Rede

von Frau Staatssekretärin Rogall-Grothe auf der

Fachkonferenz des DStGB

am 13. Juni 2012

Titel:

„Cyber-Sicherheit für Deutschland“

Sperrfrist: Redebeginn.

Es gilt das gesprochene Wort.

Begrüßung

Sehr verehrte Damen und Herren,

auch ich begrüße Sie herzlich zur Fachkonferenz „Bürgernahe Sicherheitskommunikation für Städte und Gemeinden – Schutz Kritischer Infrastrukturen“.

Informationstechnik, insbesondere das Internet sind integrale Bestandteile unseres Lebens geworden. Dies gilt für unsere geschäftlichen als auch für unsere privaten Aktivitäten. Note- und Netbooks, Smartphones und Navigationsgeräte sind aus unserem Alltag nicht mehr wegzudenken. Eine Studie des Instituts der deutschen Wirtschaft in Köln vom November letzten Jahres ist zu dem Ergebnis gekommen, dass die Hälfte aller Unternehmen in Deutschland inzwischen vom Internet abhängig ist. Was das bedeutet, führt uns eine Schätzung aus der Schweiz vor Augen, wonach bei einem Totalausfall der Informatik 25 Prozent der Unternehmen Insolvenz anmelden müssten, wenn der Schaden nicht innerhalb kürzester Zeit behoben werden könnte. Nach dieser Schätzung wäre das beispielsweise bei einer Bank schon nach zwei, bei einem Handelsunternehmen nach drei Tagen der Fall.

Auch in der Verwaltung nutzen wir moderne Informationstechnologie. Für viele Städte und Gemeinden gehört eGovernment heute zum Tagesgeschäft.

Bedrohungslage

Um die Chancen weiter ausbauen zu können, müssen wir uns auch mit den **Schattenseiten** der Internetnutzung beschäftigen. Computersysteme haben systemimmanent Anfälligkeiten, ihre digitale Vernetzung potenziert die Gefahren. Hinzu kommt, dass auch die Internetkriminalität rapide zunimmt.
Täglich werden durchschnittlich **13 neue Schwachstellen in Standard-Programmen** entdeckt. Durchschnittlich **alle zwei Sekunden wird ein neues Schadprogramm** beziehungsweise eine Variante eines Schadprogrammes erstellt. Täglich werden ca. **21.000 Webseiten** weltweit mit Schadprogrammen **infiziert**.
Die Zahl der **Cybercrime-Fälle** ist im Jahr 2010 **um 19 Prozent gestiegen**. Bei fast der Hälfte dieser Fälle handelt es sich um Computerbetrügereien wie z.B.

Phishing von Onlinebanking-Daten oder den missbräuchlichen Einsatz von Kreditkartendaten.
Der **Schaden aller Cybercrime-Delikte** beziffert sich im Jahre 2010 auf **61,5 Mio. Euro.**
Auch die Bundesverwaltung war 2011 Ziel eines Angriffs auf den Zoll. Dabei waren sensible Daten der Bundespolizei betroffen. Auch Kommunen melden sich immer öfter beim BSI mit IT-Problemen und erfragen Unterstützung bei deren Lösung.

Das Schadprogramm **Stuxnet** hat gezeigt, dass nicht nur das Internet sondern auch industrielle Infrastrukturen, die als vom offenen Internet abgetrennt galten, von gezielten IT-Angriffen nicht mehr ausgenommen sind. Stuxnet hat uns vor Augen geführt, dass die Sammlung von Informationen zur Abschätzung der Bedrohung eine erhebliche Zeit in Anspruch genommen hat. Informationen, die notwendig sind, um Schäden zu verhindern beziehungsweise Schäden zu minimieren. Dies hat die Bundeskanzlerin im Oktober 2010 zum Anlass genommen und das BMI beauftragt, eine Cyber-Sicherheitsstrategie zu entwickeln. Kritische Infrastrukturen wie zum Beispiel der **Energie-, der**

