COMPLIANCE konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 4/2022

Mehr Cyber-Resilienz dank EU DORA?

Ein einheitlicher Rechtsrahmen zur risikoarmen Digitalisierung des Finanzsektors

Seite 6

TADPF
Rechtssicherheit für Datenexporte in die USA?
Seite 10

Den Zugriff auf die sensiblen Daten vernageln
Anwendungen effektiv schützen
Seite 12

DSGVO und Geschäftsführerhaftung
Persönliche Haftbarkeit vermeiden
Seite 14

Editorial

Liebe Leserin, lieber Leser,

die Lage der Cyber-Security in Deutschland hat sich über die letzten Wochen und Monate weiter zugespitzt. Das zeigen aktuelle Zahlen, aber auch Ereignisse wie ein Vorfall in einem Landkreis in Sachsen-Anhalt: Erstmals wurde wegen eines Cyber-Angriffs dort der Katastrophenfall ausgerufen. Ende Oktober konnten einige Regionen in Baden-Württemberg keine Zahlen zur Infektionslage übermitteln, weil sie ebenfalls von einem Cyber-Angriff betroffen waren.

Die Bedrohung betrifft zunächst alle Organisationen in Deutschland (und weltweit), allerdings ist besonders die kritische Infrastruktur in den Fokus gerückt. Die Sabotage bei der Deutschen Bahn und auf Kommunikationsnetze in Frankreich haben die Anfälligkeit deutlich gemacht.

Die vergangenen Ereignisse zu Grunde gelegt stellt sich nun die Frage: Sind wir ausreichend vor Angriffen geschützt? Und im gleichen Atemzug: Wie sehr trifft uns der Ausfall von IT-Systemen?

„Die vergangenen Ereignisse zu Grunde gelegt stellt sich nun die Frage: Sind wir ausreichend vor Angriffen geschützt?“

Diese Fragestellungen lassen sich ebenso auf Organisationen übertragen und sollten kritisch in den Blick genommen werden. Mehr denn je gehört das Thema IT-Sicherheit und die Notfallvorsorge für alle Unternehmen auf den Prüfstand.

Wir hätten uns gern mit einem positiven Rückblick aus dem alten Jahr bei Ihnen verabschiedet. So bleibt uns nur, auch in schwierigen Zeiten, Danke zu sagen für die gute Zusammenarbeit und das entgegengebrachte Vertrauen. Wir hoffen auf bessere Zeiten und wünschen Ihnen einen guten Start in das Jahr 2023!

Wie geht es im Januar weiter? In den kommenden Monaten werden einige Neuerungen in Sachen Compliance dazukommen. Zu nennen seien hierbei exemplarisch das Hinweisgeberschutzgesetz sowie das Lieferkettensorgfaltspflichtengesetz. Eine Auseinandersetzung mit diesen Themen steht vielen Organisationen noch bevor – gerne sind wir hierbei an Ihrer Seite und unterstützen Sie nach Kräften, bspw. durch die Stellung eines Compliance-Officers.

Wir wünschen Ihnen viel Spaß beim Lesen
und freuen uns auf den Diskurs 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!

Nicht nur Arbeitgeber der Zukunft, sondern auch Top Service.

Zwei Gründe zur Freude: Wir wurden vom Deutschen Innovationsinstitut für Nachhaltigkeit und Digitalisierung gleich doppelt ausgezeichnet. Nicht nur unsere Zukunftsfähigkeit hat überzeugt, sondern auch unsere Servicequalität! „DIND kooperiert mit Partnern und Experten aus Wirtschaft, Wissenschaft und Politik, führt unabhängige Studien durch und prüft Unternehmen auf wichtige Aspekte für deren Zukunftsfähigkeit. Die Besten werden ausgezeichnet – als ‚Arbeitgeber der Zukunft'. Unser Siegel ist ein Erfolgsausweis und optimal für die Kommunikation mit allen Stakeholdern geeignet." Und wir gehören dazu!

Die DSGVO – Wettbewerbsnachteil oder in naher Zukunft weltweiter Standard?

Schrems I und II, Angemessenheitsbeschlüsse, Standardvertragsklauseln, geeignete Garantien, Transfer Impact Assessments – die meisten Lesenden werden diese Begriffe entweder aus der Beratungspraxis oder aus ihrer betriebsinternen Tätigkeit im Rahmen des Datenschutzes kennen. Oft stellt sich hierbei die Frage, ob die ursprüngliche Idee des Wettbewerbsvorteils durch die DSGVO sich wirklich realisiert hat oder überhaupt noch realisieren kann. Wir gehen dieser Frage in unserem Blog nach.

Team Mannheim ziehen um!

Ab dem 01.12.2022 ist es soweit: Dann beziehen unsere Mannheimer Kolleginnen und Kollegen ihr neues Büro im SleevesUp! Die neue Adresse lautet dann:

Althammer & Kill GmbH & Co. KG
P7 20
68161 Mannheim

Was sind eigentlich Penetration-Tests und warum sind sie sinnvoll?

Täglich gibt es neue Hacking-Angriffe auf die Systeme der deutschen Wirtschaft. In einer digitalen Welt ist es schwer, den Überblick zu behalten, welche Systeme für externe Personen sichtbar sind. Abhilfe können sogenannte Penetration-Tests schaffen. Hierbei schauen keine kriminellen Hackerinnen oder Hacker, sondern beauftragte Personen auf die Systeme. Ein Test kann auf unterschiedlichsten Ebenen stattfinden. Wie das genau aussieht, erfahren Sie online.

Zahl des Monats

50

Organisationen ab 50 Mitarbeitenden müssen laut Hinweisgeberschutzgesetz ab Anfang 2023 ein Meldesystem einrichten.

Auf diese Weise werden nicht nur Gesetze und interne Regelungen in einer Organisation effektiv umgesetzt, sondern auch das Vertrauen unter den Mitarbeitenden durch die Möglichkeit zur Abgabe anonymer Hinweise gestärkt.

Das Wiedersehen in Hannover

Am 29. September haben sich Mitarbeitende aus Mannheim und Düsseldorf, aber auch aus unseren „Außenstellen" wie Nürnberg und Berlin, aufgemacht und sich in unserem Hauptsitz in Hannover zusammengefunden. Es wurde gearbeitet (ja, auch das muss sein), gequatscht, gegessen, gelacht und neue Kolleginnen in Beratung und Vertrieb stießen dazu. Der Abend wurde verbucht unter „sowas müssen wir öfter machen". Denn die meisten Kolleginnen und Kollegen hat man viel zu selten um sich.

Unser Podcast

„Maximale Langeweile" beschäftigt sich mit aktuellen Themen aus der Welt der Compliance. Besonderer Schwerpunkt bilden die Themen Datenschutz und Cyber-Security. Kontroverse Diskussionen werden dabei in den Vordergrund gerückt, während harte juristische oder technische Fakten eher den Unterbau bilden. „Maximale Langeweile" erscheint jeden zweiten Donnerstag auf Spotify, bei Apple Podcast und weiteren gängigen Podcast-Diensten.

