AUSGABE 1 / 2014

In dieser Ausgabe

Newsletter für Datenschutz und Informationssicherheit

audatis.INFO

audatis Datenschutz und Informationssicherheit | NEWSLETTER

Editorial

Nachdem uns der Winter ja erst etwas später besucht, nutzten wir die kalten Tage und haben an unserem Newsletter gearbeitet.

In dieser Ausgabe haben wir Ihnen unsere erste Auflistung von Webhosting-Anbietern aus Sicht des Datenschutzes mit Bezug auf die Auftragsdatenverarbeitung und den Serverstandort mitgeliefert. Diese wird zukünftig auf unserer Webseite weitergeführt.

Genießen Sie die winterlichen Temperaturen und lesen Sie unseren Newsletter doch bei einer Tasse heißem Tee oder Kaffee.

Unser Newsletter ist für Sie gedacht, daher freue ich mich auch über Ihre Anregungen für neue Themen.

Carsten Knoop
Geschäftsinhaber

Auftragsdatenverarbeitung und Webhosting - geht das?

Wer eine Internetseite betreibt, möchte meist Daten seiner Nutzer verarbeiten. Doch wie sieht es mit dem vertraglichen Datenschutz bei deutschlands Webhostern aus?

(CK) Fast alle Betreiber von Internetseiten erheben, verarbeiten oder nutzen personenbezogene Daten ihrer Besucher. Das beginnt bei der Web-Analyse mittels IP-Adressen, wobei man sich hier noch streiten kann, ob überhaupt personenbezogene Daten nach dem Bundesdatenschutzgesetz (BDSG) vorliegen. Geht weiter über Daten die man in Kontaktformularen eintragen kann und die auf dem Server des Webhosters gespeichert werden und endet meist bei Online-Shops und anderen Web-Applikationen, wo nicht nur Mailadressen und Namen, sondern häufig auch Kontakt- und Adress- oder sogar Zahlungsdaten gespeichert werden. Das es sich hierbei um personenbezogene Daten handelt (siehe §3 Abs. 1 BDSG) wird wohl niemand abstreiten. Oder doch?

Datenschutz und Webhoster

Einige Webhoster verneinen wehement die Aussage, sie würden eine Verarbeitung personenbezogener Daten (sog. Auftragsdatenverarbeitung oder ADV) im Namen ihrer Auftraggeber durchführen. Dabei liegt das Hauptrisiko auch garnicht bei den Webhostern, sondern bei den Betreibern der Internetseiten. Denn diese müssen sich die Frage stellen, mit welcher Rechtsgrundlage

… Fortsetzung des Artikels von Seite 1 zur ADV bei Webhostern

Wer eine Internetseite betreibt, möchte meist Daten seiner Nutzer verarbeiten. Doch wie sieht es mit dem vertraglichen Datenschutz bei deutschlands Webhostern aus?

sie überhaupt personenbezogene Daten auf den Servern anderer Unternehmen erheben oder speichern dürfen. Mangels Einwilligung kann hier zumindest für deutsche Firmen regelmäßig nur eine Auftragsdatenverarbeitung (ADV) nach §11 BDSG herangezogen werden. Datenschutzfachleute sind sich hierüber auch einig. Durch diese ADV wird der Webhoster (vorher als Dritter bezeichnet) nämlich in den Verantwortungsbereich des Betreibers „integriert" und muss sich nun an die Weisungen des Auftraggebers zum Datenschutz halten.

Der Praxisfall

In der Praxis ist das Weisungsrecht bei einem großen Dienstleister natürlich etwas problematischer umzusetzen, doch stellt der Gesetzgeber hier einige Anforderungen auf, die erfüllt werden müssen, um eben diesen §11 BDSG nutzen zu können. Alternativ wäre eine Datenverarbeitung beim Webhoster nur mit Einwilligung der betroffenen Besucher/Kunden möglich und die Verantwortung für Datenpannen etc. ginge mit der Datenübermittlung zunächst auf den Webhoster über.

