Microsoft Presseservice
Paul-Heyse-Straße 29
D-80336 München

Telefon: 089/31 76 50 00
Telefax: 089/31 76 51 11

Internet Explorer 8: Sicher ist sicher

Sicherheit und Schutz der Privatsphäre sind zwei Top-Themen, wenn es um das Surfen im Internet geht. Internet Explorer 8 verfolgt einen durchgehenden Ansatz für Sicherheit und Datenschutz mit neuen Abwehrmechanismen sowie mehr Möglichkeiten, Daten zu kontrollieren und zu schützen. Dazu gehören:

1. **Domänenhervorhebung**

Internet Explorer 8 zeigt in der Adressleiste den Namen der Domäne innerhalb der URL in Schwarz an, die anderen Buchstaben in Grau. Damit kann der Anwender schnell erkennen, auf welcher Seite er sich befindet, und Phishingseiten sowie andere bedrohliche Seiten einfacher identifizieren.

2. **SmartScreen-Filter**

Der SmartScreen-Filter optimiert den Schutz vor Phishing-Angriffen und überprüft heruntergeladene Dateien auf Schadprogramme. So schützt er vor unbemerkter Installation von Malware oder bösartiger Software, die eine Gefahr für die Sicherheit von Daten, Datenschutz und Identität darstellt und zudem Computer und wertvolle Daten beschädigen kann.

3. **Cross-site Scripting (XSS)-Filter**

Dieser integrierte Filter schützt Systeme vor Angriffen, die ohne Wissen des Anwenders unter anderem zur Offenlegung von Informationen sowie dem Diebstahl von Cookies, Konten oder Identitäten dienen.

4. **Datenausführungsverhinderung**

Diese in Internet Explorer 8 in Windows 7 standardmäßig aktivierte Sicherheitsfunktion vermeidet möglichen Schaden durch Viren oder andere Sicherheitsrisiken. Gewisse Typen von Code werden daran gehindert, in den ausführbaren Speicher zu schreiben.

5. **InPrivate-Filterung**

Fast drei Viertel der deutschen Internetnutzer sind strikt gegen die Weitergabe persönlicher Daten im Internet, gemäß einer infratest-Studie. InPrivate-Filterung verhindert den Austausch persönlicher Informationen zwischen verschiedenen

Anbietern. Damit wird die Privatsphäre geschützt und der Nutzer bleibt gegenüber unbekannten Webseitenbetreibern anonym.

6. **InPrivate-Browsen**

Diese Funktion ermöglicht eine Online-Nutzung, ohne die Speicherung von Verlauf, Formulardaten, temporären Internet-Dateien, Cookies, Benutzernamen oder Passwörtern. Damit sind persönliche Daten bei Computern geschützt, die von mehreren Personen genutzt werden oder öffentlich zugänglich sind.

7. **Löschen des Browserverlaufs**

Diese Funktion wurde mit der Möglichkeit erweitert, einzelne Cookies, Verlaufselemente und andere Daten zu löschen, gleichzeitig aber die Cookies, Verlaufselemente und Daten der favorisierten Internetseiten zu behalten.

8. **Schutz vor ClickJacking**

ClickJacking ist ein Verfahren, um Anwendern über eine auf den ersten Blick harmlose Internetseite vertrauliche Daten zu entlocken. Zur Erkennung und Verhinderung können Anbieter von Webinhalten einen entsprechenden Tag in den Seiten-Header einbauen. Internet Explorer 8 zeigt Anwendern eine entsprechende Meldung an, falls der Webanbieter den Inhalt nicht zur Anzeige freigegeben hat. Nutzer können diesen aber in einem neuen Fenster öffnen.

9. **Cross-Document Messaging (XDM)**

Dies ist eine hochgradig sichere Methode zur bidirektionalen Cross-Dokumenten-Kommunikation. Internet Explorer 8 verfügt zudem über eine StaticHTML-Methode und nativer JavaScript Object Notation-Unterstützung, um Daten sicher zu desinfizieren, ohne die Leistungsfähigkeit zu beeinträchtigen.

10. **Cross-Domain Requests (XDR)**

Internet Explorer 8 unterstützt XDomainRequest-Objekte zum Abrufen sicherer öffentlicher Quellen von anderen Domänen. XDR prüft jetzt Access-Control-Allow-Origin für bestimmte URLs sowie Wildcards. Cross-Domain-Daten sind nur verfügbar, wenn die Serversignale explizit den Austausch zwischen Domänen erlauben, um den Server vor Attacken zu schützen.

