AUSGABE 3 / 2014

In dieser Ausgabe

Newsletter für Datenschutz und Informationssicherheit

audatis.INFO

audatis Datenschutz und Informationssicherheit | NEWSLETTER

Editorial

Gängige Handytarife enthalten zwar fast alle mittlerweile sog. „Datenflatrates“ aber bei genauerem Blick in die Vertragsinhalte sind diese „Flatrates“ auf ein max. Datenvolumen beschränkt. Danach fallen weitere Gebühren an oder die Übertragungsgeschwindigkeit wird gedrosselt. Daher nutzen wir im Café, am Flughafen oder im Hotel so gerne offene WLAN-Hotspots zum schnellen Surfen im Internet. Doch was muss man als Betreiber eines solchen Hotspots eigentlich beachten und wie sieht das auf Seite der Nutzer aus?

Die rechtlichen und technischen Aspekte haben wir in dieser Ausgabe für Sie zusammengetragen - als Wegweiser durch den WLAN-Dschungel.

Carsten Knoop
Geschäftsinhaber

WLAN-Hotspots ohne Angst vor Abmahnungen einrichten

Wir zeigen Ihnen wie Sie WLAN-Zugänge für Kunden und Gäste rechtssicher einrichten und als kostenlosen Service anbieten können, ohne sich dabei aufs Glatteis zu begeben.

(ST) Kostenfreie WLAN-Zugänge (Hotspots oder Access-Points) gehören mittlerweile zu einem guten Kundenservice dazu. Sie sind für Kunden, welche die Wartezeit zum Termin überbrücken möchten oder für Mitarbeiter, die in der Mittagspause ihre privaten E-Mails abrufen möchten, ein willkommener Anlaufpunkt. Hotspots bergen allerdings auch ein gewisses Risiko. Nicht nur für die Nutzer kann ein schlecht gesichertes Netzwerk gefährlich sein, sondern auch für den Anbieter.

Gefahren für WLAN Nutzer

Für die Nutzer kann der Hotspot zur Datenfalle werden. Kriminelle können am Nebentisch einen temporären Zugang eröffnen, bei dem sie die Kennung eines seriösen Anbieters verwenden und durch den kurzen Abstand zum Nutzer eine höhere Signalstärke aufweisen und dieser sich mit dem betrügerischen Netzwerk verbindet. Hierbei kommt es zu einem sogenannten „Man-in-the-Middle-Angriff“, bei dem der Täter den Datenverkehr manipuliert oder speichert, bevor die Daten an den regulären Kommunikationspartner (z.B. Webserver) weitergereicht werden. Die interessantesten Daten filtert der Täter in Echtzeit heraus und kann somit sofort in Aktion

… Fortsetzung von Seite 1 zur Einrichtung von WLAN-Hotspots

Wir zeigen Ihnen wie Sie WLAN-Zugänge für Kunden und Gäste rechtssicher einrichten und als kostenlosen Service anbieten können, ohne sich dabei aufs Glatteis zu begeben.

treten, indem er beispielsweise Accounts zu sozialen Netzwerken (Identitätsdiebstahl), Passwörter von E-Mail-Konten oder Daten zum Online-Banking abgreift und missbräuchlich verwendet.
Welche Maßnahmen Sie daher stets bei der WLAN-Nutzung beherzigen sollten, haben wir Ihnen im Kasten auf der nächsten Seite in 6 Schritten aufbereitet.

Gefahren für WLAN Anbieter
Für den Anbieter eines Hotspots kann es teuer werden, wenn der Zugang für den Austausch von strafrechtlich relevanten Daten wie illegalen Down- oder Uploads von Musik oder Filmen (sog. Filesharing) seitens der Nutzer missbraucht wird. Wer einen Internetanschluss hat, ist bisher dafür verantwortlich, was andere damit tun. Loggt sich also eine Person in das WLAN ein und bietet illegale Dateien zum Download an, haftet der Inhaber des Anschlusses. Ausgenommen davon waren bisher gesicherte WLAN-Anschlüsse.

