

Redaktion: Helmut Reimer

# Report

## Übersicht

- LfD Mecklenburg-Vorpommern: Datenschutz-Tätigkeitsberichte 2008/2009
- Insophia: EuroPriSe-Siegel für „Certified Privnote“
- ULD: Data Center Steuern von Data-Port ist datenschutzkonform
- Kabinett beschließt Gesetzentwurf zur Regelung von De-Mail-Diensten
- Begleitstudien zum neuen Personalausweis vorgestellt
- Berechtigungszertifikate für den neuen Personalausweis
- STORK: Interoperabilität von elektronischen Identitäten in Europa
- CC-Zertifikat für secunet wall packet filter
- BMBF-Forschungsprojekt: Mobilfunknetze sollen sicherer werden
- Secrypt: digiSeal® office, komfortable Signaturlösung
- BvD: Datenschutz wird zum bundesweiten Schulprojekt
- it-sa 2010 erfolgreich
- Fraunhofer beruft Prof. Michael Waidner in die Institutsleitung des SIT
- Veranstaltungsbesprechungen
  - Tagungsbericht von der DSRI-Herbstakademie 2010, 8. – 11. 09. 2010 in München
  - ISSE / GI-Sicherheit 2010, 05. bis 07. Oktober 2010 in Berlin
- Buchbesprechungen
  - Giesen, Thomas; Bannasch, Bernhard; Naumann, Tino; Dehoust, Matthias; Mauersberger, Thomas: Kommentar zum Sächsischen Datenschutzgesetz
  - Drallé, Lutz: Das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme
- Veranstaltungskalender

## LfD Mecklenburg-Vorpommern: Datenschutz-Tätigkeitsberichte 2008/2009

Seinen Tätigkeitsbericht für die Jahre 2008 und 2009 hat der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Karsten Neumann, am 21.10.2010 in Schwerin der Öffentlichkeit vorgestellt. Der Bericht umfasst sowohl den Neunten Tätigkeitsbericht gemäß § 33 Abs. 1 Landesdatenschutzgesetz (DSG M-V), also über den Datenschutz in Landes- und Kommunalbehörden und weiteren öffentlichen Stellen, als auch den Vierten Tätigkeitsbericht gemäß § 38 Abs. 1 Bundesdatenschutzgesetz (BDSG), also über die Datenschutzaufsicht über die nicht-öffentlichen Stellen im Land, wie Unternehmen, Verbände, Vereine, aber auch Privatpersonen.

„Im Berichtszeitraum 2008 und 2009 haben sich die Meldungen zum Thema Datenschutz förmlich überschlagen. Datenkandale machten die Runde und erreichten ein Maß an Öffentlichkeit, wie es diesem Thema in den letzten Jahrzehnten selten beschert war. Den gesetzgeberischen Bemühungen ist gegenwärtig allerdings eher eine symbolische als eine wirklich überzeugende Kraft beizumessen“, so Neumann heute zu den wesentlichen Entwicklungen. Er begrüßt jedoch das wachsende öffentliche Bewusstsein für die Datenschutzthemen, „auch wenn die Angst vor Skandalen ein schlechter Ratgeber ist“.

Auch der Landtag von Mecklenburg-Vorpommern hat die Diskussion aufgegriffen und die Behörde sowohl personell als auch institutionell gestärkt. Eine personelle Aufstockung um eine Stelle des höheren Dienstes bezeichnete Neumann als „zwar keinesfalls ausreichend, angesichts der Bemühungen der Landesregierung um Personalabbau aber doch eine keineswegs selbstverständliche und daher besonders begrüßenswerte Verstärkung“. Zudem begrüßte er die Stärkung seiner Beteiligungsrechte im Gesetzgebungsverfahren durch eine Änderung der Gemeinsamen Geschäftsordnung der Landesregierung und der Geschäftsordnung des Landtages.

Die öffentliche Wahrnehmung des Datenschutzes führte aber auch zu einem enormen Anstieg bei den Petitionen von Bür-

gerinnen und Bürgern. Schwerpunkt waren vor allem die Themen Videoüberwachung im nicht-öffentlichen Bereich und Sozialdatenschutz bei Hartz-IV Leistungsbezug. „Die Zahl der Petitionen ist so stark gestiegen, dass mitunter die Arbeitsfähigkeit der Behörde bedroht ist“, stellte Neumann fest. „Unterstützung brauchen aber inzwischen vor allem die Kommunen, die in Bezug auf neue E-Government-Verfahren inzwischen unter einem substanziellen Kompetenzverlust als Ergebnis des Personalabbaus leiden“, so Neumann zu den Schlussfolgerungen aus einem Projekt zum Thema „Elektronische Verwaltung und Datenschutz“.

In der zweiten Jahreshälfte 2009 hat der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern auf kommunaler Ebene Untersuchungen zum Stand der Umsetzung der Regelungen zum Datenschutz am Beispiel des elektronisch zu führenden Melderegisters durchgeführt. Dazu wurden nach Durchführung einer Erhebung mittels Fragebogen bei allen Kommunen des Landes in rund zwanzig Kommunen unterschiedlicher Art und Größe Besuche durchgeführt, bei denen die Situation vor Ort besprochen wurde und Empfehlungen zur Verbesserung des Datenschutzes gegeben wurden. Bei den Untersuchungen hat sich gezeigt, dass die wesentlichen Probleme struktureller Natur sind und nicht allein von den Kommunen gelöst werden können. Der Projekt-Bericht (siehe Punkt 6) gibt die wichtigsten der Ergebnisse wieder.

Im Ergebnis des Projektes war es erstmalig möglich, statistisch aussagekräftige Ergebnisse zur E-Government-Fähigkeit der Kommunen zu erhalten. Zwischen 30% und 45% der Behörden hatten keinen behördlichen Beauftragten für den Datenschutz oder nicht dem Gesetz entsprechend bestellt, knapp 20 % der Kommunen kannten die Einführungsempfehlungen des Innenministeriums auch ein Jahr nach Einführung nicht und nicht alle Informationen erreichten die zuständigen Empfänger.

Als Grund für eine fehlende Bestellung nannten die Kommunen (in der Reihe der Häufigkeit) 8 Jahre nach In-Kraft-Treten des Landesdatenschutzgesetzes 2002:

1. Bisher habe keiner danach gefragt.

2. Man habe innerhalb der Gemeinde keine geeignete Person gefunden.
3. Es habe intern die Bereitschaft gefehlt, zusätzliche Aufgaben zu übernehmen.
4. Der Preis für „Externe“ sei zu hoch. (Nach DSGVO M-V ist auch die Beauftragung sog. „externer“ Datenschutzbeauftragter zulässig.)
5. Politische Gremien (z. B. der Gemeindeausschuss) hätten eine externe Bestellung abgelehnt.
6. Wegen sich ständig ändernder politischer Rahmenbedingungen wolle man keine langfristige Bindung eingehen.

Zu der Resonanz in den Kommunen heißt es in dem ausführlichen Bericht: „Durch die Bank weg waren vor allem das technische Personal in den Kommunen, aber auch die in den Meldeämtern Beschäftigten Datenschutzgedanken sehr aufgeschlossen. Überall bestand in den Gesprächen Aufmerksamkeit gegenüber Datenschutzfragen, und es war uneingeschränkt die Bereitschaft festzustellen, Datenschutzempfehlungen nachzukommen. Anders gelegentlich das Leitungspersonal, das in einigen Fällen sehr reserviert auftrat. Das hatte in diesen Fällen aber auch seinen guten Grund, war es doch in der Regel ein schlechtes Gewissen verbunden mit dem Versuch, die bekannten Datenschutzmängel zu verstecken“.