Telekommunikations- oder der Finanzsektor sind vor IT-Angriffen **besonders** zu **schützen, weil Beeinträchtigungen ihrer IT-gestützten Prozesse** die Lebensgrundlagen und den wirtschaftlichen Wohlstand in Deutschland erheblich gefährden könnten. Zu den Kritischen Infrastrukturen gehören aber auch die **öffentlichen Verwaltungen von Bund, Ländern und Kommunen**. Zur Verbesserung der IT-Sicherheit für die Bundesverwaltung existiert bereits seit 2007 der **Umsetzungsplan Bund**. Mit der Erarbeitung gemeinsamer Standards - auch Sicherheitsstandards für eGovernment Anwendungen - beschäftigt sich der **IT-Planungsrat**, in dem ich in diesem Jahr den Vorsitz habe. Weitere Maßnahmen sind erforderlich, ich komme später noch einmal darauf zurück.

Cyber-Sicherheit ist gemäß der Bedeutung der IT **auf einem hohen Niveau** zu **gewährleisten**, **ohne dabei die Chancen, die das Internet bietet**, zu beeinträchtigen.

Cyber-Sicherheitsstrategie für Deutschland:

Aus diesem Grunde hat die Bundesregierung im **Februar 2011** die Cyber-Sicherheitsstrategie für Deutschland beschlossen.
Kernpunkte dieser Strategie sind

- der **verstärkte Schutz Kritischer Infrastrukturen** vor IT-Angriffen
- der Schutz der IT-Systeme in Deutschland einschließlich einer **Sensibilisierung** der **Bürgerinnen und Bürger**
- der **Aufbau eines Nationalen Cyber-Abwehrzentrums** sowie die **Einrichtung eines Nationalen Cyber-Sicherheitsrates**.

Nationales Cyber-Abwehrzentrum:

Die Einrichtung eines Nationalen Cyber-Abwehrzentrums war dringend geboten, um die Handlungsfähigkeit bei IT-Vorfällen zu verbessern. Cyber-Kriminelle orientieren sich nicht an Behördenstrukturen oder Zuständigkeiten.

Das wichtigste Mittel zur Schadensverhinderung beziehungsweise Schadensminimierung sind Informationen. Dazu gehören Informationen zu technischen Fragen, zu möglichen Schäden von potenziell Betroffenen und zu Tätern sowie das Erfahrungswissen von allen Bundesbehörden, die mit IT-Angriffen befasst sind. Mit dem **Cyber-Abwehrzentrum**, in dem das Bundesamt für Sicherheit in der Informationstechnik gemeinsam mit anderen relevanten Behörden **eine Informationsplattform bildet,** ermöglicht es uns, **schnell und abgestimmt alle wesentlichen Informationen** zu einer Schadsoftware oder einem IT-Angriff aber auch zu den möglichen Schäden und Folgen **vorliegen** zu haben. Diese können wir analysieren und **Empfehlungen zum Schutz** der IT-Systeme wie auch weiteren Schadensminimierungsmaßnahmen zur Verfügung zu stellen.

Die aufsichtsführenden Bundesbehörden über die Betreiber der Kritischen Infrastrukturen werden wir im Laufe des Jahres in die Arbeit des Cyber-Abwehrzentrums integrieren, die ersten Behörden

bereits in den nächsten Wochen. In einem zweiten Schritt soll dann ebenfalls die Anbindung von Aufsichtsbehörden auf Länderebene erfolgen – das Know How und die Analysen zu Cybersicherheit sollen auf diesem Weg mit allen involvierten und verantwortlichen Behörden ausgetauscht werden. Schon jetzt möchte ich Ihnen im Vorgriff ans Herz legen, dass ein solches Konzept nur funktioniert, wenn alle Beteiligten sich in die Zusammenarbeit aktiv einbringen. Gerade beim Schutz Kritischer Infrastrukturen ist ein hoher Grad an Expertise bei Ländern und auch Kommunen verortet – gemeinsam mit der Cybersicherheitskompetenz im BSI wird uns dies zu enormer Schlagkraft beim Cyberschutz in Deutschland verhelfen.

