Geschichte der Computersicherheit: vom Phone-Freaking zum Cyberwar

Seit es elektronische Systeme gibt, gibt es Versuche, diese – zu welchem Zweck auch immer – anzugreifen

- Bereits 1903, als Guglielmo Marconi eine öffentliche Funkverbindung mit London demonstrierte, wurden Signale von Nevil Maskelyne abgefangen und „unberechtigte" Nachrichten an das Empfangsgerät gesendet
- Seit den 1930er Jahren und während des zweiten Weltkriegs (am Ende sogar industriemäßig organisiert und erfolgreiche) Versuche, die Enigma-Verschlüsselung zu brechen
- In den 1970ern – Aufkommen der Phreaking-Bewegung (Phreaking zusammengesetzt aus **Ph**one F**reaking**)
- …

Phone Freaking

Telefon-Hacker (Phreakers) in den 1960er und 70er Jahren:

- Suche nach Schwachstellen in Telefonsystemen, um möglichst kostenlos zu telefonieren
- Verquaste ideologische Rechtfertigung: „Freiheit der Kommunikation ist Voraussetzung für Freiheit der Menschheit"
- Szene organisiert sich vermittels von „Underground" Zeitschriften, z.B. YIPL (Youth International Party Line), später bekannt als TAP (Technological American Party) – die erste „Hacker-Zeitschrift"
- **Beispiel: Blueboxing**
  - Verbindungen ließen sich durch internen Steuerton von 2.600 Hz vorgeblich beenden, Leitung zur Vermittlungsstelle blieb aber offen
  - Phreaker konnte neues (teures Fern-)Gespräch zum ursprünglichen (billigen Orts-)Tarif führen
  - Bluebox: Gerät zur Erzeugung verschiedener Steuertöne

Erste Generation von Computer-Hackern (1/2)

Mit Verbreitung der PCs etabliert sich Hacking-Szene im Untergrund:

- Einbrüche in Computersysteme, z.B.:
  - Kevin Mitnick wurde 1982 wegen Einbruch in Telefongesellschaft PacBell und Diebstahl von Dokumenten verurteilt
- 1981 wurde einer der größten Hacker-Verbände, der **CCC** – **Chaos Computer Club** – in Berlin gegründet
  - ursprünglich aus Deutschland, mittlerweile international
  - seit 1984 organisiert CCC jährlich in der Weihnachtspause einen intern. Chaos Communication Congress (C3)
  - Hamburg 2015: 32C3 mit dem Motto „Gated Communities"

Erste Generation von Computer-Hackern (2/2)

Spektakuläre Aktionen offenbarten Software-Fehler und verschiedene Sicherheitslücken, so z.B.

- **1984**: Missbrauch des neu eingeführten BTX-Diensts der Hamburger Sparkasse. Überweisung von 134.000 DM an CCC
- **1996**: CCC demonstriert Angriff gegen Microsoft ActiveX
- **1998**: CCC brach den damals von vielen GSM-SIM-Karten verwendeten COMP128 Verschlüsselungsalgorithmus
- **2008**: CCC veröffentlicht Fingerabdrücke von Bundesinnenminister Wolfgang Schäuble, um gegen Nutzung von biometrischen Daten in deutsche IDs (E-Pass) zu protestieren
- **2011**: CCC veröffentlicht die Analyse des (handwerklich schlecht gemachten) Bundestrojaners
- ...

Hacking in den 1990er Jahren

- Rasante Verbreitung von Computersystemen führt zu ebenso rasanter Entwicklung des Hacking
- Staatliche Rechtssysteme fangen an, sich zu kümmern und rechtliche Vorschriften zu erlassen, z.B.:
  - Computer Misuse Act, Großbritannien, 1990
- Angriffe auf Computersysteme werden zunehmend automatisiert ausgeführt
- Automatisierte Würmer, Scanner oder andere Angriffs-Tools verursachen riesige Flut von Sicherheitsvorfällen
- Menge der Log-Nachrichten in IT-Systemen wächst rapide
- Erste **IDS** (**Intrusion Detection Systeme**) und Überwachungssysteme werden entwickelt

Cybercrime in den 2000er Jahren

Fast jedes Computersystem wird mit dem offenen Internet verbunden. In der Folge steigt Anzahl der Sicherheitsvorfälle dramatisch an:

- Viren, Würmer, Trojaner, …
- Botnets
- Industriespionage
- Kein großes Unternehmen kommt mehr ohne IT-Sicherheitsabteilung aus
- Hacking-Software über das Internet für jedermann verfügbar → Script Kiddies
- Underground Netzwerke wie Tor, I2P und Freenet erscheinen

Heute: Cyberwar

Sicherheitsdienste der meisten Länder bauen sowohl für den Innen- als auch den Außenbereich Cyber-Verteidigungsabteilungen auf, z.B.

- Deutschland: Nationales Cyber-Abwehrzentrum
- NATO: Cooperative Cyber Defence Centre of Excellence
- USA: United States Cyber Command
- China: PLA Unit 61398

Auch offensiv werden kriegerische Akten in der virtuellen Welt begangen, z.B. **2007 in Estland:**

- Internetdienste (E-Government, Banken) wurden mittels DDoS-Attacken angegriffen – mit spürbaren Auswirkungen auf Wirtschaft und Gesellschaft
- Estlands Regierung beschuldigte Russland der Angriffe wegen eines Konflikts der beiden Länder über ein Kriegsdenkmal

Heute: Cyberwar

Sicherheitsdienste der meisten Länder bauen sowohl für den Innen- als auch den Außenbereich Cyber-Verteidigungsabteilungen auf, z.B.

- Deutschland: Nationales Cyber-Abwehrzentrum
- NATO: Cooperative Cyber Defence Centre of Excellence
- USA: United States Cyber Command
- China: PLA Unit 61398

Auch offensiv werden kriegerische Akten in der virtuellen Welt begangen, z.B. **2007 in Estland:**

- Internetdienste (E-Government, Banken) wurden mittels DDoS-Attacken angegriffen – mit spürbaren Auswirkungen auf Wirtschaft und Gesellschaft
- Estlands Regierung beschuldigte Russland der Angriffe wegen eines Konflikts der beiden Länder über ein Kriegsdenkmal