Hackback in Deutschland: Wer, was, wie und warum?

Dennis-Kenji Kipker

Bremen

Gliederung

I. Neue Herausforderungen für die Cybersicherheit – neue Strategien für die Cybersicherheit
II. Zuständigkeitswirrwarr für Hackbacks?
III. Ein alter Bekannter: Die Bundeswehr
IV. Fazit und Ausblick

Was ist passiert?

- **Netzpolitik.org: „Hackbacks stehen schon lange auf der Wunschliste deutscher Behördenchefs.“**
- Mai 2019: Recherchen des BR
- Politische Offensive der Bundesregierung zum Hackback
- Internes Konzeptpapier beschreibt den behördlichen Abstimmungsprozess nach „erheblichem Cyber-Angriff aus dem Ausland“
- „Vierstufiges“ Raster von Gegenmaßnahmen wird beschrieben

Konzeptpapier der Bundesregierung

Öffentliche Diskussion in 2019

- Zulässigkeit, Zuständigkeit und Ausgestaltung des Hackback
- Erhebliche Kritik aus Zivilgesellschaft
- Allein Aufrüstung digitaler Angriffsmöglichkeiten bietet hohes Eskalationspotenzial
- Hackback = mehr Gefahren als Sicherheiten?

Dreh- und Angelpunkt der aktuellen Debatte…

…ist deshalb nicht nur das Problem der technisch-organisatorischen Durchführung von Hackbacks, sondern vielmehr die Frage nach der Wirksamkeit und damit zugleich der Sinnhaftigkeit von derlei vorgeschlagenen Maßnahmen!

→ **Matthias Schulze: Von Glashäusern und Steinewerfen. Strategische, rechtliche und politische Überlegungen vor dem zurück hacken**

Herausforderungen und Strategien für die Cybersicherheit

- Hackback in aktueller technischer und politischer Situation wenig überraschend
- In den letzten Jahren massiv gestiegene mediale Berichterstattung über (erfolgreiche) Cyberangriffe insbesondere aus dem Ausland
- Erklärtes Ziel des Hackbacks: Eindämmung ebenjener Angriffe
- Stetig mehr Akteure im digitalen Raum: Fremde Mächte, Industriespionage, Private, „Hacktivism“
- Vgl. aktuellen Lagebericht des BSI

Cyber-Sicherheitsstrategien

- Cyber-Sicherheitsstrategie der BReg aus 2016:
  - „Aktive Maßnahmen, um das Niveau der IT-Sicherheit in Deutschland + Europa ganzheitlich zu verbessern“
  - IT-SiG (2015) und Entwurf IT-SiG 2.0 (2019)

- EU-Cyber-Sicherheitsstrategie aus 2017:
  - Europaweite Koordination und Kooperation zum Schutz des digitalen Binnenmarkts
  - EU CSA (2019), derzeit Implementierung

Zuständigkeitswirrwar für Hackbacks?

- Politische „Blaupause“ eine Sache, aber konkrete Umsetzung andere Sache
- Zentrales Problem sowohl des Konzeptpapiers als auch einer früheren (2018) Ausarbeitung des Wissenschaftlichen Dienstes des BT:

Wer ist in Deutschland für die Durchführung der „Hackbacks“ zuständig, welche Behörde besitzt die rechtlichen und technischen Kompetenzen, um hier tätig zu werden?

Nationale Zuständigkeitsverteilung für den Hackback – NCAZ

- Zentral im Fokus: Nationales Cyber-Abwehrzentrum (NCAZ)

  BSI, Bundesamt für Verfassungsschutz (BfV), Militärischer Abschirmdienst (MAD), Bundesnachrichtendienst (BND), Bundeskriminalamt (BKA), Zollkriminalamt (ZKA), Bundespolizei (BPol) Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
- Erarbeitung eines „ganzheitlichen Lagebilds“ der Cybersicherheit
- Entscheidung, ob „erheblicher Cyber-Angriff aus dem Ausland“ vorliegt, der Hackback evoziert
- Freigabe für Gegenangriff durch NCAZ +/-

Nationale Zuständigkeitsverteilung für den Hackback – „politisches Gremium“

- Weiteres Gremium entscheidet über „politische Freigabe“ des Hackbacks, Vertreter von:
  - Bundeskanzleramt
  - Auswärtiges Amt (AA)
  - Bundesministerium der Justiz und für Verbraucherschutz (BMJV)
  - Bundesministerium der Verteidigung (BMVg)
  - Bundesministerium des Innern, für Bau und Heimat (BMI)

Nationale Zuständigkeitsverteilung für den Hackback – BND

- Konzeptpapier: BND für die Durchführung von Hackbacks geeignet, denn er „bewege sich unter anderem in IT-Infrastrukturen im Ausland, sammelt konstant Informationen über Cyberangreifer, deren Vorgehen und Infrastrukturen und wertet diese detailliert aus“
- Weitere Überlegung: Zuständigkeit bei einer „Polizeibehörde“, und BND wird dabei „zwingend“ einbezogen

