Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 2/2016

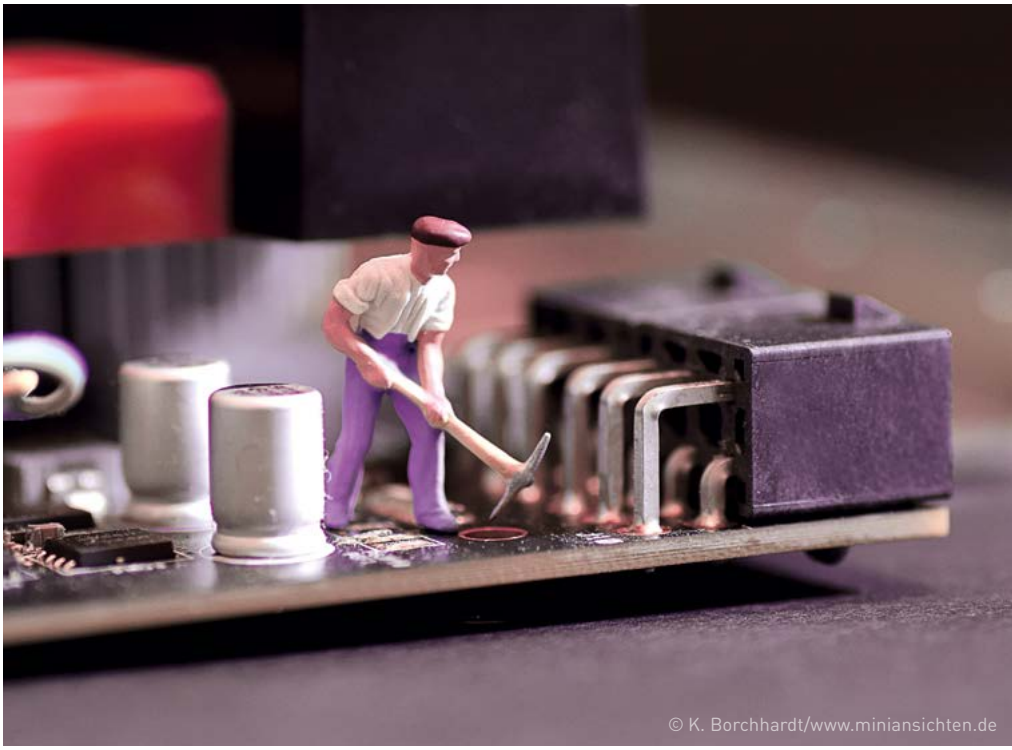
In dieser Ausgabe:

Liebe Leserin, lieber Leser,

während der Datenschutz EU-weit ab 2018 nun neu geregelt wird, zeigt sich, wie verwundbar unsere IT-Systeme aktuell sind: Trojaner Locky & Co. erpressen mit verschlüsselten Daten Geld rund um den Globus.

Eine spannende Lektüre wünschen

Thomas Althammer & Niels Kill



© K. Borchhardt/www.miniansichten.de

Erben dürfen auf Facebook-Konto zugreifen

Was wird aus einem Facebook-Account, wenn sein Inhaber stirbt? Können die Erben Zugriff auf die Inhalte verlangen? Das Landgericht Berlin beantwortet diese Frage mit Ja. Das Persönlichkeitsrecht des Verstorbenen stehe dem nicht entgegen.

Sie gehören inzwischen zu unserem Alltag: „Digitale Nachlässe". Junge wie alte Menschen hinterlassen zwar kaum noch Briefe, dafür aber immer öfter einen Facebook-Account. So war es auch bei einem tragischen Fall in Berlin. Ein 14-jähriges Mädchen hatte mit Zustimmung seiner Eltern einen Facebook-Account eingerichtet. Die Zugangsdaten hatte es seinen Eltern überlassen. Ein Jahr später verstarb das Mädchen unter unklaren Umständen. Ein Selbstmord liegt im Bereich des Möglichen.

Facebook verweigert Erben den Zugriff

Die Eltern wollten auf den Inhalt des Accounts zugreifen. Facebook verweigerte ihnen das jedoch. Stattdessen fror Facebook den Inhalt des

Accounts gewissermaßen ein. In diesem „Gedenkzustand" ist der Inhalt zwar noch vorhanden, und „Facebook-Freunde" können auf ihn weiterhin zugreifen. Sie können sogar neue Kommentare einfügen. Ein Zugriff auf den Account durch Eingabe der (an sich korrekten) Zugangsdaten ist aber nicht mehr möglich. Wenn dies versucht wird, erscheint lediglich ein Hinweis auf den Gedenkzustand des Accounts. Hierdurch will Facebook die Persönlichkeitsrechte des verstorbenen Account-Inhabers schützen.

Landgericht Berlin gewährt den Zugriff

Die Eltern ließen sich das nicht gefallen. Als rechtmäßige Erben forderten sie Facebook auf, ihnen Zugang zum Account zu gewähren. Das Landgericht Berlin gab den Eltern Recht. Zur Begründung weist das Gericht darauf hin, dass das Recht auf Zugang zu dem Account schlicht und einfach ein Teil des Erbes ist, den das Mädchen hinterlassen hat. Aufgrund seines Vertrags mit Facebook habe das Mädchen das Recht gehabt, auf die Server von Facebook zuzugreifen, soweit es seinen eigenen Account betrifft. Dieses Recht sei auf die Eltern als Erben übergegangen. Deshalb dürften nunmehr sie durch Eingabe der Zugangsdaten auf den Account zugreifen.

