Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2016

In dieser Ausgabe:

Online-Konferenzen: Vorsicht, ungebetene Gäste!
▸ **Seite 1**

Wem gehört ein verlorenes Smartphone?
▸ **Seite 2**

Flugdrohnen und die Nachbarin
▸ **Seite 4**

Orientierungshilfe E-Mail und Internet am Arbeitsplatz
▸ **Seite 6**

Finale Fassung der EU-DSGVO auf Deutsch erschienen
▸ **Seite 7**

Smartphones: Persönlicher Assistent oder heimlicher Datensammler?
▸ **Seite 8**

Akademie ▸ **Seite 10**

Aktuelles ▸ **Seite 11**

Liebe Leserin, lieber Leser,

ferngesteuerte Drohnen sind immer häufiger am Himmel zu sehen. Wir erläutern die Geschichte eines gerichtlich angeordneten Flugverbots auf Seite 4.

Eine spannende Lektüre wünschen

Thomas Althammer & Niels Kill

Online-Konferenzen: Vorsicht, ungebetene Gäste!

Virtuelle Meetings im Internet sparen Zeit und Geld. An der Sicherheit sollten Unternehmen aber nicht sparen. Doch genau das passiert gegenwärtig bei vielen Online-Konferenzen.

Regelmäßige Kommunikation ist wichtig, im Projektteam genauso wie mit Kunden. Die Treffen und persönlichen Gespräche kosten allerdings Zeit – Zeit, die kaum jemand hat.

Hinzu kommt, dass viele Teams und erst recht die Kunden weit verstreut sind, sodass lange Reisezeiten die Folge sind. Da klingt es mehr als verlockend, möglichst viele Konferenzen und Schulungen virtuell über das Internet durchzuführen. Technische Lösungen dafür gibt es reichlich. Viele sind sogar kostenlos.

Lösungen für Online-Konferenzen gibt es viele

Sicherlich wurden Sie schon zu einem Online-Meeting mit Kunden oder Teammitgliedern eingeladen. Dabei werden Sie festgestellt haben, dass der eine Kunde die Online-Konferenzlösung A, der andere die Lösung B bevorzugt. Schnell hat man eine ganze Reihe von Erweiterungen für den Webbrowser installiert, die in der Regel neben Webcam, Mikrofon und guter Internetverbindung die einzige Voraussetzung für das Online-Meeting sind. Die

Zugangsdaten für die Online-Konferenz erhalten Sie meist per E-Mail – als unverschlüsselte Mail wohlgemerkt. Oder Sie müssen sich registrieren, wobei Sie mitunter ohne ersichtlichen Grund eine Reihe von personenbezogenen Daten angeben müssen.

Verschiedene Lösungen machen es einfacher, komfortabler: Sie bekommen einen Link per Mail, den Sie zur vereinbarten Zeit anklicken, und schon kann es mit dem virtuellen persönlichen Austausch losgehen. Losgehen kann nun aber auch eine Online-Attacke oder ein Spionageversuch!

Wer lädt (wirklich) ein, wer nimmt (heimlich) teil?

Da der Link als Einladung zur Online-Konferenz in aller Regel als ungeschützte E-Mail verteilt wird, ist weder sichergestellt, dass der angegebene Absender stimmt, noch besteht Gewissheit, dass der Link zur Teilnahme nicht in die Hände unbefugter Dritter gelangt.

Das Datenschutzproblem ist offensichtlich: Es ist nicht gewährleistet, dass die Identitäten der Teilnehmer stimmen. Vertrauliche Videokonferenzen, die einfach über das ungeschützte Versenden eines Links eingeleitet werden, sind zweifellos ein Datenrisiko.

Achten Sie auf die Online-Sicherheit

Wenn Sie in Zukunft zu einer Online-Konferenz eingeladen werden oder selbst eine veranstalten, denken Sie nicht nur an den einfachen Zugang und den hohen Komfort. Vergessen Sie nicht die nötige Datensicherheit. Dazu gehören die folgenden Standardmaßnahmen:

- Verschlüsselung der Datenübertragung
- Malware-Schutz (Risiko durch infizierte Dokumente, Plug-ins und Links)
- Zugangsschutz über Benutzername und Passwort (keine direkte Teilnahme über Link)
- Kontrolle der Teilnehmerliste
- kontrollierter, bewusster Einsatz von Mikrofon und Webcam
- Beschränkung der Freigabe von (Desktop-)Inhalten. &

Wem gehört ein verlorenes Smartphone?

Sie verlieren Ihr Smartphone. Jemand findet es. Er gibt es ganz korrekt beim Fundbüro der Gemeinde ab. Was passiert eigentlich dann? Das kommt darauf an – übrigens auch darauf, in welchem Bundesland Sie Ihr Smartphone verloren haben!