Microsoft veröffentlicht ein neues Data Protection Addendum

Am Donnerstag, den 15.09.2022, hat Microsoft einen neuen Nachtrag zum Datenschutz veröffentlicht (engl. „Data Protection Addendum"). Dieser Nachtrag löst das bisherige Data Protection Addendum ab, welches Microsoft genau ein Jahr zuvor veröffentlicht hatte. Hauptgrund der neuen Version ist das Wirksamwerden der neuen EU-Standardvertragsklauseln, die seit Juni 2021 in Kraft sind. Wir nehmen online unter die Lupe, wie diese Anpassungen zu bewerten sind.

Gegen Cyberrisiken im Finanzsektor: EU DORA

Ein einheitlicher Rechtsrahmen zur risikoarmen Digitalisierung des Finanzsektors – das ist EU DORA

Von Christian Pinnecke

Die Cybergefahren nehmen in den letzten Jahren rasant zu und immer mehr Behörden und Unternehmen werden Opfer eines Cyberangriffs. Zur Steigerung der IT-Sicherheit in Deutschland wurde durch die Bundesregierung bereits 2021 das Artikelgesetz „Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)" veröffentlicht. Dadurch soll die deutsche IT-Infrastruktur, besonders die der deutschen KRISTIS-Betreiber (Kritische Infrastrukturen) besser geschützt werden.

Derzeit existieren 10 KRISTIS-Sektoren, darunter auch „Finanz- und Versicherungswesen". Aktuell definieren alle Mitglieder der Europäischen Union ihre z. B. IKT-Risiken sowie die Aufsichtsansätze im Finanzsektor selbst, was zu einer EU-weiten Instabilität des Finanzsektors führen könnte.

Was ist EU DORA und was soll damit reguliert werden?

DORA ist unter anderem ein Teil eines Pakets zur Digitalisierung des Finanzsektors auf Europäischer Ebene, das darauf abzielt, „das Innovations- und Wettbewerbspotenzial des digitalen Finanzwesens weiter zu erschließen und zu fördern und gleichzeitig mögliche Risiken zu mindern". Mit DORA sollen Cyberbedrohungen verringert und vermindert werden. Zudem schafft DORA einen Rechtsrahmen für die digitale Betriebsstabilität. Demnach müssen alle EU-Finanzunternehmen sicherstellen, dass sie in der Lage sind, allen Arten von Störungen und Bedrohungen im Zusammenhang mit IKT standzuhalten, darauf zu reagieren und sich von ihnen zu erholen.

Für wen gilt DORA und. bis wann muss es umgesetzt sein?

DORA gilt für alle vom Gesetzesentwurf zusammengefassten auf EU-Ebene regulierten „Finanzunternehmen". Namentlich werden im Gesetzesentwurf folgende Unternehmen genannt:

Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Anbieter von Krypto-Dienstleistungen, Emittenten von Kryptowerten, Emittenten von an Vermögenswerte geknüpften Token und Emittenten signifikanter an Vermögenswerten geknüpfter Token, Zentralverwahrer, zentrale Gegenparteien, Handelsplätze, Transaktionsregister, Verwalter alternativer Investmentfonds, Verwaltungsgesell-

Stichwort
DORA

Um einer EU-weiten Instabilität des Finanzsektors entgegenzuwirken, wurde im September 2020 durch die Europäische Kommission dem Europäischen Parlament ein Vorschlag für eine „Verordnung des Europäischen Parlaments und des Rats über die Betriebsstabilität digitaler Systeme" (DORA – Digital Operational Resilience Act) des Finanzsektors vorgelegt.

schaften, Datenbereitstellungsdienste, Versicherungs- und Rückversicherungsunternehmen, Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit, Einrichtungen der betrieblichen Altersversorgung, Ratingagenturen, Abschlussprüfer und Prüfungsgesellschaften, Administratoren kritischer Benchmarks, Crowdfunding-Dienstleister, Verbriefungsregister und IKT-Drittanbieter.

Am 24. September 2020 wurde der Gesetzesentwurf durch die Europäische Kommission veröffentlicht und am 11. Mai 2022 konnte der Vorsitz des Rates und das Europäische Parlament eine vorläufige Einigung über die Verordnung über digitale Betriebsstabilität (DORA) erzielen. Es ist davon auszugehen, dass DORA noch dieses Jahr förmlich angenommen wird und ab 2024 Anwendung findet.

Nachdem die DORA förmlich angenommen wurde und in Kraft getreten ist, wird sie in das nationale Recht der einzelnen EU-Mitgliedstaaten übergehen. Die werden im Anschluss die technischen Regulierungsstandards (Regulatory Technical Standards, RTS) und die technischen Durchführungsstandards (Implementing Technical Standards, ITS) ausarbeiten, die von allen Finanzunternehmen erfüllt werden müssen. Die jeweiligen nationalen Aufsichtsbehörden sollen dabei die Aufsicht der Einhaltung übernehmen.

Wer ist indirekt von DORA betroffen und wie grenzt man betroffene und nicht betroffene Unternehmen voneinander ab?

Nahezu alle Finanzunternehmen werden den neuen Vorschriften unterliegen. Prüfende werden nach der vorläufigen Einigung nicht der DORA-Verordnung unterliegen. Stattdessen werden sie Teil einer künftigen Überprüfung der Verordnung sein. Kritische Anbieter aus Drittländern, die IKT-Dienste für Finanzunternehmen in der EU bereitstellen, müssen innerhalb der EU eine Tochtergesellschaft gründen, damit die Aufsicht ordnungsgemäß durchgeführt werden kann. Kritische IKT-Drittanbieter sollen zukünftig unter die Aufsicht der Europäischen Aufsichtsbehörden (ESA) fallen.

Nach dem Grundsatz der Verhältnismäßigkeit sollen Unterschiede hinsichtlich Geschäftsmodell, Größe, Risikoprofil oder Systemrelevanz berücksichtigt werden. Kleinste Finanzunternehmen mit vermutlich weniger als 10 Beschäftigten und 2 Mio. € Jahresumsatz sollen laut EU-Kommission weniger umfassende Maßnahmen ergreifen müssen als größere Finanzunternehmen.

Was muss konkret gemacht/umgesetzt werden und wie packt man es am besten an?

Im DORA-Gesetzesentwurf sind sechs Handlungsfelder enthalten, die nahezu alle Felder des IKT-Risikomanagements abdecken. Diese sind:

IKT-Risikomanagement, Berichterstattung, Belastbarkeitstests, IKT-Risiken Dritter, Informationsaustausch und Governance

Die Finanzunternehmen unterliegen bereits einem umfangreichen Regelwerk. In DORA werden Anforderungen an den Finanzsektor gestellt, die weitestgehend in den bestehenden Regularien enthalten sein werden. Dabei ist aber zu erwarten, dass DORA die Anforderungen in anderen Ausprägungen und Detailtiefen beschreiben wird.

