Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von WLAN (ISi-WLAN)

BSI-Leitlinie zur Internet-Sicherheit (ISi-L)

Version 1.0

Vervielfältigung und Verbreitung

Dies ist ein Werk der ISi-Reihe. Ein vollständiges Verzeichnis der erschienenen Bände finden Sie auf den Internet-Seiten des BSI.

http://www.bsi.bund.de oder http://www.isi-reihe.de

Bundesamt für Sicherheit in der Informationstechnik
ISi-Projektgruppe
Postfach 20 03 63
53133 Bonn
Tel. +49 (0) 228 99 9582-0
E-Mail: isi@bsi.bund.de
Internet: http://www.bsi.bund.de

Inhaltsverzeichnis

1 Leitlinie zur sicheren Nutzung von WLAN

Der Einsatz von lokalen Funknetzen (engl. Wireless Local Area Network, WLAN) ist inzwischen weit verbreitet und gewinnt zunehmend an Bedeutung. WLAN lässt sich kostengünstig und einfach ohne das Verlegen von Kabeln installieren, ermöglicht eine Arbeitsplatz-ungebundene Nutzung des Firmennetzes oder des Internets und eignet sich hervorragend für Messen, Besprechungen und Konferenzen. Ferner ist über die Nutzung von öffentlichen Funknetzen (sog. Hotspots) ein Internet-Zugang auch unterwegs möglich. Allerdings ergeben sich bei der Nutzung von WLAN auch zahlreiche Gefährdungen, insbesondere für die Vertraulichkeit von Daten und die Verfügbarkeit der Funknetze.

Die Basis für diese Leitlinie bildet die „Technische Richtlinie Sicheres WLAN“ [TR-S-WLAN] des BSI. Dabei handelt es sich um eine dreigeteilte Studie. Teil 1: „Darstellung und Bewertung der Sicherheitsmechanismen“ gibt eine Einführung in die grundlegenden bei WLAN verwendeten Techniken und Protokolle. Des Weiteren beschreibt sie bestehende Sicherheitsmechanismen und bewertet diese. In Teil 2: „Vorgaben eines WLAN Sicherheitskonzeptes“ werden für verschiedene Einsatzszenarien die Gefährdungen durch den Einsatz von WLAN aufgezeigt und entsprechende Maßnahmen beschrieben. Diese Maßnahmen werden anschließend anhand konkreter Beispiele verdeutlicht. Schließlich enthält Teil 3 sowohl „Auswahl-“ als auch „Prüfkriterien für WLAN-Systeme“. Weitere Veröffentlichungen des BSI zu diesem Thema sind die Studie „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ [DRAHT-KOM], die kostenfrei im Internet verfügbar ist, und der WLAN-Baustein der IT-Grundschutzkataloge [ITGSK]. Die vorliegende Leitlinie fasst die wesentlichen Aspekte der genannten Dokumente zusammen.

1.1 Management Summary

Drahtlose Netze (WLAN) sind inzwischen weit verbreitet und werden meist dort eingesetzt, wo kabelgebundene Netze (LAN) zu teuer, zu umständlich oder zu unkomfortabel sind. In der Regel werden drahtlose Netze zur Erweiterung einer bestehenden Netzinfrastruktur verwendet.

Beim Einsatz von WLAN besteht ein wesentliches Problem darin, dass die Kommunikation auch noch aus großer Distanz mitgehört werden kann. Dadurch wird die Vertraulichkeit der übermittelten Daten z. B. bei E-Mails bedroht, sofern die Kommunikation nicht verschlüsselt wird. Nach wie vor sind zahlreiche WLANs nicht oder nur unzureichend verschlüsselt.

Eine weitere Gefährdung für WLAN-Installationen ist deren Anfälligkeit für Störungen der Funkverbindungen. Störungen können durch andere Geräte oder Umwelteinflüsse bedingt oder auch mutwillig provoziert sein und im schlimmsten Fall zum Verlust der Verfügbarkeit führen.

Aufgrund der Vielzahl an Gefährdungen werden in der Richtlinie zu WLAN Maßnahmen beschrieben, um diesen Gefährdungen zu begegnen. Welche Maßnahmen geeignet sind, hängt dabei von dem jeweiligen Einsatzszenario ab. Für ein WLAN, das zur Erweiterung des eigenen LAN verwendet wird, sind insbesondere folgende Empfehlungen von Bedeutung:

- Die gesamte Kommunikation über WLAN sollte angemessen verschlüsselt werden, d. h. nach Möglichkeit mittels WPA2, übergangsweise auch mit WPA, oder alternativ mittels eines VPN.
- Es sollte eine gegenseitige Authentisierung zwischen den Clients und der WLAN-Infrastruktur erfolgen (z. B. mittels EAP-TLS), um unberechtigte Mitbenutzung zu verhindern.
- Die Sicherheitsrichtlinien müssen um das Themen WLAN erweitert und konsequent umgesetzt werden.

1.2 Einführung und Überblick

Bei WLAN kommen im Vergleich zu einem LAN eine Reihe zusätzlicher Techniken und Standards zum Einsatz. Die meisten WLAN-Installationen basieren auf der Norm 802.11 des Institute of Electrical and Electronics Engineers (IEEE). Neben der IEEE 802.11 gibt es noch weitere WLAN-Spezifikationen, wie z. B. HomeRF oder HiperLAN/2, die jedoch keine praktische Relevanz mehr besitzen.

Dieser Abschnitt fasst die Grundlagen von WLAN kurz zusammen und geht dabei auf Kategorisierung von WLAN-Installationen, Techniken für die Verschlüsselung und Mechanismen zur Authentisierung ein. Abschnitt 1.2.1 nimmt zunächst eine Unterteilung von WLAN-Installationen gemäß ihres Aufbaus und ihrer Funktionsweise vor. Anschließend werden dann Methoden zur Verschlüsselung der Datenkommunikation erläutert. Dabei behandelt Abschnitt 1.2.2 die Standards WEP und WPA und Abschnitt 1.2.3 Mechanismen zur Authentisierung. Abschließend geht Abschnitt 1.2.4 auf den Einsatz von VPN ein.

1.2.1 Kategorisierung von WLAN-Installationen

Beim Einsatz von WLAN lassen sich drei wesentliche Anwendungen und Aufbauvarianten unterscheiden: der Infrastruktur-Modus, der Ad-hoc-Modus und die LAN-Kopplung. Des Weiteren ist eine gesonderte Betrachtung homogener und heterogener Netze zweckmäßig.

Infrastruktur-Modus

Die verbreitetste Anwendung von WLAN ist die drahtlose Anbindung von Clients an bestehende Netze. Dazu ist eine Ergänzung der LAN-Infrastruktur notwendig. Den Kern dieser Ergänzung bilden Basic Service Sets, die jeweils aus einem Access Point und dessen Funkzelle bestehen. Die Basic Service Sets sind über das sogenannte Distribution System mit dem LAN verbunden. Das Distribution System mitsamt aller Basic Service Sets wird als Extended Service Set bezeichnet (vgl. Abbildung 1.1). Jedes Extended Service Set besitzt einen eigenen Namen, den sogenannten Service Set Identifier (SSID). Dieser soll eine eindeutige Zuordnung zu einem Extended Service Set ermöglichen, wenn mehrere WLAN verfügbar sind.

