

Einführung in IT-Security

IT-Security

Andreas Unterweger

Studiengang Web Business & Technology
FH Kufstein

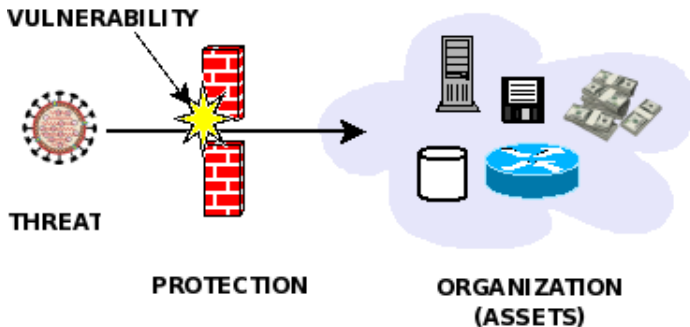
Sommersemester 2018

- Schutz vor verschiedenen Gefahren in IT-Systemen
 - (Daten-)Manipulation
 - (Daten-)Diebstahl
 - ...
 - Absicherung von Daten in IT-Systemen
 - Daten auf Servern, PCs, Laptops, Tablets und Smartphones
 - Daten auf externen Festplatten, USB-Sticks und SD-Karten
 - Über (lokale und gloale) Netzwerke übertragene Daten
 - Verarbeitete Daten (z.B. in Hardware und Software)
 - Angriffe können **nie** vollständig vermieden werden
- Katz- und Mausspiel zwischen Angreifer und Angegriffenem

- Vertraulichkeit (engl. *confidentiality*)
 - Nur Berechtigte können Informationen einsehen
 - Unberechtigte haben keinen Zugriff
 - Beispiel: Datenverschlüsselung
- Integrität (engl. *integrity*)
 - Gespeicherte Informationen bleiben unverändert
 - Unberechtigte können Daten nicht unbemerkt ändern
 - Negativbeispiel: Notenmanipulation
- Verfügbarkeit (engl. *availability*)
 - Berechtigte können (jederzeit) auf Daten zugreifen
 - Unberechtigte können Zugriff für Berechtigte nicht einschränken
 - Negativbeispiel: Denial-of-Service-Attacke

Grundbegriffe I

- Bedrohungen (engl. *threats*) durch Sicherheitslücken (engl. *vulnerabilities*)



Quelle: altheid: Definitions/Threats-vulnerabilities-assets.

<https://www.altheid.com/wiki/Definitions/Threats-vulnerabilities-assets> (Zugriff am 29.1.2017), 2010.

- Assets
 - Wertvoll bzw. schwer ersetzbar
 - Hardware, Software oder Wissen (u.a. Zugangscodes)
 - Beispiele: Dokumente mit Firmeninterna, Kundendatenbank
 - Negativbeispiel: 10 Jahre alter Kopierer ohne Netzwerkanbindung
- Risikobewertung
 - Abhängig vom Angriffsvektor (Art des Angriffs)
 - Wie wahrscheinlich ist es, dass es passiert?
 - Wie schlimm ist es, falls es passiert (inkl. rechtliche Konsequenzen)?
 - Beispiel: Diebstahl sensibler Kundendaten

Kategorisierung von Angreifern



WHITE HAT



GRAY HAT



BLACK HAT

Quelle: Linked List Corrupt: About. <http://www.linkedlistcorruption.com/about/> (Zugriff am 29.1.2017), 2017.

