Themenübersicht

1. Anwendungsmöglichkeiten des Internet−Anschlusses

Unterschiedliche Nutzungsprofile (Arbeitsplatz, lokales Netz)

- Privat: Meist Einzelanschluss mit Modem
- In Firmen: Lokales Netzwerk von Computern mit sowohl firmeninternen Netzwerkdiensten (Intranet) als auch einem Internetanschluss (meist mit hohen Übertragungsraten)

Einsatz des World Wide Web als Recherche−Hilfe sowie zum Datenaustausch

- Recherche über Suchmaschinen (Google, Yahoo...) nach bekannten Themen an jedoch unbekannten Orten
- Alternative zu altbekannten Rechercheverfahren (Bibliothek)
- Viel höhere Erfolgswahrscheinlichkeit, da globale Suche
- Bessere Verwertbarkeit des Ergebnisses, da dieses digital vorliegt und direkt weiter bearbeitet werden kann

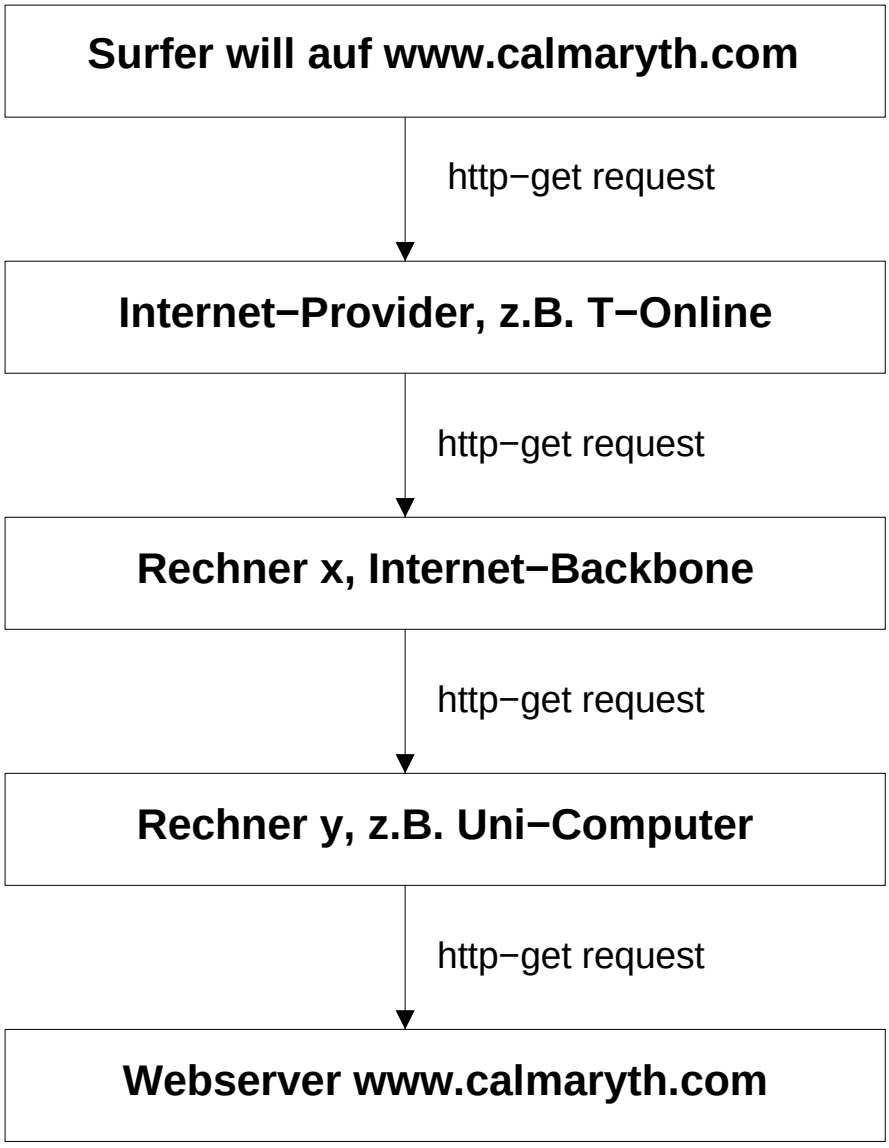
- (Legale) Downloads von Programmen und auch Spielen
  Beispiel: Mohrhuhn−Jagd, Shareware−Programme

Client/Server basierte Anwendungen (Beispiel: Musiktauschbörse Napster)

