МЕТОДЫ И СРЕДСТВА СНИЖЕНИЯ РИСКА СЕТЕВЫХ АТАК ПРИ РАЗРАБОТКЕ И ИСПОЛЬЗОВАНИИ ВЕБ-САЙТОВ В СФЕРЕ ОБРАЗОВАНИЯ

Цалко А.С.[1], Кучинский П.В.[2]

[1] *Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Беларусь, calco@bsuir.by*

[2] *НИИПФП им. А.Н.Севченко БГУ, г. Минск, Беларусь, niipfp@bsu.by*

С каждым годом растет доля сайтов, использующих широко распространенные системы управления содержимым (CMS). В конце 2017 года из 10 миллионов крупнейших веб-сайтов 29 % работают на CMS WordPress[1], что на 3 % выше 2016 года, а значит всё больше разработчиков выбирают данную систему при создании сайтов. ЦИИР БГУИР разрабатывает и обслуживает множество сайтов, в том числе на CMS WordPress. Легкость установки и использования подталкивают к выбору данной системы, но так ли это безопасно?

В декабре 2015 года была найдена критическая уязвимость в системе «Joomla», затрагивающая все использующие данную CMS сайты (около 2.5 миллионов веб-сайтов) [2]. Но как правило, использование самих CMS не несет угрозы. Основная опасность использования популярных систем заключается в расширении функционала веб-сайтов с помощью дополнительных модулей (плагинов) от сторонних разработчиков, не уделяющих проблеме безопасности должного внимания.

Была исследована безопасность веб-сайтов, написанных на скриптовом языке PHP и обслуживаемых ЦИИР БГУИР. Был проведен поиск вредоносного ПО методами сигнатурного сканирования и эвристического анализа исходных файлов веб-сайтов. В результате на небольшом количестве сайтов (менее 50) было найдено более 200 образцов вредоносного программного обеспечения.

В абсолютном большинстве доступ был получен злоумышленниками через популярные системы управления содержимым веб-сайтов и их модули. Веб-сайты и системы, разработанные ЦИИР БГУИР не были скомпрометированы.

С каждым днем вредоносный код (веб-шеллы, скрипты для рассылки спама и т. п.) становится более изощренным и сложным в обнаружении. Кроме обфускации идентификаторов и шифрования кода злоумышленники повсеместно начали использовать неявные вызовы функций посредством методов с callable аргументами, handler'ы и косвенные вызовы функций. Исходный код стараются замаскировать и сделать как можно более изменчивым, «полиморфным» или наоборот, сделать максимально простым и похожим на обычный скрипт. Вредоносное ПО размещается не только в новых файлах, а также и в системных файлах CMS, на которой функционирует сайт. В большинстве случаев это не влияет на работу сайтов, либо влияет незначительно, тем самым усложняя обнаружение атаки администраторами.

В качестве минимизации риска сетевых атак на веб-сайты, использующие популярные системы управления содержимым (CMS) предлагается использовать следующие методы и средства:

– использование сложных паролей к административным панелям любых сайтов и систем;

– ограничение доступа к панелям администрирования, ограничение попыток неудачного входа;

– запрещение регистрации пользователей при возможности;

– запрещение прав редактирования системных файлов CMS;

– запрещение возможности выполнения скриптов в тех папках, права на запись в которых невозможно выставить без сохранения функционирования CMS;

– регулярное создание резервных копий файлов и БД, на разных серверах и хранилищах;

– минимизация использования дополнительных модулей от сторонних разработчиков;

– регулярное обновление самих CMS и модулей к ним;

– осуществление проверки файлов сканерами вредоносного кода (AI-Bolit, maldet, clamav и др.).

Все вышеописанные методы позволяют снизить риск сетевой атаки, но не гарантируют полную безопасность веб-сайтов. Максимально эффективным средством является использование систем обнаружения вторжений (IDS).

Для серверов ЦИИР БГУИР, на которых размещаются сайты, работающие на скриптовом языке PHP была выбрана система OSSEC – хостовая система обнаружения вторжений. С ее помощью были решены задачи проверки контроля целостности файлов, логирования различных действий на серверах, получения событий безопасности (анализ системных журналов) и оповещений об этих событиях.

В результате всех описанных методов и средств удалось существенно повысить безопасность сайтов, использующих популярные системы управления содержимым. Количество успешных сетевых атак злоумышленников значительно снизилось: на том же количестве сайтов за месяц наблюдения не было выявлено успешных атак. Проведенная работа подтверждает актуальность выбранного направления исследования информационной безопасности веб-узлов.

Литература

1. W3Techs, Software Quality Management Consulting [Электронный ресурс]. – Режим доступа: http://w3techs.com/technologies/overview/content_management/all.

2. Sucuri Security, Critical 0-day Remote Command Execution Vulnerability in Joomla [Электронный ресурс]. – Режим доступа: https://blog.sucuri.net/2015/12/remote-command-execution-vulnerability-in-joomla.

3. Wikipedia, OSSEC [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/OSSEC.