- Mit guter Absicht (*white hat*) vs. mit böser Absicht (*black hat*)
- Klassische White Hats: Ethical Hackers (Penetration Testing mit expliziter Erlaubnis; Details zu Penetration Tests später)

Arten von Angreifern (Auswahl)

- Cyberkriminelle (engl. *cybercriminals*)
 - Verwenden (meist) illegal erlangte Daten zu ihrem eigenen Vorteil
 - Hauptmotiv monetär (Beispielziel Kontodatendiebstahl)
 - Meist sehr erfahren
- Script Kiddies
 - Verwenden fertige Angriffssoftware (meist) ohne konkretes Ziel
 - Hauptmotiv Ruhm („Meinetwegen war dieser Server nicht erreichbar“)
 - Meist unerfahren
- (Ehemalige) Mitarbeiter (verschiedene Motive)
 - Wollen Ihrem (ehemaligen) Unternehmen schaden (Motiv Rache)
 - Wollen sich bereichern (z.B. durch Verkauf von Interna)
 - Gemeinsamkeit: Haben spezielles Wissen über das Unternehmen
- Andere, z.B. Händler von (unveröffentlichten) Sicherheitslücken

Arten von Angriffen (Auswahl)

- Bösartige Software
 - Engl. *malicious software* – *malware*
 - Auch: Schadsoftware
- Netzwerkbasierte Angriffe
 - Denial-of-Service-Attacken (DoS-Attacken)
 - Man-in-the-Middle-Attacken (→ spätere Vorlesung)
- Anwendungsbasierte Angriffe (→ nächste Vorlesung)
- Social Engineering

- Führt Schadfunktionen aus
- Könnte aufgrund ihres (Maschinen-)Codes erkannt werden
- Verschiedenste Verschleierungsmethoden, z.B.
 - Polymorphismus: Tatsächlich böartiger Code ist verschlüsselt und wird erst während der Ausführung entschlüsselt und ausgeführt
 - Metamorphismus: Code schreibt sich selbst in gleichwertigen um
- Erkennung praktisch immer schwieriger
- Verschiedene Typen je nach Verbreitung und Wirkungsweise

- Viren

- Versuchen ihren Code zu reproduzieren
- „Infizieren“ dazu eine Datei (z.B. Excel-Arbeitsblatt mit Makro)
- Öffnen der infizierten Datei führt Viruscode mit aus → Verbreitung
- Bei Verbreitung zusätzliche Schadcodeausführung (z.B. Dateilöschung)

- Würmer

- Versuchen sich per Netzwerk zu verbreiten
- Nutzen Softwaresicherheitslücken aus
- Bei Erfolg Suche nach nächstem verwundbaren Rechner → Verbreitung
- Können bei Eindringen Viren und andere Schadsoftware ablegen

- Trojanische Pferde

- Verbreiten sich nicht von selbst
- Tarnen sich als scheinbar harmloses Programm (Analogie zu Troja)
- Richten im Hintergrund Schaden an (z.B. Abgreifen der PIN)

- Rootkits
 - Versuchen das Verhalten anderer Schadsoftware zu verschleiern (z.B. Programme im Taskmanager verbergen)
 - Greifen meist tief ins Betriebssystem ein → schwer zu erkennen
- Spezielle Ausprägungen (Auswahl)
 - Spionagesoftware (engl. *spyware*): Sammelt ungefragt Daten
 - Ransomware: Erpresst Geld (z.B. nach Dateienverschlüsselung)
 - Logikbombe: Richtet nach Ereignis (z.B. Zeitablauf) Schaden an
 - Hintertür (engl. *backdoor*): Ermöglicht Zugriff ohne Überprüfung
- Zusammenschluss infizierter Computer (Bots) zu einem Botnetz (zentrale Steuerung z.B. zum Versand von Spam-E-mails)

Denial-of-Service-Attacken (DoS-Attacken)

- Systeme werden mit sinnfreien/beliebigen Anfragen überhäuft
 - Mögliche Flaschenhälse (Auswahl)
 - Bandbreite der Systemanbindung (z.B. Internetleitung)
 - Rechenkapazität
 - Speicherkapazität
- Systeme können legitime Anfragen nicht mehr (zeitnahe) beantworten
- Oft schwer zu stoppen, da Legitimität der Anfragen kaum erkennbar
 - Blockierung der Senderadresse in eindeutigen Fällen möglich
 - Häufiger Fall: Verteilte (Distributed) DoS-Attacke (DDoS)
 - Quelle der Anfragen sind Bots (meist eines Botnetzes)
 - Problematischer, da keine einfache adressbasierte Blockierung möglich

