Anhang G

Glossar, Abkürzungen

Als Nachschlagewerk für den Bereich Informationstechnologie empfiehlt sich das über 3000 Seiten umfassende, regelmäßig aktualisierte Loseblattwerk: »Informationstechnologie von A–Z« aus dem INTEREST-Verlag, siehe: `www.interest.de`

ActiveX

Von Microsoft entwickelte Programmiersprache als Antwort auf →Java und →JavaScript. Der Programmcode (ActiveX Control) wird mit einem ActiveX-fähigen →Browser von einem →Web-Server geladen und auf dem lokalen Rechnersystem ausgeführt.

AES

= Advanced Encryption Standard, neuer Standard für →symmetrische Verschlüsselungsverfahren, →Rijndael-Algorithmus

AOL

= America Online; Onlinedienst und Internet-Provider

AP

= Authentication Process

Applet

In →Java geschriebener Programmcode, der auf dem lokalen Rechnersystem innerhalb einer eigenen Umgebung ausgeführt wird.

Application Gateway

Das Rechnersystem, auf dem ein oder mehrere →Proxies realisiert sind.

ARPA

= Advanced Research Projects Agency

ARPANET

= Advanced Research Projects Agency Network; weltweit erstes Datennetz, basierend auf paketorientierter Datenübertragung. Aus dem ARPANET entstand das heutige →Internet.

ASP

= Application Service Provider, stellt outgesourcte IT-Infrastruktur (Hardware, Software, Litenzen) zur Verfügung

Asymmetrische Verschlüsselung

auch Public-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem zwei verschiedene Schlüssel eingesetzt werden. Mit dem einen der beiden Schlüssel werden die Daten oder das Dokument verschlüsselt und/oder signiert, und die Entschlüsselung/Prüfung kann nur mit dem entsprechenden anderen Teilschlüssel erfolgen. Hierzu werden Algorithmen aus der Komplexitätstheorie verwendet.

Asynchroner Transfermodus

Der Asynchrone Transfermodus (ATM) ist ein Datenübertragungsverfahren, das die →Bandbreite erheblich steigern kann. Es ermöglicht das gleichzeitige Übertragen von Daten aus verschiedenen Quellen und kann so die Übertragungskapazitäten optimal ausnutzen. Damit kann eine Bandbreite von bis zu 2,3 GBit erzielt werden.

ATM

= →Asynchroner Transfermodus

Authenticode

Kontrollverfahren für die Anwendung von →ActiveX controls. Ein Programmierer von ActiveX controls hat den Zugriff auf sämtliche Systemressourcen und besitzt damit die gleichen Rechte wie der gerade angemeldete Anwender. Um einen Mißbrauch zu verhindern, kann mit der Authenticode-Technologie die Herkunft der verwendeten ActiveX controls durch digitale Signatur nachgewiesen werden.

Authentikation

Authentikation bedeutet die Verifizierung (Überprüfung) der Echtheit bzw. der Identität einer Person oder Sache. Eine Authentikation kann benutzerorientiert (→Benutzerauthentikation) oder rechnerorientiert (anhand der Rechneradresse) durchgeführt werden.

B2B

= Business-to-Business, Applikation, bei der Rechnersysteme unterschiedlicher Firmen untereinander automatisch Geschäftsabläufe abwickeln

Backdoor

= Hintertür; eine versteckte bzw. undokumentierte Programmfunktion, mit deren Hilfe vom Benutzer nicht autorisierte Personen auf dessen Rechnersystem bzw. die darauf gespeicherten Daten zugreifen können (vgl. →Trojanisches Pferd)

Bandbreite

Mit Bandbreite bezeichnet man die Datenmenge, die ein bestimmter Leitungstyp pro Zeiteinheit transportieren kann. Eine analoge Telefonleitung etwa hat eine Bandbreite von ca. 56 KBit, eine ISDN-Leitung schafft 64 KBit, bzw. im Duplex-Betrieb 128 Kbit das Ethernet 10 MBit, das Fast Ethernet 100 MBit. Ein →ATM schließlich erreicht eine Bandbreite von bis zu 2,3 GBit.

Bastion

→Application Gateway, der als einziges Rechnersystem aus dem unsicheren Netz angesprochen werden kann.

BDSG

= Bundesdatenschutzgesetz

Benutzerauthentikation

Die →Authentikation ist an den Benutzer gebunden. Dazu exisitieren bei Firewall-Systemen verschiedene Authentikationsmechanismen, z. B.:

- Eingabe von User-ID und Paßwort
- S/Key
- Token (Challenge/Response)
- Chipkarten.

Biometrie

Biometrische Authentikationsverfahren benutzen unverwechselbare physikalische Besonderheiten des Anwenders wie Fingerabdruck oder Gesichtscharakteristika zu seiner Authentifizierung.

Blowfish

→symmetrisches Verschlüsselungsverfahren, unterlag dem →Rijndael-Algorithmus beim Wettstreit um den neuen Advanced Encryption Standard (→AES)

Browser

Browser nennt man die Software, mit der Internet-Seiten gelesen werden können. Der Browser greift über das HyperText Transfer Protocol (→HTTP) auf Web-Server zu. Dokumente werden im HTML-Format vom Browser interpretiert und dem Benutzer inklusive der Bilddaten dargestellt. Geläufige Browser sind z. B. Netscape Navigator, MS Internet Explorer und Lynx.

