Protokoll zur 79. Sitzung des GDD ERFA-Kreises Stuttgart am 25. Januar 2006

1. Neues aus dem Teilnehmerkreis

Neue Teilnehmer:
Friedrich, Alexandra, Observer Argus Media GmbH, Fellbach
Müller, Reinhold, KSK Esslingen, Nürtingen, Esslingen
Wolz, Siegmund, Acterna Germany GmbH, Eningen

Als Gäste:
Bender, Hans-Juergen, Eberspächer GmbH & Co. KG, Esslingen
Reichert, Manfred, Metallwerke Kloss GmbH
Herr Röhm kommt mit H. Müller, KSK Esslingen
Schilling, Günter, Handtmannservice GmbH & Co. KG, Biberach
Teuscher, Andreas, Business Sustainability - Club
Widmaier, Stefan, Berufliche Bildung gGmbH, Tübingen

2. Nächster Termin

Als Termin für die nächste Tagung wurde der 14.06.2006, um 13:30 Uhr, vereinbart.

3. Fragen der Teilnehmer

- Anregung größerer Raum ?

  Es gibt bei der IHK noch einen größeren Raum, der allerdings nicht multimedia-geeignet ist. Deshalb soll es beim aktuellen Raum bleiben.

- Kongress des BvD (Berufsverband der Datenschutzbeauftragten) am 16./17.03.2006 in Ulm?

  s. dazu http://www.bvdnet.de/

- Es gibt seit dem 01.11.2005 eine Internetanwendung, mit der im Abo Passworte geknackt werden können. Die Adresse lautet ***http://www.rainbowcrack-online.com***. Ist diese Anwendung auch anderen Teilnehmern bekannt ist und wie wird das Gefährdungspotential eingeschätzt ?

  Auszüge aus den Diskussionsbeiträgen:
  - *In Heise Online war Ende 2005 eine Info dazu nachzulesen.*
  - *Soweit die Anwendung für Passwörter von anderen verwendet wird, ist das strafbar.*
  - *Für 29,95 EUR kommt man an den Hashwert zu jedem beliebigen Passwort.*

- Der Gesetzgeber nimmt alle Arbeitgeber in die Pflicht, ab 01.01.2006 sowohl die SV-Meldungen als auch die Beitragsnachweise ausschließlich per Datenübertragung einzureichen. Um am Datenaustausch teilnehmen zu können, ist die Zertifizierung beim Trustcenter der ITSG (Informationstechnische Servicestelle der Gesetzlichen Krankenversicherung GmbH) (http://www.itsg.de/) zu beantragen. Dafür muss eine Kopie des Personalausweises beigefügt werden.
  Wozu ist das notwendig ? Gemäß Rückfrage bei der AOK gibt es das Signaturgesetz, nach dem eine eindeutige Identifizierung erfolgen muss.

Wo ist die rechtliche Grundlage für die Ausweiskopie des Verantwortlichen / Zuständigen ? Ist dem Teilnehmerkreis diese bekannt ?

nein.
Eine Ausweiskopie ist deshalb notwendig, weil klar sein muss, dass derjenige der beantragt, berechtigt sein muss.

- Haftungsrisiko für firmeninterne Stelleninhaber – haftet ein Mitarbeiter genauso wie der Geschäftsführer ?

  Auszüge aus den Diskussionsbeiträgen:
  - *Es handelt sich hierbei um die normale Arbeitnehmerhaftung.*

- § 31 besondere Zweckbindung
  Mit dem Einsatz von Analyzern zur Fehlersuche in Netzwerken können nicht nur Verbindungsdaten, sondern auch Inhaltsdaten gelesen werden. Wie ist das zu werten ?

  Auszüge aus den Diskussionsbeiträgen:
  - *§ 31 unterliegen z. B. alle Logdaten, Traces (Datenfluss, der in Logdatei landet). Wenn sie personenbezogen sind, dürfen sie nur für bestimmte Zwecke verwendet werden.*
  - *Die Auswertung von § 31-Dateien sollte nur mit Zustimmung von DSB bzw. von BR bei Personaldaten erfolgen.*
  - *Soweit Externe den Analyzer-Einsatz vornehmen, sind sie zu verpflichten.*

- Auftrags-DV – Unternehmen haben z. T. langjährige Verträge mit Dienstleistern, in denen die Verpflichtung nach § 5 enthalten ist. Genügt es hier, eine Anlage zur Auftrags-DV zu machen oder ist ein separater Vertrag notwendig ?

  Im Normalfall reicht es aus, wenn eine Anlage gemacht wird.
  Bei Verträgen, die den Passus beinhalten, dass alle Änderungen schriftlich zu bestätigen sind, muss die Unterschrift von Auftraggeber und Auftragnehmer geleistet werden..