Unentgeltlich heißt nicht rechtlos

Von dem Hinweis, dass das Mädchen für die Nutzung des Accounts nichts zahlen musste, lässt sich das Gericht nicht beeindrucken. Dies ändere nämlich nichts daran, dass eine vertragliche Vereinbarung vorliege, aus der sich Rechte für den Account-Inhaber ergeben. Und diese vertraglichen Rechte könnten vererbt werden. Dass sie keinen materiellen Wert haben, sondern allenfalls einen ideellen Wert, ändere daran nichts.

Generell anwendbare Grundsätze zu sozialen Netzwerken

Die Entscheidung des Landgerichts Berlin vom 17.12.2015 (Aktenzeichen 20 O 172/15) ist die erste Entscheidung eines deutschen Gerichts zu diesem Thema. Sie betraf direkt zwar nur Facebook, ist aber auf Accounts bei anderen sozialen Netzwerken übertragbar. &

Umzugshelfer für Daten gesucht!

Wenn der Kunde es möchte, sollen seine Daten in Zukunft vom alten Anbieter auf den neuen übertragen werden können. So will es die Europäische Union. Bei solch einem Datenumzug ist jeder im Unternehmen gefordert – auch Sie.

Das neue Datenschutzrecht der EU, die EU-Datenschutz-Grundverordnung (EU-DSGVO), kommt – nicht sofort, aber dafür sicher. Bereits jetzt wirft die Grundverordnung ihre Schatten voraus. Denn die Unternehmen müssen sich darauf vorbereiten.

Eine der neuen Vorgaben ist das sogenannte Recht auf Datenübertragbarkeit: Personenbezogene Daten sollen einfacher von einem Anbieter auf einen anderen übertragen werden können.

Dieses neue Recht soll den Wettbewerb unter den Anbietern fördern. Denn bisher können Kunden nicht so einfach den Anbieter wechseln, die gespeicherten Daten lassen sich nur sehr mühsam umziehen. Gleichzeitig sollen Kunden mehr Kontrolle über ihre Daten bekommen und verlangen können, die eigenen Daten an einen neuen Anbieter zu übertragen.

Damit dieses neue Recht nicht nur den Wettbewerb, sondern auch den Datenschutz voranbringt, gibt es noch viel zu tun. Jeder, der selbst schon umgezogen ist, kann bestätigen, dass ein Umzug kein einfaches Unterfangen ist.

Umzüge sind immer eine Herausforderung

Man muss sehr viel vorbereiten und organisieren, und man sollte möglichst nichts vergessen. Wenn Daten von einem anderen Anbieter in die IT Ihres Unternehmens übernommen werden sollen, weil Ihr Unternehmen

einen neuen Kunden gewonnen hat, dürfen genauso wenig Fehler passieren wie in dem Fall, dass Ihr Unternehmen einen Kunden verliert und die Daten an den neuen Anbieter abgeben soll.

Gerade bei der Herausgabe, also dem Export von Daten, muss klar sein, welche Daten genau betroffen sind und übertragen werden sollen. Es darf nicht passieren, dass Daten unbeteiligter Dritter übermittelt werden.

Nun klingt der Umzug von Daten, der allein schon durch das neue EU-Datenschutzrecht in Zukunft öfter anstehen könnte, wie ein rein technisches Thema, das die IT schon lösen wird. Doch tatsächlich sind auch die Fachbereiche und die einzelnen Nutzer im Unternehmen gefragt.

© K. Borchhardt/www.miniansichten.de

Datenumzug braucht besonderen Datenschutz

Jeder, der mit den Daten des bisherigen oder neuen Kunden umgeht, muss sich bewusst sein, dass eine Datenübertragung ein Risiko darstellt. Die Schnittstellen und Module, die für den Umzug genutzt werden, können fehlerhaft sein. Die Daten können unterschiedlich strukturiert sein, wenn man das alte System mit dem neuen vergleicht. Technisch würde man sagen, dass die Datenformate nicht richtig passen.

Doch auch bei der inhaltlichen Zuordnung können Fehler auftreten: Vielleicht wurde eine Adresse in ein Kommentarfeld geschrieben, weil der Straßenname für das richtige Feld zu lang war. Oder das neue System interpretiert die alten Daten falsch. Solche inhaltlichen Fehler kann die IT nicht allein erkennen, hier sind die fachlichen Experten gefragt.

Umzüge brauchen klare Regeln

Es sollte auch nicht passieren, dass echte Kundendaten für eine Testübermittlung bereitgestellt werden. Hier sollten anonymisierte nur anonymisierte Daten herausgegeben und genutzt werden, keine echten Kundendaten.

- Es muss geklärt sein, wer welche Daten erhalten darf. Also keine Datenübertragung auf Zuruf!
- Bevor die Daten nach der Übertragung im alten System gelöscht werden, muss klar sein, ob noch Aufbewahrungspflichten bestehen.