Abmahnungen wegen UrhG
In den letzten Jahren hat sich in Deutschland eine ganze Abmahnindustrie entwickelt, die es sich zur Aufgabe gemacht hat, das Urheberrecht zu „verteidigen“ und bei Verstößen durch kostenpflichtige Abmahnungen ordentlich mitzuverdienen. Solche Abmahnungen liegen schnell bei mehreren hundert bis tausend Euro. Das Problem ist technisch gesehen ganz einfach: der auf den Anbieter zugelassene Internetzugang besitzt eine zumindest temporär eindeutige IP-Adresse, welcher alle Verstöße aus dem WLAN zugewiesenen werden. Eine Identifizierung der einzelnen Geräte und Nutzer ist nur bedingt möglich. Da der Anbieter des WLAN-Zugangs urheberrechtlich als sogenannter „Mitstörer“ eingeordnet wird, kann er haftbar gemacht werden.

Wie WLAN betreiben?
Nun stellt sich die Frage, wie der Anbieter seinen Nutzern den Service „Internetzugang“ anbieten kann ohne dabei das Risiko einzugehen, abgemahnt zu werden.

Variante 1: Hotspots
Ein einfacher Weg für den Anbieter ist es, die Verantwortung abzugeben. Mittlerweile haben sich am Markt Firmen wie „mein Hotspot“ oder die Telekom etabliert, die dem Anbieter einen Anschluss einrichten, das Risiko im Falle eines Missbrauchs übernehmen und für den Internetanschluss haften. Die Anbieter hoffen darauf, dass bei einer großen Anzahl von Kunden nur einige wenige letztendlich Opfer von Abmahnung werden und die Kosten damit gering bleiben.

Unsere Leistung

Wir beraten Sie gerne bei allen Fragen zum Einrichten und Betrieben von Hotspots und deren Absicherung. Auch VPN-Dienste stellen wir Ihnen gerne zum sicheren Surfen vor.

Oder sie sorgen mit einer einfachen, kostenfreien oder kostenpflichtigen Registrierung für eine eindeutige Identifizierung des Nutzers, der dann bei missbräuchlicher Nutzung belangt werden kann.

Auf unserer Internetseite finden Sie eine Liste von Anbietern für solche Hotspot-Dienste: [http://ds-its.eu/hotspot].

Variante 2: Proxy
Technisch möglich, aber wenig praktikabel ist die Nutzung eines Proxy-Dienstes. Ein Proxy ist eine Kommunikationsschnittstelle in einem Netzwerk und arbeitet als Vermittler, der auf der einen Seite Anfragen entgegennimmt, um dann über seine eigene IP-Adresse eine Verbindung zur anderen Seite herzustellen. Er kann damit die im WLAN des Anbieters vorhandenen Geräte gegenüber dem öffentlichen Netz pseudonymisieren (über sog. TOR-Netzwerke sogar faktisch anonymisieren). Die kostenlosen sind den kostenpflichtigen Diensten technisch gleichgestellt. Bei den kostenlosen Proxy-Diensten

