Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2018

Liebe Leserin, lieber Leser,

die Vorbereitungen für die neuen Datenschutz-Gesetze laufen auf Hochtouren: Ab dem 25.05.2018 gelten veränderte Bedingungen im Datenschutz mit einer Vielzahl neuer Auflagen. Höchste Zeit also, sich damit auseinanderzusetzen. Für Fragen und Unterstützung stehen wir Ihnen gern mit Rat und Tat zur Seite.

Was ändert sich eigentlich für Cloud-Nutzer? Und was zählt überhaupt zum Cloud-Computing? Die Wahrscheinlichkeit, dass Sie unbewusst Cloud-Dienste nutzen, ist recht groß. Die Hintergründe und die gesetzlichen Rahmenbedingungen stellen wir Ihnen in unseren Beiträgen auf den Seiten 5 und 6 vor.

Die Sensibilisierung Ihrer Mitarbeiterinnen und Mitarbeiter ist wichtiger denn je. Der „Datenschutz-Parcours“ bietet eine Alternative zu klassischen Schulungen. Lesen Sie ab Seite 8, wie der Umgang mit Datenschutz und Informationssicherheit praxisnah erarbeitetet werden kann.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Dashcam im Auto: Bußgeld!

Sie waren schon einmal Opfer einer Unfallflucht? Dann verstehen Sie vermutlich jeden, der eine Dashcam einsetzt. Das ist eine Videokamera auf dem Armaturenbrett oder in der Windschutzscheibe. Sie zeichnet auf, was vor oder hinter dem Auto passiert. Das Problem: Sie riskieren damit ein Bußgeld!

Eine Frau in München hatte genug. Vandalen hatten ihr teures Auto beschädigt. Sie waren ungestraft davongekommen. Sie selbst blieb auf ihrem Schaden sitzen. Deshalb brachte sie kurzerhand vorne und hinten im Fahrzeug eine Videokamera an. Diese Kameras liefen immer, während sie ihr Auto am Straßenrand parkte.

In dieser Ausgabe:

Schon bald zeigte sich, dass das an sich eine gute Idee war. Ein zunächst unbekannter Fahrer streifte ihr Fahrzeug und fuhr einfach weiter. Sein Kennzeichen war in einer der Videoaufnahmen deutlich zu sehen. Diese Aufnahme übergab sie der Polizei. Der Halter war leicht zu ermitteln. Die Frau konnte erfolgreich Schadensersatz geltend machen.

Erst ein Erfolg, dann gibt's Ärger

Dann allerdings bekam sie Ärger. Die Kameras waren nämlich so eingestellt, dass sie jeweils mindestens ein Fahrzeug vor und eines hinter dem Auto der Frau erfassten. Die Folge: Wenn jemand in einem dieser Fahrzeuge saß, war er auf den Aufnahmen zu sehen. Die Polizei vermutete einen Verstoß gegen den Datenschutz und informierte das Bayerische Landesamt für Datenschutzaufsicht.

150 Euro Bußgeld

Das Landesamt erließ einen Bußgeldbescheid gegen die Frau. Damit war sie nicht einverstanden und legte Einspruch beim zuständigen Amtsgericht München ein. Letztlich brachte ihr dies nichts. Das Amtsgericht verurteilte sie zu einer Geldbuße von 150 Euro.

Kein „permanentes Filmen ohne Anlass"!

Die Begründung spart nicht mit deutlichen Worten. Es heißt dort unter anderem:

- Das Interesse der gefilmten Personen überwiegt. Ihr Recht auf informationelle Selbstbestimmung wird unzulässig beeinträchtigt.
- Das Interesse an der Aufdeckung einer potenziellen Straftat muss deshalb zurückstehen.
- Das „permanente anlasslose Filmen" des Straßenraums vor und hinter dem geparkten Fahrzeug stellt einen schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung dar.
- „Es geht nicht an, dass 80 Millionen Bundesbürger mit Kameras herumlaufen, um irgendwelche Situationen aufnehmen zu können, die eine Straftat aufdecken könnten."
- „Eine permanente Überwachung jeglichen öffentlichen Raumes durch Privatbürger ist nicht zulässig."

Ein Urteil mit Folgen

Diese Überlegungen des Gerichts gelten auch für das Filmen während der Fahrt. Es macht auch keinen Unterschied, ob es sich um ein Privat- oder um ein Unternehmensfahrzeug handelt. Angesichts der Diebstahlrisiken bei Lieferfahrzeugen gibt es zu dem Urteil auch kritische Stimmen. Sie helfen im Ernstfall allerdings zunächst einmal nichts. &

Impressum

Redaktion/V. i. S. d. P.:
Niels Kill, 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.

Fotos mit Mini-Figuren:
© Katja Borchhardt
www.miniansichten.de

Anschrift:
Althammer & Kill GmbH & Co. KG
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Schutzgebühr Print-Ausgabe: 10,– €

3

Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2018

ALTHAMMER & KILL

Regeln Sie Ihren digitalen Nachlass!

