IT-Sicherheit im Handwerk

Netzwerksicherheit

Dozentenhandbuch

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Das diesem Buch zugrundeliegende Verbundvorhaben "IT-Sicherheitsbotschafter im Handwerk - qualifizierte, neutrale Botschafter für IT-Sicherheit im Handwerk finden, schulen und Awarenesskonzepte erproben (ISiK)" wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen der Task Force "IT-Sicherheit in der Wirtschaft" gefördert und durch den Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR) betreut.

Die Task Force "IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind unter: *www.it-sicherheit-in-der-wirtschaft.de* abrufbar.

Herausgeber: Institut für Technik der Betriebsführung (itb) im
Deutschen Handwerksinstitut (DHI) e.V.
Kriegsstraße 103a • 76135 Karlsruhe (Konsortialführer)

Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET) der
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz (fachliche Leitung)

Westfälische Hochschule
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43 • 45877 Gelsenkirchen
(Kooperationspartner)

Interessengemeinschaft des Heinz-Piest-Instituts für Handwerkstechnik (HPI) an der Leibniz-Universität Hannover
Wilhelm-Busch-Straße 18 • 30167 Hannover
(Kooperationspartner)

ISBN **978-3-944916-16-3**

Verlag: Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
www.hwk.de

Autorenteam

Falk Gaentzsch

Bachelor of Science und wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen. Projektleiter für das Projekt „IT-Sicherheit im Handwerk“.

Schwerpunkte:
IT-Sicherheit & Awareness
Cloud-Computing
Virtualisierung

Matteo Cagnazzo

Bachelor of Science und wissenschaftliche Hilfskraft am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen.

Prof. Norbert Pohlmann

Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor
des Instituts für Internet-Sicherheit - if(is)
an der Westfälischen Hochschule Gelsenkirchen

Einleitung

Innerhalb eines Netzwerkes teilen sich mehrere Anwender dieselben Ressourcen und können darauf zugreifen. Das Internet ist ein globales Rechnernetz an dem Firmen, Privatpersonen, Regierungen und Kriminelle teilhaben und es mitgestalten. Ohne Mechanismen, die die Sicherheit eines Netzwerkes gewährleisten, kann Kommunikation zwischen den Teilhabern kompromittiert und manipuliert werden. Angenommen Sie sind Schlosser und betreiben einen Versandhandel für Türklinken und lassen Ihre Kunden per Lastschrift bezahlen. Die Kontodaten werden dafür auf Ihrer Webseite hinterlassen und von Ihnen ausgelesen. Woher wissen Sie nun, dass ein Angreifer die Daten nicht auslesen kann? Gibt es Möglichkeiten die das Auslesen von Daten erschweren? Gibt es auch Schutzmechanismen, die das Problem lösen, aber weit über meine Anforderungen hinausgehen?
Netzwerksicherheit ist nicht nur ein Thema für Administratoren, es sollten alle Anwender zumindest ein grobes Grundverständnis der verwendeten Fachbegriffe und Mechanismen haben. Dieses Handbuch soll dazu dienen, Basis-Wissen zu vermitteln und ein schnelles Nachschlagen ermöglichen, sodass Sie Angebote von IT-Systemhäusern einordnen und Handwerksbetriebe in einem Beratungsgespräch unterstützen können.

Anmerkung zu den Beispielen in diesem Handbuch

Die Betriebe, Angriffsszenarien und Schadensbeispiele in diesem Handbuch sind frei erfunden und sollen nur die möglichen Auswirkungen von Fehlern und Angriffen verdeutlichen.

Seminarziele

Ziel dieses Handbuchs ist es, Ihnen den Hintergrund und die technischen Grundlagen zum Verständnis von Netzwerksicherheit an die Hand zu geben. Hierzu werden Kenntnisse auf dem aktuellen Wissensstand rund um sicherheitsrelevante Fragestellungen im Bereich der Rechnernetze vermittelt. Anhand von Beispielen werden mögliche Angriffsvektoren auf Rechnernetze und auch Lösungsansätze sowie Möglichkeiten der Umsetzung präsentiert.

Am Ende dieses Seminars sind Sie in der Lage:

- Softwarebedingte Gefahren für Rechnernetze zu beschreiben
- Lösungsansätze zu vermitteln
- Betriebe zu sensibilisieren

Inhaltsverzeichnis

1. Netzwerksicherheit

Um den Zusammenhang von IT und IT-Sicherheit zu verstehen stellen wir uns vor, die expandierende „Konditorei Herkerath“ möchte ihren IT-Sektor ausbauen. Hierbei muss sie ein besonderes Augenmerk auf die Netzwerksicherheit legen.
Es ist ein gewisser Basisschutz erforderlich, unter dem Clientsicherheit (Anti-Malwareprogramm, Firewall, Updates), Schutz der eigenen Kunden- und Rechnungsdaten, Backup-Lösungen sowie weitere Aspekte (Faktor Mensch, mobile Geräte) zusammengefasst sind.
Die Konditorei muss darüber hinaus Ihre Server gegen Bedrohungen absichern. Besonders Router und Switches sollten gut konfiguriert sein und mit regelmäßigen Firmware-Updates versorgt werden. Zudem sollte klar sein, welche Peripheriegeräte mit dem Sever kommunizieren.
Man stelle sich nun vor, der Geschäftsführer hat Expansionspläne und versendet diese in einer unverschlüsselten E-Mail an den stellvertretenden Geschäftsführer. Ein Konkurrent könnte diese Informationen abfangen, oder jemanden beauftragen der dies übernimmt und hätte das Betriebsgeheimnis der „Konditorei Herkerath“ ohne großen Aufwand, für sich zugänglich gemacht. Deswegen ist es wichtig, dass die Konditorei sich über verschlüsselte Übertragung von Informationen Gedanken macht.
Abschließend ist darauf zu achten, dass ein sicherer Fernzugriff auf die Unternehmensstruktur möglich ist, wenn zum Beispiel eine neue Filiale in der Nachbarstadt eröffnet wird.

1.1 Was ist Netzwerksicherheit?

Netzwerksicherheit bezeichnet das Gesamtkonzept der Planung, Ausführung und Überwachung der Sicherheit in Netzwerken zur elektronischen Datenverarbeitung. Es müssen nicht nur technische Sicherungsmaßnahmen bedacht werden sondern auch organisatorische, betriebliche und juristische Optionen. Einige der Maßnahmen können anhand der folgenden Fragen kategorisiert werden:

- Technisch: (Was wird eingesetzt?)
- Organisatorisch: (Wer darf was?)
- Betrieblich: (Wie wird Sicherheit im Betriebsablauf realisiert?)
- Rechtlich: (Was darf eingesetzt werden?)

Unter Netzwerksicherheit versteht man die Planung, Ausführung und Überwachung der Sicherheit in Netzwerken. Die Sicherheit ist in erster Linie abhängig von der eingesetzten Infrastruktur.

1.1.1 Netzwerksicherheit im Handwerk

Die Infrastruktur durchschnittlicher Handwerksbetriebe setzt sich häufig aus folgenden Komponenten zusammen: Ein Standard-Internetanschluss von einem Telekommunikationsanbieter, ein Router sowie eine darin integrierte Firewall. Unter Umständen wird ein Netzwerkswitch nachgeschaltet, um mehrere PCs an den Router anzuschließen. Hinzu kommen noch ein Telefon oder/und Faxgerät sowie weitere Telekommunikationsanlagen. Unter Umständen hat der Betrieb noch eine einfache Homepage, die keine Dienste zur Verfügung stellt oder einen selbstverwalteten Online-Shop.

1.1.2 Wirkungs- und Handlungszusammenhang

In der virtuellen Welt müssen neue Vertrauensmechanismen greifen, um vertrauliche Kommunikation zu ermöglichen.

Reale Welt vs. Virtuelle Welt

In der realen Welt haben wir von klein auf gelernt mithilfe persönlicher Kontakte und intuitiver Einschätzung die Grundwerte unseres Gegenübers zu erfassen. Auf dieser Grundlage schätzen wir die gegenseitige Wertekonformität ab. Daraus leiten wir die Vertrauenswürdigkeit unseres Gegenübers ab, um so mehr Sicherheit zu erlangen. Wir wissen, welche Bedeutung das Eingehen von Verträgen und welche Verbindlichkeit unsere eigenhändige Unterschrift hat.
In der elektronischen Welt können wir auf die altbewährten Mechanismen oft nicht zurückgreifen. Wir begegnen hier einander nicht mehr unmittelbar, sondern kommunizieren indirekt über elektronische Netzwerke wie das Internet oder das Telefonnetz. Wir wissen nicht verlässlich, mit wem wir kommunizieren. Wir wissen nicht, wer möglicherweise unsere Kommunikation abhört oder manipuliert. Das heißt, wir müssen unsere grundlegenden Sicherheitsbedürfnisse in der virtuellen Welt anders erfüllen als in der realen Welt und beispielsweise mit Datei- und Festplattenverschlüsselung für eine sichere Aufbewahrung der elektronischen Informationen (Werte) auf den Rechnersystemen sorgen.

Datenschutzgesetze müssen eingehalten werden.

Welche Sicherheitsanforderungen gibt es?

Datenschutzgesetze müssen eingehalten werden und jeder Betrieb ist selbst in der Pflicht sich gegen mögliche Wirtschaftsspionage zu schützen.
So schützt die Verschlüsselung von Datenströmen sensible Kundeninformationen vor der Einsicht durch unbekannte Dritte.

Jeder Kommunikationskanal muss geschützt werden.

Was muss geschützt werden?

Grundsätzlich sind alle Daten und Informationen die in einem Unternehmen verarbeitet werden schützenswert. Von Strategiepapieren und Entwicklungsunterlagen, über Kundendaten und Logins, bis hin zu privaten Informationen, wie zum Beispiel Bilder oder E-Mails muss ein Mindestmaß an Sicherheit gewährleistet werden. Die Grundprinzipien und Schutzmechanismen die dies gewährleisten, werden im nächsten Kapitel detailliert dargestellt.

1.1.3 Grundprinzipien

In der elektronischen Geschäftswelt sind folgende Sicherheitsmechanismen nicht mehr wegzudenken:

Authentizität / Echtheit

Wir wünschen uns den Nachweis der Urheberschaft einer Information und damit ihre Authentizität. Wir wollen wissen, wer die Information generiert und wer unsere Betriebsmittel und Dienste nutzt. Dies kann im realen Leben durch die Vorlage eines Ausweises kontrolliert werden.

Elektronisch im Handwerksbetrieb, kann eine Authentifizierung durch ein Login-System realisiert werden. Ein Mitarbeiter meldet sich mit einem eigenem Account und einem geheimen und sicheren Passwort am Arbeitsrechner an.

- Verfahren: Passwort, PIN, Biometrie[1], Smartcards (siehe Kapitel , Security-Tokens[2], Ausweis
- Beispiele: Login-Systeme, Zugangskontrollen

Vertraulichkeit

Wir benötigen Vertraulichkeit für wichtige Informationen, als Aufbewahrungsort für Betriebsgeheimnisse eignet sich beispielsweise ein Tresor. Kein unberechtigter Dritter darf in der Lage sein, die gespeicherten und die übertragenen Informationen zu lesen.

Elektronisch im Handwerksbetrieb sollten beispielsweise Passwortspeicherprogramme und verschlüsselte Ordner zum Einsatz kommen, um Daten sicher abzulegen.

- Verfahren: Verschlüsselung, Klassifizierung von Unterlagen und die Kontrolle der Zugriffsrechte
- Beispiele: SSL/TLS-Verschlüsselung (siehe Kapitel 1.6.1), Mitarbeiter-Account in jedem Handwerksbetrieb, Keepass(X)[3] als Passwort-Container

In der elektronischen Welt müssen wirksame Schutzmechanismen eingesetzt werden.

Die Bedeutung von IT-Systemen ist rasant gestiegen und damit auch die Abhängigkeit von diesen.

Schutz kann gewährleistet werden durch Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit und Anonymisierung oder Pseudonymisierung.

Integrität/ Unversehrtheit

Wir brauchen die Unversehrtheit die Integrität wichtiger Informationen. Wir möchten sicherstellen, dass die Informationen nicht durch Übertragungsfehler oder Manipulation von ihrem Originalzustand abweichen.
Im realen Leben wird ein Dokument in einem verschlossenen Umschlag verschickt. Als elektronisches Pendant hierzu werden die von einer Maschine verarbeiteten Daten mittels Zugriffskontrolle und Netzwerktrennung vor Manipulation geschützt.

- Verfahren: Prüfsummen und Digitale Signaturen
- Beispiele: S/MIME[4] oder OpenPGP (E-Mail Signierung / Verschlüsselung)

Für mehr Informationen bezüglicher digitaler Signaturen und der Verschlüsselung von E-Mails, nutzen Sie bitte das Handbuch Rechtsverbindliche Kommunikation.

Verbindlichkeit

Wir benötigen die hinreichende Beweiskraft elektronischer Kommunikationsabläufe. Wir gewährleisten so die Verbindlichkeit elektronischer Geschäftsprozesse.

Die persönliche Übergabe eines Briefes stellt die Verbindlichkeit sicher. Eine verschlüsselte und signierte E-Mail garantiert die Beweiskraft bei elektronischer Kommunikation.

- Verfahren: Protokollierung, Signaturen (Digitale Unterschrift)
- Beispiel: Signierte E-Mail Kommunikation

---

[1] Biometrie – Fingerabrücke, Gesichtsgeometrie – die Einmaligkeit von Körpermerkmalen.
[2] Security-Token – ist beispielsweise ein USB-Speicherstick mit einer weiteren Datei oder einem speziellen Schlüssel, der als Besitz nachgewiesen werden muss, um ein Login zu ermöglichen.
[3] http://keepass.info/ - ist ein Passwort-Container zum sicheren aufbewahren vieler Passwörter
[4] S/MIME – ist ein Standard für die Signatur und Verschlüsselung von E-Mails

Verfügbarkeit

Wir benötigen die Verfügbarkeit der IT-Dienste, damit unsere elektronischen Geschäftsprozesse darauf stabil und zuverlässig zurückgreifen können.

Wenn jeder Außendienstmitarbeiter ein verlässliches Dienstfahrzeug nutzen kann, ist im realen Leben Verfügbarkeit gegeben.

Elektronisch im Handwerksbetrieb sollte beispielsweise dafür Sorge getragen werden, dass der Telekommunikationsanbieter minimale Ausfallzeiten für Telefon und Internet garantiert.

Verfahren:

- Überwachen / Regulieren von Zugriffen auf Objekte (Was? Wann? Welche?)
- Beispiel: Redundanzen (siehe Kapitel 3.2.4) und Zugriffskontrolle (siehe Kapitel 1.5.4)

Anonymisierung oder Pseudonymisierung

Gewährleistet das Recht auf informationelle Selbstbestimmung, den Schutz der Privatsphäre und der damit verbundenen personenbezogenen Daten[5].
Während bei der Pseudonymisierung Rückschlüsse auf die Identität gezogen werden können, kann nach einer Anonymisierung keine Verbindung mehr zu einer Person oder einem Objekt hergestellt werden.

Informationelle Selbstbestimmung wird durch Anonymisierung gewährleistet

- Verfahren: Datensparsamkeit, Zweckbindung, Notwendigkeit, Pseudo- und oder Anonymisierung
- Beispiele: Vergabe von Nummern anstatt Klarnamen oder anonymen Nutzernamen, statt einem echten Nutzernamen.

Zusammenfassung

In der elektronischen Welt müssen wirksame Schutzmechanismen eingesetzt werden.

Die Bedeutung von IT-Systemen ist rasant gestiegen und damit auch die Abhängigkeit von diesen.

Die Schutzziele sind Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit und Anonymisierung oder Pseudonymisierung.

1.1.4 Technische Grundlagen: TCP/IP-Technologie für Internet und Intranet

Das Internet, das »Netz der Netze«, verkörpert eine einzigartige, weltumspannende Infrastruktur vernetzter Netzwerke und die Software-Technologien, auf denen diese Netzwerke aufbauen. Die TCP/IP-Technologie (Transmission Control Protocol/Internet Protocol) ist das eigentliche Herz des Internets. Erst die hohe Verwendung der TCP/IP-Protokolle ermöglichte die weltweite Vernetzung der Rechnersysteme bis hin zum kleinsten PC im letzten Winkel dieser Erde.

[5] *Personenbezogene Daten – sind Daten, die einer bestimmten oder bestimmbaren Person eindeutig zugeordnet werden können.*

Die TCP/IP-Technologie ist kein feststehendes Gebilde, sondern besteht aus unterschiedlichen Diensten und Anwendungen, die im Laufe der Jahre ständig weiterentwickelt wurden. Das TCP- und IP-Protokoll sind streng genommen nur zwei Komponenten der gesamten Kommunikations-Architektur, sie haben sich aber als übergeordneter Begriff im Sprachgebrauch durchgesetzt.

Das Internet ist eine globale Infrastruktur von Netzwerken und Software-Technologien

1.1.5 Historie von Netzwerken

Ursprünglich hatte das Internet, wie viele Projekte der Hochtechnologie, militärische Zielsetzungen. Die ersten Gedanken entstanden bereits Ende der Fünfzigerjahre, als die amerikanische „RAND Corp.“ ein Konzept für ein Kommando- und Überwachungsnetzwerk für militärische Einrichtungen entwickelte. Der Kern dieses Konzepts bestand aus einem dezentralen Aufbau, der auch nach teilweiser Zerstörung der Infrastruktur, zum Beispiel nach einem Atomschlag, die Funktionsfähigkeit der amerikanischen Militäreinrichtungen gewährleisten sollte.

Um im technologischen Wettstreit mit der Sowjetunion die amerikanische Militärtechnologie in eine führende Position zu bringen, rief die US-Regierung unter anderem die „Advanced Research Projects Agency“ (ARPA) ins Leben. Deren Aufgabe war es, neue und innovative Technologien zu entwickeln. Aus den ursprünglichen Konzepten der „RAND Corp.“ entwickelten die ARPA-Ingenieure die paketorientierte Datenübertragung, die die Datenkommunikation in den folgenden Jahren revolutionieren sollte. In den 1060er Jahren wurde zwischen der „University of California at Los Angeles“, der „University of California at Santa Barbara“, der „University of Utah“ und dem „Stanford Research Institute“ (SRI) in Menlo-Park in Kalifornien das erste experimentelle Netz (ARPANET) in Betrieb genommen. Zum Erfolg trugen die auf allen angeschlossenen Rechnern verfügbaren Dienstleistungen wie Terminalsitzung (Remote Login), Dateiübertragung (File Transfer) und Elektronische Post (Electronic Mail) bei. Im Folgenden die wichtigsten Jahreszahlen aus der Historie des Internets aufgelistet:

1977 ISO beginnt mit dem OSI-Referenzmodell (siehe Kapitel 1.2.2)

1981 PCs finden Verbreitung

1993 Mobilfunknetze (GSM) werden aufgebaut.

1994 Freigabe des Internets zur kommerziellen Nutzung

1995 Verknappung der IP-Adressen, Entwicklungsbeginn von IPv6 (siehe Kapitel 1.2.5)

2002 3G[6]: UMTS, HSDPA

2010 4G[7]: WiMax, LTE….

Die rasante Entwicklung des Internets hat aber auch Schattenseiten mit sich gebracht. Die TCP/IP-Technologie war nicht für ein solches globales Netz gedacht. Durch die in den Anfangsjahren auf wenige Teilnehmer begrenzte Ausdehnung des Internets waren Sicherheitskonzepte wie Zugriffsberechtigung, Vertraulichkeit der Daten während der Übertragung und der Schutz von Netzsegmenten vor unberechtigten Zugriffen nicht in dem Maße erforderlich wie heute. Da sich mittlerweile jeder von fast jedem Ort

[6] *3G – ist ein Mobilfunkstandard der dritten Generation*
[7] *4G – ist ein Next Genaration Mobilfunkstandard mit höheren Übertragungsgeschwindigkeiten*

auf der Welt mit dem Internet verbinden kann, sind damit natürlich auch Sicherheitsmaßnahmen unumgänglich geworden.

1.2 Funktionsweise eines Netzwerks

Ein Rechnernetz ist primär ein Übertragungssystem zwischen den angeschlossenen Rechnersystemen, die weitgehend oder vollständig autonom agieren.

1.2.1 Netzwerktopologien und Infrastruktur

Unter dem Begriff Netzwerktopologie wird die physikalische oder logische Anordnung von Geräten im Netzwerk, welche über Netzwerkkabel miteinander verbunden sind, bezeichnet. Wir wollen uns in diesem Buch, soweit nicht anders vermerkt, auf die physikalischen Aspekte beschränken.
Die Topologien lassen sich in zwei Konfigurationen aufteilen. Bei Konfiguration Eins wird eine Verbindung von Knoten zu Knoten erstellt, zum Beispiel bei der Ringtopologie. Die zweite Konfiguration ist beispielsweise die Buskonfiguration, hier sind alle Netzknoten direkt an das Übertragungsmedium angeschlossen. (siehe Abbildung 1: Netzwerk-Topologien).
Die unterschiedlichen Topologien unterscheiden sich anwendungsspezifisch schon beim Aufwand des Verkabelns oder dem Verhalten beim Ausfall eines Systemknotens.

Es gibt unterschiedliche Netzwerktopologien die hierarchisch nach Größe geordnet sind. Jedes Netzwerk dient der Übertragung von Informationen.

PAN - Personal Area Network

Beim PAN handelt es sich um ein Rechnernetz, welches sich auf die Reichweite einer Einzelperson bezieht. Ein Beispiel für ein solches PAN ist eine Maus, die statt eines Kabels eine Bluetooth-Verbindung nutzt um mit einem Rechner zu kommunizieren.

LAN - Local Area Network

Als nächstes folgt das LAN, ein privates Netz, das innerhalb eines Gebäudes oder in der Nähe arbeitet. Mit Hilfe eines LANs können mehrere Computer mit einem Drucker oder zum Austausch von Informationen verbunden werden. Werden LANs in einer geschäftlichen Umgebung eingesetzt, wird von einem Unternehmensnetzwerk (Enterprise Network) gesprochen.
Ein sehr beliebtes Beispiel für ein LAN ist zum Beispiel WLAN (Wireless-LAN), welches besonders in Privathaushalten oder Cafés häufig eingesetzt wird. Weitere Beispiele wären Ethernet, Token Ring oder FDDI[8].

MAN - Metropolitan Area Network

Das Stadtnetz oder auch MAN erstreckt sich über die Größe einer kompletten Stadt. Auf der Grundlage Glasfaserkabeln wird ein Rechnernetz geschaffen, welches eine hohe Übertragungsrate, bei möglichst geringer Fehlerrate liefert. Techniken die eingesetzt werden sind zum Beispiel Gigabit Ethernet, ATM[9] oder DQDB[10].

---

[8] Fiber Distributed Date Interface ist eine standardisierte 100Mbit/s-Netzwerkstruktur.
[9] Asynchronous Transport Mode ist ein Kommunikationsprotokoll zur Übertragung von Daten, Sprache und Video.
[10] Distributed Queue Dual Bus ist ein Hochleistungs-Übertragungsprotokoll.

WAN - Wide Area Network

Bei WAN handelt es sich um ein Rechnernetz, welches sich über ein großes Territorium, häufig ein ganzes Land oder einen Kontinent erstreckt. Hat zum Beispiel ein Unternehmen mehrere Standorte innerhalb von Europa können die Zweigstellen mit einem WAN untereinander kommunizieren. Als Technologien kommen ISDN[11], SDH[12] oder SONET[13] in Frage.

•

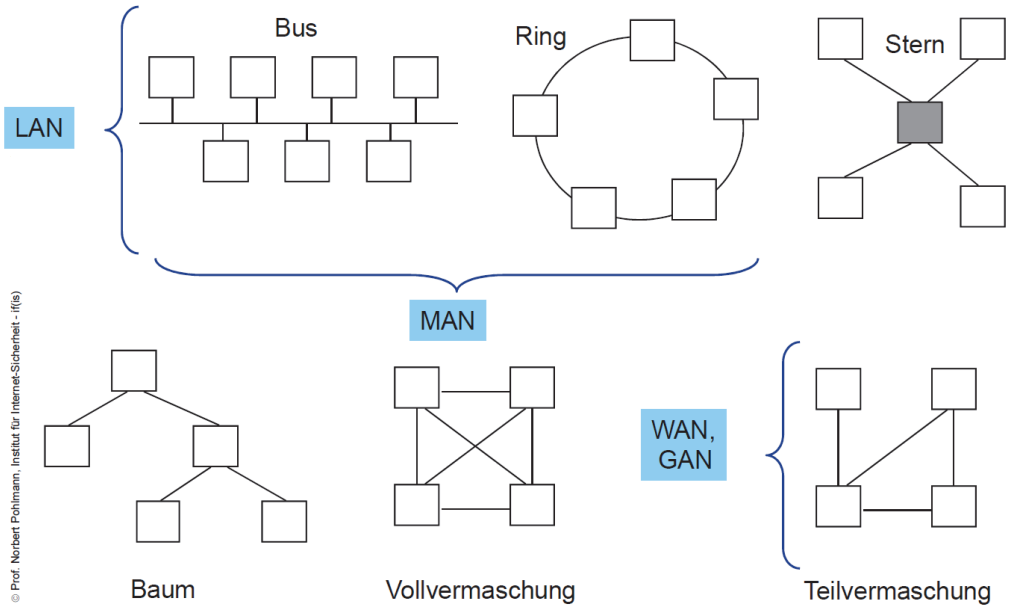


Abbildung 1: Netzwerk-Topologien

Zusammenfassung: Netzwerke

Rechnernetzwerke haben sich etabliert und sind längst unternehmerische Ressourcen, die im Fehlerfall erhebliche Schäden verursachen können.

Ein Rechnernetz ist primär ein Übertragungssystem zwischen den angeschlossenen Rechnersystemen, die weitgehend oder vollständig autonom agieren.

Das Internet, das Netz der Netze, ist die Basis unserer Informations- und Wissensgesellschaft.

[11] *Integrated Services Digital Network dient zur Übermittlung verschiedener Kommunikationsdienste*
[12] *Synchrone Digitale Hierarchie ist eine Multiplextechnik.*
[13] *Synchronous Optical Network ist eine Multiplextechnik für Datenströme zwischen 51Mbit/s und 2,5GBit/s.*

1.2.2 Das OSI-Modell[14]

Das OSI-Modell, auch ISO/OSI-Referenzmodell genannt, ist ein von der International Organization for Standardization (ISO) entwickeltes Kommunikationsprotokoll, das allgemeine Regeln für die Kommunikation in Netzwerken enthält. Da jeder Rechner seine eigene Architektur hat, wird keine Festlegung über die Implementierung gemacht.

Das OSI-Referenzmodell hat eine klare Architektur und eignet sich daher besonders gut für die Darstellung einer Kommunikationsarchitektur und der Prinzipien des Schichtenmodells. Um eine einheitliche Struktur für gegenwärtige und zukünftige Entwicklungen von Netzwerktechnologien festzulegen, wurde sich auf das so genannte OSI-Referenzmodell geeinigt und 1983 von der ISO als Standard festgelegt. In diesem Modell wird davon ausgegangen, dass ein Kommunikationsprotokoll aus mehreren Modulen besteht, von denen jedes einzelne Modul während einer Kommunikation unterschiedliche Aufgaben zu erfüllen hat.

