Datenschutz *konkret*

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2018

Liebe Leserin, lieber Leser,

das Jahr 2018 neigt sich langsam dem Ende zu und wir blicken auf ein spannendes Jahr, in dem die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten ist, zurück.

Wir bedanken uns im Namen des gesamten Teams für Ihr Vertrauen und freuen uns auf die weitere Zusammenarbeit mit Ihnen. Wir wünschen Ihnen und Ihren Angehörigen eine ruhige Weihnachtszeit und alles Gute für das Jahr 2019.

Neben den Beiträgen in diesem Heft möchten wir Sie insbesondere auf das neu gegründete datenschuetzer.network hinweisen. Wir haben uns mit namhaften Partnern zusammengetan, um unseren Kunden so bestmögliche Beratung und umfassende Begleitung bieten zu können. Auf Seite 11 berichten wir von unserem ersten Netzwerkabend zum Thema Datenschutz.

Wir wünschen eine aufschlussreiche Lektüre.

Thomas Althammer & Niels Kill

Auskunftsrecht nach der DSGVO

Die DSGVO gibt Personen, deren Daten irgendwo gespeichert sind, viele Rechte. Am wichtigsten ist dabei das „Auskunftsrecht der betroffenen Person". Wer es ausüben will, muss einige Spielregeln kennen. Der interne Aufwand für Unternehmen kann auch bei korrekten Anfragen enorm sein. Die DSGVO nimmt darauf letztlich keinerlei Rücksicht. Ob ein Antragsteller mit der Antwort inhaltlich etwas anfangen kann, ist wiederum sein Problem.

Das Auskunftsrecht gilt als das wichtigste Recht, das die DSGVO gewährt. Ein wesentlicher Grund dafür: Nur wer weiß, wo Daten über ihn gespeichert sind, kann weitere Rechte geltend machen, etwa das Recht auf

In dieser Ausgabe:

die Berichtigung von falschen Daten. Genau genommen unterscheidet die DSGVO in ihrem Artikel 15 zwei Stufen des Auskunftsrechts:

Zwei Stufen des Rechts

Stufe 1:
Die betroffene Person kann Auskunft darüber verlangen, ob ein Unternehmen oder eine Behörde überhaupt über Daten verfügt, die sie betreffen. Die Antwort auf diese Frage ist im Ergebnis einfach: Ist das der Fall, lautet die Antwort „ja" (Fall der Positivauskunft). Ist das nicht der Fall, lautet die Antwort „nein" (Fall der Negativauskunft).

Stufe 2:
Falls Daten vorhanden sind, besteht ein Anspruch der betroffenen Person, diese Daten zu erhalten. Außerdem muss sie eine ganze Reihe von Informationen zu den Daten bekommen. Dazu gehört etwa die Angabe des Zwecks, zu dem die Daten verarbeitet werden.

Berechtigte Sorge der Unternehmen vor dem Aufwand

Das umfassende Auskunftsrecht ist sicher eine große Errungenschaft des Datenschutzrechts. Dennoch sind viele Unternehmen davon nicht nur begeistert. Sie haben keineswegs etwas zu verbergen, wie manche Kritiker glauben. Vielmehr fürchten sie den Aufwand, den solche Anfragen verursachen. Er ergibt sich aus mehreren Aspekten:

- Zunächst einmal muss überall im Unternehmen gesucht werden, ob Daten über die anfragende Person vorhanden sind. Hinweise darauf, wo wahrscheinlich etwas zu finden ist, erleichtern die Suche. Beispiel: Die anfragende Person gibt an, dass sie mehrfach als Zeitarbeiter im Unternehmen gearbeitet hat. Ausdrücklich verpflichtet ist sie zu solchen Angaben nicht, sinnvoll sind sie jedoch, da sie eine Antwort wesentlich beschleunigen können.

- Der Auskunftsanspruch betrifft auch Daten auf Papier. Dies kann den Aufwand bei der Suche vervielfachen. Die DSGVO nimmt auf die Besonderheiten von Daten auf Papier letztlich keine Rücksicht mehr.

- Der Auskunftsanspruch ist zeitlich nicht begrenzt. Er erstreckt sich auf alle Daten, die vorhanden sind – auch auf solche, die schon viele Jahre unangetastet im Firmenkeller liegen.

- Der Auskunftsanspruch besteht auch dann, wenn es um sehr große Datenmengen geht, etwa um mehrere tausend Seiten.

