

Die Gefahr von Sicherheits-Updates am Beispiel von TYPO3

Am Mittwoch, dem 11.02.09, wurde die Webseite des Bundesinnenministers Dr. Wolfgang Schäuble Ziel eines Defacements, also der mutwilligen Verunstaltung durch Hacker. Tags darauf hat der Fußballspieler Kevin Kurányi auf der Vereinshomepage des FC Schalke 04 von seiner Freistellung erfahren – ebenfalls durch Hacker initiiert. Eine Studie des Instituts für Internet-Sicherheit zeigt auf, dass weitaus mehr als die beiden genannten Webseiten Opfer derselben Attacke werden können.

Über TYPO3

Das Content-Management-System TYPO3 ist ein Framework zur Erstellung von Webseiten. Es basiert auf der Skriptsprache PHP und ist unter der GPL für freie Software lizenziert. Die Software wird von einer großen Community auf der ganzen Welt eingesetzt und aktiv weiterentwickelt. Ein eigens für die Sicherheit in TYPO3 eingesetztes Team arbeitet ständig an Sicherheits-Updates und veröffentlicht diese regelmäßig in sogenannten „Security Bulletins“ (engl. etwa „Sicherheitsberichte“).

Die Chronik des „Security Bulletin TYPO3-SA-2009-02“

- **Montag, 09.02.09**
Ein Newsletter [1] wird vom TYPO3-Sicherheitsteam verschickt, welcher ein kritisches Sicherheits-Update ankündigt. So soll ein schwerwiegendes Loch im Kern der Software aufgedeckt worden sein, durch welches beliebige Dateien der TYPO3-Installation von Unbefugten betrachtet werden können (Information Disclosure und Cross-Site Scripting).
- **Dienstag, 10.02.09**
TYPO3 veröffentlicht auf seinen Internetseiten einen neuen Security Bulletin [2] zusammen mit Sicherheits-Updates für eine Vielzahl an Versionen der TYPO3-Software. Die Entwickler raten jedem Nutzer von TYPO3, die Sicherheits-Updates so schnell wie möglich zu installieren. Denn eine Veröffentlichung eines Sicherheits-Updates zieht zwangsweise auch die Publizierung des Fehlers in der Software mit sich.
- **Mittwoch, 11.02.09**
Das erste prominente Opfer des Lecks – oder des Sicherheits-Updates – ist schnell gefunden. Bislang Unbekannte haben die Internetseiten des Bundesinnenministers Dr. Wolfgang Schäuble gehackt und Werbung für eine Kampagne gegen Vorratsdatenspeicherung geschaltet [3]. Kurze Zeit später wurde die Seite vom Netz genommen und erst gegen Ende des Tages, mit einer aktuellen TYPO3-Version, wieder freigeschaltet.
- **Donnerstag, 12.02.09**
Ein zweites prominentes Opfer findet sich. Auch zwei Tage nach offizieller Bekanntgabe der Sicherheitslecks (oder drei Tage, wenn man Abonnent des Newsletters ist) ist die Vereinshomepage des FC Schalke 04 noch nicht auf den neuesten Stand gebracht. Ebenfalls Unbekannte verfassen eine Eilmeldung, dass der Spieler Kevin Kurányi von seinen vertraglichen Pflichten bis auf weiteres befreit wird [4].

Studie zur Lage der „TYPO3-Landschaft“

Waren die Fälle „Schäuble“ und „Schalke“ die einzigen Webseiten, bei denen die Verantwortlichen verpasst haben, zeitnah die veröffentlichten Sicherheits-Updates einzuspielen? Sind durch das Medieninteresse an diesen beiden Fällen auch Webmaster anderer Internetpräsenzen erinnert worden, TYPO3 auf den neuesten Stand zu bringen? Sebastian Feld vom Institut für Internet-Sicherheit hat in einer Studie ermittelt, wie hoch das Vorkommen von ungepatchten TYPO3-Webseiten drei (bzw. vier) Tage nach der Bekanntgabe des Sicherheitslecks ist.

Dazu wurde folgender Versuch in Form eines selbst geschriebenen Programms unternommen:

- Die Suchmaschine Google wird benutzt, um automatisiert an Adressen von Webseiten zu gelangen, die das CMS TYPO3 einsetzen. Das Ergebnis sind 358 Adressen, die im Folgenden analysiert werden.
- Eine auf die entsprechende Sicherheitslücke zugeschnittene Anfrage wird an jede der gefundenen Adressen geschickt. Die Antwort des Webservers gibt Informationen preis, die besagen, ob der Webserver bereits Updates erhielt oder nicht.
- Im Falle eines TYPO3-Systems ohne aktuelle Updates wird vom Programm vermerkt, dass die Webseite potentiell angreifbar ist. Es wird lediglich ein Zähler erhöht, der eigentliche Angriff findet nicht statt. Wenn die Antwort des Webservers besagt, dass die Sicherheits-Updates bereits eingespielt wurden, wird eben hierfür ein Zähler erhöht.

