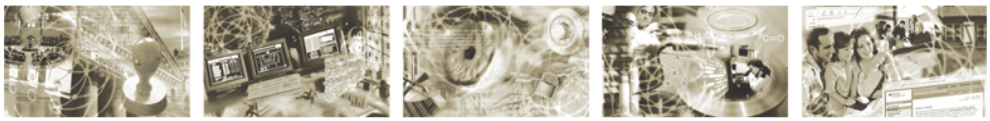
Bundesamt
für Sicherheit in der
Informationstechnik



BSI-Standards zur Internet-Sicherheit (ISi-Reihe)

Sichere Nutzung von Webangeboten (ISi-Web-Client)

Version 1.2 vom 21. September 2015

Vervielfältigung und Verbreitung

Bitte beachten Sie, dass das Werk einschließlich aller Teile urheberrechtlich geschützt ist.

Erlaubt sind 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 2015

Inhaltsverzeichnis

1 Einleitung....5

2 Grundlagen....6

2.1 Terminologie....6
2.1.1 Hypertext....6
2.1.2 WWW....6
2.1.3 Webseiten....6
2.1.4 HTML....6
2.1.5 CSS....7
2.1.6 Aktive Inhalte....7
2.1.7 URL....7

2.2 Komponenten....8
2.2.1 Webserver....8
2.2.2 Clients....9
2.2.3 Browser....9
2.2.4 ReCoBS....12
2.2.5 Proxy-Server....12

2.3 Protokolle....13
2.3.1 HTTP....13
2.3.2 TLS....15

3 Sichere Grundarchitektur für normalen Schutzbedarf....16

3.1 Internes Netz....17
3.1.1 Clients....17

3.2 Internet-PC-Zone....17

3.3 Sicherheits-Gateway....19
3.3.1 Anbieten eigener Internet-Dienste....20

3.4 Internet-Anbindung....20

3.5 Protokollierung....21

3.6 Organisatorische Regelungen....21
3.6.1 Regelung der Nutzung des Web....21
3.6.2 Freischaltung von aktiven Inhalten in vertrauenswürdigen Webangeboten....22
3.6.3 Schulungen für sicherheitsbewusste Web-Nutzung....22

4 Komponenten auswählen, konfigurieren und betreiben (normaler Schutzbedarf)....23

4.1 Grundanforderungen an ein sicheres Produkt....23
4.1.1 Internes Netz....23
4.1.2 Internet-PC-Zone....24
4.1.3 Sicherheits-Gateway....24

4.2 Konfiguration der Komponenten....26
4.2.1 Client....26
4.2.2 Internet-PC-Zone....27
4.2.3 Sicherheits-Gateway....28

4.3 Grundvorgaben für einen sicheren Betrieb....29

5 Gefährdungen und Empfehlungen mit Varianten für normalen und hohen Schutzbedarf....31

5.1 Schadprogramme....31
5.1.1 Drive-By Downloads....31
5.1.2 Downloads....33
5.1.3 Ausnutzung von Software-Schwachstellen....33

5.2 Aktive Inhalte....34
5.2.1 Java-Applets....34
5.2.2 ActiveX-Controls und COM-Komponenten....35
5.3 Vortäuschen vertrauenswürdiger Web-Inhalte....38
5.3.1 Cross-Site Scripting (XSS) und HTML-Injection....38
5.3.2 Clickjacking....39
5.3.3 URL-Spoofing....41
5.3.4 HTTP-Response Splitting und Web-Cache Poisoning....41
5.3.5 Cross-User Defacement....43
5.3.6 Redirection-Attack....43
5.3.7 Anti-DNS-Pinning....44
5.4 Identitätsdiebstahl und User-Tracking....44
5.4.1 Phishing....44
5.4.2 Session Hijacking....45
5.4.3 Cross-Site Request Forgery (CSRF) / Session Riding....46
5.4.4 Profilbildung....47
5.4.5 Werbebanner....48
5.4.6 Passwortdiebstahl aus dem Passwortmanager....49
5.5 Umgehen des Sicherheits-Gateways....50
5.5.1 HTTP-Request Smuggling....50
5.5.2 Encoding....50
5.6 Verschlüsselung und Zertifikate....51
5.6.1 Abhören unverschlüsselter Verbindungen....51
5.6.2 Fälschung von Zertifikaten....51
5.6.3 SSL-Downgrade....52
5.7 Sonstige....52
5.7.1 Prefetching....52
5.7.2 Plug-Ins....52
6 Fazit....54
7 Anhang....55
7.1 Literaturverzeichnis....55
7.2 Abkürzungsverzeichnis....56
7.3 Varianten der Grundarchitektur....58
7.3.1 Kleines Unternehmen....59
7.3.2 Mittelgroßes Unternehmen....61
7.3.3 Großes Unternehmen....63

1 Einleitung

BSI-Standards zur Internet-Sicherheit

Die BSI-Standards zur Internet-Sicherheit (ISi-Reihe) befassen sich mit der Sicherheit von IP-Netzen und -Diensten. Die ISi-Reihe richtet sich an alle Personen in Behörden und Unternehmen, die sich mit diesem Themenfeld beschäftigen und bietet ihnen dazu umfassende Informationen. Sie erläutert, mit welchen Gefährdungen zu rechnen ist und gibt Empfehlungen zu vorbeugenden Sicherheitsmaßnahmen. Insbesondere unterstützt sie bei der Planung und Realisierung von IP-Netzen und IP-Diensten. Als Ausgangspunkt dient dazu eine sichere Grundarchitektur, die sich mittels Varianten an die individuellen Gegebenheiten anpassen lässt.

Das Themenfeld lässt sich in verschiedene Bereiche untergliedern. Zu den wichtigen Bereichen, die in der ISi-Reihe behandelt werden, zählen u. a. Aufbau und Anbindung eines Netzes an das Internet sowie Nutzung und Bereitstellung von E-Mail- oder Web-Diensten. Jeder dieser Bereiche wird in einem eigenen Modul behandelt. Jedes Modul besteht aus mehreren Teilen und wendet sich zielgruppenspezifisch an Entscheidungsträger (mit dem Leitfaden ISi-L) und an diejenigen, die mit der Umsetzung der Sicherheit betraut sind (Studien ISi-S sowie Checklisten ISi-Check). Die vorliegende Studie ISi-Web-Client befasst sich mit den Aspekten der Sicherheit bei der Nutzung von Webangeboten.

Zusammen mit der Studie zum Sicheren Bereitstellen von Webangeboten [ISi-Web-Server] können bestehende Systeme in Hinblick auf den Dienst Web abgesichert oder auch neue Dienste konzipiert, umgesetzt und betrieben werden. Hierzu sind die Checklisten, die ergänzend zu jeder Studie veröffentlicht werden, eine praktische Hilfe.

Sichere Nutzung von Webangeboten

Fast alle Behörden und Unternehmen nutzen das Web zur Informationssuche oder um auf Dienstleitungsangebote zugreifen zu können. Allerdings können Angreifer Schwachstellen in Browsern oder Webangeboten nutzen, um unberechtigterweise Daten auszulesen, zu manipulieren oder schlimmstenfalls in das interne Netz einzudringen. Der Schutz der Clients vor solchen Angriffen sollte für alle Beteiligten eine hohe Priorität besitzen.

ISi-Web-Client zeigt auf, wie sich Behörden und Unternehmen vor diesen Gefahren schützen können. Die Grundlagen der Webnutzung werden in Abschnitt Fehler: Referenz nicht gefunden beschrieben. Anschließend zeigt Abschnitt 3, wie die Clients, die Browser und das interne Netz aufgebaut werden sollten, um dem Schutz der fundamentalen Grundwerte Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität Rechnung zu tragen. Empfehlungen zur Auswahl, Konfiguration und zum Betrieb der notwendigen Komponenten werden in Abschnitt 4 gegeben. Die Anforderungen an die Sicherheit variieren von Organisation zu Organisation. Um hier individuelle Anpassungen vornehmen zu können, beispielsweise für hohen Schutzbedarf oder an die Größe und Komplexität der Lösung, werden Varianten vorgestellt, bewertet und Gefährdungen zugeordnet (Abschnitt 5).

2 Grundlagen

Den meisten Web-Nutzern genügt es, im Browser eine Web-Adresse einzugeben und sich den Inhalt der Webseite anzeigen zu lassen. Das technische Zusammenspiel zwischen Client und Servern bleibt dem Benutzer im Normalfall verborgen. Um die Gefährdungen, die bei der Webnutzung entstehen, verstehen zu können und um sich effizient davor zu schützen, ist ein gewisses Verständnis für die Abläufe im Hintergrund notwendig. In diesem Abschnitt werden daher die Grundlagen der Nutzung von Webangeboten behandelt und die verwendeten Protokolle, Techniken und Komponenten beschrieben.

2.1 Terminologie

Im folgenden Abschnitt werden die wichtigsten Begriffe im Umfeld der Nutzung von Webangeboten erklärt, die für das Verständnis grundlegend sind.

2.1.1 Hypertext

Der Begriff Hypertext wurde 1965 von Ted Nelson geprägt. Er bezeichnet Informationen, die nichtlinear durch Verweise miteinander verbunden sind. Das Ziel ist es, beim Verfassen von Texten auf bereits vorhandene Informationen zurückzugreifen und diese nicht komplett wiederzugeben, sondern nur zu erweitern. Das erfolgt durch Verknüpfen der ursprünglichen Inhalte mit der Erweiterung über sogenannte Hyperlinks (kurz Links).

2.1.2 WWW

Das World Wide Web (kurz Web oder WWW) ist ein Hypertext-System. Dokumente im Web werden im Allgemeinen als Webseiten oder Internetseiten bezeichnet. Jeder Webseite ist ein Uniform Resource Locator (URL) zugeordnet, über den das Dokument abgerufen werden kann (siehe Abschnitt 2.1.7). Der Transport von Dokumenten über das Internet erfolgt über das Hypertext Transfer Protocol (HTTP).

2.1.3 Webseiten

Webseiten sind hierarchisch aufgebaute Dokumente, die typischerweise in der Dokumentenbeschreibungssprache HTML verfasst sind. Sie können neben Texten, Tabellen, Bildern, Videos und anderen Medienelementen auch ausführbare Skripte beinhalten. Webseiten können entweder statisch sein oder erst nach einer Anfrage dynamisch generiert werden.

2.1.4 HTML

Die Hypertext Markup Language (HTML) ist eine sogenannte Auszeichnungssprache, die zum Strukturieren und Beschreiben von Dokumenteninhalten in Webseiten verwendet wird. Mit Hilfe von Auszeichnungen (engl. tag) werden Inhalte bestimmten Kategorien zugeordnet, etwa `<script>` für Skripte, oder strukturiert, z. B. mit `<p>` für Paragraph. Tags werden zur inhaltlichen Auszeichnung verwendet, können jedoch auch mit typografischen Auszeichnungen angereichert werden (siehe hierzu auch Abschnitte 2.1.5 CSS).

Der Nachfolger des bereits 1999 veröffentlichten HTML 4.01 ist XHTML 1.0, das auf einem strikteren XML-Format basiert und dadurch leichter maschinell zu verarbeiten ist. Der aktuelle Standard HTML5 weicht jedoch wieder von der strengen XML-Strukturierung ab und räumt dem Web-Entwickler größere Freiräume bezüglich der Auszeichnung ein.

2.1.5 CSS

Die Mischung von inhaltlichen und typografischen Auszeichnungen in HTML wird immer wieder kritisiert. Um Design und Inhalt von Webseiten zu trennen, können Cascading-Style-Sheets (CSS) verwendet werden. CSS-Dateien definieren die Formatierung unterschiedlicher Dokument-Teile und können in HTML-Seiten eingebunden werden. Zur Änderung der Darstellung der Webseite kann die CSS-Datei zentral angepasst oder eine andere CSS-Datei eingebunden werden. Dadurch entfallen aufwändige Überarbeitungen einzelner Webseiten.

2.1.6 Aktive Inhalte

Durch aktive Inhalte lassen sich interaktive Funktionen in Webangeboten umsetzen. Hierzu wird Programmcode an den Client übertragen und dort im Browser ausgeführt. Die verschiedenen Techniken, die unter dem Oberbegriff „aktive Inhalte“ zusammengefasst werden, unterscheiden sich unter anderem durch die Art, wie sie in eine HTML-Seite integriert werden. Skriptsprachen wie JavaScript, JScript oder VBScript werden im Textformat direkt in den HTML-Code eingefügt oder in einer aus dem HTML-Code aufgerufenen Datei abgelegt. Eine weitere Möglichkeit, ausführbaren Code in eine HTML-Seite zu integrieren, ist im HTML-Code referenzierte und vorkompilierte Programmmodule wie Java-Applets oder ActiveX-Controls aufzurufen.

Barrierefreiheit

Im Allgemeinen sind aktive Inhalte schlecht für die Barrierefreiheit, da sie im Gegensatz zu reinem Text im Normalfall nicht alternativ aufbereitet werden können (beispielsweise als Audio für Menschen mit eingeschränkter Sehkraft). Häufig ist es möglich, vergleichbare Funktionen auch mit dynamischen oder sogar statischen Inhalten bereitzustellen.

Verbreitung

JavaScript ist die einzige Technik für aktive Inhalte, die nativ von allen gängigen Browsern unterstützt wird, und ist daher entsprechend weit verbreitet. Alle anderen Techniken werden nur in wenigen Browsern unterstützt (z. B. Visual Basic Script oder Dart) oder benötigen zusätzliche Plug-Ins (siehe Abschnitt 2.2.3.3). Gängig sind Plug-Ins für Adobe Flash mit seiner Skriptsprache ActionScript und im Privatbereich zunehmend auch für Microsoft Silverlight, da viele Videostreaming-Dienste auf dieser Technik aufsetzen. Die früher gängigen Java-Applets haben heute nur eine nachgeordnete Bedeutung.

2.1.7 URL

Um Inhalte im Web eindeutig bezeichnen zu können, kommen Unified Resource Locators (URLs) zum Einsatz. Diese sind eine Unterart von Unified Resource Identifier (URIs, [RFC 3986]) und beschreiben einen Ort, an dem eine Ressource gespeichert ist. Tabelle 1 erläutert die Komponenten einer URL anhand des folgenden Beispiels:

```
http://benutzer:passwort@www.domain.tld:80/verzeichnis/datei.htm?
var1=wert1&var2=wert2#Anker
```

Beispiel 1: Beispielhafte URL und ihre Komponenten

URL-Teil (Beispiel)	*Bedeutung*	*Anmerkungen*
http://	Protokoll	Als Transportprotokoll werden im Web HTTP und HTTPS genutzt. Da URIs jedoch auch für andere Dienste im Internet verwendet werden, sind noch weitere Protokolle (z. B. ftp://) definiert.
benutzer:passwort@	Benutzername und Passwort	Diese Art der Authentifizierung ist seit [RFC 7230] überholt und darf nicht mehr verwendet werden.
www.domain.tld	Domain bzw. IP-Adresse	Domain-Namen bzw. IP-Adresse des Servers, auf dem die angeforderten Inhalte gespeichert sind.
:80	Port	Der Port, auf dem der Webserver auf eingehende TCP-Verbindungen wartet.
/verzeichnis/datei.htm	Pfad	Der Pfad zu der Ressource, die beim Webserver angefragt wird. Normalerweise handelt es sich dabei um eine Datei. Manche Web-Umgebungen übergeben im Pfad jedoch auch Variablen an den Webserver, die ähnlich dem „Abfrage“-Teil behandelt werden.
?var1=wert1&var2=wert2	Abfrage (Query String)	Dynamische Webseiten ändern ihre Ausgabe auf Basis der übergebenen Benutzereingaben. Über den URL-Teil „Abfrage“ besteht die Möglichkeit, benutzerdefinierte Werte an den Webserver zu übermitteln. Der Abfrageteil wird dabei durch ein Fragezeichen (?) vom Pfad-Teil abgegrenzt. Im Normalfall bestehen die Werte aus einem Variablennamen und einem Wert. Es können beliebig viele Variable/Wert-Paare an den Webserver übermittelt werden, indem diese durch ein kaufmännisches Und (&) voneinander getrennt werden.
#Anker	Sprungmarke	Innerhalb einer Seite kann eine Sprungmarke („Anker“) definiert werden, die sich direkt ansprechen lässt. Die meisten Browser (ein Gegenbeispiel stellt Opera dar) übertragen diesen Teil der URL nicht an den Webserver, sondern lesen lediglich die HTTP-Antwort ein und setzen die Bild-Position so, dass der referenzierte Teil der Seite ganz oben im Browser-Fenster angezeigt wird.

Tabelle 1: Aufbau einer URL zur Referenzierung von Inhalten im Web

2.2 Komponenten

Das World Wide Web ist ein Internet-Dienst und nutzt als solcher die Infrastruktur des Internets. Die Komponenten im Internet, die speziell für das Bereitstellen und Nutzen von Webangeboten benötigt werden, sind im folgenden Abschnitt kurz beschrieben.

2.2.1 Webserver

Ein Webserver ist eine Software-Komponente, mit der Webangebote über HTTP bereitgestellt werden können. Häufig wird auch die Hardware, auf der ein solches Programm installiert ist, als Webserver bezeichnet.

2.2.2 Clients

Auch bei Clients lässt sich zwischen der Software-Komponente (in der Regel ein Browser, siehe Abschnitt 2.2.3) und der Hardware – also dem Endgerät an sich – unterscheiden. Endgeräte können herkömmliche PCs, aber auch Mobiltelefone, PDAs oder Tablets sein.

2.2.3 Browser

Web-Browser (kurz Browser) sind Programme zur Darstellung von Dokumenten und folgen im Wesentlichen den Sprach- und Protokoll-Standards, die von den Standardisierungsgremien W3C und IETF erarbeitet werden. Neben den Transportprotokollen HTTP und HTTPS für die Kommunikation mit Webservern haben moderne Browser häufig noch andere Funktionen. Typische Beispiele sind Funktionen als Dateibrowser sowie als Client für das File Transfer Protocol (FTP) oder BitTorrent.

Die Hauptaufgabe eines Browsers ist jedoch die Darstellung von Webseiten. Dazu werden neben HTML in der Regel ergänzende Techniken wie CSS, XML und JavaScript verwendet. Zusätzlich bieten aktuelle Browser noch die Integration von Plug-Ins, um Multimedia-Inhalte wie PDF oder Flash darzustellen.

Mit HTML5 werden Browser zu praktisch vollständigen Ausführungsplattformen für JavaScript-Applikationen aufgewertet. Mit umfangreichen Möglichkeiten zur lokalen Datenspeicherung können Offline-Applikationen im Browser sogar weitgehend unabhängig vom Server arbeiten. Des Weiteren können solche Applikationen über neue Schnittstellen flexibel nutzbare Kommunikationsverbindungen aufbauen.

2.2.3.1 Vertrauliche Inhalte in Browsern

Browser speichern zahlreiche vertrauliche Informationen, die Aufschlüsse über den Benutzer und dessen Verhalten im Web zulassen. Die wichtigsten dieser Informationen sind Cookies, Verlauf (Browser-History), Download-History, Browser-Cache und Lesezeichen. Um die Nutzung von Webangeboten komfortabler zu gestalten, können zusätzlich Formulareingaben, Passwörter und Daten von clientseitig ausgeführten Applikationen gespeichert werden.

HTTP Cookies

Bei Cookies handelt es sich um Profildaten, die von einer Webseite auf dem Client hinterlegt und bei erneutem Besuch des Webangebots ausgelesen werden können. Meist speichern Webseiten eindeutige Unterscheidungsmerkmale (IDs) auf dem Client, um diesen bei einem erneuten Aufruf der Seite wiedererkennen zu können.

Jede Webseite die besucht wird oder von der ein Element geladen wird (z. B. ein Bild) kann einen Cookie setzen. Durch die Same Origin Policy wird sichergestellt, dass Webseiten nur auf ihre eigenen Cookies zugreifen können. Werden Cookies von Webseiten gesetzt, die man selbst nicht direkt angesprochen hat, so spricht man von Drittanbieter-Cookies. Cookies von Drittanbietern werden häufig zum Tracking und zum Erstellen von Benutzerprofilen verwendet.

Alle Cookies besitzen ein Ablaufdatum, das vom Betreiber der Webseite festgelegt wird. Je nach Einsatzszenario kann ein Cookie nur für eine Sitzung (Session-Cookie) oder im Extremfall unbegrenzt lange gültig sein. Der Benutzer hat jedoch immer die Möglichkeit Cookies selbst zu löschen.

Flash Cookies

Flash-Cookies, auch als Local Shared Objects (LSO) bezeichnet, unterscheiden sich von HTTP Cookies dadurch, dass sie nicht vom Browser, sondern von einem Flash-Player verwaltet und außerhalb des Browsers gespeichert werden. Deshalb eignen sie sich besonders gut für Browser-unabhängiges Tracking. Hinzu kommt, dass sie kein Verfallsdatum besitzen. In Flash Cookies können größere Datenmengen gespeichert werden als in HTTP Cookies.

Supercookie

Als Web-Storage (auch DOM-Storage oder Supercookie) wird eine Technik für Webanwendungen bezeichnet, die einen dauerhaften (persistenten) Speicher auf den Clients der Nutzer zur Verfügung stellt. Auf diesen Speicher können Webanwendungen über eine Schnittstelle zugreifen, um dort Daten auszulesen oder abzulegen. Die Speicherkapazität ist um ein vielfaches größer als bei HTTP- oder Flash-Cookies.

Der Web-Storage lässt sich auch als Speicher für Offline-Applikationen verwenden, also Anwendungen im Browser, die auch ohne bestehende Internetverbindung genutzt werden können.

Verlauf (Browser-History)

Der Verlauf besteht aus einer Liste der besuchten Webseiten und kann sensible Informationen über den Benutzer beinhalten (beispielsweise wenn eine Seite über ein medizinisches Problem besucht wurde). Da die meisten Browser die gesamte URL im Verlauf speichern, werden somit in Abhängigkeit von der genutzten Webanwendung auch Variablen und vertrauliche Daten wie in der URL übertragene Passwörter oder Session-IDs gespeichert. Das Ausspionieren dieser Informationen durch Externe wird auch als „History-Sniffing“ bezeichnet.

Die Download-History dient als Übersicht über die vom Benutzer explizit aus dem Web heruntergeladenen und lokal gespeicherten Daten. Dokumente, die nur im Browser geöffnet wurden, sind daher nicht enthalten.

Lesezeichen

Lesezeichen – auch Favoriten genannt – sind vom Benutzer gespeicherte URLs und dienen als Sammlung der „Lieblings-Inhalte“. Da wie beim Verlauf auch Variablen in der URL enthalten sein können, gilt aus Sicherheitssicht Ähnliches wie für die Browser-History.

Cache

Im Cache werden Daten, die aus dem Internet geladen wurden, zwischengespeichert um einen erneuten Zugriff zu beschleunigen. Beim ersten Aufruf eines Webseiteninhalts kann der Webserver zusätzlich für den abgefragten Inhalt einen ETag (entity tag) vergeben, mit dem sich der Inhalt eindeutig identifizieren lässt. Wird zu einem späteren Zeitpunkt die Webseite erneut aufgerufen, so sendet der Client den ETag an den Server, der dann anhand des ETags feststellen kann, ob sich der Inhalt geändert hat und gegebenenfalls neu übertragen werden muss.

Die Eindeutigkeit des ETags kann für Tracking missbraucht werden. Im Gegensatz zu den HTTP-Cookies kann der Nutzer den Austausch von ETags nicht verbieten. Erst das Löschen des Zwischenspeichers entfernt auch die zu einem Webinhalt gehörigen ETags.

