COMPLIANCE konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 4/2023

Erpressung von 1,5 Millionen Euro Lösegeld

Lehren aus einer Cyber-Attacke
Seite 6

345 Millionen Euro Strafe gegen TikTok
Die nächste Sanktion
Seite 10

Cybersicherheit im Unternehmen
Das bringt NIS-2 mit sich
Seite 12

Der Digital Services Act
das „Grundgesetz für das Digitalzeitalter“
Seite 16

News
Seite 4

Erpressung von 1,5 Millionen Euro Lösegeld
Lehren aus einer Cyber-Attacke
Seite 6

345 Millionen Euro Strafe gegen TikTok
Die nächste Sanktion für die Plattform
Seite 10

Cybersicherheit im Unternehmen
Das bringt NIS-2 mit sich
Seite 12

Die Menschen hinter Althammer & Kill
Seite 14

Akademie
Seite 15

Der Digital Services Act
das „Grundgesetz für das Digitalzeitalter"
Seite 16

Über die Schulter geschaut
Seite 18

Editorial

Liebe Leserin, lieber Leser,

was passiert, wenn's passiert ist? Bei einem Cybervorfall bleiben oft nur Stunden, um die richtigen Entscheidungen zu treffen. Die Diakonie Stiftung Salem in Minden wurde 2022 auf 1,5 Millionen Euro erpresst. Der kaufmännische Vorstand, Christian Schultz, berichtet mit viel Offenheit im Interview, wie es zum Cyber-GAU kam und welche Folgen es hat, wenn 3 Millionen Dateien verschlüsselt werden.

Zur Erhöhung der Cybersicherheit in kritischer Infrastruktur trat die europäische NIS-2-Richtlinie in Kraft und muss bis Oktober 2024 in deutsches Recht umgesetzt werden. Mit dem zweiten Referentenentwurf liegen nun konkrete Anforderungen vor, die einige Organisationen vor Umstrukturierungen stellen werden. Wir legen dar, was Sie wissen müssen.

Ab dem Dezember ist die Einrichtung eines Hinweisgebersystems nun auch für Organisationen ab 50 Mitarbeitenden verpflichtend. Dies bringt nicht nur die Einrichtung einer Meldestelle, sondern auch die Schulung des benötigten Personals mit sich. Mehr zur Weiterbildung als Meldestellenbeauftragte/r oder zur Ombudsperson finden Sie in unserem Beileger.

Wie geht es 2024 weiter?

Wir haben etwas zu feiern, denn Althammer & Kill wird im kommenden Jahr 10 Jahre alt! Wir freuen uns über 10 Jahre guter Zusammenarbeit, des Lernens und der Weiterentwicklung. Dafür möchten wir uns bei Ihnen, unseren Kundinnen, Kunden und Partnern sehr herzlich bedanken.

Wir freuen uns auf den anhaltenden Diskurs mit Ihnen – auch im neuen Jahr. Ein gesegnetes Weihnachtsfest und einen guten Start in das Jahr 2024 wünschen

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*

Fachtagung für Datenschutz und Informationssicherheit – ein Rückblick

50 externe Teilnehmende, sechs externe Referierende, 12 Mitarbeitende von Althammer & Kill und 14 Sponsoren und Medienpartner – das war unsere erste Fachtagung für Datenschutz und Informationssicherheit in der Sozialwirtschaft und Non-Profit-Organisationen.

Gibt es Nachfrage nach einer solchen Veranstaltung? Was interessiert die Personen in der Branche wirklich? Und welches Format müsste eine solche Tagung haben? Was Anfang des Jahres als Idee begann, setzten wir Ende August in die Tat um. Am 31. August und 1. September luden wir nach Paderborn ins Hotel Vivendi ein, um gemeinsam zu diskutieren, Fragen zu klären und uns besser zu vernetzen.

Die Veranstaltung startete, nach einer kurzen Begrüßung von Thomas Althammer & Niels Kill, mit einem Experten-Panel bestehend aus Barbara Thiel (Landesbeauftragte für Datenschutz Niedersachsen a. D.), Erik Kahnt (Stellvertreter des Datenschutzbeauftragten für Kirche und Diakonie für Sachsen, Thüringen und Sachsen-Anhalt) und Christian Schulz (kaufm. Vorstand und Geschäftsführer der Diakonie Stiftung Salem gGmbH). Das Besondere hierbei? Die Teilnehmenden konnten zuvor Fragen notieren, die durch Thomas Althammer als Moderator gestellt wurden. Nach intensiver Diskussion der Referierenden untereinander ging es in die Pause und damit zum Empfang und Abendessen, welches durch die Dinnerspeech zum Thema „KI, Potentiale und Ethik“ von Dr. Christian Geyer abgerundet wurde.

Dem langen Abend voller intensiver Gespräche folgten zwei Vorträge von Joerg Heidrich und Thomas Althammer zum Thema KI, einmal aus der rechtlichen Perspektive und einmal aus der Datenschutz-Perspektive. In den anschließenden Workshop-Tracks hatten die Teilnehmenden die Wahl zwischen den Schwerpunkten Datenschutz und Informationssicherheit. Falls dort noch Fragen offengeblieben waren, konnten diese und weitere in einem der vier Barcamps zu verschiedenen Themen, die sich die Teilnehmenden vorab wünschen konnten, geklärt werden.

Den Abschluss bildete ein Impuls von Christian Klande zum Thema „Compliance mit dem Schwerpunkt des Hinweisgeberschutzgesetzes“. Wir bedanken uns bei allen Teilnehmenden, Sponsoren und Referierenden für eine gelungene Veranstaltung! Das positive Feedback freut uns und zeigt gleichzeitig, dass es eine Fortsetzung im kommenden Jahr geben sollte.

Zeit zum Geben

Wir haben uns für dieses Jahr eine andere Art des Schenkens überlegt: Jedes Team, sei es Beratung, Marketing oder auch Vertrieb, durfte sich einen Spendenzweck überlegen, der im Zuge des Weihnachtsfestes finanziell bedacht werden sollte. Bei der Wahl, welchem Zweck die 100 Euro pro Mitarbeitendem im Team zu Gute kommen, kam es zu interessanten Vorstellungen oder teilweilse sogar zum Stechen, bis man sich einigen konnte. Umso größer ist die Freude, dass unter anderem das Tierheim Wunstorf eine Spende erhalten wird.

Grundlagen zum datenschutzrechtlichen Löschkonzept

Vielen Organisationen fällt es schwer, Löschregeln für personenbezogene Daten festzulegen. Dadurch kann es zu Umsetzungsdefiziten bei den rechtlichen Löschvorgaben kommen. Bei der Erarbeitung eines Löschkonzepts handelt es sich um eine nicht einfache, aber elementare Aufgabe. Verantwortliche sollten dieses grundlegende Thema daher auch im eigenen Interesse nicht außer Acht lassen.

Zahl des Monats

72 %

der Befragten einer Studie in Kooperation mit dem TÜV-Verband gaben an, Angst vor Hacking-Angriffen zu haben, die auf der Basis von künstlicher Intelligenz automatisiert und personalisiert sind. Damit war dies die größte Sorge, die im Zusammenhang mit KI genannt wurde.

