Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

SIT TECHNICAL REPORTS

UNTERSUCHUNG VON REPUTATIONS-BASIERTEN SCHUTZMECHANISMEN GEGEN MALWARE-ANGRIFFE IN BROWSERN

03/2012

Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern

Katja Czajkowski, Markus Schneider, Ruben Wolf und York Yannikos

Hrsg. Michael Waidner

SIT Technical Reports
SIT-TR-2012-002

März 2012

Fraunhofer-Institut für Sichere
Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt

IMPRESSUM

Kontaktadresse:
Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hrsg. Michael Waidner
SIT Technical Reports
ISSN 2192-8169
SIT-TR-2012-002: Untersuchung von reputationsbasierten
Schutzmechanismen gegen Malware-Angriffe in Browsern
Katja Czajkowski, Markus Schneider, Ruben Wolf und York Yannikos

Druck und Weiterverarbeitung:
IRB Mediendienstleistungen
Fraunhofer-Informationszentrum Raum und Bau IRB, Stuttgart

© by **FRAUNHOFER VERLAG**, 2012
Fraunhofer-Informationszentrum Raum und Bau IRB
Postfach 800469, 70504 Stuttgart
Nobelstraße 12, 70569 Stuttgart
Telefon 0711 970-2500
Telefax 0711 970-2508
E-Mail verlag@fraunhofer.de
URL http://verlag.fraunhofer.de

Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern

Katja Czajkowski, Markus Schneider, Ruben Wolf und York Yannikos
Fraunhofer-Institut für Sichere Informationstechnologie SIT

In der heutigen Zeit stellt Malware im Internet ein großes Risiko für Benutzer dar, wobei Browser häufig als Einfallstore ausgenutzt werden. Aus diesem Grund sind in den Browsern Mechanismen vorgesehen, welche helfen sollen, die Benutzer vor diesen Angriffen zu schützen. Diese Mechanismen verwenden häufig Reputationssysteme, mittels derer sie Angriffsversuche von bekannten Internetadressen (URLs) oder mit bereits bekannter Malware blockieren können um somit die Risiken für Benutzer zu reduzieren. Die heutigen Browser verwenden zur Umsetzung dieser Reputationssysteme unterschiedliche Technologien. In dieser Arbeit werden die reputationsbasierten Schutzmechanismen zur Abwehr von Malware-Angriffen im Rahmen eines Black-Box-Ansatzes untersucht und verglichen. Hierzu wurden die Browser realen Angriffen ausgesetzt und die Leistungsfähigkeit der Schutzmechanismen getestet. Danach wurden die durch die Tests erhaltenen Messergebnisse anhand verschiedener Kriterien analysiert und ausgewertet.

Neben Malware-Angriffen gibt es viele weitere Angriffsmöglichkeiten, wenngleich Malware-Angriffe eine besonders relevante Kategorie von Angriffen darstellen. In dieser Studie werden deshalb ausschließlich reputationsbasierte Schutzmechanismen zur Abwehr von Malware-Angriffen betrachtet. Insofern macht diese Studie keine Aussage über andere Sicherheitseigenschaften von Browsern. Die Untersuchung und Erstellung dieser Studie wurde mit finanzieller Unterstützung der Microsoft Deutschland GmbH und dem Center for Advanced Security Research Darmstadt (CASED, www.cased.de) durchgeführt.

Key Words: Malware, Reputationssysteme, Web-Sicherheit, Hacking, Browsersicherheit

---

Kontaktadresse: Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Rheinstraße 75, 64295 Darmstadt. Web: `http://www.sit.fraunhofer.de`, E-Mail: `vorname.nachname@sit.fraunhofer.de`

INHALTSVERZEICHNIS

1. KURZZUSAMMENFASSUNG (EXECUTIVE SUMMARY)

Da Browser heute häufig als Einfallstor für Angriffe aus dem Internet dienen, ist es sinnvoll, bereits in Browsern bestimmte Schutzmechanismen gegen Angriffe aus dem Internet vorzusehen. So verfügen sie deshalb beispielsweise über Reputationssysteme, mit denen Benutzer vor Malware-Angriffen geschützt werden können. Die Mechanismen verwenden hierzu Reputationswerte von URLs und heruntergeladenen Inhalten, um die Ausführung von Angriffen zu verhindern. Die reputationsbasierten Schutzmechanismen der gängigen Browser sind heute mit einer der folgenden Technologien implementiert: Safe Browsing von Google oder SmartScreen-Filter von Microsoft.

In dieser Arbeit werden die reputationsbasierten Schutzmechanismen zur Abwehr von Malware-Angriffen von fünf verschiedenen Browsern untersucht und verglichen, die jeweils eine der beiden Technologien verwenden. Hierzu wurden über einen Zeitraum von vier Wochen URLs gesammelt, die auf Malware-Inhalte verwiesen. Die Browser wurden durch das sukzessive Aufrufen dieser URLs realen Angriffen ausgesetzt und ihre Reaktionen und Eigenschaften im Rahmen eines Black-Box-Ansatzes getestet. Zusätzlich wurde Malware gesammelt, testweise heruntergeladen und das Browser-Verhalten beim und nach dem Herunterladen analysiert. Danach wurden die durch die Tests erhaltenen Messergebnisse anhand verschiedener Kriterien analysiert und ausgewertet. Es wurden folgende Browser in der angegebenen Version betrachtet:

- Chrome 14
- Firefox 6
- Internet Explorer 8
- Internet Explorer 9
- Safari 5

Die Untersuchung und Erstellung dieser Studie wurde mit finanzieller Unterstützung der Microsoft Deutschland GmbH und dem Center for Advanced Security Research Darmstadt (CASED, `www.cased.de`) durchgeführt. Die Tests, Messungen, Analysen und Auswertungen wurden unabhängig, unparteiisch und fair durchgeführt. Fraunhofer SIT war in der Auswahl der Methodik zur Durchführung frei. Es gab weder Vorgaben von Seiten eines Browser-Herstellers zur Auswahl der Methodik noch konnte sich ein Browser-Hersteller eine von Fraunhofer SIT vorgeschlagene Methodik unter anderen auswählen. Zur Durchführung der Arbeiten hat Fraunhofer SIT die Kriterien zur Analyse und Auswertung selbst entwickelt. Keiner der betroffenen Browser-Hersteller wurde vor oder während der Durchführung dieser Arbeiten über die verwendeten Kriterien in Kenntnis gesetzt.

Die Studie betrachtet ausschließlich adress- und inhaltsbasierte Reputationssysteme der Browser zur Abwehr von Malware-Angriffen, wie sie durch Standardkonfiguration, d.h. ohne Erweiterungen und Änderung der Einstellungen, zur Verfügung stehen. Die Standardkonfiguration wurde gewählt, um die Reputationssysteme für einen typischen Benutzer, der über kein besonderes technisches Hintergrundwissen verfügt, zu untersuchen. Die Entscheidung, ausschließlich Malware-Angriffe zu betrachten, wurde aufgrund der Beobachtung getroffen, dass diese immer stärker an Bedeutung gewinnen, während die Anzahl der klassischen Phishing-Angriffe abnimmt [BSI11]. So sieht das Bundesamt für Sicherheit in der Informationstechnik (BSI) in seinem „Register aktueller Cyber-Gefährdungen und -Angriffsformen“ von Januar 2012 unter den Top 6 Gefährdungen allein 4 mit direktem Bezug zu Malware [BSI12].

Bei der Untersuchung wurden verschiedene Tests durchgeführt, deren Messergebnisse nach Ende der Testphase unter Berücksichtigung verschiedener Kriterien ausgewertet wurden: Es wurde betrachtet, welche Malware-Angriffe Browser insgesamt erkannt haben und wieviel Zeit sie dafür in Anspruch nahmen. Darüber hinaus wurden die adress- und inhaltsbasierten Reputationssysteme separat und in ihrer Kombination untersucht. Bei adressbasierter Reputation werden URLs mittels einer URL-Blacklist untersucht, während bei inhaltsbasierter Reputation eine Überprüfung des Inhalts heruntergeladener Dateien mittels einer Malware-Blacklist stattfindet.

Insgesamt haben Internet Explorer 9 und Internet Explorer 8 über alle Teilergebnisse betrachtet die besten Leistungen erzielt. Dabei konnte sich der Internet Explorer 9 auch aufgrund seines inhaltsbasierten Reputationssystem positiv vom Internet Explorer 8 abheben. Auf Platz 3 folgt Chrome 14, während Safari 5 den 4. Platz belegt und Firefox 6 das Schlusslicht bildet.

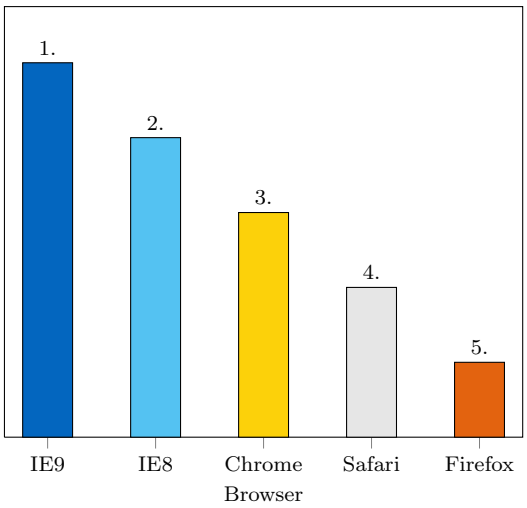

Abbildung 1. Platzierung

Im Folgenden werden einige wichtige Ergebnisse der Untersuchung zusammengefasst:

— Internet Explorer 8 und Internet Explorer 9 (SmartScreen-Filter) blockierten deutlich mehr Malware-URLs als Chrome 14, Firefox 6 und Safari 5 (Safe Browsing).
— Internet Explorer 8 und Internet Explorer 9 zeigten insgesamt eine bessere Dynamik bei der Pflege der Blacklists mit Malware-URLs als Chrome 14, Firefox 6 und Safari 5. Neue URLs mit gefährlichen Inhalten waren schneller in den Blacklists von Internet Explorer 8 und Internet Explorer 9 enthalten als in den Blacklists von Chrome 14, Firefox 6 und Safari 5.
— Internet Explorer 9 zeichnete sich besonders durch seine Application Reputation aus. Kein anderer Browser verfügte über eine solches inhaltsbasiertes Reputationssystem. Allerdings zeigte sich, dass dieser Mechanismus noch verbessert werden kann, da bei alleiniger Betrachtung der Application Reputation lediglich 14,9% der getesteten Malware aus einer gesonderten Datensammlung erkannt wurde.
— Bei der kombinierten Betrachtung von adress- und inhaltsbasierter Reputation konnte der Internet Explorer 9 mittels URL-Erkennung und Erkennung von Malware-Dateien (Application Reputation) insgesamt 39,1% der getesteten Malware blockieren.

Die Ergebnisse dieser Studie konnten die Ergebnisse von zwei Untersuchungen durch die NSS Labs [NSS11a; NSS11b] tendenziell bestätigen. Jedoch konnten die dort angegebenen Werte des Internet Explorer 9 bei der Erkennung von Malware-URLs und bei der kombinierten Erkennung von Malware-URLs und Malware-Dateien durch Application Reputation nicht nachvollzogen werden: In [NSS11a] erreichte der Internet Explorer 9 mit URL- und Application Reputation in Europa einen Erkennungswert von 100% während in der hier vorliegenden Studie höchstens 39,1% erreicht wurden.

Es sei an dieser Stelle ausdrücklich darauf hingewiesen, dass in dieser Studie ausschließlich Reputationssysteme zum Schutz gegen Malware betrachtet wurden. Andere Angriffe und Schutzmechanismen wurden nicht betrachtet. Auch wenn der Schutz gegen Malware sehr relevant für Sicherheit des Benutzers im Internet ist, so sind für die Gesamtsicherheit viele weitere Schutzmechanismen gegen andere Angriffstypen notwendig. Diese waren jedoch nicht Gegenstand der Studie und ausgehend von den Ergebnissen dieser Studie sind keine Aussagen über andere Sicherheitsmechanismen der Browser und andere Angriffstypen zulässig.

2. EINLEITUNG UND MOTIVATION

Die Anwendung moderner Informations- und Kommunikationstechnologie ist heute aus dem Alltag von Unternehmen, behördlichen Einrichtungen und Privatpersonen nicht mehr wegzudenken. Computer und Internet sind zu wesentlichen Bestandteilen des Lebens geworden und tragen in erheblichem Umfang zur Wertschöpfung in unserer Gesellschaft bei. Jedoch steigt auch die Gefahr der Verletzlichkeit, wenn Hacker versuchen, anderen zu schaden bzw. sich selbst einen Vorteil zu verschaffen. Das Spektrum dieser Angriffe ist sehr breit: Es beinhaltet das Ausspionieren vertraulicher Dokumente (z.B. Wirtschaftsspionage), das Vorspielen falscher Identitäten, das Ausspionieren von Passwörtern und Zugangsdaten für elektronische Zahlungssysteme, das Eindringen in Systeme zur Manipulation oder zum Löschen von Daten, das Infizieren von Computern zum Aufbau von Botnets für große organisierte Angriffe gegenüber Dritten (z.B. Denial-of-Service-Angriffe) oder die Beeinträchtigung der Funktion von Computern und anschließende Erpressung von Lösegeld zur Wiederherstellung des Originalzustands (z.B. Angriffe mit Ransomware).

Für diese Angriffe gibt es eine Reihe von (Ober-)Begriffen, die synonym verwendet werden z.B. *Hacking*, *Cybercrime* oder *e-Crime*. Die Relevanz dieser Angriffe wird durch aktuelle Fakten bestätigt:

- Das Bundesamt für Sicherheit in der Informationstechnik (BSI) führt in [BSI12] die Top 6 der aktuellen Cyber-Bedrohungen auf. Allein 4 davon betreffen die Verbreitung von Malware, wie beispielsweise gezieltes Hacking von Webservern zur Platzierung von Schadsoftware, Drive-by-Exploits und Malware-Infiltration über Email zur Übernahme des Rechners.
- Das BSI meldet in seinem Lagebericht zur IT-Sicherheit in Deutschland 2011 [BSI11], dass die Bedrohung durch Botnets, die in der Regel aus infizierten Computern von Privatnutzern bestehen, in den vergangenen zwei Jahren massiv zugenommen hat. Botnets werden professionell vermietet und für Angriffe genutzt.
- Das BSI stellt in [BSI11] zusätzlich fest, dass sich Identitätsdiebstahl und Identitätsmissbrauch durch die Aussichten auf finanzielle Bereicherung als rege Betätigungsfelder für

Kriminelle etabliert haben. Dabei haben sich hochprofessionelle Strukturen entwickelt. Die am häufigsten gestohlenen Informationen sind Zugangsdaten zu Handelsplattformen sowie zu Webmail-Diensten, über die wiederum weitere Zugangsdaten erlangt werden können.

