Deutscher Bundestag
Enquete-Kommission
Internet und digitale Gesellschaft

Mitglieder der Projektgruppe

Zugang, Struktur und Sicherheit im Netz

Termine	
27. Februar 2012	Sitzung
5. März	Sitzung
26. März	Sitzung

Weitere Termine entnehmen Sie bitte dem Zeitplan der Projektgruppe.

Berlin, 7. Februar 2012

Ergebnisprotokoll der 7. Sitzung der Projektgruppe Zugang, Struktur und Sicherheit im Netz am 6. Februar 2012

Vor Eintritt in die Tagesordnung
Änderungen der Tagesordnung werden nicht beantragt.

TOP 1
Diskussion des ersten Teils des Textbeitrages zu den Themenfeldern „Kriminalität im Internet – Spionage – Sabotage“

Die Mitglieder beraten das vorliegende Dokument zu den Themenfeldern „Kriminalität im Internet – Spionage – Sabotage“ (*Hinweis: Die Zeilennummern im Protokoll beziehen sich auf die am 2. Februar 2012 versandte PDF-Datei*).

Auf Wunsch eines Mitgliedes wird die Gesellschaft in Zeile 71 aufgenommen.

Ein Mitglied plädiert dafür, die in Zeile 75 genannten Zahlen zur Internetkriminalität mit den Zahlen aller Arten von Kriminalität gegenüberzustellen. Dies zeige, dass es deutlich höhere prozentuale Aufklärungsquoten im Bereich der Internetkriminalität gebe. So könne aufgezeigt werden wie gut oder schlecht die Aufklärung funktioniere. Als Quellen führt es die Studie von Freiling/ Brodowski 2011 sowie eine Studie des Max-Planck-Instituts an. Das Mitglied reicht eine Textergänzung ein. Ein Mitglied pflichtet bei. Im Internet gebe es eine besonders hohe Aufklärungsquote und dies solle benannt werden. Dennoch spricht es sich dafür aus, die Polizeiliche Kriminalstatistik (PKS) als Basis zu verwenden, da im nächsten Absatz auf die mit der PKS verbundene Problematik hingewiesen werde.

Ein Mitglied teilt mit, dass es die in Zeile 96 ff. genannte Definition deplatziert empfinde. Es schlägt vor, dass die Definition mit einer Überschrift versehen oder an einer anderen Stelle verortet werde. Im Rahmen der redaktionellen Überarbeitung des Textes wird dieser Einwand aufgegriffen.

Ein Mitglied erklärt, dass Spam von kriminellen Handlungen zu unterscheiden sei. Dies betreffe verschiedene Stellen des Textes. Spam-Mails seien zwar als sozial schädlich zu betrachten, könnten aber im juristischen Sinne nicht als Straftat charakterisiert werden. Ein Mitglied pflichtet diesem Hinweis bei, gibt aber zu bedenken, dass Vorbereitungshandlungen zur Versendung von Spam-Mails als Straftaten eingestuft werden könnten. Als Stichwort nennt es Botnetze. Ein Mitglied unterstützt diese Aussage, da beispielsweise auch fremde Server genutzt und Adressen illegal beschafft würden. Ein Mitglied erklärt, dass diese Diskussion in das *Kapitel 1.2.4.3 Spam* integriert werde. Es fasst zusammen, dass Spam für sich keine Straftat sei, es aber diverse Straftaten in Verbindung mit Spam gebe. Ein Mitglied wird gebeten, seinen Textvorschlag als Grundlage zur Verfügung zu stellen.

Ein Mitglied trägt vor, dass es Internetkriminalität nicht als Gegensatz zu IT-Sicherheit auffasse. Es störe sich am Eingangssatz zu *Kapitel 1.2.2. Gegenbegriff: IT-Sicherheit.* Man könne sagen, dass vom Begriff Internetkriminalität IT-Sicherheit zu unterscheiden sei. Ein Mitglied unterstützt diesen Vorschlag.

