Stellungnahme Dr. Sandro Gaycken
Expertengespräch „Sicherheit im Netz“

Welche Art von Angriffen sehen Sie jetzt und in den nächsten Jahren als zentrale Bedrohung für die Sicherheit von kritischen Informationsinfrastrukturen und mit welchen Akteuren sind diese verbunden?

Angriffsvarianten lassen sich passend über die Akteurstypen konzipieren. Es gibt sechs mögliche Akteure, die sich auf unterschiedliche Gefährdungsstufen abbilden lassen.
Auf den untersten Stufen befinden sich Cyber-Kleinkriminelle und Aktivisten.

(1) ***Cyber-Kleinkriminelle:*** **Diese Gruppe Akteure wird weiter präsent bleiben und anwachsen**, denn es fehlen effiziente technische und juristische Werkzeuge der Strafverfolgung. Cyber-Kleinkriminalität ist i.d.R. global verteilter, internetbasierter Betrug. Als beheimatende Länder sind solche besonders prädestiniert, bei denen eine hohe Quote arbeitsloser Informatiker mit hoher Grundarmut korrespondiert (wie Russland und China). Aber auch Informationsgesellschaften sind stark im Spektrum der Angreifer vertreten (USA).

(2) ***Aktivisten:*** Auch diese Gruppe Akteure wird in Zukunft weiter anwachsen. **Plakative Aktionen im Netz sind immer und außerdem global möglich,** generieren oft zusätzliche Aufmerksamkeit oder können per se als politische Partizipation verstanden werden. Ausschlaggebend für anhaltende Aktivitäten werden aber (1) mögliche Reichweiten und (2) anhaltende mediale Aufmerksamkeiten sein. Die Reichweiten könnten sich beschränken, da ein Grundschutz in der Regel ausreichend ist, um diese Akteure abzuwehren. Zudem könnten die Medien künftig weniger über diesen Vektor berichten, wenn er zu gängig und alltäglich wird. Beides wird den Nutzen relativieren.

(3) ***Cyberterroristen:*** **Cyberterror ist ein niedriges Risiko, da die Wahrscheinlichkeit hoher Schäden außerordentlich gering ist.** Während es technisch möglich ist, Schäden mit Terrorwirkung zu verursachen, sind solche Angriffe stark voraussetzungsreich. Hohe und unterschiedliche Fachexpertisen, Testlaboratorien und Zugriff auf nachrichtendienstliche Fähigkeiten sind notwendige Bedingungen zur Vorbereitung und Durchführung schlagkräftiger Attacken auf kritische Strukturen. Bei Terroristen ist es aufgrund der taktisch bedingten Zellenstruktur höchst unwahrscheinlich, dass sie diese Bedingungen erfüllen können. Zudem sind Cyberangriffe in diesem Format sehr teurer (mehrere Millionen Euro) und in der Vorbereitung schwerer zu tarnen als jeder Einsatz von Sprengstoffen. Diese Unwahrscheinlichkeit ist allerdings eine aktuelle Einstufung, die in Zukunft zu variieren sein könnte, wenn Cybermilitärs aus dem Dienst entlassen werden oder wenn Cybersöldner halbkriminelle Geschäftsmodelle verfolgen sollten.