Der Inhalt des Caches kann in vielen Fällen noch kritischer sein als der des Verlaufs, da ein Angreifer mit Hilfe des Caches Zugriff auf Inhalte erhalten kann, die eine Authentisierung erfordern.

Formulardaten und Passwörter

Sicherheitsrelevant sind auch die Funktionen zum Speichern von Formulardaten zur „Auto-Vervollständigung“ von Eingaben und das Hinterlegen von Benutzernamen und Passwörtern zur Authentisierung bei Webanwendungen. Beide Funktionen steigern zwar den Komfort bei der Web-Nutzung, haben jedoch im Fall von Software-Schwachstellen im Browser gravierende Auswirkungen, weil diese Informationen potenziell unberechtigt ausgelesen werden können.

2.2.3.2 Sicherheitsmodelle

Der Browser ist eine Schnittstelle des PC zur Kommunikation mit der Außenwelt. Aufgrund dieser exponierten Position werden Browser häufig als Einfallstor genutzt. Zudem werden im Browser oft

sensible Informationen, wie Login Daten, verarbeitet, was sie auch selbst als Ziel von Angriffen interessant macht.

Im Folgenden werden kurz die gängigen Sicherheitsmodelle von Browsern dargestellt.

Same-Origin-Policy

Die Same-Origin-Policy (Prinzip desselben Ursprungs) besagt, dass einzelne Webseiten im Browser besondere Rechte auf ihre eigenen Inhalte genießen. Um festzustellen, ob es sich um den eigenen Inhalt einer Webseite handelt, überprüft der Browser den Domain- bzw. Host-Eintrag, den Pfad, den Port und das verwendete Protokoll beim Zugriff auf eine Ressource.

Aufgrund dieses Prinzips kann beispielsweise JavaScript nur auf die Cookies der Webseite zugreifen, von der aus der Code geladen wurde, und nicht auf die Cookies anderer Webseiten. Auch beim Öffnen von Links in Frame-Sets oder neuen Fenstern kommt die Same-Origin-Policy zum Einsatz, indem nur Fenster oder Frames der eigenen Seite angesprochen werden dürfen.

Profile

Viele Browser bieten die Möglichkeit Profile anzulegen. Innerhalb eines Profils können sicherheitsrelevante Konfigurationen, beispielsweise das Zertifikatsmanagement, der Umgang mit aktiven Inhalten oder das Management von Cookies, festgelegt werden. Für verschiedene Nutzungsszenarien können unterschiedliche Profile erstellt werden – etwa ein restriktives Profil für Online-Banking und ein offeneres Profil für das Surfen.

Eine weniger strikte Umsetzung des Konzepts von Profilen ist das sogenannte Zonenmodell, bei dem Webseiten in Sicherheitszonen eingeordnet werden.

Sandboxing

Neben den Betriebssystem-gestützten Schutzmechanismen wie Speicherrandomisierung und Speicherschutz (siehe hierzu auch [ISi-Client]) ist es üblich verschiedene Funktionen des Browsers voneinander zu isolieren, indem beispielsweise jeder Tab in einem eigenen Prozess ausgeführt wird. Durch diese Kapselung (engl. Sandboxing) werden die Auswirkungen von Prozessen auf das Betriebssystem oder auf andere Prozesse reduziert. Dies hat beispielsweise zur Folge, dass ein Programmierfehler oder Absturz eines Prozesses nicht die Stabilität anderer Prozesse beeinträchtigt.

Zertifikatsverwaltung

Viele Webseiten verwenden inzwischen das Protokoll TLS (Transport-Layer-Security) um Verbindungen über HTTPS zu verschlüsseln (siehe Abschnitt 2.3.2). Bei TLS werden serverseitige Zertifikate genutzt. Browser müssen in der Lage sein diese Zertifikate zuverlässig zu verifizieren und zu verwalten. Dazu zählt insbesondere die vollständige Überprüfung der Gültigkeit von Zertifikaten, die Unterstützung von HTTP Strict Transport Security (HSTS) und ein konfigurierbares Zertifikatspinning, d.h. eine feste Zuordnung von einer Domain zu einem Zertifikat.

2.2.3.3 Erweiterungen

Alle gängigen Browser lassen sich durch Browser Extension modifizieren und erweitern. Es lassen sich zwei Arten von Erweiterungen unterscheiden. Beiden gemein ist, dass sie bei Bedarf lokal vom Anwender installiert werden können.

Plug-Ins

Plug-Ins sind eigenständige Programme, die den Browser um zusätzliche Funktionen erweitern. Mit Plug-Ins können Webseiten-Inhalte angezeigt werden, deren Format der Browser selbst nicht beherrscht. Damit beim Eintreffen der Daten das entsprechende Plug-In verwendet werden kann, wird den Inhalten ein MIME-Typ (Multipurpose Internet Mail Extension) zugewiesen, d. h. ein auf

das Plug-In abgestimmtes Dateiformat und eine dazugehörende Dateiendung. Anhand dieser Angaben erkennt der Browser, mit welchem Plug-In die Datei geöffnet werden kann.

Viele Plug-Ins ermöglichen die Ausführung von aktiven Inhalten im Browser. Beispiele für solche Plug-Ins sind Adobe Flash, das Java Runtime Environment, JavaFX-Script oder Microsoft Silverlight. Besondere Bedeutung kommt PDF-Reader-Plug-Ins zu, da sie häufig die Ausführung von Skripten in PDF-Dokumenten erlauben. Der Code wird dabei allerdings nicht im Browser, sondern im Plug-In selbst ausgeführt.

Add-Ons

Eine weitere Kategorie von Erweiterungen sind sogenannte Add-Ons. Auch Add-Ons erweitern die Funktionen des Browsers oder verändern bestehende Funktionen. Beispiele für Add-Ons sind Blockprogramme für Werbung oder Leisten für Suchmaschinen (sog. Toolbars).

2.2.4 ReCoBS

Eine Alternative zum direkten Surfen mittels Browser ist das Remote-Controlled Browsers System [ReCoBS]. Bei dieser Variante läuft der Browser nicht auf den Clients sondern in einer gekapselten Umgebung auf einem Terminal-Server. Die Clients loggen sich auf dem Terminal-Server ein und nutzen den dort installierten Browser. Zwischen dem Terminal-Server und dem Client werden nur grafische Informationen übertragen. Die Ausführung und die Darstellung von aktiven Inhalten sind dadurch voneinander getrennt und schädliche Inhalte haben keinen Auswirkungen auf den Client.

2.2.5 Proxy-Server

Ein Proxy-Server (meist einfach als „Proxy“ bezeichnet) agiert als Mittelsmann zwischen Client und Server und kann aktiv in die Kommunikation eingreifen. Er nimmt Anfragen der einen Seite entgegen und leitet sie zur anderen Seite weiter. Proxies werden in verschiedenen Ausprägungen eingesetzt.

Cachen und optimieren

Proxies müssen die weiterzuleitenden Inhalte schon prinzipbedingt zwischenspeichern (Caching). Anstatt die gespeicherten Inhalte direkt wieder zu löschen, werden sie oft für längere Zeit vorgehalten. Dies ist insbesondere bei häufig aufgerufenen Inhalten sinnvoll, da der Proxy sie direkt ausliefern kann und nicht erst erneut aus dem Internet laden muss.

In Netzen mit geringen Bandbreiten (z. B. Mobilfunknetzen) werden Proxies auch zur Optimierung von Inhalten genutzt – etwa zur Verkleinerung von Bildern oder zur Komprimierung von Headern.

Bei fehlerhafter Konfiguration des Proxys kann es zu Problemen – z. B. bei der Authentisierung – kommen ([RFC 3143]). Aktiviertes Caching eröffnet Angreifern zudem die Möglichkeit, Cache-Poisoning-Angriffe durchzuführen (siehe auch Abschnitt 5.3.4).

Inhalte filtern oder manipulieren

Proxies werden oft an zentraler Stelle zur Überprüfung von HTTP-Anfragen und -Antworten genutzt. Aufgrund seiner Position hat ein Proxy die Möglichkeit die Kommunikation zwischen Client und Server gezielt zu manipulieren, etwa durch das Entfernen von Kopfzeilen (z. B. den User-Agent, siehe Abschnitt 2.3.1) oder der Filterung aktiver Inhalte.

Da Proxies alle Inhalte zumindest temporär (auch bei deaktiviertem Caching) zwischenspeichern, besteht die Möglichkeit, alle über den Proxy übertragenen Informationen auf Schadprogramme zu untersuchen.

Application-Layer-Gateway

In vielen Netzen ist von den Clients kein direkter Web-Zugang erlaubt. Stattdessen werden Web-Verbindungen an einem zentralen Gateway (ALG) terminiert. Das ALG baut dann eine eigene Ver-

bindung zum Webserver auf. Diese Art des Proxies wird in der Regel zusammen mit Content Filtering verwendet.

Es gibt auch ALGs für HTTPS. Diese ermöglichen auch die Überprüfung von verschlüsselten HTTPS-Verbindungen. Allerdings wird hierbei die Ende-zu-Ende-Verschlüsselung aufgebrochen.

Steuerung des Netzwerkzugriffs

Proxies können auch eingesetzt werden, um den Zugriff zum Netz einzuschränken (z. B. Login) oder zu steuern (z. B. Bandbreiten-Management).

2.3 Protokolle

Für die Datenübertragung zwischen einem Webserver und einem Browser werden in der Regel das Hypertext Transfer Protocol (HTTP) sowie dessen verschlüsselte Variante Hypertext Transfer Protocol Secure (HTTPS) verwendet.

Während das klassische HTTP alle Informationen unverschlüsselt zwischen Client und Server überträgt, erlaubt HTTPS die Authentifizierung von Client und Server sowie die Erzeugung eines verschlüsselten Tunnels für den Informationsaustausch. Dazu müssen sowohl der Webserver als auch der Browser das Transport-Layer-Security- (TLS-) bzw. das ältere Secure-Sockets-Layer- (SSL-) Protokoll unterstützen (siehe auch Abschnitt 2.3.2). Syntaktisch gleichen sich die Protokolle HTTP und HTTPS oberhalb der TLS-Verschlüsselung.

2.3.1 HTTP

Das Hypertext Transfer Protocol (HTTP) dient zur Übertragung von Informationen im Web. Jede HTTP -Nachricht ist entweder eine Anfrage von einem Client an einen Server (Request) oder eine Antwort von einem Server (Response). HTTP ist grundsätzlich verbindungslos, d. h. dass jede Anfrage unabhängig von vorangegangenen bearbeitet wird. Folgendes Beispiel zeigt eine typischen HTTP-Request:

```
GET /cgi-bin/htsearch?config=htdig-bsi&words=HTTP&submit.x=0&submit.y=0
HTTP/1.1
Host: luise.bsi.bund.de
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.4)
Gecko/20070515 Firefox/2.0.0.4
Referer: http://www.bsi.bund.de/
```

Beispiel 2: HTTP-Anfrage-Kopfzeile

Jeder Request beginnt mit einem Schlüsselwort, das die sogenannte Methode definiert. Im obigen Beispiel ist dies die Methode GET. Die Semantik der Methode ist in [RFC 7231] festgelegt. Außer GET sind im HTTP 1.1-Standard noch die Methoden OPTIONS, HEAD, POST, PUT, DELETE, TRACE und CONNECT definiert. Tabelle 2 gibt einen Überblick über deren Funktion.

Neben diesen acht HTTP-eigenen Methoden sind in separaten RFCs noch zahlreiche weitere Methoden definiert. Eine vollständige Liste aller registrierten HTTP Methoden wird bei der IANA gepflegt[1]. Der Großteil dieser Methoden wird für WebDAV (Web Distributed Authoring and Versioning, [RFC 4918]) genutzt und ist im Kontext dieser Studie nicht relevant. Gelegentlich werden auch weitere Methoden verwendet, die nicht in RFCs standardisiert und bei der IANA registriert sind.

1 http://www.iana.org/assignments/http-methods/http-methods.xhtml

Wie in Beispiel 2 gezeigt, wird bei der HTTP-GET-Methode die zu behandelnde Ressource mit einer absoluten URL spezifiziert. Darauf folgt die verwendete Version von HTTP.

Im Anschluss an die Versionsnummer folgen die eigentlichen Kopfzeilen (engl. Header), die im Format „Kopfzeilen-Name: Wert“ aufgebaut sind. Ein Großteil davon wird vom Browser automatisch aus der Konfiguration erstellt.

In einer HTTP-Anfrage werden typischerweise eine ganze Reihe an Kopfzeilen mitgesendet. Für die sichere Nutzung von Webangeboten sind insbesondere diejenigen Kopfzeilen relevant, anhand derer Profile über die Benutzer erstellt werden können (siehe Tabelle 3). Einige weitere sicherheitsrelevante Kopfzeilen können vom Server verschickt werden (siehe hierzu [ISi-Web-Server]).

Alle Kopfzeilen können auf dem Transportweg, beispielsweise durch das Umleiten der Verbindungen über einen Proxy-Server (siehe Abschnitt 2.2.5), verändert werden. Der Proxy kann sensible Inhalte entfernen oder austauschen.

In Bezug auf die Sicherheitseigenschaften bietet HTTP relativ wenig Möglichkeiten. Die Vertraulichkeit der Informationen wird aufgrund der Klartext-Übertragung nicht geschützt. Eine Prüfung der Integrität findet lediglich auf der darunter liegenden Transportschicht statt. HTTPS hingegen bietet eine Sicherung der Vertraulichkeit und der Integrität der Informationen sowie eine Authentifizierung der Kommunikationspartner durch den Einsatz von SSL/TLS.

HTTP-Methode	***Funktion***
OPTIONS	fragt beim Webserver an, welche Optionen für die Kommunikation zur Verfügung stehen. Wird als URL ein Stern (*) angegeben, antwortet der Server mit den Methoden, die er unterstützt.
GET	stellt eine Anfrage zu einer bestimmten URL. GET wird standardmäßig verwendet, wenn im Browser auf einen Hyperlink geklickt wird oder der Benutzer eine URL manuell öffnet.
HEAD	entspricht der Funktionsweise von GET, nur dass der Server ausschließlich die Kopfzeilen und nicht den Rumpf der Antwort ausgibt.
POST	entspricht der Funktionsweise von GET, nur dass die Abfrage durch Informationen im Rumpf weiter verfeinert und die URL somit näher spezifiziert werden kann.
PUT	ermöglicht es, Informationen vom Client zum Server zu übertragen und dort dauerhaft zu speichern. Um die Integrität der Informationen am Webserver zu gewährleisten, kommt PUT aus Sicherheitssicht eine besondere Bedeutung zu.
DELETE	erlaubt das Löschen von Ressourcen am Webserver. Aus Sicherheitssicht gilt für diese Methode Ähnliches wie für PUT.
TRACE	dient in erster Linie der Fehlerbehebung bei Webservern. Eine TRACE- Anfrage wird vom Server durch die Rückgabe der genauen Anfrage (im Sinne eines „Loop-Backs“) beantwortet.
CONNECT	wird typischerweise verwendet, um HTTPS-Verbindungen über einen HTTP-Proxy zu tunneln, ohne dabei die Ende-zu-Ende-Verschlüsselung zu unterbrechen.

Tabelle 2: Überblick über die Funktionen der in [RFC 7231] definierten HTTP-Methoden

HTTP Kopfzeile	*beispielhafter Wert*	*Bedeutung*
User-Agent	Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.8.1.4) Gecko/20070515 Firefox/2.0.0.4	beinhaltet Informationen über den eingesetzten Browser, das Betriebssystem und deren Versionsnummern
Accept-Language	de-de,de;q=0.8,en-us;q=0.5,en;q=0.3	enthält eine sortierte Reihung der vom Benutzer bevorzugten Sprachen
Referer	http://www.bsi.bund.de/	gibt die Webseite an, von der aus der Benutzer auf die aktuelle Seite verwiesen wurde
Cookie	PREF=ID=fe75391b88f8e08f:TM=1179580697:LM=1179580697:S=I2UEA5vV5li-i9Q3r	überträgt kleine Dateneinheiten (meist Unterscheidungsmerkmale, also IDs), welche es dem Server-Betreiber ermöglichen, die Anfrage im größeren Kontext einer Sitzung zu betrachten

Tabelle 3: Verbreitete HTTP-Kopfzeilen, die Informationen über den Benutzer an den Webserver übertragen

2.3.2 TLS

Bei Transport Layer Security (TLS) handelt es sich um Spezifikationen zur Verschlüsselung von beliebigen Protokollen der Anwendungsebene. Neben HTTP lassen sich z. B. auch SMTP, IMAP u. a. über TLS absichern.

TLS ist eine Weiterentwicklung des inzwischen veralteten SSL. Grundsätzlich chiffrieren beide Protokolle die Informationen zwischen den Kommunikationspartnern mittels symmetrischer Kryptografie. Zum Vereinbaren eines symmetrischen Schlüssels kommen jedoch asymmetrische Verfahren auf Basis einer Public-Key-Infrastruktur (PKI) zum Einsatz.

Um überprüfbar zu machen, ob ein Schlüssel zu einer Domäne gehört, werden digitale Zertifikate verwendet. Diese werden von einer Zertifizierungsstelle (Certification Authority, CA) signiert, die selbst wiederum von einer Reihe höherer Stellen zertifiziert ist. Am Ende einer solchen Kette stehen Root-CAs, deren Zertifikate fix in den Browsern eingetragen sind und denen absolut vertraut wird.

Da es in der Vergangenheit mehrfach zu Sicherheitsvorfällen bei Zertifizierungsstellen kam, muss der Browser bei jeder Verwendung eines Zertifikats dessen Gültigkeit überprüfen. Um das Problem mit Zertifizierungsstellen zu umgehen, kann man auch Zertifikate im DNS hinterlegen (DANE [RFC 6698]). Zwingende Voraussetzung hierfür ist die Einführung von DNSSEC [RFC 4033], da über DNSSEC die Integrität der im DNS abgelegten Daten – und damit auch der im Falle von DANE hinterlegten Zertifikate – sichergestellt wird.

Hinweise zum Einsatz von TLS finden sich in [TR-02102-2].

3 Sichere Grundarchitektur für normalen Schutzbedarf

Die vorangegangenen Abschnitte haben die grundlegenden Komponenten, Protokolle, Standards und Sicherheitsmechanismen bei der Nutzung von Webangeboten erklärt. Der folgende Abschnitt zeigt, wie das Web auf sichere Weise genutzt werden kann.

Abbildung 3.1 zeigt die aus [ISi-LANA] adaptierte Grundarchitektur als Netz-Plan, die alle relevanten Systeme zur Nutzung von Webangeboten enthält.

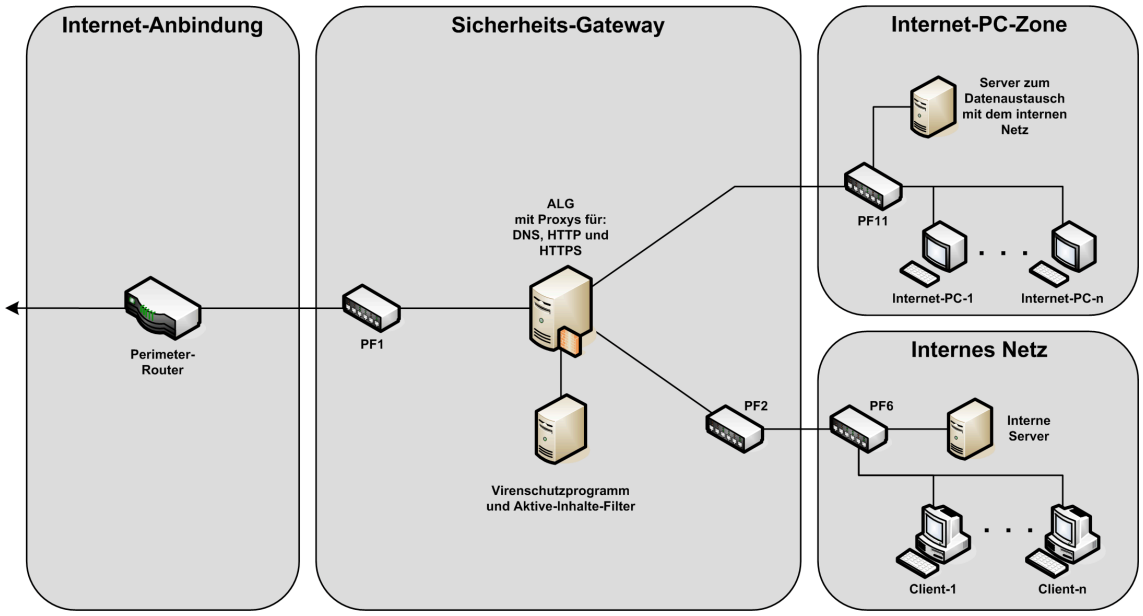


Abbildung 3.1: Grundarchitektur zur sicheren Nutzung von Webangeboten für normalen Schutzbedarf

Die Grundarchitektur unterscheidet vier Haupt-Zonen, die im Folgenden erläutert werden:

1. Internet-Anbindung
2. Sicherheits-Gateway
3. Internes Netz
4. Internet-PC-Zone

Die Web-Nutzung kann aus unterschiedlichen Zonen heraus erfolgen:

- Mitarbeiter können vom internen Netz aus Informationen im Web nachschlagen („surfen“) und interne Webanwendungen nutzen. Die Nutzung von Java-Script im internen Netz ist bei der Nutzung eines geeigneten Browsers (siehe Abschnitt 4.2.1.2) zulässig.
- Bei potenziell gefährlichen Inhalten besteht die Möglichkeit, solche Inhalte aus der Internet-PC-Zone heraus abzurufen. Hierbei handelt es sich um ein getrenntes Netzsegment mit physischen oder virtuellen Internet-PCs.
- Obwohl grundsätzlich der Zugriff von Servern auf Web-Inhalte unterbunden werden sollte, gibt es Szenarien, in denen sich eine komplette Sperre des Web-Zugriffs aus dem internen Server-Netz nicht vermeiden lässt. Für diesen Fall kann über das ALG auf definierte Webangebote auch von Servern aus zugegriffen werden.

3.1 Internes Netz

Das interne Netz (siehe Abbildung 3.2) enthält Clients und Server, die durch einen Paketfilter voneinander getrennt sind. Dieser Paketfilter verbindet das Netz auch mit dem Sicherheits-Gateway.

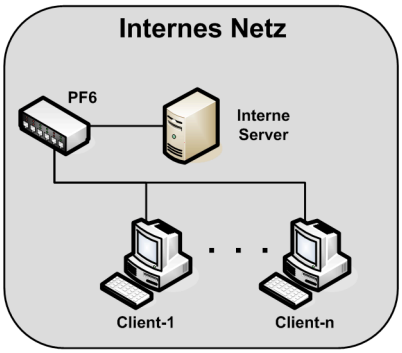


Abbildung 3.2: Grundarchitektur des internen Netzes

3.1.1 Clients

Sollte es einem Angreifer gelingen, gefährliche Inhalte am Sicherheits-Gateway vorbeizuschmuggeln, stellen die Clients die letzte Verteidigungslinie dar. Aus diesem Grund müssen auch dort Maßnahmen ergriffen werden, die verhindern, dass solche Inhalte im internen Netz Schäden anrichten können.