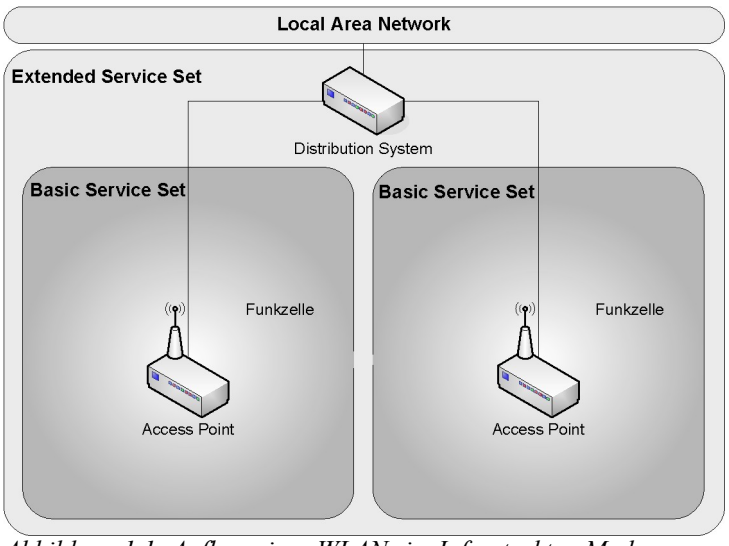

Abbildung 1.1: Aufbau eines WLANs im Infrastruktur-Modus

Ad-hoc-Modus

Es ist für Clients jedoch auch möglich direkt, also ohne entsprechende Infrastruktur, miteinander zu kommunizieren. Dieser Betriebsmodus ist derzeit vergleichsweise selten anzutreffen, könnte jedoch im Kontext von Mobile Ad-hoc Networks (MANET, auch Mesh Net) verstärkt an Bedeutung gewinnen. Darunter versteht man Netze, die sich ohne feste Infrastruktur selbstständig aufbauen und konfigurieren.

LAN-Kopplung

Eine weitere Anwendung von WLAN ist die Kopplung einzelner LAN-Segmente. Dazu müssen typischerweise größere Distanzen überbrückt werden als im Infrastruktur-Modus. Zur Verbindung kommunizieren die Kopplungselemente (sog. Wireless Bridges) meist über gerichtete WLAN-Antennen miteinander.

Homogene und heterogene Client-Umgebungen

WLAN-Infrastrukturen können auch entsprechend der Art ihrer Clients kategorisiert werden. Bei der Verwendung homogener Clients ist eine einheitliche Sicherheitsrichtlinie wesentlich einfacher zu realisieren als bei einer heterogenen Umgebung. Werden viele verschiedene Client-Geräte verwendet, so kann es unter Umständen vorkommen, dass nicht alle Geräte die bevorzugten Sicherheitsmechanismen unterstützen. Beispiele für solche Geräte sind Produkt-Scanner, Mobiltelefone oder ältere Notebooks.

1.2.2 Sicherheitsstandards

Bei der Betrachtung von WLAN-Sicherheitsstandards sind im Wesentlichen zwei Institutionen zu nennen: das Institute of Electrical and Electronics Engineers (IEEE) und die Wi-Fi Alliance. Das IEEE hat unter anderem die WLAN-Norm 802.11 spezifiziert, auf der die meisten WLAN-Installationen basieren, während die Wi-Fi Alliance die Standards WPA und WPA2 beschrieben hat.

Wireless Equivalent Privacy (WEP)

In der 1999 von der IEEE herausgegebenen Norm zu WLAN (IEEE 802.11[1]) ist WEP als Verfahren zur Authentisierung und Verschlüsselung beschrieben. Inzwischen existieren jedoch zahlreiche, frei verfügbare Programme, die automatisierte Angriffe auf WEP ermöglichen. Aus diesem Grund ist vom Gebrauch von WEP dringend abzuraten.

IEEE 802.11i

Aufgrund der Mängel des WEP-Verfahrens wurde 2001 eine eigene Arbeitsgruppe gegründet, um eine neue Sicherheitslösung zu entwickeln. Der neue Standard IEEE 802.11i wurde 2004 veröffentlicht. Ein WLAN, das nur Verbindungen erlaubt, dessen Kommunikation durch die in IEEE 802.11i spezifizierten Sicherheitsmechanismen geschützt sind, wird als Robust Security Network bezeichnet. In dieser Spezifikation werden zwei Sicherheitsprotokolle vorgestellt:

- Temporal Key Integrity Protocol (TKIP)
- CTR with CBC-MAC Protocol (CCMP)

1 Neben IEEE 802.11 gibt es auch noch andere WLAN Spezifikationen, wie z. B. HomeRF oder HiperLAN/2. Diese besitzen jedoch keine praktische Relevanz mehr.

TKIP ist lediglich als Übergangslösung gedacht, um die Abwärtskompatiblität mit bestehenden WLAN-Systemen zu gewährleisten. Es basiert auf dem gleichen Verschlüsselungsverfahren wie WEP, beseitigt jedoch die wesentlichen Schwächen von WEP. So wird beispielsweise pro Paket ein neuer Schlüssel erzeugt, um das Problem des statischen Schlüssels zu lösen. Des Weiteren wurde eine zusätzliche Integritätsprüfung eingeführt, um Paketfälschungen vorzubeugen.

Ende 2008 wurde ein Angriff auf TKIP vorgestellt, der es unter bestimmten Voraussetzung ermöglicht mehrere Pakete mit beliebigem Inhalt in das Netz zu injizieren [TeBe08]. Ein Angreifer kann dies nutzen, um das Mitlesen der Kommunikation vorzubereiten. Daher sollte bevorzugt CCMP eingesetzt werden.

Im Gegensatz zu TKIP wurde CCMP als langfristige Lösung konzipiert, die mit dem Advanced Encryption Standard (AES) ein modernes Verschlüsselungsverfahren verwendet. Dadurch wird allerdings auch neue Hardware erforderlich, da CCMP auf älteren Geräten meist nicht verwendbar ist.

Beide Verfahren benutzen einen gemeinsamen Schlüssel (Pairwise Master Key), aus dem weitere Schlüssel abgeleitet werden. Der gemeinsame Schlüssel kann entweder auf dem Client vorinstalliert werden (Pre-Shared Key), oder bei einer EAP-Authentifizierung erzeugt werden (siehe Abschnitt 1.2.3). Die aus dem gemeinsamen Schlüssel abgeleiteten Schlüssel werden in festgelegten Intervallen erneuert (Re-Keying).

Beide in IEEE 802.11i beschrieben Protokolle dienen nur zur Sicherung von Datenpaketen. Nachrichten mit Verwaltungsinformationen (sog. Management Frames) werden hingegen ungeschützt übertragen. Ein Angreifer kann diese Schwachstelle ausnutzen, um einzelne Clients von ihren Access Point zu trennen (Disassociation Angriff). Deshalb wurde 2005 eine weitere Arbeitsgruppe gegründet, die an einem Standard zum Schutz von Management Frames arbeitet. Bisher wurde hierzu jedoch kein Standard verabschiedet.