- KPMG stellt in seiner e-Crime-Studie [KPM10] fest, dass ein Viertel der von KPMG befragten Unternehmen in den drei vorangegangenen Jahren von e-Crime betroffen war. Dabei wird der Diebstahl von Kunden- oder Arbeitnehmerdaten als größtes Risiko eingeschätzt.
- KPMG erklärt in seiner e-Crime-Studie [KPM10] weiter, dass die Schadenshöhen für Unternehmen bei über 100.000 Euro bis zu Millionenbeträgen pro Einzelfall liegen. Vor allem Datendiebstahl und das Ausspähen von geschäftskritischen Unternehmensinformationen verursachen Schäden von über einer Million Euro pro Vorfall.
- Die Anzahl der nach dem Bundeskriminalamt (BKA) in der polizeilichen Kriminalstatistik erfassten Fälle von Cybercrime ist vom Jahr 2009 zum Jahr 2010 um 19,1% gestiegen [BKA10].
- Seit dem Jahr 2009 liegt die jährliche Anzahl neuer Malware weltweit im zweistelligen Millionenbereich [AV 11], Tendenz stark steigend. Momentan werden täglich weltweit mehr als 55.000 verschiedene Schadprogramme registriert [AV 11].
- Nach Aussage des Branchenverbands Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) waren in 2010 ca. 22 Millionen der deutschen Internet-Nutzer schon mindestens einmal von Malware betroffen [BIT10].

Für das Vorgehen bei diesen Angriffen lassen sich grob die folgenden Kategorien unterscheiden:

- Technische Angriffe: Bei diesen Angriffen nutzt ein Hacker ihm bekannte technische Lücken aus, um an sein Angriffsziel zu gelangen. Diese Angriffe erfordern zunächst einmal das Vorhandensein einer rein technisch bedingten Sicherheitslücke, oftmals einen hohen technischen Sachverstand zur Erkennung dieser Lücke und zur geschickten Umgehung von Schutzmaßnahmen oder zumindest die Kenntnis von Spezialwerkzeugen zur Ausnutzung dieser Lücke.
  - Direkte, rein technisch orientierte Angriffe: Hierbei wird eine Lücke in dem System ausgenutzt, das Ziel des Angriffes ist.
  - Indirekte, rein technisch orientierte Angriffe: Hierbei werden ebenfalls technische Sicherheitslücken ausgenutzt, jedoch liegen diese Lücken nicht in dem System vor, welches Ziel der Angriffe ist, sondern sie existieren in einem anderen System. So ist es beispielsweise möglich, einen Computer eines Benutzers indirekt anzugreifen, indem Angreifer Sicherheitslücken in Webservern ausnutzen und darüber Schadcode verbreiten.
- Social-Engineering-Angriffe (SEA): Bei diesem Typ von Angriffen ist in der Regel kein technisches Hintergrundwissen erforderlich. Das Angriffsziel wird nicht durch Ausnutzung von technischen Sicherheitslücken erreicht, sondern vielmehr dadurch, dass Benutzer entweder aus freien Stücken oder durch Manipulation dazu gebracht werden, sich in einer Weise zu verhalten, welche die Durchführung eines Angriffs überhaupt erst ermöglicht. Beispiele für SEA sind das Erraten von Passwörtern durch Kenntnis von persönlichen Hintergrundinformationen des Benutzers oder die erfolgreiche Aufforderung zum Herunterladen oder zur Installation von Software, welche Schadfunktionen enthält.

Für die hier vorliegende Untersuchung sind die Kategorien mit dem Ziel der Verbreitung von Malware von Interesse, bei denen die eigentliche Schwachstelle nicht im Computer des Benutzers liegt. Stattdessen werden zur Durchführung dieser Angriffe andere Schwachstellen ausgenutzt: entweder Schwachstellen in anderen Systemen oder die Schwachstelle Mensch.

Bei Malware-Angriffen soll Schadsoftware auf den Computer des Opfers gebracht werden. Das kann sowohl unbemerkt als auch unter unbeabsichtigter Mithilfe des Opfers geschehen. Bei Angriffen über das Internet stellen Browser das natürliche Einfallstor für Angriffe auf Benutzer dar. Browser lassen sich für Malware-Angriffe nutzen, ohne dass direkte technische Sicherheitslücken in den Browsern selbst gefunden und ausgenutzt werden müssen. Hierzu können Angreifer entweder Schwachstellen anderer Systeme, Software-Komponenten oder die Schwachstelle Mensch mittels SEA ausnutzen.

Das BSI stellt in seinem Bericht zur Lage der IT-Sicherheit in Deutschland für 2011 fest, dass die Angriffe über klassisches Phishing abnehmen und dafür die Anzahl der Malware-Angriffe zunimmt [BSI11]. Unter den Top 6 der aktuellen Cyber-Gefährdungen des BSI stehen 4 in direktem Bezug zu Malware [BSI12]. Heute wird selbst bei Phishing-Angriffen zum Ausspionieren von Zugangsdaten oftmals Malware wie z.B. Keylogger verwendet.

Auch wenn diese Malware-Angriffe keine Sicherheitslücken in Browsern ausnutzen, bieten heutige Browser Mechanismen zum Schutz von Benutzern an, mit denen Angriffe abgewehrt werden können. Diese Abwehrmechanismen arbeiten nach unterschiedlichen Prinzipien:

- Adressbasierte Reputation: Hierzu werden Internetadressen (URLs) entsprechende Reputationswerte zugeordnet und bekannten Angriffs-URLs in Blacklists geführt mit denen dann die Browser arbeiten. Wird eine in der Blacklist enthaltene URL angesteuert, so warnt der Browser den Benutzer vor der dahinterliegenden Website, bevor die Seite geladen wird. Die Browser laden im Hintergrund die entsprechenden Blacklists von einer zentralen Stelle die den Inhalt der Blacklist pflegt. Wichtig für die in einem Browser enthaltene Blacklist ist, dass sie stets aktuell gehalten wird und neue gefährliche URLs möglichst frühzeitig enthält. Bei der Pflege von Blacklists werden Browser-Rückmeldungen und Erfahrungen von Anwendern mit bestimmten URLs berücksichtigt.
- Inhaltsbasierte Reputation: Statt URLs werden hier heruntergeladenen Inhalten entsprechende Reputationswerte zugeordnet, welche ebenfalls in Form von Blacklists bereitgestellt werden. Auch diese Blacklists werden von den Browsern im Hintergrund über das Internet geladen und von einer zentralen Stelle gepflegt. Somit wird dem Browser ermöglicht, nach dem Herunterladen einer Datei diese dahingehend zu überprüfen, ob ihr Inhalt in der Blacklist enthalten ist, also eine bekannte Malware darstellt. Ist dies der Fall, so wird die Datei blockiert bzw. gelöscht, sodass sie nicht über den Browser ausgeführt wird und Schaden anrichten kann. Bei der Pflege dieser Blacklists werden ebenfalls Browser-Rückmeldungen und Erfahrungen von Anwendern mit bestimmten URLs berücksichtigt.

Die beiden Abwehrmechanismen können in der Praxis auch kombiniert wirken. Es wird beispielsweise bei einer Download-URL zunächst die URL überprüft. Ist diese nicht in der URL-Blacklist enthalten, dann wird die anschließend heruntergeladene Datei mit einer Download-Blacklist abgeglichen. Diese Abwehrmechanismen sind in der Praxis für Anwender sehr wichtig, denn durch aktive Warnhinweise können viele Benutzer vor Malware-Angriffen geschützt werden.

Das Fraunhofer-Institut für Sichere Informationstechnologie (Fraunhofer SIT) hat untersucht, wie gut die Reputationssysteme einiger gängiger Browser bei der Abwehr von

Malware-Angriffen wirken, d.h. wie gut diese entsprechende Angriffe erkennen und die Benutzer warnen. Hierbei wurde insbesondere berücksichtigt, wie gut die Browser gerade technisch weniger versierte Benutzer schützen, weshalb die Browser in ihren Standardausführungen untersucht und bewertet wurden. Erweiterungen, welche zusätzlich zu den Browsern installiert werden müssen (z.B. Webutation für Firefox), wurden deshalb in der Untersuchung nicht berücksichtigt. Es wird angenommen, dass ein technisch weniger versierter Benutzer den Browser wahrscheinlich in der Konfiguration nutzt, in der er ihn nach der Installation vorgefunden hat und keine Veränderungen an den Einstellungen oder bzgl. Erweiterungskomponenten vorgenommen werden. Der Studie liegt die Forderung zugrunde, dass sich auch diejenigen Benutzer sicher im Internet bewegen können sollen, die sich nur wenig mit den vielen Gefahren, Risiken und Abwehrmöglichkeiten auskennen.

In der vorliegenden Arbeit wurden die 32-Bit-Versionen der folgenden Browser für Windows 7 untersucht:

- Chrome 14
- Firefox 6
- Internet Explorer 8
- Internet Explorer 9
- Safari 5

Zur Aufbauzeit des für die Untersuchung erforderlichen Mess- und Analysesystems waren die in der vorangegangenen Liste angeführten Browser-Versionen aktuell. Während der Messung und Analyse wurden neue Versionen dieser Browser veröffentlicht. Für die Untersuchung wurden jedoch die angegebenen Browser-Versionen beibehalten, da das Mess- und Analysesystem an diese angepasst war. Inwieweit die in und nach dem Testzeitraum stattgefundenen Versionswechsel der Browser die hier gewonnenen Ergebnisse verändern würden, kann deshalb in dieser Studie nicht behandelt werden. Den Autoren ist beispielsweise bekannt, dass die im Februar 2012 veröffentlichte Version Chrome 17 im Gegensatz zu Chrome 14 zusätzlich über ein inhaltsbasiertes Reputationssystem zum Schutz gegen Malware verfügt. Zum Release-Zeitpunkt von Chrome 17 waren die Tests jedoch bereits abgeschlossen.

Bei der Durchführung der Studie wurden sukzessive URLs gesammelt, die Fraunhofer SIT als Quelle von Malware-Angriffen bekannt waren und welche zur Verbreitung von Malware benutzt wurden. Diese URLs wurden auf verschiedenen Wegen erhalten, z.B. wurden sie aus Spam-Emails extrahiert, die an Mail-Server geschickt wurden, die das Fraunhofer SIT eigens zu diesem Zweck ohne jeglichen Spam-Schutz aufgestellt hat. Für diese Adressen wurde das Verhalten der Browser über einen längeren Zeitraum hin beobachtet und analysiert. Die Browser wurden hierbei als Black Box angenommen, d.h. es wurden lediglich deren Eingaben und Ausgaben berücksichtigt. Darüber hinausgehende interne Abläufe der Browser wurden nicht betrachtet.

Zur Auswertung des Verhaltens der Browser wurden Kriterien und Metriken definiert, anhand derer die Eigenschaften der Browser quantifiziert und verglichen werden können. Die Studie wurde unabhängig, unparteiisch und fair durchgeführt. Die Vorgehensweise und die Kriterien zur Bewertung wurden von Fraunhofer SIT frei und unabhängig selbst ausgewählt. Bei Durchführung der Untersuchung waren keinem der Browser-Hersteller die verwendeten Kriterien bekannt.

Die Studie beschreibt Eigenschaften der reputationsbasierten Schutzmechanismen gegen Malware-Angriffe der betrachteten Browser für den Zeitraum der Messung. Die Aussagen

über die Eigenschaften und Leistungsfähigkeit der Schutzmechanismen basieren auf aktuellen URLs und Malware, wie sie das Fraunhofer SIT über den Betrachtungszeitraum gesammelt und für die Browser-Tests herangezogen hat. Insofern werden keine Aussagen über andere URLs und andere Malware getroffen. Es sei angemerkt, dass damit nur ein sehr kleiner Teil der URLs, von denen Angriffe ausgehen oder über welche Malware heruntergeladen werden kann, betrachtet werden konnte (siehe hierzu etwa [AV 11]). Darüber hinaus sei darauf hingewiesen, dass die beobachteten Eigenschaften und Leistungsfähigkeit der Schutzmechanismen nicht auf andere Zeiträume extrapoliert werden können. Insofern geben die Messungen und Ergebnisse für einen fiktiven Benutzer wieder, ob dieser in Abhängigkeit der betrachteten Browser in Standardeinstellung über dem gegebenen Beobachtungszeitraum vor Malware-Angriffen geschützt gewesen wäre, wenn er versucht hätte, die vom Fraunhofer SIT gesammelten URLs aufzurufen und ggf. die entsprechenden Dateien herunterzuladen.

3. GRUNDLAGEN

Die vorliegende Studie befasst sich damit, wie gut die adressbasierten und inhaltsbasierten Reputationssysteme in Browsern einen gewöhnlichen Benutzer vor Malware-Angriffen schützen. In Abschnitt 3.1 wird auf verschiedene Angriffskategorien eingegangen, vor denen Benutzer mittels reputationsbasierter Mechanismen geschützt werden können. In Abschnitt 3.2 werden einige konkrete Angriffe exemplarisch beschrieben. Abschnitt 3.3 befasst sich mit möglichen Risiken für Benutzer, die sich aus diesen Angriffen ergeben können. In Abschnitt 3.4 werden abstrakt reputationsbasierte Mechanismen zum Schutz gegen diese Angriffe beschrieben. Abschließend werden in Abschnitt 3.5 die in Browsern tatsächlich eingesetzten Technologien erläutert, welche die genannten reputationsbasierten Schutzmechanismen umsetzen.

