Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von Web-Angeboten (ISi-Web-Client)

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

Version 1.2 vom 7. Oktober 2015

Vervielfältigung und Verbreitung

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

Inhaltsverzeichnis

1 Leitlinie zur sicheren Nutzung von Web-Angeboten

Das World Wide Web ist in sehr kurzer Zeit zu einem der wichtigsten Dienste des Internets geworden – und damit auch ein attraktives Ziel für Angreifer. Das Modul ISi-Web-Client zeigt einerseits die Gefahren der Web-Nutzung auf und gibt andererseits Sicherheitsempfehlungen, um den Schutz des internen Netzes bei der Nutzung von Web-Angeboten sicherstellen zu können.

Diese Leitlinie basiert auf der zugehörigen Studie zur sicheren Nutzung von Web-Angeboten [ISi--Web-Client] und fasst die wesentlichen Erkenntnisse zusammen. Die Studie enthält zudem viele hilfreiche Empfehlungen zur Auswahl geeigneter Komponenten sowie zu deren Konfiguration und Betrieb.

1.1 Management Summary

Die Nutzung von Web-Angeboten ist heutzutage unverzichtbar. Aus der Nutzung des Webs resultieren jedoch auch Gefährdungen, die ernst zu nehmen sind. So liegen beispielsweise die Schäden, die alleine in Deutschland durch Phishing-Angriffe entstehen, bei schätzungsweise mehreren Millionen Euro. Andere Angriffe ermöglichen die Infektion von Clients mit Schadsoftware. So können Angreifer ins interne Netz eindringen und dort Daten entwenden oder manipulieren.

Um sich vor den Gefährdungen der Web-Nutzung zu schützen, sind spezielle Maßnahmen erforderlich. Dazu zählt insbesondere ein zentrales Sicherheits-Gateway, das die internen Netze vom Internet trennt und somit die erste Verteidigungslinie bildet. Dort werden potenziell gefährliche Inhalte gefiltert.

Da das zentrale Sicherheits-Gateway jedoch nicht alle Gefährdungen beseitigen kann, sind auch auf den Arbeitsplatz-PCs entsprechende Maßnahmen umzusetzen. Dazu gehört neben der Wahl eines geeigneten Browsers auch die Erstellung und die Pflege einer sicheren Konfiguration sowie ein Patch-Management.

Selbst bei einer guten Absicherung der Arbeitsplatz-PCs ist die Ausführung aktiver Inhalte im internen Netz auf JavaScript beschränkt. Für die Nutzung anderer aktive Inhalte, wie Flash oder Java-Applets, muss entweder ein separater Netzbereich mit Internet-PCs zur Verfügung stehen oder ein Remote Controlled Browser System (ReCoBS) betrieben werden.

1.2 Einführung und Überblick

In den Anfängen des World Wide Web (WWW oder Web) bestanden Webseiten hauptsächlich aus statischen Inhalten – also Texten und Bildern. Der Funktionsumfang des Browsers beschränkte sich auf die Interpretation einiger weniger Strukturelemente zur Darstellung von Text und Grafiken.

Aufgrund des großen Erfolgs entwickelte sich das Web jedoch sehr rasch weiter. Während zahlreiche neue Funktionen wie dynamische und aktive Inhalte hinzugefügt wurden, stammen viele der eingesetzten Protokolle und Schutzmechanismen immer noch aus der Anfangszeit. Aus diesem Grund hat sich die Bedrohungslage grundlegend verändert.

1.2.1 Inhalte von Web-Angeboten

Die Nutzung erfolgt im Alltag meist auf recht unkomplizierte Weise. Die gewünschte Web-Adresse wird im Browser eingetragen, woraufhin die angeforderte Seite übertragen und vom Browser dargestellt bzw. ausgeführt wird. Web-Inhalte lassen sich prinzipiell in drei Kategorien einteilen:

1. Statische Webseiten sind – wie der Name bereits sagt – unveränderlich. Sie werden auf einem Web-Server abgelegt und genau in dieser Form zum Client übertragen.
2. Dynamische Inhalte ermöglichen serverseitig veränderbare Web-Angebote, die je nach Anforderung am Server unterschiedlich generiert und zum Client übertragen werden. Sie erhöhen in erster Linie die Angriffsfläche des Web-Angebotes. Daher sind entsprechende Maßnahmen auch auf dem Webserver zu ergreifen (siehe hierzu [ISi-Web-Server]). Ein manipuliertes Web-Angebot ist jedoch auch eine Gefährdung für die Clients, die dieses Angebot besuchen.
3. Aktive Inhalte werden zuerst zum Client übertragen und durch den Browser lokal ausgeführt. Der verbreitetste Vertreter der aktiven Inhalte ist JavaScript. Während der Einsatz von JavaScript bei der Nutzung eines geeigneten Browsers in vielen Fällen zulässig ist, sind andere aktive Inhalte wie Java-Applets, ActiveX-Controls oder Flash-Anwendungen aus Sicherheitssicht kritisch zu betrachten.

