Newsletter Datenschutz
Ausgabe 10 | 2017

AdOrga Solutions

Datenschutz *Now!*

Die Mitarbeiterzeitung von AdOrga Solutions

Liebe Leserin, lieber Leser,

Datenpannen stellen ein immer noch unterschätztes Problem dar. Viele wissen nicht, wie sie sich zu verhalten haben, wenn es zu einer Datenschutzverletzung kommt.

In der aktuellen Ausgabe unserer Datenschutz *Now!* erfahren Sie, was Sie wissen müssen, damit Sie bei einer Datenpanne das Unternehmen nicht ungewollt in Schwierigkeiten bringen.

Damit es erst gar nicht zu einer Datenpanne kommt, lesen Sie diesmal, wie Sie für mehr Datenschutz bei PDF-Dokumenten sorgen können, wie Sie eine Security-App finden, die wirklich für mehr Schutz sorgt, und warum ein vernetztes Zuhause auch eine Gefahr für den betrieblichen Datenschutz darstellt.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihre Regina Mühlich, Datenschutzbeauftragte

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.

PDF: ein guter Ansatz!

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

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:

Um Dokumente und ihre möglicherweise verräterischen Zusatz-Informationen zu schützen, ist mehr nötig als ein Umwandeln in PDF

- 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 (DS-GVO). Dann kann das Verschweigen einer Datenpanne alles noch viel schlimmer machen.

Der verschwundene Laptop

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. 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.

Meldepflicht des Unternehmens ...

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 DS-GVO 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.

Einer der Datenpannen-Klassiker: der vergessene Laptop in öffentlichen Verkehrsmitteln

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 DS-GVO). 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.

Impressum

Redaktion:
Regina Mühlich (V.i.S.d.P.)
Datenschutzbeauftragte

Anschrift:
AdOrga Solutions
Drachenseestr. 15
81373 München
Telefon: +49 (0)89 411 726 - 35
E-Mail: info@adorgasolutions.de

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.

Die Suche nach dem richtigen Schutz

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.

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. Betroffen 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.

Nutzerbewertungen und Downloadzahlen sind bei einer Security-App nur die halbe Miete - ob sie wirklich etwas taugt, zeigen erst seriöse Tests

AdOrga Solutions

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.

Smart Home: Bald auch bei Ihnen daheim?

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 20172022. 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 Rheinland-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.

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 Prozent ein 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.