Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

BSI-Empfehlung für sichere Web-Browser

Das weitverzweigte Word Wide Web (WWW) stellt eine große Anzahl an Internetangeboten zur Verfügung. Von einigen dieser Angebote geht ein Sicherheitsrisiko aus, da Kriminelle oder andere Angreifer Fehler ausnutzen und versuchen könnten, Zugriff auf vertrauliche Daten der Nutzer zu erlangen oder sich Zugang zu deren IT-Systemen zu verschaffen. Meist wird das WWW heute über Web-Browser oder durch Einbindung von deren Komponenten in Anwendungen (z. B. Darstellung von Webseiten im E-Mail-Clients) genutzt. Um den potenziellen Gefahren zu begegnen, ist es wichtig, dass der eingesetzte Web-Browser und seine Komponenten zuverlässig und sicher betrieben werden. Daher beschreibt dieses Dokument Anforderungen an sichere Web-Browser und deren Komponenten für den Einsatz in Unternehmen, analog zum BSI-Mindeststandard[1] für Behörden. Diese Anforderungen sollen IT-Verantwortlichen und Herstellern eine Orientierungshilfe bei der Produktauswahl und -entwicklung bieten.

1 Sicherheitsrisiko

Aufgrund ihres Einsatzgebietes sind Web-Browser einer besonderen Gefährdung durch Schadprogramme ausgesetzt. Die dargestellten statischen und aktiven Inhalte kommen häufig aus unsicheren Quellen auf die IT-Systeme der Nutzer. Sind diese Multimedia-Dateien, Skripte oder Programme mit Schadcode behaftet, können Angreifer ggf. vorhandene Funktionen des Web-Browsers in unerwünschter Weise oder Schwachstellen unmittelbar ausnutzen. Somit steht der Web-Browser vor der Herausforderung, die auf dem IT-System gespeicherten und verarbeiteten Daten vor unerwünschtem Zugriff zu schützen und Manipulationen des IT-Systems zu verhindern sowie gleichzeitig breite Einsatzszenarien zu unterstützen.

Darüber hinaus muss der Web-Browser auch die vertrauenswürdige Kommunikation mit Web-Angeboten ermöglichen. Hierfür müssen sichere Verschlüsselungsprotokolle [BSI19] genutzt werden, sodass ein Angreifer nicht die Kommunikation der Nutzer mit dem Web-Angebot belauschen kann.

Neben den technischen Risiken besteht darüber hinaus eine Gefährdung durch fehlgeleitetes Nutzerverhalten. Per Social Engineering versuchen Kriminelle, das tatsächliche Verhalten eines Internet-Angebotes oder heruntergeladenen Programms zu verschleiern, sodass die Nutzer dazu verleitet werden, im Sinne des Angreifers zu handeln. Beispiele hierfür sind nachgeahmte Web-Seiten oder irreführende Links auf Schadprogramme.

1 https://www.bsi.bund.de/DE/Themen/StandardsKriterien/Mindeststandards_Bund/Sichere_Web-Browser/Sichere_Web-Browser_node.html

Auch aufgrund solcher Bedrohungen müssen Sicherheitsmechanismen in Web-Browsern so umgesetzt werden, dass sie standardmäßig aktiviert sind, einfach zu nutzen sind und kein Hindernis darstellen. Andernfalls ist damit zu rechnen, dass Nutzer Sicherheitsmechanismen nicht beachten oder sogar abschalten. Die Funktionalität des Web-Browsers sollte außerdem möglichst viele Anwendungsfälle abdecken, da Nutzer sonst auf einen gegebenenfalls unsicheren Web-Browser wechseln, der die benötigte Funktionalität bietet.

Eine hohe Herausforderung stellt die Überprüfung des installierten Web-Browsers und von Erweiterungskomponenten auf Unbedenklichkeit dar, die selbst für fortgeschrittene Anwender kaum möglich ist. Im Normalfall erfordert eine fehlende Überprüfbarkeit vom Nutzer ein Vertrauen in den Hersteller des Web-Browsers und des Betriebssystems sowie in die Aussteller der für die Signierung genutzten Zertifikate (Certification Authorities, CAs) oder in eine unabhängige Prüfstelle, die die Sicherheit nach einer hinreichenden und anerkannten Evaluierung erklären kann.