Ein Mitglied lehnt die Gleichsetzung von Internetkriminalität und Hackern in *Kapitel 1.2.3.1 Intrinsische Motivation* ab. Diese Darstellung sei falsch. Die Quellen (z.B. Fußnote 15) seien fragwürdig, da veraltet und aus dem Zusammenhang gerissen. Stattdessen sollten politische und ideologische Motive im Gegensatz zur finanziellen Bereicherung aufgeführt werden.

Ein Mitglied spricht sich dafür aus, auf die Unterscheidung von intrinsischer und extrinsicher Motivation zu verzichten. Ein Mitglied unterstützt diesen Vorschlag. Man solle stattdessen eine Liste möglicher Motive erstellen.

Ein Mitglied führt den Begriff des digitalen Klingelstreiches ein. Das Hacken einer Webseite falle unter diesen Begriff. Nicht jedes Eindringen in einen PC sei eine Straftat. Man solle hier zwischen Straftat und Ordnungswidrigkeit unterscheiden.

Ein Mitglied bekräftigt, dass die Frage der Motivation für das vorliegende Papier ein relevanter Aspekt sei. Schließlich helfe dies auch bei der Beantwortung der Frage, was man zur Risikoverringerung tun könne.

Ein Mitglied legt dar, dass das Bundesverfassungsgericht das Eindringen in einen fremden Computer unter Grundrechtsschutz stelle. Die Frage sei, ob man dieses Grundrecht strafrechtlich schützen wolle oder nicht. Es sei mitnichten „lustig“, in den PC

einer anderen Person einzudringen. Bei Gefährdungstatbeständen komme es nicht darauf an, welche Handlungen am PC eines Dritten vorgenommen würden. Die Straftat sei das Eindringen in den PC. Ein Mitglied merkt an, dass das Eindringen in einen fremden Computer in Deutschland nur eine Straftat sei, wenn dieser gesondert gegen das Eindringen gesichert sei.

Ein Mitglied betont, dass niemand das Eindringen in fremde Computer legalisieren wolle. Dennoch könne ein bestimmtes Eindringen als digitaler Klingelstreich aufgefasst werden.

Ein Mitglied erklärt, dass es nicht wolle, dass die Enquete-Kommission den Begriff Hacker mit Kriminellen gleichsetze. Dies sei dem Mitglied ein Hauptanliegen.

Auf Vorschlag eines Mitgliedes reicht ein Mitglied eine maximal halbseitige Erklärung des Begriffes Hacker ein. Des Weiteren teilt das Mitglied mit, dass auf die Unterscheidung in intrinsische und extrinsiche Motivation verzichtet werde. Stattdessen werde der Vorschlag des Mitgliedes aufgegriffen, eine Liste möglicher Motivationslagen zu erstellen.

Ein Mitglied plädiert dafür, den Exkurs auf Seite 9 zu streichen. Der Absatz wird ersatzlos gestrichen.

Ein Mitglied schlägt vor, den Begriff DDoS-Angriffe in Zeile 156 vorzuziehen. Die Änderung wird aufgenommen.

Ein Mitglied teilt mit, dass es das *Kapitel 1.2.4.4 Professionalisierung* für zu kurz halte. Die Tendenz der Professionalisierung werde nicht in adäquater Weise dargestellt. Auch das russische Beispiel greife zu kurz. Ein Mitglied sichert eine Überarbeitung des Kapitels zu. Die Überschrift werde um den Begriff der Organisierte Kriminalität ergänzt. Es werde dargestellt, dass Organisierte Kriminalität von Arbeitsteilung und zunehmender Nutzung legaler Angebote im Netz profitiere.

Ein Mitglied erklärt, dass in *Kapitel 1.2.5.1.4 Backdoors* ein wesentlicher Aspekt fehle. Strukturelle Backdoors seien zu erwähnen. Diese würden von Herstellern implementiert. Sie hätten politische Hintergründe und zielten auch auf Wirtschaftsspionage ab. In den vergangenen Jahren seien solche Fälle sowohl im Hardware- als auch im Software-Bereiche entdeckt worden. Ein Mitglied fügt hinzu, dass zunehmend mehr Hardware im Ausland hergestellt werde. Hardware sei so kompliziert, dass sie sicherheitstechnisch nicht mehr überprüft werden könne. Dies sei ein zunehmendes Sicherheitsrisiko.

