COMPUTERSICHERHEIT

COMPUTERARBEITSPLATZ UND NETZWERKE NUTZEN, PFLEGEN UND KONFIGURIEREN

1 NETZWERKE

2 NETZWERKTOPOLOGIEN

3 ANGRIFFE, MALWARE UND SCHUTZMÖGLICHKEITEN

4 SERVER

1 NETZWERKE

Definition Netzwerk

- Zusammenschaltung mehrerer Rechner
- Beispiel: mehrere Computer haben Zugang zu einem Drucker

Netzwerkarten

LAN = Lokal Area Network
Rechnernetz über begrenzte räumliche Gebiete
lokales/privates Datennetz

WAN = Wide Area Network
Büros mit verschiedenen Standorten können ihre LANs zu WANs erweitern und miteiander verbunden werden

GAN = Global Area Network
weltweite Verbindung über Satelit z.B. das Internet

MAN = Metropolitan Area Network
Netzwerk, dass auf eine Stadt/Region beschränkt ist

VPN = Virtuelles Privates Netzwerk
Verbindung virtueller eigener Netze im Internet

Netzwerkbegriffe

Router

- entscheidet, welchen Weg die Daten nehmen
  sorgt für optimale Verbindungswege für die zu übertragenden Daten
- fungiert als Vermittler
- Multiprotokoll-Router: können mehrere Protokolle unterstützen
- häufig integrieren sie eine Hardware-Firewall zum Schutz vor äußeren Angriffen
- von „Außen“ ist nur die IP-Adresse sichtbar

Repeater

- Gerät zur Signalverstärkung
- separates oder zentrales Bauteil in einem aktiven Hub

1 NETZWERKE

Hub
- wird auch Sternverteiler genannt
- Knotenpunkt in sternförmig angelegten Netzwerken
- aktiver Hub = mit Repeater: verteilt nicht nur sondern verstärkt auch
- passiver Hub = verteilt nur

Bridge
- Verbindung zweier Netzwerkteile oder zweier Netzwerke der gleichen Topologie, aber mit unterschiedlichen Zugriffsverfahren
- Netze können erweitwwert werden
- Verstärkerfunktion des Repeaters ist enthalten

Gateway
- Computer, der Netze durch verschiedene Schichten miteinander verbinden kann
- schließt die Funktionen eines Routers, Bridge und Repeaters ein
- übersetzt unterschiedliche Netzwerkprotokolle
- typische Anwendung: Anbindung eines lokalen Netzwerkes an das Internet z.B. mit ISDN-Karten.

Server
- Mittelpunkt eines Netzwerkes
- Computer, die den Benutzern Dienste, Dateien und Geräte zur Verfügung stellen

Host
- übernimmt Kommunikationsaufgaben
- zentrale Dienstleistungsrechner

Clients
- Computer, die auf Dienste, Dateien und Geräte des Servers zugreifen

2 NETZWERKTOPOLOGIEN

Peer to Peer
- keinen festen Server
- zur Vernetzung kleinerer Anlagen

Topologien

Bus Netz
- nutzt Koaxialkabel
- linear Netzwerk mit Terminatoren am Ende
- Leitungslänge ist begrenzt
- Anschluss weiterer Stationen nur durch Unterbrechung des Netzes
- Billig

Ring-Netz
- Server nicht unbedingt notwendig (Peer to Peer)
- keine Längenbeschränkung
- Erweiterung nur durch Unterbrechung des Rings
- Ausfall eines Rechners legt Netz lahm, wenn keine Überbrückungskabel vorhanden sind

Stern-Netz
- keine Datenkollision (Jamming)
- Erweiterung ohne Unterbrechung
- am teuersten
- Twisted Pair Kabel braucht es
- läuft mit HUB
- kann peer to peer aber auch mit Server sein

Kabelverbindungen

Koaxialkabel
- Kupferkabel
- bis zu 10 mbit/s
- für Ethernet-Netze

Twisted Pair
- Am meisten genutzt
- 2 verdrillte Kupferleitungen, deshalb weniger Störfelder
- Im Sternen-Netz vorzufinden
- UTP=Unshild = ohne Abschirmung ca 64 kbit/s
- STP=Shild = mit Abschirmung 10-100 mbit/s

2 NETZWERKTOPOLOGIEN

Glasfaserkabel
- 1 dünne Glasfaser umhüllt vom Glasmantel
- Abhösicher
- ca 100 mbit/s bis 1 Gbit/s
- zu teuer deshalb meist für Backbone-Netze genutzt

Ethernet
- häufigste Netzwerkarchitektur
- 1-10 mbit/s
- Fast Ethernet 100mbit/s
- arbeitet mit CSMA/CD Zugriffsverfahren (Carrier Multiple Access Collison Detect)
- Carrier Sense = Abhören des Netzes zum Senden und Empfangen
- Multiple Access = Rechner sendet Daten, wenn Netz frei ist, sonst nach Wartezeit
- Senden zwei Rechner gleichzeitig kommt es zur Datenkollison (Jamming). Dann setzt die Collision Detection ein. Es bemerkt die Störung und meldet es an alle Rechner. Wenn die Leitung frei ist, wird erneut gesendet.