3.1 Angriffskategorien

Mit reputationsbasierten Mechanismen lassen sich viele Malware-Angriffe abwehren, denen Browser-Nutzer im Internet ausgesetzt sind. Die damit abwehrbaren Angriffe lassen sich grob in zwei Kategorien einteilen: Social-Engineering-Angriffe (SEA) und indirekte, rein technische Angriffe. Beide Kategorien zeichnen sich dadurch aus, dass Angreifer primär keine Sicherheitslücken in Browsern ausnutzen. Im Folgenden werden die Angriffskategorien erläutert.

3.1.1 Indirekte, rein technische Angriffe

Bei dieser Art von Angriffen wird der Benutzer nicht über eine technische Sicherheitslücke in seinem Browser angegriffen. Vielmehr werden Schwachstellen in anderen Systemen ausgenutzt, um schließlich Browser-Nutzer anzugreifen. Beispielsweise könnte ein Angreifer Sicherheitslücken in Webservern ausnutzen, um Schadcode an Besucher der entsprechenden Webseiten zu verteilen.

Indirekte, rein technisch orientierte Angriffe auf Browser sind oft dann möglich, wenn andere technische Systeme nicht korrekt gewartet werden, z.B. wenn Sicherheitspatches für Webserver nicht rechtzeitig installiert werden. Einen wichtigen Ausgangspunkt für solche

Angriffe auf Browser stellen unsichere Webserver dar, welche von Angreifern derart manipuliert werden, dass über sie die Verteilung von Schadcode initiiert wird, wenn Benutzer Inhalte von diesen Webservern laden. Der Schadcode wird hierbei nicht notwendigerweise über den manipulierten Webserver direkt angeboten, sondern es kann beispielsweise ausreichend sein, lediglich einen Link auf eine URL in die Webserver-Inhalte einzubetten, von der der eigentliche Schadcode nachgeladen wird. In [PRM09] werden verschiedene Möglichkeiten für solche Angriffe über Webserver dargestellt. Aus Sicht eines Benutzers ist jeweils der Browser das Einfallstor für solche Angriffe. Aus der Perspektive des Angreifers ist dieses Vorgehen in der Regel nicht auf eine bestimmte Person ausgerichtet. Opfer können alle diejenigen Personen werden, welche eine entsprechend manipulierte Webseite zum falschen Zeitpunkt besuchen. Browser bieten deshalb heute Sicherheitsmechanismen, welche ihre Benutzer vor solchen Angriffen schützen können.

3.1.2 Social-Engineering-Angriffe (SEA)

SEA bezeichnen Angriffe, bei denen Benutzer durch zwischenmenschliche Beeinflussung oder durch geschickte Manipulation dazu gebracht werden, sich in einer Weise zu verhalten, die einen weiterführenden Angriff überhaupt erst ermöglicht. Es wird hierbei keine Schwachstelle in einem System ausgenutzt, sondern der Mensch selbst stellt die Schwachstelle dar. Angreifer benötigen oft nur wenig bis kein technisches Hintergrundwissen, da z.B. bereits das Klicken auf einen echt aussehenden Link in einer Email dazu führen kann, dass Malware heruntergeladen wird.

Da SEA direkt an der Schwachstelle Mensch ansetzen, müssen zu ihrer Durchführung keine neuen technischen Sicherheitslücken ausgenutzt oder gar gefunden werden; sie sind praktisch schon dann erfolgreich, wenn es gelingt, einen Benutzer dazu zu bringen, einen entscheidenden sicherheitskritischen Fehler zu machen. SEA werden entweder zielgerichtet für bestimmte Personen durchgeführt oder laufen unspezifisch ab, wobei viele verschiedene Personen ins Visier genommen werden in der Hoffnung, dass der Angriff bei einigen von ihnen erfolgreich ist.

3.2 Angriffe

Bei Angriffen auf Browser-Benutzer wird meist versucht, eine Malware auf deren Computer einzuschleusen. Zur konkreten Umsetzung von Malware-Angriffen gibt es viele Möglichkeiten, von denen hier einige exemplarisch aufgeführt werden sollen. Nach Aussage des BSI stellen Phishing- und Malware-Angriffe eine große Bedrohung im heutigen Internet dar. Das BSI stellt jedoch fest, dass Malware-Angriffe immer stärker zunehmen, wohingegen klassische Phishing-Angriffe in ihrer Anzahl rückläufig sind [BSI11].

3.2.1 Malware-Seite

Hier besteht das Ziel eines Angreifers darin, Malware über einen Webserver bereit zu stellen. Die Malware kann dabei bereits in eine Webseite eingebettet sein oder als separater Download zur Verfügung gestellt werden. Das Ziel, Malware auf dem Computer eines Benutzers auszuführen, kann dabei erreicht werden, indem der Benutzer selbst die Malware nach dem Herunterladen durch eine weitere Interaktion zur Ausführung bringt. Es ist jedoch auch möglich, dass eine Malware nach dem Herunterladen automatisch ausgeführt wird. In diesem Fall spricht man auch von einem *Drive-by-Download*. Ein Beispiel hierfür ist eine URL, über welche eine mit Malware infizierte PDF-Datei geladen werden kann. Da in Browsern

meist eine Komponente zur automatischen Anzeige von PDF-Dateien enthalten ist, muss ein Benutzer nicht mehr tun, als diese URL aufzurufen, um seinen Computer mit Malware zu infizieren.

Den Konsequenzen, die die Malware-Infektion eines Computers nach sich ziehen kann, sind theoretisch keine Grenzen gesetzt und hängen vom eigentlichen Ziel des Angreifers ab.

3.2.2 Malware durch Manipulation von Webserver-Inhalten

Eine weitere Möglichkeit zur Verteilung von Malware ergibt sich, wenn es einem Angreifer gelingt, den Webserver eines Dritten zu manipulieren. In diesem Fall kann er beispielsweise Links einbetten, so dass beim Klick eines Benutzers auf einen Link Malware auf dessen Computer geladen wird. Wird die Malware sogar automatisch ausgeführt, dann ist der Computer durch einen einzigen Klick in einer für den Benutzer ggf. vertrauten Umgebung infiziert.

3.2.3 Versenden von Malware-URLs

Um möglichst viele potentielle Opfer zu erreichen, kann ein Angreifer versuchen, durch das Versenden von Emails die Empfänger dazu zu verleiten, dass diese seine in den Emails enthaltenen Malware-URLs besuchen. Klickt der Email-Empfänger auf eine angezeigte URL, wird diese anschließend im Browser geladen und ggf. sogar ein Drive-by-Download angestoßen. Durch das Versenden und Anzeigen von HTML-Emails kann der Angriff gut getarnt werden, da sich hier Malware-URLs mit harmlos oder bekannt scheinenden URLs "maskieren"lassen, die als Link-Text angezeigt werden. Dieser Angriff kann selbst bei sicherheitsbewussten Benutzern gelingen, da von ihnen meist nur der Link-Text der URL, nicht jedoch die eigentliche URL kontrolliert wird.

Ein Beispiel für einen solchen Angriff wird in Abbildung 2 gezeigt. Die meisten Benutzer gehen in einem solchen Fall davon aus, dass beim Klick auf die angezeigte URL in der Email eine Verbindung zu `https://www.facebook.com/benchfolksjobs` aufgebaut wird. Der angezeigte Link-Text weicht jedoch von der eigentlichen URL ab, die stattdessen auf `http://www.malware.org/attack.pdf` verweist. Ist das entsprechende Plugin im Browser enthalten, wird die dahinterliegende präparierte PDF-Datei sofort geöffnet und der Computer ist ohne weiteres Zutun infiziert.

3.2.4 Malware über URL-Redirect

Bei einem URL-Redirect wird eine Anfrage an eine vom Benutzer eingegebene URL auf eine andere URL umgeleitet. Gelingt es einem Angreifer, einen anderen Webserver geeignet zu manipulieren, dann kann er dort für eine bekannte URL einen URL-Redirect auf eine Malware-Seite bzw. einen Drive-by-Download festlegen. Das Bemerken eines solchen Angriffs ist nicht immer einfach, da sich Inhalte und Darstellung nach Laden der umgeleiteten URL nicht zwangsläufig von den erwarteten Inhalten und Darstellung unterscheiden müssen. Aus der Perspektive eines Benutzers ist das Erkennen solcher Angriffe auch deshalb schwierig, da es Internetangebote gibt, die absichtlich von URL-Redirects Gebrauch machen, ohne dass ein Angriff vorliegt. Tippfehler in der Adresszeile, beispielsweise `www.gogle.de` wie in Abbildung 3 können so zur korrekten Adresse `www.google.de` weitergeleitet werden (Abbildung 4). Die meisten Benutzer konnten sich von den positiven Seiten eines URL-Redirects bestimmt schon einmal überzeugen, da dieser Mechanismus bei Tippfehlern zur Benutzerfreundlichkeit beiträgt. Da Benutzer dann den URL-Redirect ggf. sogar kennen

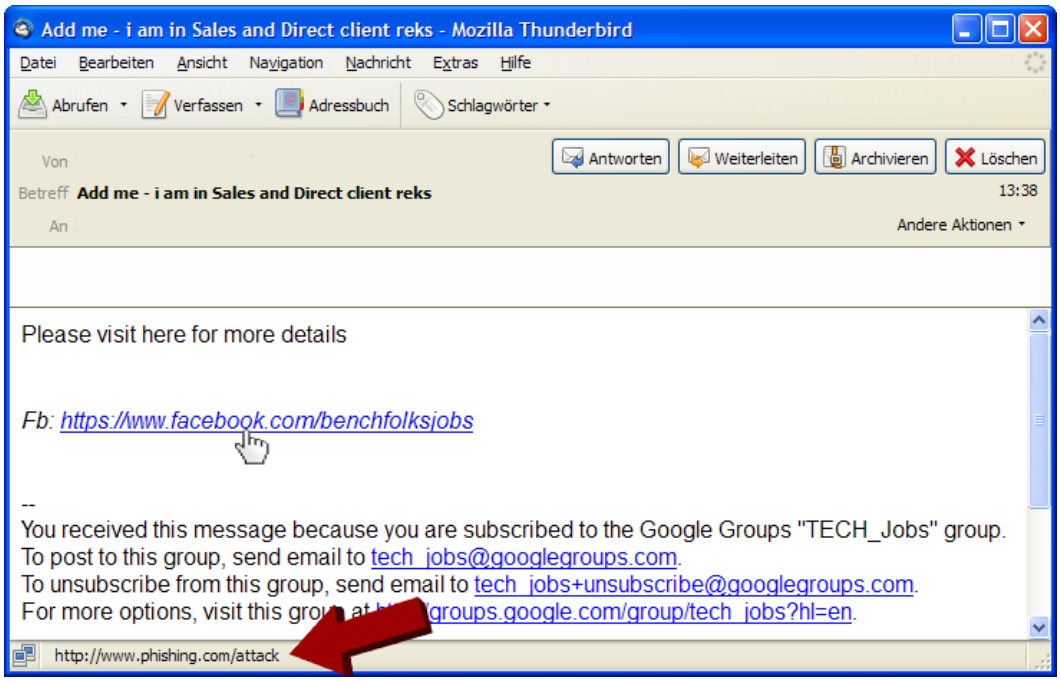

Abbildung 2. Email mit gefälschtem Link

und somit eher etwas Angenehmes damit verbinden, wird ein Angriff über URL-Redirects wahrscheinlich nicht als solcher wahrgenommen.

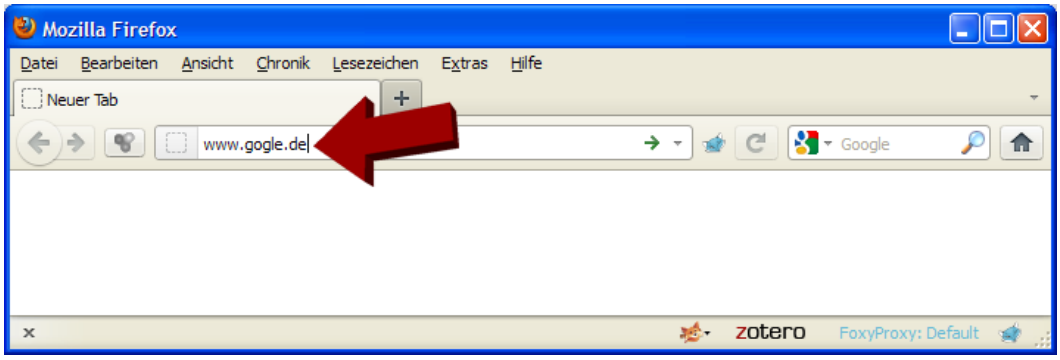

Abbildung 3. Tippfehler in der Adresszeile

URL-Redirects werden durch den Webserver festgelegt, so dass es einem Angreifer gelingen muss, den Webserver, der unter der eingegebenen URL erreichbar ist, zu manipulieren.

3.2.5 Malware über URL-Shortening

Short URLs wurden eingeführt, damit Benutzer keine langen URLs eingeben müssen bzw. damit es beim Verschicken in Emails nicht zu Zeilenumbrüchen kommt, durch welche entsprechende Links beschädigt würden, oder damit bei Diensten wie Twitter die (nach oben begrenzte) Anzahl der verwendeten Zeichen einer Nachricht nicht unnötig erhöht wird. Ein Benutzer wird beim Aufrufen einer Short URL auf die mit ihr verknüpfte und typischer-

Abbildung 4. Weiterleitung auf eine andere URL (kein Angriff)

weise längere URL umgeleitet. Short URLs sind in der Regel so gestaltet, dass sie keine Bedeutung haben, die einer natürlichen Sprache entlehnt ist.

Aus Sicht eines Benutzers ist beim Aufrufen einer Short URL nicht klar, welche URL nach der Umleitung tatsächlich aufgerufen wird. Benutzer klicken ohne größere Bedenken auf Links in Emails, wenn sie davon ausgehen, dass der Absender der Email eine aus ihrer Sicht vertrauenswürdige Person ist. Dabei wird leider oftmals nicht berücksichtigt, dass es sich bei dem angezeigten Absender gar nicht um den tatsächlichen Absender handeln muss. Die heutige Verbreitung von sozialen Netzwerken wie z.B. Facebook hilft Angreifern, das soziale Umfeld von Benutzern in Erfahrung zu bringen und somit Emails unter dem Namen und mit der Email-Adresse eines Bekannten zu versenden.

