Angriffe auf Datennetze

Im Arbeitsblatt 03 hast du Beispiele für Sicherheitslücken in Lokalen Netzen im Zusammenhang mit dem *Internet der Dinge* (IoT) kennengelernt:

- **Gekaperte Geräte**, mit denen beispielsweise **Botnetze** aufgebaut werden. Diese können z. B. für **DDoS-Angriffe** genutzt werden („Distributed Denial of Service“; dt. „Verbreitete Verweigerung des Dienstes“). Möglich ist das durch Port-Forwarding: Für Geräte, die von außen erreichbar sein müssen, werden am Router Port-Weiterleitungen eingerichtet. Dabei leitet der Router Datenpakete, die über einen bestimmten Port eintreffen, an ein zuvor festgelegtes Gerät im Lokalen Netz weiter.

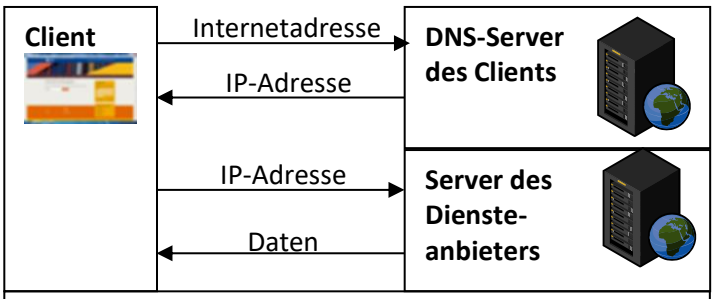
  Bei einem DDoS-Angriff werden Datennetze durch Überlastung lahmgelegt. Die arglosen Nutzer, deren Geräte für das Botnetz missbraucht werden, ahnen nichts davon, dass sie an einer kriminellen Aktion beteiligt sind. Auch zurückverfolgen lassen sich die Angriffe praktisch nicht.
  Oft entsteht der Schaden schon durch den Ausfall des Netzes. Ein DDoS-Angriff kann aber auch als Ablenkungsmanöver genutzt werden, um über einen anderen Weg in fremde Netze einzudringen.

- Hat ein Angreifer Zugriff auf den **WLAN-Router**, kann er beispielsweise durch DNS-Manipulation den gesamten Datenverkehr auf einen eigenen Server umleiten: Nach Eingabe einer Internetadresse wird die IP-Adresse eines gefälschten Internetauftritts auf einem anderen Server aufgerufen. Der Benutzer bemerkt davon nichts. Danach kann er den Internetverkehr manipulieren oder auch „nur“ mitlesen, um Zugangsdaten zu Internetdiensten zu erhalten.

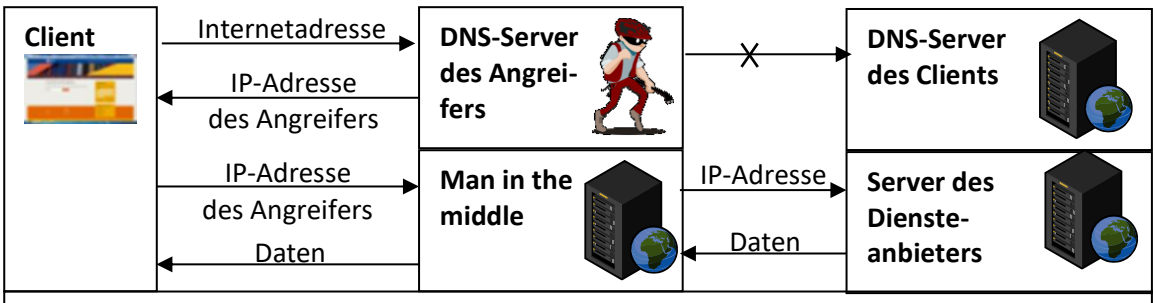
➢ Die Manipulation des Datenverkehrs nennt man **man-in-the-middle Angriff**.

Abb. rechts: Das Gerät des Nutzers kontaktiert den DNS-Server, der ihm durch den DHCP-Server im lokalen Netz – also den WLAN-Router – zugewiesen wurde.
Daraufhin kontaktiert der Client den Server des Diensteanbieters.

Wenn es einem Angreifer gelingt, den DNS-Eintrag im Router zu ändern, kann er den gesamten Datenverkehr auf einen eigenen Server umleiten:



Ablauf der Kommunikation zwischen dem Nutzer eines Dienstes, dessen Servers und dem DNS-Server



Ablauf der Kommunikation bei einem man-in-the-middle Angriff

- Beim **Snarfing** täuscht ein Angreifer einen öffentlichen WLAN-Hotspot vor und hat den gesamten Datenverkehr unbedarfter Nutzer zur Verfügung, die dieses WLAN nutzen.
- Die Adresse des DNS-Servers kann auch **direkt an dem Gerät** – z. B. einem PC – **geändert werden**, ohne die Kontrolle über den Router zu haben.