„Die Ergebnisse dieser Untersuchung belegen in aller Deutlichkeit einen enormen Handlungsbedarf des Landes. Die in der Mehrzahl sehr kleinen Kommunalverwaltungen sind mit ihrer gegenwärtigen personellen Ausstattung und technischen Infrastruktur nicht in der Lage, auch nur die geringsten Datensicherheitsanforderungen durchgängig sicherzustellen“, so bestätigt Neumann die Projektergebnisse im Vergleich zu den Erfahrungen seiner Behörde.

„Auch wenn durch den E-Government-Zweckverband mit der Beschäftigung von Datenschutzexperten in vielen Kommunen deutliche Fortschritte erzielt wurden, so ist doch das Land in der Pflicht, die Kommunen bei der Einführung von E-Government-Verfahren wesentlich intensiver und frühzeitiger zu unterstützen“, begrüßte Neumann den Schritt der kommunalen Spitzenverbände, die Kommunen bei dieser Aufgabe durch hauptamtliche Datenschutzexperten zu unterstützen.

Auf seiner letzten Sitzung hat der Landtag bereits auf Anregung des Städte- und Gemeindetages und des Landesbeauftragten

für den Datenschutz die gesetzlichen Anforderungen an die technisch-organisatorische Sicherheit zentraler Verfahren konkretisiert und dabei das Land stärker in die Pflicht genommen (Viertes Gesetz zur De-regulierung und zum Bürokratieabbau, LT-Drs. 5/3366). Nunmehr heißt es in § 3 Absatz 5: „Daten verarbeitende Stelle ist jede öffentliche Stelle, die personenbezogene Daten für sich selbst verarbeitet oder durch andere in ihrem Auftrag verarbeiten lässt oder die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“ „Nunmehr wird auch im Datenschutz das Prinzip umgesetzt: Wer bestellt, soll auch bezahlen“, zeigt sich Neumann zufrieden über die gesetzlichen Fortschritte.

### Insophia: EuroPriSe-Siegel für „Certified Privnote“

Insophia erhält das EuroPriSe-Siegel für den webbasierten Dienst Certified Privnote, der seinen Nutzern den einfachen Austausch verschlüsselter Nachrichten über das Internet ermöglicht. Das Europäische Datenschutz-Gütesiegel bestätigt, dass Certified Privnote den hohen Anforderungen der europäischen Datenschutzbestimmungen entspricht.

Certified Privnote ist ein webbasierter Dienst, der seinen Nutzern den einfachen Austausch verschlüsselter Nachrichten über das Internet ermöglicht. Der Dienst wird unter <https://certified.privnote.com> angeboten und kann registrierungsfrei genutzt werden. Der Austausch einer verschlüsselten Nachricht mit Hilfe dieses Dienstes gestaltet sich sehr einfach: Der Nutzer gibt die auszutauschende Nachricht in ein Texteingabefeld ein und schließt die Nachrichtenerstellung durch einen Klick auf den Bestätigungs-Button ab. Daraufhin wird die Nachricht sowohl im Browser des Nutzers als auch nochmals auf dem Certified Privnote-Server verschlüsselt und dann dort abgelegt. Der Nutzer erhält eine aus den beiden Zufallsschlüsseln generierte Internetadresse (URL), mittels derer die Nachricht vom Certified Privnote-Server abgerufen und entschlüsselt werden kann. Diese Adresse übermittelt er über einen beliebigen Kommunikationskanal wie z.B. Telefon, SMS, Instant Messenger oder Email an den gewünschten Adressaten der Nachricht. Der Empfänger fügt die URL in die Adresszeile seines Browsers ein und

kann so die verschlüsselte Nachricht abrufen, entschlüsseln und lesen. Nach ihrem (erstmaligen) Abruf wird die verschlüsselte Nachricht vom Certified Privnote-Server gelöscht.

Das EuroPriSe-Siegel ([www.european-privacy-seal.eu](http://www.european-privacy-seal.eu)) wird von einer unabhängigen Stelle an datenschutzfreundliche IT-Produkte und Dienstleistungen nach erfolgreichem Durchlaufen eines zweistufigen, qualitätsgesicherten Verfahrens verliehen: Auf eine Begutachtung des Produkts oder Dienstes durch hierfür zugelassene Sachverständige für die Bereiche Recht und Technik folgt eine Validierung durch die unabhängige Zertifizierungsstelle beim Unabhängigen Landeszentrum für Datenschutz ([www.datenschutzzentrum.de](http://www.datenschutzzentrum.de)). Das Siegel und die veröffentlichten Kurzgutachten sollen Verbrauchern und Unternehmen eine transparente Orientierungshilfe bei der Auswahl und Bewertung von IT-Produkten und Dienstleistungen geben. „Bei Certified Privnote handelt es sich um einen Dienst, der seinen Nutzern ein höheres Maß an Vertraulichkeit bei der Übermittlung einer Nachricht garantiert, als dies herkömmliche Email-Dienste leisten“, sagt Kirsten Bock, Leiterin der EuroPriSe-Zertifizierungsstelle beim Unabhängigen Landeszentrum für Datenschutz, auf der Public Voice Datenschutzkonferenz in Jerusalem. „Der Dienst kann wegen seiner einfachen Bedienbarkeit von allen verwendet werden, für die die Installation und Nutzung einer speziellen Verschlüsselungssoftware ein hohes Hindernis darstellt. Sichere Verschlüsselung bleibt damit nicht mehr nur den technisch versierten Internetnutzern vorbehalten.“

Insophia (Baladir S.A.) ist ein Technologieunternehmen aus Uruguay, das sich auf Dienstleistungen in den Bereichen Web Scraping, Data Mining, Open Source, Python und Linux spezialisiert hat. Bei Insophia arbeiten Mitarbeiter mit unterschiedlichem beruflichem Hintergrund kreativ zusammen. Das Unternehmen ermutigt seine Mitarbeiter zum offenen Austausch von Ideen und erwartet von ihnen unkonventionelles Denken. Insophia ist gegenwärtig das größte in Python programmierende Unternehmen in Uruguay. Weitere Informationen: [www.insophia.com](http://www.insophia.com)

## ULD: Data Center Steuern von Dataport ist datenschutzkonform

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat am 28.10.2010 Dataport für sein Konzept des Informationssicherheits-Managementsystems des Data Center Steuern ein Datenschutzaudit-Zertifikat verliehen. Herrn Matthias Kammer, Vorstandsvorsitzender von Dataport, wurde ULD-Leiter Thilo Weichert die Auditorik übergeben.

