Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 2/2017

Liebe Leserin, lieber Leser,

in der Vorbereitung dieses Kundenmagazins hat uns ein Thema besonders bewegt: Künstliche Intelligenz. Sogenannte „Chatbots“ werden schon längere Zeit im Internet eingesetzt und wir stellen auf Seite 6 die datenschutzrechtlichen Hintergründe vor.

Vergleichbare Bots könnten aber auch genutzt werden, um die politische Meinungsbildung zu beeinflussen. Als „Social Bots“ sorgen sie dann für Ärger und Verwirrung. Entsprechende Gerüchte über Wahlbeeinflussungen gab es bereits. Nach anfänglicher Besorgnis werden nun Stimmen laut, die derartige Technik selbst für die Beantwortung politischer Anfragen bei Parteien nutzen wollen.

Weitere Themen in dieser Ausgabe sind die Ausweitung der Videoüberwachung und der Boom bei Smartwatches. Wir werfen einen Blick auf Sicherheitsfunktionen und Privatsphäre ab Seite 3.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

(Noch) mehr Videoüberwachung?

„Videoüberwachungsverbesserungsgesetz“ – eine solche Bezeichnung kann wohl nur die deutsche Verwaltung erfinden. Es geht jedoch um eine ernste Sache, nämlich um den Schutz vor Terror und Gewalt. Das neue Gesetz ändert im Alltag einiges, ob bei der Busfahrt zur Arbeit oder beim Shoppen im Einkaufszentrum.

Wer schon einmal in London war, weiß davon zu berichten: Videokameras hängen buchstäblich an jeder Ecke, ob im Einkaufszentrum oder im Sportstadion. In Deutschland ist das anders. Natürlich gibt es auch hier Überwachungskameras. Aber längst nicht in die-

In dieser Ausgabe:

ser Zahl. Das liegt zunächst einmal an unterschiedlichen gesetzlichen Regelungen. Aber in Deutschland legen die Aufsichtsbehörden für den Datenschutz die Regelungen außerdem besonders eng aus. So sieht es jedenfalls die Bundesregierung. Deshalb hat sie wenige Tage vor Weihnachten gehandelt: Ein neues Gesetz soll dafür sorgen, dass Videoüberwachung leichter möglich ist als bisher.

Neuregelung für Orte mit vielen Menschen

Von der neuen Regelung betroffen sind ausschließlich Örtlichkeiten, an denen erfahrungsgemäß viele Menschen zusammenkommen. Gedacht ist an Einkaufszentren, große Sportanlagen, Vergnügungsstätten und Parkplätze. Außerdem geht es um Verkehrseinrichtungen wie Bahnhöfe und Haltestellen, aber auch um Fahrzeuge des öffentlichen Personenverkehrs (Busse, S- und U-Bahnen).

Vorbeugender Schutz

Der Schutz von Personen, die sich dort aufhalten, gilt künftig als „besonders wichtiges Interesse“. Das bedeutet: Dieser Schutz rechtfertigt es in der Regel, dass solche Örtlichkeiten per Video überwacht werden. Verwundert mag sich nun mancher fragen: War das bisher anders? Die Antwort lautet schlicht: Ja! Die Regelungen für die Videoüberwachung wurden meistens sehr eng ausgelegt.

Eher abstrakte Gefahren hielt die Datenschutzaufsicht nicht für ausreichend, um eine solche Überwachung zu rechtfertigen. Die bloße Möglichkeit, dass es zu üblen Vorfällen kommen könnte (und da und dort auch kam!), genügte nicht.

Hintergrund: Terroranschläge

Das wird sich durch die neuen Regelungen ändern. Der Grund liegt auf der Hand: Terroranschläge wie im Münchner Olympia-Einkaufszentrum oder auf dem Weihnachtsmarkt neben der Berliner Gedächtniskirche haben zu einem anderen Rechtsempfinden geführt. Daneben will man aber auch der zunehmenden Gewalt in U-Bahnhöfen und an ähnlichen Orten nicht mehr länger zuschauen. Wunder erwartet sicher dabei niemand. Denn mancher Täter wird sich von Kameras abschrecken lassen, mancher Täter nicht.

Keine Änderungen in Unternehmen

Keine Änderungen gibt es übrigens für die Videoüberwachung in den Produktionsbereichen von Unternehmen. Dort bleibt alles bei den bisherigen Regelungen. Sie haben sich bewährt. Und auch an der Supermarktkasse ändert sich nichts. Auf dem Parkplatz vor dem Supermarkt dagegen schon. Hier dürften bald neue Kameras zu sehen sein. &

