilungen Sicherheitsmaßnahmen, um die gesteckten Sicherheitsziele zu erreichen. Für den Auf- und Ausbau eines B3S Krankenhauses ist der ISB qua Funktion der erste Ansprechpartner. Ist noch kein ISB im Krankenhaus implementiert, empfehlen wir die Stellung eines/einer ISB.

3. Projektvorbereitung

Beim B3S Krankenhaus müssen u. a. folgende Bereiche berücksichtigt werden: Informationstechnik, Medizintechnik, Kommunikationstechnik, Versorgungstechnik und Datenschutz. Es gilt also ein Team zu bilden, welches sich mit den Bereichen und Prozessen auskennt. Entsprechend muss eine geeignete Kommunikationsstruktur etabliert werden.
Ein zentrales Dokument, das frühzeitig vorbereitet werden muss, ist die Erklärung der Anwendbarkeit (oder auch SoA= Statement of Applicability). In diesem Dokument werden die Anforderungen gelistet. Dabei unterscheidet der B3S zwischen MUSS, SOLL und KANN Anforderungen. Die Dokumentation im SoA berücksichtigt den Scope und die Ergebnisse der Bestandsaufnahme mit den bereits eingeführten und den geplanten Maßnahmen.

4. Definition des Geltungsbereichs

Eine schlüssige Definition und Abgrenzung des Geltungsbereichs eines B3S Krankenhaus ist entscheidend für die Umsetzung der Maßnahmen. Dabei müssen drei Bereiche betrachtet werden:

- Den räumlichen Geltungsbereich (Ort)
- Der sachliche Geltungsbereich (Prozesse, Anwendungssysteme)
- Die verwendete technische Infrastruktur (eingesetzte Technik)

Die erbrachten Leistungen durch Dritte bspw. eine Datenverarbeitung im Auftrag und/oder die Auslagerung von Dienstleistungen (bspw. externe Labore, externer Sicherheitsdienst, Beschaffung, etc.) sind unbedingt zu berücksichtigen und nach Prüfung ggf. im Geltungsbereich mit einzubeziehen. In diesem Kontext ist es wichtig, dass alle Schnittstellen zur Klinik analysiert und mit Fokus auf den Geltungsbereich und die definierten Schutzziele eingeordnet werden.

5. Erstellung einer Leitlinie

Die Leitlinie beschreibt grundlegende Ziele und Anforderungen zur Informationssicherheit. Sie gibt den Stellenwert der Informationssicherheit wieder und legt die Sicherheitsstrategie fest. In ihr sind die allgemeinen Sicherheitsziele formuliert, die Sicherheitsorganisation definiert und die regelmäßige Erfolgskontrolle und Fortschreibung geregelt.

6. Bestandsaufnahme

Zur Bestandsaufnahme nutzt man u. a. die Methoden der Dokumentenprüfung, Interviews mit Prozessverantwortlichen und Begehungen. Ziele der Bestandsaufnahme sind die Identifikation der Informationswerte, die Identifikation der Bedrohungen und Schwachstellen und die Bewertung des aktuellen Sicherheitsniveaus auf Grundlage der Anforderungen aus dem B3S. Die Ergebnisse des aktuellen Sicherheitsniveaus fließen in das SoA. Nachfolgend werden die Abweichungen, Korrekturmaßnahmen sowie Prioritäten bestimmt und in einen konkreten Maßnahmenplan überführt.

Die Einführung eines ISMS nach B3S ist eine Herausforderung – mit einem zielgerichteten Vorgehen erhöht sie jedoch die Informationssicherheit in Krankenhäusern signifikant und schützt somit das Leben der Patienten.

Mit diesen sechs Schritten ist der Anfang hin zur Umsetzung des B3S gemacht. Daran anknüpfend folgen weitere Prozesse wie die Risikoanalyse, die Umsetzung der Maßnahmen, die sehr wichtigen Awareness-Schulungen für Mitarbeitende, die Aufrechterhaltung der kritischen Dienstleistungen und die Evaluierung der Effektivität des ISMS. Die Einführung eines ISMS nach B3S ist eine Herausforderung – mit einem zielgerichteten Vorgehen erhöht es jedoch die Informationssicherheit in Krankenhäusern signifikant und schützt somit das Leben von Patientinnen und Patienten. &

Die Menschen hinter Althammer & Kill:

Danny Sellmann

Ja hallo, wer bist du denn?

Danny: Ja Moin, ich bin der Danny, 33 Jahre alt und komme aus Hannover. Ich bin gelernter Einzelhandelskaufmann, Groß- & Außenhandelskaufmann, habe mich neben der Arbeit zum Online-Marketing-Manager weiterbilden lassen und arbeite noch am Wochenende an meinem eigenen Unternehmen „YoRocket".

Wie lange arbeitest du schon bei Althammer & Kill?

Danny: Ich bin 2019 bei Althammer & Kill dazugestoßen. Der Marketing-Bereich bekam durch die stetig wachsende Unternehmensgröße immer mehr an Aufmerksamkeit. Da habe ich mich kurzerhand auf die ausgeschriebene Stelle beworben und hier bin ich jetzt seit drei Jahren tätig.

Was sind Deine Aufgaben?