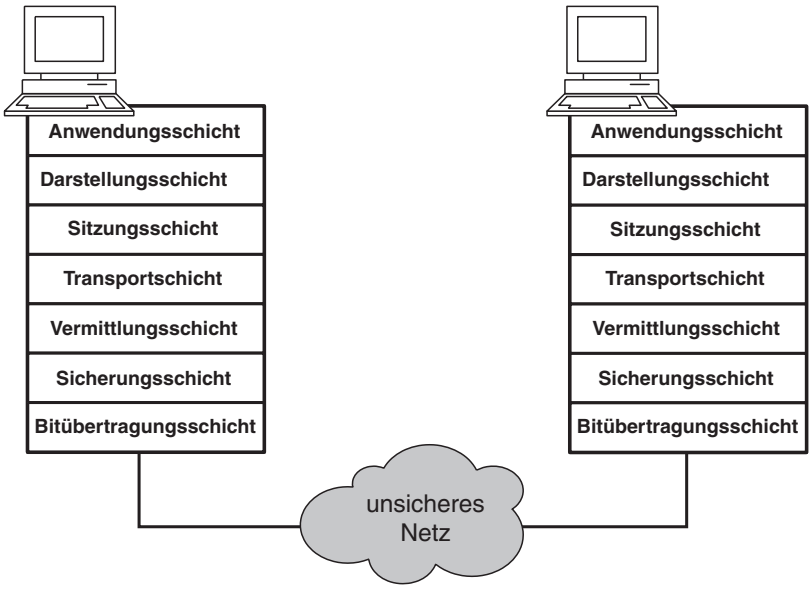


Abbildung 2: Das OSI-Referenzmodell

Das OSI-Referenzmodell besagt nun, dass bei einer Verbindung, zum Beispiel zwischen zwei Rechnersystemen, jede Schicht des Rechnersystems A mit der gleichen Schicht des Rechnersystems B kommunizieren kann. Dazu werden den Daten in jeder Schicht bestimmte Bitmuster in einem Header vorangestellt oder einem Trailer am Ende angefügt. Diese Bitmuster enthalten so genannte Protokollinformationen, die zum Beispiel darüber Auskunft geben

- wer die Daten abgesandt hat,
- wer die Daten empfangen soll,
- welchen Weg die Daten während der Übertragung nehmen sollen,
- wie die Daten weiterverarbeitet werden dürfen,
- oder wie sie vom Empfänger behandelt werden sollen.

[14] *Open System Interconnection*

Jede weitere Schicht übernimmt die Datenpakete der übergeordneten Schicht und fügt, falls dies für den Ablauf der Kommunikation notwendig sein sollte, ihre eigenen Protokollinformationen in einem weiteren Header oder Trailer hinzu. Die Auswertung der Protokolldaten erfolgt beim Empfänger nur auf der jeweils gleichen Schicht, das heißt, die Daten einer übergeordneten Schicht werden von einer niedrigeren Schicht nicht interpretiert oder ausgewertet, siehe folgende Abbildung.

Das OSI-Modell ist das Referenzmodell zur Beschreibung von Kommunikationsabläufen. Von HTTP bis Bluetooth lassen sich die unterschiedlichsten Protokolle damit beschreiben.

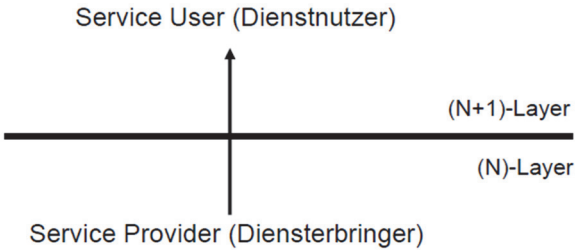


Abbildung 3: Services und Schichten

Es werden horizontale Schichten mit räumlich getrennten Instanzen geschaffen.
Eine Instanz einer höheren Schicht (vertikal) hat als „Diener“ die Schicht darunter: Sie gibt Aufgaben an ihren „Diener“ erhält und von ihm wieder Ergebnisse.

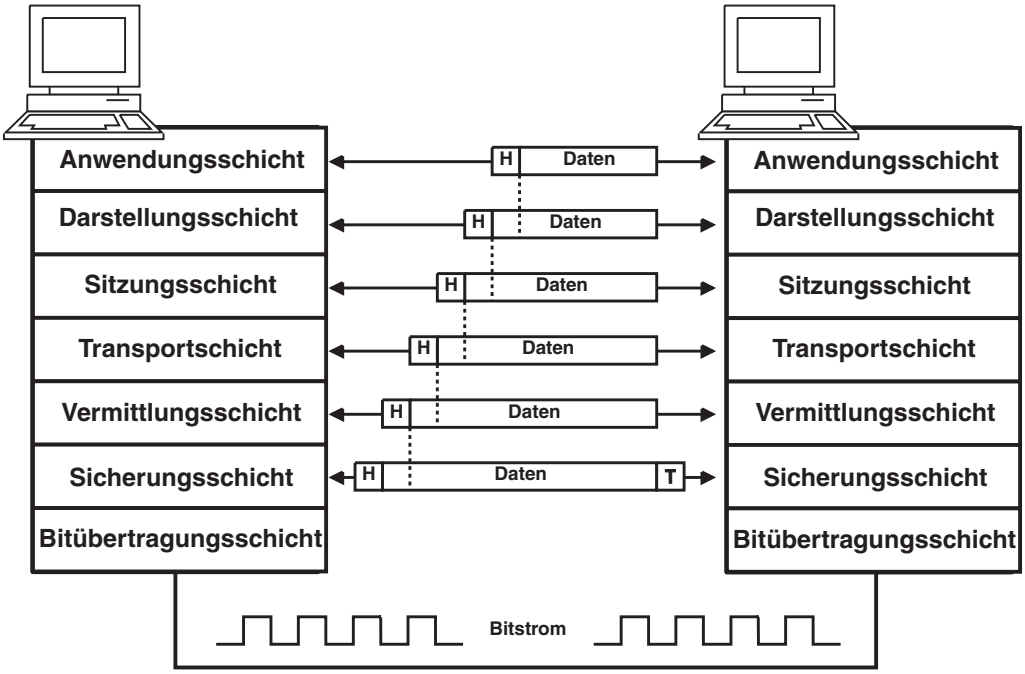


Abbildung 4: Kommunikation zwischen zwei Rechnern

Im folgenden Abschnitt soll kurz erläutert werden, welche Aufgaben die jeweiligen Schichten übernehmen:

Bitübertragungsschicht (Physical Layer)

Die Bitübertragungsschicht legt fest, wie die Daten physikalisch übertragen werden. Zu den Parametern dieser ersten Schicht gehören Informationen über die verwendeten Übertragungsmedien, wie z.B. Kupferkabel, Glasfaser, Infrarot- oder Funkübertragung, und die Spezifikation von Schnittstellen mit Spannungspegeln, Steckverbindern und Datenübertragungsraten.

Sicherungsschicht (Data Link Layer)

Die Aufgabe der Sicherungsschicht ist die sichere Datenübertragung zwischen zwei benachbarten Stationen, zum Beispiel Router, innerhalb eines Netzwerkes. Dazu werden die zu übertragenden Bits in Rahmen (Frames) zusammengefasst und mit einer Prüfsumme versehen. Wird ein solcher Rahmen unvollständig übertragen oder zerstört, so fordert der Empfänger nach einem Vergleich der Prüfsumme den entsprechenden Rahmen erneut bei dem Absender an.

Vermittlungsschicht (Network Layer)

Die Vermittlungsschicht legt die Übertragungswege (Routen) für die Daten zwischen zwei Rechnersystemen fest. Dazu werden Informationen wie zum Beispiel. Übertragungszeit, Auslastung des Übertragungsweges und so weiter benutzt, um nach festgelegten Regeln, dem Routing-Protokoll, eine Verbindung herzustellen. Die innerhalb dieser Schicht transportierten Daten werden in Datenblöcken übertragen und werden als Pakete bezeichnet.

Transportschicht (Transport Layer)

Die Transportschicht stellt eine Art virtuelle Verbindung zwischen den beiden Rechnersystemen bereit. Sie sorgt vor allem für eine Korrektur der Übertragungsfehler und ist sehr stark von den untergeordneten Schichten abhängig.

Sitzungsschicht (Session Layer)

Die Sitzungsschicht dient der Verwaltung von Kommunikationsprozessen. Dabei wird die Verbindung mit einem oder mehreren Kommunikationspartnern kontrolliert und gleichzeitig dafür gesorgt, dass die jeweilige Kommunikation synchron abläuft, das heißt, dass bei einem aufgetretenen Fehler die Daten wieder in der richtigen Reihenfolge zusammengefügt werden.

Jede Schicht übernimmt andere Aufgaben und kommuniziert mit ihrem gegenüberstehenden Kommunikationspartner.

Darstellungsschicht (Presentation Layer)

In dieser werden die zu übertragenden Daten in ein einheitliches Format gebracht. Dies ist vor allem bei der Verwendung von unterschiedlichen Zeichensätzen, zum Beispiel ASCII [15]und EBCDIC[16], notwendig. Zusätzlich können in dieser Schicht weitere Funktionen zur Umwandlung, Verschlüsselung oder Komprimierung der zu übertragenden Daten enthalten sein.

---

[15] ASCII – dieser Standard ist eine Zeichenkodierung Buchstaben und Zahlen (A = Dezimal 65 oder binär (0)1000001)
[16] EBCDIC – ist ein Standard für den Austausch von binär kodierten Dezimalziffern.

Anwendungsschicht (Application Layer)

Die Anwendungsschicht beinhaltet schließlich die eigentlichen Anwendungs- und Dienstprogramme, die über die Netzwerkverbindung ausgeführt werden sollen.

1.2.3 Das TCP/IP-Modell

In diesem Modell gibt es analog zum OSI-Referenzmodell unterschiedliche Kommunikationsebenen, die Daten von der übergeordneten Ebene zur nächsttieferen Ebene weiterreichen. Jede Kommunikationsebene fügt den Daten eigene Kontrollinformationen hinzu, bis sie über das Netz gesendet werden. Der Empfänger reicht diese Daten dann Ebene für Ebene nach oben weiter, wobei jede Ebene nur die für sie relevanten Daten auswertet und diese aus dem Datenpaket entfernt, bevor sie an die nächsthöhere Ebene weitergegeben werden.

Abbildung 5: Ebenen der TCP/IP-Protokollarchitektur

1. Die Netzzugangsebene ermöglicht einem Rechnersystem Daten zu einem anderen Rechnersystem innerhalb des direkt angeschlossenen Netzes (zum Beispiel Ethernet) zu übertragen. Dazu sind genaue Kenntnisse des zugrunde liegenden Netzaufbaus nötig. Die Netzzugangsebene umfasst die zwei unteren Ebenen des OSI-Modells und beinhaltet die Kapselung von IP-Paketen in Netzrahmen (Frames) und die Zuordnung von IP-Adressen zu physikalischen Netzadressen, zum Beispiel MAC-Adressen.
2. Die Netzwerkebene definiert den Aufbau von IP-Paketen und bestimmt, auf welchem Weg die Daten durch das Internet übertragen werden (Routing).
3. Die Transportebene stellt eine Verbindung zwischen zwei Endpunkten oder Rechnersystemen her. Die wichtigsten Protokolle sind hier TCP und UDP (siehe Kapitel 1.2.7).
4. Die Anwendungsebene beinhaltet sämtliche Programme und Dienste, die über die Netzwerkverbindung durchgeführt werden sollen. Dazu gehören vor allem Dienste wie HTTP(S) (siehe Kapitel 1.2.9) für Webseiten und SMTP(S) (siehe Kapitel 1.2.10) für E-Mail-Funktionen.

1.2.4 TCP/IP- und OSI-Modell im Vergleich

Beide Modelle dienen der Modellierung des Kommunikationssystems eines Rechners zum Austausch von Nachrichten im Rechnernetz und der Zusammenarbeit mit dem Kommunikationssystem eines anderen Rechners. Das OSI-Modell war eine Idee der International Standards Organisation (ISO), während das TCP/IP-Modell dem ARPA-NET[17], einem Vorläufer des Internets, entspringt. Heutzutage spielen die durch das OSI-Modell verwendeten Protokolle kaum noch eine Rolle, während das Modell an sich häufig verwendet wird. Konträr verhält sich das TCP/IP-Modell. Das TCP/IP-Protokoll ist immer noch weit verbreitet, während das Modell eine eher untergeordnete Rolle spielt. Der Grund hierfür ist, dass das Modell von TCP/IP zu keinem anderen Protokollstapel passt. Es ist zum Beispiel nicht möglich Bluetooth mit dem TCP/IP-Modell zu beschreiben. Das OSI-Modell ist hingegen sehr allgemein formuliert.

Beide Referenzmodelle spielen eine wichtige Rolle. Das OSI-Modell liefert eine Beschreibung von grundsätzlichen Konzepten, während das TCP/IP-Modell am häufigsten verwendet wird.

Abbildung 6: TCP/IP- und ISO/OSI-Referenzmodell im Vergleich

1.2.5 Internet-Adressen

Damit Daten im Internet ihr Ziel finden, benötigt jedes Rechnersystem im Internet hat eine bestimmte IP-Adresse und einen Namen.

Bei der Entwicklung der Internet-Adressierung wurde nicht nur hohen Wert auf die Identifizierung jedes angeschlossenen Rechnersystems gelegt, es ist darüber hinaus notwendig zu wissen, an welcher Stelle innerhalb eines Netzwerkes es sich befindet und über welche Übertragungswege die Daten ihr Ziel erreichen können.

---

[17] *Advanced Research Projects Agency Network war ein Forschungsnetz, unterstützt durch das US-Verteidigungsministerium im Zuge des Kalten Krieges. Ziel war es nach ein System zu entwickeln, dass auch nach einem Atomschlag noch funktioniert. 1974 definierten Cerf und Kahn das erste Mal das TCP/IP-Modell.*

IP-Adressen dienen der eindeutigen Bestimmung von Kommunikationspartnern.

Im IPv4-Adressraum erhält jedes Gerät im weltweiten Netzwerk eine einmalige 32 Bit oder 4 Byte lange Internet-Adresse, bestehend aus einer Netzwerk- und einer Rechnersystem-Identifikation, die als 4 Dezimalzahlen dargestellt werden und jeweils durch einen Punkt getrennt sind.

Beispiel: 11000011 . 10010011 . 00111000 . 11101101 entspricht 195 . 147 . 56 . 237

Diese Adressierung wird in fünf Klassen (Klasse A bis E) aufgeteilt. Jede dieser Klassen unterscheidet sich in der Länge der Netzwerk- und der Rechnersystem- Identifikation. Diese Aufteilung wurde getroffen, da in den Anfangstagen des ARPANET davon wurde, dass es in Zukunft nur wenige große (Klasse-A-) Netzwerke (z.B. für Militär und Forschung) geben würde. Doch nach einigen Jahren zeigte sich mit der Einführung von lokalen Netzwerken in vielen Organisationen, dass diese Annahme nicht auf Dauer tragbar war. Durch die Einschränkung der Vergabe von Klasse-A-Adressen wurden die Möglichkeiten schnell begrenzt. Aus diesem Grund wurden zwei weitere Klassen für mittelgroße (Klasse B) und kleine Netze (Klasse C) eingeführt. Den Klasse-D-Adressen fällt eine besondere Bedeutung zu. Sie werden als so genannte Multicast-Adressen bezeichnet. Das bedeutet, dass bestimmte Datenpakete nicht mehr an jedes Rechnersystem einzeln verschickt werden müssen, sondern gleichzeitig an eine ganze Gruppe von Rechnersystemen, denen eine Multicast-IP-Adresse zugeordnet wurde. Die IP-Adressen der Klasse E sind für zukünftige Anwendungen reserviert und werden derzeit zu Forschungszwecken verwendet. Sie sollen genutzt werden, um IPv6-Pakete über IPv4-Netze zu routen.

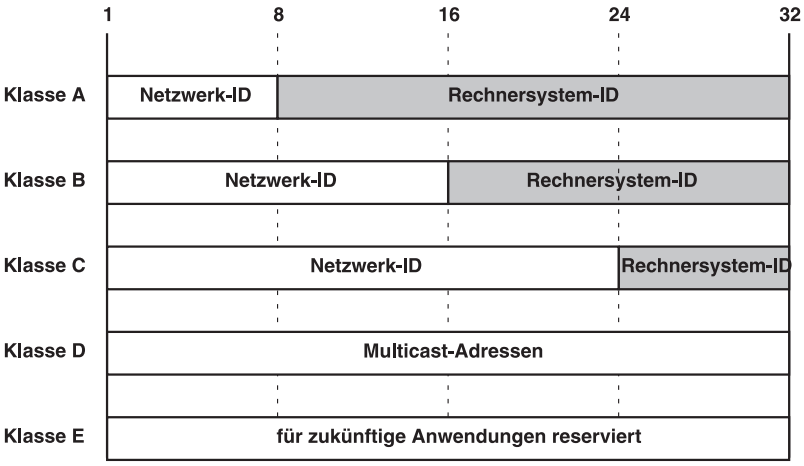


Abbildung 7: Aufbau von IPv4-Adressen und Einteilung in Klassen

Das starke Wachstum des Internet hat zu einem Mangel an IPv4-Adressen geführt. Außerdem sind dadurch die Routing-Tabellen der Backbone-Router, die die einzelnen Netze verbinden, zu groß geworden. Aus diesem Grund wurde die starre Aufteilung in nur fünf Netzklassen aufgehoben (vgl. RFC 1517). Die 32 Bit der IP-Adresse können nun beliebig auf Netz-ID und Rechnersystem-ID verteilt werden. Somit ergeben sich 33 mögliche Netzwerk-Klassen. Für die ursprünglichen fünf Klassen, die immer noch am häufigsten vorkommen, werden die alten Bezeichnungen (Klasse A bis E) weiterverwendet. Viele Anwender, die einen Internet-Anschluss über einen Internet-Service-Provider (ISP) haben, sind nur gelegentlich mit dem Internet verbunden. Für diese Rechnersysteme ist es nicht notwendig eine permanente IP-Adresse zu vergeben. Hier wird die Möglichkeit verwendet IP-Adressen automatisch zu vergeben. Wenn ein Kunde Zugang zum Internet haben möchte, wählt er zunächst einen Einwahlknoten eines Providers in seiner Nähe an. Das Rechnersystem des Providers hat zu diesem

Zweck eine Reihe von IP-Adressen für seine Kunden reserviert, die dem jeweiligen Nutzer dann automatisch zugeordnet werden. Eine solche IP-Adresse wird dabei oft nur für eine gewisse Dauer zugeordnet, diese wird Lease-Time genannt. Der Vorgang wird als dynamische IP-Adressierung bezeichnet und ist das Gegenteil zu der festen IP-Adresszuweisung, wie es beispielsweise bei Standleitungen für Unternehmen der Fall ist.

Da aufgrund des starken Wachstums des Internets abzusehen war, dass die Anzahl der freien IP-Adressen eines Tages erschöpft sein wird, wurde die Adresslänge auf 128 Bit oder 16 Byte (IPv6) vergrößert. Natürlich sind die alten IP-Adressen weiterhin gültig und können auch nach der Einführung von IPv6 verwendet werden.

Da IPv4-Adressen knapp wurden, ist IPv6 mit einem deutlich größeren Adressraum entwickelt worden.

IPv6 bezeichnet die 6. Version des IP-Protokolls, welches IPv4 ablösen wird. Die wichtigsten Verbesserungen zu Version 4 sind der vergrößerte Adressraum, der vereinfachte Header, welcher das Routing effizienter gestalten soll und die Optimierung für Echtzeitanwendungen wie VoIP[18]. RFC 2460 ist das erste einer Reihe von RFCs, welche Version 6 beschreiben.

Unternehmen verwenden heute nur noch wenige offizielle IP-Adressen. Sie genau wie Privathaushalte, mit einer äußeren IP-Adresse am Internet-Anschluss und einem dahinter verborgenen internen IP-Adressbereich, was die Adressenproblematik stark reduziert (siehe Kapitel 1.5.2).

Die IP-Adressierung ist für technische Systeme hervorragend geeignet. Im praktischen Umgang hat sich aber gezeigt, dass dieses Verfahren für viele Anwender zu kompliziert und undurchsichtig ist. Jedes an das Internet angeschlossene Netz kann zu diesem Zweck neben einem IP-Adressbereich zusätzlich einen Domainnamen erhalten. Die Domainnamen werden zentral vom Network Information Center (NIC) und seinen Unterorganisationen (z.B. DENIC in Deutschland) vergeben und verwaltet. Wenn eine Organisation einen eigenen Domainnamen verwenden möchte, so muss sie oder ihr Provider bei der verantwortlichen Unterorganisation des NIC die Zuordnung dieses Namens beantragen.

Endung	Zweck
.com	Für kommerzielle Organisationen aus Industrie und Handel
.edu	Für Universitäten und Schulen
.org	Für nichtkommerzielle Einrichtungen
.de	Für Einrichtungen in Deutschland

Tabelle 1: Beispiele für Top-Level-Domains

[18] *VoIP- Voice over Internet Protocol, ist ein Standard für Telefonie über das Internet.*

Ports

Ports sind Bestandteile von Netzwerkadressen. Dienste die über ein Netzwerk genutzt werden, wie etwa HTTP[19], DNS[20] oder DHCP sind über fest definierte Ports erreichbar. Dies kann auf folgende Weise veranschaulicht werden: Stellt Sie sich ein Verwaltungsgebäude (Server) an einer Straße (Netzwerk) vor. Die die Adresse des Gebäudes ist die IP-Adresse. Damit nun ein Anlieger weiß in welchem Raum er seine Formulare abgeben kann, braucht er eine Raumnummer. Diese wären dann die Ports des Dienstes. Für die Kommunikationsverbindung haben beide Seiten eine Port-Nummer. Die Antworten des Servers müssen an den Port zugestellt werden, der die Anfragen gestellt hat.

Ports werden benutzt, um Anwendungen auf einem Rechnersystem zu adressieren. Zur Veranschaulichung: Werden Straßen als Netzwerk betrachtet, sind die Gebäude die Server. IP-Adressen stehen anstelle der Hausanschriften und Ports sind die Räume der Gebäude.

Viele standardisierte Dienste haben auf der Server-Seite festgelegte Portnummern. Diese Standard-Ports oder auch „well known ports“ liegen im Bereich von 0-1023 und sind für diese reserviert. Die Ports von 1024 bis 49151 sind die sogenannten „registered ports“ oder seit 2011 nach RFC 6335[21] die „user ports“. Der Bereich von 49152 bis 65535 sind die „dynamic ports“. Unternehmen haben für ihre Anwendungen einen oder mehrere Ports aus diesem Bereich registriert. In Tabelle 2 sind vier Beispiele dargestellt.

Dienstname	Portnummer
http	80
DNS	53
FTP[22]	20 und 21
SMTP	25

Tabelle 2: Netzwerkdienste und ihre Standard-Ports

Gerade weil viele Dienste einen Standard-Port benutzen, ist es oft nicht erforderlich, diesen bei einem Verbindungsaufbau anzugeben. So „weiß“ ein Browser zum Beispiel, dass für den Aufruf von Webseiten der HTTP-Dienst auf Port 80 genutzt wird. Die Portnummern auf der Empfänger-Seite werden durch das Betriebssystem vergeben und liegen zwischen 1024 und 65535.

„Well known“ Ports sind festgelegte Portnummern für standardisierte Dienste. Wichtige Ports sind zum Beispiel 80 (HTTP) und 53 (DNS).

1.2.6 Protokolle

Protokolle sind Vorschriften und Regeln zum Informationsaustausch zwischen zwei oder mehr Partnern auf derselben Stufe der Funktionsschichtung eines Kommunikationssystems.

[19] *Hyper Text Transfer Protocol ist das Protokoll beziehungsweise der Dienst, welcher Webseiten bereitstellt.*
[20] *Domain Name Service ist der Dienst, welcher von Internet-Adressen beispielsweise it-sicherheit-handwerk.de oder internet-sicherheit.de auf IP-Adressen abbildet.*
[21] *http://tools.ietf.org/html/rfc6335; mehr Informationen zum Beispiel unter http://de.wikipedia.org/wiki/Liste_der_standardisierten_Ports“*
[22] *File Transfer Protocol ist ein Protokoll zum Übertragen von Daten.*

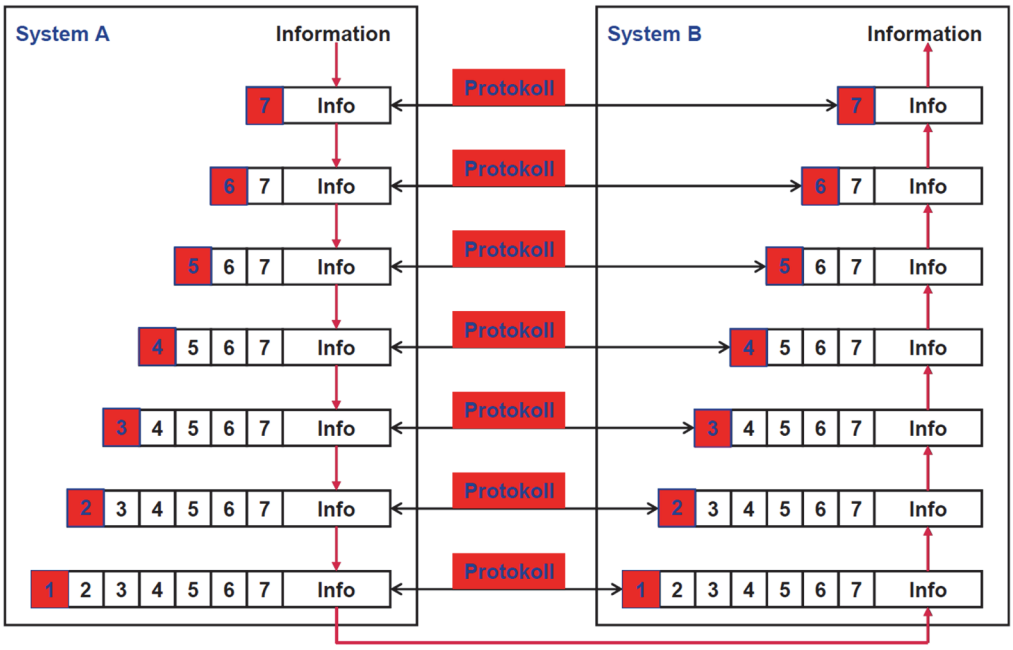


Abbildung 8: Protokollweg durch den OSI-Turm

Protokolle bestehen aus präzisen Spezifikationen in folgenden Hinsichten:

- syntaktisch (logische Datenobjekte, zum Beispiel Zeichen und Formate)
- prozedural (Konventionen der Kommunikation, zum Beispiel Steuerung, Nachrichtenfluss, Fehlerbehandlung)
- semantische (exakte Bedeutung, Auswirkungen der Nachricht)

Es gibt zwei Arten von Protokollen, die verbindungslosen und die verbindungsorientierten.

Verbindungslose und verbindungsorientierte Kommunikationsprotokolle

Grundsätzlich wird zwischen zwei Arten von Kommunikationsprotokollen unterschieden:

Bei verbindungslosen Protokollen kann Information verloren gehen, dupliziert oder verzögert werden.

Die verbindungslosen Protokolle kann mit Telegrammen vergleichen werden. Die Daten werden vom Absender in das Netz geschickt und können während der Übertragung verloren gehen, dupliziert werden oder verspätet eintreffen, ohne den Absender darüber zu informieren. Derartige Informationseinheiten werden auch Datagramme genannt. Diese Art der Kommunikation ist wie der Paketdienst einer Post-Gesellschaft. Das Paket wird an den Emüfänger abgesendet; wie es dann weitergeleitet wird, darauf kann nicht weiter Einfluss genommen werden.

Verbindungsorientierte Protokolle bestätigen den Datenempfang und bauen eine Verbindung auf und ab.

Im Gegensatz dazu bauen **die verbindungsorientierten Protokolle** eine Kommunikation nach einem bestimmten Schema auf. Zuerst wird eine virtuelle Verbindung zwischen Absender und Empfänger aufgebaut. Nach dem gegenseitigen Austausch von festgelegten Informationen erfolgt dann der eigentliche Datentransfer. Erst wenn beide Seiten den ordnungsgemäßen Empfang der Daten bestätigt haben, wird die Verbindung wieder abgebaut. Dies hat den Vorteil, dass einzelne Datenpakete die nicht vollständig oder garnicht übertragen wurden erneut versendet werden, bis sie Verlustfrei bei der Gegenstelle angekommen sind. Hier ist eine Analogie zu einem Telefongespräch zu erkennen:

Ein Teilnehmer baut die Verbindung auf, erst wenn der andere abgenommen hat, kann das Telefonat beginnen. Dabei wird dem ihrem Gesprächspartner die Telefon-

nummer eines Geschäftspartners so lange übermittelt, bis dieser die vollständige Nummer verstanden hat. Wurde eine Zahl nicht korrekt verstanden, fragt der Gesprächspartner nach und die Zahlenreihenfolge muss erneut übermittelt werden.