1.2.2 Komponenten zur Absicherung der Web-Nutzung

Die zentrale Schutzkomponente bei der Nutzung von Web-Angeboten ist das Application-Layer-Gateway (kurz ALG oder Proxy-Server). Hier werden Verbindungen der Arbeitsplatz-PCs zum Internet terminiert und analysiert. Potenziell gefährliche Inhalte werden dabei herausgefiltert.

Das zentrale Gateway kann jedoch keinen vollständigen Schutz bieten. Da bösartige Inhalte eventuell ins interne Netz vordringen können, müssen auch auf den Arbeitsplatz-PCs Maßnahmen ergriffen werden. Neben der Absicherung der PCs an sich (siehe hierzu [ISi-Client]) kommt bei der Webnutzung dem Browser eine besondere Bedeutung zu.

Grundsätzlich sollten aktive Inhalte am Client nicht ausgeführt werden. Bei der Verwendung eines geeigneten Browsers (u. a. Prozessisolation bzw. Sandboxing) ist die Nutzung von JavaScript jedoch in vielen Fällen möglich. Sollen auch andere aktive Inhalte genutzt werden, so muss dies in einem getrennten Netzbereich an speziellen Internet-PCs geschehen.

Statt der Internet-PCs kann auch ein Remote Controlled Browser System (ReCoBS) eingesetzt werden. Dabei werden die aufgerufenen Webseiten auf einem Terminal-Server geöffnet und lediglich die grafischen Informationen an den Client im internen Netz übermittelt.

1.3 Wesentliche Ergebnisse der Gefährdungsanalyse

Im Folgenden sind beispielhaft einige für die Webnutzung typische Gefährdungen dargestellt:

1.3.1 Drive-by-Download

Unter einem Drive-by-Download versteht man einen unbeabsichtigten Download, der durch das bloße Besuchen einer Webseite ausgelöst wird. Diese Art von Angriff funktioniert meist über aktive Inhalte. Anschließend werden in der Regel Sicherheitslücken in Browser, Plug-Ins oder Anwendungen ausgenutzt, um den Client mit einem Schadprogramm zu infizieren.

Ein Angreifer muss den für einen Drive-by-Download notwendigen Programmcode auf einer Webseite platzieren, die von seinem Opfer aufgerufen wird. Oftmals wird dieser Programmcode von externen Webseiten nachgeladen, deren Inhalte – z. B. Werbe-Banner – eingebunden werden.

1.3.2 Phishing

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 Web-Angebots 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, so werden diese an den Angreifer übermittelt.

Häufig kommen bei solchen Angriffen leicht abgewandelte URLs zum Einsatz, etwa *meine-bank.de* anstatt *meinebank.de*. Schafft es der Angreifer entsprechende Zertifikate für die Webseite zu generieren, so wird es für den Benutzer noch schwieriger den Angriff zu erkennen.

1.3.3 Cross-Site-Scripting (XSS)

Von Cross-Site-Scripting spricht man, wenn man einer Webseite Skripte unterschieben kann, die dann im Kontext der Webseite ausgeführt werden. Im einfachsten Fall wird ein Skript als Parameter in der URL mit übergeben. Mit dieser Art von Angriff lassen sich beispielsweise Sitzungsinformationen wie Session-Cookies auslesen. Auch andere Angriffe, etwa einige Varianten von Phishing, bedienen sich dieser Technik.

1.3.4 Session Hijacking / Session Riding

Sobald ein Benutzer erfolgreich an einem Web-Angebot authentisiert wurde, verwenden die meisten Web-Anwendungen eine Session-ID, um den Benutzer wiederzuerkennen. Gelingt es einem Angreifer diese ID auszulesen, so kann er die Sitzung übernehmen (Session Hijacking).

Für manche Angriffe benötigt der Angreifer jedoch keinen vollständigen Zugriff auf die Sitzung. Oft reicht es aus, das Opfer dazu zu bringen, im Kontext einer bereits bestehenden Sitzung eine vom Angreifer präparierte Anfrage auszulösen. Cross-Site Request Forgery (häufig auch Session Riding) basiert darauf, dass Browser bei Anfragen an ein Web-Angebot automatisch vorhandene Authentisierungsmerkmale wie etwa Session-IDs anfügen. Ein Angreifer kann – vom Benutzer unbemerkt – beliebige Web-Anfragen mit der Berechtigung des Opfers durchführen, solange das Opfer auf dem betroffenen Web-Angebot eingeloggt ist.