Recht auf eine kostenlose Kopie

Sind die Daten gefunden, hat die anfragende Person Anspruch auf eine kostenlose Kopie. Besonders bei umfangreichen Papierunterlagen kann dies für das Unternehmen ins Geld gehen. „Eine" Kopie ist dabei wörtlich zu nehmen. Wer eine zweite Kopie will, etwa weil er die erste Kopie verloren hat, muss dafür zahlen.

Notwendige Vernichtungsaktionen

Viele Firmen haben die DSGVO zum Anlass genommen, entbehrliche Unterlagen zu vernichten. Solche Aktionen sind bei Mitarbeitern nicht immer beliebt, aber wichtig. Wenn die gesetzlichen Aufbewahrungsfristen (beispielsweise aus dem Steuerrecht) abgelaufen sind, steht einer Vernichtung von Unterlagen nichts entgegen.

Grenzen bei Geschäftsgeheimnissen

Der Auskunftsanspruch geht zwar weit, Grenzen hat er aber trotzdem. So ist ausdrücklich festgelegt, dass „das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer Personen nicht beeinträchtigen" darf.

Dies wirkt abstrakt, hat aber sehr konkrete Auswirkungen. In den Erwägungsgründen der DSGVO ist als Beispiel genannt, dass der Auskunftsanspruch Geschäftsgeheimnisse nicht beeinträchtigen darf. Der Auskunftsanspruch darf sie also nicht aushebeln.

Kein Anspruch auf eine verständliche Auskunft

Wer Auskunft verlangt, erhält die Daten übrigens so, wie sie vorliegen. Ob er inhaltlich mit ihnen etwas anfangen kann, ist sein Problem.

Denn einen Anspruch auf Erläuterung des Inhalts von Daten sieht die DSGVO nicht vor. Dies wird vor allem im Bereich der Medizin wichtig. In der DSGVO heißt es ausdrücklich, dass sich der Auskunftsanspruch auch auf Daten in Patientenakten bezieht. Die Verständlichkeit der dort verwendeten Fachbegriffe und Kürzel ist damit in keiner Weise garantiert. Es ist Sache des Antragstellers, wie er damit klarkommt. &

Zugriff auf den Account eines Verstorbenen

Facebook ist nur ein Beispiel – die Frage an sich kann sich bei allen sozialen Netzwerken stellen: Was ist, wenn der Inhaber eines Accounts stirbt? Haben seine Erben dann einen Anspruch auf die Daten im Account? Der BGH hat dies in einem Grundsatzurteil bejaht. Er sieht darin keine Verletzung des Datenschutzes.

Der Fall bewegte die Öffentlichkeit sehr, schließlich ging es um ein erst 14-jähriges Mädchen. Sie war unter eine U-Bahn geraten, mit tödlichen Folgen. Die Eltern waren die Erben des Kindes, doch außer des Facebook-Accounts gab es kaum etwas zu erben. Aber auf den Inhalt des Accounts wollten sie unbedingt zugreifen, denn sie hofften auf Hinweise darauf, ob der Tod ihrer Tochter ein Selbstmord war.

Sture Haltung von Facebook

Facebook stellte sich freilich quer. Das Unternehmen berief sich auf seine selbst gemachten Regeln: Da irgendwer Facebook den Tod des Mädchens mitgeteilt hatte, wurde der Account in einen „Gedenkzustand" versetzt. Nur die beim Tod schon vorhandenen „Freunde" konnten die Einträge sehen und Erinnerungen hinterlassen. Von einem Zugriff durch Erben wollte Facebook nichts wissen.

Der BGH gewährt den Zugriff

Um ihr Ziel zu erreichen, mussten die Eltern durch drei Instanzen klagen. Beim Bundesgerichtshof (BGH) bekamen sie schließlich auf der ganzen Linie Recht. Er verurteilte Facebook dazu, den Eltern als Erben Zugriff auf die Daten im Account zu geben.

Erbrecht als Ausgangspunkt

Die Hauptargumente des BGH zum Erbrecht lauten so:

- Bei einem Erbfall geht das gesamte Vermögen des Verstorbenen auf die Erben über. Zum Vermögen in diesem Sinn gehören auch Vertragsbeziehungen. Die Eltern haben also gewissermaßen den Vertrag ihrer Tochter mit Facebook geerbt. Damit haben sie das Recht, auf den

Inhalt des Accounts zuzugreifen. Im Ergebnis ist das nichts anderes, als wenn sie ein Tagebuch oder Briefe geerbt hätten, die ihrer Tochter gehörten.

– Facebook darf diese Rechtslage nicht dadurch unterlaufen, dass es einen „Gedenkzustand" erfindet und den Zugriff blockiert. Denn im Vertrag zur Nutzung von Facebook steht davon nichts.

