KASPERSKY lab

Sicherheit für Blogs und PHP

WORDPRESS UND CO. VOR HACKERN SCHÜTZEN

Autor: Christian Funk, Senior Virus Analyst bei Kaspersky Lab

Inhalt

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

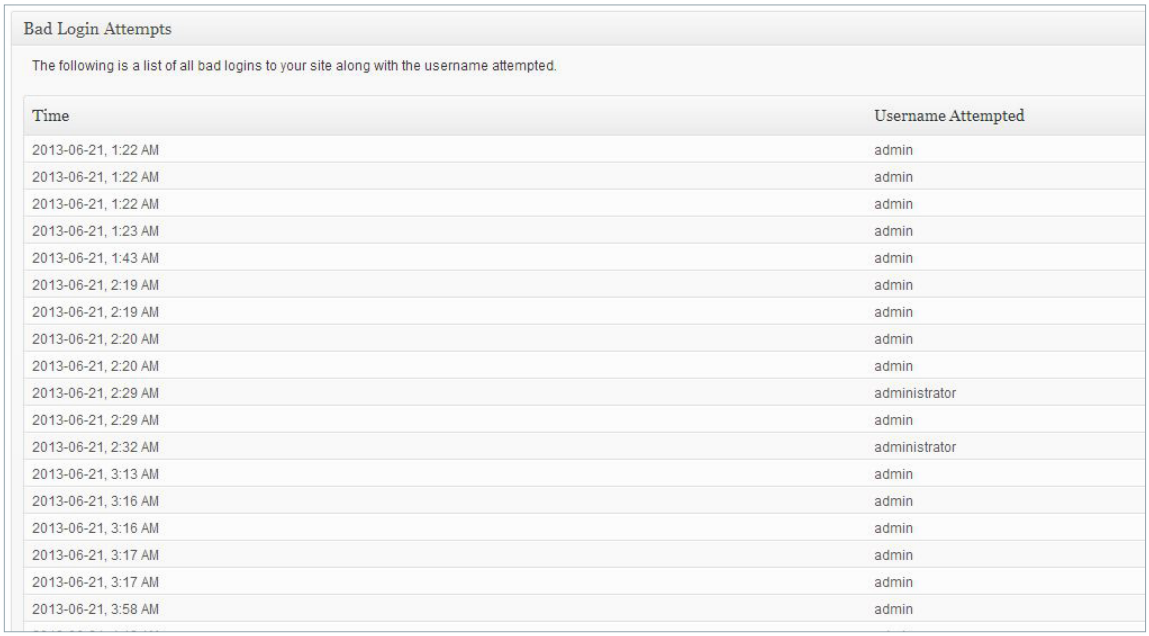
Ohne Blogs und dynamische Webseiten ist das heutige Internet undenkbar. Dank dynamischer Content Management Systeme (CMS) und fertiger Blogsysteme kann jeder, der etwas im Internet teilen möchte, innerhalb kürzester Zeit die notwendige Infrastruktur aufsetzen. Eines der bekanntesten Systeme ist Wordpress, 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.
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.

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,

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

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

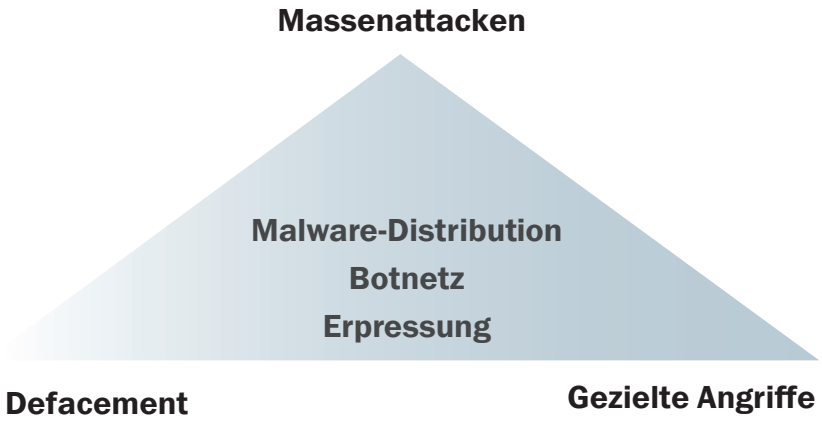
Das gilt allerdings nicht beim sogenannten „Defacement“. Die Angreifer verschaffen sich Zugang zu den Webseiten, manipulieren oder löschen die legitimen Informationen und ersetzen die eigentliche Webseite durch eigene Inhalte. Meist handelt es sich dabei um mehr oder weniger politische Aktionen, mit 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

Gezielte Blog-Attacken funktionieren wie zielgerichtetes Phishing

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.