Nur 20 % aller Internetnutzer haben irgendwie geregelt, was nach ihrem Tod mit den Accounts bei Facebook, WhatsApp & Co. geschehen soll. Bei den Internet-nutzern der Generation 65 plus sind es – man mag es kaum glauben – sogar nur 4 %! Das ist das Ergebnis einer repräsentativen Umfrage des Digitalverbands Bitkom. Alles nicht so schlimm? Dieser lockere Spruch trägt so lange, bis es ernst wird.

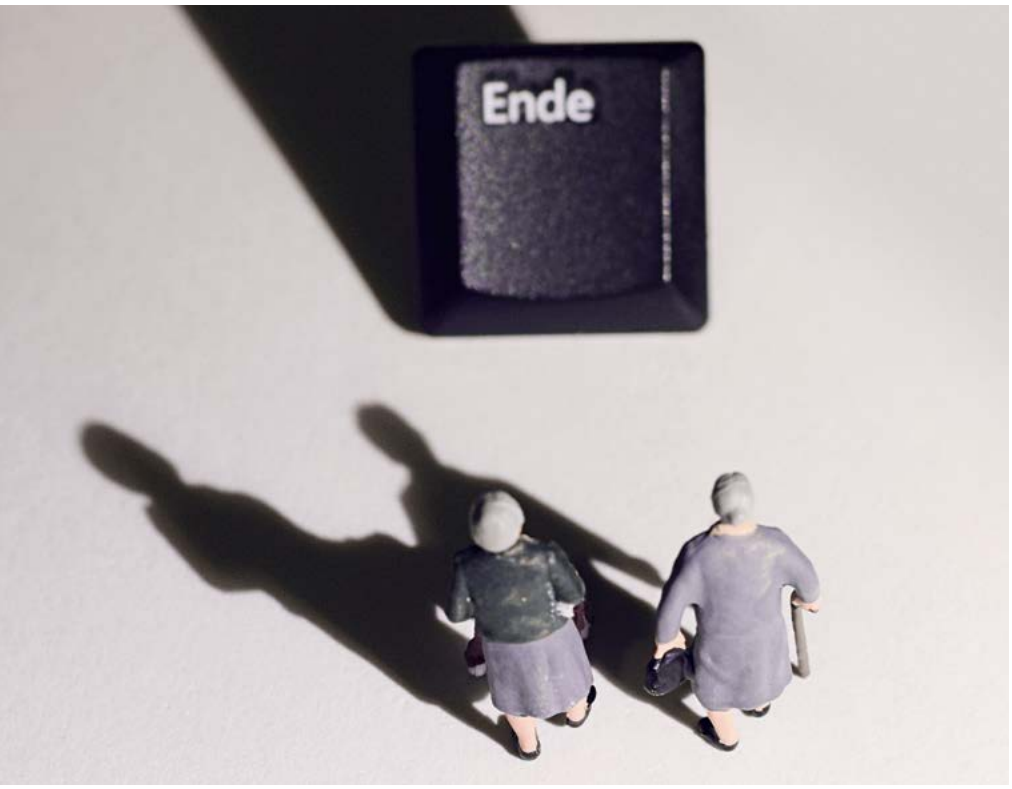
Viele Menschen leben heute regelrecht digital. Die Bankverbindung, der Stromvertrag – alles läuft über das Internet, schriftliche Unterlagen existieren überhaupt keine mehr. Bilder sind in einer Cloud abgelegt oder auf einem Smartphone, beides natürlich mit Passwort gesichert. Der gesamte Austausch mit Freunden und Bekannten läuft über Facebook, Threema usw.

Mailaccount am Arbeitsplatz

Und was geschieht im Todesfall? Kein Thema, dem man sich gern widmet. Sollte man aber! Im Unternehmen gibt es meistens Regelungen, die Lösungen ermöglichen. Das gilt vor allem für den Zugriff auf den dienstlichen Mailaccount. Ob durch eine Regelung in einer Betriebsvereinbarung oder im Arbeitsvertrag – in irgendeiner Form ist meistens vorgesehen, dass ein Team aus IT-Abteilung, Betriebsrat und Datenschutzbeauftragtem die Nachrichten sichtet. Ärger ist hier in der Praxis selten. Kaum jemand verhält sich heute noch so ungeschickt und öffnet dabei beispielsweise erkennbar private Mails.

