Datenschutz konkret

ALTHAMMER & KILL

Das Kundenmagazin von Althammer & Kill
Ausgabe 6/2016

Liebe Leserin, lieber Leser,

vor uns liegen spannende Zeiten. Mit der EU-Datenschutz-Grundverordnung wird der Datenschutz zwar nicht völlig auf den Kopf gestellt, es gibt aber in den kommenden 18 Monaten eine Menge zu tun, um Sie „fit" zu machen für die neue Gesetzesgrundlage. Wir begleiten Sie in den Vorbereitungen aktiv, damit Sie entsprechend gerüstet sind.

Gleichzeitig lesen wir in den Medien täglich von neuen Angriffen auf IT-Systeme. Ende November haben vermeintliche Hacker für große Ausfälle im Netz der Telekom gesorgt. Dieses Beispiel verdeutlicht, neben vielen anderen, dass eine intensive Auseinandersetzung mit der Absicherung unserer IT-Systeme auf allen Ebenen gefordert ist.

Trotz und mit all diesen Nachrichten freuen wir uns auf die weitere Zusammenarbeit mit Ihnen. Im Namen des ganzen Teams möchten wir uns herzlich für Ihr Vertrauen bedanken. Wir wünschen Ihnen und Ihren Lieben eine ruhige Weihnachtszeit und alles Gute für das Jahr 2017.

Thomas Althammer & Niels Kill

Terminkalender-Apps: Fast wie ein Schwarzes Brett

Geht es um eine Terminabstimmung, greifen viele inzwischen zu ihrem Smartphone. Einige Kalender-Apps sind aber keine einfachen Terminkalender, sondern kleine Plaudertaschen.

Ging es früher darum, einen freien Termin zu suchen, griff man in die Hand- oder in die Jackentasche und brachte ein kleines Büchlein zum Vorschein, den Terminkalender. Nur unter Freunden konnte es passieren, dass man seinen Terminkalender offen auf den Tisch legte, sodass auch

In dieser Ausgabe:

das Gegenüber einen Blick auf die Terminlücken werfen konnte. Den Kalender einem Dritten hinüberzureichen, wäre undenkbar gewesen.

Heute ist das anders: So mancher hat einen offenen Terminkalender, in den Dritte schauen können. Allerdings geschieht das nicht bewusst, sondern ungewollt.

Smartphones ersetzen klassische Kalender

Besondere Vorsicht ist angezeigt, wenn das Smartphone, genauer gesagt eine Terminkalender-App, den Papier-Kalender ersetzt. Wie eine Umfrage des Digitalverbands Bitkom ergab, verwenden aber mittlerweile acht von zehn Smartphone-Nutzern (83 Prozent) ihr Gerät als Kalender oder Terminplaner. Die meisten Smartphones nutzen dafür das Android-Betriebssystem. Dort gibt es als führende Kalender-App den Google-Kalender.

© K. Borchhardt/ www.miniansichten.de

Die Google-Kalender-App hat viele auf den ersten Blick praktische Funktionen, die aber auf den zweiten Blick zeigen, wie stark die Daten im Terminkalender ausgewertet werden und wie leicht andere Personen Zugang zu ihnen bekommen könnten.

Nicht nur Google Now & Co. lesen mit

Google beschreibt die Funktionen seiner Kalender-App unter anderem so: Flüge, Hotelbuchungen, Konzerte, Tischreservierungen und andere Termine aus dem E-Mail-Dienst Gmail werden automatisch zum Kalender hinzugefügt.

Mithilfe von intelligenten Vorschlägen für Termintitel, Orte und Personen lassen sich neue Termine schnell erstellen. Man fügt Kollegen als Gäste hinzu, und der Google-Kalender hilft dabei, die besten Besprechungszeiten zu suchen.

Virtuelle Assistenten wie Google Now durchsuchen den Kalender und geben Hinweise, wann man aufbrechen muss, um rechtzeitig anzukommen. Gibt man an, an welchem Ort ein Termin stattfindet, bekommt man nicht nur passende Stadtpläne und Bilder des Ortes angezeigt, auch die Werbung passt zu den Terminen.

Diese Beispiele zeigen: Mit unbedachten Klicks könnten Kollegen, Kunden und andere Personen, die man trifft, ungewollt Einsicht in Termine bekommen. Anders als beim Termin-Büchlein befinden sich die Termindaten auf den Servern des Betreibers wie Google.