- Zentraler Rechner fungiert als Vermittler zwischen Suchendem und Anbieter (mittels gespeicherter Datenbank), diese können dann Musik austauschen

(Neuerdings: Serverunabhängige Dienste, die rechtliche Verfolgbarkeit bei Piraterie wird sehr erschwert)

2. Wie funktioniert das Internet? (Stark vereinfacht:)



Wichtig: Keine direkte Verbindung zum Ziel, sondern viele Stationen (Hops) dazwischen

3. Sicherheitskritische Szenarien im globalen Netzwerk

3.1 Einkauf im Internet (Beispiel: Amazon.de)

Bestellung von Produkten durch Auswahl aus Katalog ist relativ einfach und für jedermann durchführbar

- Verschlüsselung als Schutz (z.B. bei der Übertragung von Kreditkartennummern) dringend benötigt
- Authentifizierung des Bestellers benötigt, heute meist durch (schwache?) Passwörter, in Zukunft durch digitale Signatur?

3.2 Teilnahme an Versteigerungen (Beispiel: ricardo.de)

Mitsteigern durch Mausklicks, Abwicklung des Zahlungsverkehrs erfolgt (privat) zwischen dem An− und dem erfolgreichen Mitbieter

- Authentifizierung aller Parteien dringend benötigt
- Zuverlässigkeit des Anbieters fraglich
- Viel Missbrauch (Beispiel: Laptops)

3.3 Online−Banking (Beispiel: Consors.de)

Direkte Kontoführung von zuhause aus, fast alle Transaktionen sind durchführbar (teilweise ohne Limit!)

- Authentifizierung sehr wichtig, heute: Passwort (PIN) sowie spezielle Einmal−Passwörter (TAN)
- Aber: Problem bei z.B. Diebstahl

3.4 Austausch von Emails mit Geschäftspartnern

- Gefahr des Mitlesens und der Manipulation durch Dritte (in der eigenen Firma und auf der Route zum Ziel)
- Gefahr der Fälschung durch jedermann
- Authentifizierung und Verschlüsselung dringend notwendig

Beispiel:
ECHTE NACHRICHT:

From: "Geschäftspartner" <partner@partner.com>
To: Alexander Böhm <alexander.boehm@calmaryth.com>
Subject: Vertrag
Date sent: Mon, 1 Jan 2001 17:01:37 +0100

GEFÄLSCHTE NACHRICHT:

From: "Geschäftspartner" <partner@partner.com>
To: Alexander Böhm <alexander.boehm@calmaryth.com>
Subject: Vertrag
Date sent: Mon, 1 Jan 2001 17:01:37 +0100

Erkennen Sie den Unterschied? Hier gibt es keinen!

3.5 Erkennung gefälschter Nachrichten − was ist ein Header?

Der Header ist der Umschlag einer Email:

ECHTE NACHRICHT:

Return−Path: <partner@partner.com>
Received: from localhost (root@localhost [127.0.0.1])
by guardian.calmaryth.com (8.9.3/8.9.3/SuSE Linux 8.9.3−0.1) with ESMTP id SAA00950
Envelope−to: alexander.boehm@calmaryth.com
Delivery−date: Mon, 1 Jan 2001 17:07:16 +0100
Received: from pop.mailserver.de …
Received: from [195.20.224.219] (helo=mrvdom03.mailserver.de) …
Received: from [62.155.150.179] (helo=mailserver.partner.com) …
Received: from partner (partner.partner.com [192.168.12.1])
for <alexander.boehm@calmaryth.com>; Mon, 1 Jan 2001 17:04:02
Message−ID: <000c01c0740c$1f2fa6a0$6500a8c0@partner>
From: "Geschäftspartner" <partner@partner.com>
To: =?iso−8859−1?Q?Alexander_B=F6hm?= <alexander.boehm@calmaryth.com>
Subject: Vertrag
Date: Mon, 1 Jan 2001 17:01:37 +0100
MIME−Version: 1.0
X−Priority: 3
X−MSMail−Priority: Normal
X−Mailer: Microsoft Outlook Express 5.50.4133.2400
X−MimeOLE: Produced By Microsoft MimeOLE V5.50.4133.2400
X−PMFLAGS: 571998336 0 1 P52BC0.CNM
Content−Type: text/plain;charset="iso−8859−1"
Content−Transfer−Encoding: quoted−printable

GEFÄLSCHTE NACHRICHT (Version A):