Wi-Fi Protected Access (WPA/WPA2)

Der Zeitraum zwischen dem Bekanntwerden der WEP-Schwachstellen und der Verabschiedung der IEEE 802.11i war recht lang. Da jedoch ein akuter Handlungsbedarf bestand, hat die Wi-Fi Alliance bereits 2003 WPA als vorläufigen Standard veröffentlicht. WPA entspricht Teilen von IEEE 802.11i.

TKIP und somit auch WPA sind jedoch nur als Zwischenlösungen konzipiert. Langfristig soll der Nachfolger WPA2 verwendet werden. WPA2 basiert vollständig auf IEEE 802.11i und deckt alle zwingenden Anforderungen dieser Norm ab. Damit steht bei WPA2 auch CCMP zur Verfügung. Seit 2006 müssen alle neuen WLAN-Geräte, die von der Wi-Fi Alliance zertifiziert werden sollen, WPA2 unterstützen.

Generell ist der Einsatz von WPA2 (CCMP) gegenüber WPA (TKIP) zu bevorzugen, sofern dies technisch möglich ist. Vom Einsatz von WEP ist grundsätzlich abzuraten.

1.2.3 Authentisierung

Für die Authentisierung lassen sich im Wesentlichen zwei Verfahren unterscheiden. Die erste Möglichkeit ist eine implizite Authentisierung über einen sogenannten Pre-Shared Key (PSK). Alternativ dazu kann auch eine explizite Authentisierung an einem Authentisierungs-Server verwendet werden.

Pre-Shared Key

Bei dieser Authentisierung-Methode muss jeder Client, der am WLAN teilnehmen soll, mit dem Pre-Shared Key versorgt werden. Aus diesem Grund werden Pre-Shared Keys typischerweise nur in kleinen Netzen, wie beispielsweise bei Heimnetzen, verwendet. Um bei der Verwendung von Pre-Shared Keys die Sicherheit zu gewährleisten, ist darauf zu achten, dass der Schlüssel eine ausreichende Komplexität und Länge aufweist. So sollte das Passwort neben Buchstaben auch Ziffern und Sonderzeichen enthalten und gemäß einer Empfehlung der IEEE mindestens 20 Zeichen umfassen [IEEE 802.11]. Für einen erhöhten Schutz gegen Angriffe auf schwache Passwörter sollte die maximal mögliche Länge von 63 Zeichen ausgenutzt werden. Des Weiteren sollte das Passwort regelmäßig erneuert werden.

Verfahren, die mit Pre-Shared Keys arbeiten, sind beispielsweise WPA-PSK (auch WPA-Personal genannt) und WPA2-PSK.

IEEE 802.1X

Für große WLAN-Installationen ist die Verwendung eines Pre-Shared Keys aufgrund des organisatorischen Aufwands nicht zu empfehlen. Statt dessen kann eine Authentisierung auf Basis des IEEE-Standards 802.1X erfolgen. In diesem Standard wurde mit dem Extensible Authentication Protocol (EAP) ein Gerüst spezifiziert, das zahlreiche Methoden zum Identitätsnachweis erlaubt.

Der WLAN-Client meldet sich mit seinen Authentisierungs-Daten an einem Access Point an. Dieser übermittelt die Daten des Clients zur Überprüfung an einen Authentisierungs-Servers (häufig ein RADIUS-Server) und erhält als Rückmeldung, ob der Zugang gewährt wird.

Da bei der Verwendung von EAP-Authentifizierung der gemeinsame Schlüssel nicht im Vorhinein bekannt ist, kommen nur EAP-Methoden in Frage, die eine geeignete Art von Schlüsselerzeugung unterstützen. Einige dieser Methoden erlauben eine gegenseitige Authentisierung (z. B. EAP-TLS), wohingegen andere Methoden nur eine einseitige Authentisierung (z. B. EAP-PEAP) erlauben.

Generell ist der Einsatz von IEEE 802.1X in Kombination mit einer hochwertigen EAP-Methode wie EAP-TLS zu empfehlen. Auch WPA und WPA2 unterstützen die Authentisierung gemäß 802.1X. Man spricht in diesem Fall auch von WPA-Enterprise bzw. WPA2-Enterprise.

1.2.4 VPN zur Absicherung des WLAN

Alternativ zu den oben beschriebenen Verfahren kann auch ein VPN (Virtual Private Network) zur Absicherung des Datenverkehrs in einer WLAN-Installation genutzt werden. Bis zur Einführung von WPA waren VPNs die einzige nicht-proprietäre Alternative zu WEP. Daher sind VPN-Lösungen noch in vielen WLAN-Installationen anzutreffen. Grundsätzlich kann zwischen IP-basierten VPNs und solchen, die auf SSL aufbauen, unterschieden werden. Für weitere Informationen siehe auch [ISi-VPN].

IPSec-VPN

Bei einem IPSec-VPN findet die Absicherung der Kommunikation auf IP-Ebene statt. Solche VPNs bieten einen sicheren Netzzugriff, der für höhere Protokoll-Schichten vollkommen transparent ist. Für ein solches VPN ist allerdings eine spezielle Client-Software erforderlich. Probleme bei einer Nutzung von Network Address Translation (NAT), bei der interne IP-Adressen durch externe ersetzt werden, wurden durch die Erweiterung NAT-Traversal behoben.

SSL-VPN

Eine andere Möglichkeit sind VPN-Lösungen auf Basis von SSL/TLS. Um einen ähnlichen Funktionsumfang wie beim IPSec-VPN zu erhalten, muss auch hier ein spezieller SSL-Client verwendet werden. Alternativ können SSL-VPNs auch nur mit einem Browser genutzt werden. Bei dieser Variante wird über HTTPS eine verschlüsselte Verbindung zu einem Web-Server aufgebaut. Der Nachteil ist, dass damit nur bestimmte Applikationen genutzt werden können.

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

In diesem Abschnitt werden die signifikanten Gefährdungen zusammengefasst, die beim Einsatz von WLAN bestehen. Diese Gefährdungen lassen sich entsprechend des Sicherheitsgrundwerts, den sie bedrohen, klassifizieren:

- Eindringen und Übernehmen (sog. „Hacking“)
- Täuschen, Fälschen und Betrügen (Angriffe auf die Integrität und Authentizität)
- Ausspähen und Entwenden (Angriffe auf die Vertraulichkeit)
- Verhindern und Zerstören (Angriffe auf die Verfügbarkeit)

1.3.1 Eindringen und Übernehmen

Gefährdungen durch unberechtigten Zugang

Eine solche Gefährdung besteht, wenn ein Angreifer auf das System (d. h. auf einen WLAN-Client oder Bestandteile der Infrastruktur) zugreift und dieses unter seine Kontrolle bringt. Dazu kann ein Angreifer Schwachstellen in der verwendeten Software ausnutzen. Die Kompromittierung eines Systems dient meist als Vorbereitung eines Angriffes auf einen Sicherheitsgrundwert wie z. B. die Vertraulichkeit von Daten.