Brute-Force-Attack

Beim →Hacking von kryptographischen Schlüsseln oder Passworten kann man unterschiedlich raffiniert vorgehen. Man kann beispielsweise versuchen, Anhaltspunkte zu finden und auszuwerten. Brute-Force (rohe Gewalt) bezeichnet dagegen die primitivste Art des Angriffs: man probiert einfach blindlings alle denkbaren Möglichkeiten durch. Ein solcher Angriff ist heute nicht mehr vielversprechend: Wer per Brute-Force-Attack einen 128-Bit-Schlüssel ermitteln will, braucht voraussichtlich ein Vielfaches der Lebenszeit unseres Sonnensystems.

BSI

= Bundesamt für Sicherheit in der Informationstechnik, siehe auch: `www.bsi.de`

CA

= Certification Authority; Zertifizierungsstelle, die Benutzerschlüssel als Zertifikat (elektronischer Ausweis) ausgibt. Die Zertifikate dienen zum einen der authentischen Übermittlung von Daten und zum anderen der Identitätsprüfung des Urhebers.

CCITT

= Comité Consultatif International Télégraphique et Téléphonique

CERT

= Computer Emergency Response Team; Aufgabe des CERT ist es unter anderem, als Internet-Feuerwehr schnell und effizient auf kritische Vorfälle (z. B. Hacker-Angriffe, Sicherheitslücken, Viren etc.) zu reagieren und Hilfe zu leisten und Informationen aufzubereiten und bereitzustellen. In Deutschland wird das CERT vom →DFN unterstützt.

CGI

= Common Gateway Interface; Programmschnittstelle zwischen beim Web-Server eingehenden Benutzerdaten (z. B. ausgefüllte Formulare) und angeschlossenen Programmen wie z. B. Datenbanken. Mit Hilfe von CGI-Skripten kann man Web-Seiten dynamisch gestalten und mit interaktiven Elementen versehen.

Chiffrierfehler

Wenn bei der Anwendung oder Konzeptionierung eines Verschlüsselungsverfahrens Pannen oder Nachlässigkeiten passieren, spricht man von Chiffrierfehlern. Sie haben in der Regel zur Folge, daß die erzeugten Schlüssel weniger komplex sind bzw. aus einer kleineren Menge von Kombinationen hervorgehen, als technisch möglich wäre.

Common Point of Trust

Einziger Übergang zwischen unterschiedlichen Netzen, der als vertrauenswürdig angesehen und mit Hilfe eines Firewall-Systems realisiert wird.

Content Security

Internet-Dokumente (HTML-Seiten, E-Mails) sind durch Schadensprogramme →Malware gefährdet

Cookies

Informationen, die der →Web-Server im →Browser des Clients ablegt, beispielsweise eine Kundennummer, über die der Benutzer bei einem Folgebesuch der Website identifiziert werden kann.

Corporate Network

Unternehmen und Behörden bauen mit Knoten, Routern und Multiplexern ihre eigenen Kommunikationsnetze, sogenannte »Corporate Networks«, auf.

Cracker

→Hacker, der unbefugt in fremde Computersysteme eindringt und gespeicherte Daten und Programme in böser Absicht manipuliert oder inspiziert: also mit krimineller Energie bzw. für persönlichen Vorteil.

CRL

= Certification Revocation Lists; Schwarze Liste von Zertifikaten (Benutzern), die in einem →TrustCenter geführt wird.

Daemon

Ein UNIX-Prozess, der im Hintergrund abläuft und nur bei Bedarf aktiviert wird. Typische Daemons sind z. B. ftpd (→ftp-Daemon) und httpd (→http-Daemon).

DECNET

Von Digital Equipment Corporation (DEC) entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme.

Denial of Service

Denial of Service bedeutet soviel wie Funktionsausfall oder Funktionsverweigerung. Dahinter verbirgt sich eine Vielzahl verschiedener Angriffsmöglichkeiten, die alle das Ziel haben, Internetrechner zum Absturz zu bringen oder in bestimmten Funktionen lahmzulegen. Klassische Beispiele sind das Mail-Bombing – das geplante Überlasten eines Mail-Empfängers mit einer Unzahl von E-Mails – oder das Versenden von »Nukes«, das sind IP-Pakete, die ungesicherte Betriebssysteme kurzerhand zum Absturz bringen.

DENIC

= Deutsches Network Information Center; Sitz in Karlsruhe; unter anderem für die Vergabe von →Domain-Namen mit der Endung ».de« zuständig, siehe auch: www.denic.de

DES

= Data Encryption Standard; eines der bekanntesten und am meisten verbreiteten und untersuchten symmetrischen Verschlüsselungsverfahren. Der DES wurde 1976 in den USA normiert (ANSI X3.92). Der DES-Algorithmus hat ursprünglich eine Länge von 64 Bit, wovon 56 signifikant sind. Der DES-Algorithmus wird heute meist als Triple-DES mit 128-Bit →effektiver Schlüssellänge verwendet.

DFN

= Deutsches Forschungsnetz; Der DFN-Verein war am Aufbau des deutschen Wissenschaftsnetzes →WIN beteiligt und unterstützt das →CERT in Deutschland (DFN-CERT).