Danny: Bis vor wenigen Monaten gehörte zu meinen Aufgaben alles, was den Marketing-Bereich betrifft. Angefangen bei unseren Printprodukten wie das Kundenmagazin, Flyer, Broschüren und Merkblätter bis zur Websitepflege, Social Media, Veranstaltungen, Newsletter u. v. m. Durch die personelle Aufstockung im Marketing, kann ich mich jetzt einzelnen Aufgabengebieten intensiver widmen.

Was gefällt dir besonders an der Tätigkeit des Online-Marketing-Managers?

Danny: Mir gefällt in erster Linie, dass man als Online-Marketing-Manager mit aktuellen und zukunftsträchtigen Medien arbeitet und Interessenten/Kunden mit nur wenigen Klicks erreichen kann, um u. a. die neuesten Updates zu teilen und zu informieren. Besonders in unserer Branche ist es wichtig immer up-to-date zu bleiben.

„Besonders in unserer Branche ist es wichtig, immer up-to-date zu bleiben."

Wie sieht dein Alltag als Online-Marketing-Manager aus?

Danny: Mein Alltag ist geprägt von strukturierten Abläufen und immer wiederkehrenden Aufgaben bis hin zu kurzfristigen Anpassungen oder kleineren Projekten, die den Alltag wieder spannender machen und Abwechslungen mit sich bringen. Kein Tag gleicht dem anderen, auch wenn es einige tägliche oder wöchentliche Routineaufgaben gibt, so bleibt noch Platz für neue und spannende Projekte.

Welches Projekt hat dir in deiner Zeit bei Althammer & Kill am besten gefallen?

Danny: Ein einzelnes Projekt kann ich gar nicht hervorheben. Selbst kleinere Projekte, die schnell abgeschlossen werden können, gefallen mir genauso wie größere Projekte, wo viel im Vorfeld bedacht werden muss, damit wir am Ende unser Ziel erreichen.

Eines der großen Projekte war z. B. der Relaunch der Althammer & Kill Website. Eine Website wird nie final fertig werden, sie muss ständig in Bewegung bleiben und wird ständig mit neuen Beiträgen, Ideen und Elementen gefüttert.

Welche Herausforderungen ergeben sich für dich aus dem Marketing für den B2B Bereich im Vergleich zum B2C Bereich?

Danny: Beide Bereiche haben ihre Vor- und Nachteile, wenn es um die Möglichkeiten geht, neue Interessenten zu erreichen. Im B2B-Bereich muss man mehrere Personen ansprechen können, z. B. Mitarbeitende, die sich nur informieren möchten oder für Ihr Unternehmen eines unserer Produkte heraussuchen sollen und auch die Entscheider, die am Ende beschließen, mit welchem Unternehmen sie zusammenarbeiten wollen.

Im B2C-Bereich sind die drei oben genannten Personen nur eine einzelne. Sie informiert sich und sucht das Produkt oder wird darauf aufmerksam und entscheidet am Ende selbst, ob sie das Produkt kaufen möchte oder nicht. Das macht es etwas einfacher, aber dennoch sind beide Bereiche in Ihrem Umfeld recht komplex und faszinierend zugleich. &

Privacy Shield 2.0 – Licht am Ende des Schrems II-Tunnels?

Im März 2022 haben die Europäische Kommission und die USA eine grundsätzliche Einigung über ein neues „Trans-Atlantic Data Privacy Framework“ erzielt. Ein neues Abkommen wird es wohl dennoch nicht so schnell geben.

Aus Washington (USA) hörte man seit längerem, dass an einem neuen Datenschutz-Abkommen zwischen Europa und den USA gearbeitet wird. Die Zuversicht, eine schnelle und unkomplizierte Einigung zu finden, schien auf der anderen Seite des Atlantiks über eine lange Zeit exklusiv zu existieren – in Europa war man diesbezüglich etwas zurückhaltender. Daher war die Verwunderung auch recht groß, als bei einem Besuch des US-Präsidenten Biden bei Kommissionspräsidentin von der Leyen im März dieses Jahres das „Trans-Atlantic Data Privacy Framework“ (TADPF) verkündet wurde.

Trans-Atlantic Data Privacy Framework

Das TADPF soll den transatlantischen Datenverkehr fördern – selbstverständlich auf legaler und datenschutzkonformer Basis. Freunde des Datenschutzes erinnern sich: genau diesen Versuch hat es bislang schon zwei Mal gegeben. Die Versuche nannten sich Safe Harbour Abkommen und EU-US Privacy Shield. Beide scheiterten krachend. Getreu dem Motto „Alle guten Dinge sind drei!“ wagt man einen neuen Anlauf. Organisationen und Datenschützer stellen sich spätestens seit März die Frage: sind Datenübermittlungen in die USA nun rechtlich sauber?

Eine Absichtserklärung – nicht mehr, nicht weniger

Den Worten von Frau von der Leyen und Herrn Biden müssen nun Taten folgen, denn bisher handelt es sich beim TADPF nur um eine grundsätzliche Einigung. Man **möchte** den transatlantischen Datenverkehr fördern und man **möchte** einen geeigneten Datenschutzrahmen schaffen. Inwieweit die Parteien jedoch bereit sind sich aufeinander zuzubewegen, bleibt derweilen offen. Der Erfolg (oder Misserfolg) wird davon abhängen, ob und wieweit die USA bereit sind ihre Gesetze zu ändern.