- Idee: Menschliche statt technische Schwachstellen ausnutzen
- Mögliche Ziele:
 - Informationsbeschaffung (inkl. Zugangsdaten)
 - Einschleusen von Schadsoftware
- Beispiel:
 - Recherche zu Namen der IT-Mitarbeiter einer Firma
 - Anruf bei der Sekretärin der Firma unter falschem Namen
 - Hinweis zu Installation von „Tool“ (Schadsoftware) für „Speedup“
 - Alternativ: Bitte um Passwort wegen „IT-Problem“
- Glaubwürdigkeit, Ausmaß und Opferignoranz oft entscheidend

- Informationsbeschaffung über öffentliche Quellen
 - Firmen-Internetseiten
 - Suchmaschinen
 - Durchsuchen von Abfällen (illegal)
- Phishing
 - Nachbau einer legitimen Email oder Webseite
 - Ziel: Benutzer auf Seite mit Schadsoftware locken
 - Alternativ: Schadsoftware anhängen
 - Jede Abweichung vom Original erregt Verdacht
 - Häufig Typo Squatting für Senderadresse (z.B. telecom.at)

Phishing-Beispiel I



Adaptiert von Esnouf, F.: A good phishing example. How is structured this kind of attack. <https://blogs.technet.microsoft.com/fesnouf/2010/11/08/a-good-phishing-example-how-is-structured-this-kind-of-attack/> (Zugriff am 4.2.2017), 2010.

Phishing-Beispiel II



Mettre a jour de votre Carte Crédit en ligne

Veuillez Remplir l'au dessous de la form Pour vous protéger contre l'utilisation frauduleuse de votre carte bancaire, Verified By Visa a adopté la solution SecureCode™.

Une Fois Votre Carte de crédits est confirmé seraprotégé Contre les menaces est les Fraudes en ligne.

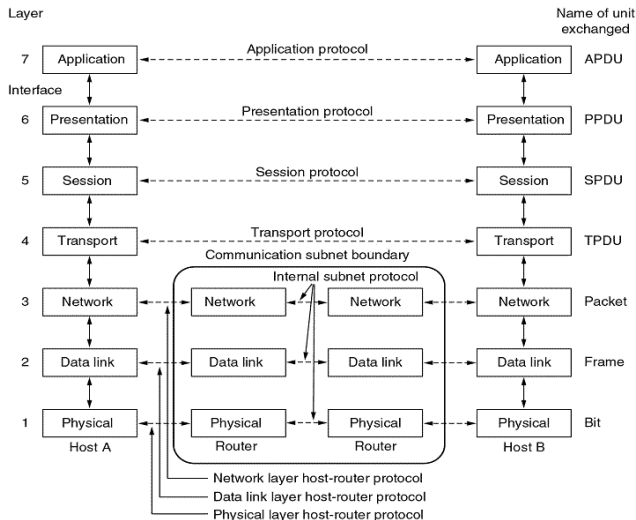
Form fields for updating credit card information:

- Civilité * : [dropdown]
- Nom * : [text input]
- Prénom * : [text input]
- Adresse * : [text input]
- ville * : [text input]
- code postal * : [text input]
- Date de Naissance * : [date picker]
- Nome De jeune fille de votre mère? * : [text input]
- Type De Carte * : [dropdown] (includes VISA and MasterCard logos)
- Numéro de carte * : [text input]
- Date d'expiration * : [date picker]
- Cryptogramme * : [text input] (includes a small image of a card)

Buttons: [Valider]

