Erster Cyber Security Summit 2012 in Bonn

Zusammenfassung

Der erste Cyber Security Summit 2012 setzt Impulse für einen innovativen und sicheren Wirtschaftsstandort Deutschland. Moderne Informations- und Kommunikationsinfrastrukturen entwickeln sich immer mehr zu einem Standortvorteil im internationalen Wettbewerb. Gleichzeitig hält vernetzte Hochtechnologie in allen Lebensbereichen Einzug. Durch diese Entwicklung wird das Netz zur kritischen Infrastruktur und zur Zielscheibe für Angriffe. Gemeinsames Ziel von Wirtschaft und Staat muss daher ein bestmöglicher Schutz sein. Heute lässt sich die Sicherheit im Cyber-Raum weder als Aufgabe einiger weniger IT-Fachleute noch als technische Herausforderung einzelner Unternehmen erreichen. Sicherheit erfordert vielmehr ein konzertiertes Handeln von Wirtschaft, Politik und Gesellschaft auf allen Ebenen.

Das neue, gemeinsam von der Münchner Sicherheitskonferenz und der Deutschen Telekom initiierte Spitzentreffen hat erstmals Führungspersönlichkeiten zusammengeführt, um das Gespräch über Gefährdungslage und Strukturen einer bereichs- und branchenübergreifenden Zusammenarbeit aufzunehmen. Der Cyber Security Summit schafft dabei wertvolle Synergieeffekte zwischen Wirtschaft und Sicherheitspolitik. Kein Staat, kein Unternehmen, kein Bürger kann eine effektive Abwehr alleine bewerkstelligen. Den Kampf gegen Kriminalität, Wirtschaftsspionage und Sabotage aus dem Netz gewinnen wir nur mit übergreifenden Kooperationen. Hierzu beschreiben acht Eckpunkte die relevanten Handlungsfelder.

1. Praktisch alle Bereiche des politischen, wirtschaftlichen und gesellschaftlichen Lebens sind heute von funktionierenden IT- und Internetstrukturen abhängig. Geschäftsprozesse zwischen Unternehmen stützen sich nahezu vollständig auf das Internet als zentrale Infrastruktur. Für die deutsche Wirtschaft ist Cyber-Sicherheit deshalb ein nachhaltiger Erfolgsfaktor – nicht nur für Informationstechnik- und Telekommunikationsunternehmen, sondern über alle Branchen hinweg. Der Cyber Security Summit hat großen Diskussions- und Handlungsbedarf gezeigt. Cyber-Sicherheit gehört auf die Tagesordnung jedes Unternehmens und jeder Unternehmensspitze – und dort ist sie heute angekommen. **Die Wirtschaft will den Austausch auf den obersten Führungsebenen verstetigen** und regelmäßige Spitzentreffen, Simulationsübungen und Workshops in Deutschland etablieren.

2. Wir verstehen Cyber-Sicherheit als eine globale Aufgabe, die neben nationalen Maßnahmen auch internationale Lösungen erfordert. Der internationale Austausch, der bereits zwischen einzelnen nationalen *Computer Emergency Response Teams* (CERT) auf einer technisch-pragmatischen Ebene stattfindet, muss auch auf der internationalen politischen und wirtschaftlichen Ebene weiter ausgebaut werden. Die **Schaffung rechtlicher und institutioneller Instrumentarien für einen internationalen Dialog** über Verhaltensnormen und vertrauensbildende Maßnahmen ist daher mit Nachdruck zu betreiben, um so die internationale Kooperation für Cyber-Sicherheit zu vertiefen.

3. In diesem Zuge benötigt Deutschland ein Bündnis für Cyber-Sicherheit, an dem sich alle Branchen beteiligen. Bisherige Aktivitäten müssen besser verzahnt, und die Akteure aus Wirtschaft, Politik und Gesellschaft sektorenübergreifend besser vernetzt werden. Vordringliche Aufgabe eines solchen Bündnisses – idealerweise unter Begleitung der Bundesregierung

und als Gemeinschaftsaktion der Spitzenverbände – ist der **Aufbau einer Plattform, auf der sich alle Industriezweige und Unternehmen aller Größen einbringen** können. Ein solches Forum wird den offenen und schnellen Transfer von Erkenntnissen z.B. über Angriffszenarien zwischen den Akteuren ermöglichen.