Wichtig ist insbesondere, die eingesetzten Programme und das Betriebssystem auf dem aktuellsten Stand zu halten. Zudem muss sichergestellt werden, dass ein Angreifer bei erfolgreicher Ausnutzung von Schwachstellen möglichst wenig Zugriff erlangt. Dies wird erreicht, indem die Benutzer nur mit den minimal notwendigen Rechten ausgestattet werden. Durch die Verwendung eigener Accounts speziell für die Web-Nutzung ist es möglich, einen eventuellen Hacker noch weiter einzuschränken (siehe Variante 5.1.1 A). Details zur sicheren Grundarchitektur von Clients sowie weitere Schutzmechanismen sind in [ISi-Client] zu finden. Informationen zum mobilen Einsatz werden in [ISi-Fern] gegeben.

Browser

Die im Web heruntergeladenen Inhalte werden im Normalfall im Browser des Clients angezeigt. Sollten aktive Inhalte im genutzten Webangebot verwendet werden, findet die Ausführung daher im Browser statt. Aus diesem Grund blockieren die Browser nach entsprechender Konfiguration solche Inhalte aus nicht vertrauenswürdigen Quellen. Zusätzlich werden unerwünschte aktive Inhalte auch von ALG geblockt.

Das Risiko eines erfolgreichen Angriffs, welcher bestehende Sitzungen an Webangeboten ausnutzt, kann erheblich gesenkt werden, indem das Öffnen mehrerer Browser-Fenster oder Tabs unterbunden wird (siehe Variante 5.4.3 A). Zahlreiche andere Angriffe auf Browser können jedoch zurzeit mit technischen Maßnahmen nicht verhindert werden. Aus diesem Grund müssen auch organisatorische Regelungen für die Nutzung des Web umgesetzt werden (siehe Abschnitt 3.6).

3.2 Internet-PC-Zone

Um potenziell gefährliche Webangebote nutzen zu können, stehen in der Internet-PC-Zone dedizierte Web-Clients zur Verfügung. Abbildung 3.3 zeigt den Aufbau der Zone. Sie wird über den Paketfilter PF11 an das ALG angebunden.

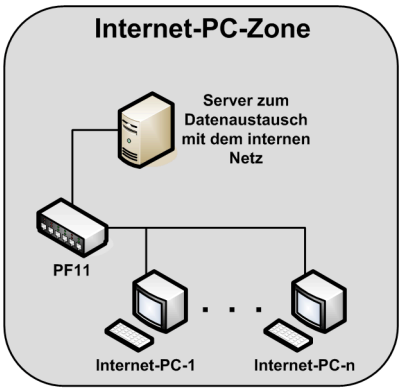


Abbildung 3.3: Grundarchitektur der Internet-PC-Zone

Es handelt sich bei der Internet-PC-Zone zwar um ein separates Netzsegment, es ist jedoch keine räumliche Trennung von den Clients im internen Netz notwendig. Bei den Internet-PCs kann es sich auch um virtuelle Clients handeln, die vom Arbeitsplatz aus genutzt werden.

In allen Varianten muss verhindert werden, dass die Internet-PCs direkten Zugriff auf Daten im internen Netz haben. Um dennoch einen gewisse Benutzerfreundlichkeit zu bieten, können Clients aus dem internen Netz Daten von einem speziellen Server abholen. Auch zum direkten Drucken ist eine eigene Lösung notwendig, beispielsweise ein eigener Drucker in der Internet-PC-Zone.

Für hohen Schutzbedarf kann alternativ zur Internet-PC-Zone ein Remote-Controlled Browsers Systems (ReCoBS) genutzt werden, mit dem sich aktive Inhalte direkt vom Arbeitsplatz aus nutzen lassen. Der eigentliche Browser läuft bei dieser Variante nicht auf den Clients im internen Netz, sondern auf einem Terminal-Server im Sicherheits-Gateway. Von dort werden lediglich grafische Informationen in das interne Netz übermittelt. Ausführung und Darstellung der aktiven Inhalte werden somit voneinander getrennt. Der Sicherheitsgewinn und der erhöhte Benutzerkomfort müssen allerdings durch zusätzlich benötigte Komponenten erkauft werden (siehe Varianten 5.2.2 A und 5.2.2 B). Für kleine Organisationen besteht mit der Variante 5.2.2 C die Möglichkeit, einzelne Systeme über virtuelle Maschinen zu konsolidieren, sodass der Hardware-Aufwand der Grundarchitektur nicht überschritten wird.

Internet-PCs

Die Internet-PCs sollten regelmäßig neu aufgesetzt oder auf einen sicheren Zustand (Snapshot) zurückgesetzt werden, um das System zu säubern. Alternativ dazu kann das Betriebssystem von einem schreibgeschützten Medium gestartet werden, sodass keine permanenten Veränderungen am System möglich sind. In beiden Fällen ist zu beachten, dass Sicherheits-Updates für eingesetzte Software, Virensignaturen und der Regelsatz der Personal Firewall bei der Systemwiederherstellung veraltet sein können und neu eingespielt werden müssen.

Server zum Datenaustausch mit dem internen Netz

Zum unidirektionalen Datenaustausch mit dem internen Netz (Informationen müssen aus dem internen Netz abgeholt werden) nutzt die Grundarchitektur einen Webserver mit HTTPS. Auf diesem Server können Internet-PCs die aus dem Web heruntergeladenen Dateien oder Druck-Jobs zwischenspeichern. Informationen mit hohem Schutzbedarf sind darauf nicht zugelassen.

Wenn ein Benutzer Daten auf dem Server ablegt, können diese später aus dem internen Netz über HTTPS abgerufen werden. Durch den Einsatz eines SSL-Proxys am ALG ist die Übertragung zwar verschlüsselt, die Daten können aber trotzdem vom Sicherheits-Gateway auf Schadprogramme untersucht werden. Auch das Entfernen von aktiven Inhalten aus transferierten Dateien ist auf diesem Weg möglich. Über ein Berechtigungskonzept wird sichergestellt, dass nur die Eigentümer der

jeweiligen Daten (also jene Benutzer, welche die Informationen am Datenaustauschserver abgelegt haben) darauf zugreifen können.

3.3 Sicherheits-Gateway

Das Sicherheits-Gateway (Abbildung 3.4) ist in einer sogenannten PAP-Struktur (Paketfilter – Application-Layer-Gateway – Paketfilter) aufgebaut und dient als zentrale Sicherheitskomponente des Netzes. Es führt eine Überprüfung aller übermittelten Pakete auf Transport- und Anwendungsschicht durch und filtert potenziell bösartige Inhalte heraus. Systeme zum Anbieten von Diensten im Internet befinden sich ebenfalls in dieser Zone, wobei alle Übergänge zwischen Zonen mit heterogenem Schutzbedarf durch Paketfilter geschützt werden. Das ALG stellt die Verbindung zwischen dem Internet und dem internen Netz her.

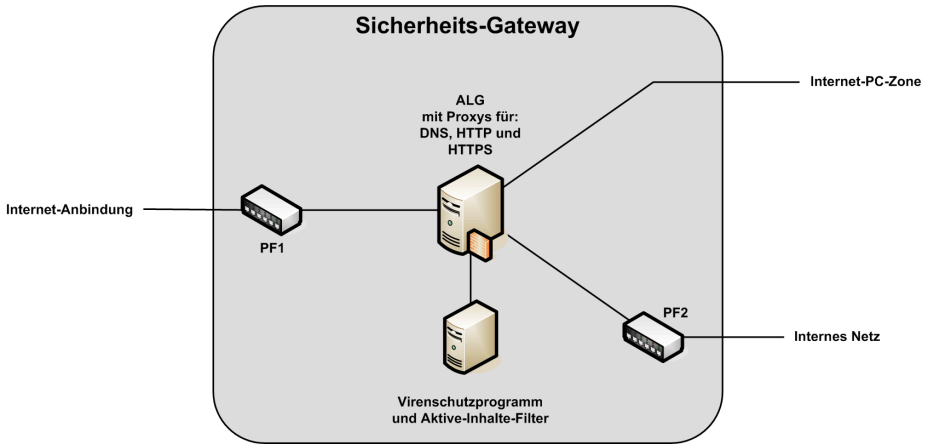


Abbildung 3.4: Grundarchitektur des Sicherheits-Gateways

Application-Level Gateway (ALG)

Für die Web-Nutzung benötigt das ALG Proxies für HTTP, HTTPS und DNS, an denen sich Benutzer authentisieren müssen. Die Ende-zu-Ende-Sicherheit von HTTPS-Verbindungen wird vom Proxy unterbrochen, wodurch die Server-Authentisierung für HTTPS-Verbindungen am Application-Level Gateway erfolgt. Dieses akzeptiert nur Webangebote mit Zertifikaten von vertrauenswürdigen Herausgebern, um das Risiko gefälschter Zertifikate zu reduzieren.

Alle Web-Inhalte werden am Proxy zwischengespeichert und an ein eigenes System zur Filterung von potenziell gefährlichen Inhalten weitergeleitet. Dadurch kann die Auslastung des ALG möglichst gering gehalten werden. Das Caching von Webangeboten durch den Proxy-Server kann bei einer langsamen Internet-Anbindung zu einem deutlichen Geschwindigkeitsgewinn führen. Dadurch entsteht jedoch auch die Gefahr, dass ein Angreifer die im Cache gespeicherten Seiten verändert und die Benutzer dadurch täuscht. Aus diesem Grund wird bei hohem Schutzbedarf empfohlen, alle Web-Inhalte unmittelbar nach der Überprüfung auf gefährliche Inhalte zu löschen und bei einer neuerlichen Anfrage wieder direkt aus dem Web zu laden (siehe Variante 5.3.4 A).

Schadprogramme und unerwünschte aktive Inhalte werden am ALG gefiltert. Interne Webangebote mit aktiven Inhalten oder externe Webangebote, denen genauso vertraut wird wie den eigenen, müssen vor der Verwendung im internen Netz explizit freigeschaltet werden. Grundsätzlich sollte auf aktive Inhalte möglichst weitgehend verzichtet werden.

Bei hohem Schutzbedarf können auch andere potenziell gefährliche Inhalte wie Frames (siehe Variante 5.3.2 B) oder Werbungen (siehe Variante 5.4.5 A) am ALG gesperrt werden. Bei besonders hohem Schutzbedarf besteht zudem die Möglichkeit, am ALG eine Einschränkung der zugelassenen Webangebote auf Basis einer Whitelist umzusetzen (siehe Variante 5.3.2 C). Wenngleich damit ein hohes Sicherheitsniveau erreicht werden kann, wird der Benutzerkomfort für die Anwender dadurch deutlich eingeschränkt.

Für die Nutzung von Webseiten beliebiger Quelle, die gesperrte Inhalte verwenden, stehen die Systeme in der Internet-PC-Zone zur Verfügung. Abhängig von der Zone, von der aus ein Webangebot aufgerufen wird, erfolgt somit eine unterschiedliche Behandlung am Application-Level Gateway.

Virenschutzprogramm und Aktive-Inhalte-Filter

Zur Entlastung des ALG kommt ein eigenes System mit einem Virenschutzprogramm und einem Aktive-Inhalte-Filter zum Einsatz. Es „säubert“ die Inhalte und gibt sie anschließend an das ALG zurück. Bei geringer Auslastung kann die Funktion des Virenschutzprogramms und Aktive-Inhalte-Filters auch in das ALG integriert werden.

Die Behandlung der überprüften Inhalte erfolgt in drei Schritten:

1. Der empfangene Inhalt wird mittels eines Virenschutzprogramms auf Schadprogramme untersucht. Falls solche vorhanden sind, liefert das System die Information an das ALG weiter. Anstelle der Inhalte wird dann nur die Meldung an den Benutzer zurückgegeben, dass Schadprogramme identifiziert wurden.
2. Abhängig von der Zone, aus der ein Webangebot aufgerufen wurde, werden die aktiven Inhalte aus den übertragenen Informationen herausgefiltert. Eine reine syntaktische Analyse ist in diesem Fall nicht ausreichend, da Browser „intelligent“ mit syntaktischen Fehlern umgehen können. Mit heuristischen Methoden können die meisten aktiven Inhalte jedoch gefunden und entfernt werden.
3. Die gesäuberten Daten werden an das ALG zurückgegeben. Ist eine Säuberung nicht möglich, werden die Inhalte verworfen und der anfordernde Benutzer darüber in Kenntnis gesetzt.

Insbesondere der zweite Schritt ist fehleranfällig, da aufgrund der Vielzahl an unterschiedlichen Varianten, mit denen aktive Inhalte in Webangebote integriert werden können, eine Umgehung des Filters trotz des Einsatzes heuristischer Methoden grundsätzlich möglich ist. Aus diesem Grund stellen die Browser der Clients eine zweite Verteidigungslinie dar, welche die Ausführung von nicht erlaubten aktiven Inhalten zusätzlich blockiert.

Um Schadprogramme, für die zum Zeitpunkt der Überprüfung noch keine Signatur verfügbar war, im Nachhinein zumindest erkennen zu können, besteht die Möglichkeit, eine erneute, zeitlich versetzte Überprüfung durchzuführen (siehe Variante 5.1.2 A). Während die Infektion mit bösartiger Software damit nicht verhindert werden kann, ist durch die rasche Erkennung zumindest eine Eindämmung des Schadens realisierbar.

3.3.1 Anbieten eigener Internet-Dienste

Das Anbieten eigener Dienste wird in den Studien [ISi-LANA], [ISi-Web-Server] sowie [ISi-Mail-Server] beschrieben und wird in diesem Dokument nicht näher erläutert.

3.4 Internet-Anbindung

Die Anbindung an das Internet erfolgt entsprechend [ISi-LANA] über einen Perimeter-Router, der die physische Grenze zwischen öffentlichem Netzbereich und eigener Infrastruktur darstellt. Bei

dem Einsatz von mobilen Clients oder Telearbeitsplätzen sollte die Web-Nutzung ausschließlich gesichert über das ALG erfolgen (siehe hierzu auch [ISi-Fern]).

3.5 Protokollierung

Die Protokollierungen der Personal Firewall und des Virenschutzprogramms auf den Clients werden zentral in der Management-Zone (siehe auch [ISi-LANA]) gesammelt und ausgewertet. Damit ist auch eine Feinabstimmung der Personal Firewalls und Virenschutzprogramme möglich.

Am ALG werden bezüglich der Web-Nutzung folgende Informationen protokolliert:

- Alle HTTP-Anfragen sowohl über die Internet-PC-Zone als auch über das interne Netz. Der jeweilige Proxy-Benutzer sollte mit dem Request gespeichert werden.
- Alle Schadprogramme, die bei der Überprüfung auf dem Proxy-Server gefunden wurden, und deren Herkunft müssen protokolliert werden. So können gegebenenfalls bestimmte Seiten, die Schadprogramme verteilen, in eine Blacklist aufgenommen werden.
- Sollten Probleme im Zusammenhang mit der Filterung von aktiven Inhalten auftreten, kann geloggt werden, welche aktiven Inhalte entfernt wurden. Mit Hilfe dieses Protokolls können Fehler leichter identifiziert werden (etwa wenn fälschlicherweise Filterungen vorgenommen wurden). Eine dauerhafte Protokollierung ist nicht notwendig.

Bei Speicherung und Auswertung der Protokolle müssen rechtliche Rahmenbedingungen beachtet werden.

3.6 Organisatorische Regelungen

In der Grundarchitektur wurde versucht, möglichst allen Gefährdungen bei der Nutzung von Webangeboten mittels technischer Maßnahmen zu begegnen. Aufgrund der zahlreichen Angriffe, die auf der Benutzer-Ebene ansetzen, können damit jedoch nicht alle Schwachstellen abgedeckt werden. Daher sind zusätzlich organisatorische Regelungen notwendig, die den Benutzern helfen, sich richtig und sicher im Web zu bewegen.

3.6.1 Regelung der Nutzung des Web

Es müssen Richtlinien definiert und verbindlich vorgeschrieben werden. In diesen Richtlinien ist festlegt in welcher Form das Web genutzt werden darf und welche Risiken sich daraus ergeben.

Zu den Inhalten zählen des Weiteren klare Definitionen in Bezug auf:

- Konfigurationseinstellungen, die ein Benutzer verändern darf,
- Inhalte, die auf keinen Fall genutzt werden dürfen (z. B. Pornografie, Extremismus etc.),
- Informationen, die keinesfalls über das Web versandt werden dürfen (auch in Foren und Chats),
- die Pflicht zur Verwendung verschlüsselter Verbindungen für bestimmte Inhalte (HTTPS),
- Informationen, die auf dem System zum Datenaustausch mit dem internen Netz abgelegt werden dürfen sowie
- Webangebote mit hohen Anforderungen an die Vertraulichkeit oder an die Integrität bei denen die URL eingetippt oder über Lesezeichen geöffnet werden sollte, anstatt über Hyperlinks.

Aufgrund von rechtlichen Rahmenbedingungen muss auch die private Nutzung des Web geregelt werden. Diese Studie gibt keine Empfehlung, ob eine private Nutzung erlaubt oder verboten sein

sollte. Wird die private Nutzung erlaubt, besteht die Möglichkeit, dass Mitarbeiter dieses Privileg missbrauchen. Im schlimmsten Fall entsteht dem Unternehmen ein beträchtlicher Schaden, wenn ein Mitarbeiter im Web illegale Tätigkeiten verrichtet. Andererseits kann das gelegentliche private Surfen die Konzentration bei der nachfolgenden Arbeit sowie die Mitarbeiter-Motivation (und somit auch die Bindung an die Institution) steigern. Ein möglicher Weg zwischen einem generellen Verbot und der unbeschränkten Lizenz zum Surfen ist die Bereitstellung eines Zeit-Kontingents, das privat im Web verbraucht werden darf. Zusätzlich können nicht-dienstliche Seiten in beliebiger Anzahl gesperrt werden.

3.6.2 Freischaltung von aktiven Inhalten in vertrauenswürdigen Webangeboten

Für die Freischaltung von aktiven Inhalten im internen Netz von bestimmten, eigenen Webangeboten oder solchen, denen genauso vertraut wird wie den eigenen, muss ein Prozess existieren. Im Zuge dieses Prozesses wird eine Risiko-Analyse durchgeführt. Dabei sollten folgende Überlegungen angestellt werden:

- Wer außer den eigenen Mitarbeitern hat sonst noch Zugriff auf das Webangebot?
- Welche Gefährdungen entstehen durch die Zulassung der aktiven Inhalte im Webangebot?
- Bei der Bewertung von aktiven Inhalten ist zwischen JavaScript und anderen aktiven Inhalten zu unterscheiden. Bei der Verwendung eines geeigneten Browsers (siehe Abschnitt 4.1.1.2) ist die Verwendung von JavaScript in vielen Fällen vertretbar.

Abhängig vom Ergebnis der Risiko-Analyse kann eine Freischaltung erfolgen oder es können andere Maßnahmen zum Schutz des internen Netzes implementiert werden.

3.6.3 Schulungen für sicherheitsbewusste Web-Nutzung

Viele der Gefährdungen basieren auf dem mangelnden Sicherheitsbewusstsein der Benutzer und lassen sich durch regelmäßige Schulungen beseitigen. Die Benutzer müssen die Gefährdungen und die richtigen Verhaltensweisen kennen, um sich und die von ihnen verarbeiteten Informationen schützen zu können. Beispiele für die Inhalte von Schulungen zur Steigerung des Sicherheitsbewusstseins sind:

- Typische Gefährdungen bei der Nutzung von Webangeboten (siehe Abschnitt 5) und
- Inhalte der organisatorischen Regelungen.

4 Komponenten auswählen, konfigurieren und betreiben (normaler Schutzbedarf)

Im vorangegangenen Abschnitt wurde die Nutzung von Webangeboten sicher in die bereits beschriebene Grundarchitektur von [ISi-LANA] integriert und vorgestellt. In den folgenden drei Unterabschnitten sollen nun umfassende Empfehlungen gegeben werden, wie die in der Grundarchitektur enthaltenen Komponenten ausgewählt, konfiguriert und betrieben werden können.

4.1 Grundanforderungen an ein sicheres Produkt

Der folgende Abschnitt beschreibt grundlegende Anforderungen an Komponenten der Grundarchitektur, die bereits bei der Beschaffung des Produkts berücksichtigt werden müssen. Allgemeine Mindestanforderungen an die Ausstattung von Netz-Komponenten und die Leistungsfähigkeit von Lieferanten finden sich in [ISi-LANA].

4.1.1 Internes Netz

4.1.1.1 Client im internen Netz

An dieser Stelle wird lediglich auf die Anforderungen an Browser als primäres Werkzeug zur Web-Nutzung eingegangen. Anforderungen an Hardware, Betriebssystem und ergänzende Sicherheitskomponenten von Clients, z. B. Virenschutzprogramm und Personal Firewall, sind in [ISi-Client] beschrieben.

4.1.1.2 Browser im internen Netz

Grundlegende Anforderungen

- Es sollte die 64-Bit Version des Browsers eingesetzt werden.
- Der Browser muss ein zentrales Management unterstützen.

Sichere Ausführung

- Der Browser muss sich mit minimalen Rechten ausführen lassen.
- Speicherschutzmechanismen des Betriebssystems (ASLR, DEP) müssen unterstützt werden.
- Prozesse für getrennte Inhalte (z. B. separate Tabs) inklusive der Ausführung von Plug-Ins müssen weitestgehend voneinander isoliert werden (Sandboxing).
- Es muss möglich sein, mehrere Instanzen des Browser zu starten. Jede Instanz sollte sich eigenständig konfigurieren lassen (Profile).

Aktive Inhalte und Plug-Ins

- Die Ausführung von aktiven Inhalten, Plug-Ins und sicherheitskritischen Standards (z. B. WebGL) sollte sich feingranular steuern lassen.
- Der Browser sollte über integrierte minimale Anzeigekomponenten für PDF- und Office-Dateien verfügen und diese Anzeigekomponente gegenüber Plug-Ins bevorzugen.

Umgang mit privaten Daten

- Die Behandlung von Cookies und Cookies von Drittanbieter muss konfigurierbar sein.
- Private Daten wie Verlauf, Cache und Formulardaten müssen sich manuell und konfigurierbar automatisch (z. B. beim Schließen des Browsers) löschen lassen.

- Der Browser-eigene Passwortmanager sollte sich mit einem Master-Passwort absichern lassen.

Verschlüsselung und Zertifikatsverwaltung

- Der aktuelle TLS-Standard muss unterstützt werden.
- Der Browser muss die Gültigkeit von Zertifikaten – inkl. der Überprüfung auf Widerruf – überprüfen können.
- Die erlaubten TLS-Versionen, Schlüssellängen und Algorithmen müssen konfigurierbar sein.
- Der Browser sollte Mixed Content Blocking unterstützen. Eine Webseite enthält Mixed Content, wenn sie Inhalte aus sicheren und unsicheren Quellen mischt.

4.1.2 Internet-PC-Zone

4.1.2.1 Virtuelle Internet-PCs

Für die Clients in der Internet-PC-Zone gelten im Wesentlichen die gleichen Anforderungen wie für Clients im internen Netz. Ein grundlegender Unterschied ist jedoch, dass die Clients in der Internet-PC-Zone regelmäßig zurückgesetzt werden sollten (z. B. täglich oder sogar nach jeder Benutzung).

4.1.2.2 Server zum Datenaustausch mit dem internen Netz

Der Server zum Datenaustausch muss mindestens die folgenden Funktionen bieten:

- Ein residentes Virenschutzprogramm muss heruntergeladene Dateien prüfen.
- Dateien müssen sich in sichere Formate konvertieren lassen.

