

Sprung auf  
Programmseite

Daten

► Programm

ITWissen



Das große Online-Lexikon  
für Informationstechnologie

Daten

Programm ►

# WEB-GEFAHREN, -SICHERHEIT

KLAUS LIPINSKI (Hrsg.)

Wiederholung  
des Programms

## Inhalt

<b>Abhörsicherheit</b>	<b>HIDS, host-based intrusion detection system</b>	<b>PPTP, point to point tunneling protocol</b>
<b>Angreifer</b>	<b>Hoax</b>	<b>Risiko</b>
<b>Angriff</b>	<b>Honeypot</b>	<b>Sabotage</b>
<b>Anwendungssicherheit</b>	<b>IDMEP, intrusion detection message exchange protocol</b>	<b>SATAN, security administrator tool for analyzing networks</b>
<b>Backdoor</b>	<b>IDS, intrusion detection system</b>	<b>Schwachstelle</b>
<b>Bedrohung</b>	<b>Incident-Response</b>	<b>Security-Appliance</b>
<b>Broadcaststurm</b>	<b>Informationssicherheit</b>	<b>Sicherheit</b>
<b>Brute-Force-Angriff</b>	<b>Internet-Sicherheit</b>	<b>Sicherheitsdienst</b>
<b>BSI, Bundesamt für Sicherheit in der Informationstechnik</b>	<b>IP-Spoofing</b>	<b>Sicherheitspolitik</b>
<b>CDSA, common data security architecture</b>	<b>IPS, intrusion prevention system</b>	<b>Sicherheitsrichtlinie</b>
<b>Content-Sicherheit</b>	<b>IPSec, IP security protocol</b>	<b>Sicherheitsvereinbarung</b>
<b>Crack</b>	<b>ISSA, information systems security association</b>	<b>SIM, security information management</b>
<b>Cracker</b>	<b>IT-Sicherheit</b>	<b>Sniffer</b>
<b>Crasher</b>	<b>ITW, in the wild</b>	<b>Snooping</b>
<b>CSRF, cross site request forgery</b>	<b>L2Sec, layer 2 security</b>	<b>Spam</b>
<b>Datensicherheit</b>	<b>Makrovirus</b>	<b>Spim, instant message spam</b>
<b>DDoS, distributed denial of service</b>	<b>Malware</b>	<b>Spoofing</b>
<b>DNSSEC, domain name system security extension</b>	<b>Man-in-the-Middle-Angriff</b>	<b>Spyware</b>
<b>DoS, denial of service</b>	<b>Netzwerksicherheit</b>	<b>Tempest, transient electromagnetic pulse emanation standard</b>
<b>Eindringen</b>	<b>NIDS, network-based intrusion detection system</b>	<b>Trojaner</b>
<b>Eindringling</b>	<b>Penetrationstest</b>	<b>Virus</b>
<b>EPIC, electronic privacy information center</b>	<b>Perimeter-Sicherheit</b>	<b>WAS, web application security</b>
<b>Fluten</b>	<b>Phishing</b>	<b>WSS, web service security</b>
<b>Hacker</b>	<b>Phreaking</b>	<b>Wurm</b>
<b>Heuristik</b>	<b>PnP-Sicherheit</b>	<b>XSS, cross site scripting</b>

## **Abhörsicherheit** *bug proof*

Unter Abhörsicherheit versteht man ganz allgemein die *Sicherheit* gegen unberechtigtes Mithören von Dritten bei der Übertragung zwischen Endteilnehmern. Dabei kann es sich sowohl um die drahtlose Übertragung mittels Funktechnik handeln als auch um das Abhören der leitungsgebundenen Übertragung über Kabel oder Lichtwellenleiter. Das Abhören betrifft die Daten- als auch die Sprachkommunikation, wobei letztere durch das Fernmeldegeheimnis geschützt ist.

Zur Vermeidung des Abhörens werden verschiedene Techniken eingesetzt. Diese reichen von der Feldstärkemessung über die OTDR-Technik und der Dämpfungsmessung der Übertragungsstrecke bis zur Verschlüsselung der Information, der gängigsten Methode gegen unberechtigtes Abhören.

Bei der Mobilkommunikation, bei der die Luftschnittstelle offen ist, werden zu diesem Zweck alle Gespräche individuell verschlüsselt. Als Verschlüsselungsalgorithmus wird ein teilnehmereigener Primzahlen-Algorithmus verwendet, der sich auf der *SIM*-Karte befindet, aber nicht ausgelesen werden kann.

## **Angreifer** *attacker*

Als Angreifer werden in der Kommunikationstechnik Personen bezeichnet, die versuchen eine verschlüsselte Nachricht auf dem Übertragungsweg abzufangen und diese zu entschlüsseln. Nicht zu verwechseln mit den *Hackern*, die sich unberechtigten Zugang zu Systemen verschaffen.

## **Angriff** *attack*

Angriffe sind unerlaubte und unautorisierte Aktivitäten zum Schaden von Ressourcen, Dateien und Programmen. Man unterscheidet zwischen passiven und aktiven Angriffen. Passive Angriffe bedrohen die Vertraulichkeit der Kommunikation, beeinflussen aber nicht die Kommunikation oder den Nachrichteninhalt. Sie zielen ausschließlich auf die unerlaubte Informationsbeschaffung. Die *Abhörsicherheit* kann durch diverse Verfahren unterlaufen werden. Eines der bekanntesten ist *Tempest*, bei dem die elektromagnetische Strahlung von Bildschirmen, Computerboards und Datenkabel empfangen und ausgewertet wird. Ein großes Angriffspotential bieten alle Datenkabel, Telefonleitungen, Lichtwellenleiter und vor allem die Funktechnik, die besonders gefährdet ist. Ist es bei Datenkabeln die elektromagnetische Strahlung, die abgehört werden kann, so besteht bei Lichtwellenleitern die Möglichkeit diese stark zu krümmen, bis die Moden das Kernglas verlassen und die optischen Signale austreten.

Bei den aktiven Angriffen werden die Nachrichten, die Komponenten des Kommunikationssystems oder die Kommunikation verfälscht. Es kann sich dabei um Angriffe kann auf Netze, um diese funktional zu stören, wie beispielsweise eine *DoS-Attacke*, um Angriffe auf den Zugang zu Systemen oder um die Entschlüsselung verschlüsselter Daten und Nachrichten. Ein aktiver *Angreifer* kann durch Einfügen, Löschen oder Modifizieren von Inhalten bestimmte Reaktionen des Empfängers auslösen und dessen Verhaltensweisen steuern. Zu diesen aktiven Angriffen gehören das Übermitteln von *Viren*, Würmern und *Trojanern*.

## **Anwendungssicherheit** *application security*

Der Schutz der Anwendungsebene ist ein wesentlicher Aspekt der *IT-Sicherheit*, da die Angriffe über Web-Applikationen erfolgen und nicht unmittelbar erkennbar sind. Die Angriffe reichen von Datendiebstahl über Wirtschaftsspionage und Datenmissbrauch bis hin zu Vandalismus. So können auf dieser Ebene Dateien

mit unternehmenskritischen Informationen und schützenswerten Zugriffsberechtigungen entnommen oder E-Commerce auf fremden Accounts missbräuchlich ausgeführt werden.

Application Security dient dem präventiven Schutz und kann durch Erkennen von IT-Risiken in die Applikationsebene implementiert werden. Bei der Anwendungssicherheit wird der Inhalt der Datenpakete überprüft und nicht der Header.

Ansatzpunkte liegen in der genutzten Software, in einer möglichen Authentifizierung bei der Anwendung oder durch geeignete Verschlüsselungsmaßnahmen. So kann man beispielsweise Angriffe, die gleichartig ablaufen wie das Cross Site Scripting (XSS), durch Einbau entsprechender Codes abwehren.

## **Backdoor** *backdoor*

Backdoors sind unberechtigte Zugriffe auf Rechner und deren Datenbestände. Wie der Name sagt, erfolgt der unberechtigte Zugriff durch die Hintertür. Der *Angreifer* erlangt über ein verstecktes, ständig laufendes Programm häufig uneingeschränkte Zugriffsrechte. Im Gegensatz zu *Trojanern* ermöglichen Backdoors einen direkten Zugriff auf den betroffenen Rechner, spionieren interessante und persönliche Daten aus und ermöglichen die Manipulation von Hard- und Software.

Backdoor werden häufig dazu benutzt um *Viren*, *Würmer* oder Trojaner auf dem angegriffenen Rechner zu installieren oder diesen für unbefugte Operationen wie *DDoS-Attacken* zu benutzen.

## **Bedrohung** *threat*

Ganz allgemein versteht man unter Bedrohung eine potentielle Gefahr, die durch eine *Schwachstelle* ausgelöst wird. Es kann sich dabei um ein Ereignis handeln, das Schaden verursacht, um einen *Angriff* auf ein System, eine Übertragungstrecke oder auf den Informationsinhalt einer Nachricht, um Spionage oder *Sabotage* oder auch um Gefahren, die unbeabsichtigt oder durch natürliche Ereignisse wie Stromausfall, absichtlich oder vorsetzlich von Mitarbeitern ausgehen. Bedrohung kann von der Technik selbst ausgehen, durch Fehlbedienungen oder Gewaltanwendung.

In der Informations- und Kommunikationstechnik kann sich die Bedrohung auf die Verfügbarkeit von Systemen und Ressourcen beziehen oder ebenso auf die Integrität und Vertraulichkeit von Nachrichten. Das Potential von Bedrohungen ist unermesslich, da es sich gleichermaßen auf Systeme und Übertragungstechniken, auf Programme und Anwendungen beziehen kann. Es gibt die aktive Bedrohung bei der Informationen oder der Systemstatus verändert werden, oder die passive Bedrohung, deren Fokus sich auf das Ausspähen von Informationen bezieht.

Mit der Bedrohungsanalyse werden alle möglichen Bedrohungsszenarien eines Kommunikations- oder Informationssystems erkannt, analysiert und dokumentiert.

## **Broadcaststurm** *broadcast storm*

Broadcast storms typically occur in the Data Link Layer where many packets from different network protocols exist on the wire. Broadcast storms are typically caused by configuration or software errors, when multiple stations respond to a broadcast.

## **Brute-Force-Angriff** *brute force attack*

Ein Brute-Force-Angriff stellt einen gewaltsamen Angriff auf einen kryptografischen Algorithmus dar. Das Verfahren probiert systematisch alle möglichen Kombinationen durch, um den Krypto-Algorithmus zu knacken.

Brute-Force-Angriffe können ebenso auf verschlüsselte Dateien, Nachrichten und Informationen oder auch auf Passwörter angesetzt werden.

Damit Brute-Force-Angriffe möglichst zeitintensiv sind, setzen die meisten Verschlüsselungssysteme sehr lange Schlüssel ein. Bei einem 32-Bit-Schlüssel wären es vier Milliarden Möglichkeiten, die heutige Personal Computer in Minuten durchprobiert hätten. Entsprechend länger dauert die Ermittlung eines 48-Bit-Schlüssels oder gar eines 64-Bit-Schlüssels, der nur in mehreren tausend Jahren zu knacken wäre.

## **BSI, Bundesamt für Sicherheit in der Informationstechnik** *GISA, German information security agency*

Das Bundesamt für *Sicherheit* in der Informationstechnik (BSI) wurde 1991 nach Inkrafttreten des BSI-Errichtungsgesetzes gegründet. Der Aufgabenbereich des BSI liegt in der Entwicklung und Förderung von Technologien für sichere IT-Netze.

Schwerpunkte der BSI-Aktivitäten sind der Schutz gegen Computer-*Viren*, die elektronische Signatur, die *Internet-Sicherheit*, der IT-Grundschutz, die Überprüfung von Sicherheitsarchitekturen und das E-Government. Verschiedenen Arbeitsgruppen befassen sich mit der Fortentwicklung des E-Government, der Bereitstellung von Computer-Dienstleistungen für Bundesbehörden sowie der Sicherheit des Internet. Das BSI erstellt Dokumente für die genannten Schwerpunkte, die über das Internet abgerufen werden können. <http://www.bsi.de>

## **CDSA, common data security architecture**

Um die *Sicherheit* beim E-Business zu gewährleisten, hat Intel die CDSA-Sicherheitsarchitektur (Common Data Security Architecture) entwickelt. Kern der CDSA-Architektur ist der CSSM-Manager, der aus diversen Programmierschnittstellen (API) besteht, über die *Sicherheitsdienste* angesprochen werden können. Diese wiederum verfügen über Module für verschiedene Verschlüsselungsverfahren sowie für die Verwaltung von Zertifikaten und Schlüsseln. Des Weiteren wird das CSSM-Management von entsprechenden Bibliotheken unterstützt, denen weitere hinzugefügt werden können. Ziel der CDSA-Aktivitäten, die von der Open Group gefördert werden, ist eine Vereinheitlichung von anwendungsspezifischen Sicherheitsmechanismen.