Diffie-Hellman

Verfahren zum Austausch eines geheimen Schlüssels über öffentliche Netzwerke

Digitale Signatur

Die Digitale Signatur garantiert den Ursprung einer Software, einer Nachricht oder sonstiger Daten. Die Digitale Signatur entspricht also einer eigenhändigen Unterschrift, die den Absender eindeutig identifiziert sowie sicherstellt, daß die empfangenen Daten nicht verfälscht wurden. Technisch basiert die Digitale Signatur auf der →asymmetrischen Verschlüsselung, d. h. dem Public-Key-Verfahren.

Digitales Zertifikat

Wer remote seine Identität nachweisen möchte – etwa durch eine Chipkarte und Eingabe einer PIN –, beruft sich damit auf eine Instanz, die dokumentiert, daß mit dieser Chipkarte und PIN auch genau diese Person verbunden ist. Diese Instanz –

Zertifizierungsinstanz bzw. →Certification Authority (CA) – bürgt für die Authentizität des Kartenbesitzers und dokumentiert diese durch ein Zertifikat. Dieses Zertifikat – in digitaler Form – dient Organisationen, die remote access zulassen, als 'Ausweis' für den User.

DMZ

= De-Militarised Zone; ein entkoppeltes, isoliertes Teilnetzwerk, das zwischen das zu schützende Netz und das unsichere Netz geschaltet wird.

DNS

= Domain Name Service; Internet-Dienst, mit dessen Hilfe die→IP-Adressen der Hosts den entsprechenden →Domainnamen und umgekehrt zugeordnet werden können. Sogenannte DNS-Server verwalten die Datenbanken mit den Adressen.

Domainnamen

Untergliederungseinheit der hierarchisch aufgebauten und weltweit eindeutigen Namen von Rechnersystemen im Internet. Die Domainnamen müssen bei den zugehörigen Verwaltungsstellen (→NIC, →DENIC) beantragt werden.

DSA

= Digital Signatur Algorithm, staatlichen Signaturverfahren in den USA, arbeitet u. a. mit dem Algorithmus →ElGamal

E-Business

= Electronic Business, Abwicklung von Geschäftsvorgängen über elektronische Medien wie das Internet

E-Commerce

= Electronic Commerce; umfaßt im Prinzip alle Schritte von Geschäftsprozessen, die auf elektronischem Wege vollzogen werden. Im Mittelpunkt stehen dabei zunächst die Möglichkeiten, sich online über Produktangebote zu informieren und Bestellungen vorzunehmen. Aber auch die Zahlung vom heimischen PC aus – Online Banking – wird bald zum E-Commerce-Alltag gehören. Und bei Zahlungen gilt noch mehr als bei Bestellungen: es muß sichergestellt sein, daß der Auftraggeber eindeutig identifizierbar ist und daß kein Unbefugter in die Transaktionen Einblick erhält.

Effektive Schlüssellänge

Werden Verschlüsselungsverfahren mehrfach durchlaufen, kann man nicht einfach die Schlüssellänge multiplizieren. Die Kryptologen haben deshalb den Begriff »effektive Schlüssellänge« eingeführt. Beispiel Triple-DES: Bei dreimaligem

Durchlauf mit je 56-Bit Schlüssellänge entspricht die Sicherheit des Verfahrens nicht etwa einer einmaligen Verschlüsselung mit der Schlüssellänge von 3 * 56-Bit = 168 Bit, sondern ist mit 128 effektiver Schlüssellänge geringer.

ElGamal

→asymmetrisches Verschlüsselungsverfahren

E-Mail

Elektronische Post; Austausch von Textnachrichten und Computerdateien über ein Kommunikations-Netzwerk, z. B. lokales Netzwerk oder das →Internet.

Ethernet

Das Ethernet wurde ursprünglich von Xerox für die Verknüpfung von Minicomputern im Palo Alto Research Center entwickelt. Inzwischen ist Ethernet eine weit verbreitete Technik zum Vernetzen von Rechnern in einem →LAN.

Extranet

Extranet heißt der Informationsaustausch zwischen →Intranets von Geschäftspartnern via →Internet (→TCP/IP basierend).

Finger

Internet-Dienst zur Ermittlung und zur Verwaltung der Benutzerinformationen eines Rechnersystems. Die dazugehörige Software ist standardmäßig Bestandteil jedes UNIX-Betriebssystems.

FTP

= File Transfer Protocol; Internet-Dienst zur Übertragung von Dateien

Gateway

Mit Gateway bezeichnet man die Verbindung zwischen zwei Netzen oder Teilnetzen, z. B. das »Tor«, durch das Daten aus dem →Internet in ein lokales Netz gelangen. Gateways arbeiten auf Schicht 7 des ISO/OSI-Modells und können zwei oder mehr Netze mit völlig verschiedenen Protokollen verbinden. Für die Informationssicherheit ist das Gateway der neuralgische Punkt – hier installiert man eine →Firewall, um aus dem Gateway ein →»Secure Gateway« zu machen.

GDD

= Gesellschaft für Datenschutz und Datensicherheit

Gopher

Internet-Dienst, der Textinformationen in Form von hierarchisch verschachtelten Auswahlmenüs strukturiert.