Datenschutz-Einstellungen und eine genaue Durchsicht der Datenschutzerklärung und der Berechtigungen für die App sind bei einem Smartphone-Kalender absolute Pflicht. Sonst könnte der eigene Kalender zum Schwarzen Brett im Internet werden. &

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,– €

Download von Schadsoftware am Arbeitsplatz

Ein Arbeitnehmer surft an seinem Arbeitsplatz immer wieder privat im Internet. Nur in den Pausen natürlich. Er weiß genau, dass die Unternehmensleitung privates Surfen verboten hat. Aber auch die Vorgesetzten wissen Bescheid. Und bisher hat keiner etwas dagegen gesagt. Eines Tages läuft es aber ziemlich schlecht: Der Mitarbeiter lädt sich eine Software herunter und speichert sie auf dem Dienst-PC. Dabei fängt er sich aggressive Schadsoftware ein. Der PC liegt lahm. Bekommt er jetzt Ärger?

Es war zwar offiziell verboten, aber im Alltag störte es niemanden, auch keinen Vorgesetzten. Und das übrigens ausgerechnet in einem Sachverständigenbüro für Kriminaltechnik. Deshalb nutzte ein Mitarbeiter in den Pausen das Internet immer wieder privat.

Ein Verstoß mit Folgen

Eines Tages installierte er eine Software auf seinem Dienst-PC, mit der man Tondateien verkleinern kann. Für seine Arbeit braucht er diese Software nicht. Leider fing er sich beim Herunterladen einen ganzen Rattenschwanz an Schadsoftware ein. Der PC lag still. Ein Fachmann musste ihn wieder in Gang bringen. Das kostete den Arbeitgeber 865 €.

Schadensersatz und fristlose Kündigung

Dieses Geld will der Arbeitgeber jetzt von seinem Arbeitnehmer zurück. Außerdem hat er ihm fristlos gekündigt. Begründung: Verstoß gegen das Verbot, das Internet am Arbeitsplatz privat zu nutzen!

Der Arbeitnehmer wehrt sich

Der Arbeitnehmer fühlte sich im falschen Film. Kann es sein, dass die Unternehmensleitung Verstöße gegen dieses Verbot erst toleriert – wenn dann aber mal etwas passiert, gleich grob wird? Das wollte er nicht glauben. Deshalb klagte er gegen die Kündigung. Außerdem weigerte er sich, die 865 Euro zu zahlen. Schließlich – so dachte er sich – muss man für Fehler am Arbeitsplatz doch im Normalfall überhaupt nicht haften. Auch wenn es einen Schaden gibt.

Fiasko bei Gericht

Mit dieser Haltung hatte er beim Landesarbeitsgericht Mainz allerdings gleich doppelt Pech: Erstens bestätigte das Gericht die fristlose Kündigung.

Zweitens verurteilte es ihn dazu, die 865 Euro zu zahlen. Für beides nennt das Gericht gute Gründe.

Fristlose Kündigung bestätigt

Was die fristlose Kündigung angeht, spielt es aus der Sicht des Gerichts kaum eine Rolle, dass die Unternehmensleitung privates Surfen tolerierte. Im konkreten Fall hilft das dem Kläger nichts. Was der Kläger getan hat, war nämlich nicht einfach „ein bisschen surfen". Vielmehr hat er für rein private Zwecke Software heruntergeladen und installiert. Das ist viel gefährlicher als reines Surfen.

Außerdem hatte der Virenscanner beim Installieren einen Warnhinweis gegeben. Den hatte der Kläger jedoch einfach weggeklickt. Das war aus der Sicht des Gerichts besonders leichtfertig.

Und schließlich hatte die Unternehmensleitung den Kläger im Laufe des letzten Jahres auch noch dreimal im Datenschutz schulen lassen. Er hätte also wissen müssen, was Sache ist.

Abmahnung entbehrlich

Insgesamt kommt das Gericht deshalb zu der Auffassung, dass sich der Arbeitgeber auf den Kläger nicht mehr verlassen kann. Aus rein privaten Interessen war dem Kläger die Sicherheit des EDV-Systems letztlich egal. Weil das schwer wiegt, musste der Arbeitgeber ihn vor einer Kündigung nicht erst abmahnen.

Dem Kläger hätte auch ohne Abmahnung klar sein müssen, dass der Arbeitgeber ein solches Verhalten auf keinen Fall toleriert. Deshalb konnte der Arbeitgeber sofort fristlos kündigen, und das Gericht erklärte diese Kündigung für wirksam.

Schadensersatzpflicht des Arbeitnehmers

Das nächste Fiasko erlebte der Kläger bei der Frage des Schadensersatzes. 865 € sind für den Kläger viel Geld. Sein Monatslohn betrug nämlich nur 2.800 € brutto. Dennoch sieht das Gericht keinen Grund, schonend mit dem Kläger umzugehen. Er muss die 865 Euro zahlen.

Den Betrag an sich hält das Gericht für angemessen. Dabei argumentiert es vereinfacht gesagt so, dass ein Fachmann, der Schadsoftware beseitigt, eben nicht billig ist. Außerdem ist eine solche Arbeit relativ aufwendig.