Return−Path: <partner@partner.com>
Received: from localhost (root@localhost [127.0.0.1])
by guardian.calmaryth.com (8.9.3/8.9.3/SuSE Linux 8.9.3−0.1) with ESMTP id SAA00950
Envelope−to: alexander.boehm@calmaryth.com
Delivery−date: Mon, 1 Jan 2001 17:07:16 +0100
Received: from pop.mailserver.de …
Received: from [195.20.224.219] (helo=mrvdom03.mailserver.de) …
//Hacker verwendet einen Dienstleister zur Einwahl, der Partner nicht
Received: from [62.21.10.27] (helo=**modem0815.dtag.de**) …
//**Hacker verwendet andere Computernamen und Adressen als Partner**
Received: from **fälscher** (**fälscher.fälscher.net** [**192.168.1.12**])
for <alexander.boehm@calmaryth.com>; Mon, 1 Jan 2001 17:04:02
//**Message−ID Nummern unterscheiden sich**
Message−ID: <**38cs92004cajs940f0vsjal49dkamsdd@fälscher**>
From: "Geschäftspartner" <partner@partner.com>
To: =?iso−8859−1?Q?Alexander_B=F6hm?= <alexander.boehm@calmaryth.com>
Subject: Vertrag
Date: Mon, 1 Jan 2001 17:01:37 +0100
//Hacker verwendet anderes Programm (Pegasus) als Partner (Outlook)
X−cs: R
X−RS−ID: <Default>
X−RS−Flags: 0,0,1,1,0,0,0
X−RS−Sigset: 0
MIME−Version: 1.0
Content−type: text/plain; charset=ISO−8859−1
Content−transfer−encoding: 8BIT

GEFÄLSCHTE NACHRICHT (Version B, mit viel Vorwissen):

Return−Path: <partner@partner.com>
Received: from localhost (root@localhost [127.0.0.1])
by guardian.calmaryth.com (8.9.3/8.9.3/SuSE Linux 8.9.3−0.1) with ESMTP id SAA00950
Envelope−to: alexander.boehm@calmaryth.com
Delivery−date: Mon, 1 Jan 2001 17:07:16 +0100
Received: from pop.mailserver.de …
Received: from [195.20.224.219] (helo=mrvdom03.mailserver.de) …
Received: from [62.155.150.179] (helo=mailserver.partner.com) …
Received: from partner (partner.partner.com [192.168.12.1])
for <alexander.boehm@calmaryth.com>; Mon, 1 Jan 2001 17:04:02
Message−ID: <000c01c0740c$1f2fa6a0$6500a8c0@partner>
From: "Geschäftspartner" <partner@partner.com>
To: =?iso−8859−1?Q?Alexander_B=F6hm?= <alexander.boehm@calmaryth.com>
Subject: Vertrag
Date: Mon, 1 Jan 2001 17:01:37 +0100
MIME−Version: 1.0
X−Priority: 3
X−MSMail−Priority: Normal
X−Mailer: Microsoft Outlook Express 5.50.4133.2400
X−MimeOLE: Produced By Microsoft MimeOLE V5.50.4133.2400
X−PMFLAGS: 571998336 0 1 P52BC0.CNM
Content−Type: text/plain;charset="iso−8859−1"
Content−Transfer−Encoding: quoted−printable

- exzellente Fälschung nicht mehr vom Original zu unterscheiden
- Verschlüsselungs− und Authentifizierungsmaßnahmen unbedingt notwendig

- Es gilt: Eine Email ist so sicher wie eine Postkarte, sie kann von jedem eingesehen und verändert werden, der sie in die Hand bekommt!

4. Viren und trojanische Pferde

4.1 Viren

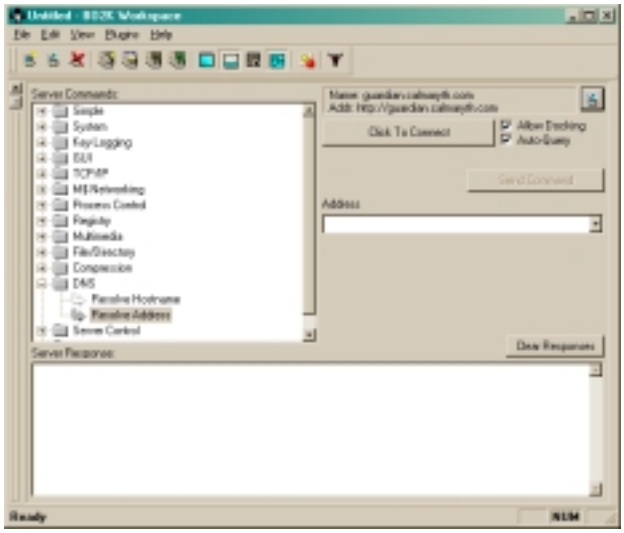
Was ist ein Virus?
- kleine, sich selbst kopierende Datenpakete
- meist (aber nicht immer) störende oder destruktive Wirkung
- traditionell: Bootsektor und Dateiviren
- neu: »moderne« Viren, meist skriptbasiert
- gefährdete Plattformen: hauptsächlich Microsoft Betriebssysteme