Protokolle können aufgegliedert werden in

- Kernprotokolle
- Dienstleistungsprotokolle
- Webprotokolle
- E-Mail-Protokolle
- Übertragungssicherheit

1.2.7 Kernprotokolle

Als Kernprotolle werden solche Protokolle bezeichnet, die in jedem TCP/IP-Stack vorhanden sind, damit TCP/IP richtig funktioniert (vgl. Comptia Security +, S. 161f)
Dieser Abschnitt stellt die wichtigsten Kernprotokolle jeder Schicht vor.

Schicht 1 – 2: Ethernet

Als Ethernet wird die nach IEEE[23] 802.3 genormte Technologie bezeichnet, welche für kabelgebundene Netzwerke die Verwendung von Software, in Form von Protokollen und Hardware spezifiziert. Ethernet ist ein Protokoll der ISO-OSI[24]-Schicht zwei.
In der Praxis werden heutzutage ausschließlich Switched-Ethernet eingesetzt. Dies ist eine Weiterentwicklung des klassischen Ethernets und verbindet mehrere Computer über Switches (siehe Kapitel 1.3.5). Es ermöglicht höhere Übertragungsraten bis zu 10-Gigabit.

Wichtige Fakten zu Ethernet sind unter anderem:

- Maximale Kabellänge: 100m (Kupfer) bei fest verlegten Leitungen. Abgezogen werden jedoch noch Übergänge wie Stecker und Kabel für Steckverbindungen. Mit Lichtwellenleitern (LWL)[25] können weitere Strecken als mit Kupfer überbrückt werden und diese Kabel sind störungsunempfindlicher.
- Die Datenstruktur, welche über Ethernet verschickt wird, nennt sich „Frame“. Ein Frame gliedert sich in unterschiedliche Felder, welche alle nötigen Informationen enthalten, um die Daten zu verarbeiten.
- Die Adressierung in Ethernet sind MAC-Adressen. MAC-Adressen werden bei der Herstellung eines Gerätes vergeben und haben einen Adressbereich von 6 Bytes. Eine MAC-Adresse wird klassischer Weise durch mit Doppelpunkten getrennten hexadezimalen Werten dargestellt: 11:22:33:AA:BB:CC. Auch wenn MAC-Adressen theoretisch pro Gerät fest vergeben sind, lassen sie sich kopieren beziehungsweise fälschen. Dies nennt man „MAC-Spoofing“.
- Die maximale Übertragungsrate beträgt aktuell 10 Gbit/s.

Die Technologie Ethernet spezifiziert die Verwendung von Software (in Form von Protokollen) und Hardware für kabelgebundene Netzwerke.

Die Adressierung in Ethernet erfolgt mittels MAC-Adressen. Diese sind pro Gerät fest vergeben und lassen sich manipulieren („MAC-Spoofing“).

[23] IEEE steht für Institute of Electrical and Electronics Engineers und ist ein Berufsverband von Ingenieuren aus den Bereichen Elektrotechnik und Informationstechnik.
[24] Das als OSI-Referenzmodell bekannte System gliedert die Kommunikation von Netzen in sieben Schichten. Auf jeder Schicht werden durch Protokolle bestimmte Aufgaben ausgeführt. Dies ermöglicht eine modulare Entwicklung von Systemen, weil Schnittstellen zu den anderen Ebenen genutzt werden können. (Vergleiche Handbuch Netzwerksicherheit).
[25] Lichtwellenleiter werden auch als Glasfaser bezeichnet

Abbildung 9 zeigt ein CAT-7-Kabel[26] aus Kupfer. Die einzelnen Adern sind paarweise miteinander verdrillt (englisch „twisted pair“) und abgeschirmt, um die Störungswirkung untereinander und durch äußere Einflüsse zu verringern.

© Hurzelchen

Abbildung 9: CAT-7-Kabel

Abbildung 10 zeigt vereinfacht, wie Multimode und Monomode Glasfaser funktionieren. Bei Multimode werden mehrere störungsfrei Lichtwellen über dasselbe Kabel gesendet. Bei Monomode wird eine einzige Lichtwelle verwendet.

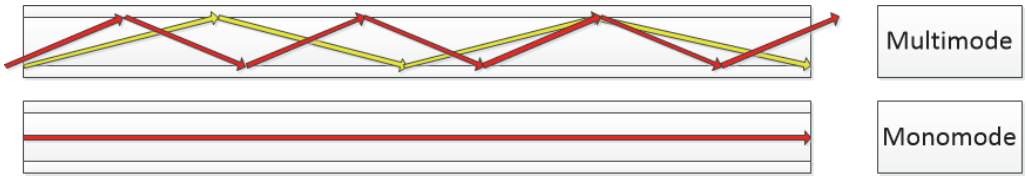


Abbildung 10: Multimode und Monomode Glasfaser

Die Tabelle 3 zeigt vier Ethernet-Standards mit deren maximaler Übertragungsgeschwindigkeit und welche Kabel mit welcher maximalen Länge verwendet werden können.

Standard	Geschwindigkeit	Kabelart und Länge
100BASE-TX	100Mbit/s	Kupfer: CAT-5;CAT-7; 100m
1000BASE-X	1Gbit/s	Kupfer: CAT-5;CAT-7; 100m
10GBASE-LRM	10Gbit/s	Fiber: Multimode; 220m
10GBASE-ER	10Gbit/s	Fiber: Singlemode: 40km

Tabelle 3: Ethernet-Standards in Zahlen

Wenn in Produktbeschreibungen die Rede von „LAN-Anschluss“, „Ethernet-Anschluss“, „1Gbit Ethernet“ und so weiter die Rede ist, bezieht sich dies auf die unterstützte Ethernet-Technologie. Ist von einer LAN-Verbindung die Rede, ist in der Regel eine kabelgebundene Verbindung zwischen zwei oder mehr Rechnern, nach diesem Standard gemeint.

Für weitere Informationen bezüglich Ethernet, nutzen Sie entsprechende Fachliteratur.

[26] *Die Kategorie (CAT) eines Kabels beschreibt dessen Leistungsvermögen in Bezug auf maximale Übertragungsfrequenz. Höhere Kategorien decken automatisch die darunterliegenden ab.*

Internet-Protokoll (IP)

Das Internet-Protokoll oder kurz IP, ist ein verbindungsloses Protokoll der Netzwerkebene. Es ist der Standard für aktuelle paketvermittlungsorientierte Netzwerke und wurde in der RFC[27] 791 (IPv4) beziehungsweise RFC 2460 (IPv6) definiert. Das Internet-Protokoll (IP) ist ein Protokoll der OSI-Schicht drei. Es wird paketvermittlungsorientiert genannt, weil die Datenstruktur des Internet-Protokolls sogenannte Pakete (IP-Pakete) sind. Hierbei wird ähnlich eines Paketversandes jedes Paket auf dem besten und schnellsten Weg an seinen Empfänger zugestellt.

Das Internet Protocol (IP) ist ein weit verbreitetes Netzwerkprotokoll der Vermittlungsschicht. Mit Hilfe von IP können Computer logisch adressiert und gruppiert werden. Es ist grundlegend für die Funktion des Internets und bietet die Basis für Routing. IPv4 wird nach und nach durch IPv6 abgelöst.

Die wichtigsten Fakten zu IP:

- Es gibt aktuell zwei Versionen von IP, welche verwendet werden: IPv4 und IPv6. Diese unterscheiden sich im Wesentlichen durch die Größe des Adressbereichs.
- IPv4 Adressen sind 32 Bit lang und ermöglichen somit die Adressierung von 2^{32} (~ 4 Mrd.) Empfängern. IPv4-Adressen werden für gewöhnlich im Dezimalsystem und durch Punkte getrennt angegeben: 123.123.123.123.
- IPv6 Adressen sind 128 Bit lang und ermöglichen damit die Adressierung von 2^{128} (~ 3,4 * 10^{38}) Empfängern. IPv6-Adressen werden durch hexadezimale Zahlen angegeben und werden durch Doppelpunkte getrennt:
  2013:0724:1414:45AF:84FF:2FAAD:23FE:1BBC
- Subnetzmasken: Bei IPv4 können über sogenannte Subnetzmasken, bei IPv6 Präfixlängen genannt, IP-Netze segmentiert werden beziehungsweise in Netz- und Hostadresse geteilt werden. Hierbei werden aufeinanderfolgende Bereiche eines IP-Adressbereichs an Grenzen getrennt, welche durch die Subnetzmaske vorgegeben werden. Angegeben werden Subnetzmasken meist durch einen Backslash „/“ und einer Dezimalzahl, welche die 1-Bits der Subnetzmaske darstellen. Beispielsweise gibt die Darstellung 192.168.100.50/25 an, dass die ersten 25 Bits der IP-Adresse zur Netzadresse gehören und die verbleibenden sieben Bits zur Adressierung der Hosts verwendet werden. Mit Hilfe von Subnetzmasken können einzelne Abteilungen eines Unternehmens getrennt werden. Um dies zu vereinfachen, werden heute Virtual-LAN (VLAN) (siehe Kapitel 1.5.3) verwendet, über die diese Netztrennung mit geeigneten Switches mit wenig Aufwand durchgeführt werden kann.

IPv4 Adressen haben 32 Bit (~4 Mrd.) und IPv6 128 Bit (~3,4 * 10^{38}) beziehungsweise 340 Sextillionen. Eine Sextillion ist eine Zahl gefolgt von 36 Nullen.

[27] *RFC steht für Request For Comments und bildet sowohl die Diskussionsgrundlage für einen Standard, als auch nach Abschluss der Diskussion den Standard selbst.*

Vergleich von IP und IPv6

Merkmal	IP	IPv6
Adressgröße	32 Bit	128 Bit
Adressanzahl	4*10^9	2^128 = 3.4*10^38
Header	13 Felder Ein Header	7 Felder -> Schnellere Verarbeitung durch Router Basis- und Zusatz-Header
Sicherheit	Keine Mechanismen zur sicheren Datenübertragung	Neue Merkmale: Authentifikation, Datenintegrität und Datenvertraulichkeit

Tabelle 4: Vergleich von IP und IPv6

<table>
<tr><td>Version</td><td>Header-länge</td><td>Service Type</td><td colspan="2">Gesamtlänge (in Bytes)</td></tr>
<tr><td colspan="3">Identifikation</td><td>Flags</td><td>Fragment-Offset</td></tr>
<tr><td colspan="2">Time To Live</td><td>Protokoll</td><td colspan="2">Header-Prüfsumme</td></tr>
<tr><td colspan="5">Quell-IP-Adresse</td></tr>
<tr><td colspan="5">Ziel-IP-Adresse</td></tr>
<tr><td colspan="4">IP-Optionen (falls vorhanden)</td><td>Füllzeichen</td></tr>
<tr><td colspan="5">IP Daten
(UDP-/TCP-Frame)</td></tr>
</table>

Abbildung 11: Header eines IPv4-Datenpaketes

Der abgebildete IPv4-Header besteht aus mehreren Feldern, die folgende Bedeutung und Funktionen haben:

- Version: Versionsnummer des verwendeten IP-Protokolls, mit dem das IP-Paket (Datagramm) erstellt wurde.
- Headerlänge: Dieses Feld bestimmt die Länge des IP-Headers in 32-Bit-Einheiten.
- Servicetyp: Kann die Wichtigkeit eines IP-Paketes mit diesem Feld festlegen und bestimmen, auf welche Art oder welchem Weg dieses IP-Paket übertragen werden soll, zum Beispiel mit geringer Verzögerung, mit hohem Datendurchsatz oder auf einer sicheren Route.
- Gesamtlänge: Die Länge des gesamten IP-Pakets in Bytes.
- Identifikation: Während der Übertragung kann ein IP-Paket in mehrere Fragmente aufgeteilt werden. Dabei wird jedes IP-Paket mit einer Identifikation versehen. Anhand dieser Identifikation und der Quell-Adresse kann ein fragmentiertes IP-Paket bei der Ankunft am Ziel-Rechnersystem wieder zusammengefügt werden.
- Flags: Das erste Bit legt fest, ob ein IP-Paket während der Übertragung fragmentiert werden darf. Das zweite Bit ist bei der Zusammensetzung einer

fragmentierten Nachricht von Bedeutung. Es bestimmt, ob die enthaltenen Daten aus der Mitte oder vom Ende der ursprünglichen Nachricht stammen.

- Fragment-Offset: Wenn eine Nachricht in mehrere Fragmente zerlegt wird, werden diese Fragmente der Reihe nach durchnummeriert und dann abgeschickt. Da die einzelnen IP-Pakete innerhalb des Netzwerks unterschiedliche Wege nehmen können, treffen die IP-Pakete beim Ziel-Rechnersystem nicht immer in der richtigen Reihenfolge ein. Dieser kann die Teile einer Nachricht erst dann wieder zu einer vollständigen Nachricht zusammensetzen, wenn er sämtliche Teile erhalten hat.
- Time to Live (TTL): Wenn ein IP-Paket vom Quell-Rechnersystem ins Netz geschickt wird, muss das Ziel-Rechnersystem nicht unbedingt erreichbar sein. In einem derartigen Fall würde das IP-Paket solange im Netz kursieren, bis das Ziel-Rechnersystem irgendwann bereit ist, das IP-Paket zu empfangen. Damit dies nicht passiert, wird vom Quell-Rechnersystem für jedes IP-Paket eine Lebensdauer in Sekunden festgelegt.
- Protokoll: In diesem Feld wird protokolliert, welche weiteren Protokolle in das IP-Paket eingebettet sind, zum Beispiel TCP, UDP oder ICMP.
- Header-Prüfsumme: Um die Unversehrtheit eines Headers zu gewährleisten, wird aus den vorhandenen Feldern eine Prüfsumme errechnet und vom Quell-Rechnersystem in dieses Feld eingetragen. Wenn das IP-Paket weitergeleitet wird oder am Ziel-Rechnersystem angekommen ist, wird die Prüfsumme neu berechnet und mit dem eingetragenen Wert verglichen.
- Quell-Adresse: Dieses Feld enthält die IP-Adresse des Quell-Rechnersystems (Absender).
- Ziel-Adresse: Dieses Feld enthält die IP-Adresse des Ziel-Rechnersystems (Empfänger)
- IP-Optionen: Dieses Feld dient hauptsächlich dem Testen von Netzwerken und der Fehlersuche. Hier können bestimmte Optionen festgelegt werden, die zum Beispiel Einschränkungen oder Informationen zur Weiterleitung der Daten enthalten.

Die IP-Adressen der Konditorei Herkerath werden durch den Router dynamisch[28] vergeben. Der Adressbereich ist 192.168.1.100 bis 192.168.1.199.

Protokolle der Schicht 4 – Transportschicht

Die Transportschicht stellt einen Transportdienst zwischen zwei Endsystemen bereit.

Die Transportschicht stellt einen netzunabhängigen Transportdienst zwischen zwei Endsystemen (end-to-end) bereit. Sie bildet die verschiedenen Netzdienste der Vermittlungsschicht mittels geeigneter Transportprotokolle, z.B. TCP und UDP auf den Transportdienst ab.

Ziel ist der sichere und bedarfsgerechte Transport von Nachrichten. Bedarfsgerecht bedeutet, dass die überlagerte Schicht die Möglichkeit der Auswahl von Güteparametern z.B. für Durchsatz, Verzögerung, Verfügbarkeit oder Restfehlerrate hat.

Aufgaben: Multiplexen und Splitten von Teilnehmer- oder Anwenderinstanzenverbindungen, Flusssteuerung

[28] *Der für die dynamische Vergabe von IP-Adressen zuständige Dienst heißt DHCP und ist in allen gängigen Heimroutern integriert. Der Client stellt eine Anfrage an das Netzwerk und erhält von dem DHCP-Server eine Antwort, welche eine IP-Adresse aus einem definiertem Bereich und deren Gültigkeitsdauer enthält.*

TCP

TCP stellt, unabhängig von diversen Netzeigenschaften, eine Ende-zu-Ende-Verbindung her

TCP[29] ist ein zuverlässiges und verbindungsorientiertes Transportprotokoll. Mit ihm kann eine zuverlässige Ende-zu-Ende-Verbindung hergestellt werden und sich dabei dynamisch an unterschiedliche Netzwerktopologien, Bandbreiten und weitere Merkmale anpassen. Das Protokoll sorgt für Fehlerbehandlung und stellt Reihenfolgenrichtigkeit her, da IP in diesen Punkten unzureichend ist. In den meisten Fällen ist das Protokoll im Kernel des Rechners implementiert.

UDP

Bei UDP handelt es sich um das zweite Protokoll auf der Transportschicht. Es ist ein unzuverlässiger, verbindungsloser Datagramm-Mechanismus. Die Anwendung muss selbst für die gewünschte Zuverlässigkeit sorgen.

Protokoll auf Schicht 5-7: DNS (Domain Name System)

- Aufgabe: Namensauflösung: Abbildung von Rechnernamen und E-Mail-Adressen auf IP-Adressen
- Arbeitet auf Anwendungsschicht (OSI-Schicht 5-7)
- Anwendungen, die den DNS-Service nutzen, sind z.B. HTTP(S), SMTP(S), FTP(S)

Um Rechnersystem-Namen entsprechende IP-Adressen zuordnen zu können, wurde in den Anfängen des Internets eine Liste der Rechnersystem-Namen von einem zentralen Server regelmäßig per Datenübertragung auf jedem Rechnersystem aktualisiert. Durch die rasante Ausbreitung des Internets ist diese Methode nicht mehr praktikabel. Aus diesem Grund wurde der Domain Name Service (DNS) entwickelt. Damit wurden die Rechnersystem-Namen nicht mehr auf jedem einzelnen Rechnersystem registriert, sondern auf speziell für diesen Dienst bereitgestellten Servern innerhalb jedes Teilnetzwerkes. Die einzelnen Rechnersysteme senden bei Bedarf Abfragen (Queries) an diese Namen-Server, die als Antwort die entsprechende IP-Adresse oder den dazugehörigen Rechnersystem-Namen liefern.

DNS dient der Umwandlung von Rechnersystemnamen in IP-Adressen. Jedes Teilnetzwerk muss einen verschlüsselten DNS-Server betreiben.

Um dieses System benutzen zu können, ist jedes Internet-Teilnetzwerk dazu verpflichtet, einen Domain-Namens-Server zu betreiben oder betreiben zu lassen, auf dem sich so genannte Zonen-Datenbanken befinden. In diesen Datenbanken befinden sich unter anderem zwei Tabellen, mit der einem bestimmten Rechnersystem-Namen die dazugehörige IP-Adresse zugeordnet werden kann und umgekehrt.

Prinzipiell muss beachtet werden, dass alle von einem DNS zur Verfügung gestellten Informationen missbraucht werden können, da diese Informationen nicht durch kryptographische Verfahren geschützt werden. Um Zugriff auf ein Rechnersystem eines Netzes zu erhalten, benötigt ein Eindringling zunächst dessen IP-Adresse, die er entweder durch blindes Probieren oder einfacher durch Auswertung der DNS-Informationen erhalten kann. Mittels dieser Informationen kann der Eindringling dann beispielsweise eine Adressfälschung (IP-Spoofing) vornehmen und damit Zugriff auf Rechnersysteme innerhalb des zu schützenden Netzes erhalten.

[29] *TCP: Transmission Control Protocol*

1.2.8 Dienstleistungsprotokolle

Neben Protokollen für die Datenübertragung werden auch begleitende Dienstleistungsprotokolle benötigt, welche auf der Vermittlungsschicht verwendet werden.

Die Vermittlungsschicht

Die Vermittlungsschicht transportiert die Pakete vom Start zum Ziel eines Endpunktes. Zu Ihren Aufgaben gehört das Durchqueren vieler Teilstrecken und den auf diesem Weg befindlichen Routern. Sie ist die unterste Schicht und muss zur Durchführung ihrer Aufgaben über die Topologie des Netzes Bescheid wissen.

Dienstleistungsprotokolle arbeiten auf der untersten Schicht und müssen die Netzwerktopologie kennen.

ARP (Address Resolution Protocol), RFC 826

Die Aufgabe von ARP ist es, den Hardware-Adressen entsprechende Netzwerkadressen zuzuordnen.
Um einen Rechner tatsächlich zu adressieren, wird die Hardware-Adresse (MAC-Adresse) des Rechners benutzt, nicht die IP-Adresse. Es muss also möglich sein, die IP-Adresse in eine MAC-Adresse umzusetzen und damit das Paket zum Partner zu übertragen.

Grundsätzlich gibt es drei Möglichkeiten:

- Statische Umsetzung
  - Die Tabelle muss von Hand gepflegt werden.
- Umwandlung der IP- in eine MAC-Adresse mit Hilfe einer Formel
  - nur möglich, wenn die MAC-Adresse frei wählbar ist
  - fehleranfällig und umständlich
- Dynamische Umsetzung durch Abfragen im Subnetz
  - dadurch werden Veränderungen der Ethernet-Adressen transparent
  - Address Resolution Protocol (ARP)

Ermittelte Adressen werden im sogenannten ARP-Cache zwischengespeichert. Dieser beinhaltet keine Sicherheitsfunktionen, sodass Adressen im Nachhinein leicht geändert werden können. Nutzen Angreifer dies aus, wird von ARP-Spoofing gesprochen. ARP-Spoofing ist die Basis einiger Angriffsszenarien.

ARP dient dazu, Hardwareadressen eine Netzwerkadresse zuzuweisen. Es gibt drei Möglichkeiten dies umzusetzen.

DHCP (Dynamic Host Configuration Protocol)

DHCP ist ein Anwendungsdienst und ermöglicht mit Hilfe eines entsprechenden Servers die dynamische Zuweisung einer IP-Adresse und weiterer Konfigurationsparameter wie Netzmaske, Gateway und DNS-Server an Rechnersysteme in einem Netzwerk.

DHCP weist dynamisch Konfigurationsparameter an Rechnersysteme im Netzwerk zu. Dies erfordert zusätzliche Administration und Planung.

Netzwerken bietet DHCP den Vorteil, dass bei Änderungen der Topologie nicht mehr alle betroffenen Workstations per Hand konfiguriert werden müssen, sondern die entsprechenden Vorgaben vom Administrator nur einmal in der Konfigurationsdatei des DHCP-Servers angepasst werden.

Auch für Rechner mit häufig wechselndem Standort (zum Beispiel Notebooks) entfällt die fehleranfällige Konfiguration - der Rechner wird einfach ans Netzwerk gesteckt und erfragt alle relevanten Parameter vom DHCP-Server.

Nachteil eines DHCP-Servers ist eine zusätzliche Belastung des Netzes durch viele Anfragen zwischen Clients und Server und einen zusätzlichen Aufwand für Administration und Planung.

1.2.9 Webprotokolle

HTTP (Hypertext Transfer Protocol)

Die Aufgabe von HTTP ist es, Daten zwischen Webclients und – Servern zu übertragen. Das Protokoll ist in RFC 2616 definiert. Es handelt sich um ein simples Anfrage-Antwort-Protokoll, welches auf TCP basiert. Es nutzt Port 80 und arbeitet auf der Anwendungsschicht (OSI-Schicht 5-7).

HTTP überträgt Daten zwischen Clients und Servern. HTTPS bietet zusätzliche Übertragungssicherheit durch Verschlüsselung mittels TLS/SSL.

HTTPS (Hypertext Transfer Protocol Secure)

Bei HTTPS handelt es sich um ein HTTP-Protokoll, das zur Übertragungssicherheit mit TLS/SSL verschlüsselt wird. Das Protokoll wird überall dort eingesetzt, wo verschlüsselte Datenübertragung gefragt ist. So zum Beispiel bei Transaktionen mit Authentifizierung. Grundlage für das Protokoll ist wieder TCP und es wird der Port 443 genutzt. Schicht Fünf wird durch SSL/TLS ersetzt, wodurch die Übertragungssicherheit eingeführt wird. Dadurch entsteht eine vertrauenswürdige Verbindung zwischen Client und Server. Die Schlüssel können über das Diffie-Hellman-Verfahren übertragen, wobei der öffentliche Schlüssel als digitales Zertifikat ausgetauscht wird.

TLS ist ein Sicherheitsprotokoll, welches verschlüsselte Kommunikation zwischen Client und Server ermöglicht.

TLS (Transport Layer Security)/SSL (Secure Socket Layer)

Seit 1999 ist SSL von TLS abgelöst worden. Ursprünglich unter RFC 2246 abgelegt, ist es heutzutage unter RFC 5246 zu finden. TLS ist ein applikationsunabhängiges Sicherheitsprotokoll, das logisch auf einem Transportprotokoll aufsetzt. Es unterstützt eine Vielzahl höherer Protokolle wie zum Beispiel HTTP, FTP, SMTP sowie Telnet[30] und weitere. Als Kern von TLS gilt die TLS-Datensatz-Protokollschicht, die einen sicheren Kanal zwischen Client und Server implementiert.

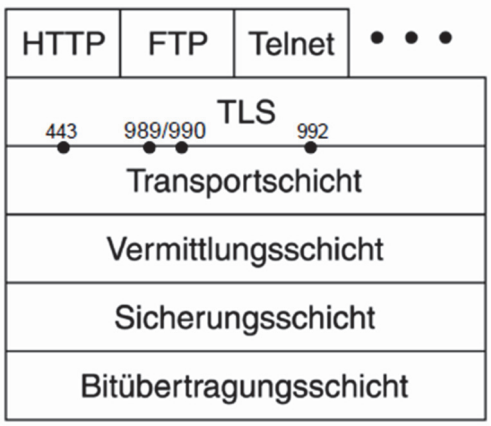


Abbildung 12: TLS im Protokollstack

[30] ***Telnet** – **Tel**etype **Net**work ist Programm für einen unverschlüsselten Austausch von zeichenorientierten Daten zwischen Client und Server. Für einen verschlüsselten Informationsaustausch wird daher heute SSH (Secure Shell) empfohlen.*

1.2.10 E-Mail-Protokolle

Den prinzipiellen Aufbau eines E-Mail-Systems zu kennen ist grundlegend für die folgend vorgestellten E-Mail-Protokolle IMAP(S), SMTP(S) und POP3(S). Das geklammerte (S) steht jeweils für die über TLS/SSL-abgesicherte Variante des Protokolls.

E-Mail-System bestehend aus zwei Teilsystemen und ist in Abbildung 13 dargestellt.

Einem Benutzeragenten (User Agent - UA), mit dem die Benutzer Nachrichten lesen/schreiben und senden/empfangen können.

Die User Agents sind lokale Programme, die eine auf Benutzerbefehle, Menüs oder Grafik basierende Methode für die Interaktion des Benutzers mit dem E-Mail-System bieten.

Auch der Versand von E-Mails basiert auf Protokollen. Nachrichten werden von Mailservern übermittelt.

Einem Nachrichtenübertragungsagenten (Message Transfer Agent - MTA), der die E-Mail zwischen den MTAs transportiert.

Der Message Transfer Agent (MTA) ist ein Prozess auf einem Server (Mail-Server), der die E-Mails im System (lokale Organisationen und/oder Internet) befördert.

