Auszug Whitepaper „Sicherheit für Blogs und PHP“

ANGRIFFSVEKTOREN GEGEN BLOGS

Ohne Blogs und dynamische Webseiten ist das heutige Internet undenkbar. Dank dynamischer Content Management Systeme (CMS) und fertiger Blogsysteme kann jeder, der etwas im Internet teilen möchte, innerhalb kürzester Zeit die notwendige Infrastruktur aufsetzen. Eines der bekanntesten Systeme ist Wordpress, das vor kurzem zehn Jahre alt wurde. Ohne diese Software wäre die aktuelle Blogging-Szene wohl kaum so stark geworden. Wordpress und andere Blogging-Systeme lassen sich einfach installieren und dank eines Erweiterungssystems mit neuen Funktionen oder anderen „Themes“ ausrüsten. Das Problem dabei: Viele Nutzer vergessen, dass sie nicht nur eine simple Webseite, sondern ein ausgewachsenes Content Management System verwenden, das Angreifern im Zweifel umfangreiche Möglichkeiten zur Verfügung stellt, um Blogs zu infizieren und für ihre Zwecke zu missbrauchen.

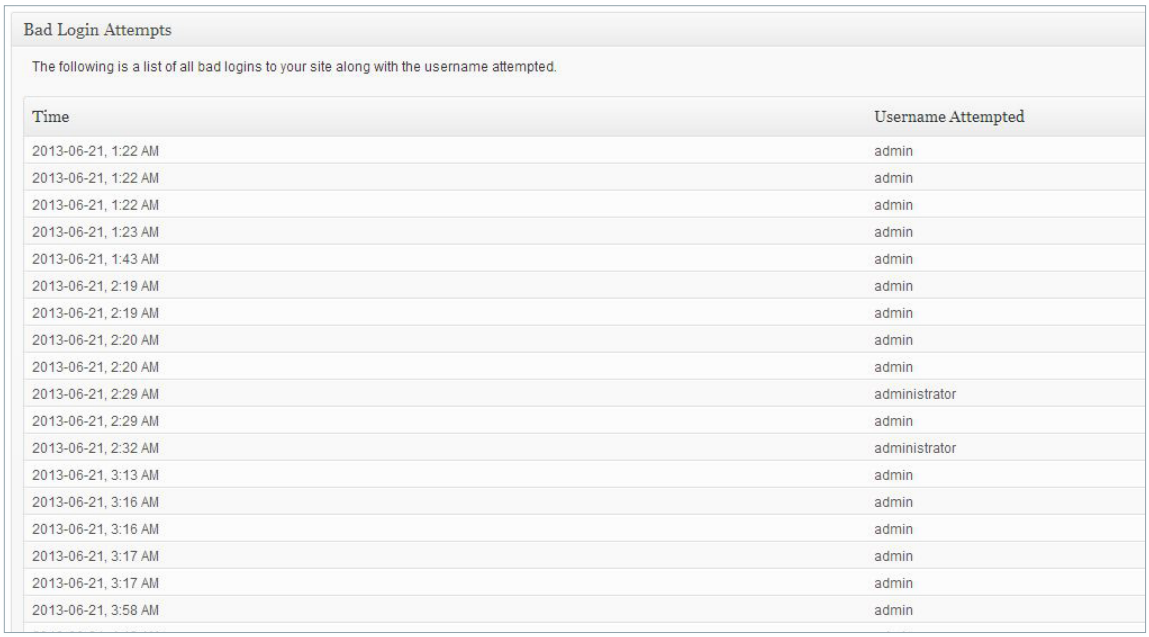
Blogs sind Content Management Systemen sehr ähnlich und daher auch ähnlich angreifbar

Wie jede Software, so enthalten auch Content Management Systeme Schwachstellen. In Wordpress wurden beispielsweise seit 2004 über 200 solcher Fehler gefunden. 47 davon ermöglichten es Angreifern, eigenen Code auf dem System auszuführen. Laut der Seite CVE Details [1] sind zudem alleine für Wordpress mindestens 43 fertige Attacken, so genannte Exploits [2], bekannt. Ähnlich sieht es bei anderen Systemen aus: Für Drupal [3] etwa listet die Seite mehr als 100 bekannte Schwachstellen, in Typo3 [4] fanden sich bislang über 150 Lücken. Dabei ist wichtig zu erwähnen, dass die aktuellen Versionen der jeweiligen Programme gegen Attacken schützen, die diese bekannten Schwachstellen nutzen (mehr dazu später). Dieser Beitrag nutzt Wordpress als praktisches Beispiel, die meisten Tipps und Vorgehensweisen lassen sich aber problemlos auf andere Systeme übertragen.