2 Sicherheitsanforderungen

Angesichts der oben aufgeführten Sicherheitsrisiken werden folgende Anforderungen an Web-Browser gestellt:

1. Sichere Programmausführung sowie Schutz vor Ausnutzung von Schwachstellen

1.1 **(A)** Nutzung von Stack- und Heapschutz sowie ausschließlich sicherer Funktionen bei der Programmerstellung
1.2 **(A)** Nutzung vorhandener Speicherschutzmechanismen des Betriebssystems (ASLR[2], DEP[3], sichere Ausnahmebehandlung)
1.3 **(A)** Ausführung des Web-Browsers mit minimalen Rechten insbesondere für Darstellung des Inhalts
1.4 **(A)** Weitestgehende Prozessisolation von voneinander getrennten Inhalten einschließlich Plugins und gegenüber dem Betriebssystem (Sandboxing)
1.5 **(Z)** Möglichkeit des Betriebs von mehreren, unterschiedlich konfigurierten Instanzen eines Web-Browsers
1.6 **(Z)** Vollständige Überprüfbarkeit sowohl des Web-Browsers als auch von mitgelieferten Erweiterungskomponenten (Verfügbarkeit von Quellcode)

2. Steuerungsmechanismen für aktive Inhalte und Erweiterungskomponenten

2.1 **(A)** Möglichst fein-granulare Kontrolle der Ausführung von JavaScript, HTML5, WebGL und Flash (Click-to-Play) sowie von installierten Erweiterungskomponenten und Plugins mit einfachen, sicheren Grundeinstellungen
2.2 **(Z)** Darstellung von Dokumentenformaten mit einer integrierten minimalen Anzeigekomponente (z. B. PDF, Office-Dateiformate)
2.3 **(Z)** Voreingestellte Bevorzugung von integrierten Darstellungsmechanismen vor Lösungen von Drittanbietern

3. Schließen von Schwachstellen

3.1 **(A)** Bereitstellung von Aktualisierungen bei Schwachstellen (insbesondere bei kritischen Schwachstellen muss eine Aktualisierung spätestens 21 Tage nach Bekanntwerden verfügbar sein)
3.2 **(A)** Schnelle und zuverlässige Verteilung von Aktualisierungen mittels automatischer Mechanismen auch für Erweiterungskomponenten und Plugins
3.3 **(A)** Schnelles automatisches Sperren oder Entfernen von anfälligen oder schadhaften Erweiterungskomponenten und Plugins
3.4 **(A)** Konfigurierbarkeit der Mechanismen zur Verteilung und Installation von Aktualisierungen für den Web-Browser und von Erweiterungskomponenten und Plugins
3.5 **(A)** Veröffentlichte Kontaktmöglichkeiten zum Sicherheitsteam des Herstellers
3.6 **(Z)** Zusammenarbeit mit und Honorierung der Arbeit von Schwachstellenfindern, um Schwachstellen noch schneller schließen zu können und zum Melden von Schwachstellen an den Hersteller zu motivieren

2 Address-Space Layout Randomization
3 Data Execution Prevention

4. Überprüfung auf unerwünschte Inhalte

4.1 **(A)** Überprüfung auf unerwünschte Inhalte (Social Engineering und Schadprogramme) unter Berücksichtigung von Datenschutzaspekten

4.2 **(Z)** Reputations-basierte Überprüfung von heruntergeladenen Dateien

5. Schutz der Vertraulichkeit privater Daten

5.1 **(A)** Konfigurierbarkeit des Verhaltens und spezifische Verwaltung von Cookies insbesondere 3rd Party Cookies sowie der Schutz von Cookies z. B. vor XSS[4], XSRF[5]

5.2 **(A)** Möglichst weitgehende Umsetzung von Same-Origin-Policy, Content-Security-Policy (mind. 2.0) sowie Subresource Integrity

5.3 **(A)** Sicherer Zugriff auf eingegebene Formulardaten der Autofill-Historie

5.4 **(Z)** Sichere Speicherung von eingegebenen Passwörtern in einem Passwortmanager unter Verwendung eines Master-Passwortes

6. Sichere Verschlüsselung von Verbindungen

6.1 **(A)** Sicheres lokales Zertifikatsmanagement

6.2 **(A)** Vollständige Überprüfung der Gültigkeit des Serverzertifikats einschließlich der Überprüfung des Widerrufs

6.3 **(A)** Unterstützung der aktuellen TLS[6]-Protokollversion (derzeit 1.2)

6.4 **(A)** Einfache Konfigurierbarkeit einschließlich einer gezielten Sperrung der vom Web-Browser genutzten TLS[6]-Versionen, Schlüssellängen und Algorithmen

