COMPLIANCE
konkret

Das Kundenmagazin
von Althammer & Kill
Ausgabe 1/2022

Cyber-Attacken erfolgreich abwehren

Die Gefahr von Cyber-Attacken steigt rapide an. Wir zeigen Maßnahmen, die Ihren Schutz deutlich erhöhen.
Seite 6

Nach den Google-Urteilen
Handlungsbedarf auf Millionen Webseiten
Seite 10

Wenn es kritisch wird
Patchmanagement als Teil der Informationssicherheit
Seite 12

Hinweisgebersystem – Von der Pflicht zur Chance
Viele gute Gründe sprechen dafür.
Seite 14

Editorial

Liebe Leserin, lieber Leser,

die Zahlen wirken erschlagend: 144 Mio. neue Schadprogramm-Varianten binnen eines Jahres. Cyber-Erpressungen entwickeln sich zur größten Bedrohung in Sachen IT-Sicherheit. Die Folgen: eine Uniklinik konnte 13 Tage lang keine Notfallpatienten aufnehmen. In einem anderen Fall wurden Lösegelder von rund 1.000 €/Mitarbeitenden gezahlt, um wieder an die eigenen Daten zu kommen.

Die gute Nachricht: Sie können sich wehren. Wir beschäftigen uns in dieser Ausgabe mit der Frage, wie sich Cyber-Attacken verhindern lassen oder wie im Falle eines erfolgreichen Angriffs die Auswirkungen möglichst gering gehalten werden. Eine wichtige Maßnahme ist nicht zuletzt das Patchmanagement, welches den Überblick über (sicherheits-)relevante Updates umfasst und auch Thema dieser Ausgabe ist.

Auf der rechtlichen Seite gibt es ebenfalls Handlungsbedarf für Organisationen. Mit den Urteilen zum Einsatz von Google Analytics und Google Fonts in Deutschland, Österreich und Frankreich muss nun deren Einsatz überdacht werden.

„Ein Hinweisgebersystem ist für alle Organisationen ab 250 Beschäftigte zu installieren."

Darüber hinaus gilt es, auf die neue EU-Hinweisgeber-Richtlinie zu reagieren. Zunächst gilt das nur für Organisationen ab 250 Mitarbeitende, ab Ende 2023 sinkt die Grenze auf 50 Beschäftigte. Wir haben ein schlankes System im Angebot, das wir Ihnen gern vorstellen. Der Vorteil: Wir bieten nicht nur eine Software-Lösung an, sondern sind auch telefonisch und per E-Mail erreichbar, um Anfragen vertraulich entgegenzunehmen. Auf Wunsch stellen wir den externen Compliance-Beauftragten für Ihre Organisation.

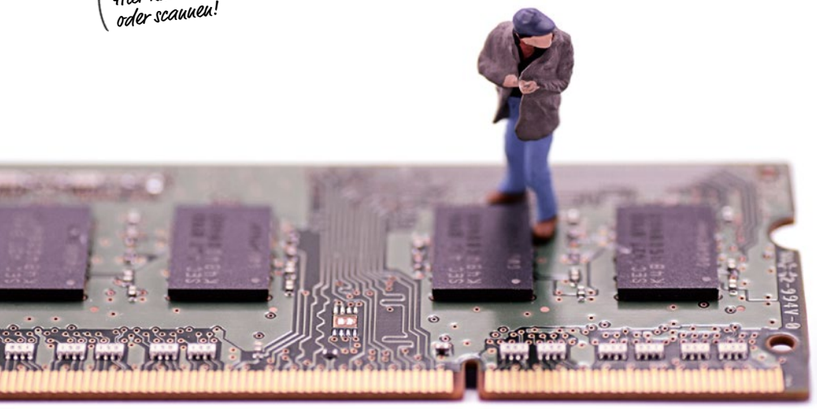
Viel Spaß beim Lesen!

Thomas Althammer & Niels Kill

Darüber wird gesprochen

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

Hier klicken oder scannen!



Informationssicherheitsmanagementsysteme wirksam einführen – So geht's!

Phishing-Attacken, gehackte Accounts, Datendiebstahl – schon ein einziger falscher Mausklick reicht aus, um gewaltigen Schaden anzurichten. Unternehmen sollten das Problem Cyberkriminalität ernst nehmen – Informationssicherheitsmanagementsysteme (ISMS) sind ein wichtiges Instrument, Informationssicherheit in Ihrem Unternehmen strukturiert zu etablieren, zu kontrollieren, aufrechtzuerhalten und permanent zu verbessern.

Zahl des Monats

57 %

aller Websites weltweit nutzen Google Analytics. Nach den wegweisenden Urteilen aus Österreich und Frankreich könnte ein Verbot des Analysetools auch bald in Deutschland folgen und für viele Websitebetreiber Handlungsbedarf hervorrufen.

BSI-Gesetz macht den Einsatz von Systemen zur Angriffserkennung verpflichtend

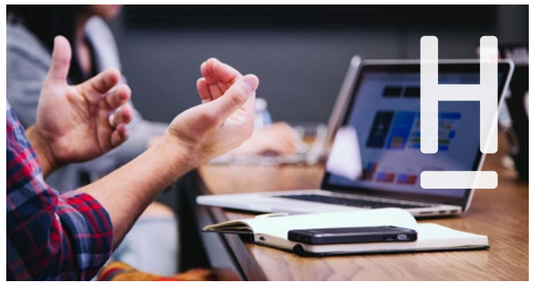
Ab dem 1. Mai 2023 müssen alle Betreiber kritischer Infrastrukturen gemäß § 8a „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" (BSI-Gesetz – BSIG) gegenüber dem BSI (Bundesamt für Sicherheit in der Informationstechnik) den Einsatz von Systemen zur Angriffserkennung (zum Beispiel ein Intrusion Detection System – IDS bzw. ein Intrusion Prevention System – IPS) nachweisen.

Datenschutz: Landgericht München verbietet Google Fonts – so müssen Sie jetzt handeln!

Die dynamische Einbindung von Google Fonts ohne Einwilligung ist rechtswidrig – so lautet das Urteil der Richter am Landgericht München (20.01.2022). In diesem Blog-Beitrag erläutern wir, wie es zu diesem wegweisenden Urteil kam und welche Handlungen nun zu tätigen sind.

Die 7 Grundelemente des Compliance-Managements

In vielen Unternehmen werden Compliance- und Risikomanagement separat betrachtet und betrieben. Risiko bedeutet die negative Abweichung von einem erwartbaren Zustand beziehungsweise eines Erwartungswertes. Im Rahmen des Risikomanagements sollten Risikofaktoren planmäßig und systematisch identifiziert, analysiert und bewertet werden. Für eine solche Bewertung und Messung des Risikos sind optimale Ausgangspunkte ein Audit oder eine Gap-Analyse.