Fehlender Überblick im Privatbereich

Im privaten Bereich sieht es weit übler aus. So banal es klingt: Hier fehlt meist schon der Überblick, welche Accounts überhaupt existieren. Früher konnten die Hinterbliebenen zum Beispiel Kontoauszüge durchsehen. Diese gaben oft erste wichtige Hinweise, etwa hinsichtlich bestehender Abos. Und Vieles, etwa eine abonnierte Zeitung, wurde sichtbar ins Haus geliefert. Heute kommt die Zeitung oft elektronisch. Das Bankkonto wird ausschließlich über das



Internet geführt. Die Kontoauszüge sind unzugänglich verschlüsselt in einem Ordner auf dem PC abgelegt.

Vollmacht für das Girokonto

Auch wenn es auf den ersten Blick nur wenig mit dem elektronischen Nachlass zu tun hat: Vor diesem Hintergrund ist es wichtig, möglichst jemandem eine Vollmacht für das Girokonto einzuräumen. Dies geschieht normalerweise direkt bei der Bank. Sinnvoll ist allein eine Vollmacht, die über den Tod hinaus gilt. Sie setzt natürlich beträchtliches Vertrauen voraus. Aber anders lässt sich kaum sicherstellen, dass im Todesfall schnell zu klären ist, wohin beispielsweise Zahlungen für elektronische Abonnements gehen.

Wunsch und Wirklichkeit

Die Empfehlung, eine vollständige und stets aktuelle Liste aller derartigen Vertragsbeziehungen zu führen, ist natürlich richtig. Aber in der Praxis klappt das nur selten. Und selbst wenn eine solche Liste existiert, wird sie vor allem nach einem unerwarteten Tod oft genug nicht gefunden.

Einzelverfügungen für bestimmte Dienste

Oft will jemand sicherstellen, dass Hinterbliebene zum Beispiel unbedingt auf eine bestimmte Cloud zugreifen können. Das kommt etwa vor, wenn dort sämtliche persönlichen Fotos aus Jahren hinterlegt sind. Theoretisch wäre es möglich, schon zu Lebzeiten mit dem Betreiber eine Zugriffsberechtigung zu vereinbaren. In der Praxis funktioniert dies jedoch kaum.

Eine Alternative besteht darin, eine ausdrückliche handschriftliche (!) Verfügung mit Datum und Unterschrift zu treffen, die das Nötige festlegt. Diese Verfügung kann man entweder zu Hause oder bei einem Notar hinterlegen. Möglich ist auch, sie demjenigen in die Hand zu geben, für den sie gelten soll.

Testament – ja, aber …

Solche Einzelfestlegungen für bestimmte Accounts oder Clouds führen im Zweifel eher zum Erfolg als allgemeine Verfügungen beispielsweise in einem Testament. Sie stellen nicht immer sicher, dass Hinterbliebene das Fernmeldegeheimnis überwinden können.

Das Fernmeldegeheimnis stellt das eigentliche Problem dar, nicht etwa das Erbrecht generell. Denn auch Accounts gehören zum Nachlass. Und dass die Erben den gesamten Nachlass erhalten, ergibt sich ohne Weiteres aus dem Bürgerlichen Gesetzbuch. Dort steht allerdings nicht, dass Erben einfach das Fernmeldegeheimnis durchbrechen können. Bei notariellen Testamenten schlagen die Notare Formulierungen vor, die auch diesen Aspekt abdecken. Allerdings kosten notarielle Testamente etwas.

Bewusste Löschungsanordnungen

Manchmal gibt es freilich auch Informationen, die man ganz bewusst lieber mit ins Grab nehmen möchte. Auch dann lohnt eine ausdrückliche Festlegung. Geeignet wäre dafür etwa folgende Formulierung in einer handschriftlichen Verfügung: „Ich möchte, dass mein Facebook-Account nach meinem Tod gelöscht wird. Vorher soll niemand vom Inhalt Kenntnis nehmen.“ &

5 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2018

ALTHAMMER & KILL

Datenschutz-Grundverordnung: Was ändert sich für Cloud-Nutzer?

Wer in Zukunft Cloud-Dienste verwenden will, muss die Vorgaben der Datenschutz-Grundverordnung (DSGVO) beachten. Doch was ändert sich im Vergleich zu heute?

Cloud Computing, also die Nutzung von IT-Ressourcen wie Rechenleistung, Applikationen und Speicherkapazität über das Internet, wird immer beliebter. Zwei von drei Unternehmen haben in Deutschland im Jahr 2016 Cloud Computing eingesetzt, so der Digitalverband Bitkom. Wenn in Kürze die Zahlen für 2017 vorliegen, wird zweifellos eine weitere Steigerung festzustellen sein.

Aus Auftragsdatenverarbeitung wird Auftragsverarbeitung

Aus Sicht des Datenschutzes handelt es sich bei Cloud Computing in der Regel um eine Auftragsdatenverarbeitung. Diesen Begriff findet man in der Datenschutz-Grundverordnung (DSGVO/GDPR), die ab 25. Mai 2018 anzuwenden ist, nicht mehr. Dort spricht man nur noch von Auftragsverarbeitung. Ist dies die einzige Änderung im Datenschutz, die Cloud-Nutzer kennen sollten? Nein, das ist sie nicht.