Besonders wenn es jetzt wieder Sommer wird, stapeln sie sich in manchen kommunalen Fundbüros regelrecht: Smartphones, Laptops und ab und an auch noch ein gutes altes Handy. Doch was tut die Fundbehörde eigentlich mit solchen Geräten?

Befundbescheinigung für den Finder

Der erste Schritt ist die Registrierung der Fundsache und des Finders. Der Finder erhält auf Wunsch eine Fundbescheinigung. Ein kluger Finder lässt sich diese – für ihn kostenlose – Bescheinigung ausstellen. Sie kann für ihn später nämlich noch einmal ein kostbares Dokument sein.

Rückgabe an den Eigentümer – oder auch nicht

Dann tut die Behörde in der Regel zunächst einmal nichts. Schließlich könnte sich der Eigentümer des Geräts melden. Und natürlich bekommt er dann sein Gerät zurück. Freilich nur dann, wenn er sein Eigentum auch nachweisen kann. Nur Naive glauben, sie könnten beim Fundbüro die dort gelagerten Geräte „einmal durchschauen“, um zu sehen, ob ihr Handy dabei ist. So einfach läuft das natürlich nicht.

Wer Glück hat, hatte sein Smartphone vielleicht in einer auffälligen selbstgebastelten Hülle stecken. Wenn

er sie gut beschreiben kann und sie wirklich ein Einzelstück ist, kann das zur Identifizierung ausreichen.

In der Regel wird es freilich komplizierter. Meist geht es nicht ohne die Seriennummer der SIM-Karte oder die IMEI/MEID-Nummer des Geräts. Sie wissen nicht, was das ist? Dann wird es im Ernstfall ganz gewiss schwierig.

Verwahrung für sechs Monate

Falls sich der Eigentümer nicht meldet oder er sein Eigentum nicht nachweisen kann, verwahrt die Fundbehörde zunächst einmal sechs Monate lang amtlich das Gerät. Manche Fundbehörde versucht, über den Handyhersteller den Eigentümer zu ermitteln. Dazu nutzt sie die eben genannten Nummern.

Manche Behörde tut dies aber auch nicht – beispielsweise weil sie dazu schlicht keine Zeit hat. Auch hängt der Umfang der Aktivitäten davon ab, welche technischen Kenntnisse die Mitarbeiter zufällig haben.

Erwerb des Eigentums durch den Finder – oder auch nicht

Sind die sechs Monate vorüber, kann der Finder verlangen, dass die Behörde ihm das Gerät herausgibt. Durch Ablauf dieser Frist ist er nämlich Eigentümer des Geräts geworden!

Das ist im Bürgerlichen Gesetzbuch so geregelt (§ 973 Absatz 1 BGB). Wichtige Ausnahmen: Sollte das Gerät in den öffentlichen Räumen einer Behörde oder in einem öffentlichen Verkehrsmittel gefunden worden sein, wird der Finder nicht Eigentümer. So will es § 978 Absatz 1 BGB.

Wer also ein mobiles Gerät beispielsweise in der U-Bahn findet, hat Pech gehabt.

In allen anderen Fällen wird ein kluger Finder sich nach sechs Monaten wieder an die Fundbehörde wenden und seine Fundbescheinigung vorlegen. Dann wird ihm das Gerät aus-

Impressum

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

Anschrift:
Althammer & Kill GmbH & Co. KG
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Schutzgebühr Print-Ausgabe: 5,– €

gehändigt. Schließlich ist er jetzt Eigentümer des Geräts.

Das Schicksal der Daten auf dem Gerät

Was passiert aber mit den Daten auf dem Gerät? Beispielsweise mit sehr persönlichen Fotos? Oder den kompletten Telefonlisten? Hier ist die Handhabung in den einzelnen Bundesländern erstaunlich unterschiedlich:

- In Bayern verlangt der Landesbeauftragte für den Datenschutz, dass die Fundbehörde die Daten auf dem Gerät entweder selbst löscht oder durch ein Fachgeschäft löschen lässt. Die Kosten hierfür stellen die Fundbehörden dem Finder in Rechnung. Zahlt er sie nicht, bekommt er das Gerät auch nicht.
- In Baden-Württemberg vertritt der Landesbeauftragte für den Datenschutz die Auffassung, dass die Fundbehörde die Daten löschen soll. Das allerdings nur dann, wenn es „ohne großen technischen Aufwand" möglich ist – was immer das heißen soll. Ansonsten sei das Gerät mitsamt den Daten an den Finder herauszugeben. Das soll vor allem gelten, wenn eine Löschung nicht möglich ist, weil technische Mittel den Datenzugriff blockieren.
- Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt argumentiert dagegen ähnlich wie der Landesbeauftragte in Bayern. Er erwartet, dass die Fundbehörde die Daten entweder selbst löscht oder von einem Fachunternehmen löschen lässt. Falls das nicht möglich ist (etwa bei Zugriffsblockaden), müsse das Gerät datenschutzgerecht entsorgt werden. An den Finder dürfe es dann nicht herausgegeben werden. Diese These erscheint freilich kühn. Schließlich ist der Finder kraft Gesetzes Eigentümer geworden, und im BGB steht nichts davon, dass die Fundbehörde sein Eigentum aus datenschutzrechtlichen Überlegungen heraus vernichten darf.