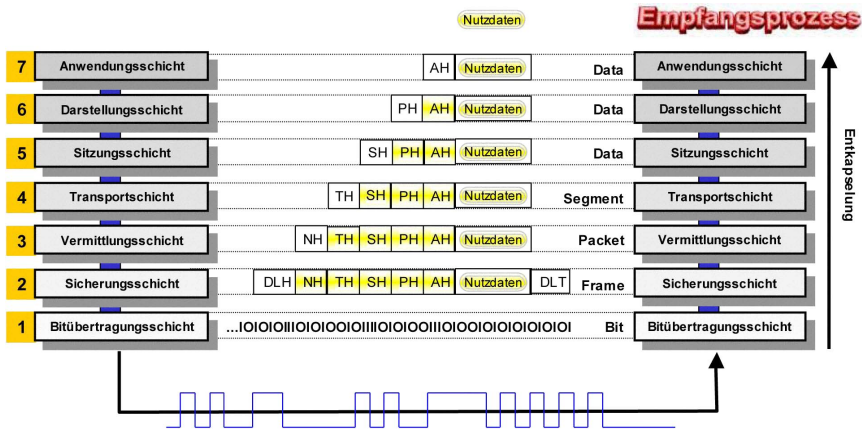
Adaptiert von Esnouf, F.: A good phishing example. How is structured this kind of attack. <https://blogs.technet.microsoft.com/fesnouf/2010/11/08/a-good-phishing-example-how-is-structured-this-kind-of-attack/> (Zugriff am 4.2.2017), 2010.

Wiederholung ISO-OSI-Modell I



Quelle: http://www.marco.panizza.name/dispenseTM/slides/layers/img/iso_osi.png (Zugriff am 5.2.2017).

Wiederholung ISO-OSI-Modell II



■ = Service Access Point (Dienstzugangspunkt)

Quelle: AIRNET: 1.1.9. Entkapselung. http://www.airnet.de/cr1-gfe/de/html/InfoAustKomp_learningObject9.xml
(Zugriff am 5.2.2017), 2015.

Wiederholung Netzwerkelemente



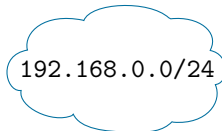
Hub
(Layer 1)



Switch
(Layer 2)



Router
(Layer 3)



Netzwerk oder
Subnetz



Rechner

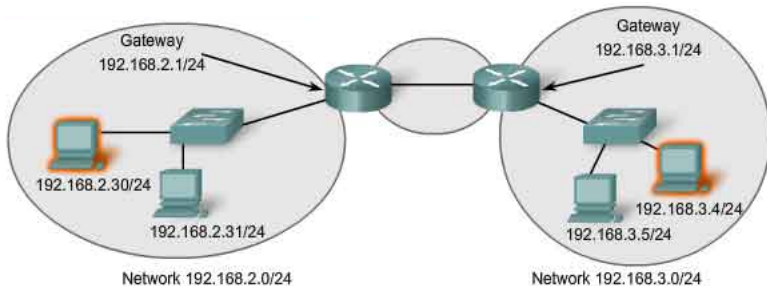


Server

- MAC-Adressen (MAC: Media Access Control)
 - 48 Bit, z.B. 08:00:27:0F:7A:56 (hexadezimal)
 - Typischerweise eine pro Netzwerkkarte/Anschluss
 - Ein Gerät kann mehrere Netzwerkkarten haben
- Nonpromiscuous Mode (Standard)
 - Netzwerkkarte reagiert nur auf eigene MAC-Adresse (als Ziel)
 - Zusätzlich: Broadcast-Adresse FF:FF:FF:FF:FF:FF
- Promiscuous Mode
 - Netzwerkkarte reagiert auf alle MAC-Adressen
 - Reaktion auf andere Rahmen möglich
- Hub repliziert nur Signal an alle Anschlüsse (ignoriert Zieladressen)
- Switch lernt Absenderadressen (ohne Details) und leitet Frames **nur** an jeweilige Zieladressen weiter

