BSI-Studie

Portale sicher betreiben

[17.10.2013] Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat eine Studie zur Sicherheit von Content-Management-Systemen veröffentlicht. Demnach lassen sich Internet-Seiten auf Basis von Open-Source-Lösungen weitgehend sicher betreiben.

Auf Content-Management-Systemen (CMS) basierende Web-Seiten sind nach wie vor ein beliebtes Angriffsziel für Hacker. Schon eine einzelne Sicherheitslücke ist eine latente Gefahr für hunderte oder tausende Websites. So etwas wie absolute Sicherheit gibt es angesichts der über ausreichend Zeit, Mittel und Wege verfügenden Angreifer nicht. Zielführender ist es, relative Sicherheit anzustreben. Denn ein geringer sicherheitstechnischer Vorsprung lässt sich meist schon mit regelmäßigen Sicherheitsupdates erreichen und bietet hinreichend Schutz gegen alle Angreifer, die mit geringem Aufwand irgendein Ziel schädigen wollen. Leichte Beute identifizieren Hacker meist mit Werkzeugen, die das Internet nach anfälligen Seiten durchsuchen und eine Auswahl lukrativer Opfer präsentieren. Um Seitenbetreiber beim Erreichen eines relativen Sicherheitsniveaus zu unterstützen, veröffentlichte das Bundesamt für Sicherheit in der Informationstechnik (BSI) kürzlich die Sicherheitsstudie Content-Management-Systeme. Die von der Firma init und dem Fraunhofer-Institut für Sichere Informationstechnologie SIT durchgeführte Studie leistet wichtige Grundlagenarbeit im Bereich der CMS-Sicherheit und untersucht die weit verbreiteten Open-Source-Systeme Drupal, Joomla!, Plone, TYPO3 und WordPress. Um nicht nur eine Aussage über den Zustand eines Systems zu einem bestimmten Zeitpunkt machen zu können, sondern die Sicherheit längerfristig einschätzen zu können, konzentrierten sich die Autoren der Studie auf die Entwicklung eines robusten Kriterienkatalogs, der eine detaillierte Beurteilung der CMS ermöglicht. Die Ergebnisse zeigen für jedes System sehr differenziert, wie Sicherheitsbelange in den unterschiedlichen Phasen des Software-Entwicklungslebenszyklus berücksichtigt werden – von der Konzeption über die Software-Erstellung, die Integration bestehender Back-End-Systeme bis hin zum späteren Betrieb. Die Kriterien werden auf vier typische Szenarien angewendet: Private Event Site, Bürgerbüro einer kleinen Gemeinde, Open Government Site einer Kleinstadt und mittelständisches Unternehmen mit mehreren Standorten.

Zentrale Ergebnisse der Studie

Im Fokus der Studie stand eine umfangreiche Analyse der bekannten Bedrohungslagen für die betrachteten Content-Management-Systeme. Den Ausgangspunkt bildete die Untersuchung gemeldeter und von den Open-Source-Projekten anerkannten Schwachstellen. Dafür wurde die National Vulnerability Database (NVD) der US-amerikanischen Standardisierungsbehörde NIST herangezogen. In ihr werden alle nachvollziehbaren Schwachstellen mit eindeutigem Identifikator geführt. Die Vermutung lag nahe, dass jene Systeme, welche bei der Beurteilung der Sicherheitskriterien gut abschneiden würden, die wenigsten Schwachstellen aufweisen würden. Im Rückblick erwies sich die Selektion und Zuordnung aber als schwierig. Die Standardisierung der gemeldeten Schwachstellen reicht gegenwärtig noch nicht aus, um daraus Rückschlüsse auf künftige Risiken beim Einsatz des jeweiligen Systems zu ziehen. Sehr aufschlussreich waren hingegen die von den Open-Source-Projekten veröffentlichten Advisories. Sie lassen sehr schnell erkennen, in welcher Frequenz SicherheitsUpdates notwendig sind, wie kritisch Lücken von der Entwickler-Community eingeschätzt und wie gut diese dokumentiert werden. Das zentrale Ergebnis der Studie: Alle betrachteten Open-Source-Systeme besitzen ein angemessenes Sicherheitsniveau und haben nachweislich einen Sicherheitsprozess zur Behebung von Schwachstellen

implementiert. Tatsächlich entspricht die Umsetzung eines solchen Sicherheitsprozesses dem aktuellen Stand der Technik, den selbst viele kommerzielle Software-Pakete nicht erreichen. Sicherheitsrelevante Unterschiede zwischen den betrachteten CMS ergeben sich vor allem aus dem Konfigurationsaufwand bei der Erstinstallation und dem Einspielen von Patches. Ein CMS zu konfigurieren ist aufwändiger als die Installation einer spezialisierten Web-Applikation. Denn das CMS liefert lediglich eine Basisinstallation, die sehr genau an die verschiedenen Anwendungsfälle und Rahmenbedingungen angepasst werden muss. Deshalb steht und fällt die effektive Sicherheit einer Website mit der Sorgfalt bei der Konfiguration und der Auswahl der Erweiterungen.

Empfehlungen für einen sicheren Betrieb

Die positive Bewertung der Open-Source-CMS darf nicht darüber hinwegtäuschen, dass keines der betrachteten Systeme unbeobachtet oder durch einen unbedarften Anwender betrieben werden kann. Die Studie empfiehlt täglich 15 Minuten professionelle CMS-Pflege pro Website. Erst dann sind die Systeme sicherheitstechnisch weitgehend gebrauchstauglich. Um den Aufwand für eine nachhaltig sichere CMS-Konfiguration, ein professionelles System-Management und regelmäßige Security Reviews überschaubar zu halten, greifen Entwickler in der Regel auf bewährte Hard- und Software-Bausteine zurück. Die Studie diskutiert diesen Ansatz anhand geeigneter Module und Konfigurationen in den vier genannten Anwendungsszenarien.
Content-Management-Systeme unterliegen dem permanenten Wettstreit zwischen Exploit-Entwicklern und Security Teams. Vor dem Hintergrund der Handlungsempfehlungen der Studie und angesichts des durch Angriffe entstehenden Schadens, sind intelligente Sicherheitsgateways ein geeignetes Mittel zur Abwehr. Denn jeder Seitenbetreiber ist solange einem latenten Risiko ausgesetzt, bis für eine Sicherheitsschwachstelle ein Bugfix verfügbar ist. Ein intelligentes Sicherheitsgateway, das unveröffentlichte Sicherheitslücken an ungewohnten Kommunikationsmustern erkennt, kann hier eine große Hilfe sein. Diese regelbasierten Firewall-Systeme erkennen von der Norm abweichendes Verhalten und verhindern, dass Websites vor dem Erscheinen von Sicherheits-Updates befallen werden. Ein sehr effektives Werkzeug sind zudem spezialisierte CMS-Sicherheitstests. Einmal gemeinsam mit einem externen Spezialisten zusammengestellt und auf das System abgestimmt, sollten die Penetration-Tests nach jedem CMS-Update durchgeführt werden.

()

Hier können Sie die BSI-Studie herunterladen.

Stichwörter: CMS | Portale, IT-Sicherheit, BSI, Open Source, Studie