Das Lieferkettensorgfaltspflichtengesetz und seine Bedeutung für KMU

Am 1. Januar 2023 ist das Lieferkettensorgfaltspflichtengesetz (LkSG) in Kraft getreten. Seitdem gilt es zunächst für alle Unternehmen mit Sitz in Deutschland und mehr als 3.000 Mitarbeitenden. Ab dem 1. Januar 2024 sinkt die Schwelle auf 1.000 Mitarbeitende.

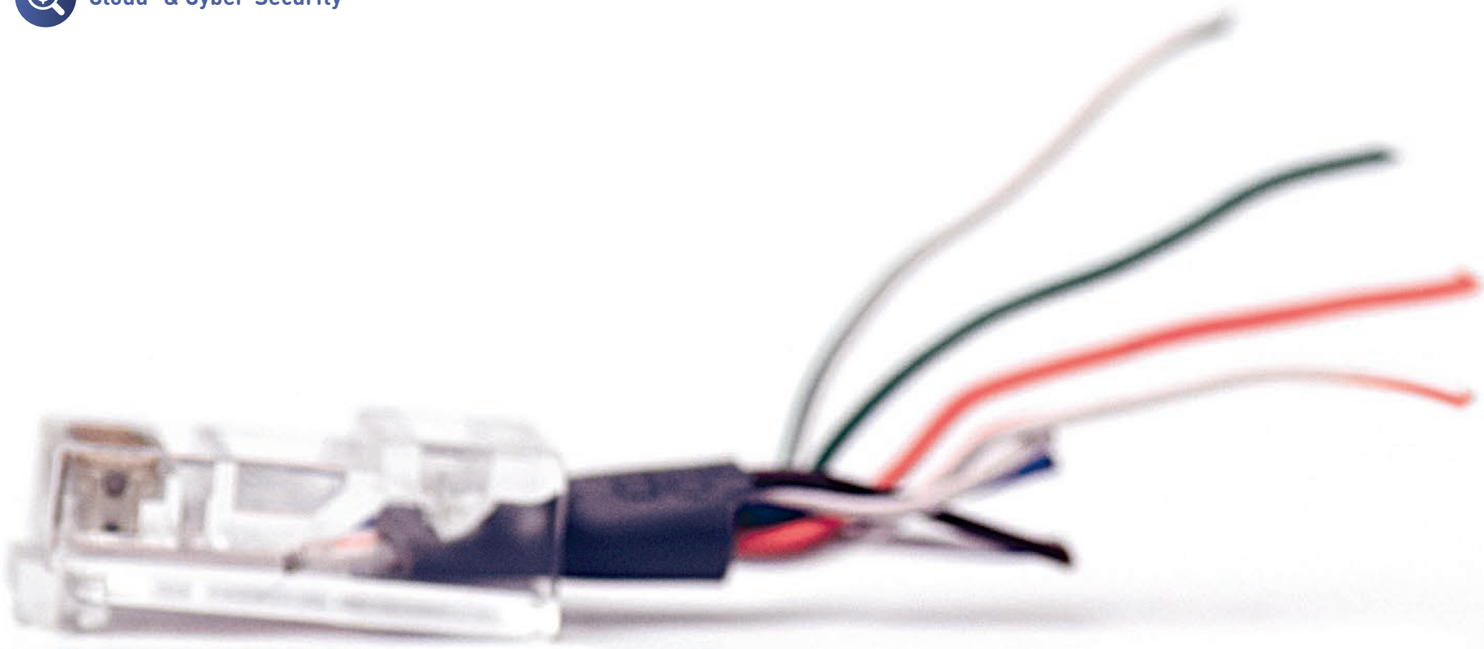
Beschäftigtendatenschutz – In Deutschland nichts Neues

Beschäftigtendaten sind ein besonderes Gut. Daher hat Deutschland als EU-Mitgliedsstaat von Art. 88 Abs. 1 DSGVO Gebrauch gemacht und mit § 26 BDSG eine „spezifischere Vorschrift(..) zur Gewährleistung des Schutzes der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext, insbesondere für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrages (...)“ geschaffen. Ob diese Vorschrift so spezifisch ist, soll in diesem Beitrag geklärt werden.

Die neue Version der Orientierungshilfe zum Hinweisgeberschutzgesetz

Nach den aktuellen Entwicklungen steht fest, dass Unternehmen mit 250 Mitarbeitenden eine Meldestelle gemäß des Hinweisgeberschutzgesetzes einrichten müssen. Für Unternehmen ab 50 Mitarbeitenden gilt eine Schonfrist bis zum 17.12.2023. In unserer neu aufgelegten Orientierungshilfe geben wir Ihnen das nötige Handwerkszeug, damit Sie die neue Richtlinie in Ihrer Organisation umsetzen können.

Jetzt hier kostenlos herunterladen:
https://www.althammer-kill.de/orientierungshilfe-hinweisgeberschutzsystems



Cloud- & Cyber-Security

Erpressung von 1,5 Millionen Euro Lösegeld: Lehren aus einer Cyber-Attacke

Im Interview schildert Christian Schultz die Folgen eines Cyber-Vorfalls im April 2022. Er ist kaufmännischer Vorstand bei der Diakonie Stiftung Salem, einem Sozialunternehmen mit rund 3.000 Mitarbeitenden.

Herr Schultz, Sie sind im April 2022 Opfer einer Cyber-Attacke der BlackCat-Gruppe geworden. Was ist damals passiert?

Christian Schultz: Der Angriff wurde durch den Diebstahl von Zugangsdaten zu einem uns unbekannten Zeitpunkt initiiert. Dies erfolgte wahrscheinlich über den kompromittierten Browser eines Mitarbeiters. Am 10.03.2022 führten die Angreifer einen Testzugriff unter Verwendung der gestohlenen Zugangsdaten durch. Der eigentliche Angriff erfolgte erst einige Tage später, am 16.03.2022:

- Auslesen der Domaininformationen, um Schwachstellen zu identifizieren.
- Suche nach und Entdecken von Sicherheitslücken im System.
- Abfischen von weiteren Zugangswegen, um die Angriffsfläche zu erweitern.
- Erfolgreiches Abfischen von NTLM-Hashes (verschlüsselte Passwörter von Benutzern)

Die Auswirkungen waren ca. 3 Mio. verschlüsselte Dateien und das Auslesen vieler Passwörter und Account-Daten. Doch zu dem Zeitpunkt haben wir zunächst nichts von den Angreifenden mitbekommen.

Was wollten die Angreifer von Ihnen?

Christian Schultz: Die Gruppierung, die hinter dem Angriff steckt, wird aufgrund identifizierter Artefakte als BlackCat oder ALPHV identifiziert. Trotz intensiver Ermittlungen konnten die Angreifer nicht belangt werden, und die Ermittlungen wurden eingestellt.

Es wurde festgestellt, dass unser Unternehmen nach den Ermittlungsergebnissen nicht das primäre Ziel des Angriffs war, sondern vielmehr als „Beifang" betrachtet wurde. Die Attacke zielte nicht auf Verwüstung oder Zerstörung ab, sondern auf die Verschlüsselung von Systemen, um uns zu erpressen. Nach dem Angriff wurde ein entsprechender Link ins Darknet entdeckt. Auf der verlinkten Seite wurde eine Forderung in Höhe von 1,5 Millionen Euro gestellt.

