

Rede  
von  
Frau Staatssekretärin Rogall-Grothe  
anlässlich des  
Zukunftsforums für  
öffentliche Sicherheit "Cybercrime"  
am 24. November 2011 in Berlin

**Sperrfrist: Redebeginn.**

**Es gilt das gesprochene Wort.**

Zeichen 14.532 = ca. 20 min

Anrede,

wenn ich in Ihre erwartungsvollen Gesichter schaue, frage ich mich: Womit soll ich beginnen? Der Anfang ist ja immer das Schwierigste. Samuel Goldwyn, einer der Gründungsväter Hollywoods, kannte das Problem. Er hat seinen Drehbuchautoren empfohlen: „Mit einem Erdbeben beginnen und dann langsam steigern.“

Ein Erdbeben im übertragenen Sinne kann ich Ihnen bieten – eigentlich gleich zwei davon.

Stellen Sie sich nur einmal folgende Szenarien vor:

- Die Stromdurchleitung durch die europäischen Stromnetze wird durch die Manipulation von Daten gestört oder die Produktions- und Planungssteuerungssysteme der großen Autokonzerne werden sabotiert...

Ein Worstcase-Szenario? Sicherlich, aber leider keine Zukunftsmusik mehr. Seit „Stuxnet“ wissen wir, dass es Schadsoftware gibt, die so programmiert ist, dass

sie gezielt bestimmte industrielle Steuerungsanlagen manipulieren kann. Und erst vor Kurzem ist eine neue, mit Stuxnet verwandte, Schadsoftware aufgetaucht – medial bekannt geworden unter dem Namen Duqu. Diese wird – anders als Stuxnet – nicht als Sabotage-Mittel sondern als Spionage-Werkzeug verwendet. Auch wenn derzeit keine Fälle von betroffenen Organisationen in Deutschland bekannt sind, zeigt der Vorfall erneut unser Bedürfnis nach Sicherheit der Systeme.

- Und das zweite Szenario: Die persönlichen Daten aller deutschen Nutzer in einem weit verbreiteten sozialen Netzwerk werden öffentlich zugänglich gemacht...

Erst Mitte Oktober ist ein Angriff auf Sony-Online-Dienste bekannt geworden, bei dem ca. 93 000 Nutzerkonten gesperrt werden mussten. Dem Unternehmen lässt sich dabei vermutlich kein Vorwurf machen. Offensichtlich haben Kriminelle sich andernorts – vermutlich durch Phishing oder Trojaner-Attacken – Nutzerdaten beschafft und zu Recht

darauf spekuliert, dass viele Nutzer aus Bequemlichkeit stets dasselbe Passwort verwenden.

Die Beispiele zeigen, dass die umfassende Durchdringung aller Bereiche der Gesellschaft mit IT zu einer hohen Verwundbarkeit der heutigen Systeme führen.

Was also tut der Staat?

Wir setzen auf einen umfassenden Ansatz, bei dem die IT des Staates, der Kritischen Infrastrukturen, der sonstigen Wirtschaft und der Bürgerinnen und Bürger einbezogen wird. Dabei kooperieren wir sowohl mit der Wirtschaft als auch mit internationalen Partnern. Hierzu einige Beispiele:

- Zum Schutz der IT der Bundesbehörden wurden in Umsetzung des „Nationalen Plans zum Schutz der IT-Infrastrukturen“ im Umsetzungsplan Bund Mindeststandards und ein IT-Sicherheitsmanagement für Bundesbehörden festgelegt.

- Im „Umsetzungsplan für kritische Infrastrukturen“ – kurz UP KRITIS hat sich die Wirtschaft im September 2007 zur Einhaltung anerkannter Mindestsicherheitsstandards und der Meldung von Sicherheitsvorfällen an das BSI bereit erklärt.
- Durch die Novellierung des BSI-Gesetzes vor zwei Jahren haben wir das Bundesamt für Sicherheit in der Informationstechnik mit neuen und deutlich erweiterten Befugnissen zum Schutz der Cybersicherheit ausgestattet. So hat das BSI nicht nur die nötigen Befugnisse für Sicherheitsmaßnahmen in den Regierungsnetzen erhalten, sondern darf auch öffentlich vor Sicherheitslücken in IT-Produkten warnen.
- Mit der Föderalismusreform II hat im Jahr 2009 durch Art. 91 c GG die Informationstechnik Einzug in die Verfassung gehalten. Ausfluss dessen ist der IT-Planungsrat, der die Zusammenarbeit von Bund und Ländern in Fragen der Informationstechnik koordiniert und zu wesentlichen Effizienzgewinnen führt.