Keinerlei Haftungserleichterung

Über irgendeine Haftungserleichterung verliert das Gericht in seiner Entscheidung kein Wort. Das lässt sich leicht erklären. Der Kläger hat den Schaden nämlich gar nicht während der Arbeit angerichtet. Die Software hat er vielmehr für rein private Zwecke während der Pause heruntergeladen. Und das hat mit der Arbeit natürlich nichts zu tun.

Wer das Urteil selbst lesen will, findet es mit dem Aktenzeichen 5 Sa 10/15 im Internet sofort.

Die wichtigste Lehre aus dem Urteil lautet: Bloß weil ein Arbeitgeber nichts unternimmt, wenn Mitarbeiter gegen ein Verbot verstoßen, ist noch lange nicht alles Mögliche erlaubt! Wenn er zum Beispiel privates Surfen duldet, nimmt er privates Herunterladen von Software nicht zwangsläufig in Kauf. &

Weitreichender Hacker-Angriff auf das Netz der Telekom

Wie Ende November bekannt wurde, ist es nun in Deutschland zu einem massiven Angriff auf DSL-Router gekommen. Hunderttausende Anschlüsse der Telekom waren lahmgelegt und konnten teils längere Zeit weder Telefon, noch Internet oder TV-Angebote nutzen.

Ziel der Hacker war es, eine Anfälligkeit von DSL-Routern zu nutzen, um Schadcode einzuschleusen. Wie sich nun herausstellte, war dieser Code fehlerhaftg, so dass dieser Angriff vergleichsweise glimpflich ausging. Die Router hatten zwar keine Sicherheitslücke, gingen aber aufgrund der massenhaften Angriffsversuche automatisch vom Netz.

In Ausgabe 4/2016 hatten wir über das Internet der Dinge (IoT) und damit verbundenen Gefährdungen der IT-Sicherheit berichtet. Wir sind der Überzeugung, dass es zu einem neuen Ansatz bei der Berücksichtigung von Datenschutz und IT-Sicherheit kommen muss. Die Anstrengungen hierzu sollten in allen Bereichen verstärkt werden, nicht nur für Geräte im Privatbereich, auch für IT-Systeme, Netze und Software im Unternehmenseinsatz. &

Darknet – das böse Internet

Gibt es außer dem Internet, das wir täglich nutzen, wirklich noch ein zweites, dunkles Internet, das Darknet? Oder ist das nur eine von den vielen Verschwörungstheorien, die derzeit im Umlauf sind?

Dass man fast alle Dinge auf der Welt für gute und für schlechte Taten benutzen kann, ist jedem klar. Dafür gibt es viele Beispiele. So kann man ein Auto benutzen, um Freunde zu besuchen oder in den Urlaub zu fahren. Und ein Notarztfahrzeug ist eigentlich aus-schließlich dazu da, Menschen zu retten. Das ändert aber nichts daran, dass man sogar damit einen Menschen absichtlich töten kann, ohne jeden Grund und einfach so.

Mit dem Internet ist es im Ausgangspunkt nicht anders. Man kann hier Freundschaften pflegen, Informationen besorgen und beispielsweise Urlaubsziele aussuchen. Aber natürlich lassen sich auch mit dem Instrument „Internet" Straftaten begehen.

Das „Tatmittel Internet"

Deutlich wird das etwa in den polizeilichen Kriminalstatistiken. Hier gibt es einen eigenen Bereich mit der Überschrift „Tatmittel Internet". Niemand wird überrascht sein, dass dort Betrügereien auftauchen, die Kriminelle mithilfe des Internets begehen. Ein aktuelles Beispiel: Auf einer Webseite wird so getan, als hätte jemand eine Ferienwohnung anzubieten. Sobald er genügend Vorauszahlungen eingesammelt hat, ist die Webseite verschwunden. Die Ferienwohnung hat es natürlich in Wirklichkeit nie gegeben. Sogar die Bilder von der angeblichen Wohnung waren von anderen Webseiten gestohlen, das heißt von dort illegal kopiert.

Wirklich übel: das „echte Darknet"

Ärgerlich, manchmal auch schlimm für die Betrogenen. Aber solche Dinge hat es ohne das Internet auch früher schon gegeben. Das Internet macht solche Straftaten manchmal nur viel leichter. Das Darknet, also das ausschließlich dunkle Internet, muss aber etwas anderes sein, das ahnt man bei solchen Beispielen sofort. Und so ist es auch.

Tatsächlich gibt es Bereiche im Internet, die ausschließlich kriminellen Zwecken dienen und mit denen ein Normalbürger nie zu tun hat. Dort geht es nur um Waffenhandel, Rauschgift und Schlimmeres. Über einen solchen Bereich des Internets haben sich zum Beispiel auch islamistische Attentäter Waffen besorgt.