## **Content-Sicherheit** *content security*

Die *Content-Security* befasst sich mit dem Schutz der Informationen vor allen bekannten *Viren*, Würmern und *Trojanern*, sowie mit der Erkennung von neuen Gefahren und die Verhinderung von *Spams*. Zur *Content-Security* gehören Sicherheitslösungen für die Abwehr von Hackerangriffen, die über Sicherheitslücken in Netzwerken und Anwendungen Schaden anrichten.

Bei der *Content-Security* werden die Daten hinsichtlich ihrer Integrität geprüft; des Weiteren wird geprüft ob sie verschlüsselt gesendet, empfangen und genutzt werden dürfen. Diese Sicherheitsprüfungen erfolgen nach einem festgelegten Regelwerk, den Policies, mit dem organisatorische und personenspezifische Kenndaten überprüft werden.

Die Maßnahmen für die *Content-Security* reichen von Anti-Virus-Programmen mit denen der Web-Verkehr und alle E-Mails gescannt werden, über die Abwehr von Hackerangriffen bis hin zu nachgeschalteten Anti-Spam-Filtern, Web-Filtern und E-Mail-Filtern. Wobei die Web-Filterung unerwünschte Webseiten ausfiltert und die E-Mail-Filterung die E-Mails inhaltsabhängig nach Text- und Anhängen durchsucht und entsprechend ausfiltert.

<b>Crack</b>	<p>Cracks sind illegale Programme, die den Kopierschutz bzw. die Seriennummernverwaltung von Software knacken und entfernen. Über das Crack-Programm kann dann kostenlos eine ansonsten kostenpflichtige Software benutzt werden. Das Crack-Programm trennt die für den Kopierschutz relevanten Programmteile und inaktiviert den Kopierschutz.</p> <p>Die Crack-Programme setzen bei der Testsoftware an und laden später die fehlenden Dateien aus dem Internet nach. Sie können auch die Software manipulieren und damit eine ständige Programmarchivierung verhindern.</p> <p>Cracks werden vorwiegend bei Spielfilmen und Videospielen eingesetzt, die auf optischen Speichermedien stehen gespeichert werden, und werden auch im Internet angeboten. Das Cracken wird als Urheberrechtsverletzung geahndet; in vielen Fällen wurde bereits gegen das Downloaden der Cracks vorgegangen.</p>
<b>Cracker</b>	<p>Ein Cracker ist eine Person, die unberechtigt in ein Computersystem eindringt. Ziel der Cracker - der Begriff wird oft synonym mit <i>Hacker</i> verwendet - ist es, die Sicherheitssysteme zu knacken und die gewonnenen vertraulichen Daten nicht zum wirtschaftlichen oder sozialen Nachteil für das betroffene Unternehmen oder die betroffene Institution auszunutzen.</p> <p>Cracker verursachen häufig Schäden an den Systemen, im Gegensatz zu Hackern, die meistens nur ihre spezifische Visitenkarte hinterlassen.</p> <p>Im deutschen Sprachgebrauch versteht man unter einem Cracker eine Person die den Kopierschutz von Systemen knackt.</p>
<b>Crasher</b>	<p>Die Begriffe <i>Hacker</i>, <i>Cracker</i> und <i>Crasher</i> haben unterschiedliche Bedeutung. Bei einem Crasher handelt es sich um jemanden, der Vandalismus in Computersystemen ausübt, diese zum Absturz bringt und vorsätzlich Schaden anrichtet.</p>
<b>CSRF, cross site request forgery</b>	<p>Cross Site Request Forgery (CSRF) ist eine Angriffsart, bei der der <i>Hacker</i> die Kontrolle über den Browser seines Opfers übernimmt. Sobald sich dieser bei einer Website eingeloggt hat, agiert er in dessen Namen indem er beispielsweise böartige Anfragen an die Web-Applikation stellt. Die CSRF-Attacken werden auch als "Session Riding" oder "One Click Attacks" bezeichnet.</p> <p>Durch diese Angriffe sind Web-Seiten relativ stark angreifbar. Verhindern lassen sich CSRF-Attacken dadurch, dass die Browser nicht die automatisch übermittelten Daten benutzen, sondern nutzerspezifischen Token verwenden.</p>
<b>Datensicherheit</b> <i>data security</i>	<p>Gesetzliche Regelungen und technische Maßnahmen, durch die die unberechtigte Speicherung, Verarbeitung und Weitergabe schutzwürdiger Daten verhindert werden soll. Ziel ist es, die Persönlichkeitsrechte des Menschen vor den Folgen der Erfassung seiner Individualdaten bei der manuellen und automatischen Datenverarbeitung zu schützen. Innerhalb eines Betriebs gehören dazu personelle, organisatorische und revisionstechnische Regelungen, außerdem geräte- und programmtechnische Schutzmechanismen.</p>

Datenschutz, Datenintegrität und Datensicherung bilden die verlässliche Informationsverarbeitung. In Deutschland ist der Datenschutz durch das "Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung" vom 27.1.1977 im Bundesdatenschutzgesetz (BDSG) verankert. Gewerbliche oder staatliche Computeranwender mit schutzbedürftigen Daten müssen Datenschutzbeauftragte einsetzen. Darüber hinaus gibt es in Deutschland das Bundesgesetz über den Datenschutzgesetz vom 19.06.1992. Es lautet: "Wer personenbezogene Daten für sich selbst oder im Auftrag für andere elektronisch bearbeitet, muss durch geeignete Maßnahmen den Verlust und den Missbrauch dieser Daten verhindern".

## **DDoS, distributed denial of service** *DDoS-Attacke*

Ein Distributed *Denial of Service* (DDoS) ist eine DoS-Attacke, die von verschiedenen Systemen aus gleichzeitig erfolgt. Die DDoS-Attacke wird zum gleichen Zeitpunkt von den verschiedenen Computern ausgelöst und ist dadurch nur schwer zu orten und noch schwieriger zu unterbinden. Die Koordination solcher DDoS-Attacken erfolgt zentral über so genannte Handler, die gleichzeitig Hilfsprogramme aktivieren.

Da die eigentlichen Attacken über die Hilfsprogramme ablaufen, ist der Verursacher schwer zu ermitteln.

## **DNSSEC, domain name system security extension**

Beim Domain Name System (DNS) findet die Kommunikation zwischen dem Nameserver und dem Client über das UDP-Protokoll statt. Dieses verbindungslos arbeitende Transportprotokoll sieht keine Authentifizierung der Nachrichtenquelle vor. Dadurch kann die Identität des Absenders vom Empfänger nicht überprüft werden. Es kann also nicht sichergestellt werden, ob die Nachricht tatsächlich von dem entsprechenden DNS-Server stammt.

Wird das Datenfeld für den Eintrag der Absenderadresse manipuliert und eine andere IP-Adresse eingetragen, gefährdet dies alle Internet-Anwendungen. Um entsprechende Manipulationen auszuschließen, hat die IETF das Domain Name System *Security* Extension (DNSSEC) entwickelt. Es handelt sich dabei um eine Protokollerweiterung des Domain Name System, die mit dem Public-Key-Verfahren arbeitet und die Nachrichtenquelle authentifiziert. Damit ist sichergestellt, dass die Antwort des Nameservers den Angaben entspricht, die ihr zugeordnet sind. Die Entwicklung von DNSSEC reicht zurück in das Jahr 1994 und ist verankert in der RFC 2535. Darüber hinaus gibt es diverse RFCs, die sich mit DNSSEC befassen. Die 2005 vorgestellte Version fasst die diversen RFCs unter der Bezeichnung DNSSEC-bis zusammen.

DNSSEC arbeitet mit kryptografischen Domain-Namen und zielt auf die Bereiche Schlüsselverteilung, Authentifizierung der Ursprungsdaten und Transaktion der Authentifizierung ab. Bei Anfragen an den DNSSEC-Server sendet dieser einen umfangreicheren DNS-Record, der mit einem Private Key unterzeichnet ist.

Der Anfragende kann damit den Response auf Echtheit und Unverfälschtheit überprüfen. Die Antwort erhält außerdem ein Zertifikat mit dem der Empfänger auch den Absender und damit den Informationsinhalt verifizieren kann. Die digitale Signatur der Datenpakete basiert auf einer Hashfunktion, die vom Empfänger erzeugt und mit der Signatur verglichen werden kann.

## DoS, denial of service *DoS-Attacke*

Denial of Service (DoS) sind Attacken im Internet zur Beeinträchtigung von Webservices, die damit außer Betrieb gesetzt werden. Diese Angriffe können durch Überlastung von Servern ausgelöst werden, so beispielsweise mittels der Bombardierung eines Mail-Servers mit einer so großen Anzahl von Mails, dass dieser seine Funktion wegen Überlast nicht mehr ausüben kann, oder durch die Überflutung eines Netzwerks mit Datenpaketen.

DoS-Attacken zielen in der Regel nicht auf den Zugang zum Netzwerk, System oder zu den Datenbeständen ab, sondern haben das Ziel einen Dienst einzuschränken, zu blockieren oder unbenutzbar zu machen. Dazu werden die zur Verfügung stehenden Programme oder Netzwerk-Ressourcen außerordentlich überbelastet.

Ein DoS-Angriff kann durch *IP-Spoofing* vorbereitet werden. Der *Angreifer* nutzt dazu eine autorisierte IP-Adresse und gelangt so in das System oder das Netzwerk, um dann seine DoS-Attacke auszuführen. Neben dem Mail-Bombing, gibt es noch das *SYN-Flooding*, das *Ping-Flooding* und die *DDoS-Attacken*.

## Eindringen *intrusion*

Jedes Eindringen in fremde Datenbestände, sei es körperlich, indem Räume betreten werden, um an die dort aufbewahrten Datenbestände heranzukommen, sei es über Datennetzleitungen, evtl. unter Umgehung des Passwortschutzes oder anderer Sicherheitsmaßnahmen, ist eine Intrusion. Intrusionen, auch versuchte, sind datenschutzrechtlich und strafrechtlich relevant.

## Eindringling *intruder*

Wer widerrechtlich in fremde Datenbestände eindringt und sie sich und anderen zur Kenntnis bringt, wird als Intruder bezeichnet. Dabei unterscheidet man zwischen passiven Intrudern, die sich nur Daten, die nicht für sie bestimmt sind, beschaffen (evtl. nach Aufbrechen einer Verschlüsselung), und aktiven Intrudern, die von ihnen gefertigte Nachrichten ins Netz einschleusen.

## EPIC, electronic privacy information center

EPIC ist eine gemeinnützige Forschungseinrichtung, die 1994 gegründet wurde und ihren Sitz in Washington D.C. hat. Der Fokus der Aktivitäten richtet sich auf die Erhaltung der bürgerlichen Freiheiten, dem Schutz der Privatsphäre und konstitutioneller Werten.

Unter diese Zielsetzung fallen auch Internet-Aktivitäten und damit die Computersicherheit, die Einschränkung durch *Hacker*, der Schutz von Minderjährigen gegen jugendgefährdende, gewaltverherrlichende, sexistische, pornografische, terroristische oder militante Inhalte, das Abhören von Gesprächen und Datenleitungen und die Sicherstellung der Informationsfreiheit. <http://www.epic.org>

## Fluten *flooding*

Bei *DoS-Attacken* werden für die Angriffe auf die Netzdienste verschiedene Flooding-Techniken benutzt. Man unterscheidet dabei zwischen dem PING-Flooding und dem SYN-Flooding. Beim Ping-Flooding, auch als Ping of Death (POD) bezeichnet, werden lange Requests an eine IP-Adresse generiert, die die gesamte Systemperformance benötigen. Beim SYN-Flooding werden fortlaufend Requests für die Synchronisation an einen TCP-Port gesendet. Auch hierbei wird das System überlastet und kann abstürzen.

## Hacker

Unter Hacker versteht man Personen, die sich über öffentliche Netze oder IP-Netze unberechtigten Zugang zu anderen Systemen verschaffen und versuchen auf den Datenbestand in fremden Systemen zuzugreifen.

Der unberechtigte Zugang erfolgt in der Regel unter Umgehung der Sicherheitssysteme. Das *Eindringen* kann bei der Datenübertragung, auf den Leitungen, den Übertragungskomponenten oder Protokollen stattfinden.