Absicherung des Betreibers

Um sich rechtlich abzusichern hat der Betreiber somit defakto kaum eine andere Möglichkeit, als eine Vereinbarung zur Auftragsdatenverarbeitung mit dem Webhoster abzuschließen, in der die gesetzlichen Anforderungen berücksichtigt werden und für welche eine, wie auch immer geartete, Prüfung regelmäßig dokumentiert wird. Die Webhoster haben aber erfahrungsgemäß nur selten „Lust" auf eine solche Vereinbarung - alleine schon wegen des Aufwands - und agumentieren damit, dass sie gar keine Verarbeitung im Auftrag durchführen würden. Doch was machen sie sonst, wenn sie dem Kunden Datenbanken, Online-Shops und Webspace zur Verfügung stellen und auf diesen im Zweifelsfall auch Zugreifen können?

Ausweg für die Betreiber

Da es für viele Betreiber von Internetauftritten schon aufwändig genug ist, den passenden Webhoster anhand von zahlreichen Kriterien und Preisen zu ermitteln, macht es das Thema Auftragsdatenverarbeitung nicht einfacher. In unserer rechts abgedruckten Liste mit *9 Schritten zu datenschutzkonformem Webhosting* haben wir die notwendigen Punkte aufgelistet, bei denen natürlich auch der Standort der Server und die IT-Sicherheit eine Rolle spielen.

Musterlösungen

Da das Problem der ADV zumindest den größeren Hostinganbietern bekannt ist, haben diese im Rahmen ihrer Compliance-Aktivitäten meist einen Standard- oder Mustervertrag zur Auftragsdatenverarbeitung ausgearbeitet, welchen sie den Kunden anbieten können. Damit kann zumindest der rechtlich notwendige Teil einfach abgearbeitet werden. Bleibt noch die Prüfung und Dokumentation übrig.

Prüfung und Dokumentation

Häufig lassen sich Betreiber von Rechenzentren und Webhoster von externen, unabhängigen Stellen prüfen und können diese Zertifikate oder Testate zur Verfügung stellen, was für den Betreiber ebenfalls als Prüfung ausreichen kann, sofern der Prüfungsinhalt passt. Bekannte Normen sind hier häufig ISO 27001 oder BSI Grundschutz sowie diverse Datenschutz-Zertifikate von verschiedenen Anbietern. Die Dokumentation ist dann dem Betreiber selbst überlassen. Aber auch hier gibt es Hilfe in Form von Vorlagen, Checklisten und Software-Tools.

Die Ergebnisse unserer Anbieterbefragung gibts auf Seite 3.

Unsere Leistung

Wir können Sie bei der Auswahl, Prüfung und Dokumentation von Dienstleistern und Auftragsdatenverarbeitern aus Sicht des Datenschutzes und der IT-Sicherheit beraten.

9 Schritte zu BDSG konformem Hosting

1. **Identifikation der zu verarbeitenden Daten:** Welche Daten werden im zukünftigen System erhoben, verarbeitet oder genutzt?
2. **Klassifikation der Daten:** Handelt es sich um personenbezogene Daten? Vielleicht sogar um nach §42a BDSG besonders zu behandelnde Daten (z.B. Kontodaten)?
3. **Auswahl des Anbieters:** Bei der Auswahl des Dienstleisters muss die technische Leistungsfähigkeit berücksichtigt werden.
4. **Standortwahl des Anbieters:** Wo der Anbieter seinen Sitz hat und wo die Daten wirklich verarbeitet werden (Rechenzentrum) spielt ebenfalls eine Rolle. Bleiben diese in Deuschland oder der EU?
5. **Vertragliche Vereinbarungen:** In den AGB ist meist nicht viel zu finden, was die Anforderungen des §11 BDSG auch nur annähernd trifft. Daher sollte die Frage nach einem Vertragsmuster zur ADV gestellt werden.
6. **Festlegung von Maßnahmen:** Die notwendigen techn. und org. Maßnahmen nach §9 BDSG sollten im ADV-Vertrag stehen.
7. **Regelmäßige Prüfung:** Legen Sie fest, wie eine Prüfung erfolgen soll bzw. wer diese macht oder ob ein Zertifikat / Testat ausreicht.
8. **Dokumentation:** Die Prüfung muss dokumentiert werden, auch wenn Sie nur eine „Papier-Prüfung" durchführen.
9. **Notfallplan:** Was passiert bei Angriffen auf Ihre Daten und wer informiert Sie bzw. andere darüber?