Kammer: „Datenschutz steht bei uns an erster Stelle, denn die Sicherheit von Bürgerdaten ist ein geschäftskritischer Faktor für IT-Dienstleister wie Dataport. Gerade Daten der Steuerverwaltungen sind sehr sensibel. Unsere Kunden der norddeutschen Verwaltungen müssen uns vertrauen können, dass wir die Daten sicher verarbeiten und aufbewahren. Datenschutz ist aber mehr als Vertrauen, nämlich ein ständiger Prozess. Mit dem Audit wollten wir das Datenschutz-Konzept des DCS ganz bewusst auf den Prüfstand stellen und von einem externen Gutachter kontrollieren lassen.“

Weichert: „Dataport und das ULD arbeiten bereits viele Jahre gut zusammen. In mehreren Auditverfahren hat sich Dataport bereits als professioneller und datenschutzbewusster IT-Dienstleister dargestellt. Im Umfeld der Steuerdatenverarbeitung sind besonders hohe Anforderungen an die IT-Sicherheit und den Datenschutz zu stellen. Sicherheitslücken und Datenschutzmängel können hier auf einen Schlag viele Bürgerinnen und Bürgern oder Unternehmen treffen. Mit dem ULD-Datenschutzaudit weist Dataport nach, dass es für den ordnungsgemäßen Betrieb der Systeme die notwendigen technischen und organisatorischen Maßnahmen geplant hat.“

Das Konzept des Informationssicherheits-Managementsystems für das Data Center Steuern umfasst auf der Grundlage einer umfangreichen Basis-Dokumentation der eingesetzten IT-Systeme und Programme technische und organisatorische Vorgaben für den Betrieb der Großrechnersysteme der Steuerdatenverarbeitung.

Dataport ist eine Anstalt des öffentlichen Rechts mit Sitz in Altenholz, Schleswig-Holstein, und der IT-Dienstleister der Verwaltungen in Schleswig-Holstein, Hamburg, Bremen und der Steuerverwaltungen Mecklenburg-Vorpommern und Niedersachsen.

Das Data Center Steuern ist das gemeinsame Steuerrechenzentrum von Bremen, Hamburg, Mecklenburg-Vorpommern und

Schleswig-Holstein. Hier werden die Daten von rund 13.000 Arbeitsplätzen in den 58 Finanzämtern der vier Bundesländer verarbeitet und jährlich rund 12 Mio. Steuerbescheide produziert. Als fünftes Trägerland wird noch in diesem Jahr Niedersachsen dem norddeutschen Steuerverbund beitreten. Damit werden ca. 12.500 Arbeitsplätze in 69 Finanzämtern von Niedersachsen hinzu kommen; die Anzahl der im DCS zu erstellenden Steuerbescheide wird sich verdoppeln.

Das Kurzgutachten mit den Ergebnissen der Auditierung veröffentlicht das ULD unter <http://www.datenschutzzentrum.de/audit/register.htm>

## Kabinett beschließt Gesetzentwurf zur Regelung von De-Mail-Diensten

Die Bundesregierung hat am 13.10.2010 den vom Bundesminister des Innern vorgelegten Entwurf eines Gesetzes zur Regelung von De-Mail-Diensten und zur Änderung weiterer Vorschriften beschlossen. Ziel des De-Mail-Gesetzes ist die Schaffung eines Rechtsrahmens für vertrauenswürdige De-Mail-Dienste im Internet.

Per „De-Mail“ sollen in Deutschland ab 2011 Nachrichten und Dokumente vertraulich, zuverlässig und sicher über das Internet versendet werden können. Grundlegende Sicherheitsfunktionen für den elektronischen Nachrichtenaustausch wie Verschlüsselung, sichere Identität der Kommunikationspartner und Nachweisbarkeit (Versand-/Eingangsnachweise), die der heute genutzten E-Mail fehlen, sollen einfach nutzbar und damit breit verfügbar gemacht werden.

Das De-Mail-Gesetz bildet hierfür den rechtlichen Rahmen. Realisiert und betrieben wird De-Mail von staatlich zugelassenen („akkreditierten“) und in der Regel privaten Anbietern, den De-Mail-Providern. Um die Akkreditierung als De-Mail-Provider vom Bundesamt für Sicherheit in der Informationstechnik (BSI) als zuständiger Behörde zu erhalten, müssen die künftigen De-Mail-Provider strenge Auflagen in den Bereichen IT-Sicherheit und Datenschutz erfüllen und die technische Zusammenarbeit mit den De-Mail-Diensten der anderen De-Mail-Anbieter nachweisen. Bürgerinnen und Bürger, Unternehmen, Behörden und sonstige Institutionen können bei einem akkreditierten De-Mail-Anbieter ihrer Wahl ein De-Mail-Postfach er-

öffnen. Hierfür wird eine sichere Identifizierung z.B. durch Vorlage eines Personalausweises erforderlich sein – ähnlich wie bei der Eröffnung eines Bankkontos. Damit sind die Kommunikationspartner eindeutig nachvollziehbar. Der Versand von De-Mails erfolgt über gesicherte Kommunikationskanäle. Die Nachrichten sind vor Mitlesen und Veränderungen geschützt. Der Nutzer kann qualifiziert elektronisch signierte Versand- und Eingangsbestätigungen mit hoher Beweiskraft erhalten („Einschreiben“).

## Begleitstudien zum neuen Personalausweis vorgestellt

Das Bundesinnenministerium hat bei dem Projekt „neuer Personalausweis“ stets den Dialog mit der Öffentlichkeit, Verbraucherschützern und Datenschützern gesucht und schon frühzeitig die Begleitforschung als Teilprojekt in die Gesamtorganisation integriert. Die Begleitforschung wurde in zwei Schritten durchgeführt: Ständen in der ersten Stufe der Begleitforschung (2007 bis 2008) noch die Anforderungen an das Dokument, die Umsetzung in den Personalausweisbehörden und die grundsätzlichen Nutzungsmöglichkeiten im Vordergrund, hat sich die zweite Phase der Begleitforschung (2009 bis 2010) insbesondere mit der Wahrnehmung und den Auswirkungen des Dokuments und seiner Funktionen bei Bürgerinnen und Bürgern sowie Wirtschaft und Verwaltung beschäftigt.

Das Bundesinnenministerium hat folgende vier Studien im Rahmen der zweiten Stufe der Begleitforschung beauftragt:

### Rechtsfragen der Haftung im Zusammenhang mit dem elektronischen Identitätsnachweis

Ruhr-Universität Bochum Lehrstuhl für Bürgerliches Recht, deutsches und internationales Wirtschaftsrecht, insb. IT-Recht, Professor Dr. Georg Borges.

Die Studie untersucht haftungsrechtliche Fragestellungen der Beteiligten bei Nutzung des neuen Personalausweises zum elektronischen Identitätsnachweis.

### Restrisiken beim Einsatz der Ausweis-App auf dem Bürger-PC zur Online-Authentifizierung mit Penetration-Test

Fachhochschule Gelsenkirchen Institut für Internetsicherheit, Prof. Dr. Norbert Pohlmann.

Die Studie dient der Identifizierung technischer Restrisiken bei der Nutzung des

elektronischen Identitätsnachweises im privaten Umfeld und soll Handlungsempfehlungen für die erforderlichen, vom Nutzer umzusetzenden IT-Sicherheitsmaßnahmen geben.

**Sicherheitsanalyse des EAC-Protokolls**  
Technische Universität Darmstadt/CASED Prof. Dr. Johannes Buchmann.  
Die Studie analysiert die kryptographischen Protokolle zum Aufbau einer sicheren Kommunikation zwischen dem neuen Personalausweis (nPA) und einem Lesegerät. Betrachtet werden dabei die Protokolle EAC, PACE und Secure Messaging.