3.3 Risiken

Die Risiken durch erfolgreiche Malware-Angriffe können für Betroffene sehr groß sein. Durch Malware auf infizierten Computern lassen sich beispielsweise Zugangsdaten ausspionieren, z.B. mit Keyloggern. So lässt sich Malware auch für die gleichen Zwecke missbrauchen wie Phishing. Ausgespähte Zugangsdaten können selbst für viele verschiedene Zwecke missbraucht werden. Da Benutzer oftmals für unterschiedliche Dienste die gleichen Passwörter verwenden [IWS04; YBAG04], steigt das Risiko weiter. Ziele von Angriffen sind vorrangig Informationen, IT-Dienste und IT-Systeme. Das BSI sieht einen Trend für eine starke Zunahme von Malware [BSI11]. Allein unter den Top 6 Cyber-Gefährdungen sieht das BSI 4 in direktem Zusammenhang mit Malware [BSI12]. Parallel zu dieser Entwicklung geht klassisches Phishing zurück. Im Folgenden werden Möglichkeiten für den Missbrauch durch Malware aufgeführt:

– Missbrauch durch Ransomware: Angreifer infizieren Computer mit dem Ziel, diese praktisch unbenutzbar zu machen z.B. durch Manipulation des Betriebssystems oder durch

Verschlüsselung wichtiger Daten, so dass der Benutzer nicht mehr darauf zugreifen kann. Um den Vorgang rückgängig zu machen, wird vom Benutzer ein Lösegeld gefordert.

— Missbrauch durch Spyware: Computer mit installierter Spyware bergen das Risiko, dass ihre Benutzer ausspioniert und vertrauliche Daten über das Internet dem Angreifer übermittelt werden. Für Unternehmen bedeutet Spyware auf Computern ein hohes finanzielles Risiko (z.B. Wirtschaftsspionage, Diebstahl von Kundendaten).

— Missbrauch durch Botnets: Werden Computer Teil eines Botnets, können sie für Angriffe auf Dritte missbraucht werden (z.B. für Denial-of-Service-Attacken auf Webangebote).

— Ausgespähte Zugangsdaten: Mittels erspähter Zugangsdaten lassen sich beispielsweise vertrauliche Informationen in Erfahrung bringen, manipulieren oder löschen und Emails unter fremder Identität versenden. Im Kontext professioneller Angriffe kann der sich daraus ergebende Schaden sehr hoch sein, z.B. durch Industriespionage oder Reputationsverlust. Auch können Privatnutzern große Verluste entstehen, beispielsweise durch in ihrem Namen initiierte und authentisierte Geldtransaktionen.

Die verschiedenen Möglichkeiten für Missbrauch haben in der Vergangenheit zu großen Schäden geführt und implizieren auch für die Zukunft enorme Risiken. Vor einer weiteren Professionalisierung der Betrugsmethoden warnt der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) [BIT10]. BITKOM zufolge haben 5% der Internet-Nutzer in Deutschland (etwa 2,5 Millionen Menschen) bis 2010 einen finanziellen Schaden durch Datendiebstähle oder Schadprogramme erlitten. Die Liste der prominenten Opfer ist sehr lang (siehe etwa [Eik11; Mü11; Spi11a; Spi11b]).

3.4 Reputationsbasierte Schutzmechanismen

Reputationsbasierte Schutzmechanismen in Browsern helfen dabei, Benutzer vor Angriffen durch Malware und insbesondere vor menschlichem Fehlverhalten bei der Browser-Nutzung zu schützen. Die reputationsbasierten Schutzmechanismen lassen sich folgendermaßen klassifizieren:

— Adressbasierte Reputationssysteme: Bei diesen Reputationssystemen werden URLs Reputationswerte zugeordnet. In Abhängigkeit des Reputationswerts einer URL warnt der Browser den Benutzer ggf. beim Aufrufen einer entsprechenden URL.

— Inhaltsbasierte Reputationssysteme: Im Gegensatz zu adressbasierten Reputationssystemen werden hier den Inhalten herunterladbarer Dateien Reputationswerte zugeordnet. In Abhängigkeit der Reputation eines Dateiinhalts warnt der Browser den Benutzer ggf. nach dem Herunterladen des Inhalts.

Diese beiden Schutzmechanismen können auch in Kombination angewendet werden und wirken explizit beim Herunterladen von Malware als zwei hintereinander liegende Verteidigungslinien.

Grundsätzlich können Reputationswerte in verschiedenen Typen von Listen verwendet werden:

— Blacklist: In dieser Liste werden alle Objekte (URL oder Dateiinhalt) notiert, die in der Vergangenheit als Mittel zur Durchführung von Angriffen beobachtet wurden. Wird ein Objekt überprüft und in der Blacklist gefunden, dann gibt der Browser eine Warnung aus bzw. blockiert das jeweilige Objekt.

— Whitelist: In dieser Liste werden alle Objekte notiert, die als garantiert harmlos und sicher gelten. Wird ein Objekt überprüft und in der Whitelis gefunden, so erlaubt der Browser den Zugriff auf das jeweilige Objekt und signalisiert Unbedenklichkeit bzw. zeigt keine Warnung an.

Jedes Objekt ist entweder in einer Blacklist, in einer Whitelist oder in keiner dieser beiden Listen enthalten. Dadurch ergeben sich die in Tabelle I gezeigten möglichen Reaktionen von Browsern.

	adressbasierte Reputation	inhaltsbasierte Reputation
enthalten in Blacklist	URL wird wegen Gefahr durch Malware blockiert	Datei wird vor Ausführung blockiert da Malware
enthalten in Whitelist	URL wird als unbedenklich eingestuft und Zugriff wird gestattet	Herunterladen und Ausführen der Datei wird erlaubt
in keiner Liste enthalten	URL ist unbekannt und unklassifiziert (weiteres Vorgehen auf eigene Gefahr)	Dateiinhalt ist unbekannt und unklassifiziert (weiteres Vorgehen auf eigene Gefahr)

Tabelle I. Mögliche Reaktionen auf Reputationswerte in Browser

Die Überprüfung der Reputation einer URL wird durchgeführt, bevor eine Verbindung zur URL aufgebaut wurde. Die Überprüfung der Reputation eines Dateiinhalts kann jedoch immer erst dann durchgeführt werden, wenn die Datei vollständig heruntergeladen wurde. Bei einer kombinierten Anwendung beider Reputationssysteme wird also immer zunächst die Reputation der URL überprüft, bevor die Reputation des Dateiinhalts überprüft werden kann. Dadurch ergibt sich die natürliche Reihenfolge dieser Verteidigungslinien.

Zur Entscheidung über Blockieren oder Zulassen können lokale oder zentrale und entfernte Black- und Whitelists sowie Kombinationen aus beiden verwendet werden. Die Verwendung lokaler Listen spart den Kommunikationsaufwand, so dass nicht für jede einzelne Entscheidung von allen Browsern zentrale Listen abgefragt werden müssen. Zentrale und entfernte Listen können dann hinzugezogen werden, wenn die Abfrage lokaler Listen nicht weiterhilft.

Von großer Bedeutung für die Sicherheit der reputationsbasierten Schutzmechanismen ist die Korrektheit und Aktualität der Listen. Das gilt sowohl für lokale als auch für zentral und entfernt gepflegten Listen. So sollten beispielsweise keine bedenklichen Objekte in der Whitelist enthalten sein. Einträge sollten grundsätzlich möglichst früh in die jeweilige Liste aufgenommen werden, um die Benutzer optimal zu schützen. Für Korrektheit und Aktualität ist neben der Pflege der Listen auch deren sichere und schnelle Verteilung notwendig, so dass auch die lokalen Listen stets die geforderte Qualität besitzen.

Zur Pflege der Listen können automatische Rückmeldungen von Browsern sowie manuelle Rückmeldungen von Browser-Nutzern verwendet werden, wie z.B. die Meldung einer Malware-URL zur Aufnahme in eine zentrale Blacklist. Neue Einträge werden dann in Listen aufgenommen, wenn ein bestimmter Schwellwert bei der Bewertung erreicht ist oder der Wahrheitsgehalt einer Meldung kontrolliert wurde.

3.5 Technologie

Für die in Abschnitt 3.4 beschriebenen Schutzmechanismen gegen Malware wurden von Microsoft und Google verschiedene Technologien entwickelt.

— Microsoft: die SmartScreen-Filter-Technologie inklusive Application Reputation

— Google: die Safe-Browsing-Technologie

Diese Technologien werden von den heutigen Browsern verwendet und werden im Folgenden kurz vorgestellt.

3.5.1 SmartScreen-Filter

Die SmartScreen-Filter-Technologie existiert in verschiedenen Entwicklungsstufen. In der ersten Entwicklungsstufe umfasst diese Technologie ausschließlich ein adressbasiertes Reputationssystem, mit dem URLs bzgl. Phishing- und Malware-Angriffe überprüft und ggf. blockiert werden können. Entsprechende Webseiten können damit sowohl ganz als auch teilweise blockiert werden. Bei teilweiser Blockierung werden diejenigen Teilinhalte einer Webseite nicht geladen (da blockiert), deren URLs in Blacklists stehen. Das adressbasierte Reputationssystem arbeitet mit lokalen und zentralen Blacklists und darüber hinaus mit lokalen Whitelists zur Reduzierung des Kommunikationsaufwands; würde es beispielsweise die lokale Whitelist nicht geben, dann müsste jede URL, die sich nicht in der lokalen Blacklist befindet, mittels der zentralen Blacklist überprüft werden. Wird eine aufgerufene URL in einer der Blacklists gefunden, so blockiert das adressbasierte Reputationssystem den Verbindungsaufbau und gibt Warnungen an den Benutzer aus. Die Aktualisierung der Blacklists erfolgt in relativ kurzen Zeitintervallen (< 60 Minuten) und beim Start des Browsers.

Die SmartScreen-Filter-Technologie beinhaltet in der zweiten Entwicklungsstufe ein inhaltsbasiertes Reputationssystem, welches mit *Application Reputation* bezeichnet wird und das ausschließlich die Überprüfung von Downloads auf Malware übernimmt. Application Reputation arbeitet mit lokalen und zentralen Black- und Whitelists und gibt ebenfalls je nach Ergebnis der Überprüfung eines Downloads entsprechende Meldungen oder Warnungen aus bzw. blockiert den Zugriff auf die heruntergeladene Datei.

Weitere Informationen zu dieser Technologie sind beispielsweise in [Mic11b; Mic11a; Mic11c; hei11; Don09] zu finden.

3.5.2 Safe Browsing

Die Safe-Browsing-Technologie wurde von Google entwickelt und ist anderen Browser-Entwicklern frei zugänglich [Goo11a; Goo11b; Sob11]. Die Safe-Browsing-Technologie liegt in Version 2 vor; von der Verwendung der Version 1 wird abgeraten [Goo11c].

Die Safe-Browsing-Technologie umfasst ausschließlich ein adressbasiertes Reputationssystem zum Blockieren von URLs. Wird eine URL aufgerufen, so wird zunächst überprüft, ob sich diese in einer lokalen Blacklist befindet, woraufhin sie ggf. blockiert und eine Warnmeldung angezeigt wird. Ist die URL nicht enthalten, dann wird sie mittels einer lokalen Whitelist überprüft und ggf. als unbedenklich eingestuft. Ist die URL weder in der lokalen Blacklist noch in der Whitelist enthalten, so wird die zentrale Blacklist zurate gezogen. Die lokale Blacklist wird ungefähr alle 30 Minuten aktualisiert.

4. RAHMEN DER UNTERSUCHUNG

4.1 Gegenstand

Gegenstand dieser Studie ist die Untersuchung der Leistungsfähigkeit von in Browser integrierten adress- und inhaltsbasierten Reputationssystemen zum Schutz vor Malware-Angriffen. Bei der Untersuchung wurde betrachtet, wie wirksam sich die reputationsbasierten Systeme in der Realität verhalten und welchen Schutz sie bieten, wenn sie realen Malware-Angriffen, initiiert durch Aufrufe von Malware-URLs, ausgesetzt sind. Zur Ermittlung der Leistungsfähigkeit wurden die untersuchten Browser unter gleichen Bedingungen über den gesamten Messzeitraum mit denselben Angriffen konfrontiert, wobei die Browser-Reaktionen beobachtet und ausgewertet wurden. Hierzu wurden über den Untersuchungszeitraum täglich neue Malware-URLs gesammelt und für die Untersuchung herangezogen. Durch die Einhaltung identischer Bedingungen wurde die Vergleichbarkeit der verschiedenen Browser ermöglicht.

Für die Untersuchung wurden die 32-Bit-Versionen der folgenden Browser für Windows 7 ausgewählt:

- Chrome 14
- Firefox 6
- Internet Explorer 8
- Internet Explorer 9
- Safari 5

Die Auswahl der Browser bzw. Browser-Familien für die Untersuchung orientiert sich an den von NSS Labs im September 2011 in [NSS11a] untersuchten Browsern. Dort wurden sechs verschiedene Browser untersucht. Für unsere Untersuchung haben wir die zu Beginn des Versuchsaufbaus aktuellen Versionen der fünf wichtigsten Browser aus [NSS11a] untersucht. Während der Durchführung der Tests und Messungen wurden für bestimmte Browser bereits neuere Versionen veröffentlicht. Um alle Messungen erfolgreich durchführen zu können, musste jedoch an den Versionen festgehalten werden, auf deren Grundlage das Test- und Messsystem aufgebaut worden war. Inwieweit die in und nach dem Testzeitraum stattgefundenen Versionswechsel der Browser die hier gewonnenen Ergebnisse verändern würden, kann deshalb in dieser Studie nicht behandelt werden. Den Autoren ist beispielsweise bekannt, dass die im Februar 2012 veröffentlichte Version Chrome 17 im Gegensatz zu Chrome 14 zusätzlich über ein inhaltsbasiertes Reputationssystem zum Schutz gegen Malware verfügt. Zum Release-Zeitpunkt von Chrome 17 waren die Tests jedoch bereits abgeschlossen.