Ebenso spezifiziert die internationale Norm ISO/IEC 27001 ff (Managementsystem für Informationssicherheit (ISMS)) und die ISO 22301 (Managementsystem für Business Continuity (BCMS)) Anforderungen, die in DORA enthalten sein werden. Weitere branchenspezifische Gesetze und Normen können und sollten zur Vorbereitung und Orientierung für DORA genutzt werden.

Zur Sicherstellung der Anforderungen sollte frühzeitig eine GAP-Analyse der bisher umsetzten Regularien oder Managementsystem durchgeführt werden, um das Delta zwischen den verschiedenen Anforderungen und der DORA zu identifizieren. Des Weiteren sollte durch ein externes Audit der Reifegrad der umgesetzten Maßnahmen und Regularien bestimmt werden. Wer einen mittleren bis hohen Reifegrad der Anforderungen und Maßnahmen erreicht hat, verfügt über eine ideale Ausgangslage und eine weitestgehende DORA-Kompatibilität. &

Sie sind betroffen?

Wir stehen Ihnen bei Althammer & Kill beratend zur Seite – nehmen Sie gern mit uns Kontakt auf.

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

Die Menschen hinter Althammer & Kill:

Brigitta Németh

Ja hallo, wer bist du denn?

Brigitta: Mein Name ist Brigitta Németh alias „Brigittttaaa“. Ich bin gebürtige Ungarin und lebe seit 2015 in Hannover. Nach meinem BWL-Studium in der wunderschönen Stadt Budapest, hat mich die Liebe nach Hannover verschlagen.

Wie lange arbeitest du schon bei Althammer & Kill?

Brigitta: Ich verstärke das Althammer & Kill-Team seit 2018, also schon seit viereinhalb Jahren.

Was sind Deine Aufgaben?

Brigitta: Zu meinen Hauptaufgaben gehören die Fakturierung und Erstellung der Lohnabrechnungen sowie die Prüfung der Reisekostenabrechnungen und die Bearbeitung der Eingangsrechnungen.

Außerdem bin ich für eine gemütliche Atmosphäre unter den Kolleginnen und Kollegen zuständig. ☺

Was gefällt dir besonders an deiner Tätigkeit?

Brigitta: Da ich noch nie ein Fan davon war, Berichte oder Reports zu schreiben, mag ich besonders, dass ich großteils mit Zahlen, Daten und Fakten zu tun habe. Des Weiteren gefällt mir besonders, dass wir bei Althammer & Kill kurze und direkte Abstimmungswege sowie ganz viel Eigenverantwortung haben.

Wie sieht dein Alltag bei Althammer & Kill aus?

Brigitta: Ich bin meistens von 8–17 Uhr im Büro, vormittags erledige ich die Routine-Aufgaben. Dazu gehören beispielsweise die Vorbereitung der Eingangsrechnungen, die Post und die Eingangsmails in meinem Postfach. Somit kann ich mich am Nachmittag meistens auf die etwas komplexeren Projekte konzentrieren.

„Ein gutes Zeitmanagement sowie die Priorisierung meiner Tätigkeiten ist eine wichtige Voraussetzung für die Einteilung der Aufgabenbereiche.“

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

Brigitta: Am aufregendsten fand ich die Zeit, als ich die Lohnabrechnungen von unserem Steuerberater übernommen habe. Desweiteren wurde am Anfang des Jahres die LearnBase GmbH aus Althammer & Kill ausgegründet, wo sich auch viele Teilprojekte und organisatorische Aufgaben in den Bereichen Verwaltung und Buchhaltung ergeben haben.

„Vor der Tür stehen manchmal verirrte Bewerber, die zu einer anderen Firma wollen, die aber schon lange nicht mehr unter diese Adresse zu finden ist.“

Deine Aufgabenbereiche sind sehr vielfältig. Wie schaffst du es da den Überblick zu behalten?

Brigitta: Die Frage stelle ich mir manchmal selbst! Ein gutes Zeitmanagement sowie die Priorisierung meiner Tätigkeiten ist eine gute Voraussetzung für die Einteilung der Aufgabenbereiche.

Welche Bitte oder Anfrage erhältst du von Kolleginnen und Kollegen am häufigsten?

Brigitta: Es gibt zwei Sätze, die ich am häufigsten höre, entweder „Kannst du bitte meine Jira-Zeiten öffnen?“ oder „Wann hast du Zeit, um etwas zu bestellen?“

Welche war die interessanteste Begegnung, die du jemals an der Eingangstür von Althammer & Kill hattest?

Brigitta: Vor der Tür stehen manchmal verirrte Bewerber, die zu einer anderen Firma wollen, die aber schon lange nicht mehr unter diese Adresse zu finden ist. &

TADPF – Rechtssicherheit für Datenexporte in die USA?

Kennen Sie noch das EU-US Privacy Shield? Das durch das Schrems-II-Urteil gekippte Abkommen bekommt einen Nachfolger, der die problematischen Datentransfers in die USA auf eine klarere Grundlage stellen könnte. Das Ergebnis von langen Verhandlungen trägt den Namen Trans-Atlantic Data Privacy Framework (TADPF).

Von Winona Wenning

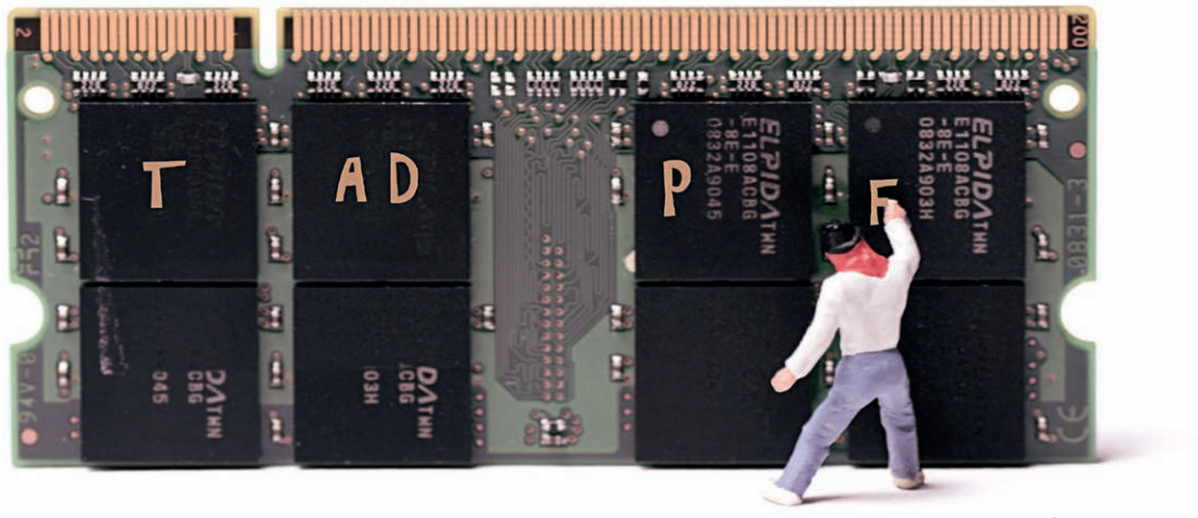
Durch das Schrems-II-Urteil (EuGH C-311/18) im Juli 2020 ergab sich ein großer Handlungsbedarf: Der Angemessenheitsbeschluss, welcher die USA zum sicheren Drittland im internationalen Datenverkehr erklärte, wurde aufgehoben. Dabei sind Datentransfers „über den großen Teich" allgegenwärtig, etwa in Konzernverflechtungen oder durch (Unter-)Auftragnehmende. Mit Wegfall des Angemessenheitsbeschluss gem. Art. 45 DSGVO standen diese Übermittlungen nun wieder auf dem Prüfstand. Meist mussten nun andere geeignete Garantien aus dem Katalog des Art. 46 DSGVO vorliegen, die den Schutz der Bertoffenen gewährleisten.

