

Forum H - Datenschutz und Datensicherheit

Neu auf dem 10. Kongress neueVerwaltung war der Forentrack Datenschutz und Datensicherheit, der die Bedeutung dieser Themen für ein erfolgreiches eGovernment unterstreichen sollte.

Ca. 60 Teilnehmende folgten den Vorträgen in den verschiedenen Foren. Das erste Thema „**Bürger, Kunde, Datensatz - persönliche Daten in der digitalen Welt**“ wurde fachkundig und engagiert von Dr. Mechthild Stöver (Frauenhofer SIT) moderiert. Zunächst stellte **Gert Metternich** (T-Systems) das BMI-Projekt DE-Mail vor, an dem sein Unternehmen führend beteiligt ist. Er räumte dabei mit verschiedenen Missverständnissen auf: DE-Mail sei vor allem ein Portal für die sichere Kommunikation zwischen Bürgern und der Wirtschaft. Es solle nicht bestehende Portale der öffentlichen Verwaltung ersetzen, auch wenn diese sich daran beteiligen könnten. Es werde keine Verbindung zwischen normalen e-mail-Adressen und dem DE-Mail-Portal geben, um Sicherheitsprobleme (z. B. Phishing) auszuschließen. Dabei wurde deutlich, dass DE-Mail gewissermaßen wie ein Schutzschirm für alle Bürger und Unternehmen wirken soll, die eine rechtsverbindliche e-Mail versenden müssen (z. B. Verträge).

Andreas Schneider, Referatsleiter beim sächsischen Datenschutzbeauftragten, berichtete über das vielfältige Aufgabengebiet seiner Behörde und über aktuelle Probleme. So schilderte er z. B. einen Fall von Videoüberwachung, bei dem jemand, der Opfer eines Verbrechens geworden war, Aufnahmen vom Täter im Internet veröffentlichte, um die polizeiliche Fahndung zu unterstützen. Sein Vortrag vermittelte die zahlreichen Aspekte von Datenschutz, sei es im Gesundheitswesen, im Personalbereich oder in den Kommunen. Er wies darauf hin, dass seine Behörde künftig personell verstärkt werde und gab seiner Hoffnung Ausdruck, dass dadurch der Datenschutz in Sachsen gestärkt werde.

Dr. Sebastian Clauss von der Technischen Universität Dresden beschrieb die Gefahr der Verkettung anonymer Internetdaten. So sei es z. B. für Kreditkarteninstitute oder Online-Händler durchaus möglich, Bestellungen ihrer Kunden so zu verketteten, dass komplexe Benutzerprofile entstehen. Seine Forschungen zielen darauf ab, hier echte Alternativen zu schaffen, wie z. B. im Projekt PRIME. Ziel sei, die Sensibilität für Privatsphäre und Datenschutz - auf neudeutsch „Privacy Awareness“ - im alltäglichen Umgang mit elektronischen Medien zu verbessern und vor allem auch Lösungen für die Nutzer zu bieten.

Im Forum „**Datenschutzkonforme IT-Sicherheit**“ wurde die gemeinsame Schnittmenge von Datenschutz und IT-Sicherheit thematisiert. Unter der Moderation von Dr. Dieter Haschke, Datenschutzexperte der dbb akademie, beschrieb **Frank Lehnert** vom

kommunalen Rechenzentrum in Lemgo (krz) seine Aufgaben als Datenschutz- und IT-Sicherheitsbeauftragter. Seine These lautete: die IT muss den Anwender bei der elektronischen Verarbeitung personenbezogener Daten so unterstützen, dass der Datenschutz automatische Beachtung findet. So müsse z. B. die IT automatisch Daten verschlüsseln, wenn sie versendet werden, damit der Anwender hier keine Fehler machen könne.

Johannes Landvogt, Abteilungsleiter beim Bundesdatenschutzbeauftragten, erläuterte ausführlich den in das BSI-Grundschutzhandbuch eingefügten Baustein Datenschutz. Anhand des BSI-Gesetzes machte er deutlich, dass der vorliegende Gesetzentwurf vom 14. Januar 2009 noch kritische Punkte enthält: so werde das BSI z. B. ermächtigt, die gesamte Datenkommunikation ohne Anonymisierung bzw. Pseudonymisierung zu überwachen und auszuwerten sowie eine Datenübermittlung an Strafverfolgungsbehörden, insbesondere bei nicht erheblichen Straftaten, vorzunehmen. Auch fehle eine Verpflichtung des BSI, Informationen über ihm bekannt gewordene Sicherheitslücken und Schadprogramme zu veröffentlichen und damit Unternehmen, Bürgerinnen und Bürger vor zu (erwartenden) Angriffen (Spionage und Sabotage) zu warnen. Ähnliche Forderungen aus den Regierungsfractionen (CDU/CSU und SPD) deuteten darauf hin, dass der Datenschutz in dem Gesetz mehr Gewicht erhalten werde. Angesichts der Tatsache, dass das Bundesdatenschutzgesetz bereits 30 Jahre alt ist, sei es nicht verwunderlich, dass es hinter der aktuellen technischen Entwicklung zurückbleibe. „Datenverarbeitung wird allgegenwärtig und permanent“, deshalb müsse das Datenschutzrecht dringend modernisiert werden.

