Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2017

Liebe Leserin, lieber Leser,

die Uhr tickt unaufhörlich. Es sind nunmehr nur noch 7 Monate bis die Datenschutz-Grundverordnung am 25. Mai 2018 in Kraft tritt. Wie Sie künftig mit eventuellen Datenpannen umgehen müssen erfahren Sie in unserem Beitrag ab Seite 3.

Sie sind sich des Schutzbedarfs Ihres Smartphones bewusst und möchten dieses deshalb mit einer zusätzlichen Software schützen? Worauf Sie bei der Auswahl der richtigen Software jedoch genau achten sollten, können Sie auf Seite 5 lesen.

Außerdem möchten wir Sie gerne auf die Seiten 9 und 10 aufmerksam machen. Auf diesen wird ein Fall der Rufschädigung via Facebook beschrieben sowie auch die datenschutzrechtlichen Folgen in diesem Zusammenhang. Lesen Sie, wo das Landgericht Düsseldorf den Geltungsbereich des Bundesdatenschutzgesetzes auch im vermeintlich privaten Bereich sieht.

Wir wünschen wieder eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Datenschutzfallen bei PDF-Dokumenten

Sie müssen ein Word-Dokument weiterleiten? Sie wollen dabei Ärger mit dem Datenschutz vermeiden? Sie wandeln das Word-Dokument deshalb in ein PDF-Dokument um? An sich eine gute Idee. Gerade deshalb sollten Sie wissen, was dabei an Details zu beachten ist. Leider kosten manche wichtigen Hilfsmittel etwas.

Word-Dokumente gehören zum Alltag im Büro. Oft ist es nötig, sie weiterzuleiten, etwa als Anhang einer E-Mail. Nachteil dabei: Der Empfänger kann alle möglichen Veränderungen sichtbar machen, die das

In dieser Ausgabe:

Dokument erfahren hat. Dabei kann er meist auch erkennen, von wem die Veränderung stammt. Der Name oder zumindest ein Kürzel stehen dabei.

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,– €

Tückisch: die Zusatzdaten bei Word

Solange das Dokument intern zwischen Kollegen ausgetauscht wird, die daran arbeiten – kein Problem! Denn dann soll ja gerade jeder wissen, wer was verändert hat. Anders sieht es aus, wenn das Dokument nach außen geht. Dann ist das nicht akzeptabel. Für solche Fälle gilt der Tipp: Wandeln Sie Word in PDF um!

Vorteile einer Umwandlung in PDF

Dieser Ratschlag ist ebenso häufig wie richtig. Die Umwandlung hat durchaus einige Vorteile. Ein PDF-Dokument kann nur noch mit relativ aufwendigen Mitteln verändert werden. Damit ist das, was Sie verschickt haben, gewissermaßen fixiert. Außerdem ist nicht mehr festzustellen, wer wann etwas am Word-Dokument verändert hat. Die Nachweise hierfür gehen bei der Umwandlung in ein PDF-Dokument verloren.

Einige typische Fallen

So weit, so gut. Dennoch bleiben einige Tücken, die man kennen sollte:

- Folgende Daten übernimmt ein PDF-Dokument vom Word-Dokument: Name der Word-Datei, Angaben zum Bearbeiter (falls sein Name drin steht, also auch der!) und verwendete Software. Wenn es sinnvoll ist, sollte man daher den Dateinamen und die Angaben zum Bearbeiter ändern.

- Manchmal sollen Teile eines PDF-Textes geschwärzt werden. Dafür bietet Adobe Acrobat das Werkzeug „Inhalt schwärzen und entfernen“. Es ist kostenpflichtig. Das Tool beseitigt den Text, der geschwärzt wird.

- Keine gute Idee ist es dagegen, den Text lediglich mit einem schwarzen Feld zu überlagern. Ein solches Feld kann der Empfänger problemlos wieder entfernen.

- Wenn Teile eines PDF-Dokuments nachträglich „weggeschnitten“ werden, sind sie in Wirklichkeit nur ausgeblendet. Der Empfänger des Dokuments kann diese Teile problemlos wiederherstellen.

Eine besonders wichtige – aber kostenpflichtige – Funktion

Am zuverlässigsten ist es, das PDF-Dokument mit der (kostenpflichtigen) Funktion „vertrauliche Dokumente veröffentlichen“ zu bearbeiten, bevor man es weitergibt. Diese Funktion erzeugt das Dokument komplett neu. Alle unerwünschten Inhalte sind danach beseitigt. &

Neue Spielregeln für den Umgang mit Datenpannen

Eine Verletzung des Datenschutzes „beichten" zu müssen, ist immer unangenehm. Jeder weiß, dass es Folgen haben kann, im schlimmsten Fall auch arbeitsrechtliche. Deshalb schweigen manche lieber. Doch Vorsicht! Ab 25. Mai 2018 gilt die Datenschutz-Grundverordnung (DSGVO). Dann kann das Verschweigen einer Datenpanne alles noch viel schlimmer machen.

