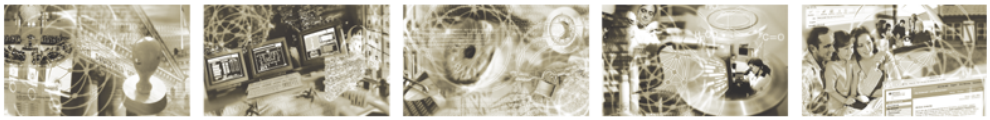
Bundesamt
für Sicherheit in der
Informationstechnik



Sicheres Bereitstellen von Web-Angeboten (ISi-Web)

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

Vervielfältigung und Verbreitung

Bitte beachten Sie, dass das Werk einschließlich aller Teile urheberrechtlich geschützt ist.
Erlaubt sind die Vervielfältigung und Verbreitung zu nicht-kommerziellen Zwecken, insbesondere zu Zwecken der Ausbildung, Schulung, Information oder hausinternen Bekanntmachung, sofern sie unter Hinweis auf die ISi-Reihe des BSI als Quelle erfolgen.
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
© Bundesamt für Sicherheit in der Informationstechnik 2008

Inhaltsverzeichnis

1 Leitlinie zum sicheren Bereitstellen von Web-Angeboten....5
1.1 Management Summary....5
1.2 Einführung und Überblick....6
1.2.1 Anwendungsszenarien für die Bereitstellung von Web-Angeboten....6
1.2.2 Grundlagen der sicheren Bereitstellung von Web-Angeboten....7
1.3 Wesentliche Ergebnisse der Gefährdungsanalyse....10
1.4 Wesentliche Empfehlungen....12
1.5 Fazit....15
2 Glossar....16
3 Stichwort- und Abkürzungverzeichnis....22
4 Literaturverzeichnis....25

1 Leitlinie zum sicheren Bereitstellen von Web-Angeboten

Das Web ist in sehr kurzer Zeit zu einem der wichtigsten Dienste des Internets geworden. Es speichert und vernetzt Informationen aus der ganzen Welt. Für Verwaltung und Wirtschaft ist es inzwischen nahezu unentbehrlich geworden. Auch das Web wird leider von Angreifern missbraucht, um in die Systeme der Benutzer einzudringen, um Informationen zu verfälschen oder um zu betrügen. Der Inhalte der vorliegenden Leitlinie basiert auf den Erkenntnissen der Studie „Sicheres Bereitstellen von Web-Angeboten“ [ISi-Web-Server]. In der Studie werden einerseits die wesentlichen Gefährdungen und andererseits die wichtigsten Sicherheitsempfehlungen beschrieben, um Web-Angebote sicher bereitstellen zu können.

1.1 Management Summary

Viele Wirtschaftsunternehmen und Behörden stellen heute Web-Angebote im Internet weltweit zur Verfügung. Sie öffnen ihre Dienstleistungen somit für eine große Anzahl von Benutzern. Gleichzeitig können aber auch Angreifer Schwachstellen der Web-Angebote ausnutzen, um unberechtigterweise Daten auszulesen, zu verändern oder den Betrieb der Dienste zu stören. Immer häufiger werden schlecht abgesicherte Web-Seiten manipuliert und missbraucht. So können auf den Rechnern der Benutzer Schadprogramme eingeschleust werden. Die infizierten Rechner werden in sogenannten Botnetzen zusammengefasst. Diese bestehen in der Regel aus Tausenden von infizierten Rechnern und können wiederum für Angriffe auf Web-Angebote, Erpressungen und das Versenden von Spam verwendet werden. Die Folgen eines erfolgreichen Angriffs auf ein Web-Angebot können weitreichend sein. Neben erheblichen finanziellen Schäden muss der Web-Seiten-Anbieter auch mit einem Image-Verlust rechen. Daher ist es für jeden Anbieter unverzichtbar, seine Web-Angebote angemessen zu schützen.

Wesentliche Grundlage zum Aufbau eines sicheren Web-Angebots ist die Absicherung der Anbindung an das Internet und der eingesetzten Netzwerktechnik. Die erforderlichen Absicherungsmaßnahmen sind in der BSI-Studie „Sichere Anbindung von lokalen Netzen an das Internet“ [ISi-LANA] beschrieben. Diese müssen jedoch durch zusätzliche Maßnahmen zum Schutz des Web-Angebots ergänzt werden, um eine ausreichende Sicherheit zu gewährleisten.

Die Studie „Sicheres Bereitstellen von Web-Angeboten“ behandelt ausführlich die besonderen Gefährdungen, die bei der Bereitstellung von Web-Angeboten beachtet werden müssen, und stellt entsprechende Gegenmaßnahmen vor. Im Mittelpunkt steht eine Grundarchitektur für den normalen Schutzbedarf, mit der alle relevanten Gegenmaßnahmen abgedeckt sind. Um diese Architektur flexibel an die Größe der Infrastruktur und individuellen Schutzanforderungen anpassen zu können, stellt die Studie zusätzlich erweiterte oder alternative Maßnahmen vor. Auch einem erhöhten Schutzbedarf kann so Rechnung getragen werden. Die vorliegende Leitlinie basiert auf dieser Studie und fasst die wichtigsten Gefährdungen und Gegenmaßnahmen zusammen.

Die Grundarchitektur beschreibt die Anordnung und Absicherung der verschiedenen zum Web-Angebot gehörenden Systeme.

- Der Web-Server nimmt die Anfragen der Benutzer entgegen. Er wird durch einen Paketfilter vor Angriffen geschützt.
- Zum Bereitstellen vieler Dienstleistungen wird eine Web-Anwendung benötigt. Damit können insbesondere Web-Angebote realisiert werden, die über ein statisches Informationsangebot

hinausgehen. Da die Web-Anwendung häufig anfällig für Schwachstellen ist, wird sie auf ein separates System ausgelagert, das über den Web-Server angesprochen werden kann und das durch einen eigenen Paketfilter abgesichert ist.

- Die Web-Anwendung als eine der zentralen Komponenten wird durch ein robustes Design geschützt. Ein- und Ausgaben müssen gefiltert werden, um Angriffe frühzeitig abzuwehren. Auf den Einsatz Aktiver Inhalte in den Web-Angeboten sollte verzichtet werden, um die Benutzer nicht unnötigen Gefahren auszusetzen.
- Viele Web-Angebote generieren auf der Basis vertraulicher Daten individuelle Antworten für die Benutzer. Dazu werden z. B. Kreditkartendaten, Daten zur Benutzer-Authentisierung oder Produktinformationen benötigt. Die Systeme, die diese Daten beinhalten, und ggf. weitere erforderliche Hintergrundsysteme werden in einer separaten Sicherheitszone aufgestellt. Ein Paketfilter stellt sicher, dass nur die Web-Anwendung Zugriff auf die Hintergrundsysteme erhält.
- Aus dem internen Netz wird auf das Web-Angebot über einen eigenen Web-Server zugegriffen. Hierüber kann das Web-Angebot auch gepflegt werden.
- Der Logging-Server protokolliert die sicherheitsrelevanten Aktionen oder sammelt die zu Abrechnungszwecken notwendigen Daten. Das Web-Angebot ist in der Grundarchitektur in ein umfassendes Patch-Management eingebunden, um Schwachstellen schnellstmöglich zu schließen. Daneben werden alle Benutzereingaben sorgfältig vor der Übergabe an die Web-Anwendung überprüft.