6 Schritte sicherer WLAN-Nutzung

1. **Verschlüsselung:** Vor der Verbindung mit dem WLAN-Hotspot im Café, Hotel oder Flughafen sollten Sie daran denken, dass auch eine verschlüsselte Verbindung mit WEP, WPA und WPA2 nicht unbedingt sicher ist. Jeder Nutzer im gleichen Netzwerk kann Ihren Datenverkehr mitlesen.
2. **SSL-Verbindungen:** Egal ob Sie E-Mails lesen, auf Webseiten surfen oder sich irgendwo einloggen. Achten Sie auf eine verschlüsselte SSL-Verbindung (am https:// zu erkennen). Nur dann können Andere im gleichen Netzwerk nicht mitlesen, welche Daten Sie mit dem Internet austauschen. Auch Anwendungen und Apps sollten nur über SSL-Verbindungen eingerichtet werden.
3. **Sicherheitshinweise:** Sie sollten unbedingt die Sicherheitshinweise im Browser beherzigen und nicht auf https-Seiten surfen, die ein unsicheres Zertifikat melden. Dies kann ein Anzeichen für einen Man-in-the-middle-Angriff sein und ein Dritter dabei auch verschlüsselte Daten mitlesen.
4. **Kostenpflichtig ist nicht gleich sicherer:** Auch bei kostenpflichtigen Angebot sollten Sie daran denken, dass das Surfen im Netz deshalb nicht sicherer sein muss.
5. **VPN-Nutzen:** Wer sich vor Angriffen aus dem lokalen Netzwerk schützen möchte, sollte unbedingt eine VPN-Verbindung nutzen. Firmen stellen diese für ihre Mitarbeiter oft zur Verfügung. Hier erhalten Sie auch privat kostenlosen VPN-Zugang: [http://ds-its.eu/vpnlst]
6. **Ausloggen:** Nach Ende einer Sitzung sollten Sie sich bei Webdiensten immer ausloggen. Das schützt vor Session-Diebstahl.

sind jedoch starke Geschwindigkeitseinbußen zu erwarten. Preislich sind die kostenpflichtigen Proxys mit den oben genannten Hotspots vergleichbar, sie übernehmen allerdings keine Haftung und sind daher aus rechtlicher Sicht nicht zu empfehlen.

Variante 3: Virtuelle Netze

Virtuelle Netzwerke sind voneinander abgeschottete Bereiche in einem Netzwerk. Der Internet-Zugang wird dabei immer nur für eine bestimmte Zeit aktiviert und häufig einem namentlich bekannten Nutzer zugeordnet. Dieser Zugang erfolgt häufig über sogenannte Voucher (Zettel mit individuellen Zugangsdaten). Der Gast erhält diesen von dem Anbieter des WLAN und muss dabei meist seinen Namen (oder z.B. die Zimmernummer) angeben. Die Zeit läuft, sobald der Nutzer den Zugang aktiviert hat. Die Registrierung für eine Nutzung liegt ganz im Ermessen des Anbieters. In jedem Fall protokolliert das System, welcher Zugang wann und wie lange das WLAN genutzt hat. Zusätzlich existiert ein Filter, der die aufgerufenen Webseiten filtern kann. Diese Lösung wird häufig in Firmennetzwerken eingesetzt, bei denen regelmäßig eine Vielzahl an fremden Personen / Gästen im Netz aktiv sein möchte. Die Kosten liegen hier durch höheren Administrationsaufwand meist über den Kosten eines externen Hotspotanbieters.

Urteile aus der Praxis

Wir haben für Sie einige Urteile von deutschen Gerichten gesammelt, welche sich mit der Haftung bei Abmahnungen und Urheberrechtsverletzungen in Zusammenhang mit der WLAN-Nutzung auseinandersetzen:

- AG Koblenz 2014: Der Betreiber eines Hotel-WLANs haftet nicht für Filesharing - bei ausreichender Sicherung [http://ds-its.eu/wlan1]
- LG Düsseldorf 2008: Filesharing - WLAN-Netz muss zumutbar gesichert sein [http://ds-its.eu/wlan2]
- BGH 2010: Sommer unseres Lebens – Störerhaftung des WLAN-Inhabers [http://ds-its.eu/wlan3]

Die Prüfung der Abläufe und Auswahl von geeigneten Dienstleistern oder Formularen ist nicht immer trivial. Wir bieten hier Hilfestellung an.

Fazit

Für welche Lösung Sie sich entscheiden, bleibt Ihnen überlassen. Wichtig ist bei allen Aspekten und Alternativen, dass Sie als WLAN-Anbieter rechtlich abgesichert sind und die Kosten moderat bleiben, um Ihnen und Ihren Gästen eine möglichst reibungsfreie und einfache Internetnutzung sicher anbieten zu können.

