Aktuelle Entwicklungen in den Cyberspace-Debatten: ein Überblick

Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg

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

Länderupdates

- Deutschland
  - Bundeswehr: "Kommando Cyber & Informationsraum" (CIR) (Aufbau bis 2021 abgeschlossen, bis zu 21.000 Dienstposten)
  - BMVg: Neue Abbteilung Cyber/ IT (CIT)
  - Bundeswehr Universität München: Neues Cyberforschungszentrum, elf neue W3 IT-Professuren mit ~260 Mitarbeitern und internationaler Master-Studiengang "Cybersicherheit"

  - BMI: Nationalen Cyber-Abwehrzentrum als zentrale Schnittstelle der zivilen, geheimdienstlichen und militärischen Institutionen, Erstellung eines einheitlichen „Cyber-Lagebildes“, Krisen-Koordinationsstelle
  - BMI: ZITiS - Zentrale Stelle für Informationstechnik im Sicherheitsbereich mit u.a. Bundeswehr als Kunde, "Zwischenhändler" für Sicherheitslücken ?
  - Inoffizieller erster Einsatz der CNO-Einheit der Bundeswehr in Afghanistan

Länderupdates /II

- USA
  - Fortsetzung des "Cyberkampfes", nun gegen jegliche terroristische Aktivitäten
  - *"work with international partners to* (..) *engage in cyberwarfare to disrupt and disable propaganda and recruiting*"
  - US Cybercommand wird eigenständige Militäreinrichtung (Unified Combatant Command) und unabhängig(er) von der NSA mit zusätzlicher Finanzierung

- Russland
  - Erstmal explizit Einrichtung einer "Abteilung für Informationssicherheit und Cyberabwehr" "zur Verteidigung der Interessen des Militärs", ~1000 Mitarbeiter
  - Russische Militärkräfte lt. Verteidigungsminister auch an intelligenter und effektiver Propaganda beteiligt ("information troops")

Länderupdates /III

- China
  - Weiterhin primär Verhandlungen zur Eingrenzung von Cyberspionage und sicheren Lieferketten
- Nordkorea
  - UNIT 180, möglicherweise verantwortlich für SONY Hack 2014, Mutmaßungen bzgl. WannaCry und Hacking gegen Zentrabank von Bangladesh

Länderupdates /IV

- EU
  - "EU CYBRID 2017" Planspiel für bessere Koordinierung der Cyberabwehr
- NATO
  - Zukünftig weitere Cyber-Übungen und verstärktes "capacity building"
  - Kooperation bei der Cyberabwehr mit der Ukraine

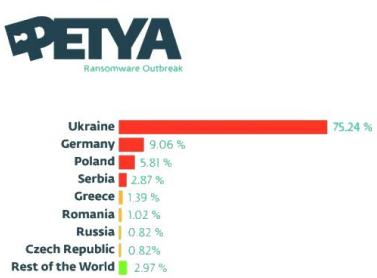
Vorfälle

- WannaCry
  - Mai 2017, scheinbare Ransomware
  - 200.000 Systeme in 150 Ländern
  - Zero-Day-Exploit in Windows-Netzwerken
  - Exploit aus Leaks von NSA-Beständen (EternalBlue)
  - "Killswitch" eingebaut

Vorfälle

- WannaCry
  - Mai 2017, scheinbare Ransomware
  - 200.000 Systeme in 150 Ländern
  - Zero-Day-Exploit in Windows-Netzwerken
  - Exploit aus Leaks von NSA-Beständen (EternalBlue)
  - "Killswitch" eingebaut

- NotPetya
  - Juni 2017, scheinbare Ransomware gegen politische Einrichtungen und Industrie in der Ukraine, Europa, Russland und USA
  - Auch EternalBlue-Exploit und explizit zerstörerischer Payload
  - Enormer wirtschaftlicher Schaden durch IT-Ausfälle



Vorfälle /II

- Cyberattacken auf Kraftwerke
  - Ukraine: SCADA-Malware *"auf Stuxnet-Niveau"* entdeckt
  - USA: DHS-Bericht zu mutmaßlich staatlichen Cyberattacken gegen Energieversorger und AKWs (aber primär Social Engineering)
  - Yukiya Amano (IAEA) berichtet über mehrere kritische Cyberattacken

- Cyberattacken der USA gegen Nordkorea
  - NY Times: seit 2014 "left of launch"-Programm um nordkoreanische Raketenprogramm zu stören: *"the attacks begin before the missiles ever reach the launchpad, or just as they lift off"*
  - Programm auch unter Trump-Administration mutmaßlich weitergeführt

Trends/Entwicklungen

- Debatten
  - BMI: Hack-Back als valide Verteidigungsstrategie
  - Handel, Wert und Aufkauf von Sicherheitslücken durch staatliche Stellen
  - Vorschläge für eine digitale "Genfer Konvention" durch Microsoft und Google
- Politik
  - Misserfolg der aktuellen UN GGE, kein gemeinsamer Bericht/Erklärung aber weitere Schritte im 1. Ausschuss der UN Generalversammlung (Oktober)
  - Veröffentlichung des CCDCOE "Tallinn Manuals 2.0"
    "how (..) existing international [human rights] laws, treaties and norms regulate state activities in cyberspace"
- Technik
  - Proliferation von Exploits (bspw. EternalBlue)
  - DDoS-Attacken als Cyberwaffen

Institut für Friedensforschung und Sicherheitspolitik
Interdisziplinäre Forschungsgruppe
Abrüstung, Rüstungskontrolle und
Risikotechnologien

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