Die im Cyber-Abwehrzentrum vertretenen Behörden haben unterschiedliche Aufgaben, aber eins gemeinsam: Sie bündeln ihre Erkenntnisse und Erfahrungen hinsichtlich neuer technischer Bedrohungen, die sie im Rahmen ihrer Aufgaben erlangen.

Mit dem Nationalen Cyber-Abwehrzentrum setzen wir unsere präventive Sicherheitspolitik fort. Es geht hier um Schadensvermeidung oder –minimierung durch schnellstmögliche Information. Mit der Einrichtung des Nationalen Cyber-Abwehrzentrum kam die Bundesregierung ihrer gesamtstaatlichen Verantwortung zur Verbesserung der IT-Sicherheit nach.

Cyber-Sicherheitsrat:

Cyber-**Sicherheit** ist eine gemeinsame – Staat und Wirtschaft gleichermaßen fordernde – Herausforderung. Nur in einem vernetzten Ansatz lassen sich präventive Instrumente und übergreifende Politikansätze koordinieren. Aus diesem Grund hat die Bundesregierung einen Cyber-Sicherheitsrat unter meiner Verantwortung ins Leben gerufen:
Drei **Sitzungen** auf Staatssekretärs-Ebene - auch von zwei Ländervertretern und unter Beteiligung assoziierter Wirtschaftsvertreter - haben bereits stattgefunden und es wurden Themenschwerpunkte **festgelegt**.
Aufgrund der geschilderten Bedrohungslage und der Abhängigkeit von verfügbarer Informations- und

Kommunikationstechnik in den Unternehmen der kritischen Infrastrukturen hat der Cyber-Sicherheitsrat aktuell seinen **Fokus** auf die Koordinierung des Vorgehens bei der **Absicherung der Kritischen Infrastrukturen** gegen IT-Beeinträchtigungen gerichtet. Weitere Themen sind **neue Technologien** und damit zusammenhängende Sicherheits-Herausforderungen und die **Position Deutschlands in internationalen Gremien zu Cyber-Fragen**. Diese internationale Dimension der Cyber-Sicherheit nimmt enorm an Bedeutung zu. Alle Staaten hängen am Internet, derzeit sind 2 Mrd. Menschen online, insbesondere in den Schwellenländern Südamerikas, Afrikas und Asiens warten Millionen Menschen auf weiteren Zugang. Daher müssen wir auch mit den Regierungen anderer Staaten über die Verbesserung der Sicherheit im Internet diskutieren und Vereinbarungen treffen. Ich komme später noch einmal auf das Thema zurück.

Ein weiteres Thema war in der letzten Sitzung am 31.5. der **größere Schutz der IT der Landes- und Kommunalverwaltungen**. Derzeit erarbeitet eine Unterarbeitsgruppe des IT-Planungsrates Vorschläge für

den Aufbau von CERT-Strukturen in den Ländern und deren Vernetzung mit dem BSI. Der Cyber-Sicherheitsrat hat die dort vertretenen Landesvertreter aufgefordert, über Fortschritte regelmäßig zu berichten.

Schutz Kritischer Infrastrukturen

Der wesentliche Kernpunkt der Cyber-Sicherheitsstrategie betrifft den Schutz der Kritischen Infrastrukturen.
Zum Schutz der Kritischen Infrastrukturen wurde seit 2005 der **Umsetzungsplan KRITIS** erarbeitet und 2007 beschlossen. Dieser sieht vor, dass privatwirtschaftliche Betreiber **Kritischer Infrastrukturen** und der **Staat eng beim IT-Schutz dieser Infrastrukturen zusammenarbeiten**. Dieser kooperative Gedanke hat sich **bewährt** und wird mit der Cyber-Sicherheitsstrategie explizit **fortgeführt**.