Massenattacken

Aufgrund seiner Popularität wurde Wordpress bereits mehrfach das Ziel von automatisierten Massenattacken. Im April 2013 erreichten diese Angriffe einen unrühmlichen Höhepunkt. Die Angreifer nutzten ein Botnet von mehr als 90.000 Rechnern, um die Admin-Zugänge zu Wordpress-Installationen zu knacken.

Vorsicht vor automatisierten Attacken und bekannten Schwachstellen



Bad Login Attempts

The following is a list of all bad logins to your site along with the username attempted.

Time	Username Attempted
2013-06-21, 1:22 AM	admin
2013-06-21, 1:22 AM	admin
2013-06-21, 1:22 AM	admin
2013-06-21, 1:23 AM	admin
2013-06-21, 1:43 AM	admin
2013-06-21, 2:19 AM	admin
2013-06-21, 2:19 AM	admin
2013-06-21, 2:20 AM	admin
2013-06-21, 2:20 AM	admin
2013-06-21, 2:29 AM	administrator
2013-06-21, 2:29 AM	admin
2013-06-21, 2:32 AM	administrator
2013-06-21, 3:13 AM	admin
2013-06-21, 3:16 AM	admin
2013-06-21, 3:16 AM	admin
2013-06-21, 3:17 AM	admin
2013-06-21, 3:17 AM	admin
2013-06-21, 3:58 AM	admin

Automatisierte Attacken testen vor allem bekannte Standardinformationen, etwa den Admin-Account. Entsprechend sollte man Standardkonten sofort ändern und/oder deaktivieren.

Eine andere Taktik ist das Ausnutzen einer bekannten Schwachstelle [2]. Diese werden beispielsweise dann bekannt, wenn Entwickler der Blog-Systeme ein Update veröffentlichen und die Änderungen beschreiben. Die Angreifer programmieren anschließend eine Software, die sich durchs Web frisst und verwundbare Installationen sucht. Ähnlich wie die Spider-Programme von Suchmaschinen hangelt sie sich dabei von Link zu Link, bis sie auf eine Webseite trifft, auf welcher die bekannte Schwachstelle enthalten ist. Dort angekommen startet das Programm die Attacke und verschafft sich Zugang zur Blog-Installation. Anschließend sucht die Malware weitere verwundbare Installationen und das Spiel beginnt von vorne. Wenn Sie also Schlagzeilen wie „100.000 Installationen von XX gehackt“ lesen, dann handelt es sich mit hoher Wahrscheinlichkeit um eine solche automatisierte Attacke.

Haben Hacker die Admin-Rechte des Blogs erlangt, wird es brandgefährlich

Nach der erfolgreichen Übernahme verfügen die Angreifer über die gleichen Rechte wie ein regulärer Admin-Nutzer – und das nutzen sie entsprechend aus. Bei Massenattacken geht es meist darum, ein Netz von Servern zu schaffen, das entweder als Datenlager für bösartige Programme dient oder die Besucher mit Malware infiziert. Das bedeutet auch, dass es sich für diese Angreifer lohnt, möglichst jede Webseite und jede Blog-Installation zu übernehmen. Egal ob es sich um den Firmenblog eines Unternehmens, den Reise-Blog eines Urlaubers oder den privaten Blog einer Familie handelt – alle Webseiten bieten Ressourcen, auf die es die Kriminellen abgesehen haben: Besucher, Traffic und Bandbreite. Angreifer, die diese Strategie verfolgen, handeln meist ähnlich wie die Betreiber von Botnets: Ihnen geht es darum, dass die offiziellen Besitzer der Seiten keinen Verdacht schöpfen und so ihre Webseiten ungewollt möglichst lange als Ressource zur Verfügung stellen.