Das Ergebnis der Studie ist wie folgt:

- Zeitpunkt der Analyse: Freitag, 13.02.09
- Dauer der Analyse: Knapp 6 Minuten
- Analysierte Webseiten: 358 (100%)
- Webseiten mit geschlossener Sicherheitslücke: 272 (75,9%)
- Webseiten ohne Sicherheits-Update: 86 (24,1%)

Fazit

Knapp ein Viertel der bei der Studie betrachteten Webseiten sind potentiell verwundbar gegen die veröffentlichte Sicherheitslücke. Diese allein schon hohe Zahl wird noch kritischer mit der Tatsache, dass bereits drei Tage seit der Veröffentlichung des Sicherheits-Updates bzw. vier Tage seit der eigentlichen Ankündigung vergangen sind.

Problematisch gerade bei diesem Sicherheitsleck ist das ungeheure „Kosten-Nutzen-Verhältnis“. Die Komplexität des Angriffs ist simpel im Vergleich zum Effekt, den er bewirkt. So kann ein Angreifer sämtliche Dateien der Webseite einsehen, inklusive den Dateien mit Passwörtern für das TYPO3-InstallTool oder die genutzte Datenbank.

Das Institut für Internet-Sicherheit empfiehlt aus diesem Grunde Updates für Software jeglicher Art schnellstmöglich einzuspielen. Dies gilt sowohl für Frameworks für Internetseiten, als auch für Virens Scanner, Firewall, Betriebssystem und allen weiteren Anwendungen, die Updates anbieten.

Eine weiterer Ratschlag kann in Bezug auf die Wahl von Passwörtern gegeben werden. Auch wenn Passwörter in der Regel verschlüsselt gespeichert sind, kann eine Analyse der gestohlenen verschlüsselten Version des Passworts auch zum Erfolg führen. Dies ist der Fall, wenn das gewählte Passwort entweder kurz ist, aus Begriffen besteht oder leicht zu erraten ist. Schwieriger zu knackende Passwörter sind mindestens 10 Stellen lang, bestehen aus Buchstaben, Zahlen und

Sonderzeichen und geben keinen Rückschluss auf den Inhaber des Passworts. Es heisst, das Passwort zu den Internetseiten von Herrn Schäuble lautete „gewinner“ [3].

Abschließend sei eine Empfehlung für Webseitenbetreiber gegeben, die TYPO3 einsetzen. Auch wenn die Updates umgehend eingespielt wurden und anscheinend keine Attacke stattgefunden hat, so können Angreifer Dateien mit verschlüsselten Passwörter gesammelt haben. Diese werden in den nächsten Tagen „in aller Ruhe“ analysiert und unter Umständen geknackt. Sind die Passwörter nicht geändert, so kommt ein Angreifer trotz Sicherheits-Updates auf das System.

[Update vom 25.02.09]

Die Studie hat im ersten Durchgang der Analyse ergeben, dass auf 86 der 358 analysierten Webseiten noch keine Sicherheits-Updates eingespielt wurden. Das bedeutet, dass 3 Tage nach Veröffentlichung der Updates 24,1% der betrachteten Webseiten ungeschützt waren. Die Analyse wurde nochmals am 17.02.09 mit derselben Menge an Webseiten durchgeführt, erneut ist das Ergebnis ernüchternd. Genau eine Woche nach Bekanntgabe der Sicherheits-Updates sind noch 80 Webseiten ungeschützt (22,3%). Ein letzter Durchgang wurde am 25.02.09 durchgeführt. Mehr als zwei Wochen sind nun vergangen, aber immer noch sind 70 der 358 betrachteten Webseiten noch nicht aktualisiert (19,5%).

[1] – <http://lists.netfielders.de/pipermail/typo3-announce/2009/000111.html>

[2] – <http://typo3.org/teams/security/security-bulletins/typo3-sa-2009-002/>

[3] – <http://www.heise.de/security/Website-von-Wolfgang-Schaeuble-ueber-Typo3-Luecke-gehackt-Update--/news/meldung/132315>

[4] – <http://www.taz.de/1/leben/internet/artikel/1/hacker-feuern-kuranyi-schalke-nicht/>

B.Sc. Sebastian Feld

if(is) – Institut für Internet-Sicherheit, FH Gelsenkirchen

feld (at) internet-sicherheit (punkt) de

<https://www.internet-sicherheit.de>