Die diesem Dokument zugrunde liegende Studie „Sicheres Bereitstellen von Web-Angeboten“ gibt darüber hinaus Empfehlungen für den sicheren Betrieb, die Konfiguration und für die Beschaffung der für das Web-Angebot notwendigen Systeme. Insgesamt lässt sich damit ein angemessener Schutz für den normalen oder hohen Schutzbedarf umsetzen.

1.2 Einführung und Überblick

Das Internet hat seinen Ursprung in einem überschaubaren, weitgehend geschlossenen Netz, das anfangs nur einige wenige Forschungseinrichtungen miteinander verbunden hat. Die so vernetzten Teilnehmer konnten einander zu Beginn im Wesentlichen vertrauen. Ziel der Entwicklung war ein ausfallsicheres Netz. Bei der Konzeption der Internet-Basistechniken spielten seinerzeit deswegen Sicherheitsaspekte wie Vertraulichkeit und Integrität hingegen nur eine untergeordnete Rolle. Durch die Öffnung des Netzes, seine weltumspannende geografische Ausweitung und seine enorm gestiegene wirtschaftliche und gesellschaftliche Bedeutung hat sich die Bedrohungslage jedoch grundlegend geändert. Die stetig wachsenden Bedrohungen betreffen vermehrt auch die Web-Angebote, wie z. B. Internet-Banking und Online-Shops. Daher ist es unverzichtbar, Abwehrmaßnahmen gegen die wachsenden Bedrohungen zu treffen. Ein Beispiel für eine solche Bedrohung ist die Manipulation der Inhalte eines Web-Auftritts, die unter Umständen zu einem schweren Ansehensverlust führen kann.

1.2.1 Anwendungsszenarien für die Bereitstellung von Web-Angeboten

Web-Angebote zählen heute zu den wichtigsten Diensten des Internets. Neben der Bereitstellung von statischen Inhalten, die von allen Benutzern weltweit abgerufen werden können, gibt es Web-Angebote, mit denen die Benutzer dynamisch interagieren können. Diese modernen Web-Angebote ermöglichen nicht nur das anzeigen von Daten, sondern die Daten können auch verändert oder gelöscht werden.

Nachfolgend werden einige Anwendungsszenarien für die Bereitstellung von Web-Angeboten beschrieben:

- *Web-Angebote zur Bereitstellung von Informationsinhalten*: Diese sind eine der häufigsten Varianten und umfassen alle Web-Angebote, die in erster Linie Information zur Verfügung stellen. Darunter fallen beispielsweise die Web-Auftritte von Firmen, Behörden, Zeitungen, Nachrichten-Portalen und Privatpersonen.
- *Web-Angebote zur Bereitstellung von Dienstleistungen aus dem öffentlichen und privaten Bereich*: Der öffentliche Bereich umfasst alle Web-Angebote des E-Governments, die es Benutzern ermöglichen, Behördenwege elektronisch abzuwickeln, wie zum Beispiel Web-Angebote der Bundesministerien. Beispiele aus dem privaten Bereich sind Anwendungen des E-Commerce, wie Internet-Banking-Portale oder Online-Shops.
- *Web-Angebote zur Bereitstellung von Suchdiensten*: Suchdienste sind grundsätzlich ebenfalls Dienstleistungen, werden jedoch auf Grund ihres speziellen Charakters explizit herausgegriffen. Informationen im Internet werden hierbei über eine breite Anzahl von Systemen aufgezeichnet und katalogisiert.
- *Web-Angebote zur Bereitstellung von Plattformen für Interessengemeinschaften*: Neben Informationsbeschaffung und Inanspruchnahme von Dienstleitungen bietet das Internet auch die Möglichkeit des Informationsaustausches zwischen Benutzern. Dies geschieht in Form von Foren, Chats, Blogs und anderen Plattformen, die primär für die Kommunikation zwischen Benutzern ausgelegt sind.

Im Ergebnis ist also festzustellen, dass die Benutzer von den zahlreichen, existierenden Web-Angebote im Internet Gebrauch machen. Es ist daher für die Benutzer von erheblicher Bedeutung, öffentliche Web-Angebote sowohl in einer abgesicherten Infrastruktur zu betreiben als auch vor den zunehmenden Angriffen zu schützen.

1.2.2 Grundlagen der sicheren Bereitstellung von Web-Angeboten

Bei der Nutzung von Web-Angeboten erfolgt der Datenaustausch mit Hilfe verschiedener Kommunikationsprotokolle. Für die Bereitstellung dynamischer Web-Angebote werden unterschiedliche Programmiersprachen und Techniken genutzt. Um Web-Angebote sicher bereitstellen zu können, müssen die Besonderheiten der eingesetzten Techniken beachtet und dafür geeignete Maßnahmen ergriffen werden.

Grundlegende Protokolle und Kommunikationsstandards

Eines der gängigsten Kommunikationsprotokolle im Zusammenhang mit Web-Angeboten ist das Hypertext Transfer Protocol (HTTP), das die Kommunikation zwischen Web-Servern und -Clients regelt. Bei HTTP handelt es sich um ein Klartextprotokoll. Die zwischen Client und Web-Server übertragenen Daten können von einem Angreifer sowohl eingesehen als auch verändert werden. Für eine verschlüsselte Übertragung kann das HTTPS-Protokoll (Hypertext Transfer Protocol Secure) eingesetzt werden. Es basiert auf HTTP und benutzt zur Verschlüsselung die Protokolle SSL (Secure Sockets Layer) oder TLS (Transport Layer Security). Zusätzlich ermöglicht es eine Authentisierung von Client und Server über Zertifikate.

Um weitere Funktionen des Web-Angebotes nutzen zu können, sind auch noch andere Techniken notwendig. Beispielsweise kann mit Hilfe des WebDAV-Protokolls (Web-based Distributed Authoring and Versioning) die Verwaltung von Dateien auf einem entfernten Web-Server erfolgen.