Token Passing
- Token Ring Netze haben eine Übertragugsrate von 4 bis 16 mbit/s
- Token Passing sendet im Netz Signale. Einmal Frei-Token und Belegt-Token
- wenn der Rechner etwas senden will, wandelt er das Frei-Token in belegt-Token um und hängt daran seine Daten. Nach dem Erhalt wird eine Bestätigung wieder zum Sender geschickt und das Token Passing weiß, dass es die Daten aus dem Netz nehmen kann. Das Belegt-Token wird wieder in ein Frei-Token gewandelt und kreist wieder im Netz.

Hub
- Aktive Hubs enthalten Repeater und verstärken zusätzlich das Datensignal
- zum Verbinden mehrerer Rechner, ohne das Netz unterbrochen wird

Router
- verbindet auch unterschiedliche Netzwerke
- somit auch Anbindung ans Internet möglich

Repeater
- ist ein Zwischenverstärker
- Kann alle Topologien und Systeme miteinander verbinden

Bridge
- ist im Repeater eingebaut
- Netzwerkstruktur muss gleich sein, aber Betriebssystem kann unterschiedlich sein!

Gateway
- Mischung aus Hub, Bridge, Router,

3 ANGRIFFE, MALWARE UND SCHUTZMÖGLICHKEITEN

Computersicherheit

Ein sicherer Computer ust die Voraussetzung für ein sicheres Arbeiten.
Überall lauern Gefahren vor welchen man seinen Computer schützen muss.
Die sogenannte Malware versteckt sich oft in Email-Anhängen und auf infizierten Webseiten, oft so gut getarnt, dass der Benutzer nichts von seiner Infizierung mitbekommt und Fremde die Überhand über seinen Computer haben.

Ziele solcher Angriffe sind:

- Überwachung des Computers und dessen Nutzer
- mißbräuchliche Nutzung des Rechners (z.B für Spam-Versand oder Speicherung von Dateien)
- Ausspähen von verwertbaren Daten (z.B Kontodaten)
- Erpressung (Verschlüsselung von Daten --> Entschlüsselung gegen Geld)

Angriffsmethoden:

Malware:
Ist der Oberbegriff für Computerprogramme, die entwickelt wurden, um vom Benutzer unerwünschte und gegebenfalls schädliche Funktionen auszuführen.

Viren:
- kleine Programme die sich an ein anderes Programm anhängen
- Wird aktiv sobald dieses Programm gestartet wird.

Würmer:
- eigenes ausführbares Programm
- häufig in Email-Anhängen
- Wird der Wurm per Doppelklick gestartet, kann er sich bspw. an alle im Adressbuch ge speicherten Adressen
- versenden (verbreiten sich durch Schneeball-Prinzip rasant)

Trojaner:
- Programm, dass sich nach außen als nützliches programm (bspw. Update) tarnt
- Im Hintergund werden jedoch schädliche Funktionen gestartet
- Gefährlich sind hier bspw: Backdoor-Programme die einen externen Zugang auf den rech ner zulassen
- Ebenfalls gefährlich Key-Logger: Die sämtliche Tastatureingaben protokollieren und so Passwörter und Benutzernamen entschlüsseln

Spyware:
- ähnliches Verhalten wie Trojaner
- spähen allerdings das Benutzerverhalten aus um bspw. gezielt Werbeanzeigen zu platzieren

3 ANGRIFFE, MALWARE UND SCHUTZMÖGLICHKEITEN

Phising-Mails:
- Emails mit dem Ziel Zugangsdaten zu ebay, Onlinebanking oder ähnlichem auszuspionieren
- Nutzer wird dazu veranlasst auf einen Link zu klicken
- gelangt somit auf eine Website auf welcher er seine Zugangsdaten eingeben soll
- Somit sind die Zugangsdaten erfasst

Drive-by-Download
- Unbewusstes und unbeabsichtigtes Herunterladen von Software auf den Rechner eines Benutzers.
- Durch das Aufrufen einer dafür preparierten Webseite wird die Schadsoftware automatisch gedownloaded.
- Dabei werden Sicherheitslücken eines Browseres ausgenutzt.

Riskware
- ist die Bezeichnung für legitime Programme, die Schaden zufügen können wenn sie von böswilligen Benutzern zweckentfremdet werden, um Daten zu löschen, sperren, modifizieren oder kopieren.
- Die Programme an sich sind nicht schädlich, sie besitzen jedoch Funktionen die für rechtswidrige Zwecke missbraucht werden können.