6.5 **(A)** Unterstützung für HSTS[7] und HPKP[8]

6.6 **(Z)** Gute Visualisierung verschlüsselter Verbindungen insbesondere des Serverzertifikats und der genutzten Protokolle und Cipher-Suiten

6.7 **(Z)** Unterstützung von Mixed Content Blocking, wobei iFrames wie aktive Inhalte behandelt werden sollten

6.8 **(Z)** Unterstützung von DNS-over-HTTPS (DoH) mit frei konfigurierbarem DoH-Server

7. Sichere Verwaltung der Einstellungen

7.1 **(A)** Vorkonfigurierte Einstellungen sollen für die grundsätzlich relevanten Anwendungsfälle wie Finanzanwendungen, Reisebuchungen, Suchmaschinen, Online-Handelsplätze, Web-Mail, PIM und soziale Netzwerke eine möglichst hohe Sicherheit bieten

7.2 **(A)** Explizite Kontrolle über die Synchronisation von Einstellungen und weiteren Browser-Daten an Cloud-Dienste (wenn eine Synchronisationsfunktion vorhanden ist)

7.3 **(A)** Möglichkeit der zentralisierten Verwaltung von Einstellungen und Aktualisierungen des Web-Browsers und seiner Erweiterungskomponenten

A: Anforderung
Z: optionale Zusatzfunktion

3 Mindestanforderungen

Alle Anforderungen aus der oben genannten Liste, die mit einem **(A)** gekennzeichnet sind, stellen die Mindestanforderungen für einen sicheren Web-Browser dar.

4 Weitere Absicherungsmöglichkeiten

Neben der Wahl des Web-Browsers stehen auch bei der Bereitstellung der Software verschiedene Möglichkeiten der Absicherung zur Verfügung. Das BSI hat hierzu die Veröffentlichung „Ab-

4 Cross-Site-Scripting
5 Cross-Site-Request-Forgery
6 Transport Layer Security
7 HTTP Strict Transport Security
8 HTTP Public Key Pinning

sicherungsmöglichkeiten beim Einsatz von Web-Browsern“[9] verfasst, die auf den Internetseiten der Allianz für Cyber-Sicherheit zu finden ist.

5 Fazit

Die aufgestellten Sicherheitsanforderungen werden derzeit noch nicht von allen Web-Browsern in sämtlichen Punkten erfüllt. Daher sollte bei der Produktauswahl genau geprüft werden, welche der genannten Anforderungen durch welchen Web-Browser, und im Hinblick auf die individuellen Nutzungsszenarien, am besten erfüllt werden. Hersteller von Web-Browsern sollen ermutigt werden, die Sicherheitsanforderungen möglichst umfassend umzusetzen.

Weitere Informationen zur sicheren Nutzung von Web-Angeboten hat das BSI im Rahmen der ISi-Reihe[10] veröffentlicht.

6 Verweise

Für weitere Informationen zu den unterschiedlichen Sicherheitsanforderungen wird auf die folgenden Quellen verwiesen:

1. [Se13, Sh13, Si11]
   1.1 [Bu10, Ma10a, Mi13a, Mi13b]
   1.2 [Br13, Ko12, Ma10b]
   1.3 [SS75]
   1.4 [Ke11]
   1.5 [Gr12, Mo13a]
   1.6 [Ei14, GD00, RVRK05, Sch03]
2.
   2.1 [Cr12, DR02, In20, Kr11, Sa20, UD18, UD19]
   2.2 [Mo20a]
   2.3 [Ho17]
3.
   3.1 [BSI18, ISO13, So12]
   3.2 [UD14a]
   3.3 [Mo20b]
   3.4 [Mo14, Th20a]
   3.5 [Mi20a, Mo20c]
   3.6 [ISO14a]
4.
   4.1 [Mi20b, Pr12, Sa10]
   4.2 [CSWY12]
5. [AVEU09]
   5.1 [Go20a, IVRW12, Mi13c, Mo20d, VZ19]
   5.2 [W3C10, W3C18, Mo19a, W3C16, Mo20i]
   5.3 [Mo20f]
   5.4 [Be12, Mo20e]
6.

6.1 [Cl04]
6.2 [ITU12, ISO14b, IETF08a]
6.3 [IETF08b, BSI19]
6.4 [Ku13]

6.5 [IETF12, Mo19b, Th20b, ES00, IETF15, Mo19c, SS12]
6.6 [1M20]

   6.7 [Mo13b, Re13]
   6.8 [IETF18, Mo20j]
7.

