Stellungnahme zum Expertengespräch der Projektgruppe Zugang, Struktur und Sicherheit im Netz der Enquete-Kommission Internet und digitale Gesellschaft des Deutschen Bundestages

Prof. Dr.-Ing. habil. Jochen H. Schiller
Institute of Computer Science
Freie Universität Berlin

Frage 1: Forschungsbedarf/Erkenntnisdefizite

Wie technische Sicherheit funktioniert, ist bekannt, aber es wird oft nicht umgesetzt. Wie steht es um den Forschungsbereich Sicherheit im Netz generell und an welchen Stellen besteht insbesondere noch Forschungsbedarf und wo sehen Sie tatsächliche Erkenntnisdefizite?

In der Tat sind die grundlegenden Algorithmen zur Verschlüsselung, die Verfahren zur Absicherung von Kommunikation und Systemen in der Wissenschaft seit langem, aber auch in der technisch interessierten Öffentlichkeit umfassend bekannt. Das Problem besteht oft darin, dass dieses Wissen nicht in Produkte oder das konkrete Handeln fließt: Betriebssysteme basieren selten auf einer sicheren Architektur, Anwendungen missachten Grundregeln der gesicherten Kommunikation, Softwareentwickler ignorieren Regeln der Entwicklung sicherer Software etc. Hinzu kommt die leider oft vorhandene Fahrlässigkeit im Umgang mit IKT-Systemen oder schlicht die Unwissenheit bei Laien. Komfort und Funktion gehen klar vor Sicherheit.

Es gibt aber durchaus noch einige Wissenslücken, die es zu schließen gilt. So bringen neue Technologien bzw. Trends auch neue sicherheitsrelevante Fragestellungen: Wie wird die Komplexität massiv verteilter, eingebetteter Systeme aus Sicherheitssicht beherrscht (Stichwörter Internet der Dinge, intelligente Umgebungen)?

Wie wirkt sich die zunehmende Vermischung von Steuerung eines Netzes mit der Nutzdatenübertragung aus (klassische Kommunikationsnetze trennen Steuerungsdaten von Nutzdaten und können damit ggf. bei Missbrauch besser eingreifen - im klassischen Internet sind alle Daten „gleich“ und somit können auch normale Nutzer die Systeme einfacher angreifen)?

Wie sehen heutige Kommunikationsstrukturen wirklich aus? Gibt es ein „national“ abschottbares Netz gegen Angriffe (oder auch nur Fehlkonfigurationen) von außen? Welche Schwachstellen gibt es und wo befinden sich diese? Wie kann eine „sanfte“ Migration weg von Kommunikationsprotokollen aus den 70er/80er Jahren des vergangenen Jahrhunderts (TCP, IP bis hin zu BGP, DNS etc.) erreicht werden? Welche Rolle spielt hierbei die immer mehr dominierende Mobilkommunikation (immerhin weit über 5 Mrd. Nutzer weltweit) und ihre spezifischen Schwachstellen? Etc.

Wie man sieht, bleiben auch im eher technischen Bereich noch viele Fragen unbeantwortet. Eher gesellschaftliche Fragestellungen werden im Kontext der dritten Frage beantwortet.

Frage 2: Risiken/Kritische Infrastrukturen/Politik

Welche Risiken ergeben sich für die Gesellschaft aus ihrer immer größer werdenden Abhängigkeit von der Netz- und Mobilkommunikation und was folgt daraus für die kritischen Infrastrukturen? Wie kann der Schutz dieser kritischen Infrastrukturen gewährleistet werden und welche Aufgaben ergeben sich hier für die Politik?

Kommunikationstechniken funktionieren „fast immer"; daraus ergibt sich eine große Erwartungshaltung in der Bevölkerung bis hin zu einem medienwirksamen Aufschrei, wenn z.B. das Mobilfunksystem auch nur teilweise, für nur einen Teil der Nutzer und auch nur für eine relativ kurze Zeit ausfällt. Gerade mit zunehmender Robustheit und eigentlich geringer Störanfälligkeit schleicht sich ein Gefühl der (trügerischen) Sicherheit ein. Dieses Verletzlichkeitsparadoxon wird durch eine immer weiter gehende Abhängigkeit verstärkt. Viele Bürger besitzen ein Mobiltelefon als primäres, immer mehr als einziges Kommunikationsmittel. Gerade in der jüngeren Generation ist dieser Trend massiv zu beobachten (aber auch 75% der über 65 Jährigen nutzen Mobilkommunikation – und verlassen sich auch immer mehr darauf). Just-in-time-Logistik, Flottenmanagement etc. funktionieren nur mit Mobilkommunikation. IKT, speziell auch die Mobilkommunikation, zählen klar zu den Kritischen Infrastrukturen und müssen auch als solche kommuniziert und behandelt werden. Dies wird umso klarer, je mehr man sich z.B. auch bei der automatischen Generierung von Notrufen durch verunfallte Autos auf diese Systeme verlässt.