4.1.3 Sicherheits-Gateway

An dieser Stelle werden Anforderungen an das ALG beschrieben, die für die Web-Nutzung spezifisch sind. Grundsätzliche Anforderungen an Paketfilter und ALGs finden sich in [ISi-LANA].

4.1.3.1 Application-Layer Gateway

Allgemein

- Es muss eine Schnittstelle für die Integration eines Virenschutzprogramms und eines Filters für aktive Inhalte geben, um beides auf separate Server auszulagern.
- Der Proxy muss Dateien komplett herunterladen und vom Virenschutzprogramm überprüfen bevor sie an den Client weitergeleitet werden.
- Der Proxy muss Informationen aus dem Request- und Response-Header filtern bzw. modifizieren können.
- Einzelne Webseiten müssen sich anhand ihrer URL freischalten lassen (Whitelist).
- Einzelne Webseiten müssen sich anhand ihrer URL, beigefügten Cookies, aktiven Inhalten oder Mime-Typen gezielt sperren lassen (Blacklist).
- Es müssen sich externe Blacklists einbinden lassen (z. B. zum Sperren von Phishing-Seiten).
- Betrieb von mindestens zwei HTTP(S)-Proxies
  Einer der Proxies steht für die Internet-PC-Zone und der andere für das interne Netz. Auf beiden Proxies müssen unterschiedliche Benutzer authentisiert werden können. Es muss mindestens eine Benutzer-abhängige Konfiguration möglich sein. Ideal ist eine Rollen-basierte Rechtezuweisung.

HTTPS

- Überprüfung von Zertifikaten anhand der folgenden Eigenschaften:
  - Überprüfung des Root-Zertifikats

  - Abgleich von aufgerufener URL mit der im Zertifikat enthaltenen URL (Common Name)
  - Überprüfung des Ablaufdatums
  - Überprüfung, ob das Zertifikat zurückgezogen wurde, beispielsweise mittels OCSP (Online Certificate Status Protocol)
- Veraltete Verschlüsselungsoptionen (z. B. SSL) und kryptografische Algorithmen (z. B. DES, MD5) müssen deaktivierbar sein.
- Eigene Zertifikate müssen nachrüstbar sein, um auch „interne“ Root-Zertifikate konfigurieren und prüfen zu können.
- Vorkonfigurierte Zertifikate müssen entfernt werden können.

4.1.3.2 Virenschutzprogramm

- Die Virensignaturen müssen automatisch aktualisiert werden.
- Das Virenschutzprogramm muss Dateitypen anhand des Inhalts und nicht nur aufgrund des MIME-Typs oder der Dateiendung erkennen.
- Gepackte Dateien müssen entpackt und überprüft werden können.

4.1.3.3 Aktive-Inhalte-Filter

- Der Filter muss mindestens die folgenden Inhalte erkennen und filtern können:
  - alle Skriptsprachen (JavaScript, JScript, VBScript, etc.)
  - einzelne sicherheitskritische Elemente von Skriptsprachen, insbesondere
    - SVG
    - WebGL
  - Java-Applets
  - ActiveX-Controls, COM2-Komponenten
  - Microsoft-Windows-Skripts
  - Flash-Komponenten
  - Silverlight-Komponenten
  - JavaFX-Komponenten
- Ausnahmen für die Filterung müssen sich in einer Whitelist festlegen lassen.
- Der Filter muss mit verschiedenen HTML-Versionen und auch fehlerhaften HTML-Code zurecht kommen.
- Der Filter sollte auch in der Lage sein kritische Code-Stellen selektiv zu entfernen.
- Der Filter sollte Profile unterstützen, um eine unterschiedliche Filterung des Netzverkehrs in die Internet-PC-Zone bzw. in das interne Netz zu ermöglichen.

4.2 Konfiguration der Komponenten

Wurden alle für die Grundarchitektur benötigten Komponenten beschafft, müssen diese konfiguriert werden. Die Punkte, die es dabei zu beachten gilt, werden im folgenden Abschnitt erläutert.

4.2.1 Client

In diesem Abschnitt werden nur die Konfigurationen beschrieben, die für die Nutzung von Webangeboten gelten. Allgemeine Konfigurationsvorgaben für PCs sind in [ISi-Client] zu finden.

4.2.1.1 Personal Firewall

Die Firewall auf dem Client sollte alle eingehenden Verbindungen blockieren. Ausgenommen sind etwaige Zugriffe vom Management-Netz. Für den Browser sind in der Regel folgende ausgehende Verbindungen ausreichend:

- 80/TCP für HTTP
- 443/TCP für HTTPS
- 53/UDP und 53/TCP für DNS

4.2.1.2 Browser

Die Konfiguration des Browsers erfolgt zentral durch den Administrator. Dabei müssen die folgenden Punkte beachtet werden:

- Die maximale Anzahl der Tage, für die der Verlauf gespeichert wird, muss begrenzt werden.
- Die Ausführung aktiver Inhalte muss deaktiviert sein. Es ist jedoch gestattet, aktive Inhalte für vertrauenswürdige Seiten mit Hilfe einer Whitelist zu erlauben. Die Verwaltung dieser Listen sollte zentral erfolgen.
- Die Installation von Add-Ons oder Plug-Ins darf ebenfalls nur durch Administratoren erfolgen. Bei der Auswahl sollte beachtet werden, dass nur Add-Ons und Plug-Ins installiert werden, welche die Sicherheit nicht beeinträchtigen (d. h. keine Plug-Ins für Flash, SVG, XAML, Java, .NET etc.).
- Die Autovervollständigung sollte deaktiviert werden, wenn mit sensiblen Informationen gearbeitet wird.
- Der Abgleich mit Listen von bekannten Phishing-Seiten u.ä. wird zentral am ALG vorgenommen und sollte im Browser deaktiviert werden.
- Heruntergeladene Dateien dürfen nicht automatisch ausgeführt werden, sondern immer erst nach expliziter Bestätigung durch den Benutzer.
- Der Browser darf nur eine definierte Liste von Zertifizierungsstellen (CA) akzeptieren. Im Regelfall sind das lediglich die Zertifikate des Proxys oder von internen Servern. Webseiten mit Zertifikaten, die von einer anderen CA signiert wurden, sollte vom Browser nicht angezeigt werden. Wird der Zertifikatsspeicher vom Browser verwaltet, darf es einem Benutzer nicht möglich sein, Zertifikate selbst hinzuzufügen. Für jede CA, die vom Browser akzeptiert wird, muss eine Widerrufsliste (CRL) verwaltet und regelmäßig aktualisiert werden.
- Cookies sollten nur für die Dauer einer Sitzung gespeichert werden, d. h. beim Beenden des Browsers gelöscht werden. Cookies von Drittanbietern sollten standardmäßig abgelehnt werden.
- Pop-Up-Fenster sollten automatisch unterdrückt werden.
- Alle Konfigurationsoptionen, welche die Same-Origin-Policy aufweichen oder umgehen, müssen deaktiviert werden.

- Als Proxy muss das zentrale Sicherheits-Gateway eingetragen werden.
- Die Startseite sollte auf ein Intranet-Seite oder auf `about:blank` gesetzt werden.
- Alle Arten des Prefetching sollten deaktiviert werden.

Konfiguration durch den Benutzer

Der Benutzer darf die oben genannte Konfiguration des Browsers nicht ändern. Ihm sollte jedoch die Möglichkeit gegeben werden folgende Funktionen zu nutzen:

- Verlauf entleeren
- Private Daten manuell und/oder automatisch löschen (z. B. beim Beenden des Browsers)
- Passwortspeicher nutzen
- Privates Surfen/Inkognito-Modus

4.2.2 Internet-PC-Zone

4.2.2.1 Internet-PCs

Die Systeme in der Internet-PC-Zone müssen mit Hilfe der Konfigurationseinstellungen besonders abgesichert werden, da in dieser Zone potenziell gefährliche Inhalte nicht nur angezeigt, sondern auch ausgeführt werden können.

- Das Betriebssystem muss minimal und besonders gehärtet sein.
- Die Systeme sollten regelmäßig neu installiert bzw. zurückgesetzt werden.
  Alle Daten am System müssen dabei durch die Original-Version ersetzt werden (lokal gespeicherte Dateien werden somit vernichtet). Anschließend müssen alle verfügbaren Sicherheits-Updates und die neuesten Viren-Signaturen eingespielt werden.
- JavaScript, VBScript und unsignierte Java-Applets dürfen generell ausgeführt werden (siehe auch Abschnitt 5.2.1). Bei Bedarf stehen auch Plug-Ins für Flash, Microsoft Silverlight und/oder JavaFX zur Verfügung. Andere aktive Inhalte wie beispielsweise signierte Java-Applets oder ActiveX-Controls müssen explizit und nur für einzelne Webseiten freigeschaltet werden.
- Der Verlauf und der Cache dürfen im Browser nicht gespeichert werden. Beim Ausloggen eines Benutzers müssen sie zudem gelöscht werden.

4.2.2.2 Server zum Datenaustausch mit dem internen Netz

- Der Server muss nach dem Minimalprinzip aufgesetzt werden. Zudem sollte das Betriebssystem so gut wie möglich abgesichert werden.
- Der Webserver sollte gemäß [ISi-Web-Server] konfiguriert werden.
- Der Zugriff auf bestimmte Verzeichnisse darf ausschließlich über HTTPS erlaubt sein.
- Eine Authentisierung der Benutzer stellt sicher, dass Mitarbeiter nur auf die von ihnen selbst abgelegten Dateien zugreifen können.
- Nach einer bestimmten Verweildauer müssen Dateien (mit Ausnahme der Betriebssystem-Dateien) automatisch gelöscht werden.
- Alle Dateien am System sollten regelmäßig auf Schadprogramme geprüft werden (vorzugsweise zu Last-armen Zeiten). Werden solche gefunden, sollte der Administrator automatisch informiert werden.

- Dateien sollten in sichere Formate konvertiert werden. Dokumente können beispielsweise in PDF/A-1 konvertiert oder gedruckt werden und Bilder können von einem Format in ein anderes umgewandelt werden, um potenziell schädliche Inhalte zu entfernen.

4.2.3 Sicherheits-Gateway

Da es sich beim Sicherheits-Gateway um die zentrale Schutzmaßnahme handelt, ist die sichere Konfiguration besonders wichtig. Der folgende Abschnitt beschreibt die Einstellungen, die für einen sicheren Betrieb getroffen werden müssen.

4.2.3.1 Application-Layer Gateway

- Jeglicher ein- oder ausgehende Netzverkehr ins interne Netz oder in die Internet-PC-Zone muss über Proxies geführt werden.
- Pakete, die nicht der Protokoll-Spezifikation entsprechen, werden verworfen.
- Zum HTTP/HTTPS-Proxy dürfen nur autorisierte Verbindungen aufgebaut werden. Anhand der Authentisierung und dem Quell-Interface erkennt der Proxy-Server, ob Informationen aus dem internen Netz oder der Internet-PC-Zone abgefragt werden. Eine Authentisierung mit Accounts der Internet-PC-Zone aus dem internen Netz darf nicht möglich sein.
- Die CONNECT-Methode sollte deaktiviert werden, da sie zum Tunneln verwendet werden kann.
- HTTP-Header mit vertraulichen Informationen müssen vom Proxy-Server entfernt oder geändert werden.
- HTTPS-Verbindungen werden am Proxy terminieren und deren Inhalt überprüfen. Eine Verbindung darf nur dann zustande kommen, wenn:
  - das Zertifikat des Servers von einer vertrauenswürdigen CA signiert wurde,
  - für die abgefragte Domäne gilt und
  - es nicht zurückgerufen wurde.
- Inhalte aus dem Internet (Webseiten oder andere Dateien) müssen vollständig heruntergeladen, auf Schadprogramme geprüft und ggf. von aktiven Inhalten bereinigt werden. Dabei muss beachtet werden, ob die Anfrage aus der Internet-PC-Zone oder vom internen Netz ausging.
  Inhalte, die vom Server zum Datenaustausch mit dem internen Netz zu einem Client-PC übertragen werden, werden wie Internetinhalte behandelt.
- Um Bandbreite zu sparen, darf der Proxy-Server Inhalte zwischenspeichern. Es dürfen jedoch keine Inhalte gespeichert werden, für die eine Authentisierung erforderlich ist. Das Risiko durch Cache-Poisoning-Angriffe muss akzeptiert werden (siehe auch Abschnitt 5.3.4). Bestimmte Varianten von HTTP-Response-Splitting- und Cache-Poisoning-Angriffen können verhindert werden, indem der Proxy-Server Antworten, in denen mehrere `<HTML>`-Tags oder „Last-Modified“-Kopfzeilen mit einem zukünftigen Datum vorkommen, verworfen werden.
- Bei jeder Anfrage muss zudem eine Gegenprüfung anhand einer regelmäßig aktualisierten Phishing-Blacklist erfolgen. Diese Blacklist sollte heruntergeladen werden. Es sollte vermieden werden, dass bei jedem Request eine Anfrage an eine Online-Blacklist gestellt wird, da der Betreiber dieser Blacklist damit feststellen könnte, welche Seiten die Benutzer besuchen. Alternativ kann auch ein Whitelist-Ansatz verwendet werden, um nur vertrauenswürdige Webangebote zuzulassen (siehe auch Variante 5.3.2 C).

4.2.3.2 Virenschutzprogramm

- Es muss eine Liste von Dateitypen definiert werden, die erlaubt bzw. verboten sind.

- Signatur-Updates sind regelmäßig einzuspielen.
- Werden Schadprogramme in Daten gefunden, müssen diese unter Quarantäne gestellt werden.

4.2.3.3 Aktive-Inhalte-Filter

- Webseiten, die aus der Internet-PC-Zone gerufen wurden, dürfen JavaScript, VBScript, Flash, Silverlight, JavaFX und unsignierte Java-Applets enthalten. Andere aktive Inhalte benötigen eine explizite Freischaltung über eine Whitelist.
- Für Webangebote, die aus dem internen Netz heraus abgefragt wurden, muss der Aktive-Inhalte-Filter alle Arten von aktiven Inhalten außer Java-Skript entfernen.
- Inhalte, die aus der Internet-PC-Zone über den Server zum Datenaustausch mit dem internen Netz zu Client-PCs übermittelt werden, werden wie Internetinhalte behandelt.
- Verdächtige Elemente, wie etwa das `<dialog>`-Element oder seamless iframes, sollten entfernt werden.

4.3 Grundvorgaben für einen sicheren Betrieb

Wie bereits in der Grundarchitektur erläutert, sind für einen sicheren Betrieb insbesondere auch organisatorische Tätigkeiten wichtig, die in diesem Abschnitt erläutert werden. Technische Grundvorgaben für den sicheren Betrieb der Netz-Infrastruktur sind in [ISi-LANA] zu finden.

Laufende Wartung von Virenschutzprogrammen

Virenschutzprogramme werden gemäß der Konfigurationsvorgaben automatisch aktualisiert. Im laufenden Betrieb muss zudem verifiziert werden, ob die Updates auch tatsächlich funktionieren (z. B. kann das Abonnement der Signaturen abgelaufen sein). Es muss daher regelmäßig das Veröffentlichungsdatum der Signaturen durch einen Administrator überprüft werden. Dies gilt nicht nur für Clients, sondern insbesondere auch für Server, da diese häufig längere Zeit nicht über die Konsole bedient werden.

Wartung von Black- und Whitelists

Für die Freischaltung von aktiven Inhalten im internen Netz ist eine Wartung der entsprechenden Whitelists notwendig. Zudem muss eine regelmäßige Analyse der Gefährdung erfolgen, die durch die Freischaltung einer bestimmten Webseite entstehen. Besonders gefährlich ist die Freischaltung von Webseiten, auf denen beliebige Benutzer eigene Inhalte erstellen können (z. B. Kommentare zu Artikeln).

Des Weiteren muss eine Wartung der Blacklist erfolgen, auf der verzeichnet ist, welche Webseiten generell gesperrt sind. Hierfür kann auf Drittanbieter zurückgegriffen werden, die solche Listen zur Verfügung stellen (etwa um bekannte Phishing-Seiten zu sperren).

Auswertung von Log-Dateien

Die Auswertung der Logs von Virenschutzprogrammen kann helfen, um bei Infektionen rasch Gegenmaßnahmen einleiten zu können. Auf diese Weise können verseuchte Webseiten erkannt und in die Blacklist aufgenommen werden.

Geordnetes Management der Benutzer-Berechtigungen

Um sicherzustellen, dass Benutzer nur die benötigten Berechtigungen haben, muss ein geordneter Prozess existieren, der definiert, wie Berechtigungen vergeben und entzogen werden. Es wird empfohlen, Informationseigentümer zu definieren, die Berechtigungen vergeben können bzw. die Vergabe gestatten. Jede Anforderung und deren Freigabe muss dokumentiert werden.

Des Weiteren müssen Benutzerrechte regelmäßig auf Aktualität überprüft werden. Veränderungen können sich z. B. ergeben, wenn ein Mitarbeiter die Abteilung wechselt.

Regelmäßige interne und externe Überprüfungen der Infrastruktur

Zum sicheren Betrieb gehört auch die Überprüfung, ob Schwachstellen in der Implementierung der Grundarchitektur vorhanden sind. Eine regelmäßige Durchführung von internen Audits stellt sicher, dass alle Sicherheitsmaßnahmen so funktionieren wie sie konzipiert wurden. Mit Hilfe von externen Audits lassen sich zusätzliche Schwachstellen in den Sicherheitsmaßnahmen aufdecken. Bei diesen Überprüfungen sollten jedoch nicht nur technische, sondern auch organisatorische Aspekte berücksichtigt werden. Alle Richtlinien im Zusammenhang mit der Nutzung von Webangeboten gilt es regelmäßig auf etwaigen Aktualisierungsbedarf zu überprüfen.

Regelmäßige Sicherheitsbewusstseins-Schulungen für Benutzer

Das Erfordernis, Benutzer regelmäßig in Sicherheitsthemen zu schulen, wurde bereits in der Grundarchitektur erwähnt. Da sich Gefährdungen bei der Web-Nutzung sehr schnell ändern, ist ein ständiges Mitverfolgen der aktuellen Gefährdungen und eine entsprechende Schulung der Benutzer notwendig.

5 Gefährdungen und Empfehlungen mit Varianten für normalen und hohen Schutzbedarf

In diesem Abschnitt werden die Gefährdungen analysiert, denen die Grundarchitektur bei der Nutzung von Webangeboten im Internet ausgesetzt ist. Neue Web-spezifische Schwachstellen werden praktisch täglich veröffentlicht. Aus diesem Grund beschreibt die Studie Gefährdungskategorien, die allgemeine Gültigkeit besitzen.

Zu jeder Gefährdung wird dargestellt, wie die Empfehlungen der Abschnitte 3 und 4 gegen diese Gefährdungen wirken und welche Restrisiken verbleiben. Darüber hinaus werden verschiedene Varianten vorgestellt, mit denen sich die Grundarchitektur anpassen lässt. Mit einigen dieser Varianten kann dieses Restrisiko weiter reduziert werden, was jedoch mit erhöhten Aufwänden einher geht. Andere Varianten lassen sich mit weniger Aufwand umsetzen, erhöhen jedoch das Restrisiko. Es muss im Einzelfall bewertet werden, welches Restrisiko noch akzeptabel ist.

5.1 Schadprogramme

Der Begriff Schadprogramm ist ein Sammelbegriff für verschiedene Arten von bösartigen Programmen (engl. Malicious Software bzw. Malware). Es lässt sich zwischen Viren, Würmern, Spyware, Ransomware, Trojanern und vielen weiteren Arten unterscheiden.

In der Regel enthalten Schadprogramme verschiedene Funktionen wie zum Beispiel das Mitlesen von Tastatureingaben oder die Fernsteuerung des infizierten Rechners. Da die meisten Schadprogramme über das Web verteilt werden, ist bei der Nutzung von Webangeboten Vorsicht geboten.

5.1.1 Drive-By Downloads

Bedrohung: Eindringen in das interne Netz oder die Internet-PC-Zone
Schwachstelle: Auslieferung von Schadprogrammen über Webseiten

Unter einem Drive-By Download versteht man einen unbeabsichtigten Download, der durch das Besuchen einer Webseite ausgelöst wird. Diese Art von Angriff funktioniert meist über aktive Inhalte und nutzt in der Regel Sicherheitslücken in Browser, Plug-Ins oder Anwendungen, aus um den Client zu infizieren.

Ein Angreifer muss den für einen Drive-By Download notwendigen Programmcode auf einer Webseite platzieren, die sein Opfer aufruft. Es muss allerdings nicht die Hauptseite direkt sein, die vom Angreifer modifiziert wird. Oftmals kommt der Programmcode von externen Webseiten, deren Inhalte (beispielsweise Werbung) eingebunden werden.

Gegenmaßnahmen in der Grundkonfiguration:

- Alle Web-Inhalte werden sowohl am ALG als auch am Client bzw. am Internet-PC auf Schadprogramme untersucht.
- Das zentrales Patchmanagement sorgt für eine zeitnahe Aktualisierung der Browser.
- Wahl eines sicheren Browsers.
- Unerwünschte aktive Inhalte werden am ALG gefiltert.
- Der Einsatz von Plug-Ins wird auf ein Minimum reduziert.

Restrisiko für internes Netz: Gänzlich neue Schadprogramme oder solche, die speziell im Hinblick auf eine bestimmte Institution entwickelt wurden,

können nicht erkannt werden.

Restrisiko für Internet-PC-Zone: Kein erhöhtes Restrisiko.

5.1.1 A Zusätzliche Variante für normalen und hohen Schutzbedarf: Eigener Benutzer für Web-Nutzung

Anwendungsbereich: normaler und hoher Schutzbedarf
Phase im Ablaufplan: Umsetzung

> Für Clients im internen Netz kann ein eigener Benutzer angelegt werden, der nur die minimal benötigten Rechte auf lokale Ressourcen besitzt und ausschließlich zur Web-Nutzung verwendet wird. Da bei Software-Schwachstellen, mit denen Code ausgeführt werden kann, meist die Rechte des aktuell eingeloggten Benutzers übernommen werden, kann diese Maßnahme helfen, im Fall einer Kompromittierung den Schaden gering zu halten. Eine Möglichkeit, diese Variante umzusetzen, ist es, den Browser unter einem dedizierten Web-Benutzerkonto laufen zu lassen. Alternativ dazu kann eine sogenannte Change-Root-Umgebung installiert werden, in welcher der Browser gestartet wird. Diese Umgebung ist zwar für den Benutzer transparent, jedoch vom Rest des Betriebssystems abgeschottet. Daher muss ein Angreifer erst aus dem Change-Root ausbrechen, um an die Daten des internen Netzes zu gelangen.
>
> Diese Maßnahme ist als nur als Ergänzung zu anderen Varianten sinnvoll und nicht zur Vereinfachung der Grundarchitektur geeignet.

Restrisiko für internes Netz: Diese Maßnahme verhindert die Kompromittierung nicht, kann jedoch helfen, den Schaden in Grenzen zu halten. Programme, die mit erhöhten Benutzerrechten laufen, stellen weiterhin ein Risiko dar.

Restrisiko für Internet-PC-Zone: Diese Variante kann nur im internen Netz angewandt werden, da in der Internet-PC-Zone ohnehin ein eigener Benutzer zum Web-Surfen eingesetzt wird.

Umsetzungsaufwand: Die Umsetzung der Variante verursacht einen mittelgroßen Konfigurationsaufwand, da für jeden Mitarbeiter (mindestens) zwei Accounts eingerichtet und gewartet werden müssen. Je nach Implementierung entsteht auch erhöhter Aufwand aufseiten des Benutzers bei der Verwendung von Webangeboten aus dem internen Netz.