Cloud-Nutzer bleiben in der Verantwortung, aber ...

Umfragen unter Cloud-Anwendern zeigen regelmäßig, dass nicht wenige Unternehmen die Verantwortung für den Schutz der Daten in der Cloud beim jeweiligen Cloud-Betreiber sehen, nicht aber bei sich. Tatsächlich ist und bleibt es so, dass das Unternehmen als Cloud-Nutzer und damit die verantwortliche Stelle im Unternehmen für den angemessenen Datenschutz Sorge tragen muss. So muss das Unternehmen unter anderem geeignete technisch-organisatorische Maßnahmen für den Schutz der Cloud-Daten mit dem Cloud-Betreiber vertraglich vereinbaren.

Durch die DSGVO neu hinzu kommt, dass ein Cloud-Betreiber als Auftragsverarbeiter auch zum Verantwortlichen wird, wenn er gegen die Vorgaben des Datenschutzes verstößt, also die Daten zum Beispiel zweckentfremdet. Dadurch wird aber nicht etwa die Verantwortung vom Cloud-Nutzer auf den Cloud-Betreiber übertragen. Vielmehr bleibt auch der Cloud-Nutzer verantwortlich. Aus der Verantwortung des Cloud-Nutzers ergibt sich, dass er wie bisher nicht einfach einen beliebigen Cloud-Anbieter auswählen sollte.

Cloud-Anbieter bei Auswahl genau prüfen

Die DSGVO fordert von Cloud-Nutzern, dass sie nur solche Cloud-Anbieter beauftragen, die hinreichende Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen so durchführen, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und die Rechte der betroffenen Person schützt.

Neu ist die Möglichkeit unter der DSGVO, dass sich die Einhaltung genehmigter Verhaltensregeln oder eines genehmigten Zertifizierungsverfahrens durch einen Auftragsverarbeiter als Faktor heranziehen lässt, um hinreichende Garantien nachzuweisen, wie es die Verordnung sagt. Das bedeutet insbesondere, dass man

als Cloud-Nutzer auf Cloud-Zertifizierungen beim Cloud-Betreiber achten sollte, die den Vorgaben der DSGVO entsprechen. In Zukunft können also geeignete Cloud-Zertifikate zu einer wichtigen Hilfe bei der Auswahl werden.

Angemessenes Datenschutzniveau ist entscheidend

Viele Clouds werden außerhalb der EU betrieben. Dann liegt eine Datenübermittlung in Drittstaaten vor, wenn personenbezogene Daten in die Cloud übertragen werden. Gleich ob es sich um die USA oder einen anderen Drittstaat handelt: Es muss grundsätzlich geprüft werden, ob das dortige Datenschutzniveau dem der DSGVO entspricht. Hierfür gibt es verschiedene Instrumente. Darunter eine Angemessenheitsentscheidung der EU-Kommission für bestimmte Länder und die sogenannte Privacy-Shield-Vereinbarung mit den USA.

Da gegenwärtig gerichtliche Prüfungen auf EU-Ebene in diesem Bereich bevorstehen, sollten Sie jeweils aktuell bei Ihrer Datenschutzbeauftragten oder Ihrem Datenschutzbeauftragten fragen, welche Grundlage für eine Datenübermittlung in Drittstaaten gilt.

Datenpannen können auch in Clouds passieren

Wird der Datenschutz verletzt, kommt es also zu einer Datenpanne, haben viele Unternehmen Schwierigkeiten, dies zeitnah festzustellen. Die verschärften Meldepflichten bei Datenschutzverletzungen (72-Stunden-Frist) vergrößern diese Probleme. Im Fall einer Cloud ist es für den Cloud-Nutzer meist sogar noch schwieriger, eine Datenpanne zu ermitteln, als es im eigenen Netzwerk schon der Fall wäre. Die DSGVO sieht deshalb vor, dass der Cloud-Betreiber Datenschutzverletzungen unverzüglich dem Cloud-Nutzer als der verantwortlichen Stelle mitteilen muss. Hierzu sollten Cloud-Nutzer aber entsprechende Meldewege mit dem Cloud-Anbieter vereinbaren. Es gibt also einiges zu tun, damit die Cloud-Nutzung in Zukunft der Datenschutz-Grundverordnung Genüge tut. &

Cloud oder nicht: Was gehört alles zum Cloud Computing?

Cloud Computing ist für Sie kein Thema? Irrtum! Mit großer Wahrscheinlichkeit sind Sie bereits seit Jahren Cloud-Nutzer, auch wenn Sie sich dessen nicht bewusst sind. Hier finden Sie Beispiele für eine unbewusste Cloud-Nutzung.