Was war noch mal das Problem?

Ein beliebtes Mittel: Die Standarddatenschutzklauseln der Kommission (SSC). Doch in bestimmten Fällen konnten auch diese keine Abhilfe leisten: War nicht der Auftragsverarbeitende im Drittland angesiedelt, sondern „nur" der Unterauftragnehmende, dann standen keine geeigneten Vertragsklauseln zur Verfügung. Erst der Erlass aktualisierter SSC im Juni 2021 sah vor, dass diese zwischen dem Auftragsverarbeitenden und seinem Unterauftragsverarbeitende abgeschlossen werden, der außerhalb des Europäischen Wirtschaftsraum sitzt.

Reichen die SSC doch nicht?

Für anderen Auswirkungen des Schrems-II-Urteils haben jedoch auch die aktualisierten SSC keine Abhilfe geschafft: Wer eben diese als Garantie im Sinne des Art. 46 DSGVO nutzt, hat als Verantwortlicher noch weitere Pflichten. Die Durchführung eines Transfer-Impact-Assessment, kurz TIA, soll das Datenschutzniveau im Land des Datenimporteurs beleuchten. Der Datenexporteur hat also der Frage nachzugehen, ob der Schutz für die Betroffenen mit dem in der EU gleichwertig ist. Besteht nach der Prüfung von Rechtslage und -Praxis Grund zur Annahme, dass dem Betroffenen etwa keine wirksamen Rechtsbehelfe zur Verfügung stünden, müssen weitere Maßnahmen zur Erhöhung des Schutzniveau ergriffen werden. Ist dies nicht möglich, muss von der Übermittlung abgesehen werden.



Klare Ansage

Eine klare Ansage ist dagegen der Angemessenheitsbeschluss der EU-Kommission: Im vorhergehenden Verfahren übernimmt dann Brüssel die Prüfung, ob ein gleichwertiges Schutzniveau im Drittland mit funktionierenden Datenschutzbehörden besteht, sodass eine Übermittlung die DSGVO aus Perspektive der Betroffenen nicht untergräbt. Mit Inkrafttreten des Angemessenheitsbeschluss bestehen für den Verantwortlichen keine zusätzlichen Hürden im Vergleich zum innereuropäischen Datenverkehr mehr.

Transatlantischer Datenschutzrahmen

Im Rahmen von Schrems-II kam der Europäische Gerichtshof aber zur Einschätzung, dass bezüglich der Vereinigten Staaten, zu den in 2020 herrschenden Rahmenbedingungen im Land, kein Angemessenheitsbeschluss bestehen kann. Hierbei waren besonders die behördlichen Befugnisse aus der FISA Section 702 und Executive Order 12333 im Fokus. Am 25. März dieses Jahres kündigten EU-Kommissionspräsidentin Ursula von der Leyen und US-Präsident Joe Biden endlich das „Trans-Atlantic Data Privacy Framwork" an. Der Transatlantische Datenschutzrahmen kann den Angemessenheitsbeschluss wieder ermöglichen, indem eine Selbstverpflichtung der USA die geäußerten Bedenken des EuGH ausräumt. Die sogenannten Executive Orders, also Durchführungsverordnungen, dienen als Grundlage der erneuten Bewertung der Kommission für ihren künftigen Angemessenheitsbeschluss.

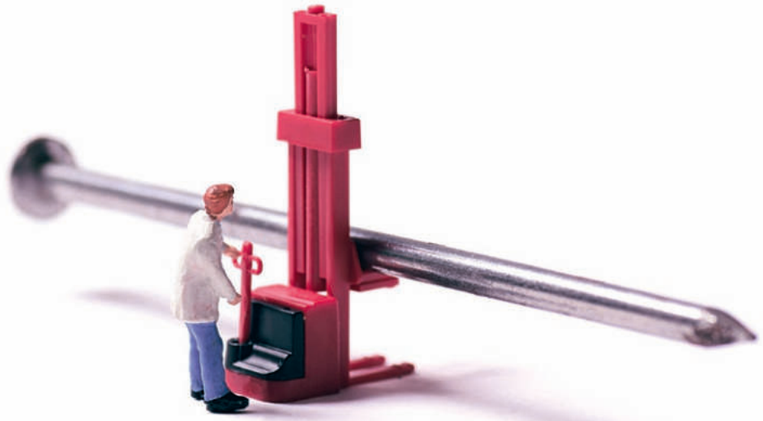
Kritisiert wurde insbesondere das in den USA geltend Überwachungsgesetz, welches die Rechte und Freiheiten der betroffenen Personen erheblich einschränken können. Daher soll ein eigenes Regelwerk geschaffen werden, welches verbindliche Garantien beinhaltet, die den Datenzugriff durch US-Geheimdienste und Nachrichtendienste beschränken. Zusätzlich werden Verfahren etabliert, die eine wirksame Überwachung der neuen Datenschutzrechte überhaupt ermöglichen. Und im Fall der Fälle soll das neue zweistufige Rechtsbehelfssystem zur Untersuchung und Beilegung von Beschwerden europäischer Betroffener bei Datenzugriffen durch Geheimdienste bereitstehen. Ein extra Datenschutzüberprüfungsgericht – der Data Protection Review Court – wird geschaffen.

Begriff	Definition
Datentransfer	Übermittlung von personenbezogenen Daten in Drittländer. Der Datenexporteur übermittelt die Daten an den Datenimporteur im Drittland.
Drittland	Land, das kein Mitglied der europäischen Union ist und nicht dem europäischen Wirtschaftsraum angehört.
Europäischer Wirtschaftsraum (EWR)	Freihandelszone, die die Europäische Union aktuell mit Island, Liechtenstein und Norwegen umfasst. EWR-weit gelten die vier Grundfreiheiten der Waren-, Dienstleistungs-, Personen- und Kapitalverkehrsfreiheit. Weiterhin gilt das EU-Sekundärrecht in Form von Verordnungen, Richtlinien, und Beschlüssen. Dies umfasst auch die DSGVO.
Angemessenheitsbeschluss	Die Angemessenheit des Datenschutzniveau in einem bestimmten Drittland kann die EU-Kommission gem. Art. 45 Abs. 3 DSGVO in einem Beschluss feststellen. Dann dürfen personenbezogene Daten im Rahmen der DSGVO wie innereuropäische Übermittlungen ohne weitere Genehmigungen in das jeweilige Land transferiert werden.