Konkret geht es um die US-Überwachungsgesetze (FISA, CLOUD Act, etc.) und die unverhältnismäßigen Befugnisse der US-Geheim- und Nachrichtendienste auf personenbezogene Daten von Europäerinnen und Europäer zuzugreifen.

Grundsätzlich scheinen die USA zu Gesetzesänderungen bereit zu sein. Ein neues Regelwerk und verbindliche Garantien sollen den Zugriff auf Daten durch US-Geheim- bzw. Nachrichtendienste „zum Schutz der nationalen Sicherheit“ auf ein notwendiges und verhältnismäßiges Maß beschränken; die Nachrichtendienste sollen Verfahren einführen, die eine wirksame Überwachung der (neuen) Datenschutz- und Grundrechte sicherstellen. Außerdem soll ein neues zweistufiges „Rechtsbehelfssystem“ zur Untersuchung und Beilegung von Beschwerden der Europäer entstehen – einschließlich eines Datenschutzüberprüfungsgerichts.

Doch wird dies am Ende reichen, um eine rechtssichere Basis für transatlantische Datenübermittlungen zu etablieren? Wer definiert notwendige und verhältnismäßige Zugriffe von US-Geheim- und Nachrichtendiensten? Exzessive Jubelstürme seitens europäischer Datenschützer konnten bislang nicht vernommen werden. Dies liegt wohl auch daran, dass juristische Texte bislang fehlen. Derweilen haben die Parteien angekündigt, die Verhandlungsergebnisse in rechtliche Dokumente zu übersetzen – ohne dabei einen Stichtag zu nennen.

Aktuell sind Datenübermittlungen in die USA mit einem nicht zu unterschätzenden Aufwand verbunden. Neben dem Abschluss von Verträgen zur Auftragsverarbeitung (DPA) müssen Organisationen (in der Regel) auch auf den Abschluss von Standarddatenschutzklauseln hinwirken.

Was wäre, wenn...

... am Ende des Verhandlungs- und Übersetzungsprozesses ein Abkommen zustande kommt, welches eine rechtssichere Datenübermittlung in die USA ermöglicht? Die Erleichterung bei Datenschützern und der Wirtschaft wäre wohl groß. Aktuell sind Datenübermittlungen in die USA mit einem nicht zu unterschätzenden Aufwand verbunden. Neben dem Abschluss von Verträgen zur Auftragsverarbeitung (DPA) müssen Organisationen (in der Regel) auch auf den Abschluss von Standarddatenschutzklauseln hinwirken. Da die USA spätestens seit Juli 2020 als unsicheres Drittland angesehen werden, ist auch eine Transfer-Folgenabschätzung (TIA) notwendig. Derzeit entsteht in Organisationen daher viel Papier, um Daten über den Atlantik übermitteln zu dürfen. Sollte ein rechtssicheres Abkommen gelingen, würden wohl viele der heutigen obligatorischen Pflichten wegfallen.

Was wäre aber, wenn am Ende der Verhandlungen bzw. des Übersetzungsprozesses ein Abkommen zustande kommt, welches unmittelbar von Datenschützern sowie Non-Profit-Organisationen wie NOYB und Co. ein drittes Mal vor den EuGH gezerrt wird, da es den europäischen Grundrechten wieder einmal nicht standhält? Dann würde sich nichts ändern! Die seit Juli 2020 bewährten Übertragungsmechanismen würden weiterhin gelten. Nur dürfte dieses Szenario in Zeiten der Digitalisierung von Organisationen und Abläufen niemanden glücklich machen.

Auswirkungen der TADPF-Ankündigung

Die Auswirkungen der TADPF-Ankündigung auf Organisationen in der EU kann zum gegenwärtigen Zeitpunkt ziemlich genau beziffert werden: sie ist gleich null – zumindest bis wir mehr erfahren, z. B. in Form von Rechtstexten. Organisationen, die ihre Datenübermittlung in die USA auf Basis von DPA, Standarddatenschutzklauseln, TIA und Co. stützen, sind gut beraten, dies weiterhin so zu handhaben.

Organisationen, die auf ein neues und schnelles Abkommen gehofft und dadurch bisher keine Maßnahmen getroffen haben, sollten spätestens jetzt reagieren. Denn niemand glaubt ernsthaft daran, dass wir kurzfristig mit einem wasserdichten Abkommen rechnen können. &

Stichwort
Transatlantischer Datenverkehr

Das TADPF soll den transatlantischen Datenverkehr fördern – selbstverständlich auf legaler und datenschutzkonformer Basis. Freunde des Datenschutzes erinnern sich: genau diesen Versuch hat es bislang schon zwei Mal gegeben. Die Versuche nannten sich *Safe Harbour Abkommen* und *EU-US Privacy Shield*. Beide scheiterten krachend

Risikomanagement in der Cloud

Viele Unternehmen beabsichtigen in „die Cloud“ zu ziehen oder nutzen bereits Cloud-Funktionalitäten. Doch was verbirgt sich überhaupt hinter diesem Begriff?

Cloud-Storage, Cloud-Ready, Privacy-Cloud, Personal-Cloud, cloudbasierte Anwendungen – es scheint, als wäre die Cloud überall und könnte alle Probleme lösen, mit welchen Unternehmen konfrontiert werden können. Die HR-Abteilung würde das Bewerbermanagement gerne effektiver gestalten? Kein Problem, hier gibt es eine Cloud-Anwendung für. Wissensmanagement? Ab in die Cloud!