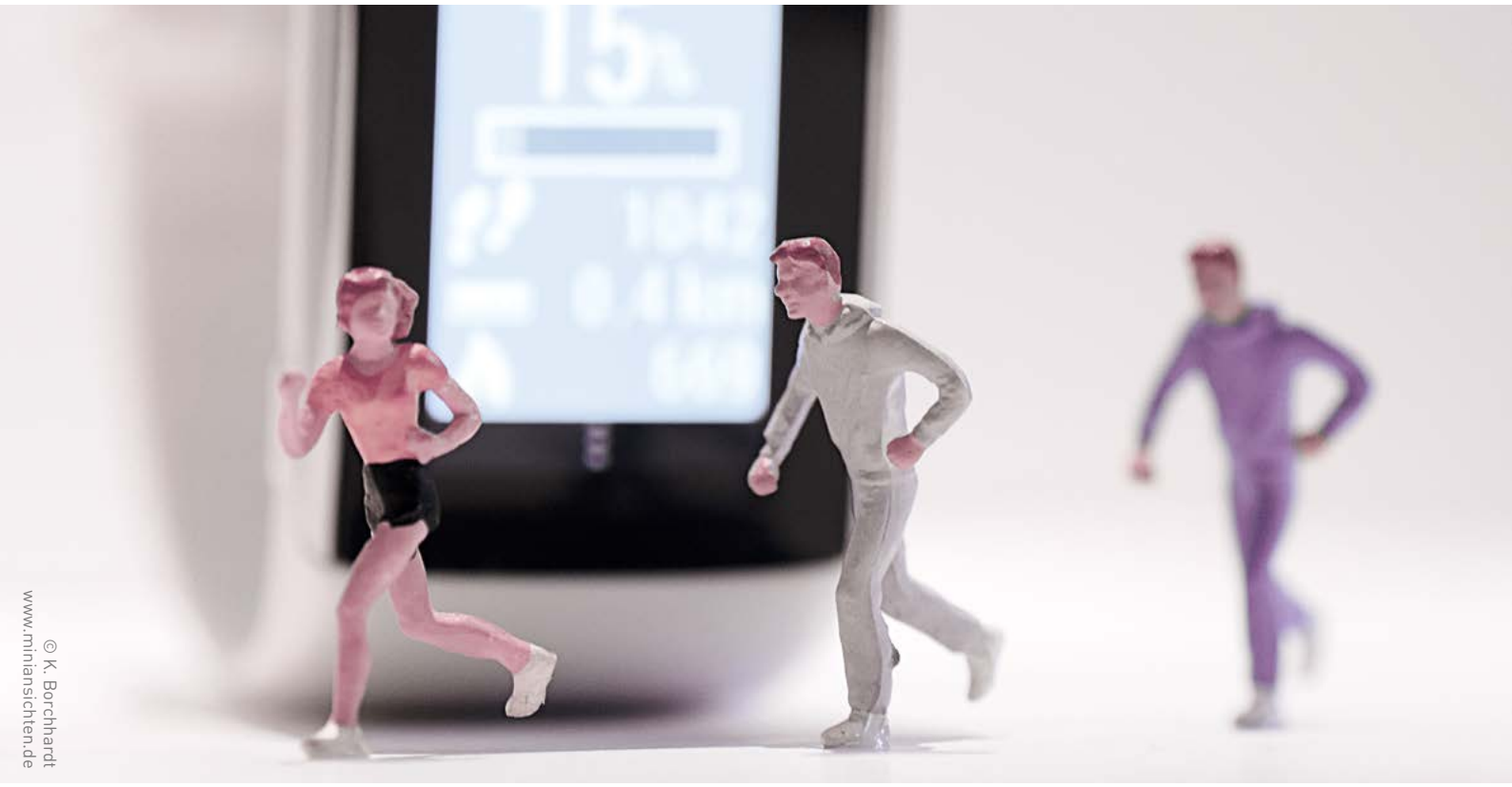
Impressum

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.

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

Schutzgebühr Print-Ausgabe: 10,– €



Smartwatches: Spione am Handgelenk?

Smartwatches, die intelligenten Armbanduhren, liegen im Trend. Um ihre Datensicherheit ist es jedoch nicht gut bestellt.

Technik stand Weihnachten 2016 bei vielen ganz oben auf dem Wunschzettel, wie der Digitalverband Bitkom mitteilte. Als Geschenke waren Mobilgeräte wie Smartphones und Tablet-Computer sehr gefragt. Auch die sogenannten Wearables wie Smartwatches und Fitness-Tracker lagen häufig unter dem Weihnachtsbaum. Doch leider wird bei aller Begeisterung vergessen, was die vielen neuen Geräte für unsere Privatsphäre bedeuten können.

Technik-Fans aufgepasst!

Gerade die Wearables, also Geräte, die wir als Nutzer am Körper tragen, sind ständig bei uns. Sie müssen den Nutzer nicht verfolgen, sondern sind mit der Person direkt und eng verbunden. Diese Nähe sollte Anlass genug sein, um über die Funktionen der Smartwatches und anderer Wearables genauer nachzudenken. So sind die Smartwatches nicht einfach nur Armbanduhren, die anstelle eines Zifferblatts ein hübsches buntes Display haben, das neben der Uhrzeit auch Fotos des Nutzers anzeigen kann.

Smartwatches können mehr, als die Uhrzeit zu verraten

61 Prozent der Personen, die sich für eine Smartwatch interessieren, wünschen sich etwa das Anzeigen der Daten von Fitness-Apps wie der zurückgelegten Strecke beim Joggen. 39 Prozent würden mit ihrer Smartwatch gern Gesundheitsdaten wie Puls oder Blutdruck messen und bei Bedarf automatisch Verwandte oder den Arzt informieren. Zudem möchten 23 Prozent die Smartwatch als Navigationsgerät einsetzen und 56 Prozent zum Anzeigen eingegangener SMS oder E-Mails, wie eine Bitkom-Umfrage ergab.