Ausblick

Die Störerhaftung aufzuheben, ist übrigens auch ein erklärtes Ziel im Koalitionsvertrag. Dort heißt es, dass man die gesetzlichen Grundlagen für die Nutzung von offenen Netzen und deren Anbieter schaffen werde. In die gleiche Richtung hat sich im Juli 2014 auch Bundeswirtschaftsminister Gabriel geäußert, indem er Cafés und Hotels per Gesetz eine Erleichterung bieten möchte. Es bleibt abzuwarten, wann und in welcher Form dies geschieht.

Datenschutz am Arbeitsplatz - die täglichen Sicherheitsmaßnahmen

Datenschutz betrifft jeden. Vor allem am Arbeitsplatz sollten einige Grundregeln beachtet werden, damit man seine Daten im täglichen Berufsleben schützen kann.

(CK) Betrachtet man einen ganz normalen Büroarbeitsplatz, so bietet dieser bereits viele Möglichkeiten um ständig gegen geltende Datenschutzgesetze (z.B. Zugangs-, Zugriffs- und Weitergabekontrolle gem. § 9 BDSG) zu verstoßen und meist unbewusst alle Regelungen der IT-Sicherheit mit Füßen zu treten. Wir möchten auf die wesentlichen Maßnahmen hinweisen und damit für mehr Datenschutz und Sicherheit im Büro und Homeoffice sorgen.

Leerer Tisch oder „Clean Desk"
Unter der Bezeichnung „Clean Desk Policy" wird meist die Regelung (des Unternehmens) verstanden, dass bis zum Feierabend jeder Schreibtisch ordentlich aufgeräumt und von jeglichem Papier befreit werden muss. Das hat mehrere Vorteile aus verschiedenen Perspektiven und kann auch zu Hause gewinnbringend angewandt werden:

1. Es liegen keine Papierunterlagen mit personenbezogenen Daten auf dem Tisch, welche von jedem Besucher und Gast sofort eingesehen werden können bzw. Interesse wecken.
2. Sie werden effizienter arbeiten, weil Sie weniger Zeit mit der Ablage und dem Suchen verbringen.
3. Sie fühlen sich besser, weil der berüchtigte „Berg voll Arbeit" nicht schon morgens auf Sie wartet.

Umgang mit Papierunterlagen
In vermutlich jedem Büro gibt es - trotz des „papierlosen Büros" - auch heute noch viele Papierunterlagen. Von Rechnungen über Verträge bis hin zu anderen Dokumenten, die teilweise „nur" zum Lesen ausgedruckt werden. Häufig enthalten diese jedoch sensible oder personenbezogene Inhalte. Sie sollten schützenswerte Unterlagen also nicht lange in der Ablage liegen lassen sondern in einem Schrank wegschließen und schon gar nicht im Papierkorb entsorgen, sondern im Aktenshredder zerstören. Ab Sicherheitsstufe 4 genügt dieser auch allen Anforderungen des BDSG.

Verräterisches Telefon
Das Telefon ist von den meisten Schreibtischen nicht wegzudenken, gerade in Büros mit vielen Mitarbeitern kann dies jedoch zu besonderer Neugier führen. Sie sollten daher bei privaten Anrufen in der Anrufliste bzw. Wahlwiederholung die Nummern löschen, welche Sie anderen nicht preisgeben möchten. In der Telefonanlage oder der Abrechnung können diese jedoch auch auftauchen.

Unsere Leistung

Wir bieten Beratung bei der Auswahl passender Sicherheitsmaßnahmen und führen auch Datenschutzaudits in Ihrem Unternehmen durch, um Ihre Schwachstellen zu finden.