Doch wie so häufig, werden die Vorteile stark beleuchtet, aber eventuelle Probleme im Dunkeln belassen. Ob es vorteilhaft ist, dass das neue HR-Programm auf Servern in einem Land mit fragwürdigen geheimdienstlichen Befugnissen liegt und ob dies überhaupt legal umsetzbar ist, sind Fragen, die allzu oft leider erst nach der Kaufentscheidung beleuchtet werden.

Cloud Computing hat die Art und Weise wie Unternehmen arbeiten revolutioniert und unser tägliches Leben erheblich beeinflusst. Wie bei jeder neuen Technologie gibt es jedoch auch bei der Nutzung der Cloud Risiken. Diese Risiken müssen sorgfältig gemanagt werden, um negative Folgen für Ihr Unternehmen zu vermeiden. Im Idealfall werden die Risiken vor der Migration in die Cloud angegangen.

Die Cloud als Allheilmittel?

Die Cloud ist ein Begriff, welcher aus der modernen Geschäftswelt kaum wegzudenken ist. Anfangs wurden vor allem Cloud-Speicher angeboten, um Privatpersonen und Unternehmen die Möglichkeit zu geben schnell und einfach Datensätze zu speichern, ohne hierfür eine physische Festplatte oder einen Server anzuschaffen. Die Cloud stellte hier also eine, von der ganzen Welt aus erreichbare, Alternative zu Speichermedien dar. Realisiert werden konnte dies durch Dienstleister, welche Rechenzentren betreiben und entsprechende Container für Kunden zur Verfügung stellen. Der Vorteil für Unternehmen und Privatpersonen ist, dass sie günstiger Speicher erwerben konnten und dieser einfach erweiterbar ist.

Mittlerweile gibt es für jede denkbare Anwendung eine Cloud-Lösung, ob es nun der einfache Speicher ist, Data-Lakes oder sogar Quanten-Computing. Die Cloud ist somit sehr flexibel und bietet Unternehmen jeglicher Art eine Plattform. Die Skalierbarkeit ist das Hauptargument für die Migration in eine Cloud-Umgebung. Während früher Speicher und andere Server gekauft und im eignen Rechenzentrum betrieben werden mussten, können heute auf Klick neue Ressourcen dazugekauft oder abbestellt werden. Dies bietet Unternehmen die Möglichkeit schnell auf dem Markt zu reagieren und neue Produkte oder Funktionen zu testen, ohne hohe Investitionen tätigen zu müssen.

Gefahren der Cloudmigration

Die Nutzung der Cloud birgt einige Gefahren, wie z. B. ein unausgereiftes Rollen- und Rechtekonzept. Ist die Zugriffsstruktur nicht sinnvoll geregelt, kann es zu Problemen und dem Abfluss von Daten kommen. Problematisch bei der Nutzung von Cloud-Diensten ist hier vor allem, dass häufig weitere Sicherheitsmechanismen wie ein Geoblocking oder auch VPN’s nicht genutzt werden, obwohl dies eigentlich möglich wäre. Angreifende kennen diese Vektoren und zielen immer häufiger genau auf diese unbedachten Cloud-migrationen ab.

Neben Angreifenden besteht die Gefahr jedoch ebenfalls durch Drittländer, die nicht dasselbe Datenschutzniveau wie die EU besitzen. Geheimdienste haben hier oft umfangreiche Rechte, welche dazu führen, dass ein Speichern personenbezogener Daten nur schwer datenschutzkonform möglich ist. Verschlüsselungen und die Anonymisierung von Daten werden nur selten eingesetzt und die Effektivität einer Verschlüsselung ist nur so hoch wie die Sicherheit des Schlüssels.

Eine weitere nicht zu unterschätzende Gefahr ist die Zukunftssicherheit. Der Einstieg in die Cloud gestaltet sich häufig einfacher als der Ausstieg. Sind die Anwendungen auf einer bestimmten Plattform performant, müssen sie dies in anderen Cloud-Umgebungen nicht sein. Cloud-Dienstleister haben somit die Möglichkeit bei der Preisgestaltung frei zu agieren, da der Wechsel eines Anbieters häufig teurer ist, als die gestiegenen Lizenzgebühren zu zahlen.

Ein geringes Risiko, das Sie dennoch berücksichtigen sollten, ist der Datenverlust. Obwohl Cloud-Anbieter Sicherheitsvorkehrungen getroffen haben, um Datenverluste zu verhindern, kann es dennoch dazu kommen. Ein prominentes Beispiel sind unter anderem zwei große deutsche Cloud-Anbieter, welche mit Problemen zu kämpfen haben. Bei einem dieser Anbieter sind massenhaft Backups, welche in der Cloud gespeichert waren, abhandengekommen.

In Cloud-Umgebungen gibt es ebenfalls häufig eine Aufgabenverschiebung. So werden Updates bei On-Premise Lösungen noch von Administratoren geprüft, bevor sie ausgerollt werden. In der Cloud geschieht dies meist erst nach dem Rollout. Häufig sind Funktionen zwar standardmäßig erst einmal deaktiviert, ein Administrator muss jedoch immer auf dem neusten Stand bleiben, um eventuell aktive Funktionen zu evaluieren.