Bei der Untersuchung wurden ausschließlich die für die Sicherheit der Benutzer vor Malware-Angriffen relevanten Aspekte betrachtet. Hier war von Interesse, wie gut Angriffsversuche durch die von den Browsern verwendeten Reputationssysteme blockiert werden. Dabei standen sowohl Umfang als auch Aktualität bzw. Verzögerungen bei der Aktualisierung der Blacklists im Fokus der Betrachtung. Andere Eigenschaften wie etwa die Verfügbarkeit von zentralen Komponenten und Antwortzeiten wurden bei der Untersuchung nicht betrachtet.

Die Untersuchung wurde ausschließlich als Black-Box-Analyse durchgeführt, d.h. es wurden nur die Ein- und Ausgaben der Browser betrachtet. Interne Browser-Vorgänge wurden nicht berücksichtigt. Die adress- und inhaltsbasierten Reputationssysteme wurden sowohl

einzeln als auch in ihrer Kombination als gestaffelte Verteidigungslinien gegen Malware-Angriffe untersucht, sofern bei den jeweiligen Browsern eine kombinierte Betrachtung möglich war. Auch wenn eine Kombination von Reputationssystemen nicht bei allen Browsern gegeben war, wurde ein Vergleich des erreichbaren Schutzumfangs vorgenommen.

Bei der Durchführung der Auswertung wurden nicht erreichbare URLs nicht berücksichtigt. URLs können beispielsweise dann nicht erreichbar sein, wenn der entsprechende Zielserver gerade überlastet ist oder ein technischer Fehler vorliegt. Generell kann nicht ausgeschlossen werden, dass nicht erreichbare URLs bei einem späteren Aufruf wieder erreichbar sind und Schaden verursachen können, wenn sie nicht blockiert werden. Da bei nicht erreichbaren URLs nicht entschieden werden kann, ob es sich um Malware-URLs handelt, wurden sie hier nicht berücksichtigt. Grundsätzlich wurden in dieser Studie ausschließlich Malware-URLs in die Auswertung einbezogen.

Die verwendeten Browser wurden ausschließlich in ihrer Standardkonfiguration untersucht. Es wurden weder benutzerseitig Änderungen der Einstellungen vorgenommen noch wurden Plugins oder sonstige Erweiterungskomponenten installiert. Bei der Untersuchung sollte der durch die Reputationssysteme erreichte Schutz gegen Malware-Angriffe für Benutzer ohne besondere technische Fachkenntnisse hinsichtlich Browser-Einstellungen und Browser-Erweiterungen im Fokus stehen. Wir nehmen an, dass genau dies für die große Mehrheit der Benutzer zutrifft. Darüber hinaus sollte Sicherheit nicht das Privileg der Benutzer mit umfassendem technischen Hintergrundwissen sein.

4.2 Untersuchte Browser

Die untersuchten Browser bieten verschiedene reputationsbasierte Mechanismen zum Schutz vor Malware-Angriffen, zu deren Umsetzung sie unterschiedliche Technologien verwenden. Tabelle II gibt hierfür einen Überblick.

	Chrome 14	**Firefox 6**	**Internet Explorer 8**	**Internet Explorer 9**	**Safari 5**
Technologie	Safe Browsing	Safe Browsing	SmartScreen-Filter ohne Application Reputation	SmartScreen-Filter mit Application Reputation	Safe Browsing
adressbasierte Reputation	ja	ja	ja	ja	ja
inhaltsbasierte Reputation	nein	nein	nein	ja	nein

Tabelle II. Technologie und Schutzmechanismen der Browser

4.3 Aussage und Deutbarkeit der Ergebnisse

Die Ergebnisse dieser Studie basieren auf den Tests und Messungen, die Fraunhofer SIT in der Zeit zwischen Beginn der Kalenderwoche 44/2011 und Ende der Kalenderwoche 49/2011 durchgeführt hat. Hierbei wurden in den ersten vier Wochen dieser Zeitspanne

Malware-URLs und Malware-Dateien gesammelt. Das Verhalten der Reputationssysteme bezüglich Malware-Schutz wurde über den kompletten Zeitraum zwischen Kalenderwoche 44 und Kalenderwoche 49 gemessen.

Die zum Test verwendeten Malware-URLs und -Dateien wurden von Fraunhofer SIT über verschiedene Quellen im Internet bezogen. Es handelte sich hierbei um ein für diesen Zweck installiertes System zur Sammlung von Spam-Emails sowie weitere öffentlich zugängliche Quellen für Malware-URLs. Insofern war es auch den Reputationssystemen möglich, diese öffentlich zugänglichen Quellen in Erfahrung zu bringen und die dort verfügbaren Malware-URLs in ihre Blacklists aufzunehmen.

Das Testsystem von Fraunhofer SIT hat sich beim Aufrufen der gesammelten Malware-URLs genau so verhalten, wie dies ein fiktiver Benutzer getan hätte, z.B. indem er auf einen Link klickt, den er in einer Email erhalten hat. Unter Betrachtung des Testsystems als fiktiver Benutzer besteht der wesentliche Unterschied lediglich darin, dass Fraunhofer SIT sich des Angriffsversuchs bewusst war. Insofern können die Beobachtungen, Ergebnisse und Aussagen dieser Studie so gedeutet werden, als würden sie sich auf einen fiktiven Benutzer je Browser beziehen, der sich über den Beobachtungszeitraum so verhalten hat wie das eingesetzte Testsystem.

Die Aussagen der Studie gelten nur für den Zeitraum der Messung und können nicht darüber hinaus extrapoliert werden. Dies ist offensichtlich, da eine Messung beispielsweise nicht vorwegnehmen kann, ob eine zentrale Komponente eines Reputationssystems aufgrund technischer Defekte vorübergehend ausfällt. Die im Messzeitraum erhaltenen Ergebnisse geben keine Aussage darüber, wie sich die Reputationssysteme bzgl. Malware-Angriffen zu anderen Zeitpunkten verhalten. Beispielsweise können die Ergebnisse dieser Arbeit keine Aussage darüber geben, wie gut die zentralen Blacklists zu einem späteren Zeitpunkt gepflegt werden.

Darüber hinaus gelten die Aussagen dieser Studie nur für die von Fraunhofer SIT gesammelten Malware-URLs und -Dateien. Grundsätzlich gibt es im Internet sehr viel mehr Angriffsquellen. Die betrachtete Anzahl an Malware-URLs und -Dateien wurden an die im Rahmen der Studie verfügbaren zeitlichen und personellen Ressourcen angepasst.

Die Studie behandelt als Schutzmechanismen gegen Malware-Angriffe ausschließlich adress- und inhaltsbasierte Reputationssysteme der Browser, wie sie durch Standardkonfiguration zur Verfügung stehen. Das bedeutet, dass die Aussagen der Studie nicht für adress- und inhaltsbasierte Reputationssysteme gelten, die über Veränderung der Einstellungen oder über Installation von zusätzlichen Browser-Komponenten erzielt wurden. Insbesondere werden keine Aussagen über andere Sicherheitsfunktionen der Browser getroffen.

Die Tests, Messungen, Analysen und Auswertungen wurden unabhängig, unparteiisch und fair durchgeführt. Das Fraunhofer SIT war in der Auswahl der Methodik zur Duchführung frei. Es gab weder Vorgaben von Seiten eines Browser-Herstellers zur Auswahl der Methodik noch konnte sich ein Browser-Hersteller eine von Fraunhofer SIT vorgeschlagene Methodik unter anderen auswählen. Zur Durchführung dieser Arbeiten hat Fraunhofer SIT die Kriterien zur Analyse und Auswertung selbst entwickelt. Keiner der betroffenen Browser-Hersteller wurde vor oder während der Durchführung dieser Arbeiten über die verwendeten Kriterien in Kenntnis gesetzt.

5. TESTAUFBAU UND MESSUNG

5.1 Architektur der Testumgebung

Es wurden Vorbereitungen getroffen, um das Verhalten aller Browser beim Aufrufen aktueller Malware-URLs unter gleichen Bedingungen zu messen und auszuwerten sowie laufend neu gesammelte URLs einzubeziehen. Dies wurde soweit möglich automatisiert durchgeführt; eine vollständig automatisierte Vorgehensweise war jedoch nicht möglich. Sämtliche URL-Aufrufe aller Browser wurden unter identischen Bedingungen getestet, um Fairness zu gewährleisten.

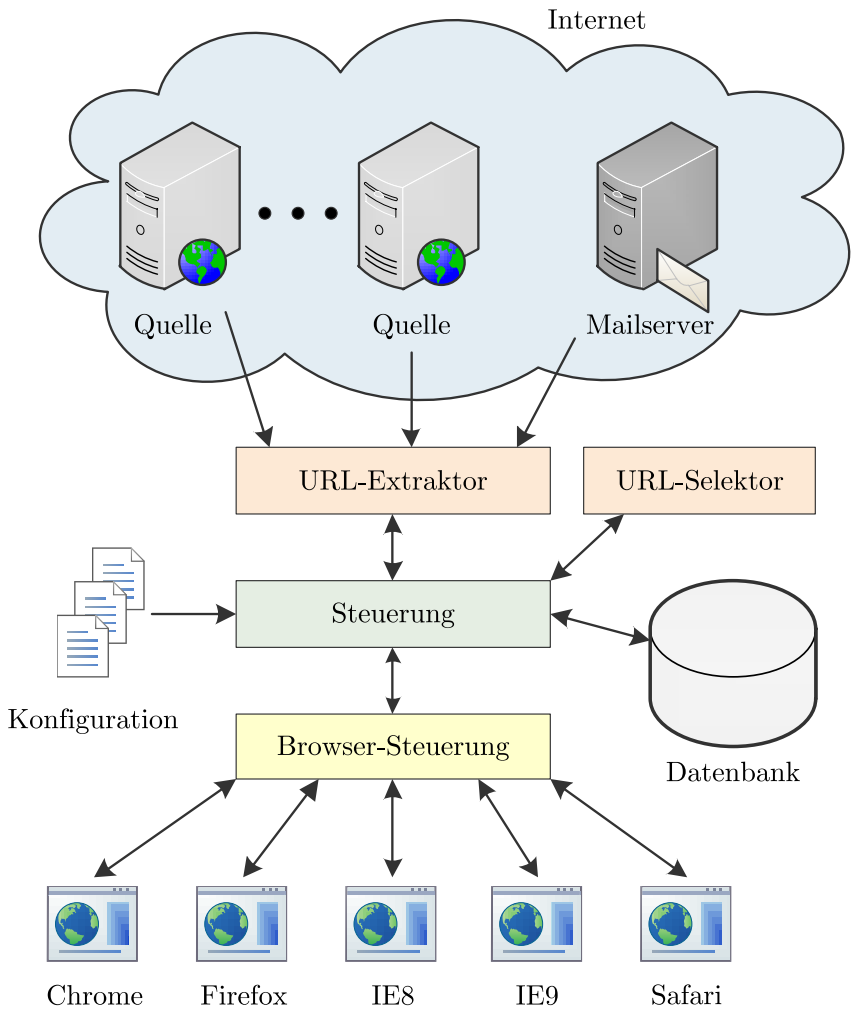

Abbildung 5. Architekturmodell

Abbildung 5 zeigt die Architektur der Test- und Messumgebung als Modell. Das Architekturmodell bezieht sich auf die Überprüfung der in dieser Studie einbezogenen Sicherheitsmechanismen der Browser. Die einzelnen Systemkomponenten der Abbildung werden im Folgenden kurz erläutert.

— Quellen: URLs wurden aus verschiedenen Quellen gewonnen. Eine Quelle war ein Mailserver ohne Spamfilter. Die Email-Adressen wurden im Internet veröffentlicht, um möglichst viel Spam zu erhalten. Zusätzliche Quellen waren verschiedene öffentlich zugängliche Webseiten, von denen dem Fraunhofer SIT bekannt ist, dass sie Malware-URLs enthalten.
— URL-Extraktor: Aus empfangenen Spam-Mails und anderen öffentlichen Quellen wurden URLs automatisch extrahiert und für die weitere Bearbeitung (z.B. Annotationen mit Meta-Daten) vorbereitet.
— URL-Selektor: Aus der Vielzahl der Angriffs-URLs wurden diejenigen ausgewählt, welche für den Test herangezogen wurden, beispielsweise solche, bei denen der Angriffstyp klar zugeordnet werden konnte. Eine URL-Auswahl war auch dann erforderlich, wenn die Anzahl der neu gesammelten URLs die Kapazität des Testsystems überstieg.
— Steuerung: Über diese Komponente wurde die Steuerung der anderen Komponenten für Tests und Messung realisiert.
— Datenbank: Die verwendeten Malware-URLs wurden gemeinsam mit zusätzlichen Metadaten wie Empfangsdatum und Testprotokollen in der Datenbank gespeichert.
— Browser-Steuerung: Diese Komponente wurde zur Steuerung und Synchronisierung von Browser-Aktionen wie beispielsweise dem zeitgleichen Aufrufen von URLs während der Testzyklen sowie zur Weiterleitung von Zwischen- und Endergebnissen an die Datenbank verwendet.

5.2 Phasen der der Testdurchführung

Die durchgeführte Messung der in die Betrachtung einbezogenen Sicherheitsmechanismen der Browser besteht aus zwei aufeinander aufbauenden Phasen.