1.4 Wesentliche Empfehlungen

Auf Basis der Empfehlungen für die sichere Nutzung von Web-Angeboten ergibt sich die in Abbildung 1.1 dargestellte Grundarchitektur, die in die Zonen Internet-Anbindung, Sicherheits-Gateway, Internes Netz und Internet-PC-Zone aufgeteilt ist.

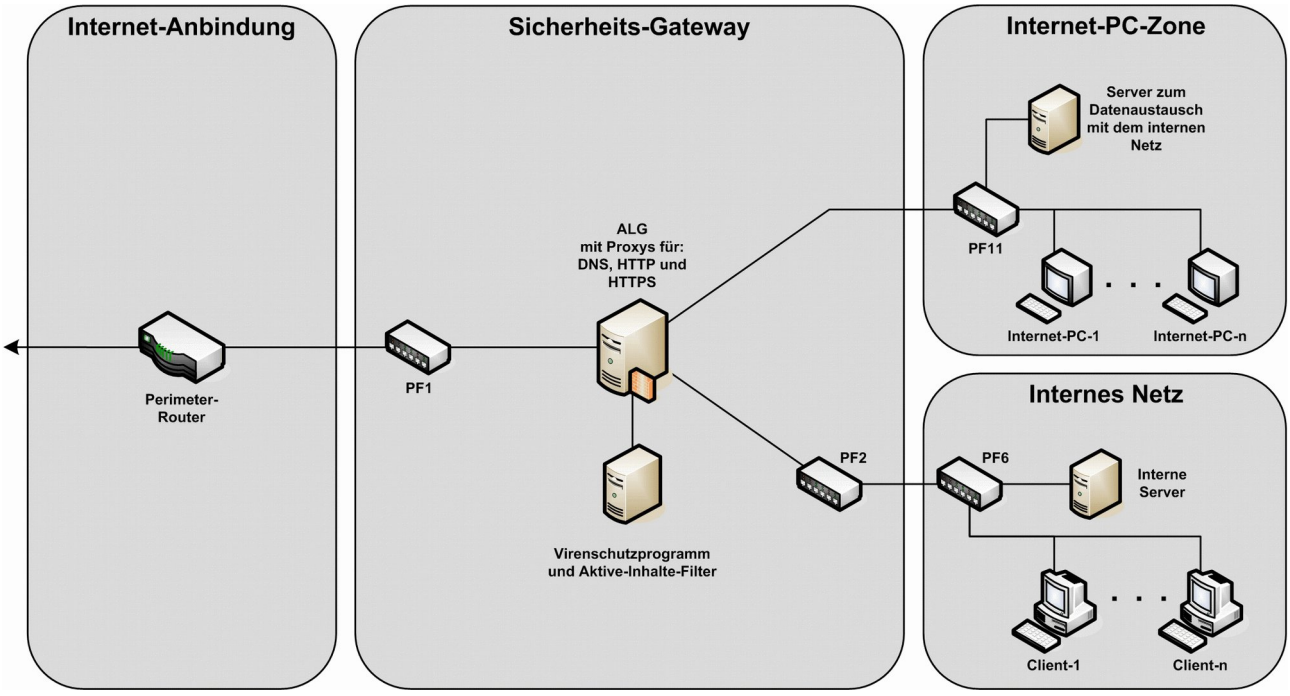

Abbildung 1.1: Grundarchitektur zur Nutzung von Web-Angeboten für normalen Schutzbedarf

1.4.1 Internet-Anbindung

Die Internet-Anbindung erfolgt über einen Perimeter-Router. Weitere Information zur Internet-Anbindung finden sich im Modul *Sichere Anbindung lokaler Netze an das Internet* [ISi-LANA].

1.4.2 Sicherheits-Gateways

Der grundlegende Aufbau des dreistufigen Sicherheits-Gateways wird im Modul zur sicheren Anbindung lokaler Netze an das Internet [ISi-LANA] beschrieben.

Speziell für die Nutzung von Web-Angeboten sind auf dem Application-Layer-Gateway (ALG) Proxy-Server für die Protokolle HTTP, HTTPS und DNS erforderlich. Verbindungen von den Clients ins Internet werden am ALG unterbrochen. Dadurch wird auch die Überprüfung von HTTPS-Verbindungen ermöglicht, was jedoch zu Lasten der Ende-zu-Ende-Verschlüsselung geht.