Elektronische Datenspeicher
Ob externe Festplatte, USB-Stick oder DVD. Häufig werden gerade größere Datenmengen zum Austausch oder für die Datensicherung auf diesen Datenträgern gespeichert. Wenn diese nicht ständig unter Verschluss sind oder auch einmal das Haus verlassen, sollten Sie die Inhalte dringend verschlüsseln. Dann kann Ihnen auch der Verlust oder Diebstahl des Datenträgers keinen Schaden anrichten. Zur Verschlüsselung eignen sich betriebssystemeigene Programme wie z.B. BitLocker oder Zusatzprogramme wie Truecrypt, Boxcryptor oder egoSecure.

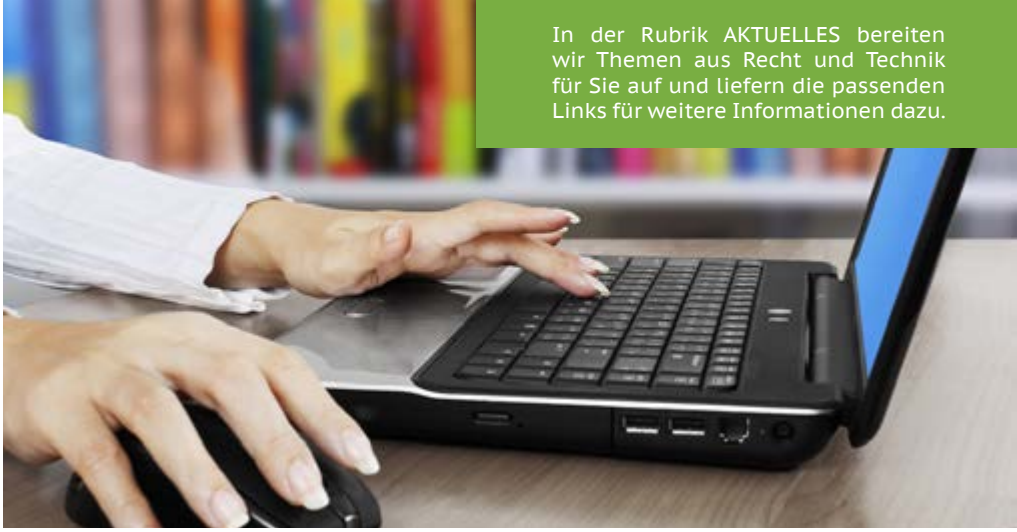
Der Computerarbeitsplatz
Wer an seinem Arbeitsplatz mit einem PC arbeitet, hat natürlich zahlreiche Regelungen zu beachten, um ein Mindestmaß an Sicherheit zu erreichen.

"Jeder Arbeitsplatz bietet zahlreiche Möglichkeiten zum Verstoß gegen Datenschutzgesetze. Durch einfache Maßnahmen lassen sich die Risiken jedoch in den Griff bekommen."

Wir haben Ihnen diese einmal ohne Anspruch auf Vollständigkeit aufgelistet:

- Beim Verlassen des Raumes den PC durch drücken von ⊞ + **L** sperren.
- Den Bildschirm so ausrichten, dass Dritte diesen nicht einsehen können.
- Niemandem (weder Kollege noch Administrator) das Passwort für Ihren persönlichen Benutzernamen mitteilen.
- Ein sicheres und komplexes Passwort verwenden (Klein- und Großbuchstaben, Sonderzeichen und Ziffern, min. 10 Zeichen lang, keine Tastaturabfolgen, Namen, Autokennzeichen, etc.).
- Passwörter nicht auf Zetteln, unter der Tastatur oder in der Schreibtischschublade aufbewahren.
- Keine fremden USB-Sticks anschließen (Infektion mit Schadsoftware möglich).
- Unverschlüsselte Datenträger nicht im Müll entsorgen, auch nicht defekte Datenträger, sondern sicher vernichten oder durch Gewalteinwirkung (z.B. Bohrmaschine) zerstören.
- Vertrauliche Daten nicht unverschlüsselt als E-Mail versenden (PGP oder S/MIME als E-Mail-Verschlüsselung verwenden oder die Anhänge vorher mit ZIP oder anderen Programmen verschlüsseln.
- Regelmäßige Updates der Software durchführen und den Virenschutz auf aktuellem Stand halten.
- Niemals ein Benutzerkonto mit administrativen Rechten zur normalen Arbeit nutzen (Schadsoftware hat dann die gleichen Rechte).