Der IT-Schutz Kritischer Infrastrukturen hat im BMI höchste Priorität. So hat Herr Bundesminister Dr. Friedrich Vorstandsvorsitzende und Wirtschaftsverbände zu Gesprächen eingeladen. Es ist wichtig, dass sich alle

Branchen explizit und umfassend um die Sicherheit ihrer von IT-abhängigen kritischen Geschäftsprozesse bemühen. Wir brauchen bundesweit einheitliche Mindeststandards und zuverlässige Meldewege, um bei IT-Vorfällen eine schnelle Information und Reaktion aller Betroffenen sicherzustellen. Außerdem müssen wir auch die Branchen und Unternehmen der Kritischen Infrastrukturen, die noch nicht Teilnehmer des Umsetzungsplans Kritis sind, in die Strukturen integrieren.

Die zunehmende Durchdringung der IT hat dazu geführt, dass auch andere **Bereiche der Wirtschaft**, die bisher **noch nicht in den Informationsaustausch mit dem BSI einbezogen waren, Hilfe angeboten werden soll.** Das BSI ergänzt in einer auf der CeBit angekündigten Kooperation mit dem BITKOM unter dem Titel „Allianz für Cyber-Sicherheit“ den kooperativen Ansatz für nicht-kritische Infrastrukturen.

Auch die **Aufsichtsbehörden** über Betreiber Kritischer Infrastrukturen spielen eine wesentliche Rolle. Neben ihrer Einbindung in die Zusammenarbeit im Nationalen

Cyber-Abwehrzentrum werden wir **gemeinsam** mit ihnen prüfen, welche **Schutzmaßnahmen den Betreibern** ggf. **vorgegeben** werden müssen und an welchen Stellen wir zusätzliche Befugnisse in Form von **Anordnungsmöglichkeiten** brauchen.
Ob und an welchen Stellen solche Regelungen auch im Falle eine IT-Krise notwendig werden könnten, werden wir auch mit den Betreibern Kritischer Infrastrukturen diskutieren.

Internationales:

Ein **weiteres Ziel** der Strategie ist das „**Effektive Zusammenwirken für Cyber-Sicherheit in Europa und weltweit“.**

So erarbeitet derzeit die EU-Kommission eine **Europäische Strategie für Internetsicherheit**. In die Diskussion von harmonisierten Mindeststandards in Europa oder auch der Notwendigkeit einer umfassenden europ. CERT-Infrastruktur bringen wir deutsche Erfahrungen nicht zuletzt auch aus der nationalen Strategie aktiv ein. So wird von Deutschland bspw. auch

eine Arbeitsgruppe geleitet, die Mechanismen für eine Koordination in IT-Lagen zwischen EU-Staaten erarbeitet.

Ebenso setzen wir uns für eine Stärkung des Mandats der Europäischen Agentur für Netz- und Informationssicherheit, „**ENISA**“ ein. Schwerpunkte der Mandatserweiterung sollten die Beratung und Überprüfung von IKT-Vorhaben von Kommission und Rat, Unterstützung bei europäischen Regulierungsvorhaben mit IT-Sicherheitsbezug und die Unterstützung bei Aufbau und Betrieb eines zentralen Cert für die EU-Institutionen sein.

Ein **weiteres** wesentliches **Ziel unserer internationalen Aktivitäten** ist die Verhandlung von **Verhaltensregeln für Staaten im Cyber-Raum, die sogenannten** „Norms of State Behavior in Cyberspace“.

Die **Etablierung** eines von möglichst vielen Staaten zu unterzeichnenden Kodex für staatliches Verhalten im Cyber-Raum, der auch **vertrauens- und sicherheitsbildende Maßnahmen** umfasst, ist Teil der Cyber-Außenpolitik. Denn nur durch ein zwischen den Staaten **abgestimmtes Vorgehen** kann den **Bedrohungen** für den Cyberraum **effektiv begegnet** werden.

