

12.06.2015 – 17:50 Uhr

## Angriff auf Bundestags-IT ein "Debakel": Ex-Innenminister Schily beklagt auf Potsdamer Sicherheitskonferenz Versäumnisse

Potsdam (ots) -

- Querverweis: Bildmaterial wird über obs versandt und ist abrufbar unter <http://www.presseportal.de/meldung/3045833> -

In der brandenburgischen Landeshauptstadt ist am Freitagnachmittag die Potsdamer Konferenz für nationale Cyber-Sicherheit zu Ende gegangen. 300 Experten von NATO, Europol, Bundesverfassungsschutz, Bundeskriminalamt und anderen Institutionen aus Politik, Wirtschaft und Wissenschaft hatten zwei Tage lang am Hasso-Plattner-Institut (HPI) aktuelle Gefährdungen wie den Hacker-Angriff auf den deutschen Bundestag und grundsätzlich notwendige Schutzmaßnahmen beraten.

Thoralf Schwanitz, tätig im Bereich Public Policy und Government Relations bei Google Deutschland, betonte am Freitag insbesondere die Wichtigkeit von Verschlüsselungsmaßnahmen. Zum Einen sei Datenverschlüsselung zum Schutz vor Hackern wichtig, zum Anderen zwingt sie Regierungen und Behörden, auf rechtsstaatlichem Wege Zugriff auf Daten zu erfragen. Allein in der ersten Jahreshälfte 2010 habe Google 15.000 behördliche Ersuchen im Kontext von Strafverfolgungen erhalten, im Jahr 2014 bereits mehr als doppelt so viele. Diesen Ersuchen werde nach rechtlicher Prüfung in rund 65 Prozent der Fälle nachgegangen. Schwanitz betonte die damit einhergehende unternehmerische Verantwortung: "Keine Regierung, auch nicht die der USA, hat einen wie auch immer gearteten Zugang durch die Hintertür zu Google".

Der frühere Bundesinnenminister Otto Schily betonte auf der HPI-Konferenz, dass persönliche Freiheitsrechte im Internet nicht durch den Rechtsstaat, sondern durch Terrorismus, organisierte Kriminalität und totalitäre Regimes bedroht würden. Auch die wachsende wirtschaftliche und politische Macht privater Konzerne wie Google und Facebook begreift er als Gefahr: "Gegen diese Konzentration versagen die Instrumente des Kartell- und Steuerrechts, hier bedarf es weiterer Beschäftigung". Er beklagte das Versäumnis, dass Cybersicherheit bei der Festlegung politischer Prioritäten noch immer nicht den gebührenden Rang einnehme. Als unzureichend bezeichnete Schily unter anderem die erst im Mai auf den Weg gebrachte Strategie der EU-Kommission zum "Digitalen Binnenmarkt", bei der angemessene Sicherheitsmaßnahmen kaum eine Rolle spielten. Dabei könnte das technologisch hinter den USA zurückgebliebene Europa gerade auf diesem Gebiet ein "Alleinstellungsmerkmal" herausbilden, so Schily.

Die Relevanz des Themas Cybersicherheit wurde durch den am Freitag im Bundestag erfolgten Beschluss des IT-Sicherheitsgesetzes noch einmal deutlich unterstrichen. Bei diesem Gesetz geht es unter anderem um strengere Internet-Sicherheitsvorschriften für Betreiber kritischer Infrastruktur, wie etwa Banken, Energieversorger oder Verkehrsunternehmen. Im Kern verlangt das Gesetz zum einen die Erfüllung festgelegter Mindeststandards zur Absicherung der Informationstechnik, zum anderen müssen zukünftig schwerwiegende Vorfälle an Behörden gemeldet werden - ansonsten drohen Bußgelder von bis zu 100.000 Euro. Das Gesetz wurde auf der HPI-Konferenz kritisch diskutiert: Wilhelm Dolle von der Unternehmensberatung KPMG etwa erwartet vom Staat mehr Unterstützungsleistungen vor allem für kleine und mittelständische Unternehmen bei der Absicherung ihrer IT. Auch für Iris Plöger vom Bundesverband der Deutschen Industrie gehen Bußgelder in die falsche Richtung, da Unternehmen ohnehin bereits ein starkes Eigeninteresse an sicherer Infrastruktur hätten.