In der Rubrik AKTUELLES bereiten wir Themen aus Recht und Technik für Sie auf und liefern die passenden Links für weitere Informationen dazu.



AKTUELLES aus Recht & Technik

Recht auf Vergessenwerden
Der EuGH hat in seinem Urteil v. 13.05.2014 (Az.: C-131/1) die Basis für das Grundrecht auf Vergessenwerden geschaffen. Die Löschung der personenbezogenen Daten kann rein aufgrund des Zeitablaufs verlangt werden. Es ist unerheblich, ob die Information rechtmäßig oder rechtswidrig erhoben und gespeichert wurde. Genauso irrelevant ist die Frage, ob die Speicherung der Informationen zu einem Schaden führt. Allerdings bestehen dadurch verschiedene Grundrechtskonflikte (Europäisches Gemeinwohl, Eingriff in die Meinungs-, Kunst- oder Wissenschaftsfreiheit), deren Behebung erst in Ansätzen skizziert sind.
[http://ds-its.eu/eughverg]

Cyberkriminelle nutzen Antiviren-Webdienst „VirusTotal", um Schadcode zu verbessern
Nach Erkenntnissen eines Sicherheitsforschers nutzen Virus-Entwickler seit Jahren Googles Webdienst „VirusTotal", um ihren Code an Antiviren-Programmen vorbeizuschmuggeln. Eigentlich ist „VirusTotal" darauf ausgelegt, den Opfern zu helfen. VirusTotal.com ist ein kostenloser Service, der es Nutzern ermöglicht Dateien einzureichen, die mit Schadsoftware infiziert sein könnten. Der Dienst scannt diese dann mit mehreren Antiviren-Engines und meldet die Ergebnisse an den Nutzer. Von Kriminellen wird dieser Dienst ebenfalls rege genutzt, um neuen Schadcode mit wenig Aufwand gegen viele Virenschutzlösungen zu testen.
[http://ds-its.eu/virust]

Wirkung von Betriebsvereinbarungen auf den Datenschutz
Häufig muss das Bundesarbeitsgericht (BAG) Betriebsvereinbarungen, die die Kontrolle von Beschäftigten regeln, überprüfen. Seit etwa zehn Jahren hat das BAG bei offenen Videoüberwachungen z.B. ausdrücklich eine Prüfung auf Verhältnismäßigkeit durch die Betriebsparteien für notwendig erachtet. In einem neueren Urteil v. 9.07.13 (Az. 1 ABR 2/13) misst es nun auch eine nicht automatisierte Erhebung von Daten an diesem Maßstab. Das BAG prüfte die Zulässigkeit einer Taschenkontrolle, die in einer Betriebsvereinbarung (BV) geregelt wurde und legte dabei den Maßstab des § 75 Abs. 2 Betriebsverfassungsgesetz (BetrVG) zugrunde.
[http://ds-its.eu/bagbv]

Informationen zu individuellen Inhouse- und Mitarbeiterschulungen

audatis Training

Wir bieten Ihnen bundesweit Inhouse- und Mitarbeiterseminare zu aktuellen Themen aus Datenschutz und Datensicherheit an. Individuell auf Ihr Unternehmen abgestimmt.

Haben Sie schon Ihre diesjährige Mitarbeiterschulung zum Datenschutz durchgeführt? Oder steht eine Maßnahme zur Sensibilisierung von Mitarbeitern auf der Agenda?

(JB) Der Gesetzgeber verlangt z.B. in § 4g BDSG, dass alle Beschäftigten in Behörden und Unternehmen regelmäßig mit den Anforderungen des Datenschutzes vertraut gemacht werden. Häufig fehlt es den Datenschutzbeauftragten oder anderen Referenten am nötigen Fach-Know-How, der Zeit oder an Präsentationserfahrung. Das Resultat ist, dass die Teilnehmer schnell mit Gesetzestexten gelangweilt werden und nicht umfangreich genug sensibilisiert sind.