Positive Nachrichten aus dem Weißen Haus

Alles hängt jedoch von der Umsetzung der notwendigen Änderungen durch Executive Orders des Präsidenten ab. Ein Verbot durch ein amerikanisches Gesetz oder durch einen verbindlichen Vertrag, wie von der EU anvisiert, wollen die USA nicht umsetzen. Datenschutzgruppen wie um Max Schrems kündigten bereits eine genaue Prüfung der Regularien an.

Am 7. Oktober gab es erfreuliche Nachrichten aus dem Weißen Haus: Präsident Biden hat die vereinbarte Executive Order erlassen. Nun bleibt die Bewertung durch die Europäische Kommission abzuwarten. Sollten alle Kritikpunkte aus der Vergangenheit an der Rechtslage vor Ort damit ausgeräumt sein, ist als nächster Schritt ein Angemessenheitsbeschluss zu erwarten. Dieser brächte Rechtssicherheit für Datenexporte in die USA in der Zusammenarbeit mit Unternehmen, die sich dem TADPF unterwerfen. Ob dieser Angemessenheitsbeschluss dem zu erwartenden Angriff durch Datenschutzaktivisten vor den Gerichten standhält, bleibt abzuwarten. &



Den Zugriff auf die sensiblen Daten vernageln

Wie Single Sign On und Mehrfaktor-Authentisierung Ihre Anwendungen schützen.

Von Matthias Niedung

Fast täglich spielen sich Szenearien wie die folgenden ab, deren Auswirkungen so gravierend sind, dass deren Behebung Tage, wenn nicht sogar Wochen beansprucht.

Montagnachmittag, die Arbeit ist erledigt, der Tag war anstrengend und plötzlich kommt da eine E-Mail. Irgendeine Anmeldung hat nicht funktioniert, beschreibt die nahezu perfekt aussehende E-Mail von Microsoft. Darin ein Link, in welchem auf eine Datei in Ihrem SharePoint verwiesen wird. Sie möchten dies vor Feierabend unbedingt noch abarbeiten. Sie klicken auf den angegebenen Link, geben Ihre Zugangsdaten zu Microsoft ein und gelangen an die Datei. Doch was Sie nicht sahen, es war gar nicht die Original-Seite von Microsoft, sondern Angreifende jubelten Ihnen ein perfektes Abbild des Originals unter. Sie machen also Feierabend und die Tage vergehen.

Im Herbst dann die böse Überraschung. In der Nacht wurden tausende E-Mails über Ihren Mail-Server versandt und gleichzeitig wurden die verlorenen Zugangsdaten auch noch am unternehmenseigenen Dokumentationssystem ausprobiert. Natürlich ein Volltreffer und die Angreifenden kopierten erst die Daten und löschten diese dann von den Systemen. Fortan hat Ihre IT wochenlang damit zu tun, die möglichen Angriffsvektoren zu identifizieren, den Angriff nachzustellen, potenzielle Sicherheitslücken zu schließen und den Zustand vor dem Angriff wiederherzustellen.

Mehrfaktor-Authentisierung als gewinnbringende Maßnahme

Um es vorwegzunehmen, Mehrfaktor-Authentisierung wird je nach Wirkungskreis auch 2-Faktor-Authentifizierung, Multi-Faktor-Authentisierung oder einfach nur MFA genannt und meint im Großen und Ganzen dasselbe. Den Schutz des Login-Prozesses mit weiteren Maßnahmen und Faktoren. Doch wie funktionieren Anwendungen eigentlich und weshalb sind mehrere Faktoren sinnvoll?

„Das Prinzip des Logins besagt einfach nur: Geben Sie mir einen Namen und ein ‚geheimes' Passwort. Wenn dies stimmt, dürfen Sie hinein."

Sehen wir uns den obigen Fall noch einmal genauer an. Sie haben an irgendeiner Stelle Ihre Zugangsdaten eingegeben und fortan können jene, die diese erbeuteten, sich an allen Diensten und Services, in welchen diese Zugangsdaten hinterlegt sind,anmelden. Denn das Prinzip des Logins besagt einfach nur: Geben Sie mir einen Namen und ein „geheimes" Passwort und wenn dies stimmt, dürfen Sie hinein.

Doch stellen Sie sich das im analogen Leben vor. Irgendjemand geht in die Bank, hat vorher Ihr Portemonnaie entwendet, geht an den Schalter und die Angestellte händigt alles Geld von Ihrem Konto aus, weil derjenige am Schalter einfach nur im Besitz Ihrer EC-Karte ist. Hier würde die Angestellte vermutlich spätestens beim Blick auf den Ausweis feststellen, dass derjenige, der den Ausweis vorzeigt nicht derjenige ist, dem das Konto gehört und die Sichtkontrolle würde Sie schützen. Da die Sichtkontrolle in der digitalen Welt nur bedingt Sinn ergibt, mussten sich die Entwickelnden anderweitig Möglichkeiten einfallen lassen, um sicherzustellen, dass jene Person, welche die Zugangsdaten anwendet, auch jene Person ist, die sich authentisieren darf.

In diesem Zuge kamen findige Entwickler auf die Idee, Dinge einzubeziehen, die direkt der Person zugehörig sind und an welche Angreifende nicht ohne erheblichen Aufwand gelangen. Neben Smartcards, USB-Dongles oder USB-Sticks haben sich vor allem Smartphones als guter, einfacher Faktor bewährt. Dabei ist das Prinzip so einfach, wie auch brillant.

Neben Ihrem Nutzernamen und dem Passwort müssen Sie im Login-Prozess meist mit einem Gerät, welches nur Sie im Besitz haben, zusätzlich nachweisen, dass Sie auch jene Person sind, die Sie vorgeben zu sein. Ob eine auf das Handy übersandte SMS mit einem PIN, ein Token in der Multi-Faktor-App oder ein persönlicher USB-Dongle - der Aufwand für einen potenziellen Angreifenden an diese Faktoren zu kommen ist schier unrentabel und damit meist ausgeschlossen.

Single-Sign-On – Fluch oder Segen?

Nicht ganz so einfach ist es, dem Single-Sign-On die selbigen schützenden Eigenschaften zuzuschreiben. Denn und das erklärt sich von allein, wenn ein Login den Zugang zu allen Applikationen ermöglicht, erhöht dies das Risiko eines möglichen Schadens überproportional.

