Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Absicherungsmöglichkeiten beim Einsatz von Web-Browsern

Das World Wide Web (WWW) ermöglicht die Nutzung vieler, heute nicht mehr wegzudenkender Internet-Dienste. Neben den klassischen Web-Angeboten sind viele andere Internet-Dienste, wie E-Mail, Messaging, Video- und Audiostreaming, Online-Spiele oder auch Kollaborationswerkzeuge, in das WWW integriert.

Zur Anzeige von Webseiten und der Interaktion mit dem Nutzer wird ein Web-Browser benötigt. Daher ist auch der Schutz vor Cyber-Angriffen wesentlich von der Sicherheit des Web-Browsers abhängig. Insbesondere durch aktive Inhalte können Angreifer Schwachstellen ausnutzen. Die Konsequenzen für den Benutzer reichen vom Zugriff auf private Daten bis hin zur Übernahme der Kontrolle über das IT-System. Dieses Dokument gibt daher Empfehlungen zur sicheren Nutzung von Web-Browsern. Die Empfehlungen richten sich an IT-Führungs- und IT-Fachkräfte in Unternehmen und Behörden, die mit den Grundkonzepten des World Wide Web und von Betriebssystemen bereits vertraut sind.

1 Grundanforderungen

Die Grundfunktion eines Web-Browsers ist das Holen angeforderter Daten von Web-Servern und deren Darstellung auf dem Bildschirm. Dabei werden die Inhalte durch den Web-Browser selbst oder durch Erweiterungskomponenten (sog. *Plugins*) interpretiert. Da Schwachstellen in Web-Browsern und ihren Erweiterungskomponenten nahezu ausschließlich durch aktive Inhalte ausgenutzt werden können, stellen diese damit die größte Gefahr für die sichere Nutzung von Web-Browsern dar. Dennoch können aktive Inhalte zumeist nicht einfach abgeschaltet werden, weil diese häufig von Web-Diensten benötigt werden. Bei der sicheren Nutzung von Web-Browsern muss daher sowohl die Nutzbarkeit von Web-Diensten als auch die Absicherung vor der Ausnutzung von Schwachstellen in Web-Browsern berücksichtigt werden.

Die Grundvoraussetzung für sichere Konfigurationen stellt die Verwendung eines nach aktuellem Stand der Technik möglichst sicheren Web-Browsers dar. Neben einem aktuellen Patch-Stand sollte dieser insbesondere die Ausführung von aktiven Inhalten so kapseln, dass selbst bei Ausnutzung von Schwachstellen der Zugriff auf das IT-System des Nutzers verwehrt bleibt. Die Kapselung darf sich dabei nicht nur auf den Web-Browser selbst beschränken, sondern sollte zudem die Erweiterungskomponenten miteinbeziehen. Darüber hinaus sind auch das schnelle Schließen von Schwachstellen und die Verteilung von Updates durch den Hersteller insbesondere dahin gehend wichtig, dass öffentlich bekannt gewordene Schwachstellen nicht ausgenutzt werden können. Außerdem sollten die Ausführung aktiver Inhalte und das Browser-Verhalten möglichst fein-granular konfigurierbar sein.

Um die sichere Web-Nutzung auch bei nicht geschlossenen kritischen Schwachstellen in einem spezifischen Web-Browser zu ermöglichen, sollte grundsätzlich ein weiterer

alternativer Web-Browser genutzt werden können. Zur Umsetzung dieser Anforderung sind daher stets zwei Web-Browser für den Betrieb auf den IT-Systemen der Nutzer unmittelbar einsatzbereit vorzuhalten (Zwei-Browser-Strategie), auch wenn regelmäßig nur einer dieser beiden Browser genutzt wird.

2 Implementierungsmöglichkeiten

Die Möglichkeiten zur sicheren Nutzung von Web-Browsern gehen von einer Grundkonfiguration aus, bei welcher der Web-Browser direkt auf dem IT-System des Nutzers installiert ist. Darüber hinaus werden Separierungsmöglichkeiten für Anwendungen diskutiert, mit deren Hilfe sich die Sicherheit der Nutzung des Web-Browsers weiter erhöhen lässt.

3 Direkte Installation

Die direkte Installation eines Web-Browsers auf dem IT-System des Nutzers hat den Vorteil, dass der Funktionsumfang des Browsers nicht eingeschränkt wird. Außerdem kann der Browser vollständig die Funktionen des Betriebssystems nutzen, sodass die Aktualisierung von Software-Komponenten unterstützt und die Administration der Konfiguration erleichtert wird.

Sollten in einer Unternehmensumgebung allerdings mehrere Betriebssysteme verwendet werden, müssen demnach auch mehrere Konfigurationen gepflegt werden. Bei der erfolgreichen Ausnutzung einer Schwachstelle ist das IT-System des Nutzers direkt betroffen, sodass sich Schadsoftware auch dauerhaft (persistent) auf dem System installieren kann.

3.1 Anwendungsvirtualisierung

Virtualisierte Anwendungen laufen in einer virtuellen Umgebung innerhalb des Betriebssystems ab, in der alle Dateien und Komponenten enthalten sind, die das Programm zur Ausführung benötigt. Hierzu muss die virtualisierte Anwendung zu einer speziellen Konfiguration zusammengefasst werden, die zur Laufzeit die virtuelle Umgebung im Betriebssystem des Nutzers erzeugt. Im Wesentlichen werden hierbei Systemaufrufe durch die virtuelle Umgebung abgefangen, interpretiert und nach festgelegten Regeln an das Betriebssystem weitergegeben.