Nationale Zuständigkeitsverteilung für den Hackback – BND

- Kompetenzzuweisung an BND äußerst fragwürdig!
- § 1 Abs. 2 BNDG: Nachrichtendienstbehörde mit der Aufgabe, solche Informationen, die zur Gewinnung von Erkenntnissen über das Ausland, die von außen- und sicherheitspolitischer Bedeutung für die BRD sind, zu sammeln und auszuwerten
- **Klartext:** BND darf zwar umfassende Informationen über relevante Daten sammeln, aber nicht selbst aktive Cyberangriffe durchführen
- Wäre beim Hackback aber gerade der Fall!

Nationale Zuständigkeitsverteilung für den Hackback – BVerfSch

- § 3 BVerfSchG: Behörde sammelt und wertet solche Informationen aus, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten gegen die BRD für eine fremde Macht betreffen, oder solche Bestrebungen umfassen, die gegen die freiheitliche demokratische Grundordnung, den Bestand oder die Sicherheit des Bundes oder eines Landes gerichtet sind oder eine ungesetzliche Beeinträchtigung der Amtsführung der Verfassungsorgane zum Ziel haben
- Tatbestand kann zwar durch unzulässige Cyber-Intervention erfüllt sein, BVerfSch wird aber vornehmlich im Inland tätig

Nationale Zuständigkeitsverteilung für den Hackback – BSI, BKA und weitere

- § 3 BSIG: Ausschließlich für Aufrechterhaltung und Förderung der operativ-technischen IT-Sicherheit und zur Zusammenarbeit mit Staat und Wirtschaft zuständig, hierunter fallen keine aktiv geführten technischen Angriffe, die Einrichtungen im Ausland betreffen und diese im Zweifelsfall kompromittieren oder zerstören sollen
- BKA: Vornehmlich eine Strafverfolgungsbehörde, die zwar Computerdelikte ermitteln kann und soll, aber nicht selbst Cyber-Angriffe im Ausland durchführt
- BPol: Ähnliche Probleme, soweit Tätigwerden im Ausland
- Weitere Behörden aus NCAZ: Technische Kompetenz vorhanden?!

Ein alter Bekannter: die Bundeswehr

- **Rechtliche Crux beim Thema Hackback:** Klassische Zuständigkeitsabgrenzungen verschwimmen mit der grenzüberschreitenden Natur und der Vielzahl von Interessen und Akteuren bei Cyber-Angriffen
- Wo befinden wir uns im Bereich der Prävention, wann beginnt die Gefahrenabwehr, was sind die Anforderungen an repressive Handlungen?
- Sind „Hackbacks“ im Ausland überhaupt als klassische nachrichtendienstliche, polizeiliche oder repressive Maßnahmen zu qualifizieren?
- → Einiges spricht dafür, dass dem nicht so ist – womit wir wieder beim altbekannten Thema „Bundeswehr und Cyber-Angriff“ wären

Ein alter Bekannter: die Bundeswehr

- Diskussion der letzten Jahre zum Thema: umfassend wie fruchtlos
- **Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr (2016):** Grundlegende Strategie für das Tätigwerden der BW im digitalen Raum, sog. „Cyber- und Informationsraum“ (CIR)
- CIR: „Der Raum, in dem Informationen generiert, verarbeitet, verbreitet, diskutiert und gespeichert werden. Der Cyberraum ist der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyberraum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann.“

Ein alter Bekannter: die Bundeswehr

- April 2017: Indienststellung eines eigenen „Kommando Cyber- und Informationsraum“ (KdoCIR), zuständig für den CIR
- 2018: „Zentrum Cyberoperationen“ (ZCO) innerhalb des KdoCIR wird begründet – technische Kapazitäten für „Offensivmaßnahmen im digitalen Raum“, ergo: Hackbacks
- → **Problem:** Tätigwerden der Bundeswehr im CIR setzt voraus, dass die hohen verfassungsrechtlichen Hürden für den Einsatz deutscher Streitkräfte erfüllt sind!