Offensichtlich gelangen so vertrauliche Daten wie E-Mails und SMS und sogar hochsensible Gesundheitsdaten auf die intelligenten Armbanduhren. Trotzdem haben lediglich 30 Prozent der Befragten Angst vor

Datenmissbrauch. Nur jeder Vierte hat die Sorge, dass Hacker die Smartwatch angreifen könnten. Da stellt sich die Frage, wie datenschutzfreundlich und sicher Smartwatches und andere Wearables wirklich sind.

Mehrere Aufsichtsbehörden für den Datenschutz haben sich dieser Frage angenommen und verschiedene Wearables sowie die zugehörigen Fitness-Anwendungen überprüft – mit ernüchterndem Ergebnis.

Prüfungen der Aufsichtsbehörden sind alarmierend

Bereits die Datenschutzerklärungen erfüllen meistens nicht die gesetzlichen Anforderungen. Sie sind in der Regel viele Seiten lang, nur schwer verständlich und enthalten lediglich pauschale Hinweise zu essenziellen Datenschutzfragen, so die Aufsichtsbehörden. Beunruhigend sind auch die Aussagen zur Datenweitergabe: Der Nutzer erfährt oftmals weder, an wen genau die Daten weitergegeben werden, noch kann er widersprechen. Generell sind die Daten aber auch für Werbezwecke und zur Profilbildung äußerst interessant.

Viele Geräte bieten keine Möglichkeit, Daten selbstständig vollständig zu löschen. Weder im Gerät selbst noch im Nutzerkonto gibt es eine Löschfunktion. Mitunter werden die Fitness-Daten der Nutzer nicht nur von der Smartwatch auf das Smartphone übertragen, sondern direkt an den Anbieter oder an Partnerunternehmen des Anbieters. In der Regel ist dies mit Risiken verbunden, derer sich die Nutzer bewusst sein sollten, so die Datenschützer.

Sicherheitsfunktionen sind bei Smartwatches eine Seltenheit

Im Vergleich zu Smartphones sind die Smartwatches auch kaum mit Sicherheitsfunktionen ausgestattet, obwohl viele Modelle vergleichbare Betriebssysteme und die Möglichkeit haben, Apps zu installieren. Einen Schutz vor Schadsoftware, eine Verschlüsselung der gespeicherten Daten, eine Verschlüsselung der Datenübertragung und einen Zugangsschutz zumindest über eine Passwortabfrage sucht man in aller Regel vergebens.

Neben der Privatnutzung der Smartwatches nimmt auch der berufliche Einsatz zu. Es gibt inzwischen bereits ausgesprochene Business-Smartwatches. Firmen-Mails landen dann ebenso auf der Smartwatch wie digitale Dokumente. Denn der Speicherplatz ist dank Erweiterung über Speicherkarten durchaus üppig. Trotzdem haben selbst die Business-Smartwatches kaum Sicherheitsfunktionen zu bieten. Einige bringen einen Passwortschutz mit. Erst wenige Anbieter haben die Möglichkeit geschaffen, dass Sicherheits-Apps entwickelt und später installiert werden.

Vorsicht ist angebracht

Misstrauen Sie also dem geliebten Weihnachtsgeschenk Smartwatch. Machen Sie es nicht einfach zu Ihrem persönlichen Begleiter und Assistenten, der immer dabei ist und alle Termine und E-Mails kennt. Sonst könnten die vertraulichen Daten schneller die Armbanduhr verlassen, als Sie denken, und Sie hätten womöglich einen Spion am Handgelenk. Nutzen Sie die vielfältigen Funktionen deshalb nur mit Vorsicht. Achten Sie darauf, dass die Verbindungen zwischen Smartwatch und anderen Geräten keinesfalls ständig aktiv sind. So unterbinden Sie auch eine mögliche Übermittlung der aktuellen Standortdaten und eine dauerhafte Ortung durch Dritte. &

Nützliche Sicherheitstipps vom BSI

BSI – bisher noch nie gehört? Das ist schade! Denn das „Bundesamt für Sicherheit in der Informationstechnik" hilft Unternehmen und Normalbürgern gleichermaßen. Von seinen Sicherheitstipps kann jeder profitieren. Machen Sie einen Versuch!

„Ich surfe nur auf vertrauenswürdigen Seiten, darum muss ich mich nicht vor Cyber-Angriffen schützen."

So denkt mehr als einer. Schön wär's, kann man dazu nur sagen!

Scheinbar sichere Internetseiten

Natürlich ist es vernünftig und richtig, sich von dubiosen Internetseiten von vornherein fernzuhalten. Das allein reicht aber nicht. Denn, so das BSI: „Leider können auch vertrauenswürdige Seiten hin und wieder von Schadsoftware betroffen sein. Sie kann sich beispielsweise in Werbebannern verstecken und sich unbemerkt auf dem PC des Nutzers installieren. Sogenannte Drive-by-Downloads, bei denen Inhalte ohne Zutun des Nutzers im Hintergrund heruntergeladen werden, können auch über populäre Internet-Seiten erfolgen."

Bequeme öffentliche WLANs

„Das Surfen in öffentlichen WLANs spart nicht nur Kosten, sondern ist auch sicher."