Da bei WLAN-Installationen häufig mobile Endgeräte (z. B. Notebooks) verwendet werden, besteht auch die Gefahr, dass ein Angreifer ein solches Gerät in seinen Besitz bringt und somit Zugriff auf das WLAN hat. Voraussetzung dafür ist, dass die Authentisierungs-Merkmale des Benutzers (beispielsweise Passwörter) auf dem entwendetem Gerät gespeichert sind.

Gefährdungen durch fehlerhafte Konfiguration

Ein Beispiel für eine Gefährdung ist, dass ein Access Point nicht entsprechend den Sicherheitsrichtlinien konfiguriert ist und voreingestellte Passwörter nicht geändert wurden. Dies kann es einem Angreifer erheblich vereinfachen den Access Point zu kompromittieren.

Eine weitere Schwachstelle in der Konfiguration besteht, wenn WLAN-Clients nicht nur Verbindungen mit voreingestellten Access Points aufbauen können. In diesem Fall kann ein Angreifer

einen zusätzlichen Access Point in Reichweite platzieren und Clients dazu bewegen, sich bei ihm statt am regulären Access Point anzumelden. Geht ein Client eine solche Verbindung ein, so kann der Angreifer über diese Verbindung Angriffe auf den Client starten. Selbst wenn WLAN-Karten und Adapter entsprechend konfiguriert sind und keine Verbindungen zu fremden Access Points erlauben, können Benutzer diesen Schutz überwinden, indem sie zusätzliche WLAN-Adapter (etwa über USB) anschließen.

Gefährdungen durch Hotspots

Eine erhöhte Gefährdung besteht, wenn Clients auch in Netzen anderer Betreiber, insbesondere an Hotspots, genutzt werden. Um das Web-Portal von Hotspots zu erreichen, müssen die Ports für DHCP, HTTP und gegebenenfalls auch DNS für alle IP-Adressen freigeschaltet sein. Zudem erfolgt die Anmeldung am Hotspot häufig über eine Web-Oberfläche, die Aktive Inhalte verwendet. Um sich anzumelden, müssen Aktive Inhalte also am WLAN-Client zugelassen sein. Dadurch bietet der Client eine größere Angriffsfläche (siehe auch [ISi-Web-Client]).

1.3.2 Täuschen, Fälschen und Betrügen

Gefährdung durch unzureichende Authentisierung des Clients

WLAN verwendet ein offenes Medium, d. h. es kann von jedem genutzt werden. Daraus ergeben sich mehrere mögliche Angriffswege auf die Authentizität. Wird keine Authentisierung durchgeführt, so kann ein Angreifer versuchen als Client eine bestehende WLAN-Installation mitzubenutzen. Gelingt ihm dies, so kann er beispielsweise Spam-E-Mails verschicken oder illegale Inhalte herunterladen.

Gefährdung durch fremde Hardware

Ein weiterer Angriff auf die Authentizität besteht darin, dass ein Angreifer sich als Teil der WLAN-Infrastruktur ausgibt. Er könnte beispielsweise einen zusätzlicher Access Point (Rogue Access Point) bereitstellen, der keine Verschlüsselung verlangt. In diesem Szenario würden WLAN-Nutzer sich beim Angreifer statt am richtigen Access Point anmelden. Der Angreifer kann dann über die bestehende Verbindung Angriffe auf den Client starten. Ebenso kann er den gesamten Netzverkehr seines Opfers mitlesen (Man-in-the-Middle-Angriff).

Gefährdungen durch Paketfälschungen

Bei unverschlüsselten oder WEP-verschlüsselten Netzen sind auch Angriffe auf die Integrität von Nachrichten möglich. In der WEP-Spezifikation ist zwar eine Prüfsumme vorgesehen, um Übertragungsfehler zu erkennen, aber diese Prüfsumme eignet sich nicht zur Abwehr systematischer Paketfälschungen. Unter bestimmten Bedingungen ist es möglich auch in ein mit WPA verschlüsseltes Netz einige Pakete zu injizieren [TeBe08].

1.3.3 Ausspähen und Entwenden

Gefährdungen durch Abhören der Luftschnittstelle

Da sich die Ausbreitung von Funkwellen nicht genau kontrollieren lässt, kann ein mit einem ausreichend sensiblen Empfangsgerät ausgerüsteter Angreifer den Netzverkehr auch aus einiger Entfernung noch abhören. Wird der Netzverkehr nicht verschlüsselt, so kann der Angreifer die übertragenen Informationen mitlesen. Davon betroffen sind unter Umständen auch vertrauliche Daten, wie beispielsweise E-Mails.

Eine besondere Gefährdung für den WLAN-Client besteht bei der Nutzung von öffentlichen Hotspots. Hotspots verwenden häufig keine oder nur schwache Sicherheitsmechanismen, um Kunden einen unkomplizierten Zugang zu ermöglichen. Dadurch sind Übertragungen in der Regel leicht abzuhören.

Aber selbst wenn der Netzverkehr verschlüsselt wird, kann ein Angreifer versuchen diese Verschlüsselung zu brechen. Bei Verwendung statischer Schlüssel, wie bei WEP, WPA-PSK oder WPA2-PSK, kann ein Angreifer mittels einer Wörterbuch-Attacke versuchen, den Schlüssel zu erraten. Besonders gefährdet sind dabei Funknetze, die zur LAN-Kopplung eingesetzt werden, da diese Verbindungen stationär sind und ein Angreifer somit viel Zeit für seinen Angriff hat. Auch führen solche Kopplungen oft über Terrain, das nicht unter der Verfügungsgewalt des WLAN-Betreibers liegt, was dem Angreifer das Mithören der Übertragungen erleichtern kann.

Gefährdungen durch Abhören der Ethernet-Anbindung

Eine weitere Möglichkeit zum Ausspähen von Daten ist der Anschluss zusätzlicher Geräte an die Netz-Infrastruktur, sofern diese zugänglich ist (z. B. für einen Innentäter). So kann ein Angreifer beispielsweise einen Hub zwischen die Access Points und das Distribution System schalten, um den gesamten Netzverkehr abzuhören. Dieses stellt selbst bei einer Verwendung von WPA/WPA2 eine Gefährdung dar, da sich die Absicherung durch diese Methoden nur auf die Luftschnittstelle bezieht, die Ethernet-Anbindung aber nicht weiter berücksichtigt.

Auch der Anschluss eines weiteren Access Points birgt erhebliche Gefahren. Dieses gilt insbesondere für Access Points, die vom Angreifer selbst installiert wurden, aber auch für von Mitarbeitern angeschlossene Access Points, die unzureichend konfiguriert sind und z. B. keine Verschlüsselung erzwingen.

1.3.4 Verhindern und Zerstören

Gefährdungen durch Hardware-Schäden

Durch Hardware-Schäden kann es zu Störungen im Funkverkehr und damit zu Einbußen bzw. dem Verlust der Verfügbarkeit kommen. Dieses betrifft insbesondere WLAN-Geräte, die außerhalb von geschützten Räumen angebracht werden (z. B. zur LAN-Kopplung oder zur Abdeckung offener Plätze). Sie sind zusätzlichen Gefährdungen ausgesetzt, wie beispielsweise vorsätzliche Beschädigungen durch Angreifer oder umweltbedingte Schäden durch Witterung oder Blitzeinschlag.