Probleme bei der Anbieter auswahl, Vertragsgestaltung oder Prüfung? Wir helfen Ihnen gerne persönlich weiter: info@audatis.de

ADV-Übersicht Webhosting '14

Die Auswahl an Anbietern im Bereich Webhosting ist zwar groß, dafür fällt die Entscheidung für eine datenschutzkonforme Lösung aber leichter.

Anbieter	Webseite	ADV	Standort	Hosting
1&1 Internet AG	1und1.de	--	DE	ab 3,99 €
1blu AG	1blu.de	--	DE	ab 4,90 €
Abonda - ProviderWeb	abonda.de	--	DE	ab 1,00 €
Alfahosting GmbH	alfahosting.de	++	DE	ab 0,99 €
All-inkl.com Neue Medien Münnich	all-inkl.com	++	DE	ab 4,95 €
BSB Service GmbH	server4you.de	--	EU, WE	ab 4,85 €
BUSYMOUSE Business Systems GmbH	busymouse.de	++	DE	ab 9,99 €
Contabo GmbH	contabo.de	--	DE	ab 2,99 €
Deutsche Telekom AG	t-online.de	--	DE	ab 4,95 €
domainfactory GmbH	df.eu	--	DE	ab 1,15 €
evanzo e-commerce GmbH	evanzo.de	--	DE	ab 3,99 €
FLATBOOSTER GmbH	flatbooster.com	--	DE	ab 1,25 €
goneo Internet GmbH	goneo.de	--	DE	ab 1,95 €
Greatnet.de GmbH	greatnet.de	--	DE	ab 2,90 €
Hetzner Online AG	hetzner.de	0	DE	ab 1,90 €
Host Europe GmbH	hosteurope.de	++	DE	ab 3,99 €
ISPpro Internet KG	euserv.de	--	DE	ab 1,99 €
Mittwald CM Service GmbH & Co. KG	mittwald.de	++	DE	ab 4,99 €
Strato AG	strato.de	++	DE	ab 2,99 €
TwoolT GmbH	serverway.de	--	DE	ab 1,90 €
WebhostOne GmbH	webhostone.de	--	DE	ab 1,50 €

Unsere ADV-Übersicht der Webhosting-Anbieter beinhaltet nur Firmen mit Sitz in Deutschland und hat keinen Anspruch auf Vollständigkeit.

Wir haben neben dem Umgang mit dem Thema: Verarbeitung personenbezogener Daten im Auftrag (ADV) gem. §11 BDSG auch die Serverstandorte sowie den günstigsten Hostingpreis / Monat ohne Berücksichtigung von Sonderkonditionen angegeben.

Die Angaben stammen von den Webseiten der Anbieter oder aus direkten Anfragen bei diesen.

Stand: 31.01.2014
(alle Angaben ohne Gewähr)

Legende ADV:

--	nicht möglich
0	kostenpflichtig mögl.
++	kostenfreie Vorlage

Legende Standort:

DE	in Deutschland
EU	in der EU / EWR
WE	weltweit verteilt

[http://ds-its.eu/advlist]

Der Nutzer als Detektor für Sicherheitsvorfälle und Datenklau

Moderne IT-Sicherheitslösungen unterstützen uns dabei, Internetattacken und Datenpannen möglichst frühzeitig zu erkennen. Doch es kommt auch auf den Benutzer an …

(WK) Wenn Ihr Antivirenprogramm Alarm schlägt, ist immer Vorsicht angesagt. In den meisten Fällen wurde tatsächlich ein gefährliches Schadprogramm entdeckt. Manchmal aber liegt auch ein guter Virenschutz falsch und verdächtigt eine harmlose Datei. Sie als Nutzer sollten trotzdem jede Warnung und Alarmmeldung ernst nehmen und sich so verhalten, wie es Ihr Unternehmen für den Fall einer Virenwarnung vorsieht. Manchmal aber übersehen Sicherheitslösungen mögliche Gefahren und tatsächliche Attacken. Hier sind Sie als Nutzer gefragt, die Augen offen zu halten.