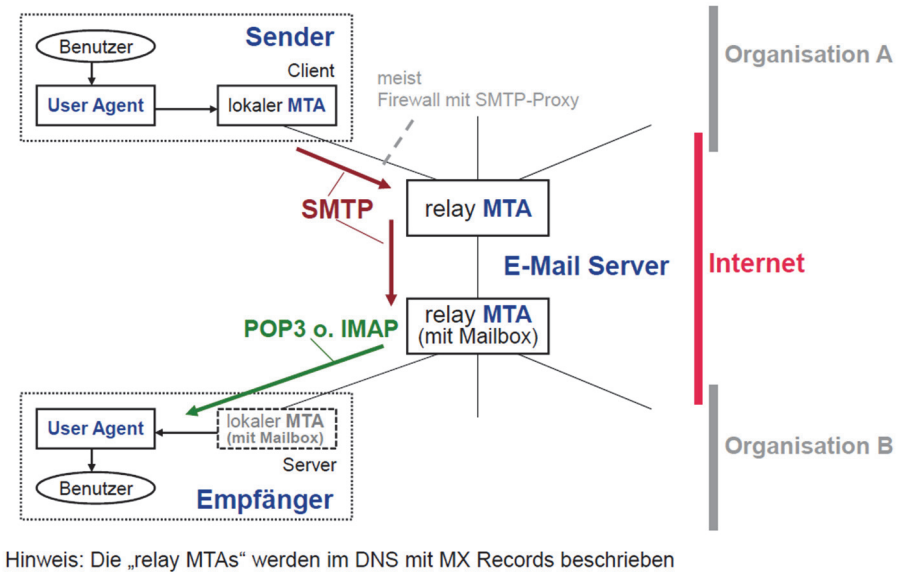


Abbildung 13: E-Mail-System

SMTP(S) (Simple Mail Transfer Protocol)

SMTP ist ein Protokoll aus dem Jahre 1982, dass E-Mails zwischen UA-MTA sowie zwischen den MTAs (in Organisationen und Internet) befördert werden. Es handelt sich um ein Client/Server-Protokoll. SMTP läuft auf Port 25 und wird mit STARTTLS abgesichert. Wird SMTP über TLS/SSL abgesichert spricht man von SMTPS.

POP3(S) (Post Office Protocol Version 3)

POP3 ist ein Protokoll, welches einen UA mit einem MTA verbinden kann und die E-Mails können von diesem MTA auf den UA kopiert werden. Über Port 110 wird eine TCP-Verbindung eingerichtet und es gibt nach dem erfolgreichen Verbindungsaufbau drei Zustände:

IMAP(S) (Internet Message Access Protocol)

Bei IMAP handelt es sich um ein Protokoll, welches es dem Benutzer erlaubt, auf dem MTA verschiedene Mailboxen zu halten und zu manipulieren. Es erlaubt dem Nutzer, E-Mails zentral zu verwalten. Der Verbindungsaufbau erfolgt über Port 143 und ist besonders empfehlenswert, wenn von verschiedenen Geräten auf ein Postfach zugegriffen werden soll. Das Herunterladen einer Mail muss bei diesem Protokoll explizit veranlasst werden. Dadurch, dass nichts lokal gespeichert wird, eignet sich dieses Protokoll besonders bei langsamen Internetverbindungen oder bei Geräten mit wenig Speicherplatz.

Es gibt drei vorherrschende Mail-Protokolle.

1.2.11 Übertragungssicherheit

IPSec

IPSec ist ein weltweiter Sicherheitsstandard für den geschützten IP-Datentransfer. Er wurde von der Internet Engineering Task Force (IETF) entwickelt. Ziel war es eine gemeinsame Sprache zu entwickeln, mit der Sicherheitsprodukte unterschiedlicher Hersteller miteinander kommunizieren können. IPSec ergänzt IPv4 um folgende Funktionen:

- Jedes Paket kann gegen Manipulation und vor Wiedereinspielung geschützt werden.
- Jedes Paket kann verschlüsselt werden.
- Die IP-Kommunikation kann gegen Verkehrsflussanalyse geschützt werden.
- Die Kommunikationspartner (Personen oder VPN-Gateways) können authentisiert werden (mehr Informationen zu VPNs finden Sie im Kapitel 4.2).

IPSec implementiert geschützten Datentransfer.

Um IPSec zu realisieren benötigt, werden zwei zusätzliche Header, nämlich Authentication Header und Encapsulated Security Payload. Des Weiteren sind Security Associations für die Policy, Verschlüsselungsalgorithmen und das Key-Management verantwortlich. Durch die Nutzung von Diffie-Hellman-shared secrets bleibt bei IPSec die gesamte Kommunikation zwischen zwei Kommunikationspunkten abgesichert.

X. 509

X.509 gilt als der Standard für digitale Zertifikate in einer Public-Key-Infrastruktur (PKI). Seit der ersten Standardisierung hat es drei Versionen gegeben. Die aktuelle dritte Version ist in RFC 5280 beschrieben. Ein X.509-Zertifikat wird immer an einen Namen, E-Mail-Adresse oder seit Version drei an einen DNS-Eintrag gebunden. Das Zertifikat enthält wichtige Informationen wie zum Beispiel das Verschlüsselungsverfahren des öffentlichen Schlüssels und den öffentlichen Schlüssel selbst. Des Weiteren ist die zertifizierende Organisation vermerkt. Die Zertifikate können an den Dateinamenserweiterungen „.cer“ oder „.pem“ erkannt werden.

X.509-Zertifikate enthalten den Public-Key der Organisation, für die das Zertifikat ausgestellt wurde.

SSH (Secure Shell)

Bei SSH handelt es sich um Protokolle, mit der eine sichere Verbindung zu einem entfernten Gerät hergestellt werden kann, um dieses Gerät zum Beispiel aus der Ferne zu warten. Das Protokoll wurde ursprünglich entwickelt um unsichere Protokolle wie Telnet und RSH[31] zu ersetzen. Mit Hilfe von SSH können verschiedene TCP/IP-Verbindungen getunnelt werden, so dass der Netzwerkverkehr verschlüsselt wird. PuTTY[32] ist eine SSH-Lösung, die bei Microsoft Windows und Unix Systemen zum Einsatz kommt. Eine freie Implementierung von SSH ist OpenSSH.

Mit Hilfe von SSH kann eine verschlüsselte Tunnel-Verbindung zu einem entfernten Gerät hergestellt werden.

[31]RSH – Remote Shell ist eine veraltetes Programm zur Wartung beziehungsweise zum Fernzugang, das unter dem Betriebssystem UNIX verwendet wurde.
[32]http://www.chiark.greenend.org.uk/~sgtatham/putty/ -freie Software zur Herstellung von SSH-Verbindungen.

1.3 Informationssicherheit als Grundvoraussetzung

Wozu brauchen wir Sicherheit in der Informationstechnik?
Ein PC, wie er in den meisten Handwerksbetrieben vorhanden ist, hat heute in etwa die gleiche Leistungsfähigkeit wie ein kleines Rechenzentrum in den Achtzigerjahren. Bei diesen Rechenzentren genügten noch Sicherheitsmaßnahmen, die mithilfe von organisatorischen und personellen Regelungen durchgeführt wurden. Dazu gehörten unter anderem:

- Zugangskontrollen zu den Gebäuden und Räumen der Rechenzentren.
- Kontrollierte und definierte Arbeitsabläufe und entsprechende Auftragsabwicklung.
- Trennung zwischen Personal der Fachabteilung (Anwendern) und DV-Mitarbeitern (Programmierern, Operateuren usw.).

Sicherheit in der IT wird immer notwendiger, da sie ins Zentrum von Unternehmen rückt. Strategische Sicherheitskonzepte sind nötig, um die Sicherheit zu gewährleisten.

Die EDV stand abgeschottet in einem Gebäude, wodurch die externen Bedrohungen überschaubar waren und das Betriebssystem des Hosts war für den Schutz der Ressourcen vor unerlaubtem Zugriff zuständig.
Durch moderne informationstechnische Konzepte wie Client-Server, Down-Sizing, Out-Sourcing, Internet, Intranet und so weiter, in denen Informationen über ein angreifbares Netz ausgetauscht werden, ist besonders die Sicherheit und die Verfügbarkeit der Daten bedroht.
Außerdem sind die informationstechnischen Sicherungen von Arbeitsplatzrechnern, insbesondere von PCs, wesentlich schwächer als die von klassischen Großrechnern. Der Benutzer eines Arbeitsplatzrechners kann heute gleichzeitig Anwender, Operator oder Programmierer sein, was neue Risiken mit sich bringt.

Die heutigen verteilten Rechnersysteme lassen sich nicht mehr allein durch organisatorische Maßnahmen schützen. Es müssen zusätzliche technische Sicherheitsmechanismen bereitgestellt werden, die eine sichere und beherrschbare Informationsverarbeitung ermöglicht. Dazu sind strategische Sicherheitskonzepte notwendig, die Vertraulichkeit, Integrität und Verfügbarkeit von Rechnersystemen, Daten, Programmen und Personen als wesentliche Bestandteile von Organisationen aufbauen und erhalten. Außerdem müssen Verbindlichkeit und Zurechenbarkeit der Vorgänge und Veranlassungen – wo immer notwendig – garantiert werden.

1.3.1 IT-Sicherheit in der Informationsgesellschaft

Welche Rolle spielt IT-Sicherheit in der Informationsgesellschaft?
In den letzten Jahren haben sich die Werte der Informationen und damit der Schutzbedarf beträchtlich vergrößert.

Der steigende Wert von Informationen auf Rechnersystemen ist ein wichtiger, wenn nicht der wichtigste Wirtschaftsfaktor geworden.
Beispiele hierfür sind:

- Vollständige Entwicklungs- und Fertigungsunterlagen
- Geschäfts- und Betriebsergebnisse, Strategiepläne
- Logistikinformationen: Falls Rechnersysteme oder Daten nicht mehr verfügbar sein sollten, weiß kein Mitarbeiter mehr, wie groß das Lager ist, was produziert werden soll, welche Kunden was bestellt haben und wann an wen geliefert werden soll.
- Kundendaten stellen einen erheblichen Wert dar, den es zu schützen gilt.

Rechnersysteme ermöglichen eine effiziente Verarbeitung und rationelle Abwicklung von Aufgaben, die in vielen Bereichen anders kaum noch zu erfüllen sind. Wir sind in solchem Ausmaß von Rechnersystemen abhängig, dass unsere wirtschaftliche Leistungsfähigkeit gefährdet ist, wenn die Funktionsfähigkeit der Rechnersysteme nicht in angemessener Weise gewährleistet werden kann. Die meisten Geschäftsprozesse wurden in der Vergangenheit auf dem Papier (zum Beispiel Angebotserstellung, Auftragsannahme, Bestellungen, Liefereingang) oder persönlich (z.B. bei Kundenbesuchen) abgewickelt. Diese Abläufe können weitaus rationeller gestaltet werden, indem der personelle und materielle Aufwand durch elektronische Verfahren ersetzt wird. Alle oben aufgezählten Geschäftsprozesse können per Rechnersystem erstellt und elektronisch übertragen werden, sodass kein Medienbruch mehr auftritt.

Die Funktionalität von Rechnersystemen ist essentieller Bestandteil für wirtschaftliche Leistungsfähigkeit.

1.3.2 IT-Sicherheit als Wirkungs- und Handlungszusammenhang

IT-Sicherheit beschäftigt sich mit dem Schutz von Werten gegen Angriffe, wobei Angreifer das Ziel haben, die Werte für eigene Zwecke zu nutzen oder den Eigentümer zu schädigen:

Die Sicherung der Werte (Assets) liegt in der Verantwortung des Eigentümers (Owner) der Werte. Die Angreifer (Threat agents) wollen mit einem Angriff (threats) auf die Werte auch deren Vorteile ausnutzen und handeln somit gegen den Eigentümer der Werte. Der Eigentümer nimmt den Angriff als Reduzierung seiner Werte wahr – sofern er ihn bemerkt.

Die Gewährleistung der IT-Sicherheit und somit auch die Haftbarkeit bei Schäden, die durch Kompromittierung dieser entstehen, liegen in der Verantwortung des Eigentümers.

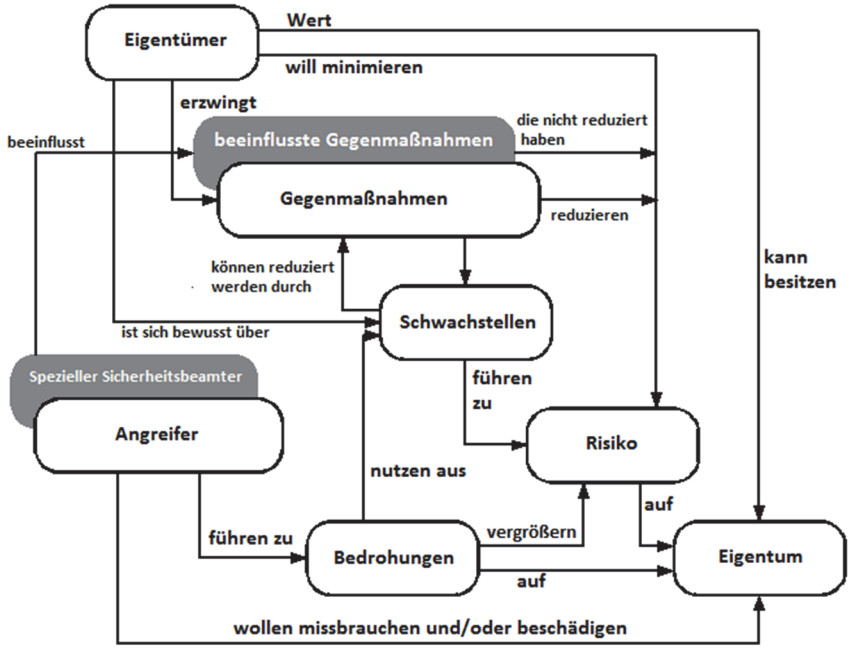


Abbildung 14: Bedrohungen für Informationswerte

Spezielle Angreifer (zum Beispiel Geheimdienste) sind in der Lage, die Hersteller von Gegenmaßnahmen zu beeinflussen, damit diese Möglichkeiten einbauen, die es diesem Angreifer erlauben, trotz der Gegenmaßnahmen auf die Werte zuzugreifen.

Für den Eigentümer bedeutet dies wiederum eine Reduzierung seiner Werte und ist als »trügerische Sicherheit« in Wirklichkeit eine Scheinreduzierung seines Risikos.

Die Angriffe auf IT-Werte beziehen sich in der Regel – aber nicht ausschließlich – auf: Informationen und Daten, Ressourcen oder Dienstleistungen. Ein Schutz dieser zu schützenden Objekte kann nur gewährleistet werden durch die Gewährleistung von Authentizität, Integrität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit, sowie Anonymisierung und Pseudonymisierung.

1.3.3 Gefahren nicht geschützter Netzwerke

Nicht geschützte Netzwerke machen es einem potentiellen Angreifer sehr einfach an die essentiellen Werte innerhalb eines Unternehmens zu kommen. Es ist wichtig in allen Ebenen eines Unternehmens für die Sicherheit des Netzwerks und der Anwendungen in ihm zu sorgen.

1.3.4 Vorteile geschützter Netzwerke

Geschützte Netzwerke machen es einem Angreifer schwer, an die kritischen Werte in einem Unternehmen zu kommen. Will ein Angreifer in ein geschütztes Netzwerk eindringen, benötigt er wesentlich mehr Ressourcen und Know-How. Es gilt die 80/20-Regel bei dem Schutz von Netzwerken. Das heißt 20% der möglichen Sicherheitsmaßnahmen*, bringen Schutz vor 80% der Angriffe, während für die übrigen 20% an Sicherheit, 80%* der Maßnahmen *benötigt werden. Ein kleines Investment in die Sicherheit bietet einen großen Schutz.*

1.3.5 Die wichtigsten Netzwerkkomponenten

Ein Netzwerk besteht aus mehreren Komponenten. Diese können nach dem Baukasten-Prinzip einfach hinzugefügt, ersetzt oder entfernt werden. Wichtige Gruppen sind hierbei die Netzkoppelelemente, Firewall Elemente sowie Peripheriegeräte.

Netzkoppelelemente

Netzkoppelelemente verbinden zwei Netze, die aufgrund technischer oder geographischer Gegebenheiten nicht direkt durch ein Kabel gekoppelt werden können. Im allgemeinen Fall sind dies Stationen an zwei Netzen, welche durch ihre Funktion eine Verbindung zwischen den Netzen herstellen.

- Ein Beispiel:

Die Konditorei Herkerath hat ein lokales Netzwerk aufgebaut und möchte dieses nun mit dem Internet verbinden. Das Unternehmensinterne LAN soll nun an das Internet angeschlossen werden. Hierfür wird ein Router benötigt, der Netzwerkpakete zwischen den Rechnernetzen weiterleiten kann.

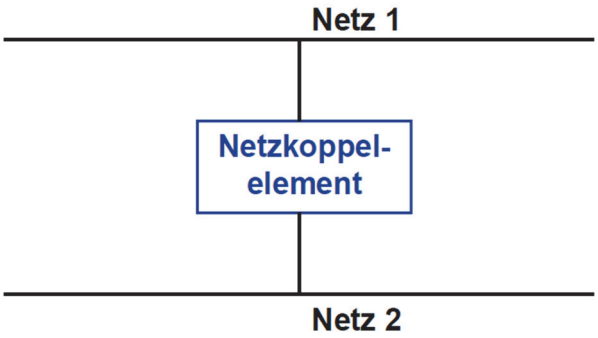


Abbildung 15*: Netzkoppelement*

Switch

Abbildung 16: Rückansicht eines Switches

Ein Switch ist eine Netzwerk-Hardwarekomponente, welche für die Verbindung von Maschinen desselben Netzwerks verwendet wird.
Grundlegend existieren zwei Kategorien von Switches, Layer-2 und Layer-3. Die Layer-2-Switches arbeiten nur auf der OSI-Schicht zwei und verarbeiten damit nur Adressierung mittels MAC-Adressen. Als Erweiterung sind Layer-3-Switches in der Lage auf der OSI-Schicht drei zu arbeiten beziehungsweise Adressierungen mittels IP-Adressen zu verarbeiten. Sie sind somit eine Kombination aus Switch und Router. Die Intelligenz des Switches ist so ausgelegt, dass bekannt ist, welche Geräte beziehungsweise MAC-Adressen, an welchem Netzwerkanschluss angekoppelt sind. Erhält der Switch nun ein Frame für ein Gerät, leitet dieser es an den entsprechenden Anschluss weiter. In den heutzutage verwendeten Heimroutern sind meistens 4-Port-Switches integriert um ein Heimnetz aufzubauen.

Switches dienen zur Verbindung von Geräten desselben Netzwerks. Sie arbeiten mit MAC-Adressen und werden auch als Multiport- Bridge bezeichnet.

Bridge

Die Idee hinter Bridges ist es, ein lokales Datenaufkommen durch die Bildung von logischen Teilnetzen vom restlichen Netzwerk zu entkoppeln. Bridges arbeiten auf Schicht 2 des OSI-Modells. Sie ermöglicht es, bestimmte Beschränkungen bei Zugriffsverfahren zu überwinden und leitet nur die benötigten Pakete weiter. Eine Spezialform der Bridge bildet die MAC-level Bridge, welche Netzsegmente mit gleichem Medienzugangsprotokoll, zum Beispiel Ethernet, miteinander verbindet. Die Bridge leitet im Gegensatz zum Router weniger Daten durch und hat eine geringere Portdichte.

Bridges entkoppeln lokales Datenaufkommen durch Bildung von logischen Teilnetzen.

Abbildung 17: Netzwerk-Bridge

Hubs arbeiten wie ein Bus, bieten dadurch keinen geregelten Datenaustausch und sollten durch Switches ersetzt werden

Hub

Hubs arbeiten auf Schicht 1 und können als Vorgänger der Switches gesehen werden. Im Netzwerk eingesetzt bilden sie physikalisch immer eine Sterntopologie, sind logisch jedoch nichts anderes als ein Bus aufgebaut, da jede versendete Information alle Teilnehmer erreicht. Aus Sicherheitsaspekten müssen Hubs durch Switches ersetzt werden, damit ein geregelter Datenaustausch zwischen Sender und Empfänger stattfinden kann. Neben diesem Sicherheitsaspekt ist ein weiterer Grund für das Austauschen, dass ein Hub für einheitliche Geschwindigkeit auf allen Ports sorgt.

Abbildung 18: Netzwerk-Hub

Managed-Switch

Ein Managed-Switch hat dieselben Aufgaben wie ein normaler Switch, verfügt allerdings über programmierbare Ports, über die sich ein VLAN[33] aufbauen lässt (siehe Kapitel 1.5.3).

WLAN-Adapter

Ein WLAN-Adapter ist ein Gerät, welches meist mit Hilfe eines USB-Anschluss an einen Rechner angeschlossen werden kann, um eine Netzverbindung herzustellen. Diese Lösung wird häufig verwendet, wenn der Rechner über keine Netzwerkkarte verfügt.

[33] *VLAN: Virtual LAN ist ein logisches Teilnetz innerhalb eines Netzwerks oder Switch*

Router

Abbildung 19: Rückansicht eines WLAN-Routers

Router sind wie Switches eine Netzwerkkomponente. Sie dienen der Verbindung von unterschiedlichen Netzen und leiten die Netzwerkpakete zwischen diesen weiter. Ein weit verbreitetes Beispiel ist der WLAN-Router in vielen Privathaushalten. Dieser verbindet das Heimnetzwerk mit dem Internet. Die Heimrouter weisen im Gegensatz zu klassischen Routern jedoch eine erweitere Funktionalität auf und übernehmen die Aufgabe von mehreren Geräten, unter anderem die eines Access-Points[34] und eines Switches und bieten oft Schutzfunktionen wie Firewalls. Router sind Geräte der OSI-Schicht drei und werden auch dazu genutzt, um zwischen unterschiedlichen Protokollen zu vermitteln.

Router verbinden unterschiedliche Netze und arbeiten auf OSI-Schicht drei mit IP-Adressen. Sie sammeln Informationen über den Zustand des Netzes und nutzen diese, um die IP-Pakete zum Ziel weiterzuleiten.

Der Router der Konditorei Herkerath ist ein handelsübliches Gerät des Internetanbieters und wurde entsprechend der mitgelieferten Anleitung konfiguriert. Dieser stellt über den nachgeschalteten 16-Port-Switch (Layer-2) allen Maschinen den Internetzugang bereit. Der Router bietet eine Firewall-Funktion, welche jedoch nicht speziell konfiguriert wurde.

Gateway

Durch ein Gateway werden Netze ab der 4. Schicht - der Transportschicht, oder höher miteinander gekoppelt. Die Netzwerke die miteinander verbunden werden haben meist nichts gemeinsam. So kann das eine Netzwerk mit der Protokollfamilie TCP/IP arbeiten und das zu verbindende Netzwerk arbeitet mit Hilfe von SNA[35] oder DECnet[36]. Die Software eines Gateways muss also in der Lage sein, einen Übergang zwischen den unterschiedlichen Protokollen zu ermöglichen. Ein weiteres Beispiel ist ein SMS-Gateway, welches es ermöglicht SMS-Nachrichten auf anderen Geräten als Mobiltelefonen zu empfangen.

Gateways ermöglichen einen Übergang zwischen unterschiedlichen Protokollen.

Abbildung 20: Rückansicht eines Gateways

[34] *Access-Points sind WLAN-Schnittstellen. Weitere Informationen im Handbuch WLAN-Sicherheit.*
[35] *Systems Network Architecture – hierarchische Netzwerkorganisation entwickelt von IBM in den 70er-Jahren*
[36] *Digital Equipment Corporation Network: Von der DEC im Jahre 1975 eingeführtes, homogenes Netzwerk zum Vernetzen ihrer Minicomputer*

Netzwerkkarte

Die Netzwerkkarte verbindet ein Endgerät direkt mit einem Netzwerk.

Bei der Netzwerkkarte handelt es sich um eine Platine oder eine andere Hardwarekomponente, die das Endgerät direkt mit dem Netzwerk verbindet. Dadurch ist sie die physikalische Schnittstelle zum Netzwerk und übertragt Daten. Zusätzlich hat sie allgemeine Kommunikationsfunktionen, wie zum Beispiel Funktionen der Kompression oder Flusskontrolle.

Firewall-System

Ein Firewall-System kontrolliert die Kommunikationsdaten und reglementiert die ein- und ausgehenden Verbindungen.

Ein Firewall-System wird als Schranke zwischen das zu schützende Netz und das unsichere Netz geschaltet, sodass der gesamte Datenverkehr zwischen den beiden Netzen nur über das Firewall-System möglich ist. Auf dem Firewall-System werden Sicherheitsmechanismen implementiert, die diesen Übergang sicher und beherrschbar machen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitspolitik, protokolliert sicherheitsrelevante Ereignisse und alarmiert bei starken Verstößen den Security- Administrator.

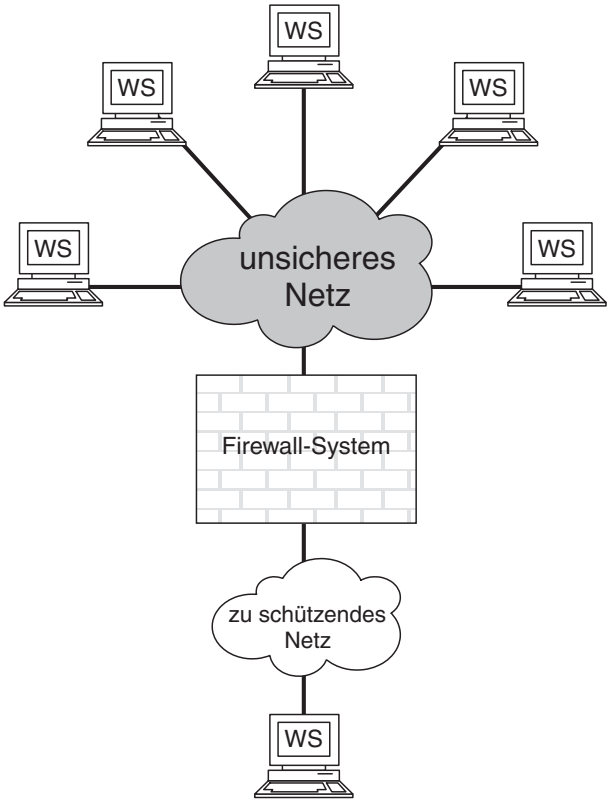


Abbildung 21: Firewall-System

Peripherie und Wechselmedien

Externe Quellen und Medien werden als Peripheriegeräte bezeichnet. Drucker sind ein häufig angewandtes Peripheriegerät im Netzwerk.

Allgemein ist ein Peripheriegerät ein Gerät, welches mit vorher definierten Rechnereinheiten kommunizieren kann. Da es sich meist um Eingabe-, Ausgabe oder Speichergeräte handelt, kann es Daten Senden und Empfangen. Klassische Peripheriegeräte sind Maus, Tastatur und Bildschirm. Innerhalb eines Netzwerks kann zum Beispiel ein Drucker mit mehreren Rechnern verbunden werden, damit von allen Rechnern innerhalb des Netzwerks über den verbundenen Drucker gedruckt werden kann. Dadurch können Kosten eingespart werden, da nicht jeder User einen eigenen

Drucker benötigt und spezielle Druckaufträge, wie zum Beispiel Farbdruck, verarbeitet werden können.

1.3.6 Zusammenfassung

Überblick Netzkoppelelemente:

Die Umgehung der physikalischen Begrenzung der Ausdehnung eines lokalen Netzes kann mit Hilfe von Repeater / Hubs realisiert werden.

Das lokale Datenaufkommen kann durch die Bildung von logischen Teilnetzen vom restlichen Netzwerk zu entkoppeln werden. Hierzu sind Bridges/Switches besonders gut geeignet.

Teilnetze können mit Routern zu einem Netz für den bereichsübergreifenden Verkehr verbunden werden.

Um Netze mit unterschiedlichen Protokollarchitekturen miteinander zu koppeln, können Gateways verwendet werden.

Gewährleistung der Sicherheit im internen Netzwerk (Firewall)

Mit Hilfe von Firewalls kann die Sicherheit von internen Netzwerken gesichert werden.

Netzwerke können durch Endgeräte (Peripheriegeräte) erweitert werden.

1.4 Sicherheitsmodule im Netzwerk

Sicherheitsmodule sind Peripheriegeräte die dafür sorgen, dass die Vertrauenswürdigkeit und Integrität eines IT-Systems gesichert werden kann. Mit Hilfe von effizienter und sicherer Ausführung von kryptographischen Operationen werden geschäftskritische IT-Systeme geschützt. Dafür kann es nötig sein, die kryptographischen Schlüssel mit Hilfe von Software zu schützen, um physikalische Angriffe oder Seitenkanalangriffe auszuschließen.