Zur Einstufung**:** Für diese Akteurstypen gilt, dass sie zwar oft deutlich sichtbar, entgegen landläufiger Meinungen aber kaum gefährlich sind. Kleinkriminelle sind bislang kaum in der Lage, pro Angriff größere Beträge zu erbeuten, auch wenn sie insgesamt große Beträge erbeuten können (De Minimism-Problem). Aktivisten können keine kritischen Strukturen kritisch gefährden (haben dies auch nie getan, auch nicht in populären Fällen wie Estland 2007) und legen vorrangig wenig relevante Systeme wie Webseiten temporär lahm. Dies korrespondiert unmittelbar den Fähigkeiten dieser Akteurstypen. Sie können zwar organisatorisch im Umfang von Schwarmintelligenz, insgesamt aber nur auf begrenzt hohe offensive Expertisen zugreifen, können nur besonders gängige Angriffsvektoren wie das Internet nutzen und verfügen auch sonst über keine weiteren Angriffsboni. Insbesondere für die Verursachung von Folgeschäden nach dem IT-Einbruch fehlt ihnen in der Regel jegliche Kenntnis. Das schränkt ihre Möglichkeit und damit auch mögliche Gefährdungen durch diese Akteure stark ein. **Die geringe Gefährdung ist unbedingt relevant für die Allokation von Ressourcen auf Gegenmaßnahmen.** So werden aktuell viele Strafverfolgungsmittel konzipiert, die bereits gegen diese niedrigschwelligen Angreifer kaum effizient sind (zB Vorratsdatenspeicherung), und es werden Schutz- und Aufklärungskonzepte gegen technische Werkzeuge gefördert, die außerhalb dieser ungefährlichen und wenig relevanten Aktivitäten keine Rolle spielen (zB Botnetze).

Auf den oberen Gefährdungsstufen (mittlere sind m.E. nicht auszumachen) finden sich organisierte Kriminelle, militärisch-nachrichtendienstliche Angreifer und Cybersöldner.

(4) ***Organisierte Kriminalität:*** Dieser Angreifertyp ist aktuell noch in der Entstehung. Die OK hat erst seit Kurzem umfänglich gemerkt, dass Fähigkeiten in diesem Bereich hochgradig profitabel sind.

Die OK wird sich im Gegensatz zu den Cyber-Kleinkleinkriminellen hocheffiziente, professionelle Angreiferteams mit nachrichtendienstähnlichen, zusätzlichen Angriffsvektoren zusammenstellen. Mit diesen Teams wird sie prinzipiell Zugriff auf alle IT-Strukturen weltweit haben, da für dieses Angreifermodell keine hinreichenden Sicherungen existieren. Zudem sind diese Angreifer kaum zu detektieren und nie zu identifizieren – ein Problem, das sich durch keinen technischen Fortschritt beheben lassen wird. Die entstehende stille, risikofreie Allmacht verlagert das Spektrum der Tätigkeiten und Ziele. Statt klassische Betrugsmodelle an Einzelnutzern aufzuziehen, wird die OK stärker profitable Aktivitäten wie Industriespionage, Industriesabotage, Finanzmarktspionage und Finanzmarktmanipulation verfolgen. Diese Aktivitäten werden auch bereits beobachtet. **Finanzmärkte sind ein besonders brisantes Ziel, da sie aufgrund ihrer hohen Anforderungen an IT und Daten prinzipiell nicht gegen hocheffiziente Angreifer zu sichern sind. Finanzmarktmanipulation ist für diese Akteure gegenwärtig bereits umfassend möglich und wird mittelfristig nicht abgewehrt werden können.** Ebenfalls in diesen Bereich können professionalisierte Industriespione gerechnet werden, die inzwischen ebenfalls hohe Fähigkeiten erarbeitet haben, aber stärker lokal für unterschiedliche Auftraggeber in unterschiedlichen Kontexten arbeiten.