Ein Mitglied wirft ein, dass nicht nur auf das einzelne IT-System abgestellt werden solle, sondern auch die Infrastruktur und die Backdoor in die gesamte Infrastruktur erwähnt werden müsse. Ein Mitglied schlägt vor, explizit Hardware in das Kapitel aufzunehmen. Zudem bietet sie an, einen Textbeitrag mit fünf bis zehn bekannten und belegbaren Fälle zu erstellen.

Ein Mitglied plädiert dafür, das Wort Userland in Zeile 295 zu ersetzen. Ein Mitglied sichert zu, dass das *Kapitel 1.2.5.1.5 Rootkits* noch einmal überarbeitet werde.

Ein Mitglied teilt mit, dass es das Thema Adware aus dem *Kapitel 1.2.5.1.6 Ad- und Spyware* streichen wolle und das Kapitel dahingehend überarbeiten werde.

Ein Mitglied fragt nach, wo der von ihr eingereichte Text zum Thema Online-Durchsuchung (Stichwort Staatstrojaner) verortet werden solle. Ein Mitglied teilt mit, dass dies ein Werkzeug und Mittel zur Strafverfolgung sei und als solches in diesem Kapitel verortet werde.

Auf Vorschlag eines Mitgliedes wird das *Kapitel 1.2.5.2 Andere Methoden des Hacking* umbenannt in *Andere Angriffsmethoden*.

Ein Mitglied stellt fest, die Zeilen 342 bis 343 suggerierten, Software werde immer unsicherer. Dies sei nicht der Fall. Weiter stellt es die Erwähnung der Firma Adobe in Zeile 352 sowie 355 in Frage. Zum Veröffentlichungszeitpunkt des Berichtes könne die getroffene Aussage nicht mehr zutreffend sein. Daher solle stattdessen auf die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) veröffentlichten Warnmeldungen Bezug genommen werden.

Ein Mitglied spricht sich dafür aus, die grundsätzliche Formulierung in Zeile 343 beizubehalten. Die Anzahl der Bedrohungen steige. Es handle sich um einen Wettlauf zwischen Sicherheit und Bedrohung.

Ein Mitglied pflichtet dem anderen Mitglied bei, dass auf die Benennung einzelner Firmen verzichtet werden sollte. Es bevorzuge den Hinweis auf das BSI. Auch den Einwand hinsichtlich der Zeilen 342 bis 343 könne es nachvollziehen. Der Satz sollte dahingehend umformuliert werden, dass mit fortschreitender Komplexität der IT-Systeme auch die Anzahl der entdeckten Sicherheitslücken steige. Beide Änderungen werden in den Text aufgenommen. In Zeile 355 werden zusätzlich Browsererweiterungen aufgenommen. Ein Mitglied spricht sich dafür aus, ausführlicher zu erklären, warum Plugins Angriffsziele seien.

Ein Mitglied macht darauf aufmerksam, dass Phishing technisch immer raffinierter werde. Der Aspekt wird in *Kapitel 1.2.6.2 Social Engineering & Phishing* aufgenommen.

Ein Mitglied plädiert dafür, vor oder nach Kapitel *1.2.6.3 Ausnutzen des Anwenderverhaltens* ein Kapitel Ausnutzen des Anbieterverhaltens einzufügen. Es liege nicht immer nur am Nutzerverhalten. Sicherheitslücken würden von Anbietern nach Bekanntwerden nicht immer ausreichend schnell geschlossen. Kriminelle nutzten diesen Zeitvorsprung aus.