Wir sprechen uns dafür aus, die Verhaltensregeln im Cyber-Raum **zunächst** im Rahmen eines **politisch** verbindlichen **VN-Verhaltenskodex** zu vereinbaren. Unser Ziel ist es, trotz und jenseits ideologischer Verwerfungen in einer differenzierten Welt eine rasche

Verständigung im gesamtgesellschaftlichen Interesse aller Staaten zu erzielen.
IT-Ausfälle jedenfalls dürften als reale Gefahr und globale Bedrohung eingeschätzt werden. Denn auch Länder, die nicht unsere Freiheitsmaßstäbe teilen, sind Teil des globalen Internets und damit sind auch deren Computersysteme und IT-gestützten Infrastrukturen grundsätzlich sehr verwundbar.

Wirtschaftsstandort Deutschland – Know-How-Schutz:

Cyber-Sicherheit können wir heute nicht nur von der nationalen oder internationalen Warte betrachten, sondern müssen dies insbesondere als **ein komplexes Geflecht unterschiedlicher Rahmenbedingungen** ansehen – die zum Beispiel durch Datenschutzbestimmungen, Vernetzungen oder Virtualisierung konkurrieren.

Durch die Konkurrenz in einer **globalisierten Welt** stehen auch deutsche Unternehmen unter **stetigem Druck** des internationalen **Wettbewerbs.**
Problematisch wird es, wenn die für die **Gewährleistung nationaler Cyber-Sicherheit** wichtigen **Nischenprodukte** sich **im internationalen Wettbewerb nicht behaupten** können und somit auf dem **nationalen Markt nicht mehr zur Verfügung** stehen.
Als Gründe werden oftmals eine fehlende Finanzierbarkeit bzw. die fehlende Wirtschaftlichkeit von Sonderlösungen genannt. Es gibt auch Fälle, bei denen aus Kostengründen **IT-Sicherheitsaspekte** in den **Hintergrund** gerückt werden mussten.
Sensible Daten, sei es in Unternehmen oder in der Verwaltung, bedürfen eines **besonderen Schutzes**, der

sich oftmals auch in den verwendeten IT-Produkten widerspiegelt.
Der **Staat** wird daher prüfen müssen, inwiefern **technologische Souveränität in Deutschland** notwendig ist und wie wir diese erhalten bzw. fördern können.

Ausblick

Mit der Verabschiedung der Cyber-Sicherheitsstrategie für Deutschland hat die **Bundesregierung** ihren Handlungsrahmen zur **Verbesserung der IT-Sicherheit** in Deutschland abgesteckt.
Die **Umsetzung** der Ziele wird seit Verabschiedung aktiv vorangetrieben. Durch gezielte Maßnahmen versuchen wir, IT-**Sicherheits-know-how in Deutschland** zu **erhalten**.

Aber: Der Staat allein kann Cyber-Sicherheit nicht gewährleisten. Zwar müssen die öffentlichen Verwaltungen von Bund, Ländern und Kommunen ihre Aufgaben wahrnehmen und ihre selbstbetriebenen Systeme adäquat schützen.
Cyber-Sicherheit kann jedoch nur in einem umfassenden, kooperativen Ansatz verfolgt werden, der

alle Akteure einbezieht. Wir brauchen ein **Zusammenspiel aller gesellschaftlichen Gruppen und eine gemeinsame Übernahme von Verantwortung**.
Damit meine ich die **nationale Verantwortung für die Gewährleistung von IT-Sicherheit auch durch Unternehmen.**
Es muss uns ein gemeinsames Anliegen sein, die technologische Souveränität und wissenschaftliche Kapazität Deutschlands auf dem Gebiet der Informations- und Kommunikationstechnik zu stärken, weiterzuentwickeln und vertrauenswürdige Produkte am Standort Deutschland zu produzieren.

Ich danke für Ihre Aufmerksamkeit.