Westfälische Hochschule

Wissen.
Was praktisch zählt.

Unser (un)sicheres Web:

Update-Verhalten von Websites und seine Auswirkungen auf die Sicherheit

Autoren: Nurullah Demir, Tobias Urban, Kevin Wittek, Norbert Pohlmann

Heutzutage nutzen wir das Web für verschiedene Aufgaben und Dienste (z. B. um mit unseren Freunden zu sprechen, Ideen auszutauschen, sich zu unterhalten oder zu arbeiten). Diese Dienste verarbeiten viele persönliche und wertvolle Daten, die geschützt werden müssen.
Eine wesentliche Rolle im Sicherheitskonzept jeder Anwendung ist der Aktualisierungsprozess der verwendeten Komponenten. Das Nicht-Aktualisieren von Software kann schwerwiegende Auswirkungen auf die Sicherheit haben. Zum Beispiel war der Grund für den Dataleak bei Equifax, von der 143 Millionen Menschen betroffen waren, die Nutzung einer Software mit einer bekannten Schwachstelle, die bereits in einer neueren Version vorlag. Es ist jedoch aus unterschiedlichen Gründen nicht immer einfach und erforderlich, eine Software auf dem neuesten Stand zu halten.
Um zu verstehen, wie aktuell die im Web verwendete Software ist und um die möglichen Auswirkungen auf die Sicherheit zu verstehen, gehen wir folgendermaßen vor:

1. Wir führen eine große Messung auf 5.6M Webseiten durch und analysieren ca. 250 unterschiedliche Softwaretypen – im Zeitraum von 18 Monaten.
2. Wir zeigen, dass 96% der Webseiten mindestens eine veraltete Software nutzen, die meistens mehr als vier Jahre alt sind.
3. Wir zeigen, dass 95% der Webseiten mindestens eine Software einsetzen, für die mindestens eine Schwachstelle existiert.

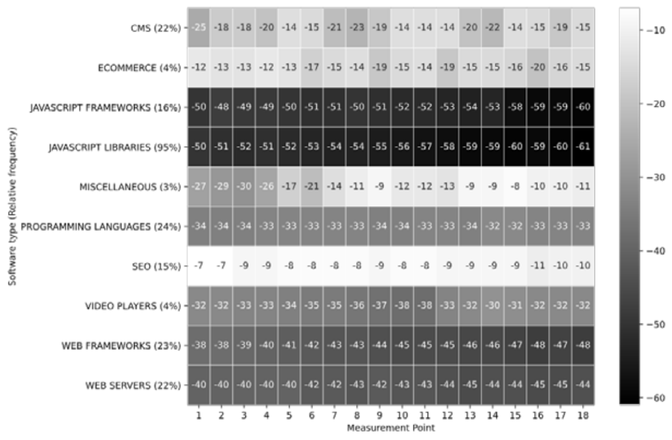

Abb 1:
Das Durchschnittsalter (in Monaten) der am häufigsten verwendeten 10 Softwaretypen für alle Messpunkte. Im Durchschnitt sind die eingesetzte Software mehr als vier Jahre alt und es existieren für diese Software 41 neuere Versionen. Nur bei 6% der Webseiten war alle eingesetzte Software up-to-date.

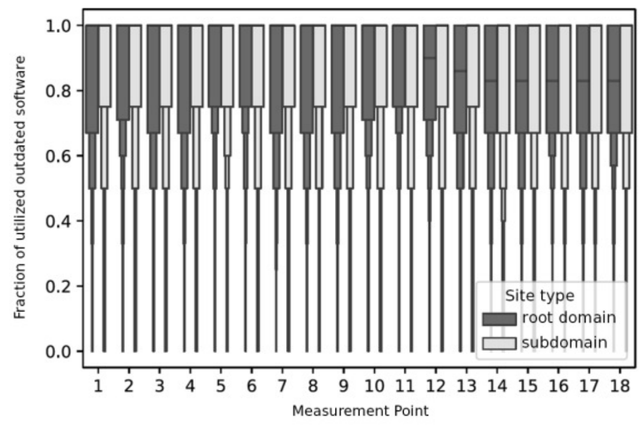

Abb 2:
Bruchteile der verwendeten veralteten Softwareprodukte in den analysierten Webseiten (1 = kein Produkt ist aktuell).
Der größte Teil (~70%) der eingesetzten Software ist bei den Webseiten veraltet. In Subdomains ist der Einsatz von veralteter Software höher.