Jedenfalls an der Ersparnis ist etwas dran. Doch sollte man auch bedenken, dass die Datenübertragung zwischen dem mobilen Gerät und dem Router, der die Internetverbindung herstellt, meist unverschlüsselt erfolgt. Deshalb empfiehlt das BSI: „Über öffentliche WLANs sollten nie vertrauliche Daten übertragen werden, es sei denn, sie werden zuvor lokal auf dem eigenen Gerät verschlüsselt oder über ein virtuelles privates Netzwerk (VPN) übertragen. Das gilt vor allem, wenn auf das Heim- oder Firmennetzwerk zugegriffen werden soll."

Bitte denken Sie dabei daran, die Vorschriften Ihres Unternehmens für externe Zugriffe auf das Firmennetzwerk zu beachten!

Scheinbar uninteressante Daten

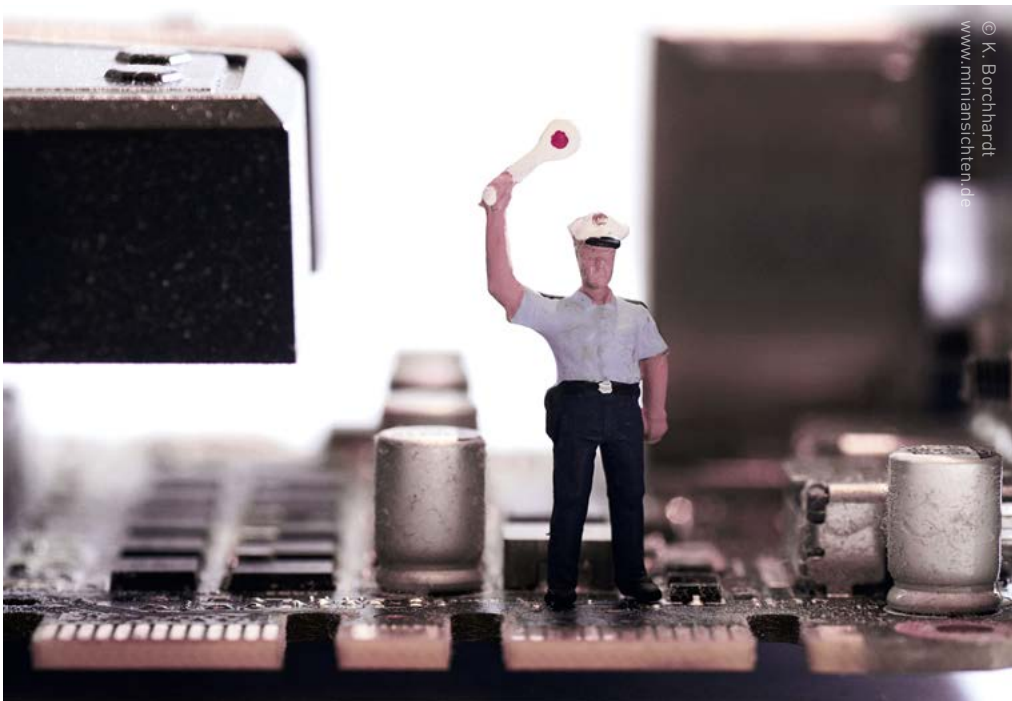
„Ich habe nichts zu verbergen und keine wichtigen Daten, also bin ich doch kein Ziel für Cyber-Kriminelle und muss mich deshalb nicht schützen."

Für Unternehmensdaten gilt das natürlich niemals. Aber vielleicht wenigstens für Ihre privaten Daten?

Das BSI sieht auch das anders: „Diese Ansicht ist grundlegend falsch. Cyber-Kriminelle können alle Daten für ihre Zwecke nutzen. Jeder, der mit einem ungeschützten Gerät im Internet surft, einkauft oder Online-Banking betreibt, hinterlässt eine Vielzahl an Daten, für die sich Cyber-Kriminelle interessieren. Das sind nicht unbedingt die auf dem Rechner gespeicherten Urlaubsfotos, Korrespondenzen oder andere private Dokumente.

Von einem ungeschützten Rechner können Kriminelle dort gespeicherte oder im Internet übertragene Zugangs-, Konto- und Kreditkartendaten leicht stehlen und missbrauchen."

Wiegen Sie sich also nicht in falscher Sicherheit und achten Sie auch beim privaten Rechner auf einen aktuellen



Virenschutz sowie auf regelmäßige Updates aller Programme!

Gelöscht und trotzdem noch vorhanden

„Wenn ich alle Daten von meinem Gerät lösche und anschließend den Papierkorb leere, sind die Daten ein für alle Mal weg."

Sie sind gut mit der EDV vertraut und lächeln über so viel Naivität? Glückwunsch! Aber kennt sich Ihr Kollege genauso gut aus? Man kann über das Thema nicht oft genug sprechen: „Durch das Verschieben von Dateien in den Papierkorb bleiben die Dateien vollständig auf dem Speichermedium erhalten. Auch nach Leeren des Papierkorbs lassen sich Daten mit wenig Aufwand wiederherstellen, da bei diesem Vorgang lediglich die Verweise auf die Daten im Index, dem Inhaltsverzeichnis der Festplatte, gelöscht werden und der Bereich zum Überschreiben freigegeben wird." So der Hinweis des BSI zu diesem Thema.