9 https://www.allianz-fuer-cybersicherheit.de/dok/6649786
10 https://www.bsi.bund.de/ISi-Reihe

7.2 [Co11, Go20b, Mo20g, Mo20h]
7.3 [Go20c, Go20d, Mi20c]

7 Referenzen

[1M20] 1&1 Mail & Media (Hrsg.): „SSL“, Webseite, 1&1 Mail & Media, o. J., URL: https://hilfe.web.de/sicherheit/ssl.html (Stand 13.01.2020).

[AVEU09] Amt für Veröffentlichungen der Europäischen Union (Hrsg.): „Richtlinie 2009/136/EG des Europäischen Parlaments und des Rates vom 25. November 2009“, Amtsblatt der Europäischen Union, L 337, 11-36, Amt für Veröffentlichungen der Europäischen Union, 18.12.2009, URL: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:DE:PDF.

[Be12] Bestuzhev, D.: „How to survive attacks that result in password leaks?“, Webseite, Kaspersky Lab ZAO, 13.07.12, URL: https://www.securelist.com/en/blog/208193675/How_to_survive_attacks_that_result_in_password_leaks (Stand 13.01.2020).

[Br13] Bravo Navarro, A.: „How Effective is ASLR on Linux Systems?“, Webseite, J. A. Bravo Navarro, 02.03.2013, URL: http://securityetalii.es/2013/02/03/how-effective-is-aslr-on-linux-systems/ (Stand 13.01.2020).

[BSI18] BSI (Hrsg.): „CS-E Handhabung von Schwachstellen“, BSI-CS 019, Version 1.10, BSI, 11.07.2018, URL: https://www.bsi.bund.de/ACS/DE/_downloads/techniker/programmierung/BSI-CS_019.pdf.

[BSI19] BSI (Hrsg.): „Kryptographische Verfahren: Empfehlungen und Schlüssellängen; Teil 2 - Verwendung von Transport Layer Security (TLS) Version 2014-01“, TR-02102-2, BSI, 22.02.2019, URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf.

[Bu10] Burrell, T.: „The Evolution of Microsoft's Exploit Mitigations“, Präsentation, Hackito Ergo Sum Conference, Paris, 08.04.2010, URL: www.hackitoergosum.org/2010/HES2010-tgarnier-Evolution-of-Microsofts-Mitigations.pdf.

[Cl04] Clercq, J. de: „Windows Server 2003 Security Infrastructure: Core Security Features“, HP Technologies, Digital Press, März 2004.

[Co11] Coutandin, A.: „How to FSyncMS Installieren – Firefox Sync eigener Server“, Webseite, Arwed Coutandin, 24.07.2011, URL: http://www.ohnekontur.de/2011/07/24/how-to-install-fsyncms-firefox-sync-eigener-server/ (Stand 13.01.2020).

[Cr12] Crume, J.: „Dodging a drive-by attack“, Webseite, Jeff Crume, 19.09.2012, URL: http://insideinternetsecurity.wordpress.com/2012/09/19/dodging-a-drive-by-attack/ (Stand 13.01.2020).

[CSWY12] Czajkowski, K.; Schneider, M.; Wolf, R.; Yannikos, Y.: „Untersuchung von reputationsbasierten Schutzmechanismen gegen Malware-Angriffe in Browsern“, SIT Technical Report, SIT-TR-2012-002, Frauenhofer Irb Verlag, März 2012, URL: https://www.sit.fraunhofer.de/fileadmin/dokumente/studien_und_technical_reports/Malware_a4.pdf.

[DR02] Dormann, W.; Rafail, J.: „Securing Your Web Browser“, Webseite, Software Engineering Institute, Carnegie Mellon University, 01.01.2002, URL: https://resources.sei.cmu.edu/asset_files/WhitePaper/2002_019_001_496700.pdf (Stand 13.01.2020).

[Ei14] Eich, B.: „Trust but verify“, Webseite, Brendan Eich, 11.01.2014, URL: https://brendaneich.com/2014/01/trust-but-verify/ (Stand 13.01.2020).

[ES00] Ellison, C.; Schneier, B.: „Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure“, Computer Security Journal, Band 16, Nr. 1, S. 1-7, Computer Security Institute, 2000, URL: https://www.schneier.com/paper-pki.pdf.