Die Umzugs-Checkliste für Daten

- Jeder Umzug ist eine Herausforderung, auch bei Daten.
- Module, Schnittstellen und Formate, die beim Umzug zum Einsatz kommen, können fehlerhaft sein.
- Die Zuordnung der alten Datenstruktur zur neuen Struktur muss nicht nur technisch, sondern auch fachlich geprüft werden.
- Um Umzüge zu erleichtern, sollten Datenfelder immer nur so genutzt werden, wie es die Dokumentation beschreibt, Umfunktionieren kann dazu führen, dass die falschen Daten übertragen oder dass die richtigen Daten falsch interpretiert werden.
- Verlangt der neue Anbieter Testdaten für die Umzugsprobe, dürfen

Daten ohne echten Kundenbezug, also Demo-Daten, zum Einsatz kommen. Zudem sollten Kundendaten nicht ohne ausdrückliche interne Freigabe übermittelt werden, zum Beispiel weil ein (angeblicher) Kunde anruft und sagt, er wechsle zu einem anderen Anbieter und brauche seine Daten nun dort.

Zum einen muss klar sein, welche Daten wirklich übertragen werden können

Zum anderen muss die Identität des Kunden überprüft sein. Sonst könnten Datendiebe auf krumme Ideen kommen und Daten wegen eines angeblichen Anbieterwechsels abfragen.

Die Umzugsliste auf der vorherigen Seite hilft dabei, dass Sie als möglicher Umzugshelfer nichts vergessen, weder bei neuen Kunden und Kundendaten, noch beim Wechsel eines Kunden zum Wettbewerber. Der Schutz der Kundendaten hat eine hohe Bedeutung, auch bei ehemaligen Kunden. &

Körperverletzung durch einen Mitpatienten

Sie sind Patient in einem Krankenhaus. Ein Mitpatient hat einen Wutanfall und bricht Ihnen den Arm. Können Sie vom Krankenhaus seine Anschrift verlangen? Und warum hat auch Ihr Arbeitgeber Interesse an dieser Anschrift?

Mancher, der ins Krankenhaus muss, wird dort nicht gesund, sondern im Gegenteil noch kränker. Und das liegt keineswegs immer an den Ärzten. Auch Mitpatienten können eine echte Gesundheitsgefahr darstellen. Diese Erfahrung musste ein junger Mann machen, der sich in einer Fachklinik behandeln ließ.

Von Anfang an hatte er sich mit seinem Bettnachbarn nicht gut verstanden. Aber nun kam es ganz dick: Der Mitpatient bekam einen Wutanfall und schlug mit aller Kraft zweimal die Zimmertür gegen den Arm des jungen Mannes. Der Arm war danach gebrochen.

Schmerzensgeld – aber ohne Anschrift des Täters?

Als das Opfer wieder zu Hause war, wollte es Schmerzensgeld vom Täter. Den Vor- und den Nachnamen des Täters hatte das Opfer während seines Krankenhausaufenthalts zufällig mitbekommen. Die Adresse leider nicht. Deshalb wandte es sich an das Krankenhaus und bat dort um die

© K. Borchhardt/www.miniansichten.de

Anschrift. Das Krankenhaus lehnte diese Auskunft jedoch ab.

Sorge des Krankenhauses wegen seiner Schweigepflicht

Bei der Anschrift gehe es – so die Klinik – um personenbezogene Daten, und für diese Daten gelte die ärztliche Schweigepflicht. Deshalb könne man dem Opfer die Anschrift leider nicht mitteilen. Falls man dies tun würde, müssten die Verantwortlichen mit einem Verfahren wegen Verletzung der ärztlichen Schweigepflicht rechnen.

BGH: Anspruch auf Auskunft durch das Krankenhaus besteht!

Damit wollte sich das Opfer nicht zufrieden geben. Es verklagte das Krankenhaus auf Herausgabe der Anschrift. Mit Urteil vom 9. Juli 2015 (Aktenzeichen III ZR 329/14) gab der Bundesgerichtshof (BGH), bis zu dem der Fall schließlich gelangt war, dem Opfer Recht. Das geschah fast drei Jahre nach dem Krankenhausaufenthalt im November 2012.

Begründung des Gerichts

Zur Begründung seiner Entscheidung wies der Bundesgerichtshof auf Folgendes hin:

- Um Schadensersatzansprüche durchsetzen zu können, muss ein Kläger nicht nur den Namen des mutmaßlichen Täters kennen. Vielmehr braucht er auch dessen Anschrift. Ansonsten ist es nämlich schlicht nicht möglich, eine Klage auf Schadensersatz zuzustellen.
- Es ist richtig, dass die Anschrift eines Patienten der ärztlichen Schweigepflicht unterliegt. Auf der anderen Seite hat das Opfer jedoch ein berechtigtes Interesse daran, mögliche Ansprüche gegen den Täter gerichtlich durchzusetzen. Das berechtigte Interesse, Ansprüche auch durchsetzen zu können, berührt den „Anspruch auf Justizgewährung". Er ist im Grundgesetz zwar nicht ausdrücklich erwähnt, aber letztlich aus den Grundrechten des Opfers abzuleiten.
- Mit dieser Rechtslage wäre es nicht zu vereinbaren, wenn sich ein Krankenhaus ausnahmslos und ohne jede Abwägung weigern könnte, Angaben zur Identität des mutmaßlichen Täters zu machen. Datenschutzregelungen haben nicht den Zweck, einem Patienten die vollständige Anonymität auch dann zu sichern, wenn er einen Mitpatienten vorsätzlich verletzt. Deshalb ist das Krankenhaus verpflichtet, dem Opfer die Anschrift seines früheren Mitpatienten zu nennen. Ansonsten stünde das Opfer nämlich faktisch rechtlos da. Es hätte zwar vom Prinzip her einen Schadensersatzanspruch gegen den Täter, könnte ihn aber nicht durchsetzen.
- Jedenfalls wenn eine vorsätzliche Körperverletzung im Raum steht, ist es regelmäßig angemessen und geboten, dass das Auskunftsinteresse des Geschädigten den Vorrang gegenüber dem Datenschutzinteresse des Schädigers hat.