GSM

= Global System for Mobile Communications; Standard für digitale Mobilfunknetze.

Hacker

Als Hacker werden allgemein Anwender bezeichnet, die sehr vielfältige Kenntnisse im Umgang mit der Computertechnologie und Computerprogrammierung besitzen und sich oft damit beschäftigen. Der Begriff wird auch häufig für Personen verwendet, die sich unbefugten Zugang zu fremden Computersystemen verschaffen. Das Hacking sollte man aber keinesfalls mit Computersabotage, Computerspionage oder Computerbetrug gleichsetzen. Viele Hacker arbeiten aus sportlichen oder wissenschaftlichen Motiven und machen ihre Erkenntnisse der Öffentlichkeit zugänglich, was der Entwicklung von Sicherheitsmechanismen zugute kommen kann. Im Gegensatz zum →Cracker »arbeiten« Hacker also ohne kriminelle Energie bzw. nicht für persönlichen Vorteil.

Hacking

→Hacker

HMAC

Algorithmus, der eine →One-Way-Hashfunktion mit Verschlüsselung kombiniert und so eine digitale Signatur eines Dokumentes erzeugt

HTML

= HyperText Markup Language; Seitenbeschreibungssprache, mit der Elemente (Texte, Grafiken, →Hyperlinks, etc.) der Web-Seiten einfach formatiert werden können. HTML ist das derzeit wichtigste im WWW verwendete Dateiformat.

HTTP

= HyperText Transfer Protocol; Internet-Dienst, mit dem Daten zwischen →Web-Server und →Web-Browser ausgetauscht werden.

Hyperlink

Ein mit Hilfe von →HTML markierter Querverweis in einer Web-Seite auf eine Informationsquelle (→URL) im World Wide Web. Durch Aktivierung eines Hyperlinks z. B. per Mausklick wird der Benutzer zu dieser Quelle geführt, wobei er von →Web-Server zu Web-Server geleitet werden kann.

ICMP

= Internet Control Message Protocol; Ein Internet-Protokoll der Netzwerkschicht, welches eine Fehlerkorrektur und andere Informationen liefert, die für die IP-Paketverarbeitung von Bedeutung sind.

IDEA

= International Data Encryption Algorithm; 1990 von Lai und Massey als Alternative zum →DES vorgestelltes →symmetrisches Verschlüsselungsverfahren mit 128 Bit Schlüssellänge.

IKE

= Internet-Key-Exchange, Verfahren zum Austausch von Schlüsseln, Standardverfahren für →IPSec

Internet

Das Internet ist ein weltweites, dezentrales Rechnernetz, das auf dem →TCP/IP-Protokoll basiert. Das Internet ist inzwischen das populärste Netz der Welt mit über 350 Millionen Anwendern (Stand: 2/2001). Es bietet seinen Benutzern zahlreiche Dienste an, wie z. B. →FTP, →E-Mail, →World Wide Web, →Gopher.

Intranet

Internes Netz einer Organisation oder eines Unternehmens, das auf der Internet-Technologie und dem →TCP/IP-Protokoll basiert.

IP

= Internet Protocol; Dieses Netzwerkprotokoll definiert den Aufbau und die Adressierung von Datenpaketen in TCP/IP-Netzwerken.

IP Spoofing

Das Einfügen einer falschen IP-Absenderadresse in eine Internet-Übertragung. Das Ziel dieser Aktion ist der unberechtigte Zugriff auf ein Computersystem.

IP-Adresse

Weltweit eindeutige Adresse eines am Internet angeschlossenen Rechnersystems. Die IP-Adresse besteht aus einem Zahlencode von vier Zahlen von 0 bis 255 (z. B. 192.168.1.2). Die Vergabe erfolgt international vom →NIC bzw. in Deutschland vom →DENIC.

IPRA

= Internet Policy Registration Authority

IPSec

Verfahren zur Erweiterung der normalen →IP-Pakete um →Authentikation und Verschlüsselung, zukünftiger Standard

IPv6

= Internet Protocol Version 6; erweiterte Version des Internet-Protokolls mit vergrößertem Adressraum sowie Funktionen für Sicherheit.

IPX

= Internetwork Packet Exchange; von Novell verwendetes Netzwerkprotokoll. Im Schichtenmodell (→OSI-Modell) ist IPX auf der gleichen Ebene wie das IP einzuordnen.

ISDN

= Integrated Services Digital Network; weltweites digitales Kommunikationsnetzwerk zur integrierten Übertragung von Sprache und Daten.

ISO

= International Organization for Standardization; internationale Vereinigung, in der jedes Mitgliedsland durch die führende Standardisierungsorganisation vertreten ist. Die ISO arbeitet an der weltweiten Vereinheitlichung technischer Standards, u. a. auf den Gebieten der Kommunikation und des Informationsaustausches. Hier ist an erster Stelle das weithin akzeptierte →OSI-Modell zu nennen.

ISS

= Internet Security Systems; amerikanischer Hersteller des Firewall-, Intranet- und Web-Security-Scanners. Die Scanner testen Rechnersysteme auf Schwachstellen, indem sie bekanntgewordene Internet-Angriffe ausführen.

IT

= Information Technology

ITSEC

= Information Technology Security Evaluation Criteria; von Frankreich, Deutschland, Großbritannien und den Niederlanden festgelegte Kriterien für die Zertifizierung von IT-Systemen.