[GD00] González-Barahona, J.M.; Daffara, C. (Hrsg.): „Free Software / Open Source: Information Society Opportunities for Europe?“, Version 1.2, European Working Group on Libre Software, April 2000, URL: http://eu.conecta.it/paper.pdf.

[Go20a] Google (Hrsg.): „Cookies in Chrome löschen, aktivieren und verwalten“, Webseite, Google, o. J., URL: https://support.google.com/chrome/answer/95647?hl=de (Stand 13.01.2020).

[Go20b] Google (Hrsg.): „Lesezeichen, Passwörter und andere Daten auf allen Ihren Geräten aufrufen“, Webseite, Google, o. J., URL: https://support.google.com/chrome/answer/165139?hl=de&ref_topic=1693469 (Stand 13.01.2020).

[Go20c] Google (Hrsg.): „Chrome Browser Deployment Guide“, Google-Dokument, Google, Mai 2019, URL: http://goo.gl/2QvOT.

[Go20d] Google (Hrsg.): „Google Chrome verwalten“, Webseite, Google, o. J., URL: https://support.google.com/chrome/a/answer/188446?hl=de (Stand 13.01.2020).

[Gr12] Grossman, J.: „The Web Won't Be Safe or Secure until We Break It“, ACM Queue - Web Security, Band 10, Heft 11, 10 Seiten, ACM, November 2012, URL: http://dl.acm.org/citation.cfm?id=2390758.

[Ho17] Hoffman, C.: „This Is Why You Don’t Need Adobe Reader“, Webseite, MakeUseOf Limited, 02.02.2017, URL: http://www.makeuseof.com/tag/this-is-why-you-dont-need-adobe-reader/ (Stand 13.01.2020).

[IETF08a] IETF Network Working Group (Hrsg.): „Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile“, RFC 5280, Internet Engineering Task Force, Mai 2008, URL: http://tools.ietf.org/html/rfc5280.

[IETF08b] IETF Network Working Group (Hrsg.): „The Transport Layer Security (TLS) Protocol Version 1.2“, RFC 5246, Internet Engineering Task Force, August 2008, URL: http://tools.ietf.org/html/rfc5246.

[IETF12] IETF: „HTTP Strict Transport Security (HSTS)“, RFC 6797, Internet Engineering Task Force, November 2012, URL: http://tools.ietf.org/html/rfc6797.

[IETF13] IETF Web Security (Hrsg.): „Public Key Pinning Extension for HTTP“, Entwurf, Version 09, Internet Engineering Task Force, 27.11.2013, URL: http://tools.ietf.org/pdf/draft-ietf-websec-key-pinning-09.pdf.

[IETF15] Internet Engineering Task Force: „Public Key Pinning Extension for HTTP“, RFC 7469, Internet Engineering Task Force, April 2015, URL: https://tools.ietf.org/html/rfc7469.

[IETF18] Internet Engineering Task Force: „DNS Queries over HTTPS (DoH)“, RFC 8484, Internet Engineering Task Force, Oktober 2018, URL: https://tools.ietf.org/html/rfc8484.

[In20] InformAction (Hrsg.): „NoScript - JavaScript/Java/Flash blocker for a safer Firefox experience! - what is it?“, Webseite, InformAction, o. J., URL: http://noscript.net/whats (Stand 13.01.2020).

[ISO13] ISO/IEC JTC 1/SC 27 (Hrsg.): „Information technology - Security tequniques - Vulnerability handling processes“, ISO/IEC DIS 30111:2013-01, International Organization for Standardization, 22.10.2013, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53231.

[ISO14a] ISO/IEC JTC 1/SC 27 (Hrsg.): „Information technology - Security tequniques - Vulnerability disclosure“, ISO/IEC FDIS 29147:2014, Entwurf, International Organization for Standardization, Feb 2014, URL: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=45170.

[ISO14b] ISO/IEC JTC 1/SC 6 (Hrsg.): „Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks“, ISO/IEC 9594-8:2008, International Organization for Standardization, März 2014, URL: https://www.iso.org/standard/64854.html.

[ITU12] ITU (Hrsg.): „Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks“, ITU-T Recommendation X.509 (10/2012), International Telecommunication Union, Oktober 2012, URL: http://handle.itu.int/11.1002/1000/11735.