Datenschutz kein Hindernis

Kein Problem sieht der BGH im Datenschutz. Dabei unterscheidet er folgendermaßen:

– Für das verstorbene Mädchen gelten die Datenschutz-Regelungen nicht mehr. Die Datenschutz-Grundverordnung (DSGVO) bezieht sich ausdrücklich nur auf lebende Personen, auf Daten Verstorbener ist sie nicht anzuwenden.

– Die Kommunikationspartner des Mädchens, die Einträge auf Facebook hinterlassen haben, können sich prinzipiell auf die DSGVO berufen. Zu Lebzeiten des Mädchens war die Verarbeitung dieser Daten jedoch erforderlich, weil die Kommunikation über den Account sonst nicht funktioniert hätte. Damit war die Verarbeitung berechtigt, auch der Tod des Mädchens ändert daran nichts, die Verarbeitung der Daten durch Facebook bleibt weiterhin rechtmäßig. Die Erben des Mädchens nehmen nur die Möglichkeit zum Datenabruf wahr, die das Mädchen zu Lebzeiten selbst hatte.

Noch zwei kurze Hinweise

Wichtig ist bei diesen Überlegungen, dass sie generell für alle Erben gelten. Keine Rolle spielt, dass die Erben des Mädchens zugleich ihre Eltern waren und das Sorgerecht besaßen.

Mit dem Aktenzeichen III ZR 183/17 ist das Urteil im Internet leicht zu finden. &

Die DSGVO und die Löschung von Daten

Daten löschen? Das machen wir jeden Tag! Irgendwelche Probleme dabei? Nein, wieso? So laufen typische Dialoge ab, wenn man dieses Thema in Unternehmen anspricht. Aber ganz so einfach war es schon bisher nicht, und die Datenschutz-Grundverordnung (DSGVO) bringt außerdem noch einige Neuerungen.

Was bedeutet es eigentlich, Daten zu löschen? Das Verschieben der Daten in einen elektronischen Papierkorb reicht jedenfalls nicht aus. Das dürfte jedem klar sein. Oder vielleicht doch nicht?

Löschen als Zerstörung

Nur zur Sicherheit: Wenn Sie Daten mit ein paar Mausklicks „wiederherstellen" können, sind sie nicht wirklich gelöscht. Sie sind dann nur an einer anderen Stelle als bisher gespeichert, eben im „Papierkorb".

Aber was heißt Löschen dann? Der Europäische Gerichtshof verwendet klare Worte, um den Begriff „Löschen" verständlich zu erklären. Daten sind dann gelöscht, wenn sie „zerstört" sind. Die Daten dürfen also auf keinem Weg mehr rekonstruierbar/wiederherstellbar sein.

Daten auf Papier

Bei Daten auf Papier bedeutet dies beispielsweise, das Papier zu verbrennen. Zerkleinern kann man es natürlich auch. Aber das muss so geschehen, dass niemand mehr die Seiten wieder zusammensetzen kann. Unterschiede danach, wie schutzwürdig die Daten sind, macht das Recht dabei nicht. Für alle personenbezogenen Daten gelten bei einer Löschung vielmehr dieselben Regeln. Dies ist für viele noch ungewohnt und kann auch recht teuer werden. Aber so ist es eben.

Elektronische Daten

Elektronische Daten lassen sich auf den ersten Blick recht schnell

löschen. Eine Möglichkeit ist das Überschreiben, jedoch steckt der Teufel hier im Detail. Viele Löschfunktionen bewirken lediglich, dass die entsprechenden Bereiche auf dem Datenträger (etwa einer Festplatte) nicht mehr gegen ein Überschreiben geschützt sind. Das heißt allerdings noch lange nicht, dass sie auch tatsächlich bald überschrieben werden. Manchmal geschieht dies auch nie.

Wundern Sie sich also nicht, wenn die EDV erklärt, dass das Löschen von Daten nicht so banal ist, wie viele denken.

Gesetzliche Anlässe zur Löschung

Wann Daten gelöscht werden müssen, ist in Art. 17 DSGVO ausführlich geregelt. Zumindest die wichtigsten Fälle der Löschungspflicht sollte man kennen:

Rechtswidrige Verarbeitung

Wenn Daten unrechtmäßig verarbeitet wurden, müssen sie ohne Ausnahme gelöscht werden. Ein klassisches Beispiel: Um bestimmte Daten überhaupt verarbeiten zu dürfen, hat ein Unternehmen die Einwilligung der betroffenen Personen eingeholt.