Als Gegenmaßnahmen gegen Hacker empfehlen sich u.a. das regelmäßige Auswechseln von Passwörtern, die Beseitigung von *Schwachstellen* im System, das Abschalten von nicht genutzten Systemdiensten, das Callback als Kommunikationsroutine, die Überwachung von Service-Eingängen und der Einsatz von *IDS-Systemen*.

## **Heuristik** *heuristics*

Heuristik ist die Lehre von Methoden zum Auffinden neuer Erkenntnisse. Heuristische Verfahren werden beispielsweise beim Aufspüren neuer *Viren* angewendet und zwar vorwiegend in dem Zeitraum, in dem noch kein neues Update für die Virens Scanner entwickelt wurde. Um zu verhindern, dass in dem Zeitraum in dem die Hersteller die Updates für neue Viren entwickeln, der Schaden durch ein neues Virus möglichst gering gehalten wird, werden die Schädlinge mittels heuristischer Verfahren abgefangen. Hierbei suchen die Virens Scanner nach verdächtigen Codes, die beispielsweise die Festplatte formatiert oder unerwartete Online-Verbindungen aufbaut. Das Erkennen solcher Phänomene wird vom Virens Scanner angezeigt.

## **HIDS, host-based intrusion detection system**

Das HIDS-Verfahren (Host-Based *Intrusion* Detection System) ist ein Intrusion Detection System (*IDS*), das Angriffe auf einen Host erkennt und unterbindet. Dieses Verfahren setzt auf typische Angriffsmuster von lokalen *Angriffen* und Konfigurationsänderungen der IT-Systeme. Dabei wird jeder Host von einem Sensor überwacht, der den Datenverkehr an den Host auf Angriffe hin untersucht und Datei- oder Konfigurationsänderungen erkennt. Darüber hinaus sollte ein HIDS-System auch Anwendungs-Logdateien, Systemdateien sowie Logdaten auf Anwendungs- und Kernebene einschließen um mögliches *Spoofing* oder Bypass-Operationen zu verhindern. Bei Erkennen eines bestimmten Musters löst das System darauf hin eine Aktion, beispielsweise einen Alarm aus.

Vorteile des HIDS sind, dass sie Angriffe auf Betriebssystemebene, im lokalen Umfeld des Hosts, erkennen und dass sie direkt feststellen können, ob ein Angriff erfolgreich war.

## **Hoax**

Hoaxes sind elektronische Falschmeldungen, die bewusst durch Dritte über E-Mails verbreitet werden. Die Hoaxes enthalten Text, der in die Irre führen soll wie eine Zeitungsentee oder ein Aprilscherz, richten aber keinen direkten Schaden an. Um eine weite Verbreitung zu finden, werden sie als Kettenbrief gehandhabt. Eine Hoax kann alle Themenbereiche tangieren, von Unternehmens- und Börsennachrichten über den Umweltschutz, das Wetter bis hin zu Warnhinweisen. Sie verbreiten sich extrem schnell und werden von Virens Scannern nicht erkannt.

## **Honeypot**

Die exakte Übersetzung des Wortes Honeypot ist Honigtopf. In der *IT-Sicherheit* handelt es sich um einen im Netzwerk installierten Dienst, der für den *Angreifer* ein interessantes Ziel darstellen soll und Angriffe auf das Netzwerk protokolliert. Honeypots sind im Netzwerk installiert, werden aber von den berechtigten Netzwerkbenutzern nicht angesprochen, weil sie ihnen unbekannt sind und die darauf installierten Dienste nicht dem eigentlichen Geschäftszweck dienen. Sie stellen lediglich für Angreifer ein vermeintlich

interessantes Ziel dar.

Wird der Honeypot angesprochen, werden alle Vorgänge von diesem protokolliert und je nach Interessenlage kann ein Alarm ausgelöst werden. Aus dem protokollierten Dokument können Rückschlüsse über die Vorgehensweise der Angreifer und über eventuelle neue Angriffstechniken gezogen werden. Mit diesen Erkenntnissen können dann solche oder ähnliche *Angriffen* abgewehrt werden.

Honeypots sind flexible *Security*-Einrichtungen mit verschiedenen Sicherheitsanwendungen. Sie sind nicht auf ein spezielles Problem fixiert, sondern können vielfach für die Informationssammlung, das Entdecken von Angriffen und die Prävention eingesetzt werden.

Man unterscheidet bei den Honeypots zwischen den Produktions-Honeypots, die einfach zu benutzen sind und einen begrenzten Informationsumfang erfassen können, und den Forschungs-Honeypots, die komplex sind hinreichend Informationen erfassen und analysieren können. Während die erstgenannten in Firmen eingesetzt werden, findet man die anderen in Forschungs-, Verwaltungs- und Militäreinrichtungen.

**IDMEP, intrusion detection message exchange protocol**  
*IDMEP-Protokoll*

*Intrusion* Detection Message Exchange Protocol (IDMEP) ist ein Sicherheitsprotokoll, das von der IETF entwickelt wird und vor Eindringlingen in IP-Netze warnen soll. Das IDMEP-Protokoll kann wesentlich zur Verbesserung des Netzwerkverhaltens im Falle eines Angriffs beitragen. Es erkennt Angriffe, die von einer Domain auf eine andere ausgeführt werden. Wenn eine Quelldomain einen *Angriff* erkennt, kann sie das Ziel-Netzwerk für diesen Angriff identifizieren. Sie sendet einen Alarm, aus dem die Art des Angriffs hervorgeht und der automatisch über das gesamte Netzwerk gesendet wird. Darüber hinaus wird eine Referenz wie die URL übersandt oder eine Systemdatei, die weitere Informationen für den Netzwerk-Administrator enthält.

Das IDMEP-Protokoll kann auf dem SNMP-Protokoll Version 3 basieren.

**IDS, intrusion detection system**  
*IDS-System*

*Intrusion* Detection System (IDS) sind autarke Systeme, die *Eindringlinge* erkennen und Attacken auf IT-Systeme und Netze vermeiden. Diese IDS-Überwachungssysteme sollten nicht bekannt sein, keine Dienste anbieten, Angriffe protokollieren, Eindringlinge erkennen und nach Möglichkeit Gegenmaßnahmen einleiten. Alles was im Netzwerk anormal ist, sollte von dem IDS-System erkannt und protokolliert werden. Dazu benutzen IDS-Verfahren Sensoren, die anormalen Datenverkehr aufspüren und mit vorgegebenen Mustern vergleichen. Dabei unterscheidet man zwischen dem Misuse Detection und dem Anomaly Detection. Das Misuse Detection basiert auf dem Vergleich von Mustern oder Signaturen. Beim Anomaly Detection wird hingegen jedes Verhaltensmuster, das sich außerhalb des normalen Datenverkehrs bewegt, als *Angriff* gewertet.

**Incident-Response**  
*incident response*

Da keine absolute *Sicherheit* gegen Datendiebstahl, Infektionen mit *Viren* und Würmern oder gegen unberechtigten Zugriff gegeben ist, müssen Unternehmen, wenn sie solche Vorfälle feststellen, entsprechende Werkzeuge bereitstellen, damit die Verantwortlichen angemessen auf solche Vorgänge reagieren können. Diese Thematik ist im Incident-Response verankert, der Reaktion auf Sicherheits-Vorfälle.

Ein Incident ist ein Vorfall; das kann ein *Eindringen* in ein Sicherheitssystem sein, der unberechtigte Zugriff,

der Datendiebstahl, das Ausspähen von Passwörtern oder der Ausfall eines Rechners oder Speichers. Mit dem Incident-Response wird auf diesen Vorfall reagiert. Es ist eine spezielle, auf die Unternehmensbedürfnisse zugeschnittene Vorgehensweise mit der möglichst viele Informationen über sicherheitsrelevante Vorfälle gesammelt und ausgewertet werden. Ziel dieser Maßnahmen ist es einen Datenverlust so gering als möglich zu halten.

Die diversen Incident-Response-Tools unterscheiden sich funktional und lassen sich in forensische Werkzeuge und Live-Tools gliedern, wobei sich die erstgenannten auf Spurensuche begeben und letztere unmittelbar auf Ereignisse reagieren.

## Informationssicherheit *information security*

Schwachstellen	Gefahrenpotential
<b>Physische Schwachstellen</b>	<b>Einbruch in Gebäude und Computerräume</b>
<b>Natürliche Schwachstellen</b>	<b>Natürliche Ereignisse, Blitzeinschlag, Erdbeben, Staubeinwirkung</b>
<b>Mediale Schwachstellen</b>	<b>Beschädigte oder entwendete Datenspeicher, CDs, DVDs oder Bänder</b>
<b>Hard-/Software-Schwachstellen</b>	<b>Softwarefehler und unsachgemäße Benutzung der Hardware</b>
<b>Kommunikationsleitungen</b>	<b>Abhören der Übertragungsmedien</b>
<b>Emissionen</b>	<b>Kompromittierende Emissionen von Bildschirmen und Schaltungen</b>
<b>Personenbezogene Schwachstellen</b>	<b>Unsachgemäße Behandlung und Manipulation der Geräte</b>

Informationssicherheit ist der Präventivschutz für Persönlichkeits- und Unternehmens- Informationen und ist auf kritische Geschäftsprozesse fokussiert. Ein solcher Schutz bezieht sich gleichermaßen auf Personen, Unternehmen, Systeme und Prozesse und wird durch Integrität, Verfügbarkeit, Vertraulichkeit, Verbindlichkeit, Nachweisbarkeit und Authentizität erzielt. Die Informationssicherheit soll den Verlust, die Manipulation, den unberechtigten Zugriff und die

*Schwachstellen in der Informationssicherheit*

Verfälschung von Daten verhindern.

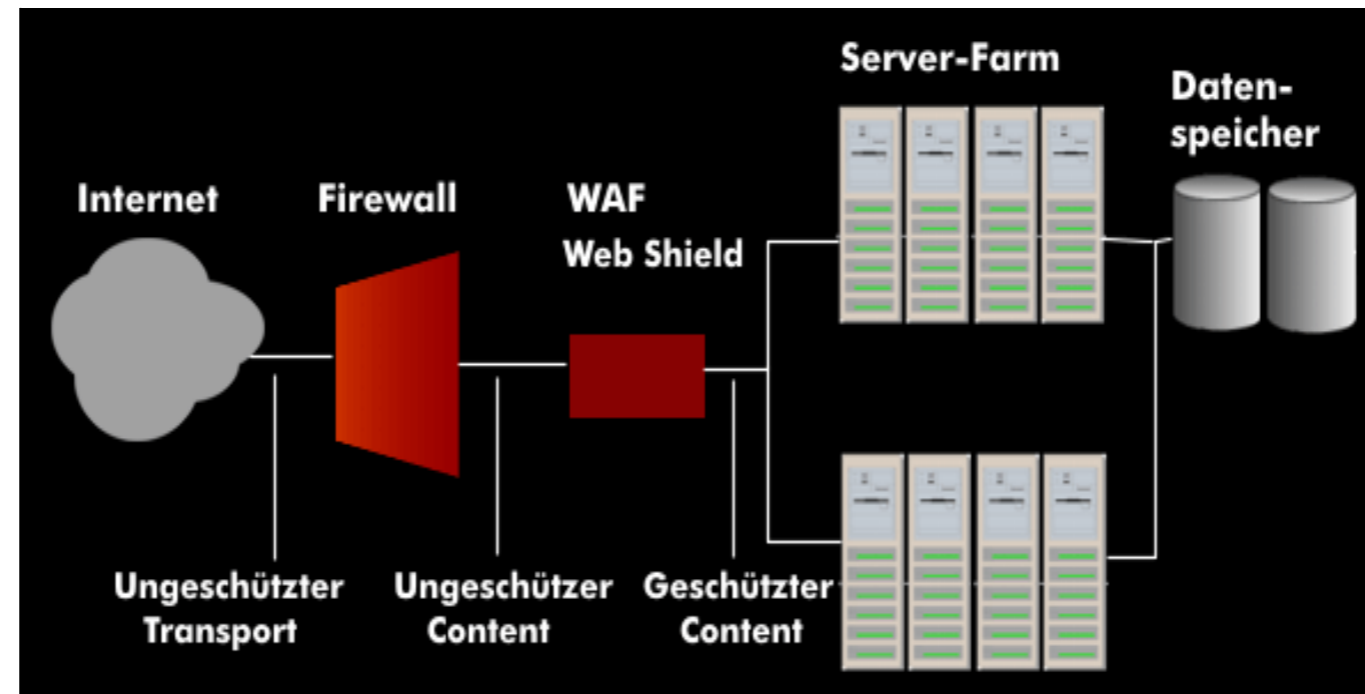
Die Basis für die Informationssicherheit kann durch konzeptionelle, organisatorische und operative Maßnahmen erreicht werden. Dazu gehört die Umsetzung von sicherheitsrelevanten Grundsätzen eines Unternehmens, die so genannte Informationssicherheitspolitik. In dieser sind die Ziele des Unternehmens und die Realisierung festgelegt.