Theorie und Praxis: Althammer & Kill kooperiert mit Hochschule Hannover

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

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

LearnBase

LearnBase – vom Projekt zur Eigenständigkeit

Mitarbeitende zu verschiedenen Themen zu unterweisen, zählt meist nicht zur Kür, sondern zur Pflicht vieler Unternehmen. Was zuvor durch Präsenzveranstaltungen gelöst wurde, braucht heute neue Ansätze, um den Bedürfnissen der Organisation und der Mitarbeitenden gerecht zu werden.

Durch LearnBase können Mitarbeitende die Schulungen direkt im Browser starten, egal ob zu Hause oder im Dienst, ob mit eigener Mailadresse oder ohne, und so direkt neue Kenntnisse erwerben. Was 2018 als Projekt im Hause Althammer & Kill begann, ist seit 2022 eine selbstständige GmbH. Wir freuen uns auf ein Jahr, das mit Eigenständigkeit, neuen Kolleginnen und Kollegen und vielen Ideen startet. Besuchen Sie uns online!

Der Podcast: „Maximale Langeweile"

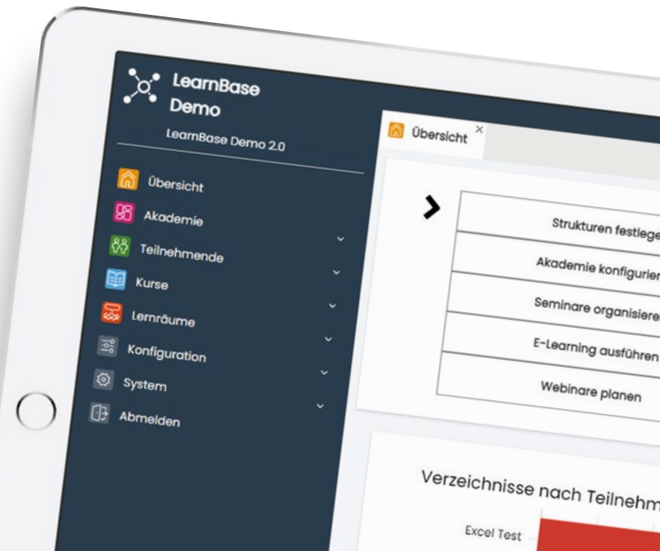
Anfang November 2021 veröffentlichten Simon Lang und Maximilian Klose die erste Folge ihres Datenschutz- und Cyber-Security-Podcast „Maximale Langeweile". Althammer & Kill unterstützt die Kreativität seiner Mitarbeitenden mit zeitlichen und finanziellen/technischen Ressourcen.

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. Ziel von Maximilian und Simon ist das unterhaltsame Vermitteln von Inhalten, ohne dabei zu kleinteilig zu werden. Dieser Podcast ist für alle geeignet, die sich unterhalten lassen möchten und dabei noch etwas über Compliance-relevante Themen erfahren wollen.

„Maximale Langeweile" erscheint jeden zweiten Donnerstag auf Spotify, bei Apple Podcast und weiteren gängigen Podcast-Diensten:

Spotify

Apple Podcast



Cyber-Attacken erfolgreich abwehren

Der Bericht zur Lage der IT-Sicherheit des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ist eindeutig: Die Gefahr von Cyber-Attacken und daraus folgenden Erpressungsversuchen steigt rapide an. Es geht den Cyberkriminellen häufig um die Erlangung von Schweige-, Löse- oder Schutzgeld.

Viele (erfolgreiche) Angriffe werden niemals publik, doch einige sind in regelmäßigen Abständen in Fachmedien oder in der Presse zu finden. So wie der Fall eines Universitätsklinikums: Ganze 13 Tage konnte dieses keine Notfall-Patienten aufnehmen. Schuld war eine Ransomware-Attacke. Dieses Beispiel zeigt, dass Cyber-Angriffe jede Organisation treffen können.

Doch warum nehmen Cyber-Attacken stetig zu? Sicherlich ist die rasant an Fahrt aufnehmende Digitalisierung als einer der Gründe aufzuführen. IT-Strukturen von Organisationen werden komplexer, Systeme leistungsfähiger und Anwendungen umfangreicher. Dadurch fehlt es häufig an einem allumfassenden Überblick zu den Aspekten Datenschutz, IT- und Informationssicherheit. Es wird davon ausgegangen, dass IT-Systeme und Anwendungen „per se sicher sind“. Doch dies stimmt meist nur bis zum nächsten Software-Update. Werden Patches nicht installiert, sind IT-Systeme und Anwendungen verwundbar.

Neun Maßnahmen, um Ihre Organisation vor Cyber-Attacken zu schützen

Hundertprozentigen Schutz gibt es nicht. Dieses Mantra gilt auch in der Cyber-Security. Dennoch existieren zahlreiche Maßnahmen, um den Schutz deutlich zu erhöhen.

Mitarbeitende schulen und Awareness schaffen
Systeme und Anwendungen werden immer sicherer – sofern die Updates gut organisiert sind. Der Faktor „Mensch“ rückt daher immer öfter in den Fokus von Cyber-Kriminellen. Daher ist es wichtig, dass alle Mitarbeitenden über die aktuellen Gefahren aufgeklärt werden. Mit sogenannten Security Awareness Maßnahmen werden z. B. anhand von Simulationen Attacken im Rahmen von Phishing-Kampagnen nachgebildet, deren Ergebnis

Stichwort

Ransomware

Ransomware leitet sich vom englischen Wort „ransom“, also zu Deutsch „Lösegeld“ ab. Hierbei handelt es sich um ein Schadprogramm, mit dessen Hilfe ein Angreifer den Zugriff des Nutzers/Eigentümers auf die eigenen Daten bzw. auf das gesamte Computersystem verhindern kann, indem bspw. das gesamte System verschlüsselt wird. Das Opfer muss für die „Freilassung“ ein Lösegeld zahlen.

ausgewertet und passgenaue Schulungs- und Sensibilisierungskonzepte (Poster, Plakate, etc.) ausgearbeitet.

Richtlinien erstellen
Richtlinien enthalten Vorgaben, um die Sicherheit von Anwendungen und Systemen wirksam zu schützen, wie z. B. Anweisungen zur Passwortgestaltung oder dem turnusmäßigen Wechsel. Außerdem werden Kommunikations- und Meldewege aufgezeigt, wenn verdächtige Aktivitäten wie „komisch anmutende" E-Mails entdeckt werden. Richtlinien geben der gesamten Organisation Orientierung und Sicherheit.