5.1.1 B Variante für hohen Schutzbedarf: Verzicht auf JavaScript

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit
Phase im Ablaufplan: Umsetzung

> Bei hohem Schutzbedarf sollte auf den Browsern im internen Netz auf JavaScript zu verzichten. Das ALG muss dazu auch JavaScript ausfiltern. Auch der Browser im internen Netz sollte so konfiguriert werden, dass er keine aktiven Inhalte ausführt.

Restrisiko für internes Netz: Mit dieser Maßnahme wird der Gefährdung ausreichend begegnet.

Restrisiko für Internet-PC-Zone: Für die Internet-PC-Zone ist diese Maßnahme nicht angemessen, da sie dem Konzept der freien Internetnutzung in der Internet-Zone widerspricht.

Umsetzungsaufwand: Der Umsetzungsaufwand ist gering. Der Benutzerkomfort wird durch diese Maßnahme stark eingeschränkt, da die Nutzung von JavaScript nur in der Internet-PC-Zone möglich ist.

5.1.2 Downloads

Bedrohung: Eindringen in das interne Netz oder in die Internet-PC-Zone
Schwachstelle: Öffnen von Schadprogrammen durch die Benutzer

Eine Infektion mit Schadcode kann auch erfolgen, wenn ein Benutzer eine infizierte Datei herunterlädt und diese ausführt.

Gegenmaßnahmen in der Grundkonfiguration:

- Alle Web-Inhalte werden sowohl am ALG als auch am Client bzw. am Internet-PC auf Schadprogramme untersucht.
- Schulungen zur sicherheitsbewussten Web-Nutzung helfen den Benutzern Schadprogramme zu erkennen.

Restrisiko für internes Netz: Gänzlich neue Schadprogramme oder solche, die speziell im Hinblick auf eine bestimmte Institution entwickelt wurden, können nicht erkannt werden.
Restrisiko für Internet-PC-Zone: Kein erhöhtes Restrisiko.

5.1.2 A Variante für hohen Schutzbedarf: Erneute, zeitlich versetzte Überprüfung für Dateien aus dem Web

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit
Phase im Ablaufplan: Konzeption

Bei Implementierung dieser Variante wird eine Kopie aller Dateien, die von den Benutzern aus dem Web geladen werden, für mehrere Stunden oder Tage temporär auf einem eigenen System abgelegt. Nach Veröffentlichung aktualisierter Signaturen erfolgt eine neuerliche Überprüfung der Kopien auf Schadprogramme. Dadurch können auch Schadprogramme, für die zum Zeitpunkt des Herunterladens noch keine Virenschutz-Signaturen existierten, zumindest im Nachhinein identifiziert werden.

Restrisiko für internes Netz: Die beschriebene Variante kann nicht vor der Infektion mit Schadprogrammen schützen, sondern ermöglicht lediglich kürzere Reaktionszeiten, sollte ein Sicherheitsvorfall eintreten. Speziell auf die Institution zugeschnittene Schadprogramme können auch mit dieser Variante nicht identifiziert werden.
Restrisiko für Internet-PC-Zone: Da die Maßnahme am Sicherheits-Gateway implementiert wird, besteht für die Internet-PC-Zone im Vergleich zum internen Netz kein erhöhtes Restrisiko.
Umsetzungsaufwand: mittelgroßer Konfigurationsaufwand am Virenschutz-System

5.1.3 Ausnutzung von Software-Schwachstellen

Bedrohung: Eindringen in das interne Netz, die Internet-PC-Zone, das Sicherheits-Gateway
Schwachstelle: Software-Schwachstellen

Einige Schadprogramme verbreiten sich aktiv durch das Ausnutzen von Software-Schwachstellen weiter. Ein prominentes Beispiel ist der Computerwurm *Conficker*, der im Jahre 2009 mehrfach für Pressemeldungen sorgte. Dieser Wurm hat eine Schwachstelle ausgenutzt, die mehrere Microsoft Windows Versionen betroffen hat und die Ausführung von Programmcode erlaubte. Neben Software-Schwachstellen hat Conficker auch Netzwerkfreigaben zur Weiterverbreitung verwendet.

Gegenmaßnahmen in der Grundkonfiguration und im Betrieb:

- Patch-Management gemäß [ISi-E]
- Minimalprinzip
- Alle Web-Inhalte werden sowohl am ALG als auch am Client bzw. am Internet-PC auf Schadprogramme untersucht.

Restrisiko für internes Netz:	Sogenannte Zero-Day-Schwachstellen – also Software-Fehler, die noch nicht veröffentlicht wurden – stellen ein Sicherheitsrisiko dar, dem nur sehr schwer durch schützende Maßnahmen begegnet werden kann. Auch die Zeitspanne zwischen der Veröffentlichung einer Schwachstelle und dem Einspielen eines entsprechenden Patches bedeutet eine Gefährdung der Systeme.
Restrisiko für Internet-PC-Zone:	Da in der Internet-PC-Zone mehr Inhalte zugelassen sind als im internen Netz, besteht dort ein erhöhtes Restrisiko.

5.2 Aktive Inhalte

Aktive Inhalte können von Angreifern entweder aufgrund von Software-Schwachstellen im Interpreter der Inhalte oder durch Konfigurations- bzw. Verhaltensfehler ausgenutzt werden, um in die Systeme der Institution einzudringen. Da Software-Schwachstellen präventiv kaum zu verhindern sind (siehe Abschnitt 5.1.3), wird im folgenden Abschnitt nur auf Konfigurations- und Verhaltensfehler eingegangen. Im internen Netz sollten aktiven Inhalte daher restriktiv gehandhabt werden.

5.2.1 Java-Applets

Bedrohung: Eindringen in die Internet-PC-Zone oder das interne Netz
Schwachstelle: Verwendung von bösartigen oder unsicheren Webangeboten

Die Entwickler signierter Java-Applets können selbst definieren, ob die von der Java-Sandbox zur Verfügung gestellten Rechte ausreichen oder ob weitere Rechte (etwa der Zugriff auf lokale Ressourcen) für die Ausführung erforderlich sind. Soll ein signiertes Applet mit erweiterten Rechten geladen werden, erhält der Benutzer eine Sicherheitswarnung, die jedoch leicht missverstanden werden kann (siehe Abbildung 5.1).

Abbildung 5.1: Sicherheitswarnung beim Laden eines signierten Java-Applets

Erst ein Klick auf den Link Weitere Informationen ... offenbart, dass das Applet weitergehende Rechte erlangt, wenn die Ausführung akzeptiert wird. Handelt es sich um bösartigen Code, kann das signierte Applet in das lokale System des Benutzers eindringen.

Natürlich können auch gutartige Applets Schwachstellen enthalten, die ein Angreifer missbrauchen kann, um den Client zu kompromittieren. Die Ausführung unsignierter Applets ist nicht unproblematisch, da in der Vergangenheit der Ausbruch aus der Sandbox über längere Zeiträume möglich gewesen ist.

Gegenmaßnahmen in der Grundkonfiguration:

- Signierte Java-Applets werden vom Aktive-Inhalte-Filter sowohl für das interne Netz als auch für die Internet-PC-Zone gefiltert (in der Internet-PC-Zone können vertrauenswürdige Java-Applets per Whitelist freigeschaltet werden).
- Die Ausführung signierter Java-Applets ist bei allen Browsern (sowohl im internen Netz als auch in der Internet-PC-Zone) generell deaktiviert. Einzelne Java-Applets können per Whitelist freigeschaltet werden.

Restrisiko für internes Netz:	Für normalen und hohen Schutzbedarf sind diese Maßnahmen ausreichend.
Restrisiko für Internet-PC-Zone:	Da in der Internet-PC-Zone signierte Java-Applets freigeschaltet werden dürfen, besteht im Vergleich zum internen Netz ein erhöhtes Restrisiko aufgrund eventueller Schwachstellen in erlaubten Applets.

5.2.2 ActiveX-Controls und COM-Komponenten

Bedrohung: Eindringen in das interne Netz oder die Internet-PC-Zone
Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Registrierte und installierte ActiveX-Controls haben Zugriff auf lokale Ressourcen und können beliebigen Code mit den Rechten des aktuell eingeloggten Anwenders ausführen. Damit ein ActiveX-Control Schaden am System anrichten kann, muss der Benutzer eine neue Komponente, die bösartigen Code enthält, explizit akzeptieren. Alternativ dazu können jedoch auch Schwachstellen in bereits installieren Controls, die als Safe for Scripting markiert sind, zur Kompromittierung führen.

Neben ActiveX-Controls werden auch COM-Komponenten unter bestimmten Umständen im Browser geladen und ausgeführt. Bei Schwachstellen in registrierten COM-Komponenten kann ein Angreifer aus dem Internet Zugriff auf lokale Ressourcen erlangen und beliebigen Code ausführen.

Gegenmaßnahmen in der Grundkonfiguration:

- ActiveX-Controls und COM-Komponenten werden vom Aktive-Inhalte-Filter sowohl für das interne Netz als auch für die Internet-PC-Zone gefiltert.
- Die Ausführung von ActiveX-Controls und COM-Komponenten ist bei allen Browsern (sowohl im internen Netz als auch in der Internet-PC-Zone) deaktiviert. Einzelne Komponenten können per Whitelist freigeschaltet werden.

Restrisiko für internes Netz:	Für normalen und hohen Schutzbedarf sind diese Maßnahmen ausreichend.
Restrisiko für Internet-PC-Zone:	Da in der Internet-PC-Zone bestimmte aktive Inhalte freigeschaltet werden dürfen, besteht im Vergleich zum internen

Netz ein erhöhtes Restrisiko aufgrund eventueller Schwachstellen in erlaubten ActiveX-Controls oder COM-Komponenten.

5.2.2 A Variante für hohen Schutzbedarf: Einsatz eines ReCoBS

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit
Phase im Ablaufplan: Konzeption

Ein Remote-Controlled Browsers System (ReCoBS) ermöglicht die Nutzung von Webangeboten mit aktiven Inhalten vom Arbeitsplatz-PC aus und ist somit eine Alternative zur Internet-PC-Zone.

Der Nutzer verbindet sich über ein Terminal-Server-Protokoll (TSP) mit dem ReCoBS und öffnet dort das gewünschte Webangebot im Browser. Potenziell gefährliche Inhalte werden damit auf einem sicher konfigurierten Terminal-Server ausgeführt. Lediglich die Bild-Informationen werden zum APC ins interne Netz übertragen. Die Kommunikation zwischen dem internen Netz und dem Terminal-Server muss über einen TSP-Proxy im ALG geleitet werden.

Um zu verhindern, dass ein Angreifer im Fall einer Kompromittierung die im ReCoBS gesammelten Authentisierungsmerkmale auch im internen Netz verwenden kann, kommt ein eigener Verzeichnis-Server zur Speicherung von Benutzer-Accounts zum Einsatz. Abbildung 5.2 zeigt die Integration des ReCoBS in die Grundarchitektur.

Je nach Anzahl der gleichzeitigen Anwender kann gegebenenfalls ein Load-Balancer zwischen mehreren ReCoBS-Servern benötigt werden. Der Terminal-Server sollte regelmäßig mit einem als sicher verifizierten Festplatten- oder CD-Abbild neu aufgesetzt werden. Dabei werden Hintertüren geschlossen, die ein Angreifer bei einer eventuell unbemerkten Kompromittierung installiert hat.

Da eine Verbindung lediglich vom internen Netz zum ReCoBS, nicht jedoch umgekehrt möglich ist, muss eine Schnittstelle zum Speichern und Drucken von Informationen geschaffen werden. Dazu kann der in der Grundarchitektur beschriebene Server zum Datenaustausch mit dem internen Netz verwendet werden (siehe Abschnitt 3.2).

In Bezug auf die Konfiguration der Systeme müssen auf allen eingesetzten Komponenten Personal Firewalls installiert werden. Der gesamte Netzverkehr muss über das ALG erfolgen, sodass die abgefragten Webangebote auf Schadprogramme und verbotene aktive Inhalte untersucht werden können.

Die Anforderungen an ein ReCoBS sind in [ReCoBS] detailliert beschrieben. Bei hohem Schutzbedarf sind alle Anforderungen zu erfüllen. Benötigt man ein ReCoBS nur bei normalem Schutzbedarf können einzelne Anforderungen verringert werden. Derartige Änderungen sind jedoch einer Risikoanalyse zu unterziehen. Ein Beispiel ist die von den Benutzern gewünschte Copy-and-Paste-Funktion. Ein aktivieren dieser Funktion ermöglicht dem Terminal-Server aus der DMZ heraus auf die Zwischenablage der Clients und damit auf die dort gespeicherten vertraulichen Daten zuzugreifen. Bei normalen Schutzbedarf kann unter Abwägung des Risikos dieses Vorgehen jedoch akzeptabel sein, bei hohem Schutzbedarf ist davon abzuraten.

Restrisiko: Wird das ReCoBS von einem Angreifer kompromittiert, kann der gesamte Web-Verkehr, der über das ReCoBS erfolgt,

abgehört werden.

Restrisiko für Internet-PC-Zone: Diese Variante ersetzt die Internet-PC-Zone.

Umsetzungsaufwand: Die Verwendung eines ReCoBS bedeutet anfangs einen hohen Beschaffungs- und Konfigurationsaufwand. Dieser Aufwand kann jedoch unter Umständen durch die bequemere und unkomplizierte Nutzung von Webangeboten mit aktiven Inhalten durch die Anwender ausgeglichen werden.

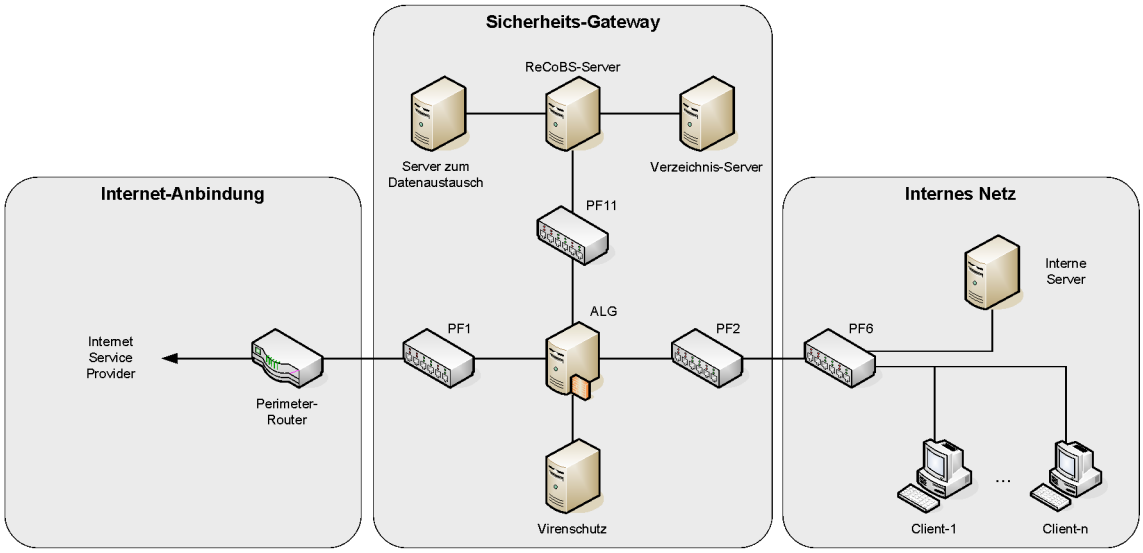


Abbildung 5.2: Sichere Grundarchitektur bei Einsatz von ReCoBS

5.2.2 B Variante für hohen Schutzbedarf: Virtuellen Maschinen auf dem ReCoBS-Server

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit

Phase im Ablaufplan: Konzeption

Eine Trennung zwischen einzelnen Benutzern wird erreicht, wenn als Ergänzung von Variante 5.2.2 A jeder Benutzer eine eigene virtuelle Maschine am ReCoBS-Server startet. Wird eine virtuelle Maschine kompromittiert, hat der Angreifer nur auf die betroffene Instanz des Systems Zugriff. Somit kann zwar die Web-Nutzung eines Benutzers mitverfolgt werden, nicht jedoch jene aller Anwender. Daraus ergibt sich ein Sicherheitsvorteil gegenüber dem herkömmlichen ReCoBS.

Da der Betrieb einer virtuellen Maschine deutlich mehr Ressourcen benötigt als die Bereitstellung einer Terminal-Server-Sitzung, können bei Umsetzung dieser Variante deutlich weniger Benutzer pro physischem System bedient werden.

Restrisiko: Über Schwachstellen in der Software, welche die virtuellen Maschinen bereitstellt, könnte es einem Angreifer gelingen, auf das Host-System zu gelangen und somit wieder den Web-Verkehr aller Benutzer abzuhören. Das Risiko ist jedoch geringer als in Variante 5.2.2 A.

Restrisiko für Internet-PC-Zone: Diese Variante ersetzt die Internet-PC-Zone.

Umsetzungsaufwand: Für den Betrieb der virtuellen Maschinen sind mehr Ressourcen

erforderlich. Dieser Variante verursacht daher einen höheren Beschaffungsaufwand als Variante 5.2.2 A.

5.2.2 C Variante für hohen Schutzbedarf: Konsolidierung der ReCoBS-Komponenten über virtuelle Maschinen

Anwendungsbereich: hoher Schutzbedarf (wenige Anwender)
Phase im Ablaufplan: Konzeption

Durch den Einsatz von virtuellen Maschinen können die einzelnen Komponenten des ReCoBS in Variante 5.2.2 A (Terminal-Server, Verzeichnis-Dienst und System zum Datenaustausch mit dem internen Netz) konsolidiert und auf einem einzigen physischen System betrieben werden. Diese Variante darf nicht mit der in Abschnitt 5.2.2 B beschriebenen verwechselt werden. Der Unterschied besteht darin, dass die virtuellen Maschinen hier nicht zur Trennung der Benutzer dienen, sondern zur Konsolidierung der eingesetzten Hardware. Aus Performance-Gründen ist es insbesondere für kleinere Institution mit wenigen gleichzeitigen Benutzern geeignet.

Restrisiko: Sollte der ReCoBS-Server kompromittiert werden, kann ein Angreifer unter Umständen durch Schwachstellen in der Software, welche die virtuellen Maschinen bereitstellt, auf das Host-System gelangen. Von dort aus ist auch der Zugriff auf den Verzeichnis-Server und das System zum Datenaustausch mit dem internen Netz möglich. Dieses Restrisiko ist jedoch recht gering und kann mit Hilfe von Patch-Management gut kontrolliert werden.

Restrisiko für Internet-PC-Zone: Diese Variante ersetzt die Internet-PC-Zone.

Umsetzungsaufwand: Aufgrund der Konsolidierung der ReCoBS-Komponenten und der Einsparung der Internet-PC-Zone bedeutet diese Variante im Vergleich zur Grundarchitektur normalerweise keinen erhöhten Beschaffungsaufwand. Durch die Notwendigkeit, einen Verzeichnis-Dienst betreiben zu müssen, kann der Konfigurationsaufwand unter Umständen geringfügig größer sein. Im Gegenzug ergibt sich durch das ReCoBS eine bequemere und unkomplizierte Nutzung von Webangeboten mit aktiven Inhalten.

5.3 Vortäuschen vertrauenswürdiger Web-Inhalte

Angriffe wie Phishing (Abschnitt 5.4.1) werden durch das Vortäuschen vertrauenswürdiger Inhalte noch effizienter. In vielen Fällen liegen die Schwachstellen in den genutzten Webangeboten und auf der Client-Seite. Da die Angriffe in erster Linie jedoch den Client schädigen, ist es wichtig, die existierenden Angriffsvarianten zu kennen.

5.3.1 Cross-Site Scripting (XSS) und HTML-Injection

Bedrohung: Fälschen von Web-Inhalten
Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Sowohl Cross-Site Scripting (häufig mit „XSS“ abgekürzt) als auch HTML-Injection ermöglicht es einem Angreifer, dem Opfer auf vertrauenswürdigen Webangeboten nicht vertrauenswürdige Inhalte zu präsentieren. Während bei Cross-Site Scripting aktive Inhalte verwendet werden, muss sich der Angreifer bei HTML-Injection auf statische HTML-Inhalte beschrän-

ken. Meist können Cross-Site-Scripting-Schwachstellen auch für HTML-Injection genutzt werden.

Unterschieden wird zwischen permanenten und flüchtigen Cross-Site-Scripting- und HTML-Injection-Schwachstellen. Während bei der permanenten Variante Inhalte dauerhaft verändert werden können, muss ein Angreifer bei flüchtigem Cross-Site Scripting den Code etwa in einem Link transportieren.

Für die Ausnutzung einer flüchtigen HTML-Injection-Schwachstelle übermittelt der Angreifer seinem Opfer meist eine Mail mit einem Link. In den URL-Parametern des Links werden Web-Inhalte angegeben, die beim Öffnen des anfälligen Webangebots dargestellt werden. Der Angreifer könnte beispielsweise ein zweites Login-Formular auf der Webseite anzeigen lassen. Gibt das Opfer seinen Benutzernamen und das Passwort in dieses Formular ein, werden seine Daten nicht an das vertrauenswürdige Webangebot, sondern an den Angreifer gesandt.

Permanente Cross-Site-Scripting- und HTML-Injection-Schwachstellen sind beispielsweise bei Foren oder Gästebüchern zu finden, bei denen ein Angreifer dauerhaft Inhalte ablegen kann, indem er diese z. B. in einen Gästebucheintrag einbettet.

Da sich die Schwachstellen durch fehlerhafte Eingaben-Filterung im genutzten (vertrauenswürdigen) Webangebot begründen, müssen sie auch dort behoben werden (siehe hierzu auch [ISi-Web-Server]).

Gegenmaßnahmen in der Grundkonfiguration:

- Schulungen zur sicherheitsbewussten Web-Nutzung helfen den Benutzern, Angriffe zu erkennen.

Restrisiko für internes Netz:	Die Benutzer im internen Netz sind anfällig für HTML-Injection-Angriffe, da gegen diese zurzeit keine technischen Maßnahmen möglich sind.
Restrisiko für Internet-PC-Zone:	In der Internet-PC-Zone können aufgrund der zugelassenen aktiven Inhalte sowohl Cross-Site-Scripting- als auch HTML-Injection-Angriffe durchgeführt werden. Daher besteht ein deutlich erhöhtes Restrisiko gegenüber dem internen Netz.

5.3.2 Clickjacking

Bedrohung: Ausführen ungewollter Aktionen auf Webseiten
Schwachstelle: Täuschung des Benutzers

Beim Clickjacking wird die Darstellung einer Webseite durch eine andere Webseite überlagert. Der Angreifer verleitet den Benutzer dazu, auf der angezeigten Seite „Klicks“ durchzuführen, die auf der überlagerten Seite Aktionen ausführen.

Durch die Überlagerung von Web-Inhalten der vom Anwender aufgerufenen Web-Applikation durch unsichtbare (transparente) HTML-Elemente eines Angreifers kann dem Anwender eine reguläre Nutzung der Web-Applikation vorgetäuscht werden, während er mit den HTML-Elementen des Angreifers interagiert. So kann ihm z. B. eine Passworteingabe in seiner Web-Applikation vorgetäuscht werden, obwohl er die Anmeldedaten in für ihn nicht sichtbare Eingabefelder eines Formular des Angreifers eingibt. Ein Klick auf den Anmelde-Button führt dann nicht zur gewünschten Anmeldung, sondern zum Übertragen der Daten an einen Server des Angreifers.