4.2 Trojaner

Funktionsweise eines Trojanischen Pferdes
- Funktionsweise gleicht dem historischem Vorbild,
- Spezialfall von Virus (setzt aktives Zutun des Benutzers voraus)

Typischer Ablauf einer Infiltrierung durch einen Trojaner
- Benutzer erhält eine Email mit Attachment (meist: xxx−image.exe oder newyear01.exe) meist von Bekannten oder Kollegen
- Benutzer führt Datei (=Trojaner) aus
- System ist infiltriert

Was macht ein Trojanisches Pferd?
- Funktionsweise identisch mit Viren (verbreiten und Ärger machen)
- Sonderfälle: sog. Hintertüren, Bsp.: Back Orifice Netbus, Sub7
- Gefährdete Plattformen: Alle



Beispiel: Benutzeroberfläche eine BO2K−Trojaners (Client, Windows)

5. Der Rechner im Netz

Sichtbarkeit eines Rechners im Netz

- eindeutige Identifikation durch eine IP−Adresse (12−stellige Zahl der Form xxx.xxx.xxx.xxx) sowohl im lokalen Netz als auch im Internet
- wichtig beim Verbinden zu anderen Rechnern:

Routing in IP−Netzen (vereinfacht)

- Benutzer möchte auf www.calmaryth.com (gibt dies in den Browser ein)
- Rechner (IP−Adresse 1.1.1.1) des Benutzers frägt bei entsprechendem Rechner des Internetdiestleisters (=Nameserver):
  »Sage mir die IP−Adresse von www.calmaryth.com«
- Nameserver antwortet:«www.calmaryth.com ist 123.123.123.123«
- Rechner des Benutzers schickt Anfrage an 123.123.123.123:
  »Zeige mir bitte die Internetseite an, ich bin 1.1.1.1« (http−get)
- 123.123.123.123 sendet antwort an 1.1.1.1 (Daten)

Unterschiedliche Adressenvergabe (dynamisch / statisch)

- Bei dial−up Verbindungen (Call−by−Call, Flatrate...) meist dynamische Adressenvergabe, d.h. die IP−Adresse ändert sich von Verbindung zu Verbindung.
- Bei Standleitungen oder speziellen Anforderungen statische IP−Adressen (IP−Adresse bleibt gleich).

6. Angriffe (von ausserhalb) auf den Rechner

6.1 Verwendung eines Portscanners (Beispiel: nmap)

Was ist ein Port:
- genaue Adressierung eines Dienstes auf einem Computer
- »Verfeinerung« der Adressangabe durch die IP−Adresse

Beispiel:
Rechner: 192.168.1.1 Port: 80 ist äquivalent mit
Haus: Hauptstrasse 29 Stockwerk: 3. Etage

Funktionsweise eines Portscans:
- Zielrechner wird »abgetastet«, es wird ermittelt welche Dienste der Computer anbietet.
- dient in der Regel der Informationsgewinnung über ein Zielsystem
- fast immer Vorbereitung für einen Angriff
- Aber: Ein Portscan selbst ist kein Angriff

Beispiel für das Resultat eines Scans gegen guardian.calmaryth.net:

Port	State	Protocol	Service
21	open	tcp	ftp
22	open	tcp	ssh
23	open	tcp	telnet
25	open	tcp	smtp
37	open	tcp	time
79	open	tcp	finger
80	open	tcp	http
110	open	tcp	pop−3
111	open	tcp	sunrpc
113	open	tcp	auth
119	open	tcp	nntp
139	open	tcp	netbios−ssn
513	open	tcp	login
514	open	tcp	shell
515	open	tcp	printer
3128	open	tcp	squid−http