Offene Fehlerkultur leben
Fehler sind menschlich und „sich wegducken" ist die falsche Antwort auf einen Fehler. Kommt es zu einer Unachtsamkeit (z. B. wurden Zugangsdaten fälschlicherweise eingegeben) sollte den Mitarbeitenden Unterstützung bei der Beseitigung angeboten werden. Denn nur so lassen sich Angriffe wirklich aufdecken.

Überblick verschaffen
Inventarlisten aller IT-Systeme und Anwendungen ist bei der Masse an Hard- und Software ein Muss, denn nur so können die einzelnen Komponenten professionell nachgehalten werden. Daher sollte eine regelmäßige Bestandsaufnahme stattfinden, um z. B. sogenannte „Schatten-IT" festzustellen und aus der Organisation zu entfernen.

Systeme auf dem aktuellen Stand halten
IT-Systeme und Anwendungen stammen meist von kommerziellen Anbietern. Daher durchlaufen diese einen (Produkt-)Lebenszyklus und werden nach einer gewissen Zeit nicht weiter supportet. Insbesondere in Zeiten, in denen neue Schadsoftware zu hunderttausenden pro Tag neu entstehen, sollten alle IT-Systeme und Anwendungen immer auf dem neusten Stand sein. Auf Sicherheitsupdates von Herstellern ist entsprechend und bestmöglich umgehend (nach vorheriger Prüfung) zu reagieren. Veraltete IT-Systeme und Anwendungen sollten ausgetauscht werden.

Stichwort

Schatten-IT

Als Schatten-IT werden Hard- und Software bezeichnet, die von Mitarbeitenden in die Organisation eingebracht, jedoch nicht von der IT-Abteilung getestet oder freigegeben wurden.

Netzwerke segmentieren
Was sich im Schiffsbau bewährt hat, kann auch auf IT-Systeme übertragen werden. Durch das Einziehen von Schotten kann im Falle eines Lecks sichergestellt werden, dass das Schiff nicht mit Wasser überflutet wird und schlussendlich untergeht. Übertragen auf die IT- und Informationssicherheit bedeutet dies: Werden Systemkomponenten und insbesondere Netzwerke voneinander „abgeschottet", sind bei einem Schadensereignissen die anderen Systemkomponenten nicht mit betroffen. Bei einer erfolgreichen Ransomware-Attacke sind somit nicht gleichzeitig alle IT-Systeme „infiziert" und das Schadensmaß wird reduziert.

Regelmäßig auf Gefahren hinweisen
Institutionen, Fachmedien und Experten auf dem Gebiet der Cyber-Security veröffentlichen nahezu täglich Informationen zu aktuellen Gefährdungen in der IT-Landschaft. Die eigene IT-Abteilung sollte entsprechende Informationen fortlaufend monitoren und für die eigene Organisation bewerten können. Bei konkreten Gefahren sollten alle Mitarbeitenden, z. B. durch einen internen Newsletter, umgehend informiert werden und Handlungsempfehlungen an die Hand gegeben werden.

Security by Design
Security by Design bedeutet, dass bei der Einführung neuer IT-Systeme und Anwendungen der Sicherheit von Anfang an umfassende Beachtung zu schenken ist. Im Rahmen von Digitalisierungsvorhaben werden häufig altgediente und „vertraute" Komponenten ausgetauscht. Viele Sicherheits- und Compliance-relevante Aspekte ändern sich hierdurch. Dieser Umstand ist bei Digitalisierungsvorhaben zu berücksichtigen, auch bei kleineren Projekten.

Der objektive Blick von außen
Sicherheit bedeutet auch, die eigenen Arbeitsabläufe stetig auf den Prüfstand zu stellen. Oftmals hilft hier der Blick von außen, um Lücken zu entdecken (Stichwort: Betriebsblindheit). Optimalerweise unterstützen Expertinnen und Experten vor einem Sicherheitsvorfall, indem gemeinsam IT-Systeme und Anwendungen abgesichert werden. Doch auch wenn es zu einem Sicherheitsvorfall gekommen ist, können Externe dabei helfen, das Schadensausmaß zu reduzieren und die Sicherheit wieder herstellen. &

Die Menschen hinter Althammer & Kill:

Fabian Brandenburger

Ja hallo, wer bist du denn?

Fabian: Hi, ich bin Fabian, 30 Jahre jung und komme aus Reilingen in Baden-Württemberg und habe klassisch Jura an der Uni Mainz studiert. Ich bin einer der Berater bei Althammer & Kill am Standort Mannheim.

Wie lange arbeitest du schon bei Althammer & Kill?

Fabian: So ziemlich genau seit 1 Jahr, seit dem 01.01.2021.

Was sind Deine Aufgaben?

Fabian: Ich bin Jurist im Bereich der Beratung bei A&K und bin spezialisiert auf größere Kunden, wie Wirtschaftsunternehmen und Diakonien.

Was gefällt dir besonders an der Tätigkeit des Beraters?

Fabian: Mir gefällt besonders gut, dass ich täglich mit den verschiedensten Fragestellungen zum Thema Datenschutz und Informationssicherheit konfrontiert bin. Aufgrund meiner Kunden sind dies immer sehr komplexe Sachverhalte, in die ich mich immer wieder neu eindenken und einarbeiten muss.
Mir gefällt es, optimale Prozesse und Lösungen zusammen mit unseren Kunden zu erarbeiten und gleichzeitig bei dem Kunden das Gespür für den Datenschutz zu intensivieren.

Wie sieht dein Alltag als Berater bei Althammer & Kill aus?

Fabian: Der Beratералltag kann sehr fordernd sein. Bei einigen Kunden muss erst noch ein Datenschutzmanagement aufgebaut werden und teilweise werden nicht immer gleich alle Verbesserungsvorschläge von dem Kunden angenommen. In der Regel sortiere ich die Anfragen morgens in unser Ticketsystem ein. Gleichzeitig priorisiere ich gewisse Anfragen und Themen.
Mein Anspruch ist stets, zumindest eine Eingangsmail an den Kunden unmittelbar zurückzusenden, damit dieser weiß, dass ich die Anfrage in Bearbeitung genommen habe. Mein Alltag ist auch sehr geprägt von der kollegialen Zusammenarbeit. Gerne tauschen wir uns dann über Beratungsthemen aus, um eine einheitliche Beratung zu gewährleisten.

Wo bist du für unsere Kunden unterwegs?