Ach übrigens: Auch in Scangeräten und Fotokopierern gibt es Datenträger mit großer Kapazität, die alles längerfristig festhalten. Wird das Gerät gestohlen, hat der Dieb Zugriff auf all diese Daten.

Attacke per Mail

„Wenn ich eine E-Mail nur anschaue, aber keinen Anhang öffne, kann nichts passieren."

Klarer Fall: Bevor man einen Anhang öffnet, sollte man immer erst einmal überlegen, ob die Mail vertrauenswürdig ist. Aber für sich allein reicht das nicht als Schutz. Denn, so das BSI: „Viele E-Mails sind farbig, mit verschiedenen Schriften und Grafiken gestaltet. Dort kann schädlicher Code versteckt sein, der bereits beim Öffnen der Mail ausgeführt wird, ohne dass dafür ein Anhang angeklickt werden muss."

Empfehlung daher: „Deshalb sollten Nutzer in ihrem E-Mail-Programm die Anzeige von E-Mail im HTML-Format deaktivieren."

Sie möchten noch mehr Tipps?

Dann geben Sie in einer Suchmaschine einfach „BSI Sicherheitsirrtümer" ein! &

Chatbots: hilfreiche Antworten oder neugierige Automaten?

Viele Online-Shops und Support-Seiten bieten Besuchern über Chat-Fenster Unterstützung bei Fragen an. Meist stecken keine Menschen, sondern Maschinen dahinter. Das hat Folgen für den Datenschutz.

Im Internet kann man alles finden. Wenn man es denn findet. Viele Online-Shops haben ein so umfangreiches Sortiment, dass man sich als Kunde eigentlich eine Beratung wünscht, wie man sie im Geschäft um die Ecke gewöhnt ist. Nur wartet im Internet niemand, um den Kunden zu unterstützen, so scheint es.

Doch plötzlich geht ein Dialog auf der Webseite auf, und es meldet sich ein Berater, der seine Hilfe anbietet. Meist ist es ein kleines Chat-Fenster, mit einem Foto oder einer Zeichnung, die eine Person zeigt. Die Person stellt sich mit einem Satz vor, und man kann seine Fragen stellen.

Solche Fenster findet man nicht nur in Online-Shops, sondern auch auf vielen Support-Webseiten. Neben der altbekannten FAQ-Liste, die Antworten auf die häufigsten Fragen vorhält, trifft man häufig auf diese Art von virtuellem Supportmitarbeiter, mit einer Meldung in einem Chat-Fenster, in das man seine Fragen und Probleme eintragen kann.

Support und Beratung vom Automaten

Die Antworten und Tipps aus dem Chat-Fenster sind teilweise so gut, dass man eine echte Person dahin-

ter vermuten könnte, jemanden aus einem Callcenter vielleicht. Oftmals sind es aber keine Menschen, die antworten, sondern Automaten, sogenannte Chat-Roboter oder Chatbots.

Nun könnte es einem ja gleichgültig sein, ob es nun ein Chatbot oder ein Callcenter ist, abgesehen von der Frage nach den wegfallenden Arbeitsplätzen. Doch es ergeben sich weitere Konsequenzen aus der Entwicklung, dass sich die Betreiber von Webseiten in Zukunft vermehrt für Automaten entscheiden werden. Die Chatbots sollen möglichst intelligent sein. Denn andernfalls sind die Nutzer unzufrieden, und es sind doch Menschen für Beratung und Support nötig. Deshalb werden Chatbots so entwickelt, dass sie den Besucher so weit wie möglich analysieren, um die Antworten persönlich und passend zu gestalten. Ebenso werden die Fragen der Besucher gespeichert und ausgewertet, um sich auf die Fragen immer besser vorbereiten zu können – automatisiert, versteht sich.

Vorsicht bei der Eingabe persönlicher Informationen

Betrachtet man die Datenschutzerklärungen verschiedener Anbieter von Chatbots, lässt sich feststellen, dass die Anbieter teilweise die IP-Adressen und andere Daten der Besucher speichern, die Rückschlüsse auf die fragenden Personen zulassen. Wer dann noch in seinen Fragen persönliche Details verrät, kann ungewollt ermöglichen, dass der Anbieter ein detailliertes Besucherprofil erzeugt. Je nach Anbieter und Betreiber lässt sich dieses Besucherprofil auch anders nutzen als dazu, die automatische Kundenbetreuung zu verbessern.

Bevor Sie also im nächsten Online-Shop oder Support-Forum dem virtuellen Berater Ihre Fragen anvertrauen, schauen Sie sich am besten die Datenschutzerklärung der Webseite und zum Chatbot an.

Datensparsamkeit ist Trumpf

Denken Sie zudem auch hier an die Datensparsamkeit: Es geht weder um Smalltalk noch um einen persönlichen Kontakt, wenn Sie einen Chatbot nutzen, sondern um eine automatische FAQ-Liste, die mitunter sehr neugierig sein kann. So hilfreich solche Dienste in Online-Shops und auf anderen Webseiten auch erscheinen – es geht eventuell eher um Ihre Daten, nicht nur um eine virtuelle Kundenberatung. &

Kennen Sie die Risiken durch Automaten und Chatbots im Internet? Testen Sie Ihr Wissen!