**Nutzbarkeit und Akzeptanz der Software AusweisApp zur Nutzung des neuen Personalausweises**  
Universität Potsdam Hasso-Plattner-Institut, Professor Dr. Christoph Meinel.  
Die Studie beschäftigt sich mit den Fragestellungen, ob die neuen Funktionen des Personalausweises von den Nutzern angenommen werden und wie deren Sicherheitswahrnehmung ist.  
Die Studienergebnisse wurden heute durch die Verfasser und das Bundesinnenministerium am 15.10.2010 der Öffentlichkeit präsentiert und sind in dem Personalausweis, so wie er am 1. November 2010 kommen wird, berücksichtigt.  
Zusammenfassungen der Studienergebnisse sind über die Website des BMI verfügbar.  
Die Studie zu den Restrisiken beim Einsatz der AusweisApp liegt erst als Zwischenbericht vor und wird unmittelbar nach Fertigstellung in Kürze veröffentlicht.

## Berechtigungszertifikate für den neuen Personalausweis

Vertreter der Deutschen Post Com GmbH und der Bundesdruckerei haben am 29.10.2010 als erste Berechtigungszertifikate-Anbieter ihre Registrierungsunterlagen gemäß der Personalausweisverordnung nach dem am 1. November 2010 in Kraft tretenden Personalausweisgesetz persönlich an das Bundesamt für Sicherheit in der Informationstechnik überreicht. D-Trust als Trustcenter der Bundesdruckerei und Signtrust, Trustcenter der Deutschen Post, werden zukünftig Berechtigungszertifikate für zugelassene Diensteanbieter im Bereich des neuen Personalausweises ausstellen.

Über Berechtigungszertifikate können Diensteanbieter für ihre Kunden Online-Dienstleistungen basierend auf der eID-Anwendung des neuen Personalausweises bereitstellen. Das BSI betreibt die Wurzelzertifizierungsinstanz für Berechtigungszertifikate, welche den Zugriff auf ausgewählte Daten des Personalausweises ermöglichen.

## STORK: Interoperabilität von elektronischen Identitäten in Europa

Elf am EU-Projekt STORK teilnehmende europäische Länder starteten am 25.10.2010 Pilotprojekte, um sichere, grenzüberschreitende eID-Dienste anzubieten. Die sechs Pilotprojekte mit den Titeln „Grenzüberschreitende Authentifizierung für elektronische Dienste“, „Safer Chat“, „Studenten-Mobilität“, „Grenzüberschreitende elektronische Zustellung“, „Adressänderung“ und „Kommissionsdienste“ sind ab sofort für die Öffentlichkeit zugänglich. Die sechs Pilotprojekte werden nach dem offiziellen Start nun weiter schrittweise verbessert. Gleichzeitig wird ihre Integration in vorhandene Real-Live-Portaldienste der zugrundeliegenden STORK-Interoperabilitätsplattform erprobt.

Das Projekt STORK (Secure Identity Across Borders Linked) hat zum Ziel im Rahmen des IKT-Förderprogramms der Europäischen Union eine EU-weite Plattform für die Interoperabilität von elektronischen Identitäten (eIDs) einzuführen. Die Plattform wird es den Bürgerinnen und Bürgern ermöglichen, ihre nationalen eIDs für eGovernment-Dienste in mehreren europäischen Ländern zu nutzen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) vertritt in dem von der EU geförderten Projekt die Bundesrepublik Deutschland. Ziel ist es unter anderem, den deutschen Bürgern die Nutzung des neuen Personalausweises auch für Internetangebote aus ganz Europa zu ermöglichen.  
Die sechs laufenden STORK-Pilotprojekte:

### Grenzüberschreitende Authentifizierung für elektronische Dienste:

Mit dem Pilotprojekt wird der sichere Zugang zu vorhandenen Online-Behördendiensten von Mitgliedstaaten durch Bürgerinnen und Bürger aus anderen Mitgliedsstaaten möglich. Sie können ihre eigenen nationalen elektronischen Identitätsnach-

weise für den Zugang zu diesen Diensten nutzen.

### SaferChat:

Um eine höhere Internetsicherheit für Kinder und Jugendliche zu erreichen, werden Lehrerinnen und Lehrer in den verschiedenen Ländern innerhalb festgelegter Altersgruppen Aufgaben und sichere Chatträume für ihre Schülerinnen und Schüler entwickeln. Ziel ist es, grenzüberschreitendes E-Learning zu ermöglichen und die Schülerinnen und Schüler zu ermuntern, mit Altersgenossen in anderen Ländern zusammenzuarbeiten. Es werden darüber hinaus Peer-to-Peer-Bildungspakete zusammengestellt, die vor allem das Bewusstsein für Internetsicherheit schärfen sollen.

### Studenten-Mobilität:

Dieses Pilotprojekt ermöglicht es Studenten, sich mit Hilfe ihres eigenen nationalen elektronischen Ausweises (Personalausweis, digitale Zertifikate) auf Online-Verwaltungsdienste von Universitäten einzuschreiben (Erasmus-Programme), sich zu authentifizieren und andere entsprechende akademische Dienste zu nutzen. Darüber hinaus dient das Pilotprojekt als ein notwendiger erster Meilenstein für die Analyse eines zukünftigen Datenaustauschs zwischen Universitäten unterschiedlicher Länder innerhalb des Europäischen Systems zur Anrechnung von Studienleistungen.

### Grenzüberschreitende elektronische Zustellung:

Ziel dieses Pilotprojekts ist es, nationale Portale für elektronische Zustellungen (e-Delivery) an Bürgerinnen und Bürger aus dem Ausland durch Nutzung ihrer nationalen eID zugänglich zu machen. Darüber hinaus sollen mit diesem Pilotprojekt die öffentlichen Verwaltungen in die Lage versetzt werden, Dokumente an Bürgerinnen und Bürger verschiedener Länder direkt über das e-Delivery-Portal des jeweiligen Landes zu senden.

### Adressänderung:

Mithilfe dieses Pilotprojekts soll eine Plattform für einen interoperablen Dienst zur Adressänderung geschaffen werden. Ausländischen Bürgerinnen und Bürgern wird unter Nutzung ihres eigenen eID-Ausweises ermöglicht, alle relevanten Empfänger über eine Adressänderung zu informieren, ohne dass die derzeit in den einzelnen Mitgliedsstaaten geltenden Verfah-

ren geändert werden. Dieses wird durch die Nutzung der von STORK definierten Interoperabilitätsplattform zur Identifikation und Authentifizierung der eIDs der Bürgerinnen und Bürger sowie durch die Definition zweier Szenarien für die Dienste (Abfrage und Aktualisierung der Adresse) erreicht.

#### Kommissionsdienste:

Der European Commission Authentication Service (ECAS) unterstützt die Anmeldung für eine Vielzahl von Anwendungen der Kommission. Durch die Ergänzung von ECAS in die STORK-Plattform wird die nationale eID nahtlos integriert. Nachdem vor kurzem die technische Integration beendet wurde, werden die Dienste nach und nach durch die Produktionsdienste der Europäischen Kommission optimiert.

### CC-Zertifikat für secunet wall packet filter

Am 19.10.2010, dem Eröffnungstag der IT-Sicherheitsmesse it-sa in Nürnberg, überreichte Bernd Kowalski, Abteilungsleiter beim Bundesamt für Sicherheit in der Informationstechnik (BSI), ein Zertifikat nach Common Criteria an Dr. Rainer Baumgart, Vorstandsvorsitzender der secunet Security Networks AG.

