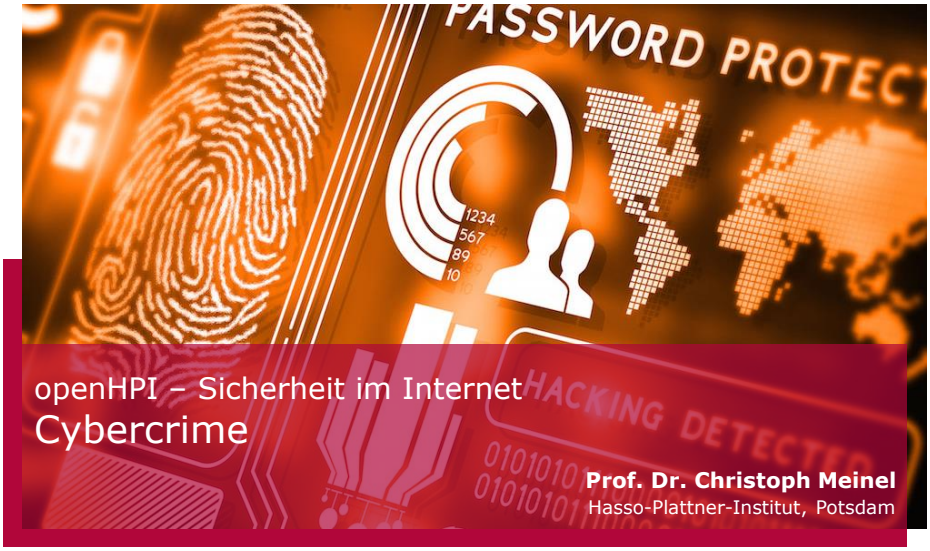

Schadensbetrachtungen im Internet

Schaden, der durch Cybercrime verursacht wird, kann nur sehr schwer exakt beziffert werden

- sehr hohe Anzahl von oft unentdeckten Sicherheitsvorfällen im Internet
- Verschiedenartigkeit der Angriffe

Das gleiche gilt in Bezug auf die **Anzahl der gefährdeten Systeme** und die **Missbrauchsanfälligkeit von Anwendungen** im Internet

- Einige Sicherheitslücken und Schwachstellen sind nur einer kleinen Zahl von Hackern oder Geheimdienstlern bekannt (Zero-Day / Zero-Day Exploit) und können nur von diesen missbraucht werden

Schwachstellen und Exploits

Schwachstelle eines Softwaresystems:

- "fehlende oder unzureichend umgesetzte Sicherheitsmaßnahme" (BSI-Standard 100-2)
- Software-Fehler, der eine Sicherheitslücke / Angriffsfläche auf IT-Systemen öffnet

Exploit:

- Software, die Schwachstelle (Sicherheitslücke) ausnutzt, um Zugriff auf das Zielsystem oder dort höhere Berechtigungen zu erlangen
- Exploit enthält **Schadcode**, der nach der Ausnutzung der Schwachstelle auf dem Zielsystem den vom Angreifer erwünschten Effekt bewirkt

Schwachstellen und Exploits: Beispiele (1/3)

Beispiel aus dem nicht-digitalen Leben:

- Sicherheitspersonal im Gefängnis überprüft Pakete nicht, wenn Sie weniger als 500g wiegen – die fehlende Überprüfung ist eine **Schwachstelle**
- Ein Freund eines Insassen schickt ein Paket mit einem Kuchen, in dem ein Mobiltelefon versteckt ist
  ➔ Paket mit präpariertem Kuchen unter 500g ist ein **Exploit**
- Der Exploit (Paket unter 500 Gramm) enthält also den Schadcode (Kuchen mit Mobiltelefon). Wenn das Sicherheitspersonal den Kuchen an den Insassen weitergibt (den **"Schadcode ausführt"**), bekommt der Insasse das Mobiltelefon
- Das Gefängnis (**Zielsystem**) wurde durch Einschmuggeln eines illegalen Telefons manipuliert, ein **Sicherheitsvorfall** ist erfolgt

Schwachstellen und Exploits: Beispiele (2/3)