Ein Laptop mit Kundendaten ist weg. Wahrscheinlich blieb er vor ein paar Tagen schlicht im Zug liegen. Das Gerät ist schon fünf Jahre alt und wurde nur noch ausnahmsweise benutzt. Also vermisst es niemand wirklich. Und die Kundendaten sind im EDV-System natürlich noch vorhanden. Da wird auch niemand misstrauisch.

Meldepflicht des Unternehmens …

Also lieber mal einfach nichts sagen nach dem Motto „Wird schon gut gehen"? Schon jetzt ist das keine gute Idee. Ab 25. Mai 2018 kann diese Taktik sogar richtig übel enden. Schon jetzt sind Unternehmen verpflichtet, bestimmte Datenpannen der Datenschutzaufsicht zu melden. Ausgangspunkt ist dabei, dass Daten unbefugt übermittelt wurden. Das bedeutet vereinfacht gesagt, dass sie zu Unrecht in die Hände von Außenstehenden gelangt sind.

Das allein reicht aber nicht, um eine Meldepflicht entstehen zu lassen. Vielmehr muss noch hinzukommen, dass „schwerwiegende Beeinträchtigungen" für die Rechte der Personen drohen, um deren Daten es geht.

… bisher oft nur Theorie

Diese Einschränkung führt bisher dazu, dass im Ergebnis oft keine Meldepflicht besteht. Beispiel: Ein Laptop geht verloren. Die Daten auf dem Laptop sind jedoch nach dem Stand der Technik verschlüsselt. Dann kann man davon ausgehen, dass keine schwerwiegenden Beeinträchtigungen drohen. Folge: Eine Meldepflicht entsteht im Ergebnis nicht.

Künftig sieht es anders aus

Die Regelungen der DSGVO für die Meldepflicht sehen anders aus. Sie

kennen eine solche Einschränkung nicht. Vielmehr muss ein Unternehmen künftig jede „Verletzung des Schutzes personenbezogener Daten" der Datenschutzaufsicht melden.

Diese Meldepflicht ist in keiner Weise eingeschränkt. Das bedeutet: Der Verlust eines Laptops mit personenbezogenen Daten muss auch dann gemeldet werden, wenn wahrscheinlich alles ausreichend verschlüsselt war.

Meldefrist: 72 Stunden

Das Brisante dabei: Bei der Meldung an die Datenschutzaufsicht ist eine Frist von 72 Stunden zu beachten. Wird sie grundlos überschritten, droht dem Unternehmen schon deshalb ein Bußgeld. Ausreden von der Art „Unser Mitarbeiter hat uns die Panne intern nicht verraten" gelten dabei nicht. Die Antwort darauf wäre: „Dann bringen Sie Ihren Mitarbeitern eben bei, dass Datenpannen gleich zu melden sind."

Online-Formulare in Vorbereitung

In der Praxis wird es darauf hinauslaufen, dass eine Meldung an die Datenschutzaufsicht künftig relativ häufig notwendig ist. Die ersten Aufsichtsbehörden (etwa das Bayerische Landesamt für Datenschutzaufsicht) stellen dafür schon Online-Formulare bereit.

Ausnahme: Benachrichtigung der Betroffenen

Ob den Betroffenen, um deren Daten es geht, „etwas passieren" kann, spielt bei der Meldepflicht keine Rolle. Dieser Aspekt wird erst wichtig, wenn es um die Benachrichtigung der Betroffenen geht. Sie ist gesondert geregelt (Art. 34 DSGVO). Die Betroffenen müssen nur dann benachrichtigt werden, wenn ihnen „voraussichtlich ein hohes Risiko droht".

Am Beispiel des verschlüsselten Laptops wird wieder deutlich, was das bedeutet: Sind die Daten auf dem Laptop nach dem Stand der Technik verschlüsselt, droht kein hohes Risiko, wenn er Unbefugten in die Hände gerät. Die Folge: Die Betroffenen müssen nicht benachrichtigt werden.

