Bundesamt
für Sicherheit in der
Informationstechnik

BSI-Veröffentlichungen zur Cyber-Sicherheit

ANALYSEN

Überprüfung der Wirksamkeit der BSI-Konfigurationsempfehlungen für Windows 7

Auswirkungen der Konfiguration auf den Schutz gegen aktuelle Drive-by-Angriffe

Zusammenfassung

Das Ziel dieser Untersuchung ist es, die BSI-Empfehlungen zur Cyber-Sicherheit für Windows 7 unter realen Bedingungen eines Drive-by-Angriffs zu überprüfen. Um Unterschiede zwischen der BSI-Konfiguration und einer veralteten Konfiguration zu verdeutlichen, wurden dabei jeweils Vergleichssysteme auf Basis von Windows 7 erstellt. Alle Testsysteme wurden innerhalb des Untersuchungszeitraums Angriffen von 100 Drive-by-Webseiten ausgesetzt.

Die Ergebnisse zeigen, dass die BSI-Empfehlungen für Windows 7 die Sicherheit gegen Drive-by-Angriffe signifikant gegenüber einer veralteten Windows 7-Installation erhöht:

Testkonfiguration	Erfolgreicher Exploit und erfolgreiche Infektion	Erfolgreicher Exploit, Infektion aber durch Microsoft Security Essentials blockiert	Kein Drive-by-Exploit, nur Download	Kein erfolgreicher Angriff
veraltetes Windows 7	36	10	3	51
Windows 7 nach BSI-Empfehlung	0	0	4	96

- Das Testsystem mit Windows 7 und veralteten Anwendungsprogrammen wurde in 36 von 100 Fällen mit Schadsoftware infiziert. In 10 weiteren Fällen wurde der Exploit bzw. das Schadprogramm durch Microsoft Security Essentials detektiert und eine Infektion blockiert.
- Im Vergleich dazu wurde das Testsystem mit Windows 7, das nach den Empfehlungen des BSI konfiguriert wurde, nicht infiziert.

Die detaillierten Ergebnisse finden Sie auf Seite 4.

Ausgangslage

Das Ziel dieser Untersuchung ist es, die im BSI erstellten Empfehlungen für die sichere Konfiguration von Windows 7 auf ihre Wirksamkeit hin zu überprüfen. Es soll gezeigt werden, wie effektiv die mittels der BSI-Empfehlungen abgesicherten Systeme im Vergleich zu veralteten bzw. standardmäßig konfigurierten PCs mit dem Betriebssystem Windows 7 gegen aktuelle Drive-by-Angriffe geschützt sind.

Als Testszenario zur Prüfung der Wirksamkeit sollen 100 tagesaktuelle URLs abgerufen werden, über die zum Untersuchungszeitraum Drive-by-Angriffe durchgeführt werden. Drive-by-Angriffe sind eine aktuell sehr verbreitete Methode, um Schadprogramme ohne Kenntnis des Anwenders und ohne Nutzerinteraktion zu installieren und auszuführen. In der Regel genügt ein Besuch einer Webseite, um das System mit Schadsoftware zu infizieren.

Testkonfigurationen und Durchführung

Hard- und Softwareauswahl sowie Konfiguration der Systeme

Für die Untersuchung wurden zwei unterschiedliche Konfigurationen getestet und miteinander verglichen. Um eine Vergleichbarkeit zu erreichen, ist die Konfiguration für das Betriebssystem Windows 7 nach BSI-Empfehlungen einer veralteten Konfiguration von Windows 7 gegenübergestellt worden. Mit beiden Systemen wurden anschließend 100 identische URLs abgerufen.

Konfiguration nach BSI-Empfehlung

In den Empfehlungen zur Cyber-Sicherheit für Windows 7 werden zahlreiche Einstellungen sowie Software-Empfehlungen und -Alternativen beschrieben. Diese mussten im Vorfeld der Untersuchung auf eine sinnvolle Auswahl an Softwarekomponenten beschränkt werden. Mit Ausnahme des Betriebssystems selbst wurde die Auswahl auf kostenlose Produkte/Software beschränkt. Als Virenschutzprogramm auf den Windows 7 Systemen wird das kostenlose Microsoft Security Essentials eingesetzt.