Gegenstand der Zertifizierung ist die Paketfilter-Komponente für IPv4 Netze secunet wall packet filter, Version 3.0.3, eine Software-Komponente, die die Paketfilter-Funktionalität für Netzwerkkomponenten zur Verfügung stellt. Das Zertifikat bestätigt die erfolgreiche Produktprüfung nach Common Criteria, Version 3.1 mit der Vertrauenswürdigkeitsstufe EAL 4+. Die Verbindung von IP-Netzen unterschiedlicher Sicherheitsstufen erfolgt in der Regel unter Einbindung spezieller Netzwerkkomponenten mit Firewall-Funktionalität an deren Übergangsstellen. Diese Komponenten haben die Aufgabe, die unterschiedlichen Netze voneinander zu separieren. Der Datenfluss zwischen den Netzen wird entsprechend definierter Filterregeln entweder erlaubt oder verboten. Der secunet wall packet filter, Version 3.0.3 wird als Modul in andere Produkte, wie Firewalls oder VPN-Komponenten integriert. Er ist daher nicht als Endprodukt für Endkonsumenten gedacht, sondern wird an Entwickler anderer Anwendungen für Netzwerkkomponenten ausgeliefert, die diesen in ihre Anwendung integrieren.

Die SRC Security Research & Consulting GmbH – eine vom BSI anerkannte Prüfstelle für Common Criteria – hat das Verfahren als Prüfstelle begleitet.

### BMBF-Forschungsprojekt: Mobilfunknetze sollen sicherer werden

Im März hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem Bericht festgestellt, dass Sicherheitsrisiken durch Smartphones steigen und sich die Lage im Bereich IT-Sicherheit weiter verschärft. Gerade der mobile Internetzugriff mit Smartphones ist davon betroffen. In einem vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekt – genannt ASMONIA – soll nun ein Konsortium aus Telekommunikationsunternehmen und Wissenschaftsinstituten effektivere Schutzmechanismen für Mobilfunknetze entwickeln. Das Konsortium konzentriert sich auf Sicherheitskonzepte für netzübergreifende Frühwarnsysteme für Mobilfunknetze der 4. Generation. ASMONIA wurde am 1. September 2010 gestartet und soll bis Mai 2013 abgeschlossen sein.

Die Datenflut in den Netzen steigt weiter an: bis 2015 wird der globale Datenverkehr über Mobilfunknetze voraussichtlich auf 23 Exabytes angestiegen sein; das entspricht dem Datenaufkommen von 6,3 Milliarden Menschen, die täglich ein digitalisiertes Buch herunterladen. Heute nutzen 400 Millionen Menschen ein Smartphone, in fünf Jahren werden es drei Milliarden sein.<sup>1</sup> Dabei arbeiten immer mehr Smartphones mit frei verfügbaren, offenen Betriebssystemen, was neue Sicherheitsrisiken birgt. Der Auftrag an ASMONIA lautet demnach, ein netzübergreifendes Schutzkonzept zu entwickeln, damit die Kommunikation via Mobilfunk in deutschen Netzen wieder sicherer wird. Zwei Ziele stehen im Fokus: Zum einen soll die Sicherheit der Endgeräte wie Smartphones verbessert werden, indem neue Verfahren die Verletzung der Systemintegrität erkennen lassen. Zum anderen soll die Sicherheit in den Netzen steigen, indem Angriffe über Netzgrenzen hinweg erkannt, bewertet und abgewehrt werden.

Das Konzept beruht auf einem industrieweiten, neuen Ansatz, das einen klaren Ausgangspunkt hat: Der Datenaustausch

zwischen den Netzbetreibern muss optimiert werden, um in ganz Deutschland und in allen Mobilfunknetzen auf Angriffe entsprechend reagieren zu können. Eingesetzt werden sollen neue Verfahren der Anomalieerkennung von Malware, intelligente Analyseverfahren und elastische Systeme wie Cloud Computing, damit Attacken gegen Netzkomponenten und Endgeräte rasch abgewehrt werden können. Durch das netzübergreifende Zusammenspiel dieser Sicherheitsmechanismen werden Mobilfunknetze und Kommunikationsdienste besser geschützt.

Nokia Siemens Networks hat die Projektleitung von ASMONIA übernommen. Weitere Mitglieder des Projektkonsortiums sind das Fraunhofer-Institut für Sichere Informationstechnologie, Cassidian (bislang EADS Defence & Security), die ERNW GmbH, die Rheinisch-Westfälische Technische Hochschule Aachen und die Hochschule Augsburg. Dieses Konsortium wird in seiner Arbeit durch die Deutsche Telekom AG, das Bundesamt für Sicherheit in der Informationstechnik sowie die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherungsaufgaben unterstützt. Angriffsanalyse und Schutzkonzepte für Mobilfunkbasierte Netzinfrastrukturen unterstützt durch kooperativen Informationsaustausch (ASMONIA) ist ein BMBF-gefördertes Forschungsprojekt zur Entwicklung eines ganzheitlichen Schutzkonzeptes für mobilfunkbasierte Kommunikationsnetze und -dienste. Es adressiert den Schwerpunkt, „Sicherheit in unsicheren Umgebungen / Sicherheit in der mobilen Welt“ der BMBF Bekanntmachung zur Förderung der IT-Sicherheit vom 26.8.2009 [BMBF09]. Weitere Informationen: [www.asmonia.de](http://www.asmonia.de)

### Secrypt: digiSeal® office, komfortable Signaturlösung

digiSeal® office ist eine innovative Signatursoftware für den Einzelarbeitsplatz. Sie bietet nutzerfreundlich neue Funktionen. Die per Grafik-Signet (z.B. eingescannte Unterschrift, Firmenlogo, Wappen o.ä.) ‚sichtbare‘ elektronische Signatur ist nun auf einfache und komfortable Weise völlig frei im PDF, das zu signieren ist, platzierbar.

So erkennt man auf den ersten Blick, dass das Dokument eine elektronische Signatur trägt, die Authentizität und Integrität der Daten gewährleistet.

Daneben lassen die Berliner Spezialisten für die elektronische Signatur die Programm-

<sup>1</sup> Schätzungen von Nokia Siemens Networks

Oberfläche ihres digiSeal® office im neuen Look erscheinen:

Die Funktionsbuttons sind größer und optisch modern gestaltet. Zudem gibt es neue Auswahloptionen (z.B. für das gewünschte Grafik-Signet), die übersichtlich im Dialogfenster angeordnet sind. Neue Voreinstellungen erleichtern schließlich die Auswahl bei qualifizierten Zertifikaten. Dabei werden nach der ersten Konfiguration nicht benötigte Zertifikate der Signaturkarte nicht mehr angezeigt.

Mit dem neuen digiSeal® office geht das Erstellen einer elektronischen Signatur flexibler und schneller vonstatten. Dies vereinfacht den Signaturprozess deutlich.

Weitere Informationen auf [www.secrypt.de](http://www.secrypt.de).

## BvD: Datenschutz wird zum bundesweiten Schulprojekt

Die meisten Schüler nutzen Online-Chats und soziale Netzwerke wie SchülerVZ und Facebook, um schnell und einfach miteinander zu kommunizieren. Dabei stellen viele, bewusst oder unbewusst, sehr persönliche Informationen oder Fotos ins Internet. Denn die jungen User sehen häufig nur Spaß und Kommunikationsmöglichkeiten, nicht aber die Gefahren des Mediums. Um das zu ändern, gehen Mitglieder des Arbeitskreises Schule im Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. direkt in die Klassenzimmer. Das Projekt soll nach zweijährigem Testlauf in NRW, Hessen und Bayern jetzt deutschlandweit erfolgreich sein.