- Offensichtliche Sicherheitslücken sind nicht das einzige Risiko, wenn „smarte“ Geräte in einem WLAN betrieben werden. Vielmehr wird durch den Zweck der Geräte die Firewall des Routers untertunnelt, indem über das Internet von außen darauf zugegriffen wird, was ja auch oft sinnvoll ist, z. B.:
  - Schaltsteckdosen, um Geräte ein- und auszuschalten.
  - Steuerbare Überwachungskameras, um Kameraschwenks auszuführen.
  - Rasenmäher- oder Staubsaugerroboter, um sich über den Stand der Arbeiten zu informieren.
  - Heizungsthermostate, um die Raumtemperatur überwachen und ändern zu können.

  ... und viele weitere:
  - Rollladen- und Garagentorsteuerung, sprachgesteuerte Assistenten, Webcams, ...
- Es gibt auch Fälle, in denen die Kommunikation smarter Geräte mit dem Gerätehersteller zumindest fragwürdig ist. Das sind zum Beispiel:
  - Smart-TVs, die Fernsehgewohnheiten übermitteln, ohne dass der Nutzer etwas davon erfährt. Der betroffene Dienst HbbTV war bei einem Test im Jahr 2014 bei vielen Geräten standardmäßig aktiviert. Bei verschiedenen Geräten war es auch einfach möglich, Zugangsdaten z. B. für Amazon oder Maxdome – sogar für Online-Banking – zu ermitteln. (vgl. c’t 2014, Heft 4, S. 78-81)
  - Hat ein Krimineller Zugriff auf das Gerät, kann er darüber hinaus z. B. auch eine eventuell am Smart-TV vorhandene Kamera aktivieren, ohne dass man etwas davon bemerkt. (vgl. z. B. https://www.heise.de/security/meldung/Per-Web-und-USB-Stick-Smart-TVs-vielfaeltig-angreifbar-2797227.html)
- Die Probleme dabei sind: Das WLAN ist auch außerhalb der Wohnung erreichbar. Jeder kann also von der Straße aus darauf zugreifen. Wenn ein Krimineller Zugriff auf den Router hat, kann er beliebige Angriffe starten. Und viele Smarthome-Komponenten untertunneln die Sicherheitsmechanismen des Routers, weil sie von außen erreichbar sein müssen. Zusätzlich verfügen solche Geräte oft nur über unzureichende Sicherheitsmaßnahmen und kommunizieren teilweise sogar unverschlüsselt.
- **Wir sind auch für das verantwortlich, was wir nicht tun!** Wer sich nicht um die Sicherheit seiner IT-Ausstattung kümmert, schadet potentiell nicht nur sich selbst, sondern auch der Allgemeinheit. Deshalb wurden im IT-Unterricht bereits Maßnahmen in Bezug auf Datenschutz und Datensicherheit besprochen (vgl. Lerninhalte 1.4–05 *Risiken bei der Nutzung digitaler Kommunikationsformen* sowie 1.8–04 *Datensicherheit*).

Einfallstore

- Bist du der Meinung, der E-Mail Account ist nicht besonders schützenswert, weil „du ja nichts zu verbergen hast“ bzw. auch „nicht Schlimmes passieren kann“ wie z. B. Diebstahl von Geld?
  Da irrst du dich: Die E-Mail Adresse ist ein zentraler Teil deiner Online-Identität: Ein böswilliger Mensch kann nicht nur in deinem Namen E-Mails versenden, um plausible Spam-Mails zu versenden oder deinen Ruf zu schädigen: Bei einfachen „Passwort vergessen?“-Optionen kann sich jeder ein neues Kennwort für eine ganze Reihe von Diensten zusenden lassen, um z. B. in deinem Namen einzukaufen und dabei die Lieferadresse zu fälschen.
- Für Angriffe auf Datennetze wird häufig ein Computer kompromittiert. Wenn es dem Angreifer gelingt, auf einem Gerät Daten auszuspähen oder zu manipulieren (wie z. B. Benutzernamen und Kennwörter) kann er sich innerhalb des Lokalen Netzes weiter vorarbeiten. Damit kann er Zugriff auf weitere Daten und Geräte bekommen. Der Zugriff auf ein Gerät erfolgt häufig mit Hilfe von Schadprogrammen. Es gibt aber andere Methoden, an Zugangsdaten zu einem Computer bzw. zu einem Netzwerk zu gelangen. Einige hast du schon kennengelernt (vgl. Lerninhalte 1.4–05, S. 3):
  - Links und Dateianhänge, die unbedarfte Benutzer in E-Mails öffnen.
  - Schadsoftware, die über Programme eingeschleust wird, welche der Computernutzer installiert.
  - Direkte Angriffe auf Computer.
  - Infizierte Webseiten, die Sicherheitslücken des Browsers ausnutzen (Drive-by-Download).
  - Nutzung von Filesharing-Netzwerken.
- Auch mittels USB-Sticks, die man auch legal kaufen kann, wird in Datennetze eingedrungen.

A Bearbeite das Arbeitsblatt 04: Einfallstore für Angriffe auf Datennetze