Fabian: Ich bin dem Althammer & Kill-Standort Mannheim, also Süddeutschland zugeordnet. Der Standort ist der jüngste von den Dreien (neben dem Hauptstandort Hannover und einem weiteren in Düsseldorf) und soll auch weiterhin wachsen. Die meisten meiner Kunden sind in Süddeutschland, grundsätzlich bin ich aber bundesweit im Einsatz. Künftig soll ich neben meiner Beratung auch Business Development am Standort in Mannheim betreiben. Das bedeutet, wir werden an Vorträgen etc. zum Thema Datenschutz und Informationssicherheit teilnehmen. Wenn dies wieder möglich ist auch Live, sodass ich auf solchen Veranstaltungen persönlich anzutreffen sein werde.

„Aus Datenschutzsicht wird es spannend, wie die Gerichte und die Politik zum Thema Datentransfer in Drittländer abschließend Stellung nehmen."

Welche Themen werden deiner Meinung nach besonders wichtig im Bereich IT und Datenschutz?

Fabian: Im Bereich Cyber Security sehe ich das Thema Phishing, Social Engineering und Internet of Things als Schwerpunktthemen. Aus Datenschutzsicht wird es spannend, wie die Gerichte und die Politik zum Thema Datentransfer in Drittländer abschließend Stellung nehmen. Ein wichtiges Thema seit Mitte 2020, aber es gibt noch keine klaren Vorgaben wie abschließend damit umgegangen werden soll. &

Nach den Google-Urteilen – Handlungsbedarf auf Millionen Webseiten

Das neue Jahr startete mit einem Knall! Und das obwohl vielerorts die „Böllerei“ zu Silvester verboten war. Innerhalb des ersten Quartals wurden zahlreiche wegweisende Urteile veröffentlicht, die Webseitenbetreibende und Datenschutzbeauftragte aufhorchen ließen.

Der Einsatz von Trackingtools wie Google Analytics sowie die generellen Einbindungen von Cookies, Diensten und Plugins stand schon lange in der Kritik. Mit den nun veröffentlichten Urteilen könnte sich das Thema endgültig erledigt haben. Zeitgleich entsteht massiver Handlungsbedarf auf Seiten der Webseitenbetreibenden.

Was ist geschehen?

Nahezu gleichzeitig veröffentlichten der Datenschutzbeauftragte aus Österreich und die französische Datenschutz-Aufsichtsbehörde CNIL Urteile zu artverwandten Themen. Der österreichische Datenschutzbeauftragte urteilte, dass der Einsatz von Google Analytics auf einer österreichischen Webseite bzw. die Übermittlung der IP-Adresse des Webseitenbesuchenden an Google, nicht rechtmäßig sei:

- Durch den Einsatz von Google Analytics würden personenbezogene Daten des Webseitenbesuchenden (einzigartige Nutzer-Identifikations-Nummern, IP-Adresse etc.) an Google übermittelt.
- Die Standarddatenschutzklauseln böten kein angemessenes Schutzniveau, da Google der Überwachung durch US-Geheimdienste (FISA 702) unterliege.
- Trotz Pseudonymisierung der personenbezogenen Daten sei es durch die große Anzahl an Daten, die im Internet anfallen, leicht möglich die betroffene Person zu identifizieren.

Der österreichische Datenschutzbeauftragte kommt damit zur Erkenntnis, dass „das Tool Google Analytics (jedenfalls in der Version vom 14. August 2020) somit nicht in Einklang mit den Vorgaben von Kapitel V DSGVO genutzt werden kann“. Zu einem Bußgeld ist es indes nicht gekommen – die Verarbeitung von personenbezogenen Daten mittels Google Analytics wurde jedoch untersagt.

Die CNIL hingegen hat größere Geschütze aufgefahren und Bußgelder in Höhe von 210 Millionen Euro verhängt (kumuliert). Betroffen sind Google und Facebook. Die CNIL wirft den Unternehmen vor, die Einwilligung zur Platzierung von Cookies sehr simpel, die Ablehnung jedoch deutlich schwerer gestaltet zu haben.

Auch ein Urteil aus München dürfte für Millionen von Webseiten Relevanz besitzen. Das LG München sprach einem Besucher einer Webseite 100 Euro Schadensersatz zu, da personenbezogene Daten (IP-Adresse) beim Besuch einer Webseite an Google übermittelt würden. Der Schadensersatzanspruch begründet sich aus dem individuell empfundenen Unwohlsein, welches durch die Übermittlung ausgelöst wurde. Hierbei handelt es sich um einen immateriellen Schaden, der gemäß der DSGVO geahndet werden kann. Ausschlaggebend für die Übermittlung der IP-Adresse war das dynamische Einbinden von Google Fonts. Die Richter erkannten die berechtigten Interessen der Betreiberin der Webseite nicht an - eine Übermittlung der IP-Adressen an Google wurde daher untersagt. Google Fonts lässt sich, anders als viele andere Drittanbieterdienste, auf der eigenen Webseite bzw. auf dem (Web)Server einbinden, sodass eine Übermittlung der IP-Adresse des Webseitbesuchenden an Google nicht notwendig ist.

Lessons Learned

Aus diesen Urteilen entsteht dringender Handlungsbedarf: Webseitenbetreibende sind aufgerufen, die Verarbeitungsvorgänge auf ihren Webseiten auf Rechtmäßigkeit zu überprüfen.

Überprüfung auf Analyse- und Tracking-Tools:

1. Prüfen Sie, ob Analyse- und Trackingtools auf Ihrer Webseite eingebunden sind. Eventuell ist das auch ohne Ihr Wissen durch Agenturen geschehen.
2. Prüfen Sie, ob es sich bei den eingesetzten Analyse- und Trackingtools um Lösungen von Drittanbietern handelt, die personenbezogenen Daten wie z. B. IP-Adressen in Drittstaaten übermitteln.
3. Unterbinden Sie solche Übermittlungen. Insbesondere dann, wenn es datenschutzkonformere Alternativen gibt, oder die Analyse- und Trackingtools keinen Mehrwert für Sie bieten.

Cookies auf Rechtmäßigkeit überprüfen:

1. Prüfen Sie, welche Cookies beim Aufruf Ihrer Webseite gesetzt werden. Sind diese technisch notwendig oder optional?
2. Prüfen Sie, ob die optionalen Cookies erst nach wirksamer Einwilligung gesetzt werden.
3. Stellen Sie sicher, dass die Einwilligung genauso einfach gestaltet ist wie die Ablehnung der Cookies.

Überprüfung auf sonstige eingebundene Drittanbieter:

1. Prüfen Sie, welche Dienste von Drittanbietern beim Aufruf Ihrer Webseite geladen werden.
2. Prüfen Sie, ob diese Drittanbieterdienste Verbindungen in Drittstaaten aufbauen.
3. Prüfen Sie, ob diese Drittanbieterdienste direkt auf der Webseite eingebunden werden können (siehe Google Fonts) bzw. greifen Sie auf datenschutzkonformere Alternativen zurück.
4. Stellen Sie andernfalls sicher, dass die eingebundenen Dienste erst nach einer Einwilligung Daten übermitteln.