11. **Per-site ActiveX**

Diese Funktion reduziert Oberflächenangriffe, indem ein implizierter SiteLock angeboten wird. Damit können ActiveX-Steuerelemente nur vom Ort ihrer Installation aus ausgeführt werden.

Weitere wichtige Funktionen aus Vorgängerversion

Mit Hilfe der Extended Validation SSL-Zertifikate ist der Datenverkehr zwischen Browser und dem jeweiligen Webserver wesentlich fälschungssicherer, weil eine strenge Überprüfung der Identität des Webserver-Betreibers bzw. SSL-Zertifikatsantragsstellers stattgefunden hat. Wenn eine Webseite im Internet Explorer 8 geöffnet wird, die die Anforderung des Extended Validation Standards erfüllt, färbt sich die URL-Leiste grün. Eine Anzeige neben dieser grünen Leiste stellt abwechselnd den im Zertifikat angegebenen Namen des Unternehmens und die Zertifizierungsstelle dar, die das Zertifikat ausgegeben hat. So lässt sich etwa beim Online-Banking sicherstellen, dass die Seite tatsächlich die originale der Bank ist.

Um die Privatsphäre sowie die Sicherheit des Computers optimal zu schützen, lassen sich unter Sicherheit/Browsereinstellungen verschiedene Einstellungen ändern. Dazu gehört das Festlegen von standardmäßigen und benutzerdefinierten Sicherheitsstufen für das Internet, das Intranet und bestimmte Websites sowie die Einstellungen für Cookies und Popupblocker.

Studienergebnisse

Gemäß einer unabhängigen Studie von Cenzic Inc. wurden im ersten Halbjahr 2009 nur 15 Prozent aller Schwachstellen in Browsern beim Internet Explorer festgestellt. 44 Prozent der Schwachstellen wurden bei Firefox identifiziert, bei Safari 35 Prozent und bei Opera 6 Prozent. Alle Web-Browser zusammen waren für 8 Prozent der Schwachstellen im Internet verantwortlich, zu 90 Prozent kommerzielle Web-Anwendungen und zu 2 Prozent Web-Server (http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q1-Q2-2009.pdf).

Eine von Microsoft in Auftrag gegebene Studie von NSS Labs (http://nsslabs.com/browser-security) testete aktuelle Browser-Versionen darauf, wie viele Angriffe diese durch schädliche Software und Phishing abwehren konnten. Der Internet Explorer 8 warnte bei 81 Prozent der gefährlichen Downloads, deutlich mehr als Firefox 3 (27%), Safari 4 (21%),

Chrome 2 (7%) und Opera 10 (1%). Bei 83 Prozent aller Phishing-Seiten gab der Internet Explorer 8 Warnmeldungen aus, gefolgt von Firefox 3 (80%), Opera 10 (54%), Chrome 2 (26%) und Safari 4 (2%).

Der siebte Microsoft Security Intelligence Report (SIRv7, http://www.microsoft.com/sir) zeigt, dass der in Internet Explorer 8 eingeführte SmartScreen-Filter einen messbaren Schutz vor Phishing- und Malware-Angriffen bietet. Obwohl der Anteil „verschiedener unerwünschter Software“ von 35 Prozent der Malware-Aufrufe im zweiten Halbjahr 2008 auf 44,5 Prozent im ersten Halbjahr 2009 stieg, sank der Anteil der bereinigten Computer für diese Kategorie von 22,8 Prozent auf 14,9 Prozent. Dies lässt schließen, dass SmartScreen und ähnliche Technologien diese Bedrohungen höchstwahrscheinlich erfolgreich abfangen, bevor sie auf Computer heruntergeladen werden.

Textlänge: 6.693 Zeichen

Microsoft Presseservice
Fink & Fuchs Public Relations AG
Paul-Heyse-Straße 29
D-80336 München
Tel.: 0 89 - 3176-5000
Fax: 0 89 - 3176-5111
E-Mail: prserv@microsoft.com
http://www.microsoft.de/presse
http://twitter.com/microsoftpresse

Vorstand: Dipl.-Kfm. Stephan Fink | Dipl.-Ing. Martin Fuchs
Vorsitzender des Aufsichtsrats: Thomas Weidmann
Amtsgericht Wiesbaden, HRB 7013

Servicepartner der Microsoft Deutschland GmbH
E-Mail: prserv@microsoft.com

http://www.microsoft.de/presse
http://twitter.com/microsoftpresse