[IVRW12] Iversen, S.; Vogelsang, L.; Riedel, S.; Weinmann, A.: „Die Einstellung macht's: Werbung und Privatsphäre im Internet", Broschüre, Arbeitsgemeinschaft der deutschen Familienorganisationen e.V. (AGF), November 2012, URL: http://www.ag-familie.de/media/agfdoc/AGF_Werbung_im_Internet_webversion.pdf.

[Ke11] Keetch, T.: „Practical Sandboxing on the Windows Platform", Whitepaper, Black Hat Europe 2011, Barcelona, 2011, URL: http://media.blackhat.com/bh-eu-11/Tom_Keetch/BlackHat_EU_2011_Keetch_Sandboxes-WP.pdf.

[Ko12] Kortchinsky, K.: „10 years later, which vulnerabilities still matter?", Präsentation, GreHack 2012, Grenoble, 29.10.2012, URL: http://ensiwiki.ensimag.fr/images/e/e8/GreHack-2012-talk-Kostya_Kortchinsky_Crypt0ad_-10_years_later_which_in_memory_vulnerabilities_still_matter.pdf.

[Kr11] Krebs, B.: „Blocking JavaScript in the Browser", Webseite, Krebs on Security, 25.05.2011, URL: https://krebsonsecurity.com/2011/05/blocking-javascript-in-the-browser/ (Stand 13.01.2020).

[Ku13] Kuketz, M.: „Unsichere SSL-Verschlüsselung im Browser abschalten", Webseite, Mike Kuketz, 19.11.2013, URL: http://www.kuketz-blog.de/unsichere-ssl-verschluesselung-im-browser-abschalten/ (Stand 13.01.2020).

[Ma10a] Madej, R.: „Assessing the Tux Strength: Part 1 - Userspace Memory Protection", Webseite, MWR InfoSecurity, 29.06.2010, URL: https://labs.mwrinfosecurity.com/blog/2010/06/29/assessing-the-tux-strength-part-1---userspace-memory-protection/ (Stand 13.01.2020).

[Ma10b] Madej, R.: „Assessing the Tux Strength: Part 2 – Into the Kernel", Webseite, MWR InfoSecurity, 02.09.2010, URL: https://labs.mwrinfosecurity.com/blog/2010/09/02/assessing-the-tux-strength-part-2---into-the-kernel/ (Stand 13.01.2020).

[Mi13a] Mitre Corporation (Hrsg.): „CWE-242: Use of Inherently Dangerous Function", Webseite, Mitre Corporation, 16.07.2013, URL: http://cwe.mitre.org/data/definitions/242.html (Stand 13.01.2020).

[Mi13b] Mitre Corporation (Hrsg.): „CWE-676: Use of Potentially Dangerous Function", Webseite, Mitre Corporation, 16.07.2013, URL: http://cwe.mitre.org/data/definitions/676.html (Stand 13.01.2020).

[Mi13c] Microsoft (Hrsg.): „Löschen von Cookiedateien in Internet Explorer", Webseite, Microsoft, 23.11.2013, URL: http://support.microsoft.com/kb/278835/de (Stand 13.01.2020).

[Mi20a] Microsoft (Hrsg.): „Report a Computer Security Vulnerability", Webseite, Microsoft, o. J., URL: https://www.microsoft.com/de-de/msrc/faqs-report-an-issue (Stand 13.01.2020).

[Mi20b] Microsoft (Hrsg.): „SmartScreen-Filter: Häufig gestellte Fragen", Webseite, Microsoft, o. J., URL: http://support.microsoft.com/de-de/help/17443/windows-internet-explorer-smartscreen-faq (Stand 13.01.2020).

[Mi20c] Microsoft (Hrsg.): „Internet Explorer 11 (IE11) - Bereitstellungshandbuch für IT-Spezialisten", Webseite, Microsoft, o. J., URL: https://docs.microsoft.com/de-de/internet-explorer/ie11-deploy-guide/ (Stand 13.01.2020).

[Mo13a] MozillaZine (Hrsg.): „Opening a new instance of your Mozilla application with another profile", Webseite, MozillaZine, 09.10.2013, URL: http://kb.mozillazine.org/Opening_a_new_instance_of_Firefox_with_another_profile (Stand 13.01.2020).

[Mo13b] Mozilla Foundation (Hrsg.): „Mixed Content Blocking Enabled in Firefox 23!", Webseite, Mozilla Foundation, 10.04.2013, URL: https://blog.mozilla.org/tanvi/2013/04/10/mixed-content-blocking-enabled-in-firefox-23/ (Stand 13.01.2020).