Leider stellt sich heraus, dass dabei rechtliche Fehler passiert sind und dass die Einwilligung unwirksam ist. Die Folge: Die betroffenen Daten sind zu löschen!

Widerruf einer Einwilligung

Ein nicht ganz so klassisches Beispiel: Jemand hat eine Einwilligung erteilt und widerruft sie. Welche Folgen hat das? Der Ausgangspunkt ist klar: Alles, was bis zum Widerruf mit den Daten geschehen ist, bleibt rechtmäßig. So regelt es Art. 7 Abs. 3 Satz 2 DSGVO.

Folgen eines Widerrufs

Aber wie sieht es ab dem Widerruf aus? Müssen die Daten jetzt gelöscht werden? Nicht so ohne Weiteres! Denn vor allem im geschäftlichen Bereich kann es nötig sein, die Daten noch länger vorrätig zu halten. Das gilt in erster Linie dann, wenn Buchführungspflichten oder steuerliche Pflichten das Unternehmen dazu zwingen.

Das sind dann rechtliche Verpflichtungen, gegen die das Unternehmen nichts machen kann. Die Folge: Weil es um die Erfüllung einer rechtlichen Verpflichtung geht (in diesem Fall gegenüber dem Staat), dürfen die Daten noch gespeichert werden, solange diese Pflicht besteht (Art. 17 Abs. 3 Buchst. b DSGVO). Der Widerruf der Einwilligung ändert daran nichts.

Immer beachten: Zweckbindung

Doch Vorsicht: Die Speicherung ist nur genau für die Pflicht erlaubt, die erfüllt werden muss. Unzulässig wäre es beispielsweise, die Daten noch zu verwenden, um dem Kunden Werbematerial zuzuschicken. Die Verwendung für diesen Zweck muss ausgeschlossen werden. Die DSGVO spricht hier von einer „Einschränkung der Verarbeitung“ (so die Überschrift von Art. 18 DSGVO). Früher bezeichnete man dies meist als „Sperrung“.

Vorsicht vor Bußgeldern!

Solche und ähnliche Fälle zeigen, dass eine Löschung nicht nur technisch schwierig sein kann, sondern auch in rechtlicher Hinsicht ganz erhebliche Fragen aufwirft. Man sollte sie in jedem Fall ernst nehmen, denn zumindest wenn grobe Fehler passieren, kann dies durchaus zu einem Bußgeld seitens der Datenschutzaufsicht führen. &

Datenschutz in Fahrzeugen: Nicht nur an neue Firmenwagen denken

Vernetzte Fahrzeuge sind weder Zukunftsmusik, noch sind die Datenrisiken auf kostspielige Neuwagen beschränkt. Jedes Fahrzeug, privat oder geschäftlich, kann zu einem Connected Car werden. Machen Sie sich mit den Folgen vertraut!

Wer in diesen Tagen eine Automobilmesse besucht, trifft dort häufig auf Facebook und Google. Und wer die Hallen einer IT-Messe betritt, sieht eine große Zahl an Fahrzeugen an den Messeständen. Vernetzte Fahrzeuge, auch Connected Cars genannt, gehören zu den Top-Trends. Doch nicht nur die Industriebranchen haben großes Interesse, auch die Nutzer sind aufgeschlossen, wie Umfragen zeigen.

Digitalisierung der Fahrzeugbranche

Ob optimale Routenplanung und Navigation oder der Einsatz von autonomen Fahrzeugen auf der Straße: Die Mehrheit der Bundesbürger wünscht sich laut Digitalverband Bitkom den Einsatz von Künstlicher Intelligenz (KI), um den Verkehrsfluss zu optimieren und Unfälle zu vermeiden. So halten es 58 Prozent für sinnvoll, mithilfe von KI selbstfahrende Fahrzeuge auf die Straße zu bringen.

Rund 9 von 10 Unternehmen der Automobilbranche (86 Prozent) fordern eine gesetzliche Verpflichtung, anonymisierte Fahrzeugdaten bereitzustellen. Dabei sagt jedes vierte Unternehmen (25 Prozent), es sollten alle Daten zur Verfügung gestellt werden müssen, 61 Prozent plädieren für ausgewählte Daten.