Sicherheitsmodule sorgen für den Schutz geschäftskritischer IT-Systeme.

1.4.1 Chip-basierte Module

Chip-basierte Module sind Module, welche die kryptographischen Operationen und Applikationen auf einem Chip gespeichert haben. So sind Smartcards ein Beispiel für solche Chip-basierten Module, aber auch eine VISA- oder EC-Karte beinhaltet ein solches Sicherheitsmodul. Dort liegen relevante Daten, im Normalfall, nicht im Klartext vor, sondern müssen durch einen Schlüssel – die PIN-Nummer (kurz PIN) – entsperrt werden.

Chip-basierte Module sind Smartcards, die kryptographische Operationen auf einem Chip gespeichert haben.

Smartcard

Eine »intelligente Chipkarte« (»Smartcard«) ist ein IT-System in der genormten Größe der EC-Karte, das dem Nutzer Sicherheitsdienstleistungen zur Verfügung stellt.
Eine Smartcard enthält:

- einen Prozessor (CPU)
- Arbeitsspeicher (RAM)- und ROM (read-only memory)-Speicher
- ein »schlankes« Betriebssystem im ROM

- eine I/O-Schnittstelle, über die die gesamte Kommunikation stattfindet (Kontaktflächen oder kontaktloses Interface)
- einen EEPROM (*electrically erasable programmable read-only memory)*, auf dem die geheimen Schlüssel, z.B. ein privater RSA-Schlüssel oder andere symmetrische Schlüssel, sowie persönliche Daten (Passworte etc.) sicher gespeichert sind
- Sonstiges, beispielsweise einen Co-Prozessor, der symmetrische oder asymmetrische Verschlüsselung sehr schnell durchführt (Krypto-Prozessor)

1.5 Getrennte Netze

Durch die Trennung von Computernetzen können beispielsweise Verwaltungsnetze sicher von Produktionsnetzwerken abgeschottet werden. In den folgenden Abschnitten werden einige gängige Techniken dargestellt.

1.5.1 Subnetze

Idee

- Trennung eines Netzwerks in Teilnetzwerke, im Handwerksbetrieb zum Beispiel mit dem Ziel, Produktion und Verwaltung zu trennen

Vorteile

- Lösung mit einfachsten Mitteln
- Keine zusätzliche Hardware benötigt
- Schnelle Berechnung der IP-Adressen mit Hilfe von Tools (beispielsweise http://www.heise.de/netze/tools/netzwerkrechner)

Subnetting separiert Netze voneinander, dies bietet allerdings keinen umfassenden Schutz, da es umgangen werden kann.

Das Bilden von Subnetzen, dass sogenannte Subnetting, ermöglicht durch die Konfiguration der Netzwerkschnittstellen in den Geräte, dass diese miteinander kommunizieren können oder, je nach Anwendungsfall, nicht miteinander kommunizieren können. Die Konfiguration benötigt keine spezielle Hardware, lediglich die Netzwerkeinstellungen müssen angepasst. Aus diesem Grund ist dies eine kostengünstige Möglichkeit der Netzseparierung.

Einen umfangreicheren Exkurs zum Thema „Subnetting“ und ein dazu passendes Praxisbeispiel finden Sie im Handbuch „IT-Sicherheit in der Produktion“.

1.5.2 Network Address Translation (NAT)

NAT bezeichnet das Ändern von Quell- und Zieladressen und -ports (NAPT, Network Address Port Translation) in IP-Paketen beim Versenden über einen entsprechend konfigurierten Router mittels sogenanntem „Masquerading“.

- Standard in Routern

NAT ist die Änderung von Quell- und Zieladressen/ports durch das Ersetzen von Adressinformationen in Datenpaketen. Dadurch können IP-Adressen gespart werden.

lokales Netz (LAN)

Quell IP:Port	Ziel IP:Port
192.168.0.2:5000	170.0.0.1:80
192.168.0.3:5000	170.0.0.1:80
192.168.0.5:5001	170.0.0.1:80

Router
==========>
Masquerading

öffenliches Netz (WAN)

Quell IP:Port	Ziel IP:Port
205.0.0.2:6000	170.0.0.1:80
205.0.0.2:6001	170.0.0.1:80
205.0.0.2:6002	170.0.0.1:80

Abbildung 22: Masquerading

Einfacher dargestellt bedeutet dies, dass beispielsweise private Netzwerke hinter einem Router vor der Erreichbarkeit aus dem Internet geschützt werden. Nach außen sind alle internen Netzwerkteilnehmer hinter der durch den Internet-Service-Provider zugewiesenen IP-Adresse des Routers verborgen. Anfragen aus dem privaten Netzwerk hin zu einem Service im Internet werden so mittels Masquerading auf die Router IP-Adresse und einem speziell zugewiesenen Port (205.0.0.2:6000 siehe Abbildung 22) übersetzt. Die Antworten von einem Service im Internet werden wiederum über

den Router an die zugewiesene IP-Adresse des internen Netzwerkteilnehmers zurückvermittelt.
Vorteile dieser Technik sind Einsparungen bei der Vergabe von IP-Adressen, da nach außen nur eine IP-Adresse für ein größeres Privates Netzwerk benötigt wird. Zudem wird die Sicherheit erhöht, was die Informationssammlung und das Ausspähen von Sicherheitslücken der internen Netzwerkteilnehmer verhindert. Nachteile des Masqueradings sind unter anderem, dass NAT-Gateways nicht mit dem OSI-Modell konform sind. Es kann zu Protokollkomplikationen durch umgeschriebene Header kommen und die Ende-zu-Ende-Konnektivität kann eingeschränkt sein, da Zieladressen in einem privaten Netzwerk verschleiert sind. Des Weiteren ist es problematisch für Netzwerkdienste die auf Rückkanäle angewiesen sind, wie zum Beispiel die IP-Telefonie.

1.5.3 VLAN (Virtual Local Area Network)

Mit VLAN werden Netzwerke auf Ethernet-Ebene separiert. Die Trennung kann individuell gestaltet werden.

Mit Virtual LAN oder VLAN ist ein Teil der Ethernet-Technologie gemeint. Die Verwendung von VLAN erlaubt es bei entsprechender kompatibler Hardware, Netzwerke in logische Teilnetzwerke zu trennen. Hierbei weiß die Hardware, meist ein konfigurierbarer Switch, an welchem Port welche Maschine angebunden, beziehungsweise welches Teilnetz angeschlossen ist. Je nach Einstellung kann die Kommunikation zwischen Teilnetzen erlaubt oder verboten werden. VLANs sind also ein Werkzeug für die Netzseparierung auf Ethernet-Ebene. Die Trennung kann hierbei völlig individuell gestaltet werden. Ein Beispiel für ein VLAN mit einem Switch ist in Abbildung 23 zu sehen, hier ist ein gesamtes Netzwerk in zwei Teilnetze aufgespaltet.

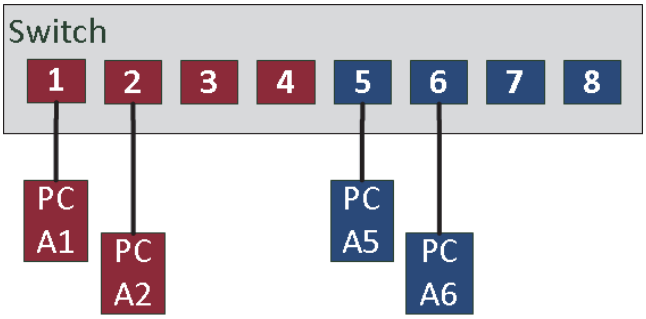


Abbildung 23: VLAN-Switch mit zwei VLANs

VLAN-fähige Hardware ist zwar in der Anschaffung teurer als herkömmliches Netzwerkequipment, dafür kann es jedoch einfach konfiguriert werden und bietet eine hohe Flexibilität.

Auch die Verbindung von VLANs über mehrere Switches ist möglich, wie in Abbildung 24 dargestellt.

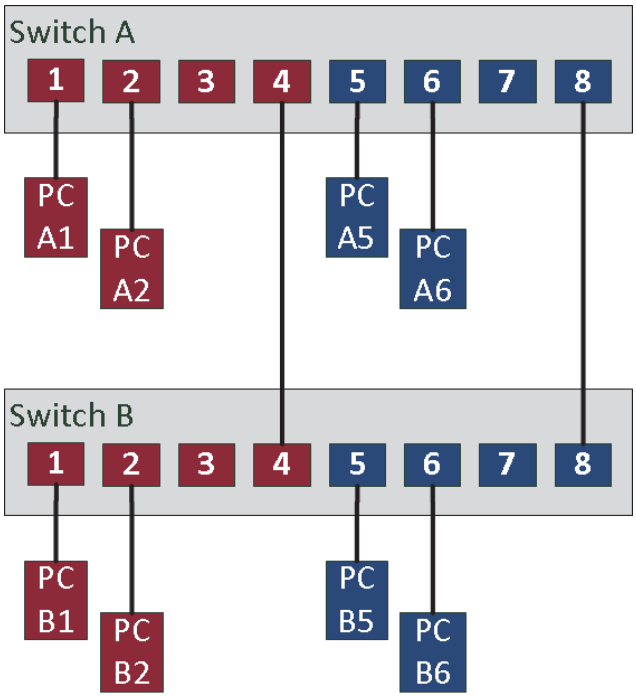


Abbildung 24: Zwei VLANs mit zwei Switchen

1.5.4 NAC – Network Access Control

Network Access Control (NAC) ist eine Technologie, mit der der Zugang zu einem Rechnernetzwerk, abhängig vom Benutzer und der Integrität des zum Zugriff eingesetzten Rechnersystems, gesteuert wird. Ein Rechnersystem muss demnach die durch das Netzwerk vorausgesetzten Regeln erfüllen.

NAC ist eine regelbasierte Zugriffskontrolle für Rechnersysteme.

Wird durch ein Rechnersystem eine Verbindung zu einem Netzwerk aufgebaut, findet neben einer Nutzerauthentifizierung eine Überprüfung des eingesetzten Rechnersystems statt. Diese Überprüfung basiert auf Messungen der Konfiguration des Rechnersystems und einem Vergleich dieser Messung mit Sicherheitsrichtlinien des Netzwerks. Rechnersysteme mit einer, aus Sicht des Netzbetreibers, fehlerhaften Konfiguration, beispielsweise veraltete Antivirensignaturen oder ein nicht aktuelles Betriebssystem, kann entdeckt und präventiv dem Netzwerk mit anderen angeschlossenen Rechnersystemen und angebotenen Diensten fern gehalten werden.

1.6 Einführung in die Kryptographie

Vertraulichkeit von Daten als grundlegender Sicherheitsdient.

In der elektronischen Geschäftswelt benötigen wir als grundlegenden Sicherheitsdienst Vertraulichkeit, damit kein Unautorisierter in der Lage ist, die gespeicherten oder übertragenen Informationen zu lesen. Mithilfe der Verschlüsselung kann eine Vertraulichkeit der Daten während der Speicherung und Übertragung erzielt werden.

1.6.1 Grundlagen der Verschlüsselung

Es gibt unterschiedliche Möglichkeiten, die Verschlüsselung von Daten bei der TCP/IP-Kommunikation durchzuführen.

Sicherheitsfunktionen können entweder auf Applikations- oder Kommunikationsebene angewendet werden.

Eine erste Möglichkeit ist die Integration von Sicherheitsfunktionen auf der Applikationsebene, zum Beispiel Verschlüsselung in einer E-Mail-Anwendung. Eine weitere Möglichkeit ist die direkte Integration von Sicherheitsfunktionen in den Kommunikations-Stack, wie zum Beispiel zwischen der Netzwerk- und der Transportebene als Virtual Private Network (VPN) oder oberhalb der Transportschicht als Secure Socket Layer (SSL).

Es muss immer kryptographische Endpunkte geben. Diese müssen nicht zwingend die Kommunikationsendpunkte sein.

Bei Verschlüsselungskonzepten muss immer eine Sicherheitskomponente auf der Gegenseite vorhanden sein, mit der kryptographisch kommuniziert wird. Damit bei der Verschlüsselung auf beiden Seiten der gleiche Schlüssel vorhanden ist, muss ein gemeinsames Schlüssel-Management organisiert werden. Die Organisation eines Schlüssel-Managements ist immer dann sehr einfach, wenn die Sicherheitskomponenten im selben Verantwortungsbereich liegen. Ist dies nicht der Fall, muss ein Schlüssel-Management realisiert werden, dem die unterschiedlichen Verantwortungsbereiche vertrauen.

Ziel der Verschlüsselung

Das Ziel der Verschlüsselung ist es, Daten in einer solchen Weise mathematisch zu transformieren, dass es einem Angreifer nicht möglich ist die Originaldaten(clear text, plain text) aus den transformierten Daten(cipher text, Chiffretext) zu rekonstruieren. Natürlich muss hierbei beachtet werden, dass dem legalen Benutzer eine Möglichkeit der Invertierung zurück zu den Originaldaten erhalten bleibt. Man spricht allgemein nicht von Transformation sondern von „Verschlüsselung“ und „Entschlüsselung“.

1.6.2 Elementarverschlüsselung

Es gibt mehrere Möglichkeiten, Daten zu verschlüsseln und zu entschlüsseln. Schon in der Antike wollte wurden einfache Verschlüsselungstechnologien genutzt, damit Informationen nicht von Feinden abgefangen und gelesen werden können. So ziehen sich diverse Verschlüsselungsverfahren, wie zum Beispiel die Caesarverschlüsselung oder Atbatsch-Verschlüsselung, durch die Geschichte der Kryptographie.

Heutzutage spielen diese Verfahre keine Rolle mehr, da sie schon ohne Computer lösbar waren und der Aufwand zum Entschlüsseln vernachlässigbar klein ist. Es wurden weitere Verfahren zum Verschlüsseln von Nachrichten entwickelt, wobei im Folgenden auf die wichtigsten Verfahren eingegangen werden soll.

Beispiel: Einmal-Schlüssel

Verschlüsselung gibt es seit der Antike, diese Verfahren spielen heutzutage aber keine Rolle mehr.

Dieses Verfahren wird auch individuelle Wurmverschlüsselung, Zahlenwurm oder One-Time-Pad genannt. Der Einmal-Schlüssel zählt zu den „absolut sicheren“ Verschlüsselungsverfahren. Das Verfahren benötigt für jede Nachricht einen Zahlenwurm beziehungsweise einen Schlüssel, der mindestens die Länge des zu übermittelnden Klartexts haben muss.

Beispiel: Substitutionen

Andere Umsetzungen der Elementarverschlüsselung sind Substitutionen. Hierbei werden Buchstaben des Schlüsseltextes durch andere Buchstaben oder Zahlen ersetzt. Diese Verfahren können gebrochen werden, da ein genügend langer Schlüsseltext viele stilistisch erfassbare Regelmäßigkeiten aufweist und der Schlüssel so ermittelt werden kann.

1.6.3 Symmetrische Verschlüsselungsverfahren

Symmetrische Verfahren nutzen für Ver- und Entschlüsselung denselben Schlüssel.

Verschlüsselungsverfahren, die für die Verschlüsselung von Daten den gleichen Schlüssel verwenden wie für ihre Entschlüsselung, werden als symmetrische Verschlüsselung oder Private-Key-Verfahren bezeichnet.

Gängige Verfahren sind beispielsweise die AES-(Advanced Encryption Standard) oder Camellia-Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit. Vorteilhafter sind Schlüssellängen von 192 Bit beziehungsweise 256 Bit.

Der Nachteil von symmetrischen Verschlüsselungsverfahren wie beispielsweise AES ist, dass beide Kommunikationspartner über den gleichen Schlüssel verfügen müssen. Der Schlüssel, von dessen Geheimhaltung die Sicherheit abhängt, muss von einem Kommunikationspartner an den anderen übermittelt werden. Dieser Unsicherheitsfaktor muss durch eine sichere Methode zur Schlüsselverteilung minimiert werden. Im Extremfall kann dies zum Beispiel die persönliche Übermittlung durch einen Kurier sein. Das Risiko besteht darin, dass die Schlüssel, von deren Geheimhaltung die Sicherheit des Verfahrens abhängt, durch Nachlässigkeit, Vorsatz oder Zufall in falsche Hände geraten können.

Der Vorteil von Private-Key-Verfahren wie dem AES ist jedoch, dass es sehr performant und daher sehr schnell arbeitet. Es gibt Hardware-Lösungen, die bis zu 1 GBit/s und Software-Lösungen, die bis zu mehreren MBit/s verschlüsseln können.

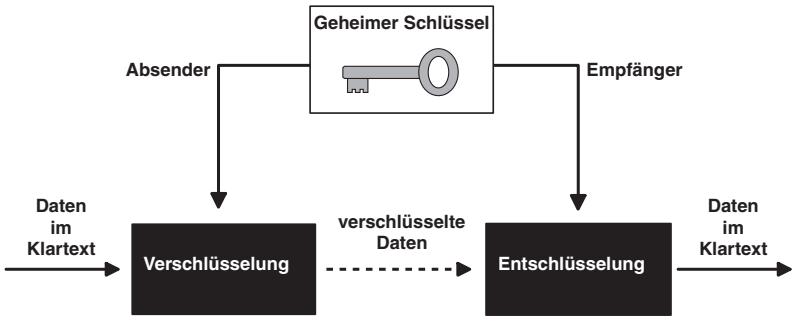


Abbildung 25: Symmetrische Verschlüsselung/ Private Key-Verfahren

1.6.4 Asymmetrische Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren lösen das Problem der Schlüsselverteilung. Es gibt einen privaten und einen öffentlichen Schlüssel.

Um die Schlüsselverteilung, das klassische Problem der Kryptographie zu vereinfachen, wurden Verfahren entwickelt, die mit so genannten „öffentlichen Schlüsseln“ (public keys) arbeiten. Ein Public-Key-Verfahren oder asymmetrisches Verfahren arbeitet daher mit zwei verschiedenen Teilschlüsseln, dem öffentlichen Schlüssel, der beispielsweise in ein öffentliches Verzeichnis hochgeladen wird und dem privaten Schlüssel, der ausschließlich im Besitz des Schlüsselerstellers ist.

Das Beispiel der E-Mailverschlüsselung mittels öffentlicher Schlüssel soll im Folgenden die Funktionsweise von Public-Key-Verfahren verdeutlichen:

Dazu erzeugt sich ein E-Mailnutzer (Bob) einen öffentlichen und einen privaten Schlüssel mittels PGP[38]. Der öffentliche Schlüssel kann an Kommunikationspartner verteilt werden. Alternativ kann dieser auch in ein öffentliches Schlüsselverzeichnis geladen werden.
Der private Schlüssel hingegen bleibt ausschließlich unter der Kontrolle des Nutzers (Bob genannt).

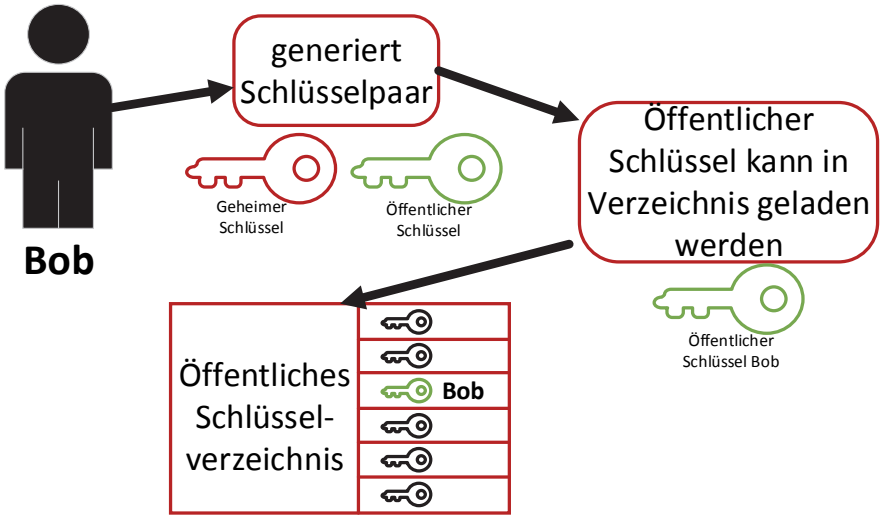


Abbildung 26: Private- / Public-Key

Wenn ein Kommunikationspartner, in diesem Beispiel Alice genannt, Bob eine verschlüsselte E-Mail schreiben will, verwendet sie den öffentlichen Schlüssel von Bob. Sie kann dabei den Schlüssel direkt mit Bob austauschen oder sie besorgt sich den Schlüssel aus einem öffentlichen Schlüsselverzeichnis. Nachdem die E-Mail mit dem öffentlichen Schlüssel von Bob verschlüsselt wurde, wird sie an Bob versendet. Bob findet nun die verschlüsselte E-Mail in seinem Postfach. Daraufhin verwendet er seinen privaten Schlüssel, um die E-Mail zu entschlüsseln (siehe Abbildung 27).

[38] *PGP – Pretty Good Privacy ist eine Programm zur E-Mailverschlüsselung*

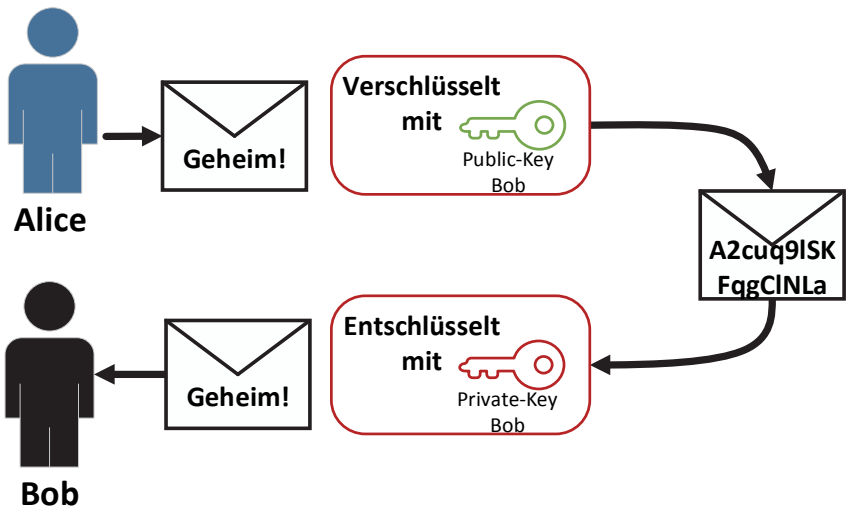


Abbildung 27: Asymmetrische Verschlüsselung / Entschlüsselung

Weitere praktische Anwendungen:

- Gesicherter Schlüsselaustausch mittels öffentlicher Schlüssel
- Elektronische Signaturen
- Authentifizierung

1.6.5 One-Way-Hashfunktionen

So genannte Hashfunktionen werden verwendet, um die Echtheit und die Integrität von Daten zu sichern. Dazu werden Funktionen verwendet die aus einem Dateiinhalt einen eindeutigen und einmaligen Prüfwert erzeugen.

Die One-Way-Hashfunktion ist eine Signatur der Prüfsumme einer Nachricht.

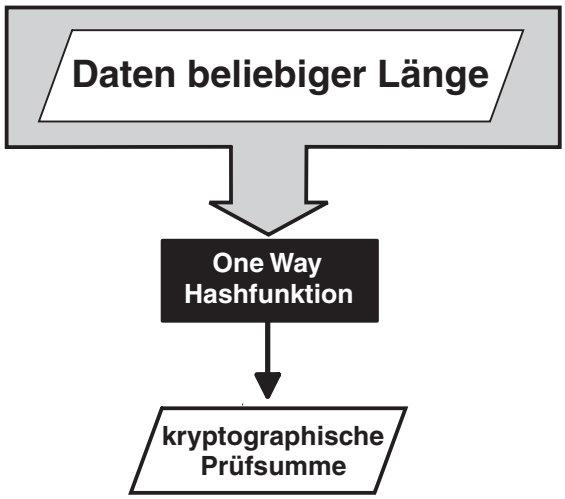


Abbildung 28: One-Way-Hashfunktion

Praktisches Beispiel:

Sie bekommen eine Installationsdatei von einem Bekannten und wollen prüfen, ob diese Datei in irgendeiner Weise manipuliert wurde. Dazu kann auf der Herstellerseite der Software oft ein zur Installationsdatei passenden Hashwert gefunden werden. In diesem Fall ist es die Installationsdatei Keepass2[40] für Windows.

Die Installationsdatei heißt „KeePass-2.28-Setup.exe“ und ihre Hashwerte sind:

MD5: F6FA98D076AAF2497E5FD189648E6ACA

und

SHA1: CDCDB6F86112D2A7A5B7094B7C49A30FDB2D280C

Wenn die Datei mit den Hash-Funktionen MD5 oder SHA1 geprüft wird und die zuvor dargestellten Werte aufweist, ist die Datei nicht verändert worden.

MD5 gilt noch als sicher, es wird aber empfohlen Hash-Funktionen mit einer höheren Kollisionsresistenz zu verwenden, beispielsweise SHA1, SHA256, SHA3 512 und SHA2 512.

1.7 Zusammenfassung

Fazit: Kryptographie

Kryptographische Verfahren sind die Basis der meisten Sicherheitssysteme.

Die Sicherheit eines kryptographischen Systems

- hängt niemals von der Geheimhaltung der Algorithmen ab
- basiert ausschließlich auf der Geheimhaltung des privaten Schlüssels

Für die Sicherheit einer Verschlüsselung sind vier Faktoren ausschlaggebend.

- der verwendete Algorithmus
- die Schlüsselgenerierung
- die Schlüssellänge
- die Aufbewahrung des Schlüssels

[40] *http://keepass.info/integrity.html*

2. Schwachstellen und Angriffsmöglichkeiten

Das 80/20-Prinzip gilt für die Kosten von IT-Sicherheit und Schäden.

Die Kosten für die IT-Sicherheit und Schäden der IT-Infrastruktur eines Unternehmens verhalten sich nach dem Paretoprinzip. Dies beschreibt, dass 20% der möglichen IT-Sicherheitsmechanismen 80% Schutz vor potentiellen Bedrohungen liefern. Das bedeutet, dass mit dem Einsatz der richtigen IT-Sicherheitsmaßnahmen, durch einen relativ geringen Aufwand, ein sinnvoller Grundschutz für IT-Systeme hergestellt werden kann. Das Problem ist, dass die Sensibilität für IT-Sicherheit in vielen Unternehmen noch nicht ausreichend ist. Weiterhin ist das Verhältnis zwischen Umsatz und Ausgaben für die IT-Sicherheit nicht ausreichend.
Dadurch steigt die Wahrscheinlichkeit von Angriffen, da diverse Angriffsvektoren ausgenutzt werden können. So kann ein Angreifer zum Beispiel simple Programmierfehler bei Datenbankanwendungen ausnutzen, um massenhaft geheime Informationen abzugreifen. Eine fehlerhafte Konfiguration von Software bietet ebenso eine große Angriffsfläche. So ist es grundsätzlich ratsam, Standard-Passwörter nach der Inbetriebnahme diverser Komponenten zu ändern. Dies hört sich logisch an, ist aber ein Grund warum viele Router, Webcams, ja sogar ganze Heizungsanlagen höchst verwundbar im Internet aufzufinden sind.

2.1 Gründe für Angriffe

Vielfältige Gründe, Motivationen und Hintergründe für Angriffe.

Gründe für den Angriff auf ein IT-System sind so vielfältig wie kriminelle, wirtschaftliche oder politische Handlungen in der realen Welt. Berufskriminelle treibt das Geld an, während Spione – im Auftrag von Wirtschaft oder Regierung, Geld und Informationen gewinnen wollen. Terroristen verfolgen dagegen eher politische Interessen oder wollen mit Vandalismus Zeichen setzen. Eine Gruppe die damit heraussticht sind die so genannten Hacker. Sie haben meist einfach Spaß an der Technik und suchen die Anerkennung innerhalb der Community oder die Herausforderung ein „sichereres“ System zu knacken. Natürlich gibt es auch innerhalb der Hackercommunity schwarze Schafe die zerstörungswütig sind oder einen Service außer Kraft setzen wollen. Diese werden Black hat’s genannt, während Hacker, die die Sicherheit eines Systems überprüfen, sogenannte White hat’s sind.
In der Zeit nach den Veröffentlichungen durch Edward Snowden[41] ist auch klar, dass Behörden ebenfalls an Informationen, die die Strafverfolgung vorantreiben könnten, interessiert sind.