6.2 Denial−of−Service Angriffe (DoS−Angriffe)

Was ist Denial−of−Service?
- Ausschalten eines Zieldienstes oder eines gesamten Systems durch Manipulation
- Einfachste Angriffsform, da hier »nur« kaputt gemacht wird
- Meist von sog. »Skript−Kiddies« ausgeführt, denen das Wissen für aufwendigere Techniken fehlt −−> gefährlich, da diese meist die tatsächlichen Folgen (hohe Verluste) nicht richtig einschätzen können

Beispiele:
- Denial−of−Service Angriff auf ein Auto durch Ausbau der Batterie −−> Auto lässt sich nicht mehr starten (erst nach Einbau einer neuen Batterie)
- (Primitiver aber wirksamer) DoS Angriff auf einen Computer durch Ziehen des Netzsteckers −−> Computer versagt den Dienst

6.3 Spezialfall: Distributed−Denial−of−Service (DDoS)

Was ist Distributed−Denial−of−Service?
- Gleiche Funktionsweise wie DoS jedoch:
- Angriff erfolgt gleichzeitig von mehreren (sehr vielen) Seiten aus

Beispiele:
- DDoS Angriff auf das öffentliche Abwassersystem durch gleichzeitiges Ziehen der Klospülung aller Haushalte im Ort
  −−> Folge: Abwassersystem ist überlastet und »nimmt keine weiteren Aufträge an«
- DDoS Angriff auf ein Flugzeug durch gleichzeitiges Hochspringen aller Passagiere −−> Absturz (wörtlich) des Zielsystems (=Flugzeug)

- Angriff im letzten Jahr (2000) auf mehrere grosse Internetdienstleister durch massenhaftes Senden von Anfragen von tausenden Rechnern aus (in Verbindung mit Trojanischen Pferden)
  −−> Massive (Image−) Verluste in der IT−Industrie
  Eingesetzte Programme: Stacheldraht, TFN (Tribe Flood Network)...

6.4 Sniffing

Was ist sniffing?
Mithören von Verbindungen zwischen zwei Rechnern
- Auffangen von sensiblen Daten (z.B. Passwörter)

Funktionsweise von sniffing:
- Weitgehend automatisiert durch Programme (tcpdump, Iris, ...)
- Leicht durchführbar auch ohne Kenntnisse

Übliche Szenarien:
- Mithören (»promiscuous mode«) im lokalen Netz (z.B. gleicher Hub)
- »Man in the middle« sieht Kommunikation, die über seinen Rechner läuft (z.B. Gateway) ein und kann ggf. die Kommunikation auch verändern
- Nutzung von hochspezialisierten Programmen zum gezielten Abhören auf einzelne Daten (Beispiel: L0phtCrack sucht nach Passwortsequenzen zur Anmeldung auf Microsoft−Servern)

6.5 Spoofing

Was ist spoofing?
- Fälschen der Angaben des Urspungsortes (»decoy host«)
  Beispiel: Senden eines Briefes unter falschem Namen
- IP−spoofing: Fälschen der Ursprungs−IP−Adresse

Übliche Szenarien:
- Verschleierung des Ursprungsortes von z.B. Portscans oder Angriffen
- Täuschung von Sicherungssystemen
  Beispiel: A vertraut B, C gibt sich als B aus −−> A vertraut C
- Indirekter Angriff auf die gespoofte Adresse
  Beispiel: C gibt sich als B aus und greift A an −−> A schlägt gegen B zurück (z.B. mit Hilfe eines sog. »Strike−back Firewallsystems«)
  −−> B ausgeschaltet (bei (D)DoS−Attacken nutzbar)

6.6 Exploits

Was sind exploits?
- Exploits (engl.: »to exploit« = ausbeuten) sind bestimmte Angriffe (meist automatisiert in Form von Skripten oder kleinen Programmen), die sich Implementierungsschwächen in Software zu Nutze machen.
- viele Exploits setzen auf Hintertüren auf, die (früher) in Software eingebaut wurden (z.B. für Fernwartung)

Anwendung von exploits:
- Angreifer informiert sich mit z.B. erweiterten Portscans (sog. »Bannerscans«) über die auf dem Zielsystem installierten Programme
- ist ein Programm mit bekannter Schwachstelle dabei, kann ein Exploit genutzt werden
- meist führt dies zur vollständigen Kontrolle über das Zielsystem

Funktionsweise von (remote) exploits:
- Buffer overflows senden mehr Daten als (z.B. in Parametern) erlaubt an das Zielsystem und erzeugen einen »kontrollierten Absturz«, nach dem dem Angreifer eine Benutzeroberfläche zur Verfügung steht (grob skizziert)
- Format string Angriffe nutzen Programmierfehler aus, um durch den Einsatz von (C−spezifischen) Format−Optionen eine Benutzeroberfläche zu erhalten
- viele weitere Formen denkbar