In vernetzten Autos entsteht eine Vielzahl von Daten, etwa zur Motorleistung, zum Fahrverhalten oder auch zur Position des Fahrzeugs. Der großen Mehrheit der Bürger ist es wichtig zu wissen, welche Daten erzeugt werden (83 Prozent) und wer sie nutzt (93 Prozent), so der Bitkom-Verband. Dabei fordern die meisten, dass der Eigentümer des Fahrzeugs (69 Prozent) bzw. der Fahrer (57 Prozent) entscheiden soll, wer die Daten nutzen darf. 28 Prozent wollen diese Entscheidung dem Gesetzgeber überlassen, nur zwei Prozent dem Automobilhersteller.

Fahrzeugdaten sind Thema für den Datenschutz

Die Aufsichtsbehörden für den Datenschutz haben bereits mehrfach auf die Datenrisiken durch die Fahrzeugvernetzung hingewiesen: In modernen Fahrzeugen sammeln bereits heute unzählige Sensoren Daten zum Fahrverhalten und den zurückgelegten Wegen, so die Aufsichtsbehörden. Daraus lassen sich detaillierte Persönlichkeitsprofile erstellen. Fahrerinnen und Fahrer müssen daher jederzeit die volle Hoheit über die Verwendung personalisierbarer Fahrzeugdaten haben. Grundsätzlich sollten sie über jede Datenverwendung (im Sinne einer vollständigen Transparenz) unterrichtet werden. Damit dies möglich ist, sind datenschutzgerechte Technologien und Voreinstellungen notwendig.

Achtung: Nicht nur moderne Fahrzeuge betroffen

Das Thema „Vernetzte Fahrzeuge“ ist inzwischen nicht mehr auf moderne Firmenwagen beschränkt, auch wenn auf den Messen immer die neusten Modelle an den Ständen stehen.

Vorhandene Entertainment-Systeme im Auto, Freisprechanlagen und Navigationssysteme lassen sich leicht um neue Funktionen ergänzen, durch Upgrades, durch die Verknüpfung via Bluetooth oder USB-Stecker mit dem Smartphone des Fahrers oder der Fahrerin, aber auch durch neue Lösungen, die einfach in den Zigarettenanzünder im Altfahrzeug gesteckt werden und dann einen digitalen Assistenten wie Siri, Alexa oder Google Assistant an Bord holen.

Wenn Sie also in einen älteren Firmenwagen einsteigen, kann auch dies ein vernetztes Fahrzeug sein. Die Digitalisierung macht vor älteren Fahrzeugen nicht zwingend halt. Fragen Sie deshalb, was das Fahrzeug alles kann, das Sie nutzen wollen und seien Sie kritisch bei neuen Geräten, die Sie in dem Fahrzeug anbringen wollen! &

Wie lassen sich neue Anwendungen datenschutzgerecht testen?

Ständig kommen neue Cloud-Dienste auf den Markt. Doch leisten sie, was sie versprechen? Wenn Sie dies testen wollen, denken Sie auch an den Datenschutz, bevor Sie zum Beispiel Kundendaten testweise in eine Cloud übertragen.

Im Jahr 2017 nutzten zwei Drittel aller Unternehmen (66 Prozent) Rechenleistungen aus der Cloud, so eine Umfrage des Digitalverbands Bitkom. Wer Cloud-Anwendungen nutzt oder damit plant, für den ist Datenschutz das Top-Kriterium, wenn es um die Auswahl eines Cloud-Dienstleisters geht.

Dabei gaben praktisch alle Unternehmen (97 Prozent) an, dass für sie die Konformität mit der Datenschutz-Grundverordnung (DSGVO) auch bei Cloud-Lösungen unverzichtbar ist.

In der Vergangenheit beklagten jedoch viele Unternehmen Ausfälle der Cloud-Lösungen. Insgesamt konnten sieben von zehn Cloud-Anwendern (69 Prozent) kurzzeitig nicht auf ihre Cloud-Dienste zugreifen. Dafür gibt es verschiedene Ursachen: Am häufigsten waren technische Probleme aufseiten des Cloud-Providers (46 Prozent) dafür verantwortlich.

Es ist deshalb auch aus Datenschutzsicht mehr als sinnvoll, nicht nur auf dem Papier zu prüfen, ob ein Cloud-Dienst sicher und zuverlässig ist.

Erst testen, dann nutzen

Es sollte selbstverständlich sein, einen neuen Cloud-Dienst ausgiebig zu testen, um zu sehen, ob er die fachlichen und technischen Anforderungen erfüllt. Auch die Datenschutzfunktionen einer Cloud-Lö-

sung gehören auf den Prüfstand, bevor der Dienst zum Einsatz kommt.

