diesem Jahr sind es nur noch 37 Prozent. In Deutschland liegt der Anteil 2011 gerade einmal bei 28 Prozent. Hierzulande werden derartige Schutzprogramme kaum längerfristig wahrgenommen. Nur 23 Prozent der befragten Unternehmen beteiligten sich länger als zwei Jahre.

**Zwiespältige Einstellung gegenüber staatlichen Schutzprogrammen**

Unternehmen sind hin- und hergerissen, wenn es um ihre Einstellung gegenüber staatlichen CIP-Programmen geht. Gefragt, was sie von den Schutzprogrammen der Regierung halten, enthielten sich 42 Prozent einer Antwort oder bewerteten diese als neutral (in Deutschland: 46 Prozent). Generell zeigten Unternehmen dieses Jahr im Vergleich zu 2010 eine geringere Bereitschaft, sich an CIP-Programmen ihrer Regierung zu beteiligen (57 Prozent in 2011 gegenüber 66 Prozent in 2010, in Deutschland sind es sogar nur 47 Prozent).

**Mangelhafte Vorbereitung auf den Ernstfall**

Grundsätzlich fühlen sich Unternehmen dieses Jahr auf einen Cyberangriff weniger gut vorbereitet als in 2010. Das überrascht nicht: Wenn eine Organisation Cybergefahren als gering einschätzt, wird sie sich auch nicht mit aller Kraft dagegen wappnen. Nach Selbsteinschätzung der Unternehmen verringerte sich ihre Fähigkeit, Angriffe abzuwehren, im Durchschnitt um acht Prozentpunkte: So gaben in der aktuellen Studie 60 bis 63 Prozent an, dass sie wenig bis sehr gut gegen Attacken gerüstet sind – verglichen mit 68 bis 70 Prozent in 2010. In Deutschland fühlen sich dieses Jahr nur 48 bis 57 Prozent wenig bis sehr gut geschützt.

## Die Datenschutzbeauftragten in Behörde und Betrieb. 9. Auflage der Info 4 des BfDI

Diese Broschüre stellt die wichtigsten Rechtsvorschriften für interne Datenschutzbeauftragte vor, verbunden mit einführenden Erläuterungen und praktischen Hinweisen. Sie richtet sich an die internen Datenschutzbeauftragten, aber auch an die interessierten Bürger und Mitarbeiter in Unternehmen und Verwaltungen.
Sie steht unter *http://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO4.html?nn=409164*
zum Download zur Verfügung.

## Plädoyer für ein gemeinsames Cyberverständnis möglichst vieler Staaten

Auf der London Conference on Cyberspace, die am 1. und 2. November 2011 auf Einladung des Außenministers William Hague in der britischen Hauptstadt stattfand, plädierte die Beauftragte der Bundesregierung für Informationstechnik, Staatssekretärin Cornelia Rogall-Grothe, für ein verantwortliches Verhalten der Staatengemeinschaft im Cyber-Raum auf Basis eines breit konsentierten Verhaltenskodexes.

In ihrer Rede vor hochrangigen Regierungsvertretern aus der ganzen Welt legte Rogall-Grothe die Haltung der Bundesregierung zu der international zunehmend diskutierten Frage dar, wie Konflikte zwischen Staaten im ökonomischen und gesellschaftlichen Interesse verhindert und bewältigt werden können. „Bei allen unterschiedlichen Interessen in einer differenzierten Welt kann es – nicht zuletzt unter ökonomischen Gesichtspunkten – einen gemeinsamen Nenner geben: bei der Achtung von Menschenrechten, beim Bemühen um die Stabilität der kritischen Infrastrukturen gegen Ausfälle sowie im Rahmen der (digitalen) Entwicklungshilfe", erläuterte sie in London.

Zu einer gemeinsamen Grundhaltung von einem freien und sicheren Cyberraum führte Rogall-Grothe aus: „Ein für alle Staaten offenes und von möglichst vielen zu teilendes Verständnis könnte die Sicherheit sowie Berechenbarkeit von Aktivitäten im Cyberraum, Transparenz sowie vertrauens- und sicherheitsbildende Maßnahmen, die Bekämpfung von Cyberkriminalität sowie die internationale Zusammenarbeit erfassen". Aus einem solchen gemeinsamen Cyberverständnis ließen sich, in Übereinstimmung mit internationalem Recht, eine Reihe genereller Prinzipien ableiten, die von einer friedvollen Nutzung des Cyberraums bis hin zur Zusammenarbeit von Staaten bei schwer zuzuordnenden Cyberattacken sowie konkreten vertrauensbildenden Maßnahmen und Kooperationsmechanismen reichen. Für einen im Entstehen begriffenen internationalen Rechtsrahmen könne man, so Rogall-Grothe, zunächst an ein politisch verbindliches „Soft Law"-Instrument denken, das langfristig auch rechtlich verbindlich weiterentwickelt werden könne.

Der Redetext ist auf der Website *http://www.cio.bund.de/SharedDocs/Reden/DE/2011/20111101_london_conference_on-cyberspace_bfit.html* verfügbar.

## DFG-Graduiertenkolleg „Neue Herausforderungen für die Kryptografie in ubiquitären Rechnerwelten"

Großer Erfolg für das Horst Görtz Institut und die Ruhr-Universität Bochum: Ihr Antrag auf Einrichtung eines Graduiertenkollegs wurde von der Deutschen Forschungsgemeinschaft (DFG) angenommen. Dieses startet 2012 und wird von der DFG für viereinhalb Jahre mit über 4 Millionen Euro gefördert. In dieser Zeit wollen die IT-Experten vor allem für mehr Sicherheit in zukünftigen IT-Anwendungen sorgen. Konkrete Beispiele sind die intelligente Verkehrslenkung oder der elektronische Personalausweis und deren Vernetzung über die „Cloud". Es handelt es sich um das einzige Graduiertenkolleg in Deutschland, das die ständig wichtiger werdende Datensicherheit als Thema hat.

**Sicherheit im Internet der Dinge**

Im digitalen Zeitalter sind kommunizierende medizinische Implantate oder die Kommunikation zwischen Automobilen längst Realität geworden. Diese Anwendungen agieren im Allgemeinen nicht in geschlossenen Netzen, sondern senden Daten zwischen kleinen eingebetteten Knoten und der „Cloud", einem üblicherweise sehr großen und oft nicht scharf definierten Server und PC-Netz. Dabei weisen die neuartigen Anwendungen einen erheblichen Sicherheitsbedarf auf, beispielsweise bei der intelligenten Verkehrslenkung oder der Schutz digitaler Inhalte für den iPod oder das Kindle e-Buch. Im GRK 1817 „Neue Herausforderungen für die Kryptografie in ubiquitären Rechnerwelten" sollen die Grundlagen für die Sicherheit in diesen sogenannten pervasiven Anwendungen erforscht werden. Ebenso werden die Wissenschaftlerinnen und Wis-