Die BSI-Empfehlungen zur Konfiguration eines PCs mit dem Betriebssystem Windows stehen auf den Webseiten der Allianz für Cybersicherheit zum Download zur Verfügung: https://www.allianz-fuer-cybersicherheit.de/ACS/DE/OffenerBereich/Empfehlungen/empfehlungen_node.html.

Konfiguration veralteter Systeme

Es wurde die Annahme getroffen, dass im Allgemeinen von ungepatchten Anwendungen, welche sich nicht automatisch aktualisieren, von Standardkonfigurationen, wie einem aktivierten Java-Plug-in im Browser oder einem Administratorkonto als Hauptbenutzer ausgegangen werden kann.

Entgegen der ursprünglichen Planung, bei dem veralteten Windows 7-System den Internet Explorer 8 zu verwenden, wurde der Internet Explorer 9 installiert, da der Internet Explorer 9 mittlerweile über die automatische Update-Funktion von Windows verteilt wurde. Es handelt sich dabei um die Standardeinstellung, die ein Anwender nach der Installation des Betriebssystems bewusst abschalten müsste. Im Unterschied zu den Konfigurationen nach BSI-Empfehlung lag der Fokus bei den veralteten Systemen darauf, eine Konfiguration zu wählen, die der eines normalen Nutzers von Windows 7 in der Wirklichkeit entspricht.

Die Tabelle im folgenden Abschnitt zeigt eine Übersicht der jeweiligen Testkonfigurationen.

Übersicht der Testkonfigurationen

System	Konfiguration
Windows 7 nach BSI-Empfehlung	64-Bit Betriebssystem
	Betriebssystem-Updates: aktiv, aktueller Patch-Stand
	Virenschutz: Microsoft Security Essentials
	Browser: Google Chrome 21 (aktuell)
	PDF-Reader: Adobe Reader X (aktuell)
	Office-Suite: Libre Office 3.6.0.4 (aktuell)
	Java-Runtime: nicht installiert
	Adobe Flash Player: aktuell im Browser Chrome
	Benutzerkonto: Standardnutzer
veraltetes Windows 7	64-Bit Betriebssystem
	Betriebssystem-Updates: aktiv, aktueller Patch-Stand
	Virenschutz: Microsoft Security Essentials
	Browser: Internet Explorer 9 (32-Bit)
	PDF-Reader: Adobe Reader 9.4
	Office-Suite: LibreOffice 3.4.3 (1 Jahr alt)
	Java-Runtime: Java 6 Update 26 (1 Jahr alt)
	Adobe Flash Player: Version 10.3.183.5 (1 Jahr alt)
	Benutzerkonto: Administrator

Auswahl der URLs

Die Auswahl der URLs, von denen Drive-by-Angriffe ausgehen, erfolgte zufällig auf Basis tagesaktueller Erkenntnisse. Die verwendeten URLs wurden erst im Untersuchungszeitraum definiert, da diese in der Regel nur für einen begrenzten Zeitraum aktiv Schadsoftware über Drive-by-Exploits verteilen. Durch diese Vorgehensweise wurde die zum Zeitpunkt der Untersuchung vorherrschende Bedrohungslage mit berücksichtigt.

Die folgende Tabelle zeigt eine Auflistung nach Art des jeweiligen Angriffstools. Dabei ist zu beachten, dass eine URL auch mehreren Typen von Angriffstools zugeordnet werden kann. Es kann z. B. der Fall eintreten, dass sich hinter einer URL ein Blackhole Exploit-Toolkit befindet, aber ein nicht anfälliges System dennoch eine Weiterleitung auf einen Schadsoftware-Downloadlink erhält. Diese Fälle sind in der Tabelle sowohl bei „Blackhole“ als auch bei „Weiterleitungen/Downloadlink auf Schadsoftware“ zugeordnet.