Die beste und effektivste Alternative ist eine spannende Schulung Ihrer Mitarbeiter mit aktuellen Themen und einem hohen Nutzwert sowohl für das Unternehmen als auch für die teilnehmenden Mitarbeiter.

Themenbausteine

Wir haben daher zielorientierte Formate zur Mitarbeiterschulung konzipiert, die sich nach Arbeitsbereichen gliedern. Die Formate sind als Basisschulung oder fachliche Aufbauschulung aus folgenden Themen wählbar:

- Basisschulung für alle Mitarbeiter / Azubis
- Callcenter / Support
- Personalverwaltung / Personalentwicklung
- Marketing / Vertrieb
- Gesundheitswesen / Arztpraxen / Zahnarztpraxen
- Buchhaltung / Controlling
- EDV / IT-Administration

Die Schulungen werden durch „Live Hackings“ zu aktuellen Themen wie Smartphones, IT-Sicherheit, Cloud, etc. ergänzt, um einen gewissen Erlebnisfaktor zu garantieren.

Jedes Modul dauert ca. 2 Std. und ist damit auch zeitlich in den Arbeitsalltag gut integrierbar. Mit unseren Teilnahmebescheinigungen können Sie die durchgeführten Schulungen für Aufsichtsbehörden, Kunden, Patienten und Geschäftspartner dokumentieren.

Offene Seminare / Webinare

Wir bieten einige Themen als offene Seminare für alle Interessierten und vor allem kleinere Unternehmen an. Außerdem werden ausgewählte Themen als Webinar angeboten, damit Sie unabhängig vom Ort und ohne Reisekosten Ihre Weiterbildungsanforderungen erfüllen können.

Seminare bei Ihnen im Haus

Alle unsere Seminare können Sie auch für Ihre eigene Inhouse-Schulung buchen. Dabei lohnt sich die Investition meist schon ab 4 Teilnehmern und hat ausschlaggebende Vorteile:

- Inhalte an Ihr Corporate Design angepasst
- Keine Reisezeit und Reisekosten Ihrer Mitarbeiter
- Genügend Zeit für Fragestellungen aus dem eigenen betrieblichen Ablauf

Melden Sie sich gerne bei uns.

Der audatis Shortlink

Sie finden weitere Informationen zu den Veranstaltungen auf der rechten Seite und die jeweiligen Veranstalter über unseren Shortlink-Service:

http://ds-its.eu/SHORTCODE

*Dabei ersetzen Sie den **SHORTCODE** einfach durch den entsprechenden Wert in [**eckigen Klammern**], welcher unter jedem Veranstaltungshinweis steht und geben diesen in die Adresszeile Ihres Internet Browsers ein.*

Weiterbildung ist ein wichtiger Bestandteil der betrieblichen und persönlichen Entwicklung. Hier listen wir qualitativ hochwertige Angebote auf.

Veranstaltungstermine September - Dezember 2014

Ausgewählte Seminare und Fachtagungen zu den Themen Datenschutz und Datensicherheit von September bis Dezember 2014 im gesamten Bundesgebiet.