Bisher waren die professionellen Datenschützer ehrenamtlich an Schulen in Nürnberg, Frankfurt, Remscheid und Bielefeld tätig. Weitere Einsätze in Berlin, Brühl und Gütersloh sind terminiert oder in Planung. Hauptzielgruppe sind Schüler in den Jahrgangsstufen 6 und 7. Doch mit der Ausdehnung des Wirkungskreises steigt auch der Ressourcenbedarf. Bessere Unterrichtsmaterialien, technische Ausrüstung wie beispielsweise Beamer und der Einsatz weiterer, auch pädagogisch qualifizierter Datenschützer kosten Zeit und Geld.

Um die Lehrveranstaltungen effizient planen und durchführen zu können, braucht die Initiative jetzt Sponsoren aus der Wirtschaft. Denn für die Schulen soll das Angebot weiterhin kostenlos zur Verfügung gestellt werden.

„Eine Unterstützung würde nicht nur einen großen Imagegewinn in einer hochinteressanten Zielgruppe mit sich bringen,

sondern auch Wissen vermitteln, das später den Arbeitgebern nutzt“, weiß Datenschutzbeauftragter Thomas Floß (Versmold), Sprecher und Initiator des Arbeitskreises.

Die ersten Erfahrungen bestätigen, dass deutlich mehr Aufklärungsarbeit an weiteren Schulen geleistet werden muss. Der Berufsverband hat sich deshalb dafür entschieden, die Aktion „Datenschutz geht zur Schule“ auszuweiten. Wer das Projekt unterstützen oder die eigene Schule als nächsten Einsatzort der Datenschützer vorschlagen möchte, kann über die Internetseite des Bundesverbandes unter [www.bvdnet.de](http://www.bvdnet.de) Kontakt aufnehmen.

## it-sa 2010 erfolgreich

Die it-sa hat sich als eine der bedeutendsten IT-Sicherheitsmessen etabliert. Rund 7100 Besucher (2009: 6600) aus Wirtschaft, Forschung und Behörden haben sich auf der Messe bei 304 Ausstellern (2009: 257) über neueste Produkte und Entwicklungen der IT-Sicherheit informiert. Damit ist die Messe in diesem Jahr deutlich größer geworden. Die Ausstellungsfläche wuchs um 70 Prozent.

Von den vorregistrierten Besuchern kamen ca. 20 Prozent aus Nürnberg und München, während zusammen 80 Prozent aus dem restlichen Bundesgebiet und dem Ausland stammten. In diesem Jahr reisten Fachkräfte aus 27 verschiedenen Ländern zur it-sa nach Nürnberg.

Großer Beliebtheit bei den Besuchern erfreuten sich die vier offenen Foren direkt in der Messehalle. In den drei Tagen wurden hier über 320 Fachvorträge präsentiert. Ein besonderer Publikumsmagnet waren die täglichen Live-Hacking-Vorführungen sowie die Keynotes von Taher Elgamal (Axiway) und Nir Zuk (Palo Alto).

Messe-Premiere hatte die 1000 qm große Sonderfläche „Das perfekte Rechenzentrum“, auf der 22 Unternehmen alle Aspekte rund um die Sicherheit im Rechenzentrum (RZ) abgebildet haben. Ergänzt wurde dieses Ausstellungsangebot durch geführte Touren und das Forum Orange in der Messehalle. Dort gab es überwiegend 15-minütige Vorträge zur RZ-Sicherheit und zur Konvergenz physischer und logischer Sicherheit zu sehen.

Die ebenfalls neue Sonderfläche Convergence-Area war für Besucher eine zentrale Anlaufstelle rund um das Zusammenspiel von physischer und IT-Sicherheit. Alle Ein-

zelkomponenten der Aussteller waren hier miteinander verwoben und boten den Besuchern die Möglichkeit, mit einem vor Ort ausgestellten Unternehmensausweis die Ausstellungsstücke auszuprobieren.

Nach dem großen Erfolg der „IAM-Area“ auf der letztjährigen it-sa präsentierte die Peak Solution GmbH auch dieses Jahr wieder durchgängige Lösungsszenarien rund um das Thema Identity- und Accessmanagement. Die Besucher der Area erhielten praxisnahe Antworten auf alle Fragen zur Planung und Umsetzung von Anwendungen für die effiziente Verwaltung und sichere Nutzung digitaler Identitäten und Berechtigungen.

Ein weiterer Baustein im Erfolgskonzept der it-sa waren auch 2010 die zahlreichen Workshops, Tagungen und Mitgliederversammlungen im direkt angeschlossenen Kongresszentrum. Insgesamt luden 14 Fachveranstaltungen zum Besuch ein, unter anderem ein Grundschutztag des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie der it-sa Datenschutztag, organisiert von Computas.

Die it-sa bot auch dieses Jahr eine im deutschsprachigen Raum einmalige Konzentration auf das Thema IT-Sicherheit. Die nächste it-sa findet vom 11.–13. Oktober 2011 in Nürnberg statt.

## Fraunhofer beruft Prof. Michael Waidner in die Institutsleitung des SIT

Professor Dr. Michael Waidner wird Mitglied in der Institutsleitung des Fraunhofer-Instituts für Sichere Informationstechnologie SIT. Ab 1. Oktober 2010 übernimmt er die Leitung des eigenständigen Institutssteils Darmstadt während sich die langjährige Institutsleiterin Professor Claudia Eckert ganz dem Ausbau des Institutssteils München widmet. Einmal mehr ist es Fraunhofer gelungen, einen namhaften Wissenschaftler zu gewinnen, der bislang in der Industrie und im Ausland tätig war. Michael Waidner war bislang Chief Technology Officer für Sicherheit bei IBM. Bis 2006 leitete er die Sicherheitsforschung im IBM Zurich Research Laboratory in Rüschlikon, Schweiz, wo er sich unter anderem durch seine Arbeiten zum technischen Datenschutz, zum Sicherheitsmanagement und zur mathematischen Beweisbarkeit von Sicherheitseigenschaften einen Namen machte. 2006 wechselte er von der Schweiz zur Firmenzentrale nach New York, wo er

als Hauptverantwortlicher für technische Strategie und Sicherheitsarchitektur maßgeblich daran beteiligt war, IBM zu einem der erfolgreichsten Anbieter von IT-Sicherheitsprodukten und Dienstleistungen zu machen.

Professor Michael Waidner ist auch langjähriges Mitglied des Beirats unserer Zeitschrift. Die Herausgeber gratulieren ihm zur Berufung.

## Veranstaltungsbesprechungen

**Britta Mester**

**Tagungsbericht von der DSRI-Herbstakademie 2010, 8. – 11. 09. 2010 in München**

Bereits zum 11. Mal fand vom 8.-11. September 2010 die Herbstakademie der Deutschen Stiftung für Recht und Informatik (DSRI) statt. Als diesjähriger Veranstaltungsort wurden die beeindruckenden Räumlichkeiten des Münchner Künstlerhauses gewählt. Die Herbstakademie ist inzwischen eine der bedeutendsten Konferenzen zum IT-Recht und zeichnet sich insbesondere dadurch aus, dass aktuelle und praxisrelevante Themen Gegenstand der zahlreichen Referate und Diskussionen sind. In diesem Jahr stand die Tagung unter dem Titel „Digitale Evolution – Herausforderungen für das Informations- und Medienrecht“. Erstmals wurde ein Teil der Tagung in parallele Workshops aufgeteilt, so dass für die Teilnehmer und Teilnehmerinnen die Möglichkeit bestand, sich zur Vertiefung spezieller Fragen aus dem Informationsrecht einen Themenbereich auszuwählen.