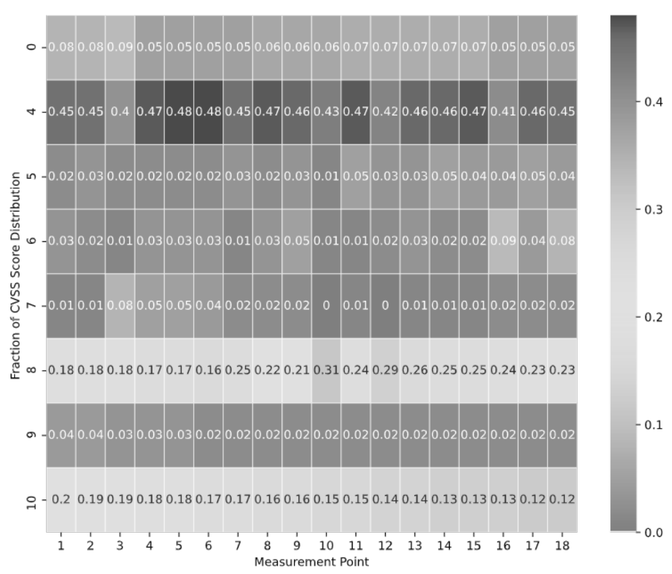

Abb 3:
Verteilung der Schwere der identifizierten Schwachstelle (CVSS-Werte) in Webseiten nach Messpunkten (10 = sehr kritische Schwacshtelle).
Während die Anzahl der Webseiten mit kritischen Schwachstellen sinkt, steigt die Anzahl der Webseiten mit einer Schwachstelle. In unserer letzten Messung (Juni 2020) identifizierten wir bei 12% der Webseiten mindestens eine Software mit einer sehr kritischen Schwachstelle (CVSS=10).

Tab. 1: Top-10-Schwachstellen in unserem letzten Messpunkt (Juni 2020) nach relativer Häufigkeit auf Webseiten.
Die Schwachstelle Cross-site-Scripting ist der am meisten vorkommende Schwachstellentyp und bei 92% der Software und 28% der Webseiten zu identifizieren.

Vulnerability Type (CWE)	Relative Frequency
CWE-79 Improper Neutralization of Input During Web Page Generation (‘Cross-site Scripting’)	0.92
CWE-20 Improper Input Validation	0.32
CWE-400 Uncontrolled Resource Consumption	0.27
CWE-200 Exposure of Sensitive Information to an Unauthorized Actor	0.24
CWE-476 NULL Pointer Dereference	0.24
CWE-601 URL Redirection to Untrusted Site (‘Open Redirect’)	0.22
CWE-125 Out-of-bounds Read	0.22
CWE-119 Improper Restriction of Operations within the Bounds of a Memory Buffer	0.20
CWE-787 Out-of-bounds Write	0.19
CWE-190 Integer Overflow or Wraparound	0.17
CWE-284 Improper Access Control	0.17

Wir zeigen, dass ältere Software mehr kritische Schwachstellen haben und dass die Durchführung eines Updates einen signifikanten Effekt auf Sicherheit hat. Nach Durchführung eines Updates hat sich die Schwere der Schwachstellen (CVSS) im Schnitt von 6.5 (Medium) auf 2.4 (LOW) gesenkt.

Kontakt

Prof. Dr. (TU NN) Norbert Pohlmann
Tel. +49 209 9596-515
E-Mail: norbert.pohlmann@w-hs.de

Nurullah Demir
Tel. +49 209 9596-515
E-Mail: demir@internet-sicherheit.de

Institut für Internet-Sicherheit – if(is)
E-Mail: information@internet-sicherheit.de
Tel.: +49 209 9596-515
www.internet-sicherheit.de

Westfälische Hochschule
Neidenburger Straße 43
45897 Gelsenkirchen
www.w-hs.de

if(is) internet-sicherheit