



openHPI – Sicherheit im Internet Exkurs: Advanced Persistent Threat

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

APT – Advanced Persistent Threat

APT – Advanced Persistent Threat (dt. fortgeschrittene, andauernde Bedrohung) ist ein gezielter Angriff, z.B. auf Regierungen, Militär, Industrie, Behörden oder Aktivisten

- Getarnte und extrem ausgeklügelte Angriffsmethoden
 - Ausnutzung noch unbekannter Schwachstellen („0-Days“)
 - Verwendung von Hintertüren in Software
 - Starke Einbeziehung von Methoden des Social Engineering, z.B. → Spear Phishing
- Meist über einen längeren Zeitraum andauernd
 - Sicherung eines bleibenden Zugangs zum Zielsystem
 - Langsames und schrittweises Vorgehen, um Aufdeckung zu Verhindern

ÁPTs in der Regel motiviert durch:

- Großflächiges Ausspähen sensibler Informationen, z.B. Wirtschafts- und Industriespionage, politische Spionage, ...
- Beeinträchtigung oder Zerstörung von kritischen Infrastrukturen (Öl, Gas, Strom, Telekommunikation, ...)

Angreiferprofil:

- Verfügt über extrem umfangreiche Ressourcen
- Nahezu unerschöpfliche finanzielle Mittel
- Große Anzahl professioneller Hacker
 - also z.B. Regierungen, große Unternehmen, Militär, ...

→ APT gehen über bisher besprochene Angriffe weit hinaus

APT sind hochspezialisierte Angriffe

Hauptanliegen:

- Angriff darf möglichst **nicht entdeckt** werden
- Verwendung von allgemein noch **unbekannten** bzw. sehr **selten eingesetzten Angriffswerkzeugen**
- Teilweise werden auch **Werkzeuge neu entwickelt**, um einer Entdeckung zu entgehen
- Einschleusen von Schadcode beim Opfer über **spezialisierte Social Engineering-Angriffe**
 - Opfer werden dazu vorher monatelang ausgekundschaftet

Eingesetzte Schadsoftware nutzt **bisher unbekannte Sicherheitslücken** aus

- Einkauf von Exploits (**0-days**) auf dem **Hacker-Schwarzmarkt** mit Garantie, dass bisher niemand diese Sicherheitslücke bzw. den Exploit kennt
- APT-Angriffe sind nahezu unmöglich zu entdecken
 - Allgemein zugängliche Schutzsoftware, wie z.B. Anti-Virussoftware und Firewalls kennen Muster der APTs noch nicht und sind daher wirkungslos
 - Ausgenutzte Sicherheitslücken sind allgemein unbekannt
 - ...

Exkurs: Advanced Persistent Threat | Sicherheit im Internet | Prof. Dr. Christoph Meinel 5

Stuxnet ist eine **Schadsoftware**, die 2010 auf den Computern von iranischen Anlagen zur Urananreicherung entdeckt wurde

- Ausnutzung zahlreicher damals noch **unbekannter Sicherheitslücken**
 - allein 4 Sicherheitslücken im Windows-Betriebssystem
 - weitere Lücken in Steuerungssoftware (SCADA) für Uranzentrifugen
 - zu dieser Zeit waren Angriffe auf Steuerungsanlagen nur eine Fiktion, die in einigen Forschungspapieren behandelt wurde
- Einschleusung durch Social Engineering
 - Übergabe eines USB-Sticks mit verstecktem Stuxnet

Exkurs: Advanced Persistent Threat | Sicherheit im Internet | Prof. Dr. Christoph Meinel 6

Vermutliches Ziel des Angriffs:

- Störung des Atomprogramms / der Urananreicherung im Iran
- Erste Variante des Wurms tauchte Juni 2009 auf
 - wurde zu dieser Zeit jedoch noch nicht als Stuxnet erkannt
 - lief bis Juli 2010 ohne Entdeckung

Angreifer hatte extrem viele Ressourcen

- Frühe Vermutung: Hinter dem Angriff müssen **staatliche Infrastrukturen** stecken
- Nach Berichten von Edward Snowden stehen hinter dem Angriff wohl die USA und Israel

Exkurs: Advanced Persistent Threat | Sicherheit im Internet | Prof. Dr. Christoph Meinel 7

APT1 ist der Name einer **Spionageabteilung**, die APT-Angriffe auf mindestens 141 internationale Unternehmen durchgeführt hat

- Jahrelang wurden geheime Dokumente und Daten abgezogen
- Aufgedeckt im Februar 2013 durch Sicherheitsunternehmen Mandiant
- Anzeichen deuten darauf hin, dass der Angriff bereits seit 2006 gefahren wurde

Angreifer hatte extrem viele Ressourcen zu Verfügung

- Wieder Vermutung: Hinter den Angriffen steckt ein Staat
- Wahrscheinlich ging Angriff von China aus: Spezielle Spionageabteilung 61398 der People's Liberation Army

Exkurs: Advanced Persistent Threat | Sicherheit im Internet | Prof. Dr. Christoph Meinel 8