Erfolgt die Authentisierung und das Schlüsselmanagement nach IEEE 802.1X, so bildet der Authentisierungs-Server unter Umständen einen „single point of failure“, bei dessen Ausfall keine Neuanmeldungen am WLAN mehr möglich sind.

Gefährdungen durch Störsignale

Eine andere grundlegende Gefährdung für die Verfügbarkeit von WLAN ist, dass es bei der Nutzung von Funk zu Interferenzen und Störungen kommen kann. WLAN-Installationen nach den Standards IEEE 802.11b/g und teilweise auch 802.11n nutzen das ISM-Band im 2,4 GHz Bereich. So kann es neben Überlagerungen mit benachbarten WLAN auch zu Störungen durch Mikrowellenherde oder Bluetooth-Geräte kommen, die dasselbe Frequenzband verwenden.

Abgesehen von diesen unbeabsichtigten Überlagerungen kann ein Angreifer natürlich auch mutwillig Störungen provozieren. Dazu kann er Geräte in der Nähe des WLAN platzieren, die auf dem gleichen Frequenzband wie das WLAN senden. Dieses können z. B. andere WLAN-Geräte oder auch Störsender sein. Außerdem kann die Verbindungsqualität durch Wettereinflüsse beeinträchtigt werden. Bei allen Störungen, egal ob unbeabsichtigt, vorsätzlich oder wetterbedingt, ist mit Leistungseinbußen zu rechnen, die im schlimmsten Fall zum Verlust der Verfügbarkeit führen.

Gefährdungen durch gefälschte Pakete

Ein weiterer Angriff auf die Verfügbarkeit ist das Trennen einzelner Clients vom jeweiligen Access Point durch das gezielte Injizieren von Management-Paketen. Dabei wird eine Schwachstelle der IEEE 802.11 Spezifikation ausgenutzt, wodurch es möglich ist einzelne Clients an der Nutzung des WLAN zu hindern.

Bei einer Verwendung von WPA bzw. TKIP besteht zudem eine Gefährdung durch einen weiteren Angriff auf die Verfügbarkeit. Die bei WPA verwendete Integritätsprüfung dient zur Erkennung von Manipulationen an Paketen. Sobald diese mehr als zwei Manipulationen pro Minute registriert, werden alle Übertragungen der zugehörige MAC-Adresse für eine Minute ignoriert. Ein Angreifer kann über diesen automatischen Sperrmechanismus gezielt einzelne Clients vom Netz ausschließen. Dazu muss er lediglich im Namen des Clients, den er sperren möchte, Pakete mit ungültiger Prüfsumme versenden.

1.4 Wesentliche Empfehlungen

In diesem Abschnitt werden Empfehlungen und Maßnahmen für die sichere Nutzung von WLAN gegeben, um den Gefährdungen aus Abschnitt 1.3 zu begegnen. Die Empfehlungen richten sich dabei nach dem jeweiligen Anwendungsfall der WLAN-Installation.

1.4.1 Absicherung eines Infrastruktur-WLANs

Es wird empfohlen, die Kommunikation auf der Luftschnittstelle mit WPA2 zu verschlüsseln oder wenn dies technisch nicht möglich ist zumindest WPA zu verwenden. Insbesondere bei einer Verwendung von WPA ist darauf zu achten, dass die verwendeten Schlüssel in kurzen Abständen neu ausgehandelt werden (Re-Keying). Falls aufgrund mangelnder Unterstützung einige Geräte sogar auf WEP zurückgreifen müssen, so sollten diesen Geräten weniger Rechte bei der WLAN-Nutzung eingeräumt werden. Diese Trennung zwischen einzelnen Geräteklassen oder Benutzergruppen sollte nach Möglichkeit physisch durch mehrere Access Points umgesetzt werden. Auf diese Weise lässt sich der Zugriff auf das WLAN und auf vertrauliche Daten entsprechend des verwendeten Sicherheitsstandards regeln.

Die Authentisierung sollte gemäß IEEE 802.1X erfolgen. Besteht eine Public-Key Infrastruktur (PKI), in der jeder WLAN-Client mit einem Zertifikat ausgestattet ist, so wird die Verwendung von EAP-TLS empfohlen. Andernfalls kann mit Abstrichen in der Schutzwirkung auch EAP-

MSCHAPv2 in Kombination mit EAP-PEAP, -FAST oder -TTLS verwendet werden. Bei kleinen WLAN-Installationen ist auch der Einsatz von Pre-Shared Keys möglich, wobei das Passwort eine ausreichender Länge und Komplexität aufweisen muss. Das Passwort sollte dabei die maximale Schlüssellänge ausnutzen und neben Ziffern, Klein- und Großbuchstaben auch Sonderzeichen enthalten (siehe auch [ITGSK]).

Maßnahmen für Access Points

Voreingestellte Standard-Passwörter und SSIDs müssen bei der Konfiguration von Access Points geändert werden. Dabei ist zu beachten, dass neu gewählte SSIDs keinen Rückschluss auf die verwendete Hardware, das Netz oder den Betreiber zulassen.

Zum Schutz der Access Points sollten diese unzugänglich montiert werden (z. B. in Zwischendecken), um Manipulationen vorzubeugen. Ferner sind unsichere Administrationszugänge (über die Luftschnittstelle oder unsichere Protokolle) zu deaktivieren. Wenn andere Möglichkeiten zur Verfügung stehen, sollte von der Verwendung eines Web-Interfaces zur Konfiguration abgesehen werden.

1.4.2 Absicherung mobiler Clients

Mobile Clients werden häufig in fremden Umgebungen eingesetzt und sind deshalb vermehrt Gefährdungen ausgesetzt. Aus diesem Grund sollten sie besonders abgesichert sein. Zu den üblichen Maßnahmen zählen unter anderem die Absicherung des Betriebssystems, Festplattenverschlüsselung, Einsatz einer Personal Firewall und eines Virenschutzprogramms und das Arbeiten mit eingeschränkten Benutzerrechten.

Zusätzlich ist für die WLAN-Konfiguration Folgendes zu beachten: Das automatische Verbinden zu verfügbaren WLANs sollte deaktiviert werden. Rechner, die nicht für die Hotspot-Nutzung gedacht sind, sollten so konfiguriert sein, dass eine Verbindung nur zu voreingestellten WLAN-Installationen möglich ist. Benutzer sollten auch keine zusätzlichen WLAN-Adapter (z. B. über USB) anschließen dürfen, um zu verhindern, dass die vorgegebene Konfiguration umgangen wird. Des Weiteren sollte der Ad-hoc-Modus in der Client-Konfiguration deaktiviert werden, wenn er nicht explizit benötigt wird.