Haben Sie gezahlt?

Christian Schultz: Nein.

Wie sind Sie in der Bewältigung vorgegangen?

Christian Schultz: Den Angriff haben wir erst am 18.03.2022 am Vormittag bemerkt. In der Nacht zuvor wurden Passwörter geändert, die Datensicherung kompromittiert und mit der Verschlüsselung der Festplatten auf Servern und Clients begonnen. Ab 8 Uhr in der Früh hatten wir die ersten Probleme beim Zugriff auf die Systeme. Gegen 10:30 Uhr wussten wir, dass es sich um einen Cyberangriff handelt und eine Lösegeldforderung im Raum steht.

Als Sofortmaßnahmen versuchten wir, Dateien und Datenbanken auf externen Festplatten zu sichern, da das Backup von der Attacke betroffen war. Parallel erfolgte die Meldung des Datenschutzvorfalls bei Vorstand/DSB und Erstattung der Anzeige bei der Polizei. Alle noch laufenden Server und Systeme haben wir versucht zu isolieren und Passwörter zu ändern – darunter auch die Zugänge zu von uns genutzten Cloud-Diensten.

Im weiteren Verlauf haben wir schnell gemerkt, dass es nicht ohne externe Unterstützung geht. Dabei haben uns Beratungshäuser unterstützt, die auf die Aufarbeitung von Cyberangriffen spezialisiert sind. Mitarbeitende von Althammer & Kill waren in die Beratungen und Entscheidun-

Christian Schultz, kaufmännischer Vorstand bei der Diakonie Stiftung Salem

gen zum Wiederaufbau der Infrastruktur eingebunden.

Wichtig war die Offline-Schaltung aller Standorte und Außerbetriebnahme der E-Mail-Systeme, um den Angriff einzudämmen. Für die forensische Analyse wurden Systeme isoliert. Am 01.04.2022 fiel die Entscheidung für einen vollständigen Wiederaufbau mit einer neuen Server-Landschaft.

Wo gab es die größten Herausforderungen?

Christian Schultz: Die IT-Abteilung befand sich in einer Situation völliger Überforderung im Umgang mit dem Cyberangriff. Folgende Herausforderungen wurden identifiziert:

1. Fehlende Dokumentation: Es existierte keine ausreichende Dokumentation, was die Reaktion auf den Angriff erschwerte. Der Mangel an schriftlichen Protokollen und Ablaufbeschreibungen behinderte die Effizienz und Koordination bei den Rettungsversuchen.
2. Fehlende Konzepte für Cyberangriffe: Es lagen keine vordefinierten Konzepte oder Notfallpläne für den Umgang mit Cyberangriffen vor. Das Fehlen eines klaren Handlungsleitfadens erschwerte die adäquate Reaktion auf den Angriff und die Koordination der betroffenen Maßnahmen.
3. Personelle Belastung der IT-Abteilung: Die IT-Abteilung war personell angeschlagen, was zusätzlichen Druck und Erschwernisse bei der Bewältigung des Vorfalls mit sich brachte. Die begrenzten personellen Ressourcen könnten die Reaktionszeit beeinträchtigt haben.

„Wichtig war die Offline-Schaltung aller Standorte und Außerbetriebnahme der E-Mail-Systeme, um den Angriff einzudämmen."

Wir haben viel daraus gelernt. Die vorgehenden Schwierigkeiten bieten auch eine Chance zur Verbesserung der IT-Sicherheitsstruktur und zur Schaffung robusterer Maßnahmen zur Bewältigung von Cyberbedrohungen.

Wie lange hat der Notbetrieb angehalten, wann waren Sie wieder arbeitsfähig?

Christian Schultz: Der Zeitraum vom Notbetrieb bis zur vollständigen Arbeitsfähigkeit erstreckte sich grob über etwa 12 Monate. Allein die Grundstruktur war für ca. 1,5 Monate nicht verfügbar. Viele Menschen waren nur per Handy erreichbar und hatten über längere Zeit keinen Zugriff auf ihre E-Mails.

Während dieser Zeit wurde ein vollständig neues Betriebskonzept erstellt, das auf Sicherheit, Flexibilität und effizienter Verwaltung abzielte. Der Einsatz von Thin Clients wurde optimiert, wobei die Vorteile der einfacheren Administration, höheren Sicherheit und kostengünstigeren Wartung im Fokus standen.

Die Entscheidung für Mobile Devices wurde getroffen, um den Anforderungen an digitale Zusammenarbeit gerecht zu werden, insbesondere aufgrund der verstärkten Bereitstellung von Software als Web-Varianten.

Trotz der erfolgreichen Wiederherstellung bleiben Herausforderungen in Sachen IT-Sicherheit. Der kontinuierliche Fokus auf Schulungen und Ressourcen für Mitarbeitende ist entscheidend, um zukünftige Risiken zu minimieren.

Was hat Sie der Vorfall insgesamt gekostet?

Christian Schultz: Die Gesamtkosten für den Vorfall lassen sich nicht exakt beziffern, da der Vorfall einen bereits geplanten Investitionsbedarf beschleunigt hat. Es wird geschätzt, dass die Investitionen in Technologien, Dienstleistungen und den personellen Ausbau der IT-Abteilung in etwa im Bereich von 1,5 bis 2 Millionen Euro liegen.

Nicht eingerechnet sind Mehrarbeit und die mentale Belastung, die von den Kollegen der Diakonie geleistet und ertragen werden mussten. Das lässt sich monetär nicht quantifizieren. Diese immateriellen Kosten können erheblich sein und verdeutlichen, dass die Auswirkungen von Cyberangriffen weit über finanzielle Aspekte hinausgehen können.

Was haben Sie aus den Ereignissen gelernt und was geben Sie anderen Organisationen als Empfehlung mit?

Christian Schultz:

1. Verteilen Sie Investitionen angemessen und gezielt, ohne bei der IT-Sicherheit zu sparen.
2. Führen Sie regelmäßige Penetrationstests durch, um Schwachstellen in der IT-Infrastruktur zu identifizieren.
3. Schaffen Sie ein Bewusstsein für die zentrale Bedeutung der IT, denn ohne sie kommen Geschäftsprozesse zum Erliegen.
4. Testen Sie Wiederherstellungsszenarien, um die Wirksamkeit und insbesondere die Dauer für eine Wiederherstellung im Blick zu behalten.
5. Erstellen Sie einen Plan für Krisensituationen, der nicht nur IT-bezogene Probleme, sondern auch andere kritische Ereignisse abdeckt.
6. Implementieren Sie eine klare IT-Strategie, abgestimmt auf die langfristigen Ziele der Organisation und auf Grundlage einer umfassenden IT-Sicherheitsarchitektur.

Herr Schultz, viele Unternehmen scheuen den Weg in die Öffentlichkeit nach einem solchen Vorfall. Haben Sie vielen Dank für die offenen Worte! &

Impressum

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

Haftung und Nachdruck:
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit vorheriger Genehmigung der Althammer & Kill GmbH & Co. KG gestattet.