Frage: Fragefenster bei Online-Shops und Support-Seiten liefern nur Antworten und speichern nichts. Stimmt das?

a. Ja, denn FAQ-Listen speichern ja auch nichts.
b. Nein, meine Fragen und Kommentare können gespeichert werden.
c. Nein, sogenannte Chatbots speichern mitunter sogar die IP-Adressen der Besucher.

Lösung: Die Antworten b. und c. sind richtig. Nicht jedes Fragefenster führt zur Speicherung der IP-Adresse und anderer personenbezogener Daten, doch manche Chatbots tun dies. Die Eingaben dagegen werden sogar häufig gespeichert, um zu erfahren, was die Nutzer am meisten interessiert. Zusammen mit den personenbezogenen Daten können dadurch genaue Nutzerprofile entstehen.

Frage: Steht in der Datenschutzerklärung des Online-Shops nichts dazu, speichert der Chatbot auch nichts. Stimmt das?

a. Nein, denn viele Datenschutzerklärungen im Internet sind unvollständig. Zudem meinen viele Webseitenbetreiber, der Anbieter der Chatbot-Software sei dafür zuständig.
b. Ja, dann werden meine Angaben nicht gespeichert und ausgewertet.

Lösung: Die Antwort a. ist richtig. Genau wie beim Einsatz von Webanalyse-Werkzeugen vergessen viele Webseitenbetreiber, dass sie auf die Datenspeicherung und Datenauswertung hinweisen müssen. Zudem haben viele Hersteller von Chatbot-Software selbst gar keine Datenschutzerklärung, oder der Besucher des Online-Shops findet sie kaum. Beachten Sie in jedem Fall, dass Sie sparsam mit Ihren Daten umgehen und so wenig wie möglich preisgeben, wenn Sie einen Chatbot nutzen.

Öffentlichkeitsarbeit und Bildrechte bei Facebook – Versuch eines praxisnahen Brückenschlags

Viele Unternehmungen hegen im Rahmen der Öffentlichkeitsarbeit den Wunsch, Fotos von öffentlichen oder internen Veranstaltungen in verschiedenen Print- oder Online-Medien zu publizieren. Häufig ergibt sich dadurch ein Zielkonflikt mit den Persönlichkeitsrechten der abgebildeten Personen. Dieser Artikel zeigt rechtskonforme und dabei praxisnahe Lösungswege auf.

Eine besondere Variante des Persönlichkeitsrechts ist das sogenannte Recht am eigenen Bild, das etwas versteckt im Kunsturheberrechtsgesetz (KunstUrhG) geregelt ist. Es wurde verabschiedet nachdem Journalisten im Jahre 1898 unbefugt den Leichnam des ehemaligen Reichskanzlers Otto von Bismarck fotografiert hatten und versuchten, die Aufnahmen zu veröffentlichen.

Da das Recht am eigenen Bild vorher unbekannt war, musste das Reichsgericht, nachdem die Täter dingfest gemacht werden konnten, die Vernichtung der Fotos mit einem mutmaßlichen Hausfriedensbruch der Fotografen begründen. Aus dieser rechtlichen Regelungslücke entstand das Bedürfnis, die Verletzung des höchstpersönlichen Lebensbereichs durch unbefugte Bildaufnahmen explizit legislativ zu ahnden. Das in der Folge verabschiedete und bis heute gültige Kunsturheberrechtsgesetz spricht hier eine klare Sprache: Demnach dürfen Bildnisse lediglich mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.

Auch nach dem Ableben fotografierter Personen ist für einen Zeitraum von zehn Jahren eine Einverständniserklärung Familienangehöriger einzuholen. Von der Einwilligungspflicht ausgenommen sind:

- Aufnahmen aus dem Bereich der Zeitgeschichte,
- Fotos bei denen vordergründig eine Landschaft oder ein besonderer Ort abgebildet werden soll,
- Aufnahmen, die dem Kunstinteresse dienen oder Fotos, welche von öffentlichen Veranstaltungen, Aufzügen und ähnlichen Vorgängen angefertigt werden.

Besonders der letzte Punkt, Aufnahmen von öffentlichen Veranstaltungen, ist vor dem Hintergrund häufig klärungs- und auslegungsbedürftig. Der Sinn und Zweck der Einwilligungsfreiheit des KunstUrhG besteht in dem ebenfalls grundgesetzlich geschützten Recht der Berichterstattung über ein öffentliches Ereignis. Somit sind die beiden widerstreitenden Rechtspositionen gegeneinander abzuwägen. Juristen nennen diesen Vorgang praktische Konkordanz.

Im Ergebnis muss folglich hinsichtlich der Abbildungsfreiheit darauf geachtet werden, ob nicht eher einzelne Personen auf dem zu publizierenden Foto im Vordergrund stehen, denn dann wäre eine Einwilligung einzuholen, oder ob tatsächlich der Eventkontext der Veranstaltung transportiert wird und somit das Berichterstattungsmerkmal an Gewicht zunimmt.