Nach Begrüßung durch den Vorsitzenden des Vorstands der DSRI, Prof. Dr. Jürgen Täger, eröffnete mehrere Vorträge zur Novellierung und zu aktuellen Fragen des Datenschutzrechts die Veranstaltung. Thematisch bildete das Datenschutzrecht in diesem Jahr aufgrund der Gesetzesänderungen und zahlreicher Konflikte einen Schwerpunkt. Nach einem Überblick von RA Dr. Flemming Moos über die mit den BDSG-Novellierungen im Jahr 2009 eingetretenen und noch zu erwartenden Änderungen wurde der Beschäftigtendatenschutz und der hierzu vorliegende Regierungsentwurf einer gesetzlichen Neuregelung von RA Dr. Marc Philipp Weber behandelt. Diana Kunst, LL.M. setzte sich im Zusammenhang mit der rechtlichen Beurtei-

lung des e-Discovery auch mit den dabei zu berücksichtigenden besonderen Datenschutzanforderungen hinsichtlich der Beschäftigtendaten auseinander. RA Stephan Schmidt, Akad. Rat. Florian Albrecht, M.A., und RA David Seiler thematisierten in ihren Vorträgen den neuen § 32 BDSG und die rechtliche Zulässigkeit des Mitarbeiterscreenings aus verschiedenen Blickwinkeln.

Gleich drei Vorträge befassten sich mit der für die Praxis besonders relevanten „Auftragsdatenverarbeitung“. RA'in Dr. Anna Gosche sowie Justiziarin Dorothee Freise, LL.M. berichteten von den bisher mit § 11 BDSG gemachten Erfahrungen; RA Dr. Uwe Hajda problematisierte besonders die Umsetzungsprobleme in Unternehmen.

Verfassungsrechtlichen Fragestellungen kennzeichneten die Vorträge von RA'in Dr. Britta Heymann, die sich mit dem Spannungsverhältnis zwischen Persönlichkeits- und Kommunikationsgrundrechten beschäftigte, sowie von RA Dr. Christoph Ritzer und Dipl.-Jur. Martin Sebastian Haase, LL.M., die jeweils europarechtliche Aspekte einbrachten. Konkrete und sehr aktuelle Anwendungsszenarien waren Gegenstand der Vorträge der Dipl.-Informatikerin Petra Beenken zusammen mit Dr. jur. Silke Jandt zum intelligenten Energienetz (smart meter) und von RA Thomas Spohr zum Elektronischen Patientendossier. RA Lennart Schübler und RA Prof. Dr. Rainer Erd behandelten den hoch aktuellen Datenschutz in Sozialen Netzwerken.

In einem weiteren, von RA'in Dr. Ursula Widmer am Samstag moderierten Workshop zeigte RA Joachim Dorschel auf, wie Datenschutz und IT-Sicherheit bei der Vertragsgestaltung berücksichtigt werden. Dr. Elisabeth Hödl und RA'in Dr. Christina Hofmann prüften die Rechtmäßigkeit des Listbrokings in Österreich; RA Dr. Sebastian Meyer, LL.M. stellte die Interpretation der vom Betroffenen selbst in das Netz gestellten Daten als konkludente Einwilligung zur Datenverarbeitung in Frage.

In dem von RA'in Dr. Henriette Picot moderierten Workshops „Gaming“ stand neben der Erörterung von Rechtsfragen von Computerspielen (RA Tobias Haar und Dr. Andreas Lober) vor allem der Jugendschutz im Netz, insbesondere im Hinblick auf geplante Reformen, in den Vorträgen von Dr. Britta A. Mester und von RA'in Nadine Schützel im Mittelpunkt. Aus datenschutzrechtlicher Sicht waren die Beiträge von RA Lawrence J. Siry Ph. D. JD BA und Sandra Schmitz, LL.M. sowie von RA Thorsten Feldmann,

LL.M. zu online betriebenen Archiven von großer Relevanz.

Neben diesen datenschutzrechtlichen Themen gab es zahlreiche weitere hoch interessante und aktuelle Beiträge zum Telekommunikations-, Softwarevertrags-, Immaterialgüter- und Internetrecht. So ging es etwa in dem von RA Henning Krieg, LL.M. moderierten Workshop zum Internetrecht u. a. in einem von RA Dr. Oliver M. Habel gehaltenen Vortrag um die Zulässigkeit personalisierter Werbung in Social Communities. Darüber hinaus thematisierte Maximilian Becker Struktur und Schutzbereich des Domainrechts, und RA Sami Bdeiw die wirksame Einbeziehung von AGB's im elektronischen Geschäftsverkehr. Der Workshop schloss mit einem Überblick über die Rechtsfragen bei der Abwicklung von Zahlungsströmen über E-Commerce-Plattformen von RA Dr. Stephan Appt, LL.M. sowie einem Update zum Internetrecht von RA Jan Pohle.

Abgerundet wurde diese außergewöhnlich Veranstaltung wieder einmal durch ein ebenso eindrucksvolles Rahmenprogramm, welches mit einer Begrüßung durch die Münchener Stadträtin RA'in Beatrix Zurek im Neuen Rathaus sowie eines Besuchs in den außergewöhnlichen Räumen der „Juristischen Bibliothek“ im Rathaus begann. Bei einer Führung durch die Sonderausstellung „Das Oktoberfest 1810-2010“ des Münchner Stadtmuseums sowie einem Abendessen im historischen „Augustinerkeller“ gelang das Networking auf angenehme Weise.

Der voluminöse Tagungsband zur Herbstakademie 2010 mit den wissenschaftlichen Beiträgen aller Referenten ist bereits zu dem günstigen Preis von 49,80 € erschienen; er sollte in keiner Bibliothek von Informationsrechtlern fehlen. Er ist über den Buchhandel erhältlich und kann über [mail@olwir.de](mailto:mail@olwir.de) direkt bestellt werden.

**Helmut Reimer**

**ISSE / GI-Sicherheit 2010, 05. bis 07. Oktober 2010 in Berlin**

Die von der eema und TeleTrusT mit Unterstützung der Europäischen Kommission gegründete Konferenz Information Security Solutions Europe (ISSE) fand in diesem Jahr zum 12. Mal statt. Konferenzpartner war die Gesellschaft für Informatik (GI) mit der alle zwei Jahre stattfindenden Jahrestagung des Fachbereiches Sicherheit. Für das Gastgeberland übernahm Bundesinnenminister Dr. Thomas de Maizière die

Schirmherrschaft über die Veranstaltung. Das Maritim-Hotel Berlin in der Stauffenbergstrasse bot ein angemessenes Ambiente für die inhaltlich breit gefächerten Angebote der Konferenz, die diesmal 470 Teilnehmer aus 27 Ländern besuchten. Aus Deutschland kamen rund 300 Interessierte, darunter hatten sich 81 speziell für die GI-Sicherheit angemeldet. An der Ausstellung beteiligten sich über 25 Institutionen und Unternehmen.