Java

Von Sun Microsystems entwickelte plattformunabhängige Programmiersprache für das Internet. Java-Programme (→Applets) werden von einem →Web-Server auf das lokale Rechnersystem übertragen und dort von einem Java-Interpreter ausgeführt.

Java-Applet

→Applet

JavaScript

Von Netscape definierte und in die HTML-Syntax integrierte Skriptsprache. JavaScript-fähige →Web-Browser interpretieren den in einer Web-Seite enthaltenen Programmcode und führen ihn aus.

Kompromittierung

Kompromittierung ist ein allgemeiner Oberbegriff für alle Formen der Vertraulichkeitsverletzung.

Kryptoanalyse

Ziel der Kryptoanalyse ist die Entschlüsselung von Geheimschriften und Codes. Im Bereich des elektronischen Datenverkehrs kann man Kryptoanalyse als eine Form von →Hacking bezeichnen.

Kryptogesetz

Das sogenannte Kryptogesetz definiert, unter welchen Bedingungen ein kryptographisches Verfahren zur →Verschlüsselung und Signatur von →E-Mails als so sicher gilt, daß der so übermittelte Inhalt rechtsverbindlichen Charakter hat wie ein Dokument auf Papier. Das deutsche Gesetz hierzu hat Pioniercharakter.

Kryptographie

Kryptographie ist der Zweig der →Kryptologie, der sich gezielt mit der Entwicklung von Verschlüsselungs- und Codierungsverfahren befaßt. Diese Wissenschaft ist sehr alt – schon im alten Ägypten beschäftigte man sich mit Geheimschriften. Heute geht es dagegen vorwiegend um mathematische Verschlüsselungsverfahren für den elektronischen Datenverkehr. Auch die →digitale Signatur beruht auf kryptographischen Verfahren.

Kryptographischer Algorithmus

Jedes kryptographische Verfahren beruht darauf, einen verständlichen Text nach bestimmten Regeln in unverständlichen Zeichensalat zu verwandeln. Bei elektro-

nischer Verschlüsselung geschieht dies nach einem bestimmten Algorithmus, wobei die Länge des Algorithmus beeinflußt, wie schwer →Hacker den Text entschlüsseln können. Zur Zeit gelten Schlüssellängen von 128 Bit als sicher.

Kryptographisches Protokoll

Die auf Algorithmen basierenden Verschlüsselungsverfahren müssen in die technologischen Gegebenheiten der Datenkommunikationsstrukturen eingebunden werden – dafür sorgt ein kryptographisches Protokoll.

Kryptologie

Oberbegriff für →Kryptographie und →Kryptoanalyse

Kryptoregulierung

Kryptoregulierung ist der staatliche Versuch, die Verbreitung und Verwendung leistungsfähiger Verschlüsselungsverfahren einzuschränken. Grund: Die Behörden fürchten, daß zu raffinierte Verfahren die Möglichkeiten zur Verbrechensbekämpfung beschneiden könnten. Die USA leiden unter sehr strikter Kryptoregulierung; in Deutschland konnte ein solches Gesetz verhindert werden.

LAN

= Local Area Network – auf deutsch auch: lokales Netz. Darunter fallen Netzwerke, die einen relativ kleinen, abgegrenzten Bereich umfassen – im Gegensatz zum →WAN.

LDAP

= Lightweight Directory Access Protocol, Protokoll zum Zugriff auf →Verzeichnis-Dienste

MAC

= Media Access Control; Protokoll der Netzzugangsebene

oder

= Message Authentication Code; →One-Way-Hashfunktion

Mailbombe

die unerwünschte Zusendung einer großen Menge von E-Mails (oder einer einzelnen sehr großen E-Mail) an einen bestimmten Empfänger oder eine Gruppe von Empfängern mit dem Ziel, den empfangenden Mailserver (bzw. ein Postfach) zu blockieren

Mailbox

elektronischer Briefkasten; Rechnersystem, das per →Modem angewählt wird und auf dem ein Programm läuft, das dem Benutzer erlaubt, Nachrichten anderer Benutzer zu lesen oder ihnen zu schreiben. Meist besteht zusätzlich die Möglichkeit, Dateien herunter- oder heraufzuladen. (siehe auch →E-Mail)

MailTrusT

Ein →TeleTrusT Projekt, in dem die Interoperabilität vielfältiger technologischer Komponenten und Produkte, die die Anwendung der →digitalen Signatur ermöglichen, durch kompatible Ausführung von Verschlüsselung und gemeinsamer Schnittstelle erreicht wurde.

Malware

Eine besondere Gefahr beim Austausch von Dateien als Anhänge von Mails oder WWW-Dokumenten, ist die Gefahr, daß neben der eigentlichen Information (Daten, Programme) sogenannte Malware (Viren, Würmer, Trojanische Pferde, ...) mitgesendet wird, die im Prinzip immer den Empfänger Schaden soll.

MAZ

Größter deutscher Internet-Provider, Sitz in Hamburg.

M-Business

= Mobile Business, Abwicklung geschäftlicher Vorgänge über Mobiltelefone

M-Commerce

= Mobile Commerce, Handel über elektronische Medien (Internet) unter Einbeziehung von Mobiltetefonen

MD4

→One-Way-Hashfunktion, wird häufig im Microsoft-Umfeld eingesetzt

MD5

Von Rivest entwickelte →One-Way-Hashfunktion zur Unterstützung von Authentikationsverfahren.