Die wirksamsten Maßnahmen gegen Clickjacking kann der Betreiber der Webseite ergreifen, z. B. indem er der Webseite einen sogenannten Framebuster hinzufügt. Dabei handelt es sich um

JavaScript-Code, der die Darstellung in einem einem Frame unterbinden soll. Es gibt jedoch auch Angriffe, die diese Art von Schutz umgehen können. Besser ist das Setzen des `X-Frame-Options` Headers mit dem Wert `SAMEORIGIN` oder `DENY` durch den Webserver.

Gegenmaßnahmen in der Grundkonfiguration:

- Sensible Webangebote werden durch direkte Eingabe der URL und nicht per Klick auf Links aufgerufen
- Ausfiltern verdächtiger Code-Stellen am ALG

Restrisiko: Die Anti-Clickjacking-Maßnahmen können keinen absoluten Schutz gegen solche Angriffe bieten, fangen aber viele Versuche ab. Der Betreiber der Webseite sollte Maßnahmen zur Absicherung seiner Webanwendungen umsetzen.

5.3.2 A Variante für normalen Schutzbedarf: Verwendung gutartiger Browser-Erweiterungen

Anwendungsbereich: normaler Schutzbedarf bezüglich Vertraulichkeit und Integrität
Phase im Ablaufplan: Konfiguration

Es gibt Browser-Erweiterungen die einen Schutz gegen Clickjacking-Angriffe beinhalten. Diese Plug-Ins können jedoch erfassen, welche Webseiten besucht wurden und somit Profile über das Surfverhalten des Nutzers erstellen.

Restrisiko für internes Netz: Die Maßnahme ist für normalen Schutzbedarf ausreichend.
Restrisiko für Internet-PC-Zone: Die Maßnahme ist für normalen Schutzbedarf ausreichend.
Umsetzungsaufwand: Diese Variante verursacht einen geringen Aufwand.

5.3.2 B Variante für hohen Schutzbedarf: Blockieren von Webseiten mit Frames

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit und/oder Integrität
Phase im Ablaufplan: Umsetzung

Mit Hilfe des Aktive-Inhalte-Filters können zusätzlich zu aktiven Inhalten auch Webangebote mit Frames blockiert werden. Einzelne Angebote, die keine hohen Anforderungen an Vertraulichkeit und Integrität stellen, können mittels Whitelist-Ansatz explizit zugelassen werden. Die Verwendung von Frames auf Webseiten ist heute nicht mehr üblich wie noch vor einigen Jahren. Daher ist nur mit geringen Einschränkungen zu rechnen wodurch der Aufwand zur Pflege der Whitelist überschaubar bleibt.

Restrisiko für internes Netz: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.
Restrisiko für Internet-PC-Zone: Diese Maßnahme ist für die Internet-PC-Zone nicht angemessen. Daher besteht dort weiterhin erhöhtes Restrisiko.
Umsetzungsaufwand: Die Implementierung der Variante verursacht einen geringen Konfigurationsaufwand. Webseiten, die Frames benutzen müssen im Betrieb zur Whitelist hinzugefügt werden.

5.3.2 C Variante für hohen Schutzbedarf: Einschränkung zugelassener Webangebote nach Whitelist-Ansatz

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit, Integrität oder Verfügbarkeit
Phase im Ablaufplan: Umsetzung

Bei hohem Schutzbedarf besteht die Möglichkeit, im internen Netz nur vertrauenswürdige Webangebote – basierend auf einem Whitelist-Ansatz – zuzulassen.

Dadurch kann die Gefahr minimiert werden, dass unbeabsichtigt gefälschte oder bösartige Webangebote aus dem internen Netz besucht werden.

Bei Umsetzung dieser Maßnahme dürfen die Benutzer ausschließlich explizit erlaubte Webseiten besuchen, was eine drastische Einschränkung der Anwender zur Folge hat. Aus diesem Grund ist die Variante auch bei hohem Schutzbedarf optional.

Restrisiko für internes Netz: Mittels HTML-Injection- oder HTTP-Response-Splitting-Schwachstellen in den zugelassenen Webangeboten können trotz dieser Variante nicht-vertrauenswürdige Inhalte eingeschleust werden.

Restrisiko für Internet-PC-Zone: Die Maßnahme ist für die Internet-PC-Zone nicht angemessen.

Umsetzungsaufwand: Die Implementierung der Variante verursacht zwar nur einen geringen Konfigurationsaufwand, es ist jedoch im Betrieb eine laufende Wartung der Whitelist notwendig. Zudem muss ein Prozess existieren, um Seiten der Whitelist hinzuzufügen, und die Benutzer werden zusätzlich eingeschränkt, da viele Webseiten nicht mehr nutzbar sind.

5.3.3 URL-Spoofing

Bedrohung: Fälschen der angezeigten URL

Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Bei URL-Spoofing wird eine andere URL angezeigt, als eigentlich dem aktuell besuchten Webangebot entsprechen würde. Da Benutzer Webangebote meist anhand der angezeigten URL identifizieren, kann ein Vertrauensverhältnis vorgetäuscht werden. Während beim Link-Spoofing (ein Link führt zu einer anderen Seite als im Link-Text angegeben) die tatsächliche URL i.d.R. in der Statusleiste sichtbar ist, ist die Manipulation beim URL-Spoofing für den Benutzer nicht unmittelbar erkennbar.

Beispielsweise könnte ein Angreifer mittels HTML-Injection eine nicht vertrauenswürdige Seite in einem eingebetteten Frame darstellen. Da Browser stets die URL des übergeordneten Frame-Sets anzeigen, hätte der Benutzer nicht die Möglichkeit, auf den ersten Blick die Herkunft des Frames selbst zu erkennen. Außerdem werden immer wieder Software-Fehler bekannt, die das Fälschen der angezeigten URL ermöglichen.

Ein Teil der existierenden Schwachstellen kann durch die Umsetzung der Variante 5.3.2 B verhindert werden.

Gegenmaßnahmen in der Grundkonfiguration:

- Schulungen zur sicherheitsbewussten Web-Nutzung helfen den Benutzern, Angriffe zu erkennen.

Restrisiko für internes Netz: Bei Schwachstellen im Browser oder Sicherheitslücken im genutzten Webangebot kann URL-Spoofing möglich sein.

Restrisiko für Internet-PC-Zone: Bei Schwachstellen im Browser oder Sicherheitslücken im genutzten Webangebot kann URL-Spoofing möglich sein.

5.3.4 HTTP-Response Splitting und Web-Cache Poisoning

Bedrohung: Fälschen von Web-Inhalten

Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

HTTP-Response Splitting ähnelt von der Funktionsweise stark den Angriffen Cross-Site Scripting und HTML-Injection. Anstatt Inhalte direkt in die Ausgabe der Webanwendung ein-

zuschleusen, werden sie bei HTTP-Response Splitting jedoch in die HTTP-Header eingefügt. Da diese Kopfzeilen auf der Client-Seite erzeugt und auf dem Server nicht gespeichert werden, sind hier permanente Angriffe nur in Verbindung mit anderen Angriffen möglich. Eine Möglichkeit zur Ausnutzung dieser Gefährdung stellen Hyperlinks dar, in welche die gefälschten Inhalte eingebettet werden.

In Verbindung mit Web-Cache Poisoning kann der Angriff auch zu einem semi-permanenten Angriff werden. Dazu manipuliert ein Angreifer die „Last-Modified"-Kopfzeile und fügt der HTTP-Antwort einen gefälschten Inhalt an. Dieser wird im Cache des ALG bzw. dem Cache des Browsers gespeichert und bei jeder neuen Anfrage an den Client zurückgeliefert. Erst wenn der Cache seine Gültigkeit verliert oder das Webangebot eine neue Version der Seite veröffentlicht, werden die „vergifteten" Inhalte überschrieben. Analog zum beschriebenen Cache-Poisoning sind auch Angriffe auf den Application-Cache von HTML5-Offline-Appliaktionen denkbar.

Auch bei HTTP-Response Splitting handelt es sich um eine Schwachstelle auf Webanwendungsebene. Gegenmaßnahmen auf Clientseite können daher lediglich versuchen, solche Angriffe auf Basis einzelner Symptome zu erkennen und zu unterbinden. Die Behebung der Schwachstelle selbst ist nur von Seiten des Webangebot-Betreibers möglich (siehe [ISi-Web--Server].

Gegenmaßnahmen in der Grundkonfiguration:

- Um Web-Cache-Poisoning-Angriffen vorzubeugen, verwirft das Sicherheits-Gateway Anfragen, bei denen die Last-Modified-Kopfzeile mit einem Datum in der Zukunft versehen ist.
- HTTP-Antworten mit mehreren <HTML>-Tags werden vom Sicherheits-Gateway gefiltert.

Restrisiko für internes Netz:	Das Fälschen von Web-Inhalten durch HTTP-Response Splitting kann auf Nutzer-Seite nicht vollständig verhindert werden. Die Maßnahmen gegen Web-Cache Poisoning helfen nicht, wenn der Angreifer das „Last-Modified"-Datum auf den aktuellen Wert setzt. Der Web-Cache bleibt dann solange „vergiftet", bis das Webangebot eine neuere „Last-Modified"-Kopfzeile schickt oder der Cache verfällt.
Restrisiko für Internet-PC-Zone:	kein erhöhtes Restrisiko

5.3.4 A Variante für hohen Schutzbedarf: Kein Caching

Anwendungsbereich: hoher Schutzbedarf bezüglich Integrität
Phase im Ablaufplan: Umsetzung

Um Web-Cache-Poisoning-Angriffe zu verhindern, kann das Caching von Webseiten sowohl auf den Browsern des internen Netzes und der Internet-PC-Zone als auch am HTTP-Proxy des ALG deaktiviert werden. Dadurch wird jede Web-Anfrage an den entsprechenden Server im Web weitergeleitet. Dies geschieht unabhängig davon, ob die Abfrage in jüngster Vergangenheit bereits durchgeführt wurde und eine zwischengespeicherte Version der Antwort im Cache liegt. Das temporäre Caching zur Überprüfung der heruntergeladenen Inhalte auf aktive Inhalte und Schadprogramme wird nicht eingeschränkt.

Bei der Umsetzung dieser Maßnahme muss darauf geachtet werden, dass bei deaktiviertem Caching mit deutlich erhöhtem Netzverkehr in das Web zu rechnen ist. Dies könnte unter Umständen zu einer höheren Auslastung der Internet-Verbindung sowie

zu erhöhtem Download-Volumen führen. Zudem sollte sichergestellt werden, dass auch aufseiten des Providers kein Caching stattfindet.

Restrisiko: Diese Variante beseitigt die Gefährdung „Web-Cache Poisoning“ sowohl für das interne Netz als auch für die Internet-PC-Zone bei normalem und hohem Schutzbedarf. Flüchtige Angriffe mittels HTTP-Response Splitting können jedoch trotz der Implementierung dieser Variante ausgenutzt werden.

Umsetzungsaufwand: Geringer Konfigurationsaufwand aber eine höhere Auslastung der Internet-Verbindung

5.3.5 Cross-User Defacement

Bedrohung: Fälschen von Web-Inhalten

Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

HTTP-Response-Splitting-Schwachstellen (siehe Abschnitt 5.3.4) können von einem Angreifer ausgenutzt werden, um mit nur einer HTTP-Anfrage zwei Antworten zu generieren. Das wird möglich, wenn es dem Angreifer gelingt, Text und Zeilenumbrüche in den HTTP-Header einzuschleusen und so einen zweiten gültigen Header zu erzeugen. Teilen sich zwei Anwender (etwa aufgrund eines gemeinsam genutzten Proxy-Servers) eine TCP-Verbindung, kann die zweite Antwort des Servers einem anderen Benutzer zugeordnet werden. Dieser erhält dadurch die gefälschten Inhalte, welche vom Anwender nicht von der tatsächlichen Antwort unterschieden werden können.

Gegenmaßnahmen in der Grundkonfiguration:

- Der HTTP-/HTTPS-Proxy-Server im Sicherheits-Gateway betreibt kein Connection-Sharing zwischen Benutzern.

Restrisiko: Die Grundarchitektur beseitigt die Gefährdung „Cross-User Defacement“ sowohl für das interne Netz als auch für die Internet-PC-Zone bei normalem und hohem Schutzbedarf. Dies gilt allerdings nur unter der Voraussetzung, dass kein Proxy-Server auf der Seite des Providers zum Einsatz kommt.

5.3.6 Redirection-Attack

Bedrohung: Fälschen von Web-Inhalten

Schwachstelle: (Unbeabsichtigte) Verwendung von gefälschten Webangeboten

Bei Redirection-Attacks (Angriffen durch Umleitung) wird der Benutzer nach dem Click auf einen Hyperlink auf eine andere Seite als erwartet weitergeleitet. Dazu wird häufig ein anfälliges Skript auf einer vertrauenswürdigen Seite genutzt, das den Besucher auf eine andere URL umleitet. Alternativ dazu ist auch eine Weiterleitung über eingeschleuste aktive Inhalte möglich. Viele Webseiten bieten eine solche Funktion beispielsweise an, um die Weiterleitung zu anderen Webseiten zu ermöglichen. Die Webseite, zu der der Benutzer gelangen soll, wird dabei häufig als Parameter in der URL angegeben. Dieser kann von einem Angreifer manipuliert werden.

Die Gefährdung basiert darauf, dass Anwender meist nur den Domänen-Teil einer URL überprüfen, um die Vertrauenswürdigkeit eines Webangebots zu verifizieren.

Gegenmaßnahmen in der Grundarchitektur und im Betrieb:

- Schulung der Benutzer zur sicherheitsbewussten Nutzung des Webs
- Restriktive Handhabung aktiver Inhalte werden im internen Netz

Restrisiko im internen Netz: „Normale“ Weiterleitungen von anfälligen Webangeboten können weiterhin für diesen Angriff missbraucht werden.
Restrisiko für Internet-PC-Zone: In der Internet-PC-Zone besteht kein Schutz gegen diesen Angriff (weder gegen die Weiterleitung mittels aktiver Inhalte noch gegen anfällige Weiterleitungen vertrauenswürdiger Webangebote). Es ist zurzeit technisch nicht möglich, diese Art von Angriffen zu unterbinden, ohne dabei gleichzeitig den Funktionsumfang einzuschränken.

5.3.7 Anti-DNS-Pinning

Bedrohung: Entwenden vertraulicher/interner Informationen
Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Bei DNS-Pinning handelt es sich um eine Sicherheitsmaßnahme von Browsern, die dazu dient, die Änderung der zu einem Domänen-Namen gehörigen IP-Adresse während einer Sitzung zu unterbinden, da so die Same-Origin-Policy umgangen werden könnte. Zu diesem Zweck hält der Browser intern eine Liste vor, in der die Zuordnung zwischen Domänen-Namen und IP-Adressen zwischengespeichert wird. Selbst wenn die Time-to-Live (TTL) eines DNS-Eintrags nur sehr kurz ist (beispielsweise eine Sekunde), wird der Eintrag nur beim ersten Aufruf einer bestimmten Domäne abgefragt.

Anti-DNS-Pinning umgeht diese Schutzmaßnahme, indem es den Browser des Benutzers zwingt, den Domänen-Namen eines Webservers erneut abzufragen. Das ermöglicht es dem Angreifer, durch das Ändern des DNS-Eintrags des Webangebots auf eine interne IP-Adresse, HTTP-Anfragen an Systeme im internen Netz zu leiten. Die Daten werden anschließend mittels XMLHttpRequest an den Angreifer übermittelt. Dadurch kann der Benutzer praktisch als Proxy verwendet und beispielsweise auf das Intranet einer Institution zugegriffen werden.

Gegenmaßnahmen in der Grundarchitektur:

- Da in der Grundkonfiguration alle Informationen über das Sicherheits-Gateway geleitet werden, ist Browser-basiertes Anti-DNS-Pinning nicht möglich.
- Die Einschränkung der Ausführung aktiver Inhalte im internen Netz erschwert die Übertragung der Daten an den Angreifer mittels XMLHttpRequest.

Restrisiko für internes Netz: Aufgrund der Durchführung aller DNS-Abfragen vom Sicherheits-Gateway aus ist Anti-DNS-Pinning des HTTP-Proxys im ALG möglich. Da in der Grundarchitektur jedoch alle Ein- und Ausgänge des Sicherheits-Gateways mittels Paketfilter geschützt sind, muss ein Angreifer auch diese Komponenten kompromittieren, um von dort aus weiter in interne Netze einzudringen.
Restrisiko für Internet-PC-Zone: Es besteht kein erhöhtes Restrisiko.

5.4 Identitätsdiebstahl und User-Tracking

5.4.1 Phishing

Bedrohung: Entwenden von Authentisierungsmerkmalen oder vertraulicher Informationen
Schwachstelle: (Unbeabsichtigte) Verwendung von gefälschten Webangeboten

Phishing ist ein Kunstwort aus den Begriffen Password und Fishing. Es handelt sich dabei um einen Angriff, bei dem versucht wird, vertrauliche Informationen durch das Vortäuschen eines vertrauenswürdigen Webangebots zu entwenden. Das Opfer wird dazu auf eine Webseite gelockt, die der Angreifer präpariert hat. Werden dort Informationen wie Passwörter, PINs, TANs oder Kreditkartennummern eingegeben, übermittelt sie der Webserver an den Angreifer.

Obwohl in den Medien meist nur von Phishing-Angriffen auf Online-Banking-Portale berichtet wird, können alle Webangebote, auf denen persönliche oder vertrauliche Informationen verarbeitet werden, Ziel eines solchen Angriffs werden.

Neuere Phishing-Angriffe nutzen auch Schwachstellen in den Webangeboten wie beispielsweise Cross-Site Scripting oder HTML-Injection, um ihre Angriffe zu verschleiern. Mit dem `<dialog>`-Element kann dies auch ohne Scripting erfolgreich durchgeführt werden. Da in einem solchen Fall sowohl die Domäne als auch das TLS-Zertifikat des angegriffenen Webangebots unverändert bleibt, kann das Opfer nur mehr sehr schwer feststellen, ob es sich um Phishing handelt. Eine weitere neue Art dieser Gefährdung nutzt Schadprogramme, um den Inhalt vertrauenswürdiger Webangebote direkt am attackierten System auszutauschen. Auch dabei bleiben URL und TLS-Zertifikat gültig.

Gegenmaßnahmen in der Grundkonfiguration:

- Das Sicherheits-Gateway überprüft jeden Request gegen Phishing-Blacklists.
- Die Einschränkung aktiver Inhalte im internen Netz erschwert Phishing-Angriffe auf Basis von Cross-Site Scripting.
- Das ALG akzeptiert nur gültige TLS-Zertifikate (siehe Abschnitt 4.2.3.1).
- Filterung verdächtiger Code-Stellen am ALG
- Benutzer werden angewiesen, die Einstiegsseiten von Webangeboten mit hohen Anforderungen an die Integrität nicht mittels Klicken auf Hyperlinks zu öffnen.
- Schulung der Benutzer zur sicherheitsbewussten Nutzung des Webs

Restrisiko für internes Netz:	Benutzer können trotz regelmäßiger Schulungen und den Maßnahmen der Grundarchitektur auf Links zu Phishing-Seiten hereinfallen. Insbesondere Phishing-Angriffe auf Basis von HTML-Injection-Schwachstellen können technisch nicht vollständig verhindert werden.
Restrisiko für Internet-PC-Zone:	In der Internet-PC-Zone ist das Restrisiko gegenüber dem internen Netz deutlich erhöht, da auch Phishing-Angriffe über Cross-Site-Scripting-Schwachstellen durchgeführt werden können.

5.4.2 Session Hijacking

Bedrohung: Entwenden von Authentisierungsmerkmalen
Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Sobald ein Benutzer erfolgreich an einem Webangebot authentisiert wurde, verwenden die meisten Webanwendungen eine Session-ID, um den Benutzer wiederzuerkennen. Gelingt es einem Angreifer, diese ID auszulesen, kann er die Sitzung mittels Session Hijacking übernehmen. Meist laufen Sessions nach einer bestimmten Dauer der Inaktivität aus oder werden durch die Verwendung von Logout-Funktion beendet. Eine Übernahme ist nur möglich, solange die Sitzung aktiv ist.

Da sich Session Hijacking technisch nur schwierig verhindern lässt, muss sichergestellt werden, dass die Session-ID eines Webangebots nicht in die Hände eines Angreifers gelangt. Zum Stehlen der Session-ID wird meist Cross-Site Scripting verwendet. Schutzmechanismen dagegen müssen im genutzten Webangebot implementiert werden (siehe [ISi-Web-Server]).

Gegenmaßnahmen in der Grundkonfiguration:

- Einschränkung der Ausführung aktiver Inhalte im internen Netz
- Benutzer werden angewiesen, Webangebote mit hohen Anforderungen an die Integrität und/oder an die Vertraulichkeit ausschließlich über HTTPS zu nutzen

Restrisiko für internes Netz: Es kann nicht ausgeschlossen werden, dass ein Angreifer die Session-ID eines Benutzers auslesen kann.
Restrisiko für Internet-PC-Zone: Es besteht die Möglichkeit, Session-IDs über Cross-Site-Scripting-Schwachstellen in Webangeboten auszulesen. Das Restrisiko wird daher als groß eingestuft.

5.4.3 Cross-Site Request Forgery (CSRF) / Session Riding

Bedrohung: Fälschen bzw. unberechtigtes Verändern von Informationen
Schwachstelle: Verwendung von unsicheren oder bösartigen Webangeboten

Aufgrund der Architektur des Web gilt die Same-Origin-Policy zwar für aktive Inhalte und spezielle HTML-Tags wie etwa Frames, nicht jedoch für normale Hyperlinks. Während diese Funktionen bei rein statischen Inhalten kein Sicherheitsproblem darstellt, kann die Integrität der von dynamischen Webangeboten gespeicherten Informationen gefährdet werden.

Cross-Site Request Forgery (häufig auch als Session Riding bezeichnet) basiert darauf, dass Browser bei der Erstellung einer HTTP-Anfrage an ein Webangebot automatisch eventuell vorhandene Authentisierungsmerkmale wie etwa Session-IDs an den Request anfügen. Ein Angreifer kann daher – vom Benutzer unbemerkt – beliebige Web-Anfragen mit der Berechtigung des Opfers durchführen, solange das Opfer auf dem betroffenen Webangebot eingeloggt ist. Zwar erhält der Angreifer die Antwort auf seine Anfrage nicht zurück, in vielen Fällen kann eine so eingeschleuste Web-Anfrage jedoch genügen, um die Integrität der vom Benutzer im Web gespeicherten Information zu kompromittieren.

Die Auswirkungen der Gefährdung kann folgendes Beispiel verdeutlichen: Surft ein Benutzer, während er in seinem Online-Banking-Portal eingeloggt ist, auf die Seite eines Angreifers, kann dieser im Namen des eingeloggten Opfers eine Abfrage abschicken, die eine Überweisung durchführt. Dazu muss der Angreifer in seiner Seite lediglich einen HTML-Bild-Tag einfügen, der eine Grafik von folgender Beispiel-URL lädt:
http://www.beispielbank.xyz/ueberweisung.jsp?
an_knr=123456789&an_blz=12345&betrag=1.000,-+EUR (für dieses Beispiel wurden aktuelle Sicherheitsmaßnahmen in Online-Banking-Systemen wie beispielsweise TANs ignoriert).