Abwägung meist schwierig

Unter die Abbildungsfreiheit des KunstUrhG fallen auch Bildveröffentlichungen von Demonstrationen, Faschingsumzügen, Sport- und Kulturveranstaltungen sowie von politischen Versammlungen. Allerdings müssen die Veranstaltungen, was die Personenzahl angeht, eine gewisse Mindestgröße aufweisen, sodass vereinzelte Individuen nicht länger aus der Masse hervorstechen. Darüber hinaus ist nach der Rechtsprechung ein unter den Fotografierten bestehender gemeinsamer Partizipationswille an dem Event erforderlich.

Folglich ist für die Veröffentlichung eines Fotos von zufällig zusammenstehenden Fahrgästen in öffentlichen Verkehrsmitteln oder badenden Personen am Strand grundsätzlich die vorgehende Einwilligung einzuholen.

Eine weitere Rückausnahme zur Verbreitungsfreiheit nach dem KunstUrhG besteht, wenn durch die Veröffentlichung ein berechtigtes Interesse des Abgebildeten verletzt würde.

Für eine solche Rechtsverletzung trägt allerdings prozessual der Abgebildete die Nachweispflicht, d. h. dieser muss darlegen und beweisen, dass durch die Verbreitung des Fotos seine persönlichen Interessen in einem beträchtlichen Maße tangiert werden.

- Zusammengefasst sind also die folgenden Punkte bei der Veröffentlichung von Fotoaufnahmen ohne Einwilligung zu prüfen:
- Das Vorliegen einer gewissen Mindestgröße der aufgenommenen Personengruppe,
- bei welcher der Fokus nicht auf einzelne Personen im Vordergrund gerichtet ist,
- ein gemeinsamer Partizipationswille an der Veranstaltung besteht und
- keine evidenten persönlichen Interessen der Abgebildeten verletzt werden.

Die Einwilligung

Für die Zustimmung zur Veröffentlichung bedarf es einer Willenserklärung der Abgebildeten, welche ausdrücklich oder durch schlüssiges (konkludentes) Handeln erfolgen kann.

An eine stillschweigende Zustimmung sind allerdings besondere Anforderungen zu stellen. Eine solche kommt regelmäßig nicht in Betracht, wenn die Publikationsform oder die Umstände der geplanten Veröffentlichung unbekannt sind beziehungsweise noch gar nicht feststehen.

Bei Minderjährigen ist die Einwilligung der gesetzlichen Vertreter, also in der Regel eines Elternteils, einzuholen. Bei Personen ab ca. 14 Jahren, welche bereits eine gewisse Reife und somit eine einschlägige Einsichtsfähigkeit erreicht haben, ist eben-

CeBIT

Volle Messetage auf der CeBIT

Vom 20.–24.03.2017 hatte die CeBIT in Hannover ihre Pforten geöffnet. Althammer & Kill war in Halle 5 auf dem Gemeinschaftsstand des Landes Niedersachsen vertreten. Was als Versuchsballon gedacht war entpuppte sich als voller Erfolg. Die Tage waren prall gefüllt mit interessanten Gesprächen und Kontakten. Neben neuen Anfragen und Interessenten haben wir uns besonders über die zahlreichen Besuche unserer Kunden gefreut.

Schwerpunkt der IT-Messe waren diesmal Robotik, künstliche Intelligenz und IT-Sicherheitsthemen. Aber auch der Boom bei Drohnen stand im Fokus – wie unsere Standnachbarn eindrucksvoll bewiesen. So wurde die unter der Drohne montierte Kamera von vielen datenschutzrechtlich hinterfragt. Herzlichen Dank an dieser Stelle allen Besuchern auf unserem Stand! &

falls, neben der Einwilligung der Eltern, die Zustimmung des abgebildeten Minderjährigen einzuholen. Die einmal erteilte Einwilligung kann grundsätzlich nur unter besonders engen Voraussetzungen widerrufen werden – die meisten Klagen scheitern in diesem Kontext vor den Zivilgerichten.

Widerruf von (ehemaligen) Mitarbeiterfotos

In der Einwilligungserklärung von Unternehmen, etwa zwecks Veröffentlichungen im Firmenprospekt oder auf der Homepage, wird meist ein Widerrufsrecht vereinbart. Im Falle eines Ausscheidens aus dem Betrieb, ist mit diesem freilich nicht die automatische Rücknahme der Erlaubniserteilung verbunden. Diese ist folglich ausdrücklich gegenüber dem alten Arbeitgeber bekanntzugeben. Anders ist die Rechtslage, soweit die Fotoaufnahmen der Erfüllung der Arbeitspflicht dienen. So hat etwa ein Mannequin keinen Anspruch auf Widerruf.

Folgende Regeln sollten bei der Veröffentlichung von Bildern berücksichtigt werden:

1. Die Teilnehmer/innen an öffentlichen oder internen Veranstaltungen sollten über den Umfang der avisierten Publikation vorab genau informiert werden.

2. Die Art der Veröffentlichungen, etwa Firmenprospekt, Intranet, gemeinsames Laufwerk, Facebook-Auftritt (ebenso andere soziale Netzwerke wie etwa Google+) oder die Unternehmens-Homepage sollten möglichst vorab feststehen und bekannt gegeben werden.