Beispiele:
- Einwurf von geringwertigen ausländischen Münzen in deutschen Zigarettenautomat zum »günstigen Erwerb« von Zigaretten
- Format−String−Vulnerability im Bind 8 DNS−Server

6.7 (Inter−)Aktive Inhalte von Internet−Angeboten

Was sind aktive Inhalte?
- Aktive Inhalte sind kleine Programme oder Animationen
- »Aufpeppen« von Webseiten
- Realisierung interaktive Elemente wie z.B. Online−Banking

Funktionsweise aktiver Inhalte:
- Plug−Ins erweitern die Funktionen des Webbrowsers
- Funktionen dieser Plug−Ins werden über Skripte oder (binäre) Dateien genutzt

Beispiele:
- Programme in Java (Online−Banking)
- Javascripts (Besucherzähler, Datumsanzeige)
- Macromedia Shockwave / Flash (Animationen, Musik)
- Microsoft Active−X Applets
- ...

6.8 Gefahren durch aktive Inhalte

(Radio−)Active−X

Anfang 1997 gelang es dem Chaos Computer Club, mittels eines Active−X Applet auf einer Webseite den gesamten Computer des Opfers so fernzusteuern, dass Banktransaktionen (mittels Quicken) in dessen Namen getätigt wurden (natürlich für den Benutzer unsichtbar).
Sicherheitsrisiko: hoch

Java:

Ende 2000 wurden Fehler in der Netscape−Version des Java−Plugins gefunden (Java Virtual Machine), die den vollständigen Dateiaustausch mit dem Rechner des Opfers erlaubten (ohne dessen Wissen)
Sicherheitsrisiko: hoch

Shockwave / Flash:

Galt als sicher bis Januar 2001.
Seitdem ist eine massive Verwundbarkeit durch Buffer−Overflows bekannt.
Sicherheitsrisiko: hoch

6.9 Social Engineering

Was ist Social Engineering?

- Täuschen eines Opfers im persönlichem Kontakt (z.B. per Email oder Telefon)

Funktionsweise:

Dem Opfer wird eine Email unter falschem Namen (siehe Kapitel 1) gesendet, in der es zu einer vom Einbrechenden gewollten Handlung verleitet wird (Herausgabe von Daten, Vornehmen von Änderungen am PC)

Beispiele:

- Ein »Administrator« fordert per Email dazu auf, das Benutzerkennwort auf »Mohrhuhn« zu ändern
- Die »Abteilung IT« fordert per Telefon dazu auf, schnellstens das Programm »xy« von der Adresse »xy.foobar.org« zu installieren.

6.10 Täuschung durch falsche Domain−Namen

Funktionsweise:

- Beispielbank hat unter www.beispielbank.de ihr Online−Banking Angebot (Zugriff mit PIN)
- Angreifer kauft die Adresse www.beispiel−bank.de und hinterlegt eine gleichaussehende Seite. Gibt der Benutzer nun seine PIN ein, erhält diese der Angreifer
- Täuschung ist beliebig ausbaubar (TAN−Tricks, Verschleierung durch Links auf das Orginal, volle Funktionalität)
- Aber: Fällt natürlich schnell auf (Alternative: Aufhacken des Web(!)−Servers der Bank (meist von Online−Banking Server getrennt)).

6.11 Falsches Vertrauen

Gesicherte Datenverbindungen via Internet werden mit Hilfe von
a) Verschlüsselungstechniken (SSL, SSH)
b) sog. Zertifikaten hergestellt.

In Zertifikaten garantiert eine bekannte Zertifizierungsstelle (Certification Authority = CA) für die Integrität des Dienstleisters und dessen Webangebot / Verschlüsselungssystem.

Beispiele für CAs sind: IKS Jena, Verisign, CCC (private CA)

Die selbe Zertifikat−Technik kommt auch bei (z.B. Java−)Zusatzprogrammen zum Einsatz, wo vertrauenswürdige Applets erweiterte Privilegien haben.

Was versteht man unter »falschem Vertrauen«?
- Dem Besucher einer Seite wird durch falsche oder abgelaufene Zertifikate eine nicht−existente Sicherheit vorgespielt.

Beispiel:
- Nicht vertrauenswürdige Applets mit gefälschten Zertifikaten übernehmen die Kontrolle über ein Zielsystem.