Ein Mitglied befürwortet eine entsprechende Ergänzung ausdrücklich. Im Bereich der Smartphones müsse sich der Nutzer beispielsweise auf den Anbieter verlassen. Die Aussage, dass in den meisten Fällen der Anwender zur Unsicherheit beitrage, sei in Zukunft nicht mehr treffend. Die Systeme seien zwar einfacher zu bedienen, aber schwerer zu konfigurieren. Daher müsse sich der Nutzer stärker auf den Anbieter verlassen.

Ein Mitglied teilt mit, dass ein entsprechendes Unterkapitel eingefügt werde.

Ein Mitglied wünscht einen Hinweis zur Hackerethik in *Kapitel 1.3.1 Motivation der Angreifer verringern*. Dieser könne zur Erläuterung der intrinsischen Motivation von politischen und ideologischen IT-Angriffen („Hacks“) beitragen. Ein entsprechender Textbeitrag wird eingereicht.

Die Mitglieder diskutieren die Notwendigkeit der Fußnote 98 in *Kapitel 1.3.2.2 Entwicklung sicherer Software*. Die Fußnote wird gestrichen.

Ein Mitglied trägt vor, dass der BITKOM e.V. ein Mittelstands-CERT betrieben habe, welches jedoch kaum genutzt worden sei. Es sei daher nicht nur die Schulung der Nutzer, sondern auch ein gewisser Appell an die Selbstverantwortung der Nutzer notwendig.

Ein Mitglied sagt, dass sich mittelständische Unternehmen oft keine IT-Sicherheitsexperten leisteten und keinen Bedarf an Schulungsmaßnahmen zeigten. Hier sei der Gesetzgeber gefragt. Es müsse eine Incentivierung erfolgen. Die Prioritätensetzung der Unternehmer müsse erzwungen werden. Appelle alleine reichten nicht. Ein Mitglied fügt hinzu, dass auch Privatpersonen in der Pflicht seien, sich mit IT-Sicherheit auseinanderzusetzen. Es wird ein Verweis zum Bericht der Projektgruppe Medienkompetenz hinzugefügt.

Ein Mitglied erklärt, dass das *Kapitel 1.3.2.4 Nutzung sicherer Systeme* überarbeitet werde. Es fehle der Aspekt, dass die Sicherheitsanforderungen je nach Infrastruktur variierten.

Ein Mitglied äußert, dass mit einer zunehmenden Vernetzung, beispielsweise durch SmartGrid, immer komplexere Systeme mit immer mehr Schnittstellen entstünden. Dadurch sei Sicherheit immer schwieriger zu erreichen. Es sei zwar möglich sichere SmartGrid-Endgeräte herzustellen, aber diese seien dann so teuer, dass der Einsatz von SmartGrid unökonomisch werde. Ein Mitglied fügt hinzu, dass SmartGrid letztendlich zu steigender Komplexität der Netzsteuerung führe. Durch steigende Komplexität werde es immer schwieriger Sicherheit aufrechtzuerhalten. Beide Aspekte werden in den Text aufgenommen.

Auf Vorschlag eines Mitgliedes wird der Satz in Zeile 524 f. gestrichen.

Ein Mitglied weist darauf hin, dass die Cybercrime Convention nicht unumstritten sei. Im Sinne einer ausgewogenen Darstellung müssten auch Kritikpunkte erwähnt werden. Zwei Mitglieder reichen einen Textbeitrag ein.

Auf Wunsch eines Mitgliedes wird zu *Kapitel 1.4.1.2 G8: Subgroup on High-Tech Crime* eine Quelle nachgereicht.

TOP 2
Verschiedenes

Ein Mitglied teilt mit, dass sich der zweite Teil des Papieres zu den Themenfeldern „Kriminalität im Internet – Spionage – Sabotage“ noch in der internen Abstimmung befinde.

Aus diesem Grund bittet es um Verschiebung der für den 10. Februar 2012 geplanten Klausurtagung.

Die für den 10. Februar 2012 geplante Klausurtagung wird verschoben. Ein neuer Termin wird ermittelt.

Der nächste Sitzungstermin ist Montag, der 27. Februar 2012.