Ein alter Bekannter: die Bundeswehr

- Zentrale Anforderungen aus dem GG: Artt. 26, 35, 87a
- **Art. 87a GG:** Findet auch auf Außeneinsätze Anwendung – Streitkräfte dürfen außer zur Verteidigung nur dann eingesetzt werden, wenn durch GG ausdrücklich zugelassen
  - Ausnahmevorbehalt in völkerrechtskonformer Auslegung eng zu lesen, betrifft i.e.L. inneren Notstand oder überregionale Unglücksfälle
- Informationstechnische Operationen des Militärs sind Einsatz bewaffneter Streitkräfte bzw. eine bewaffnete Unternehmung, soweit mit traditioneller militärischer Einwirkung vergleichbar

Ein alter Bekannter: die Bundeswehr

- Vergleichbarkeit mit militärischer Einwirkung setzt nicht zwingend militärische Kampfhandlungen voraus

  Ausreichend: Anwendung militärischer Gewalt erscheint konkret möglich; Droh- und Einschüchterungspotenzial durch personelle und sachliche Mittel der BW gegeben, prognostische Erwartung ausreichend

- Da mittels informationstechnischer Mittel eine (erhebliche) Sabotage staatlicher Infrastrukturen möglich ist, dürfte „Hackback“ regelmäßig mit einem physischen Angriffsmittel vergleichbar sein

Ein alter Bekannter: die Bundeswehr

- Verfassungsrechtliche Folge: Einsatz der Bundeswehr für Hackback setzt Verteidigungsfall voraus
- **Verteidigungsfall:** Reaktion auf eine (auch nur unmittelbar bevorstehende) militärische und eindeutig dem Angriffsziel zurechenbare Gewaltanwendung, die von außen kommt, oder den Beistand eines angegriffenen Staates erfordert, soweit das Völkerrecht dies zulässt (vgl. Art. 51 UN-Charta)
- Erheblichkeitsgrenze zum militärischen Angriff nur dann überschritten, wenn die zur erfolgreichen Abwehr des Angriffs gängigen polizeilichen Mittel nicht mehr ausreichen

Ein alter Bekannter: die Bundeswehr

- Eng auszulegende verfassungsrechtliche Kriterien dürften für gegenwärtig skizzierten Regelfall des Hackbacks nicht erfüllt sein
- Problem außerdem: zur Entscheidung über den Hackback ist nicht das im Konzeptpapier skizzierte politische Entscheidungsgremium befugt, sondern der **Bundestag**
- Offensivmaßnahmen der Bundeswehr im CIR, die nicht unter das Selbstverteidigungsrecht fallen, sind als **„act of aggression“** völkerrechtswidrig (Missachtung des Gewaltverbots)

Ein alter Bekannter: die Bundeswehr

→ Einsatz der Bundeswehr (in jedweder Hinsicht) nur absolute Ausnahme und nicht Regelfall!

→ Darum gehen auch Überlegungen fehl, allgemein einen NATO-Bündnisfall für Cyberattacken anzunehmen, da diese vielfach nicht die Schwelle zu einem geforderten bewaffneten Angriff überschreiten!

→ Hackback deshalb höchstens für den Fall eines tatsächlich unmittelbar bevorstehenden Angriffs rechtlich zulässig!

Fazit und Ausblick

- Unabhängig von der aktuell geführten juristischen Debatte sollte die technische und gesellschaftspolitische Effektivität von Hackbacks Gegenstand weiterer Untersuchung sein
- Nachrichtendienste sowie Polizei- und Strafverfolgungsbehörden sind zur Durchführung von Hackbacks nicht die richtigen Akteure
- Gegenwärtig dürfen Hackbacks keine erheblichen Cyberangriffe sein, die einer militärisch geführten Operation gleichkommen
- Soweit aber aktive Gegenmaßnahmen unterhalb der militärischen Schwelle politisch diskutiert werden, ist zu erwägen, das BSI noch stärker als bisher einzubeziehen, vgl. Entwurf für das IT-SiG 2.0 („aktive Detektion“)

Weiterführende Quellen & Literatur

- Gleichnamiger Beitrag im Verfassungsblog: https://verfassungsblog.de/hackback-in-deutschland-wer-was-wie-und-warum/
- *Tanriverdi*, BR Recherche: Bundesregierung skizziert Hackback-Pläne: https://www.br.de/nachrichten/deutschland-welt/internes-papier-bundesregierung-skizziert-hackback-plaene
- *Biselli,* Aktiv, passiv, responsiv: Cyberangriffe durch die Bundeswehr? Definitionssache.*:* https://netzpolitik.org/2016/aktiv-passiv-responsiv-cyberangriffe-durch-die-bundeswehr-definitionssache
- *Meister/Biselli*, Geheimes Bundestagsgutachten attackiert Hackback-Pläne der Bundesregierung: https://netzpolitik.org/2019/geheimes-bundestagsgutachten-attackiert-hackback-plaene-der-bundesregierung/#2019-08-27_Bundestag-WD_Cyber-Abwehr-in-Deutschland
- *Wissenschaftlicher Dienst des Bundestages,* Verfassungsmäßigkeit von sog. „Hackbacks“ im Ausland: https://www.bundestag.de/resource/blob/560900/baf0bfb8f00a6814e125c8fce5e89009/wd-3-159-18-pdf-data.pdf
- Juristisches: *Schaller*, GSZ 2018, 57 und *Ziolkowski*, GSZ 2019, 51