newsletter

Zukunftsforum Öffentliche Sicherheit

17. Juli 2014

Inhalt

Liebe Mitglieder,

das 22. Zukunftsforum hat sich mit dem umfassenden Begriff der Digitalen Souveränität beschäftigt. Gemeinsam mit 11 Referenten aus Politik, Behörden, Wissenschaft und Wirtschaft sind wir den entsprechenden Fragestellungen nachgegangen. Um der großen Anzahl unserer Vortragenden, vor allem aber deren Redebeiträgen gerecht zu werden, beschäftigt sich dieser newsletter diesmal nur mit einem Thema.

Die Gedankengänge, Diskussionsbeiträge, aber auch die sich daraus ergebenden Lösungsansätze, lesen Sie auf den folgenden Seiten.

Wir wünschen Ihnen allen einen schönen Sommer und eine erholsame

Mit besten Grüßen

Verena Mummert
Geschäftsführerin
Zukunftsforum Öffentliche Sicherheit e.V.

22. Zukunftsforum "Digitale europäische Souveränität - welchen Beitrag kann die Wirtschaft leisten?"

Die Frage, wie sich die Sicherheit des Internets zurückgewinnen lässt, wird seit längeren beraten. Eine Lösungsoption ist die digitale Souveränität. Gemeinsam mit Fachpolitikern des Deutschen Bundestages, Vertretern des Auswärtigen Amtes, des Bundesministeriums für Wirtschaft und Energie, des Bundesamtes für Sicherheit in der Informationstechnik, dem Leiter der Schweizer Melde- und Analysestelle für Informationssicherung sowie Experten aus Wirtschaft und Wissenschaft debattierten wir Chancen und Risiken dieser Möglichkeit.

Wie lassen sich Souveränität und Sicherheit im Internet zurückgewinnen? Foto: Frank Schwarz

Der erste Themenblock definierte die politische Zielsetzung. Die Mitglieder des **Bundestagsausschusses Digitale Agenda MdB Thomas Jarzombek** und **MdB Lars Klingbeil** hoben folgende Aspekte hervor:

- Mehr Eigenverantwortlichkeit: Deutschland muss Verschlüsselungsstandort Nummer 1 werden
- Mehr Gründungen und Forschung im Bereich open source und Sicherheit
- Strategie: E-Mail made in Germany bzw. Europe

BMWi und Auswärtiges Amt: Strategien auf nationaler und europäischer Ebene Foto: Frank Schwarz

Daniel Faust vom **Auswärtige Amt** beschrieb die Schwierigkeiten beim Aufbau einer einheitlichen Europäischen Cyberstrategie:

- (Zu-) viele Beteiligte bei der Cyberpolitik: Europ. Kommission, Europ. Rat, Staaten
- Diverse Einzelprojekte
- Fragmentierung der digitalen Märkte
- Mangelnde Interoperabilität
- Mangelnde Investition in die Netze
- Unzureichende Forschung und Investition
- Gleichzeitig Zunahme der Cyberkriminalität
- Keine gemeinsame Datenschutzverordnung

Referatsleiterin Gertrud Husch stellte die „Initiative Sicherheit in der Wirtschaft“ des **Bundesministeriums für Wirtschaft und Energie** vor:

- Webseitencheck und Beratungszentrum als direkte Hilfe für kleine und mittlere Unternehmen.
- Bei derzeit über 9.000 Unternehmen, die sichere und zuverlässige Lösungen anbieten, sollen Deutsche IT-Sicherheitsunternehmen künftig verstärkt unterstützt werden.
- Gründung einer Dialogplattform und Beginn eines langfristigen Dialogprozesses mit der Wirtschaft, um gemeinsam nach Lösungen zu suchen.
- Einsatz existierender Verschlüsselungstechniken soll künftig stärker unterstützt werden.

Von links nach rechts: Pascal Lamia, Leiter Melde- und Analysestelle Informationssicherung MELANI in der Schweiz, Michael Bartsch, (Moderator), T-Systems GmbH, Andreas Könen Vizepräsident Bundesamt für Sicherheit in der Informationstechnik
Foto: Frank Schwarz

Der zweite Themenblock zeigte unterschiedliche behördliche und staatliche Cyberstrategien und begann mit einem Blick in das Nachbarland Schweiz. Dabei hob **Pascal Lamia**, **Leiter der Melde- und Analysestelle Informationssicherung MELANI**, insbesondere den dezentralen Ansatz hervor:

- Die beteiligten Akteure, die Departemente (= Ministerien), KRITIS wie Energie- und Bankensektor und private Wirtschaft haben eine prinzipielle Eigenverantwortung, die sie in ihrem Interesse wahrnehmen.
- Ziele sind in erster Linie Prävention, Frühwarnsystem, Risikoanalysen, Kontinuität, um die Resilienz zu stärken.
- Keine Meldepflicht. Bei einer effektiven Cyberstrategie ist das Vertrauen der beteiligten Akteure untereinander sehr entscheidend.