Ein wichtiger Ansatz für die *Sicherheit* von Informationssystemen ist der British Standard BS 7799 sowie der ISO-Standard 17799 als Implementierungsleitfaden. Diese beiden Sicherheitsstandards werden in der Security-Norm ISO 27001 berücksichtigt.

## Internet-Sicherheit *Internet security*

Als weltweit größter Netzverbund bietet das Internet *Angreifern* hinreichende Möglichkeiten, sich unberechtigten Zugriff auf Datenbestände und Ressourcen zu verschaffen, Datenbestände und übertragene Daten zu manipulieren und zu sabotieren. Die technischen Möglichkeiten für das unberechtigte *Eindringen* in fremde Datenbestände reichen vom Abhören von Passwörtern, über das *IP-Spoofing*, bei

Übertragungsstrecke mit  
Web-Shield



dem sich der *Eindringling* einer gefälschten IP-Adresse bedient, über das IP-Hijacking, bei dem der Angreifer eine bestehende IP-Verbindung übernimmt, den *Replay-Angriff*, bei dem der Angreifer gezielt vorher gesammelte Informationen einsetzt, um dadurch fehlerhafte Transaktionen auszuführen, über das

*SYN-Flooding*, einem gezielten Angriff auf den Server, um diesen durch Überlast von seinen eigentlichen Aufgaben abzulenken, bis hin zum *Man-in-the-Middle-Angriff*, einer Attacke, bei der die Kommunikation zwischen zwei Partnern abgefangen und manipuliert wird.

Wirkungsvolle Maßnahmen gegen diese *Bedrohungen* bieten so genannte Web-Shields, die als Application Layer Gateway (ALG), auch bekannt als Web Application Firewall (WAF), agieren. Im Gegensatz zu klassischen Firewalls und *IDS-Systemen* untersuchen die genannten Systeme die Kommunikation auf der Anwendungsebene.

## IP-Spoofing IP spoofing

*Adressen-Spoofing* oder IP-Spoofing nennt man im Internet das Vortäuschen einer falschen IP-Adresse zum Zwecke der Vorteilsnahme. Beim *Angriff* über das IP-Spoofing verwendet der Angreifende die Netzwerkadresse eines autorisierten Benutzers und erhält dadurch den Zugriff auf bestimmte Ressourcen eines Netzwerks oder eines Systems.

Gelingt es dem *Angreifer* beim Spoofing die Routing-Tabellen dahin gehend zu manipulieren, dass die gespoofte Adresse bedient wird, wird er wie ein autorisierter Benutzer behandelt.

Gegenmaßnahmen gegen das IP-Spoofing zielen primär auf die Konfiguration der Zugriffskontrolle ab. So lässt beispielsweise ein IP-Source-Guard nur die IP-Adressen zu, die mittels *DHCP-Snooping* an einem bestimmten Port eingehen. Andere Methoden konzentrieren sich auf bessere Authentifizierungen wie beim Einmalpasswort (OTP).

## IPS, intrusion prevention system IPS-System

Im Gegensatz zu einem *Intrusion Detection System (IDS)* hat das Intrusion Prevention System (IPS) keine überwachende und alarmauslösende Funktion, sondern kontrolliert unmittelbar den Traffic. Das IPS-System ist direkt in die Datenleitungen geschaltet und überwacht die ein- und ausgehenden Datenpakete der Netzwerk-Komponenten. Angriffe und vom normalen Datenverkehr abweichende Bitmuster werden über

Signaturen erkannt und blockieren den Datenverkehr. Unterstützt wird diese Sperrfunktion durch intelligente Verhaltensmuster und anomale Algorithmen, die auf der Applikationsebene arbeiten.

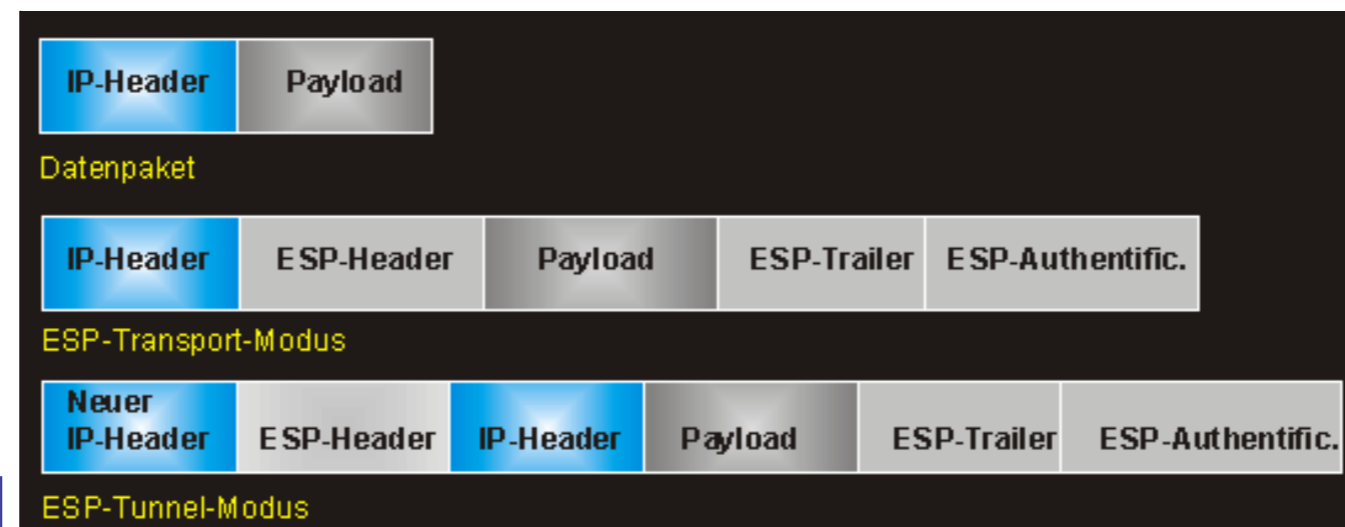
IPS-Systeme sollten die Datenanalyse in Hochgeschwindigkeit ausführen können und dürfen selbst unter Hochlast nicht den legitimen Datenverkehr blockieren. Die Schutzmechanismen wie Signaturanalysen, das Erkennen von Protokollabweichungen, Firewall-Funktionen und Zugriffskontrollen müssen robust sein.

## IPSec, IP security protocol IPSec-Protokoll

IP *Security* Protocol (IPSec) ist ein Standardisierungsvorschlag der IETF, in dem Verfahren und Protokolle für einen herstellerübergreifenden sicheren und geschützten Datenaustausch mittels des IP-Protokolls festgelegt werden. Die Normungsaktivitäten laufen seit 1995. Der Normenrahmen von IPSec definiert die Vorgehensweise für die Datenintegrität, die Vertraulichkeit der Inhalte sowie die Verwaltung der kryptografischen Schlüssel. Die Bestandteile von IPSec sind der Authentication Header (AH), die Encapsulating-Security-Payload (ESP), die *Security Association* (SA), der Security-Parameter-Index (SPI) und der Internet Key Exchange (IKE).

Zu Beginn der Kommunikation wird zwischen den an der Kommunikation beteiligten Rechnern das benutzte Verfahren geklärt und ob die Datenübertragung in einem Tunnel erfolgen soll oder nicht. Daher unterscheidet das IPSec-Framework je nach Art der Verschlüsselung zwischen dem Authentication Header-basierten Transportmodus und dem ESP-basierten Tunnelmodus. Im ersten Fall, dem verschlüsselten AH-Header, bleibt der ursprüngliche IP-Header erhalten, die Quell- und Zieladressen bleiben ungeschützt. Der AH-Header liegt zwischen den IP-Headern und den Headern der Transportprotokolle. Die Authentisierung erfolgt entweder mittels des MD5-Algorithmus oder mit SHA, wobei die Authentisierung nur die Datenfelder des AH-Headers umfasst, die während der Übertragung unverändert bleibt. Dazu gehört der Nachrichteninhalte des AH-Headers, wodurch Veränderungen bemerkt werden können.

Im Gegensatz dazu bietet der Tunnelmodus, basierend auf der verschlüsselten ESP-Payload, eine höhere Sicherheit für das übertragene Datenpaket, da ja der gesamte Rahmen verschlüsselt wird. Das Datenpaket bekommt einen neuen Header in dem die Quell- und Zieladresse versteckt sind und nur die Tunnelendpunkte erkennbar.



Das Protokoll wurde speziell für die Verbindung zwischen zwei LANs entwickelt. Dabei schützt IPSec die Datenpakete des IP-Protokolls vor möglichen Modifikationen und vor Ausspähungen. IPSec beeinflusst weder die Kommunikationsprotokolle

*IPSec im Transport- und Tunnelmodus*

noch die Anwendungs-programme, sodass das Internetworking über Router nicht beeinträchtigt wird. Authentisierungsverfahren, die mittels IPSec erstellt wurden, können zwischen den Daten von zugelassenen und nicht zugelassenen Kommunikationspartnern unterscheiden. Die Autorisierungsverfahren basieren auf den MD5-Hash-Algorithmen mit 128 Bits, die Verschlüsselung auf dem DES-Algorithmus mit 56 Bits in Cipher Block Chaining (CBC). Mit IPSec kann jeglicher IP-Datenverkehr geschützt werden: TCP, UDP, ICMP, HTTP, FTP, SNMP, Telnet, usw. IPSec ist in den RFCs 1825 bis 1829 und 2401 beschrieben und standardisiert.

## ISSA, information systems security association

Die Non-Profit-Organisation ISSA (*Information Systems Security Association*) ist weltweit vertreten und kümmert sich um das Thema *IT-Sicherheit*. Die ISSA hat mehr als 6.000 Mitglieder und setzt bei der Information über die Sicherheitsbelange, über *Schwachstellen* in der IT-Infrastruktur an. Sie informiert und schult und hat ein eigenes Diskussionsplattform. Darüber hinaus hat sie *Sicherheitsrichtlinien* für Unternehmen, KMUs und Heimarbeitsplätze entwickelt.  
<http://www.issa.org>

## IT-Sicherheit *IT security*

Die *IT-Sicherheit* tangiert alle technischen Maßnahmen zur Verringerung des Gefährdungspotenzials für IT-Anwendungen und -Systeme. Alle mit dem Gefährdungspotenzial in Zusammenhang stehenden Schutzmaßnahmen, wie die Entwicklung von Sicherheitskonzepten, die Vergabe von Zugriffsberechtigungen und die Implementierung von Sicherheitsstandards, sind Aspekte der IT-Sicherheit. IT-Sicherheit ist die technische Umsetzung der Sicherheitskonzepte unter wirtschaftlichen Aspekten.



Die IT-Sicherheit umfasst alle gefährdeten und daher schützenswerten Einrichtungen, Systeme und Personen. Dazu gehören u.a. Gebäude, Netze, Hardware und Software sowie die an den Systemen Arbeitenden. Ziel der IT-Sicherheit ist es, die Verfügbarkeit von Systemen und Daten sicherzustellen, die Vertraulichkeit zu gewährleisten, damit weder Unbefugte auf Dateien zugreifen können und die Dateien auch bei der Übertragung weiterhin vertraulich bleiben, die Sicherstellung der Authentizität und der Integrität der Daten. Für die physikalische IT-Sicherheit gibt es mehrere nationale und europäische Standards, so die Definition der Brandabschnitte nach DIN 4102 oder die in den EN-1047-Standards spezifizierten

*Sicherheitskonzept*

Belastungsgrenzen für Daten und Systeme. Darüber hinaus gibt es Richtlinien und Güteklassen für den Einbruchschutz mit der Beschreibung des Mauerwerks.

## ITW, in the wild ITW-Virus

Die Bekämpfung von *Viren* setzt voraus, dass deren Struktur bekannt ist. Aus diesem Grund werden alle bekannten und jemals vorgekommenen Viren, die als ITW-Viren (In The Wild) bezeichnet werden, in Datenbanken von der Organisation Wildlist erfasst und dem Anwender unter <http://www.wildlist.org> zur Verfügung gestellt. Insgesamt gibt es über 80.000 bekannte ITW-Viren, von denen allerdings nur etwa ein Prozent jemals verbreitet war.