Gefahrendetektor: Nutzer

Keine noch so gute Software kann es mit der menschlichen Intelligenz aufnehmen, weder heute und wahrscheinlich auch nicht in Zukunft. Eine Sicherheitslösung kann immer nur auf Basis der Regeln reagieren, die in der Anwendung hinterlegt sind. Selbst die Analysen, die verdächtiges Verhalten von Dateien und Programmen (Heuristik) entdecken und bewerten, arbeiten immer auf einer definierten Grundlage.

Neuartige Angriffe stellen für technische Lösungen deshalb immer eine große Herausforderung dar. Das trifft natürlich auch für uns Nutzer zu. Doch wir können mit unserem Gespür für mögliche Risiken zur Gefahrenabwehr beitragen.

Vorsicht ohne Übertreibung

Nun sollen Sie natürlich nicht immer gleich einen Angriff vermuten, wenn etwas scheinbar Ungewöhnliches am PC, Smartphone oder Drucker passiert. Aber es ist wichtig, vorsichtig und aufmerksam zu sein, denn auch bei installierter und aktivierter Sicherheitssoftware könnten Angreifer versuchen, personenbezogene Daten einzusehen, zu manipulieren und zu stehlen.

Ein Gespür für mögliche Anzeichen eines Angriffs oder einer Sicherheitspanne können Sie entwickeln, indem Sie sich angewöhnen, auf Vorkommnisse zu achten, die ein Alarmzeichen sein können, aber nicht müssen.

1. Dateien sind versteckt oder wurden verschoben:

- Wenn Sie zum Beispiel feststellen, dass eine von Ihnen erstellte Datei plötzlich an anderer Stelle im Netzwerk liegt und Sie sie nur noch über eine Suche finden, könnte dahinter eine Ihnen nicht bekannte Maßnahme der Systemadministration stecken, zum Beispiel im Rahmen einer Reorganisation.
- Es könnte aber auch ein unerlaubter Zugriff eines Dritten vorliegen. Fragen Sie deshalb zur Sicherheit nach, wenn Ihre Dateien plötzlich wandern.

2. Das Passwort funktioniert nicht mehr:

- Vielleicht stellen Sie fest, dass eines Ihrer Kennwörter nicht mehr gültig zu sein scheint. Dann könnte aus Sicherheitsgründen ein Zurücksetzen der Passwörter erfolgt sein, oder Sie haben vergessen, gemäß Passwortrichtlinie ein neues Passwort zu wählen. In aller Regel wären Sie dann aber zuerst intern informiert worden.

"Alleine der Einsatz von Sicherheitslösungen bietet keine ausreichende Sicherheit im Unternehmensnetzwerk. Der aufmerksame Nutzer und fähige Administrator sind ebenso wichtig."

Unsere Leistung

Wir bieten forensische Analysen an, um Manipulationen und Datenklau zu identifizieren und gerichtsverwertbar aufzubereiten. Außerdem helfen wir bei Präventionsmaßnahmen.

- Möglich ist aber auch, dass ein Angreifer Ihr Benutzerkonto geknackt hat und Sie nun aussperrt, indem er ein neues Passwort vergeben hat. Um dieses Risiko nicht einzugehen, sollten Sie Passwortprobleme, die sich nicht offensichtlich erklären lassen, an Ihre Systemadministration melden.