- Ein Unternehmen will eine ziemlich umfangreiche Datenerhebung (mit Alter, Wohnort, Straße, Schule,...) machen für eine Analyse, in welchem Umfeld Werkstätten für Schwerbehinderte,.. benötigt werden. Es müssen zwar keine Namen angegeben werden, aber in kleinen Orten kann man zum Personenbezug kommen ?

  Die Erhebung ist zwar anonym, aber der DSB muss sehen, was mit den Daten gemacht werden soll. Nachdem mehrere Institutionen beteiligt sind, können ggf. bestimmte Daten intern bleiben.

- Ein Mitarbeiter bekommt einen PC als Arbeitsmittel gestellt. Im Unternehmen gibt es keine Policies, die den Gebrauch regeln. Nun besteht der Verdacht, dass der PC genutzt wird für kriminelle Handlungen. Auf welcher Grundlage kann die Harddisk überprüft werden ?

  Auszüge aus den Diskussionsbeiträgen:
  - *Bei Verdacht auf einen Straftatbestand ist die Staatsanwaltschaft einzuschalten.*
  - *Für den DSB ist die Frage, ob sich der Verdacht auf einen Straftatbestand so erhärtet, dass die Staatsanwaltschaft eingeschaltet werden muss.*
  - *Internet-/E-Maildaten unterliegen § 88 TKG (zwecks aktuellem Stand s. Anlage 2); von Unternehmensseite sollten bei einer Überprüfung des PC die Partitionen außen vor bleiben, auf denen sich Daten von Lotus Notes / Outlook / o. ä. befinden.*
  - *Mit Hilfe von Tools könnte geschaut werden, welche Dateien auf dem PC sind.*

- *Bei wirtschaftskriminellem Hintergrund kann Rat eingeholt werden bei der Aufsichtsbehörde.*
- *Zwecks evtl. doch vorhandener Regelungen zur Privatnutzung sollten der Arbeitsvertrag, BV, ... durchgeschaut werden.*
- *Eine mögliche Verfahrensweise könnte wie folgt sein:*
  auf den Betroffenen zugehen, ihn fragen, ob er Interesse hat an einer Aufklärung und mit einer Überprüfung seines PC einverstanden ist.
- *Es gibt hierzu derzeit noch keine Urteile, Kommentare. Es wäre interessant, wenn diese Thematik von GDD-Seite aufgegriffen und dazu ein Aufsatz veröffentlicht werden könnte.*
- *Bei der Aufsichtsbehörde kamen schon vermehrt Fragen zum Arbeitnehmerdatenschutz an. Ihre Empfehlung ist:*
  a) Es existiert eine interne Regelung zur Auswertung von Daten (die jedem Mitarbeiter bekannt zu machen ist). Dann kann der PC beschlagnahmt werden und z. B. im Beisein von DSB und BR eingesehen werden.
  b) Es gibt keine Regelung. Dann ist eine Info an den Betroffenen zu geben, aber mit dem Hinweis darauf, dass der PC beschlagnahmt werden kann.
- *Wenn klar ist, dass die Daten gesichert werden können, dann sollte eine forensische Sicherung (Verwendbarkeit digitaler Beweise vor Gericht) gemacht werden – Analyse z. B. mit EnCase.*

- GdPdU – Finanzbeamte können Daten auf ihre Laptops überspielen, ... ? Kann der DSB die Prüfer auf § 5 BDSG verpflichten ?

  - *Der OFD sagt, für Beamte gilt hoheitliches Recht, nicht das BDSG (s. dazu Anlage 1)!*
  - *Das IM BW war mit dieser Thematik noch nicht befasst. Ein Beamter ist von seiner Dienstpflicht her auf das BDSG verpflichtet.*

4. ***Datenschutz- und –analyse-Tools (BDSG-, Audit-Basics)*** *(Ulrich Rummel)*

s. dazu auch http://www.demal-gmbh.de/

5. 26. Tätigkeitsbericht des LDSB Baden-Württemberg (Uwe Dieckmann)

s. beigefügte Powerpoint-Präsentation

Auszüge aus den Diskussionsbeiträgen:

- *Vertraulichkeit empfangener Nachrichten – Postfachinhaber ist verstorben:*
  Bei nicht zugelassener Privatnutzung hat Arbeitgeber Zugang zwecks Wahrung seiner geschäftlichen Interessen.
  (Das Fernmeldegeheimnis gilt auch bei Toten.)
  Wenn die Privatnutzung zugelassen ist, geht man davon aus, dass für private Mails ein Extra-Postfach vorhanden ist.
- *Zertifizierungen:*
  Stand heute sind die Zertifikate noch an Personen gebunden; es gibt offenbar noch keine für Stellen. Hier sollte man noch zu funktionsbezogenen Zertifizierungen kommen.
- *Das Amtsgericht Darmstadt entschied mit dem Urteil vom 30.06.2005 (300 C 397/04), dass Internet-Access-Provider die Verbindungsdaten der jeweiligen Kunden nur solange speichern dürfen, wie es zu Abrechnungszwecken erforderlich ist. Beklagt wurde in diesem Fall die T-Online AG von einem ihrer Kunden. Dieser hatte einen Vertrag über eine Flatrate abgeschlossen und forderte die Unterlassung der Aufzeichnung, da diese nicht nötig sei. Er hatte insoweit Erfolg, allerdings kann er nicht die Löschung sämtlicher Daten verlangen, da auch bei Flatrate-Tarifen z. B. die Volumina der herunter geladenen Datenmengen kostenrelevant sein können.*