Wichtig: Gerätenummern festhalten!

Für Unternehmen wie Privatpersonen lautet der wichtigste Rat: Sorgen Sie dafür, dass die identifizierenden Nummern jedes Geräts sicher festgehalten sind. Dann besteht nämlich die Chance, das Gerät zurückzuerhalten, und Fragen des Datenschutzes stellen sich nicht mehr. Kostenlos ist eine Rückgabe übrigens nicht. Die meisten Behörden haben eine Gebührenordnung und verlangen 15 bis 25 Euro. &

Flugdrohnen und die Nachbarin

Angeblich sollte die Flugdrohne nur die Dachrinne inspizieren. Plötzlich schwebte sie dann aber doch über dem Liegestuhl der Nachbarin. Die wehrte sich dagegen vor Gericht – und zwar höchst erfolgreich.

Die Frau war empört. Eben noch lag sie entspannt auf der Liege in ihrem Garten und genoss die Sommersonne. Da hörte sie über sich ein Geräusch, ähnlich dem einer Sense. Beunruhigt schaute sie nach oben. Wenige Meter über ihr schwebte eine Flugdrohne.

Die Frau sprang hoch und rannte durchs Haus auf die Straße. Draußen vor ihrer Haustür traf sie einen Nachbarn an. Der hantierte gerade mit der Fernbedienung einer Flugdrohne. Neben ihm standen zwei weitere Nachbarn, die sich für das Ganze interessierten.

Müde Ausreden des Drohnenpiloten

Als die Frau den Nachbarn zur Rede stellte, flüchtete er sich in Ausreden. Immerhin räumte er ein, dass seine Drohne mit einer Kamera ausgestattet ist. Auch gab er zu, dass die Kamera seiner Drohne gerade eingeschaltet war. Das Teil über dem Liegestuhl sei aber auf keinen Fall seine Drohne gewesen. Er habe lediglich seine eigenen Dachrinnen und die Dachrinnen seiner Nachbarn neben ihm kontrollieren wollen. Mit der Sache im Garten habe er nichts zu tun.

Die Frau glaubte ihm kein Wort. Sie hatte in ihrem Garten Ruhe haben wol-

len. Die Chancen dafür standen an sich gut, denn der Garten war durch eine hohe Hecke geschützt. Umso empörter war sie jetzt. Da von einer Entschuldigung oder etwas Ähnlichem seitens ihres Nachbarn keine Rede war, ging sie vor Gericht.

Gerichtliches Verbot auf Antrag der Nachbarin

Dort beantragte sie, den Nachbarn zur Unterlassung zu verurteilen. Das Gericht sollte ihm verbieten, mit einem funkgesteuerten Fluggerät – gleich ob mit oder ohne Kamera – das Grundstück der Frau zu überfliegen. Für den Fall, dass er sich nicht an das Verbot hält, sollte dem Nachbarn ein Ordnungsgeld bis zu 250.000 Euro angedroht werden. Das Gericht gab der Frau Recht und entschied so, wie von ihr beantragt.

Drohnen verletzen rasch die Privatsphäre

Das Gericht begründete seine Entscheidung wie folgt:

- Das Überfliegen eines Nachbargrundstücks mit einer Drohne, die Bilder anfertigt, stellt einen Eingriff in die Privatsphäre dar.
- Zur Privatsphäre gehört es, dass geschützte private Bereiche respektiert werden. Nur so kann man dort ungestört für sich sein, zu sich kommen, sich entspannen und sich auch einmal gehen lassen. Derartige private Bereiche (so wie hier der Garten mit einer hohen Hecke) sind Rückzugsorte. Werden sie ausgespäht, verletzt das das allgemeine Persönlichkeitsrecht.
- Der Wunsch des Nachbarn, als Hobby seine Drohne herumfliegen zu lassen, muss hinter dem Persönlichkeitsrecht der Frau zurücktreten. Es gibt genügend andere Flächen und Räume, in denen der Nachbar seinem Hobby nachgehen kann, ohne jemanden zu stören.
- Es geht – so das Gericht – nicht um ein Flugverbot oder um das Untersagen einer kindlich-unschuldigen Freizeitbeschäftigung wie beispielsweise das Steigenlassen eines Drachens oder die Steuerung eines Modellflugzeugs per Fernbedienung. Vielmehr gehe es um eine Beeinträchtigung des Persönlichkeitsrechts durch das Ausspähen mit einer Drohne, die über eine Kamera verfügt.