Kein Zugang über normale Suchmaschinen

Wer sich nicht genau vorstellen kann, wie so etwas funktioniert, sollte einmal kurz darüber nachdenken, wie er eine Seite im Netz findet. Dazu ist eine Suchmaschine nötig, beispielsweise Google. Viele glauben, dass solche Suchmaschinen alles finden, was es im Netz gibt. So einfach ist es jedoch nicht. Eine Suchmaschine findet nur

die Seiten, an die sie andocken kann. Und natürlich lässt sich eine Seite auch so programmieren und einrichten, dass dies nicht gelingt. Dann finden sie jedenfalls die gängigen Suchmaschinen nicht.

Zugangscodes und anonymisierte Kommunikation

Hier bietet sich dann ein Anknüpfungspunkt für kriminelle Aktivitäten. Eine Webseite wird so eingerichtet, dass sie nur jemand findet, der die genaue Adresse kennt und – das macht die ganze Sache noch ein Stück perfekter – der einen Zugangscode eingeben kann, nach dem die Seite fragt.

Die Adresse und den Zugangscode müssen die Beteiligten auf irgendeinem Weg vorher untereinander austauschen. Dafür bieten sich spezielle Seiten in sozialen Netzwerken an. Sie sind ebenfalls so ausgestaltet, dass man nicht „einfach so" hineinkommt, sondern erst, wenn man auf Anfrage zugelassen wird.

Zusätzlich ist es denkbar, dass die Kommunikation über ein Netzwerk erfolgt, das Verbindungsdaten anonymisiert. Besonders das Netzwerk Tor wird in diesem Zusammen-hang oft genannt.

Bedenken sollte man dabei, dass es für viele Menschen auf der Welt äußerst wichtig ist, nur über Netzwerke zu kommunizieren, in denen sie anonym bleiben können. Man denke etwa an Oppositionelle in Diktaturen. Solche Netzwerke sind also nicht automatisch böse oder gar kriminell. Sie lassen sich aber leicht in kriminelle Aktivitäten „einbauen".

Unter Beobachtung des Bundeskriminalamts

All dies zeigt, dass man in das Darknet nicht einfach so durch Zufall hineingerät. Wer dort anzutreffen ist, will ganz bewusst dort sein und braucht einige Kenntnisse über die Funktionsweise des Internets.

Niemand muss also befürchten, beim Surfen versehentlich in den dunklen Teil des Internets hineinzugeraten. Ernst zu nehmen ist er aber trotzdem. Aus gutem Grund spielt das Darknet eine große Rolle im Bundeslagebild Cybercrime, das das Bundeskriminalamt (BKA) jedes Jahr veröffentlicht. &

Licht in die Schatten-IT: Warum Absprachen mit der IT wichtig sind

Wenn Sie selbst die Software auswählen und installieren, die Sie brauchen, ist das keine Unterstützung für die IT-Administration, sondern eine Gefahr für vertrauliche Daten.

Dank der IT wird vieles einfacher, so heißt es jedenfalls. Doch nicht immer passt die verfügbare Software oder Hardware zu den aktuellen Aufgaben.

Mitunter scheint sich die vorhandene IT überhaupt nicht für die täglichen Aufgaben im Büro zu eignen. Vielleicht ist es Ihnen auch schon so gegangen, dass Sie am liebsten eine andere IT-Lösung gehabt hätten.

Einige Anwender melden ihre IT-Probleme bei den IT-Administratoren, andere sprechen ihre Vorgesetzte oder ihren Vorgesetzten an. So mancher Nutzer wird selbst aktiv, sucht sich einfach im Internet die passende Lösung und setzt sie im Unternehmen ein. Was wie eine gute Idee und Unterstützung für die IT-Abteilung aussieht, ist sehr riskant. Kaum etwas fürchten IT-Administratoren mehr als den eigenmächtigen Anwender. Die IT, die Nutzer selbst installieren, wird auch Schatten-IT genannt – aus gutem Grund.

Im Schatten lauern Gefahren

Die Schatten-IT ist die IT, die die Administratoren nicht so einfach oder gar nicht sehen können. Anders gesagt, es ist die IT, von der die IT-Abteilung nichts weiß und um die sie sich deshalb nicht kümmern kann. Wenn Sie

jetzt denken „Macht ja nichts, ich kümmere mich selbst um die Lösungen, die ich zusätzlich brauche oder besser gebrauchen kann", übersehen Sie, dass die IT-Sicherheit nicht jede Form von IT im Unternehmen schützt.

Damit zum Beispiel eine Software automatisch aktualisiert wird, muss sie zum einen entsprechend eingestellt werden. Sie muss in der Patch-Verwaltung vorgesehen sein, und das Herunterladen der Patches oder Fehlerbehebungen muss an der Firewall des Unternehmens erlaubt werden, um nur einige Schritte zu nennen, die Administratoren machen. Nicht zuletzt müssen sie die Patches auf Schadsoftware prüfen. Installiert der Anwender seine Tools selbst, kann es passieren, dass die Antiviren-Software des Unternehmens sie nicht überprüft – mit massiven Folgen für Datensicherheit und Datenschutz.