2.2 Angreifer/Täter

Trifft technisches Wissen auf kriminelle Energie hat man perfekte Voraussetzungen für einen Angreifer.

Am zutreffendsten lassen sich Angreifer mit den zwei folgenden Eigenschaften einordnen:
Das technische Wissen und die kriminelle Energie.
Zur Veranschaulichung sind die beiden Werte in ein Koordinatensystem eingezeichnet. An der horizontalen Achse können Sie das Maß des technischen Wissens eines bestimmten Angreifers ablesen. Die vertikale Achse hingegen beschreibt die kriminel-

[41] http://de.wikipedia.org/wiki/Edward_Snowden *Whistleblower, hat die Abhöraktivitäten der National Security Agency (NSA) aufgedeckt.*

le Energie des Angreifers. Folgend wird jeder Quadrant, stellvertretend für die Merkmale des Angreifers, im Detail erläutert.
Wie die Gefahren im Einzelnen aussehen, die den angeschlossenen oder miteinander vernetzten Rechnersystemen im Internet drohen, finden Sie im Kapitel 2.3.

Abbildung 29: Das Verhältnis von Wissen zu krimineller Energie

2.2.1 Skript-Kiddies

Der Begriff „Skript-Kiddies“ setzt sich zusammen aus „Skript“ (eine Textdatei mit Computerbefehlen) und „Kid“ (englisch für Kind). Die sogenannten Skript-Kiddies finden Sie im Quadranten unten links (siehe Abbildung 29). Das bedeutet, dass Angreifer dieser Kategorie grundsätzlich kein oder nur wenig technisches Wissen besitzen und auch kaum kriminelle Energie. Meist nutzen sie vorgefertigte Programme samt Anleitung, um in IT-Systeme einzudringen und Schaden anzurichten. In Kombination mit offenen, sogenannten „ungepatchten“ Sicherheitslücken und entsprechenden Exploits werden Skript-Kiddies gefährlich. Häufige Beweggründe von Skript-Kiddies sind der Spieltrieb, der Hang zu Imponieren oder schlichter Vandalismus.

2.2.2 IT-Sicherheits-Experten

Die IT-Sicherheits-Experten finden Sie im Koordinatensystem (siehe Abbildung 29) unten rechts. Genau genommen zählen diese Personen nicht zu den Angreifern. Vielmehr stehen IT-Sicherheits-Experten auf der Seite der „Guten“, weshalb sie auch als „ethische Hacker“ bezeichnet werden. IT-Sicherheits-Experten besitzen ein enormes Grundlagenwissen im Bereich der IT-Sicherheit und agieren nicht mit krimineller Energie. Oftmals versuchen sie die Sicherheit von IT-Systemen oder Anwendungen zu verbessern, indem sie eigenständig Sicherheitslücken aufspüren und diese den entsprechenden Entwicklern bekannt geben. Nicht selten beauftragen Unternehmen solche IT-Sicherheits-Experten. In sogenannten Penetrationstests versucht ein IT-Sicherheits-Experte in das System eines Unternehmens einzudringen. Mit dieser Methode können gefundene Sicherheitslücken aufgedeckt und geschlossen werden, sodass böswillige Angreifer weniger Chancen haben, Schaden in einem Unternehmensnetzwerk anzurichten.

2.2.3 Wirtschaftsspione / Kriminelle

Wirtschaftsspione oder Kriminelle werden umgangssprachlich als „Hacker“ bezeichnet und sind in dem abgebildeten Quadraten oben rechts zu finden (siehe Abbildung 29). Mit viel Hintergrundwissen im Bereich der IT-Sicherheit und zudem mit viel krimineller Energie unterschiedlicher Ausprägung, stellen diese Angreifer die eigentlichen digitalen Gangster und Banditen dar. Diese Hacker handeln entweder aus eigener Motivation, das heißt mit dem Ziel des direkten Gewinns oder aber im Auftrag. Neben organisiertem Verbrechen mit Diebstahl, Betrug, Diffamierung und dergleichen wächst der Bereich um (Wirtschafts-)Spionage immer stärker an. Um an eine gewisse Technologie zu gelangen, kann ein Unternehmen entweder teure Forschung betreiben oder aber mit besonders kriminellen Absichten einen Hacker anheuern, der das entsprechende Wissen bei einem Konkurrenzunternehmen stiehlt.

2.2.4 Innentäter

Die letzte zu beschreibende Gruppe von Angreifern kann als Innentäter beschrieben werden. Trotz wenig technischem Wissen stellen sie mit viel krimineller Energie (siehe Abbildung 29 Quadrant oben links) ein hohes Gefahrenpotential dar. Diese „Angreifer von Innen“ sind aufgrund ihres geringen technischen Wissens vielleicht nicht in der Lage zu hacken, können jedoch an Informationen oder Gegenstände gelangen, die für einen Angriff ausgenutzt werden können (Insider-Wissen). Ein Beispiele für einen solchen Angriff ist das Ausschleusen von maliziösen Programmen, der Verkauf sensibler Unternehmensdaten, Erpressung und vieles mehr. Aus Sicht der Informationssicherheit sind Innentäter schwer anzugehen. Viele der technischen Sicherheitsmaßnahmen schützen gegen Angreifer außerhalb der Unternehmensmauern – und nicht oder nur wenig gegen Angreifer von innen.

2.3 Angriffsarten in Kommunikationssystemen

Was passiert bei einem Angriff?
Bei einem Angriff wird durch einen aktiven oder passiven Eingriff, eine ungewünschte Aktion mit Objekten gewährt. Die Ziele eines Angriffes sind meist Informationsgewinne, das Auslösen einer Reaktion oder die Nutzung der vorhandenen Ressourcen. Das Ausnutzen von Ressourcen wird etwa bei einem DDoS-Angriff (siehe Kapitel 2.3.2) benötigt, um beispielsweise einen Webserver lahm zu legen.

2.3.1 Passive Angriffe

Ein passiver Angriff erfolgt ohne Modifizierung der übertragenen Nachrichten. Hierbei beeinflusst der Angreifer den Betrieb der betrachteten IT-Systeme nicht oder zumindest nicht merkbar. Er führt einen passiven Angriff im Regelfall willentlich und gezielt durch. Sein Ziel ist die Erlangung wertvoller geheimer Informationen.

Passive Angriffe beeinflussen die Funktionalität der IT-Systeme nicht. Ziel sind meist geheime Informationen.

Dies führt er meist in unzulässiger, strafbarer Weise aus. Ein passiver Angreifer bleibt oft gänzlich oder zumindest für lange Zeit unentdeckt und kann so latent über einen längeren Zeitraum großen Schaden anrichten.

Passive Angriffe sind in ihrer Zielrichtung und Angriffsart unterscheidbar:

Abhören der Kommunikation

Beim Abhören der Kommunikation gelangt der Angreifer auf dem Übertragungsweg an den Informationsinhalt. Er kann ihn als unberechtigter Lauscher zu seinen Zwecken verwerten. Hierbei ist das Kommunikationsmedium selbst sein Angriffsobjekt.

Ausforschen der Kommunikationspartner

Das Ausforschen der Kommunikationspartner ist die Vorstufe einer umfassenden Kommunikationsflussanalyse. Die Angriffsart erlaubt auch ohne Kenntnis des eigentlichen – möglicherweise verschlüsselten – Nachrichteninhalts Rückschlüsse auf den Nachrichteninhalt. Sie gewinnt ihre Erkenntnisse aus der Ermittlung der Identität der Kommunikationspartner.

Analyse des Kommunikationsflusses

Die Analyse des Kommunikationsflusses gibt dem passiven Angreifer auch bei Einsatz der wirksamsten Verschlüsselungsverfahren Informationen über Zeitpunkte, Kommunikationsvolumina, Art und Richtung des Datentransfers. Diese Informationen können – mit anderen Informationen zusammengeführt – recht aussagekräftig sein.

Beispiel: Sniffing

Fürs sogenannte „Sniffing“ (englisch für „Schnüffeln“) werden Tools zur Datenfluss-Analyse wie Wireshark[42] verwendet. Ziele sind Passwörter und vertrauliche Informationen.

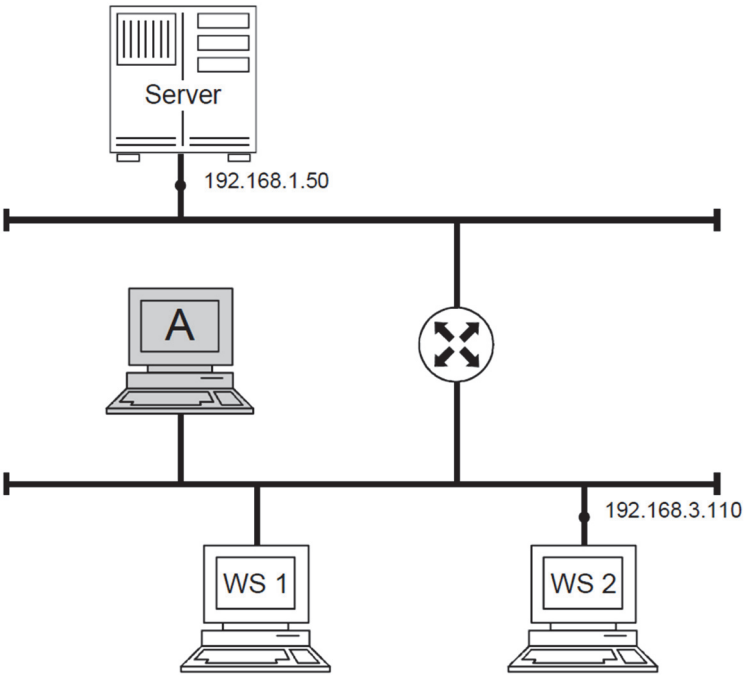


Abbildung 30: Passiver Angriff (Angreifer = A)

Fazit:

Passive Angriffe können nicht verhindert werden. Mittels geeigneter Verschlüsselung können Daten jedoch für Angreifer wertlos gemacht werden.

[42] https://www.wireshark.org/ *Netzwerkanalysesoftware zur Aufzeichnung von Netzwerkverkehr.*

2.3.2 Aktive Angriffe

Aktive Angriffe beeinflussen die Funktionalität von IT-Systemen. Der Angreifer verursacht Veränderungen.

Neben der Gefährdung durch passives Abhören unterliegen die Kommunikationsströme auch der Bedrohung durch aktive Angriffe. Hier manipuliert der Angreifer den Nachrichtenstrom oder er beeinflusst die Verfügbarkeit und Konsistenz der IT-Systeme und IT-Dienste.

Der aktive Angreifer greift direkt in den Kommunikationsstrom oder in eine der Kommunikationskomponenten ein und verfälscht die zu übertragenden Daten. Er setzt seine Angriffe physisch durch das Auftrennen des Kommunikationsmediums oder softwarebasiert durch den Eingriff in die Programme der aktiven Kommunikationskomponenten um. Der aktive Angreifer verursacht Veränderungen. Das bietet im Gegensatz zum passiven Angriff konkrete Ansatzpunkte für eine zeitnahe Erkennung des Angriffs. Diese schnelle Erkennung ist die unverzichtbare Grundlage für eine wirksame Reaktion durch prompte angemessene Gegenmaßnahmen.

Aktive Angriffe können auf vielfältige Weise erfolgen. Der Angriffsort kann entweder auf dem Übertragungsweg oder auf den IT-Systemen der Kommunikationspartner, also beim Sender oder beim Empfänger, liegen. Nachrichten können als Ganzes oder in Teilen manipuliert werden. Typische aktive Angriffe sind:

- Dienst- und Kommunikationsunterbindung
- Nachrichtenverzögerung
- Wiederholungsangriffe
- Nachrichtenverfälschung

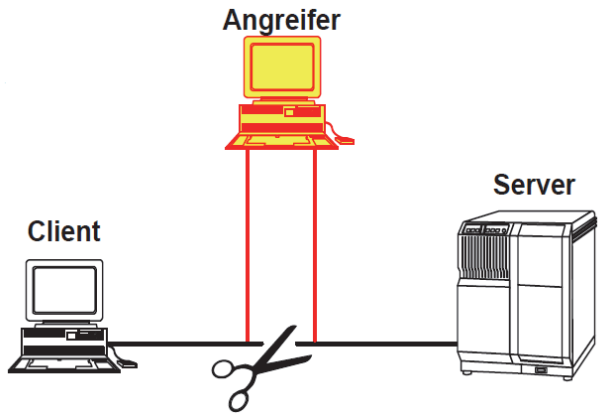


Abbildung 31: Aktiver Angriff (Quelle: Folien Pohlmann)

Beispiele:
Einen zielgerichteten Angriff auf kritische Infrastrukturen einer Organisation werden als Advanced Persistent Thread, kurz APT bezeichnet.
Wenn zu viele Anfragen zur Überlastung eines Servers führen, handelt es sich um eine DDoS-Attacke (Distributed Denial of Service = Verweigerung des Dienstes)

Fazit:
Aktive Angriffe können durch geeignete Schutzmaßnahmen erkannt und die Zielerreichung verhindert werden.

2.3.3 Exploit

Exploits nutzen Schwachstellen in einem Rechnersystem aus. Aktuelle Exploits können über spezielle Suchmaschinen im Internet gefunden werden.

Ein Exploit ist ein Computerprogramm oder Script, welches Schwächen eines Softwaresystems ausnutzt, damit es Zugriff darauf erhält. Die Entwicklung und Veröffentlichung von Exploits durch IT-Sicherheitsexperten, dient der Demonstration von Sicherheitslücken. Diese Lücken können in Browsern oder weit verbreiteter Standardsoftware, wie zum Beispiel PDF-Readern enthalten sein. Die Verbreitung erfolgt meist durch präparierte Dokumente über gefälschte Webseiten oder E-Mails. Durch Exploits werden Hersteller von Software dazu gezwungen, möglichst schnell auf diese Lücke zu reagieren. Sind in einem Programm Sicherheitslücken bekannt, aber es gibt noch keinen Sicherheitsupdate, sollte auf Alternativprogramme ausweichen werden. Eine geeignete Maßnahme zur Behebung von Schwachstellen ist es, dass Betriebssystem und die Anwendungen aktuell zu halten. Dabei können Programme, die den Updatestatus aller installierten Programme überwachen und eine Übersicht über notwendige Sicherheitsupdates liefern, wie zum Beispiel „secunia“, helfen.

•

Abbildung 32: Oberfläche des Programms secunia

2.3.4 Unberechtigte Rechteausweitung

Rootkits geben einem Angreifer unberechtigt erweiterte Rechte.

Dies beschreibt die Ausnutzung eines Programmier- oder Konfigurationsfehlers eines Programms, um einem Benutzer oder einer Anwendung unberechtigte Zugriffe, zum Beispiel auf Ressourcen zu gestatten. Ein Beispiel dafür sind Rootkits, die verborgene Administratorrechte für unerwünschte Programme liefern oder durch den erhaltenen Rootzugriff[43] solche Programme installieren. Wenn der Verdachte besteht, dass ein Rootkit installiert wurde, dann ist eine Neuinstallation des Betriebssystems unausweichlich.

[43] *Ein Rootzugriff ist der Zugriff auf der höchsten Rechteebene in einem Computersystem, Auch Administrationsrecht genannt.*

2.3.5 Vortäuschen einer falschen Identität

Es gibt viele Möglichkeiten dem Benutzer eines Webdienstes vorzutäuschen, dass er sich auf der korrekten Webseite befindet. Eine weit verbreitete Methode ist das so genannte Phising. Dabei wird dem Benutzer vorgetäuscht, dass er sich auf der gewünschten Webseite befindet, in Wahrheit wurde diese aber durch eine Kopie ersetzt. Das Ziel eines Phising-Angriffs ist es, Login-Details wie Nutzernamen den dazu passenden Passwörtern zu stehlen.

•

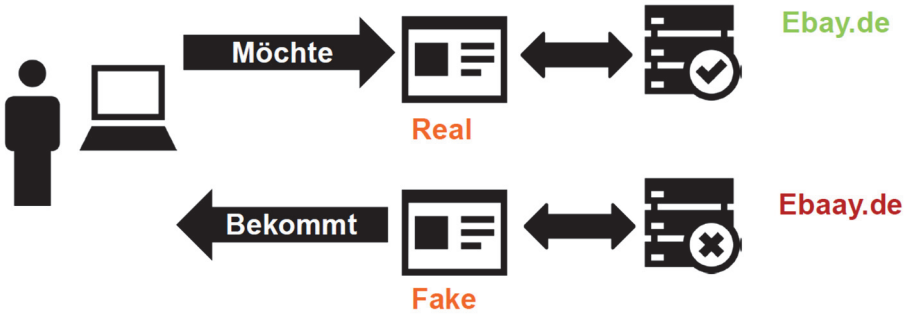


Abbildung 33: Phishing-Angriff

2.3.6 Code Injection

Von Code-Injection wird gesprochen, wenn es dem Angreifer gelingt ausführbaren Programmcode in ein IT-System einzuschleusen und diesen auszuführen. Dies kann zum Beispiel durch einen Drive-by-Download geschehen. Hierbei ruft ein Interntnutzer eine präparierte Webseite auf und startet dadurch unbewusst einen Dateidownload. In dieser Datei ist der ausführbare Code versteckt. Dies wird möglich, wenn der Browser oder Plugins wie beispielsweise Flash[44], Sicherheitslücken aufweist.

Code Injection beschreibt den Vorgang des Einschleusens von Code über Webanwendungen.

2.3.7 Angriff über Sonderzeichen

Bei dieser Methode verwendet ein Angreifer Sonderzeichen, mit der Absicht schädliche Nebeneffekte hervorzurufen. Unzureichend gesicherte Webseiten lassen so Funktionsaufrufe zu, über die der Angreifer unter Umständen auf beliebige Verzeichnisse zugreifen kann. Ein Beispiel ist das Directory Traversal, bei der über Sonderzeichen wie „/“ oder „\“ die Pfadangabe verändert wird und somit ein Zugriff auf Dateien oder Verzeichnisse erfolgt die nicht öffentlich zugänglich sein sollten.

Es werden Sonderzeichen eingeschleust, die schädliche Nebeneffekte aufrufen.

Ein weiteres Beispiel ist SQL-Injection. SQL-Injection wird möglich, wenn Webseiten eine Anfrage direkt als SQL[45]-Abfrage an eine im Hintergrund befindliche Datenbank versenden. Wird die Eingabe nur unzureichend validiert und die Maskierung nicht korrekt vorgenommen, kann ein ausführbares Skript an die Datenbank geschickt werden und dadurch direkter Einfluss auf die Abfrage genommen werden. Bei unzureichend gesicherten Datenbanken können so Passwörter, Kreditkarteninformationen und weitere hoch kritische Daten unberechtigt ausgelesen werden.

[44] *Flash ist eine Technologie, die interaktive Inhalte auf einer Internetseite darstellen kann.*
[45] *SQL – Structured Query Language, ist eine weit verbreitete Datenbanksprache.*

2.3.8 Man in the Middle

Ein Angreifer schaltet sich zwischen zwei Kommunikationspartner und manipuliert den Kommunikationsfluss zwischen den beiden.

Bei einem Man in the Middle-Angriff steht der Angreifer zwischen zwei Kommunikationspartnern und versucht die transferierten Daten zu manipulieren. Zum Beispiel kann es einem Angreifer bei TLS/SSL-Verbindungen gelingen, ein gefälschtes Paket an den Sever zu senden und ihn dadurch dazu veranlassen, den anfragenden Client mit einer alten oder sogar ganz ohne Verschlüsselungsmethode zu bedienen. Dies ist möglich, da Client und Server anfangs unverschlüsselt das Verschlüsselungsverfahren aushandeln. Dadurch entsteht Angriffsfläche für einen Man in the Middle-Angriff.

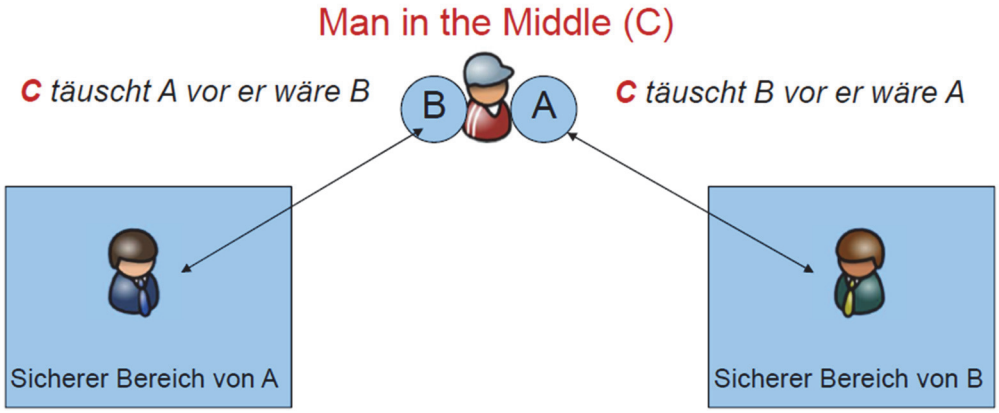


Abbildung 34: Man-in-the-Middle-Angriff

2.4 Zusammenfassung

Fazit: Schwachstellen und Angriffsmöglichkeiten

IT-Geräte, IT-Prozesse und die elektronischen Werte sind Wirtschaftsgüter, welche angemessen geschützt und abgesichert werden müssen.

Bei einem Angriff wird durch einen aktiven oder passiven Eingriff eine ungewünschte Aktion mit Objekten ausgeübt.

Die Sicherheit der IT liegt in der Verantwortung des Eigentümers.

Wirkungs-und Handlungszusammenhang der IT-Sicherheit ist sehr komplex und braucht eine genaue Analyse und Bewertung.

Die Angriffsmöglichkeiten, die Eintrittswahrscheinlichkeit und die Schäden sind sehr vielfältig und zeigen den notwendigen Handlungsbedarf auf.

3. Sicherheitsmaßnahmen

Maßnahmen zur Erhöhung des IT- Sicherheitsniveaus können in drei Kategorien gegliedert werden:

- Organisation
- Administration
- Technik

Verbesserung durch Optimierung betrieblicher Abläufe.

Eine organisatorische Schutzmaßnahme verbessert die IT-Sicherheit durch die Optimierung der betrieblichen Abläufe. Sie plant die Umsetzung der Geschäftsvorfälle, die Funktion und die Verantwortungsbereiche der Mitarbeiter. Ein typisches Beispiel einer organisatorischen Schutzmaßnahme ist die Organisationsanweisung, wie beim Funktionswechsel eines Mitarbeiters mit dessen Zugangs- und Zugriffsrechten umzugehen ist.

Verbesserung durch effiziente Verwaltung der IT-Systeme.

Eine administrative Schutzmaßnahme gewährleistet das IT-Sicherheitsniveau durch die effiziente Verwaltung der IT-Systeme. Sie überwacht die Umsetzung, die Fortschreibung und die Wirksamkeit der Sicherheitsmaßnahmen. Charakteristische Beispiele administrativer Schutzmaßnahmen sind die Verwaltung der Kommunikationsregeln auf einem Firewall-System oder die Betreuung eines Intrusion Detection Systems zur Erkennung von Angriffen auf die IT-Systeme.

Verbesserung durch Einsatz von Hard- und Software.

Eine technische Sicherheitsmaßnahme erzielt durch den Einsatz von Hard- und Software das gewünschte IT-Sicherheitsniveau. Sie wirkt maschinell Angreifern und deren Angriffen entgegen. Bezeichnende Beispiele für technische Schutzmaßnahmen sind Firewall- und Angriffserkennungssysteme sowie Verschlüsselungskomponenten zum Betrieb eines Virtuellen Privaten Netzes (VPN).

IT-Sicherheit ist stets im Wandel. Sie entwickelt sich dynamisch und die Organisation wird damit zu einem kontinuierlichen Prozess.

Die IT-Sicherheit ist leider kein einmalig und für immer erreichbares Ziel wie eine wissenschaftliche Erkenntnis. Die Anforderungen an die IT-Sicherheit unterliegen einem stetigen Wandel. Interne Anforderungen an zusätzliche Sicherheitsfunktionen und externe Anforderungen als Resultat neuer Angriffsszenarien und zusätzlicher bekannt gewordener Schwachstellen der IT-Dienste sind nur mit einem dynamischen Vorgehen zu erfüllen.
Die Organisation der IT-Sicherheit ist daher ein kontinuierlicher Prozess, der stetig die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und Beweiskraft der IT-Systeme und IT-Dienste einer Organisation gewährleisten soll. Ein solcher Prozess ist geeignet zu planen und zu managen.
Zu den organisatorischen Aufgaben des IT-Sicherheitsmanagements gehören:

- die Fortschreibung der IT-Sicherheitsziele
- die Anpassung der Sicherheitsstrategien
- die Erweiterung der Sicherheitsleitlinien der Organisation
- die Festlegung und Fortschreibung der IT-Sicherheitsanforderungen
- die Auswahl und Priorisierung zu treffender Schutzmaßnahmen.

IT-Sicherheit ist stets eine Management-Aufgabe. Nur wenn die Leitung einer Organisation voll hinter den IT-Sicherheitszielen und den damit verbundenen Aktivitäten steht, kann diese Aufgabe erfolgreich wahrgenommen werden.

Ökonomie von IT-Sicherheitsmaßnahmen

Unter dem alleinigen Kostengesichtspunkt ist es unsinnig, eine IT-Schutzmaßnahme zu etablieren, deren Aufwand den Ertrag aus Risikoverringerung und Kosteneinsparung übertrifft. Ebenso ökonomisch unsinnig ist es, eine Schutzmaßnahme nicht umzusetzen, die einen geringeren Aufwand als das durch sie abgedeckte Risiko verursacht.

Aus ökonomischer Sicht, ist ein durchschnittliches Sicherheitsniveau das angestrebte Ziel.

Führen zum Beispiel unzureichende Notfallvorkehrungen zu einem mehrtägigen Produktionsausfall, übertrifft die erwartete Schadenshöhe meist die überschaubaren Kosten von redundanzerhöhenden Schutzmaßnahmen. Umgekehrt nehmen Direktbanken für das Onlinebanking in der Regel von hochsicheren, aber aufwändigen Chipkarten-Authentisierungssystemen für ihre Kunden Abstand, da die Marge bei diesen Kunden zu schmal ist, um eine größere Zusatzinvestition zu tragen. Sie verlagern lieber die Risiken auf den Kunden und führen unergonomische PIN-TAN- oder PIN-iTAN-Verfahren zur Authentisierung weiter durch.

Eine hundertprozentige Sicherheit ist nicht zu realisieren. Meist kosten die letzten 20% mehr als die ersten 80% eines Sicherheitsziels. Auch lohnt in der Regel ein über IT-Systeme und Zeit ungleichmäßiges Sicherheitsniveau weniger als ein homogenes. Daher ist meist ein Grundschutz, der ein durchschnittliches Sicherheitsniveau anstrebt, ein ökonomisch sinnvoller Schritt zu mehr Sicherheit.

3.1 Organisatorische Maßnahmen

IT-Sicherheit zu etablieren ist ein hoch komplexer Prozess, der von vorneherein gut organisiert werden muss. Es gibt einige Hilfestellungen, wie zum Beispiel IT-Sicherheitsleitlinien, an denen sich Unternehmen orientieren können, um ein schlüssiges Konzept zu erstellen.

3.1.1 IT-Sicherheitsleitlinien

Eine organisationsweite IT-Sicherheitsleitlinie hat die Aufgabe, alle Aspekte einer sicheren Nutzung der Informationstechnik innerhalb einer Organisation abzudecken.