Schutzgebühr Print-Ausgabe: 5,– €

Gestaltung:
Designbüro Winternheimer, *winternheimer.net*

Fotos Mini-Figuren:
Katja Borchhardt, *miniansichten.de*

Anschrift:
Althammer & Kill GmbH & Co. KG
Roscherstraße 7 · 30161 Hannover
Tel. +49 511 330603-0
althammer-kill.de

345 Millionen Euro Strafe gegen TikTok

Die irische Datenschutzbehörde (DPC) verhängt eine Geldstrafe in Höhe von 345 Millionen Euro gegen die beliebte Social-Media-Plattform TikTok. Der Schwerpunkt der Untersuchung lag auf der Erhebung und Verarbeitung von Daten von Kindern und Jugendlichen.

Von Jessica Henning

TikTok ist eine chinesische Social-Media-Plattform, auf der Videos, wie etwa Lippensynchronisation von Musikvideos und andere kurze Clips (von Tipps und Tricks über Katzen- und Tanzvideos ist alles dabei), veröffentlicht werden. Im Januar 2023 zählte TikTok weltweit ca. 1,6 Milliarden Nutzende, von denen 1,1 Milliarden monatlich aktiv sind. Innerhalb dieser Nutzerschaft machen Personen im Alter von 10 bis 29 Jahren etwa 63 % aus.[1]

TikTok hat die Altersfreigabe in den Nutzungsrichtlinien der App auf 13 Jahre festgelegt, was bedeutet, dass sie für Kinder und Jugendlich ab diesem Alter gedacht ist. Im Google Play Store ist die USK-Altersfreigabe hingegen ab 12 Jahren festgelegt.

Das sind die Vorwürfe

Da sich ein Unternehmenssitz der Social-Media-Plattform in Irland befindet, steht TikTok auch unter der Aufsicht der irischen Datenschutzbehörde. TikTok ist schon in der Vergangenheit negativ bei anderen Datenschutzbehörden aufgefallen, was in Geldstrafen resultierte (z. B. von der niederländischen Datenschutzbehörde am 22. Juli 2021 mit einer Geldstrafe in Höhe von 750.000 Euro, wegen nicht ausreichenden Informationen gem. Art. 12 DSGVO).

Im September 2021 leitete die irische Datenschutzbehörde eine Untersuchung gegen die Tochtergesellschaft des chinesischen Unternehmens ByteDance ein. In der Untersuchung wurde der Zeitraum von Sommer bis Ende 2020 betrachtet. Dabei wurden Verstöße bei der Verarbeitung der Daten Minderjähriger festgestellt.

Obwohl TikToks Nutzungsrichtlinien eine Altersfreigabe ab 13 Jahren vorsehen, wurden im Prüfungszeitraum viele Videos von jüngeren Kindern gefunden. TikTok wurde vorgeworfen, bei der Altersüberprüfung nicht genau genug zu sein und die Risiken für Kinder unter 13 Jahren nicht ausreichend zu berücksichtigen. Dies steht im Widerspruch zu Erwägungsgrund 38 der DSGVO, der insbesondere einen Schutz bei der Erstellung von Nutzerprofilen fordert.

Darüber hinaus wurden Kinder durch Pop-up-Fenster ermutigt, ihre Beiträge „jetzt“ und „öffentlich“ zu posten. Wenn sie ihren Beitrag als „privat“ veröffentlichen wollten, mussten sie zuerst „Abbrechen“ wählen und anschließend die Datenschutzeinstellungen aufrufen.

Die Auswirkungen der verschiedenen Einstellungsoptionen waren unklar. Beiträge von Nutzenden im Alter von

13 bis 17 Jahren konnten grundsätzlich von jedem eingesehen werden. Zudem sei es auch bei Profilen von Minderjährigen so voreingestellt gewesen, dass jeder ihre Posts kommentieren konnte.

Ein weiterer Verstoß bestand darin, dass TikTok nicht den Grundsatz „Privacy by Default“ beachtete. Dieser Grundsatz verlangt, dass Apps, Software und andere Verarbeitungsvorgänge standardmäßig datenschutzfreundliche Einstellungen verwenden. Diesen Grundsatz hat TikTok nicht eingehalten.

Zudem bereitete die Einstellung „Familienverbindung“ Schwierigkeiten, da sie es ermöglichte, das TikTok-Konto von Minderjährigen mit dem eines Elternteils zu verknüpfen, ohne jedoch zu überprüfen, ob das verknüpfte Konto tatsächlich einem Angehörigen oder Vormund gehörte.

Die Folgen:

Am 1. September 2023 stellte die DPC fest, dass gegen folgende Artikel verstoßen wurde:
- Art. 5 Abs. 1 lit. c DSGVO
- Art. 5 Abs. 1 lit. f DSGVO
- Art. 24 Abs. 1 DSGVO
- Art. 25 Abs. 1 DSGVO
- Art. 25 Abs. 2 DSGVO
- Art. 12 Abs. 1 DSGVO
- Art. 13 Abs. 1 lit. e DSGVO

Außerdem wurden folgende Korrekturbefugnisse ausgeübt:
- Ein Tadel
- Eine Anordnung, die TikTok verpflichtet, innerhalb von drei Monaten nach Mitteilung der Entscheidung, ihre Verarbeitung in Einklang mit der DSGVO zu bringen
- Eine Verwaltungsstrafe in Höhe von insgesamt 354 Millionen Euro.

Wie reagiert TikTok?

Ein Unternehmenssprecher äußerte, TikTok sei mit der Strafe an sich und insbesondere mit der Höhe der Geldbuße nicht einverstanden. Das Unternehmen betonte, dass sich die Untersuchungsergebnisse in erster Linie auf Einstellungen bezogen, die vor drei Jahren gültig waren. „Die meisten dieser Ergebnisse sind aufgrund von Maßnahmen, die wir bereits vor Beginn der Untersuchung eingeführt haben, nicht mehr relevant“, teilte das Unternehmen mit. Dazu gehört unter anderem die Standardisierung der Privatsphäre-Einstellungen auf „privat“ für alle Konten von Nutzenden unter 16 Jahren. Das Unternehmen prüft derzeit seine weiteren Schritte. Darüber hinaus wurden seit Anfang des Jahres rund 17 Millionen Konten gelöscht, da sie mutmaßlich Kindern unter 13 Jahren gehörten.

Aussicht

Es ist zu beobachten, dass immer mehr Länder Strafen gegen TikTok verhängen. Bereits im April dieses Jahres hatte die britische Datenschutzbehörde eine Geldstrafe in Höhe von 12,7 Millionen Pfund (entspricht etwa 14,78 Millionen Euro) gegen TikTok verhängt. Der Vorwurf lautete ebenfalls, dass TikTok im Jahr 2020 die Registrierung von bis zu 1,4 Millionen Kindern unter 13 Jahren zugelassen und deren Daten ohne Zustimmung ihrer Eltern verwendet hatte. Auch die Niederlande verhängte 2021 eine Geldstrafe in Höhe von 750.000 € sowie die USA 2019 in Höhe von 5,7 Millionen Dollar, weil die Verarbeitung der Daten von Kindern unzulässig und intransparent war.