Entscheidung auch für Arbeitgeber wichtig

Vordergründig hat die Entscheidung nur für denjenigen Bedeutung, der durch einen Mitpatienten verletzt worden ist. Bei näherer Betrachtung ist sie jedoch auch für Arbeitgeber wichtig. Der Grund: Wer krank ist und deshalb nicht arbeiten kann, genießt normalerweise Lohnfortzahlung. Das gilt auch dann, wenn die Krankheit auf eine vorsätzliche Körperverletzung zurückgeht, die ein anderer dem Arbeitnehmer zugefügt hat.

Information des Arbeitgebers geboten

Dem Arbeitgeber ist es jedoch natürlich nicht zuzumuten, gewissermaßen für die Straftaten anderer zu zahlen. Deshalb hat er in solchen Fällen gegen den Täter einen Ausgleichsanspruch hinsichtlich der Kosten für die Lohnfortzahlung. Er ist in § 6 Entgeltfortzahlungsgesetz geregelt.

Falls man als Arbeitnehmer von jemandem verletzt wird und deshalb Lohnfortzahlung in Anspruch nimmt, sollte man deshalb seinen Arbeitgeber unverzüglich über die Hintergründe informieren. Das ist ein Gebot der Fairness, aber auch eine rechtliche Pflicht. &

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

Kryptoviren: Vorbeugen statt zahlen!

Kryptoviren wie Locky sind derzeit eines der zentralen IT-Sicherheits-Themen. Weshalb sind sie so gefährlich und wie können sich Unternehmen dagegen schützen?

Die Gefährlichkeit der aktuellen Viren liegt darin, dass die E-Mail als Träger sehr professionell gemacht ist und es ziemlich schwierig ist, zu erkennen, ob es sich hierbei um eine reguläre E-Mail handelt. Dem Empfänger wird z.B. vermittelt, dass eine Rechnung noch nicht beglichen wurde. Öffnet dieser das Dokument, aktiviert sich das Makro und verschlüsselt den gesamten Inhalt der Festplatte! Eine Entschlüsselung ist dann nur noch möglich, wenn das geforderte Lösegeld an die Erpresser überwiesen wird.

Diese achten bei der Gestaltung auf regionale Aspekte, wie Sprachen und Zeitzonen. Zusätzlich wird die infizierte E-Mail so manipuliert, dass sie von einem vermeintlich bekannten Unternehmen zugestellt wird. Ein Misstrauen beim Empfänger stellt sich möglicherweise gar nicht erst ein. Es lässt sich also festhalten, dass Gruppen am Werk sind, die höchst professionell die Angriffe von der Entwicklung bis zur Deaktivierung der Viren auf infizierten IT-Systemen planen und durchführen.

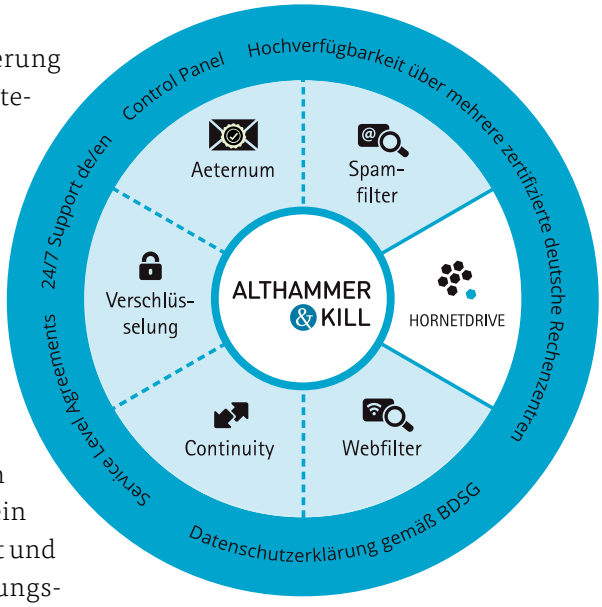
Zuletzt zahlte die Stadtverwaltung Dettelbach, trotz Abraten der Polizei und des BSI, das geforderte Lösegeld i.H.v. 490 € für die Entschlüsselung der Daten, weil kein alternativer Lösungsweg in Betracht gezogen werden konnte. Allerdings wurde nur ein Teil der Daten wiederhergestellt und die Ausfall- und Instandsetzungskosten werden auf über 100.000 € geschätzt.

Eine vollständige Entschlüsselung muss stark angezweifelt werden, deshalb raten auch wir davon ab, im Falle einer Infizierung, mögliche Lösegelder an die Erpresser zu überweisen.

Vorbeugen statt Zahlen

Zu einer vernünftigen Strategie gegen Locky und Co. gehören vor allem eine regelmäßige Datensicherung, das Einspielen von Updates, das Schützen der Verzeichnisse auf Servern vor unbefugtem oder unnötigem Zugriff und ein angemessener Virenschutz. Aber auch das kritische Prüfen jeder E-Mail durch den Empfänger selbst, ist von großer Bedeutung.