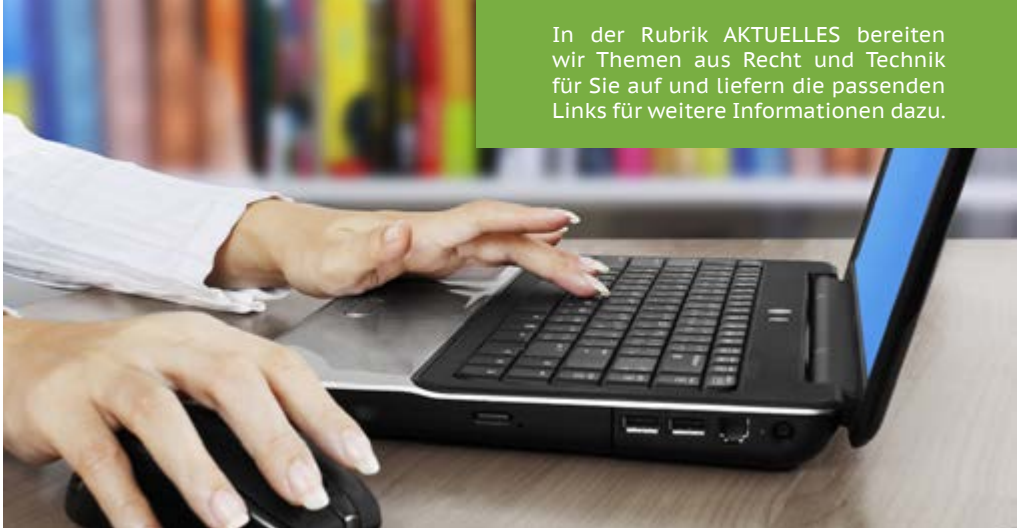
3. Weitere Anzeichen für Angriffe könnten sein:

- Plötzliche Veränderungen an Ihren Dateien, die Sie sich nicht erklären können.
- E-Mails im Gesendet-Ordner, die nicht von Ihnen stammen.
- Veränderungen an Einstellungen und Optionen bei Software und Geräten, die Sie sich nicht erklären können.
- Unerklärliche Fehler beim Versuch der Benutzeranmeldung.
- Unerwartete, gehäufte Störungen bei Ihren Geräten.

Schnelle Reaktionen

Damit die Folgen eines möglichen IT-Sicherheitsvorfalls so gering wie möglich bleiben, sind im Verdachtsfall schnelle, aber besonnene Reaktionen wichtig. Es sollte nicht so sein, dass eine Datenpanne im Unternehmen erst auffällt, wenn sich die betroffenen Kunden oder Nutzer beschweren. Daher ist ein vorher festgelegtes Verfahren bei sog. „Incidents" sinnvoll.

Wenn Sie denken, dass etwas nicht stimmt und vielleicht ein Angriff oder eine Datenpanne vorliegen könnte, melden Sie dies der Systemadministration oder dem Datenschutzbeauftragten.



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

Kein umfassender Auskunftsanspruch gegen Schufa

Der Bundesgerichtshof (BGH) hat nun im Urteil (VI ZR 156/13) entschieden, dass die Schufa keine Auskunft über die Gewichtung der Kriterien für ein Scoring liefern muss. Ausgangspunkt war die gescheiterte Autofinanzierung der Klägerin. Mit ihrer Revision hatte sie ihr Verlangen weiterverfolgt, hinsichtlich einzelner Scorewerte Auskunft darüber zu erhalten, welche Merkmale zur Scoreberechnung in welcher Gewichtung eine Rolle spielen. Dabei geht es im Kern um eine Auslegung der Vorschrift des §34 Abs. 4 S. 1 Nr. 4 BDSG. Hier muss der Betroffene grundsätzlich über das Zustandekommen und die Bedeutung der Wahrscheinlichkeitswerte im Einzelfall und nachvollziehbar in allgemein verständlicher Form informiert werden. Jedoch eben nicht die Berechnungsformel offenlegen, da sich diese auf ein Geschäftsgeheimnis bezieht.
[http://ds-its.eu/bgh15613]

Kopien des Personalausweises

Das Verwaltungsgericht Hannover (10 A 5342/11) hat bestätigt, dass es sich bei dem pauschalen Kopieren bzw. Einscannen und der anschließenden Speicherung von Personalausweisen um eine unzulässige Praxis handelt. Geklagt hatte eine Logistikdienstleister, der für mehrere tausend Fahrer u.a. von Speditionen, Fahrzeuge bereitstellt und die Personalausweise der Fahrer beim Abholen eingescannt und auf einem eigenen Rechner abgespeichert hatte.
[http://ds-its.eu/perso]