Neben der Kommunikation zwischen Web-Anwendungen und deren Benutzern kommt es durch Service-orientierte Architekturen zunehmend auch zur direkten Kommunikation zwischen Web-Anwendungen unterschiedlicher Dienstanbieter und somit zur gegenseitigen Nutzung von Funktionalitäten. Diese Kommunikation erfolgt in der Regel über sogenannte SOAP-Nachrichten. SOAP ist ein Kommunikationsprotokoll, das den Austausch von Daten zwischen Computersystemen über ein Netz regelt und somit die Nutzung entfernter Dienste erlaubt. Auch bei SOAP handelt es sich um ein Klartextprotokoll, das standardmäßig keine Sicherheitsmechanismen bietet. Einem Angreifer kann es so gelingen, die übertragenen Daten mitzulesen. Dies ist besonders dann relevant, wenn unternehmenskritische Daten mit Hilfe von SOAP über öffentliche Netze übertragen werden.

Grundlegende Techniken und Komponenten

Eine Web-Anwendung stellt den Benutzern Informationen und Funktionen zur Verfügung, die mit Hilfe eines Browsers genutzt werden können. Ähnliche Funktionen bieten Web-Services, jedoch wird in diesem Fall die Ausgabe der Ergebnisse nicht für einen Browser aufbereitet. Die Daten werden vom Web-Service in strukturierter Form zum anfragenden System zurückgeliefert. Web-Anwendungen sind folglich zur direkten Kommunikation mit einem Benutzer ausgelegt, während Web-Services zur Kommunikation zwischen Computersystemen bzw. den darauf betriebenen Programmen verwendet werden.

Eine wesentliche Komponente bei der Bereitstellung von Web-Angeboten ist der Web-Server. Dieser nimmt Anfragen der Benutzer entgegen und liefert entsprechende Antworten an den Client zurück. Bei dynamischen Inhalten leitet der Web-Server allerdings die Anfragen an eine Web-Anwendung weiter, die die entsprechenden Funktionen verarbeitet und die Ergebnisse an den Web-Server zurück liefert. Je nach Art der Anfrage greift die Web-Anwendung auch auf Hintergrundsysteme zu. Dieser Begriff umfasst dabei u.a. Datenbank-Server und Verzeichnis-Server. Während Datenbank-Server für die dauerhafte Speicherung von Daten der Web-Anwendung verwendet werden, dienen Verzeichnis-Server der zentralen Verwaltung von Benutzerdaten. Besonders dort, wo Systeme zum Teil über Jahrzehnte gewachsen sind, liegen oft noch viele Daten in sogenannten Alt-Systemen vor, die zum Teil geschäftskritische Anwendungen beziehungsweise Daten beherbergen. Gelingt einem Angreifer die Kompromittierung einer Web-Anwendung, so besteht die Möglichkeit, sich mit den Hintergrundsystemen zu verbinden und diese anzugreifen.

Programmiersprachen und Frameworks für dynamische Web-Angebote

Für die Bereitstellung dynamischer Web-Angebote stehen unterschiedliche Programmiersprachen zur Verfügung. Eine frühe Methode dynamische Inhalte zu generieren, ist das Common Gateway Interface (CGI), welches es im Wesentlichen erlaubt, Programme auf dem Web-Server aufzurufen. Die Ergebnisse des Aufrufs werden in die Antwort des Web-Servers integriert. Eine ähnliche Funktionalität kann auch durch eine Vielzahl an neueren Technologien erreicht werden. Für jede eingesetzte Technologie müssen Vorkehrungen getroffen werden, um den sichereren Betrieb zu gewährleisten.

Neben bereits verbreiteten Technologien wie CGI und der Skriptsprache PHP haben sich in der jüngeren Vergangenheit auch Java-basierte Frameworks zunehmend etabliert. Mit Java Server Pages (JSP) kann Java-Code in HTML-Seiten integriert werden. Dabei steht mit der Java Enterprise Edition ein Framework zur Verfügung, mit dem umfangreiche Web-Anwendungen erstellt werden können.

Eine ähnliche Funktion bietet auch das .NET-Framework von Microsoft, das sogenannte Active

Server Pages (ASP) verwendet. Ein sehr junges Framework ist AJAX (Asynchronous JavaScript and XML), mit dem versucht wird, den Komfort von lokalen Clients auch bei Web-Anwendungen innerhalb des Browsers zu bieten.

Technologien zur Authentisierung

Bei der Bereitstellung von dynamischen Web-Angeboten ist es häufig erforderlich, einen Benutzer eindeutig zu identifizieren und ihm dadurch entsprechende Rechte zuzuweisen. Für diese Authentisierung stehen unterschiedliche Verfahren zur Verfügung. Meistens wird dabei auf eine Kombination von Benutzername und Passwort gesetzt, welche vor der Nutzung des Web-Angebots angegeben werden muss. Eine der einfachsten Varianten dabei ist die HTTP Basic Authentication, auch wenn sie kaum noch verwendet wird, da sie die Anmeldedaten unverschlüsselt versendet. Im Rahmen der entsprechenden Weiterentwicklung (Digest Authentication) wurde das Problem gelöst, indem das Passwort in eine Prüfsumme einfließt und es einem Angreifer nicht auf einfache Weise möglich ist, das Passwort auszulesen.

Eine weitere, sehr verbreitete Form der Authentisierung ist die sogenannte formularbasierte Authentisierung. Dabei werden die Anmeldedaten vom Benutzer über ein Formular auf der Web-Seite erfragt und an die Web-Anwendung übertragen. Werden die Daten mittels einer gesicherten HTTPS-Verbindung gesendet, ist es für einen Angreifer nur sehr schwer möglich, die Daten auf dem Übertragungsweg im Klartext auszulesen. Eine sehr sichere Authentisierung, welche bisher jedoch noch kaum zum Einsatz kommt, kann mit Hilfe von Zertifikaten erfolgen. Dabei ist für eine Anmeldung an einem System sowohl der Besitz eines gültigen Zertifikats als auch das Wissen des zugehörigen Passworts erforderlich. Eine zertifikatsbasierte Authentisierung setzt allerdings das Vorhandensein einer Public Key Infrastructure (PKI) voraus, die die Zertifikate ausstellt, verwaltet und überprüft.

Um Benutzer von Web-Anwendungen nach einer erfolgreichen Authentisierung beim Aufruf weiterer Seiten wiederzuerkennen, werden häufig Session-IDs verwendet. Session-IDs sind Werte, die nach einem erfolgreichen Login vom Web-Server zum System des Anwenders übertragen und bei erneuten Anfragen wieder an den Web-Server mitgesandt werden. Auf diese Weise erkennt die Web-Anwendung, dass es sich um eine Anfrage eines bereits authentisierten Benutzers handelt. Die Realisierung von Session-IDs kann unterschiedlich erfolgen. So können sie beispielsweise als kleine Textdateien, sogenannte Cookies, auf der Client-Seite abgespeichert oder innerhalb der aufgerufenen URL mitverschickt werden.