— Sammelphase: Die zu testenden Malware-URLs wurden über einen Zeitraum von vier Wochen gesammelt, beispielsweise über speziellen Webseiten mit Malware-Sammlungen und Mailserver ohne Spamfilter, und für die Tests ausgewählt (siehe Abbildung 5). Die Sammlung, Auswahl und Kategorisierung der Malware-URLs lief soweit möglich automatisiert ab; eine zusätzliche manuelle Überprüfung war hierbei oftmals notwendig. Die Sammlung von Malware-URLs diente sowohl für den Test von adressbasierten Reputationssystemen als auch für inhaltsbasierte Reputationssysteme als Grundlage, da beispielsweise eine Malware-Datei, deren URL von einem adressbasierten Reputationssystem nicht als gefährlich erkannt wurde, trotzdem noch nach dem Download durch ein inhaltsbasiertes Reputationssystem geblockt werden kann. Für die Analyse des nur im Internet Explorer 9 enhaltenen inhaltsbasierten Reputationssystem wurde vor Testdurchführung seine separate Sammlung aus 369 verschiedenen Malware-Dateien erstellt.
— Testphase: Während der Testphase wurde zyklisch gemessen, ob und wie schnell eine Malware-URL oder -Datei von den verschiedenen Browsern als gefährlich erkannt wird. Ein Messzyklus beinhaltete das Aufrufen von 70–100 URLs je Browser. Gleiche URLs wurden dabei nahezu zeitgleich in allen Browsern getestet. Sämtliche Messungen erfolgten aus Sicht eines Benutzers. Nach jedem einzelnen URL-Aufruf wurde jeder Browser in den Zustand von vor Beginn des aktuellen Messzyklus zurückgesetzt, um vergleichbare Ausgangssituationen zu erhalten und Messfehler auszuschließen, welche möglicherweise der zuletzt aufgerufenen URL geschuldet waren. Pro Messzyklus kamen stets neu ausgewählte URLs hinzu. Wurde eine URL durch einen Browser als gefährlich eingestuft

und der Benutzer gewarnt, so wurde diese URL für diesen Browser in den folgenden Messzyklen nicht mehr berücksichtigt. Andernfalls wurde die URL im nächsten Messzyklus erneut überprüft, maximal jedoch in 28 aufeinanderfolgenden Zyklen (das entspricht einem Zeitraum von sieben Tagen). Danach wurde diese URL für diesen Browser als nicht erkannt vermerkt. Damit die am Ende der vierwöchigen Sammelphase erhaltenen URLs im gleichen Umfang wie die ersten URLs der gesamten Testphase getestet werden konnten, erstreckte sich die Testphase auf insgesamt fünf Wochen. Bei den getesteten URLs wurden sowohl die Reaktion der adressbasierten Reputationssysteme als auch die der inhaltsbasierten Reputationssysteme berücksichtigt, sofern der betrachtete Browser über ein inhaltsbasiertes Reputationssystem verfügte. Zusätzlich wurden mit einer davon unabhängige Sammlung von 369 Malware-Dateien über den Betrachtungszeitraum Tests der inhaltsbasierten Reputationssysteme durchgeführt. Hierbei wurde täglich überprüft, welche Malware-Dateien in welchem Zeitrahmen blockiert wurden. Von den in der Studie untersuchten Browsern verfügte nur der Internet Explorer 9 über ein inhaltsbasiertes Reputationssystem.

6. ANALYSE UND AUSWERTUNG

6.1 Überblick

In diesem Kapitel werden 7 Kriterien beschrieben, anhand derer die Reputationssysteme der Browser bewertet werden. Die Auswertung jedes einzelnen Kriteriums ist als Teilergebnis zu verstehen. Die Kriterien sind transparent und nachvollziehbar, wurden von Fraunhofer SIT selbst und unabhängig erstellt und lassen einen objektiven und transparenten Vergleich zu. Sie orientieren sich an den aus Anwendersicht erwünschten Eigenschaften der von den Browsern verwendeten Reputationssysteme, wie Umfang der Black- und Whitelists oder Aktualität und Verzögerungen bei der Pflege dieser. Darüber hinaus lässt die differenzierte Betrachtung Analysen spezieller Eigenschaften hinsichtlich des Schutzumfangs der Browser zu. Die verwendeten Reputationssysteme (adressbasierte und inhaltsbasierte) zur Abwehr von Malware-Angriffen wurden bei der Analyse und Auswertung sowohl einzelnen als auch kombiniert betrachtet. Alle betrachteten Kriterien verwenden Metriken, die der Quantifizierung von Browser-Eigenschaften dienen und somit ihre Vergleichbarkeit fördern. Die Werte dieser Metriken resultieren aus den im Betrachtungszeitraum erhaltenen Messergebnissen.

Nicht alle betrachteten Schutzmechanismen werden von jedem der hier untersuchten Browser unterstützt. Da jeder einzelne Mechanismus jedoch von Relevanz für die Bewertung des Malware-Schutzes sind, werden auch diejenigen Browser in die entsprechenden Einzeltests einbezogen, die einzelne Mechanismen nicht unterstützen.

Insgesamt waren über den Betrachtungszeitraum von insgesamt 568 gesammelten URLs 447 erreichbar, von denen es sich bei 261 um erreichbare Malware-URLs handelte. In der vorliegenden Studie wurden ausschließlich die erreichbaren Malware-URLs zur Untersuchung in den Abschnitten 6.2, 6.3, 6.4 und 6.6 herangezogen. Von diesen URLs waren unterschiedlich viele in den Blacklists der Browser enthalten. In den nachfolgenden Einzeltests wurde überprüft, ob bzw. wie schnell URLs im Betrachtungszeitraum in Blacklists aufgenommen wurden. Untersuchungen der inhaltsbasierten Reputation wurden in den Abschnitten 6.5,

6.6, 6.7 und 6.8 vorgenommen. In Abschnitt 6.8 wurden 369 verschiedene Malware-Dateien aus unterschiedlichen Quellen für die Bewertung der inhaltsbasierten Reputation betrachtet.

6.2 Anteil erkannter Malware-URLs

Die Rahmenbedingungen für dieses Teilergebnis wurden hier so gewählt, dass ausschließlich erreichbare Malware-URLs betrachtet wurden. URLs, die andere Angriffe ermöglichten, wurden hier nicht betrachtet. Für die über den Betrachtungszeitraum erreichbaren URLs wurde für alle Browser überprüft, ob diese in der Blacklist des jeweiligen Browsers enthalten waren und somit blockiert wurden. Wurde eine URL in die Sammlung der zu betrachtenden URLs aufgenommen, dann wurde über einen Zeitraum von sieben Tagen alle sechs Stunden überprüft, ob die URL in einer aktualisierten Blacklist enthalten war. Die Überprüfung derselben URL wurde in den verschiedenen Browsern nahezu zeitgleich vorgenommen. Wurde die URL bis zum Ende des siebten Tages nicht in die Blacklist eines Browsers aufgenommen, so wurde sie von diesem nicht weiter überprüft und als unbedenklich bzw. nicht erkannt bewertet. Die Geschwindigkeit, mit welcher die URLs in die Blacklists aufgenommen wurden, wurde in dieser Metrik nicht berücksichtigt.

Die Auswertung der Tests und Messungen ergab hier, dass Malware-URLs durch die SmartScreen-Technologie sehr viel besser gefiltert wurden als durch die Safe-Browsing-Technologie. Zwar wurden von den Browsern mit SmartScreen-Technologie nur etwa ein Drittel der Malware-URLs insgesamt als solche erkannt, jedoch waren dies immer noch drei- bis viermal so viel, wie bei den Browsern mit Safe-Browsing-Technologie. Bemerkenswert ist hier, dass Safari 5 und Firefox 6 weniger als 10% der Malware-URLs erkannt haben.

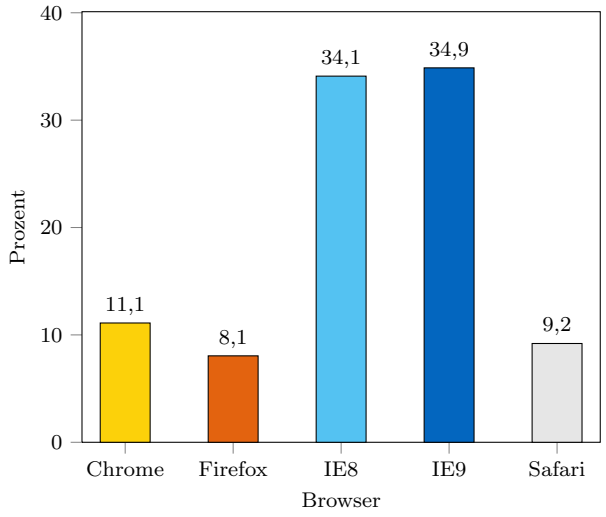

Abbildung 6. Anteil der erkannten Malware-URLs je Browser

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9
(2) Internet Explorer 8
(3) Chrome 14
(4) Safari 5

(5) Firefox 6

6.3 Mittlere Verzögerung bei der Erkennung von Malware-URLs

Für die über den Betrachtungszeitraum gesammelten erreichbaren Malware-URLs wurde für alle Browser überprüft, mit welcher mittleren Verzögerung diese in die Blacklist des jeweiligen Browsers aufgenommen wurden. Referenzpunkt für den Start der Messung war der Zeitpunkt, zu welchem eine URL in die Sammlung der zu betrachtenden URLs eingetragen wurde. In welchem Zeitraum davor eine URL bereits für Malware-Angriffe genutzt wurde, war unbekannt und ist daher nicht in die Berechnung der mittleren Verzögerung eingeflossen. Wurde eine URL in die Sammlung aufgenommen, dann wurde über einem Zeitraum von sieben Tagen alle sechs Stunden überprüft, ob die URL in einer aktualisierten Blacklist eines jeden Browsers enthalten war. Die Überprüfung derselben URL wurde in den verschiedenen Browsern nahezu zeitgleich vorgenommen. Wurde die URL bis zum Ende des siebten Tages nicht in die Blacklist eines Browsers aufgenommen, dann wurde sie nicht weiter überprüft.

Es ist darauf hinzuweisen, dass die mittleren Verzögerungswerte immer gemeinsam mit den jeweiligen Anzahlen derjenigen Malware-URLs betrachtet werden müssen, die von den Browsern als nicht gefährlich eingestuft wurden. Grundsätzlich können Malware-URLs, die als nicht gefährlich eingestuft wurden, zunächst nicht bei der Mittelwertberechnung von Verzögerungen berücksichtigt werden, da für sie kein Verzögerungswert vorliegt. Würden also zum Vergleich der Browser die mittleren Verzögerungswerte ohne Betrachtung der Malware-URLs berechnet werden, die als nicht gefährlich eingestuft wurden, dann würden diejenigen Browser besser bewertet werden, die nur sehr wenige Malware-URLs sehr schnell als gefährlich eingestuft haben, verglichen mit denjenigen, die insgesamt sehr viele Malware-URLs als gefährlich einstuften, dafür jedoch längere Zeit brauchten. Um diesem Umstand Rechnung zu tragen, wurden alle Malware-URLs, die im Überprüfungszeitraum von sieben Tagen als nicht gefährlich eingestuft wurden, für die Mittelwertberechnung so behandelt, als wären sie nach weiteren sieben Tagen (also nach insgesamt 14 Tagen) von den jeweiligen Browsern als gefährlich eingestuft worden.

Die mittlere Verzögerung bei der Erkennung von Malware-URLs ist bei allen Browsern relativ groß. Viele Malware-URLs wurden entweder eher spät oder gar nicht erkannt. Größenordnungsmäßig liegen die Werte bei Browsern, welche die Safe-Browsing-Technologie verwenden, ungefähr um ein Drittel niedriger als bei Browsern, welche die SmartScreen-Filter-Technologie einsetzen.

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9

(2) Internet Explorer 8

(3) Chrome 14

(4) Safari 5

(5) Firefox 6

6.4 Anteil sofort erkannter Malware-URLs

Für die über den Betrachtungszeitraum gesammelten Malware-URLs wurde für alle Browser überprüft, ob die URLs bereits beim ersten Testzyklus in der Blacklist des jeweiligen

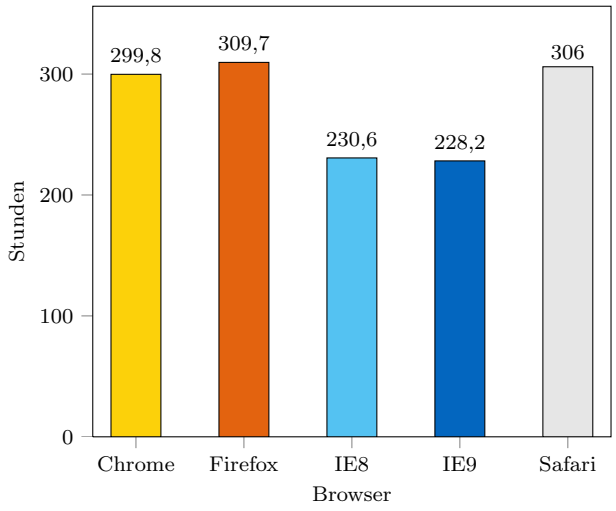

Abbildung 7. Mittlere Verzögerung bei der Erkennung von Malware-URLs je Browser

Browsers enthalten waren und somit direkt blockiert werden konnten. Hierbei wurden nur erreichbare Malware-URLs berücksichtigt.

Insgesamt wurden über den Betrachtungszeitraum 261 erreichbare Malware-URLs überprüft. Von diesen waren beim ersten Testzyklus unterschiedlich viele bereits in den Blacklists der jeweiligen Browser enthalten.

In dieser Betrachtung reagieren die Browser mit SmartScreen-Filter-Technologie schneller als die Browser mit Safe-Browsing-Technologie. Die SmartScreen-Filter-Technologie blockierte im ersten Test ungefähr eine von sechs bis sieben Malware-URLs. Die Safe-Browsing-Technologie konnte im Vergleich dazu nur eine von ungefähr neun bis zwölf Malware-URLs blockieren.