3. Zudem sollten aus Datenschutzgesichtspunkten nur die tatsächlich nötigen Personen, etwa im Falle der Veröffentlichung im Intranet, Zugriff erhalten (Die Veröffentlichung der Fotos einer Weihnachtsfeier einer einzelnen Abteilung im Gesamtintranet wäre hier unverhältnismäßig).

4. Fotos von einzelnen Personen können, auch im Rahmen des betrieblichen Intranets, nur mit ausdrücklicher Einwilligung veröffentlicht werden. Bei Minderjährigen ist das Einverständnis (zumindest) eines Elternteils einzuholen; falls erstere über 14 sind zusätzlich von den Jugendlichen selbst.

5. Ist die vorstehend geschilderte Verbreitungsfreiheit nach dem KunstUrhG nicht gegeben, sollte zu Beweiszwecken stets eine schriftliche Einwilligungserklärung der Fotografierten unterzeichnet werden.

Fazit und praktische Lösungsvorschläge

Die Brücke zwischen dem Recht am eigenen Bild von Teilnehmern an Veranstaltungen sowie dem Arbeitnehmerdatenschutz vis-a-vis der unternehmerisch gebotenen Öffentlichkeitsarbeit zu schlagen, fällt, wie vorstehend deutlich wurde, nicht immer leicht und ist mit einer mitunter juristisch komplexen Interessenabwägung verbunden. Dennoch kann eine rechtswidrige Bildveröffentlichung Schadenersatz- und andere zivilrechtliche Ansprüche, z. B. auf Unterlassung, Herausgabe, Löschung, Geldentschädigung, Auskunft oder Gegendarstellung, sowie unter Umständen einen schwer zu beziffernden „Flurschaden“ begründen. &

Termine

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

19.04.2017, Düsseldorf
Die neue Datenschutz-Grundverordnung (DS-GVO) für mittelständische Unternehmen
Die hohe Komplexität der DS-GVO bringt für Unternehmen spürbare Veränderungen gegenüber dem bisher geltenden BDSG mit sich.

25.–27.04.2017, Dortmund
Ausbildung IT-Sicherheitsbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Informationssicherheit auf Basis von IT-Grundschutz und der IT-Sicherheitsverordnung (ITSVO-EKD)

25.–27.04.2017, Nürnberg
Messe Altenpflege 2017
Wir freuen uns auf Ihren Besuch!

26.–27.04.2017
Fachtagung IV/IT des BEB: Vortrag Smartphone-Einsatz
Regelungsbedarf und Lösungswege in der Sozialwirtschaft

09.–11.05.2017, Dortmund
Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft
Grundlagenseminar Datenschutz auf Basis von BDSG, DSG-EKD und KDO

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

News

Aus unserem aktuellen Newsletter:

Der gläserne iPhone Nutzer: Vom großen Bruder in der Hosentasche
https://www.althammer-kill.de/news-detail/der-glaeserne-iphone-nutzer-vom-grossen-bruder-in-der-hosentasche.html

Neuregelung § 203 StGB: Wird die Schweigepflicht reformiert?
https://www.althammer-kill.de/news-detail/neuregelung-203-stgb-wird-die-schweigepflicht-reformiert.html

Heartbleed feiert 3. Geburtstag
https://www.althammer-kill.de/news-detail/Heartbleed-feiert-3ten-geburtstag.html

Angeln auf Google-Passwörter
https://www.althammer-kill.de/news-detail/angeln-auf-google-passwoerter.html

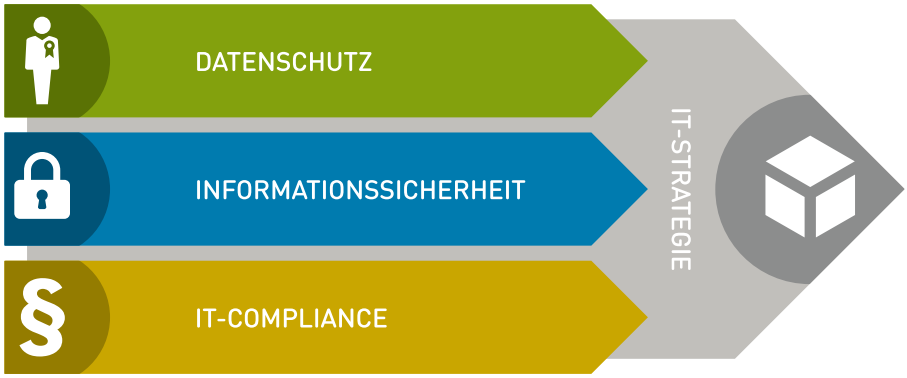
Rückblick 2016 und Vorschau auf 2017
https://www.althammer-kill.de/news-detail/rueckblick-auf-2016-und-vorschau-auf-2017.html

Risiko für kommerzielle Website-Betreiber beim Setzen von Links
https://www.althammer-kill.de/news-detail/risiko-fuer-kommerzielle-website-betreiber-beim-setzen-von-links.html

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

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). &

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 u. 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

Dr. Jan Holling
Berater für Datenschutz
Tel. +49 5139 973949-4
jh@althammer-kill.de

Andreas Hellmann
Berater für Datenschutz u. IT-Sicherheit
Tel. +49 211 936748-34
ah@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

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

Mitglied im:

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