Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Mitglieder der Projektgruppe

Zugang, Struktur und Sicherheit im Netz

Termine	
6. Februar 2012	Sitzung
10. Februar 2012	Klausurtagung ab 14 Uhr
27. Februar 2012	Sitzung

Weitere Termine entnehmen Sie bitte dem Zeitplan der Projektgruppe.

Berlin, 24. Januar 2012

Ergebnisprotokoll der 6. Sitzung der Projektgruppe Zugang, Struktur und Sicherheit im Netz am 23. Januar 2012

Vor Eintritt in die Tagesordnung
Das Protokoll der Sitzung vom 16. Januar 2012 wird nachgereicht.

Änderungen der Tagesordnung werden nicht beantragt.

TOP 1
Diskussion des vorliegenden Textbeitrages zum Themenfeld „Schutz kritischer Infrastrukturen“
Der Vorsitzende dankt für die Erstellung des Textes.

Auf Vorschlag des Vorsitzenden werden alle Arbeitstexte der Projektgruppe durch das Sekretariat redigiert. Das Sekretariat wird den Mitgliedern eine redigierte Fassung zur Prüfung zukommen lassen.

Die Mitglieder beraten das vorliegende Dokument zum Themenfeld „Schutz kritischer Infrastrukturen“ (*Hinweis: Die Zeilennummern im Protokoll beziehen sich auf die am 19. Januar 2012 versandte PDF-Datei*).

Ein Mitglied lehnt die Darstellung einer vollständigen Abhängigkeit vom Internet (Zeile 5 bis 6) ab. Gleichwohl betont es, dass es hohe Abhängigkeitsgrade gebe. Die Aussage müsse relativiert werden. Die Formulierung wird entsprechend angepasst, so dass auch die Fußnote entfallen kann.

Ein Mitglied wünscht, dass die Definition kritischer Infrastrukturen (Zeile 65 bis 68) ergänzt werde. Es reicht eine entsprechende Ergänzung ein.

Ein Mitglied empfiehlt, dass der Begriff „IKT“ durch „IT“ bzw. „IT-Sektor“ durchgängig ersetzt werde. Es führt an, dass dies

auch in der Projektgruppe Wirtschaft, Arbeit, Green IT so gehandhabt werde. Die Mitglieder stimmen zu.

Ein Mitglied bittet um Prüfung, ob sich die Aussage in Zeile 152 bis 153 auf kritische Infrastrukturen oder kritische IT-Infrastrukturen beziehe. Das Sekretariat wird mit der Prüfung beauftragt. Des Weiteren müsse in Zeile 150 der Begriff der Kommunikationsbranche, der sich auf die Werbebranche beziehe, durch IT-Branche ersetzt werden. Der Begriff wird ersetzt.

Ein Mitglied teilt mit, dass er an Zeile 153 anschließend einen Einschub wünsche: auch der Deutsche Bundestag müsse hier erwähnt werden. Es habe vom Referat für IT-Sicherheit die Aussage erhalten, dass es bisher keine Angriffe auf die Infrastruktur des Deutschen Bundestages gegeben habe. Dies halte er für unrealistisch und finde die Auskunft unbefriedigend. Ein Mitglied fügt hinzu, dass sich die Auskunft auf erfolgreiche Angriffe bezogen habe, bezweifle dies jedoch auch.

Ein Mitglied erläutert, dass sich die Aussage in Zeile 150 bis 151 auch auf mittelständische Unternehmen beziehen müsse. Es bezweifelt, dass kleine und mittelständige Unternehmen sowie Behörden überhaupt ein ausreichendes Problembewusstsein hätten. Eine entsprechende Formulierung wird in das Dokument aufgenommen.

Ein Mitglied macht darauf aufmerksam, dass Daten nicht gestohlen werden könnten (Zeilen 171 und 178), da es sich nicht um eine bewegliche Sache handle. Lediglich eine Festplatte oder ein USB-Stick könne gestohlen werden. Es plädiert daher für die Formulierung „widerrechtlich kopiert“. Ein Mitglied widerspricht und weist darauf hin, dass auch bereits das widerrechtliche zur Kenntnis nehmen von Daten unter den Begriff des Diebstahls falle. Es spricht sich für die Beibehaltung des Begriffes „stehlen“ aus. Die Mitglieder verständigen sich auf die Formulierung „Ausspähen von Daten“.