Schadsoftware / Toolkit / Exploit	Anzahl an URLs
Blackhole Exploit-Toolkit	78
Flash-Exploit	1
Java-Exploit	3
PDF-Exploit	2
Weiterleitungen/Downloadlink auf Schadsoftware	6
Sonstige	14

Auswertung der Ergebnisse

Die folgende Tabelle zeigt eine Übersicht der Gesamtergebnisse für die getesteten Konfigurationen. Die Ergebnisse sind in vier unterschiedliche Kategorien eingeteilt:

- Erfolgreicher Exploit und erfolgreiche Infektion: Beim Aufruf einer Webseite wurde das System erfolgreich über einen Exploit angegriffen und ein Schadprogramm installiert.
- Erfolgreicher Exploit, Infektion aber durch Microsoft Security Essentials blockiert: Beim Aufruf einer Webseite wurde das System erfolgreich über einen Exploit angegriffen. Das installierte Virenschutzprogramm verhinderte jedoch die Installation eines Schadprogramms.
- Kein Drive-by-Exploit, nur Download: Beim Aufruf einer Webseite wurde das System ohne Erfolg angegriffen und über eine Weiterleitung ein normaler Download eines Schadprogramms gestartet. Dieses Schadprogramm wurde jedoch nicht ausgeführt (siehe Seite 5).
- Kein erfolgreicher Angriff: Aufgrund der Konfiguration konnte eine Schadsoftware-Infektion vermieden werden.

Testkonfiguration	Erfolgreicher Exploit und erfolgreiche Infektion	Erfolgreicher Exploit, Infektion aber durch MSE blockiert	Kein Drive-by-Exploit, nur Download	Kein erfolgreicher Angriff
veraltetes Windows 7	36	10	3	51
Windows 7 nach BSI-Empfehlung	0	0	4	96

Ein veraltetes Windows 7 System ohne BSI-Empfehlungen konnte nur etwa die Hälfte (51) dieser Angriffe abwehren. Zusätzlich wurden 10 Angriffe durch das installierte Virenschutzprogramm Microsoft Security Essentials detektiert und die Infektion im Anschluss unterbunden, in 3 Fällen erfolgte lediglich ein Download. Im Vergleich dazu wurde das Windows 7-System nach BSI-Empfehlungen in keinem Fall erfolgreich infiziert.

Zu Vergleichszwecken wurde noch ein Testsystem mit einer veralteten Windows XP Installation (Administrator-Benutzerkonto, kein aktueller Patch-Stand, Virenschutz nicht installiert, Browser Internet Explorer 6, etc.) den Drive-by-Angriffen ausgesetzt. Hier gab es 88 erfolgreiche Infektionen, 2 Downloads ohne Infektion und nur in 10 Fällen keinen erfolgreichen Angriff.

Ausgenutzte Schwachstellen

Hinter den für den Test zufällig ausgewählten URLs wurde in den meisten Fällen das Exploit Toolkit Blackhole identifiziert. Das Toolkit nutzt abhängig von der Konfiguration zum Zeitpunkt des Tests insbesondere Exploits für die im Folgenden aufgelisteten Schwachstellen. Diese sind nach dem Zeitpunkt ihres Bekanntwerdens sortiert. Weitere Informationen zu den aufgelisteten Schwachstellen können auf den Webseiten des National Institute of Standards and Technology (NIST) entnommen werden: http://web.nvd.nist.gov/view/vuln/search.