Beispiel: CVE-2010-2553

- Software-Fehler in dem Media-Codec in Windows XP, Vista und 7 erlaubt Angreifer Remote Code Execution (**Schwachstelle**)
- Angreifer bereitet eine Media-Datei (z.B., ein Video) vor und schickt diese Datei oder Link auf Web-Seite mit diesem Video an Benutzer ➔ vorbereitete Video-Datei ist ein **Exploit**
- Da der Media-Codec einen Software-Fehler enthält, wird während der Video-Decodierung der vom Angreifer eingeschmuggelte Code ausgeführt, z.B. Code, der Daten des Opfers löscht ➔ Code für Löschung der Daten ist **Schadcode**

CVE steht für "Common Vulnerabilities and Exposure" und ist eine Datenbank mit bekannten Schwachstellen

Schwachstellen und Exploits: Beispiele (3/3)

Technisches Beispiel:

- Web-Service bietet Kontakt-Formular an. Der vom Nutzer eingegebene Text wird **ungeprüft** in einer SQL Datenbank abgespeichert (Schwachstelle)
- Programmiertechnisch realisiert mit SQL Kommando:
  - `INSERT INTO TABLE Kontaktanfrage VALUES (TEXT)`
- Angreifer kann nun einen Exploit – **SQL Injection Exploit –** schreiben, um Daten aus der Datenbank auszulesen oder gar zu löschen:
  - in Formular eingeschmuggelter Text: `a);DROP TABLE users;` ➔ Exploit. Schadcode: `DROP TABLE users;`
  - Ausgeführtes SQL Kommando: `INSERT INTO TABLE Kontaktanfrage VALUES (a);DROP TABLE users;`

Exploit-Typen

Exploits können auf Basis des ausgenutzten Schwachstellen-Typs klassifiziert werden

Häufigste Schwachstellen-Typen:

- Buffer Overflow
- SQL Injection
- Code Injection
- Cross-Site Scripting

Zero-Day Exploit ist Exploit, für den es (noch) keine entsprechenden Patches/Updates gibt. Mit Zero-Day sind oft auch Exploits gemeint, die auf für den Hersteller unbekannte Schwachstellen basieren

  - Entwickler hatten also noch keine Zeit (null Tage / **zero days**), die Sicherheitslücke zu beheben

Angriffe auf ein IT-System (1/2)

Angriff ist ein Prozess, bei dem durch Ausführung eines **Exploits**, also durch Ausnutzung einer Schwachstelle, versucht wird, Zugriff auf ein Zielsystem zu erlangen mit dem Ziel,

- die ordnungsgemäße Funktion zu stören oder das System zum Absturz zu bringen oder
- im System gespeicherte Daten einzusehen, zu manipulieren oder gar zu löschen

Angriffe auf ein IT-System (2/2)

Angreifer kann auch vorformulierte Exploits nutzen, anstatt sie selbst zu entwickeln:

- **Metasploit** ist eine Software für "Penetration Testing", die Hunderte von Exploits für verschiedene Plattformen, Betriebssysteme und Softwaresysteme zur Verfügung stellt
- http://www.exploit-db.com
  - sammelt Exploits aller Art
  - stellt mehr als 30 000 Exploits zur Verfügung

Sicherheitsvorfall

Sicherheitsvorfall – Security Incident

- erfolgreicher Angriff auf ein IT-System

Reaktion in großen Unternehmen: „Security Incident Response Team" folgt einfach einem vorab entwickelten Reaktionsplan

- Log-Nachrichten für eine spätere Analyse speichern
- die betroffenen Systeme / Dateien ermitteln
- betroffene Systeme aus der Operation nehmen und durch Backupsysteme ersetzen
- andere Systeme überprüfen
- betroffene Systeme wiederherstellen und updaten
- Daten- und andere Verluste analysieren
- Problem melden

Sicherheitsvorfall

Sicherheitsvorfall – **Security Incident**

- erfolgreicher Angriff auf ein IT-System

Reaktion in großen Unternehmen: „Security Incident Response Team" folgt einfach einem vorab entwickelten Reaktionsplan

- Log-Nachrichten für eine spätere Analyse speichern
- die betroffenen Systeme / Dateien ermitteln
- betroffene Systeme aus der Operation nehmen und durch Backupsysteme ersetzen
- andere Systeme überprüfen
- betroffene Systeme wiederherstellen und updaten
- Daten- und andere Verluste analysieren
- Problem melden