4. Wir wollen den **offenen Austausch über Angriffsszenarien auf freiwilliger Basis** fördern. Mit dieser Bereitschaft schaffen wir ein Klima, in dem Abwehrmaßnahmen gegen Cyber-Attacken schneller entwickelt und geteilt werden. Nur ein mutiger, transparenter und auch aus den Unternehmen heraus gewollter Umgang mit Angriffen aus dem Cyber-Raum stärkt das Gesamtsystem. Eine entsprechende Eigeninitiative der Wirtschaft muss sich daher ebenso frei entfalten können. Wir unterstützen die Integration der Wirtschaft in die Nationale Cybersecurity-Strategie der Bundesregierung und der EU-Kommission.

5. Die Zahl der Akteure und Experten, die sich mit Cyber-Sicherheit beschäftigen, ist noch nicht ausreichend. Insbesondere mittelständische Unternehmen benötigen Zugang zu Kapazitäten und Know-how sowie Unterstützung, um sich mit anderen Unternehmen zu vernetzen. **Eine sichere Informationsgesellschaft braucht eine wachsende Gemeinschaft (Community) von Ansprechpartnern** in den Unternehmen, die als „Cyber-Wehr“ bei einem Sicherheitsvorfall die Lage einschätzen, den Informationsfluss sicherstellen und Verteidigungsmaßnahmen einleiten und führen können. Im öffentlichen Sektor müssen ebenfalls Ansprechpartner benannt sein, die die Informationen aus der Wirtschaft um Erkenntnisse der Regierungsstellen und Nachrichtendienste ergänzen. Darüber hinaus müssen Vorschläge ausgearbeitet werden, wie Cyber Security als Disziplin in der innerbetrieblichen sowie in der universitären Aus- und Weiterbildung

gestärkt werden kann.

6. Wir setzen uns ein für den **Erhalt technologischer Souveränität am Standort Deutschland**. Ein sicheres Gesamtsystem setzt die Sicherheit ausgereifter Hardware-Komponenten und deren Lieferketten voraus. Der missbräuchliche Zugang zu Informations- und Kommunikationsanlagen beispielsweise durch eingebaute „Backdoor-Technologien“ muss ausgeschlossen sein. Auch die Einführung von nicht marktreifen Produkten unter fahrlässiger Duldung nachträglicher Mängelbeseitigung (Updates, Patches) darf nicht an der Tagesordnung sein.

7. Die Bereitschaft zur Schaffung einer erhöhten Cyber-Sicherheit muss eine Priorität in jedem Unternehmen sein. Mit Aufklärungs- und Sensibilisierungsarbeit trägt die deutsche Wirtschaft darüber hinaus zu einer sicheren Informationsgesellschaft bei. Experten schätzen, dass sich bereits 90 Prozent der Sicherheitsprobleme lösen ließen, indem Unternehmen, öffentliche Hand und Bevölkerung ihre Systeme sicherheitstechnisch gut warten und stets auf den neuesten Stand bringen. Aus diesem Grund setzen wir uns für die **Sensibilisierung von Mitarbeiterinnen und Mitarbeitern in Unternehmen, Institutionen und Organisationen** ein. Ein Mehr an Cyber-Sicherheit in Unternehmen wird ferner durch die Einführung einheitlicher Sicherheitsrichtlinien und die Schaffung von Sicherheitsarchitekturen erreicht.

8. Um die Bevölkerung insgesamt auf diesem so wichtigen Weg für den Standort Deutschland aufzuklären und mitzunehmen, sprechen wir uns ferner für **geeignete mediale Maßnahmen zur Sensibilisierung der Öffentlichkeit** aus. Wie für den Staat und die Wirtschaft sollte Cyber-Sicherheit auch für Privatleute einen hohen Stellenwert einnehmen. Jeder

Computernutzer sollte eigene Maßnahmen zur Cyber-Sicherheit ergreifen, um sich und sein persönliches Umfeld gegen digitale Angriffe zu schützen.

Der Zuspruch zum ersten Cyber Security Summit 2012 in Bonn bestärkt unsere Erwägungen, das Spitzentreffen auch im Jahr 2013 durchzuführen. Darüber hinaus sollen in übergreifenden Arbeitsgruppen, Workshops und Leuchtturmprojekten die genannten Handlungsfelder weiter konkretisiert werden.

Bonn, 12. September 2012

www.cybersecuritysummit.de
www.twitter.com/CYSS2012