Ohne große Einschränkung der Benutzbarkeit wird das IT-System des Nutzers durch die virtuelle Umgebung sowohl vor einer Kompromittierung als auch vor einer Persistenz von Angriffen geschützt, da Schadsoftware selbst bei einer Ausnutzung einer Schwachstelle nicht in direktem Kontakt mit dem Betriebssystem steht. Allerdings erfordert jede Aktualisierung des Web-Browsers oder seiner Erweiterungskomponenten eine erneute spezielle Zusammenstellung der Konfiguration und deren Verteilung. Außerdem ist die Anwendungsvirtualisierung nicht auf alle Web-Browser und Betriebssysteme anwendbar.

3.2 Betriebssystemvirtualisierung

Die Betriebssystemvirtualisierung ermöglicht es, getrennt vom laufenden Betriebssystem (Host) ein weiteres Betriebssystem (Gast) virtuell zu betreiben. Hier kann dann der Web-Browser genutzt werden. Die Virtualisierung bildet einen vollständigen Computer mit allen Hardware-Ressourcen, wie Prozessor, Festplatte, Arbeitsspeicher und Grafikkarte, ab. Dabei ist der Gast vom Host vollständig isoliert. Die Kommunikation zwischen Gast und Host ist auf wenige Möglichkeiten beschränkt (Austauschverzeichnisse, gemeinsame Nutzung von Netzwerk und Zwischenablage). Hierdurch ist das IT-System des Nutzers vor einer Kompromittierung und vor einer Persistenz von Angriffen noch einmal wesentlich höher geschützt, als bei der Anwendungsvirtualisierung.

Dagegen sind kleinere Einschränkungen bei der Benutzbarkeit möglich. Zudem ist häufig eine größere Leistungsfähigkeit der IT-Systeme erforderlich. Weiterhin ist die Aktualisierung eines Web-Browsers und der dazugehörigen Betriebssystemvirtualisierung sowie deren Verteilung aufwendiger als bei der Anwendungsvirtualisierung. Allerdings können durch den Einsatz der

Betriebssystemvirtualisierung verschiedene Web-Browser und Betriebssysteme nebeneinander unterstützt werden.

3.3 Terminalserver-Installation

Ein Terminalserver ermöglicht den Betrieb eines Web-Browsers entkoppelt vom IT-System des Nutzers. Auf dem Terminalserver können unabhängig vom Client Web-Browser und Betriebssysteme eingesetzt werden. Das IT-System des Nutzers ist vor einer Kompromittierung und Persistenz von Angriffen ähnlich stark geschützt, wie bei der Betriebssystemvirtualisierung. Im Falle eines erfolgreichen Angriffs können jedoch direkt mehrere Nutzer des Terminalservers betroffen sein.

Beim Terminalserver muss die Aktualisierung und Konfiguration des Web-Browsers nur einmal zentral durchgeführt werden, was den Wartungsaufwand reduziert. Allerdings werden für eine Terminalserver-Installation ein dedizierter leistungsfähiger Server und leistungsfähige Netze benötigt, um flüssiges Arbeiten zu ermöglichen.

4 Bewertung der Vor- und Nachteile

Die Vor- und Nachteile der verschiedenen Implementierungsmöglichkeiten lassen sich wie folgt zusammenfassen:

	Direkte Installation	Anwendungs-virtualisierung	Betriebssystem-virtualisierung	Terminalserver-Installation
Benutzbarkeit (Funktion, Performance)	+	+	o	o
Schutz vor Kompromittierung	-	o	+	+
Schutz vor Persistenz bei Ausnutzung einer Schwachstelle	-	o	+	o
Aufwand für die Aktualisierung der Software-Komponenten	+	-	-	+
Aufwand für die IT-Infrastruktur (Installation, Betrieb und Wartung)	+	+	o	-
Unterstützung von verschiedenen Plattformen	-	-	+	+

Tabelle: Bewertung der Vor- und Nachteile der Implementierungsmöglichkeiten (gut (+), mittel (o), schlecht (-))

5 Zusammenfassung

Die Basis für die sichere Web-Nutzung stellt immer die Verwendung eines nach dem aktuellen Stand der Technik möglichst sicheren Browsers dar. Wird dieser mithilfe einer Anwendungsvirtualisierung eingesetzt, verbessert sich die Sicherheit im Vergleich zur direkten Installation nur wenig, während sich der Aufwand für die Aktualisierung des Web-Browsers stark erhöht. Erst die Betriebssystemvirtualisierung und die Terminalserver-Installation verbessern durch ihre starke Kapselung den Schutz vor einer Kompromittierung und einer Persistenz von Schadsoftware bei der Ausnutzung einer Schwachstelle deutlich.

Andererseits muss der damit einhergehende Mehraufwand – bei der Betriebssystemvirtualisierung für die Aktualisierung des Web-Browsers und bei der Terminalserver-Installation für die IT-Infrastruktur – berücksichtigt werden. Deshalb sollten diese beiden Möglichkeiten dort zum Einsatz kommen, wo das Schutzniveau dieses erfordert oder die Nutzung eines direkt installierten sicheren Web-Browsers nicht möglich ist.

Unabhängig von der Implementierung empfiehlt sich immer eine Zwei-Browser-Strategie, um bei Bedarf stets eine alternative Möglichkeit zur Web-Nutzung zur Verfügung zu haben.

Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.