Deutschland hat die Chance ausgiebig genutzt, auf einer unabhängigen europäischen IT-Sicherheitskonferenz politische Positionen und technische Innovationen und Entwicklungen international zur Diskussion zu stellen. Der Bundesinnenminister sprach in seiner – von den Konferenzteilnehmern sehr positiv aufgenommenen – Keynote zur Eröffnung der Konferenz einige Eckpunkte der Internetpolitik der deutschen Regierung an. Er verdeutlichte, dass IT-Sicherheit als politisches Ziel nur durch gemeinsame Aktivitäten von Forschung, Wirtschaft und Verwaltung schrittweise verbessert werden kann und nur in Ausnahmefällen mit neuen staatlichen Regulierungen unterstützt werden sollte. Ebenso sieht er die Sensibilisierung aller Beteiligten – insbesondere aber der Internetnutzer – als dauerhafte Aufgabe in Verantwortung aller Beteiligten. Auf europäischer Ebene verfolge Deutschland das Ziel, europaweit Sicherheitsthemen für die IT zu etablieren und so ein harmonisiertes IT-Sicherheitsniveau in der EU zu fördern, auf das sich alle Beteiligten verlassen können. Wichtige Dienste auf dem Weg dorthin leistet die seit 2004 bestehende Europäische Agentur für Netz- und Informationssicherheit „ENISA“, deren Position gestärkt werden sollte.

In weiteren Keynotes nahmen *Bernd Kowalski* (als Vertreter des BSI-Präsidenten *Michael Hange*) zur Notwendigkeit internationaler IT-Sicherheitsstandards und *Jürgen Maurer* (Vizepräsident des BKA) zum Stand der Ermittlungen gegen Identitätsdiebstahl, Bankkartenmissbrauch und Internetkriminalität Stellung.

Wenige Wochen vor dem Start der Ausgabe des neuen Personalausweises wurde die ISSE auch dazu genutzt, um die inhaltlichen Elemente der eID-Funktionalität und ihrer Anwendung in einem Workshop ‚eID and the New German Identity Card‘ vorzustellen. Mit ca. 85 Teilnehmern hatte dieser Workshop eine hervorragende Resonanz. Die inhaltliche Vorbereitung der ISSE 2010 / GI-Sicherheit erfolgte im von TeleTrust geleiteten internationalen Programmkomitee der ISSE mit eema und der ENISA (European Network and Information Security Agency) und parallel in einem eigenen Programmkomitee der GI-Sicherheit. In Fachkreisen besitzt die ISSE ungebrochene Anziehungskraft. Dem internationalen Programmkomitee lagen über 100 Beitragsvorschläge vor und für die GI-Sicherheit gab es 50 Angebote. Deren Evaluierung ermöglichte ein qualitativ anspruchsvolles Programm mit gemeinsamen Plenarveranstaltungen am ersten, zweiten und letzten Konferenztag und fünf parallelen Tracks (drei für die ISSE und zwei für die GI-Sicherheit). Zusätzlich gab es einen weiteren Track mit anwendungsorientierten Beiträgen einiger Sponsoren.

Die Keynote von Microsofts Vizepräsident für Trustworthy Computing, *Scott Charney*, behandelte das Thema ‚Rethinking the Cyber Treat: Creating a Safer, More Trusted Internet‘. Die Präsentation beruht auf einer Ausarbeitung von ihm ‚Collective Defense – Applying Public Health Models to the Internet‘, die auf der Download-Website von Microsoft verfügbar ist. Nach dem Vorbild des Gesundheitswesens, das Personen mit ansteckenden Krankheiten durch Quarantäne isoliert, um keine weiteren Personen anzustecken, sollen infizierte Geräte in Netzen erkannt und betroffene Anwender informiert, und bei der Lösung des Problem unterstützt werden. Nur Geräten mit einem „gültigen Gesundheitspass“ sollte die Anbindung ans Internet erlaubt werden. Charneys Ideen sind eng an die bereits in modernen Windows-Versionen als Network Access Protection (NAP) integrierte Schutztechnik für Unternehmensnetze angelehnt. Auch dort prüfen Health Registration Authorities (HRAs) von Clients vorgelegte Health Certificates und entscheidet dann, ob das Gerät Zugriff auf das restliche Netzwerk erhält. Ob sich dieses Konzept auch für Internetzugänge einsetzen lässt, bleibt offen. Die Idee ist an sich nicht neu und korrespondiert mit Initiativen zur Bekämpfung von Botnet-Angriffen in Deutschland (eco/BSI), Australien, Kanada, Japan, Südkorea und den Niederlanden.

In den Konferenztracks der ISSE wurden insgesamt 54 Beiträge geboten. Schwerpunkte bildeten

- Identity and Security Management,
- Technical and Economical Aspects of Cloud Security,
- Security Services and Large Scale Public Applications,
- Privacy and Data Protection,

- Threats and Countermeasures,
- Smart Grid Security and Future Aspects,
- Biometrics and Technical Solutions.

Fast alle Beiträge sind im Tagungsband zur ISSE dokumentiert.

Auf der ISSE vergibt TeleTrust jährlich für herausragende IT-Sicherheitsprodukte oder -lösungen einen Innovationspreis. Den ‚TeleTrust Innovation Award 2010‘ erhielt mit dem Votum einer internationalen Jury das Berliner Fraunhofer-Institut für offene Kommunikationssysteme (FOKUS) für die Entwicklung einer technischen Lösung, die die Verwendung des neuen Personalausweis mit Microsofts fortgeschrittener Generation der kryptographischen ‚U-Prove-Technologie‘ koppelt. Damit wird eine Technologie gewürdigt, die die informationelle Selbstbestimmung in der globalen virtuellen Welt fördert und personenbezogene Daten schützt.

Schon Tradition hat die zusammenfassende Bewertung der aktuellen Erkenntnisse zur Sicherheit von Kryptoverfahren durch den führenden europäischen Kryptologen *Bart Preneel* im Abschlussplenum der Konferenz. Er konnte feststellen, dass im vergangenen Jahr keine qualitativ neuen Angriffe auf die Sicherheit von Kryptoverfahren bekannt geworden sind. Er verdeutlichte jedoch erneut, dass die letztendlichen Grundlagen aller IT-Sicherheitslösungen selbst verletzlich bleiben und dass ein kompetentes Forschungsumfeld erforderlich ist, um mit Innovationen und Angriffen sensibel umgehen zu können.

Das Rahmenprogramm der ISSE bot wiederum Möglichkeiten für Fachgespräche und die Anbahnung von Kontakten.

Die wichtigsten Beiträge der Konferenz sind im Buch zur ISSE 2010 zusammengefasst:

Norbert Pohlmann, Helmut Reimer, Wolfgang Schneider (Editors)

ISSE 2010 – Securing Electronic Business Processes, Vieweg + Teubner Verlag | Springer Fachmedien Wiesbaden GmbH 2011, ISBN 978-3-8348-1438-8, 407 S.

## Buchbesprechungen

Ulrich Fastenrath

Giesen, Thomas; Bannasch, Bernhard; Naumann, Tino; Dehoust, Matthias; Mauersberger, Thomas: **Kommentar zum Sächsischen Datenschutzgesetz, LexisNexis, 1. Aufl. 2010, 454 Seiten**

Dieser Kommentar schließt eine Lücke. Das Datenschutzrecht des Bundes und der Län-