Die IT-Sicherheitsleitlinie wird als schriftliches Dokument erstellt und bildet die Grundlage des IT-Sicherheitsmanagements. Sie legt Leitlinien fest, schreibt aber keine Implementierung vor. Die IT-Sicherheitsleitlinie wird offiziell verabschiedet und in Kraft gesetzt. Jeder Mitarbeiter muss Kenntnis über die wichtigsten Inhalte der IT-Sicherheitsleitlinie erlangen.

Die IT-Sicherheitsleitlinie definiert die Rahmenbedingungen der IT-Sicherheit für eine konkrete Organisation. Sie enthält eine Definition der grundsätzlichen Sicherheitsziele und der Strategien für die Umsetzung dieser Ziele.

Die Leitlinie definiert die Rahmenbedingungen für eine konkrete Organisation anhand von grundlegenden Sicherheitszielen.

Eine generelle IT-Sicherheitsleitlinie besteht aus den Sicherheitsleitlinien und weiteren Rahmenvorgaben der Organisation, wie den grundlegenden Sicherheitszielen, den Strategien, den Verantwortungsbereichen und den Methoden zur Gewährleistung des benötigten IT-Sicherheitsniveaus.

1. **Festlegung der wesentlichen IT-Sicherheitsziele**

In der ersten Phase der Erstellung der IT-Sicherheitsleitlinie sind die spezifischen IT-Sicherheitsziele der Organisation zu ermitteln, die das Unternehmen und damit auch diese Leitlinie verfolgt.

Der folgende Katalog für typische Sicherheitsziele kann dabei hilfreich sein:

- aktives Risikomanagement (Schadensvermeidung und Schadensbegrenzung)
- Sicherstellung der Kontinuität der Arbeitsabläufe

- Sicherung der investierten Werte
- Vertraulichkeit der verarbeiteten Informationen
- Gewährleistung der aus gesetzlichen Vorgaben resultierenden Anforderungen
- Gewährleistung des Vertrauens der Kunden in die Organisation
- hohe Verlässlichkeit des Handelns, insbesondere in Bezug auf Vertraulichkeit,
- Richtigkeit und Rechtzeitigkeit
- Korrektheit, Vollständigkeit und Authentizität der Daten und Dienste
- Reduzierung der im Schadensfall entstehenden Kosten
- Gewährleistung der besonderen Reputation

Zur Präzisierung dieser Ziele dienen folgende fünf Fragen:

- Welche IT-Dienste nutzt die Organisation für ihre wesentlichen wertschöpfenden Prozesse?
- Welche essenziellen Aufgaben können ohne IT-Unterstützung nicht mehr durchgeführt werden?
- Welche wesentlichen Entscheidungen hängen von der Genauigkeit, Integrität oder Verfügbarkeit der durch die IT-Systeme verarbeiteten Information ab?
- Welche Daten und Dienste erfordern hohe oder höchste Vertraulichkeit?
- Welche Auswirkungen hätte eine gravierende Verletzung der Sicherheit (Verlust von Vertraulichkeit, Integrität und/oder Verfügbarkeit)?

Im ersten Schritt werden die wesentlichen Ziele festgelegt, die mit Hilfe von fünf Fragen präzisiert werden können.

2. **Die zweite Phase analysiert die in der ersten Phase benannten qualitativen**

Umwandlung von Qualitativen in Quantitative Sicherheitsziele.

Sicherheitsziele quantitativ. Es gilt, die erforderlichen Sicherheitsniveaus festzulegen. Die Quantifizierung kann anhand des Rasters der elementaren IT-Sicherheitsziele Vertraulichkeit, Integrität, Authentizität, Verbindlichkeit und Verfügbarkeit vereinfachend erfolgen.

3. **Ausarbeitung der IT-Risikomanagement-Strategie**

Die IT-Risikomanagement-Strategie legt fest, wie die definierten Sicherheitsziele zu verfolgen sind. Die generelle organisationsweite IT-Sicherheitsleitlinie kann und soll lediglich eine abstrakte Beschreibung der gewählten Strategie liefern. Die konkreten Umsetzungen sind nachgeordneten IT-Systemsicherheitsleitlinien vorbehalten. Die nachfolgende Aufzählung liefert Beispiele für Strategien in der generellen IT-Sicherheitsstrategie:

- die Definition grundlegender IT-Sicherheitsprozesse
- die klare Einordnung aller Verantwortlichkeiten in den IT-Sicherheitsprozess
- die eingesetzte Methodik zur Bewertung der IT-Sicherheit
- die Art und generelle Umsetzung des Risikomanagements
- die Umsetzung der Qualitätssicherung
- die Entwicklung einer IT-Systemsicherheitsleitlinie für jedes IT-System
- die Etablierung einer organisationsweiten Kontinuitätsplanung
- die Voraussetzungen für eine sichere externe Kommunikation
- die Orientierung an internationalen Richtlinien und Standards
- IT-Sicherheit als integraler Bestandteil im gesamten Lebenszyklus eines IT-Systems
- die Förderung des Sicherheitsbewusstseins aller Mitarbeiter

Im letzten Schritt soll eine abstrakte Beschreibung der Sicherheitsleitlinie erfolgen.

Kleine bis Mittelständige Betriebe sollten die zuvor genannten Punkte als Auswahl nutzen.

IT-Sicherheitsleitlinie für KMU

Den Sicherheitsverantwortlichen in kleineren und mittleren Betrieben ist zu empfehlen, die Einzelpunkte als Auswahlmenü zur Erstellung einer kompakteren IT-Sicherheitsleitlinie zu nutzen. Nur die für das Unternehmen und seine wertschöpfenden Prozesse wesentlichen Schritte und Regelungen sollten in die unternehmensspezifische IT-Sicherheitsleitlinie aufgenommen werden. Dieses Vorgehen erzielt einen angepassten Aufwand für das IT-Sicherheitsmanagement.

3.1.2 Der IT-Sicherheitsbeauftragte

Der IT-Sicherheitsbeauftragte hat die fachliche Verantwortung für alle IT-Sicherheitsfragen innerhalb des Betriebs. Zu seinen Pflichten gehören:

- die Leitung des IT-Sicherheitsprozesses in der Organisation
- die verantwortliche Mitwirkung an der Erstellung und Weiterentwicklung der IT-Sicherheitskonzepte
- die Gesamtverantwortung für die Realisierung der ausgewählten Sicherheitsmaßnahmen
- die Planung und Koordination von Schulungs- und Sensibilisierungsveranstaltungen
- die Gewährleistung der IT-Sicherheit im laufenden Betrieb
- die Einsatzplanung der für IT-Sicherheit zur Verfügung stehenden Ressourcen
- die Wahrnehmung der datenschutzrechtlichen Belange lt. Datenschutzgesetz in der jeweils gültigen Fassung

Der IT-Sicherheitsbeauftragte kann einzelne Aufgaben delegieren, die Gesamtverantwortung für die IT-Sicherheit verbleibt aber bei ihm.

Der IT-Sicherheitsbeauftragte hat diverse Pflichten. Er kann delegieren, die Verantwortung bleibt aber bei ihm. Ihm kommt eine zentrale Bedeutung im IT-Sicherheitsprozess zu.

Abhängig von Größe und Aufgaben einer Organisation kann oft die Trennung der datenschutzrechtlichen und der übrigen IT-sicherheitsspezifischen Aufgaben sinnvoll sein. Aufgrund der Komplexität und Vielfalt der Aufgaben besteht auch, wie bereits oben erwähnt, die Möglichkeit, diese Funktion durch mehrere Personen abzudecken.

Der Funktion des IT-Sicherheitsbeauftragten kommt eine zentrale Bedeutung für die Effizienz des IT-Sicherheitsprozesses zu. Daher sollte diese Rolle in jedem Fall – also auch bei kleinen Betrieben – definiert und klar einer Person (eventuell zusätzlich zu anderen Aufgaben) zugeordnet sein. Ferner sollte der IT-Sicherheitsbeauftragte in seiner Rolle direkt der Geschäfts- oder Behördenleitung berichten.

3.1.3 Klassifizierung von Informationen

Im Arbeitsalltag kommen Beschäftigte mit einer Vielzahl an betrieblichen Informationen in Kontakt. Damit Beschäftigte wissen, wie sie mit den jeweiligen Daten umzugehen haben, sollten Betriebe sollten klare Vorgaben machen. Es wird von einer Klassifizierung der Informationen gesprochen.

IT-Sicherheitsklassen

- Öffentlich: kein besonderer Schutz erforderlich
- Intern: Schutz durch Beschränkungen von Zugang und Zugriff
- Vertraulich: erhöhter Schutzbedarf; Realisierung mit Hilfe von Schließanlagen sowie Verschlüsselung.

Beachtung von geltendem Recht und Richtlinien des Betriebs.	Informationen nur mit Bedacht im Netz veröffentlichen.
Gespräche vertraulich halten.	Betriebliche IT-Systeme nur für betriebliche Zwecke verwenden.
Informationen nur an Personen senden, die diese erhalten dürfen	Daten sicher löschen, Akten schreddern, Datenträger zerstören.
Aufbewahrungsorte sensibler Informationen stets abschließen	Prinzip „Aufgeräumter Schreibtisch“ umsetzen.

Tabelle 5: Beispiele für den Umgang mit geschäftlichen Daten

3.2 Komponentensicherheit

Um die Sicherheit von IT-Systemen zu gewährleisten müssen die jeweiligen Komponenten, zum Beispiel Client und Server, absichert werden.

3.2.1 Absicherung von Clients

Unter der Absicherung von Clients ist zum Beispiel das Absichern von Arbeitsplatzrechnern, Workstations oder Terminals zu verstehen.

Grundarchitektur nach BSI

Es ist für eine funktionierende IT-Landschaft von funktionaler Bedeutung, dass Arbeitsplatzrechner vor Angriffen geschützt werden. Dabei sollte die Arbeitsfähigkeit der Anwender, durch die Sicherheitsmaßnahmen nicht eingeschränkt werden. Ein Client sollte als Minimalsystem realisiert werden. Es sollte auf alle nicht verwendeten Hard- und Softwarekomponenten verzichtet werden.
Das BSI empfiehlt auf diese Minimalarchitektur weitere Schutzkomponenten, zum Beispiel:

Arbeitsplatzrechner müssen vor Angriffen geschützt werden.

- Ausführungskontrolle
  - Verhindert den Start von ausführbaren Dateien
- Virenschutzprogramm
  - Prüft Dateien auf der Festplatte und Wechselmedien auf schädliche Inhalte
- Personal Firewall
  - Kontrolliert ein- und ausgehende Verbindungen
- Gerätekontrolle
  - Regelt, welche Geräte über externe Schnittstellen angeschlossen werden dürfen
- Benutzerverwaltung
  - Gewährt einem Benutzer die Rechte, welche für die Arbeit benötigt werden
- Logging
  - Erfasst Ereignisse und Meldungen zur gegenwärtigen Erkennung von Sicherheitsvorfällen

3.2.2 Absicherung von Servern

Wenn das Unternehmen auch Server betreibt, müssen diese ebenfalls abgesichert werden.

Grundarchitektur nach BSI

Neben der Absicherung von Clients ist es für jede funktionierende IT von Bedeutung, dass ihre Server sicher und stabil laufen. Schaffen es Angreifer Zugriff auf einen Server zu erhalten, können sie Daten abgreifen oder manipulieren oder die Verfügbarkeit des Servers beeinflussen. Ein Server sollte ebenfalls als Minimalsystem konzipiert sein. Die Grundarchitektur des BSI umfasst dabei folgende Punkte:

Absicherung der Server ist von funktionaler Bedeutung für die IT.

- Integritätsprüfung
  - Überwachen von Betriebssystemrelevanten Dateien
- Benutzerverwaltung
  - Zentrales Berechtigungsmanagement mit Zugangskontrolle der einzelnen User
- Patch- und Änderungsmanagement
  - Durch regelmäßige Patches und Updates werden potentielle Schwachstellen reduziert und die Systemstabilität gesteigert
- Datensicherung
  - Bei Datenverlust können Daten aus einem Backup wiederhergestellt werden
- Monitoring
  - Beobachten der relevanten Funktionen einzelner Komponenten, um einen Ausfall rechtzeitig zu bemerken

3.2.3 Absicherung von Netzwerkkomponenten

Netzwerkkomponenten müssen ebenfalls gegen Kompromittierung durch Dritte geschützt werden. Ein gehackter Router lässt sich Beispielsweise für einen DDoS-Angriff[46] nutzen.

Maßnahmen nach BSI

- Firewall
- Zutritts-, Zugangs- und Zugriffskontrolle
- Anti-Malware-Programme
- Schutz vor Ausfällen
- Hardware-Sicherheit
- Notfallvorsorge
- Nicht zuletzt: Schulungen des Personals

Besonders kritische Dienste, müssen durch Alternativsysteme redundant sein.

3.2.4 Redundanzen

Sind die Verfügbarkeitsanforderungen an bestimmte Dienste besonders hoch, müssen durch Alternativsysteme Redundanzen geschaffen werden, die auch bei Ausfall von Teilsystemen die Mindestanforderungen an die Verfügbarkeit und Wirksamkeit des Gesamtsystems gewährleisten.

[46] *Distributed Denial Of Service*

3.3 Sichere Authentifizierung

Bei sicherer Authentisierung und Identifizierung, geht es darum sicherzustellen, dass mit der Person oder dem Gegenstand kommuniziert wird, für den sich der Partner ausgibt. Dies gilt natürlich invers. In diesem Kapitel soll es um generelle Authentisierungsverfahren und Passwortsicherheit gehen.

Authentifizierung und Identifikation stellt sicher, dass der Kommunikationspartner der ist, der er zu sein scheint.

3.3.1 Generelle Authentisierungsverfahren

Es gibt einige grundlegende Authentisierungsverfahren wie zum Beispiel das Passwort-Verfahren. Es gilt als das einfachste Verfahren zur Authentisierung, aber auch als das anfälligste. Es ist eine verschlüsselte Übermittlung des Passworts erforderlich. Zudem muss der User sich an Passwortregeln halten, um ein sicheres zu generieren. Hiervon abgeleitet ist das Einmal-Passwort und wie der Name schon sagt, ist dieses Passwort für den einmaligen Gebrauch verwendbar. Es gibt hierbei zwei Methoden, entweder werden die Passworte im Vorfeld bestimmt und verteilt oder der Benutzer kann sie nach einem definierten Verfahren berechnen.

Beim Challenge-Response-Verfahren muss sich ein Computersystem kryptographisch beweisen, dazu braucht es einen Schlüssel und ein Verfahren. Ein Beispiel ist, dass es eine Zufallszahl als Challenge erhält und als Response die Signatur übermittelt.

Die Authentisierung mit Hilfe von Biometrischen Verfahren ist die Identifikation des Users mit Hilfe von biometrischen Merkmalen. Dies lässt sich wiederum in zwei Unterkategorien teilen. Auf der einen Seite Aktive Merkmale wie zum Beispiel Stimme, Unterschrift oder Tippverhalten und die passiven Merkmale wie zum Beispiel Fingerabdruck, Retina, Iris oder Ohr. Sie sind nutzbar als Zugangskontrollen.

Es gibt mehrere Authentifikationsverfahren. Das Passwort, das Einmal-Passwort, das Challenge-Response-Verfahren sowie Biometrische Verfahren.

3.3.2 Passwortsicherheit

Um einen professionellen Umgang mit Passwörtern zu ermöglichen, bedarf es Hilfsmitteln – denn leicht zu merkende Passwörter sind meist auch für Angreifer leicht erratbar oder schnell zu berechnen – wenn beispielsweise ein persönlicher Bezug besteht, beispielsweise der Name des Betriebs oder wenn das Passwort im Wörterbuch steht. Deutlich sicher sind Passwörter, welche sich an den folgenden Vorgaben orientieren:

- Starke Passwörter sind kryptisch und enthalten mind. 12 Zeichen, Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen
- Keine Universalschlüssel verwenden
- Nutzen Sie Passwort-Manager wie keePass(X)[47]
- Die wichtigsten Passwörter gehören in den Kopf! Merken Sie sich Masterpasswörter mit Eselsbrücken.
- Passworteingabe mit Bedacht!
    - nur an vertrauenswürdigen Rechnern
    - nur bei SSL / TLS-Verschlüsselung (https in Adresszeile, Schloss-Symbol)

Passwörter müssen, um Sicherheit zu gewährleisten, sicher gewählt und mit Bedacht eingesetzt werden.

[47] http://keepass.info/ *Keepass ist ein freier Passwort-Manager.*

3.3.3 Zutritt-, Zugangs- und Zugriffsverwaltung

Um die IT-Infrastruktur zuverlässig verwalten zu können, müssen Kontrollmechanismen eingeführt werden, welche nachvollziehbar machen, wer was, wann und wo getan hat. Angenommen es hat ein Einbruch in die Systeme stattgefunden, dann ist eine gute Protokollierung als Vorkehrung notwendig, um die Ereignisse rekonstruieren zu können.

Damit dies gewährleistet ist, sollte nach dem Minimalismus-Prinzip („Es darf nur der, der muss.“) verfahren werden. Muss ein Mitarbeiter aus der Verwaltung Zugang zum Rechner in der Produktion erhalten? Ist es notwendig, dass alle Mitarbeiter auf alle Ordner in der Server-Freigabe zugreifen können? Diese und ähnliche Fragen sind im Vorfeld zu klären.

Bei Berechtigungen für Zutritt, Zugang und Zugriff ist es empfehlenswert nach dem Motto zu verfahren: „Es darf nur der, der muss“.

Wenn möglich, sollte die Protokollierung genutzt werden. Hierzu zählen zum Beispiel Logdateien[48] der Dienste. Zu einer guten Infrastruktur gehört eine zentrale Nutzerverwaltung. Diese kann zum Beispiel auch auf dem Server laufen, welcher als Ablage für die Daten dient.

Ein weiterer zentraler Bestandteil eines Netzwerkes ist die Nutzerauthentifizierung. Hierbei wird sichergestellt, dass ein Nutzer auch tatsächlich Zugriff auf einen Dienst oder eine Maschine erhalten darf. Dies geschieht in der Regel über die Verwendung von Nutzernamen und Passwort.

Als Beispiel für eine solche zentrale Nutzerverwaltung und Authentifizierung seien hier mit LDAP und RADIUS zwei zugrunde liegende Protokolle genannt, die im Folgenden erläutert werden.

LDAP – Lightweight Directory Access Protocol

LDAP ist ein Protokoll, das die Abfrage und die Bearbeitung von Informationen eines Verzeichnisdienstes über das TCP/IP-Netzwerk ermöglicht. Eine weit verbreitete Umsetzung von LDAP und Beispiel für einen Verzeichnisdienst ist Microsofts Active Directory.

Das Lightweight Directory Access Protocol ist gemäß RFC4510[49] und RFC4511[50] spezifiziert. Es stellt die Definition für Abfragen und Änderungen eines Verzeichnisdienstes bereit. Ein Verzeichnisdienst ist eine hierarchische Datenbank in einem Netzwerk und basiert auf dem Client-Server-Modell. Hierbei handelt es sich um ein Verzeichnis, in welchem Informationen in einer Baumstruktur gespeichert werden. Diese können dann von Clients abgefragt werden. Als Beispiel können auf diese Weise Adressbücher für E-Mail-Clients und Nutzerverwaltungen einfach realisiert werden.

Durch die Verwendung einer Baumstruktur können geographische und andere hierarchische Strukturen geeignet abgebildet werden.

Eine weit verbreitete Umsetzung des LDAP-Protokolls ist das Active Directory von Microsoft. Dieses ist auf allen Microsoft Servern implementiert und bietet viele durch LDAP spezifizierte Funktionen, wie etwa eine komfortable Nutzer- und Rechteverwaltung an.

RADIUS – Remote Authentication Dial In User Service

Das Radius Protokoll ist nach RFC2865[51] spezifiziert und stellt Authentifizierung, Autorisierung und Konfigurationsinformationen für Netzwerke bereit. Das Client-Server Protokoll wird zum Beispiel bei Einwahlverbindungen wie ISDN, DSL oder WLAN in einem Netzwerk eingesetzt.

---

[48] Als Logdateien werden Dateien der Dienste bezeichnet, in welchen alle Vorkommnisse protokoliert wurden. Zum Beispiel die Ereignisanzeige in Windows Betriebssystemen.
[49] http://tools.ietf.org/html/rfc4510
[50] http://tools.ietf.org/html/rfc4511
[51] http://tools.ietf.org/html/rfc2865

3.3.4 Wissen und Besitz

Die Zwei-Faktor-Authentisierung ist ein Identitätsnachweis, bei dem zwei unabhängige Komponenten miteinander verknüpft werden, um die Identität nachzuweisen. Ein Beispiel ist die EC-Karte. Um Geld am Geldautomaten abzuholen, muss der Benutzer die Karte besitzen, sowie die PIN kennen. Fehlt eine Komponente, kann der Geldautomat kein Geld ausgeben.

3.4 System- und Netzwerküberwachung

3.4.1 Firewalls

Firewalls bilden praktisch die erste Verteidigungslinie gegen Angriffe von außerhalb. Sie sind in jedem Fall so zu konfigurieren, dass sie nur die unbedingt erforderlichen Verbindungen zulassen. Besonders sicherheitskritisch ist zudem die Einbindung der Firewall. Es darf keine Kommunikation an Ihr vorbeifließen. Fließen Protokollelemente an der Firewall vorbei, ist der Schutz nicht gewährleistet. Firewalls werden in vier Kategorien eingeteilt:

- Paketfilter
- Stateful Packet Inspection (SPI, im deutschen „Zustandsorientierte Paketüberprüfung“)
- Application Gateway
- Adaptive Proxy

Ein Firewall-System wird wie ein Pförtner zwischen das zu schützende und das unsichere Netz geschaltet, sodass der Datenverkehr zwischen den Netzen nur über das Firewall-System möglich ist.

Um die Funktionsweisen der verschiedenen Firewall-Systeme zu erläutern wird hier die Analogie zu einem Pförtner, welcher ankommende Lieferanten kontrolliert, hergestellt.

Die vier Firewall-Systeme sind: Packet Filter, Stateful Packet Inspection, Application-Gateway und Adaptive Proxy.

„Paket Filter-Pförtner“ schauen auf das Logo des ankommenden LKW und lassen diesen passieren, wenn ihnen dieses bekannt ist.

„Stateful Paket Inspection-Pförtner“ schauen nicht nur nach dem LKW, sondern kontrollieren auch den Lieferschein und begutachten das Paket von außen. Ist alles ok, lassen sie den LKW mit dem Paket passieren.

Der „Application-Gateway-Pförtner” schaut nicht nur die Adressen der eingehenden Lieferungen an, er öffnet auch jedes Paket, prüft den kompletten Inhalt und checkt die Arbeitspapiere des Absenders nach einer klar festgelegten Reihe von Beurteilungskriterien. Nach der erfolgten detaillierten Sicherheitsüberprüfung unterzeichnet der Pförtner den Lieferschein und schickt den LKW wieder auf seinen Weg. Anschließend bestellt er einen vertrauenswürdigen Fahrer der eigenen Firma, der nun die Pakete zum eigentlichen Empfänger bringt. Die Sicherheitskontrolle ist an dieser Stelle wesentlich zuverlässiger und der Fahrer der Fremdfirma erhält keinen weiteren Einblick in das Firmengelände. Die Überprüfungen nehmen zwar mehr Zeit in Anspruch, dafür können jedoch auch mehr sicherheitsgefährdende Aktivitäten ausgeschlossen werden.

Der „Adaptive Proxy Pförtner“ arbeitet in der ersten Phase (Verbindungsaufbauphase) wie der Application Proxy: Er schaut sich nicht nur die Adresse der eingehenden Pakete an, er öffnet auch das Paket und überprüft den gesamten Inhalt. Wenn der Adaptive Proxy den Lieferanten seit langem kennt, dann sendet er den LKW des Lieferanten durch das Tor, damit dieser die Lieferung direkt zustellt. Kennt er den Lieferanten jedoch nicht, dann verabschiedet er den LKW-Fahrer nach Ausladung der Lieferung und bestellt den firmeneigenen Fahrer, der im eigenen LKW das Paket zum Empfänger bringt.

Je nach Umfang des Produktionsnetzes sollte eine entsprechende Firewall eingesetzt werden. Weitergehende Informationen, welche Anforderungen eine Firewall erfüllen sollte, sind vom BSI erhältlich.[52]

3.4.2 Unified Threat Management

Das Unified Threat Management (UTM) ist eine Technologie die, die Zugangspunkt des Internet-Service-Provides positioniert wird. Die oft kleine Box kann, weil sie zwischen das Firmennetzwerk und das Internet geschlossen wird, den gesamten Netzwerkverkehr überwachen.

Ein UTM kann dabei folgende Aufgaben übernehmen:

- Firewall-Funktionen
- Antimalware / Antivirus
- Anti-Spam
- VPN-Gateway
- Inhaltsfilterung

3.4.3 IDS/IPS – Intrusion Detection System/Intrusion Prevention System

Ein IDS dient zur Erkennung von Angriffen. Ein IPS ermöglicht zusätzlich eine automatisierte Reaktion, indem es beispielsweise die Kommunikation beendet.

Intrusion Detection Systeme (IDS) sind Softwarelösungen, welche darauf spezialisiert sind, Einbrüche in Netzwerke automatisch zu erkennen und im Falle eines Einbruchs die zuständigen Personen zu alarmieren. Hierbei werden ähnlich wie bei Antivirus-Lösungen bekannte Muster mit dem bestehenden Netzwerkverkehr abgeglichen. Trifft ein bekanntes Muster auf einen Datenstrom zu, wird Alarm geschlagen. Es gibt auch IDS, die mit statistischen Analysen oder Heuristiken arbeiten um auch unbekannte Angriffe erkennbar zu machen. Dadurch werden ähnliche Angriffe erkennbar gemacht, so dass ein Abweichen von der Norm erkannt wird. IDS sind damit genau wie Firewalls nur so gut, wie ihre Konfiguration und die Aktualität ihrer Signaturen. Des Weiteren erfolgt mit einem IDS nur das eruieren von Angriffen. Allerdings werden die Angriffe nicht blockiert und es wird nicht in den Angriff eingegriffen. Open Source-Software für IDS sind Snort[53] oder Hogwash[54].

Intrusion Prevention Systeme (IPS) bieten zusätzlich zu den Funktionen eines IDS die Möglichkeit, auf erkannte Angriffe automatisch zu reagieren. Hierzu wird bei einem erkannten Angriff zum Beispiel der Datenstrom gekappt oder die Firewall-Regeln werden entsprechend beeinflusst, um einen Abbruch der Verbindung vorzunehmen. Des Weiteren kann das IPS unfragmentierte Datenstreams, TCP-Fehler oder ungewollten Transport von Daten aufdecken und bereinigen. Bekannte Open Source-Implementierungen sind Snort oder Lokkit.

Der Einsatz und die Überwachung mittels IDS oder IPS sollte durch Experten durchgeführt werden.

[52] https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Themen/Sicherheitskomponenten/SicherheitsGatewayFirewall/sicherheitsgatewayfirewall_node.html
[53] https://www.snort.org/ Snort IDS
[54] http://hogwash.sourceforge.net/docs/overview.html Hogwash IDS

3.4.4 SIEM – Security Information and Event Management

Als SIEM-System bezeichnet wird eine Software bezeichnet, die in der Lage ist, sicherheitsrelevante Meldungen auszuwerten und Administratoren zu benachrichtigen. Hierzu werden Meldungen und Nachrichten von allen Datenquellen der Infrastruktur aggregiert: Netzwerk, IDS/IPS, Firewall, Server, Clients, Datenbanken, Anwendungen, und so weiter. SIEM ist eine Zusammenfassung der ehemals getrennten Kategorien SIM – Security Information Management und SEM – Security Event Management.
Hersteller von SIEM-Systemen und deren Produkte sind unter anderem (Dr. Dobb's, 2007):

- Check Point – Eventia[55]
- eIQ Networks – SecureVue[56]
- Symantec - SIM appliance[57]

SIEM-Systeme werten sicherheitsrelevante Meldungen aus und helfen bei der Bewältigung der Datenflut.

Diese Liste erhebt keinen Anspruch auf Vollständigkeit und dient dazu, zu verdeutlichen, dass auch in diesem Bereich eine Vielzahl von Anbietern und Lösungen vorhanden sind.