(5) ***Militärisch-nachrichtendienstliche (staatliche) Angreifer:*** Mit Ausnahme bereits etablierter Akteure wie Russland und China ist auch dieses Angreifersegment gegenwärtig erst noch im Entstehen und wird erst in drei bis sieben Jahren vollständig operationsbereit sein. Dann allerdings werden weltweit offensive Cybertruppen existieren, auch in Schwellen- und Entwicklungsländern, da die Einstiegskosten in den offensiven Cyberwar vergleichsweise gering und die Voraussetzungen zu bewältigen sind. Auch für diesen Akteur gilt das Paradigma, dass er auf jede IT-Struktur Zugriff hat (ob am Internet oder nicht), dass er nahezu nicht detektierbar und absolut nicht identifizierbar ist. Außerdem kann dieser Akteur taktisch vorgehen und komplexe Zielmengen verfolgen. Es ist allerdings je nach Stand der Fähigkeiten nur ein begrenztes Spektrum von Zielen gleichzeitig verfolgbar. **Staatliche Cyberangriffe sind nur in einigen wenigen Szenarien denkbar.** Allerdings eröffnet der Cyberwarfare einige neuartige strategische Optionen, die bereits in Friedenszeiten zu großen Problemen führen können und gegenwärtig noch nicht angemessen begriffen sind. **Besorgniserregend sind hier etwa präventive Installationen oder Feldtests von Cyberwaffen an Kritischen Infrastrukturen, propagandistisch-manipulative Information Operations im Web 2.0 oder das bislang wenig beachtete Feld der Economic Operations**, dem mit dem Cyberzugriff auf ganze Wirtschaften vollkommen neue Optionen eröffnet werden. Ein fremdes Land kann gegenwärtig mit einiger Geduld für geringe Kosten und Risiken über Wirtschaftsspionage und Wirtschaftsmanipulation in den Ruin geführt werden, während das eigene Land proportional wirtschaftlich (und geostrategisch) aufgebaut werden kann. Diese Einsicht setzt sich aktuell weltweit durch und wird bestimmt Interessenten finden. Westliche Informationsgesellschaften sind dann besonders intensiv betroffen, Deutschland zusätzlich stark, da hier viel Forschung und Entwicklung betrieben wird.

(6) ***Cybersöldner*****:** Söldnerfirmen avisieren allem Anschein nach den taktischen Feldhacker als Geschäftsmodell. **Dieser Hacker wäre spezifisch auf Cyberangriffe auf militärisches Gerät im Feld spezialisiert und könnte bei High-Tech-Armeen im entscheidenden Moment technische Vorteile abschalten oder manipulieren.** Da High-Tech-Armeen ohne ihre Hochtechnik leicht von kampferprobten Low-Tech-Armeen besiegt werden können, ergibt sich ein Geschäftsmodell für den Cybersöldner, der dann in asymmetrischen Konflikten an die technisch unterlegenen Parteien vermietet werden kann. Für die Taliban etwa wäre eine gute Truppe von Cybersöldnern von unschätzbarem Wert.

Zur Einstufung**:** Diese Akteure sind erkennbar gefährlicher, da sie wesentlich bessere Fähigkeiten ausbilden können. Sie kommen so an alles heran, können ihre Angriffe besser ausbeuten. Sie sind zudem nicht auf das Internet als Angriffsvektor angewiesen, da sie über Innentäter verfügen können. **Gegen diesen Akteur helfen keine der aktuell debattierten Maßnahmen** zu Abwehr, Aufklärung, Identifizierung, Beherrschung, Regulierung, Verrechtlichung. Sie sind zudem besonders „stille" Angreifer, denn im Gegensatz zu den schwachen Angreifern sind sie kaum sichtbar, da sie Detektion hocheffizient vermeiden können und wollen, und sie tendieren auch in ihren Wirkungen eher zu einer über lange Zeiträume laufenden katastrophalen Kumulation an sich kleiner und unscheinbarer Einzeleffekte. **Das macht ein Erkennen von Aktivitäten und Interessen, eine Genese hinreichender politischer Aufmerksamkeit und eine Konzeption von Gegenmaßnahmen in**

diesem Fall sehr schwierig und langwierig – eine zusätzliche Hürde, die diese Angreifer einplanen können und der offensive Tätigkeiten in diesem Bereich zusätzlich attraktiv macht.

Inwieweit sehen Sie Angriffsszenarien, bei denen die Struktur des Internets wirklich relevant ist und welche weiteren Gefahrenquellen gibt es noch?