Neue Spielregeln im Überblick

Die Spielregeln für die Zeit ab 25. Mai 2018 lassen sich so zusammenfassen:

- Jeder Mitarbeiter, dem eine Datenpanne unterläuft, muss möglichst sofort seine Vorgesetzten einschalten.
- Nur so lässt sich vermeiden, dass dem Unternehmen ein möglicherweise teures Bußgeldverfahren droht.
- Meldungen von Unternehmen an die Datenschutzaufsicht werden künftig viel häufiger sein als bisher.
- Für sie gilt eine Frist von 72 Stunden. Sie lässt sich nur einhalten, wenn jeder Mitarbeiter Pannen sofort intern meldet.
- Eine Meldung an die Datenschutzaufsicht hat für sich allein noch keine negativen Konsequenzen. Es kann aber natürlich vorkommen, dass die Datenschutzaufsicht genauer nachfragt, was eigentlich genau passiert ist.
- Eine Meldung an die Datenschutzaufsicht führt nicht automatisch dazu, dass die Betroffenen über die Datenpanne benachrichtigt werden. Eine solche Benachrichtigung der Betroffenen ist an relativ enge Voraussetzungen geknüpft. &

5
Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2017

ALTHAMMER & KILL

Was sagen Bewertungen über IT-Sicherheitslösungen?

Hält die Security-App, was sie verspricht? Das ist eine berechtigte Frage, doch die Antwort ist nicht leicht. Anerkannte Produkttests helfen.

Kaum eine Woche vergeht, ohne dass die Medien von Online-Attacken und Hackern berichten. Die Internetkriminellen lassen sich immer neue Angriffsmethoden einfallen. Man liest von diversen Erpresser-Viren, Banking-Trojanern und spionierenden Smartphone-Apps. Bei so vielfältigen Bedrohungen braucht man einen guten Schutz, der sich auf die neuen Gefahren einstellt.

© Katja Borchhardt
www.miniansichten.de

Wie steht es um Ihre Endgeräte? Ist Ihr Smartphone richtig geschützt? Das ist nicht nur für Sie privat ein wichtiges Thema. Wenn Sie Ihr Smartphone auch für Ihre Arbeit nutzen dürfen, dann betrifft dies zusätzlich den Datenschutz im Unternehmen. Sind Sie sich sicher, dass zum Beispiel die Sicherheits-App auf Ihrem Smartphone tatsächlich einen guten Schutz bietet?

Bewertungen in App-Stores reichen nicht

Viele Nutzer orientieren sich dort, wo sie die Security-Apps auf das eigene Smartphone herunterladen können: im App-Store, bei Android-Geräten bei Google Play. Dort findet man zu jeder App die Anzahl der bisherigen Downloads, die durchschnittliche Bewertung in Sternen und oftmals auch Nutzerkommentare.

Wurde die Security-Apps schon häufig heruntergeladen, ist die Anzahl der Bewertungssterne hoch und sind die Kommentare durchweg positiv, glaubt man, eine gute App gefunden zu haben.

Leider sind die Informationen in den App-Stores nicht ausreichend, um eine gute Security-App zu finden. Zum einen können die Nutzer, die kommentieren und Sterne vergeben, in aller Regel nicht wirklich beurteilen, ob die Funktionen für Sicherheit sorgen oder nicht. Oftmals stehen Komfort, leichte Bedienbarkeit, schnelle Installation und guter Preis im Mittelpunkt. Keine Frage, das sind ebenfalls wichtige Kriterien. Über die Schutzwirkung für das Smartphone und Ihre Daten darauf sagen sie aber nichts aus.

Es gibt noch ein weiteres Problem mit den Bewertungen in App-Stores: Sie können gefälscht und gekauft sein. Es sind Fälle bekannt, in denen ganz gezielt gute Kommentare zu Apps gekauft und veröffentlicht wurden, die sich später als schädlich oder nutzlos erwiesen. Es ist deshalb wichtig, andere Quellen bei der Suche nach Security-Apps zu nutzen.

Viele Security-Apps fallen in Tests durch

Anerkannte Institute wie die Fraunhofer-Institute, Stiftung Warentest und AV-Test prüfen regelmäßig, wie gut Security-Apps sind – leider nicht immer mit einem positiven Ergebnis: Im Mai 2016 zum Beispiel meldeten die Forscher des Fraunhofer SIT (Sichere Informationstechnologie), dass sie Lücken in Android-Sicherheits-Apps gefunden hatten. Betrof-

fen waren weltweit bis zu 675 Millionen Installationen bei Nutzern.

Durch Ausnutzung der Schwachstellen konnten Angreifer etwa die Schutzfunktion der Sicherheits-Apps abschalten, ohne dass die Nutzer es merkten. Auch persönliche Daten wie Adressbuch oder Kalender ließen sich stehlen. Im schlimmsten Fall konnte die Sicherheits-App selbst in Erpresser-Software (Ransomware) verwandelt werden, mit deren Hilfe Verbrecher zum Beispiel das Handy sperren konnten, um auf diese Weise vom Smartphone-Besitzer letztlich ein hohes Lösegeld zu erpressen.