Cross-Site Request Forgery lässt sich von Seiten des Nutzers eines Webangebots technisch zurzeit nicht verhindern. Maßnahmen gegen diese Gefährdung müssen daher vom Betreiber eines Webangebots umgesetzt werden (siehe [ISi-Web-Server]).

Gegenmaßnahmen in der Grundkonfiguration:

- Schulung der Benutzer zur sicherheitsbewussten Nutzung des Webs

Restrisiko für internes Netz: Maßnahmen gegen diese Gefährdung können technisch praktisch nicht erzwungen werden, ohne dabei die

Benutzerfreundlichkeit drastisch zu reduzieren (siehe Variante 5.4.3 A). Daher ist das Restrisiko einzig und allein vom Sicherheitsbewusstsein der Benutzer sowie von der Sicherheit der genutzten Webangebote abhängig. Es wird als hoch eingestuft.

Restrisiko für Internet-PC-Zone: Das Restrisiko in der Internet-PC-Zone ist gegenüber dem internen Netz erhöht, da hier auch die Ausnutzung von Cross-Site Request Forgery über aktive Inhalte möglich ist.

5.4.3 A Variante für hohen Schutzbedarf: Unterbinden paralleler Browsing-Sessions

Anwendungsbereich: hoher Schutzbedarf bezüglich Integrität
Phase im Ablaufplan: Umsetzung

Einige Varianten von Cross-Site-Request-Forgery-Angriffen können unterbunden werden, indem maximal ein Browser-Fenster (und darin nur ein Tab/Register) gleichzeitig geöffnet wird. Bei der Implementierung dieser Variante muss das gleichzeitige Öffnen mehrerer Browser-Fenster bzw. -Register daher unterbunden werden.

Die größtmögliche Effizienz kann diese Maßnahme nur dann erreichen, wenn alle Benutzer Funktionen wie „Eingeloggt bleiben“ nicht nutzen und sich stets von den verwendeten Webangeboten abmelden.

Die Umsetzung der Variante ist auch bei hohem Schutzbedarf optional.

Restrisiko für internes Netz: Vergisst ein Benutzer, sich von einem Webangebot abzumelden, bevor er auf eine andere Seite surft, oder wird ein Benutzer etwa über Cookies von einer Anwendung automatisch wiedererkannt, können trotz der Unterbindung paralleler Browsing-Sessions Cross-Site-Request-Forgery-Angriffe erfolgreich sein.

Restrisiko für Internet-PC-Zone: Da die Umsetzung der Variante den Benutzerkomfort bei der Verwendung von Webangeboten deutlich einschränkt, wird empfohlen diese Variante nur im internen Netz umzusetzen. Das Restrisiko in der Internet-PC-Zone ist daher gegenüber dem internen Netz deutlich erhöht.

Umsetzungsaufwand: geringer Konfigurationsaufwand

5.4.4 Profilbildung

Bedrohung: Ausspähen von Verhaltensmustern
Schwachstelle: Nutzung des Web

Als Profilbildung werden die Analyse des Benutzerverhaltens und die Erstellung von detaillierten Profilen über einzelne Web-Benutzer bezeichnet. Solche Profile werden in der Praxis häufig eingesetzt, um den Benutzern passende Werbung anzuzeigen.

Zur Identifizierung der Benutzer wird bei der Erstellung eines Profils eine eindeutige ID benötigt. Eine solche bietet entweder die IP-Adresse, von der aus Web-Anfragen gestellt werden, oder Cookies, die auf den Systemen der Web-Besucher hinterlegt werden. Während bei der Verwendung von IP-Adressen keine eindeutige Identifizierung einzelner Anwender möglich ist (mehrere Benutzer teilen sich eine IP-Adresse aufgrund von NAT, dynamischen Adressen, Mehrbenutzersystemen oder Proxies), können mittels Cookies auch benutzerspezifische Profile erstellt werden. Durch längerfristige Aufzeichnung des Surf-Verhaltens können bei

entsprechender Auswertung zum Teil sehr detaillierte Rückschlüsse auf die Anwender gezogen werden.

Besonders detaillierte Auswertungen können dann erstellt werden, wenn auf möglichst vielen unterschiedlichen Webangeboten Code platziert werden kann, der Informationen über die Besucher an einen Server übermittelt. In diesem Zusammenhang sind besonders die Anbieter von Online-Werbung und Statistik- bzw. Webanalyse-Diensten zu nennen, da sie diese Möglichkeit haben.

Hyperlinks auf Webangebote, die vom Benutzer bereits besucht wurden, werden im Browser normalerweise in einer anderen Farbe dargestellt als Hyperlinks zu Seiten, die noch nicht aufgerufen wurden. Ein möglicher Angriff basiert darauf, dass ein Angreifer sein Opfer auf eine Webseite lockt, auf der eine große Liste an Links präsentiert wird. Dort kann der Angreifer durch Überprüfung der Link-Farbe feststellen, welche der Angebote bereits vom Benutzer besucht wurden.

In der Praxis kommt der Angriff meist in Kombination mit Phishing-Angriffen zum Einsatz, da über den Verlauf unter Umständen festgestellt werden kann, bei welcher Bank der Benutzer Kunde ist.

Gegenmaßnahmen in der Grundkonfiguration:

- Regelung der Nutzung des Webs
- Schulungen für sicherheitsbewusste Web-Nutzung
- Cookies und Verlauf werden nach jeder Sitzung gelöscht; zudem müssen sie vom Benutzer explizit pro Domäne erlaubt werden.
- Aufgrund der Kanalisierung der Web-Anfragen über das Sicherheits-Gateway kann auf Basis der IP-Adresse kein Rückschluss auf einzelne Benutzer gezogen werden.

Restrisiko für internes Netz:	Da die Möglichkeit, Profile über einzelne Benutzer zu erstellen, Web-immanent ist, können nur Maßnahmen getroffen werden, die versuchen, so viele Informationen über den Benutzer wie möglich zu verschleiern. Die Grundkonfiguration setzt zahlreiche solcher Maßnahmen um. Dennoch müssen aufgrund der Architektur des Web bestimmte Informationen übertragen werden. Daher ist das Restrisiko in erster Linie vom Sicherheitsbewusstsein der Benutzer abhängig. Loggen sich diese z. B. in ein Webangebot ein, so ist eine Profilbildung weiterhin möglich.
Restrisiko für Internet-PC-Zone:	Da vielfach aktive Inhalte zum Sammeln von Benutzerdaten verwendet werden, ist das Restrisiko in der Internet-PC-Zone gegenüber dem internen Netz erhöht.

5.4.5 Werbebanner

Bedrohung: Eindringen in das interne Netz oder die Internet-PC-Zone
Schwachstelle: Auslieferung von Schadprogrammen über Werbebanner

Zahlreiche Webangebote nutzen Werbung als Einnahmequelle. Diese Praxis ist vollkommen legitim und für Betreiber von Webseiten oft notwendig, birgt jedoch für Nutzer auch gewisse Gefahren. Dazu zählen neben der Möglichkeit zur Profilbildung auch die Verbreitung von Schadprogrammen.

Es gab in der Vergangenheit mehrere Fälle, bei denen über Webseiten, die man in der Regel als vertrauenswürdig einstufen würde, Schadprogramme verteilt wurden. Es wurde dabei nicht die eigentliche Webseite vom Angreifer manipuliert, sondern der Dienst über den die Werbeanzeigen bereitgestellt werden.

Gegenmaßnahmen in der Grundkonfiguration:

- Alle Web-Inhalte werden sowohl am ALG als auch am Client bzw. am Internet-PC auf Schadprogramme untersucht.

Restrisiko für internes Netz: Gänzlich neue Schadprogramme oder solche, die speziell im Hinblick auf eine bestimmte Institution entwickelt wurden, können nicht erkannt werden.
Restrisiko für Internet-PC-Zone: Kein erhöhtes Restrisiko.

5.4.5 A Variante für hohen Schutzbedarf: Blockieren von Werbung

Anwendungsbereich: hoher Schutzbedarf
Phase im Ablaufplan: Umsetzung

Bei hohem Schutzbedarf sollten am Sicherheits-Gateway Werbe-Server mittels einer Blacklist blockiert werden.

Restrisiko für internes Netz: Die Verbreitung von Schadsoftware ist auch über andere Kanäle möglich. Die Profilbildung durch Anbieter von Werbung wird verhindert, der Betreiber des Webangebots kann jedoch weiterhin Benutzer-Profile erstellen.
Restrisiko für Internet-PC-Zone: Das Restrisiko in der Internet-PC-Zone ist gegenüber dem internen Netz höher.
Umsetzungsaufwand: Geringer anfänglicher Konfigurationsaufwand, jedoch laufende Wartung der Blacklist notwendig.

5.4.6 Passwortdiebstahl aus dem Passwortmanager

Bedrohung: Auslesen von Passwörtern
Schwachstelle: Unsichere Speicherung von Passwörtern

Passwörter sollten komplex sein, damit sie nicht anfällig für Wörterbuchangriffe sein. Des Weiteren sollten Passwörter nicht wiederverwendet werden, d. h. ein Passwort sollte idealerweise exklusiv für ein Webangebot verwendet werden.

Da sichere Passwörter in der Regel so komplex sind, dass sie schwierig zu merken sind, sollte ein Passwort-Manager verwendet werden. Alle gängigen Browser bringen eigene Passwort-Manager mit. Es werden jedoch immer wieder Angriffe bekannt, mit denen sich Passwörter aus diesen Passwort-Managern extrahieren lassen.

Eine gute Alternative sind eigenständige Passwort-Manager, also eigene Programm. Diese sind meist robuster gegen Angriffe.

Gegenmaßnahmen in der Grundkonfiguration:

- keine

Restrisiko: Auch stand-alone Passwort-Manager können Schwachstellen aufweisen, die das Auslesen von Passwörtern erlauben.

5.5 Umgehen des Sicherheits-Gateways

5.5.1 HTTP-Request Smuggling

Bedrohung: Verhindern der Filtermechanismen des Sicherheits-Gateways
Schwachstelle: Schwachstellen in der Konfiguration der Komponenten im Sicherheits-Gateway

Ziel von HTTP-Request Smuggling ist es, bösartige HTTP-Anfragen von innen durch das Sicherheits-Gateway zu schmuggeln, um Filter-Mechanismen zu umgehen. Zu diesem Zweck werden in den HTTP-Kopfzeilen mehrere Content-Length-Parameter mit unterschiedlichen Werten angegeben.

Unterscheidet sich die Interpretation der Kopfzeilen zwischen dem Ziel-Webserver und dem Sicherheits-Gateway (indem beispielsweise der Ziel-Webserver den ersten Content-Length-Wert verwendet, das Sicherheits-Gateway jedoch den zweiten), kann der interne Angreifer den Filter des Sicherheits-Gateways umgehen.

Gegenmaßnahmen in der Grundkonfiguration:

- Nicht RFC-konforme Requests (etwa mit mehreren Content-Length-Parametern) werden vom Sicherheits-Gateway verworfen.

Restrisiko: Die Grundarchitektur beseitigt die Gefährdung für normalen und hohen Schutzbedarf sowohl im internen Netz als auch in der Internet-PC-Zone.

5.5.2 Encoding

Bedrohung: Einschleusen aktiver Inhalte
Schwachstelle: Umgehen des Filters für aktive Inhalte

Auf gute Filter-Mechanismen lassen sich umgehen. Bei der Vielzahl von Möglichkeiten HTML-Code zu schreiben, kann ein Versagen der Filter nicht ausgeschlossen werden. Insbesondere die neuen Möglichkeiten, die HTML5 bietet, um Scripte einzubetten, stellen Filter für aktive Inhalte auf eine harte Probe.

Gegenmaßnahmen in der Grundkonfiguration:

- Restriktiver Umgang mit aktiven Inhalten am Browser im internen Netz

Restrisiko: Durch das Blockieren aller aller aktiven Inhalte (außer JavaScript) im internen Netz wird dieser Maßnahme für normalen Schutzbedarf ausreichend begegnet.

5.5.2 A Variante für hohen Schutzbedarf: Einfügen eines Content-Security-Policy Headers

Anwendungsbereich: hoher Schutzbedarf bezüglich Vertraulichkeit und/oder Integrität
Phase im Ablaufplan: Umsetzung

Um die Ausführung von JavaScript im internen Netz zu unterbinden, kann der HTTP-Proxy des ALG einen `Content-Security-Policy` Header hinzufügen. Dies signalisiert dem Browser eine Richtlinie für den Umgang mit JavaScript.

Restrisiko für internes Netz: Durch diese Maßnahme wird der Gefährdung auch bei hohem Schutzbedarf ausreichend begegnet.
Restrisiko für Internet-PC-Zone: Diese Maßnahme ist für die Internet-PC-Zone nicht angemessen.
Umsetzungsaufwand: Die Implementierung der Variante verursacht einen geringen

Konfigurationsaufwand.

5.6 Verschlüsselung und Zertifikate

5.6.1 Abhören unverschlüsselter Verbindungen

Bedrohung: Ausspähen von HTTP-Abfragen und/oder HTTP-Antworten
Schwachstelle: Unzureichender Schutz der externen Kommunikationsverbindungen

Bei der Verwendung von unverschlüsselten Verbindungen (HTTP anstelle von HTTPS) können alle übertragenen Informationen am Transportweg zwischen dem Client und dem Ziel-Webserver abgehört werden. Dazu muss ein Angreifer Zugriff auf einen Router am Weg der Pakete oder auf die physische Leitung haben.

Gegenmaßnahmen in der Grundarchitektur:

- Die von der Grundarchitektur geforderte Regelung der Nutzung des Web verlangt die Verwendung von HTTPS zur Übermittlung vertraulicher Informationen.

Restrisiko für internes Netz: Die Beschränkung auf HTTPS-Verbindungen könnte zwar technisch erzwungen werden, es gibt jedoch Webangebote die nur über HTTP erreichbar sind. Aus diesem Grund ist das Restrisiko direkt mit dem Sicherheitsbewusstsein der Benutzer verbunden, da diese darauf achten müssen, vertrauliche oder interne Informationen ausschließlich über verschlüsselte Verbindungen zu übermitteln.

Restrisiko für Internet-PC-Zone: Für die Internet-PC-Zone besteht in Bezug auf das Abhören unverschlüsselter Verbindungen gegenüber dem internen Netz kein erhöhtes Restrisiko.

5.6.2 Fälschung von Zertifikaten

Bedrohung: Fälschen von Web-Inhalten
Schwachstelle: Schwachstellen in der Konfiguration der Komponenten im Sicherheits-Gateway

Um die Authentizität eines Servers feststellen zu können, kommen meist SSL- oder TLS-Zertifikate zum Einsatz. Die Sicherheit dieser Authentisierungsmethode beruht darauf, dass gewissen Zertifizierungsstellen (CAs) vertraut wird. Ein Vertrauensverhältnis entsteht, indem das Zertifikat einer CA im Zertifikatsspeicher des ALG (oder des Browsers) gespeichert wird.

Da Betreiber von Webangeboten auch eigene Zertifikate ausstellen können, lässt sich Authentizität nur schwer überprüfen. Auch von CAs signierte Zertifikat sind nicht zwangsläufig vertrauenswürdig. In der Vergangenheit sind mehrere Fälle bekannt geworden, bei denen CAs kompromittiert wurden oder Zertifikate ohne genaue Prüfung ausgestellt wurden.

Gegenmaßnahmen in der Grundkonfiguration:

- Das Sicherheits-Gateway akzeptiert nur Zertifikate, die von einer gültigen und vertrauenswürdigen CA signiert wurden und terminiert die SSL-/TLS-Verbindung.
- Browser sind sowohl in der Internet-PC-Zone als auch im internen Netz zentral so konfiguriert, dass sie nur Zertifikate akzeptieren, die von einer gültigen CA signiert wurden.

Restrisiko: Die Vertrauenswürdigkeit einer CA kann nicht zweifelsfrei sichergestellt werden. Andererseits können auch selbst signierte

Zertifikate vertrauenswürdig sein.

5.6.3 SSL-Downgrade

Bedrohung: Mitlesen von verschlüsseltem Verkehr
Schwachstelle: Ausweichen auf eine schwache Verschlüsselung wegen Abwärtskompatibilität

Ein Man-in-the-Middle Angreifer kann erzwingen, dass eine Verbindung zu einem Webserver mit SSL statt TLS verschlüsselt wird. Das war auch der Ansatz des *POODLE* Angriffs in 2014. SSL ist inzwischen veraltet und sollte nicht mehr verwendet werden. Einige Webserver bieten SSL jedoch noch als Rückfalloption an, da es Besucher mit veralteten Browsern geben könnte, die noch kein TLS unterstützen.

Inzwischen unterstützen viele Browser `TLS_FALLBACK_SCSV` mit dem sich ein Downgrade verhindern lässt oder bieten zumindest die Möglichkeit SSL zu deaktivieren.

In der Grundarchitektur wird die Verbindung nicht vom Browser, sondern vom Proxy auf dem ALG aufgebaut.

Gegenmaßnahmen in der Grundkonfiguration:

- Das ALG akzeptiert keine SSL-Verbindungen.

Restrisiko: Mit dieser Maßnahme wird der Gefährdung ausreichend begegnet.

5.7 Sonstige

5.7.1 Prefetching

Bedrohung: Übertragung von Informationen ohne das Wissen des Nutzers
Schwachstelle: keine

Prefetching wird im Browser dafür verwendet Informationen oder Dateninhalte zu verlinkten Webseite im Voraus zu laden. Dadurch können die Webseiten bei einem Aufruf des Browser-Links ggf. schneller vom Browser dargestellt werden.

Je nach Art des Prefetchings werden Daten direkt zu einer verlinkten Webseite gesendet, obwohl diese vom Benutzer nicht aufgerufen wurde. Dadurch besteht die Gefahr, dass persönliche Daten über den Benutzer übermittelt werden oder das ohne des Wissens des Benutzer Seiten kontaktiert werden, die im schlimmsten Fall illegale Inhalte oder Schadsoftware enthalten.

Aus diesem Grund wird auch besonders von Browser-Erweiterungen abgeraten, die derartige Mechanismen verwenden, z.B. um Webseiten schneller darstellen zu können.

Gegenmaßnahmen in der Grundkonfiguration:

- Prefetching wird im Browser deaktiviert.

Restrisiko: Der Gefährdung wird mit der Deaktivierung von Prefetching hinreichend begegnet. Durch die Deaktivierung können jedoch die Ladezeiten von Webseiten steigen.

5.7.2 Plug-Ins

Bedrohung: Auslesen von Informationen aus dem Browser

Schwachstelle: Fehlende Rechteverwaltung

Einige Plug-Ins fordern bei der Installation Rechte ein – etwa den Zugriff auf Lesezeichen oder den Verlauf. Für manche Plug-Ins sind diese Rechte auch notwendig. Dennoch sollte man sich bewusst machen, dass die Anbieter dieser Plug-Ins mit diesen Informationen auch in der Lage sind, Nutzerprofile zu erstellen.

Unabhängig von der Möglichkeit Informationen über den Benutzer zu sammeln, erhöht jedes Plug-In die Angriffsfläche des Browsers und die Gefahr einer Infektion (siehe Kapitel 5.1.1).

Gegenmaßnahmen in der Grundkonfiguration:

- Die Verwendung von Plug-Ins wird auf ein Minimum reduziert.

Restrisiko: Auch der Browser kann Schwachstellen enthalten, die sich für eine Infektion ausnutzen lassen.

6 Fazit

Für viele Unternehmen und Institution ist der Zugriff auf Webangebote beinahe unverzichtbar geworden. Indem Anwender aus dem internen Netz Seiten im Web nutzen, sind sie zahlreichen Gefährdungen ausgesetzt, welche die Verfügbarkeit, die Vertraulichkeit und die Integrität der Unternehmensdaten kompromittieren können. Über das Web kann es Angreifern gelingen, in die internen Systeme einzudringen. Sie können Benutzer täuschen, betrügen und schließlich auch wertvolle Informationen entwenden oder ganz einfach den Betrieb der Infrastruktur verhindern.

Die Basis für die sichere Nutzung von Webangeboten ist eine sichere Anbindung an das Internet. Mit der Absicherung der unteren drei Schichten des TCP/IP-Referenzmodells beschäftigt sich die Studie auf [ISi-LANA], auf der diese Studie aufbaut. Bei dem Anbieten von Webanwendungen oder der Verwendung anderer Internet-Dienste können die Maßnahmen zur sicheren Web-Nutzung um die Anforderungen der Studien zum jeweiligen Thema ergänzt werden.

Um die Basis-Infrastruktur vor Gefährdungen zu schützen, die speziell bei der Nutzung von Webangeboten auftreten können, wurden in der vorliegenden ISi-Web-Client-Studie Empfehlungen erarbeitet, wie solchen Gefahren durch eine Kombination aus technischen und organisatorischen Maßnahmen begegnet werden kann. Die robuste Grundarchitektur wurde ergänzt um Anforderungen an die zu betreibenden Geräte, sichere Konfigurationseinstellungen und Prozesse für einen reibungslosen und störungsarmen Betrieb, bei dem Sicherheitsaspekte an erster Stelle stehen. Das Restrisiko wird damit auf ein Maß reduziert, das für Unternehmen mit normalem Schutzbedarf noch tragbar ist.

Speziell im Bereich der Nutzung von Webangeboten gibt es jedoch auch einige Gefährdungen, vor denen ein Schutz sehr schwierig ist. Dazu zählen insbesondere Schwachstellen in den Webangeboten Dritter, die es einem Angreifer im schlimmsten Fall ermöglichen, vertrauliche Informationen zu stehlen oder die Anwender in einer Weise zu täuschen, dass diese ihre Authentisierungsmerkmale an den Angreifer übermitteln. Auch Schwachstellen in Standardsoftware stellen eine Gefahr dar, vor der ein vollständiger Schutz nicht möglich ist, da zwischen dem Bekanntwerden einer Sicherheitslücke und der Installation des entsprechenden Patches immer eine gewisse Zeitspanne vergeht, in der die Systeme nicht geschützt sind. Hier gilt es, den potenziellen Schaden einer erfolgreichen Kompromittierung möglichst gering zu halten, indem eine konsequente Trennung zwischen Zonen mit unterschiedlichem Schutzbedarf erzwungen wird.

Da die Anforderungen an die Größe und Komplexität der eingesetzten Lösung von Institution zu Institution stark variieren können, beschreibt die Studie zahlreiche Architektur- und Konfigurationsvarianten. Durch Umsetzung dieser Varianten kann einerseits die Grundarchitektur durch ergänzende Maßnahmen auch für Netze mit hohem Schutzbedarf angepasst werden und andererseits der Aufwand bei kleineren oder unkritischeren Anwendungsfällen reduziert werden. Mit einer Reduktion des Umsetzungsaufwands geht jedoch auch immer eine Erhöhung des Restrisikos einher. Hier muss von Fall zu Fall entschieden werden, ob die Kostenersparnis das Restrisiko rechtfertigen kann.