Mime

= Multipurpose Internet Mail Standard. Standard zum Verschicken von Multimediadateien bei E-Mails.

Modem

= Modulator/Demodulator; Ein Gerät, das den Austausch von Daten über Drahtleitungen ermöglicht. Die klassische Verwendung nutzt die konventionelle Telefonleitung, um sich ans →Internet anzuschließen und →E-Mails zu verschicken. Es gibt aber auch Modems für ISDN-Leitungen, Fernsehkabel, Stromleitungen, Standleitungen usw.

Modulation

Manche Datenleitungen, etwa die analoge Telefonleitung, werden durch einen ständigen Stromfluß aufrechterhalten – das sogenannte Trägersignal. Die eigentliche Informationsübermittlung geschieht durch geringfügige Schwankungen oder sonstige Veränderungen, also durch Modulation des Trägersignals.

MTA

= Message Transport Agent; Programm, das für die Annahme und Weiterleitung von →E-Mails verantwortlich ist.

Multiplexverfahren

Technik, die es ermöglicht, mehrere separate Signale über eine einzelne Leitung zu übertragen.

Nameserver

→DNS

NCSA

= National Computer Security Association; Verein von Anwendern und Hard- und Softwareherstellern mit dem Ziel, Benutzern bei der Erhöhung der Sicherheit, der Wahrung der Integrität ihrer Informationen und der Reduzierung der Bedrohungen durch Computer-Viren zu unterstützen. NCSA entwickelte Kriterien für die Zertifizierung von Firewall-Systemen.

Netz

Netz oder Netzwerk nennt man eine Gruppe von Computern und angeschlossenen Geräten, die durch Kommunikationseinrichtungen miteinander verbunden sind. Die Netzwerkverbindungen können permanent (zum Beispiel über ein Kabel) oder zeitweilig (etwa über das Telefon oder andere Kommunikationsverbindungen) eingerichtet werden und verschiedene Größenordnungen und Ausdehnungen haben.

NMS

= Network Management System

NNTP

= Network News Transport Protocol; Internet-Dienst, mit dem die News-Artikel transportiert werden.

One-Way-Hashfunktion

Auf eine Nachricht, deren Länge variabel ist, wird eine sogenannte One-Way-Hashfunktion angewendet, die eine kryptographische Prüfsumme fester Länge als Ergebnis erzeugt (z. B. →MD5).

OSI

= Open Systems Interconnection

OSI-Schichtenmodell

auch OSI-Referenzmodell genannt; ein von der →ISO entwickeltes Kommunikationsprotokoll, das allgemeine Regeln für die Kommunikation in Netzwerken enthält.

OTP

= One-Time-Password (Einmal-Passwort); das Konzept »Einmal-Passwort« legt fest, daß ein Passwort nur einmal für eine Authentikation verwendet werden darf.

Passwort

Das einfachste Authentikationsverfahren ist das Passwort-Verfahren. Die Stärke dieses Verfahrens beruht allerdings lediglich auf der Geheimhaltung und der Qualität (Länge/Nichttrivialität) des Passwortes.

PEM

= Privacy Enhanced Mail; in den →RFCs 1421-1424 festgelegter Standard für die Verschlüsselung und Authentizität von →E-Mails.

PGP

= Pretty Good Privacy; ein von Phil Zimmerman entwickeltes Verschlüsselungsverfahren, welches auf →RSA und →IDEA basiert.

Phreaker

Personen, die in Telefonleitungen, Anrufbeantwortern und →Voiceboxen ihr Unwesen treiben.

PIN

= Personal Identification Number; eine Codenummer, die einem berechtigtem Benutzer zugewiesen ist.

PKI

= Public Key Infrastructure, Infrastruktur zur Erstellung und Verwaltung von Schlüsselpaaren und →Zertifikaten

POP3

= Post Office Protocol; Standard zur Übermittlung von →E-Mails.

PPP

= Point to Point Protocol; wird zum Austausch von Datenpaketen per →Modem im →Internet verwendet. Das PPP liegt eine Ebene unter →TCP/IP und kümmert sich nur um die serielle Datenübertragung und ihren Aufbau.

PPTP

Point-to-Point Tunneling Protocol, VPN-Protokoll im Microsoft-Umfeld

Private-Key-Verfahren

→Symmetrisches Verschlüsselungsverfahren

Proxy

Ein Proxy ist ein Stellvertreter des →Servers gegenüber dem Client und ein Stellvertreter des Client gegenüber dem Server. Nach der →Authentikation des Clients bzw. des Servers gegenüber dem Proxy arbeitet dieser für beide Seiten transparent. Proxies existieren für die Dienste →HTTP, →SMTP, →FTP, →Telnet u. a.