## L2Sec, layer 2 security L2Sec-Protokoll

Eigenschaften	Tunneling-Protokolle		
	PPTP	L2TP	IPsec
Authentifizierung des Nutzers	Ja	Ja	Nein
Unterstützung von NAT	Ja	Ja	Nein
Multiprotokollfähigkeit	Ja	Ja	Nein
Dynamische Zuweisung von Tunnel-IP-Adressen	Ja	Ja	N/A
Verschlüsselung	begrenzt	Nein	Ja
Public Key Infrastructure	Nein	Nein	Ja
Überprüfung der Authentizität von Paketen	Nein	Nein	Ja
Unterstützung von Multicast	Ja	Ja	Nein

Das Layer 2 *Security*-Protokoll (L2Sec) soll bestimmte *Schwachstellen* eliminieren, die IPsec bei Remote-Access-Lösungen aufweist. L2Sec hat einen größeren Overhead als IPsec und bietet keine Einzelsicherung von Prozessen oder Ports. Bei L2Sec werden alle Datenpakete in einen Tunnel gepackt und dieser wird dann als Ganzes gesichert. L2Sec basiert auf anerkannten Sicherheitsstandards und Zertifikaten und kann für Browser, E-Mails, Datenbank-Anwendungen oder Terminal-Emulationen genutzt werden. Layer-2-Security ist von Microsoft bereits funktionell im RFC 2716 beschrieben.

## Tunneling-Techniken im Vergleich

## Makrovirus macro virus

zu normalen *Viren* in einer Makrosprache erstellt. Da Makros wiederkehrende Tastatureingaben und Programmabläufe automatisieren helfen, können Computerviren über Makroprogramme erstellt und reproduziert werden.

Makroviren sind in Dokumenten eingelagert und werden bei Aufruf und Weitergabe der Dateien verteilt. Durch diese einfache Verbreitung können Makroviren enorme Schäden verursachen, beispielsweise durch Veränderung der Zahlen in einer Tabellenkalkulation.

Makroviren werden im Gegensatz

## Malware

Unter den Oberbegriff Malware fallen alle unerwünschten Software-Aktivitäten, die die *IT-Sicherheit* oder die Funktionsfähigkeit von Computern und Systemen beeinträchtigt. Dazu zählen im Einzelnen *Viren*, *Trojaner* und *Würmer*, *Flooding* und *DoS-Attacken*, *Spyware*, *Spams*, *Hoaxes* usw. Bei Malware handelt es sich immer um Aktivitäten, die vom Benutzer nicht erwünscht sind.

Die technischen Verfahren mit denen die Malware-Aggressoren ihre Opfer ausspähen sind auf einem hohen technischen Niveau. Gängige Antiviren- und Anti-Malware-Programme sind auf nicht in der Lage die Angriffe zu erkennen oder aufzuspüren. Wenn die Malware-Angriffe ihre Aufgaben erfüllt und Konstruktionspläne, Kontennummern oder andere Informationen ausgespäht haben, verwischen die Programme ihre eigenen Spuren. Häufig kann der entstandene Schaden und das *Eindringen* erst dann rekonstruiert werden, wenn der Privatmann oder das Unternehmen bereits geschädigt wurde.

## Man-in-the-Middle-Angriff *man-in-the-middle attack*

Man-in-the-Middle ist ein *Angriff* auf den Kommunikationskanal zwischen zwei Partnern. Der *Angreifer* versucht dabei den Kommunikationskanal unter seine Kontrolle zu bringen, und zwar in der Art und Weise, dass die Kommunikationspartner nicht feststellen können ob sie miteinander oder mit dem Angreifer kommunizieren.

Abhilfe schaffen hier nur eindeutige Identifikation der Teilnehmer, ohne dem Angreifer die Identifikation preiszugeben.

## Netzwerksicherheit *network security*

Die Netzwerksicherheit ist eine Symbiose aus Richtlinien und Vorschriften, aus Produkten und Diensten. Sie tangiert alle Unternehmensebenen, vom Benutzer über den Administrator bis hin zur Unternehmensführung. Es ist ein Maßnahmenkatalog in Form einer *Security Policy*, die dafür sorgen muss, dass die Zugriffsberechtigung, Autorisierung, Identifikation und Authentifizierung verwaltet werden, dass jede Attacke, jeder unerlaubte Zugriff, jede Art der *Sabotage*, der Manipulation, des Missbrauchs und der Beeinflussung der Datenbestände und Ressourcen verhindert oder unmittelbar erkannt wird und dass das Einschleusen von *Viren*, *Würmern* oder *Trojanern*, *DoS-Attacken* oder *IP-Spoofing* nicht möglich ist. Ausgehend von einem solchen Maßnahmenkatalog können technische Lösungen implementiert werden. An netzwerkumfassenden Konzepten gibt es Network Access Control (NAC) von Cisco und anderen Unternehmen, Network Access Protection (NAP) von Microsoft und Trusted Network Connect (TNC) von der Trusting Computing Group.

## NIDS, network-based intrusion detection system

Network-based *Intrusion* Detection System (NIDS) ist eine *IDS*-Technologie zur Erkennung von Eindringlingen in eine Kollisionsdomäne eines Netzwerks. Bei diesem Intrusion Detection System (IDS) werden alle Datenpakete der Kollisionsdomäne an einem zentralen Punkt oder direkt auf der Leitung abgegriffen und auf bekannte oder vermutete Angriffsmuster hin untersucht. NIDS-Systeme können die Datenpakete in Echtzeit analysieren, untersuchen jede aktive Verbindung und können auf diese Weise extrem schnell reagieren und auch *DoS-Attacken* erkennen, nur keine verschlüsselten Daten.

Tritt ein bestimmtes Verhaltensmuster oder eine Unregelmäßigkeit in den Datenpaketen auf, das einen *Angriff* darstellen könnte, wird ein Aktion ausgelöst. Das kann ein Alarm sein, eine E-Mail oder Gegenmaßnahmen.

# WEB-GEFAHREN -SICHERHEIT

## Penetrationstest *PT, penetration testing*

Ein Penetrationstest (PT) dient dem Auffinden von Sicherheitslücken in IT-Systemen. Er eignet sich im Besonderen für das Auffinden von *Schwachstellen*, die die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen gefährden. Der Penetrationstest untersucht alle Schwachstellen an denen die Informationsverarbeitung und die Kommunikation gefährdet sein könnten.

Penetrationstests können sich auf interne und externe Tests beziehen und werden in der Regel nach herstellerspezifischen Erfahrungswerten durchgeführt, da das Testverfahren selbst nicht standardisiert ist. Bei den Schwachstellentests unterscheidet man zwischen dem Penetrationstest, der automatisiert ist, und dem Vulnerability-Scan, bei dem die Ergebnisse manuell ausgewertet werden. Der Vulnerability-Scan überprüft ebenfalls die Verletzlichkeit der IT-Systeme mit einem Vulnerability-Scanner. Neben der Scan-Technik werden bei Penetrationstests spezielle Hacking-Tools eingesetzt, um unberechtigte Zugriffe zu simulieren. Dazu gehören ebenso manuell ausgeführte Attacken, um in die Netzwerk-Infrastruktur einzudringen.

## Perimeter-Sicherheit *perimeter security*

Perimeter-Sicherheit betrifft die Sicherheit am Übergang zwischen dem Unternehmensnetz und dem Internet. Für die Perimeter-Sicherheit sind bestimmte Richtlinien definiert, die die IT-Technik des Unternehmens gegen das Gefahrenpotential schützen, das durch *Viren*, *Würmer* und *Hacker* verursacht wird. Zu den in den Richtlinien genannten Möglichkeiten gehören Firewalls, Virens Scanner und Anti-Viren-Software sowie Web-Filtertechniken.

## Phishing



Beispiel, in der die Postbank auf gefälschte Home-Pages zum Zwecke des Phishings hinweist

Mit der Wortschöpfung Phishing, das sich aus Passwort und Fishing zusammensetzt, ist ebenso wie das Pharming eine Technik, bei der der *Angreifer* versucht, die persönliche Identifikations-Nummer (PIN) und die Transaktionsnummer (TAN) von Bankkunden über das Internet abzufragen und damit Finanztransaktionen durchzuführen. Die Angreifer, die Phisher, fragen über gefälschte Bank-Homepages die vertraulichen Daten ab. Zu diesem Zweck wird eine nachgemachte Homepage eines Geldinstituts ins Internet gestellt. Nach dem Zufallsprinzip werden E-

Mails mit einem Link auf die gefälschte Homepage versandt. In diesen E-Mails werden Sicherheitsaspekte oder bankrelevante Themen behandelt mit dem Hinweis auf die angebliche Homepage. Die in die nachgebildeten Homepages eingetragenen persönliche Identifikationsnummern und Transaktionsnummern

werden ausgefiltert und stehen den Angreifern unmittelbar für unberechtigte Finanztransaktionen auf der richtigen Homepage zur Verfügung.

## **Phreaking**

Das Phreaking ist eine ältere Methode zur Umgehung von Telefonkosten, die ursächlich mit den Vermittlungstechniken in Telefonnetzen und dort im Besonderen mit der Signalisierung zusammenhängt. Die Kreativität der Phreaker, das sind diejenigen, die das Phreaking beherrschen, hat sich nicht nur auf das Nachbilden von Signalisierungssequenzen beschränkt. Phreaker analysieren und modifizieren die *Schwachstellen* der verschiedenen Einwahltechniken und Bezahlformen, einschließlich der Telefonkarten oder Callingcards, und setzen die Erkenntnisse konsequent zum eigenen kostenlosen Telefonieren ein. Was die Signalisierung betrifft, so arbeiten Fernmeldenetze in den USA, in Kanada, Australien und China mit der älteren C5-Signalisierung, die als Innenband-Signalisierung mit Zweit- und Mehrtonverfahren im Sprachkanal arbeitet, also keinen unabhängigen Signalisierungskanal benutzt, wie beispielsweise das Signalisierungssystem Nr. 7 (CCS7). Die Steuersignale und -sequenzen der C5-Signalisierung können somit direkt aus dem Sprachkanal ausgefiltert und für eigene Zwecke missbraucht werden. Da die Betreibergesellschaften die Steuersequenzen wegen des Phreaking ändern, arbeiten die Phreaker mit Frequenzscannern, die die Frequenzen automatisch scannen, die Sequenzen aufzeichnen und das Ganze noch in einen Softwaredialer einbringen. Über das Monitoring der Carrier können Phreaker mittels Fangschaltung erfasst werden.

Das Phreaking, das besonders bei internationalen Verbindungen interessant ist, ist ein globales Problem. National ist das Phreaking, bedingt durch die verwendete Außenband-Signalisierung schwierig.

## **PnP-Sicherheit** *plug and play security*

Plug-and-Play (PnP) ist ein Schnittstellenkonzept für das konfliktfreie Anschließen von Peripheriegeräten an einen Personal Computer. Das schnelle Erkennen der angeschlossenen Peripheriegeräte bietet aber nicht nur Vorteile, sondern auch diverse *Risiken*, da durch unberechtigten Zugriff wichtige Daten aus den Personal Computern (PC) kopiert, ebenso aber auch Daten, *Viren* und *Trojaner* über die Plug-and-Play-Schnittstelle in das Firmennetz eingespeist werden können. In diesem Zusammenhang darf die Entwicklung der Mobilspeicher wie dem USB-Stick nicht außer Acht gelassen werden. Dieses Risiko wird durch drahtlose Schnittstellen wie Wireless-USB noch erhöht, da der Anwender häufig nicht erkennen kann, wer mit seinem Computer gerade kommuniziert. Die Betriebssysteme bieten keine Möglichkeit der Schnittstellenkontrolle.

Sicherheitsaspekte von Schnittstellen ist daher ein Thema der Netzwerk- und *IT-Sicherheit*. Bei der Absicherung der Schnittstellen kommt es auf die konsequente Umsetzung der Sicherheitsregeln an. Diese Umsetzung kann durch Sicherheitsmodule vorgenommen werden, die die Nutzung der PnP-Geräte überwachen. Die Echtzeitüberwachung von Schnittstellen und Peripheriegeräten ist ein Punkt bei der Lösung der Schnittstellen-Sicherheitsproblematik, die automatische Geräteerkennung und schnelle Freigabe ein weiterer. Die PnP-Geräte, die eine Zugangsberechtigung haben, werden zentral oder direkt am Arbeitsplatz über Fernzugriff registriert. Die Einstellungen können entweder direkt im Active Directory von Windows oder im NetWare Directory Service (NDS) zentral verwaltet werden.

## PPTP, point to point tunneling protocol

Das Point to Point Tunneling Protocol (PPTP) ist ein Tunneling-Protokoll für VPNs. Das Protokoll ist kein offizieller Standard sondern geht auf eine Initiative von Ascend, Microsoft, 3COM und US Robotics zurück und ist eine Erweiterung des PPP-Protokolls.