Selbst wenn es Gütesiegel sowie Datenschutz- und IT-Sicherheitszertifikate gibt, bleibt insbesondere die Frage, ob die fachlichen Anforderungen des Nutzers, der Abteilung oder allgemein des Unternehmens erfüllt werden können. Um das zu überprüfen, sind in der Regel Testdaten erforderlich. Die Aufsichtsbehörden für den Datenschutz weisen bereits seit vielen Jahren darauf hin, dass der Testfall für den Datenschutz bereits der Ernstfall ist.

Achtung: Ein Test ist bereits der Ernstfall

Deshalb kommt es auf die richtige Vorbereitung der Testdaten an. Ein denkbarer Schutz für die Testdaten mit Personenbezug wäre die Verschlüsselung. Doch vielfach werden die Daten nicht verschlüsselt, weil die zu testende Cloud-Lösung nicht mit den verschlüsselten Daten umgehen kann.

Deshalb sind Verschlüsselungslösungen sinnvoll und hilfreich, die aus den Echtdaten sogenannte Tokens erzeugen. Bei der Tokenisierung werden die zu schützenden, vertraulichen Daten durch Daten desselben Typs, also passender Art und Länge ersetzt. Die neuen Werte (Tokens) weisen aber keinen echten Personenbezug mehr auf.

Datenschutzniveau muss stimmen

Dadurch simulieren die entsprechend veränderten Daten die Nutzung echter Daten, ohne jedoch den Datenschutz zu gefährden. Fachliche Tests der Funktionen einer Cloud-Lösung werden so möglich, ohne personenbezogene Daten zum Test in eine Cloud zu übertragen.

Nicht nur bei Cloud-Diensten, die jenseits der EU betrieben werden, könnte dies sonst zum Datenschutzproblem werden, sondern generell muss sichergestellt sein, dass das Datenschutzniveau der Cloud-Lösung den Vorgaben der DSGVO entspricht.

Wichtig ist es dabei, nicht einfach eine Lösung dafür zu nutzen, die der Anbieter, den man testen möchte, bereitstellt. Oftmals lässt sich dann nicht ausschließen, dass Mitarbeiter des Anbieters die Testdaten unerlaubt wieder zugänglich machen könnten. Die Verschlüsselung und die Tokenisierung sollten immer in der Hoheit des Nutzers liegen, die Schlüssel sollten also beim Anwender vorgehalten werden, auch schon im Testfall. &

Denken Sie beim Test an den Datenschutz?

Frage: Wird eine Cloud-Lösung lediglich getestet, muss es kein Datenschutzkonzept dafür geben. Stimmt das?

a. Nein, nicht nur im Produktivfall muss der Datenschutz stimmen, auch bereits im Testfall.
b. Ja, denn beim Testen werden ja nur Testdaten genutzt.

Lösung: Die Antwort a. ist richtig. Bereits im Testfall muss der Datenschutz beachtet werden. Zudem nutzen viele Unternehmen als Testdaten ihre echten Produktivdaten. Denn der Test soll ja realistisch sein, so denken sie. In Wirklichkeit vergessen sie dabei den Datenschutz, wenn sie die Testdaten nicht richtig aufbereiten.

Frage: Testdaten ohne Personenbezug sind unrealistisch und machen Tests wertlos. Stimmt das?

a. Ja, denn eine Lösung zur Kundendatenverwaltung muss mit Kundendaten getestet werden.
b. Nein. Sind die Testdaten richtig aufbereitet und von ihrem Personenbezug befreit, bleiben sie fachlich korrekte Daten für den Test.

Lösung: Hier ist die Antwort b. richtig. Mit dem richtigen Verfahren behalten die Testdaten die Struktur und Länge, die sie fachlich brauchen. Ein solches Verfahren ist die sogenannte Tokenisierung. Wie oben erläutert, werden bei der Tokenisierung die zu schützenden vertraulichen Daten durch Daten desselben Typs, also passender Art und Länge, ersetzt. Die neuen Werte (Tokens) weisen aber keinen echten Personenbezug mehr auf. Der Datenschutz lässt sich so auch im Testfall wahren und verhindert keinen Test.

9

Datenschutz *konkret* –
Das Kundenmagazin von Althammer & Kill
Ausgabe 4/2018

ALTHAMMER & KILL

Einmal-Passwörter per SMS: Sind sie wirklich sicher?

Ein Passwort allein reicht als Schutz vor unberechtigtem Zugang zu IT-Systemen oftmals nicht aus. Deshalb nutzen viele Online-Dienste zusätzlich Einmal-Passwörter, die sie per SMS an den Nutzer schicken und die als zweiter Sicherheitsfaktor dienen. Doch wie sicher ist das?