Die Urteile sind nicht vom Himmel gefallen. Vielmehr wird das EuGH-Urteil (Schrems II) konsequenter umgesetzt; so wie es die Richter am EuGH von den Aufsichtsbehörden eingefordert haben. Die Zeit scheint gekommen, die Webseiten auf datenschutzkonforme Beine zu stellen.

Wenn es kritisch wird – Patchmanagement als Teil der Informationssicherheit

Mitte Dezember 2021. Was sich in den Nachrichten als „normales Softwareproblem“ ankündigte, wurde zu einem kosten- und zeitintensiven Treiber in Rechenzentren und IT-Infrastrukturen. Die beliebte Java Bibliothek Log4J hatte eine Schwachstelle, die es Angreifern ermöglichte, nur durch das Übermitteln bestimmter Zeichenketten Systeme zu übernehmen. Das Problem? Viele Softwarehersteller und IT-Rechenzentren mussten zunächst prüfen, ob entsprechende Bibliotheken auch bei Ihnen vorhanden sind.

Grundlage der vielen Überstunden war, dass die Bibliothek in vielen Software-Installationen vorhanden, eingesetzt oder zumindest installiert war. Selbst Anbieter von entsprechenden Systemen benötigten Zeit, um zu prüfen, ob Ihre Produkte von der Lücke betroffen waren. Der Wettlauf gegen die Zeit – es standen schon zahlreiche Anleitungen zur Ausnutzung der Schwachstelle bereit – hatte begonnen. Unternehmen, die noch kein entsprechendes Patchmanagement aufbauten, hatten nun die Aufgabe, schnell und effizient dieses vorrübergehend zu steuern. Hier sind diejenigen im Vorteil, die wissen, was für Systeme Sie betreiben und prüfen können, ob diese betroffen sind.
Kurzum: eine entsprechende Dokumentation in Form eines Verzeichnisses bleibt Grundlage für ein effektives Patchmanagement.

Prozesse zum Patch- und Änderungsmanagement

Doch nur weil ein Überblick vorhanden ist, bedeutet dies noch nicht, dass ein Patchmanagement somit reibungslos implementiert werden kann. Neben dem schnellen Eingreifen bei Sicherheitsproblematiken ist es wesentlich, dass Änderungen auch in die Prozesse der Unternehmen eingebunden sind. Wer darf Änderungen einspielen? Wie werden diese vorher geprüft? Wer muss zur Überprüfung der Funktionalität der Updates mit einbezogen werden?
Das Bundesamt für Sicherheit in der Informationssicherheit (BSI) hält für die Aufrechterhaltung der IT im Kontext des Patch- und Änderungsmanagements den Baustein „OPS.1.1.3: Patch- und Änderungsmanagement“ vor. Insgesamt 14 Maßnahmen referenziert das BSI zum ordnungsgemäßen Patchmanagement.
So sind häufig auftretende Probleme: Applikationen, die nicht mehr ordnungsgemäß funktionieren, plötzlich auftretende Schwachstellen, weil bestehende Konfigurationen überschrieben wurden oder ein Ausfall ganzer Systeme, da die Voraussetzungen für ein Patch nicht gegeben waren.

Effektives Patchmanagement benötigt aussagekräftige Dokumentationen.

Keine Zeit zu verlieren – Patchen als wesentliche Grundlage der Sicherheit

Schnelligkeit ist eine Prämisse für ein effektives Patch- und Änderungsmanagement. Im Worst-Case zählt jede Minute, um die entsprechenden Patches einzuspielen und so die Bedrohung für die Unternehmenswerte zu reduzieren. Die Grundhaltung, never change a running system, wird sonst zu einem kostenintensiven und unter Umständen existentiellen Risiko. Leider zeigt die Praxis all zu oft, dass Systeme nicht in Änderungsprozesse eingebunden und von zahlreichen Schwachstellen betroffen sind. Werden diese Systeme zu einem Einfallstor und ein Angreifer kann sich dort einnisten, beginnt das Aufklären durch forensische Maßnahmen.
Um schnell und effektiv agieren zu können ist selbstredend ein permanenter Blick auf die aktuellen Bedrohungen und

Vorgehen der Angreifenden zu wahren. Neben den entsprechenden Certs des Bundes und der Bundesländer, sind auch einschlägige Medien wie exploit-db ein guter Kompass für die Übersicht zur Bedrohungslage.

Erkennen Sie Problematiken für Ihren Unternehmenskontext, thematisieren Sie diese und schaffen Sie sich ein Gremium, welches die aktuellen Bedrohungen einordnen und bewerten kann. Statten Sie dieses Gremium mit einer entsprechenden Handlungsbefugnis aus und entwickeln Sie Maßnahmen und Strategien, um auf diese Bedrohungen hin bewusst und sinnvoll agieren zu können.

Gemeinsam gegen aktuelle Bedrohungen

Wir unterstützen Sie selbstverständlich bei auftretenden Problematiken rund um Schwachstellen und Sicherheit. Ob bei der Einbindung des Patch- und Änderungsmanagements in Ihr bestehendes Informationssicherheitsmanagementsystems nach ISO 27001, oder bei der zeitnahen Sensibilisierung, Einschätzung und Unterstützung akuter Sicherheitsproblematiken sind wir Ihr bewährter Partner. Zahlreiche ausgebildete Informationssicherheitsspezialisten und „gute Hacker“ stehen Ihnen mit der entsprechenden Expertise zur Verfügung.

Zum Schluss: Die A&K Checkliste

Folgende Punkte möchten wir Ihnen als kleine Checkliste mit auf den Weg geben:

- Alle Systeme sind dokumentiert und ausreichend beschrieben.
- Prozesse zum Patchmanagement sind definiert und implementiert.
- Ein Prozess zur Erkennung und Behebung kritischer Schwachstellen ist in Ihr Notfallmanagement mit eingebunden.
- Ein Überblick über Ansprechpartner und verlässliche Software-Quellen ist angelegt.
- Alle Prozesse und Maßnahmen bezüglich des Patchmanagements werden überprüft und ausgewertet.
- Neue Maßnahmen werden, insofern Mängel festgestellt wurden, entwickelt und umgesetzt. &

Hinweisgebersystem – Von der Pflicht zur Chance

Seit Dezember 2021 greift die EU-Whistleblower-Richtlinie. Auch wenn der nationale Gesetzgeber bislang kein nationales Gesetz auf den Weg gebracht hat – viele gute Gründe sprechen für die Implementierung eines Hinweisgebersystems.