Risikomanagement

Wie können also die angesprochenen Risiken behandelt werden?

Der Cloud-Einstieg muss sorgfältig geplant werden. Es empfiehlt sich die Anbieter genau zu prüfen, um auf potentielle Probleme frühzeitig reagieren zu können. Hier ist vor allem die Frage zu klären, ob das Nutzen der Cloud-Infrastruktur mit der aktuellen Gesetzeslage konform möglich ist. Ebenso muss geprüft werden, welche und in welchem Umfang Daten in der Cloud verarbeitet werden können. Dies kann dazu führen, dass einige Anwendungen nicht in der Cloud betrieben werden können oder eben entsprechende Sicherheitsmechanismen etabliert werden müssen, um einen reibungslosen Betrieb zu gewährleisten.

Während die Migration in die Cloud schon sehr viele Ressourcen beansprucht, kann ein Weggang aus der Cloud zu weiteren Problemen führen, wenn dieser nicht von Anfang an mitgedacht wird. Es ist somit wichtig genau zu prüfen, inwieweit geschäftskritische Funktionalitäten auch außerhalb der Cloud gehostet werden können. Ebenfalls muss bei einem Einstieg in die Cloud über Rollen und Rechte innerhalb des Unternehmens nachgedacht werden. Eine granulare Verteilung der notwendigen Zugriffsrechte muss nicht nur bedacht, sondern auch gepflegt werden. Um eben diese Zugriffsrechte zu verteilen ist es wichtig, die Rollen im Unternehmen zu kennen und zu definieren.

Fazit

Ein Cloud-Einstieg muss wohl durchdacht sein. Risiken dürfen nicht unterschätzt werden. Doch sind diese Vorkehrungen getroffen, können Cloud-Lösungen Unternehmen entlasten und Ihnen die Möglichkeit geben, kostengünstig und flexibel zu agieren. Der Gewinn an Sicherheit ist für die meisten Unternehmen immens, wenn die Sicherheitsmechanismen sorgfältig implementiert werden. Alles in allem lässt sich somit festhalten, dass es keine Angst vor der Cloud geben sollte, eher einen Respekt, der dazu führt, die Prozesse sorgsam zu durchdenken. &

Tipp vom Admin
Trotzdem Backups anlegen!

Datenverlust bei Kunden von Clouddienstleistern trifft diese meistens unvorbereitet, da Vertrauen in die Ausfallsicherheit besteht. Deshalb ist es wichtig, Backups vorzuhalten, welche auf Medien gespeichert werden, die außerhalb der Cloud liegen.

Backups, die außerhalb von Netzwerken aufbewahrt werden, sind die sicherste Lösung.

Rechtstreue und Legalitätspflicht: Der Compliance-Beauftragte

Für die Einhaltung gesetzlicher Regelungen und Vorgaben ist die Organisationsleitung - im Rahmen der Legalitätspflicht - verpflichtet, angemessene Präventionsstrukturen aufzubauen. Ganz allgemein kann man dieses als Compliance-Management-System bezeichnen.

Die Größe und der Umfang richten sich vor allem nach der Größe, der Komplexität und dem Risiko der jeweiligen Organisation. Kurzum: Gesetzliche Pflichten müssen an geeignete Personen delegiert, entsprechende Verfahrensanweisungen wirksam in Kraft gesetzt und die Einhaltung kontrolliert werden. Die Person, die ein Compliance-Management-System auf Basis der bereits vorhandenen Strukturen vernetzt, pflegt, kontrolliert und aktualisiert, bezeichnet man üblicherweise als Compliance-Beauftragten.

Anders, als im Datenschutzbereich gibt es jedoch keine explizite gesetzliche Pflicht, eine solche Position einzurichten. Trotzdem kommt der Position eine immer wichtigere Bedeutung zu.

Compliance – Bedeutung für Organisationen

Ein stichhaltiges Compliance-Management ist für Organisationen von herausragender Bedeutung.
So sorgt eine gelebte Compliance-Kultur nicht nur für eine rechtskonforme und redliche Führung der Organisation, sondern trägt auch dazu bei, dass ein Compliance-konformes Mitarbeitendenverhalten etabliert wird. Außerdem trägt eine Kultur der Regel- und Rechtstreue dazu bei, Verstöße konsequent aufzudecken bzw. zu verhindern und straf- sowie zivilrechtliche Risiken zu minimieren. Doch dazu müssen Spielregeln aufgestellt werden – genau an dieser Stelle fungiert der Compliance-Beauftragte als Spielleiter.

Compliance-konforme unternehmerische Handlungen begründen sich aus vielen Gesetzen wie z. B. aus dem Bürgerlichen Gesetzbuch (BGB), dem GmbH-Gesetz, dem Gesetz gegen Wettbewerbsbeschränkungen (GWB), dem Wertpapierhandelsgesetz (WpHG) und vielen mehr.

Aufgabengebiet(e) des Compliance-Beauftragten

Zunächst muss festgehalten werden, dass „Compliance“ eine Aufgabe der Organisationsleitung ist (und bleibt). Sie kann die Umsetzung jedoch „wegdelegieren“ und einen Compliance-Beauftragten mit dem Aufbau und der Unterhaltung eines Compliance-Managementsystems beauftragen. Dafür benötigt die Rolle des Compliance-Beauftragten Weisungsfreiheit und umfassende Befugnisse, um bspw. Fehlverhalten und Verstöße zu ermitteln und aufzudecken.