Da sich die aktuellen Viren vor allem über Anhänge oder Links in E-Mails verbreiten, ist ein zentraler Schutz



an vorderster Front der Datenkommunikation dringend anzuraten, die E-Mails müssen also bereits geprüft werden, bevor sie im E-Mail-Programm erscheinen. Allerdings werden für dieses Szenario vielmals Lösungen innerhalb des eigenen Netzwerkes eingesetzt, die auf die Schnelligkeit der Virenentwicklung nicht reagieren können. Diese sind keineswegs schlecht, sie aber als einzigen Schutz vor der aktuellen Virenwelle zu betreiben, steht auf dem Prüfstand!

Spam- und Virenschutz aus der Cloud

Ein Methoden-Mix, entwickelt von spezialisierten Dienstleistern, der E-Mails sowie optional auch den gesamten Internetverkehr noch außerhalb des eigenen Netzwerkes vor Viren und sonstiger Schadsoftware schütz, kann die Sicherheit deutlich erhöhen.

Haben Sie Fragen?

Wir unterstützen Sie gerne bei der Vorbeugung gegen Kryptoviren und der Optimierung Ihres E-Mail Spam- und Virenschutzes.

Bei Interesse stellen wir Ihnen unser Angebot im Bereich IT-Sicherheit gern persönlich vor:
info@althammer-kill

Althammer & Kill stellt in Zusammenarbeit mit Hornetsecurity eine Spam- und Virenschutzlösung zur Verfügung, die mittlerweile über 18 unterschiedliche Virenscanner zur Erkennung von Schadsoftware verfügt. Allein für das Erkennen von Makro-Viren in Office-Dokumenten sind derzeit 8 Virenscan-Methoden im Einsatz, die auf verschiedene Angriffsszenarien reagieren.

Neue Viren werden am schnellsten und besten über unsere Honeypots erkannt. Dahinter stecken E-Mail-Adressen, die nur einem einzigen Zweck dienen, nämlich Spam- und Virenmails einzufangen. Die Inhalte werden analysiert und in die Untersuchungskriterien aufgenommen. In den vergangenen drei Monaten lag der Durchschnitt bei knapp 400 neuen Virenvarianten täglich, wobei die höchste Zahl bei 2732 neuer Virentypen lag, die unsere Filter erkennen und herausfiltern mussten. &

Datenschutz-Grundverordnung: Vergessen will gelernt sein

Das neue EU-Datenschutzrecht wird das sogenannte Recht auf Vergessenwerden einfordern. Doch kann das Internet denn überhaupt vergessen? Nicht wirklich!

Schon vor Jahren gab es die Idee, Daten mit einem digitalen Radiergummi für immer aus dem Internet zu löschen. Mehrere Seiten forderten ein Recht auf Vergessenwerden. Allerdings zeigte sich schnell, dass das Internet nicht vergisst. Auch wenn man zum Beispiel ein Bild verschlüsselt und den Schlüssel löscht, ist das Bild nicht weg. Es kann zahllose Kopien im Internet geben, die ohne Schlüssel sichtbar sind.

Das Recht auf Vergessenwerden kommt trotzdem

Aber obwohl es den Radiergummi für das Internet nicht gibt, steht das Recht auf Vergessenwerden in der kommenden EU-Datenschutz-Grundverordnung (EU-DSGVO). Nun könnte man meinen, es mache doch keinen Sinn, ein Recht vorzusehen, das sich technisch nicht umsetzen lässt. Doch die EU-DSGVO verlangt nichts Unmögliches – aber sie verlangt viel. So gehört zum Recht auf Vergessenwerden, dass die schon aus dem deutschen Datenschutzrecht bekannten Löschpflichten umgesetzt werden: Wenn die Betroffenen nicht möchten, dass ihre Daten weiterverarbeitet werden, und es keine legitimen Gründe für deren

© K. Borchhardt/www.miniansichten.de

Speicherung gibt, müssen die Daten gelöscht werden.

Löschen ist auch nach Veröffentlichung der Daten ein Muss

Ebenso sieht die EU-DSGVO vor, dass andere Stellen, die die zu löschenden Daten erhalten haben, über die Löschpflicht oder den Löschwunsch des Betroffenen informiert werden. Das ist im Bundesdatenschutzgesetz (BDSG) bereits heute so geregelt. Das neue EU-Datenschutzrecht spricht aber zusätzlich von öffentlich gemachten Daten und davon, Links auf die zu löschenden Daten oder auf zu löschende Datenkopien zu entfernen.

Man kann also davon ausgehen, dass Unternehmen und Behörden auch dann die Löschpflichten angehen müssen, wenn die Daten bereits im Internet veröffentlicht sind. Dabei verlangt die Datenschutz-Grundverordnung jedoch keine Wunder, sondern das wirtschaftlich und technisch Machbare. Man kann aber nicht einfach sagen: „Die Daten sind im Internet zu finden, Löschen ist da sowieso nicht möglich." Vielmehr gilt es, zum Beispiel Suchmaschinenbetreiber dazu zu bringen, die Links auf die Daten aus ihrem Bestand zu nehmen.