Rootkits
- Sammlung von Softwarewerkzegen, die nach „Einbruch“ in ein Softwaresystem installiert werden um zukünftige Aktionen des Eindringlings zu verstecken.
- Zweck eines Rootkits ist es, Schadprogramme vor den Antivirenprogrammen und dem Benutzer durch Tarnung zu verbergen.
- Der Eindringling kann mit den Rechten des Administrators agieren und zum Beispiel Backdoorprogramme installieren, die es ihm in Zukunft erleichtern auf den Rechner zuzugreifen.

3 ANGRIFFE, MALWARE UND SCHUTZMÖGLICHKEITEN

Schutzmöglichkeiten:

1. regelmäßige Updates des Betriebssystems und der installierten programme (schließt Sicherheitslücken)

2. Einen extra Account mit Administratorenrechten anlegen.
   Selbst einen Account mit eingeschränkten Administratorenrechten benutzen.
   Sollten Hacker diesen hacken, können sie keine Programme installieren o.ä.

3. Nutzung eines Antivirenprogramms

4. besondere Vorsicht bei Dateianhängen in Emails

5. Regelmäßig Back-ups machen
   Sinnvoll ist es, Back-ups nicht nur auf der integrierten festplatte sondern auch extern abzusichern. Dafür eigenen sich externe Festplatten oder externe Server.

6. Image-Programme
   Image-Programme rmöglichen es, alle Dateien eines Mediums (Festplatte oder Partition) in einer Datei zu speichern und komprimieren.
   Das Image ist eine Art Zeitmaschine. Wenn das gespeicherte Image eingespielt wird,ist es wie ein Zeitsprung zurück.

7. Firewall
   Die Firewall überprüft eintreffende Datenpakete hinsichtlich ihrer IP Adresse und Zieladresse und untersucht sie auf schädliche Inhalte.
   Außerdem überprüft sie auch den rechner verlassende Datenpakete.
   So kann sie verhindern, dass schädliche Software die sich bereits auf dem Rechner befindet keine Informationen nach außen geben kann. Auf diese Weise kann sie bspw. Spyware entdecken.

8. Sicherheitseinstellungen im Internetbrowser installieren

9. Speichermedium verschlüsseln

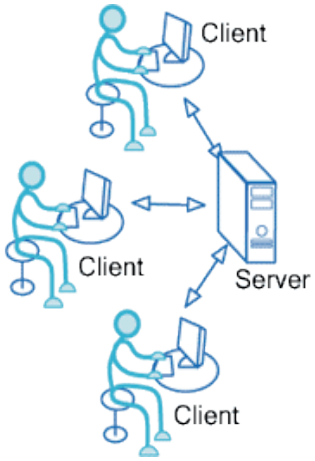
4 SERVER

Client-Server-Modell:

Viele Anwendungen funktionieren in einer Client/Server Umgebung. Das bedeutet, dass die Client-Rechner (Rechner, die zum Netzwerk gehören) Kontakt aufnehmen zu einem Server, der meist ein Rechner mit sehr großer Eingangs-Ausgangs-Kapazität ist, welcher ihnen die Dienste bereitstellt. Diese Dienste sind Programme, die Daten liefern - zum Beispiel die Zeit, Dateien, eine Verbindung, etc.
Die Dienste werden von Programmen genutzt, die Client-Programme heißen und auf den Client-Rechnern ausgeführt werden. Als Clients (FTP Client, E-Mail Client, etc.), bezeichnet man also Programme, die auf einem Client-Rechner laufen und im Stande sind, Informationen zu verarbeiten, die von einem Server eingeholt werden.

Funktionsprinzip eines Client/Server Systems:

- Der Client sendet eine Anfrage an den Server,
  mittels seiner IP Adresse und dem Port, die sich auf einen bestimmten Dienst des Servers bezieht
- Der Server empfängt die Anfrage und
  antwortet mit Hilfe der Adresse des Client-Rechners und seinem Port



Es gibt verschiedene Server-Klassen:

1. File-Server: Stellt seinen Clients Dateien und Platz auf dem Dateisystem bereit. Zusätzlich übernimmt er die Sicherung der Benutzerdateien.

2. Applications-Server: ermöglicht dem Anwender den Zugriff auf ein oder mehrere Anwen dungsprogramme.

3. Datenbank-Server: Auf ihm läuft eine große Datenbank. Die Aufgabe des Servers ist die Verwaltung und Organisation der Daten, die schnelle Suche, das Einfügen und das Sortieren von Datensätzen.

4. Internet-Server: Stellt Internet- und Intranet-Dienste bereit. Typische Dienste umfassen das WorldWideWeb, den DomainName-Service, sowie E-Mail...

5. Media-Server: stellen Multimedia-Daten (Audio-, Videoclips) in Echtzeit und höchster Dienstqualität zur Verfügung.