6.12 Spyware

Was ist Spyware?
- Software (oftmals sog. Free− oder Shareware), die nach der Installation und/oder während des laufenden Betriebes Verbindungen zur Herstellerfirma aufbaut und Daten dorthin übermittelt.

Funktionsweise
- Spyware nutzt existierende Internetverbindungen (den sog. Backchannel) zum Übertragen von Daten
- übertragenen Daten sind z.B. eine Liste installierten Software u.ä.

Beispiele:
- Aureate/Radiate
- Naviant
- DownloadAccel

6.13 Cookies

Was sind Cookies?

- Kleine (Text−)Dateien, die von Webseiten unter Benutzung des Browsers auf der Festplatte des Surfenden gespeichert werden

Funktionsweise:

- HTML−Quellcode der Webseite platziert (meist über Javascripts) den Cookie auf der Festplatte und kann diesen (bei Kenntnis des Namens) auch wieder auslesen.

Beispiele:

- Persönliche Begrüßung bei Amazon.de (»Willkommen Hans Meier«)
- Versionsabfrage bei Dilsberg−Systems.com (»Seit Ihrem letzten Besuch haben wir die Seite aktualisiert«)

7. Sicherheitskonzepte

Zum Schutz vor den genannten Risikofaktoren existieren Lösungen und Lösungsansätze, die teilweise schon als Software implementiert sind.

7.1 Schutz vor Viren und Trojanischen Pferden

Software:
- Gängige Virenscanner von diversen Firmen (Symantec, McAfee...)
- Komplette Security−Pakete (Norton Internet−Security...)
- Gezielte Scanprogramme, die speziell auf einen Virus zugeschnitten sind (Anti−CIH)

Einschätzung:
- Ein Virenscanner gehört zwanghaft zur Ausstattung jedes (Windows−)PC, das Verbreiten von »alten« Viren kann dadurch gestoppt werden
- Bei der Wahl sollten besonders die einfache und schnelle Verfügbarkeit von Updates berücksichtigt werden
- Aber: Virenscanner erkennen nur bekannte Viren, neue Viren werden meist nicht erkannt (da die heuristischen Suchverfahren oftmals nicht greifen)

Benutzer:
- Hinterfragen der Notwendigkeit einer Software (»Brauche ich das wirklich?«)
- Woher beziehe ich meine Software? (Privater Server einer unbekannten Firma? Wie seriös ist der Anbieter?)
- Vorsicht bei Share− und Freeware!
- Illegale Downloads, sogenannte »Warez« bringen das größte Risiko mit sich, da im Schadensfall niemand haftbar gemacht werden kann

Einschätzung:
- Wichtig ist: »Erst denken, dann installieren«

7.2 Schutz vor aktiven Angriffen

Software:
- Firewalls (Ipchains, (Veloci−)Raptor, Firewall 1, Pix...)
- »Personal Firewalls« (Zonealarm, BlackIce Defender, Norton...)
- Verschlüsselungsprogramme (PGP...)

Einschätzung:
- Firewalls sind wichtig, jedoch sehr schwer zu konfigurieren
- »Personal Firewalls« sind gefährlich
- Verschlüsselung ist wichtig, jedoch sollte man auch hier auf die Qualität des Produktes achten (Sicherheitslücken in PGP)

Benutzer:
- Pflege und Absicherung der Installation ist notwendig
- Installation von Updates und Patches:
  Betriebssystem auf dem neuesten (Sicherheits−)Stand halten
- Keine Installation von Software mit bekannten Sicherheitslücken
- Kein Anbieten von (Netzwerk−)Diensten, die nicht benötigt werden
- Vorsicht bei der Wahl des (Server−)Betriebssystems
- Vorsicht bei der Weitergabe von Daten (z.B. an Geschäftspartner)

Einschätzung:
- Ein gut informierter Benutzer/Systemverwalter ist durch KEINE Software zu ersetzen
- Installation von Firewalls sind bei Dial−Up Verbindungen sinnvoll, bei Standleitungen obligatorisch
- Externe Begutachtung (sog. »Auditing«) verhindert Betriebsblindheit

7.3 Schutz vor aktiven Inhalten von Webseiten

Software:
- Filter, die aktive Komponenten filtern

Einschätzung:
- Filter lassen sich austricksen
- Filterung von Inhalten jeder Art ist prinzipiell Unfug (Details in der Zusammenfassung)