Dabei ist es notwendig zu verstehen, wie das Single-Sign-On prinzipiell funktioniert. Mit SSO wird eine zentrale Anmeldung ermöglicht und einzelne Anwendungen fragen bei dieser an, ob der Benutzende erstens existiert und dieser Zugriff auf die Anwendung erhalten darf. Zudem wird abgeglichen, ob die Zugangsdaten richtig sind und erst dann wird der Zugriff auf die Anwendung oder den Dienst gewährt. Fortan kommunizieren die Dienste dann über ausgestellte Tokens und Sessions und ermöglichen so einen autorisierten Zugang zu den Daten und Informationen. Während es natürlich von Vorteil ist, nur ein System zu betreiben, in welchem Zugangsdaten vorliegen, hat dieser Prozess natürlich auch einige Risiken implementiert.

Wer also Single-Sign-On einplant, umsetzt und zur Nutzung durch die Benutzenden anbietet, sollte gerade beim Single-Sign-On sowohl die Chancen, als auch die Risiken genau betrachten und entsprechende Maßnahmen zum Schutz des Single-Sign-On erarbeiten und implementieren. Hierbei sind folgende Fragen zu betrachten und durch professionelle Unterstützung zu überprüfen:

- Wird das Single-Sign-On-System sicher betrieben?
- Nutzen Sie hierfür ein Standard-Produkt oder ist dies eine Eigenentwicklung?
- Sind die Rechte und Befugnisse tatsächlich und sinnvoll hinterlegt?
- Wird das System gepflegt?
- Haben Sie weitere Schutzmaßnahmen wie MFA eingebunden?
- Kommunizieren die Dienste auch richtig und wie vom SSO vorgesehen?
- Gibt es geregelte On- und Offboarding-Prozesse?

Fazit

Während sich also die Mehrfaktor-Authentisierung zumeist schnell und wirksam auf die Sicherheit Ihrer Daten auswirkt, ist beim Single-Sign-On der gewünschte Effekt erst zu erreichen, wenn dieser durch entsprechende zusätzliche Maßnahmen angereichert wird. Dabei ist aber zu betrachten, dass eine gepflegte und professionell eingesetzte Lösung auch hier den Sicherheitseffekt für Ihre Daten entsprechend erhöhen kann. Richtig implementiert können die beiden vorgestellten Lösungen gegen zahlreiche Angriffe effizient schützen und ein Blick auf die Einführung lohnt sich somit allemal. &

Brauchen Sie Hilfe?

Natürlich stehen wir Ihnen bei Althammer & Kill auch hier beratend zur Seite und unterstützen Sie bei der Einführung genannter Möglichkeiten.

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

Cloud- & Cyber-Security

DSGVO und Geschäftsführerhaftung

Bußgelder und Schadensersatzpflichten, die sich aus der DSGVO begründen, können ein hohes Risiko für eine Organisation darstellen. Das Fehlen eines Datenschutz- bzw. Compliance-Management-System kann zu einer persönlichen Haftung der Geschäftsführung führen.

Von Simon Lang und Christian Klande

Können Geschäftsführungen persönlich haftbar gemacht werden, wenn die Organisation durch einen Datenschutzverstoß Bußgelder oder Schadensersatz zahlen muss? Den Urteilen der OLG Dresden (Az. 4 U 1158/21) und Nürnberg (Az.: 12 U 1520/19) zu schlussfolgern, muss man diese Frage wohl mit „Ja!“ beantworten.

Hinweis: Die Nachfolgenden Informationen beziehen sich gleichermaßen auf die Datenschutz-Grundverordnung wie auch auf kirchliche Datenschutzgesetze wie z. B. dem Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (DSG-EKD) und dem Katholischen bzw. Kirchlichen Datenschutz (KDG).

Begründung

Sofern Geschäftsführerinnen und Geschäftsführer ihrer Aufsichtspflicht verletzen oder ihre Organisation nicht gesetzeskonform organisieren, haften sie unter Umständen persönlich für Bußgelder oder Schadensersatz, die gegen die Organisation ausgesprochen werden. Dies ergibt sich, neben den oben aufgeführten Urteilen der Oberlandesgerichte, unter anderem auch aus dem GmbHG (§ 43) sowie dem AktG (§ 93). Beide Gesetze verlangen von der Geschäftsführung oder dem Vorstand, dass sie ihrer Aufgaben sorgfältig und gewissenhaft nachkommen. Es besteht Ausstrahlungskraft auf andere Rechtsformen wie Vereine und Stiftungen.

Zu den Aufgaben zählt u.a. die Einhaltung datenschutzrechtlicher Vorgaben, die sich aus der DSGVO, dem BDSG und weiterer spezifischer Datenschutzgesetze ergeben. Werden diese Vorgaben missachtet oder nicht in einem „sorgfältigen“ und „gewissenhaften“ Maße nachgekommen, können Bußgelder oder Schadensersatzansprüche (z. B. ausgelöst durch fehlende Dokumentationen, rechtswidriger Verarbeitungen oder Datenpannen) auf die Geschäftsführung oder den Vorstand abgewälzt werden – mit entsprechendem persönlichen (unbegrenztem) Haftungsrisiko. D&O-Versicherungen springen oftmals nur ein, solange keine grobe Fahrlässigkeit oder Vorsatz vorliegt.

Die Rolle des Datenschutzbeauftragten

Wie sieht oben aufgeführter Sachverhalt jedoch aus, wenn ein/e Datenschutzbeauftragte/r durch das Management bestellt wurde? Die Antwort lautet: Es kommt darauf an. Zu unterscheiden ist, ob die Rolle des Datenschutzbeauftragten durch einen internen Mitarbeitenden ausgefüllt wird, oder ob hierzu ein externes Beratungsunternehmen beauftragt wurde.

Externer Datenschutzbeauftragter: Wenn der Datenschutzbeauftragte durch ein externes (Beratungs-) Unternehmen gestellt wird, geschieht dies auf Grundlage eines Vertrages. Kommt es zu nicht ausreichender oder falscher Beratung, haftet das Beratungsunternehmen für Beratungsfehler bereits bei leichter Fahrlässigkeit. Jedoch besteht seitens der Geschäftsleitung des zu beratenden Unternehmens eine Mitwirkungspflicht. Werden Ratschläge des externen Datenschutzbeauftragten nicht angenommen oder dieser nicht in wichtige und datenschutzrelevante Fragestellungen eingebunden, dreht sich der Spieß wieder um. Daher ist es wichtig den externen Datenschutzbeauftragten nicht als „Feigenblatt“ zu verstehen. Im Zweifel schützt dieses Feigenblatt nicht vor Strafe, wenn eine konstruktive Zusammenarbeit nicht angenommen wird.

Interner Datenschutzbeauftragter: Ist ein interner Datenschutzbeauftragter bestellt, haftet dieser, wie alle anderen Mitarbeitenden des Unternehmens, nach den Regeln des innerbetrieblichen Schadensausgleichs nicht für leichte Fahrlässigkeit und bei mittlerer und grober Fahrlässigkeit in der Regel nur anteilig. Bei Vorsatz, also einem willentlichen Pflichtverstoß, besteht alleinige und volle Haftung.