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

Gegenmaßnahmen nach Attacken

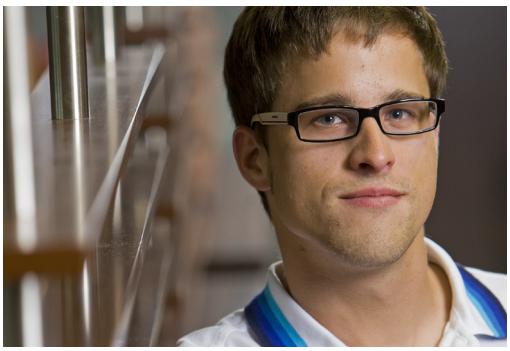
Wenn man Opfer eines Angriffs wurde, sollte man zunächst Ruhe bewahren und keine überstürzten Aktionen starten. Im ersten Schritt sollte der betroffene Server offline genommen und die Seite durch eine einfache, statische HTML-Seite ersetzt werden. Wichtig: Wer Anzeige erstatten will, der sollte als Erstes einen Experten für Forensik hinzuziehen, der Beweise so sichern kann, dass diese von den Strafverfolgungsbehörden verwertet werden können.

In jedem Fall sollte der Betroffene zunächst alle lokalen Systeme mit einem Virenscanner checken [5]. Nur so lässt sich sicherstellen, dass die eigenen Systeme sauber sind. Anschließend empfiehlt es sich, einen Experten, etwa vom Webspace-Anbieter, hinzuzuziehen, der bei der Reinigung des Blogs hilft. Oftmals ist es enorm schwer, alle infizierten Elemente zu finden und zu entfernen. Eine gute Anlaufstelle sind die Support-Seiten des jeweiligen Blog-Anbieters, Wordpress etwa hat eine umfangreiche FAQ zu dem Thema zusammengestellt [6]. Im nächsten Schritt sollten alle Passwörter geändert werden [7], um den Zugang zum Webinterface, FTP- und Datenbankserver zu schützen.

Das Erste-Hilfe-Set nach einer Attacke: Computer scannen, Blog reinigen, Passwort ändern und Backup nutzen

Wer auf ein aktuelles Backup zurückgreifen kann, hat es relativ leicht: Damit kann man den rabiaten Weg gehen und die Inhalte des Webspaces und der Datenbank einfach löschen. Anschließend sollte der Blog komplett neu aufgesetzt und das letzte Backup eingespielt werden. Für Wordpress wird das auf dieser Seite erklärt [8].

Ohne Backups wird es dagegen schwer: Zunächst sollten alle Daten auf einem lokalen System gesichert werden. Bei Opfern einer Defacement-Attacke könnten die wichtigen Daten noch vorhanden sein. Das Füttern einer passenden Suchmaschine mit der Nachricht oder dem Namen der Angreifer und Begriffen wie „Gegenmaßnahmen“, „Clean“ oder „Help“ ergeben gute Tipps. Oft finden sich hier entsprechende Anleitungen, mit denen zumindest die eigene Seite wiederhergestellt werden kann.



KASPERSKY-EXPERTE CHRISTIAN FUNK EMPFIEHLT: SCHUTZ DURCH VORSORGE

Schutz und Vorsorge

Besser als Aufräumen nach der Attacke ist das Verhindern der Attacke an sich. Tatsächlich kann man mit ein paar einfachen Regeln die Angriffsfläche auf den eigenen Blog deutlich verringern und vor allem Massenattacken und Defacements wirkungsvoll verhindern.

Blogs schützt man am besten präventiv

Die wichtigste Regel lautet: Updates. Egal ob es sich um eine neue Version des Blogsystems, eines Plugins oder eines Themes handelt, sobald die Macher eine Aktualisierung zur Verfügung stellen, sollte diese schnellstmöglich installiert werden. Der Grund dafür ist oben beschrieben: Spätestens wenn eine behobene Schwachstelle dokumentiert wurde, werden Angreifer diese in ihre Programme integrieren. Allerdings sollte man sich hier nicht in Sicherheit wiegen: Selbst bevor Schwachstellen offiziell bekannt werden, können diese den Kriminellen bereits bekannt sein.