Wiederholung Layer-3-Adressierung I

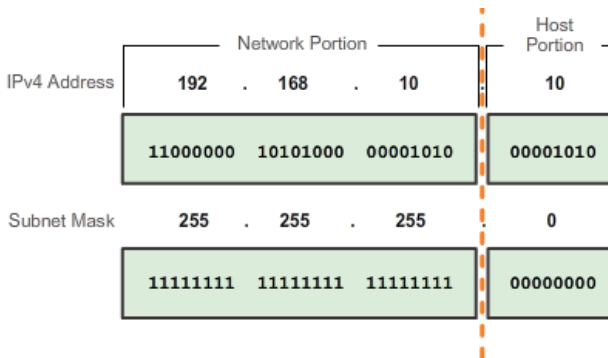
- IP(v4)-Adressen (IP: Internet Protocol)
 - 32 Bit, z.B. 192.168.0.1 (Oktette dezimal gruppiert)
 - Typischerweise eine pro Gerät
 - Manche Geräte (vor allem Server) haben mehrere IP-Adressen
- Router (Gateways) vermitteln Pakete zwischen verschiedenen Netzen



Adaptiert von Unbekannt: OSI Network Layer. http://www.highteck.net/EN/Network/OSI_Network_Layer.html (Zugriff am 5.2.2017), unbekannt.

Wiederholung Layer-3-Adressierung II

- Subnetze (über Subnetzmaske)
 - Unterteilung der IP-Adresse in Netzwerk- und Hostteil
 - CIDR-Notation mit Anzahl Netzwerkbits, z.B. 192.168.10.10/24

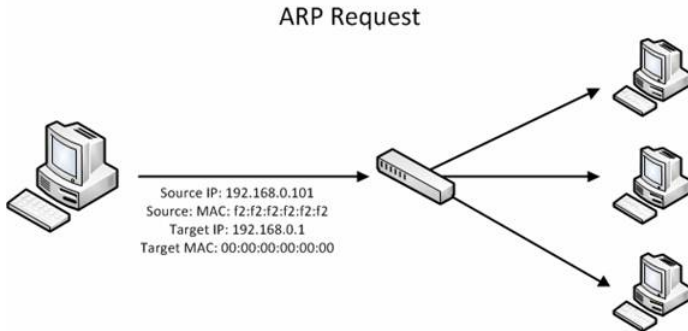


Adaptiert von SC Labs: CCNA Chapter 9 Subnetting IP Networks.

<http://sclabs.blogspot.co.at/2013/09/ccna-chapter-9-subnetting-ip-networks.html> (Zugriff am 5.2.2017), 2013.

Wiederholung Layer-3- zu Layer-2-Adressauflösung I

- Address Resolution Protocol (ARP)
 - Löst IP- in MAC-Adressen auf
 - Anfrage (Request) als Broadcast im lokalen Netz
 - Antwort (Response) vom Rechner mit angefragter IP



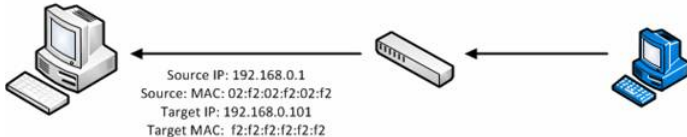
Adaptiert von Sanders, C.: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1).
<http://techgenix.com/understanding-man-in-the-middle-attacks-arp-part1/> (Zugriff am 5.2.2017), 2010.

Wiederholung Layer-3- zu Layer-2-Adressauflösung II

- ARP Cache

- Tabelle mit bekannten IP-MAC-Adresszuordnungen
 - Einmal angefragte Adressen werden nach Antwort gespeichert
- Wiederholte Anfragen nicht notwendig

ARP Response

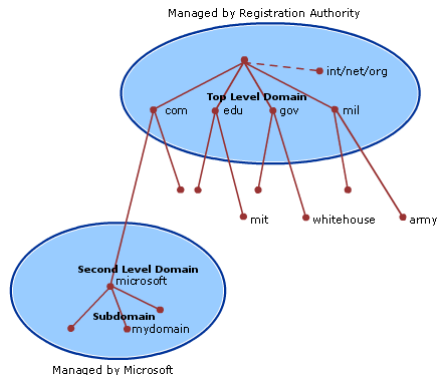


Adaptiert von Sanders, C.: Understanding Man-in-the-Middle Attacks – ARP Cache Poisoning (Part 1).
<http://techgenix.com/understanding-man-in-the-middle-attacks-arp-part1/> (Zugriff am 5.2.2017), 2010.