Eine weitere Besorgnis besteht hinsichtlich des möglichen unbefugten Zugriffs chinesischer Behörden auf Nutzerdaten, ohne dass die Nutzenden darüber informiert sind. TikTok hat in diesem Zusammenhang das „Project Clover“ ins Leben gerufen, um das Vertrauen europäischer Nutzender zurückzugewinnen. Dieses Projekt soll sicherstellen, dass der Zugriff auf persönliche Daten europäischer Nutzender strikt geregelt und transparent ist. Hierfür sollen künftig Rechenzentren in Dublin und Norwegen eingesetzt werden.

...

[1] https://tridenstechnology.com/de/tiktok-nutzer-statistik/
[2] vgl. Erwägungsgrund 38 DSGVO

Stichwort
Schutzbedürftige Personen

Daten von Kindern und Jugendlich gelten im Datenschutzrecht als Daten von besonders schutzbedürftigen Personen. Das bedeutet, dass eine höherer Schutzbedarf beim Umgang mit den Daten besteht. Zudem sind Kindern die Risiken und Folgen sowie ihrer Rechte bei der Verarbeitung ihrer personenbezogenen Daten möglicherweise weniger bewusst.[2]

Cybersicherheit im Unternehmen – das bringt NIS-2 mit sich

NIS-2 steht für “Network und Information Security 2”, es ist die überarbeitete Version der Richtlinie NIS aus dem Jahre 2016. Ein im Mindeststandard einheitliches, EU-weites Sicherheitsniveau ist das Ziel von NIS-2.

Von Wulf Bolte, Rodney Wiedemann, Christian Pinnecke und Maximilian Klose

Ende 2022 wurde NIS-2 im Europäischen Parlament verabschiedet und trat im Januar 2023 in Kraft; bis Oktober 2024 muss NIS-2 in nationale Gesetze überführt und somit verbindlich in den Ländern umgesetzt werden.

NIS-2 wurde als Reaktion auf die erhöhte Bedrohung von kritischen Infrastrukturen durch digitale Angriffe eingeführt, um solche potenziell katastrophalen Angriffe zu verhindern.

NIS-2 ist die Antwort der Europäischen Union auf die wachsenden Bedrohungen durch Cyberangriffe und zunehmende Professionalisierung der Cyberkriminalität. Angesichts der fortschrittlichen Ausstattung und der Macht staatlicher Akteure besteht in der EU ein zunehmendes Risiko für Cyberangriffe.

Für wen ist das relevant?

In Deutschland sind Schätzungen zufolge zwischen 29.000 und 40.000 Unternehmen von der NIS-2 betroffen. Unternehmen aus 18 definierten Sektoren, ab 50 Mitarbeitenden und 10 Millionen Umsatz, unterliegen NIS-2. Insofern können zukünftig unter anderem auch IT-Dienstleister, Onlinemarkplätze, Maschinenbauunternehmen, Lebensmittelversorger, Labore und Forschungseinrichtungen dazugehören, wenn sie die Schwellenwerte übersteigen. Das bringt schlagartig eine ganze Reihe an Unternehmen in die Verantwortung, die sich vorher nur wenig mit ihrer Informationssicherheit auseinandergesetzt haben.

Mit welchen Sanktionen ist zu rechnen?

Die betroffenen Unternehmen müssen sich intensiv mit ihrer Informationssicherheit auseinander- und notwendige Maßnahmen umsetzen, ansonsten drohen empfindliche Strafen mit bis zu maximal 10 Millionen Euro oder 2 % des gesamten weltweiten Jahresumsatzes. Um diesen Sanktionen zu entgehen, muss die logische Konsequenz gezogen werden, dass die betroffenen Unternehmen ein Informationssicherheitsmanagementsystem (ISMS) implementieren.

Was sind die größten Herausforderungen?

Die NIS-2-Richtlinie forciert ein höheres Maß an Cybersicherheit. Dies führt zu technologischen wie auch personellen Herausforderungen. Die Vorgaben für die betroffenen Unternehmen werden denen angenähert, die aktuell schon größtenteils für kritische Infrastrukturen gelten, was eine ganze Reihe neuer Aufgaben mit sich bringt.

Nehmen wir als Beispiel die Angriffserkennung. Ein Frühwarnsystem hilft nur dann, wenn auch die Mitarbeitenden mit ihm umgehen können. So fällt allein an dieser Stelle auf, dass es neben den rein finanziellen Aspekten auch Knowhow-Probleme geben wird.

Um Knowhow aufzubauen, müssen Mitarbeitende die entsprechenden Zeiten haben, was auf einem angespannten Arbeitsmarkt und häufig überlasteten IT-Abteilungen nur schwierig umsetzbar ist. Weiterhin müssen aktuelle Sicherheitsregelungen überarbeitet werden, was zu einer neuen Prozessstruktur führen kann und wiederum Personal und Zeit bindet. Auch bei der Umsetzung und Planung von neuen Regelungen ist es wichtig, dass das Personal entsprechende Kenntnisse der Informationssicherheit besitzt, da jetzt die Regelungen auch überprüft werden und bei einer Nichtkonformität hohe Strafen vorgesehen sind. Ein funktionierendes ISMS wird somit für die von der NIS-2 betroffenen Unternehmen unabdingbar.

„Die Umsetzung der NIS-2 ist vermutlich bei vielen getrieben durch Zwang. Dennoch sind die Vorteile nicht von der Hand zu weisen.“

Über welchen Zeitrahmen sprechen wir?

Im Dezember 2022 hat die EU die neue NIS-2-Richtlinie (EU 2022/2555) veröffentlicht, die am 16. Januar 2023 in Kraft getreten ist. Bis zum 17.Oktober 2024 müssen die Mitgliedsstaaten die neue Richtlinie in ein nationales Gesetz verabschieden. Bereits 2023 gab es 3 Referentenentwürfe, den letzten im September dieses Jahres.

Möglicherweise werden die neuen Rechtsverordnungen für die Umsetzung der NIS-2-Richtlinie noch dieses Jahr durch den Bundestag verabschiedet. Die Verkündung sowie das Inkrafttreten des NIS-2-Umsetzungsgesetzes ist für Oktober 2024 geplant. Die daraus resultierenden Maßnahmen haben zum Teil eine Umsetzungsfrist von einem Werktag bis hin zu zehn Monaten. Einige Maßnahmen treten möglicherweise erst ab Januar 2026 in Kraft.

Welche Vorteile ergeben sich durch die Umsetzung?

Die Umsetzung der NIS-2 ist vermutlich bei vielen getrieben durch Zwang. Dennoch sind die Vorteile nicht von der Hand zu weisen. Die Informationssicherheit war oft nur ein freiwilliger, halbherzig betrachteter Anteil im Management. Experten warnen seit Jahren, dass es nicht gut steht um die Infrastrukturen. Jetzt wird ein Rahmenwerk geschaffen, welches den aktuellen Stand der Technik forciert.

Die Sicherheit wird teilweise immens erhöht, wodurch die Anzahl der Datenlecks und Hacks vermutlich zurückgehen wird und Daten von Kunden, Mitarbeitenden und/oder Patienten besser geschützt werden. Langfristig werden IT-Abteilungen durch neue Technologien entlastet und das Management hat klare Prozesse in Notfällen.