Die Cloud ist in aller Munde, kaum ein Bericht über moderne IT erwähnt nicht Cloud Computing. Trotzdem ist vielen nicht bewusst, was genau unter Cloud Computing zu verstehen ist, und damit, was alles zur Cloud gehört. Dadurch denken viele Unternehmen und Privatanwender oft auch gar nicht an die Datenschutzvorgaben, die bei der Cloud-Nutzung zu beachten sind.

Vielleicht haben auch Sie bei der Lektüre der vorherigen Seite gedacht, „Cloud Computing betrifft mich nicht, blättere ich also weiter." Nun lesen Sie schon wieder von der Cloud, aus gutem Grund!

Was ist Cloud Computing überhaupt?

Sehr wahrscheinlich sind Sie Cloud-Nutzer, auch wenn Sie Cloud Computing gar nicht aktiv ausgewählt haben. Unter Cloud Computing versteht man jede Nutzung von IT-Ressourcen über das Internet, also auch die Nutzung von Anwendungen, die nicht lokal installiert, sondern über den Browser genutzt werden.

Typische Cloud-Anwendungen

Viele denken bei Cloud Computing zuerst an Speicherdienste aus der Cloud, auch Cloud Storage genannt. Wer keinen Cloud-Speicherdienst wie Dropbox, Apple iCloud, Google Drive oder Microsoft OneDrive

nutzt, meint deshalb, die Cloud nicht zu verwenden. Das stimmt aber gar nicht. Hier sind drei Beispiele dafür.

1. Die Cloud über den Browser

Haben Sie ein E-Mail-Konto bei Ihrem Provider, und rufen Sie Ihre E-Mails über den Browser ab? Dann nutzen Sie Web-Mail. Web-Mail ist aber letztlich nichts anderes als Cloud-Mail, also die Nutzung von E-Mail-Diensten über das Internet und damit aus der Cloud. Ihre E-Mails liegen also in einer Cloud, wenn Sie das Web-Mail-Angebot Ihres Providers nutzen.

Genauso verhält es sich bei Kalenderdiensten, die Sie über Ihren Browser verwenden, und bei vielen anderen Anwendungen, die Sie mittels Browser bedienen.

2. Die Cloud über das Betriebssystem

Die Cloud kann aber auch über das Betriebssystem kommen. Verwenden Sie zum Beispiel Windows 10, nutzen Sie ganz automatisch ein sogenanntes Cloud-basiertes Betriebssystem.

Die meisten der neuen Betriebssysteme verwenden Komponenten, die in einer Cloud liegen, oder sie sind eng mit einer Cloud verknüpft.

Das passiert, indem sie zum Beispiel als Standardspeicherort einen Cloud-Speicher vorsehen und nicht etwa das lokale Endgerät, also beispielsweise den PC, den Sie nutzen. Selbst wenn Sie den Standardspeicherort verändern, wird das Betriebssystem mit einer Cloud verbunden bleiben.

3. Die Cloud über das Smartphone und das Tablet

Nicht nur Smartphones und Tablets, deren Speicherplatz nicht über eine Speicherkarte erweiterbar ist, sind eng mit Clouds verbunden. Die Liste der installierten Apps, der Bildschirmhintergrund, die persönlichen Einstellungen – das sind nur einige Beispiele von Daten, die in einer Cloud vorgehalten werden. Das erleichtert den Umzug von einem Smartphone auf ein anderes. Aber dadurch liegen Ihre Daten in der Cloud.

Viele Wege führen in die Cloud

Sie sehen also: Viele Wege führen in die Cloud. Davon sind viele nicht willentlich und bewusst gewählt, sondern eine Folge des gewählten Betriebssystems oder des Endgeräts. Anwendungen, die sich überall nutzen lassen und nur einen Browser voraussetzen, sind ebenfalls in den meisten Fällen aus der Cloud. Machen Sie sich deshalb mit dem Datenschutz in der Cloud vertraut. Sie sind mit hoher Wahrscheinlichkeit ein Cloud-Nutzer. Blättern Sie deshalb auf den vorherigen Beitrag zurück! &

Wissen Sie, ob Sie eine Cloud nutzen? Machen Sie den Test.

Frage: Wer keine Daten im Internet speichert, nutzt auch keine Cloud. Stimmt das?

a. Ja, denn dann liegen ja alle Daten im Netzwerk oder auf dem Endgerät.
b. Nein, denn Cloud-Speicher sind nur ein Beispiel von Cloud Computing. Es gibt noch viele andere Formen von Cloud-Diensten.

Lösung: Die Lösung b. ist richtig. Bezieht man IT-Dienste über das Internet, nutzt man eine Cloud. Es müssen keine Speicherdienste sei. Es können auch Anwendungen wie E-Mail oder der Kalenderdienst sein. Der Datenschutz in der Cloud sollte deshalb für alle Internetnutzer ein Thema sein.