Andreas Könen, Vizepräsident Bundesamt für Sicherheit in der Informationstechnik (BSI)
Foto: Frank Schwarz

Die Maßnahmen der Schweizer MELANI, ließen sich auf Deutschland nicht übertragen, erklärte **Andreas Könen** vom **BSI**, da die Zahl der Akteure zu groß sei. Er forderte daher:

- Meldepflicht, um Informationen, die für die Gesamtsicherheitslage notwendig sind, auch tatsächlich zu erhalten.
- Verbesserung der Cybersicherheitstechnologie und Forensikfähigkeiten in Deutschland. Unter anderem durch mehr Forschung und Universitätsangebote.
- Exaktes Wissen der Bürger und Unternehmen, wo sich ihre Daten befinden und die Verfügungsgewalt darüber, dass sie in dem von ihnen gewünschten Rechtsraum verbleiben.
- Bei der maßgeblichen Bedeutung von Reaktion und Resilienz müssten alle Akteure in die Lage versetzt werden, Angriffe zu detektieren, darauf angemessen und schnell zu reagieren und anschließend die Handlungsfähigkeit wieder herzustellen. Dies gelingt nur durch Fort- und Weiterbildung.

Der dritte Themenblock beleuchtete die Möglichkeiten von Wissenschaft und Wirtschaft, etwas zur Sicherheit und Souveränität des Internets beizutragen. **Matthias Kammer**, vom **Deutschen Institut für Vertrauen und Sicherheit im Internet (DIVSI)** betonte gleich zu Anfang: „Eine wichtige Herausforderung für die Wissenschaft, Wirtschaft usw. bezüglich des Endnutzers wird sein, dessen Sicherheitsbedürfnis und dessen Convenience-Erfahrungen zusammen zu bringen, damit die bestehenden Sicherheitsprodukte mehr und wirklich genutzt werden. Dies ist deshalb so wichtig weil drei Viertel der deutschen Bevölkerung die Herstellung von Sicherheit im Internet an Staat und Wirtschaft delegiert." Konkrete Vorschläge machte **Prof. Dr. Claudia Eckert, TU München / Fraunhofer AISEC**:

Von links nach rechts: Matthias Kammer, DIVSI: Prof. Dr. Claudia Eckert, TU München / Fraunhofer AISEC; Dr. Andreas Leifeld, (Moderator); Michael Kranawetter Mircrosoft Deutschland GmbH; Bernhard Schneck, Genua GmbH
Foto: Frank Schwarz

- Schlüsseltechnologieherrschaft in Kernbereichen: Bau von smarter, sicherer Sensorik, Hardware und Software, die als Sicherheitsventile fungieren.
- um Qualitätsstandards mitzubestimmen, braucht es die Befähigung zur Bewertung von Produkten und Systemen. Wir benötigen Analyseverfahren, Prüfmethoden und Labore.

Diese Vorschläge wurden in der anschließenden Diskussion durch die Vertreter der Wirtschaft diskutiert und erweitert. **Michael Kranawetter von Microsoft Deutschland** GmbH befürwortete: „Eine Kombination von globalen Angeboten mit lokalen Ergänzungen. Sogenannte Sicherheitsanker, die von einem deutschen Hersteller produziert oder vom BSI zertifiziert werden könnten." Ähnlich sah dies auch der **Geschäftsführer der Genua GmbH Bernhard Schneck**: „Es ist wichtig Systeme zu bauen, die Sicherheit auf dem gewünschten Niveau gewährleisten und gleichzeitig interoperabel sind mit den Weltmarktführern Unsere digitale Souveränität muss auf der bestehenden Netzinfrastruktur aufsetzen. Zum Beispiel durch Kryptotechnologie. So könnten zwar noch andere mitlesen, aber dies nicht verstehen."

Christian Stuchlik, itWatch GmbH Foto: Frank Schwarz

Um die Wettbewerbsfähigkeit deutscher IT-Sicherheitsunternehmen und somit die digitale Souveränität zu stärken, schlug **Christian Stuchlik, Vertriebsleiter der itWtach GmbH** einen Souveränitätsfond vor, der nationale IT-Sicherheitslösungen mitfinanzieren könne.

→ → → Alle in diesem Forum debattierten Thesen, weiterführenden Ansätze sowie die erarbeiteten Ergebnisse werden Eingang das Grünbuch der AG Cybersecurity finden, das derzeit zusammengestellt und verfasst wird.

Impressum:
V.i.S.d.P.:
Verena Mummert, Geschäftsführerin, info@zukunftsforum-oeffentliche-sicherheit.de
Zukunftsforum Öffentliche Sicherheit e.V.,
Kaiserin-Augusta-Allee 31, 10589 Berlin

Geschäftsführender Vorstand:
Lutz Diwell, Axel Dechamps, Dr. Volkmar Schön, Michael Bartsch, Marie-Luise Beck, Stephan Boy