Public-Key-Verfahren

→Asymmetrisches Verschlüsselungsverfahren

RC4 / RC5

→Symmetrisches Verschlüsselungsverfahren

Registration Authority

Bestandteil einer →PKI, untergeordnete Institution, die einer →Certification Authority einen Teil der Routineaufgaben abnimmt

Remote access

Mit Remote access wird die Möglichkeit bezeichnet, aus räumlicher Distanz über ein öffentliches Netz Zugang zu einem Rechnersystem oder lokalem Netz zu erhalten und dort agieren zu können. Da Remote access-Verbindungen von Natur aus ein besonders großes Risiko bedeuten, müssen Sicherheitsvorkehrungen getroffen werden, um Authentizität und Vertraulichkeit zu garantieren. Mit Verschlüsselungs- und Zugangskontrollsystemen kann Remote Access gesichert werden.

RFC

= Request for Comment; Textdokumente, die Vorschläge für neue Internet-Standards zusammenfassen.

Rijndael

→symmetrisches Verschlüsselungsverfahren mit einer für die nächsten Jahrzehnte ausreichenden Schlüssellänge, soll das weit verbreitete →DES ablösen

RIP

= Routing Information Protocol; →Router

Router

Router sind Geräte zur Kopplung verschiedener Netze. Sie leiten Datenpakete auf der günstigsten Route »durch das Gewirr der Netzwerke« zu ihrem Ziel. Dabei arbeiten sie meistens auf Schicht 3 des ISO/OSI-Referenzmodells.

RSA

→Asymmetrisches Verschlüsselungsverfahren, benannt nach den Entwicklern Rivest, Shamir und Adleman. Das bekannteste, bewährteste und am besten untersuchte asymmetrische Verfahren.

S/MIME

= Secure Multipurpose Internet Mail Standard.

Um Mechanismen zur Authetication, Verschlüsselung und Signatur erweiterter →MIME Standard

SATAN

= System Administrator Tool for Analyzing Networks; ein Programm zur Überprüfung von IP-Netzwerken. Getestet werden dabei Schwachstellen, die ein Angreifer über das Internet ausnutzen kann, um sich unbefugt Zugang zu einem Rechnersystem zu verschaffen.

Secure Gateway

→Gateway nennt man den Zugang, der ein lokales Netz mit einem öffentlichen Netz verbindet. Wenn der Betreiber des lokalen Netzes kontrollieren will, wer wann unter welchen Bedingungen Zugang zu welchen Diensten erhalten soll, richtet er durch Sicherheitsmaßnahmen einen Secure Gateway ein. Ein Secure Gateway muß v.a. in der Lage sein, die Authentizität von Besuchern zu überprüfen und entsprechende Zugangsrechte zu differenzieren. Größtmögliche Sicherheit bietet hier ein High-level-Firewall-System.

Secure Shell

Telnet-ähnliches Protokoll, das innerhalb von Unix-VPNs Anwendung findet

Security Policy

Eine wohldurchdachte Security Policy bildet die Grundlage für die Sicherheit in Organisationen. Dazu zählen die Definition von Sicherheitszielen, die Bestimmung des Schutzbedarfs der Daten, die Analyse der Kommunikationsstrukturen und anderes mehr. Erst auf dieser Basis können konkrete Sicherheitsmaßnahmen geplant und durchgeführt werden.

Security Token

Ein Security Token ist ein Datenträger (z. B. Chipkarte oder Diskette), mit dem der User seine Zugangsberechtigung nachweisen kann, wenn er die richtige →PIN kennt. Die →Authentikation funktioniert nach dem Challenge-Response-Prinzip: Das Firewall-System, das den Zugriff gewähren kann, stellt eine Challenge, auf die der Security Token eine Response schickt und damit den User authentifiziert.

Server

Ein Server ist ein Rechner innerhalb eines lokalen Netzes, der den anderen Rechnern seines Netzes Informationen zur Verfügung stellt.

SET

= Secure Electronic Transaction, Protkoll aus dem Bereich des →E-Commerce, erlaubt das Bezahlen von Waren und Dienstleistungen über das Internet

SHA

= Secure Hash Algorithm, oft auch SHA-1 genannt, →One-Way-Hashfunktion

S-HTTP

= Secure HTTP; um Kryptographiefunktionen erweiterte Version des Protokolls →HTTP.

SKIP

= Simple Key Management for Internet Protocols, Protokoll zum Schlüsselaustausch, wird beim Einsatz von →IPSec wahlweise anstelle des üblichen →IKE verwendet

SMIB

= Security Management Information Base

SMTP

= Simple Mail Transport Protocol; Internet-Dienst zur Übertragung von →EMails.

SNA

= Systems Network Architecture; von IBM entwickelte und verwendete Kommunikationsarchitektur für Rechnersysteme.

SSL

= Secure Socket Layer; Protokollschicht zum sicheren Transport von höheren Internetprotokollen wie →HTTP.

Symmetrische Verschlüsselung

auch Private-Key-Verfahren genannt; Verschlüsselungsverfahren, bei dem für die Verschlüsselung der Daten der gleiche Schlüssel verwendet wird wie für ihre Entschlüsselung. Die bekanntesten symmetrischen Verschlüsselungsverfahren sind →DES, →AES und →IDEA.

TCP

= Transmission Control Protocol; das Protokoll innerhalb des →TCP/IP, das die Trennung der Datennachrichten in Pakete steuert und die empfangsseitige Zusammensetzung und Überprüfung auf Vollständigkeit der Datenpakete überwacht.

TCP/IP

= Transmission Control Protocol/Internet Protocol; Kommunikations-Architektur im Internet/Intranet. →TCP, →IP

TeleTrusT e.V.