Frage: Nur wenn ich eine Anwendung über den Browser nutze, ist eine Cloud im Spiel. Stimmt das?

a. Ja, lokal installierte Anwendungen haben mit der Cloud nichts zu tun.
b. Nein, auch lokale Applikationen können eine Verbindung zur Cloud haben.

Lösung: Die Antwort b. ist auch hier richtig. Selbst Anwendungen, die man auf seinem Endgerät installiert, können mit einer Cloud verknüpft sein. Ein Beispiel sind Office-Programme, die die gemeinsame Arbeit an einem Dokument unterstützen oder die eine Dokumentenbearbeitung von jedem Gerät aus anbieten. Solche Anwendungen speichern die Dokumente in einer Cloud ab, sodass mehrere Nutzer oder Geräte zugreifen können. Somit wandern auch vertrauliche Dokumente in eine Cloud, wenn man nicht aufpasst. Wichtig ist es dann immer, den Datenschutz der jeweiligen Cloud zu hinterfragen. Nur datenschutzkonforme, sichere Clouds sollten zum Einsatz kommen.

Datenschutz und Gamification: „Spielerische“ Sensibilisierung für Datenschutz und Datensicherheit

Experten aus dem Bereich der Psychologie empfehlen Alternativen zu klassischen Belehrungen in Unternehmen. Das persönliche Erleben von Alltagssituationen in der Simulation kann zu einem besseren Verständnis von Datenschutz und Datensicherheit und deren Anwendung führen.

Jedes Jahr veröffentlichen verschiedene Institute in Deutschland die Prozentsätze der Schäden, die durch Datenverlust entstanden sind. Im letzten Jahr sind im Durchschnitt mehr als 60 Prozent aller Vermögensschäden, die durch Datenverlust, Datenklau oder Datenmanipulation entstanden sind, durch Beteiligung eigener Mitarbeitenden entstanden. Demnach werden für weniger als 40 Prozent des Schadensvolumens hohe Investitionen für Technik im Bereich Firewalls, externe Zugriffsbeschränkungen, Virenschutz oder ähnliches getätigt.

Angemessener Umgang mit beiden Themen

Es stellt sich die Frage, wie man effektiv und besonders nachhaltig dem weitaus größeren Gefahrenblock Herr werden kann. Der angemessene Umgang mit diesen beiden Themen ist in Unternehmen in vier Ausprägungen zu kategorisieren:

Kategorie 1: Es erfolgt keine Belehrung und auch keinerlei Sensibilisierung der Mitarbeiter.

Kategorie 2: Mit der Einstellung unterschreiben die neuen Mitarbeiter eine Datenschutz- und Verschwiegenheitserklärung.

Kategorie 3: Die Mitarbeiter erhalten schriftlich Informationsmaterial und neue Anweisungen der Geschäftsführung.

Kategorie 4: Der Datenschutzbeauftragte führt Awareness-Veranstaltungen durch. Den Mitarbeitern werden Filme, Berichte und Illustrationen gezeigt, die anregen, das gezeigte Problem und dessen Lösung auf die tägliche Arbeit zu projizieren. E-Learning-Konzepte unterstützen diese Vorgehensweise.

In den Kategorien 1 bis 3 ist die Sensibilisierung von Anfang an gegen Null anzusetzen. Die Mitarbeiter handeln nach eigenem Sicherheitsverständnis und somit stark individuell. Bei der Stufe 4 ist festzustellen, dass das Verständnis für Datenschutz und Datensicherheit während und kurz nach der Veranstaltung bei den Teilnehmern sehr präsent ist. In der täglichen Flut an Informationen und Aufgaben kann das Erlernte jedoch auch schnell wieder in den Hintergrund treten.

Nicht nur wissen, sondern auch bewusst danach handeln

Aus der Wissenschaft der Psychologie über die Ansteuerung des Unterbewusstseins und der stetigen Präsenz von Informationen ist bekannt, dass es zwei Verfahren gibt, um etwas Gelerntes nicht nur zu wissen, sondern bewusst danach zu handeln.

- Nach dem Grundsatz der Wiederholung muss eine Information, z. B. wie datenschutzkonform und sicher mit IT-Systemen umgegangen wird, viele Male in das Unterbewusstsein einfließen, um zu einem automatischen Handeln zu werden (ins Bewusstsein gelangen). Eine ständige Wiederholung kann jedoch herausfordernd bis unakzeptabel wirken.

- Durch Emotionen werden Informationen deutlich besser aufgenommen und bleiben präsenter. Sie verschwinden nicht in den Tiefen des Unterbewusstseins. So kann sich noch jeder an die Geburt des eigenen Kindes, den besonderen Restaurantbesuch, den einmaligen Heiratsantrag oder die rasante Skiabfahrt erinnern. Auch wenn der Informationseingang einmalig, nur wenige Sekunden gedauert und bereits Jahrzehnte her ist: Die Zugabe von Emotionen reduziert die Anzahl der Wiederholungen.