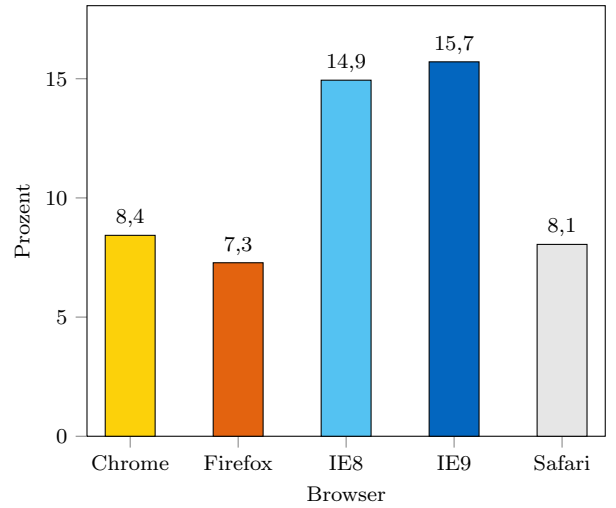

Abbildung 8. Anteil sofort erkannter Malware-URLs je Browser

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9

(2) Internet Explorer 8
(3) Chrome 14
(4) Safari 5
(5) Firefox 6

6.5 Erkannte heruntergeladene Malware in zweiter Verteidigungslinie

Systeme zur Bewertung der Reputation heruntergeladener Inhalte ermöglichen das Blockieren von Malware, wenn die URL durch URL-Reputation nicht erkannt und somit nicht geblockt wurde. In diesem Teilergebnis geht es um die ausschließliche Betrachtung von solchen inhaltsbasierten Reputationssystemen. Hierfür wurde untersucht, welcher Anteil von kritischen Inhalten nach Passieren des URL-Filters und anschließendem Download als Malware-Datei erkannt wurde. Der Anteil bezieht sich hierbei auf die Gesamtanzahl von erreichbaren Malware-URLs, also auch solche, die nicht direkt auf eine Malware-Datei zum Download verweisen.

Die Berücksichtigung der inhaltsbasierten Reputation wird bei den in dieser Arbeit betrachteten Browsern nur vom Internet Explorer 9 angeboten (Application Reputation).

	Chrome	**Firefox**	**IE8**	**IE9**	**Safari**
Erkannte heruntergeladene Malware in 2. Linie[2] (6.5)	-	-	-	+	-

Tabelle III. Zusätzlicher Schutz durch Reputation zur Erkennung von heruntergeladener Malware in zweiter Verteidigungslinie

Der Internet Explorer 9 verwendet neben der adressbasierten Blacklist noch eine inhaltsbasierte Blacklist, in der Malware aufgeführt ist, und eine inhaltsbasierte Whitelist, in der unbedenkliche Inhalte aufgeführt sind. Wird eine Datei heruntergeladen, deren Inhalt in der Liste der unbedenklichen Inhalte enthalten ist, dann meldet der Browser, dass diese Datei kein Risiko für den Benutzer darstellt. Wird der Dateiinhalt in keiner der Listen geführt, dann weist der Internet Explorer 9 den Benutzer darauf hin, dass der Inhalt unbekannt ist und keine Aussage hinsichtlich des damit verbundenen Risikos getroffen werden kann. Da innerhalb dieser Auswertung definitiv Malware heruntergeladen wurde, wurde ausschließlich bewertet, ob der Browser den geladenen Inhalt als Malware erkannte. Eine Nichterkennung wurde dementsprechend negativ bewertet. Eine darüber hinaus gehende Einordnung einer Malware als unbedenklicher Inhalt durch den Browser wäre fatal für den Benutzer.

Bei der Bewertung der zweiten Verteidigungslinie durch Application Reputation wurden die folgenden Aspekte analysiert:

— Welcher Malware-Anteil kann durch Application Reputation erkannt werden, wenn die erste Verteidigungslinie (URL-Reputation) nicht vorhanden ist?
— Welcher Malware-Anteil kann durch Application Reputation erkannt werden, nachdem die erste Verteidigungslinie (URL-Reputation) nicht erfolgreich war?
— Welcher Malware-Anteil kann durch Application Reputation und URL-Reputation simultan erkannt werden?

Der Internet Explorer 9 lieferte bei der Messung folgende Ergebnisse: Insgesamt konnten 7,3% der Malware durch Application Reputation erkannt werden. 3,1% der Malware wurden

sowohl durch URL-Reputation als auch durch Application Reputation geblockt. Effektiv wurden durch Application Reputation 4,2% zusätzliche Malware als solche erkannt.

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9

(2) Chrome 14, Firefox 6, Internet Explorer 8, Safari 5

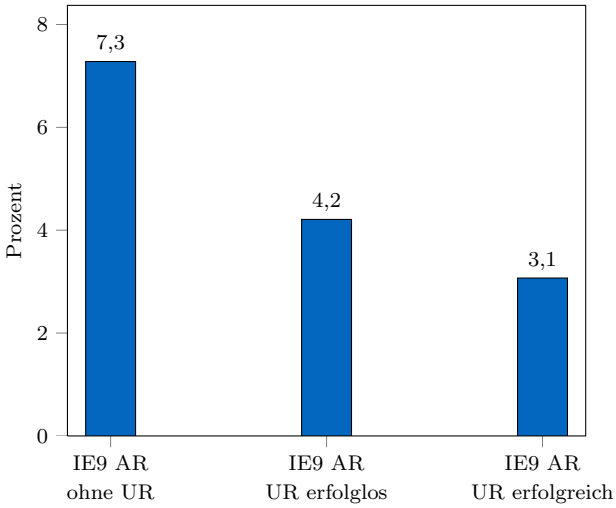

Abbildung 9. Anteil von erkannter Malware im Internet Explorer 9 durch Application Reputation bei nicht aktiver URL-Reputation (links), ohne Erkennung durch URL-Reputation (Mitte), simultane Erkennung durch Application Reputation und URL-Reputation (rechts)

6.6 Durch Kombination erkannte Malware-Angriffe

In diesem Teilergebnis wird die Wirkung der adressbasierten Reputation und der inhaltsbasierten Reputation zusammen analysiert und bewertet. Es werden dabei ausschließlich erreichbare Malware-URLs betrachtet. Hierzu werden die Ergebnisse aus den Abschnitten 6.2 und 6.5 kombiniert.

Die Browser mit SmartScreen-Technologie erkannten über den Betrachtungszeitraum mehr Malware-URLs und -Dateiinhalte als die Browser mit Safe-Browsing-Technologie. Die Kombination der Überprüfung von URL und Inhalt verbesserte das Ergebnis für den Internet Explorer 9 erneut. Dabei kam das Potenzial der Erkennung durch Application Reputation nicht ganz zum Tragen, da einige Dateiinhalte, die durch Application Reputation erkannt worden wären, bereits vorher durch die Reputation der auf die Datei verweisenden URL blockiert wurden.

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9

(2) Internet Explorer 8

(3) Chrome 14

(4) Safari 5

(5) Firefox 6

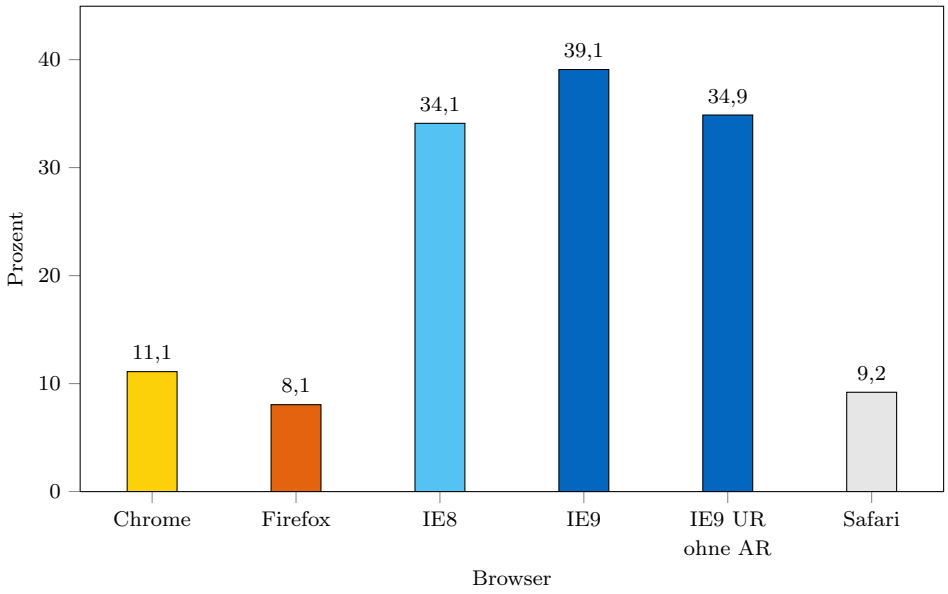

Abbildung 10. Anteil der durch kombinierte Schutzmechanismen erkannten Malware-Angriffe je Browser (zzgl. Vergleich für Internet Exlorer 9: Anteil der durch Kombination von URL-Reputation und Application Reputation erkannten Malware-Angriffe (links), Anteil der erkannten Malware-Angriffe durch URL-Reputation ohne anschließende Inhaltserkennung durch Application Reputation (rechts))

6.7 Anteil erkannter Malware aus unabhängiger Datensammlung

In Abschnitt 6.6 wurden Dateien überprüft, die über URLs geladen wurden, die im Rahmen der täglich erneuerten URL-Sammlung gefunden wurden. Dabei wurde eine Erkennung mittels adressbasierter Reputationssysteme sowie eine Erkennung der ggf. heruntergeladene Malware mittels inhaltsbasierter Reputationssysteme untersucht. Für eine weitere Aussage zur Leistungsfähigkeit der inhaltsbasierten Reputationssysteme wurde außerdem eine separate größere Menge von Malware untersucht. In diesem Teilergebnis geht es darum, Analysen und Aussagen über diese separate Sammlung von Malware durchzuführen.

Hierzu wurden zu Beginn der Versuchsreihe insgesamt 369 verschiedene Malware-Dateien aus dem Internet heruntergeladen. Anschließend wurde vier Wochen lang täglich überprüft, ob die jeweilige Malware in den Blacklists des inhaltsbasierten Reputationssystems des Internet Explorer 9 enthalten war. Es sei darauf hingewiesen, dass bei diesem Teilergebnis ausschließlich der Internet Explorer 9 getestet wurde, da dieser der einzige der betrachteten Browser war, der über ein inhaltsbasiertes Reputationssystem verfügte.

	Chrome	**Firefox**	**IE8**	**IE9**	**Safari**
Anteil erkannter Malware aus Datensammlung[2] (6.7)	-	-	-	+	-

Tabelle IV. Zusätzlicher Schutz durch inhaltsbasierte Reputation; Anteil erkannter Malware aus unabhängiger Datensammlung

Da es sich bei der gesammelten Malware um Dateien handelte, die von verschiedenen Quellen aus dem Internet heruntergeladen und nicht selbst entwickelt wurden, gab es für die inhaltsbasierten Reputationssysteme eine realistische Chance, die Malware in die Blacklist aufzunehmen. Die Malware-Sammlung wurde für die Messreihe auf einem Server in

einem internen Test-LAN abgelegt und bei den täglichen Tests über ständig wechselnde URLs von dort geladen. Somit konnte eine Filterung durch adressbasierte Reputation umgangen werden und über den gesamten Messzeitraum hinweg ausschließlich der Einfluss der inhaltsbasierten Reputationssysteme analysiert und bewertet werden.

Wurde eine Malware innerhalb des Messzeitraums in die Blacklist aufgenommen, dann wurde diese als erkannt bewertet. Hierbei wurde das reine Vorkommen in der Blacklist innerhalb des Messzeitraums bewertet. Es wurde nicht betrachtet, zu welchem Zeitpunkt die Malware in die Blacklist aufgenommen wurde.

Der Internet Explorerer 9 hat von den 369 verschiedenen Malware-Dateien insgesamt 55 als solche erkannt. Das entspricht einem Anteil von 14,9%.

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

(1) Internet Explorer 9

(2) Chrome 14, Firefox 6, Internet Explorer 8, Safari 5

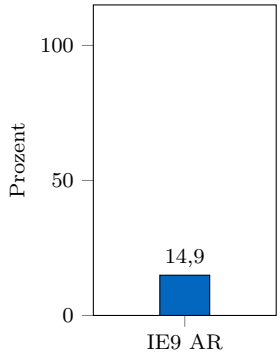

Abbildung 11. Anteil erkannter Malware durch den Internet Explorer 9

6.8 Mittlere Verzögerung bei Erkennung von Malware aus unabhängiger Datensammlung

Bei diesem Teilergebnis geht es darum, eine Aussage über das Verzögerungsverhalten des inhaltsbasierten Reputationssystems im Internet Explorer 9 zu treffen. Hierzu wurden die Rahmenbedingungen aus Abschnitt 6.7 angenommen. Für den Anteil der vom Internet Explorer 9 erkannten Malware wurde die mittlere Verzögerung gemessen, mit der die Malware in die Blacklist aufgenommen wurde. Als Referenzzeitpunkt für die Verzögerung wurde der erste Tag der Messung festgelegt.

Da lediglich der Internet Explorer 9 über ein inhaltsbasiertes Reputationssystem verfügt, ergibt sich folgende Auswertung: Für den in Abschnitt 6.7 gegebenen Anteil der erkannten Malware wurde eine mittlere Verzögerung von 40,1 Stunden ermittelt. Das bedeutet, dass gefundene Malware im Mittel in etwas mehr als 1,5 Tagen in die Blacklist aufgenommen und somit geblockt wurde. Bei der Bewertung dieser Verzögerung ist zu berücksichtigen, dass insgesamt 314 der 369 getesteten Malware-Dateien, also der überwiegende Teil, nicht gefunden wurden — dieses Ergebnis ist sicher noch verbesserungsfähig. Andererseits ist die Erkennung jeder einzelnen Malware für sich positiv zu bewerten.

Die Auswertung ergibt folgende Reihenfolge unter den Browsern:

	Chrome	Firefox	IE8	IE9	Safari
Mittlere Verzögerung Erkennung aus Datensammlung[2] (6.8)	-	-	-	+	-

Tabelle V. Zusätzlicher Schutz durch inhaltsbasierte Reputation; Mittlere Verzögerung bei Erkennung von Malware aus unabhängiger Datensammlung

(1) Internet Explorer 9

(2) Chrome 14, Firefox 6, Internet Explorer 8, Safari 5

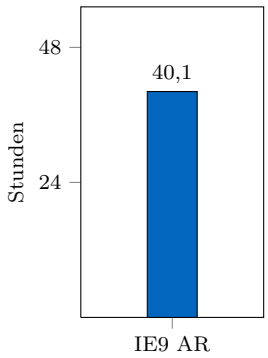

Abbildung 12. Mittlere Verzögerung bei der Erkennung von Malware durch den Internet Explorer 9

7. GESAMTAUSWERTUNG UND ERGEBNIS

In diesem Kapitel werden die einzelnen Ergebnisse aus den vorangegangenen Abschnitten aufbereitet und zusammengestellt. Darunter sind einzelne Ergebnisse, bei denen alle betrachteten Browser miteinander verglichen werden sowie Einzelergebnisse, in denen Aussagen über Eigenschaften der inhaltsbasierten Reputation getroffen werden (siehe Abschnitte 6.5, 6.7 und 6.8). Jeder Mechanismus zur Abwehr von Malware-Angriffen ist von Bedeutung, um eine Bewertung des Malware-Schutzes vorzunehmen. Daher werden auch die Browser in die Auswertung der Einzeltests einbezogen, die den Mechanismus nicht anbieten. Darüber hinaus werden die Ergebnisse dieser Untersuchung mit den Ergebnissen anderer aktueller Untersuchungen verglichen.