Wiederholung Namensauflösung I

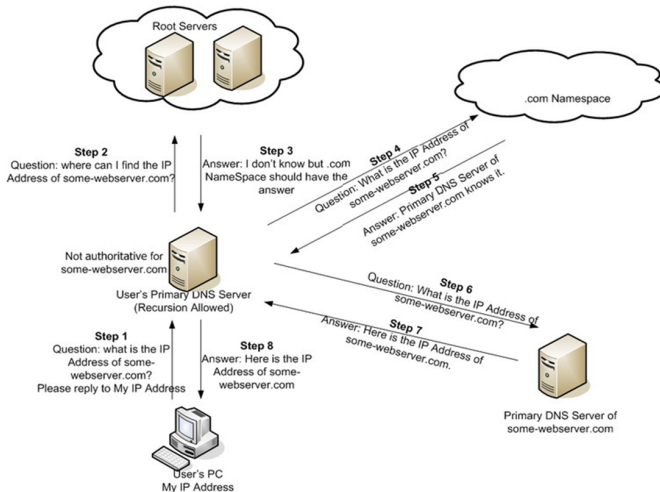
- Domain Name System (DNS)

- Löst (Domain-)Namen in IP-Adressen auf (A(ddress) Records)
- Hierarchischer Aufbau: Verteilte Server mit Zuständigkeiten



Adaptiert von Microsoft: DNS Architecture. [https://technet.microsoft.com/en-us/library/dd197427\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/dd197427(v=ws.10).aspx)
(Zugriff am 5.2.2017), 2017.

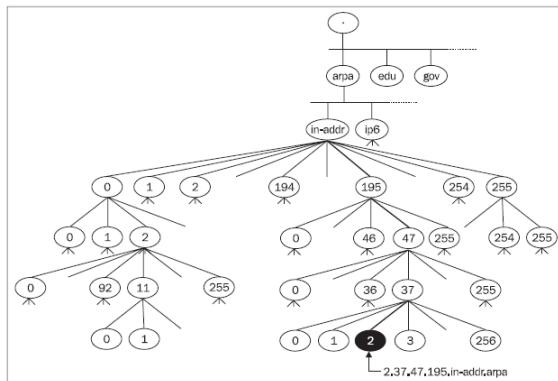
Wiederholung Namensauflösung II



Quelle: LeaseWeb: Domain Name System (DNS). <https://kb.leaseweb.com/display/KB/Knowledge+Base?pageId=6520935> (Zugriff am 5.2.2017), 2015.

Wiederholung Namensauflösung III

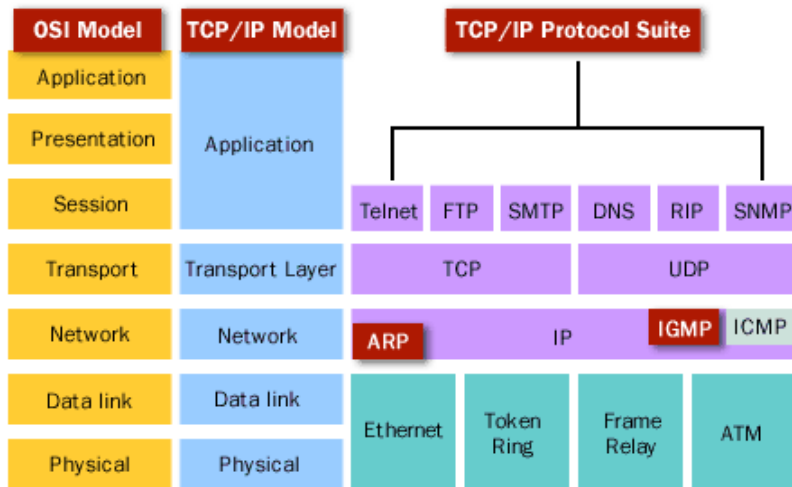
- Reverse DNS (Teil von DNS)
 - Löst IP-Adressen in (Domain-)Namen auf (PTR (Pointer) Records)
 - In DNS-Hierarchie unter `arpa.in-addr` (Beispiel `195.47.37.2`)