Die Schatten-IT beginnt bereits bei einzelnen Apps

Die Schatten-IT beginnt nicht erst dann, wenn ein Mitarbeiter Online- oder Cloud-Dienste im Internet nutzt, die nicht betrieblich freigegeben sind. Es geht auch nicht nur um die Office-Lösung, die man auf dem betrieblich genutzten Notebook nachinstalliert, weil man diese oder jene Anwendung bevorzugt.

Bereits eine einzelne, kleine Smartphone-App ist Schatten-IT, wenn sie auf einem betrieblich genutzten Smartphone installiert wird, selbst wenn das mobile Endgerät dem Nutzer gehört, er es aber für das Unternehmen einsetzt.

Ist die eigenmächtig installierte App verseucht oder spioniert sie Daten aus, können schnell Firmendaten oder personenbezogenen Daten in falsche Hände gelangen. Betriebliche IT-Sicherheitslösungen werden das oftmals nicht verhindern können. Denn sie kontrollieren nicht ohne weiteres Apps, die der Nutzer in Eigenregie installiert.

Sprechen Sie sich mit der IT ab!

Denken Sie deshalb daran: Brauchen Sie andere IT-Lösungen oder kennen Sie Lösungen, die besser für Ihre Aufgaben geeignet erscheinen, dann sprechen Sie mit der Person, die Ihnen Ihre IT-Ausstattung übergeben hat, mit der IT-Administration oder mit Ihrer Führungskraft.

Alleingänge sind gefährlich (und können sogar arbeitsrechtliche Konsequenzen haben, wie der Beitrag ab Seite 3 zeigt). Im Schatten können Gefahren lauern, die man übersieht. Das gilt auch für die Schatten-IT. &

Welche Risiken bringt die Schatten-IT mit sich?

Frage: Die IT-Sicherheitslösungen Ihres Unternehmens schützen die gesamte IT. Stimmt das?

a. Ja, natürlich, sonst hätte die IT-Abteilung etwas falsch gemacht.
b. Nein. Es kann sein, dass die IT, die die Nutzer ohne Beteiligung der IT-Abteilung einsetzen, ungeschützt bleibt.

Lösung: Die Antwort b. ist richtig. Die sogenannte Schatten-IT ist der IT-Abteilung nicht bekannt. Deshalb kann sie sie im IT-Sicherheitskonzept auch nicht berücksichtigen. Von einem automatischen Schutz kann man nicht ausgehen.

Frage: Nutze ich eine Cloud-Lösung aus dem Internet, besteht keine Gefahr für die interne IT. Deshalb sind keine Freigaben für Cloud-Lösungen nötig. Stimmen Sie zu?

a. Für die IT-Sicherheit stimmt das. Denn Gefahren in einer Cloud sind ja nicht im betrieblichen Netzwerk vorhanden.
b. Nein. Denn jede IT-Nutzung kann zum Risiko werden, wenn die IT-Sicherheit nicht stimmt, auch bei Cloud-Lösungen.

Lösung: Die Antwort b. ist erneut richtig, denn Cloud-Lösungen sind als Teil der IT zu sehen. Gefahren aus der Cloud bedrohen die Daten des Unternehmens und können auch das interne Netzwerk betreffen. Ganz gleich, um welche IT es geht, ob Smartphone, App, Cloud oder etwas anderes, ohne Freigabe darf IT nicht eingesetzt werden. Eigenmächtig installierte oder genutzte IT gehört zur Schatten-IT, die das Datensicherheitskonzept des Unternehmens nicht ohne Weiteres berücksichtigt. Deshalb bedroht Schatten-IT den Datenschutz.

Achtung Datenschutz-Kontrolle!

Achtung Datenschutz-Kontrolle! Behörden in Niedersachsen und Nordrhein-Westfalen inspizieren Unternehmen im Hinblick auf die Übermittlung personenbezogener Daten in die USA

© K. Borchhardt/ www.miniansichten.de

Im Rahmen einer bundesweiten konzertierten Aktion der vorgenannten und acht weiteren Datenschutzaufsichtsbehörden, soll die Verarbeitung personenbezogener Daten außerhalb der Europäischen Union in 500 zufällig ausgewählten Betrieben eingedämmt werden.

Die ab sofort beginnenden Kontrollen intendieren den bis dato eher leichtfertigen bzw. ahnungslosen Umgang mit der Übermittlung ohne nötige Rechtsgrundlage einzudämmen. „Jedes Unternehmen muss ein vollständiges Bild über seine internationalen Datentransfers haben", äußerte sich vor diesem Hintergrund Barbara Thiel, die Landesbeauftragte für den Datenschutz Niedersachsen.