Der nächste Schritt ist das Abhärten der Web-Applikation. Hinter diesem Begriff verstecken sich bewährte Mittel und Wege, um die eigene Angriffsfläche weiter zu verringern. Für Word-

press haben die Macher eine umfangreiche Dokumentation [9] zusammengestellt, für alle anderen Systeme gibt es ähnliche Anleitungen. Im Zweifel hilft eine Suche nach „System-name + Hardening“.

Folgende Punkte gelten für die meisten Systeme:

- Verbergen Sie die Versionsnummer: So haben Angreifer eine deutlich kleinere Chance, mit automatisierten Skripten herauszufinden, ob Ihr System veraltet ist.
- Ignorieren Sie den Standard-Admin-Nutzer: Dieser ist meist sehr gut dokumentiert, entsprechend einfach können ihn Kriminelle abfragen. Besser ist es, den eigentlichen Admin-Account nach der Installation einzumotten oder zu deaktivieren und einen dedizierten, neuen Account anzulegen.
- Nutzen Sie die verfügbaren Rechtestufen: Nicht jeder Nutzer benötigt einen Vollzugriff. Selbst wenn Sie Ihren Blog alleine führen, sollten Sie bei alltäglichen Aufgaben einen Account mit möglichst wenig Rechten verwenden. Denn Vollzugriff benötigen Sie eigentlich nur für Updates des Systems.
- Achten Sie auf Berechtigungen: Oftmals müssen nicht alle Daten auf dem Webserver von jedermann les- und schreibbar sein. Beschäftigen Sie sich mit den notwendigen Berechtigungen und passen Sie diese für Ihre Installation an.
- Je weniger Plugins, desto besser: Jedes Plugin öffnet potenziell einen neuen Weg in Ihr System. Achten Sie darauf, möglichst wenige Erweiterungen zu installieren. Unnötige Erweiterungen sollten Sie zumindest deaktivieren, idealerweise sogar löschen.
- Updates, Updates, Updates: Installieren Sie Aktualisierungen, sobald diese verfügbar sind. Achten Sie zudem darauf, dass alle verwendeten Plugins und Themes aktiv weiterentwickelt werden – nichts ist schlimmer, als auf veraltete Software zu setzen.
- Nutzen Sie Sicherheits-Plugins: Eine Ausnahme von der „möglichst wenig Erweiterungen“-Regel stellen Sicherheits-Plugins dar. Diese können oftmals viele der Best-Practices automatisch durchführen und den eigenen Blog gegen Angreifer schützen (siehe Bilder unten).
- Backups: Nutzen Sie die Funktionen Ihres Systems, um in regelmäßigen Abständen Sicherungen anlegen zu lassen. Dadurch können Sie im Falle einer Attacke Ihr System schneller wieder zum Laufen bringen.

Erweiterungen wie Better Security für WordPress integrieren eine ganze Reihe von Best-Practice-Ansätzen für die Sicherung der Website.

Einmal eingerichtet blockieren Sicherheitserweiterungen fehlerhafte Zugriffe automatisch.

Schutz für PHP

PHP-Seiten sind bei Unternehmen beliebt, aber auch leicht angreifbar

Nicht jedes Unternehmen setzt zwingend auf ein komplettes Content Management System, einige entscheiden sich lieber für ein PHP-basiertes System, um die eigene Webseite zu betreiben oder Dienste zur Verfügung zu stellen. Das hat zunächst den Vorteil, dass man gegen Attacken auf verwundbare Blogging-Plugins geschützt ist. Allerdings ist auch PHP keineswegs eine uneinnehmbare Festung für Angreifer, im Gegenteil. Seit 2000 listet CVE Details [10] über 340 gefundene Schwachstellen und mindestens 41 Exploits auf.
Attacken auf PHP finden daher ebenso statt, wie Angriffe auf Blog-Systeme. Das liegt auch daran, dass man bei einer erfolgreichen Attacke auf PHP umfassende Rechte auf dem Zielsystem erhält, da PHP den Unterbau für interaktive Seiten und Systeme liefert. Wer also eine erfolgreiche Attacke entwickelt, kann diese für zahlreiche Webseiten und -Dienste nutzen.