Das Internet ist für Angreifer und Angegriffene relevant, wenn es zur kritischen Komponente für kritische Prozesse wird. Da diese Kritikalität aber pro Land, pro Technik, pro Prozess sehr unterschiedlich sein kann, ist es schwer, allgemeine Aussagen zu treffen. Wir können aber folgende Punkte festhalten:

(1) **Das Internet ist in steigendem Maße relevant und kritisch für die Wirtschaft, und zwar für ihre Organisation, ihre Produktion wie für das Verwalten des Wissens aus Forschung und Entwicklung.** Damit ergeben sich für Angreifer entsprechende Inzentive für Wirtschaftsspionage und -sabotage. Dies gilt wie erwähnt in besonders hohem Maße für die Finanzmärkte. Alle Angreifertypen sind hier prinzipiell möglich, schwache Angreifer werden allerdings keine kritischen Schäden, sondern eher temporäre Störungen anrichten. Starke Angreifer dagegen können und werden kritische Schäden anrichten, dabei aber unsichtbar bleiben.

(2) **Für andere kritische Prozesse hängt deren Vulnerabilität von Art und Ausmaß der freiwilligen Exposition zum Internet ab.** Kritische Infrastrukturen zB können über das Internet angegriffen werden, wenn sie dort exponiert sind. Wer angreifen kann, hängt von der Art der Sicherung ab. Schwache Angreifer werden mit einem gewissen (aber vielfach noch zu definierenden) Grundschutz abgewehrt werden können. Starke Angreifer lassen sich zum Teil nur durch Rückzug aus der Vernetzung (Entnetzung) abwehren. Es muss hier allerdings noch flächendeckender als bisher evaluiert werden, was überhaupt wo in welcher Weise am Internet hängt. Das BSI sollte entsprechend angewiesen und personell verstärkt werden. Leider kommen immer wieder haarsträubend naive Vernetzungen ans Tageslicht. Zwei Beispiele von kritischen Strukturen mit nahezu ungeschützten Internetzugängen sind einige Steuerungen von Schleusentoren und einige Notrufnummern.

(3) Das Internet ist allerdings nicht das Kernproblem der IT-Sicherheit. Das Kernproblem der IT-Sicherheit sind die Hosts, die IT-Systeme selbst. Dies gilt vor allem aufgrund des Aufkommens der starken Angreifer. **Starke Angreifer sind nicht auf das Internet angewiesen, um IT-basierte Angriffe vorzubereiten oder durchzuführen.** Eine Verfügbarkeit ihrer Ziele im Internet kann aber in höherem Maße zu entsprechenden Angriffen verleiten, da die Kosten und Risiken solcher Angriffe weit niedriger und nahezu immer lohnend sind.

Welche Schutzmechanismen erachten Sie im Hochsicherheitsbereich, im normalen Sicherheitsbereich und bei privaten Anwendern für effektiv?

(1) Hochsicherheitsbereiche sind Hochsicherheitsbereiche, da sie sich gegen starke Angreifer schützen müssen. Entsprechend muss auch mit starken Cyberangreifern in diesen Bereiche gerechnet und ein proportionaler Schutz implementiert werden. Davon sind wir allerdings weit entfernt. **Gegenwärtig existieren nur theoretische Konzepte zu proportionalem Schutz gegen starke Angreifer.** Es muss ein Schutz der potentiellen Zielsysteme sein, und er muss grundlegend architekturell gedacht werden, d.h., es müssen vollständig neue Modelle von Hardware und Software konzipiert und gebaut werden, während die alten Technologien nicht länger verwendet werden sollten. Konventionelle IT-Sicherheitstechnik, Angreiferidentifikation über Forensik oder Netzüberwachung, Angreiferregulierung (sei es über Völkerrecht, Abschreckung, Vertrauensbildung oder Waffenkontrollen) und ähnliche, traditionelle Konzepte dagegen werden nicht länger hinreichend effizient sein, nicht einzeln und nicht kombiniert. **Im Hochsicherheitsbereich beherrschen aktuell „Schlangenölverkäufer“ aus Wirtschaft und Wissenschaft einige Debatten und Entscheidungsgremien**, die entsprechenden Schutz versprechen, allerdings nur konventionelle und inhärent ineffiziente Sicherheit haben können. Einige (nicht alle) Arbeitsebenen in Ministerien und Behörden sind zudem personell nicht gut und spezifisch genug ausgestattet, um entsprechend sachkundige Urteile für Anschaffungsentscheidungen treffen zu können. Gegenwärtig sind bereits einige Millionen an Fördergelder in Schlangenölprojekte unterwegs. Das wird durchgehend verschwendetes Geld sein, da in Kürze ohnehin noch echte Sicherheitsmaßnahmen angeschafft werden müssen.