Das ebenfalls partizipierende bayerische Landesamt für Datenschutzaufsicht stellt auf seiner Internetseite den Audit-Fragebogen, welcher für die Prüfung verwendet wird, zur Verfügung. Dieser enthält 25 Fragen und verlangt detaillierte Stellungnahmen bezüglich folgender digitaler Dienstleistungen von Unternehmen außerhalb der EU, abzielend auf beliebte standardisierte cloudbasierte Unternehmenssoftware-Lösungen, betreffend:

- Fernwartung,
- Reisemanagement,
- Customer-Relationship-Management (z. B. Salesforce),
- Marketing (z.B. Integrate),
- Bewerbermanagement (z. B. iCIMS Talent Platform),
- Skill-Datenbanken (z. B. TrackStar),
- externe Speicherlösungen (z. B. Cloud-Dienste wie Dropbox),
- Kollaborationsplattformen (z. B. Doodle)
- Chat oder Messaging Systeme (z. B. WhatsApp oder Threema)
- Videokonferenzsysteme (z. B. Skype)
- Dokumenten Austauschsysteme (z. B. Google Drive)
- Unternehmenswikis (z. B. PBworks, Wikia)
- Ticketing- oder Supportsysteme (z. B. Freshdesk),
- Qualitätsmanagement (z. B. Orgavision),
- Risikomanagement oder weitere Compliance Produkte (z. B. IsoMetrix) und schließlich ebenfalls
- der Übermittlung von personenbezogenen Daten innerhalb einer Konzernmatrixstruktur in das EU-Ausland.

Vorangestellt ist dem Datenschutz-Audit der zehn Behörden darüber hinaus ein spezielles Kapitel bezüglich der Auslagerung von Datenverarbeitung in die USA, welches auch die hochaktuelle Datenübermittlung auf der Grundlage des neuen sog. Privacy Shield tangiert.

Unsere akuten Handlungsempfehlungen

Stellen Sie sicher, dass, falls Sie obige oder vergleichbare Dienste nutzen, eine Rechtsgrundlage gegeben ist. Diese kann insbesondere bei US-amerikanischen Unternehmen mithilfe folgender Instrumente auf eine rechtssichere Basis gestellt werden.

- Safe Harbor,
- EU-U.S. Privacy Shield,
- Standardvertrag,
- Standardvertrag mit Zusatzregelungen/Änderungen,
- Einzelvertrag,
- BCR sowie der
- Einwilligung der Betroffenen.

Insbesondere beim Privacy Shield Instrument, dem sog. EU-US-Datenschutzschild, sollten Sie sich proaktiv vergewissern, dass Ihr Dienstleister eine gültige Privacy-Shield-Zertifizierung besitzt. Die dazu notwendige Privacy-Shield-Liste des US Department of Commerce ist unter https://www.privacyshield.gov/list kostenlos einsehbar. &

Quellen und weiterführende Literatur

https://www.lda.bayern.de/de/index.html

https://goo.gl/qAFIkR

Mit Brief und Siegel: Neue Zertifizierungsangebote von Althammer & Kill

Immer mehr Stellen fordern Nachweise und Testate im Datenschutz und zur Umsetzung von IT-Sicherheitsmaßnahmen. Althammer & Kill hat das Zertifizierungsprogramm neu aufgestellt.

In der EU-Datenschutzg-Grundverordnung ist es fest verankert: Datenschutzsiegel, Prüfzeichen und datenschutzspezifische Zertifizierungsverfahren sollen gefördert werden, um die Einhaltung der gesetzlichen Vorgaben nachweisen zu können.

Schon heute fällt es aufgrund der Komplexität in Technik und Verarbeitungsvorgängen häufig schwer, Datenflüsse und technische Schutzmaßnahmen transparent zu bewerten. An dieser Stelle können Testate und Nachweise unabhängiger Stellen helfen, um die Einhaltung von Standards und rechtlichen Vorgaben zu bestätigen.

Konkrete Prüfgrundlage erforderlich

Ein Beispiel hierfür ist der Bereich Auftragsdatenverarbeitung. Für die Sicherheit in einem Rechenzentrum ist es nicht dienlich, wenn jeder Kunde einzeln im Rahmen einer Begehung als Vor-Ort-Kontrolle die Angemessenheit der getroffenen technischen und organisatorischen Maßnahmen überprüft.

Mithilfe eines Datenschutz-Siegels anhand dokumentierter Prüfkriterien kann der Betreiber des Rechenzentrums von einem unabhängigen Auditor ein Testat erwirken und seinen Kunden zur Verfügung stellen.