Eine Wiederholungsgefahr besteht

Zwar hat der Nachbar eine Unterlassungserklärung abgegeben und versprochen, das Grundstück der Nachbarin künftig nicht mehr zu überfliegen. In dieser Erklärung hat er jedoch keine Vertragsstrafe für den Fall versprochen, dass er gegen seine Erklärung verstößt. Damit ist die Unterlassungserklärung rechtlich gesehen unzureichend und beseitigt die Wiederholungsgefahr nicht. Die Entscheidung des Amtsgerichts Potsdam trägt das Datum 16. April 2015 und das Aktenzeichen 37 C 454/13. Sie ist im Internet leicht zu finden. Es handelt sich um die erste bekannt gewordene Entscheidung in einem solchen Fall.

Haftungsrisiko in mehrfacher Hinsicht

Sie zeigt, dass bei Flugdrohnen Vorsicht geboten ist, auch im Hinblick auf den Datenschutz. Hinzu kommt das Haftungsrisiko durch die Beschädigung von Sachen oder gar durch die Verletzung von Personen.

Transparenz schaffen!

Was sollte man tun, wenn man wirklich nur die Dachrinne inspizieren will oder Ähnliches? Das kann ausgesprochen sinnvoll sein und beispielsweise mühsame Klettereien ersparen. Deshalb setzen inzwischen sowohl Privatleute als auch etwa Handwerker durchaus Flugdrohnen ein, die über eine Kamera verfügen. Sofern die Gefahr besteht, dass sich ein Nachbar dadurch beeinträchtigt fühlt, sollte man ihn schlicht vorher informieren. Falls es trotzdem Beschwerden gibt, bietet es sich an, den Betroffenen die Aufnahmen ansehen zu lassen. Dann ist meist schnell geklärt, ob es wirklich um die Dachrinne ging oder doch eher um die Nachbarin auf der Sonnenliege. &

Orientierungshilfe E-Mail und Internet am Arbeitsplatz

Die Datenschutzaufsichtsbehörden des Bundes und der Länder haben eine Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und Internet am Arbeitsplatz veröffentlicht

E-Mail und Internet am Arbeitsplatz sind mittlerweile in den meisten Unternehmen Standard. Dabei nutzen Arbeitnehmer die digitalen Informations- und Kommunikationswege häufig nicht nur für betriebliche Belange, sondern auch für private.

Schutz personenbezogener Daten im Fokus

Die Aufsichtsbehörden erreichen daher immer wieder Anfragen von Arbeitgebern, ob und in welchem Umfang die private Nutzung überwacht werden darf.

Dabei geht es den Arbeitgebern in erster Linie um die Aufrechterhaltung der Systemsicherheit und um den Zugriff auf betriebliche E-Mails, wenn der Beschäftige abwesend ist. Nicht zuletzt hat der Arbeitgeber auch ein Interesse daran, das Verhalten und die Leistung der Beschäftigten zu kontrollieren.

Insbesondere geht die Orientierungshilfe darauf ein, welchen Schutz die in der Kommunikation via E-Mail anfallenden personenbezogenen Daten genießen – und zwar sowohl der Beschäftigten selbst als auch ihrer Kommunikationspartner und anderer Betroffener wie etwa Dritter, deren Namen in einer E-Mail genannt wird. Unter anderem werden folgende Themenbereiche behandelt:

- Dürfen Arbeitnehmer am Arbeitsplatz das Internet privat nutzen?
- Dürfen vom Arbeitsplatz aus private E-Mails versendet werden?
- Darf ein Arbeitgeber auf das E-Mail-Postfach der Beschäftigten zugreifen, wenn diese abwesend sind?
- Darf ein Arbeitgeber die Internetnutzung kontrollieren?
- Welche Vorgaben kann ein Arbeitgeber zur Nutzung digitaler Dienste machen?

Neben Regelungen zur ausschließlich betrieblichen Nutzung finden sich auch Regelungen wenn eine private Nutzung erlaubt oder geduldet ist. Zudem geht die Orientierungshilfe auch auf besondere Regelungen für Geheimnisträger (Betriebsrat, Datenschutzbeauftragte, Betriebsarzt etc.) ein.