Der Compliance-Beauftragte ist dabei jedoch weder „Spion in den eigenen Reihen“ noch „Handlanger der Organisationsleitung“. Er handelt im Interesse der gesamten Organisation und aller Stakeholder, indem er Schaden von der Organisation bestmöglich abwendet. Dies kann ihm nur gelingen, wenn er umfassende Fachkenntnisse in allen Compliance-relevanten Bereichen besitzt und auf die Entwicklung und Umsetzung eines effektiven Programms zur Einhaltung gesetzlicher und selbst auferlegter Vorschriften hinwirken kann. Der Compliance-Beauftragte prüft proaktiv vorhandene Prozesse und Praktiken in der gesamten Organisation auf Konformität und schult die Mitarbeitenden entsprechend den internen und externen (rechtlichen) Vorgaben. Umfassende IT-Kenntnisse gehören ebenso zum Repertoire eines Compliance-Beauftragten wie ökonomischer Sachverstand.

Die Krux der Freiwilligkeit

Anders als beispielsweise in der Datenschutz-Grundverordnung fordern keine europa- oder deutschlandweit allgemeingültigen Gesetze oder Verordnungen die Stellung eines Compliance-Beauftragten über alle Organisationen hinweg. Kann man aus diesem Umstand schlussfolgern, dass die Benennung eines Compliance-Beauftragten maximal auf Freiwilligkeit beruht? Weit gefehlt, denn auch wenn keine Pflicht zur Benennung einer ausgewählten Person besteht, sind Gesetze und Vorgaben von jeder Organisation einzuhalten.

Compliance-konforme unternehmerische Handlungen begründen sich aus vielen Gesetzen wie z. B. aus dem Bürgerlichen Gesetzbuch (BGB), dem GmbH-Gesetz, dem Gesetz gegen Wettbewerbsbeschränkungen (GWB), dem Wertpapierhandelsgesetz (WpHG) und vielen mehr. Nichtkonformes Handeln kann Sanktionen nach sich ziehen - vom Ausschluss aus öffentlichen Vergabeverfahren bis hin zur persönlichen Haftung der Organisationsleitung. Daraus lässt sich schlussfolgern, dass eine Notwendigkeit zur Benennung eines Compliance-Beauftragten besteht, der alle notwendigen Fachkenntnisse besitzt, um Compliance-konformes Handeln aller Akteure der Organisation sicherzustellen.

Für Compliance-Beauftragte wird es spannend

Compliance, bzw. das Bewusstsein darüber, hält immer mehr Einzug in deutsche und europäische Organisationen. Beste Beispiele hierfür sind die EU-Whistleblower-

Richtline sowie das Lieferkettensorgfaltspflichtengesetz. Erstere Richtlinie wurde bislang noch nicht in ein nationales Gesetz überführt, obwohl dies bis Ende 2021 hätte geschehen müssen. Es ist davon auszugehen, dass der nationale Gesetzgeber dies bald nachholen wird, denn ein neuer Referentenentwurf wurde bereits Anfang April 2022 veröffentlicht. Vermutlich wird dieser in den nächsten Monaten verabschiedet. Ab diesem Zeitpunkt besteht (nach derzeitiger Lage) die Pflicht zur Einrichtung eines internen Hinweisgebersystems ab einer Organisationsgröße von 50 Mitarbeitenden. Derzeit befinden wir uns in Deutschland daher in einer (ungewollt) verlängerten Vorbereitungsphase, die von den Organisationen genutzt werden sollte. Sobald das nationale Gesetz erscheint, wird es wohl keine Übergangszeit mehr geben (können).

Das Lieferkettensorgfaltspflichtengesetz wiederum wurde im Sommer 2021 vom Deutschen Bundestag beschlossen und ist ab dem 1. Januar 2023 für Organisationen in Deutschland oder mit einer Zweigniederlassung in Deutschland mit min. 3.000 Beschäftigten gültig. Ab dem 1. Januar 2024 reduziert sich die Grenze der Beschäftigten auf 1.000. Das Gesetz soll der Verbesserung der internationalen Menschenrechtslage dienen, indem es Anforderungen an ein verantwortungsvolles Management von Lieferketten festlegt. Analog zur EU-Whistleblower-Richtlinie müssen Organisationen Kommunikationskanäle zur Meldung von Verstößen etablieren. Für die Aufarbeitung der gemeldeten Vorfälle bedarf es innerhalb der Organisation fachkundiges Personal. Kurz gesagt: Es bedarf einen Ansprechpartner für Compliance - einen Compliance-Beauftragten.

Fazit

Organisationen sind gut beraten, die Funktion und Rolle eines Compliance-Beauftragten auszuarbeiten und zu etablieren. Fehlt innerhalb der Organisation die notwendige Fachkunde, können auf externe Compliance-Beauftragte zurückgegriffen werden. Die EU-Whistleblower-Richtlinie und das Lieferkettensorgfaltspflichtengesetz sind zwei aktuelle Beispiele dafür, dass professionelle Compliance für Organisationen immer wichtiger wird. &

In eigener Sache

Althammer & Kill unterstützt Organisationen bei der Erfüllung ihrer gesetzlichen Verpflichtungen, indem der externe Compliance-Beauftragte gestellt wird. Außerdem betreibt Althammer & Kill ein selbst entwickeltes Meldeportal, um die gesetzlichen Anforderungen der EU-Whistleblower-Richtlinie (und rechtzeitig auch des Lieferkettensorgfaltspflichtengesetzes) für Organisationen pragmatisch und wirksam umsetzbar zu machen. –
Sprechen Sie uns einfach an!