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Viele im Zusammenhang mit Web-Angeboten verwendete Technologien sind für eine Reihe von Angriffen anfällig. Die in den folgenden Abschnitten beschriebenen Angriffe können sowohl das Web-Angebot selbst als auch die Benutzer bedrohen. Die Absicherung des Web-Angebots ist daher nicht nur für den Schutz der eigenen Daten und Prozesse unabdingbar, sondern auch notwendig um Schaden von den Benutzern fernzuhalten. Viele der Angriffe, die erst beim Benutzer wirksam werden, indem sie ihm beispielsweise eine gefälschte Seite präsentieren, können nur auf der Seite des Web-Angebots verhindert werden. Grundsätzlich lassen sich die Bedrohungen in die Kategorien „Eindringen in Systeme und Fälschen von Daten“, „Identitätsdiebstahl“ und „Verhindern von Diensten“ (Denial of Service) einteilen.

Eindringen in Systeme und Fälschen von Daten

Diese Gefährundungskategorie fasst alle Angriffe zusammen, mit denen ein Angreifer in Bereiche eindringen kann, für die er keine Zugriffsberechtigungen besitzt. Dabei werden entweder Sicherheitsmaßnahmen überwunden oder systemspezifische Schwachstellen ausgenutzt. Kann ein Angreifer durch eine bestehende Schwachstelle in einem Web-Angebot in ein System eindringen, so stellt das kompromittierte System sodann auch eine Gefährdung für weitere Komponenten dar. Ausgehend vom ursprünglich angegriffenen System können weitere Dienste und Anwendungen Ziele bösartiger Attacken werden. Damit sind auch Angriffe auf Systeme möglich, die ursprünglich für den Angreifer nicht erreichbar waren. Eine besondere Gefährdung geht von Schwachstellen in Standard-Web-Anwendungen aus, da hierfür oftmals Schadprogramme öffentlich zur Verfügung stehen, die auch von einem Angreifer ohne tiefgehende technische Kenntnisse verwendet werden können.

Eine typische Schwachstelle stellt auch die Ausführung von Betriebssystembefehlen über eine Web-Anwendung dar. Werden Benutzereingaben zur Ausführung von Befehlen am Server herangezogen, die Eingaben jedoch nicht ausreichend geprüft, so besteht für einen Angreifer die Möglichkeit, über die Web-Anwendung beliebige Befehle einzuschleusen und auszuführen. Damit kann der Angreifer die Kontrolle über das System übernehmen, sensible Daten auslesen oder die Funktionsfähigkeit beeinträchtigen. Das Eindringen in Systeme kann ebenfalls durch die Ausnutzung von Speichermanagement-Schwachstellen erfolgen. Diese entstehen durch fehlerhafte Programmierung und können von einem Angreifer dahingehend ausgenutzt werden, dass Befehle im Speicher des angegriffenen Systems abgelegt und anschließend ausgeführt werden.

Möglicherweise stehen einem Angreifer Datei-Upload-Funktionalitäten für Angriffe zur Verfügung. Im Falle, dass die übermittelten Dateien nicht auf Dateityp und Inhalt geprüft werden, lassen sich Dateien mit beliebigem Programmcode hochladen, der anschließend auf dem Server ausgeführt wird. Wenn ein unberechtigter Zugriff erlangt wird, können beispielsweise bei einem Online-Shop Daten von Kunden oder Kreditkarteninformationen ausgelesen werden.

Darüber hinaus besteht auch die Möglichkeit, die vom System zur Verfügung gestellten Daten zu fälschen. Dies kann gezielt dazu verwendet werden, um den Web-Auftritt der betroffenen Plattform zu verändern. Ein Angreifer kann etwa aufgrund der unzureichenden Filterung der Benutzereingaben Inhalte einer Datenbank verändern (SQL-Injection-Schwachstelle) und so gefälschte Informationen verbreiten, zum Beispiel indem die Preise bei einem Online-Shop verändert oder Produkte gelöscht werden.

Identitätsdiebstahl

Weitere Gefahren für Web-Angebote liegen im Identitätsdiebstahl. In dieser Kategorie werden alle Gefährdungen zusammengefasst, bei welchen ein Angreifer die Identität eines legitimen Benutzers übernimmt und Aktionen in dessen Namen durchführen kann.

Wie in Abschnitt 1.2.2 bereits beschrieben, identifiziert eine Web-Anwendung einen Benutzer durch eine sogenannte Session-ID. Dabei handelt es sich um einen vom Server generierten Wert, der nach einer erfolgreichen Authentisierung dem Benutzer zugeteilt und bei jeder erneuten Anfrage mit gesandt wird. Gelingt es einem Angreifer, die Session-ID eines Benutzers zu ermitteln, so kann der Angreifer beliebige Aktionen unter Verwendung des betroffenen Benutzerkontos durchführen.

Ein solcher Angriff kann beispielsweise durch eine Cross-Site-Scripting-Schwachstelle in einer Web-Anwendung erfolgen. Dabei übermittelt der Angreifer Script-Code an die anfällige Web-Anwendung. Wird die Eingabe nicht ausreichend gefiltert, so wird der Script-Code beim Abruf der Daten über den Web-Server auf dem Client des Benutzers ausgeführt und kann beispielsweise die Session-ID an den Angreifer übermitteln. Der Angreifer kann auf diese Weise die Identität des Benutzers übernehmen, ohne den entsprechenden Benutzernamen und das Kennwort zu kennen.

Wird die Kommunikation zwischen Client und Web-Server unverschlüsselt durchgeführt und ist ein Angreifer in der Lage, die Kommunikation abzuhören, so können auch die übertragenen Zugangsdaten eingesehen werden. Dadurch ist der Angreifer nicht mehr an eine Session-ID gebunden, sondern kann die erlangten Zugangsdaten beliebige weitere Male verwenden, um Aktionen unter dem Namen des betroffenen Benutzers durchzuführen.

Eine ähnliche Gefahr geht von schwachen Passwörtern aus. Oft wählen Benutzer einfache Passwörter ohne Sonderzeichen oder Zahlen, da diese leicht zu merken sind. Dabei wird jedoch vergessen, dass ein Angreifer mit Hilfe automatisierter Tools sehr viele Passwörter ausprobieren kann. So lassen sich oft schnell die richtigen Zugangsdaten erraten und die Identität des Benutzers übernehmen.

Identitätsdiebstahl kann auch durch sogenannte hybride Phishing-Angriffe erfolgen. Dabei versucht ein Angreifer mit Hilfe gefälschter Nachrichten gültige Anmeldedaten eines Benutzers zu erhalten. Ist ein Angreifer in der Lage (beispielsweise auf Grund einer Cross-Site-Scripting-Schwachstelle) Inhalte des Web-Auftritts zu beeinflussen, so kann er den Benutzer durch eine gefälschte Eingabemaske dazu auffordern, seine Anmeldedaten einzugeben. Im Hintergrund werden die Zugangsdaten an den Angreifer übermittelt, welcher dadurch Zugang zu den betroffenen Benutzerkonten erhält. Obwohl gängige Browser einen Basisschutz gegen Phishing-Angriffe bieten, erfolgt der wirksamste Schutz durch Absicherung des Web-Angebots sowie durch Sensibilisierung der Benutzer.