Betriebsvereinbarung für die private Nutzung des Internets

„Dieses Papier schafft endlich Klarheit im Dschungel der Kommunikation am Arbeitsplatz. Es enthält Hinweise zur datenschutzgerechten Kommunikation im modernen Büro und bietet erstmals eine Mustervereinbarung, die von den Unternehmen als Vorlage genutzt werden kann. Sowohl Arbeitgeber als auch Beschäftigte erfahren, welche Rechte sie haben, aber auch welche Pflichten es zu beachten gilt“ so Reinhard Dankert, Datenschutzbeauftragter von Mecklenburg-Vorpommern und Vorsitzender der Datenschutzkonferenz.

Die Orientierungshilfe dient in erster Linie privaten Arbeitgebern, Beschäftigten sowie Betriebsräten und stellt die datenschutzrechtlichen Anforderungen für die Bereitstellung von E-Mail und Internet am Arbeitsplatz dar, kann aber auch eine Orientierung für Behörden sein. Dabei werden sowohl die aktuelle Rechtslage als auch arbeitsrechtliche Grundsätze berücksichtigt. &

Weitere Hinweise

Die Orientierungshilfe steht auf der Seite des LfDI zum Download bereit:
www.datenschutz-mv.de/datenschutz/publikationen/informat/internet/oh-internet-arbeitsplatz.pdf

Finale Fassung der EU-DSGVO auf Deutsch erschienen

Ab Mai 2018 gilt in Europa ein einheitliches Datenschutzrecht, das das Bundesdatenschutzgesetz und die Landesdatenschutzgesetze weitestgehend ersetzen wird.

Die zweijährige Umsetzungsfrist hat begonnen und ab dem 25.05.2018 gilt EU-weit das neue Datenschutzrecht. Die wichtigsten Punkte für Unternehmen im Überblick:

© K. Borchhardt/ www.miniansichten.de

Einheitlich: Alle 28 Mitgliedsländer erhalten erstmalig ein tatsächlich einheitliches Datenschutzniveau. Nur wenige Öffnungsklauseln für strengere nationale Vorschriften sind vorgesehen.

Vorrang: Die EU-DSGVO gilt vor nationalen Regelungen. 99 Artikel und 174 Erwägungsgründe helfen bei der Auslegung der teils komplexen Vorschriften.

Transparenz: Die Betroffenenrechte wurden deutlich gestärkt. Unternehmen müssen umfassender und genauer als bisher informieren. Auf die Unternehmen kommt hier viel Arbeit zu.

Verantwortlichkeit: Der Datenschutz wird mit der EU-DSGVO deutlich gestärkt. Die Einhaltung von Vorgaben muss dokumentiert und im Zweifel auch vor Gericht bewiesen werden können.

Arbeitnehmer: Noch unklar ist die Zukunft des Beschäftigtendatenschutzes, der in der EU-DSGVO eher schwach geregelt ist. Möglicherweise bleibt § 32 BDSG als Teil einer nationalen Öffnungsklausel erhalten.

Betriebsvereinbarungen: Zwischen Mitarbeitervertretung und Arbeitgeber können weiterhin Vereinbarungen geschlossen werden. Diese müssen aber an die EU-DSGVO angepasst werden.

Datenschutzbeauftragte: Die EU-DSGVO sieht etwas andere Grundbedingungen vor, ab wann ein Datenschutzbeauftragter zu bestellen ist. Die Bundesregierung hat jedoch angekündigt, eine nationale Regelung ähnlich der bisherigen Praxis zu erlassen bzw. den § 4f im BDSG bestehen zu lassen.

Auftragsdatenverarbeitung: Externe Dienstleister werden stärker als bisher mit in die Verantwortung genommen. Auch weitere Verfahren ändern sich, z. B. die Forderung nach Datenübertragbarkeit, Privacy by Design und Privacy by Default sowie das Recht auf Vergessen werden als Grundprinzipien eingeführt. Zwei Jahre Vorbereitungszeit dürften für einige Unternehmen sehr knapp bemessen sein.

Bußgelder: Verstöße werden deutlich stärker geahndet als bisher. Es drohen Bußgelder bis zu 20 Mio. EUR oder 4% des Jahresumsatzes einer Unternehmensgruppe weltweit. &

Benötigen Sie weitere Informationen?

Gern beraten und unterstützen wir Sie bei der Vorbereitung auf die neuen gesetzlichen Grundlagen.

Weitere Details:
www.althammer-kill.de/news-detail/auswirkungen-der-eu-datenschutzgrundverordnung.html

WhatsApp jetzt endlich Ende-zu-Ende verschlüsselt

WhatsApp hat vor einigen Wochen endlich umgesetzt, worauf viele gewartet haben: Alle Nachrichten und Telefonate über den beliebten Messenger-Dienst werden komplett Ende-zu-Ende verschlüsselt.