Entsprechend müssen auch PHP-basierte Anwendungen gegen bösartige Besuche geschützt werden. Die wichtigste Regel ist auch hier die Aktualisierung von Komponenten. Egal ob PHP oder unterstützende Programme wie etwa ImageMagick: Sobald neue Versionen erhältlich sind, sollten die Verantwortlichen diese schnellstmöglich in Update-Pläne aufnehmen, um bekannte Schwachstellen zu schließen und die eigene Angriffsfläche zu minimieren.

Schritt Nummer 2 ist das Härten der PHP-Installation. Ähnlich wie bei Wordpress gibt es zahlreiche Anleitungen und Ressourcen zum Thema PHP Hardening. Einen ersten Ansatz liefert dafür die offizielle Dokumentation [11], zahlreiche andere Ressourcen im Web sind nur eine einfache Suchanfrage entfernt.

Fazit

Kaspersky Lab empfiehlt drei Denkansätze zur Blog-Sicherheit

Der Schutz der eigenen Web-Anwendung, sei es ein Wordpress-Blog, ein Foren-System oder eine selbst gebaute PHP-Anwendung, muss von Anfang an in die Konzeption einfließen. IT-Security ist nichts, das man nachträglich „anflanschen“ kann, nur wenn sie von Anfang an tief mit dem System verzahnt ist, kann sie wirklich schützen.

Unabhängig vom System helfen diese drei Denkansätze:

- Zugriff minimieren: Jeder Nutzer sollte nur so viele Rechte erhalten, wie er zur Ausführung seiner Aufgaben benötigt. Zu dieser Regel gehört auch, dass keine allgemein zugänglichen Admin-Konten existieren, die man „schnell mal aus Zeitersparnis“ nutzen kann. Jede Aktion eines jeden Nutzers muss stets klar zuzuordnen und nachvollziehbar sein.
- Begrenzung: Nicht jeder benötigt alle Funktionen, die PHP, Wordpress und Co. zur Verfügung stellen. Es schadet nicht, eine genaue Inventur der jeweils verfügbaren Funktionen vorzunehmen und alle Unnötigen zu deaktivieren. Das verringert die Angriffsfläche und so die Chance für Attacken enorm. Das ist keine Einzelaktion, sondern ein Prozess, der regelmäßig – spätestens beim Erscheinen einer neuen Programmversion – wiederholt werden muss.
- Vorbereitung und Wissen: Selbst wenn eine Attacke erfolgreich ist, kann ein etablierter Backup-Prozess den Schaden eingrenzen und minimieren. Entsprechend ist es wichtig, diese Strategie frühzeitig zu etablieren und regelmäßig zu überprüfen. Dazu zählt auch eine Kontrolle der Backups, ob diese vollständig und fehlerfrei sind. Zudem müssen sich die Verantwortlichen über Aktualisierungen und neue Schwachstellen in den verwendeten Produkten auf dem Laufenden halten.

Wer sich diese Funktionen nicht zutraut oder schlicht keine Zeit hat, alle Aufgaben selbst durchzuführen, muss seinen Traum vom eigenen Blog nicht aufgeben. Allerdings sollte man dann genau überlegen, wo man die Seite aufsetzt. Für den Anfang könnte es etwa reichen, ein gehostetes Blog-System beim Anbieter zu nutzen, Wordpress bietet das etwa unter Wordpress.com an. Alternativ gibt es Webspace-Anbieter, die sich exakt auf den sicheren Betrieb solcher Webseiten spezialisiert haben. Diese bieten oftmals auch die Möglichkeit einer White-Labeled-Installation, so dass sich der Blog nahtlos in die Webseite des Unternehmens integriert.

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
[5] http://www.kaspersky.com/de/home_user
[6] http://codex.wordpress.org/FAQ_My_site_was_hacked
[7] http://www.kaspersky.com/de/news?id=207566607
[8] http://codex.wordpress.org/Restoring_Your_Database_From_Backup
[9] http://codex.wordpress.org/Hardening_WordPress
[10] http://www.cvedetails.com/product/128/PHP-PHP.html?vendor_id=74
[11] http://www.php.net/manual/de/security.php