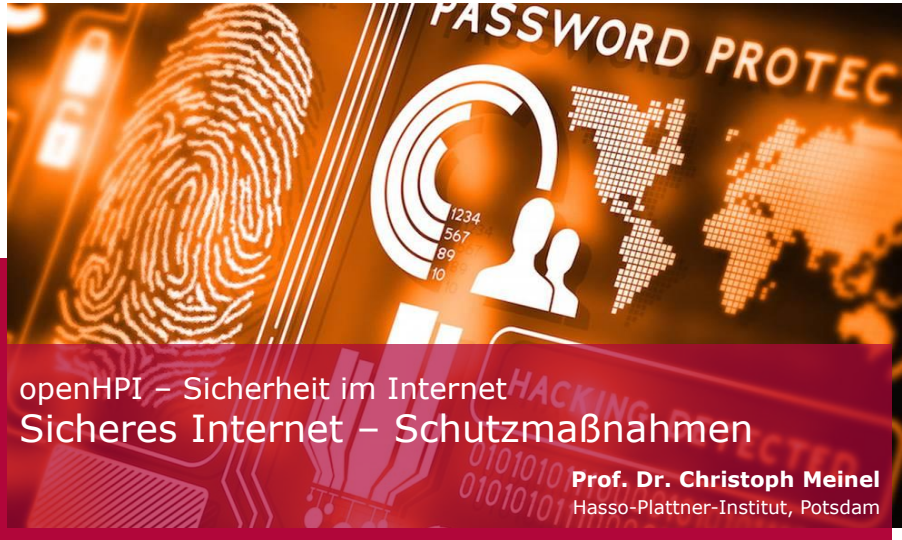




openHPI – Sicherheit im Internet Sicheres Internet – Schutzmaßnahmen

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

Sicheres Internet – Schutzmaßnahmen

Die aktuelle Kurswoche hat gezeigt, welche unterschiedlichen Gefahren auf den **offenen Transportwegen** im Internet lauern

- Zur Erinnerung:
 - Ausspähen von Daten
 - Manipulation von Daten
 - Störung von Diensten
 - Übernahme der Kontrolle fremder Computersysteme
 - ...
- **Gute Nachricht:** viele dieser Gefahren können durch wenige Schutzmaßnahmen gemindert oder sogar ganz gebannt werden

Das Fehlen von Authentifikationsmechanismen ist grundlegender Designfehler der Internetprotokolle

- Mit **verlässlicher Authentifikation** kann sichergestellt werden, dass nur vertrauenswürdige Nutzer Zugang zu den verschiedenen Ressourcen (Daten, Services, Speicher, Rechenpower, ...) erlangen

Daher: **Starke Authentifikation ist wichtige Schutzmaßnahme**

- Einsatz starker Authentifikationsverfahren in sämtlichen Protokollschichten, von der Internet- bis zur Anwendungsschicht, ermöglicht **sichere Feststellung der Identität** eines Nutzers bzw. des **Ursprungs einer Anfrage**
 - Durch Mehrfaktor-Authentifikation
 - Durch digitale Zertifikate
 - ...

Absicherung auf der **Internetschicht**

- **IPsec** sichert Internet Protocol IP durch sichere Authentifikation und Verschlüsselung ab
- Neues IP-Protokoll IPv6 unterstützt Authentifizierung bereits von vornherein

Absicherung auf der **Transportschicht**

- Verwendung von TLS/SSL zur Authentifikation mittels digitaler Zertifikate, z.B. auch implizit bei HTTPS

Absicherung auf der **Anwendungsebene**

- Verwendung von **Ende-zu-Ende Authentifikation** vermittels digitaler Zertifikate, z.B. in Emails über **PGP** oder **SMIME**
- Verwendung von **Mehrfaktor-Authentifikation**, z.B. über Einmalpasswörter, Smart-Tokens oder biometrische Faktoren

Verschlüsselung hält Daten und Nachrichten gegenüber Dritten geheim, indem sie unlesbar gemacht werden

- Deshalb: **Sensible Daten verschlüsseln**, sobald sie über ein offenes Netzwerk wie das Internet übertragen werden sollen
- **Empfehlung: Einsatz hybrider Verschlüsselung** (→ Kurswoche 5)
 - Schlüsselaustausch über 2-Schlüssel-Verschlüsselung
 - Datenaustausch über 1-Schlüssel-Verschlüsselung
- Bereits besprochene **Authentifikationsprotokolle** auf den verschiedenen Protokollschichten nutzen bzw. basieren auf Verschlüsselungstechnologie
 - z.B. IPsec, TLS/SSL, PGP/MIME, ...

In bestimmtem Umfang können bösartige Netzwerkverbindungen durch Schutzsoftware wie z.B. Firewalls unterbunden werden

Firewalls

- Erlauben nur Verbindungen zu Diensten, die von außen zugreifbar sein sollen
- Erlauben keine ausgehenden Verbindungen ohne explizite Erlaubnis
 - kann z.B. Botnet-Software lahmlegen, weil diese nicht mit Command & Control-Server kommuniziert kann

Keine unnötigen Dienste

- Firewalls blockieren Zugriffe auf Dienste von nicht-vertrauenswürdigen Netzen
- Noch besser: nur Dienste installieren, die auch wirklich benötigt werden

Regelmäßige Updates (1/2)

Allermeisten Angriffe im Internet nutzen **(bekannte)**

Schwachstellen in Software aus

- Sobald Softwarehersteller Fehler und Schwachstellen in ihrer Software entdecken, entwickeln sie sogenannte **Patches** oder **Updates**
- Nach Installation dieser Updates sind die Fehler beseitigt und die Schwachstellen geschlossen
- Daher wichtige Schutzmaßnahme:
 - Regelmäßig nach aktuellen Updates Ausschau halten und diese zeitnah installieren

Regelmäßige Updates (2/2)

HPI bietet kostenlosen Service – **HPI-VDB** –, der hilft, über eine Webabfrage Schwachstellen (engl. Vulnerabilities) in Softwareprogrammen auf dem eigenen System zu finden

- Webadresse: <https://hpi-vdb.de>



- Button „Selbstdiagnose“ drücken und Dienst zeigt Schwachstellen für den installierten Browser an

Allerdings kann man mit Updates und Firewalls allein nicht allen Bedrohungen aus dem Internet begegnen

Deshalb Empfehlung:

- Öffnen von Webseiten und Internetdiensten in einer speziellen Schutzumgebung – **Sandbox** (dt. **Sandkasten**) und Ausführung mit möglichst niedriger Berechtigung
- Browser öffnen heute schon häufig jede Seite in eigener Sandbox. Böartiger Webdienst erhält damit nur Zugriff auf die stark limitierte Ausführungsumgebung der Sandbox
- Auch einige **Anti-Viren-Programme** machen es möglich, **alle Anwendungen in einer Sandbox** auszuführen
- Genereller Trend: **Verabschiedung von Administratorkonten**, mit dem alles gemacht werden kann, Einrichtung von eingeschränkten Nutzerkonten

Angewohnheit und Problem vieler Dienstbetreiber:

Speicherung zu vieler Daten

- Grund für Speicherung sämtlicher Daten, deren man habhaft werden kann: „vielleicht kann man später mit den Daten noch etwas anfangen“
- **Sicherheitsrisiko:** bei einem Sicherheitsvorfall fallen alle gesammelten Daten in die Hände der Datendiebe

Deshalb müssen Nutzer und Dienstbetreiber **Prinzip der Datensparsamkeit** walten lassen

- Angabe und Speicherung nur der Daten, die wirklich zur Bereitstellung eines Dienstes nötig sind