Quelle: Packt Publishing: Sample Chapter: Domain Name System.

http://www.codeguru.com/cpp/sample_chapter/article.php/c12013/Sample-Chapter-Domain-Name-System.htm (Zugriff am 5.2.2017), 2006.

Wiederholung TCP/IP-Modell

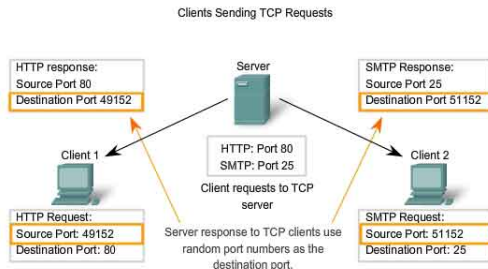


Quelle: Distributed Networks: The TCP/IP protocol Suite.

<http://www.distributednetworks.com/dhcp-tcp-ip/module3/tcp-ip-protocolSuite.php> (Zugriff am 5.2.2017), unbekannt.

Wiederholung Transportprotokolle (Auswahl)

- Transmission Control Protocol (TCP)
 - Verbindungsorientiert mit zuverlässiger Übertragung
 - Wird z.B. von HTTP verwendet
- User Datagram Protocol (UDP)
 - Verbindungslos ohne zuverlässige Übertragung
 - Wird z.B. von DNS verwendet
- Ports separieren transportierte Protokolle pro IP



Adaptiert von Unbekannt: OSI Transport Layer. http://www.highteck.net/EN/Transport/OSI_Transport_Layer.html
(Zugriff am 5.2.2017), unbekannt.

Wiederholung Anwendungsschichtprotokolle (Auswahl)

- Hypertext Transfer Protocol (HTTP) – Port 80
 - Übertragung von Dateien (Webseiten, Grafiken, Skripte etc.)
 - Client-Server-Architektur, wobei Client meist Web-Browser
- Simple Mail Transfer Protocol (SMTP) – Port 23
 - Emailversand und -übertragung (zwischen Mailservern)
 - Zum (clientseitigen) Emailabruf meist IMAP oder POP
- Secure Shell (SSH) – Port 22
 - Fernzugriff auf andere Rechner (Befehlsausführung)
 - Beinhaltet SCP (siehe unten)
- Secure Copy Protocol (SCP) – über SSH
 - Erstellen von Dateikopien auf anderen Rechnern
 - Kopieren von Dateien von anderen Rechnern

Wiederholung Internet Control Message Protocol (ICMP)

- Bestandteil des TCP/IP-Stacks
- Setzt wie UDP direkt auf IP auf (keine Garantien)
- Hauptanwendungen:
 - Informationsaustausch zwischen Geräten
 - Rückmeldung in Fehlerfällen
 - Tests für Fehlersuche und -behandlung
- Typische Werkzeuge basierend auf ICMP (Auswahl):
 - ping (ICMP *Echo Request* mit *Echo Reply*): Überprüfung der Erreichbarkeit eines Ziel(-rechner-)s über dessen IP
 - tracert/traceroute: Wiederholter *Echo Request* zur Zeitmessung aller Teilstrecken bei IP-basierter Übertragung zu einem Ziel(-rechner)

Fragen?