Am Ende des ersten Tages wurde dann in einem Roundtable die Frage diskutiert: **„Bürgervertrauen und eGovernment - Sind unsere Daten sicher?“** Unter der souveränen und gut informierten Moderation von Manfred Kloiber (Deutschlandfunk) diskutierten **Prof. Dr. Dirk Heckmann** (Universität Passau), **Dr. Heike Stach** (Bundesinnenministerium) und **Johannes Landvogt** (Abteilungsleiter beim Bundesdatenschutzbeauftragten) Möglichkeiten, das Vertrauen der Bürger in den Datenschutz zu stärken, um eGovernment dauerhaft zum Erfolg zu verhelfen. Vor dem Hintergrund der Datenschutzverstöße bei Telekom, Bahn, Lidl usw. müsse nach Ansicht von Prof. Heckmann die Politik eindeutige Signale senden, dass das Spannungsverhältnis von Datenschutz und Sicherheitspolitik ausgewogen bleiben werde. Hier verunsichere die Politik oft den Bürger anlässlich von terroristischen Angriffen oder kriminellen Aktivitäten mit Forderungen nach mehr Überwachung. Dr. Stach, die als Leiterin des Projekts DE-Mail einen wesentlichen Beitrag zu mehr Sicherheit im Bereich e-Mail leisten möchte, stellte das Projekt ausführlich vor und wies darauf hin, dass dieses Bürgerportal für die rechtsverbindliche Kommunikation über das Internet durch seine Verschlüsselungsmechanismen eine große Bedeutung haben werde. Banken, Versicherungen, mittelständische Unternehmen hätten ein großes Interesse bekundet. Erstaunt zeigte sie sich über manche unsachliche Kritik der Medien, die auf Grund einer gewissen Zurückhaltung des BMI im Rahmen des Gesetzgebungsverfahrens unverdiente Resonanz erhielten. Johannes Landvogt begrüßte das Projekt grundsätzlich als einen Schritt in die richtige Richtung, auch wenn seitens der Datenschützer noch einige Bedenken bestehen.

Der zweite Kongresstag begann mit dem Forum **„Chefsache Datenschutz“** und Datensicherheit unter der Moderation von Dr. Dieter Haschke (dbb akademie). **Andreas Schmidt** von der Zeppelin University Friedrichshafen sprach über

Korruptionsbekämpfung mit E-Government. Anhand eines Drei-Phasenmodells „vor, während und nach der Korruption“ stellte er traditionelle Lösungsansätze zur Verhinderung von Korruption dar und ergänzte diese durch Hinweise auf zusätzliche elektronische Möglichkeiten. So ließe sich z. B. durch eLearning oder ein Portal zum Thema Korruption bereits im Vorfeld wirksame Prävention betreiben. Auch die elektronische Akte oder die eVergabe böten Möglichkeiten einer wirksamen Kontrolle. Durch Business Intelligence ließen sich auch Auffälligkeiten diagnostizieren, die allerdings **nur** bei konkretem Verdacht und unter Beachtung des Datenschutzrechts anwendbar sei. Im Gegensatz zu den USA und Großbritannien gebe es in Deutschland noch keine Kultur des Umgangs mit dem whistleblowing (Melden von Korruptionsfällen an Vorgesetzte). In den USA seien whistleblower „Helden“, bei uns eher Nestbeschmutzer.

Prof. Jürgen Müller von der Berufsakademie Thüringen in Gera erläuterte verschiedene Aspekte der Chefsache Datenschutz. Ausgehend von einer Umfrage unter 107 Sicherheitsexperten aus aller Welt, die ein mangelhaftes IT-Sicherheitsbewusstsein von Führungskräften deutlich erkennen lässt, wies er auf die persönliche Haftung von Führungskräften und mögliche materielle und ideelle Schäden für Unternehmen und Behörden hin. Chefsache sei auch die Berufung des Datenschutzbeauftragten, der entsprechende fachkundig und zuverlässig sein müsse und eine unabhängige Stellung habe. Nach einer Beschreibung des Aufgabengebietes des Datenschutzbeauftragten wies Prof. Müller nachdrücklich und an einigen Beispielen darauf hin, dass auch die IT-Sicherheit Chefsache sei.

Das letzte Forum mit dem Thema „**Werkzeuge, Organisation und Strukturen**“ in der Datensicherheit wurde von Dr. Volker Franke (dbb akademie) moderiert, der für die Konzeption des gesamten Forentracks verantwortlich war. Zunächst schilderte **Frank Lehnert**, IT-Sicherheits- und Datenschutzbeauftragter im kommunalen Rechenzentrum Lemgo den Weg zum ISO 27001 Zertifikat auf der Basis von IT-Grundschutz. Er erläuterte dabei das Vorgehen zur Einführung eines gesteuerten Sicherheitsprozesses und die Entwicklung bzw. Umsetzung der Informationssicherheitsstrategie auf der Grundlage der BSI-Standards (100-1 bis 100-3) und der IT-Grundschutz-Kataloge. Schließlich stellte **Alexander Koderman** von der SerNET GmbH das Open Source Tool verinice vor, mit dem der IT-Grundschutz optimal verwaltet werden kann. Das Programm unterstützt den IT-Sicherheitsbeauftragten bei der IT-Strukturanalyse, der Feststellung des Schutzbedarfs, der Modellierung sowie der Aufrechterhaltung der IT-Sicherheit. Damit wird das Erfassen des IT-Verbundes, die Definition und Zuordnung von Schutzbedarfsstufen, die Planung und Dokumentation von Maßnahmen, die Erstellung eines Umsetzungsplanes und die Aufgabenverteilung sowie die Erstellung von Referenzdokumenten für die Zertifizierung erleichtert.

Der Forentrack schlug somit einen großen Bogen: vom Bürger als Betroffener und als Kunde, über das Zusammenspiel von Datenschutz und Datensicherheit bis hin zur Verantwortung der Politik und der Führungskräfte sowie der Aufgaben der Datenschutz- und IT-Sicherheitsbeauftragten. Diese Vielfalt der Aspekte zeigte auf, dass dem Thema nicht nur eine wesentliche Bedeutung für das eGovernment und die Akzeptanz der Bürger hat, sondern auch für das politische Vertrauen in die elektronische Demokratie.