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

Impressum

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

Veranstaltungen und Termine

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

Hier klicken oder scannen!

21.–22. Juni 2022 – Online-Seminar
ISO 27001 Foundation Zertifikatskurs

Unser ISO 27001 Grundlagenseminar vermittelt Ihnen das Basiswissen der international anerkannten Norm für Informationssicherheit ISO 27001.

In dem zweitägigen Kurs lernen Sie die Norm kennen und können diese fortan in Ihrem Unternehmen adressieren. Vorkenntnisse werden nicht benötigt, denn der Referent geht mit Ihnen gemeinsam die Mindesanforderungen der Norm sowie Maßnahmen zur Umsetzung durch.

Sie haben nach Abschluss des Seminares die Möglichkeit, an einer Zertifikatsprüfung der international anerkannten ICO-Cert teilzunehmen (zzgl. Prüfungsgebühr). Nach bestandener Prüfung sind Sie qualifiziert, um den Professional Kurs zum international anerkannten Information Security Officer zu belegen.

26.–29. September 2022 – Online-Seminar
ISO 27001 Professional – Information Security Officer

Unser ISO 27001 Professional-Seminar vermittelt Ihnen das weiterführende Fachwissen der international anerkannten Norm für Informationssicherheit ISO 27001 und ergänzender Normen.

In dem viertägigen Kurs vermitteln wir Ihnen auf Basis des erfolgreichen Foundation Zertifikates tiefgreifendes Wissen und bereiten Sie so auf das erfolgreiche Bestehen der Zertifikatsprüfung vor.

Nach Abschluss des Seminares haben Sie die Möglichkeit, an einer Zertifikatsprüfung der international anerkannten ICO-Cert teilzunehmen (zzgl. Prüfungsgebühr). Bei bestandener Prüfung besitzen Sie den zertifizierten Nachweis der fachlichen Kenntnisse zur Normenreihe ISO27X.

09. Juni 22 – Webinar
LearnBase – Einführungs-Webinar
Mit LearnBase können Sie Ihre Kolleginnen und Kollegen online schulen, eigene Inhalte für Unterweisungen und E-Learnings zur Verfügung stellen oder selbst Seminare oder Webinare organisieren. Wir stellen Ihnen die Lernplattform vor.

15. Juni 2022 – Webinar
Umsetzung der EU-Whistleblower-Richtlinie: Das Hinweisgebersystem
Wir stellen Ihnen das Hinweisgebersystem von Althammer & Kill vor, das sich ganz einfach bei Ihnen einbinden lässt, alle Daten völlig anonym behandelt und die Anforderungen an die neue Richtlinie optimal erfüllt.

29. Juni 2022 – Webinar
Microsoft 365, AWS & Co. – sicher in die Cloud
Microsoft 365, Amazon Web Services und ähnliche Anwendungen sind ein Problemfall für Datenschützer – denn es sind sogenannte „Cloud-Dienste". Wir zeigen, worauf Entscheider im Rahmen ihrer IT-Strategie achten sollten und welche rechtlichen Herausforderungen bei der Einführung gemeistert werden müssen.

Haben Sie Fragen?

Ihr Ansprechpartnerin für alle Themen rund um die Althammer & Kill-Akademie:

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

Der Berater-Alltag bei Althammer & Kill

Julian Lang ist bereits seit über vier Jahren als Berater für Datenschutz und Informationssicherheit bei Althammer & Kill tätig.

Was die Arbeit des Beraters ausmacht, was er daran schätzt und welche Themen seiner Meinung nach in Zukunft noch relevanter werden, erzählt Julian in unserem Format „Über die Schulter geschaut".

Was ist bisher dein größtes Projekt gewesen?

Julian: Da ich mehrere größere Projekte begleitet habe und einige immer noch als Datenschutzbeauftragter begleite, ist die Frage nicht so einfach zu beantworten. Eines der größeren Projekte war die Einführung eines Datenschutz-Management-Systems (DSMS) bei einem großen diakonischen Träger mit über 2.000 Mitarbeitenden und um die 20 Organisationseinheiten. Die Diversität der Tätigkeitsfelder hat die Organisation der Zusammenarbeit erschwert und wir mussten ausprobieren, wie wir am effizientesten zusammenarbeiten können.

Der für uns richtige Weg war die Benennung von Datenschutzkoordinatorinnen und -koordinatoren je Organisationseinheit mit regelmäßigen Treffen. Nicht selten haben soziale Träger viele Tätigkeitsfelder wie z. B. ambulante und stationäre Pflegedienste, diverse soziale Beratungsangebote, Kindertageseinrichtungen, Kliniken und viele weitere Tätigkeitsfelder. Das Ziel jedes Management-Systems sollte es m. E. sein, standardisierte Vorgehensweisen zu entwickeln und einzuführen.