Im Gegensatz zu anderen Tunneling-Protokollen wie L2F und L2TP hat PPTP keine umfassende Verschlüsselung und unterstützt keine tokenbasierte Methode der Authentifizierung. Zur Datensicherung der Datenübertragung verfügt PPTP über einen 40- oder 128-bit großen RC4-Algorithmus sowie über die mögliche Nutzung von RADIUS-Passwort-Logons (PAP oder CHAP).

PPTP kann das IP-Protokoll, das IPX-Protokoll, DECnet, AppleTalk, NetBIOS und NetBEUI verarbeiten.

Hierzu wird das Multi-Protokoll-PPP in einem Tunnel gekapselt. Zu diesem Zweck wird die modifizierte Version von GRE V2 (Version 2 von Generic Routing Encapsulation) zugrunde gelegt. Das PPTP-Protokoll



dient zur Absicherung von Wählverbindungen, aber auch von LAN-LAN-Verbindungen. Dabei kann über eine vorhandene IP-

*PPTP verkapselt die verschlüsselten PPP-Pakete in das GRE-Protokoll*

Verbindung ein PPTP-Tunnel aufgebaut werden. PPTP kann keine Multipoint-Verbindungen herstellen, sondern ausschließlich Punkt-zu-Punkt-Verbindungen, allerdings in beliebigen Stellen im Virtual Private Network (VPN).

### Risiko *risk*

Unter Risiko versteht man die Wahrscheinlichkeit für den Eintritt eines Schadensfalles. Ein solches Schadensereignis kann in der IT-Technik durch bestimmte *Schwachstellen* in den Systemen, Komponenten, Kommunikationsnetzen oder Software auftreten, die zufällig oder vorsätzlich ausgenutzt werden. Das bedeutet, dass die *Sicherheit* der Systeme unmittelbar von dem Risiko abhängig ist: Je höher das Risiko, desto geringer ist die vorhandene Sicherheit und umgekehrt. Das Risiko beginnt da, wo die Sicherheit aufhört. Je höher die Sicherheit veranschlagt wird, desto geringer ist das Risiko.

Werden die risikobehafteten Schwachstellen durch methodische Verfahren ermittelt, spricht man von Risikoanalyse. Bei einer solchen Analyse werden technische und menschliche Schwachstellen erforscht, damit die Häufigkeit und die Länge der Schadensfälle eingeschränkt und reduziert werden kann. Die Ergebnisse der Risikoanalyse fließen in das Risikomanagement ein.

Risiken lassen sich klassifizieren nach den Objekten, den Aktivitäten, den Urhebern und der Ursache, nach der Häufigkeit und der Schadenshöhe.

### Sabotage *sabotage*

Sabotage ist ein vorsätzlicher Eingriff in ein System oder Programm um dessen Funktion zu beeinträchtigen und den wirtschaftlichen Ablauf zu stören. Sie kann sich auch auf die Beschädigung von Einrichtungen oder Systemen beziehen.

Im Gegensatz zur Manipulation setzt die Sabotage kriminelle Energie voraus.

## SATAN, security administrator tool for analyzing networks

SATAN (*Security Administrator Tool for Analyzing Networks*) ist ein Programm, das Sicherheitslücken in Netzen feststellt, diese registriert und Lösungsvorschläge unterbreitet.

Satan gehört zu den Security-Scannern, die die Sicherheitslücken in den Konfigurationen von Personal

Computern aufspüren und die *Schwachstellen* in vernetzten System feststellen und diese einem Test unterziehen. Mit dem Programm, das zentral eingesetzt wird und über gute Reporting-Funktionen verfügt, kann der Administrator des Schwachstellen in der *IT-Sicherheit* feststellen und beheben. Das Programm kann als Vorläufer der *IDS-Systeme* angesehen werden.

**Schwachstelle**  
*VM, vulnerability management*

Das Vulnerability Management (VM) befasst sich mit den sicherheitsrelevanten Schwachstellen in IT-Systemen. Mit dem VM-Management sollen Prozesse und Techniken erarbeitet werden, mit denen zur Steigerung der *IT-Sicherheit* eine Sicherheitskonfiguration in Unternehmen eingeführt und verwaltet werden kann. Das Vulnerability Management umfasst die Schwachstellenanalyse unter Berücksichtigung der in den Standards BS 7799 resp. ISO 17799 detailliert beschriebenen Faktoren Mensch, Maschine, Umgebung und Daten.

Darüber hinaus spielt beim VM-Management das Common Vulnerability Scoring System (CVSS), mit dem ein Rating- Index erstellt wird, eine wesentliche Rolle.

**Security-Appliance**  
*security appliance*

Um den gestiegenen Sicherheitsanforderungen hinsichtlich der Abwehr von *Viren, Spams* oder *Würmer* gerecht zu werden, oder um die IP-Telefonie zu sichern, nutzt man speziell ausgerüstete *Security-Appliances*.

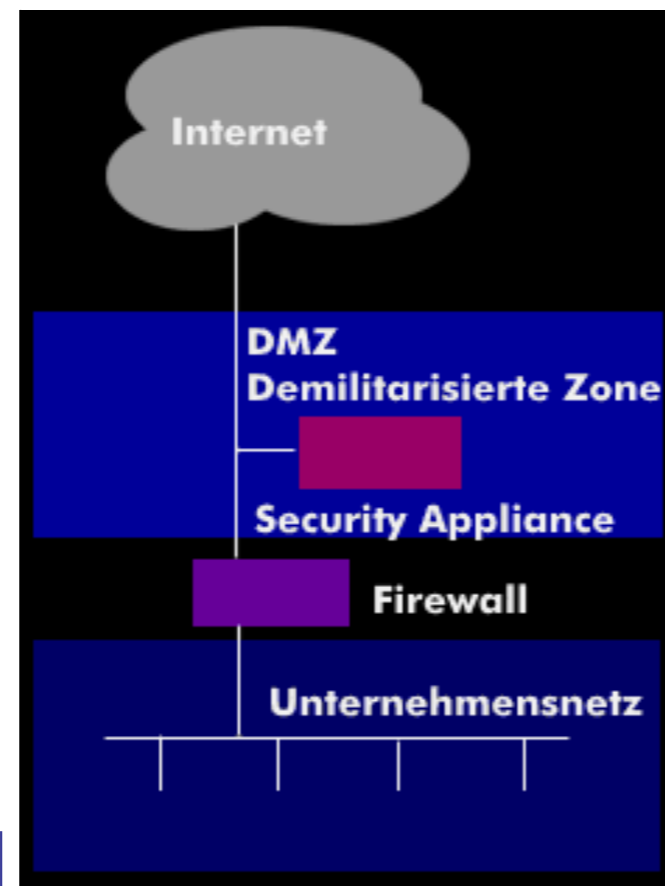
Es handelt sich dabei um einen Appliance, der, ausgestattet mit der entsprechenden Software, bestimmte Gefahren abwehren kann. Ist der Security-Appliance so ausgestattet, dass er nur für eine spezielle Gefahr

konzipiert ist und eine Aufgabe innerhalb eines Gesamtsystems ausübt, spricht man von einem *Specialized Security Appliance (SSA)*. Dagegen erledigt der *Unified Thread Management Appliance (UTMA)* alle Sicherheitslösungen, die durch verschiedenste Gefahren hervorgerufen werden können. *Security-Appliances* können die Funktionen von Firewalls und VPN-Gateways, von Virensclannern URL- und Content-Filtern, *IDS-* und *IPS-Systemen* übernehmen. Sie sind mit Hochleistungsprozessoren ausgestattet, haben Arbeitsspeicher von mehreren hundert Megabyte oder auch einigen Gigabyte, Festplatten, IDE-Controller, Ethernet- und USB-Schnittstellen.

Unter *Sicherheit* sind alle technischen und organisatorischen Maßnahmen zu verstehen die Daten schützen. Dieser Schutz wird bei den Bedienenden realisiert, in Systemen und Computern, bei der Übertragung sowie in Diensten und Anwendungen. Unter Berücksichtigung des möglichen Gefährdungspotentials werden Sicherheitsmechanismen implementiert, die das *Eindringen* in Systeme, das Abhören der Übertragungswege, die Manipulation, die *Sabotage* und das Löschen von Datensätzen verhindern soll.

*Security Appliance in demilitarisierter Zone (DMZ)*

**Sicherheit**  
*security*



Zu den personenbezogenen Schutzmechanismen gehören die Autorisierung und Authentifizierung durch Passwörter oder persönlicher Identifikationsnummer (PIN), biometrische Daten oder Signaturen. Die systembezogenen Sicherheitskriterien gehören zur *IT-Sicherheit* und umfassen technische und organisatorische Maßnahmen. Dazu gehören die Installation eigener Sicherheitsarchitekturen mit Firewalls, das Sicherheitsmanagement und die Schlüsselverwaltung.

Kennzeichnend für die übertragungstechnische Sicherheit, die *Netzwerksicherheit* und die *Internet-Sicherheit*, sind die Verschlüsselungsverfahren und die Datenübertragung mit Sicherheitsprotokollen. Anwendungsorientierte Schutzmaßnahmen haben branchenspezifische Eigenschaften, wie beispielsweise bei geschäftlichen Transaktionen, bei denen digitale Signaturen und Transaktionsnummern die Sicherheit verbessern.

Unter Sicherheit fallen alle Kriterien, die die Integrität, Verfügbarkeit, Vertraulichkeit, Verbindlichkeit, Betriebssicherheit und Authentizität betreffen.

## Sicherheitsdienst *security service*

Sicherheitsdienste sollen Angriffe abwehren. Es handelt sich dabei um Technologie-unabhängige Sicherheitsmaßnahmen, die durch ihre Leistungsmerkmale genau definiert sind und in die Schichtenstruktur der Sicherheitsarchitektur eingebunden werden. Die fünf primären Sicherheitsdienste Vertraulichkeit, Integrität, Authentifizierung, Zugriffskontrolle und Unwiderrufbarkeit werden durch Sicherheitsmechanismen

Sicherheitsdienste	Vertraulichkeit	Datenintegrität	Authentifizierung	Zugriffskontrolle	Unwiderrufbarkeit
<b>Verschlüsselung</b>	x	x			
<b>Digitale Signatur</b>			x		
<b>Zugriffskontrolle</b>				x	
<b>Integritätssicherung</b>		x			x
<b>Datenstromerweiterung</b>	x				
<b>Authentifizierung</b>			x	x	
<b>Leitweglenkungskontrolle</b>	x	x			
<b>Notarisierung</b>			x		x

realisiert. Neben den genannten Sicherheitsdiensten gibt es weitere, die detaillierter sind, wie die Unversehrtheit der Nachricht oder der Kommunikationsnachweis. Jeder Sicherheitsdienst basiert auf einem oder mehreren Sicherheitsmechanismen.

Ein Sicherheitsdienst ist die Vertraulichkeit, mit der sichergestellt wird, dass nur Befugte auf entsprechende Informationen zugreifen können. Sie schützt vor passiven *Angriffen* und damit vor dem unbefugten Mitlesen von übertragenen Nachrichten und gespeicherten Informationen. Bei den aktiven Angriffen steht die Veränderung der Information und die damit einhergehende Reaktion des Empfängers im Vordergrund. Die Vertraulichkeit basiert auf den Sicherheitsmechanismen Verschlüsselung und Integrität.

Der Sicherheitsdienst Datenintegrität überprüft die Datenunversehrtheit und zeigt an ob Datenströme verändert, manipuliert, modifiziert, gelöscht oder vertauscht wurden.

Ein weiterer Sicherheitsdienst ist die Zugriffs-

*Sicherheitsdienste und deren -mechanismen*

kontrolle, die durch entsprechende Mechanismen die Möglichkeiten des unberechtigten Zugriffs auf Programme und Daten weitestgehend eingeschränkt. Mit der Vertraulichkeit wird sichergestellt, dass Informationen nur für Befugte zugänglich sind. Die Authentifikation des Kommunikationspartners und des Ursprungs der Nachrichten, der Empfänger- und Urhebernachweis, sind weitere sicherheitsrelevante Dienste.

## **Sicherheitspolitik** *security policies*

In der Sicherheitspolitik werden die Regeln und Verfahrensweisen festgelegt, nach denen die Datenübermittlung, -verarbeitung und -speicherung erfolgen. Sie berücksichtigt personelle, technische, organisatorische und rechtliche Einflussfaktoren.

Bei den personellen Einflussfaktoren geht es um das Bedienpersonal, der Zuverlässigkeit, Sensibilität und Vertrauenswürdigkeit. Es geht um die Antworten auf Fragen wie "Wer darf auf welche Daten zugreifen?" oder "Wer ist für die Sicherheitspolitik verantwortlich?"