Haftung vermeiden

Wenn keine „sorgfältige“ und „gewissenhafte“ Datenschutzorganisation existiert, besteht die Gefahr der persönlichen Haftung. Was ist also zu tun, um diese Haftung zu vermeiden? Kurz gesagt: den Datenschutz so organisieren, dass es zu keinem Bußgeld und keinem Schadensersatzanspruch kommen kann. Dies beinhaltet u.a.:

1. Bestellung eines juristisch und technisch versierten Datenschutzbeauftragten – spätestens, wenn mindestens 20 Mitarbeitende in der Organisation ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind, wird die Bestellung zur Pflicht. Hierbei zählen die Köpfe, nicht die Vollzeitstellen.
2. Die Beratung des Datenschutzbeauftragten ernstnehmen und entsprechend gewissenhaft umsetzen. Der Datenschutzbeauftragte sollte bei allen Fragestellungen rund um die Verarbeitung personenbezogener Daten einbezogen werden. Das gilt insbesondere auch, wenn neue IT-Systeme eingeführt werden sollen (bspw. bei einem Wechsel von OnPremise- zu Cloud-Diensten).
3. Regelmäßige Schulung aller Mitarbeitenden zu datenschutzrechtlichen und informationssicherheitstechnischen Aspekten im Kontext ihrer Arbeit.
4. Anforderungen der Datenschutz-Grundverordnung umsetzen und die verantwortlichen Personen (z. B. Datenschutzbeauftragter, Prozessverantwortliche, IT-Verantwortliche usw.) mit den dafür notwendigen Kompetenzen und Zeiten ausstatten. Hierzu zählen insbesondere die Dokumentationspflichten, die sich aus der Datenschutz-Grundverordnung ergeben wie z. B.:
   - Erstellung und Führung eines vollständigen Verzeichnisses von Verarbeitungstätigkeiten.
   - Auswahl und Dokumentation geeigneter technischer und organisatorischer Maßnahmen.
   - Einhaltung der Rechte betroffener Personen aus Kapitel 3 DSGVO (Informationspflichten, Auskunft, Berichtigung, Löschung, Datenübertragbarkeit usw.). Dies betrifft insbesondere auch die Fristwahrung etwaiger Betroffenenrechte.
5. Datenschutzkonforme Organisation bzgl. der Einbindung von Auftragsverarbeitenden, die im Auftrag der Organisation personenbezogene Daten verarbeiten:
   - Abschluss von Verträgen zur Auftragsverarbeitung.
   - Ggfs. Abschluss von Standardvertragsklauseln, wenn personenbezogene Daten außerhalb der EU bzw. des EWR übermittelt werden.
   - Prüfung der technischen und organisatorischen Maßnahmen des Dienstleisters.
   - Ggfs. Vereinbarung weiterer Schutzmaßnahmen, wenn der außereuropäische Dienstleister Gesetzen im Heimatland unterliegt, die mit der Datenschutz-Grundverordnung nicht vereinbar sind.

Geschäftsführinnen, Geschäftsführer und Vorstände sind gut beraten, datenschutzkonforme Prozesse sogfältig und gewissenhaft zu implementieren und nachweisen zu können. So kann eine eventuelle persönliche Haftung abgewendet werden. Schöner Nebeneffekt: Durch datenschutzkonforme Prozesse können gleichzeitig auch Bußgelder und Schadensersatzansprüche gegen die Organisation abgewendet werden. Die Einhaltung des Datenschutzes liegt somit im gesamtorganisatorischen Interesse – nicht nur im Interesse einzelner Stakeholder. &

Wo gehobelt wird, da fallen Späne.

Oder: Wo Digitalisierung stattfindet, braucht es Software-Entwickler.

Marian wartet Systeme, programmiert Anwendungen und hilft Kollegen, wenn es mit „Aus- und wieder Anschalten“ nicht funktioniert.

Was genau machst du bei Althammer & Kill bzw. LearnBase?

Marian: Angefangen habe ich als „purer“ Software-Entwickler bei Althammer & Kill und habe das Verwaltungsportal sowie das alte E-Learning-Portal von Althammer & Kill programmiert. Später habe ich dann das Grundgerüst für LearnBase (E-Learning „Version 2“) gebaut, was ich jetzt aber größtenteils abgegeben habe an die Programmierer von LearnBase. Des Weiteren habe ich immer mal wieder bei Pen-Tests und Code-Review-Projekten mitgeholfen, da ich mit der technischen Seite sehr vertraut bin.

Darüber hinaus verwalte ich die Server- und IT-Infrastruktur und bin somit quasi auch Systemadministrator. Seit neustem mache ich auch Seminare/Webinare zu Programmierthemen.

Was studierst du?

Marian: Ich mache momentan meinen Bachelor in Informatik an der Leibniz Uni Hannover und schreibe nächstes Semester meine Abschlussarbeit.

Wie sieht dein Alltag bei Althammer & Kill und LearnBase aus?

Marian: Kommt darauf an, was momentan alles anliegt. Ich bearbeite meistens erstmal Bug-Reports und Support-Tickets von Kollegen. Wenn gerade nichts los ist, programmiere ich in der Regel am aktuellen Projekt weiter oder bin mit der Wartung unserer Server beschäftigt.

Welche Anfragen bekommst du von Kolleginnen und Kollegen am häufigsten?

Marian: Am häufigsten melden sich Kollegen bei mir, wenn irgendetwas nicht läuft – sei es einer unserer Server-/Web-Anwendungen, oder es gibt einen Fehler in einer von mir programmierten Anwendung. Darüber hinaus werde ich auch oft von den anderen Entwicklern um Rat gebeten, da ich recht viel Erfahrung bei vielen Programmierthemen habe.

Wie schaffst du es, Studium, Arbeit und Privatleben unter einen Hut zu bekommen?

Marian: Ich arbeite nur Teilzeit bei Althammer & Kill und lasse mir beim Studium auch etwas mehr Zeit als von der Regelstudienzeit vorgesehen ist, sodass am Ende eine ganz gute Balance zwischen Studium, Arbeit und Privatem entsteht. Des Weiteren kann ich auch viel von zu Hause arbeiten, sodass ich vergleichsweise wenig Reisezeit habe.

Inwiefern hat dich die Pandemie in deinem Studium und deiner Arbeit eingeschränkt?

Marian: Da ich größtenteils mit Computern und Servern zu tun habe, hielten sich die Einschränkungen für meine Kerntätigkeiten ziemlich im Rahmen. Nur Meetings fanden nun meistens online statt, aber das machte mir nicht viel aus. Ich habe bereits vor der Pandemie hauptsächlich im Home-Office gearbeitet, sodass dies für mich keine riesige Umstellung war.

Was willst du nach deinem Studium machen? Was wäre dein Traumjob?