Bereits am ersten Tag der Potsdamer Konferenz für nationale Cyber-Sicherheit waren die Ernsthaftigkeit und zunehmende Bedrohung von Cyberangriffen von hochrangigen politischen Akteuren verdeutlicht worden. Nato-Vizegeneralsekretär Prof. Jamie Shea erklärte am Donnerstag, dass ein Cyberangriff den Bündnisfall auslösen und ein gemeinsames Eingreifen der Verteidigungskräfte notwendig machen könnte. Ab einer gewissen Größenordnung sei so eine Attacke mit einem bewaffneten Angriff gleichzusetzen, betonte Shea. Eine Antwort der Nato auf solche Attacken müsse nicht nur auf digitalem Weg folgen.

Dass die Cyberwelt sich durch eine neue Form der Asymmetrie auszeichne, betonte Dr. Hans-Georg Maaßen, Präsident des Bundesamtes für Verfassungsschutz. Nordkorea etwa verfüge nur über drei Zugänge zum World Wide Web, und sei dennoch in der Lage gewesen, einen schwerwiegenden Angriff auf den global operierenden Sony-Konzern zu fahren. In Zusammenhang mit der Cyberattacke auf den Deutschen Bundestag erklärte Maaßen, dass er es nicht für ausgeschlossen halte, dass ein anderer Staat hinter dieser Attacke stehe. Maaßen fürchtet sogar, dass es sich um einen Cyberangriff eines ausländischen Nachrichtendienstes handeln könne.

Michael Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), warnte davor, dass die Cyberspionage auch in Zukunft weiter zunehmen werde. Der Schritt hin zu Sabotage sei nur ein kleiner. Hange betonte, dass in den 1990er Jahren noch alles mit Kryptoprodukten gesichert werden konnte. "Mit der Technologie von heute funktioniert der Perimeterschutz nicht mehr", so Hange. Angreifer würden systematisch nach einzelnen Schwachstellen in Softwareprodukten suchen und über Hintertüren in Systeme einfallen. Verteidiger müssten aber komplette Systeme schützen. Angesichts tausender Schwachstellen sei das eine kaum leistbare Aufgabe. Wenn es flächendeckend geschafft werde, Systeme zu 80 bis 90 Prozent sicher gegen Cyberangriffe zu schützen, würden sich Angriffe von Cyberkriminellen schon nicht mehr lohnen.

Dass dazu nicht nur technische Lösungen vonnöten sind, argumentierte am Donnerstag HPI-Direktor Prof. Christoph Meinel. Zu den Gegenmaßnahmen gehöre auch, das Sicherheitsbewusstsein der Mitarbeiter zu stärken, die Menschen zu sensibilisieren durch Aufklärung und Weiterbildung. Zudem wies Meinel darauf hin, dass sich das HPI mit der Echtzeitabwehr von Cyberangriffen als

einem der Forschungsschwerpunkte befasst. Dreh- und Angelpunkt sei hierbei das am HPI mitentwickelte In-Memory-Datenmanagement.

Das gemeinsame Pilotprojekt "Online-Datentresor" zwischen dem HPI und der Bundesdruckerei soll in der Zukunft für Unternehmen sowie Privatpersonen ermöglichen, Dokumente zuverlässig in der öffentlichen Cloud zu sichern und zu verwalten. Neben modernen Verschlüsselungs- und Verteilungsmechanismen zeichnet sich diese Lösung auch dadurch aus, dass die Cloud-Speicher ausschließlich durch zertifizierte deutsche Unternehmen bereitgestellt werden. Diese komplett deutsche Lösung verhindert also zum Beispiel, dass die sensiblen Dokumente deutscher Nutzer den Vorschriften des US-amerikanischen Rechtsraums unterliegen, sobald sie in der Cloud gespeichert werden.

Um die Forschung auf dem Gebiet der digitalen Identität noch weiter voranzubringen, haben HPI und Bundesdruckerei auf der Potsdamer Sicherheitskonferenz das "Secure Identity Lab" eröffnet. Ab sofort werden junge Wissenschaftler eingestellt, die innovative Konzepte und Technologien zur Identitätssicherung entwickeln und bewerten sollen. Es gehe darum, schon jetzt die Grundlagen für vertrauensvolle Geschäfts- und Kommunikationsprozesse in der digitalen Welt von morgen zu sichern, hieß es.

Kontakt:

HPI-Pressestelle: presse@hpi.de. Pressesprecher Hans-Joachim Allgaier, M.A., Tel. +49 (0)331 5509-119, Mobil +49 179 2675466.

Diese Meldung kann unter <https://www.presseportal.ch/de/pm/100007820/100774126> abgerufen werden.