Damit sind Konversationen und Datenaustausch von ca. einer Milliarde Nutzer weltweit vor abhörenden Augen und Ohren geschützt. Die Verschlüsselung funktioniert über Betriebssystem-Grenzen hinweg, auch in Gruppen-Chats.

Die Technologie dahinter wurde von Open Whisper Systems entwickelt. Grundlage ist das quelloffene Signal-Protokoll, das auch in Apps wie TextSecure eingesetzt wird.

Nachrichten, Fotos, Videos oder Anrufe werden erst wieder auf dem Gerät des Empfängers entschlüsselt. Die Server für den Datenaustausch bekommen nur verschlüsselte Datenpakete und können den Inhalt der Kommunikation nicht mitlesen.

Smartphones: Persönlicher Assistent oder heimlicher Datensammler?

Smartphones sind nicht nur Mini-Computer, mit denen man auch telefonieren kann. Smartphones haben das Zeug zum persönlichen Assistenten. Die Frage ist nur, wie vertrauenswürdig dieser Assistent ist.

Der Weg zum Bahnhof hat länger gedauert als gedacht, leider war in der Innenstadt für das Taxi kein Durchkommen. Gerade am Gleis angekommen, sehen Sie, wie Ihr gebuchter Zug abfährt. Da ist der Ärger groß, wäre man doch früher zum Bahnhof aufgebrochen! Doch woher hätten Sie auch wissen sollen, dass es zu knapp ist? Die Antwort lautet: von Ihrem Smartphone!

Ob Sie ein Android-Smartphone, ein Smartphone mit Windows 10 oder ein iPhone nutzen: Mobile Betriebssysteme bringt inzwischen eine Applikation mit, die sich als virtueller persönlicher Assistent bezeichnen lässt. Die entsprechenden Apps heißen Google Now, Cortana oder Siri.

„Es wird Zeit, aufzubrechen"

Unter bestimmten Voraussetzungen kann Ihr Smartphone Ihnen tatsächlich sagen, dass Sie früher los müssen, um Ihren Zug noch zu bekommen. Dazu nutzen Smartphones bzw. Siri, Cortana oder Google Now die Informationen über Ihre geplante Zugfahrt, Ihren aktuellen Standort, Ihr bevorzugtes Transportmittel und die aktuelle Verkehrslage vor Ort.

Ihr virtueller Assistent berechnet den Zeitpunkt, an dem Sie zum Beispiel

mit dem Taxi starten müssen, erinnert Sie daran und liefert auch gern die Nummer des nächsten Taxiunternehmens, auf Wunsch ruft Ihr Assistent sogar direkt für Sie an. Sie müssen nur noch das Telefonat führen und ins Taxi steigen.

Assistenz ist eine Vertrauensstellung

Keine Frage, so eine virtuelle Assistenz ist auf den ersten Blick eine feine Sache. Jede Mitarbeiterin, jeder Mitarbeiter hat plötzlich den Service, den sonst nur die Chefetage kennt, so scheint es. Allerdings ist die Assistenz eine App und keine speziell ausgewählte, zuverlässige Person des Vertrauens. Siri, Cortana und Google Now haben enorme Kenntnisse über Sie als Nutzer, damit sie so hilfreich sein können.

Was können die Assistenten?

Ihre aktuellen Standortdaten sind nur ein Beispiel, der Zugriff auf Ihren Terminkalender, Ihre Kontakte und persönlichen Vorlieben sind weitere. Andere Beispiele für praktische, aber nicht wirklich harmlose Funktionen der Assistenz-Apps sind die personalisierten Hinweise,

- wenn der Verkehrsstau ein früheres Aufbrechen notwendig macht (Sie werden geortet),
- wenn sich das Abfluggate ändert (Ihre Reisepläne werden durchsucht) oder
- wenn der Wecker automatisch zur richtigen Zeit klingelt (Ihr Assistent kennt Ihren üblichen Tagesablauf).

Datenschutz-Optionen brauchen mehr Beachtung

Dabei bleibt das Wissen über Sie nicht etwa bei der auf Ihrem Smartphone installierten App, nicht einmal auf Ihrem mobilen Endgerät. Die Assistenz-Apps sammeln nur die Daten. Die Auswertung findet in einem Cloud-Dienst statt, von dort kommen auch die oftmals hilfreichen Hinweise und Services. Leider ist das vielen Nutzern nicht klar.

Auch wenn die virtuellen Assistenten weniger komfortabel werden oder Sie sie sogar gar nicht nutzen können, sollten Sie auf die Datenschutz-Optionen der Apps achten. Wenn Sie nicht die Zugriffe der jeweiligen Assistenz-App auf Ihre Daten einschränken, könnte die App Sie orten, Ihren Kalender, Ihre SMS und Ihre E-Mails lesen und Ihre Eingaben oder Sprachbefehle speichern, um daraus Ihre persönlichen Vorlieben zu lernen.