Löschen betrifft auch die Offline-Welt

Bei all der Diskussion um einen digitalen Radiergummi und das bleibende Gedächtnis des Internets darf die Offline-Welt nicht vergessen werden. So hatte die EU-Agentur für Netz- und Informationssicherheit (ENISA) nicht nur erklärt, dass ein digitaler Radiergummi technisch unmöglich ist. ENISA hatte vielmehr auch auf die entscheidende Rolle der Suchmaschinenbetreiber und auf die klassischen Speichermedien verwiesen. Das Recht auf Vergessenwerden betrifft nämlich auch alle zu löschenden Daten, die sich nicht im Internet befinden. Offline können zahllose Kopien von Daten vorliegen, die Sie beim Löschen nicht vergessen dürfen. So können Daten, die im Firmennetzwerk gelöscht wurden, durchaus noch:

- als Kopie auf externen Festplatten im Home-Office von Mitarbeitern,
- auf USB-Sticks des Außendienstes oder
- auf mobilen Endgeräten wie Smartphones liegen.

Auch wenn sie dort verschlüsselt gespeichert sind (was zu hoffen ist), besteht die Löschverpflichtung, wenn es keine rechtlichen oder vertraglichen Gründe mehr dafür gibt, sie aufzubewahren. Deshalb: Vergessen Sie das Löschen nicht! &

Denken Sie daran, personenbezogene Daten rechtzeitig zu löschen? Machen Sie den Test!

Frage: Ein Kunde hat seinen Vertrag gekündigt. Müssen Sie alle Daten sofort löschen?

a) Ja, ohne gültigen Vertrag dürfen die Daten nicht mehr gespeichert werden.
b) Nein, es ist nicht erforderlich, sie sofort zu löschen, wenn es Aufbewahrungspflichten gibt.

Lösung: Die Antwort b. ist richtig. Es gibt viele rechtliche Vorgaben, die fordern, Daten länger vorzuhalten. So sieht das Handelsgesetzbuch (HGB) eine Aufbewahrung von Geschäftsunterlagen (§§ 238, 257, 261 HGB) vor. Ebenso gibt es Aufbewahrungsvorschriften nach § 147 Abgabenordnung (AO), um nur einige Vorgaben zu nennen.

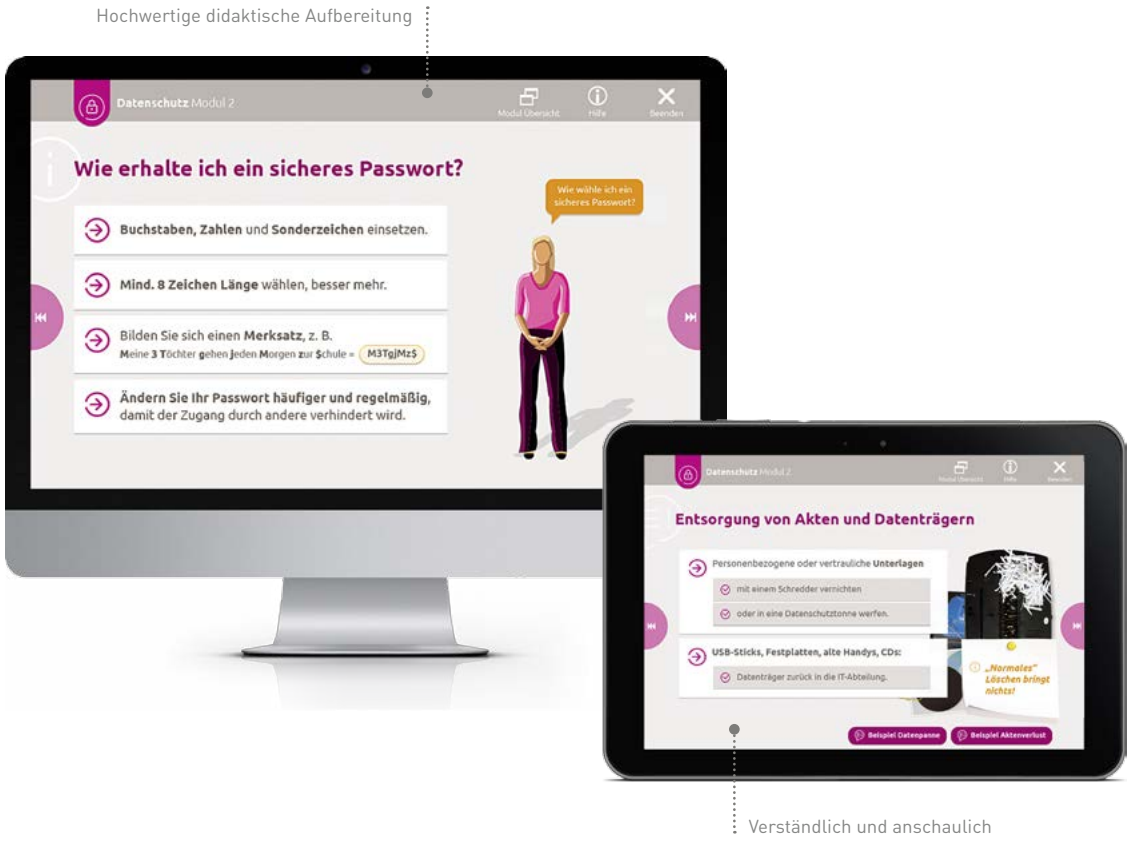
Frage: Sind Daten einmal im Internet gelandet, lassen sie sich nicht mehr löschen. Das Internet vergisst nichts, deshalb entfällt jede Löschpflicht für das Internet. Ist das so?

a) Ja, denn wenn man im Internet etwas löscht, ist das vergebene Mühe. Es gibt zahllose Kopien, die man nicht komplett löschen kann
b) Nein, auch wenn man nicht alle Datenkopien im Internet finden und löschen kann, bleibt die Löschpflicht bestehen..