Die technischen Einflussfaktoren sind geprägt durch die vorhandenen Computer, die Art und Sensibilität der Daten und der Software, aber auch durch räumliche Gegebenheiten, die Art der eingesetzten Übertragungsmedien und -techniken, sowie die Anzahl der Prozesse usw. Bei der Technik stellen sich Fragen hinsichtlich der Daten, der Art der Vermittlung oder der Verkehrsbeziehungen. So beispielsweise: "Welche Verkehrsbeziehungen sind erlaubt?" oder "Auf welcher Schicht werden die *Sicherheitsdienste* installiert?"

Bei den organisatorischen Einflussfaktoren handelt es sich um solche, die sich mit den Arbeitsabläufen der Benutzer beschäftigen. Bei diesen Einflussfaktoren geht es um die vielen sicherheitsrelevanten Aspekte, wie "An wen werden Alarme gemeldet?" oder "Welche Maßnahmen sind zu treffen, damit die Sicherheitspolitik eingehalten wird?"

Darüber hinaus muss sich die Sicherheitspolitik auch nach den Gesetzen und rechtlichen Vereinbarungen richten. Zu nennen sind das Bundesdatenschutzgesetz (BDSG), Signaturgesetz (SigG), Teledienstschutzgesetz (TDDSG) und andere. Letztlich geht es auch um die Rechtsverbindlichkeit der Informationen, um deren Urhebernachweis oder Kommunikationsnachweis.

## **Sicherheitsrichtlinie** *security directive*

Sicherheitsrichtlinien sind unternehmensspezifische Regeln in denen die Ziele für alle sicherheitsrelevanten Arbeitsgebiete festgelegt sind.

In Unternehmen definieren die Sicherheitsrichtlinien die Regeln, die die Mitarbeiter, die an der Ausarbeitung der Richtlinien beteiligt sein sollten, in ihrem Arbeitsgebiet beachten müssen. Zu den wichtigsten Interessengruppen in einem Unternehmen gehören die Sicherheits- und Netzwerkadministration, Arbeitnehmervertreter, Vertreter der Nutzergruppen und der Geschäftsführung. Die ausgearbeiteten Sicherheitsrichtlinien sollten von den Nutzern umgesetzt und akzeptiert werden, sie sollten die *Sicherheit* des Netzwerks und der Systeme gewährleisten und die Rechte und Pflichten der Nutzer, der Administration und der Geschäftsführung klar regeln. Bestandteile der Sicherheitsrichtlinien umfassen die Beschaffung der Software, Computer- und Netzwerktechnik und die darin realisierten Sicherheitsstandards, die Zugriffsberechtigungen und alle Maßnahmen die dem Datenverlust und der Abwehr von *Angriffen* dienen, die Betriebs- und Wartungsrichtlinien und das Reporting, um nur einige zu nennen.

In die Sicherheitsrichtlinien fließen die nationalen und internationalen Sicherheitsstandards für die Bewertung und Zertifizierung von IT-Systemen ein. Dazu gehören die europäischen Information Technology Security Evaluation Criteria (ITSEC), die amerikanischen Trusted Computer Security (TCSEC) und die Common Criteria for Information Technology Security Evaluation (CC). Außerdem befasst sich Kapitel 1 des britischen Standards BS 7799 für das Sicherheitsmanagement mit den Sicherheitsrichtlinien für das Management und für die Betreuung der *IT-Sicherheit*.

## **Sicherheitsvereinbarung** *SA, security association*

*Security associations (SA)* are entered into by two entities communicating via *IPSec* before communication starts. SAs are negotiated for the Authentication Header (AH) and Encapsulated Security Payload (ESP). They are valid for unidirectional communication, that is for one transmission direction only. As communication is bidirectional, at least two SAs are required for the transmission. Security Associations are the underlying individual basis of any *IPSec* connection. They precisely define how the host or the security gateway can connect to the target component and how the target responds. A SA is always unique and is characterized by three major elements: the Security Parameter Index (SPI) the target IP address and the Security Protocol Identifier.

## **SIM, security information management**

*Security Information Management (SIM)* sind Systeme in denen Events und Logfiles von vielen Stellen in Kommunikationssystemen gesammelt werden, um sie in Echtzeit zu verknüpfen, archivieren, verarbeiten, analysieren und um daraus aktuelle und historische Berichte zu erstellen.

Es gilt, das Netz live zu überwachen und auf kritische Ereignisse hin zu untersuchen. Der Ansatz für die Bewertung der Ereignisse kann aus verschiedenen Sichtweisen erfolgen, so beispielsweise aus Benutzersicht, bei der sich die Fragen nach dem wo, wann und wie sich Jemand eingeloggt, auf welche Systeme er zugegriffen hat und welche Ereignisse dadurch ausgelöst wurden.

Da die Daten der SIM-Systeme aus verschiedenen Quellen stammen, von Netzwerkkomponenten, Systemen, Firewalls, Anwendungen oder Virensclannern, ist deren Inhalt auf die eigene Funktion ausgerichtet. Sie bewerten daher die auftretenden Ereignisse aus vollkommen unterschiedlichen Betrachtungswinkeln. Darüber hinaus haben sie die verschiedensten Formate, die eine SIM-Plattform verarbeiten muss.

## **Sniffer** *Schnüffler*

Sniffer sind Softwareapplikationen, mit denen vertrauliche Daten im Internet abgefangen werden können. Diese Applikationen können in unberechtigter Weise eingesetzt werden, sie werden aber auch vom Administratoren für die Fehlersuche und Datenverkehrsadministration benutzt werden.

Ein Sniffer, der sich auf das Ausspähen von Datenpaketen spezialisiert hat, nennt man Packet Sniffer. Ein solcher Packet Sniffer späht alle Datenpakete aus, die über eine bestimmte Kollisionsdomäne gesendet werden. Es handelt sich um eine Software, die sich der Netzwerkkarte bedient und Datenpakete von Anwendungsprotokollen ausspäht, die unverschlüsselt übertragen werden, wie das Telnet-Protokoll, das FTP-Protokoll, das SMTP-Protokoll und einige mehr.

Sniffer können durch verschiedene Maßnahmen abgewehrt werden, so durch eine konsequente Authentifizierung unter Verwendung eines kombinierten, einmalig und zufällig vergebenden Passwortes

(OTP), das sich aus zwei Faktoren zusammensetzt: der PIN und einem zufällig vergebenden Kennwort. Weitere Methoden um Sniffer abzuwehren bestehen in einer hierarchisch aufgebauten Switching-Architektur und in Verschlüsselung des Übertragungskanal, beispielsweise mittels *IPSec*.

## **Snooping**

Unter Snooping versteht man das Abhören einer Verbindung auf einem Broadcast-Medium, einem Chat oder der IP-Telefonie. Der Mithörende, beispielsweise ein *Hacker*, kann dadurch in den Besitz von vertraulichen Daten wie Passwörter kommen.

Neben dem genannten Snooping gibt es noch das Bus-Snooping bei dem jeder Teilnehmer auf dem Hostbus Adressen anderer Teilnehmer mitlesen kann.

## **Spam** *spam mail*

Spams, Spam-Mails, oder auch Junk-Mails, sind unverlangt zugesendete E-Mails und SMS. Das können auch Newsartikel sein, die an viele Newsgroups verteilt werden. Im normalen Sprachgebrauch sind damit unerwünschte Nachrichten gemeint, an denen man kein Interesse hat. Eine Spam-Mail ist vergleichbar einer nicht angeforderten postalischen Wurfsendung. Die unerwünschten elektronischen Massenaussendungen werden auch als Unsolicited Bulk E-Mail (UBE) bezeichnet, die kommerziellen E-Mails als Unsolicited Commercial E-Mail (UCE).

Für die Aussendung von Spams gibt es spezielle Programme für das Internet. So können Spam-Mails über Chats ebenso verbreitet werden wie über ICQ.

Die Kreativität der Spam-Autoren kennt kaum Grenzen. So sind Spam-Mails zu komplexen und spezialisierten Anwendungen mutiert. Sie sind mit Flash-Animationen, versteckten Inhalten oder *Spyware* bestückt.

Zur Verhinderung von Spams gibt es diverse Spam-Filter gegen unerwünschte Massen-E-Mails, E-Mail-Filter zur inhaltlichen Filterung von E-Mails nach Text- und Anhängen sowie Web-Filter zur Blockierung von unerwünschten E-Mail-Adressen.

Die Organisationen MAPS und CAUCE haben sich speziell mit der Verhinderung von Spam-Mails auseinander gesetzt und bieten verschiedene Listen mit den Server-Adressen, von denen regelmäßig Spams versandt werden.

## **Spim, instant message spam**

Instant Messages *Spams* werden als Spims bezeichnet. Die Spammer haben sich damit einen weiteren Anwendungsbereich für ihre unerwünschten Werbebotschaften oder nicht angeforderten Mitteilungen erschlossen. Neben den Spams und Spam-Telefonaten, den Spits, gibt es auch die Instant Message Spams (Spim).

Wenn Unternehmen ein einheitliches Instant Messaging (IM) auf Server und Clients einsetzen, kann die Gefahr der Spims ausgeschlossen werden, da die Hersteller sichere Konfigurationsmechanismen vorsehen.

Die Spimmer besorgen sich ihre Informationen aus Benutzer-Verzeichnissen, die von vielen Instant-Messaging-Programmen angelegt werden. Es daher wichtig, dass keine rein privaten Angaben in diesen Verzeichnissen abgelegt werden und dass man auch darauf achtet, dass keine Benutzernamen für Instant Messaging auf Websites publiziert werden.

## **Spoofing**

In der Internet-Terminologie hat das Spoofing eine eigene Bedeutung, und zwar die Angabe einer falschen Adresse. Durch die falsche Internet-Adresse täuscht jemand vor, ein autorisierter Benutzer zu sein. Maßnahmen gegen das Spoofing, die den Missbrauch von IP-Adressen verhindert, nennt man Anti-Spoofing.

Es gibt das *IP-Spoofing*, DNS-Spoofing, WWW-Spoofing und ARP-Spoofing, die mit simulierter IP-Adresse anhand der Host-Adresse oder des Domain-Namen oder mit der Zuordnung zwischen IP- und Hardware-Adresse fungieren.

## **Spyware**

Der Begriff Spyware ist eine Wortschöpfung aus Spy (Spionieren) und Ware. Es handelt sich dabei um eine Software, die das Online-Verhalten von Webnutzern, das sich im Surfen ausdrückt, ausspioniert und dieses Wissen an andere weitergibt. Aus den Ergebnissen, die in der Regel in Tabellen gespeichert und über E-Mails an den Urheber gesendet werden, können Rückschlüsse auf das Werbeverhalten gezogen und die Werbewirksamkeit durch gezielten Einsatz von abgestimmten Methoden gesteigert werden. Spyware wird als unerwünschte Software auf Workstations installiert, sie verhält sich penetrant und ist potenziell gefährlich. Der Zweck ist die Bereicherung des Urhebers. Sie wird durch *Trojaner* und mit E-Mails auf den Anwender-PC heruntergeladen.

Spyware kann dann zu einer ernsthaften Gefahr werden, wenn vertrauliche Informationen des angemeldeten Nutzers weitergegeben werden. Dazu gehören u.a. die Abfolge der Tastatureingaben, der Benutzername, der Hashwert des Administrator-Passwortes, E-Mail-Adressen, Kontaktdaten sowie Anmelde- und Nutzungsinformationen zu Instant-Messaging.

## **Tempest, transient electromagnetic pulse emanation standard**

Tempest sind Sicherheitslücken, die durch elektromagnetische Strahlung verursacht werden. Es handelt sich dabei um kompromittierende Strahlung von Geräten, Kabeln und vor allem Bildschirmen, die abgehört werden können und somit ein potentiell *Risiko* für den Benutzer darstellen.

Generell entstehen bei jedem Stromfluss elektromagnetische Felder, die von Kabeln oder Geräten abgestrahlt werden. Bei Kathodenstrahlröhren (CRT) ist diese Abstrahlung besonders hoch, da die Beschleunigungsspannungen für den Elektronenstrahl im zweistelligen Kilovolt-Bereich liegen und Kathodenstrahlröhren nur über ein geringes Abschirmpotential verfügen. Diese Strahlung kann man mit entsprechenden Empfangseinrichtungen wie Spektrumanalysatoren aus einiger Entfernung erfassen und auswerten. Man sieht dann zeitgleich die Informationen auf dem Bildschirm, die der Benutzer sieht. Diese Abhörtechnik nennt sich Tempest und gilt in gleicher Weise für Kabel, Geräte, Netzwerke und Systeme. Tempest wird in der Literatur als "zeitweilige Abstrahlung und flüchtige Übertragung" bezeichnet, als "Temporary Emanation and Spurious Transmission", aber auch als "transienter elektromagnetischer Puls", als "Transient electromagnetic Pulse Emanation Standard".