Lassen Sie Ihrer Assistenz nicht zu viel Freiraum, sondern machen Sie klare Vorgaben zu dem von Ihnen gewünschten Datenschutz. Virtuelle Assistenten können eine Hilfe sein, aber auch sehr neugierige Datensammler. &

Vertrauen Sie den Assistenz-Apps zu viele Daten an? Testen Sie sich!

Frage: Ihr Smartphone erinnert Sie an Ihren Hochzeitstag. Woher hat das Smartphone diese Information?

a) Wenn ich den Hochzeitstag nicht im privaten Kalender vermerkt habe, kann es das nicht wissen.
b) Die Assistenz-App könnte meine E-Mail an meine Tochter gelesen haben, in der ich über die geplante Überraschung zum Hochzeitstag etwas geschrieben habe.

Lösung: Die Antwort b. ist richtig. Wenn Sie nicht verhindern, dass Ihr virtueller Assistent Ihre E-Mails auswertet, findet er auch dort Ihre Hinweise auf Termine und wertet sie aus. Achten Sie auf die Datenschutz-Einstellungen der entsprechenden App.

Frage: Sie haben die GPS-Ortung bei Ihrem Smartphone deaktiviert. Trotzdem scheint Ihre Assistenz-App zu wissen, wo Sie gerade sind. Wie kann das sein?

a) Die Assistenz-App kann auch das genutzte WLAN oder die aktuelle Mobilfunkzelle für die Ortung auswerten.
b) Überhaupt nicht, ohne GPS-Daten kann ich nicht geortet werden..

Lösung: Die Antwort a. ist richtig. Je nach Datenschutz-Einstellung können auch Ihre Netzwerkdaten Ihren aktuellen Standort verraten. Beschränken Sie die Zugriffsrechte der Assistenz-App, sodass das von Ihnen gewünschte Datenschutzniveau tatsächlich auch vorhanden ist. Vermeiden Sie also zum Beispiel die Ortung über die Netzwerkanalyse durch die App, wenn Sie Ihre aktuelle Position nicht in eine Cloud übertragen wollen.

Akademie

Ausbildung Datenschutzbeauftragte
Grundlagenseminar Datenschutz
inkl. Ausblick auf die EU-Datenschutzgrundverordnung

Das Seminar vermittelt in kompakter Form das „Handwerkszeug“ für die Aufgaben eines betrieblichen Datenschutzbeauftragten auf Grundlage der aktuellen Datenschutzgesetze. Anschauliche Beispiele aus der Datenschutzpraxis vermitteln das komplette Basiswissen. In nur drei Tagen erlernen Sie so die notwendige Fachkunde.

Inhalte des Seminars

- Einführung und Sensibilisierung
- Rechtliche Grundlagen des Datenschutzes
- Grundzüge und Vergleich der Gesetze
- Rechtsstellung, Anforderungen und Aufgaben des Datenschutzbeauftragten
- Daten: Erhebung, Verarbeitung und Nutzung
- Rechte der betroffenen Personen
- Bereichsspezifischer Datenschutz
- Praktische Fallbeispiele
- Informationssicherheit
- Technische- und organisatorische Maßnahmen
- Die ersten 100 Tage des Datenschutzbeauftragten
- Aktuelle Herausforderungen (Cloud Computing, Social Media)

Termine

Ausbildung Datenschutzbeauftragte allgemein
27.–29.09.2016, Hannover
18.–20.10.2016, Düsseldorf

Ausbildung Datenschutzbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft
06.–08.09.2016, Düsseldorf
12.–14.09.2016, Hannover

Ausbildung IT-Sicherheitsbeauftragte
Grundlagenseminar Informationssicherheit
auf Basis von IT-Grundschutz und ITSVO-EKD

Das Seminar vermittelt anschaulich und praktikabel das „Handwerkszeug” für die Aufgaben eines IT-Sicherheitsbeauftragten. Die Teilnehmer eignen sich ein fundiertes aktuelles Fachwissen an, mit dem sie den professionellen Schutz ihrer Informationen und IT-Systeme gewährleisten können.