Zusätzlich zur Protokollprüfung werden die übertragenen Inhalte am ALG auf potenziell gefährliche Inhalte wie Schadprogramme und aktive Inhalte überprüft. Schadprogramme werden grundsätzlich herausgefiltert. Mit Ausnahme von JavaScript sind aktive Inhalte im internen Netz nicht zulässig und werden ebenfalls gefiltert. Für die Internet-PC-Zone sind diese Filter weniger restriktiv eingerichtet, da in dieser Zone auch andere Inhalte genutzt werden dürfen.

1.4.3 Internes Netz

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. Details zur Absicherung von Clients-PCs finden sich in der Studie [ISi-Client].

Speziell für die Nutzung von Web-Angeboten ist insbesondere zu beachten, dass aktive Inhalte sehr restriktiv gehandhabt werden. In Bezug auf Sicherheit kommt dem Browser hierbei eine besonders wichtige Aufgabe zu, da er vertrauliche Informationen über den Benutzer speichert. Bei der Verwendung eines geeigneten Browsers (u. a. Prozessisolation bzw. Sandboxing) und einem gepatchten System ist die Verwendung von JavaScript in den meisten Fällen zulässig. Andere aktive Inhalte, wie Flash-Anwendungen oder JavaApplets, sind grundsätzlich nicht zulässig.

Um eine Infektion des Clients zu verhindern, ist es neben dem Einspielen von Aktualisierungen erforderlich, dass die Benutzer nur mit den minimal notwendigen Rechten ausgestattet werden. Im Idealfall wird ein eigenes Benutzerkonto exklusiv für die Web-Nutzung verwendet.

1.4.4 Internet-PC-Zone

Um auch potenziell gefährliche Web-Angebote nutzen zu können, stehen in der Internet-PC-Zone spezielle Web-Clients zur Verfügung. Hierbei kann es sich um dedizierte PCs oder virtuelle Maschinen handeln.

Die Internet-PC-Zone ist vom internen Netz durch Paketfilter und das ALG abgeschottet. Dadurch sinkt jedoch die Benutzerfreundlichkeit, da in der Internet-PC-Zone Dateien zwar aus dem Web heruntergeladen, jedoch nicht ins interne Netz übertragen werden können. Zum Datenaustausch mit dem internen Netz ist daher ein spezieller Server in der Internet-PC-Zone vorgesehen.

Variante ReCoBS

Eine Alternative zur Internet-PC-Zone ist das Remote Controlled Browser System (ReCoBS). Hierbei laufen die Browser auf einem Terminal-Server, der im Sicherheits-Gateway steht. Von dort werden lediglich die Bildschirminhalte auf die Clients im internen Netz übertragen. Die Clients im internen Netz sind somit keiner Gefährdung ausgesetzt. Die Browser-Sessions auf dem Terminal-Server können nach Beendigung zurückgesetzt werden.

1.5 Fazit

Indem Benutzer aus dem internen Netz auf Webseiten zugreifen, entstehen zahlreiche Gefährdungen, welche die Verfügbarkeit, die Vertraulichkeit und die Integrität der Unternehmensdaten kompromittieren können. Über das Web kann es Angreifern gelingen, in internen Systeme einzudringen, Benutzer zu täuschen und wertvolle Informationen zu entwenden.

Um die Basis-Infrastruktur vor Gefährdungen zu schützen, die bei der Nutzung von Web-Angeboten auftreten können, wurden in der Studie ISi-Web-Client Empfehlungen erarbeitet, wie solchen Gefahren durch eine Kombination aus unterschiedlichen Maßnahmen begegnet werden kann.

Das Sicherheits-Gateway bildet die erste Verteidigungslinie, an der Verbindungen terminiert und überprüft werden. Ein zuverlässiger Schutz ist jedoch nicht immer möglich. Daher zielen einige Maßnahmen in der Studie darauf ab, den potenziellen Schaden einer erfolgreichen Kompromittierung möglichst gering zu halten. Dazu gehört die Trennung zwischen den Arbeitsplatz-PCs und Internet-PCs.

Mit den vorgestellten Maßnahmen ist eine hinreichend sichere Nutzung des Webs möglich.

2 Literaturverzeichnis

[ISi-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), Absicherung eines PC-Clients, 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-Web-Client] Bundesamt für Sicherheit in der Informationstechnik (BSI), Sichere Nutzung von Web-Angeboten, 2015, 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/