Bis Konzepte zu IT-Hochsicherheit entwickelt sind, können folgende Schritte erfolgen:

1. Entwicklung von Sicherheitsmetriken zur Messung von Cyberrisiken und zur Objektivierung der Debatten und Maßnahmen
2. Information Sharing mit anderen Staaten zu starken Angreifern
3. Ausstattung und Beauftragung der Auslandsnachrichtendienste zur Aufklärung starker Angreifer im Ausland
4. Beforschung der starken Angreifer und ihrer Möglichkeiten und Interessen
5. Beforschung der Dilemmata wie der drastischen Grenzen von Ad Hoc-Schutzkonzepten und von Attribution und ihrer Folgen
6. Beforschung und Produktisierung proportionaler Schutz, vorzugsweise bei vertrauenswürdigen und sicheren Produzenten
7. Einrichtung einer staatlichen Hackergruppe, die auf dem Niveau starker Angreifer operieren kann und die zur staatlichen Evaluation des Schutzes kritischer Strukturen herangezogen werden kann
8. Einrichtung unabhängiger beratender Fachgremien zur Steuerung von Maßnahmen
9. Einrichtung zusätzlicher Kompetenzen und Stellen in den drei für das Verständnis von Cybersicherheitsfragen zuständigen Ministerien BMI, BMVg und Außenministerium, nicht nur im BMI
10. Inzentivierung stärker interdisziplinärer Forschung anstelle rein technischer oder rein politikwissenschaftlicher Forschungen

(2) **Im Sicherheitsbereich muss die Sicherheit pro System oder Prozess und proportional zu den dort zu erwartenden Angreifern entwickelt werden.** In einigen Fällen wird hier ein Grundschutz ausreichend sein, in anderen (wie etwa bei forschenden und entwickelnden, mittelständischen Unternehmen) muss eventuell ein Hochsicherheitsmodell implementiert werden. Je nach Struktur und Bedrohungslage ließen sich Vorgaben erstellen, die zu erfüllen wären. **Einige Schutzkonzepte (Software, Hardware, Organisation) könnten vom BSI entwickelt, ausgerollt und kostengünstig zur Verfügung gestellt werden.** Hier wäre auch eine Umkehr des Umgangs mit dem „Hackerparagraphen“ zielführend, die Unternehmen per Gesetz dazu verpflichtet, bestimmte Hackingtools regelmäßig gegen die eigenen Systeme einzusetzen, um die eigenen Schwachstellen zu finden.

(3) Der private Anwender ist i.d.R. nur von Cyber-Kleinkriminellen unmittelbar betroffen und kann auch nur dort reagieren. **Als Gegenmaßnahme wird hier vorrangig die Sensibilisierung eine wichtige Rolle spielen.** Einen Ausbau der Möglichkeiten der Strafverfolgung sollte man ebenfalls avisieren, allerdings müssen diese effizient sein und dürfen angesichts der in diesem Fall doch eher geringen Bedrohungslage keine zu voluminösen Trade-Offs mit Freiheitsrechten und Datenschutzbefindlichkeiten beinhalten. **Ob es effiziente und verträgliche Strafverfolgung in diesem Bereich je geben kann, kann bezweifelt werden.** Konventionelle Forensik mit Ermittlern scheint den technischen Mitteln vorzuziehen zu sein, wofür allerdings deutlich mehr Stellen in den Kriminalämtern geschaffen werden müssen, die sich mit Cyberkriminalität befassen können. Zudem müssen hier praktisch globale Rechtsabkommen begründet werden, was eine weitere, nicht-technische Hürde darstellt.

Kontakt:
Dr. Sandro Gaycken
Institut für Informatik
Freie Universität Berlin
s.gaycken@fu-berlin.de