Anlage 1: Rechtssprechung zum Datenzugriff

FG Rheinland-Pfalz vom 20.01.2005

Zum Datenzugriff gem. § 147 Abs. 6 AO:
Die Anforderung der Überlassung eines Datenträgers mit den Sachkonten des Jahres 2002 im Rahmen einer Betriebsprüfung bei einer Bank entspricht den gesetzlichen Vorgaben des § 147 Abs. 6 AO; ein Ermessensfehlgebrauch bei der Auswahl der Methode des Datenzugriffs ist nicht zu erkennen. Es ist Sache der Bank, ihre Datenbestände so zu organisieren, dass bei der Herausgabe des Datenträgers keine durch § 30 a AO geschützten Daten offenbart werden. Az. 4 K 2167/ 04

Thüringer Finanzgericht v. 20.04.2005

Rechtmäßigkeit einer Aufforderung zur Datenträgerüberlassung, kein Anspruch des Steuerpflichtigen auf Unterzeichnung einer Bestätigung des Betriebsprüfers:

1. Die Aufforderung zur Datenträgerüberlassung ist bei summarischer Prüfung auch ohne Unterzeichnung einer Bestätigung des Betriebsprüfers, die CD sicher vor unbefugtem Zugriff aufzubewahren, sie nicht zu kopieren und nach Abschluss der Prüfung wieder zurückzugeben, rechtmäßig und verhältnismäßig. Der Steuerpflichtige hat weder nach dem Gesetz noch nach den Verwaltungsgrundsätzen (BMF-Schreiben vom 16.7.2001, BStBl 2001 I S. 415 „GDPdU") Anspruch auf Erteilung einer solchen Bestätigung.

2. Der Gesetzgeber hat mit der gesetzlichen Ausgestaltung des Steuergeheimnisses hinreichende Sicherheitsvorkehrungen gegen eine missbräuchliche Verwendung der erteilten Angaben auch im Hinblick auf die Datenträgerüberlassung getroffen. Allein der Umstand, dass die geforderten Daten mit dem Datenträger den Machtbereich des Steuerpflichtigen verlassen, rechtfertigt keine strengeren Anforderungen. Az.: III 46/05 V, rkr.

Anlage 2: Bundesverfassungsgericht urteilt - Mail- und Handydaten bleiben geschützt

L e i t s ä t z e

zum Urteil des Zweiten Senats vom 2. März 2006

- 2 BvR 2099/04 -

Die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Verbindungsdaten werden nicht durch Art. 10 Abs. 1 GG, sondern durch das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG) und gegebenenfalls durch Art. 13 Abs. 1 GG geschützt.
§§ 94 ff. und §§ 102 ff. StPO genügen den verfassungsrechtlichen Anforderungen auch hinsichtlich der Sicherstellung und Beschlagnahme von Datenträgern und den hierauf gespeicherten Daten und entsprechen der vor allem für das Recht auf informationelle Selbstbestimmung geltenden Vorgabe, wonach der Gesetzgeber den Verwendungszweck der erhobenen Daten bereichsspezifisch, präzise und für den Betroffenen erkennbar bestimmen muss. Dem wird durch die strenge Begrenzung aller Maßnahmen auf den Ermittlungszweck Genüge getan (vgl. Beschluss des Zweiten Senats des Bundesverfassungsgerichts vom 12. April 2005 - 2 BvR 1027/02 -).
Beim Zugriff auf die bei dem Betroffenen gespeicherten Verbindungsdaten ist auf deren erhöhte Schutzwürdigkeit Rücksicht zu nehmen. Die Verhältnismäßigkeitsprüfung muss dem Umstand Rechnung tragen, dass es sich um Daten handelt, die außerhalb der Sphäre des Betroffenen unter dem besonderen Schutz des Fernmeldegeheimnisses stehen und denen im Herrschaftsbereich des Betroffenen ein ergänzender Schutz durch das Recht auf informationelle Selbstbestimmung zuteil wird.
BUNDESVERFASSUNGSGERICHT

- 2 BvR 2099/04 -
Verkündet
am 2. März 2006