3.5 Sicherer Fernzugriff

Ein sicherer Fernzugriff kann mit einfachen Methoden umgesetzt werden, dazu sind in den folgenden Abschnitten einige Technologieren dargestellt.

3.5.1 VPN – Virtual Private Network

Ein virtuelles privates Netzwerk, kurz VPN, ist ein Netzwerk, welches in einem anderen Netzwerk gekapselt arbeitet. Als Vergleich kann sich einen Kabelkanal vorgestellt werden, in welchen unterschiedliche Kabel eingezogen sind. Der Kabelkanal ist das Trägernetz und die Kabel bilden die abgekapselten Tunnel. Heutzutage ist das Internet mit seiner weiten Verbreitung und guten Zugänglichkeit in der Regel das Basisnetzwerk in welchem gekapselt wird.
Um über das Internet ein eigenes privates Netzwerk aufzubauen nutzt man Gateways. Diese stellen die Verbindungspunkte zu einem Teil des privaten Netzwerks dar. Die Verwendung von Gateways bietet den Vorteil, dass sowohl andere Gateways mit dahinter geschaltetem Netzwerk, als auch Clients sich direkt mit diesen verbinden können. Die Verbindung der unterschiedlichen Punkte eines virtuellen Netzwerks nennt man auch Tunnel. Dies ist darin begründet, dass alle Daten an den jeweiligen Punkten durch die Verwendung eines VPN-Protokolls ein- und wieder ausgepackt werden. Das Netzwerk wird durch eine Verschlüsselung des Tunnels privat – von außen kann der Inhalt der getunnelten Kommunikation nicht eingesehen werden. In Abbildung 35 wird exemplarisch dargestellt, wie durch die Verwendung von Gateways ein virtuelles Netz erzeugt wird.

Ein Gateway ist ein Protokollumsetzer zwischen unterschiedlichen Netzwerkprotokollen, der es ermöglicht, dass Daten z.B. aus dem Internet in ein lokales Netz gelangen und umgekehrt. Gateways arbeiten auf den Schichten 4 bis 7 des ISO/OSI-Modells.

[55] *http://www.checkpoint.com/products/er/*
[56] *http://www.eiqnetworks.com/products/securevue/log-management-and-siem*
[57] *http://www.symantec.com/business/support/index?page=landing&key=52517*

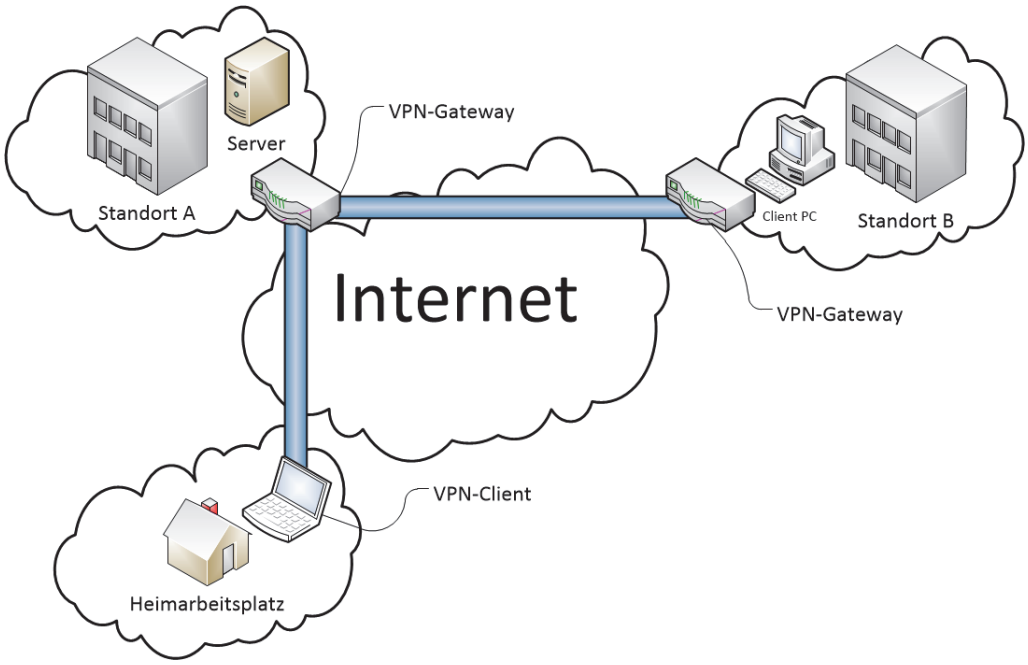


Abbildung 35: Ein VPN mit Gateways und Client

Auf der Grafik ist zu erkennen, dass am Standort A ein Server in einem Netzwerk vorhanden ist. Dieser soll für die Arbeitsplätze am Standort B und den Heimarbeiter zu erreichen sein. Hierzu wird ein VPN-Gateway genutzt. Da mehrere Arbeitsplätze am Standort B den Zugriff benötigen, bietet es sich an, die Verbindung von einem zentralen Punkt aus zu regeln. Aus diesem Grund wurde hier ein weiterer VPN-Gateway eingerichtet. Für alle Netzteilnehmer am Standort B ist der Server an Standort A nun so zu erreichen, als ob der Server lokal angebunden wäre. Für den einzelnen Mitarbeiter zu Hause wird ein VPN-Client verwendet, welcher sich mit dem Gateway verbindet und damit am privaten Netzwerk teilnimmt.
Der Einsatz von VPNs bietet unter anderem folgende Vorteile:

- Gateways sind unabhängig von den Arbeitsplätzen und deren Betriebssystemen (Windows, Linux, Apple).
- Gateways bieten Sicherheit in der Kommunikation zwischen Geräten, welche normalerweise keine Sicherheit implementieren.
- In heterogenen Systemen (andere Hardware, Software und so weiter) kann derselbe Gateway verwendet werden.
- Gateways sind als zentraler Punkt leichter „sicher“ zu realisieren
- Die Sicherheit ist nicht abhängig von anderen Systemkomponenten oder Anwendungen.
- Mit einem VPN-Client können Personen authentifiziert werden.

Für VPNs haben sich zwei Technologien durchgesetzt: IPSec und SSL-VPN.

IPSec – Internet Protocol Security

IPSec ist ein weiterer Sicherheitsstandard und beruht auf einer ganzen Liste von RFCs. Er wurde von der Internet Engineering Task Force (IETF) entwickelt und ist eine gemeinsame Erweiterung des Internet-Protokolls (IP) um Verschlüsselungs- und Authentisierungsmechanismen für Sicherheitsprodukte verschiedener Hersteller. Als Erweiterung des IP-Protokolls bietet IPSec folgende Sicherheitsfunktionen:

IPSec ist ein Sicherheitsstandard und eine Erweiterung des IP-Protokolls, das speziell für VPN entwickelt wurde.

- Schutz der Pakete gegen Manipulation.
- Verschlüsselung der Pakete.
- Schutz vor Wiedereinspielung der Pakete. Dies verhindert zum Beispiel, dass aufgezeichnete Befehle ein weiteres Mal von anderen gesendet werden können.
- Schutz vor Verkehrsflussanalyse. Dies verhindert, dass durch Beobachtung des Verkehrs Rückschlüsse auf die Teilnehmer gemacht werden können.
- Authentisierung der Kommunikationspartner (Gateways oder Nutzer).

Diese Funktionen bilden die vollständige Umsetzung aller Anforderungen für VPNs.

SSL-VPN

Die als SSL[58]-VPN bekannt gewordene Technologie nutzt TLS, Transport Layer Security Protocol, zur Herstellung einer sicheren, verschlüsselten Verbindung.
Die bekannteste und am weitesten verbreitete Implementierung von SSL-VPN ist OpenVPN[59]. Diese zeichnet sich besonders durch ihre einfache Konfigurierung aus und wird von vielen Betrieben schon lange erfolgreich eingesetzt. OpenVPN wird als Open-Source Software gepflegt und ist somit kostenfrei einsetzbar. Die Verschlüsselung und Authentifizierung wird bei SSL-VPN über das TLS-Protokoll hergestellt.

SSL-VPN nutzt das TLS-Protokoll zur Herstellung einer verschlüsselten Verbindung. Eine bekannte Implementierung ist die Open-Source Lösung OpenVPN.

Wenn Sie VPNs nutzen möchten empfiehlt sich die Verwendung von OpenVPN.

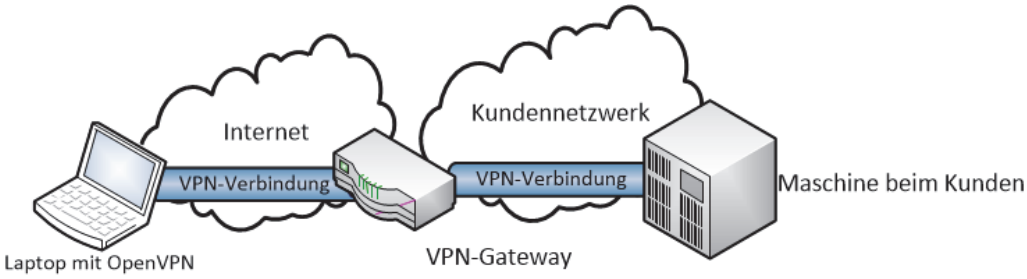


Abbildung 36: VPN-Verbindung vom Client zum Gateway

[58] *SSL steht für Secure Socket Layer*
[59] *www.openvpn.de*

3.6 DMZ – Demilitarized Zone

Eine DMZ bezeichnet einen von innen und außen abgesicherten aber von außen erreichbaren Bereich.

Als eine demilitarisierte Zone wird in der Informatik den Umstand bezeichnet, Bereiche eines Netzwerks gesichert von außerhalb erreichbar zu machen. Hierzu werden Router und Firewalls eingesetzt. Durch die Trennung eines Netzwerks in den öffentlichen und nicht-öffentlichen Bereich, wird eine Schutzzone für das interne Netz kreiert. Das BSI empfiehlt im IT-Grundschutz den Aufbau einer DMZ mit Hilfe einer zweistufigen Firewall: Die erste Firewall trennt die Server vom Internet und die Zweite trennt die DMZ mit den Servern vom Intranet ab. Eine Verbindung des Intranets zum Internet ist über die beiden Firewalls möglich. Dies ist in Abbildung 37 dargestellt. Für eine DMZ sollten Firewalls verschiedener Hersteller verwendet werden, da ansonsten im Falle einer Schwachstelle direkt beide Firewalls überwunden werden könnten.

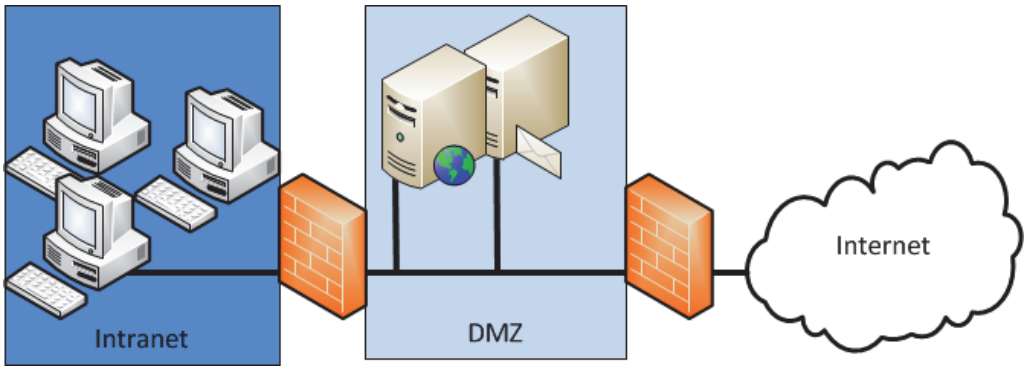


Abbildung 37: Eine DMZ mittels zweistufiger Firewall

3.7 Zusammenfassung

In diesem Kapitel wurden diverse Maßnahmen und Möglichkeiten zur Gewährleistung der IT-Sicherheit aufgezeigt. Neben einem guten Konzept zur Erstellung einer IT-Sicherheitsstrategie und der Durchführung dieser im Unternehmen ist es von essentieller Bedeutung, einen groben Überblick über Lösungsansätze in der IT-Sicherheit zu haben. Die einzelnen Komponenten innerhalb des Firmennetzwerks sollten gegen Zugriff von außerhalb abgesichert werden. Dazu gehören mindestens ein starkes Verfahren zur Authentifikation der Nutzer, sowie eine Lösung zur System- und Netzwerküberwachung. Das Mittel der Wahl sollte eine Firewall sein. Ergänzend kann es notwendig sein, ein VPN-Netzwerk aufzubauen um zum Beispiel Filialen oder Dienststellen in einer anderen Stadt, sicher an das Firmennetzwerk anzubinden.

4. Praxisbeispiele für das Handwerk

In den folgenden Abschnitten finden Sie einige kurze Einsatzszenarien im Handwerk.

4.1 Netzwerkanalyse

Bei der Arbeit mit Netzwerktechniken treten häufig Fehler oder andere Problemen auf. Da Netzwerke komplexe Gebilde aus Geräten und Kabeln darstellen, finden Sie im Handbuch „IT-Sicherheit in der Produktion“ Tipps, um Erste-Hilfe-Maßnahmen durchzuführen. Diese Tipps gelten generell für alle Netzwerke, stellen aber eine Auswahl dar, welche mit Hinblick auf Produktionsnetze besonders relevant sind. Beantwortet werden die folgenden Fragen:

- Wie teste ich die Verbindung von zwei Teilnehmern eines Netzwerks?
- Wie kann ich meine Einstellungen bei Netzwerkgeräten sichern?
- Wie kann ich meine Firewall-Einstellungen testen?
- Wie kann ich eine Client-Firewall einstellen, um eine Verbindung zu blockieren?
- Wie schalte ich USB-Ports an Computern aus?

4.2 Virtual Private Network (VPN)

Die Konditorei Herkerath expandiert in die Nachbarstadt. Es wird eine neue Filiale eröffnet und diese soll an das Unternehmensnetz angeschlossen werden. Zudem stellt die Konditorei einen Außendienstler ein. Dieser reist durch die Städte auf der Suche nach weiteren Standorten und braucht ebenfalls eine Verbindung zum Unternehmensnetzwerk. Im Unternehmen steht ein VPN-Gateway zur Verfügung. Die neue Filiale soll von Gateway-zu-Gateway verbunden werden, während der mobile Außendienstler sich über einen Client in das VPN-Netzwerk einwählen soll.

Wichtig für den Betrieb ist es, dass die Daten vertraulich übertragen werden und die Integrität gewährleistet wird. Die Daten sollen also nach Möglichkeit verschlüsselt übertragen werden. Dadurch kann kein Unbefugter die Daten mitlesen oder manipulieren. Der Schutz vor Manipulation führt zur Gewährleistung der Integrität. Zudem soll die gewählte Lösung über eine hohe Verfügbarkeit gewährleisten. Dadurch wird die Ausfallsicherheit erhöht und es ist eindeutig feststellbar, dass die Filialen untereinander kommunizieren. Frei verfügbare Softwarelösungen für VPN-Netzwerke sind zum Beispiel OpenVPN oder Tinc.

4.2.1 Gateway to Gateway

Die Gateway-zu-Gateway Verbindung ist das Mittel zur Wahl, um zwei stationäre Punkte, zum Beispiel die beiden Konditoreifilialen, innerhalb eines VPN-Netzwerks zu verbinden. Mit Hilfe eines Gateways können heterogene Systeme, unabhängig von ihren Sicherheitskomponenten, miteinander verbunden werden. Das heißt, es muss nicht dieselbe Netzstruktur und Hardware in den Filialen genutzt werden, da der Netzwerkverkehr an das Zentrale Gateway geleitet wird und zum anderen getunnelt wird. Dort wird er entsprechend weiterverarbeitet. Dieses Konzept ist zudem leicht

realisierbar. Dadurch passt es zu den Anforderungen der Konditorei, die erfüllt werden müssen, um eine neue Filiale in das Unternehmensnetz zu integrieren.

4.2.2 Client to Gateway

Die Client-Lösung ist kostengünstiger als die Gateway-Lösung und kann auf dem Endgerät des Außendienstmitarbeiters realisiert werden. Der Außendienstmitarbeiter kann mit dieser Lösung zudem eindeutig identifiziert werden, da er sich im VPN-Netzwerk mit seinen Zugangsdaten authentifizieren muss. Es wird eine gesicherte Ende-zu-Ende-Verbindung zwischen dem Client und dem Gateway aufgebaut. Dadurch kann der Außendienstmitarbeiter abhörsicher auf die Unternehmensdaten zugreifen, auch wenn er sich nicht in Reichweite des Unternehmensnetzwerks befindet.

4.3 Das Konzept Firewall

Um den ein- und ausgehenden Netzwerkverkehr zu beobachten und zu bewerten, möchte die Konditorei Herkerath eine Firewall betreiben.

4.3.1 Personal Firewall

Die Personal Firewall wird auf einem Host-Rechner installiert und schützt diesen vor Angriffen aus dem öffentlichen Netz. Sollte ein Rechner mit Malware infiziert sein, kann sie die anderen Rechner im Netzwerk vor Befall schützen, da sie auch den ausgehenden Netzwerkverkehr analysiert. Es kann zudem genau analysiert werden, welche Applikationen, welche Netzwerkedienste nutzen und anfordern. Dadurch wird ein applikationsspezifisches Filtern möglich. Ein großer Nachteil dieses Systems ist, dass die Firewall-Software selbst angegriffen werden könnte.

4.3.2 Dedizierte Firewalls

Unter einer dedizierten Firewall ist ein externes Gerät zu verstehen, auf dem eine Firewall implementiert ist. Dedizierte Firewalls können ein eigenes Betriebssystem haben und auf unterschiedliche Netzwerkebenen zugreifen. Mit Hilfe der dedizierten Firewall lässt sich eine klare Trennung zwischen privatem und öffentlichem Netzwerk realisieren, da nicht der PC, sondern die Firewall an das Internet angeschlossen wird und als Kommunikationspartner dient. Für die Konditorei Herkerath besteht dadurch außerdem die Möglichkeit, das Netz der Personalabteilung vom restlichen Unternehmensnetzwerk abzukoppeln. Dadurch wird die Sicherheit der Mitarbeiterdaten gegenüber internen Angriffen erhöht.

4.4 Zusammenfassung

Die oben genannten Beispiele sollen als Hilfestellung dienen, wie Sie die Sicherheit in einem Unternehmensnetzwerk erhöhen können und sich gegen externe Angriffe schützen. Im Praxisfall muss immer abgewogen und analysiert werden wo sich kritische Daten und Werte befinden und wie diese optimal geschützt werden können. Firewalls werden dabei meist verwendet um den Netzwerkverkehr abzusichern und zu analysieren, während VPN-Systeme die integrere, sichere Übertragung von Daten gewährleisten sollen. Eine Kombination beider Methoden ist in den meisten Anwendungsszenarien sinnvoll und erwünscht.

5. Checkliste „Netzwerksicherheit“

IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

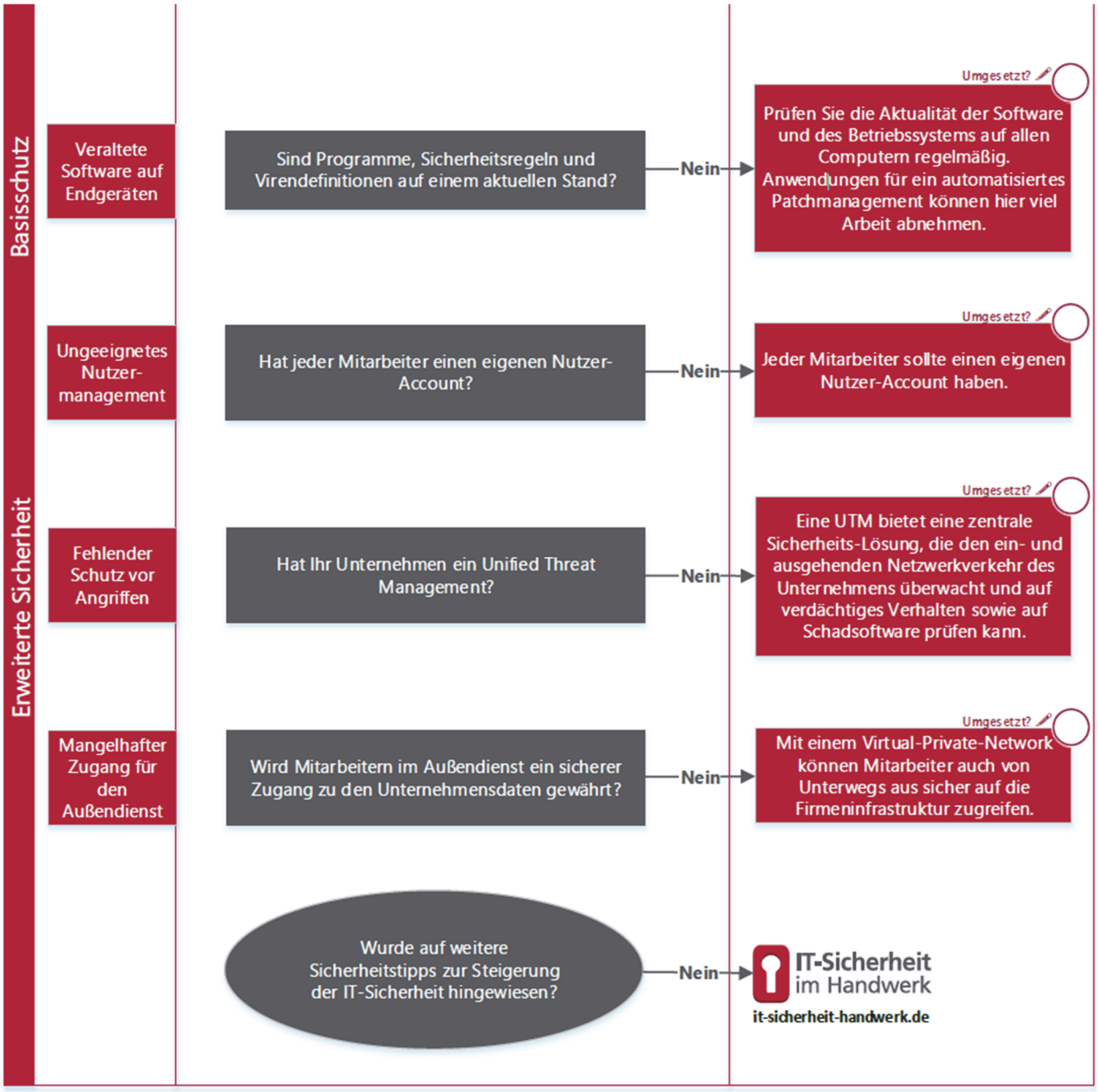
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Netzwerksicherheit

	Gefahr/ Risiko	Erhebung des Ist-Zustands		Maßnahme
Geeignete Unterstützung	Fehlende professionelle Unterstützung	Haben Sie einen kompetenten Partner, der Sie beim Aufbau oder beim Betrieb ihrer Netzwerkinfrastruktur unterstützt?	Nein →	Umgesetzt? Sie sollten ein Zertifiziertes Systemhaus auswählen, was Sie kompetent und vertrauenswürdig in allen Belangen rund um das Thema Netzwerksicherheit unterstützt.
Erfassen Sie den Bestand	Keine Bestands-erfassung	Ist geklärt, welche Netzwerkteilnehmer auf das interne Netzwerk und welche auf das Internet zugreifen dürfen?	Nein →	Umgesetzt? Erstellen Sie eine Liste mit Netzwerkteilnehmern, die auf das interne Netzwerk und auf das Internet zugreifen dürfen.
		Existiert eine Übersicht über notwendige Programme?	Nein →	Umgesetzt? Vielen Anwendern ist nicht klar, welche Applikationen auf das Internet zugreifen dürfen. Erstellen Sie eine Liste mit Anwendungen die unbedingt einen Zugriff auf das Internet benötigen.
Etablieren Sie einen Basisschutz	Fehlender Basisschutz	Besitzen Ihre Geräte einen Basisschutz, der mindestens einen aktuellen Antivirenschutz und eine Firewall beinhaltet?	Ja →	Umgesetzt? Sorgen Sie dafür, dass auf jedem Netzwerkteilnehmer eine Firewall installiert ist. Eine Security Suite, eine Kombination aus Antivirus und Firewall aus einer Hand ist hier empfehlenswert
		Sind die Firewall-Systeme angelernt worden oder basieren diese auf vordefinierten Regeln?	Ja →	Umgesetzt? Firewall-Regeln sind für einen unerfahrenen Nutzer immer voreinzustellen, sie erlauben seriösen und geprüften Anwendungen automatisch einen Internetzugang. Regelerstellung über einen manuellen Eingriff sollte nur durch erfahrenes Personal vorgenommen werden.



TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Task Force „IT-Sicherheit in der Wirtschaft"
Die Task-Force „IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de

itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is) - Institut für Internet-Sicherheit der Westfälischen Hochschule

6. Weblinks

- http://www.it-sicherheit-handwerk.de/
- https://www.internet-sicherheit.de/
- http://www.heise.de/security
- http://www.wireshark.org/
- https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

7. Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. (12. März 2012). *Industrial Control System Security - Top 10 Bedrohungen*. Abgerufen am 5. August 2013 von https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Content_Cyber-Sicherheit/Analysen/Statistiken/BSIa004.html

Deering, S., & Hinden, R. (Dezember 1998). *Internet Protocol, Version 6 (IPv6).* Abgerufen am 29. Januar 2014 von RFC 2460: http://tools.ietf.org/html/rfc2460

Dr. Dobb's. (05. Februar 2007). *SIEM: A Market Snapshot.* Abgerufen am 19. August 2013 von http://www.drdobbs.com/siem-a-market-snapshot/197002909

heise.de. (31. Januar 2007). *Ein Ping - und Solaris gerät in Panik*. Abgerufen am 9. August 2013 von http://www.heise.de/security/meldung/Ein-Ping-und-Solaris-geraet-in-Panik-140956.html

NIST. (17. Juni 2009). *Report to NIST on the Smart Grid Interoperability Standards Roadmap.* Abgerufen am 24. Januar 2014 von http://www.nist.gov/smartgrid/upload/InterimSmartGridRoadmapNISTRestructure.pdf

Pohlmann, N. (2003). *Firewall-Systeme – Sicherheit für Internet und Intranet, E-Mail-Security, Virtual Private Network, Intrusion Detection-System, Personal Firewalls.* Bonn: MITP-Verlag.

Pohlmann, N., & Blumberg, H. (2006). *Der IT-Sicherheitsleitfaden.* Heidelberg: REDLINE GmbH.

Postel, J. (September 1981). *Internet Protocol.* Abgerufen am 29. Januar 2014 von RFC 791: http://tools.ietf.org/html/rfc791

Rigney, C., Willens, S., Simpson, W., & Rubens, A. (Juni 2000). *RFC2865.* Abgerufen am 29. Januar 2014 von RFC2865: http://tools.ietf.org/html/rfc2865

Ryan, T. (2010). *Getting In Bed with Robin Sage.* Abgerufen am 7. August 2013 von https://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf

Sermersheim, E. J. (Juni 2006). *Lightweight Directory Access Protocol (LDAP): The Protocol.* Abgerufen am 29. Januar 2014 von RFC4511: http://tools.ietf.org/html/rfc4511

Stahl, L.-F. (November 2013). Gefahr im Kraftwerk. *c't*, S. 78 ff.

Technische Universität Dresden. (2012). *DIN EN 61131.* Abgerufen am 19. August 2013 von http://www.et.tu-dresden.de/ifa/uploads/media/PLT1_002-IEC61131-Architektur_03.pdf

Zeilenga, K. (Juni 2006). *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.* Abgerufen am 29. Januar 2014 von RFC4510: http://tools.ietf.org/html/rfc4510

8. Stichwortverzeichnis

I

K

L

M

N

O

P

R

S

T

U

V

W

X

9. Abbildungsverzeichnis

10. Tabellenverzeichnis

9 783944 916163