Hack-Backs und Active Defense

Technische Implikationen und Herausforderungen

- Thomas Reinhold // cyber-peace.org -

Definitionen von Hack-Backs

IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

- Allgemein: potentiell invasive Aktivitäten in fremden IT-Systemen
- Aktive Verteidigung:
  the process of analysts monitoring for, responding to, learning from, and applying their knowledge to threats (SANS-Institut für Cyber-Sicherheit)
- Cyber-Gegenangriff:
  the protection of a designated Communications and Information System (CIS) against an ongoing cyberattack by employing measures directed against the CIS from which the cyberattack originates, or against third-party CIS which are involved (NATO CCDCOE)
- "Irgendetwas dazwischen"

Was sollen Hack-Backs können

- Beweissicherung
- Digitale Rettungsmission
- Unmittelbare Abwehr einer Bedrohung
- Digitaler Rettungsschuss als Ultima-Ratio
- Militärisches Wirkmittel unterhalb der Eskalationsstufe eines bewaffneten Angriffs
- Abschreckung potentieller Angreifer

"Rückverfolgung und gegebenenfalls das Unschädlichmachen eines Servers aus dem Ausland." Thomas de Maizière

"Wir haben ein Interesse daran, dass Angreifer die Daten verlieren, die sie gestohlen haben. Man muss solche Daten eventuell zum Schutz des Opfers zerstören." Hans-Georg Maaßen

Relevanz und Häufigkeiten von Cyberattacken

- Vorfälle von „Cyber-Angriffsformen nach der Definition des BSI (..) auf Behörden und öffentliche Stellen in dem Jahr 2016“

Gezieltes Hacking von Webservern	2
Drive-by-Exploits zur breitflächigen Infiltration	1.572.655
Gezielte Malware-Infiltration über E-Mail / Social Engineering	ca. 3/Woche
Distributed Denial of Service-Angriffe (DDoS)	17
Ungezielte Verteilung von Schadsoftware mittels SPAM oder Drive-by-Exploits	3.815.611
Mehrstufige Angriffe	0
	5.388.441

Informationsfreiheitsanfrage: https://fragdenstaat.de/anfrage/cyber-angriffsformen-nach-bsi-2016/

Schwierigkeiten und Herausforderungen (I)

- Attribution des Angreifers
  1. Woher erfolgt der Angriff
  2. Ist der identifizierte Ursprung wirklich der echte Angreifer

  => Gefahr von Fehlzuweisungen

  => politische oder militärische Eskalation
- Offenlegen der eigenen Fähigkeiten
  - viele Tools im Cyberspace leben von Verborgenheit
  - Verwendete Sicherheitslücken offenbahren Zugriffspunkte die dann geschlossen werden
  - Gegner lernen aus der Analyse des verwendeten Codes für Trainig der Abwehr
- Wirksamkeit vs. Aufwand
  - Löschen von Daten: Daten werden durch Angreifer sofort kopiert
  - Reconnaissance: Invasive Abwehrmaßnahmen erfordern umfangreiches Wissen über Ziel
  - "Hydra"-Problem: Resiliente Steuerungsstrukturen beim Angreifer erfordern Hack-Backs gegen viele Systeme

Schwierigkeiten und Herausforderungen (II)

- Aufbau und Modernisierung von "Hack-Back-Arsenalen"
  - Breite Palette an Cyber-Tools nötig für alle möglichen Gefahrenszenarios
  - Umfangreiche und "breite" Intelligence nötig über potentielle Ziele
  - Aktualisierung und Eigensicherung der Cyber-Arsenale (Umgang mit Sicherheitslücken)
- Zuständigkeiten, Befugnisse und Rechtliche Grenzen
  - WD-Gutachten: Verweis auf das Verbot friedensstörender Handlungen nach Art. 26 Abs. 1 GG
  - Nachrichtendienste primär mit Aufklärungs- aber nicht Eingriffsbefugnissen
  - Offensive Hack-Hack-Fähigkeiten sind gleichzeitig Angriffswerkzeuge
- Außen- und Sicherheitspolitische Signalwirkung und Umgang
  - Regeln für Cyber-Diplomatie
  - Diplomatische Ankündigung von Hack-Backs unterminiert deren Wirksamkeit

Alternativen zu Hack-Backs

- Gute Verschlüsselung gegen "Datenabfluss"
- Starke und kontinuierliche IT-Sicherheit
- Hersteller-Haftung bei Software und Hardware zur Verbesserung der Produktpflege
- Politische Sanktionen
- Politische Ächtung von Cyber-Attacken
- Defensive Maßnahmen bevorzugen
  - Sperren von IP-Bereichen
  - Umlenken von DDoS-Strömen

Fazit

- Investition in Verteidigung
- IT-Sicherheit ist das "shaping of the battlefield"
- Hohe Risiken & Kosten bei ungewissen Ergebnissen
- Effektives Management des fachlichen Know-Hows
- Fokus auf Unsicherheit von IT anstelle von IT-Sicherheit

Thomas Reinhold
cyber-peace.org
reinhold@ifsh.de