Alarmierend ist dabei die Erkenntnis, dass selbst viele Netzbetreiber feststellen, dass sie nur wenig Einblick in ihren Datenverkehr und noch weniger Möglichkeiten zu dessen Beeinflussung haben. Im Großen und Ganzen kann laut einer Umfrage der Fa. Arbor Networks Inc. davon ausgegangen werden, dass viele Mobilnetzbetreiber (GSM, UMTS, aber auch WLAN hotspots) hinsichtlich der Sicherheit auf dem Stand von Festnetzbetreibern von vor 8-10 Jahren sind. Diese Netze werden aber bereits massiv angegriffen; knapp die Hälfte der Angriffe führen auch zu gewissen Beeinträchtigungen bei Kunden. Da mobile Endgeräte (Handys, Smartphones etc.) auch nichts anderes als Computer mit Betriebssystemen sind, ist es klar, dass sie sowohl Angriffsziele als auch Angriffsmittel sein können. Knapp 10% der Netzbetreiber gehen davon aus, dass zwischen 10 und 25% der Endgeräte in Mobilnetzen an Botnets teilnehmen. Dramatischer ist die Aussage, dass über die Hälfte der Netzbetreiber keinerlei Aussagen darüber machen können, ob in ihrem Netz derartiges geschieht. Eigene Tests zeigen, dass auch in deutschen UMTS-Netzen durchaus Geräte Ziel von Angriffen sind.

Es ist illusorisch, ein Netz wie das Mobilkommunikationsnetz, welches auch für sicherheitskritische Belange genutzt wird – und sei es nur der Notruf – vom allgemeinen Internet mit seinen Gefahrenszenarien zu trennen. Im Gegenteil, das Mobilkommunikationsnetz wird und ist teilweise schon DAS Internet für viele Menschen bzw. der Zugang zu selbigem. Der Schutz dieser kritischen Infrastruktur kann daher im Wesentlichen nur durch Aufklärung, Erforschung der spezifischen Schwachstellen und vor allem Beachtung des Standes der Wissenschaft und Technik erzielt werden. Sicherheit muss insbesondere hier ein wesentliches Merkmal, ein Wettbewerbsvorteil werden – etwas mit dem man werben kann und das auch entsprechend honoriert wird. Die Politik kann hier ein wesentlicher Initiator einer verbesserten Sicherheitskultur sein – muss aber natürlich die *key player* mit ins Boot holen um nicht als einsamer Mahner ignoriert zu werden. Im Bereich der spezifischen Forschungsförderung wird hier schon der richtige Weg gegangen. Firmen sollten aus Eigeninteresse eine verbesserte Sicherheitskultur leben – eine gesetzliche Verpflichtung zur

Veröffentlichung von Vorfällen (*cyber incident disclosure*) wäre hier ein sicher erfolgversprechendes Hilfsmittel.

Frage 3: Umgang mit Unsicherheiten/Risikokommunikation/Sicherheitsmanagement

Wir allen wissen, dass vollständige Sicherheit eine Illusion ist. Insbesondere technische Systeme werden niemals frei von Unsicherheiten sein und es ist ein Sicherheitsmanagement geboten. Was ist der richtige Umgang mit diesen Unsicherheiten, wie kann ein solches Sicherheitsmanagement zum Umgang mit Risiken aussehen? Sollte man darüber kommunizieren und in welcher Form? Sind die Unternehmen, der Einzelne oder die Politik der richtige Adressat einer solchen Kommunikation?

Eine wesentliche Basis in der IKT sind sicherlich die vom BSI veröffentlichten Standards zur IT-Sicherheit (IT-Sicherheitsmanagement und IT-Grundschutz). Klassische strategische Aufgaben (Bedrohungsanalysen, Schwachstellenanalyse, Erstellen von Sicherheitskonzepten, Festlegung von Verantwortlichkeiten etc.) und operative Aufgaben (Risikoanalyse, Planung von Maßnahmen, Schulung, Überwachung der Umsetzung etc.) sind notwendig, aber nicht hinreichend. Diese Aktivitäten sind oft sehr technisch orientiert, beinhalten aber selten die möglichst transparente Kommunikation von Risiken, Vorfällen, Gegenmaßnahmen etc. nach außen. Sicherheitsmanagement wird oft nur im Kontext eines Unternehmens gesehen, als wäre das Thema ein abschottbares, internes (die Problematik des Schutzes gewisser Interna wird natürlich gesehen, darf aber nicht immer und überall vorgeschoben werden!).

Im Bereich „Sicherheit im Netz“ gilt wie überall, dass nur ein Aufbau des Vertrauens im Vorfeld eines Ereignisses – z.B. durch bewusste, verantwortungsvolle Risikokommunikation – die Krisenkommunikation während oder nach einem Ereignis glaubwürdig macht. Verneint man das Vorhandensein von Risiken im Vorfeld und suggeriert man eine umfassende Sicherheit, die nicht vorhanden ist, so hat man automatisch jegliche Glaubwürdigkeit verspielt, sollte doch einmal etwas passieren. Dies gilt gleichermaßen für Unternehmen wie für Politik in ihrem Verhältnis zu Kunden bzw. Bürgern.

Natürlich spielen auch die Medien – klassische wie neue – eine wesentliche Rolle bei der Kommunikation von Sicherheitsvorfällen und Unsicherheiten. Gerade letztere, die „neuen“ Medien, sind prädestiniert für die Verbreitung von Informationen zu Vorfällen im Netzbereich und gewinnen nicht selten die Deutungshoheit unter Betroffenen. Politik und Unternehmen haben nicht länger die unbestrittene Deutungshoheit, insbesondere dann nicht, wenn der Verdacht einer Vertuschung aufkommt (berechtigt oder nicht ist hierbei oft zweitrangig).