Verhindern von Diensten

Neben Schwachstellen, welche zum Zugriff auf sensible Informationen ausgenutzt werden können, gibt es Angriffe, die die Verfügbarkeit von Systemen gefährden oder beeinträchtigen. Derartige Schwachstellen sind ebenfalls kritisch, da legitime Benutzer von der Verwendung des Web-Angebots abgehalten werden und dem Anbieter dadurch sowohl ein Image-Verlust, als auch finanzieller Schaden droht.

Wird bei einer Web-Anwendung beispielsweise ein Benutzerkonto nach mehreren fehlgeschlagenen Anmeldeversuchen gesperrt, so kann ein Angreifer durch mehrmalige Falscheingaben legitime Benutzer bewusst permanent aussperren.

Neben der Sperrung von Benutzerkonten kann ein Angreifer auch die Verfügbarkeit eines Web-Angebots vollständig unterbinden. Vielfältige Gründe dafür machen eine Aufzählung aller

Schwachstellen nicht möglich. Ein Beispiel ist eine Endlosschleife in einer Web-Anwendung, welche sämtliche System-Ressourcen wie Speicher oder Festplattenkapazität verbraucht. Das Ausnutzen einer Speicher-Management-Schwachstelle stellt eine weitere Möglichkeit dar, durch die die Web-Anwendung oder ein Hintergrundsystem zum Absturz gebracht wird und den Benutzern nicht mehr zur Verfügung steht.

Ein Schutz gegen solche Angriffe auf die Verfügbarkeit von Diensten kann nur durch sichere Softwareentwicklung erreicht werden. Durch Benutzereingaben darf es einem Angreifer nicht möglich sein, interne Programmvorgänge des Web-Angebots so zu beeinflussen, dass die Funktionsfähigkeit beeinträchtigt wird oder unberechtigte Aktionen durchgeführt werden können.

Eine weitere Gefährdung geht von Distributed Denial of Service (DDoS)-Angriffen aus. Dabei erzeugen viele fremde Rechner gleichzeitig eine hohe Netzlast, sodass das Web-Angebote für legitime Benutzer unerreichbar ist.

1.4 Wesentliche Empfehlungen

Um Web-Angebote ausreichend sicher zur Verfügung stellen zu können, müssen die folgenden Grundprinzipien beachtet und umgesetzt werden:

- *Verzicht auf Aktive Inhalte*: Die meisten Funktionen, die in Web-Angebote mittels Aktiver Inhalte realisiert werden, können auch ohne deren Einsatz umgesetzt werden. Die Benutzer der Web-Angebote sind dann nicht mehr gezwungen in ihrem Browser Aktive Inhalte zuzulassen. Dies erhöht den Schutz der Benutzer, da viele Angriffe Schwachstellen in der Implementierung von Aktiven Inhalten ausnutzen.
- *Kontextsensitive Filterung von Benutzereingaben, Datei-Uploads und Ausgaben*: Alle von einem Benutzer an ein Web-Angebot übermittelten Daten müssen so gefiltert werden, dass sie die Sicherheit und den Betrieb der Anwendung nicht beeinträchtigen oder beeinflussen können. Die Ausgabe des Web-Angebots muss sorgfältig geprüft werden, um zu verhindern, dass manipulierte oder vertrauliche Daten an die Benutzer gesendet werden.
- *Sichere Datenübertragung*: Alle zwischen Client und Web-Server übertragenen vertraulichen Daten müssen in verschlüsselter Form (beispielsweise durch SSL) übermittelt werden.
- *Sichere Authentisierung von Benutzern*: Neben sicheren Passwörtern und der verschlüsselten Übertragung von Anmeldedaten müssen auch die nach der Authentisierung übertragenen Session-IDs sicher erzeugt und behandelt werden.
- *Aktualität durch Patch-Management*: Web-Anwendungen müssen in ein umfassendes Patch-Management eingebunden werden, um Schwachstellen in Standardapplikationen schnellstmöglich beheben zu können.
- *Konfiguration nach dem Minimalprinzip*: Auf Web-Seiten dürfen Benutzern nur jene Funktionen zur Verfügung gestellt werden, welche für die Nutzung unbedingt notwendig sind. Web-Server, Web-Anwendungs-Server und Hintergrundsysteme müssen ebenfalls minimal konfiguriert sein. Dies verringert die mögliche Angriffsfläche und verhindert die Ausnutzung von Schwachstellen in Diensten, welche für einen funktionsfähigen Betrieb nicht zwingend benötigt werden.
- *Absicherung von Hintergrundsystemen*: Zum sicheren Betrieb eines Web-Angebots genügt es nicht, nur den Web-Server vor einem Fremdzugriff zu schützen. Da bei der Bearbeitung von Anfragen auch Hintergrundsysteme, wie beispielsweise Datenbanken, beteiligt sind, müssen alle involvierten Systeme bei der Umsetzung des Sicherheitskonzepts beachtet werden.

Basierend auf den angeführten Prinzipien ergibt sich eine Empfehlung für eine sichere Grundarchitektur, welche für normalen Schutzbedarf zur Umsetzung empfohlen wird (siehe Abbildung 1.1).