Die Praxis bei solchen Komplexträgern zeigt jedoch auch, dass nicht alles zu vereinheitlichen ist und jeder Bereich auch individuell betrachten werden muss. Das macht es aber auch spannend!

Was gefällt dir besonders an der Tätigkeit als Berater für Datenschutz und Informationssicherheit?

Julian: Die Vielseitigkeit. Man hat jeden Tag mit super interessanten und sehr unterschiedlichen Menschen zu tun und lernt jeden Tag dazu. Zusätzlich entwickeln sich die Themen Datenschutz und Informationssicherheit stetig weiter und man muss ständig am Ball bleiben. Natürlich ist der Job auch manchmal stressig, aber für mich käme aktuell kein anderer Job in Frage.

Welche war die größte Herausforderung, die dir je bei der Arbeit mit einem Kunden begegnet ist?

Julian: Die Zusammenarbeit mit jedem neuen Kunden stellt zunächst eine Herausforderung dar. Es gilt sich aufeinander „einzugrooven" und die gegenseitigen Erwartungshaltungen zu klären.

Als besonders herausfordernd habe ich es empfunden, wenn eine Schlüssel-Ansprechpartnerin oder Ansprechpartner beim Kunden wechselt. Wenn die vorherige Ansprechpartnerin oder Ansprechpartner für einen nicht mehr verfügbar ist, weil diese oder dieser das Unternehmen verlassen hat, ist eine strukturierte Datenschutzorganisation und eine vorherige Übergabe umso wichtiger.

Welche Themen beschäftigen unsere Kundinnen und Kunden am meisten?

Julian: Im Datenschutz definitiv das Schrems II Urteil und die Zulässigkeit der Beauftragung von US-amerikanischen Unternehmen und deren Dienste.

Welches Thema liegt dir am besten/wozu berätst du am liebsten?

Julian: Ich mag am liebsten sehr spezifische Projekte, wie z. B. die Begleitung bei der Durchführung einer Datenschutz-Folgenabschätzung. Hier vereinigen sich Datenschutz und Informationssicherheit.

Stichwort
Datenschutz-Folgenabschätzung

Die DSFA ist eine Risikoanalyse, wie man sie auch aus anderen Bereichen des täglichen (Wirtschafts-)Lebens kennt. Ermittelt werden Schadenspotenziale und Eintrittswahrscheinlichkeiten von Ereignissen, wie z. B. Hacking, Datenverlust durch Brand usw.

Die daraus resultierenden potenziellen Folgen werden bewertet und auf Basis dessen entschieden, ob eine Datenverarbeitung stattfinden darf.

Welche Themen werden deiner Meinung nach im Jahr 2022 noch relevanter?

Julian: Ich denke, dass einige Unternehmen noch Nachholbedarf bei ihrer Informationssicherheit haben. Die letzten Jahre haben gezeigt, dass immense Schäden aufgrund von Hackerangriffen oder technischen oder menschlichen Fehlern entstehen können. Zusätzlich gibt es immer strengere Regularien, die von Unternehmen berücksichtigt werden müssen.

Wie eng arbeitest du mit den anderen Beratern zusammen?

Julian: Vor Corona sehr eng. Durch Corona war es uns lange Zeit nicht mehr möglich vor Ort zusammen zu arbeiten, weshalb dieses „Teamgefühl" ein wenig auf der Strecke geblieben ist. Ich bin aber guter Dinge, dass wir dieses Gefühl zukünftig wieder bekommen werden.

Wie läuft eine Beratung klassischerweise ab?

Julian: In der Regel fängt man mit einer Bestandsaufnahme an und ermittelt den Ist-Stand des Unternehmens und definiert Maßnahmen. Diese Maßnahmen arbeitet man sukzessive mit seinem Ansprechpartner ab, bis man ein etabliertes und funktionsfähiges Datenschutz-Management- und/oder Informationssicherheits-Management-System aufgebaut hat. Danach gilt es die Managementsysteme aktuell zu halten und auf Neuerungen wie z. B. Gesetzesänderungen zu reagieren. Um die Aktualität und Weiterentwicklung der Managementsysteme zu erreichen, führt man regelmäßige Audits durch.

ALTHAMMER & KILL

Digitalisierung sicher gestalten

Althammer & Kill bietet pragmatische Lösungskonzepte für Datenschutz und Digitalisierung. Wir beraten bundesweit im Umfeld Datenschutz, Informationssicherheit, Cloud- und Cybersecurity und Compliance.

Unsere rund 45 Mitarbeitende an den Standorten Hannover, Düsseldorf und Mannheim sind als externe Datenschutzbeauftragte, Informationssicherheits- und IT-Experten für mehr als 500 Kunden unterschiedlichster Branchen tätig.

Althammer & Kill GmbH & Co. KG

Roscherstraße 7 · 30161 Hannover · Tel. +49 511 330603-0
Mörsenbroicher Weg 200 · 40470 Düsseldorf · Tel. +49 211 936748-0
Kaiserring 10–16 · 68161 Mannheim · Tel. +49 621 121847-0

vertrieb@althammer-kill.de
althammer-kill.de

Qualitätsmanagement nach Plan mit der ISO 9001:2015.

Mitgliedschaften

NIEDERSACHSEN DIGITAL · BvD e.V. · FINSOZ · GDD