Ganz allgemein sollten Organisationen Regeln einhalten, um (Haftungs-)Risiken zu reduzieren und Chancen zu nutzen. Im ureigensten Interesse liegt natürlich auch die Einhaltung interner Richtlinien und Prozessabläufe. Die Einhaltung von Regeln – also Regelkonformität – wird als Compliance bezeichnet. Compliance betrifft sowohl Unternehmen der Privatwirtschaft, Vereine, Verbände, Stiftungen, Behörden und sonstige Einrichtungen der öffentlichen Hand wie auch sonstigen Organisationen (z. B. Nichtregierungs-Organisationen) – also jegliche Organisationsform unabhängig von der Größe. Die Folgen nicht oder nur teilweise regelkonformen Verhaltens ist mit vielen Risiken verbunden und kann existenzbedrohend sein. Berühmt ist das dem ehemaligen stellvertretenden US-Justizminister Paul McNulty zugeschriebene Zitat: *„If you think compliance is expensive, try non-compliance."*

In der Praxis kann dieses bedeuten:

- Bußgelder seitens öffentlicher Stellen
- Schadensersatzansprüche von Lieferanten, Kunden und Mitarbeitenden
- Nachteile in individuellen Arbeitsgerichtsprozessen
- Arbeitsrechtliche Sanktionen
- (Haft-) Strafen für Führungskräfte und Mitarbeitende (sog. Garantenstellung)
- Schadensersatzansprüche gegen Führungskräfte und Mitarbeitende
- Ausschluss von öffentlichen Aufträgen
- Verlust von Wettbewerbsfähigkeit
- Reputationsschäden
- Schwierigkeiten bei der Auftragserlangung durch Integritätsprüfungen
- Verlust von Mitarbeitenden & Knowhow
- Steuernachzahlungen
- Entzug von Genehmigungen oder Betriebserlaubnissen
- Berufsverbote

Dabei geht es nicht allein um Folgen für den „normalen" Mitarbeitenden oder die Organisation selbst, sondern vor allem um die (persönliche) Haftung der Organe (Vorstand, Geschäftsführung, Aufsichtsrat, Beirat u. ä.). Zu nennen ist hier in erster Linie die sog. Legalitätspflicht. Unternehmensleitungen sind verpflichtet, dafür zu sorgen, dass die Organisation nicht gegen Gesetze verstößt.

Auch wenn die Pflicht zur Einhaltung die Organisation primär selbst betrifft, kommt eine persönliche Haftung der Vertreter in Betracht, wenn keine angemessenen Schutzmechanismen installiert wurden.

Hinweisgebenden eine Plattform bieten

"Wenn Sie mit unserer Leistung zufrieden waren, sagen Sie es weiter. Wenn nicht, sagen Sie es uns." – Diese oder ähnliche Formulierungen sind Ihnen sicherlich das ein oder andere Mal über den Weg gelaufen. Die Intention dahinter ist klar: Image-Verstärkende Informationen sollen nach Außen kommuniziert, negative Erfahrungen jedoch intern aufgearbeitet werden. So verhält es sich auch mit der Entgegennahme von Hinweisen. Erinnern Sie sich an den Whistleblower Edward Snowden? Aus der Compliance-Perspektive ist diese Person ein Hinweisgeber. Er hat auf Missstände aufmerksam gemacht, indem er diese nach außen getragen hat. Organisationsleitungen sind dazu verpflichtet, auf die Einhaltung hinzuwirken und Missstände aufzudecken sowie diesen einen Riegel vorzuschieben. Das kann jedoch nur funktionieren, wenn es innerhalb der Organisation Personen gibt, die nicht wegschauen, wenn Unrecht geschieht. Die EU-Whistleblower-Richtlinie will diesen Menschen Schutz bieten und Organisationen dazu verpflichten, geeignete Meldewege einzurichten: sogenannte (anonyme) „Hinweisgebersysteme". Was auf dem ersten Blick wie eine neue Pflicht wirkt, bietet echte Chancen. Denn ein wirksames Hinweisgebersystem schützt vor allem auch die eigene Organisation!

„If you think compliance is expensive, try non-compliance."

Paul McNulty
ehemaliger stellvertretender US-Justizminister

Gute Gründe sprechen dafür

Laut EU-Whistleblower-Richtlinie sind Organisationen seit Dezember 2021 und ab 250 Mitarbeitende dazu verpflichtet, ein Hinweisgebersystem zu implementieren. Ende 2023 beträgt der Schwellenwert nur noch 50 Mitarbeitende. Wenn also zum gegenwärtigen Zeitpunkt keine Pflicht besteht, sprechen dennoch viele gute Gründe für eine Implementierung:

1. Auch ohne Hinweisgebersystem sind Organisationsleitungen verpflichtet, Compliance-Anforderungen einzuhalten. Ein wirksames Hinweisgebersystem stellt eine wichtige Informationsquelle dar und trägt zur Enthaftung der Organisationsleitung bei.
2. Anonymen Hinweisgebern geht es nicht um Ruhm. Diese Menschen wollen der Organisation helfen und Schaden abwehren. Fehlverhalten und Missstände können durch vertrauenswürdige Meldewege reguliert werden, ohne dass ein Image-Schaden befürchtet werden muss.
3. Die konsequente Einhaltung aller Compliance-Anforderungen schafft Vertrauen bei Mitarbeitenden, Kunden, und Lieferanten. Ein offen kommuniziertes Hinweisgebersystem verstärkt diesen Eindruck.

Auf die richtige Umsetzung kommt es an

In der Praxis haben sich IT-gestützte Meldeportale, die über das Internet erreichbar sind, anstelle von E-Mails oder Ähnlichem, bewährt. Diese erlaubt dem Empfänger die direkte Kommunikation mit dem Meldenden – und das völlig anonym. Neben der Anonymität sollten noch folgende Aspekte bedacht werden:

1. Die Bewertung von gemeldeten Vorfällen sollte durch ausgewiesene und zur Verschwiegenheit verpflichtete Experten erfolgen.
2. Verfahren zur Analyse des Vorfalls müssen innerhalb von sieben Tagen eröffnet werden.
3. Nach Abschluss des Verfahrens ist der Hinweisgebende über den Ausgang in Kenntnis zu setzen.
4. IT-gestützte Hinweisgebersysteme müssen höchsten Datenschutz- und Informationssicherheits-Standards entsprechen. Die Durchführung einer Datenschutz-Folgenabschätzung ist daher obligatorisch.
5. Durch die Erhebung personenbezogener Daten sind die datenschutzrechtlichen Pflichten einzuhalten, denn in den meisten Fällen enthalten Meldungen höchst sensible Informationen wie z. B. Anschuldigungen zu möglichen Straftaten. &

Sie möchten mehr erfahren, z. B. über das Hinweisgebersystem von Althammer & Kill?