Die wesentliche Ursache für viele der gefundenen Schwachstellen bei Security-Apps lag darin, dass die Apps im Stundentakt Updateinformationen herunterladen, zum Beispiel Muster für die Erkennung von Viren. Diese Informationen kommen von den Herstellerservern. Die Apps prüften aber nicht ausreichend, ob das Update möglicherweise manipuliert war.

Im Februar 2017 berichteten die Forscher des Fraunhofer SIT, dass sie Lücken in Android-Passwort-Management-Apps gefunden hatten. Solche Lösungen werden eingesetzt, um Passwörter sicher zu speichern. Sicherheitslücken in diesen Tools können also massive Folgen haben.

Anerkannte Testberichte helfen weiter

Die Security-Apps mit den Sicherheitslücken hatten durchaus positive Bewertungen bei den App-Stores. Kein Wunder also, woher sollten die Nutzer von den Schwachstellen wissen, die die Forscher später entdeckten. Es empfiehlt sich deshalb, dass Sie sich an anerkannten Testberichten orientieren, die nicht nur auf Nutzererfahrungen beruhen, sondern die tatsächlich professionelle Produkttests auswerten.

Beispiele für solche Testberichte zu Security-Apps finden Sie regelmäßig etwa bei AV-Test (https://www.av-test.org/de/antivirus/). Auch Stiftung Warentest (https://www.test.de) nimmt Security-Apps unter die Lupe. Ganz gleich, welches anerkannte Prüfinstitut Sie als Quelle nutzen: Sie werden dort nicht nur Nutzerkommentare finden, sondern Ergebnisse von Sicherheitstests. Solche Tests sollten Ihre Entscheidungsgrundlage sein. &

Das smarte Home Office: Gefahr für den Datenschutz?

Smart Home klingt nach Vernetzung im Privathaushalt. In Wirklichkeit aber bringt Smart Home auch Risiken für betriebliche Daten mit sich. Höchste Zeit, sich zu informieren.

Der deutsche Smart-Home-Markt boomt und wird sich bis 2022 auf 4,3 Milliarden Euro verdreifachen, so die Studie „Der deutsche Smart-Home-Markt 2017–2022. Zahlen und Fakten" des Verbands der Internetwirtschaft (eco) anlässlich der Internationalen Funkausstellung (IFA) 2017 in Berlin.

Viele Neuheiten auf der IFA drehten sich um das vernetzte Zuhause. Für das hohe Interesse an Smart Home und die Vielfalt an neuen Angeboten gibt es gute Gründe: Die Vernetzung von Waschmaschine, Fernseher oder Heizung sorgt für mehr Komfort im Alltag und kann zudem zu Energieeinsparungen führen, wie das BSI (Bundesamt für Sicherheit in der Informationstechnik) ausführt.

Bequem, aber nicht ohne Risiko

Doch das BSI macht noch auf etwas Anderes aufmerksam: Smart-Home-Geräte werden per Software gesteuert und können über das Internet mit der Außenwelt und untereinander vernetzt werden. Gerade das bringt neue Risiken mit sich, die Nutzer im Blick haben sollten.

Auch die Aufsichtsbehörden für den Datenschutz und die Verbraucherschützer machen auf die Risiken aufmerksam. Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit in Rhein-

land-Pfalz, Prof. Dr. Kugelmann, zum Beispiel sagte: „Es wird zunehmend deutlich, dass in einer digitalisierten Umwelt vermeintlich belanglose technische Daten wie zum Beispiel die Verbrauchswerte der Heizung geeignet sind, Dritten tiefe Einblicke in den Lebensalltag Einzelner zu verschaffen."

Smart Home: keine reine Privatsache

Nun scheinen diese Datenrisiken nur den Privathaushalt zu betreffen, also kein Problem für den betrieblichen Datenschutz zu sein.

Dem ist aber nicht so: Durch die Nutzung privater Geräte zu betrieblichen Zwecken (BYOD = Bring Your Own Device), die private Nutzung betrieblicher Geräte und durch Telearbeit kommt es dazu, dass Firmengeräte oder betrieblich genutzte Geräte in das Smart Home eingebunden werden. Damit werden die Smart-Home-Risiken plötzlich zu Unternehmensrisiken.

Smart Home: Bald auch bei Ihnen daheim?