STIFTUNG DATENSCHUTZ

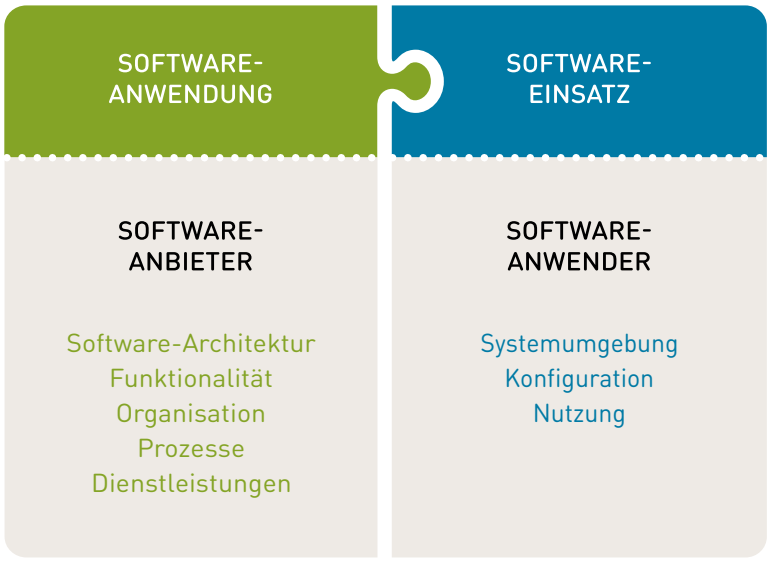
Althammer & Kill bietet derzeit zwei abgestufte Siegel im Bereich Datenschutz an: „Zertifizierter Datenschutz“ und „Geprüfter Datenschutz“. Beide Gütesiegel sind seit kurzem bei der Stiftung Datenschutz (siehe Download unter https://stiftungdatenschutz.org/aufgaben/zertifizierung/) verzeichnet und lassen sich in branchen- und produktspezifischen Ausprägungen beantragen, sozusagen maßgeschneidert für den jeweiligen Bedarf.

Anforderungen konkret benennen

Im Rahmen einer Zertifizierung muss im Einzelfall geprüft werden, welche Prüfungsgrundlage angemessen ist. Es lassen sich Unternehmen, Produkte oder Dienstleistungen begutachten, für die jeweils sehr unterschiedliche Anforderungen gelten. Ein Produkt oder eine Software wird beispielsweise nach Datenschutz-Eigenschaften innerhalb der Lösung bewertet. Ein Unternehmen wiederum sollte

darstellen, welche organisatorischen und technischen Maßnahmen zur Gewährleistung von Datenschutz und IT-Sicherheit angewandt werden.

Die jeweiligen Kriterien bestimmen die genaue Bezeichnung und Begründung auf den von Althammer & Kill vergebenen Siegeln mitsamt Urkunde und Zertifizierungsbericht.



Erfolgreiche Zertifizierung für Software-Lösung in der Sozialwirtschaft

Die Firma Connext Communication GmbH aus Paderborn hat ihre Software-Familie Vivendi auf Einhaltung von Datenschutz-Vorgaben überprüfen lassen. Im Rahmen der Audits und Workshops wurde ein bereits guter Umsetzungsgrad von Datenschutz-Maßnahmen bestätigt und weiter ausgebaut.

Als Grundlage für die detaillierte Überprüfung wurde in diesem Fall die „Orientierungshilfe Informationssysteme im Sozialwesen (OH-SOZ)“ herangezogen. Sie umfasst einen Kriterienkatalog, der auf den Datenschutzgesetzen von Bund, Land und Kirchen basiert. Grundlage ist eine in 2014 von den Aufsichtsbehörden veröffentlichte Orientierungshilfe für Krankenhausinformationssysteme, die auf die Belange der Sozialwirtschaft übersetzt wurde.

Datenschutz-Funktionen realisiert

In einem mehrmonatigen Prozess sind vielfältige Änderungen zur Verbesserung der Datenschutzkonformität in Connext-Vivendi eingeflossen. Im Oktober 2016 war es dann soweit: das Zertifikat für die Erfüllung der Hersteller-Vorgaben der OH-SOZ wurde erteilt und dem Connext-Geschäftsführer, Jörg Kesselmeier, übergeben. Er sieht darin einen weiteren Meilenstein in der Unternehmensentwicklung: „Die Zertifizierung gibt den Anwendern nun noch mehr Sicherheit beim Datenschutz. Dies ist ein klarer Mehrwert für Vivendi-Kunden.“

Für Einrichtungen und Träger in der Sozialwirtschaft lässt sich nun der datenschutzkonforme Einsatz von Vivendi ebenfalls überprüfen.

Solche Produkt-Zertifizierungen wird es in Zukunft häufiger geben: Mit der EU-Datenschutz-Grundverordnung gelten ab 2018 verschärfte Bedingungen im Datenschutz. Mit der Zertifizierung werden wesentliche Forderungen nach „Privacy by Design“ und „Privacy by Default“ gemäß Artikel 25 der DS-GVO schon heute erfüllt.