Insgesamt waren über den Betrachtungszeitraum von insgesamt 568 gesammelten URLs 447 erreichbar, von denen es sich bei 261 um Malware-URLs handelte. In der vorliegenden Studie wurden ausschließlich die erreichbaren Malware-URLs zur Untersuchung herangezogen. Von diesen URLs waren unterschiedlich viele in den Blacklists der Browser enthalten. In den Einzeltests in den Abschnitten 6.2, 6.3, 6.4 und 6.6 wurde überprüft, ob bzw. wie schnell URLs im Betrachtungszeitraum in Blacklists aufgenommen wurden. In den Abschnitten 6.5, 6.6, 6.7 und 6.8 wurden die inhaltsbasierten Mechanismen betrachtet.

Bei der durchgeführten Untersuchung von reputationsbasierten Schutzmechanismen in Browsern zur Abwehr von Malware-Angriffen stellte sich heraus, dass sich die fünf Browser

in ihrer Erkennungsleistung von Malware-URLs und Malware signifikant unterscheiden. Internet Explorer 8 und Internet Explorer 9 zeigten deutliche Vorteile bei der Erkennung von Malware-URLs gegenüber Chrome 14, Firefox 6 und Safari 5. Die Darstellung der Einzelplatzierungen ist in Tabelle VI gegeben.

	Chrome	**Firefox**	**IE8**	**IE9**	**Safari**
Anteil erkannter Malware-URLs (6.2)	3	5	2	1	4
Mittlere Verzögerung bei der Erkennung von Malware-URLs (6.3)	3	5	2	1	4
Anteil sofort erkannter Malware-URLs (6.4)	3	5	2	1	4
Erkannte heruntergeladene Malware in zweiter Verteidigungslinie (6.5)	2	2	2	1	2
Durch Kombination erkannte Malware-URLs (6.6)	3	5	2	1	4
Anteil erkannter Malware aus unabhängiger Datensammlung (6.7)	2	2	2	1	2
Mittlere Verzögerung bei Erkennung von Malware aus unabhängiger Datensammlung (6.8)	2	2	2	1	2
Durchschnittswerte	2,57	3,71	2	1	3,14

Tabelle VI. Gesamtübersicht

Bei der Betrachtung adressbasierter Reputation zeigen die Teilergebnisse stets die gleiche Rangfolge: Internet Explorer 9, Internet Explorer 8, Chrome 14, Safari 5 gefolgt von Firefox 6. Bei der inhaltsbasierten Reputation gibt es mit dem Internet Explorer 9 nur einen Gewinner, da dieser als einziger einen solchen Mechanismus unterstützt. Dementsprechend teilen sich alle anderen Browser den zweiten Platz.

Die Teilergebnisse der Abschnitte 6.5, 6.7 und 6.8 zeigen, dass die Weiterentwicklung der SmartScreen-Filter-Technologie durch Application Reputation grundsätzlich sehr positiv zu bewerten ist, jedoch ist auf Grundlage der in dieser Untersuchung gewonnenen Ergebnisse die Erkennungsleistung noch deutlich zu verbessern. Dass der Internet Explorer 9 mit Application Reputation überhaupt eine integrierte Malware-Erkennung besitzt, ist insbesondere vor dem Hintergrund einer weiter zunehmenden Bedrohung durch Malware positiv zu bewerten. Somit reagiert Microsoft mit der Application Reputation des Internet Explorer 9 auf einen wichtigen aktuellen Trend.

Es ist festzuhalten, dass Internet Explorer 9 stets besser abschneidet als Internet Explorer 8. Weiterhin übertrifft Chrome 14 in allen betrachteten Kategorien Firefox 6 und Safari 5.

Ausgehend von der durchschnittlichen Platzierung in Tabelle VI und den weiteren Betrachtungen ergibt sich die Platzierung in Abbildung 13.

Im Folgenden werden die Ergebnisse dieser Studie in Zusammenhang mit den Ergebnissen anderer Arbeiten gebracht. In [Acc11] wurde die Sicherheit von verschiedenen Browsern miteinander verglichen, d.h. es wurden neben den Reputationssystemen zahlreiche weitere sicherheitsrelevante Funktionen betrachtet. Darüber hinaus war die Untersuchung der reputationsbasierten Schutzmechanismen nicht allein auf Malware-Angriffe fokussiert, wie dies in der vorliegenden Studie der Fall ist, sondern es wurden zusätzlich noch Phishing-Angriffe zur Bewertung der reputationsbasierten Schutzmechanismen betrachtet. Die Bewertung erfolgte in [Acc11] aggregiert für Malware- und Phishing-Angriffe, wobei der Malware-Teil nicht vollständig ist, da dort Application Reputation explizit ausgeschlossen wurde. Bei

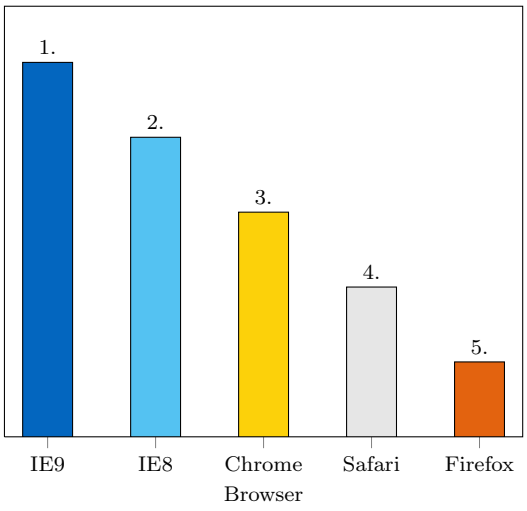

Abbildung 13. Platzierung

dieser aggregierten Bewertung schneiden beide Technologien, SmartScreen-Filter und Safe Browsing, ungefähr gleich gut ab. Insofern stimmen die wesentlichen Aussagen hinsichtlich der Leistungsfähigkeit von Reputationssystemen in Browsern mit der vorliegenden Studie nicht überein, was jedoch den unterschiedlichen Betrachtungsrahmen geschuldet sein mag.

Vergleicht man die Ergebnisse der vorliegenden Studie mit den Ergebnissen aus [NSS11a; NSS11b], dann können dort zumindest gleiche Tendenzen festgestellt werden, wenngleich die in beiden Untersuchungen gemessenen Werte weit auseinander liegen. In [NSS11a; NSS11b] schneiden Internet Explorer 8 und Internet Explorer 9, wie auch in der vorliegenden Arbeit, bei der Bewertung der Reputationssysteme zum Malware-Schutz besser ab als die anderen Browser. In [NSS11a; NSS11b] sind wie in der vorliegenden Untersuchung ebenfalls deutliche Unterschiede in der Erkennungsleistung zwischen Internet Explorer 8 und Internet Explorer 9 auf der einen Seite und Chrome, Firefox und Safari auf der anderen Seite zu erkennen. Dennoch gibt es auch erwähnenswerte Unterschiede zwischen [NSS11a; NSS11b] und der vorliegenden Untersuchung: Auch wenn der Internet Explorer 9 in der vorliegenden Untersuchung die besten Ergebnisse bei der Erkennungsleistung erzielen konnte, so liegen die gemessenen Werte weit entfernt von den Ergebnissen in [NSS11a; NSS11b]. Für die Erkennung von Malware-URLs werden in [NSS11a; NSS11b] Werte von über 90% angegeben; in der vorliegenden Untersuchung konnten jedoch nur Erkennungswerte von 34,9% gemessen werden (siehe Abschnitt 6.2). Bei der Kombination von adressbasierter und inhaltsbasierter Reputation (siehe Abschnitt 6.6) konnte der Internet Explorer 9 einen Wert von 39,1% erreichen, wohingegen in [NSS11a; NSS11b] Erkennungswerte von über 99% angegeben werden.

Abschließend bleibt festzustellen, dass der Schutz gegen Malware zwar offensichtlich immer wichtiger wird, es sich bei Reputationssystemen jedoch nur um einen — wenngleich sehr relevanten — Mosaikstein im Gesamtbild der Sicherheit von Browsern handelt. Es sei ausdrücklich darauf hingewiesen, dass ausgehend von den Betrachtungen und Ergebnissen zur Leistungsfähigkeit von Reputationssystemen in Browsern keine Aussagen zu anderen Browser-Sicherheitsmechanismen getroffen werden können und auch keine Verallgemeinerungen zur Gesamtsicherheit der Browser zulässig sind.

LITERATUR

[Acc11] Accuvant Labs: *Browser Security Comparison — A Quantative Approach*. http://www.accuvant.com/sites/default/files/AccuvantBrowserSecCompar_FINAL.pdf, Dezember 2011

[AV 11] AV Test: *Malware*. http://www.av-test.org/en/statistics/malware/, 2011

[BIT10] BITKOM: *Online-Kriminelle gehen immer raffinierter vor*. http://www.bitkom.org/de/themen/54750_65010.aspx, September 2010

[BKA10] BKA (Bundeskriminalamt): *Cybercrime - Bundeslagebild 2010*. http://www.bka.de/nn_224082/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrime2010,templateId=raw,property=publicationFile.pdf/cybercrime2010.pdf, 2010

[BSI11] BSI (Bundesamt für Sicherheit in der Informationstechnik): *Die Lage der IT-Sicherheit in Deutschland 2011*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2011.pdf?__blob=publicationFile, 2011

[BSI12] BSI (Bundesamt für Sicherheit in der Informationstechnik): *Register aktueller Cyber-Gefährdungen und -Angriffsformen*. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/BSI-A-CS_001.pdf, 2012

[Don09] Dongen, Wouter S. van: *Browser Security*. http://staff.science.uva.nl/~delaat/rp/2008-2009/p07/report.pdf, 2009

[Eik11] Eikenberg, Ronald: *Hacker ohne Grenzen*. c't, 16/11, 2011

[Goo11a] Google: *Google Safe Browsing API*. http://code.google.com/intl/de-DE/apis/safebrowsing/, 2011

[Goo11b] Google: *Google Safe Browsing API — Developer's Guide*. http://code.google.com/intl/de-DE/apis/safebrowsing/developers_guide_v2.html, 2011

[Goo11c] Google: *SafeBrowsing API*. http://code.google.com/intl/de-DE/apis/safebrowsing/, 2011

[hei11] heise: *iX: Features und Maßnahmen gegen Browser-Angriffe*. http://www.heise.de/ix/meldung/iX-Features-und-Massnahmen-gegen-Browser-Angriffe-1177075.html, 2011

[IWS04] Ives, Blake; Walsh, Kenneth R. ; Schneider, Helmut: The domino effect of password reuse. In: *Communications of the ACM* 47 (2004), April, Nr. 4

[KPM10] KPMG: *e-Crime-Studie 2010 — Computerkriminalität in der deutschen Wirtschaft*. http://www.kpmg.de/docs/20100810_kpmg_e-crime.pdf, 2010

[Mü11] Müller, Eva: *Mata Hari lebt.* http://www.manager-magazin.de/unternehmen/it/0,2828,781309,00.html, 2011

[Mic11a] Microsoft: *Funktionen von Internet Explorer 8.* http://windows.microsoft.com/de-DE/internet-explorer/products/ie-8/features/safer, 2011

[Mic11b] Microsoft: *SmartScreen-Filter: Häufig gestellte Fragen.* http://windows.microsoft.com/de-DE/windows-vista/smartscreen-filter-frequently-asked-questions, 2011

[Mic11c] Microsoft: *SmartScreen-Filter: Häufig gestellte Fragen.* http://windows.microsoft.com/de-DE/windows-vista/smartscreen-filter-frequently-asked-questions, 2011

[NSS11a] NSS Labs: *Web Browser Security — Socially-Engineered Malware Protection — Comparative Test Results Europe.* http://www.nsslabs.com/assets/noreg-reports/2011/nss%20labs_q2_2011_browsersem_FINAL.pdf, Mai 2011

[NSS11b] NSS Labs: *Web Browser Security — Socially-Engineered Malware Protection — Comparative Test Results Global.* http://www.nsslabs.com/assets/noreg-reports/2011/nss%20labs_q3_2011_browsersem%20GLOBAL-FINAL.pdf, August 2011

[PRM09] Provos, Niels; Rajab, Moheeb Abu ; Mavrommatis, Panayiotis: Cybercrime 2.0: When the Cloud Turns Dark. In: *Communications of the ACM* 53 (2009), April, Nr. 4, S. 43 – 47

[Sob11] Sobrier, Julien: *Google Safe Browsing v2 API: implementation notes — Technical information about using Google Safe Browsing v2.* http://code.google.com/intl/de-DE/apis/safebrowsing/developers_guide_v2.html, 2011

[Spi11a] Spiegel Online: *Angriff auf Technologiebörse — Nasdaq-Hacker hatten Zugriff auf Firmendaten.* http://www.spiegel.de/netzwelt/netzpolitik/0,1518,793101,00.html, 2011

[Spi11b] Spiegel Online: *Bundesbehörde warnt vor Zombie-Armeen.* http://www.spiegel.de/netzwelt/netzpolitik/0,1518,767822,00.html, 2011

[YBAG04] Yan, Jeff; Blackwell, Alan; Anderson, Ross ; Grant, Alasdair: Password Memorability and Security: Empirical Results. In: *IEEE Security & Privacy* 2 (2004), September-October, Nr. 5

ISSN: 2192-8169