Stellen Sie sich vor, ein Freund teilt Ihnen mit, dass er eine Spam-Mail von Ihnen bekommen hat. Entweder jemand benutzt Ihren Namen für Spam, oder Ihr Web-Mail-Konto wurde missbraucht.

Sie versuchen, sich bei Ihrem Web-Mail-Zugang anzumelden, doch Ihr Passwort wird nicht mehr akzeptiert. Der Grund: Ihr Mail-Provider hat den Spam-Versand von Ihrem Web-Mail-Konto festgestellt und Ihr Konto deshalb sicherheitshalber deaktiviert.

Zugangsdaten werden gestohlen oder geknackt

Wie konnte das geschehen? Offensichtlich hatte ein Spammer Ihr Mail-Passwort. Entweder es war ungeschützt gespeichert, Sie haben es eingegeben während Ihre Tastatureingaben mitgeschnitten wurden oder aber Ihr Passwort war so einfach, dass ein Angreifer es schlicht erraten und geknackt hat.

Um das zu vermeiden, setzen immer mehr Online-Dienste neuerdings auf eine sogenannte Zwei-Faktor-Authentifizierung.

Zusätzliche Sicherheitsfaktoren sollen davor schützen

Dabei reicht ein Passwort zur Anmeldung nicht aus. Es gibt einen zweiten Sicherheitsfaktor, der ebenfalls für die Anmeldung benötigt wird. Meist ist dies ein sogenanntes Einmal-Passwort, ein für Sie generiertes zweites Passwort, das nur ein einziges Mal gilt.

Dieses Einmal-Passwort wird an den Nutzer meistens per SMS geschickt. Im Online-Banking wird dabei aus Sicherheitsgründen gefordert, dass das Smartphone, mit dem das Banking gemacht wird, nicht das gleiche Gerät sein darf, an welches das Einmal-Passwort per SMS gesendet wird. Doch wie sicher sind Einmal-Passwörter per SMS überhaupt?

Ungeschützte SMS sind ein Risiko

In der Regel liegen Nachrichten, die per SMS eingetroffen sind, unverschlüsselt auf dem Smartphone oder Handy. Eine Verschlüsselung findet man nur dann, wenn man die Nachrichten-App oder die SMS-App in einem geschützten Bereich auf dem Smartphone betreibt. Zudem muss man sich klarmachen, dass viele Apps bei ihrer Installation oder im Rahmen eines App-Updates die Berechtigung verlangen, SMS zu lesen.

Nicht jede App, die auf SMS zugreifen will, braucht diese Berechtigung, im Gegenteil. Zudem gibt es bösartige Apps, die die SMS auslesen und den Inhalt missbrauchen könnten, zum Beispiel um einen starken Zugangsschutz zu umgehen, bestehend aus Nutzer-Passwort und Einmal-Passwort, das per SMS eingetroffen ist.

Angriffe auf starken Zugangsschutz waren bereits erfolgreich

Berichte über Vorfälle in dieser Art (etwa der sogenannte Reddit-Hack) zeigen, dass man nicht ohne Weiteres annehmen kann, dass die SMS, mit der das Einmal-Passwort geschickt wird, sich nicht ausspähen lässt. Außer des Nutzer-Passworts könnte also auch das Einmal-Passwort, das per SMS kommt, in unbefugte Hände geraten.

Was ist genau beim Reddit-Hack passiert? Darüber hat zum Beispiel der IT-Sicherheitsanbieter 8com berichtet. Das Unternehmen Reddit setzt für seine Mitarbeiter auf eine Zwei-Faktor-Authentifizierung.

Trotzdem konnten Mitte Juni Hacker in die Datenbanken von Reddit eindringen und Nutzerdaten erbeuten. Um sich Zugang zu den internen Netzwerken zu verschaffen, mussten die Kriminellen sowohl das Passwort als auch das Einmal-Passwort in der SMS des jeweiligen Mitarbeiters eingeben. Die SMS erhielten sie, indem sie sich eine Kopie der SIM-Karte des Mitarbeiters mit derselben Nummer beschafften. So konnten sie die SMS abfangen.

An eine Kopie einer SIM-Karte zu gelangen, ist nicht so kompliziert, wie man denkt, berichtet 8com. Manchmal reicht schon ein Anruf beim Anbieter, dass die SIM-Karte kaputt sei und man eine neue brauche. Zwar muss man sich dann legitimieren, aber viele Menschen geben die dafür relevanten Informationen wie den Geburtstag ganz öffentlich im Internet preis.