Neue Siegel für Stellung von Datenschutzbeauftragten und IT-Sicherheitsbeauftragten

Ab dem 2. Quartal 2017 können alle Kunden, bei denen Althammer & Kill den DSB oder den IT-SiBe stellt, das neue Siegel-Design auch als Nachweis für die Begleitung und Unterstützung im Bereich Datenschutz verwenden. Damit wird bestätigt, dass der von Althammer & Kill gestellte Datenschutzbeauftragte bzw. IT-Sicherheitsbeauftragte die gesetzlichen Vorgaben erfüllt und das Unternehmen für die laufende Begleitung und Kontrolle einen professionellen Dienstleister beauftragt hat. &

Termine

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

17.01.2017, Bielefeld
FHdD Webinar – IT-Compliance im Gesundheits- und Sozialwesen
Mit zunehmender Abhängigkeit von IT-Systemen müssen auch Unternehmen und Organisationen im NonProfit-Bereich den rechtskonformen und sicheren Betrieb von Hardware und Software gewährleisten.

23.-25.01.2017, Paderborn
Ausbildung IT-Sicherheitsbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft

15.02.2017, Paderborn
Privacy by Design
Datenschutz nimmt Anbieter und Administratoren stärker in die Pflicht

21.-23.02.2017, Paderborn
Ausbildung Datenschutzbeauftragte
Fokus Kirche, Non-Profits und Sozialwirtschaft

09.–10.03.2017, Eichstätt
Fachtagung Sozialinformatik
Das „Familientreffen" der Branche in Eichstätt

20.–24.03.2017, Hannover
CeBit 2017
Besuchen Sie uns in Halle 5, Stand G27. Wir freuen uns auf Ihren Besuch!

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

News

Aus unserem aktuellen Newsletter:

Achtung Datenschutz-Kontrolle!
https://www.althammer-kill.de/news-detail/achtung-datenschutz-kontrolle.html

Internet of Things: Schwachstellen am Beispiel IP-Kameras
https://www.althammer-kill.de/news-detail/internet-of-things-schwachstellen-am-beispiel-ip-kameras.html

Kopierverbot für Ausweise
https://www.althammer-kill.de/news-detail/kopierverbot-fuer-ausweise.html

Kosten von Datenpannen und Pflicht zur Selbstanzeige
https://www.althammer-kill.de/news-detail/kosten-von-datenpannen-und-pflicht-zur-selbstanzeige.html

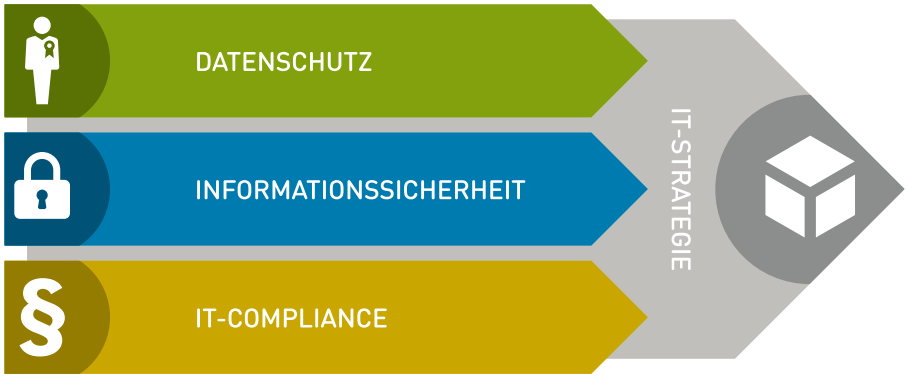
Keine Chance für CEO-Fraud, Ransomware und Co.
https://www.althammer-kill.de/news-detail/keine-chance-fuer-ceo-fraud-ransomware-und-co.html

Chrome warnt vor unverschlüsselten Websites
https://www.althammer-kill.de/news-detail/chrome-warnt-vor-unverschluesselten-websites.html

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

Althammer & Kill – Wir schützen Ihre Daten.

Althammer & Kill ist ein auf Datenschutz, Informationssicherheit und IT-Compliance spezialisiertes Unternehmen. Unsere Mitarbeiter sind zertifizierte Datenschutzbeauftragte, IT-Sicherheitsexperten, ausgebildete IT-Compliance-Beauftragte und IT-Berater.



Datenschutz

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

Informationssicherheit

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

IT-Compliance

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

IT-Strategie

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

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

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

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

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

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

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

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

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

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

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

Althammer & Kill GmbH & Co. KG

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

Hauptsitz Düsseldorf:
Neuer Zollhof 3 · 40221 Düsseldorf
Tel. +49 211 936748-0 · Fax -48

Standort Hannover:
Buchenhain 15 · 30938 Burgwedel
Tel. +49 5139 973949-0 · Fax -9

Mitglied im:

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