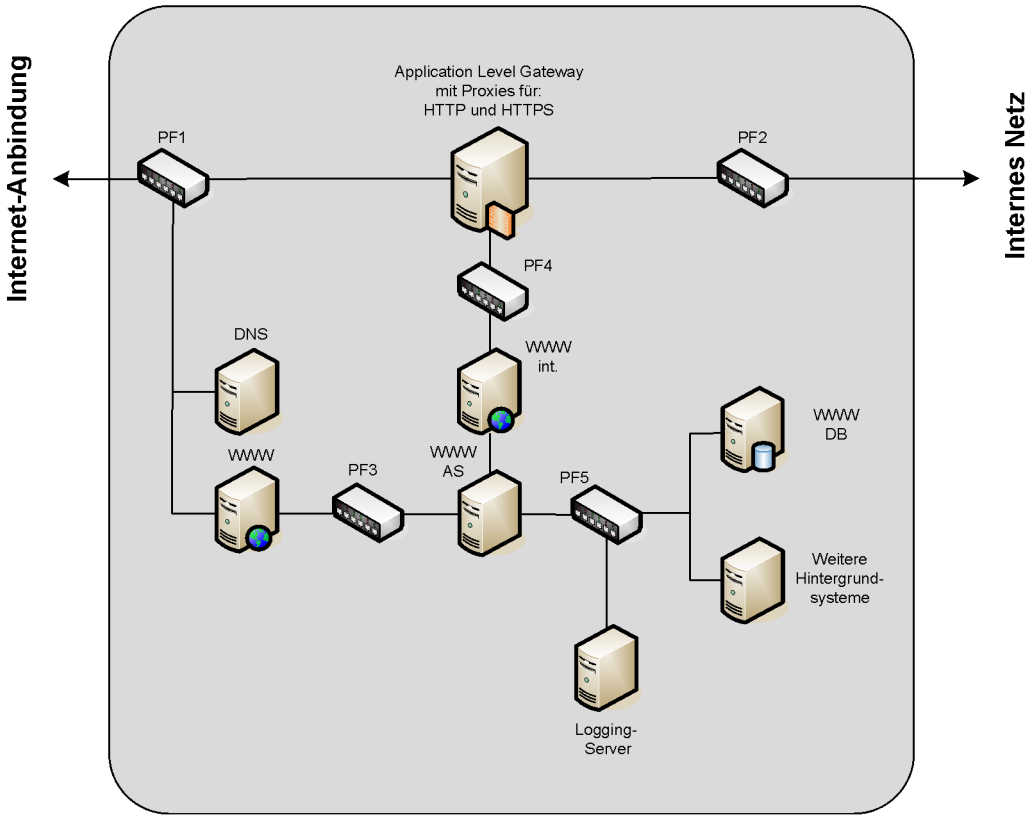


Abbildung 1.1: Grundarchitektur für normalen Schutzbedarf

Die zum Anbieten von Web-Angeboten benötigte Infrastruktur wird mit Hilfe von Paketfiltern (PF) in mehrere Segmente unterteilt. Gelingt es einem Angreifer, Zugriff auf ein System zu erlangen, so wird durch den Einsatz der Paketfilter die Möglichkeit zur Ausnutzung weiterer Schwachstellen eingeschränkt.

Die Web-Anwendung selbst läuft auf einem separierten Web-Anwendungs-Server (WWW AS). Der Zugriff auf diesen Server erfolgt jedoch nicht direkt, sondern ausschließlich über einen Web-Server (WWW). Alle benötigten Hintergrundsysteme, wie z. B. der Datenbank-Server (WWW DB), und der Logging-Server befinden sich in einer weiteren Demilitarisierten Zone (DMZ), die ebenfalls durch einen Paketfilter vom Web-Anwendungs-Server getrennt ist.

Zum Zugriff auf das Web-Angebot aus dem internen Netz steht ein eigener Web-Server mit der Bezeichnung „WWW int.“ zur Verfügung, der sich in derselben DMZ wie der Web-Anwendungs-Server befindet. Dieser Web-Server kann auch genutzt werden, um das Web-Angebot inhaltlich zu gestalten.

Die Wartung der Web-Anwendung erfolgt nur über die Administrationszugänge aus der Management-Zone heraus. Dabei handelt es sich um ein durch Paketfilter abgesichertes Netz, welches ausschließlich zur Administration und Wartung der eingesetzten Systeme verwendet wird. Abbildung 1.2 zeigt den Aufbau der Grundarchitektur für normalen Schutzbedarf gemeinsam mit der zugehörigen Management-Zone.

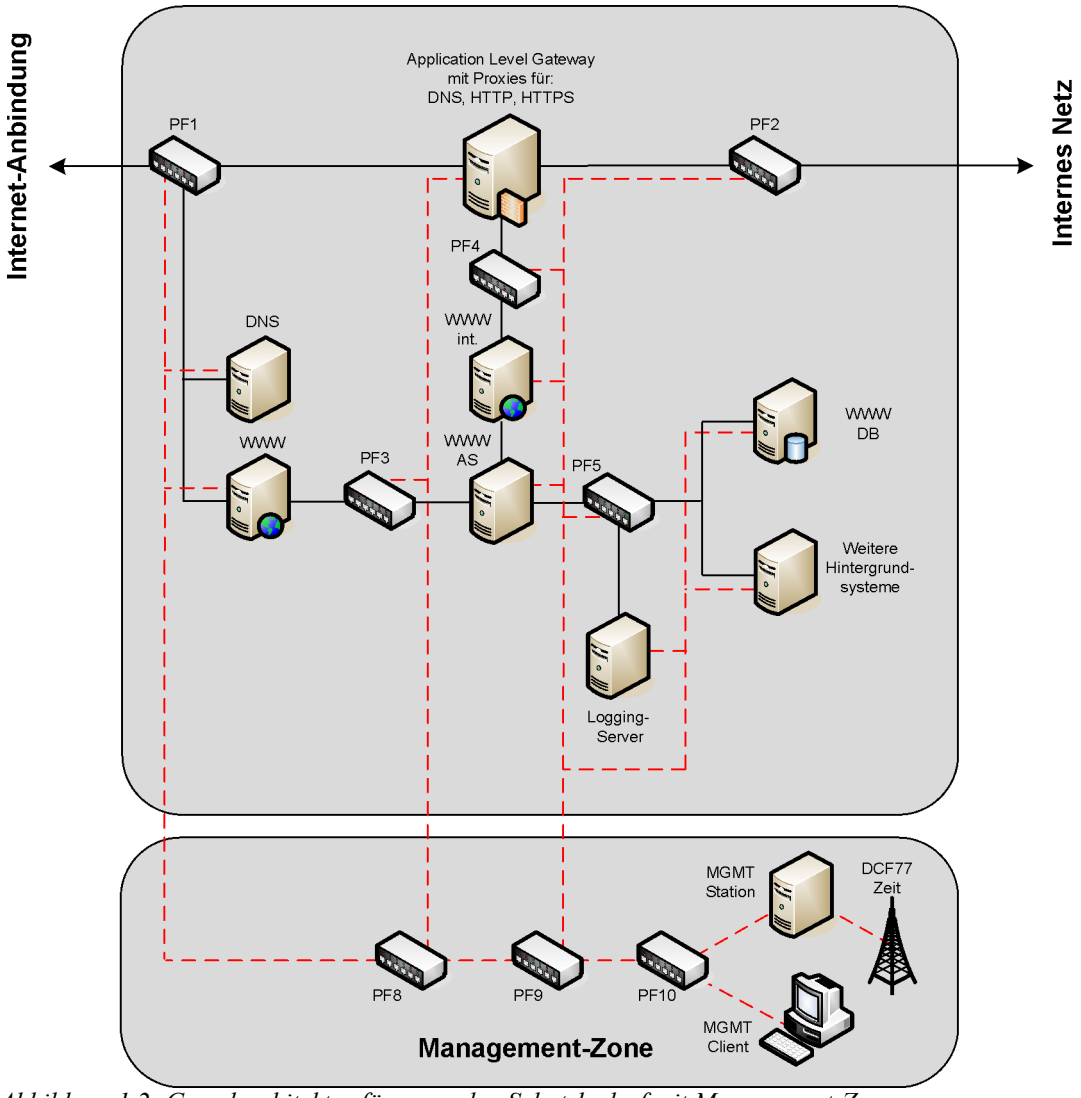


Abbildung 1.2: Grundarchitektur für normalen Schutzbedarf mit Management-Zone

Durch Verwendung einer Management-Zone erfolgt eine vollständige Trennung der Nutzdaten-Schnittstellen von den Management-Schnittstellen der einzelnen Systeme, wodurch die Sicherheit erhöht wird. Fernadministration darf nur möglich sein, wenn sich der Administrator zuvor über eine gesicherte Verbindung von einem sicheren Client in die Management-Zone eingewählt hat. Von dort aus ermöglicht eine zentrale Management-Station die Administration der Systeme über eine gesicherte Verbindung. Die Uhrzeit aller Systeme wird mit Hilfe des Network Time Protocol (NTP) synchronisiert, wobei als Referenzzeitquelle ein DCF77-Empfangsmodul verwendet werden kann.