Unsere Compliance-Experten stehen Ihnen mit Rat und Tat zur Seite.

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

Unser Service-Desk bei der Arbeit

Frank Boje ist Berater für Datenschutz und Informationssicherheit. Als Mitarbeiter in unserem Service-Desk hat er stets ein offenes Ohr für Fragen, Sorgen und Anmerkungen unserer Kundinnen und Kunden.

Egal, ob es um die Prüfung von Verträgen oder um die Umsetzung der neuesten Gesetzesänderung geht, beim Service-Desk ist man zunächst immer an der richtigen Adresse.

Was sind die häufigsten Anfragen, die über den Service Desk reinkommen?

Frank: Viele unserer Kunden veröffentlichen als Kontaktadresse für Datenschutzanfragen die Support-E-Mail kontakt-dsb@althammer-kill.de. Daher kommen insbesondere Anfragen von Betroffenen zuerst im Service-Desk an. Dabei handelt es sich in der Regel um Auskunftsersuchen zu den gespeicherten Daten, aber auch Anfragen zum Löschen von personenbezogenen Daten.

Was ist dein größtes Projekt bisher gewesen?

Frank: Da ich neben meiner Rolle als Mitarbeiter im Service-Desk auch der Datenschutzkoordinator für Althammer & Kill bin, ist das glaube ich mein größtes Projekt. Bei den Kundenprojekten sind die die Größten, bei denen Du wirklich alles von Anfang an machst, also begonnen bei der Bestandsaufnahme über die Maßnahmenplanung zusammen mit dem Kunden bis hin zur regelmäßigen Betreuung.

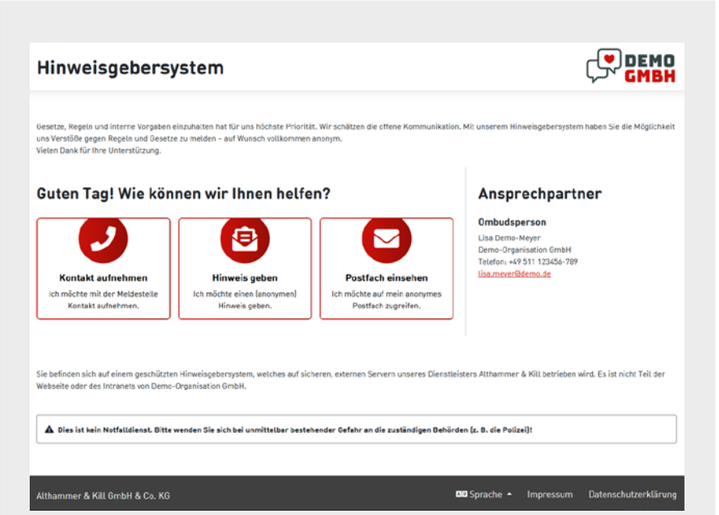
Wie erreicht man am besten den Service Desk?

Frank: Der Service-Desk ist von 09:00 Uhr bis 17:00 Uhr telefonisch über die +49 511 330603-90 in Hannover bzw. +49 211 966748-90 in Düsseldorf und +49 621 121847-90 in Mannheim zu erreichen. Wer lieber eine Mail schreibt, kann dies rund um die Uhr tun. Die kontakt-dsb@althammer-kill.de haben wir ständig im Blick und antworten in der Regel noch am selben Tag.

Welche Themen beschäftigen unsere Kundinnen und Kunden am meisten?

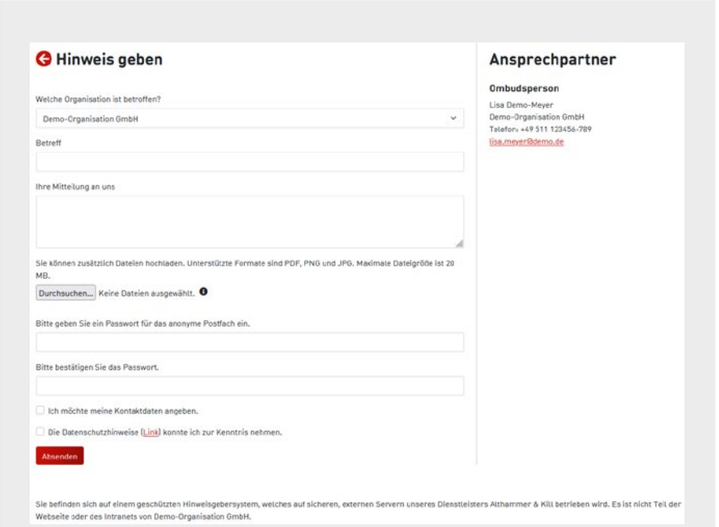
Frank: Das ist sehr unterschiedlich und lässt sich von uns gar nicht vorhersagen. Wenn der europäische Gerichtshof eine richtungsweisende Entscheidung fällt, dann kann es gut sein, dass sich auch viele unserer Kundinnen und Kunden mit diesem Thema beschäftigen müssen. Etwas, was regelmäßig vorkommt, ist die Prüfung von Verträgen zur Auftragsverarbeitung. Dort ist auch ein sehr positiver Trend erkennbar. Die Kundinnen und Kunden hinterfragen selbst bei dem Einsatz neuer Software oder Dienstleister, ob dies mit dem Datenschutz vereinbar ist.

Das Thema „Hinweisgebersystem" wird tendenziell immer wichtiger und wird im Jahr 2022 einige Unternehmen beschäftigen. Welche Aufgaben hat hierbei der Service Desk?



Hinweisgebersystem, Startseite

Frank: Die „Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden" wird uns dieses und die folgenden Jahre tatsächlich sehr beschäftigen.
Die Hinweisgeberrichtlinie enthält selbst verschiedene Regelungen zum Datenschutz. Z. B. im EG 54, 74 oder 76. Das heißt, wenn ein Mandant ein Hinweisgebersystem einführen möchte, müssen wir ihn in den Fragen des Datenschutzes kompetent beraten. Auf der anderen Seite bietet Althammer & Kill eine eigene Plattform für Hinweisgeber an. Dort ist es wichtig, unterschiedliche Mel-

