Stellungnahme des BSI zu Fragen der Enquete-Kommission „Internet und digitale Gesellschaft“ zur Vorbereitung des Expertengespräches „Sicherheit im Netz“ am 28. November 2011

Andreas Könen
Leiter des Fachbereiches Sicherheit in Anwendungen und Kritischen Infrastrukturen Koordination und Steuerung, Bundesamt für Sicherheit in der Informationstechnik

Frage 1: Welche staatlichen Aggressoren sind dem BSI bisher beim Monitoring der Bundesnetzwerke aufgefallen und in welcher Art und Weise sind die jeweiligen Aggressoren vorgegangen? Gibt es eine Verbindung zwischen staatlichen Angriffen und organisierter Kriminalität?

a) Das BSI betreibt mit dem Monitoring der Bundesnetzwerke ein System, welches vor allem der Prävention vor und der Detektion von Angriffen dient. Bei der Detektion konzentriert sich das BSI auf die technische Betrachtung der verwendeten Angriffstechniken und die Entwicklung geeigneter Präventionsmaßnahmen gegen solche Angriffe. Die weitere Bewertung der einzelnen Angriffe und insbesondere die Täteridentifikation obliegt dann abhängig von der Art des erfolgten Angriffes den Polizeibehörden oder Nachrichtendiensten des Bundes.

b) Typische Angriffe auf die Bundesverwaltung laufen über E-Mails mit bösartigen Anhängen und über infizierte Webseiten und in selteneren Fällen als direkte Angriffe auf Webseiten des Bundes. Sieht man von den typischen Massenphänomenen Spam und Phishing ab, die der Cyberkriminalität zuzurechnen sind, handelt es sich bei den Angriffen auf die Bundesverwaltung um elektronische Spionage.

c) Ein Erkennungsmerkmal von Spionage-Angriffen gegen die Bundesverwaltung war seit dem Jahr 2005 die Verwendung bösartiger, d.h. mit Schadsoftware infizierter Dokumente. Durch Tätergruppen der Organisierten Kriminalität (OK) wurde solche Angriffe erst ab dem Jahre 2009 und dies fast ausnahmslos gegen Privatpersonen angewendet. Insofern haben sich die eingesetzten Techniken der Spionage und der OK einander angenähert. Ob allerdings Verbindungen zwischen OK und staatlichen Angriffen bestehen, lässt sich aus den dem BSI vorliegenden Daten nicht ablesen.

Frage 2: Welche zukünftigen Entwicklungen im Hinblick auf "Cyberterrorismus" zeichnen sich bereits jetzt ab?

Das BSI erlangt Informationen zu elektronischen Angriffen aus eigenen Befugnissen gegenüber der Bundesverwaltung, aus der Kooperation mit den Kritischen Infrastrukturen, der übrigen deutschen Wirtschaft und mit ausländischen Partnerbehörden sowie durch Auswertung öffentlich zugänglicher Quellen. Wird unter Cyberterrorismus die direkte Auslösung von Schadensereignissen mit Verletzung oder Tötung von Personen, hohen Schadenssummen und der Gefährdung der staatlichen Ordnung über das Internet verstanden, so sind alle bisher bekannten Angriffe sind der Cyberkriminalität, der Cyberspionage oder der Cybersabotage zuzurechnen. Lediglich folgende Fälle könnten bei deutlich weiter gefasster Definition dem Phänomen Cyberterrorismus zugerechnet werden:

Beispiel 1: Estland 2007 - Die Kommunikationsinfrastruktur eines Staates wird über mehrere Tage sehr stark gestört.

Beispiel 2: Georgien 2008 - parallel zu einer militärischen Auseinandersetzung fanden Angriffe über das Internet auf Georgien statt.
Beispiel 3: Hacktivismus durch NoNameGroup und Anonymous - Hier gab es teilweise wahllose DoS-Angriffe auf Firmen, aber auch Informationsbeschaffungen durch das Hacken von Webservern.

Insgesamt sieht das BSI für die nahe oder mittlere Zukunft keine Entwicklungen hin zu Angriffen und Gefährdungen, die die Bezeichnung „Cyberterrorismus“ im engeren Sinn verdienen. Für die Angriffsformen der Cyberspionage und Cybersabotage fällt diese Beurteilung deutlich pessimistischer aus.

Frage 3: Welche Mittel wendet das BSI bisher an, um den Schutz kritischer Infrastrukturen zu gewährleisten und welche Anforderungen an den Schutz sind zukünftig erforderlich?

a) Mittel zum Schutz Kritischer Infrastrukturen
Grundsätzlich sind die Betreiber Kritischer Infrastrukturen selbst in der Verantwortung, den notwendigen Schutz sicherzustellen. Dies gilt in Bezug auf alle relevanten Aspekte, einschließlich der potentiellen IKT-spezifischen Bedrohungen.