Fazit

Ab dem 17. Oktober 2024 tritt die neue NIS-2-Richtlinie (Network and Information Security Directive 2) (EU 2022/2555) in Deutschland durch nationales Recht in Kraft. Durch Erweiterung der Sektoren (wesentliche auf elf und wichtige auf sieben) und Anpassung der Schwellenwerte bezüglich mittlerer und großer Unternehmen müssen ca. 30.000 Unternehmen in Deutschland das neue Recht anwenden und umsetzen. Bei Nichtbeachtung drohen der Organisation empfindliche Strafen.

Die entsprechenden Unternehmen müssen eine Reihe von Informationssicherheits- und Meldeprozessen, wie z. B. Incident Management, Business Continuity oder Riskmanagement, in die Organisation integrieren, um eine stärkere Cyber-Resilienz in Deutschland, aber auch in der gesamten Europäischen Union sicherzustellen. Prüfen Sie daher rechtzeitig, ob Ihre Organisation auch das neue Gesetz umsetzen und anwenden muss. &

Fragen oder Unklarheiten?

Sprechen Sie uns gerne an! Wir prüfen gemeinsam mit Ihnen, ob Ihre Organisation das neue Gesetz umsetzen und wie das in der Praxis aussehen kann.

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

Die Menschen hinter Althammer & Kill:

Sinem Gülüm

Ja hallo, wer bist du denn?

Sinem: Hallo, ich bin Sinem Gülüm und ich komme aus Hildesheim. Ich habe meine zweite Ausbildung als Groß- und Außenhandelskauffrau 2022 erfolgreich absolviert und bin kurz darauf direkt zu Althammer & Kill in den Vertrieb gewechselt.

Wieso hast du dich bei Althammer & Kill beworben? Wie bist du auf uns aufmerksam geworden?

Sinem: Mir wurde Althammer & Kill von einem Bekannten empfohlen, der selbst auch im Vertrieb bei Althammer & Kill tätig ist. – Er hat einen sehr guten Job gemacht, denn die Bewerbung ließ nicht lange auf sich warten.

Wie lange arbeitest du schon bei Althammer & Kill?

Sinem: Seit einem Jahr bin ich Teil des Teams.

Was genau sind deine Aufgaben?

Sinem: Die Betreuung der Bestandskunden und die Neukunden-Akquise füllen meinen Arbeitstag. Außerdem darf ich eigene Kampagnen starten, und mich frei entfalten, welches eine gute Abwechselung in den Arbeitsalltag bringen.

Du bist sowohl für Althammer & Kill als auch für LearnBase tätig (gewesen). Wie unterscheidet sich die Arbeit bei beiden Organisationen?

Sinem: Die Organisationen sind ähnlich und unterschiedlich zugleich. Bei LearnBase sind die Entscheidungswege etwas kürzer, doch da das Unternehmen jünger ist, liegt unser Hauptaugenmerk darin, die LearnBase bekannter zu machen! Das ist eine der Tatsachen, welche mir sehr gefällt, denn wir haben bei LearnBase eine Unternehmensgröße, wo wir noch sehr stark auf die Bedürfnisse der Interessenten und Kunden eingehen können, um uns auch stätig weiterentwickeln zu können. – Althammer & Kill genießt in der Branche bereits einen guten Ruf und einen hohen Bekanntheitsgrad. Dadurch ist der Austausch mit den Kunden/Interessenten sehr angenehm.

„Freude an der Arbeit und den Austausch mit Menschen."

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

Sinem: Sehr unterschiedlich. Ich schreibe Angebote, plane Kampagnen, betreue Bestandskunden, nehme Anregungen und Vorschläge entgegen, präsentiere die Produkte in Live-Vorstellungen, halte Webinare uvm.

Was gefällt dir besonders an der Arbeit hier?

Sinem: Das tolle Arbeitsklima unter den Kollegen. Der Austausch mit den Kunden und die Vielfältigkeit. Ich kann mir die Arbeit so aufteilen, wie ich produktiv bin. Es gibt Tage, da telefoniere ich sehr gerne, doch auch andere, an denen ich mich lieber an die Planung der nächsten Kampagnen mache.

Welche Eigenschaften sollte ein Mitarbeiter im Vertrieb deiner Meinung nach unbedingt mitbringen?

Sinem: Freude an der Arbeit und den Austausch mit Menschen. Eine Leidenschaft für das Produkt und ein gesundes Maß an Neugier und die Aufgeschlossenheit, Neues aufzunehmen.

Ist dir ein Telefonat/ein Gespräch mit einem Kunden oder einem Interessenten besonders im Gedächtnis geblieben? Wenn ja, warum?

Sinem: Eine Aussage ist mir tatsächlich im Gedächtnis geblieben, und zwar hatte eine Interessentin viele Fragen, was alles mit der LearnBase möglich ist. Ich habe ihr einiges erzählt, ihre Fragen beantwortet und das Feedback war: Mensch, mit dem System ist ja alles möglich, was wir uns wünschen und sogar noch mehr. – Solche Aussagen freuen uns selbstverständlich sehr. &

Althammer & Kill Akademie

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

12. Dezember 2023 – kostenloses Webinar

Das Hinweisgebersystem von Althammer & Kill

Wir erklären die Richtlinie, zeigen Anforderungen und Pflichten auf und stellen Ihnen das Hinweisgebersystem von Althammer & Kill vor. Dieses lässt sich ganz einfach bei Ihnen einbinden, behandelt alle Daten völlig anonym und erfüllt die Anforderungen an die Richtlinie optimal. So können Sie Ihre Meldestelle einfach und nach der EU-Whistleblower-Richtlinie implementieren.

10. Januar 2024 – kostenloses Webinar

HowTo Social Media – Unternehmensrichtlinien für die Nutzung sozialer Netzwerke

Social Media ist aus dem Unternehmenskontext kaum noch wegzudenken. Kanäle wie Facebook, Instagram und Co. sind ideal, um im Kontakt mit der Zielgruppe zu stehen, Bekanntheit zu fördern oder Werbung dort zu schalten, wo sich potenzielle Kunden aufhalten. Doch die oft aus den USA stammenden Plattformen bergen gewisse datenschutzrechtliche Risiken.

24. Januar 2024 – kostenloses Webinar

Security Awareness: Der Weg zur Human Firewall

Systeme werden immer sicherer und dennoch sind erfolgreiche Hacker-Angriffe an der Tagesordnung. Wie passt das zusammen? Menschen können ein effektiver Schutz gegen Angriffe sein, wenn sie die Bedrohung kennen. Cyber-Security im Zeitalter von Cloud und Co. bedeutet vor allem, dass ein Bewusstsein bei Mitarbeitenden geschaffen werden muss.

21. Februar 2024 – kostenloses Webinar

Bring Your Own Device – Fallstricke vermeiden

Privathandy im Firmenkontext? Bring your own device (BYOD) ist hier das Zauberwort. Aus der Perspektive der Informationssicherheit und des Datenschutzes ist der BYOD-Ansatz jedoch risikobehaftet und es ist eine sorgfältige Abwägung erforderlich. Wir zeigen Risiken auf und geben Maßnahmenempfehlungen aus Datenschutz- und Informationssicherheits-Perspektive.