Gegen Tempest gibt es diverse Schutztechniken, die die kompromittierende Emission (KEM) von Kabeln, Systemen, Geräten und Displays einschränkt. Dazu gehören in erster Linie Abschirmungen, wobei das Material und die Blechdicke eine wesentliche Rolle spielen. Dadurch erhält das Gerät oder System eine entsprechende HF-Dichtigkeit. Die Dichtigkeit setzt dabei lückenlose geschlossene und verschraubte oder überlappende Slotbleche voraus. Auch die Außenseiten, die Front, Seiten und Rückwand müssen

lückenlos und überlappend geschlossen sein. Kabel müssen abgeschirmt und die Schirmung einwandfrei geerdet sein. Zur Verhinderung des Tempests gibt es EMV-Klebebänder, EMV-Dichtungen, -Dämmmatten und Ferritkerne für die stromführenden Leitungen.

## Trojaner *trojan*

Unter einem Trojaner, auch als trojanischen Pferd bezeichnet, versteht man ein Programm, das neben seiner eigentlichen Funktion noch weitere, unbekannt Funktionen aufweist. Bei seiner Ausführung richtet ein trojanisches Pferd Schaden »von innen« an. Dabei werden Datenbestände und Passwörter ausspioniert und über das Internet versendet, ebenso aber auch Systemkonfigurationen verändert oder gelöscht. Trojaner missbrauchen Computer und rüsten in diesen zusätzliche Funktionen nach, mit denen sie Zugangsdaten, Passwörter und Seriennummern erfassen oder die Remote-Eigenschaften und die Systemadministration beeinträchtigen, so beispielsweise als *Spyware*, zur Aussendung von *Spams* oder für Angriffe auf Server.

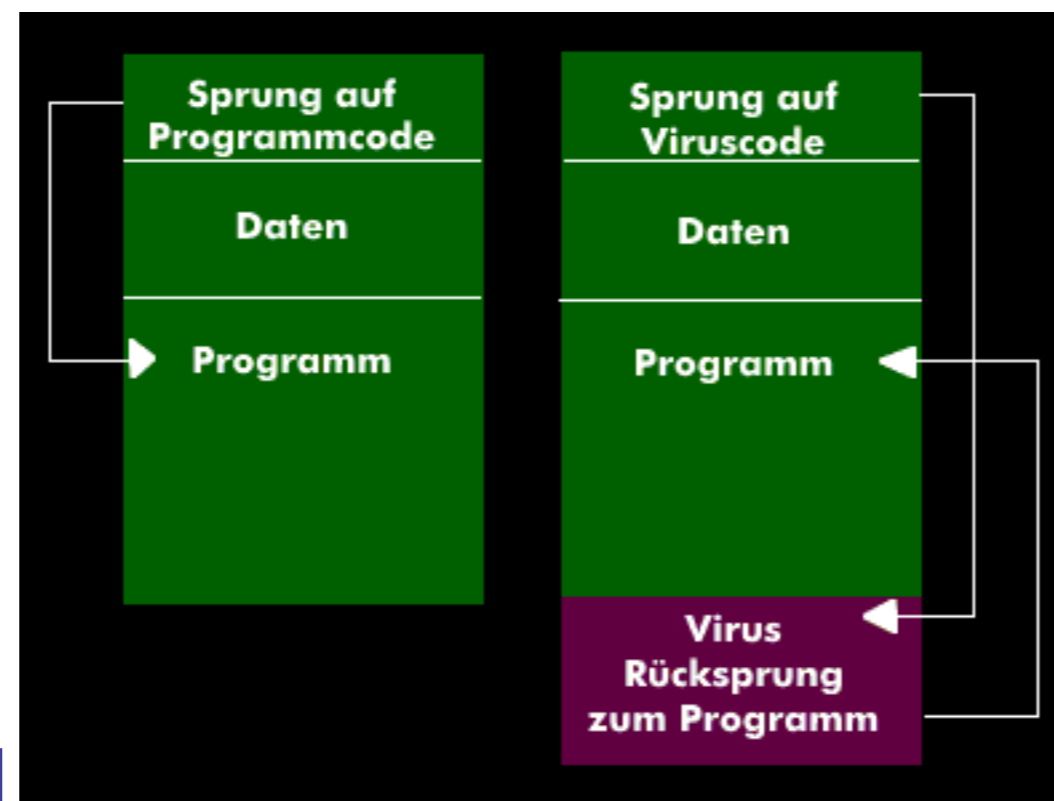
Trojaner verbreiten sich über Anhänge von E-Mails, aber auch über Tauschbörsen.

Trojaner kann man dadurch verhindern, indem man keine Software aus unbekannt Quellen auf seinen Computer lädt oder diese vorher durch einen Virens Scanner checkt.

## Virus *virus*

Innerhalb weniger Jahre hat sich das Virus-Problem von einer theoretischen zu einer realen *Bedrohung* für Computer und Datennetze entwickelt. Alle Arten von Geräten, Mainframes, Workstations und Netzwerken sind bisher erfolgreich angegriffen und geschädigt worden. Hauptausbreitungsursachen sind Disks und Datennetze.

Bei den Viren unterscheidet man zwischen Computerviren, Dateiviren, Systemviren und Bootsektor-Viren.



Ein typischer Computervirus ist ein einfaches Programm, das sich selbst reproduziert, sich in normalen Programmen versteckt und dessen Zweck es ist, durch Infizierung andere Soft- und Hardware zu behindern oder zu zerstören. Wenn infizierte Programme ablaufen, stecken sie auch andere Programme und andere Computer an, mit denen sie in Kontakt kommen. Wenn ein Computervirus einmal ein Programm befallen hat, dann kann er Programme zerstören, Daten vernichten, Zahlenwerte in einer Tabellenkalkulation verändern, Festplatten neu formatieren und damit ihren gesamten Datenbestand vollständig vernichten oder jeden nur möglichen Schaden anrichten, den der

Programmablauf ohne und mit  
Virenprogramm

Programmierer des Virus eingeplant hat. In fast allen Fällen bleibt der Virus unbemerkt, während er sein Zerstörungswerk vollbringt. Auch die Virenerkennung mittels Virenscannern gestaltet sich zunehmend schwieriger, da neuere Viren Tarnfunktionen besitzen und sich vor Virenscannern verbergen können. Viren werden über das Internet verbreitet, und zwar über die Dateianhänge von E-Mails und Software-Downloads. Sie werden in Datenbanken von Wildlist als *ITW-Viren* erfasst und stehen Anwendern unter <http://www.wildlist.org> zur Verfügung.

## WAS, web application security Web-Applikationssicherheit

Web *Application Security* (WAS) schützt Web-Anwendungen und Webservices vor *Angriffen*, die über das HTTP-Protokoll erfolgen. Ziel dieser Angriffe ist es, in den Rechner einzudringen oder die Web-Aktivitäten zu blockieren. Ein Beispiel für diese Attacken ist das Cross Site Scripting (XSS).

Die Web-Applikationssicherheit umfasst diverse netzwerktechnische, technologische und anwendungsspezifische Aspekte, die weit über die Programmierung und Konfiguration hinausgehen. Aus diesem Grund hat sich für die Umsetzung der Web-Applikationssicherheit ein Modell aus sechs Ebenen bewährt, in dem alle Aspekte berücksichtigt werden. Erst wenn alle Ebenen dieses Modells betrachtet wurden, gilt eine Web-Anwendung als hinreichend sicher.

	Ebene	Inhalt
6	Vorschriften und Bestimmungen	Einhealtung gesetzlicher Regelungen und unternehmensspezifischer Vorgaben
5	Semantik	Schutz vor Täuschung und Betrug
4	Logik	Absicherung von Prozessen und Workflows als Ganzes
3	Implementierung	Vermeiden von Programmierfehlern, die zu Schwachstellen führen
2	Technologie	Richtige Wahl und sicherer Einsatz von Technologie
1	System	Absicherung der auf der Systemplattform eingesetzten Software
0	Netzwerk & Host	Absicherung von Host und Netzwerk

Da die Sicherheitsmechanismen der Firewalls auf der Netzwerk- und Transportschicht stattfinden, können bei Einhaltung der Zugangskriterien die Angriffe auch auf der Anwendungsschicht erfolgen. Dies soll die Web Application Security verhindern. Das WAS-Konzept setzt daher auf der Anwendungsschicht Application Layer Gateways (ALG) oder Web Application Firewalls (WAF), auch Web Shields genannt, ein. Die Web Shields untersuchen potenzielle

Hackeraktivitäten auf Sicherheitslöcher in der Server-Software. Sie sind an bestimmten Mustern im Footprint zu erkennen oder sie profitieren von einer fehlerhaften Programmierung. Werden solche Attacken entdeckt, sperrt der Web Application Firewall (WAF) den Zugriff und verhindert damit, dass die *Sicherheit* der Website unterlaufen wird.

Im Gegensatz zu den Web Shields sind die ebenfalls in die Web-Sicherheit eingebundenen XML-Firewalls auf Webservices spezialisiert.

Das Sechs-Ebenen-Modell für die Web Application Security (WAS)

## WSS, web service security

Web Service Security (WSS) spielt bei der Absicherung von SOA-Umgebungen eine wesentliche Rolle. Es handelt sich um ein nachrichtenorientiertes Sicherheitsprotokoll, das eine Nachricht vom Sender bis zum Empfänger schützt. Der nachrichtenorientierte Ansatz hat gegenüber einem übertragungstechnischen den Vorteil, dass in verteilten SOA-Strukturen die Nachrichten über Vermittlerstellen hinweg geschützt werden. Sie werden nicht nur von einem Webservice benutzt, sondern von mehreren Diensten und Clients, die in verschiedenen Programmiersprachen entwickelt werden und auf unterschiedlichen Plattformen arbeiten. Die Sicherheit der Webservices zielt auf datenrelevante Sicherheitsaspekte: mit der Integrität wird sichergestellt, dass die Nachrichten während der Übertragung nicht verändert wurden; die Vertraulichkeit schützt die Daten mittels Verschlüsselung und die Authentifizierung der Nachrichten. Bei der Integrität setzt WSS auf XML Digital Signature (XMLDSig), die vom World Wide Web Consortium (W3C) standardisiert wurde. Für die Verschlüsselung der Daten, zur Wahrung der Vertraulichkeit setzt WSS auf XML Encryption, ebenfalls von W3C. Und was die Authentifizierung anbetrifft, so werden die Nachrichten empfängerseitig mit referenzierten Sicherheits-Token geprüft.

## Wurm *worm*

Ein Wurm ist ein infizierter Programmcode, der sich normalerweise über die vorhandene Infrastruktur, über Netzwerkverbindungen oder den Anhang von E-Mails ausbreitet und auf anderen Systemen Schaden anrichtet. Würmer können auch das Adressbuch des Benutzers für die Verbreitung benutzen. Würmer sind schädliche, autonome Programmroutinen, die sich, sobald sie codiert und freigesetzt werden, automatisch vervielfältigen um möglichst viele Rechner zu befallen. Sie dringen über Sicherheitslücken in die Systeme ein und richten dort Schaden an, indem sie unerwünschte Aktionen auslösen. Das können Nachrichten sein, die plötzlich auf dem Bildschirm erscheinen; sie können aber auch Dateien löschen, Festplatten formatieren oder den Prozessor mit sinnlosen Aufgaben eindecken.

## XSS, cross site scripting

Cross Site Scripting (XSS) sind Angriffe auf Webservices über das HTTP-Protokoll. Bei diesen *Angriffen* wird ein XSS-Loch bei der Eingabe von Benutzerdaten genutzt. Ein solches XSS-Loch entsteht, wenn eine Applikation Daten, die von Nutzern stammen, an einen Browser sendet, ohne vorher die Inhalte zu überprüfen oder diese zu verschlüsseln. Mit den XSS-Angriffen können *Hacker* beeinträchtigende Skripte im Browser des Angegriffenen ausführen und darüber Angriffe mittels *Phishing* oder *Malware* zu initiieren. Jede in Browsern unterstützte Skriptsprache ist anfällig auf diese Attacken. Schutz gegen das Cross Site Scripting kann erreicht werden, wenn alle eingehenden Daten anhand einer Überprüfungsliste, einer so genannten Whitelist, überprüft werden.