[Mo14] MozillaZine (Hrsg.): „Software Update", Webseite, MozillaZine, 23.07.2014, URL: http://kb.mozillazine.org/Software_Update (Stand 13.01.2020).

[Mo19a] Mozilla Foundation: „Content Security Policy (CSP)", Webseite, Mozilla Foundation, 05.11.2019, URL: http://developer.mozilla.org/en-US/docs/Web/HTTP/CSP (Stand 13.01.2020).

[Mo19b] Mozilla Foundation (Hrsg.): „HTTP Strict Transport Security“, Webseite, Mozilla Foundation, 16.11.2019, URL: https://developer.mozilla.org/en-US/docs/Security/HTTP_Strict_Transport_Security (Stand 13.01.2020).

[Mo19c] Mozilla Foundation: „HTTP Public Key Pinning (HPKP)“, Webseite, Mozilla Foundation, 23.03.2019, URL: https://developer.mozilla.org/de/docs/Web/Security/Public_Key_Pinning (Stand 13.01.2020).

[Mo20a] Mozilla Foundation (Hrsg.): „View PDF files in Firefox“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/en-US/kb/view-pdf-files-firefox-without-downloading-them (Stand 13.01.2020).

[Mo20b] Mozilla Foundation (Hrsg.): „Add-ons, die Stabilitätsprobleme oder Sicherheitsrisiken verursachen, werden auf eine Sperrliste gesetzt“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/de/kb/Sperrliste-fuer-Add-ons (Stand 13.01.2020).

[Mo20c] Mozilla Foundation (Hrsg.): „Security Center“, Webseite, Mozilla Foundation, o. J., URL: https://www.mozilla.org/security/ (Stand 13.01.2020).

[Mo20d] Mozilla Foundation (Hrsg.): „Cookies – Informationen, die Websites auf Ihrem Computer ablegen“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/de/kb/cookies-informationen-websites-auf-ihrem-computer (Stand 13.01.2020).

[Mo20e] Mozilla Foundation (Hrsg.): „Gespeicherte Passwörter mit einem Master-Passwort schützen“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/de/kb/Gespeicherte-Passwoerter-mit-einem-Master-Passwort-schuetzen (Stand 13.01.2020).

[Mo20f] Mozilla Foundation (Hrsg.): „Formular-Autovervollständigung“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/de/kb/Formular-Autovervollstaendigung (Stand 13.01.2020).

[Mo20g] Mozilla Foundation (Hrsg.): „Wie richte ich Firefox Sync ein?“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/de/kb/wie-richte-ich-firefox-sync-ein (Stand 13.01.2020).

[Mo20h] Mozilla Foundation (Hrsg.): „Run your own Sync-1.5 Server“, Webseite, Mozilla Foundation, o. J., URL: http://mozilla-services.readthedocs.io/en/latest/howtos/run-sync-1.5.html (Stand 13.01.2020).

[Mo20i] Mozilla Foundation: „Subresource Integrity“, Webseite, Mozilla Foundation, 03.01.2020, URL: http://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity (Stand 13.01.2020).

[Mo20j] Mozilla Foundation: „Firefox DNS-over-HTTPS“, Webseite, Mozilla Foundation, o. J., URL: https://support.mozilla.org/en-US/kb/firefox-dns-over-https (Stand 13.01.2020).

[Pr12] Provos, N.: „Safe Browsing - Protecting Web Users for 5 Years and Counting“, Webseite, Google, 19.06.2012, URL: http://googleonlinesecurity.blogspot.de/2012/06/safe-browsing-protecting-web-users-for.html (Stand 13.01.2020).

[Re13] Regan, A.: „Mixed Content: What Instructors and Instructional Designers Need to Know“, Webseite, IT Technology and Learning group, Pepperdine University, 30.08.2013, URL: http://peptechlearn.blogspot.de/2013/08/mixed-content-what-instructors-and.html (Stand 13.01.2020).

[RVRK05] Renner, T.; Vetter, M.; Rex, S.; Kett, H.: „Open Source Software - Einsatzpotenziale und Wirtschaftlichkeit“, Studie, Fraunhofer Irb Verlag, 2005, URL: http://wiki.iao.fraunhofer.de/images/6/63/Fraunhofer-Studie-Open-Source-Software.pdf.

[Sa10] Sachweh, S.: „URL-Filter und Websicherheit“, Präsentation, T.I.S.P. Community Meeting 2010, Köln, November 2010, URL: https://www.teletrust.de/fileadmin/_migrated/content_uploads/04-TISP-ComMeeting-Sachweh-URL-Filter_und_Websicherheit.pdf.