Aus Sicherheitsgründen sind die Teilsegmente der Management-Zone durch Paketfilter getrennt. Um den Hardware-Aufwand zu reduzieren, besteht bei erhöhtem Risiko die Möglichkeit, einzelne Paketfilter zusammenzulegen.

1.5 Fazit

Web-Angebote bieten Angreifern eine Vielzahl unterschiedlicher Angriffsmöglichkeiten, die für eine erfolgreiche Kompromittierung genutzt werden können. Das größte Gefährdungspotential geht von der Web-Anwendung selbst aus, da diese zum Teil sehr umfangreiche Funktionalitäten und komplexe Schnittstellen bietet. Darüber hinaus dürfen auch die Gefahren nicht vernachlässigt werden, die von unterstützenden Systemen wie Web-Servern oder Hintergrundsystemen ausgehen.

Die hier behandelten Gegenmaßnahmen helfen, die Web-Anwendung sicher zu gestalten. In der Studie „Sicheres Bereitstellen von Web-Angeboten“ [ISi-Web-Server] werden sie näher erläutert und ergänzt. Es werden effiziente und effektive Maßnahmen beschrieben, die auch bei schon bestehenden Umgebungen umgesetzt werden können. Neben den rein technischen Punkten werden auch relevante Aspekte aus den Bereichen Recht und Sicherheitsbewusstsein behandelt, da sie eng mit der Thematik verzahnt sind und somit nicht isoliert betrachtet werden sollten.

Zusammen mit der Absicherung der unteren drei Schichten des TCP/IP-Referenzmodells gemäß dem Modul „Sichere Anbindung von lokalen Netzen an das Internet“ [ISi-LANA] wird somit das sichere Bereitstellen von Web-Angeboten ermöglicht.

2 Glossar

Administrator

Ein Administrator verwaltet und betreut Rechner sowie Computer-Netze. Er installiert Betriebssysteme und Anwendungsprogramme, richtet neue Benutzer-Kennungen ein und verteilt die für die Arbeit notwendigen Rechte. Dabei hat er im Allgemeinen weitreichende oder sogar uneingeschränkte Zugriffsrechte auf die betreuten Rechner oder Netze.

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.

Authentisierung (engl. authentication)

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

Bedrohung (engl. threat)

Eine Bedrohung ist ganz allgemein ein Umstand oder Ereignis, durch das ein Schaden entstehen kann. Der Schaden bezieht sich dabei auf einen konkreten Wert wie Vermögen, Wissen, Gegenstände oder Gesundheit. Übertragen in die Welt der Informationstechnik ist eine Bedrohung ein Umstand oder Ereignis, das die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bedrohen kann, wodurch dem Besitzer der Informationen ein Schaden entsteht.

Benutzer-Kennung (engl. user account)

Die Benutzer-Kennung ist der Name, mit dem sich der Benutzer einem IT-System gegenüber authentisiert. Dies kann z. B. der tatsächliche Name sein, ein Pseudonym, eine Abkürzung oder eine automatisch vergebene Kombination aus Buchstaben oder Ziffern.

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.

CGI (Common Gateway Interface [engl.])

CGI-Programme sind im HTML-Dokument eingebunden und von diesem aus aufrufbar. Sie können selbst HTML-Code erzeugen und an einen Browser senden. CGI wird häufig für die Erstellung von

Gästebüchern, von Formularen und Zählern eingesetzt.

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.

DDoS (Distributed Denial of Service [engl.])

Ein koordinierter DoS-Angriff auf die Verfügbarkeit von IT mittels einer größeren Anzahl von angreifenden Systemen.

DMZ (Demilitarisierte Zone)

Eine DMZ ist ein Zwischennetz, das an Netzübergängen gebildet wird, aber weder zu dem einen, noch zu dem anderen Netz gehört. Sie stellt ein eigenes Netz dar, das nicht so stark gesichert ist wie das eigentlich zu schützende Netz. DMZ werden bei einfachen Sicherheits-Gateways üblicherweise an einer dritten Schnittstelle des Paketfilters erzeugt. Besteht das Sicherheits-Gateway aus Paketfilter - Application-Level Gateway - Paketfilter, dient in der Regel eine weitere Schnittstelle des Application-Level Gateways (ALG) als DMZ-Schnittstelle. Verfügen Paketfilter oder ALG über mehr als drei Schnittstellen, können weitere DMZ gebildet werden.

E-Commerce [engl.]

Electronic Commerce. Handel über das Internet. Unterbereich des E-Business.

Framework [engl.]

Framework (engl. für Rahmenwerk, Fachwerk) ist ein Begriff aus der Software-Technik. Ein Framework gibt eine Anwendungs-Architektur vor.

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.

HTML (Hypertext Markup Language [engl.])

Für Web-Seiten verwendete Auszeichnungssprache, die von allen Browsern verstanden wird.

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 http://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.

Java

Java ist eine Programmiersprache. Häufig wird Java in Form von Java-Applets auf Web-Seiten genutzt. Damit Java-Programme funktionieren, muss auf dem betreffenden Rechner oder im Browser das Java Runtime Environment (JRE) installiert sein. Java zählt zu den Aktiven Inhalten.

JavaScript [engl.]

JavaScript ist eine Programmiersprache, die oft auf Webseiten eingesetzt wird. Mit ihr ist es z. B. möglich, Pop-Up-Fenster zu öffnen, Berechnungen durchzuführen oder Formulareingaben zu überprüfen. JavaScript ist Bestandteil aller neuen Browser. JavaScript zählt zu den Aktiven Inhalten.

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.

Patch [engl.]

Ein Patch (vom englischen "patch", auf deutsch: Flicken) ist ein kleines Programm, das Software-Fehler wie z. B. Sicherheitslücken in Anwendungsprogrammen oder Betriebssystemen behebt.

Phishing [engl.]

Versuch von Betrügern, IT-Anwender irrezuführen und zur Herausgabe von Authentisierungsdaten zu bewegen. Dies wird in den meisten Fällen bei Online-Banking-Verfahren eingesetzt.