Benutzer:
- Risikovermeidung durch »richtige« Konfiguration des Internetbrowsers
- Ausschalten von nicht benötigten Elementen (»Ich brauche kein Java« −−> Java ausschalten)
- Hohe Sicherheitseinstellungen bei Internetbrowsern führen zu häufigen Nachfragen an den Benutzer und schaffen einen Überblick über Aktivitäten im »Hintergrund«

Einschätzung:
- Mit relative wenig Fachwissen lässt sich ein Browser gut absichern
- Beste Taktik: Ausschalten aller Zusatzfunktionen und selektives Aktivieren

7.4 Zusammenfassung Sicherheitskonzepte

- Gesellschaftliche Probleme lassen sich durch Technik nie vollständig lösen
- Ein informierter und aufmerksamer Benutzer/Administrator kann jede Software ersetzen und übertreffen
- Vorsicht ist besser als blindes Vertrauen auf vorformulierte Lösungen
- Regelmäßiges kritisches Auditing hält das Problembewußtsein wach

8. Diskussion

9. Quellen und Links

Empfohlene Internet−Links:

Chaos Computer Club	www.ccc.de
L0pht Heavy Industries	www.l0pht.com
Microsoft	www.microsoft.com
Rootshell	www.rootshell.com
Rüdiger Weis	www.informatik.uni−mannheim.de/~rweis/
Initiative Sicherheit im Internet	www.sicherheit−im−internet.de
Systems Internals	www.sysinternals.com
Internet−Browser−Analyse	www.privacy.net/anonymizer
Bundesamt für Sicherheit in der IT	www.bsi.de
Felix von Leitner	www.fefe.de
Team Teso	www.team−teso.net
IKS Jena	www.iks−jena.de

(Stand 05.02.01)

Empfohlene Literatur:

Kryptoanalysis

Adi Shamir, Nicko van Someren: Playing hide and seek with stored keys
Adi Shamir: Factoring large numbers with the TWICKLE Device
Bruce Schneier: Angewandte Kryptographie (ISBN: 3−89319−854−7)

Verschlüsselung

Amtsblatt EU Rahmenbedingungen für elektronische Signaturen
Berufskammer der Steuerberater et al: Feldversuch Elektronischer Rechtsverkehr ()
Bundeswirtschaftsminister Dr. Werner Müller: Mehr verschlüsseln!
Presseerklärung über Förderung des Projektes ”Open Source und IT− Sicherheit (Berlin, 18.11.99)

Firewalls und IDS Systeme

Linux Firewall How−To
BSI−Empfehlungen zum Schutz vor verteilten Denial of Service− Angriffen im Internet
Dr. Stefan Wolf et al: Erkennung und Behandlung von Angriffen aus dem Internet
Andreas Bonnard, Christian Wolff: Gesicherte Verbindung von Netzen mit Hilfe einer Firewall
Kurt Seifried: Linux Administration Security Guide
debis IT Security Services: Grundlagen, Forderungen und Marktübersicht für IDS und IRS
BSI−Cert: Sicherheit beim Betrieb von Web−Servern
Dr. K. Fuhrberg, BSI: Sicherheit im Internet

LAN− und WAN−Sicherheit

van Hauser / THC: How to cover your tracks in the internet
Secure Networks Inc. : A simple TCP spoofing attack
Trend Micro: Corporate Virus Protection
Dan Farmer, Wietse Venema: Improving the Security of Your Site by Breaking Into it
Felix von Leitner, Convergence: IP Version 6
Felix von Leitner: Routing in IP Netzen
Felix von Leitner, Code Blau Security Concepts: TCP−IP Penetrationsmöglichkeiten
»Bavaria Tommy«”: Makrovirus Melissa
»Cyberdemon_98«”: Short Hacking Guide
(Tsutomu Shimomura: How Mitnick hacked Tsutomu Shimomura with an IP sequence attack) mit Vorbehalt

Sonstiges

Detlef Kröger, Marc A. Gimmy: Handbuch zum Internetrecht (ISBN: 3−540−65418−6)
Michael Kofler: Linux Installation, Konfiguration und Anwendung (ISBN: 3−8273−1475−5)
Anonymous: Linux hacker’s guide (ISBN: 3−8272−5622−4)

Die angegebenen Dokumente finden Sie meist über Suchmaschinen direkt im Internet. Teilweise sind die Texte unter Pseudonymen veröffentlicht, der genaue Autor ist in diesem Fall nicht bekannt. Bei Büchern ist die ISBN−Nummer mit angegeben.

Weitere Informationen finden Sie auf unserer Webseite **www.calmaryth.com**