Lösung: Die Antwort b. ist wieder richtig. Die Löschpflicht betrifft auch Daten, die im Internet veröffentlicht wurden. Man muss alles tun, was wirtschaftlich vertretbar und technisch machbar ist, um die Daten im Internet zu löschen. Dazu gehört auch der Hinweis an Suchmaschinenbetreiber, dass sie die Links auf die zu löschenden Daten entfernen sollen. Vergessen werden dürfen aber auch nicht die Daten auf den lokalen Speichermedien, die viele Datenkopien vorhalten könnten. Das Recht auf Vergessenwerden ist also ein Recht auf umfassendes Löschen im Rahmen des wirtschaftlich und technisch Machbaren.

E-Learning Datenschutz und IT-Sicherheit

Zur Erfüllung der Unterweisungspflichten nach § 4 g BDSG, § 22 DSG-EKD, § 21 KDO und entsprechenden Landesdatenschutzgesetzen.



E-Learning ist für viele Unternehmen keine flüchtige Modeerscheinung mehr, sondern fester Bestandteil des Fort- und Weiterbildungsangebotes. Wer heute jedoch darüber nachdenkt, neue Lernformen einzuführen, sieht sich mit einer unüberschaubaren Fülle von Inhalten, Lerntechnologien und didaktischen Modellen konfrontiert.

Zusammen mit dem Vincentz-Verlag haben wir daher auf Basis des freien Kursmanagementsystems „Moodle" ein E-Learning-Modul über den Schutz vertraulicher Daten und Systeme entwickelt. Die Inhalte sind verständlich, anschaulich und hochwertig didaktisch aufbereitet. Die Sensibilisierung Ihrer Mitarbeiter ist wichtiger denn je: Datenschutz und IT-Sicherheit sind in den Fokus gerückt.

Verstöße oder Datenpannen haben unter Umständen größere Auswirkungen auf Ihre Kundenbeziehungen. Die gesetzlich vorgeschriebene Unterweisung Ihrer Mitarbeiterinnen und Mitarbeiter stellt insbesonders größere Organisationen mit einer Vielzahl von Standorten, dezentralen Strukturen oder Schichtbetrieben vor Herausforderungen. Unser E-Learning-Modul zu Datenschutz und IT-Sicherheit berücksichtigt die organisatorischen und technischen Vorgaben entsprechend Bundesdatenschutzgesetz und den 16 Landesdatenschutzgesetzen in Deutschland.

Zeitdauer: ca. 40 Minuten
Lernkontrolle: auf Wunsch möglich
Technische Voraussetzungen: Internetzugang und Browser (einfachste Bedienung ohne Installation oder sonstige Betriebskosten) &

Haben Sie Interesse?

Wir lassen Ihnen gern ein unverbindliches Angebot zukommen:
info@althammer-kill

Akademie

Ausbildung Datenschutzbeauftragte Fokus Kirche & Sozialwirtschaft

18.05. – 20.05.2016, Düsseldorf
07.06. – 09.06.2016, Hannover

Das Seminar vermittelt in kompakter Form das „Handwerkzeug" für die Aufgaben eines Datenschutzbeauftragten auf Grundlage der Datenschutzgesetze DSG-EKD, KDO und BDSG. Anschauliche Beispiele aus der Datenschutzpraxis vermitteln das komplette Basiswissen. In nur drei Tagen erlernen Sie so die notwendige Fachkunde.

Zielgruppe

Die Ausbildung richtet sich an (zukünftige) Datenschutzbeauftragte auf Basis der folgenden gesetzlichen Grundlagen:

- Betriebsbeauftragte und örtlich Beauftragte für den Datenschutz (§ 22 DSG-EKD)
- Betriebliche Beauftragte für den Datenschutz (§ 20 KDO)
- Beauftragte für den Datenschutz (§ 4f BDSG)

Inhalte des Seminars

- Einführung und Sensibilisierung
- Rechtliche Grundlagen des Datenschutzes
- Grundzüge DSG-EKD, KDO und BDSG
- Rechtsstellung, Anforderungen und Aufgaben des Beauftragten
- Daten: Erhebung, Verarbeitung und Nutzung
- Rechte der betroffenen Personen
- Bereichsspezifischer Datenschutz
- Praktische Fallbeispiele
- IT-Sicherheit
- Technische- und organisatorische Maßnahmen
- Die ersten 100 Tage des Datenschutzbeauftragten
- Aktuelle Herausforderungen wie Cloud Computing, Social Media u.a.
- Fragen und Antworten

Ausbildung IT-Sicherheitsbeauftragte Fokus Kirche & Sozialwirtschaft

31.05. - 02.06.2016, Hannover
28.06. – 30.06.2016, Düsseldorf

Neben der Einführung in technische und organisatorische Aspekte der IT-Sicherheit ist die praxisorientierte Umsetzung der Informationssicherheit nach IT-Grundschutz des BSI bzw. der IT-Sicherheitsverordnung der EKD (ITSVO-EKD) wesentlicher Inhalt des Kompaktseminars.

Zielgruppe

Die Weiterbildung richtet sich an Fach- und Führungskräfte sowie Entscheider, die für die IT-Sicherheit verantwortlich sind. Ausgewählte Bedrohungen, Gegenmaßnahmen und Wirksamkeitskontrollen werden demonstriert und die Vorgehensweise zur Entwicklung eines IT-Sicherheitskonzeptes in Gruppenarbeiten geprobt.