6. März 2024 – kostenloses Webinar

Microsoft 365, AWS & Co. – sicher in die Cloud

Microsoft 365, Amazon Web Services und Co. sind ein Problemfall für Datenschützer – denn es sind sogenannte „Cloud-Dienste". Wir stellen Ihnen die datenschutzrechtliche Einordnung und Umsetzungsmöglichkeiten unter praktischen Gesichtspunkten vor, zeigen worauf Entscheider im Rahmen ihrer IT-Strategie achten sollten und welche rechtlichen Herausforderungen bei der Einführung von cloudbasierten Diensten 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 Digital Services Act – das „Grundgesetz für das Digitalzeitalter“

Schon Anfang 2020 hatte die EU-Kommission angekündigt, in der Datenwirtschaft zukünftige eine führende Rolle übernehmen zu wollen und die EU zu einer Gesellschaft zu machen, die „dank Daten in der Lage ist, in der Wirtschaft wie im öffentlichen Sektor bessere Entscheidungen zu treffen“.

Von Arne Wolff

Um die digitale Wirtschaft zu fördern und die Produktivität allgemein zu steigern, müsse der rechtliche Rahmen für den Umgang mit Daten verbessert und „Pools mit hochwertigen Daten“ bereitgestellt werden. Eine zentrale Rolle kommt dabei dem Digital Services Act (DSA) zu, den die EU-Kommission selbst als „Grundgesetz für das Digitalzeitalter“ versteht.

Schon seit dem 25.08.2023 gelten die neuen Regelungen für sogenannte „Very Large Online-Plattforms“ (VLOPs) und „Very Large Online Search Engines“ (VLOSEs) und erlegen diesen Internet-Anbietern und Suchmaschinen eine Vielzahl an Vorschriften auf. Diese „Gatekeeper“ – Plattformen mit mindestens 45 Millionen Nutzerinnen und Nutzer in der EU – werden im Bestreben, Desinformation und Intransparenz in Netz zurückzudrängen, stärker in die Pflicht genommen.

Ein Who’s Who des Internets

Alibaba AliExpress, Amazon Store, Apple AppStore, Bing, Booking.com, Facebook, Google Play, Google Maps, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Wikipedia, X (the company formerly known as Twitter), YouTube und Zalando werden von der EU-Kommission als VLOPs eingestuft1 – was nicht unwidersprochen blieb: Amazon und Zalando wehren sich gegen die Kategorisierung als Gatekeeper.
Die Bestimmungen des DSA werden für Gatekeeper direkt von der EU-Kommission durchgesetzt und verdrängen für diese Anbieter das Netzwerkdurchsetzungsgesetz (NetzDG). Die Kommission hat dazu fünf Referate eingerichtet, die verschiedene Rechtsgebiete abdecken sollen.

Ambitionierte Regeln

Vor allem Anbieter von Onlinediensten und sozialen Medien sollen künftig „systemische Risiken“ adressieren müssen. Gemeint sind insbesondere Themen wie Wahlmanipulation, Desinformation durch “Fake News“, Cybermobbing oder jugendgefährdende Inhalte – waren die VLOPs doch bisher recht zögerlich, wenn es darum ging, solche Inhalte zu löschen. So sollen „europäische Werte wie Demokratie und Rechtsstaatlichkeit“ im virtuellen Raum verteidigt werden.

Die Liste der Bestimmungen, die zunächst die VLOPs und VLOSE nun konkret erfüllen müssen, ist lang und zielt vor allem darauf ab, nachteilige Auswirkungen auf öffentliche Sicherheit oder Wahlprozesse zu verhindern und allgemein die Menschenwürde zu schützen:

- Die User müssen klar darüber informiert werden, nach welchen Kriterien ihnen bestimmte Inhalte empfohlen werden, und es muss eine neutrale, nicht auf Profiling beruhende Alternative angeboten werden.
- Die Plattformen müssen jegliche Werbung kennzeichnen, die User darüber informieren, wer diese finanziert und Archive aller bei ihnen geschalteten Werbeanzeigen anlegen.
- Außerdem darf Werbung künftig nicht mehr auf Basis sensibler personenbezogener Daten2 und nicht mehr speziell an Kinder ausgespielt werden.
- Es müssen Meldeplattformen für illegale Inhalte eingerichtet werden.
- Die Betreiber müssen verdächtige Inhalte an die Behörden melden und der Verbreitung illegaler Inhalte im Internet und negativen Auswirkungen auf die Meinungs- und Informationsfreiheit entgegenwirken.
- Die Inhaltsmoderation der Betreiber muss transparent erfolgen: werden Inhalte gelöscht, müssen die Verfasser über die Gründe informiert werden und erhalten ein Widerspruchsrecht.
- Die Plattformen müssen über klare allgemeine Geschäftsbedingungen verfügen und sie sorgfältig und ohne Willkür durchsetzen.
- Die Betreiber müssen Risikobewertungen für ihre Plattformen erstellen und extern unabhängig prüfen lassen.
- Verkaufsplattformen müssen Kontaktdaten, Einträge im Handelsregister sowie weitere relevante Informationen der Anbieter offenlegen.
- Sogenannte „Dark Patterns“ –Gestaltungsmethoden, die Nutzer bewusst manipulieren sollen – sind künftig ausdrücklich untersagt.
- Die Plattformen müssen Transparenzberichte über Moderationsentscheidungen zu Inhalten veröffentlichen.

Bei Nichteinhaltung drohen empfindliche Geldstrafen – bis zu sechs Prozent des globalen Umsatzes können es werden. Die Entscheidung darüber erfolgt im Einzelfall – und im Zweifel vor Gericht.

Die Schere im ~~Kopf~~ Algorithmus

Die VLOPs könnten jetzt versucht sein, nach dem Motto „lieber zu viel als zu wenig“ Inhalte zu löschen, bloß weil sie gegen die Richtlinien verstoßen könnten – das sogenannte „Overblocking“. Bekannt ist dies bisher vor allem von Löschungen aufgrund angeblicher Urheberrechtsverletzungen, die im Nachgang allzu oft einer Überprüfung nicht standhalten konnten.

Dass die Beurteilung von Inhalten zunehmend automatisiert erfolgt, obwohl noch keine Technologie die rechtlichen Grenzen zwischen gesetzwidrigen und zulässigen Äußerungen ausreichend sicher nachzeichnen kann, erhöht die Gefahr der „überschießende Moderation“. Im DSA ist deshalb ist ein Widerspruchsrecht fest verankert; zudem sollen User, die übermäßig oft falsche Meldungen abgeben, abgemahnt und letztlich vorübergehend vom Meldesystem ausgeschlossen werden können. Es muss sich allerdings erst erweisen, ob diese Maßnahmen wirksam sind.

Bei Nichteinhaltung drohen empfindliche Geldstrafen – bis zu sechs Prozent des globalen Umsatzes können es werden.

Zusätzlich droht auf politischer Ebene Konfliktpotential für die europäische Staatengemeinschaft, denn ein Land könnte versuchen, unliebsame Inhalte – die woanders aber völlig unproblematisch sind – europaweit löschen zu lassen.