BankingTrojaner nutzt ausgeblendete Dateieindungen aus

Seit Anfang des Jahres wird über gefälschte Rechnungs- und Überweisungs-Mails ein Banking-Trojaner verbreitet. Die E-Mails sind in guter deutscher Sprache verfasst und geben vor, Rechnungen der Telekom, Vodafone oder Überweisungsdetails der Volksbank zu enthalten. Auffällig ist, dass sich die E-Mails an echte Rechnungsmails anlehnen und sowohl Text als auch Formatierung imitieren. Die heruntergeladene Datei weist die Endung **.pdf.exe** auf. Es wird also darauf gehofft, dass der Benutzer die EXE-Datei selbst ausführt, da Windows standardmäßig die Dateiendungen ausblendet. Hier heißt es nicht Klicken!

Neues Webinar zur Sicherheit von Content-Management-Systemen

Unser neustes Webinar für zeitgemäße Weiterbildung von Web-Administratoren liefert aktuelle Informationen und wichtige Hinweise zur Absicherung von webbasierten CMS.

(JB) Mit diesem Webinar soll den Administratoren und Verantwortlichen das Hintergrundwissen zu Angriffstechniken und grundlegendes Handwerkszeug zu Abwehrmaßnahmen an praktischen Fallbeispielen vermittelt werden. Um die webbasierten CMS-Anwendungen wie z.B. Wordpress, Joomla oder Typo3 bzw. andere oder eigene Systeme und damit auch die Daten Ihres eigenen Unternehmens oder der Nutzer schützen zu können, wird das Wissen der Angreifer benötigt.

Ohne Reisekosten und -zeit
Da sich die Anreise- und Übernachtungskosten für ein Tagesseminar häufig nicht rechnen und noch dazu die investierte Zeit für An- und Abreise verhältnismäßig hoch ist, haben wir uns für diese internetaffine Zielgruppe zu einem weiteren Webinar entschlossen.

Rahmenbedingungen
In 2 Einheiten á 120 Minuten bringt unser IT-Security-Experte Carsten Hennig Sie auf den neusten Stand. Die Inhalte werden durch Präsentation, Live-Demonstration und Fragerunden begleitet. Damit Sie Ihren Arbeitstag trotz Weiterbildung noch nutzen können, findet ein Block am Vormittag und einer am Nachmittag statt.

Technische Voraussetzungen
Für die Teilnahme an unserem

Online-Seminar benötigen Sie keine besondere Technik. Lediglich eine bestehende Internetverbindung, Kopfhörer bzw. ein Headset oder Lautsprecher sowie ein installiertes Adobe Flash Plugin ab Version 10.3. Die Verwendung einer Web-Cam ist optional möglich.
Sie können die Voraussetzungen für den Einsatz von Adobe Connect vorab testen: [http://ds-its.eu/webcheck]

Ablauf und Inhalt des Webinar
Im ersten Block zwischen 10 und 12 Uhr werden folgende Themen behandelt:

- Grundgedanken zum Hosting und zu Anbietern von Web- und Cloud-Speicher.
- Einführung in PCIDSS.
- sicheren Betrieb eines CMS planen und umsetzen.
- Fragen und Antworten

Im zweiten Block von 14 bis 16 Uhr geht es um die folgenden Inhalte:

- Regelmäßige Updates und Patches automatisieren.
- Logging und Monitoring .
- Webserver-Sicherheit beurteilen und verbessern.
- Web Application Firewalls.
- Fragen und Antworten

Testen Sie unser Webinar
Mit folgendem Buchungscode erhalten Sie einen Rabatt von 49,- € auf Ihre Buchung: **wbcms**
Wir wünschen Ihnen viel Spaß beim Ausprobieren dieser neuen Lernform und viel Erfolg.
[http://ds-its.eu/wbcms]