Um in dem Themenbereich Datenschutz und Datensicherheit entsprechende Emotionen zu verpacken, wurde das Prinzip eines

Datenschutz- und Datensicherheits-Parcours entwickelt. Dieser wird fallspezifisch auf ein Unternehmen zugeschnitten und folgt dem Gamification-Prinzip. Das Konzept soll eine nachhaltige und langfristige Sensibilisierung der Mitarbeiter gewährleisten.

Unterschiedlichen Charaktere, Hierarchien und Wissensstände berücksichtigen

Bis zu 36 Mitarbeiter werden anfangs durch den Parcoursleiter informiert, was Sie gleich im Parcours erwartet. Bereits die Einteilung in bis zu 6 Gruppen zu je 6 Teilnehmern durch den Parcoursleiter berücksichtigt erste emotionale Einflüsse: Gruppe sollten mit möglichst unterschiedlichen Charakteren, Hierarchien und Wissensständen besetzt sein. Dadurch wird sichergestellt, dass innerhalb des Durchlaufs des Parcours kräftig diskutiert wird. Die Bekanntgabe, dass die Gruppen gegeneinander spielen und die beste Gruppe einen adäquaten Preis erhält, sorgt für zusätzliche Emotionen und Motivation.

Jede Gruppe besetzt einen Tisch und sie werden dort von dem Tischleiter begrüßt. Dieser erläutert die Aufgabe und den Bezug zur Realität. Nach dem sichergestellt wurde, dass alle Gruppen eingewiesen wurde, wird vom Parcoursleiter der Startschuss gegeben.

Innerhalb von 90 Sekunden müssen die Gruppen an ihren Tischen die entsprechende Aufgabe gemein-

schaftlich lösen. Datenschutzfragen werden auf diese Weise spielerisch erlernt.

Die Aufgaben orientieren sich an die Fachspezifika des Unternehmens, der Fach- oder Berufsgruppe sowie an Auffälligkeiten und Vorschläge des Datenschutz- und Informationssicherheitsbeauftragten. Dabei sind die einzelnen Tische ganz unterschiedlich von der Herangehensweise: neben einfache Puzzle- und Zuordnungsspielen sind manche Spiele und Rätsel deutlich komplexer, z. B. beim Erraten eines Laptops oder spannenden Knobelaugaben.

Lösungen werden bewertet und bepunktet

Nach Ablauf der Zeit nennt die Gruppe ihre untereinander abgestimmte Lösung. Diese wird vom Tischleiter bewertet und bepunktet. Der Tischleiter erläutert der Gruppe die richtige Lösung, begründet diese, geht auf Fragen ein und erläutert die Fehler. Nach dem Rotationsprinzip durchlaufen die Gruppen alle Stationen. Sie erkämpfen sich bei jeder Station weitere Punkte.

Ohne Fleiß kein Preis

Zum Ende, wenn die Gruppen alle Stationen durchlaufen haben, werden die Punkte je Gruppe von den Tischleitern addiert und die Gruppensieger ermittelt. Währenddessen diskutiert der Parcoursleiter mit den Teilnehmern diesen Parcours, die Empfindungen und die einzelnen Lösungen. In einer angemessenen Zeremonie werden die Sieger bekannt gegeben. Die Siegergruppe erhält einen Preis, für den sich der Wettkampf gegenüber den anderen gelohnt hat.

Die bis zu sechs Wissensbereiche, die die Teilnehmer in kürzester Zeit langfristig verinnerlicht haben, sind im Unterbewusstsein eingepflanzt, verankert und präsent. Sie werden bei jedem Besuch eines Parcours zunehmend zum Fachmann der operativen Anwendung von Datenschutz und Datensicherheit.

Der Datenschutz-/Datensicherheits-Parcours bietet sich an als:

Offene Veranstaltung: In einer Stadt senden mehrere Unternehmen ihr Mitarbeiter. Dabei werden zwar keine unternehmensspezifische Cooperate Designs umgesetzt, doch die Zusammensetzung mit Unbekannten innerhalb einer Gruppe stärkt das Wir-gefühl innerhalb der Gruppe.

Innerhalb von einem Unternehmen: Dabei wird vor Ort mit dem Cooperate Design und der ganz spezifischen Thematik des Unternehmens gearbeitet. &

Folgen von IT-Angriff: Weltkonzern Maersk 10 Tage offline

„Man weckte mich um vier Uhr morgens“ sagte der Maersk-Vorsitzende Jim Hagemann Snabe beim Weltwirtschaftsforum in Davos. Am 27.06.2017 verursachte die Schadsoftware „NotPetya“ einen großflächigen Ausfall der IT-Systeme, der das Unternehmen mehrere hundert Millionen Euro gekostet haben dürfte.