Wer ein Smart Home hat und darin ein Home Office betreibt, verzichtet meist darauf, für das Home Office ein eigenes, getrenntes Netzwerk zu betreiben. Stattdessen arbeiten die vernetzte Heizung des Hauses und der Drucker im Home Office im gleichen Netzwerk. Die App zur Steuerung des Smart Home läuft auf dem gleichen Smartphone wie die betrieblichen Apps. Es ist deshalb entscheidend, dass die Datensicherheit im Smart Home stimmt – für den privaten Nutzer und für das betroffene Unternehmen.

Smart Home braucht mehr Datenschutz, auch aus Unternehmenssicht

Wie eine Studie des Digitalverbands Bitkom ergab, wünschen sich die Smart-Home-Nutzer und -Interessenten mehr Sicherheit.

So sagen 92 Prozent derjenigen, die bereits Smart-Home-Anwendungen besitzen, dass ihnen unabhängige Zertifikate und Siegel zur Sicherheit vor Hacker-Angriffen sehr oder eher wichtig sind. Einen vom Hersteller garantierten Schutz vor Hacker-Angriffen finden 89 Prozent wichtig.

Auch Datenschutz spielt eine große Rolle beim Kauf. So sagen 84 Prozent, dass ihnen ein hoher Datenschutzstandard wichtig ist, ein unabhängiges Siegel dafür wäre für 79 Prozentwein wichtiges Kaufargument. Zwei Drittel (68 Prozent) achten beim Kauf außerdem darauf, dass die Smart-Home-Daten nur in Deutschland gespeichert werden.

Diese Forderungen an Smart Home werden auch den Unternehmen im Datenschutz helfen. Achten Sie deshalb auf sichere Smart-Home-Lösungen, für sich selbst und für den betrieblichen Datenschutz! &

Wie schätzen Sie die Risiken im Smart Home ein? Machen Sie den Test!

Frage: Ohne Home Office können sich Smart Home-Risiken nicht am Arbeitsplatz auswirken. Stimmt das?

a. Ja, denn das Smart Home endet an den Wänden der Wohnung oder des Hauses.
b. Nein, Angriffe auf ein Smart Home können auch den Arbeitsplatz im Unternehmen erreichen.

Lösung: Die Antwort b. ist richtig. Lässt man sich zum Beispiel Statusnachrichten aus dem Smart Home per E-Mail schicken und ruft man dann die Mail am Arbeitsplatz oder auf dem betrieblichen Smartphone ab, können die Attacken auch das Firmennetzwerk erreichen. Gleiches gilt, wenn die Smart-Home-Apps auf einem betrieblichen oder betrieblich genutzten Gerät laufen.

Frage: Für die Absicherung des Smart Home gibt es noch keine Lösung, denn ein Virenschutz für eine Heizung existiert nicht. Stimmt das?

a. Ja, oder wie sollte man eine Anti-Malware-App dort installieren?
b. Nein, es gibt durchaus Schutzlösungen für das Smart Home. Man muss sie nur einsetzen.

Lösung: Die Antwort b. ist auch hier richtig. Zum einen können und müssen die Smartphones und Tablets, die zur Steuerung des Smart Home genutzt werden, abgesichert werden, mit professionellen Security-Apps. Zum anderen gibt es Schutzlösungen, die nicht auf den Smart-Home-Geräten installiert werden müssen, sondern den Datenverkehr überwachen und Angriffe als Schutzschild abwehren können.

Ärger mit E-Mail-Verteilern

Praktikanten passiert es, erfahrenen Mitarbeitern allerdings auch: Eine größere Zahl von Adressaten soll parallel eine inhaltlich identische Mail erhalten. Der Versand erfolgt versehentlich so, dass jeder Empfänger alle anderen Adressaten sehen kann. Ein klarer Verstoß gegen den Datenschutz ! Manchmal verhängt die Datenschutzaufsicht auch ein Bußgeld gegen den „Täter". Lesen Sie, wie sich solche Pannen leicht vermeiden lassen!

Wie so oft sollte es schnell gehen. Der Kunden-Newsletter war diesen Monat sowieso schon spät dran. Also schnell einen früheren Text für die Mail an die Kunden herüberkopiert, ihn inhaltlich leicht angepasst, den Newsletter angehängt und dann hinaus damit!

Schon nach wenigen Minuten kam der erste Anruf. Ein Kunde war stocksauer und beschwerte sich: „Wie kann es sein, dass auch alle anderen Newsletter-Empfänger sehen können, dass ich den Newsletter beziehe?" Die ehrliche Antwort wäre gewesen: Die Aushilfe hat aus den drei Möglichkeiten der Adressierung leider die falsche ausgewählt und mit dem Cc-Feld gearbeitet!