Fortsetzung folgt

Ab 17. Februar 2024 gilt der DSA dann auch für die kleineren Dienste, und zwar auf nationaler Ebene. Die Mitgliedsstaaten müssen sich also selbst um die Um- und Durchsetzung kümmern. In Deutschland werden vor allem das Netzwerkdurchsetzungsgesetz (NetzDG), das Telemediengesetz (TMG) und voraussichtlich auch das Jugendschutzgesetz (JuSchG) noch angepasst werden müssen; fest steht die Bundesnetzagentur als zuständige Aufsichtsbehörde.

Ist jetzt Schluss mit Hetze im Netz? Zu hoffen wäre es allemal. Das Ziel ist klar, doch ob die getroffenen Maßnahmen ausreichen, es zu erreichen, wird sich erst erweisen müssen. Ob es wirklich funktioniert, die Bewertung, was im Netz illegal ist und was nicht, quasi an die Plattformbetreiber outzusourcen, bleibt ebenfalls abzuwarten. Und aufmerksam zu beobachten. &

Kein Tag ist wie der andere

Danny erzählt vom abwechslungsreichen Alltag des Online Marketing-Managers und den Tücken, Datenschutz leicht verständlich zu vermarkten.

Wer bist du? Welche Ausbildung hast du?

Danny: Moin, mein Name ist Danny Sellmann, ich bin verheiratet und seit vier Monaten Papa einer kleinen Tochter.

Ich bin ausgebildeter Kaufmann im Einzelhandel sowie im Groß- und Außenhandel. Nach meinen beiden kaufmännischen Ausbildungen hatte ich die Chance, im Marketing einzusteigen und habe mich dort berufsbegleitend zum Online Marketing Manager weitergebildet.

Wie lange arbeitest du schon bei Althammer & Kill?

Danny: Seit fast fünf Jahren arbeite ich hier bei Althammer & Kill im Marketing und habe in dieser Zeit eine Vielzahl von interessanten Projekten betreut.

Wie hat es dich zu Althammer & Kill verschlagen?

Danny: Mit der Einführung der DSGVO im Jahr 2018 wurde bei Althammer & Kill eine neue Stelle als Online Marketing Manager geschaffen. Das Unternehmen ist stark gewachsen und dadurch sind auf einen Schlag mehr Marketingaufgaben angefallen, die ohne Marketing-Manager nicht mehr zu bewältigen waren. Nach zwei Kennenlernrunden mit Thomas Althammer hat es gematcht. Ich wollte mich zu diesem Zeitpunkt beruflich weiterentwickeln und fand die Möglichkeit, Teil eines neu geschaffenen Bereichs zu werden, sehr interessant.

Was sind deine Aufgaben? Wie sieht dein Alltag aus?

Danny: Meine Aufgaben sind sehr vielfältig und alles andere als eintönig. Ich betreue zum Beispiel die A&K-Website, den Social-Media-Kanal, unterstütze bei Dreharbeiten zu unseren Success Stories und bin in diversen Events, Messen und Projekten involviert.

Kein Tag im Jahr ist wie der andere. Im Marketing gibt es nur sehr wenige wiederkehrende Aufgaben, die nach Schema F ablaufen. Das macht den Bereich gerade so interessant und abwechslungsreich.

Warum bist du Online Marketing Manager geworden?

Danny: Ich bin mir sicher, dass der Online-Bereich die Zukunft des Marketings ist. Es passiert so viel in diesem Umfeld — er entwickelt sich so schnell (z.B. im Bereich KI) und die Möglichkeiten, potenzielle Kunden auf neuen Kanälen zu erreichen, gibt es im „klassischen" Marketing so nicht.

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.

Nutzt du bereits künstliche Intelligenz in deinem Arbeitsalltag?

Danny: Ja, KI ist auch im Marketing nicht mehr wegzudenken. Obwohl sich immer wieder neue Möglichkeiten ergeben, Aufgaben mit KI zu vereinfachen, bin ich gespannt, welche Möglichkeiten es in Zukunft geben wird, KI effizient und als Marketing-Assistent einzusetzen.

Was glaubst du, wie wird sich die Weiterentwicklung von künstlicher Intelligenz auf deine Arbeit auswirken?

Danny: Ich bin mir sicher, dass KI meine Arbeit positiv beeinflussen und vieles vereinfachen wird. In diesem Thema steckt so viel

„Ich bin mir sicher, dass KI meine Arbeit positiv beeinflussen und vieles vereinfachen wird."

Potenzial, das heute leider noch nicht annähernd ausgeschöpft wird. Man muss aber auch die Kehrseite der Medaille sehen und die Ergebnisse kritisch hinterfragen, denn die Manipulationsmöglichkeiten sind ebenfalls enorm.

Wie unterscheidet sich das Marketing einer Dienstleistung vom Marketing eines Produkts?

Danny: Im Gegensatz zu einem Produkt kann eine Dienstleistung nicht angefasst und „sichtbar" präsentiert werden. Dienstleistungen sind erklärungsbedürftiger, müssen aber trotzdem kurz erklärt werden können, um Interesse zu wecken. Genau das ist die Herausforderung und macht die Vermarktung einer Dienstleistung so spannend.

Was gefällt dir besonders an deiner Tätigkeit bei Althammer & Kill?

Danny: Ich schätze die Zusammenarbeit mit meinem Team. Es macht Spaß, an innovativen Kampagnen und Projekten zu arbeiten und dabei verschiedene Marketingkanäle zu nutzen, um unsere Zielgruppe zu erreichen. Außerdem finde ich es faszinierend, die Wirkung unserer Marketingstrategien zu beobachten und zu sehen, wie wir das Interesse und die Zufriedenheit unserer Kunden steigern können.

Was waren bisher deine Highlights bei Althammer & Kill?

Danny: Der Relaunch unserer Website war definitiv ein Highlight. Es war ein spannendes Projekt, bei dem wir das Design und die Benutzerfreundlichkeit unserer Website verbessert haben. Es erforderte viel Kreativität und Planungsarbeit, aber das Endergebnis war es auf jeden Fall wert.

Ein weiteres Highlight waren die bisherigen Teamevents, die wir regelmäßig veranstalten. Diese Veranstaltungen haben nicht nur dazu beigetragen, dass wir als Team enger zusammengerückt sind, sondern auch dazu, dass wir uns außerhalb der Arbeit besser kennen gelernt haben.

Besonders gut gefällt mir auch die Abwechslung in meiner Tätigkeit bei Althammer & Kill. Durch neue Herausforderungen und Projekte habe ich die Möglichkeit, mich ständig weiterzuentwickeln und mein Fachwissen zu erweitern.

ALTHAMMER & KILL

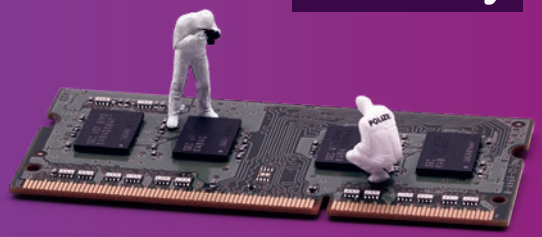
Pragmatische Lösungskonzepte für Datenschutz & Digitalisierung.

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

Datenschutz

Informations-sicherheit

Cloud- & Cyber-Security



Compliance

althammer-kill.de