Betroffene Anwendung	Version	CVE (Common Vulnerabilities and Exposures) Number	CVSS Severity (Common Vulnerability Scoring System)	Bekannt seit
Adobe Reader	Vor 9.3 und älter, vor 8.2 und älter	CVE 2009-4324	9.3 (hoch)	15.12.2009
Adobe Reader	Vor 9.3.1 und älter, vor 8.2.1 und älter	CVE 2010-0188	9.3 (hoch)	22.02.2010
Adobe Flash Player	Vor 10.2.154.27 und älter	CVE 2011-0611	9.3 (hoch)	13.04.2011
Adobe AIR	Vor 2.6.19140	CVE 2011-0611	9.3 (hoch)	13.04.2011
Adobe Reader	Vor 9.4.4 und 10.01	CVE 2011-0611	9.3 (hoch)	13.04.2011
Java	Java 6/7 Update 27 und älter	CVE 2011-3544	10.0 (hoch)	19.10.2011

Betroffene Anwendung	Version	CVE (Common Vulnerabilities and Exposures) Number	CVSS Severity (Common Vulnerability Scoring System)	Bekannt seit
Java	Java 6 Update 32 und älter, Java 7 Update 4 und älter, Java 5 Update 35 und älter, Java 1.4.2_37 und älter	CVE 2012-1723	10.0 (hoch)	16.06.2012
Java	Java 7	CVE 2012-4681	10.0 (hoch)	28.08.2012

Die Ergebnisse bestätigen die bisherigen Erkenntnisse des BSI, dass das Exploit-Toolkit Blackhole das am häufigsten genutzte Exploit-Toolkit ist. In der Untersuchung wurde es von 78 der 100 untersuchten URLs benutzt.

Besonderheiten

Ausbleibende Angriffsversuche bei Google Chrome

Bei der Untersuchung ist aufgefallen, dass manche Exploit-Toolkits Filter auf die UserAgents der Browsers verwenden. So wurde oftmals beobachtet, dass Anfragen mit dem UserAgent „Chrome“ ohne Versuch eines Angriffs auf die Webseite google.com weitergeleitet wurden. Der Verdacht liegt nahe, dass Angreifer vorab prüfen, ob eine erfolgreiche Infektion per Drive-by-Angriff möglich ist, oder ob fehlende Schwachstellen und implementierte Sicherheitsfeatures des eingesetzten Browsers erfolgreiche Angriffsversuche unwahrscheinlich machen. Lohnt sich ein Angriff nicht, wird die Anfrage auf eine unauffällige Webseite (wie z. B. google.com) weitergeleitet.

Normaler Download einer Schadsoftware

Es wurde beobachtet, dass eine Anfrage in einigen Fällen ohne erfolgreichen Drive-by-Angriff auf einen Downloadlink eines Schadprogramms (z. B. einer Datei surprise.exe) weitergeleitet wurde. Der Download des Schadprogramms wurde hierbei automatisch gestartet, aber das Programm nicht automatisch ausgeführt. Dazu wäre die zusätzliche Interaktion des Nutzers erforderlich. Beim beobachteten Vorgehen handelt es sich um den Versuch, das angegriffene System trotz des misslungenen Drive-by-Angriffs zu infizieren.

Angriffsversuche auf die aktuelle Java 7-Schwachstelle CVE 2012-4681

Hinter den abgerufenen URLs befanden sich Exploits, welche versuchten, die aktuelle Java 7 Zero-Day-Schwachstelle (CVE 2012-4681 von August 2012) auszunutzen. Dieser Exploit funktioniert jedoch nur bei der Java-Laufzeitumgebung Version 7 und nicht mit der für den Test genutzten Java Version 6. Wäre die verwundbare Version auf den Testsystemen installiert gewesen, wären diese mit hoher Wahrscheinlichkeit erfolgreich infiziert worden.

Fazit

Die Ergebnisse zeigen, dass die BSI-Konfigurationsempfehlungen für Windows-Betriebssysteme die Angriffsfläche von Drive-by-Downloads deutlich minimieren. Es konnte gezeigt werden, in welchem Ausmaß ein aktueller Patch-Stand für Betriebssystem und Anwendungen, das Deaktivieren unnötiger Erweiterungen im Browser sowie die Verwendung eines Browsers mit einer guten Sandbox-Technik, z. B. Google Chrome, die meisten Angriffe abwehren und sogar Angriffsversuche aufgrund der Konfiguration unterbleiben.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an cs-info@bsi.bund.de gesendet werden.