- Zentraler Träger von internetbasierten Angriffen sind Bot-Netze. Mit dem vom Branchenverband eco im September 2010 gestarteten Anti-Bot-Netz-Beratungszentrum erhalten betroffene Internetnutzer Hilfestellungen, um Schadsoftware von ihren PCs zu entfernen und damit die Bot-Verbreitung zu verringern. Ich halte das für eine gelungene Initiative. Das BMI hat sie deshalb auch mit einer Anschubfinanzierung unterstützt und Experten des BSI haben technischen Sachverstand beigetragen.

Anrede,

bei all diesen Aktivitäten haben wir besonderen Wert auf die Vernetzung unterschiedlicher Akteure gelegt.

Dennoch hat „Stuxnet“ im Sommer 2010 bewiesen, dass sich die Bedrohungen im Cyberraum ständig weiterentwickeln und neue Lösungen fordern.

Cyberangriffe werden in den nächsten Jahren nicht nur in der Komplexität, sondern auch in der Anzahl weiter zunehmen. Damit sie nicht irgendwann der gesellschaftlichen und wirtschaftlichen Prosperität

unseres Landes ernsthaft schaden, ist ein vorausschauendes Handeln nötig.

Wir brauchen ein funktionierendes und sicheres Internet. Beiden Bedürfnissen kommt die im Februar dieses Jahres von der Bundesregierung beschlossene Cyber-Sicherheitsstrategie nach. Wir wollen damit Cyber-Sicherheit in Deutschland auf einem hohen Niveau gewährleisten, ohne dabei die Chancen, die das Internet bietet, zu beeinträchtigen.

Kernpunkte dieser Strategie sind:

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

Anrede,

das Nationale Cyber-Abwehrzentrum ist weder eine neue Behörde mit weitreichenden Eingriffsbefugnissen noch eine Servicestelle für Unternehmen und Bürgerinnen und Bürger, die ihre Systeme gegen Angriffe absichern möchten.

- Das Cyber-Abwehrzentrum ist eine Informationsplattform, an der das BSI, das BKA, das BfV, das BBK, die Bundespolizei, das ZKA, der BND und die Bundeswehr beteiligt sind. Zukünftig sollen die aufsichtsführenden Behörden über Betreiber kritischer Infrastrukturen hinzukommen.
- Das Wissen und die Erfahrungen aller Beteiligten werden im Cyber-Abwehrzentrum erstmals strukturell zusammengeführt. Es verfolgt dabei einen kooperativen Ansatz, bei dem die beteiligten Behörden unter Wahrung ihrer jeweiligen Aufgaben und Zuständigkeiten zusammenarbeiten. Doppelstrukturen entstehen nicht.

Wer sich also unter dem Cyber-Abwehrzentrum eine neue Superbehörde vorgestellt hat wird – je nach Standpunkt – enttäuscht oder beruhigt. Unsere Antwort auf global vernetzte Täter muss die Vernetzung von Experten sein, die sich dem Problem aus ihrer jeweiligen Perspektive und mit ihrer ganz spezifischen Kompetenz annehmen.

- Das Cyber-Abwehrzentrum kann
  - schnell und abgestimmt alle technischen Informationen zu einer Schadsoftware oder einem IT-Angriff beschaffen,
  - diese analysieren,
  - auf dieser Grundlage rasch fundierte Empfehlungen zum Schutz der IT-Systeme zur Verfügung stellen.

Auf politisch-strategischer Ebene ist der Nationale Cyber-Sicherheitsrat das Gremium für vernetzte Zusammenarbeit. Der Cyber-SR tagt auf Staatssekretäresebene unter meinem Vorsitz dreimal jährlich und darüber hinaus anlassbezogen. Teilnehmer sind meine Kollegen aus dem BMF, AA, BMVg, BMWi,

BMBF, ein Vertreter des BK, zwei Länder- sowie vier Wirtschaftsvertreter.

