openHPI – Sicherheit im Internet
Angreifer und ihre Motive

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Potenzielle Angreifer

Kenntnis des Profils möglicher Straftäter im Internet und ihrer Motive hilft, Internet-basierte Computersysteme abzusichern

Es gibt verschiedene Gruppen von Cyberkriminellen mit ganz unterschiedlichen Motivationslagen, z.B.

- Insider – Mitarbeiter der eigenen Unternehmung
- „Script Kiddies"
- Underground Hacker / Cracker
- Computerspezialisten
- Gewöhnliche Kriminelle, z.B. Erpresser, Drogenmafia, …
- Terroristen
- Industriespione und Geheimdienstspione

Insider

Mitarbeiter im eigenen Unternehmen

Ein großer Teil des Missbrauchs von Computersystemen wird nachweislich von Mitarbeitern des eigenen Unternehmens verursacht

Motive: Neben Inkompetenz und Fahrlässigkeit auch Gefühl der schlechten Behandlung, Frustration, Unfug, Rache, ...

- Internet-Angriffe möglich auch innerhalb von Intranets
- Naivität oder Unachtsamkeit → „Social Hacking"
- Neue Gefahrenpotentiale durch Integration von Home-Offices und mobilen Geräten in das Unternehmensnetz
  → „bring your own device (BYOD)"
- Nichteinhaltung interner Sicherheitsanweisungen führt zur Mitschuld

„Script Kiddies"

Angreifer ohne tiefergehende Kenntnisse

Größte Zahl von Einbruchsversuchen (meist erfolglos) werden durch Anwendung von Hacker-Tools („Scripts) von weniger beschlagenen Angreifern (ohne eigenes Know-How) durchgeführt

Motive:

- Kombination aus Neugier, Spieltrieb, Selbstbehauptung ...
- In der Mehrzahl der Fälle ziellos und ohne direkte kriminelle Absicht
- Angreifer dieser Kategorie sind meist jüngeren Alters (Schüler, Studenten) – daher der Begriff „Kiddies"
- Viele Hacker-Tools sind zum Download im Internet verfügbar, oft aber ohne gewisse Grundkenntnisse nicht effektiv einsetzbar
- Besonders gefährlich: **Denial-of-Service-Attacken** (**DoS**)

Hacker

Nichtkommerziell orientierte Elite der Hacker-Community:

- Ursprung in „Phone Freak"–Bewegung der späten 60er in USA
- In Deutschland am bekanntesten:
  CCC – **Chaos Computer Club** in Hamburg
- Organisation über Bulletin Boards (Foren), Hacker-Zeitschriften, Konventionen, …
- Meist verdeckte Insider-Kommunikation:
  - Austausch über Schwachstellen und Sicherheitslücken in wichtigen IT-Systemen, insbesondere in IT-Sicherheitssystemen
  - Entwicklung und Austausch von Exploits
  - Aufdeckung von Lücken im Datenschutz und in Mechanismen zum Schutz sensibler Informationen

Profi-Hacker und Computer-Kriminelle

Kommerzialisierung des Internet und sich entwickelnder Markt für Auftragsangriffe und Datendiebstähle/–Manipulationen, sowie Erpressung, Kreditkartenmissbrauch, Online-Bankraub, … lockt Kriminelle aller Couleur

- Professionelle Datendiebe aus der Hacker-Szene, ehemalige Geheimdienst-Mitarbeiter, Computer-Spezialisten, ...
- Ausführen spezifischer Aufgaben, z.B.
  - Industriespionage, Geheimdienstspionage, …
  - Einbrüche in hochsichere IT-Systeme
  - DDoS-Angriffe, gezielte Angriffe auf Netzwerke
  - Entwicklung von Viren und Würmer
- Schwarzmarkt für Auftragskriminalität und gestohlene Daten:
  - Infos über bisher unbekannte Schwachstellen werden für mehrere zehntausend Euro gehandelt
  - Exploit- und Viren-Märkte im „Darknet"

Gewöhnliche Kriminelle

Traditionelle kriminelle Szene, insbesondere organisierte Kriminalität (z.B. Drogenmafia) hat Potentiale und globalen Marktplatz des Internets erkannt

- Nutzen Internet für alle Arten von Computer-Kriminalität, insbesondere für Angriffe gegen Finanz- und Einkaufssysteme, Missbrauch von geleakten Identitätsdaten, …
- Anders als im realen Leben sind Behörden oft nur (noch) unzureichend gerüstet, Kriminelle im Internet zu verfolgen. In der Folge verlegen Kriminelle ihre Kommunikation und kriminellen Aktivitäten auf das Internet
- Wunsch von staatlichen Sicherheitsbehörden, wie BND, CIA, NSA, etc., nach "Hintertüren" für kryptographisch geschützte Systeme

Terroristen

Enorme Zunahme der Nutzung des Internets durch Terroristen bzw. zu terroristischen Zwecken:

- Propaganda verbreiten
- Geldquellen erschließen, Leute rekrutieren, Netzwerke pflegen, …
- Kommunikation und Koordination von Anschlägen und terroristischen Aktionen
- Beispiele für Nutzung des Internets:
  - Verbreitung von Propaganda-Videos, Webseiten, z.B. YouTube Videos von Enthauptungen von Geiseln durch IS
  - Bauanleitungen für Bomben
  - Straßen- und Gebäudepläne für Anschlagsplanung
  - …

Industrie- und Geheimdienstspione

Internet bietet umfassende Möglichkeit für Industrie- und Geheimdienstspionage

- Diebstahl geheimer Informationen von Konkurrenten oder aus anderen Ländern
  - PRISM-Spähprogramm von USA
  - XKeyscore-Spähprogramm in Deutschland
- Politisch oder wirtschaftlich motivierte Angriffe auf Dienste und IT-Systeme

Beispiel: Stuxnet

- Malware, die Windows-Netzwerke sowie proprietäre programmierbare Systeme von Industrieanlagen angreift
- **Ziel**: Zerstörung iranischer Urananreicherungsanlagen
- Nutzt mehrere (!) Zero-Day Schwachstellen

Industrie- und Geheimdienstspione

Internet bietet umfassende Möglichkeit für Industrie- und Geheimdienstspionage

- Diebstahl geheimer Informationen von Konkurrenten oder aus anderen Ländern
  - PRISM-Spähprogramm von USA
  - XKeyscore-Spähprogramm in Deutschland
- Politisch oder wirtschaftlich motivierte Angriffe auf Dienste und IT-Systeme

Beispiel: Stuxnet

- Malware, die Windows-Netzwerke sowie proprietäre programmierbare Systeme von Industrieanlagen angreift
- **Ziel**: Zerstörung iranischer Urananreicherungsanlagen
- Nutzt mehrere (!) Zero-Day Schwachstellen

Angreifer und ihre Motive | Sicherheit im Internet | Prof. Dr. Christoph Meinel 9