7 Anhang

7.1 Literaturverzeichnis

[ISi-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), Absicherung eines PC-Clients, 2011, http://www.isi-reihe.de/

[ISi-E] Bundesamt für Sicherheit in der Informationstechnik (BSI), BSI-Standards zur Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, 2011, http://www.isi-reihe.de/

[ISi-Fern] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherer Fernzugriff auf lokale Netze, 2010, http://www.isi-reihe.de/

[ISi-LANA] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sichere Anbindung lokaler Netze an das Internet, 2014, http://www.isi-reihe.de/

[ISi-Mail-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicherer Betrieb von E-Mail-Servern, 2008, http://www.isi-reihe.de/

[ISi-Web-Server] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sicheres Bereitstellen von Web-Angeboten, 2008, http://www.isi-reihe.de/

[ReCoBS] Bundesamt für Sicherheit in der Informationstechnik (BSI), Remote-Controlled Browsers System - Grundlagen und Anforderungen, 2005, https://www.bsi.bund.de/cln_134/ContentBSI/Themen/sinet/Gefaehrdungen/AktiveInhalte/schutzmoeglichkeiten/recobs/kurzinformation.html

[RFC 3143] Internet Engineering Task Force (IETF), Known HTTP Proxy/Caching Problems, 2001, http://tools.ietf.org/html/rfc3143

[RFC 3986] Internet Engineering Task Force (IETF), Uniform Resource Identifier (URI): Generic Syntax, 2005, http://tools.ietf.org/html/rfc3986

[RFC 4033] Internet Engineering Task Force (IETF), DNS Security Introduction and Requirements, 2005, http://tools.ietf.org/html/rfc4033

[RFC 4918] Internet Engineering Task Force (IETF), HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV), 2007, http://tools.ietf.org/html/rfc4918

[RFC 6698] Internet Engineering Task Force (IETF), The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA, 2012, http://tools.ietf.org/html/rfc6698

[RFC 7230] Internet Engineering Task Force (IETF), Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing, 2014, http://tools.ietf.org/html/rfc7230

[RFC 7231] Internet Engineering Task Force (IETF), Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content, 2014, http://tools.ietf.org/html/rfc7231

[TR-02102-2] Bundesamt für Sicherheit in der Informationstechnik (BSI), Verwendung von Transport Layer Security (TLS), 2015 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2_pdf.pdf

7.2 Abkürzungsverzeichnis

APC	Arbeitsplatz PC
ALG	Application Layer Gateway
CA	Certification Authority
COM	Component Object Model
CRL	Certificate Revocation List
CSRF	Cross Site Request Forgery
CSS	Cascading Style Sheets
CVV	Card Verification Value
DANE	DNS-based Authentication of Named Entities
DES	Data Encryption Standard
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DOM	Document Object Model
FTP	File Transfer Protocol
HTML	Hypertext Markup Language
HSTS	HTTP Strict Transport Security
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IP	Internet Protocol
JS	JavaScript
LSO	Local Shared Object
MD	Message Digest
OCSP	Online Certificate Status Protocol
PC	Personal Computer
PDF	Portable Document Format
PIN	Personal Identification Number
PKI	Public Key Infrastructure
ReCoBS	Remote Controlled Browser System
RFC	Request for Comments
SMTP	Simple Mail Transfer Protocol
SOP	Same Origin Policy
SSL	Secure Socket Layer
SVG	Scalable Vector Graphic
TAN	Transaction Authentication Number

TCP	Transfer Control Protocol
TLS	Transport Layer Security
TTL	Time To Live
UDP	User Datagram Protocol
URI	Unified Resource Identifier
URL	Unified Resource Locator
USB	Universal Serial Bus
VoIP	Voice over IP
W3C	World Wide Web Consortium
WebDAV	Web-based Distributed Authoring and Versioning
WebGL	Web Graphics Library
WMF	Windows Metafile
WWW	World Wide Web
XAML	Extensible Application Markup Language
XML	Extensible Markup Language
XSS	Cross Site Scripting

7.3 Varianten der Grundarchitektur

In Abschnitt 3 wurde eine sichere Grundarchitektur für eine große Organisation mit normalem Schutzbedarf vorgestellt, die das sichere Nutzen von Webangeboten im Internet beschreibt.

Darüber hinaus wurden in Abschnitt 5 verschiedene Architektur- und Konfigurationsvarianten beschrieben. Hier wurde gezeigt wie sich die Internet-Nutzung einerseits in kleinen, unkritischen IT-Infrastrukturen mit moderatem Aufwand realisieren lässt, andererseits aber auch wie sie in großen Unternehmen mit hohem Schutzbedarf umgesetzt werden kann.

Eine Abweichung von der Grundarchitektur hat jedoch Auswirkungen auf die Gefährdungen, denen das Unternehmen ausgesetzt ist. Hier muss der Nutzer abwägen, ob das unter Umständen erhöhte Restrisiko zu tragen ist oder nicht.

Im folgenden Anhang werden einige Beispiele vorgestellt, wie die Architektur an eine veränderte Unternehmensgröße oder einen veränderten Schutzbedarf angepasst werden kann und welche Konsequenzen dies auf die Gefährdungslage hat.

Im Fokus stehen dabei die Änderungen, die sich auf das interne Netz und die Internet-PC-Zone beziehen. Änderungen, die das Sicherheits-Gateway, das Management-Systems und die Internetanbindung betreffen, sind in [ISi-LANA] und [ISi-Web-Server] beschrieben.

Für jedes vorgestellte Szenario werden Annahmen getroffen, die beispielhaft eine kleine, mittelgroße bzw. große Organisation kennzeichnen. Aufbauend auf diesen Annahmen werden Änderungsmöglichkeiten aufgegriffen, die bereits als Varianten in Abschnitt 5 vorgestellt worden sind. Die Änderung der Gefährdungslage des Unternehmens durch die Abweichung von der Grundarchitektur wird jeweils in einer Tabelle dargestellt.

In der Tabelle bedeutet „↑↑“ deutlich erhöhte Gefährdung, „↑“ erhöhte Gefährdung, „↔“ Gefährdung, wie bei Verwendung der Grundarchitektur, „↑↓“ teils erhöhte, teils erniedrigte Gefährdung, „↓“ verringerte Gefährdung und „↓↓“ deutlich verringerte Gefährdung.

7.3.1 Kleines Unternehmen

Annahmen

Für ein kleines Unternehmen werden folgende Annahmen getroffen:

- Es handelt sich um keine Behörde.
- Wenige Clients und Server im internen Netz.

Änderungen der Grundarchitektur für den normalen Schutzbedarf

Bei einem kleinen Unternehmen mit normalem Schutzbedarf kann das ALG gemäß [ISi-LANA] aufgrund der hohen Kosten entfallen. Ebenso kann die Internet-Zone entfallen. Stattdessen können aktive Inhalte für vertrauenswürdige Webangebote explizit freigeschaltet werden.

Es ergeben sich an der Grundarchitektur und den zugehörigen Empfehlungen folgende Änderungen für ein kleines Unternehmen mit normalem Schutzbedarf (vgl. Abbildung 7.1):

- Das ALG entfällt.
- Die Internet-PC-Zone entfällt.

Konsequenzen für die Gefährdung des Unternehmens

Kleines Unternehmen – normaler Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↑↑	Aktive Inhalte werden nicht zentral gefiltert; Unzureichende Trennung von Arbeitsplatz-PC und Internet-PC
Täuschen/Betrügen	↑	Keine zentrale Filterung bösartiger Inhalte (z. B. Trojanische Pferde)
Entwenden/Ausspähen	↑	Keine zentrale Filterung bösartiger Inhalte (z. B. Spyware, Phishing-Seiten)
Verhindern/Zerstören	↑	Keine zentrale Filterung von Anfragen

Tabelle 4: Konsequenzen für die Gefährdung eines kleinen Unternehmens mit normalem Schutzbedarf

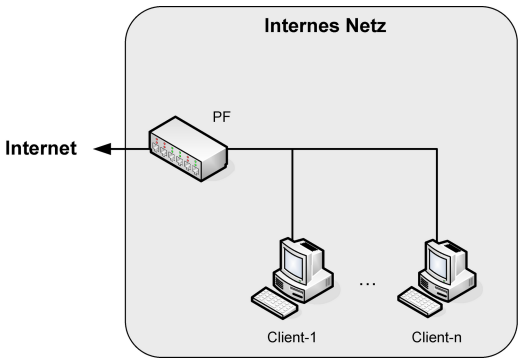


Abbildung 7.1: Variante für ein kleines Unternehmen mit normalem Schutzbedarf

Änderungen der Grundarchitektur für den hohen Schutzbedarf

Besteht ein hoher Schutzbedarf, etwa für vertrauliche Informationen von Kunden, so sollte der PC auf dem diese Daten verwaltet werden, nicht an das Internet angebunden sein. Zur Internet-Nutzung können gesonderte PCs verwendet werden (vgl. Abbildung 7.2):

- Das ALG entfällt.
- Das interne Netz ist nicht ans Internet angebunden.

Konsequenzen für die Gefährdung des Unternehmens

Kleines Unternehmen – hoher Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↑↓	Erhöhtes Risiko, da keine zentrale Filterung vorgenommen wird; Verringertes Risiko, da über das Internet kein Zugriff auf die schützenswerten Daten möglich ist
Täuschen/Betrügen	↑	Keine zentrale Filterung bösartiger Inhalte (z. B. Trojanische Pferde)
Entwenden/Ausspähen	↑↓	Erhöhtes Risiko, da keine zentrale Filterung bösartiger Inhalte (z. B. Spyware, Phishing-Seiten); Verringertes Risiko, da über das Internet kein Zugriff auf die schützenswerten Daten möglich ist
Verhindern/Zerstören	↑	Keine zentrale Filterung von Anfragen

Tabelle 5: Konsequenzen für die Gefährdung eines kleinen Unternehmens mit hohem Schutzbedarf

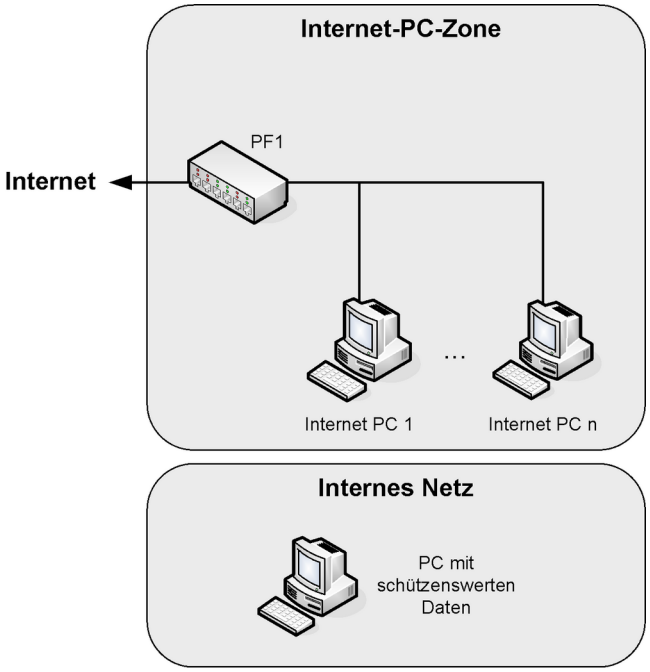


Abbildung 7.2: Variante für ein kleines Unternehmen mit hohem Schutzbedarf

7.3.2 Mittelgroßes Unternehmen

Annahmen

Für ein mittelgroßes Unternehmen werden folgende Annahmen getroffen:

- Mittlere Anzahl von Clients und Severn im internen Netz.

Änderungen für den normalen Schutzbedarf

Für den normalen Schutzbedarf können folgende Varianten verwendet werden (vgl. Abbildung 7.5):

- Verwendung von USB-Sticks anstelle des Datenaustausch-Servers (Variante Fehler: Referenz nicht gefunden)

Das Unternehmen ist bei seiner Risikoanalyse zu der Auffassung gelangt, dass das damit verbundene erhöhte Risiko tragbar ist.

Konsequenzen für die Gefährdung des Unternehmens

Mittelgroßes Unternehmen – normaler Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↑	Dateien werden auf dem Weg ins interne Netz nicht an zentraler Stelle geprüft.
Täuschen/Betrügen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Entwenden/Ausspähen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Verhindern/Zerstören	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur

Tabelle 6: Konsequenzen für die Gefährdung eines mittelgroßen Unternehmens mit normalem Schutzbedarf

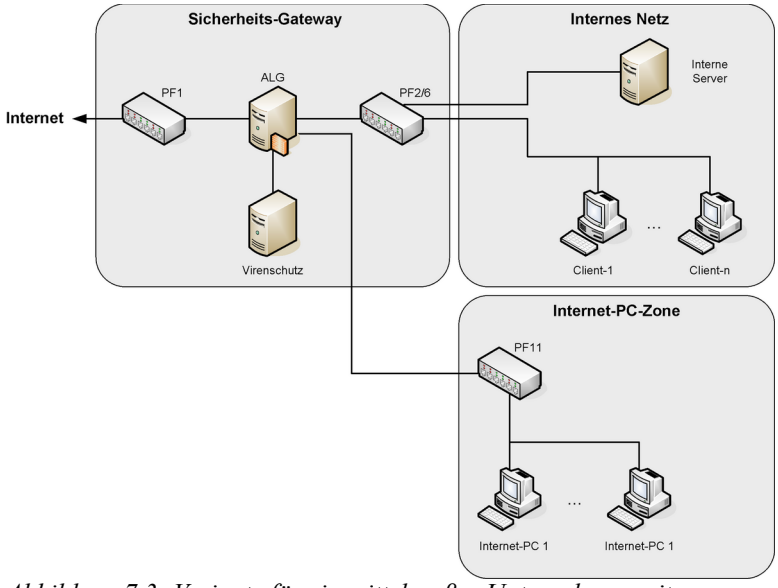


Abbildung 7.3: Variante für ein mittelgroßes Unternehmen mit normalem Schutzbedarf

Änderungen für den hohen Schutzbedarf

Für ein mittelgroßes Unternehmen mit hohem Schutzbedarf ist von einer Vereinfachung der Grundarchitektur abzuraten. Die Grundarchitektur kann jedoch erweitert oder modifiziert werden. Für den normalen Schutzbedarf können beispielsweise folgende Änderungen verwendet werden (vgl. Abbildung 7.4):

- Einsatz eines ReCoBS (Variante 5.2.2 A oder 5.2.2 C)
- Unterbinden von parallelen Browsing-Sessions (Variante 5.4.3 A)

Konsequenzen für die Gefährdung des Unternehmens

Mittelgroßes Unternehmen – hoher Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↓	Die Internet-PC-Zone wird durch ein ReCoBS ersetzt
Täuschen/Betrügen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Entwenden/Ausspähen	↓	Unterbinden paralleler Browsing-Sessions erschwert Session Riding Angriffe
Verhindern/Zerstören	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur

Tabelle 7: Konsequenzen für die Gefährdung eines mittelgroßen Unternehmens mit hohem Schutzbedarf

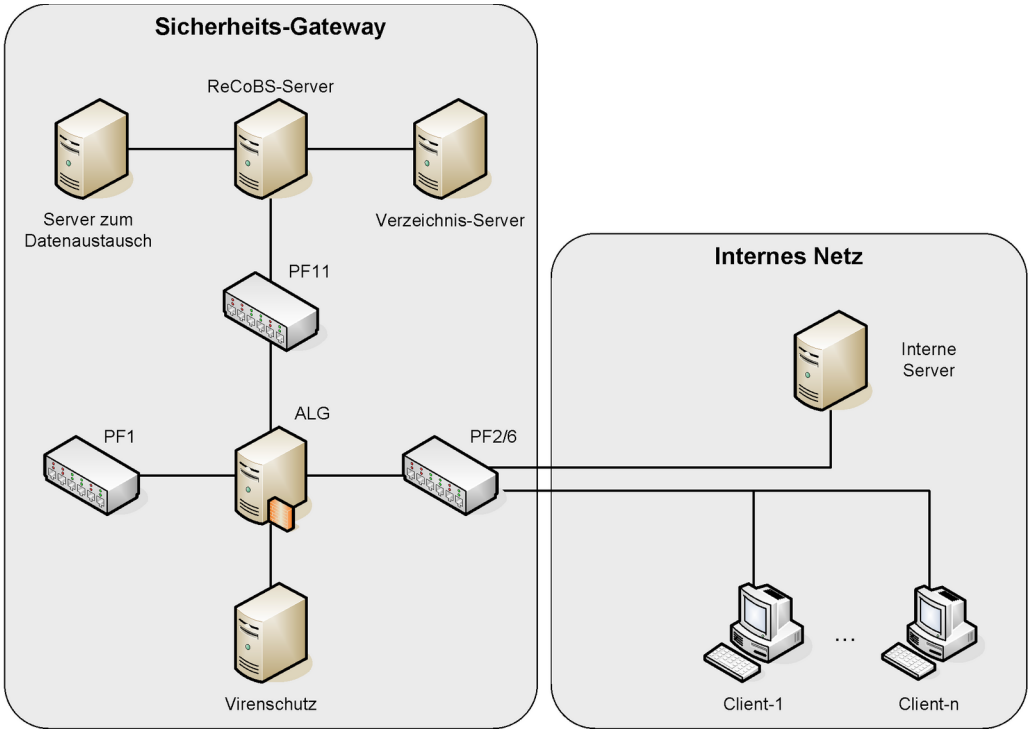


Abbildung 7.4: Variante für ein mittelgroßes Unternehmen mit hohem Schutzbedarf

7.3.3 Großes Unternehmen

Für ein großes Unternehmen werden folgende Annahmen getroffen:

- Große Anzahl von Clients und Servern im internen Netz.

Änderungen für den normalen Schutzbedarf

Das Unternehmen hat festgestellt, dass die Grundarchitektur mit ihren Empfehlungen den eigenen Sicherheitsansprüchen entspricht und verzichtet somit auf den Einsatz von Varianten.

Konsequenzen für die Gefährdung des Unternehmens

Großes Unternehmen – normaler Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Täuschen/Betrügen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Entwenden/Ausspähen	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur
Verhindern/Zerstören	↔	Kein erhöhtes Risiko im Vergleich zur Grundarchitektur

Tabelle 8: Konsequenzen für die Gefährdung eines großen Unternehmens mit normalem Schutzbedarf

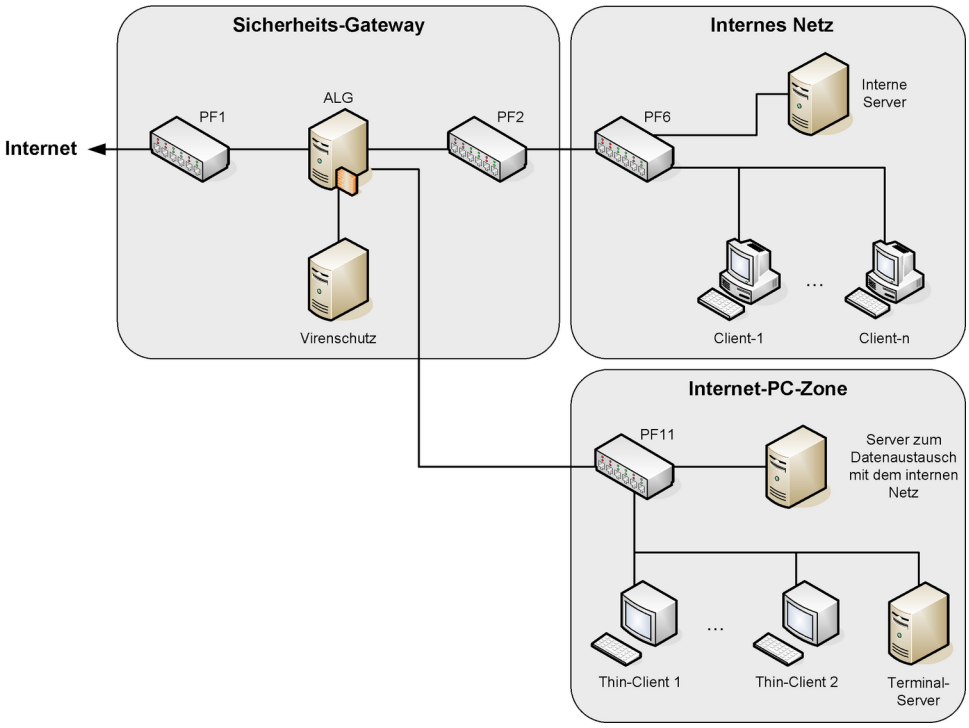


Abbildung 7.5: Variante für ein großes Unternehmen mit normalem Schutzbedarf

Änderungen für den hohen Schutzbedarf

Für den hohen Schutzbedarf können folgende Varianten verwendet werden (vgl. Abbildung 7.6):

- Erneute, zeitlich versetzte Prüfung für Dateien aus dem Web (Variante 5.1.2 A)
- Verwendung virtueller Maschinen auf dem ReCoBS-Server (Variante 5.2.2 B)
- Blockierung von Webseiten mit Frames (Variante 5.3.2 B)
- Einschränkung zugelassener Webangebote mit Whitelist-Ansatz (Variante 5.3.2 C)
- Verzicht auf Caching (Variante 5.3.4 A)
- Unterbinden von parallelen Browsing-Sessions (Variante 5.4.3 A)
- Blockieren von Werbung (Variante 5.4.5 A)

Konsequenzen für die Gefährdung des Unternehmens

Großes Unternehmen – hoher Schutzbedarf		
Bedrohung	Gefährdung	Bemerkung
Eindringen	↓↓	ReCoBS mit virtuellen Maschinen erschwert das Eindringen ins interne Netz
Täuschen/Betrügen	↓	Verzicht auf Caching verhindert Cache-Poisoning im eigenen Netz
Entwenden/Ausspähen	↓	Unterbinden paralleler Browsing-Sessions erschwert Session Riding Angriffe Blockierung von Werbung erschwert Profilbildung
Verhindern/Zerstören	↓	Einschränkung auf zugelassene Webangebote verringert die Angriffswahrscheinlichkeit

Tabelle 9: Konsequenzen für die Gefährdung eines großen Unternehmens mit hohem Schutzbedarf

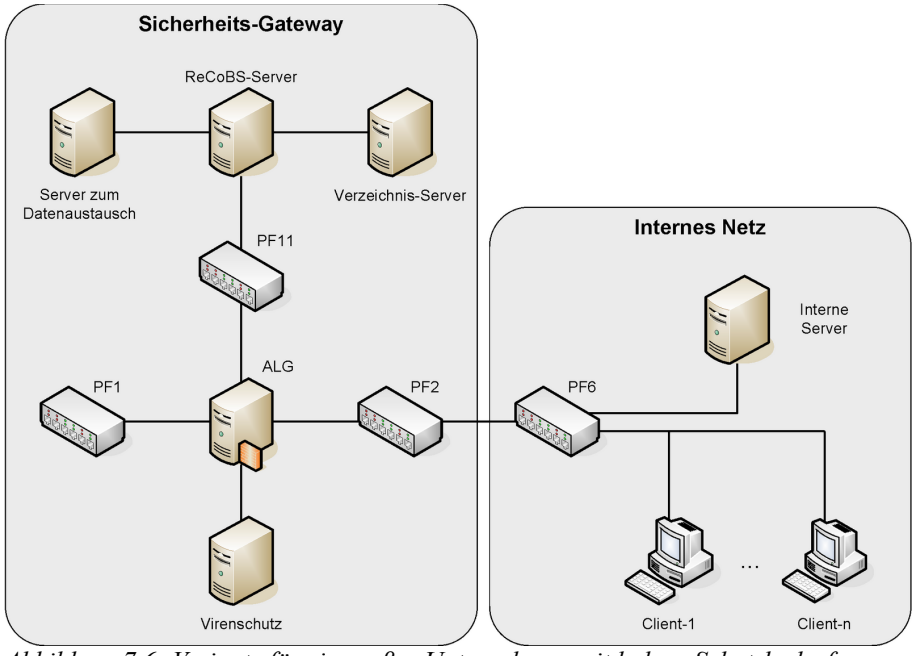


Abbildung 7.6: Variante für ein großes Unternehmen mit hohem Schutzbedarf