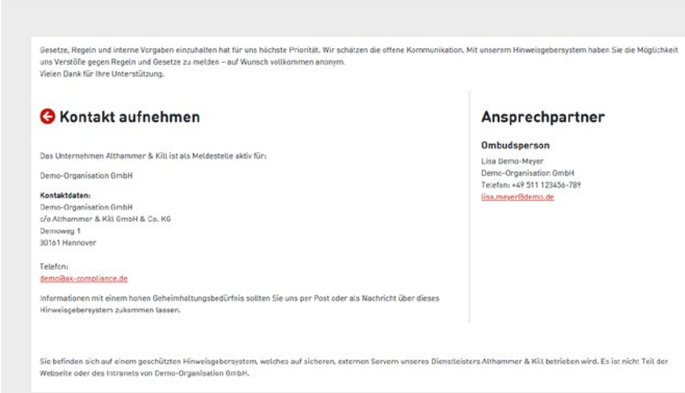


Hinweisgebersystem, Formular

dekanäle zur Verfügung zu stellen. Ein regelmäßig fachlich kompetent besetzter Service-Desk ist in solch einem Fall unumgänglich. So sieht der Erwägungsgrund 74 auch vor, dass „die für die Bearbeitung der Meldungen zuständigen Mitarbeiter … speziell geschult und auch mit den geltenden Datenschutzvorschriften vertraut“ sind, „damit sie die Meldungen bearbeiten und die Kommunikation mit dem Hinweisgeber sowie geeignete Folgemaßnahmen sicherstellen können.“ Mit einem „einfachen Callcenter“ kommt man da nicht weiter, deshalb sind wir ja da.

Was war die skurrilste Anfrage, die du bisher bekommen hast?

Frank: Das ist schwer zu beantworten. Da wir bei einigen Autohäusern ein Mandat als Datenschutzbeauftragter haben, gibt es immer wieder Anfragen von potentiellen Kunden, die, statt die Rufnummer des Autohauses zu wählen, die veröffentlichte Telefonnummer des Datenschutzbeauftragten anrufen, um sich nach einem bestimmten Auto zu erkundigen.


Gesetze, Regeln und interne Vorgaben einzuhalten hat für uns höchste Priorität. Wir schätzen die offene Kommunikation. Mit unserem Hinweisgebersystem haben Sie die Möglichkeit uns Verstöße gegen Regeln und Gesetze zu melden – auf Wunsch vollkommen anonym.
Vielen Dank für Ihre Unterstützung.

Kontakt aufnehmen

Das Unternehmen Althammer & Kill ist als Meldestelle aktiv für:

Demo-Organisation GmbH

Kontaktdaten:
Demo-Organisation GmbH
c/o Althammer & Kill GmbH & Co. KG
Demoweg 1
30161 Hannover

Telefon:
demo@ak-compliance.de

Informationen mit einem hohen Geheimhaltungsbedürfnis sollten Sie uns per Post oder als Nachricht über dieses Hinweisgebersystem zukommen lassen.

Ansprechpartner

Ombudsperson
Lisa Demo-Meyer
Demo-Organisation GmbH
Telefon: +49 511 123456-789
lisa.meyer@demo.de

Sie befinden sich auf einem geschützten Hinweisgebersystem, welches auf sicheren, externen Servern unseres Dienstleisters Althammer & Kill betrieben wird. Es ist nicht Teil der Webseite oder des Intranets von Demo-Organisation GmbH.

Hinweisgebersystem, Kontakt

Aber der Fall, der uns am Meisten zum Schmunzeln gebracht hatte, war wohl der Autofahrer, der nicht mehr aus der Tiefgarage des Einkaufszentrums kam, weil er sein Parkticket verloren hatte. Da das Einkaufszentrum ebenfalls zu unseren Mandanten zählt und es in der Tiefgarage eine Videoüberwachung gab, war die auf dem Hinweisschild veröffentlichte Telefonnummer des Datenschutzbeauftragten seine letzte Rettung. Zum Glück konnten wir dem Unglücklichen die Nummer des Centermanagements raussuchen, sodass er gerettet werden konnte und nicht in der Tiefgarage übernachten musste.

Wie eng arbeitest du mit den anderen Beratern zusammen?

Frank: Ohne eine gute Zusammenarbeit geht gar nichts. Nicht nur zwischen Service Desk und den Beratenden, auch bei den Beratenden untereinander. Datenschutz und Compliance sind so umfangreiche Fachgebiete, dass wir alle von dem interdisziplinären Team bei Althammer & Kill profitieren. Auch im Service Desk können die Fragen mal so speziell sein, dass es einfacher ist einen Kollegen mit ins Boot zu nehmen, der mit dem Thema schon mehrfach zu tun hatte, als sich das gesamte Thema komplett allein zu „erarbeiten“. &

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.
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
Schutzgebühr Print-Ausgabe: 5,– €

Veranstaltungen und Termine

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

Hier klicken oder scannen!

5. April 2022 – Webinar
LearnBase – Einführungs-Webinar
Fortbildungen sind in Zeiten von Digitalisierung, Homeoffice und Kontaktverboten schwierig geworden. Vielfach besteht der Wunsch, auf neue Möglichkeiten des Lernens zurückzugreifen. Wir zeigen, warum LearnBase die richtige Wahl für digitale Fortbildungen ist und machen eine Tour durchs System.

26. April 2022 – Online-Seminar
Privacy by Design – Datenschutz für Software-Entwickler
Wenn Software die Datenschutz-Gesetze verletzt, drohen Bußgelder und Reputations-Schäden. Je später im Entwicklungsprozess der Datenschutz berücksichtigt wird, desto teurer und zeitaufwendiger sind die Reparaturen. Unser Seminar vermittelt an praktischen Beispielen das Grundwissen, um von Anfang an Datenschutz-freundliche Entscheidungen zu treffen und umzusetzen. Die Teilnehmer lernen die Grundprinzipien, die sie bei Design und Implementierung im Blick behalten sollten.

ALTEN PFLEGE
Die Leitmesse 2022

26.–28. April, Essen
Messe Altenpflege 2022
Hier können Sie am Stand von LearnBase auch den ein- oder anderen Mitarbeitenden von Althammer & Kill treffen.

28.04.–05.07.
Microsoft NGO-Tour 2022 mit Althammer & Kill
Es erwarten Sie Praxisvorträge zu konkreten Digitalisierungsprojekten und Experten-Sessions zu den Themen Datenschutz, Compliance und Cybersicherheit.

10.–11. Mai 2022 – 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.

17. Mai 2022 – Online Seminar
Hackerangriffe - So schützen Sie Ihre Organisation!
Systeme werden immer sicherer und dennoch sind erfolgreiche Hackerangriffe an der Tagesordnung. Wie passt das zusammen? Häufig sitzt das Problem hierbei vor dem Computer, denn Menschen können zwar ein effektiver Schutz gegen Angriffe sein, sie aber genauso gut auslösen. Cybersecurity im Zeitalter von Cloud und Co. bedeutet vor allem, dass ein Bewusstsein bei Mitarbeitenden geschaffen werden muss.

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

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

Althammer & Kill GmbH & Co. KG

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

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

ISO 9001:2015

Mitgliedschaften

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