Diese Verantwortung kann und soll den Betreibern nicht abgenommen werden. Dies gilt insbesondere auch für den IKT-spezifischen Schutz von Kritischen Infrastrukturen allgemein sowie für den Schutz Kritischer IKT-Infrastrukturen, also des Anteils IKT-spezifischer Infrastrukturen, die für Staat, Wirtschaft und Gemeinwesen kritisch im Sinne der Definition Kritischer Infrastrukturen sind.

Staatliche Eingriffsbefugnisse bestehen für das BSI in Bezug auf IKT-Sicherheit Kritischer Infrastrukturen in der Regel weder allgemein noch konkret. Daher kann das BSI den unmittelbaren Schutz Kritischer Infrastrukturen durch Anwendung eigener Mittel nur begrenzt gewährleisten.

Dennoch besteht natürlich ein erhebliches staatliches Interesse, den notwendigen Schutz Kritischer Infrastrukturen sicherzustellen. Im Rahmen seines Auftrags trägt des BSI hierzu in verschiedensten Bereichen umfangreich bei. Beispielhaft sollen hier folgende Punkte genannt werden:

- Besondere Berücksichtigung des Schutzes Kritischer Infrastrukturen bei der Umsetzung der Cybersicherheitsstrategie des Bundes
- Kooperation mit Betreibern Kritischer Infrastrukturen bei der strategischen Umsetzung des IKT-spezifischen Schutzes Kritischer Infrastrukturen (Kontext: Cybersicherheitsstrategie des Bundes, Umsetzungsplan KRITIS)
- Einbindung von Betreibern Kritischer Infrastrukturen in die Warn- und Krisenkommunikation des IT-Lagezentrums und des IT-Krisenreaktionszentrums des Bundes, das im BSI betrieben wird
- Spezifische Berücksichtigung von Aspekten des Schutzes Kritischer Infrastrukturen bei der täglichen Beobachtung der IKT-Lage
- Besondere Behandlung von IKT-Vorfällen mit Relevanz für Kritische Infrastrukturen (z.B. Stuxnet)

Darüber hinaus sind die allgemeinen Tätigkeiten des BSI eine gerade für den Schutz Kritischer Infrastrukturen unverzichtbare Grundlage. Dies sind beispielsweise:

- Bereitstellung allgemeiner Empfehlungen zum Schutz von IKT-Systemen. Diese enthalten auch wesentliche Hinweise für den Schutz Kritischer Infrastrukturen enthalten (IT-Grundschutz nach BSI, ISi-Reihe et al.)

- Bereitstellung von Studien und Sicherheitsanalysen zu spezifischen IKT-Themen und IKT-gestützten Basistechnologien
- Verbesserung des Schutzes von IKT-Systemen allgemein. Dies trägt auch zur Verringerung der allgemeine Bedrohung für Kritische Infrastrukturen bei.

b) Zukünftige Anforderungen für den Schutz kritischer Infrastrukturen
Die Anforderungen, die an den allgemeinen wie auch den IKT-spezifischen Schutz Kritischer Infrastrukturen gestellt werden müssen, sind heute wie in der zukünftigen Entwicklung stark von den allgemeinen Anforderungen an die jeweiligen Kritischen Infrastrukturen wie auch von der jeweiligen technischen Implementierung abhängig.
Beispielsweise werden Anforderungen an Großtransaktionen im Finanzdienstleistungsbereich primär die Integrität der Transaktion sicherstellen müssen, während in der Energieversorgung eine nahezu ununterbrochene Stromversorgung sichergestellt werden muss.
Solche besonderen Anforderungen müssen dann in der Zusammenarbeit mit den jeweiligen Aufsichtsbehörden mit Blick auf die spezifisch notwendige IKT-Sicherheit gewährleistet werden.

Die Fortentwicklung Kritischer Infrastrukturen in der IKT-Technik muss so gestaltet werden, dass der notwendige IKT-spezifische Schutz auch in Zukunft gewährleistet werden kann. Dies erscheint nur dann wirtschaftlich realisierbar, wenn IKT-Sicherheitsaspekte schon in der fachlichen wie auch in der allgemeinen technischen Auslegung zukünftiger Kritischer Infrastrukturen von Anfang an ausreichend mit berücksichtigt werden.

Hierzu kann das BSI durch die Bereitstellung von Mindeststandards, Technischen Richtlinien, Best Practises und ggf. rechtlich verbindliche Vorgaben zur Weiterentwicklung der Informationssicherheit bei den Kritischen Infrastrukturen beitragen. Insbesondere implementiert das BSI aktuell auf Basis der Cyberstrategie des Bundes im Cyberabwehrzentrum eine enge Kooperation mit den Aufsichtsbehörden der Kritischen Infrastrukturen.