Inhalte des Seminars

- Einführung in die IT-Sicherheit
- Rechtliche Rahmenbedingungen
- Verfügbare Normen
- Organisatorische Sicherheitsmaßnahmen
- Technische Sicherheitsmaßnahmen
- Entwicklung eines IT-Sicherheitskonzeptes (BSI)
- Praxisorientierte Vorgehensweise nach BSI IT-Grundschutz
- Definition IT-Verbund, Durchführung Strukturanalyse, Schutzbedarfsfeststellung
- Pflege und Optimierung des IT-Sicherheitskonzeptes
- Rechtliche Fallstricke der IT-Sicherheit
- Besondere Themen wie (Sozial-)Datenschutz, Schweigepflicht, Fernmeldegeheimnis
- Haftung des IT-Sicherheitsbeauftragten

Termine

Ausbildung IT-Sicherheitsbeauftragte
20.–22.09.2016, Hannover
11.–13.10.2016, Düsseldorf

Ausführliche Seminarbeschreibungen und Anmeldemöglichkeiten finden Sie hier:
www.althammer-kill.de/akademie.html

Termine

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

22.09.2016, Karl-Bröger-Zentrum, Nürnberg
Seminar Datenschutz-Praxis
Seminar Datenschutz-Praxis für IT-Abteilungen und Software-Anbieter
Anmeldung über: www.finsoz.de

18.10.2016, Bonifatiushaus, Fulda
Seminar IT-Notfallmanagement
Praxisorientiertes Seminar zum Einstieg in ein strukturiertes IT-Notfallmanagement
Anmeldung über: www.finsoz.de

26.10.2016 – 27.10.2016, Nürnberg
Messe ConSozial 2016
Wir freuen uns auf Ihren Besuch!

10.11.2016, Fachtagung, Berlin
Datenschutz in der Medizin Update 2016
Angebot unseres Kooperationspartners:
www.esturias.de/programm-2016

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

News

Aus unserem
aktuellen Newsletter:

Stets auskunftsfreudig: Blackberrys haarsträubender Umgang mit vertraulichen Daten
www.althammer-kill.de/news-detail/stets-auskunftsfreudig-blackberrys-haarstraeubender-umgang-mit-vertraulichen-daten.html

Störerhaftung fällt… vielleicht?!
www.althammer-kill.de/news-detail/stoererhaftung-faellt-vielleicht.html

Verbraucher informieren – Abmahnungen vermeiden!
www.althammer-kill.de/news-detail/online-streitbeilegung-verbraucher-informieren-abmahnungen-vermeiden.html

Briefpost – Verletzung des Briefgeheimnisses droht!
www.althammer-kill.de/news-detail/briefpost-verletzung-des-briefgeheimnisses-droht.html

Finale Fassung der EU-DSGVO auf Deutsch erschienen
www.althammer-kill.de/news-detail/finale-fassung-der-eu-dsgvo-auf-deutsch-erschienen.html

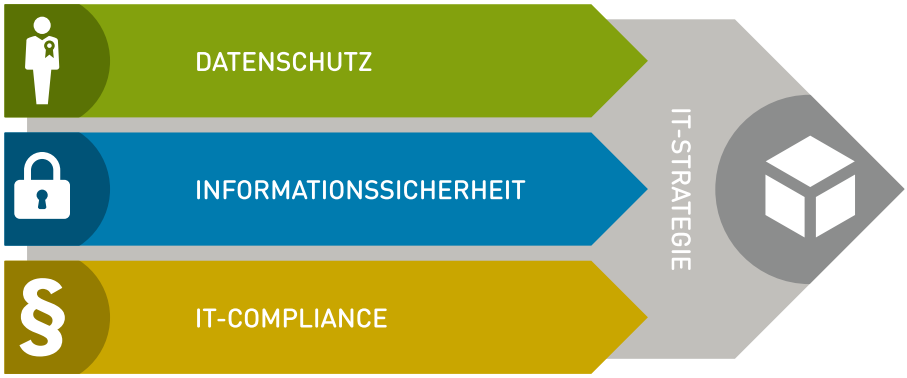
Anmeldemöglichkeiten zu unserem Newsletter finden Sie unter:
www.althammer-kill.de

12 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 3/2016

ALTHAMMER & KILL

Althammer & Kill – Wir schützen Ihre Daten.

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



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). &

Niels Kill
Geschäftsführer
Tel. +49 211 936748-20
nk@althammer-kill.de

Thomas Althammer
Geschäftsführer
Tel. +49 5139 973949-2
ta@althammer-kill.de

Frank Keusemann
Fachkraft für Arbeitssicherheit
Tel. +49 211 936748-60
fk@althammer-kill.de

Mariusz Bucki
Berater für IT-Sicherheit
und Datenschutz
Tel. +49 211 936748-30
mb@althammer-kill.de

Lars Begerow
Berater für IT-Strategie
Tel. +49 211 936748-40
lb@althammer-kill.de

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 211 936748-0
ak@althammer-kill.de

Katja Borchhardt
Organisation & Marketing
Tel. +49 211 936748-0
kb@althammer-kill.de

Althammer & Kill GmbH & Co. KG

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

Mitglied im:

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Standort Hannover:
Buchenhain 15 · 30938 Burgwedel
Tel. +49 5139 973949-0 · Fax -9