[Sa20] Samuel, J. (Hrsg.): „RequestPolicy - Open source Firefox extension to control cross-site requests“, Webseite, Justin Samuel, o. J., URL: https://www.requestpolicy.com/index.html (Stand 13.01.2020).

[Sch03] Schneier, B.: „Internet Shield: Secrecy and security“, Webseite, Bruce Schneier, 02.03.2003, URL: https://www.schneier.com/essay-033.html (Stand 13.01.2020).

[Se13] Seacord, R.C.: „Secure Coding in C and C++“, 2. Auflage, Addison-Wesley Professional, 2013.

[Sh13] Shunn, A.: „Secure Development is much easier than you think“, Webseite, Dr. Dobb's Journal, 22.07.2013, URL: http://www.drdobbs.com/security/secure-development-is-much-easier-than-y/240158709 (Stand 13.01.2020).

[Si11] Simpson, S. (Hrsg.): „Fundamental Practices for Secure Software Development“, Whitepaper, 2. Auflage, SAFECode, Arlington, 08.02.2011, URL: http://www.safecode.org/wp-content/uploads/2018/01/SAFECode_Dev_Practices0211.pdf.

[So12] Sondhi, R.: „EMC's Approach to Vulnerability Response“, Webseite, EMC Product Security Blog, EMC Corporation, 14.12.2012, URL: http://blog.dellemc.com/en-us/emcs-approach-to-vulnerability-response/ (Stand 13.01.2020).

[SS12] Soghoian, C.; Stamm, S.: „Certified Lies: Detecting and Defeating Government Interception Attacks againt SSL“, Proceedings of the 15th international Conference on Financial Cryptography and Data Security (FC'11), Lecture Notes in Computer Science, Band 7035, S. 250-259, Springer, 2012, URL: http://link.springer.com/chapter/10.1007%2F978-3-642-27576-0_20.

[SS75] Saltzer, J.H.; Schroeder, M.D.: „The protection of information in computer systems“, Proceedings of the IEEE, Band 63, Heft 9, S. 1278-1308, IEEE, September 1975, URL: http://dx.doi.org/10.1109/PROC.1975.9939.

[Th20a] The Chromium Project (Hrsg.): „Turning Off Auto Updates in Google Chrome“, Webseite, Google, o. J., URL: http://dev.chromium.org/administrators/turning-off-auto-updates (Stand 13.01.2020).

[Th20b] The Chromium Project (Hrsg.): „HTTP Strict Transport Security“, Webseite, Google, o. J., URL: https://www.chromium.org/hsts (Stand 13.01.2020).

[UD14a] ubuntu Deutschland e. V. (Hrsg.): „Konfiguration“, Webseite, ubuntu Deutschland e. V., 21.01.2014, URL: http://wiki.ubuntuusers.de/Aktualisierungen/Konfiguration (Stand 04.02.2014).

[UD18] ubuntu Deutschland e. V. (Hrsg.): „Sicheres Surfen“, Webseite, ubuntu Deutschland e. V., 11.11.2018, URL: http://wiki.ubuntuusers.de/Firefox/Sicheres_Surfen (Stand 13.01.2020).

[UD19] ubuntu Deutschland e. V. (Hrsg.): „Sicheres Surfen“, , , , ubuntu Deutschland e. V., 06.12.2019, URL: http://wiki.ubuntuusers.de/Firefox/Sicheres_Surfen.

[VZ19] Verbraucherzentrale: „Cookies kontrollieren und verwalten“, Webseite, Verbraucherzentrale, 28.10.2019, URL: http://www.verbraucherzentrale.de/wissen/digitale-welt/datenschutz/cookies-kontrollieren-und-verwalten-11996 (Stand 13.01.2020).

[W3C10] W3C (Hrsg.): „Same Origin Policy“, Webseite, World Wide Web Consortium, 06.01.2010, URL: http://www.w3.org/Security/wiki/Same_Origin_Policy (Stand 13.01.2020).

[W3C16] W3C (Hrsg.): „Subresource Integrity“, , World Wide Web Consortium, 23.06.2016, URL: http://www.w3.org/TR/SRI/.

[W3C18] W3C (Hrsg.): „Content Security Policy Level 3“, , World Wide Web Consortium, 15.10.2018, URL: http://www.w3.org/TR/CSP3/.