TeleTrusT e.V. – siehe: www.teletrust.de – wurde 1989 gegründet, und hat sich die Förderung von Wissenschaft, Normung und Bildung im Bereich der Entwicklung einer verläßlichen Informations- und Kommunikationstechnik zum Ziel gesetzt.

Im TeleTrusT arbeiten Forschung, Anbieter, Organisationen und Behörden zusammen. Der TeleTrusT war an der Formulierung des deutschen Signaturgesetzes beratend mitbeteiligt.

Trojanisches Pferd

ein unverdächtig erscheinendes Programm, das im Hintergrund vor dem Benutzer verborgene und von diesem unerwünschte Funktionen ausführt, z. B. eine →Backdoor öffnet, gespeicherte Daten verändert oder vertrauliche Informationen sammelt und an einen Server schickt.
Die Bezeichnung »Trojanisches Pferd« geht auf Homers Odyssee zurück: Nachdem die Griechen Troja lange erfolglos belagert hatten, ließen sie ein hölzernes Pferd vor den Stadtmauern zurück, in dem sich ihre tapfersten Soldaten versteckten. Die Trojaner holten das Pferd in die Stadt, in der Nacht öffneten die versteckten Krieger ihren Mitstreitern die Tore und Troja wurde verwüstet.

TrustCenter

→CA

UDP

= User Datagram Protocol; ein verbindungsloses Übertragungsprotokoll für das Internet. Im Gegensatz zum →TCP/IP findet bei diesem Protokoll keine Überprüfung der ordnungsgemäßen Zustellung von Datennachrichten statt.

URL

= Uniform Resource Locator; ein URL bezeichnet die eindeutige Adresse eines Internet-Servers bzw. einer bestimmten Information darauf. Er beinhaltet Angaben wie Typ der Ressource, mit der verbunden werden soll (z. B. →WWW, →FTP, →Gopher), Serveradresse, Portnummer, etc. Ein URL wird im →Browser eingegeben oder durch einen →Hyperlink aktiviert.

USV

= Unterbrechungsfreie Stromversorgung; wird an hochverfügbaren Rechnersystemen eingesetzt, um den Ausfall der Stromversorgung zu überbrücken oder die Stromversorgung solange zu gewährleisten, bis die Rechnersysteme kontrolliert heruntergefahren worden sind.

Verschlüsselung

Informationen werden verschlüsselt, um sie gegen unberechtigte Einblicke oder Verwendung zu schützen. Verschlüsselungsverfahren beruhen auf komplexen mathematischen Berechnungen (Algorithmen), wobei die Länge der Schlüssel und die Qualität des Algorithmus maßgeblich für die Sicherheit sind.

Verzeichnis-Dienst

Bestandteil einer →PKI, enthält frei definierbare Datenstrukturen und ein Protokoll zum Zugriff auf diese

Viren

Programme, die sich selbst unbemerkt in andere Programme kopieren und zu einem definierten Zeitpunkt meist zerstörerische Aktivitäten ausführen.

Voicebox

Rechnersystem für Teilnehmer in Mobilfunknetzen, das wie ein Anrufbeantworter Nachrichten aufzeichnet.

VPN

= Virtual Private Network; logisches Netz innerhalb eines konventionellen Netzes, in dem nur verschlüsselte Verbindungen zwischen einzelnen Rechnersystemen oder Teilnetzen zugelassen werden. Durch die Verschlüsselung geschieht die Kommunikation über das öffentliche Netz vertraulich, so daß die Verbindung quasi privat (virtual private) stattfindet.

W3C

= World Wide Web Consortium; Organisation zur Koordinierung der weiteren Entwicklung des →WWW durch Erarbeitung von Spezifikationen und Referenzsoftware.

WAN

= Wide Area Network. Darunter versteht man offene, weiträumige Netze – z. B. ISDN, X.25.

WAP

= Wireless Application Protocol, »Netzwerkstack« für Mobiltelefone

Web-Server

Rechnersystem, das den auf →HTTP basierenden Internet-Dienst →WWW zur Verfügung stellt.

WIN

= Wissenschaftsnetz; mit Hilfe des →DFN aufgebautes Datennetz, das alle wichtigen Universitäten und Forschungseinrichtungen Deutschlands miteinander verbindet.

WTLS

= Wireless Transport Layer Security, Ebene innerhalb des →WAP-Stacks, nimmt Sicherungsfunktionen wahr, an das Netzwerkprotokoll →SSL angelehnt

Würmer

Programmcodes, die sich – ähnlich wie Viren – selbsttätig in Netzwerken verbreiten; im Unterschied zu Viren integrieren Würmer sich jedoch nicht in andere Programme oder Dateien

WWW

= World Wide Web; die komplette Sammlung von Hypertext-Dokumenten, die auf HTTP-Servern weltweit abgelegt sind.

X.400

OSI-Standard für E-Mail-Systeme.

X.500

OSI-Standard für Benutzerverzeichnisse.

X.509

Weit verbreiteter Standard für →Zertifikate

Zertifikat

Datenstruktur, die eine Identifikation des Besitzers, seinen öffentlichen Schlüssel, ein Ablaufdatum und die digitale Signatur einer →Certification Authority enthält