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit / Shortlink
16.09. bis 17.09.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	Köln, 09:00 - 17:00 Uhr [itsds]
29.09. bis 01.10.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Köln, 10:00 - 17:00 Uhr [semdsb]
07.10. bis 08.10.	Seminar: Datenschutzmanager (TÜV Rheinland)	Frankfurt, 09:00 - 17:00 Uhr [semdsm]
07.10. bis 09.10.	it-sa IT-Security Messe und Kongress (Messe Nürnberg)	Nürnberg, 09:00 - 17:00 Uhr [mesits]
21.10. bis 23.10.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Stuttgart, 10:00 - 17:00 Uhr [semdsb]
03.11. bis 05.11.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Hannover, 10:00 - 17:00 Uhr [semdsb]
06.11.	Seminar: Datenschutz im Personalwesen (aconso Academy)	München, 09:00 - 14:00 Uhr [sempds]
19.11.	Seminar: Datenschutz in der Zahnarztpraxis (audatis Training)	Bad Salzuflen, 14:00 - 19:30 Uhr [semdent]
26.11. bis 27.11.	Workshop: Grundlagen der IT-Forensik praxisnah (audatis Training)	Hannover, 09:00 - 17:00 Uhr [wksitf]
01.12.	Webinar: Aktuelles im Datenschutz (audatis Training)	Online, 09:00 - 16:00 Uhr [wbdsa]
10.12.	Seminar: Datenschutz für IT-Leiter und IT-Experten (audatis Training)	Berlin, 09:00 - 17:00 Uhr [dsitl]

Nächstes Mal

Die nächste Ausgabe des audatis.INFO Newsletters für Datenschutz und Informationssicherheit erscheint Ende Q4 / 2014.

Einige Auszüge aus den Themen der nächsten Ausgabe:

- Was Software für den Datenschutzbeauftragten leistet
- Personalausweise kopieren
- Aktuelle Veranstaltungen zu Datenschutz und Datensicherheit

Haben Sie eigene Themenvorschläge für die nächste(n) Ausgabe(n), dann freuen wir uns über Ihre Post: newsletter@audatis.de

Impressum

audatis® - Datenschutz und Informationssicherheit
Consulting | Training | Services
Inh. Carsten Knoop

Wittekindstr. 3
32051 Herford

Redaktion
V.i.S.d.P. Carsten Knoop (CK)
Jill Bohrenkämper (JB)
Sebastian Treptow (ST)

Erscheinungsweise
4 x jährlich

Haftung und Nachdruck
Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Jeglicher Nachdruck, auch auszugsweise, ist nur mit ausdrücklicher Genehmigung der Redaktion gestattet.

Arbeitshilfen zum Datenschutz online

(CK) Vielen Datenschutzbeauftragten und Unternehmensverantwortlichen geht es ähnlich: das Bundesdatenschutzgesetz (BDSG) und andere Datenschutzgesetze sind nicht immer einfach zu verstehen und bei der Umsetzung der notwendigen Maßnahmen bleiben häufig Fragen offen.

Darum haben wir eine kommentierte Version des BDSG sowie anderer Gesetze zum Datenschutz als Arbeitshilfe in Print und PDF herausgegeben, in welcher wir die wesentlichen Inhalte allgemeinverständlich erklären und Umsetzungshinweise geben.
[http://ds-its.eu/ahdsg]

Ergänzend dazu haben wir zahlreiche kostenlose und kostenpflichtige Checklisten, Muster und Vorlagen erstellt, welche wir Ihnen gerne zur Verfügung stellen. In der „Arbeitshilfe Datenschutzgesetze“ werden diese direkt mit Shortlink und QR-Code verknüpft und passend zum jeweiligen Paragraphen beschrieben. Alternativ können diese aber auch direkt online über folgenden Shortlink eingesehen und heruntergeladen werden.
[http://ds-its.eu/checkds]

Wir möchten Ihnen damit zu wesentlichen Themen des Datenschutzes einfache und praxisnahe Hilfestellungen geben und freuen uns natürlich über Ihre Rückmeldung und Verbesserungsvorschläge. Melden Sie sich gerne auch bei Fragen zur Dokumentennutzung.

Carsten Knoop
Geschäftsinhaber, Datenschutzauditor
Fon: 05221 85496 - 90
Mail: carsten.knoop@audatis.de

Jill Bohrenkämper
Assistentin der Geschäftsleitung
Fon: 05221 85496 - 92
Mail: j.bohrenkaemper@audatis.de

Sebastian Treptow
Wirtschaftsjurist, Datenschutzbeauftragter
Fon: 05221 85496 - 93
Mail: s.treptow@audatis.de