Lassen Sie mich schließlich Ihre Aufmerksamkeit noch auf zwei weitere Projekte lenken:

- Im Rahmen des 2008 aufgesetzten Projektes „Netze des Bundes“ bauen wir derzeit ein neues Regierungsnetz auf. Hierfür werden rund 410 Millionen € für Investitionen und laufende Betriebskosten in die Hand genommen. Dieses Netz soll künftig auch die Grundlage für die Kommunikation zwischen Bund und Ländern bilden. Wesentliche Anforderung für dieses Nachfolgenetz des derzeitigen Regierungskommunikationsnetzes IVBB ist eine erhöhte Sicherheit und Krisenfestigkeit.
- Und ganz aktuell: Vom 30. November – 1. Dezember 2011 führen wir die diesjährige LÜKEX durch. Diese Übung wird sich als „Nationale IT-Übung“ mit den Herausforderungen befassen, die das gemeinsame Krisenmanagement des Bundes und der Länder bei IT-Vorfällen zu bewältigen hätte. Es werden Auswirkungen simuliert, die ein komplexes

Schadprogramm für die Bundesverwaltung, die Netze der Bundesländer sowie Betreiber Kritischer Infrastrukturen verursachen könnte.

Wir setzen mit all diesen Maßnahmen unsere präventive Sicherheitspolitik fort. Es geht um Schadensvermeidung und Schadensminimierung. Für eine verlässliche Sicherheitsvorsorge müssen Staat und Wirtschaft partnerschaftlich zusammenarbeiten. Die jeweiligen Akteure sind auf die gegenseitige Unterstützung angewiesen.

Das gilt auch auf internationaler Ebene: Da Cyber-Kriminalität ein weltweites Problem ist, prüfen wir mit unseren internationalen Partnern stetig, wie wir die Zusammenarbeit der Strafverfolgungsbehörden weltweit verbessern können. Dazu gehört u.a., dass wir uns für die Zeichnung der Cyber-Crime-Convention des Europarates durch möglichst viele Staaten einsetzen. Mit dieser Konvention werden Harmonisierungen im Bereich des Computerstrafrechts geschaffen und die schnelle Zusammenarbeit der Strafverfolgungsbehörden wird unterstützt.

Langfristiges Ziel ist aber auch, Verhaltensregeln für Staaten im Cyber-Raum zu etablieren. Hierbei soll es einmal um den Umgang und die Abwehr von Cyber-Angriffen gehen. So soll z.B. jeder Staat verpflichtet werden, Angriffe, die von seinem Territorium kommen, unverzüglich abzustellen. Außerdem sollen alle Staaten ein rund um die Uhr erreichbares Lagezentrum einrichten. Denn Kriminelle kennen keine Dienstzeiten und das gilt erst recht für den globalen Cybercrime.

Anrede,

lassen Sie mich meine Ausführungen noch einmal an den eingangs erwähnten Beispielen konkretisieren:

- Eine Störung der Stromnetze durch die Manipulation von Daten:

Für kritische Infrastrukturkomponenten und Infrastrukturen brauchen wir besondere Mindestsicherheitsstandards. Gemeinsam mit den Betreibern erörtern wir im UP KRITIS die Anfälligkeit der für die Gesellschaft elementar wichtigen

Dienstleistungen und klären, welche Schutzmaßnahmen angemessen sind. Zudem prüfen wir, ob wir im Fall konkreter Bedrohungen zusätzliche Anordnungsmöglichkeiten brauchen, wie wir sie beispielsweise schon aus dem Bereich des Verkehrsleistungsgesetzes kennen. Hiernach können Verkehrsunternehmen im Fall einer schweren Krise durch Beschluss der Bundesregierung zur Bereitstellung ihrer Dienste verpflichtet werden, sofern der Bedarf anderweitig nicht adäquat gedeckt werden kann.

Gerade die Betreiber kritischer Infrastrukturen müssen sich ihrer hohen Verletzbarkeit und der daraus resultierenden großen Verantwortung bewusst sein. Aber selbst große Unternehmen in Deutschland können bei Problemen mit ihrer Hardware oder Software in der Regel nicht direkt auf die Hersteller zugehen – aus Sicht der großen insbesondere ausländischen Hersteller ist ein deutsches Unternehmen eines von vielen. Hier hilft aber das gute Renommee des BSI und seine Warnbefugnis.