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.

Risiko (engl. risk)

Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens.

Schutzbedarf (engl. protection requirements)

Der Schutzbedarf beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

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.

Sicherheitskonzept (engl. security concept)

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

Sicherheitsmaßnahme (engl. saveguard control)

Mit Sicherheitsmaßnahme werden alle Aktionen bezeichnet, die dazu dienen, Sicherheitsrisiken zu steuern und entgegenzuwirken. Dies schließt organisatorische, personelle, technische und infrastrukturelle Sicherheitsmaßnahmen ein. Synonym werden auch die Begriffe Sicherheitsvorkehrung oder Schutzmaßnahme benutzt.

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.

TCP (Transmission Control Protocol [engl.])

Verbindungsorientiertes Protokoll der Transportschicht im TCP/IP-Referenzmodell, welches auf IP aufsetzt.

TLS (Transport Layer Security [engl.])

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

Upload [engl.]

Mit einem Upload werden Daten vom eigenen Computer auf einen Rechner im Netz hochgeladen.

URL (Uniform Resource Locator [engl.])

Adressierungsschema für Dokumente und sonstige Dateien im Internet, bestehend aus Protokoll und Adresse.

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.

XML (Extensible Markup Language [engl.])

Eine Erweiterung der für die Entwicklung von Web-Seiten standardisierten Programmiersprache HTML. Daten können hierin nach vom Programmierer frei zu definierenden Regeln sehr flexibel in bestimmten Formaten dargestellt und so z. B. als Input für eine weiterverarbeitende Software genutzt werden.

Zertifikat

Der Begriff Zertifikat wird in der Informationssicherheit in verschiedenen Bereichen mit unterschiedlichen Bedeutungen verwendet. Zu unterscheiden sind vor allem das IT-Grundschutz-Zertifikat, Schlüsselzertifikate, IT-Sicherheitszertifikate und CC-Zertifikate.

3 Stichwort- und Abkürzungverzeichnis

Administrator....14, 16
Ajax (Asynchronous JavaScript and XML)....9
Aktive Inhalte....
  Java....8, 18
  JavaScript....9, 18
ALG (Application-Level Gateway)....17
Anwendungsschicht....18
Applet....18
AS (Applikations-Server)....13
ASP (Active Server Pages)....8f.
Auszeichnungssprache....17
Authentisierung....6f., 9, 11f., 16, 19
Bedrohung....6, 10, 16f., 20
Benutzer-Kennung....11, 16
Betriebssystem....16f., 19
Bit (Binary Digit)....18
BMI (Bundesministerium des Innern)....16
CC (Common Criteria)....21
CGI (Common Gateway Interface)....8, 16
Chiffrat....21
DB (Database)....13
DCF77....14
DDoS (Distributed Denial of Service)....12, 17
DMZ (Demilitarisierte Zone)....13, 17
DoS (Denial of Service)....10, 12, 17
E-Business....17
E-Commerce....7, 17
E-Mail (Electronic Mail)....2, 20
Framework....8f., 17
Gefährdung....5, 10ff., 16f.
  DDoS (Distributed Denial of Service)....12, 17
  DoS (Denial of Service)....10, 12, 17
  Phishing....11, 19
  Spam....5, 20
Gefährdungsanalyse....3, 10
Grundarchitektur....5f., 13
Hardware....14, 17, 20
HTML (Hypertext Markup Language)....8, 16ff., 21
HTTP (Hypertext Transfer Protocol)....7, 9, 18
HTTPS (HTTP secure)....7, 9, 18
Hyperlink....18
Hypertext....7, 17f.
ID (Identifikations-Nummer)....9, 11f.
Informationssicherheit....21
INFOSEC (Information Security)....16
Integrität....6, 16, 18
Internet-Schicht....18

IP (Internet Protocol)....15, 18ff.
IPv4 (Internet Protocol Version 4)....18
ISi (Internet-Sicherheit)....
ISi-L (ISi-Leitfaden)....1
ISi-Reihe....2
IT-Grundschutz....21
IT-Sicherheit....18, 21
Informationssicherheit....21
Integrität....6, 16, 18
Verfügbarkeit....11f., 16f., 21
Vertraulichkeit....6, 16, 21
IT-Sicherheitszertifikat....21
Java....8, 18
JavaScript....8f., 18
JRE (Java Runtime Environment)....18
JSP (Java Server Pages)....8
NTP (Network Time Protocol)....14
Online-Shop....6f., 10
Paketfilter....5f., 13f., 17, 19
Passwort....9, 11f., 19
Patch....6, 12, 19
Phishing....11, 19
PHP (Hypertext Preprocessor)....8
PKI (Public Key Infrastructure)....9, 19
Protokoll....
HTTP (Hypertext Transfer Protocol)....7, 9, 18
HTTPS (HTTP secure)....7, 9, 18
IP (Internet Protocol)....15, 18ff.
IPv4 (Internet Protocol Version 4)....18
SOAP....8
SSL (Secure Sockets Layer)....7, 12, 18, 20
TCP (Transmission Control Protocol)....15, 18ff.
TLS (Transport Layer Security)....7, 18, 20
Prüfsumme....9, 19
Risiko....14, 19
RSA (Rivest, Shamir, Adleman Public Key Encryption)....20
Schadprogramm....5, 10, 17
Virus....17
Schlüsselzertifikat....21
Schutzbedarf....5f., 13, 19
Schwachstelle....5f., 10ff., 17, 20
Sicherheits-Gateway....17
ALG (Application-Level Gateway)....17
Paketfilter....5f., 13f., 17, 19
Sicherheitskonzept....12, 20
Sicherheitsmaßnahme....10, 20
Sicherheitszone....6
Skript....8
SOAP....8
Spam....5, 20

SQL (Structured Query Language).....10
SSL (Secure Sockets Layer).....7, 12, 18, 20
TCP (Transmission Control Protocol).....15, 18ff.
TCP/IP-Referenzmodell.....
Anwendungsschicht.....18
Internet-Schicht.....18
Transportschicht.....19f.
TLS (Transport Layer Security).....7, 18, 20
Transportschicht.....19f.
Upload.....10, 12, 20
URL (Uniform Resource Locator).....9, 18, 21
Verfügbarkeit.....11f., 16f., 21
Verschlüsselung.....
Chiffrat.....21
Vertraulichkeit.....6, 16, 21
Virus.....17
Web-Anwendung.....5f., 8ff., 15
WWW (World Wide Web).....13, 16, 18
XML (Extensible Markup Language).....9, 21
Zertifikat.....7, 9, 21
IT-Sicherheitszertifikat.....21

4 Literaturverzeichnis

[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-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Schriftenreihe zur Internet-Sicherheit: Sichere Anbindung lokaler Netze an das Internet, 2007, http://www.bsi.bund.de/fachthem/sinet/