Maersk transportiert knapp 20 % des Welthandels in seinen Schiffen und Containern. „Alle fünfzehn Minuten erreicht eines unserer Schiffe mit zehn bis zwanzigtausend Containern einen Hafen irgendwo auf der Welt“. Infolge des Angriffs konnten Schiffe weltweit nicht be- oder entladen werden. Ganze zehn Tage dauerte der Notbetrieb ohne Computer, zurück zu Papier und Stift.

Die IT-Abteilung stand vor der Aufgabe, 45.000 Clients und 4.000 Server neu installieren zu müssen – eine Kraftanstrengung, wie Snabe formulierte. „Wir müssen aufhören, bei diesem Thema so naiv zu sein“.

Neben Maersk waren auch andere namhafte Unternehmen von der Cyberattacke betroffen: Das zur FedEX-Gruppe gehörende Unternehmen TNT bezifferte den Schaden durch NotPetya auf 300 Millionen US-Dollar. &

11 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 1/2018

ALTHAMMER & KILL

News

Aus unserem aktuellen Newsletter:

Datenschützer in Sorge! GPS-Sender soll Schulkinder ortbar machen und andere Verkehrsteilnehmer warnen.
https://www.althammer-kill.de/news-detail/datenschuetzer-in-sorge/

Cyber-Versicherungen
https://www.althammer-kill.de/news-detail/cyber-versicherungen/

Datenschutz beim Weihnachtsmann
https://www.althammer-kill.de/news-detail/datenschutz-beim-weihnachtsmann/

Nicht verschlüsselte E-Mails entsprechen nicht dem Stand der Technik!
https://www.althammer-kill.de/news-detail/nicht-verschluesselte-e-mails-entsprechen-nicht-dem-stand-der-technik/

Neuer IT-Grundschutz vorgestellt
https://www.althammer-kill.de/news-detail/neuer-it-grundschutz-vorgestellt/

Kopie des Personalausweises jetzt zulässig!
https://www.althammer-kill.de/news-detail/kopie-des-personalausweises-jetzt-zulaessig/

Anmeldemöglichkeiten zum Newsletter finden Sie unter:
www.althammer-kill.de

Termine

Wir freuen uns auf persönliche Begegnungen –
zum Beispiel im Rahmen der folgenden Veranstaltungen:

06.–08.03.2018, Hannover
Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Datenschutz auf Basis von DSGVO/BDSG (neu), DSG-EKD und KDO

06.–08.03.2018, Hannover
Messe Altenpflege 2018
Wir freuen uns auf Ihren Besuch!

17.–19.04.2018, Paderborn
Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Datenschutz auf Basis von DSGVO/BDSG (neu), DSG-EKD und KDO

17.–19.04.2018, Berlin
conhIT 2018
Wir freuen uns auf Ihren Besuch!

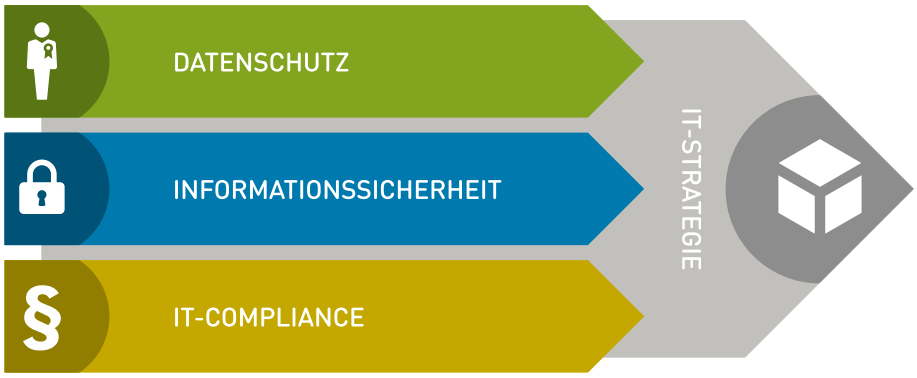
24.–26.04.2018, Paderborn
Ausbildung IT-Sicherheitsbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Informationssicherheit auf Basis von IT-Grundschutz und der IT-Sicherheitsverordnung (ITSVO-EKD)

02.05.2018, Paderborn
Privacy by Design: Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht
Spätestens mit der EU Datenschutz-Grundverordnung (DSGVO) sollten Unternehmen bereits bei der Auswahl von IT-Lösungen berücksichtigen, inwieweit diese datenschutzrechtlichen Anforderungen genügen.

Termin verpasst? Anruf oder E-Mail genügt und wir lassen Ihnen gern weitere Informationen zukommen.

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ).

Althammer & Kill GmbH & Co. KG

Standort Hannover:
Thielenplatz 3 · 30159 Hannover
Tel. +49 511 330603-0

Standort Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0

info@althammer-kill.de
www.althammer-kill.de

Mitglied im:

FINSOZ e.V. · GDD Mitglied · BvD e.V. Mitglied · Hannover IT