Inhalte des Seminars

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

Eine ausführliche Seminarbeschreibung und Anmeldemöglichkeiten finden Sie unter:
https://www.althammer-kill.de/akademie.html

Termine

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

18.05. – 20.05.2016, Düsseldorf /07.06. – 09.06.2016, Hannover
Ausbildung Datenschutzbeauftragte
Fokus Kirche & Sozialwirtschaft
Anmeldung über: www.althammer-kill.de

31.05. – 02.06.2016, Hannover /28.06. – 30.06.2016, Düsseldorf
Ausbildung IT-Sicherheitsbeauftragte
Fokus Kirche & Sozialwirtschaft
Anmeldung über: www.althammer-kill.de

09.06.2016 Fachtagung, München
„Datenschutz in der Medizin – Update 2016“
Angebot unseres Kooperationspartners:
http://www.esturias.de/übersicht-09-06-2016/

10.06.2016 Symposium, München
„Die EU-Datenschutzgrundverordnung:
Fragen und Antworten zur praktischen Umsetzung“
Angebot unseres Kooperationspartners:
http://www.esturias.de/übersicht-10-06-2016/

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

News

Aus unserem
aktuellen Newsletter:

„Like“-Buttons auf Websites verletzt Datenschutzregeln
https://www.althammer-kill.de/newsletter-detail/like-buttons-auf-websites-verletzt-datenschutzregeln.html

Verschlüsselungs-Trojaner: Krankenhäuser und Stadtverwaltung kaufen sich frei
https://www.althammer-kill.de/newsletter-detail/verschluesselungs-trojaner-krankenhaeuser-und-stadtverwaltung-kaufen-sich-frei.html

Safe-Harbor-Update
https://www.althammer-kill.de/newsletter-detail/safe-harbor-update.html

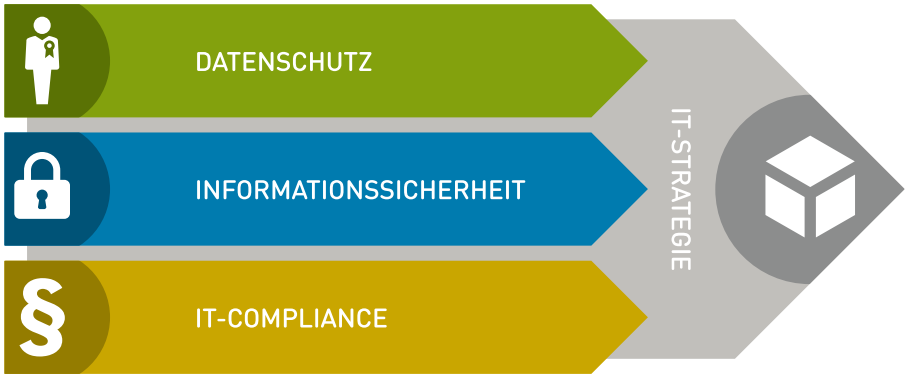
Orientierungshilfe zur Nutzung von E-Mail und Internet am Arbeitsplatz
https://www.althammer-kill.de/newsletter-detail/orientierungshilfe-zur-nutzung-von-e-mail-und-internet-am-arbeitsplatz.html

Auswirkungen der EU-Datenschutzgrundverordnung
https://www.althammer-kill.de/news-detail/auswirkungen-der-eu-datenschutzgrundverordnung.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 IT-Berater, zertifizierte Datenschutzbeauftragte und ausgebildete IT-Compliance-Beauftragte.



Datenschutz

Durch unsere langjährige Erfahrung in unterschiedlichsten Branchen können wir praxisgerechte Lösungen für Ihr Unternehmen entwickeln. Sei es im Rahmen eines konkreten Projektes oder als langfristige Begleitung Ihres Unternehmens z. B. in der Funktion als externer Datenschutzbeauftragter.

Informationssicherheit

Sind Ihre Systeme sicher? In unserer vernetzten Welt fällt es immer schwerer, den Durchblick zu behalten. Angriffe von außen oder ungewollter Informationsverlust: die Risiken sind vielfältig. Wir begleiten Sie zu Security-Fragen, prüfen die Sicherheit Ihrer Systeme und stellen den IT-Sicherheitsbeauftragten.

IT-Compliance

Gesetze, Verordnungen, Normen – da fällt es nicht immer leicht, Compliance-Verstöße zu verhindern. Wir begleiten branchenorientiert und liefern passende Konzepte für einen rechtssicheren Betrieb Ihres Unternehmens, z. B. im Rahmen des Risiko- und Notfallmanagements.

IT-Strategie

Welche Ziele möchten Sie mithilfe der Informationstechnologie in Ihrem Unternehmen erreichen? Wo liegen Möglichkeiten, Nutzen und Wertschöpfung? Wir orientieren unsere Arbeit an Ihren Zielen und begleiten bei der Auswahl und Gestaltung passender Strategien.

Wir sind Mitglied der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD), des Berufsverbandes der Datenschutzbeauftragten Deutschlands e. V. (BvD) und des Fachverbands Informationstechnologien in Sozialwirtschaft und Sozialverwaltung e. V. (FINSOZ). &

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

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

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

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

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

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

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

Althammer & Kill GmbH & Co. KG

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

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