Drei Varianten des Mailversands

Wenn eine Mail an viele Adressaten zugleich gehen soll, gibt es drei Varianten:

Variante 1: Alle Empfänger werden in das An-Feld eingetragen.

Variante 2: In das An-Feld schreibt man die eigene Mail-Adresse. Die eigentlichen Adressaten kommen in das Cc-Feld.

Variante 3: Wieder schreibt man in das An-Feld die eigene Mail-Adresse. Die eigentlichen Adressaten kommen in das Bcc-Feld.

Im Normalfall immer nur Bcc nehmen!

Dass Variante 1 nicht geht, war auch der Aushilfe klar. Hier sieht jeder Empfänger auch alle anderen Empfänger, das wusste sie. Allerdings meinte sie, dass Variante 2 und Variante 3 irgendwie dasselbe sind. Ein großer Irrtum! Bei Variante 2 kann jeder Empfänger die vollständigen Adressen aller anderen Empfänger im Cc-Feld sehen. Bei Variante 3 sieht ein Empfänger die Adressen der anderen Empfänger im Bcc-Feld dagegen gerade nicht!

Wie das? Des Rätsels Lösung ist einfach. Cc (also Variante 2) bedeutet „für alle sichtbare Kopie", Bcc (also Variante 3) heißt dagegen „Blindkopie, für die anderen Empfänger nicht sichtbar". Damit ist klar: Wer den Datenschutz beachtet, verwendet in solchen Fällen immer Variante 3 (Bcc) und nie Variante 2 (Cc)!

Bußgeld für Mitarbeiter persönlich

Einfach nur blöd gelaufen und mit einem „Tut mir leid!" für die Aushilfe erledigt? Leider nein. Mehrere Aufsichtsbehörden für den Datenschutz (unter anderem in Bayern) haben in solchen Fällen auch schon gegen Mitarbeiter persönlich Bußgelder von einigen 100 Euro verhängt. Die Rufschädigung für das Unternehmen kommt hinzu. Sie ist oft erheblich. &

9 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2017

ALTHAMMER & KILL

Rufschädigung in Facebook-Nachrichten

In Facebook (aber natürlich auch in anderen sozialen Netzwerken!) schreibt so mancher Nachrichten, die er als Brief nie versenden würde. Wenn die Nachricht einen geschäftlichen Bezug hat, gibt es rasch Ärger. Das ist den meisten klar. Aber wenn es um private Dinge geht? Dass es auch dann Grenzen gibt, hat das Landgericht Düsseldorf kürzlich klargestellt.

Ein Mann und eine Frau lernten sich über Facebook kennen. Rasch freundeten sie sich an. Im Mai/Juni 2016 war die Frau finanziell klamm. Gerne gab ihr der Mann ein Darlehen in Höhe von 3.050 Euro. Wie so oft hörte dann leider beim Geld die Freundschaft auf. Es gab Streitereien wegen der Rückzahlung.

© Katja Borchhardt
www.miniansichten.de

Die Frau wollte dem Mann ihre finanzielle Lage erklären. Deshalb schickte sie ihm einen Kontoauszug als Screenshot. Der Kontoauszug zeigte einen Kontostand von minus 5.865,70 Euro. Als Dispo-Rahmen waren 6.000 Euro genannt, als noch „frei verfügbar“ 134,30 Euro.

Weitergabe eines Kontoauszugs

Kaum hatte der Mann den Screenshot auf dem Bildschirm, schickte er ihn an einen Herrn T. Dabei gab er folgende Erläuterungen zum Besten: „Kontostand Deiner Teilhaberin. Die ist pleite. Bei mir hat sie auch noch 3.000 Euro Schulden. Nur zur Info. Bei uns hat es richtig geknallt.“ Wie zu erwarten leitete Herr T. die Nachricht an die Frau weiter.

Antrag auf einstweilige Verfügung beim Landgericht Düsseldorf

Den Inhalt der Nachricht fand die Frau überhaupt nicht lustig. Sie betreibt nämlich zusammen mit Herrn T. einen Friseursalon. Deshalb fürchtete sie geschäftliche Schwierigkeiten. Sofort schaltete sie daher einen Rechtsanwalt ein. Der forderte von dem Mann, der die Nachricht an Herrn T. weitergegeben hatte, zwei Dinge:

1. Hören Sie auf, Daten über den Kontostand meiner Mandantin an Dritte weiterzugeben!

2. Hören Sie auf, gegenüber Dritten zu behaupten, meine Mandantin sei pleite!

Das war dem Mann reichlich egal. Er reagierte auf das Schreiben des Anwalts schlicht nicht. Daraufhin schaltete der Anwalt das zuständige Landgericht Düsseldorf ein und beantragte eine einstweilige Verfügung.