1.4.3 Sichere Hotspots

Für den Anbieter eines Hotspots kommen im Vergleich zum Betreiber eines Infrastruktur-WLAN noch ein Web-Server und Web-Anwendungen hinzu, die als Anmelde- und Abrechnungs-System verwendet werden. Für kleinere Hotspots werden häufig auch spezielle Geräte (sog. Appliances) verwendet. Die Sicherheit dieser Systeme hängt von der Absicherung des Betriebssystems, der Konfiguration der Firewall und der Programmierung der Web-Anwendung ab (siehe auch [ISi-Web-Server]).

Betreiber von Hotspots sollten ihren Kunden die Möglichkeit bieten, die Kommunikation zu verschlüsseln und ihnen erlauben ein VPN aufzubauen. Die Anmeldung am Hotspot sollte über eine gesicherte Verbindung (HTTPS) erfolgen, damit auch die Übermittlung der Anmeldedaten geschützt ist.

Mobile Clients dürfen nicht direkt über den Hotspot auf das Internet zugreifen, sondern müssen erst eine gesicherte Verbindung mit dem internen Netz aufbauen und können über dieses das Internet nutzen. Dazu meldet sich der mobile Client zunächst am Access Point des Hotspots an und baut

über diesen eine Verbindung zum VPN-Gateway des internen Netzes auf. Die Kommunikation zwischen Client und VPN-Gateway erfolgt dann über einen verschlüsselten Kanal. Vom VPN-Gateway aus kann er dann über das Sicherheits-Gateway des internen Netzes auf das Internet zugreifen. Der Zugriff auf das Internet ist dementsprechend durch die Mechanismen des Sicherheits-Gateways geschützt. Weitere Empfehlungen zur mobilen Nutzung finden sich in der Studie „Sicherer Fernzugriff auf lokale Netze“ [ISi-Fern].

Die Sicherheitsmechanismen eines VPN greifen im Gegensatz zu denen von WLAN im Allgemeinen erst auf Layer 3 oder höher. Ist das WLAN an sich nicht geschützt, so ist darauf zu achten, dass der Client auch gegen Angriffe auf tieferen Protokollebenen geschützt wird.

1.4.4 Absicherung einer LAN-Kopplung

Um die Vertraulichkeit und die Integrität einer drahtlosen LAN-Kopplung zu schützen, lässt sich sowohl ein VPN, als auch WPA2 verwenden.

Der Vorteil einer VPN-Lösung liegt insbesondere darin, dass die Verschlüsselung der Kommunikation bis zum VPN-Server gegeben ist. Das gilt allerdings nicht, wenn zur Kopplung Wireless Bridges eingesetzt werden, die bereits ein VPN-Gateway enthalten. In diesem Falle endet die Verschlüsselung bereits an der Bridge und der Betreiber muss dafür Sorge tragen, dass der Zugang zur Ethernet-Schnittstelle der Bridge ausreichend gesichert ist.

Auch bei der Verwendung von WPA2 ist zu beachten, dass die Verschlüsselung an der Bridge endet und der Zugang zur Ethernet-Schnittstelle entsprechend gesichert sein muss. Wird WPA2 mit einem Pre-Shared Key verwendet, so besteht zusätzlich die Gefährdung einer Wörterbuch-Attacke gegen diesen Schlüssel.

Dieser Nachteil kann vermieden werden, wenn die Authentisierung nicht über einen statischen Schlüssel, sondern mittels IEEE 802.1X erfolgt (WPA2-Enterprise). Hierbei sollte eine gegenseitige Authentisierung der Wireless Bridges erfolgen, die periodisch wiederholt werden sollte (Re-Authentisierung).

Die Verfügbarkeit ist auf der Luftschnittstelle nicht mit Sicherheit zu gewährleisten, da Störsignale sehr einfach und effektiv erzeugt werden können. Es besteht lediglich die Möglichkeit redundante Übertragungswege zu schaffen.

1.5 Fazit

Der Einsatz von WLAN ermöglicht eine komfortable, kostengünstige und unkomplizierte Erweiterung kabelgebundener Netze. Auch bietet es die Möglichkeit zur Kopplung nahe gelegener Standorte, ohne die Notwendigkeit Kabel zu verlegen. Andererseits ist die Verwendung von WLAN auch mit erheblichen Gefahren verbunden, die insbesondere die Vertraulichkeit von Daten und die Verfügbarkeit des Netzzuganges betreffen.

Während sich die Verfügbarkeit von WLANs im Allgemeinen nicht gewährleisten lässt, lassen sich die Integrität und die Vertraulichkeit der Kommunikation mittels geeigneter Verfahren, wie WPA2 oder eines VPN, schützen.

Welche Verfahren zur Verschlüsselung und zur Authentisierung zum Einsatz kommen, ist vom jeweiligen Einsatzgebiet abhängig. Detailliertere Informationen dazu finden sich in weiteren Publikationen des BSI, wie der Studie „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ [DRAHT-KOM], dem WLAN-Baustein der IT-Grundschutzkataloge [ITGSK] und insbesondere

der „Technische Richtlinie Sicheres WLAN“ [TR-S-WLAN]. Letztere enthält neben einer Einführung in das Thema und der ausführlichen Beschreibung und Bewertung der Sicherheitsmechanismen auch konkrete Beispiele für verschiedene Einsatzszenarien.

2 Glossar

ALG (Application-Level Gateway [engl.])

Filterfunktionen oberhalb der Transportschicht werden von einem sogenannten Application-Level Gateway übernommen, auch Sicherheits-Proxy genannt. Ein Proxy ist eine Art Stellvertreter für Dienste in Netzen. Er nimmt Daten an seinem Eingang entgegen und leitet sie nach einer Prüfung an den eigentlichen Dienst weiter. Mittels eines Proxys lassen sich Datenströme auf der Anwendungsschicht verwerfen, modifizieren oder gezielt weiterleiten. Implizit nehmen ALGs auch Funktionen auf den darunter liegenden Schichten des TCP/IP-Modells wahr. ALGs unterbrechen den direkten Datenstrom zwischen Quelle und Ziel. Bei einer Kommunikationsbeziehung zwischen Client und Server über das ALG hinweg nimmt das ALG die Anfragen des Clients entgegen und leitet sie an den Server weiter. Bei einem Verbindungsaufbau in umgekehrter Richtung, also vom Server zum Client, verfährt das ALG analog. Diese Kommunikationsform ermöglicht es dem ALG beispielsweise, bestimmte Protokollbefehle auf der Anwendungsschicht zu filtern. Das ALG kann zudem die strikte Einhaltung von Anwendungsprotokollen erzwingen, unerwünschte Anwendungsdaten aus den Datenpaketen entfernen (bzw. austauschen) oder Verbindungen anwendungsspezifisch protokollieren.

Angriff (engl. attack)

Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen.

Authentifizierung (engl. authentication)

Unter einer Authentifizierung versteht man die Prüfung einer Authentisierung, d. h. die Überprüfung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Dies kann unter Anderem durch Passwort-Eingabe, Chipkarte oder Biometrie erfolgen.

Authentisierung (engl. authentication)

Unter einer Authentisierung versteht man die Vorlage eines Nachweises eines Kommunikationspartners, dass er tatsächlich derjenige ist, der er vorgibt zu sein.