- Zweites Beispiel: Die Produktions- und Planungssteuerungssysteme der großen Autokonzerne werden sabotiert:

Sabotage ist ein zunehmendes Cybercrime-Phänomen. Nicht nur große, sondern auch kleine und mittelständische Unternehmen können davon betroffen sein. Die Schäden können immens sein, das Erpressungspotential ist hoch. Leider erfahren staatliche Stellen oft erst sehr spät oder gar nicht von diesen Fällen, da die Unternehmen Angst davor haben, dass der Vorfall öffentlich bekannt wird und ihr wirtschaftlicher Schaden dadurch noch größer wird.

Hier müssen wir die Zusammenarbeit intensivieren und für Vertrauen werben. Teilweise fehlt es aber auch noch auf Seiten der Wirtschaft an institutionellen Voraussetzungen für eine enge Zusammenarbeit.

Mit einem positiven Beispiel geht hier die Versicherungswirtschaft voran. Sie hat ein Krisenreaktionszentrum für IT-Sicherheit, kurz LKRZV, eingerichtet, das für die anlassbezogene Kommunikation

zur Krisenfrüherkennung und die Kommunikation und Alarmierung zur Krisenbewältigung zur Verfügung steht. Hier findet eine Informationsbündelung auf Branchenebene statt, so dass sich das LKRZV zu Recht als Sicherheitsdrehscheibe der Versicherungswirtschaft bezeichnet. Ähnliche brancheninterne Single Points of Contact bestehen bei den Sparkassen und den Geschäftsbanken, der Telekommunikationsbranche sowie den Internet Providern.

Anrede,

solch eine Kontaktstelle gilt es, in jeder Branche einzurichten. Ein Informationszentrum, das aus der Branche für die Branche arbeitet und in nationale Krisenreaktionsstrukturen eingebunden ist. Auf staatlicher Seite steht das BSI als Kontaktstelle zur Verfügung. Nun muss die Wirtschaft ihrer Verantwortung nachkommen und einen institutionellen Gegenpart in den jeweiligen Branchen schaffen, damit wir im Krisenfall keine kostbare Zeit auf der Suche nach Ansprechpartnern und bei der Klärung von Zuständigkeiten verlieren.

Sie sehen, wir sind auf einem guten Weg. Aber der Cyberraum verändert sich ständig. Den neuen Herausforderungen wollen wir nicht hinterherlaufen, sondern möglichst immer einen Schritt voraus sein. Damit das gelingt, muss jeder sein Bestes geben. Dies gilt für den Staat, die Bürgerinnen und Bürger, aber auch und im Besonderen für die Wirtschaft.

Anrede,

welche Schlüsse können wir also ziehen?

Zunächst einmal, dass IT-Sicherheit unverzichtbar ist, auch wenn sie Geld kostet. Allerdings sollten die Überlegungen der letzten 20 Minuten deutlich gemacht haben, dass auch in diesem Bereich gilt, dass Prävention günstiger ist, als der nicht ganz unwahrscheinliche Schadensfall. Um nur eine Zahl zu nennen: Von 2009 bis 2010 hat sich der Schaden aller Cybercrime-Delikt auf über 60 Mio. € fast verdoppelt.

Auch müssen wir uns der Tatsache bewusst sein, dass IT-Sicherheit keine einmalige Aufgabe, sondern ein

dauerhafter Prozess ist. Sicherheitssysteme haben ein Verfallsdatum und müssen daher permanent aktualisiert werden.

Für den Staat ist die Gewährleistung von Freiheit und Sicherheit im Cyber-Raum eine moderne Form der Daseinsvorsorge im 21. Jahrhundert. Dieser Verantwortung müssen wir gerecht werden. Zwar ist Selbstregulierung immer besser als der Zwang zur staatlichen Regulierung, aber wo es um Leib und Leben oder das Funktionieren kritischer Infrastrukturen geht, ist staatliches Handeln im Zweifel nicht vermeidbar.

Deshalb mein eindeutiger Appell an die Wirtschaft: Kommen Sie Ihrer Verantwortung bei der Gewährleistung der Cyber-Sicherheit nach – sichern Sie Ihre Systeme, investieren Sie, bauen Sie Kontaktstellen auf und v.a. nutzen Sie die entsprechenden staatlichen Stellen als Partner für eine vertrauensvolle Zusammenarbeit. Staat und Wirtschaft müssen sich bei diesem komplexen Thema partnerschaftlich ergänzen.

Keiner kann die Herausforderungen für sich alleine meistern.

Vielen Dank.