Trotzdem: Zwei-Faktor-Authentifizierung bleibt wichtig

Bedeuten Vorfälle wie der Reddit-Hack, dass ein starker Zugangsschutz gar nicht stark ist? Sicherheitsexperten sagen, dass es in jedem Fall besser ist, ein Einmal-Passwort zusätzlich einzusetzen, als nur ein einzelnes Passwort. Doch man sollte lieber zu anderen Methoden übergehen, um Einmal-Passwörter zu erzeugen, etwa zu Security-Token.

Security-Token sind spezielle Geräte, um Einmal-Passwörter zu erzeugen. Sie haben im Vergleich zu Smartphones einige Vorteile. Unter anderem installiert der Nutzer auf Security-Tokens keine fremden Apps, die die Erlaubnis bekommen, SMS-Nachrichten zu lesen, und dies missbrauchen könnten. Zudem brauchen Security-Token keine SIM-Karten, die Datendiebe „nachbestellen“ könnten. &

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.

Gestaltung: Ralf Winternheimer
www.winternheimer.net

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

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

Schutzgebühr Print-Ausgabe: 10,– €

DATCON ALTHAMMER & KILL HEIDRICH RECHTSANWÄLTE praemandatum

Das datenschuetzer.network

Das datenschuetzer.network versteht sich als ein Zusammenschluss von Datenschutzspezialisten, die sich dem gemeinsamen Ziel verschrieben haben, Ihre Expertise zum Vorteil Ihrer Kunden zu bündeln.

Das Thema Datenschutz ist aufgrund der gesetzlichen Neuerungen im Umbruch. In den nächsten Jahren ist mit einer Vielzahl von Verfahren und Urteilen zu rechnen, die sich deutlich auf die praktische Umsetzung der rechtlichen Anforderungen auswirken werden.

Unser Ziel: Die bestmögliche Beratung

Um diesen Veränderungen optimal begegnen zu können, haben wir uns in einem fachlichen Netzwerk mit anderen Experten zusammengeschlossen, um unseren Kunden so bestmögliche Beratung und umfassende Begleitung bieten zu können.

Unsere Partner im Netzwerk

Neben Althammer & Kill zählen zu diesem Netzwerk namhafte weitere Partner, wie praemandatum, DatCon und die Kanzlei Heidrich Rechtsanwälte. Die Erfahrung dieser Unternehmen in den Bereichen Datenschutz und Informationssicherheit reicht bis in die 1990er Jahre zurück. Das Netzwerk bündelt so die Kompetenz von mehr als 50 Mitarbeitenden mit unterschiedlichen fachlichen Schwerpunkten.

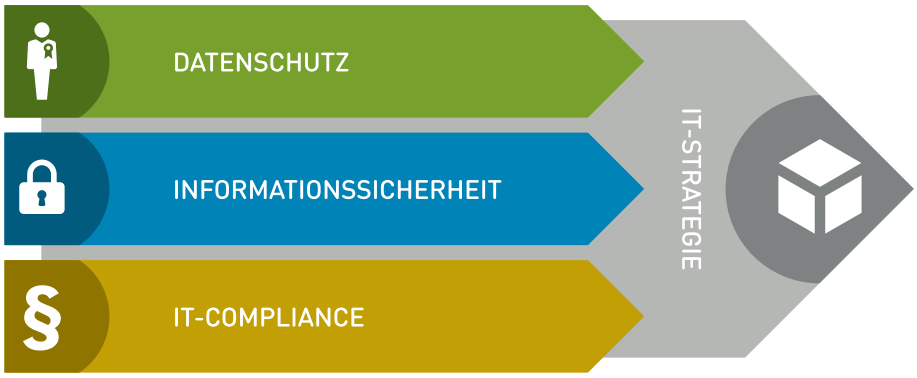
Zum Auftakt: Netzwerkabend Datenschutz

Am 15. November fand in der Venture-Villa in Hannover der erste gemeinsame Netzwerkabend mit anschließendem Experten-Talk statt. Die rege Beteiligung der zahlreichen Teilnehmer am Talk machte einmal mehr deutlich, dass es zum Thema DSGVO noch viel Gesprächsbedarf gibt. Weitere Veranstaltungen sind in Planung. &

Mehr Informationen:
datenschuetzer.network

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.



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).

Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für 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 die 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 Sie bei der Auswahl und Gestaltung passender Strategien.

Althammer & Kill GmbH & Co. KG

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

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

Standort Mannheim:
Kaiserring 10–16 · 68161 Mannheim
Tel. +49 621 121847-0

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

Mitglied im:

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