Eine harte Entscheidung des Gerichts

Eine solche einstweilige Verfügung erließ das Landgericht tatsächlich. Der Inhalt lässt sich als „hammerhart“ bezeichnen:

– Dem Mann wird untersagt, Daten über den Kontostand weiterzugeben. Außerdem wird ihm untersagt, zu behaupten, die Frau sei pleite.

– Für den Fall, dass er gegen diese Anordnungen verstößt, droht ihm das Gericht ein Ordnungsgeld in Höhe von bis zu 250.000 Euro an.

– Alternativ kann eine Ordnungshaft von bis zu sechs Monaten verhängt werden.

„Die ist pleite" – was heißt das?

Die rechtliche Begründung des Gerichts ist für den geschäftlichen wie für den privaten Bereich gleichermaßen interessant. Das gilt vor allem für die Frage, ob man behaupten darf, dass jemand pleite sei. Dazu hält das Gericht fest:

– Eine solche Aussage ist nicht nur eine Meinungsäußerung, sondern die Behauptung einer Tatsache. Übersetzt heißt eine solche Behauptung nämlich: Der, um den es geht, ist zahlungsunfähig, finanziell ruiniert oder bankrott.

– Eine solche Behauptung schädigt den Ruf. Wer sie aufstellt, muss deshalb beweisen, dass sie wahr ist.

– Kann er dies nicht, muss er die Behauptung unterlassen.

Beweisen oder schweigen!

Daraus folgt: Bevor man behauptet, jemand sei pleite, sollte man erst einmal Unterlagen haben, die das beweisen. Die Maßstäbe sind dabei streng. Zwar befand sich das Konto der Frau, um die es hier ging, im Minus. Auch hatte sie zumindest auf diesem Konto kaum noch einen freien Kreditrahmen.

Aber all dies sagt im Zweifelsfall nichts. Denn möglicherweise hat sie noch ein anderes Konto, auf dem sie zusätzlichen Spielraum hat. Und vielleicht hat sie sogar so viel Bargeld, dass sie das Konto leicht ausgleichen könnte. All das sind Dinge, die ein Außenstehender normalerweise nicht weiß und daher nicht beurteilen kann. Deshalb lautet die Devise: Vorsicht mit solchen Behauptungen!

Datenschutz „unter Privatleuten" oder nicht?

Klargestellt hat das Gericht auch, dass sich der Mann an die Datenschutzgesetze halten muss, wenn er eine solche Nachricht in sozialen Netzwerken schreibt.

Immer wieder hört man, die Datenschutzgesetze würden für „ausschließlich persönliche Tätigkeiten" nicht gelten. Das steht so tatsächlich in § 27 Abs. 1 Bundesdatenschutzgesetz. Allerdings: Wer in einem Netzwerk eine persönliche Nachricht erhält und sie an andere Personen weitergibt, der verlässt damit den rein persönlichen Bereich.

Das gilt vor allem dann, wenn besonders vertrauliche Daten enthalten sind wie etwa Kontodaten. Ähnliches würde für medizinische Daten gelten. Wenn Nachrichten im geschäftlichen Bereich weitergegeben werden, ist das ohnehin nie eine „ausschließlich persönliche Tätigkeit".

Der Beschluss des Landgerichts ist im Internet leicht zu finden, wenn man das Aktenzeichen des Urteils 5 O 400/16 eingibt (Vorsicht: O wie „Oma", keine Null!). &

Neuer IT-Grundschutz – Was ist neu?

Der am 11. Oktober 2017 vom Bundesamt für Sicherheit in der Informationstechnik in seiner neuen Fassung vorgestellten IT-Grundschutz befasst sich jetzt verstärkt mit den Anforderungen und Bedürfnissen von kleinen und mittelständischen Unternehmen und Behörden sowie mit aktuellen Themen wie Internet-of-Things, Cloud, Virtualisierung und industriellen Kontrollsystemen.

Er gliedert sich in das IT-Grundschutz-Kompendium, die neuen BSI-Standards 200-1, 200-2 und 200-3 sowie einen „Leitfaden zur Basis-Absicherung", welcher sich speziell an kleine und mittelständische Behörden und Unternehmen richtet.

Auf diese Weise soll der neue IT-Grundschutz neben der Verschlankung und strukturellen Anpassung der Inhalte auch die Möglichkeit bieten, Themen in Zukunft schneller aktualisieren und aufbereiten zu können. Damit will das BSI sowohl den immer schneller werdenden Entwicklungszyklen in der Informationstechnik als auch Änderungen in der rechtlichen Grundlage Rechnung tragen.