Authentizität (engl. authenticity)

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Baustein

Der Begriff dient im IT-Grundschutz zur Strukturierung von Informationstechnik und ihrer Einsatzumgebung. Bausteine sind die Einheiten innerhalb einer Schicht (z. B. IT-Systeme, Netze). Sie beschreiben teils technische Komponenten (wie Verkabelung), teils organisatorische Verfahren (wie

Notfallvorsorge-Konzept) und besondere Einsatzformen (wie Häuslicher Arbeitsplatz). In jedem Baustein werden die betrachtete IT-Komponente und die Gefährdungslage beschrieben sowie organisatorische und technische Sicherheitsmaßnahmen empfohlen.

Betriebssystem (engl. operating system)

Das Betriebssystem ist ein Steuerungsprogramm, das es dem Benutzer ermöglicht, seine Dateien zu verwalten, angeschlossene Geräte (z. B. Drucker, Festplatte) zu kontrollieren oder Programme zu starten. Weit verbreitet sind z. B. Windows, Linux oder MacOS.

Browser [engl.]

Mit Browser (von "to browse", auf deutsch: schmökern, blättern, umherstreifen) wird Software zum Zugriff auf das World Wide Web bezeichnet. Das Programm interpretiert die ankommenden Daten und stellt sie als Text und Bild auf dem Bildschirm dar.

BSI (Bundesamt für Sicherheit in der Informationstechnik) (engl. Federal Office for Information Security)

Bundesbehörde im Geschäftsbereich des Bundesministerium des Innern.

Client [engl.]

Als Client wird Soft- oder Hardware bezeichnet, die bestimmte Dienste von einem Server in Anspruch nehmen kann. Häufig steht der Begriff Client für einen Arbeitsplatzrechner, der in einem Netz auf Daten und Programme eines Servers zugreift.

DNS (Domain Name System [engl.])

Das Domain Name System übersetzt alphanumerische Adressnamen (z. B. www.bsi.bund.de) in numerische Adressen (z. B. 194.95.177.86). Auch eine Übersetzung in die umgekehrte Richtung ist mit dem DNS möglich. Alphanumerische Namen für Rechner sind für die Benutzer einfach zu behalten und einzugeben. Da allerdings IPv4 und IPv6 Adressen in numerischer Form verlangen, ist eine Adressumsetzung durch das DNS notwendig.

Gefährdung

Eine Gefährdung ist eine Bedrohung, die konkret auf ein Objekt über eine Schwachstelle einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt. So sind beispielsweise Computer-Viren eine Bedrohung oder eine Gefährdung für Anwender, die im Internet surfen. Nach der oben gegebenen Definition lässt sich feststellen, dass alle Anwender prinzipiell durch Computer-Viren im Internet bedroht sind. Der Anwender, der eine virenbefallene Datei herunterlädt, wird von dem Computer-Virus gefährdet, wenn sein Computer anfällig für diesen Typ Computer-Virus ist. Für Anwender mit einem wirksamen Schutzprogramm, einer Konfiguration, die das Funktionieren des Computer-Virus verhindert, oder einem Betriebssystem, das den Virencode nicht ausführen kann, bedeutet das geladene Schadprogramm hingegen keine Gefährdung.

Hacking [engl.]

Hacking bezeichnet im Kontext von Informationssicherheit Angriffe, die darauf abzielen, vorhandene Sicherheitsmechanismen zu überwinden, um in ein IT-System einzudringen, seine Schwächen offen zulegen und es gegebenenfalls - bei unethischem Hacking - zu übernehmen.

HTTP (Hypertext Transfer Protocol [engl.])

Das Hypertext Transfer Protocol dient zur Übertragung von Daten - meist Webseiten - zwischen einem HTTP-Server und einem HTTP-Client, also z. B. einem Browser. Die Daten werden über Uniform Resource Locators (URL) eindeutig bezeichnet. URLs werden meist in der Form Protokoll://Rechner/Pfad/Datei angegeben. Protokoll steht dabei für Protokolle der Anwendungsschicht, Rechner für den Namen oder die Adresse des Servers und der Pfad der Datei gibt den genauen Ort der Datei auf dem Server an. Ein Beispiel für eine URL ist www.bsi.bund.de/fachthem/sinet/index.htm.

HTTPS (HTTP secure [engl.])

Protokoll zur sicheren Übertragung von HTML-Seiten im Internet. SSL/TLS dient dabei zur Absicherung der Client-Server-Kommunikation.

Hypertext

Elektronisches Dokumentenformat, das Querverweise (Hyperlinks) zwischen unterschiedlichen Dokumenten vorsieht, die Standard-Darstellungsform im WWW.

Integrität (engl. integrity)

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen. Wenn der Begriff Integrität auf "Daten" angewendet wird, drückt er aus, dass die Daten vollständig und unverändert sind. In der Informationstechnik wird er in der Regel aber weiter gefasst und auf "Informationen" angewendet. Der Begriff "Information" wird dabei für "Daten" verwendet, denen je nach Zusammenhang bestimmte Attribute wie z. B. Autor oder Zeitpunkt der Erstellung zugeordnet werden können. Der Verlust der Integrität von Informationen kann daher bedeuten, dass diese unerlaubt verändert, Angaben zum Autor verfälscht oder Zeitangaben zur Erstellung manipuliert wurden. Integrität ist ein Grundwert der IT-Sicherheit.

IP (Internet Protocol [engl.])

Verbindungsloses Protokoll der Internet-Schicht im TCP/IP-Referenzmodell. Ein IP-Header enthält in der Version IPv4 u. a. zwei 32-Bit-Nummern (IP-Adressen) für Ziel und Quelle der kommunizierenden Rechner.

IPSec (Internet Protocol Security [engl.])

Erweiterung des Internet-Protokolls IP zur Sicherstellung von Integrität, Authentizität und Vertraulichkeit. IPSec ist in der Version 6 des Internet-Protokolls (IPv6) enthalten.

IT-Sicherheit (engl. IT Security)

IT-Sicherheit bezeichnet einen Zustand, in dem die Risiken, die beim Einsatz von Informationstechnik aufgrund von Gefährdungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind. IT-Sicherheit ist also der Zustand, in dem Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind.

NAT (Network Address Translation [engl.])

Network Address Translation (NAT) bezeichnet ein Verfahren zum automatischen und transparenten Ersetzen von Adressinformationen in Datenpaketen. NAT-Verfahren kommen meist auf Routern und Sicherheits-Gateways zum Einsatz, vor allem, um den beschränkten IPv4-Adressraum möglichst effizient zu nutzen und um lokale IP-Adressen gegenüber öffentlichen Netzen zu verbergen.

Paketfilter (engl. packet filter)

Paketfilter sind IT-Systeme mit spezieller Software, die den ein- und ausgehenden Datenverkehr anhand spezieller Regeln filtern. Ihre Aufgabe ist es, Datenpakete anhand der Informationen in den Header-Daten der IP- und Transportschicht (z. B. Quell- und Ziel-Adresse, -Portnummer, TCP-Flags) weiterzuleiten oder zu verwerfen. Der Inhalt des Pakets bleibt dabei unberücksichtigt.