Sonderfall Defacement

Defacement = digitaler Vandalismus

Das gilt allerdings nicht beim sogenannten „Defacement“. Die Angreifer verschaffen sich Zugang zu den Webseiten, manipulieren oder löschen die legitimen Informationen und ersetzen die eigentliche Webseite durch eigene Inhalte. Meist handelt es sich dabei um mehr oder weniger politische Aktionen, mit denen die Aktivisten auf ihrer Meinung nach massive Missstände hinweisen wollen. Oftmals handelt es sich dabei um Skript-Kiddies, also Möchtegern-Hacker, die fertige Baukästen nutzen, um möglichst viel digitalen Vandalismus anzurichten.

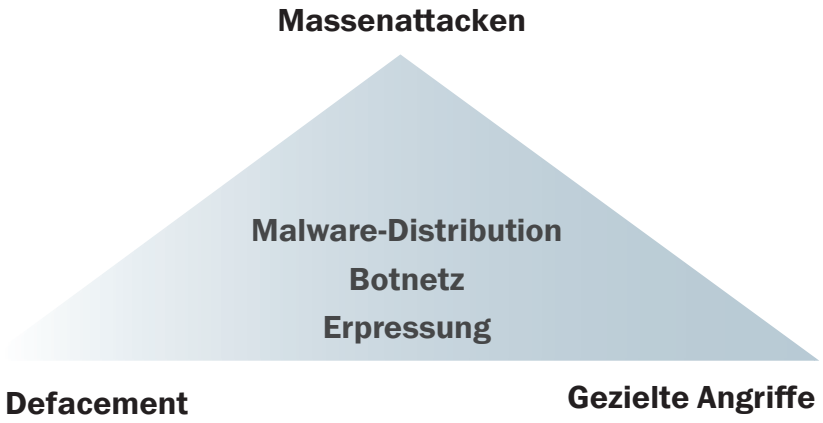
Für die Besitzer von Webseiten sind Defacements oft ärgerlicher als „normale“ Attacken. Denn hier geht es darum, größtmögliche Aufmerksamkeit oder Schaden anzurichten. Häufig löschen oder überschreiben die Angreifer einfach alles, was sie auf dem Server vorfinden.

Ein Beispiel für ein Massen-Defacement: Die Angreifer setzen hier auf automatisierte Baukästen, die anfällige Installationen automatisch mit solchen Protestnachrichten „aufhübschen“.

Gezielte Angriffe

Im Gegensatz zur Masseninfektion haben gezielte Attacken meist nur eine oder wenige Webseiten im Visier. Hier geht es in der Regel darum, einem Unternehmen Schaden zuzufügen oder durch die Übernahme eines Blogs oder einer Webseite weitere Angriffe vorzubereiten. Ähnlich wie bei gezielten Phishing-Attacken kundschaften die Angreifer das Ziel oft lange und ausführlich aus, um dann zuzuschlagen, wenn sich eine Möglichkeit bietet.

Gezielte Blog-Attacken funktionieren wie zielgerichtetes Phishing



Angriffsvektoren und Ziele: Mittels Massenattacken, „Defacements“ und gezielten Angriffen können Cyberkriminelle Schädlinge verbreiten, Botnetze aufbauen und Blogbetreiber erpressen.

Quellen:
[1] http://www.cvedetails.com/vendor/2337/Wordpress.html‘
[2] http://www.viruslist.com/de/analysis?pubid=200883806
[3] http://www.cvedetails.com/product/2387/Drupal-Drupal.html?vendor_id=1367
[4] http://www.cvedetails.com/vendor/3887/Typo3.html

Dieser Text ist Teil des Kaspersky-Whitepapers „Sicherheit für Blogs und PHP - Wordpress und Co. vor Hackern schützen“. Das Whitepaper ist unter http://www.kaspersky.com/de/downloads/pdf/kaspersky_whitepaper_blogs_und_security_final.pdf abrufbar oder kann bei kaspersky@essentialmedia.de per E-Mail angefragt werden.