Ein Mitglied teilt mit, dass in Zeile 196 eine Korrektur notwendig sei. Command- und Control-Server brächten mit der Schadsoftware Conficker infizierte PCs zu „koordiniertem“ – nicht zu „koordinierendem“ – Handeln.

Ein Mitglied bittet um die Anpassung der Aussage, dass die Schadsoftware Stuxnet „ein qualitativer Wendepunkt in der IT-Sicherheitsgeschichte von Deutschland“ gewesen sei. Stuxnet habe weltweite Auswirkungen gehabt. Die Wörter „von Deutschland“ werden gestrichen.

Ein Mitglied plädiert für eine Ergänzung in Zeile 225: Zerstörungen seien zwar bisher nicht verwirklicht worden, stellten aber eine sehr realistische Gefahr dar. Die Ergänzung wird aufgenommen.

Die Mitglieder diskutieren, ob der Faktor „Mensch“ und die menschliche Unzulänglichkeit – sei es als Anwender, Designer oder Programmierer – als Bedrohung einen eigenständigen Absatz im Text erhalten solle.

Ein Mitglied plädiert dafür, die bereits getroffene Einteilung in menschliches und technisches Versagen beizubehalten. Ein Mitglied betont, dass heutige IT-Systeme derart komplex seien, dass sie nicht mehr in Gänze erfasst werden könnten. Die Mitglieder einigen sich, den Faktor „Mensch“ nicht explizit zu thematisieren, da dieser bereits an anderen Stellen im vorliegenden Dokument sowie in weiteren Dokumenten ausreichend genannt werde. Anstatt des Faktors „Mensch“ wird ein Absatz zur Komplexität aufgenommen.

Ein Mitglied teilt mit, dass es keine Beurteilung über die Darstellung treffen könne, dass das Bundesamt für Verfassungsschutz (BfV) und der Bundesnachrichtendienst (BND) (Zeile 380 bis 382) „im Vorfeld wichtige Erkenntnisse über gegenwärtige Bedrohungen und mögliche Ziele für Angriffe auf kritische Infrastrukturen im Inland“ lieferten. Auf Vorschlag eines Mitgliedes wird der Satz dahingehend umformuliert, dass dies eine von mehreren Aufgaben des BfV und des BND sei.

Ein Mitglied wirft die Frage auf, warum der AK KRITIS der Gesellschaft für Informatik e.V. in Zusammenhang mit Regelungen und Maßnahmen hinsichtlich der IT-Sicherheit auf Bundesebene angeführt werde (Zeile 383 ff.). Der Absatz wird gestrichen.

Ein Mitglied bezieht sich auf die Zeilen 431 ff. und merkt kritisch an, dass das Thema IT-Sicherheit beim Spitzencluster-Wettbewerb des Bundesministerium für Bildung und Forschung nicht berücksichtigt worden sei. Aus München habe es eine Bewerbung mit dem Ziel gegeben, ein Spitzencluster im Bereich IT-Sicherheit aufzubauen. Schließlich sei dieses Thema enorm wichtig und der Aufbau nationaler Kompetenzen sei zu fördern. Ein Mitglied reicht eine entsprechende Ergänzung ein.

Ein Mitglied empfiehlt die Erwähnung der NATO Policy on Cyber Defence anschließend an Zeile 507. Der entsprechende Hinweis wird aufgenommen.

Ein Mitglied bittet um Prüfung, ob das in Zeile 503 erwähnte „Defence against Terrorism Program of Work“ auch auf den Schutz kritischer Informationsinfrastrukturen abziele, ggf. müsse explizit auf den relevanten Aspekt hingewiesen oder ein anderes Programm herangezogen werden. Der Text wird vom Sekretariat geprüft und ggf. angepasst.

TOP 2
Verschiedenes
Der Vorsitzende bittet die Mitglieder um Prüfung, ob am 13. März 2012 die Möglichkeit bestehe eine weitere Klausurtagung durchzuführen. Die Mitglieder der Projektgruppe verneinen dies.

Die Projektgruppe legt fest, dass die für den 10. Februar 2012 geplante Klausurtagung ab 14 Uhr (bis *Open End*) stattfindet.

Der nächste Sitzungstermin ist Montag, der 6. Februar 2012.