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 Februar - April 2014

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

Termin	Veranstaltungsbeschreibung	Ort / Uhrzeit / Shortlink
05.02. bis 06.02.	Seminar: Datenschutzauditor (TÜV Rheinland Akademie)	Hannover, 09:00 - 17:00 Uhr [tuvdsa]
17.02. bis 19.02.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Frankfurt, 10:00 - 17:00 Uhr [dsb214]
25.02. bis 26.02.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	Berlin, 09:00 - 17:00 Uhr [itsds]
04.03. bis 06.03.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	Leipzig, 10:00 - 17:00 Uhr [dsb314]
11.03.	Seminar: Datenschutz für IT-Leiter und IT-Experten (audatis Training)	Berlin, 09:00 - 17:00 Uhr [dsitl]
11.03.	Seminar: Web-Security für Web-Entwickler (audatis Training)	Berlin, 09:00 - 17:00 Uhr [wswe]
18.03. bis 19.03.	Seminar: IT-Sicherheit für Datenschutzbeauftragte (audatis Training)	Frankfurt, 09:00 - 17:00 Uhr [itsds]
20.03.	Webinar: Sicherheit von Content-Managm.-Syst. (CMS) (audatis Training)	Online, 10:00 - 16:00 Uhr [wbcms]
25.03. bis 27.03.	Ausbildung zum betrieblichen Datenschutzbeauftragten (Forum Fachseminare FFS)	München, 10:00 - 17:00 Uhr [dsb3214]
08.04. bis 09.04.	Workshop: Datenschutz praxisnah und gesetzeskonform (audatis Training)	Berlin, 09:00 - 17:00 Uhr [dsws]
10.04.	Webinar: Aktuelles im Datenschutz (audatis Training)	Online, 09:00 - 17:00 Uhr [wbdsa]

Nächstes Mal

Die nächste Ausgabe des audatis.INFO Newsletters für Datenschutz und Informationssicherheit erscheint Ende Q2 / 2014.

Einige Auszüge aus den Themen der nächsten Ausgabe:

- Was Software für den Datenschutzbeauftragten leistet
- Datenschutz am Arbeitsplatz
- Sicherer Datenaustausch im Web und E-Mail-Verschlüsselung
- Aktuelle Veranstaltungen zu Datenschutz und Datensicherheit

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

Die Sicherheit von Web-Seiten testen

(CK) Wer im Internet Web-Anwendungen zur Verfügung stellt, ist auch für deren Sicherheit als Betreiber verantwortlich. Das können

- einfache Web-Seiten,
- aufwändige Blogs + Foren
- oder Online-Shops

sein, die über das Web erreichbar sind. Da sich nicht nur Hacker weltweit auf diesen Seiten austoben können, sondern auch frustrierte Mitarbeiter und Kunden oder neugierige „Skript Kiddies“ ihr Können im „Hacken“ von Webseiten unter Beweis stellen wollen, sollten einige Grundregeln beachtet werden.

Es sollten regelmäßig Sicherheitstests durchgeführt werden, um die gängigsten Einfallstore für Manipulationen, Datenklau und Schadsoftware frühzeitig zu identifizieren und beheben zu können. Dabei können zahlreiche Ansätze, teilweise auch in Kombination sinnvoll sein. Im klassischen Penetrationstest (Pentest) wird versucht die Web-Seite durch externe Angriffe auf Schwachstellen abzuklopfen. Dies erfordert jedoch sehr viel Erfahrung und kann bei falscher Anwendung zu Schäden führen. Eine Quellcode-Analyse ist eine vertiefendere Stufe und versucht bereits dort die Sicherheitslücken zu identifizieren und zu beseitigen.

Wir haben das für Sie in ein flexibles Angebot gepackt: [https://audatis.de/pentest]

audatis®
Datenschutz und Informationssicherheit | NEWSLETTER

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)

Erscheinungsweise
4 x jährlich

Carsten Knoop
Geschäftsinhaber
Fon: 05221 / 854 96 - 90
Mail: carsten.knoop@audatis.de

Jill Bohrenkämper
Assistentin der Geschäftsleitung
Fon: 05221 / 854 96 - 92
Mail: j.bohrenkaemper@audatis.de