Haben Sie Fragen oder benötigen Sie Unterstützung?
Wir freuen uns über Ihre Kontaktaufnahme:
info@althammer-kill.de

11 **Datenschutz** *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 5/2017

ALTHAMMER & KILL

News

Aus unserem aktuellen Newsletter:

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/

IT-Angriffe auf das Gesundheitswesen sorgen für Verunsicherung- Virusattacken abwehren
https://www.althammer-kill.de/news-detail/it-angriffe-auf-das-gesundheitswesen-sorgen-fuer-verunsicherung-virusattacken-abwehren/

Notfallplan – Wann ist Ihr Unternehmen wieder einsatzfähig?
https://www.althammer-kill.de/news-detail/notfallplan-wann-ist-ihr-unternehmen-wieder-einsatzfaehig/

DSGVO – ohne in Ruhe gereifte Geschichte überholt Sie die Zeit! (Also nichts Neues!)
https://www.althammer-kill.de/news-detail/dsgvo-ohne-in-ruhe-gereifte-geschichte-ueberholt-sie-die-zeit-also-nichts-neues-310/

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

Termine

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

07.11.2017, Hamburg
Die neue Datenschutz-Grundverordnung (DSGVO) für das Gesundheitswesen
Die Datenerhebung und -verarbeitung erfolgt in Arztpraxen, Krankenhäusern und Pflegeheimen in einem besonders sensiblen Bereich. Daraus resultiert ein besonderes Schutzbedürfnis und es gelten strenge Voraussetzungen.

07.11.2017 – 08.11.2017, Nürnberg
Messe ConSozial 2017
Wir freuen uns auf Ihren Besuch!

08.11.2017, Düsseldorf
Die neue Datenschutz-Grundverordnung (DSGVO): Änderungen, Auswirkungen, Umsetzung
Durch die Verabschiedung der neuen DSGVO ändert sich die datenschutzrechtliche Situation in Deutschland. In unserem Seminar lernen Sie den Status quo von Änderungen, Auswirkungen und Umsetzung kennen.

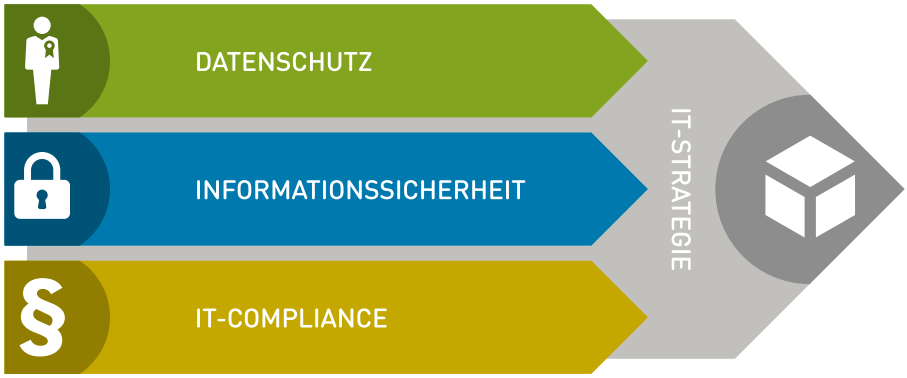
15.11.2017 – 16.11.2017, Paderborn
Vivendi Anwendertreffen 2017
Treffen Sie uns auf dem Connext Anwendersymposium in Paderborn!

27.11.2017 – 28.11.2017, Karlsruhe
Vivendi Anwendertreffen 2017
Treffen Sie uns auf dem Connext Anwendersymposium in Karlsruhe!

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). &

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

Thomas Althammer
Geschäftsführer
Tel. +49 511 330603-10
ta@althammer-kill.de

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

Mariusz Bucki
Berater für IT-Sicherheit u. Datenschutz
Tel. +49 511 330603-30
mb@althammer-kill.de

Sören Hartmann
Assistent der Geschäftsführung
Tel. +49 511 330603-36
sh@althammer-kill.de

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

Daniela Hörnicke
Beraterin für Datenschutz
Tel. +49 511 330603-38
dh@althammer-kill.de

Dr. Jan Holling
of Counsel
Tel. +49 511 330603-32
jh@althammer-kill.de

Milad Jalal
Berater für Datenschutz
Tel. +49 511 330603-42
mj@althammer-kill.de

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

Andreas Klostermann
Berater für IT-Sicherheit
Tel. +49 511 330603-0
ak@althammer-kill.de

Althammer & Kill GmbH & Co. KG

www.althammer-kill.de

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

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