Marian: Ich würde gerne weiterhin Software entwickeln, am liebsten interaktive Sachen an denen Leute Spaß haben, wie z. B. gute Web-Anwendungen oder Videospiele. IT-Sicherheit liegt mir aber ebenfalls am Herzen, insofern könnte ich mir auch gut vorstellen, weiterhin Code-Reviews und Pen-Tests durchzuführen.

Welche Module im Studium findest du am spannendsten und wie kannst du die Erkenntnisse, die du daraus gewinnst in deiner Arbeit umsetzen?

Marian: Die Veranstaltungen, die mir am besten gefallen haben, waren zum einen „White-Hat-Hacking“, wo es darum ging das „hacken“ zu lernen, indem man wöchentliche Herausforderungen bewältigt, und „Betriebssystembau“, wo man ein eigenes Betriebssystem programmieren konnte, welches dann auf einem echten, handelsüblichen Laptop lief. Ersteres hilft ganz klar bei Pen-Tests, aber auch bei der Serveradministration, da man lernt worauf man zu achten hat, um möglichst sicher unterwegs zu sein. Letzteres ist eher eine Sache, die ich persönlich sehr spannend finde.

Welche Arbeit findest du spannender, die für LearnBase oder für Althammer & Kill und wieso?

Marian: Da ich eigentlich überwiegend mit Althammer & Kill zu tun habe, würde ich spontan auch Althammer & Kill sagen. Am interessantesten finde ich dort Code-Reviews, da man dort einen Einblick bekommt, wie es um die Sicherheit von Apps, die wir im alltäglichen Leben antreffen steht – und ich kann natürlich auch meinen Beitrag leisten, diese für alle sicherer zu machen.

Stichwort
Code-Review

Keine Software ist frei von Fehlern oder Mängeln. Um diese zu finden und damit die Qualität der Software zu verbessern, werden Code-Reviews durchgeführt.

Ein Code-Review ist somit eine planvolle Untersuchung von Quellcode.

Meta und seine Dienste – wer hat unsere Daten?

Spätestens seit dem Cambridge-Analytica-Skandal 2018 hätten die User der Plattform Facebook hellhörig werden müssen. Damals wurden die Daten von Millionen Facebook-Usern für ein politisches Microtargeting genutzt, um die US-Wahl im Jahre 2018 auf ein politisches Meinungsbild zu lenken.

So führte Donald Trump seinen Onlinewahlkampf und konnte damit höchstwahrscheinlich das Wahlverhalten der Wählenden beeinflussen. Auch das Brexit-Referendum 2016 wurde durch intensives Microtargeting begleitet.

Beide Wahlergebnisse wurden durch eine Auswertung der Nutzerprofile auf der Plattform Facebook beeinflusst – beim Brexit-Referendum mit Hilfe des kanadischen Technologieunternehmens „AggregateIQ", welches auch mit CA zusammenarbeitete. Übrigens völlig legal.

Personenbezogene Daten sind also wichtig – nicht nur individuell, sondern auch gesellschaftlich. Das macht sie umso interessanter für Missbrauch und die Konzerne, deren Geschäftsmodell auf der Akkumulation und Weitergabe von Daten basiert, zu einem lohnenden Ziel für Hacker.

Meta ist ein US-amerikanisches Technologieunternehmen, dem unter anderem die Plattformen Instagram, Facebook und Messengerdienste wie WhatsApp und der Facebook-Messenger gehören. Im Jahr 2021 kam es zu einen großen Datenleck: Die Daten von über einer halben Milliarde Usern wurden in einem Hacker-Forum veröffentlicht – darunter auch 6 Millionen User aus Deutschland. Diese Daten waren personenbezogen.

Wie konnten diese Daten ausgespäht werden?

Bis 2018 war es bei Facebook möglich, durch die Eingabe einer Telefonnummer oder einer E-Mail-Adresse das Profil des zugehörigen Users zu finden – wahrscheinlich hat jemand einfach Telefonnummern „durchprobiert" und so die Daten zusammengetragen. Es kann aber auch ganz anders gewesen sein, denn Facebook schweigt sich über die Schwachstelle aus und ließ lediglich verlautbaren, dass die Lücke geschlossen worden sei.

Gegen Facebook ist in Folge ein Urteil vor dem Landgericht Zwickau wegen Verstoßes gegen die Datenschutz-Grundverordnung (DSGVO) ergangen. Das Unternehmen muss nach einem Versäumnisurteil 1000 Euro Schadenersatz an einen Betroffenen zahlen (Urteil vom 14. September 2022, Az.: 7 O 334/22).

Wie können Sie verhindern, dass alle Ihre Daten an die Anbieter einer Applikation übermittelt werden?

Je weniger Sie Ihre personenbezogenen Daten streuen, desto geringer ist die Wahrscheinlichkeit, von einer Datenpanne betroffen zu werden. Deshalb ist es ratsam, Datenübertragungen zu minimieren. Dazu sollten Sie wie folgt vorgehen:

1. Übernehmen Sie keine automatisch voreingestellten Einstellungen – nehmen Sie die Einstellungen manuell vor.
2. Prüfen Sie zudem in den Einstellungen der Applikation auf Ihrem Endgerät, welche Rechte Sie vergeben müssen, um die Applikationen nutzen zu können – sie können diese auch nachträglich wieder entziehen.
3. Bei Facebook können Sie zusätzlich in Ihrem User-Konto einsehen, worauf die Plattform Zugriff hat und diesen ggfs. beschränken. &

Veranstaltungen und Termine

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

Hier klicken oder scannen!

18. Januar 2023 – Webinar

Das Hinweisgebersystem von Althammer & Kill

Ohne Edward Snowden wüssten wir wohl bis heute nicht um die Methoden der amerikanischen Geheimdienste. Er war mutig und hat sich getraut, Missstände öffentlich zu machen – er war der Hinweisgeber. Durch die EU-Whistleblower Richtlinie müssen Systeme eingerichtet werden, die Hinweisgebern wie Edward Snowden erlauben, offen zu sprechen und dabei Anonymität zu bewahren. Die Rede ist von Hinweisgebersystemen.

Die Pflicht zur Einrichtung von internen Meldestellen gilt, stufenweise, für Beschäftigungsgeber und Organisationseinheiten mit jeweils in der Regel mindestens 50 Beschäftigten. Es ist damit zu rechnen, dass Unternehmen mit in der Regel mehr als 249 Beschäftigten die internen Meldestellen, auch aufgrund des von der EU-Kommission eingeleiteten Vertragsverletzungsverfahren, noch im Jahr 2022 eingerichtet haben müssen. 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.

8.–9. Februar 2023 – 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.

Am Ende des Seminars haben Sie die Möglichkeit, an einer Prüfung mit dem Zertifikatsabschluss „Datenschutzkoordinator/in" teilzunehmen. Dieses Zertifikat dokumentiert Ihre Datenschutzkompetenz gegenüber der Aufsichtsbehörde, Vorgesetzten, Geschäftspartnern und Mitarbeitenden Ihrer Organisation.

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

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
P7 20 · 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