Passwort

Geheimes Kennwort, das Daten, Rechner, Programme u. a. vor unerlaubtem Zugriff schützt.

PKI (Public Key Infrastructure [engl.])

Sicherheitsinfrastruktur, die es ermöglicht, in nicht gesicherten Netzen (z. B. Internet) auf der Basis eines von einer vertrauenswürdigen Stelle ausgegebenen Schlüsselpaares (vgl. asymmetrische Verschlüsselung) verschlüsselt Daten auszutauschen bzw. Signaturen zu erzeugen und zu prüfen.

Protokoll (engl. protocol)

Beschreibung (Spezifikation) des Datenformats für die Kommunikation zwischen elektronischen Geräten.

Prüfsumme (engl. checksum)

In der Informatik ist eine Prüfsumme eine einfache Maßnahme zur Gewährleistung von Datenintegrität bei der Datenübermittlung oder -speicherung.

Schwachstelle (engl. vulnerability)

Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.

Server [engl.]

Als Server wird Soft- oder Hardware bezeichnet, die bestimmte Dienste anderen (Clients) anbietet. Typischerweise wird damit ein Rechner bezeichnet, der seine Hardware- und Software-Ressourcen in einem Netz anderen Rechnern zugänglich macht. Beispiele sind Applikations-, Daten-, Web- oder E-Mail-Server.

Sicherheits-Gateway

Ein Sicherheits-Gateway (oft auch Firewall genannt) gewährleistet die sichere Kopplung von IP-Netzen durch Einschränkung der technisch möglichen auf die in einer IT-Sicherheitsleitlinie als ordnungsgemäß definierte Kommunikation. Sicherheit bei der Netzkopplung bedeutet hierbei im Wesentlichen, dass ausschließlich erwünschte Zugriffe oder Datenströme zwischen verschiedenen Netzen zugelassen und die übertragenen Daten kontrolliert werden. Ein Sicherheits-Gateway für normalen Schutzbedarf besteht im Allgemeinen aus mehreren, in Reihe geschalteten Filterkomponenten. Dabei ist zwischen Paketfilter und Application-Level Gateway (ALG) zu unterscheiden.

Sicherheitskonzept (engl. security concept)

In einem Sicherheitskonzept werden die konzeptionellen Sicherheitsanforderungen systematisch festgelegt und das Vorgehen zu ihrer Umsetzung in Maßnahmen beschrieben.

Spam [engl.]

Gängige Bezeichnung für unverlangt zugesandte Werbepost per E-Mail.

SSL (Secure Sockets Layer [engl.])

Protokoll zur sicheren Kommunikation über das Internet, insbesondere zwischen Client und Server, basiert auf dem Verschlüsselungsalgorithmus RSA.

TLS (Transport Layer Security [engl.])

Protokoll zur sicheren Datenübertragung über das Internet. Nachfolger von SSL.

Verfügbarkeit (engl. availability)

Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese den Benutzern stets wie gewünscht zur Verfügung stehen. Verfügbarkeit ist ein Grundwert der IT-Sicherheit.

Verschlüsselung (engl. encryption)

Verschlüsselung (Chiffrieren) transformiert einen Klartext in Abhängigkeit von einer Zusatzinformation, die Schlüssel genannt wird, in einen zugehörigen Geheimtext (Chiffrat), der für diejenigen, die den Schlüssel nicht kennen, nicht entzifferbar sein soll. Die Umkehrtransformation - die Zurückgewinnung des Klartexts aus dem Geheimtext - wird Entschlüsselung genannt.

Vertraulichkeit (engl. confidentiality)

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein. Vertraulichkeit ist ein Grundwert der IT-Sicherheit.

Virenschutzprogramm

Ein Virenschutzprogramm ist eine Software, die bekannte Computer-Viren, Computer-Würmer und Trojanische Pferde aufspürt, blockiert und gegebenenfalls beseitigt.

Virus (engl. virus)

Ein Computer-Virus ist eine nicht selbstständige Programmroutine, die sich nach ihrer Ausführung selbst reproduziert und dadurch vom Anwender nicht kontrollierbare Manipulationen in Systembereichen, an anderen Programmen oder deren Umgebung vornimmt.

VPN (Virtual Private Network [engl.])

Ein Virtuelles Privates Netz (VPN) ist ein Netz, das physisch innerhalb eines anderen Netzes (oft dem Internet) betrieben wird, jedoch logisch von diesem Netz getrennt wird. In VPNs können unter Zuhilfenahme kryptografischer Verfahren die Integrität und Vertraulichkeit von Daten geschützt und die Kommunikationspartner sicher authentisiert werden, auch dann, wenn mehrere Netze oder Rechner über gemietete Leitungen oder öffentliche Netze miteinander verbunden sind. Der Begriff VPN wird oft als Bezeichnung für verschlüsselte Verbindungen verwendet, zur Absicherung des Transportkanals können jedoch auch andere Methoden eingesetzt werden, beispielsweise spezielle Funktionen des genutzten Transportprotokolls.

Webserver [engl.]

Ein Webserver ist eine Software-Komponente, mit der Web-Angebote über HTTP und HTTPS bereitgestellt werden können. Er nimmt Anfragen von Clients, wie z. B. Browsern, entgegen und beantwortet diese, indem er angefragte Dokumente ausliefert. Häufig wird auch die Hardware, auf dem eine Webserver-Software installiert ist, als Webserver bezeichnet.

WLAN (Wireless Local Area Network [engl.])

Mit WLAN werden drahtlose Netze bezeichnet, die auf der als IEEE 802.11 bezeichneten Gruppe von Standards basieren, die vom Institute of Electrical and Electronics Engineers (IEEE) spezifiziert wurden.

3 Stichwort- und Abkürzungsverzeichnis

4 Literaturverzeichnis

[TR-S-WLAN] Bundesamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie Sicheres WLAN, 2005, http://www.bsi.bund.de/literat/tr/trwlan

[DRAHT-KOM] Bundesamt für Sicherheit in der Informationstechnik (BSI), Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte, 2007, http://www.bsi.bund.de/literat/tr/trwlan

[ITGSK] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT Grundschutzkataloge, Stand 2008, http://www.bsi.bund.de/gshb/

[TeBe08] Martin Beck & Erik Tews, Practical Attacks against WEP and WPA, 2008, http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[IEEE 802.11] Institute of Electrical and Electronics Engineers, Part 11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications, 2007, http://standards.ieee.org/getieee802/download/802.11-2007.pdf

[ISi-VPN] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Reihe zur Internet-Sicherheit: Virtual Private Network, 2009, http://www.bsi.bund.de/fachthem/sinet/

[ISi-Web-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Reihe zur Internet-Sicherheit: Sichere Nutzung von Web-Angeboten, 2008, http://www.bsi.bund.de/fachthem/sinet/

[ISi-Web-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicheres Bereitstellen von Web-Angeboten, 2008, http://www.bsi.bund.de/fachthem/sinet/

[ISi-Fern] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sicherer Fernzugriff auf lokale Netze, in Bearbeitung, http://www.bsi.bund.de/fachthem/sinet/