Сайты образовательных и научных учреждений пользуются у поисковых систем высоким авторитетом. Материалы, размещенные на таких сайтах, быстрее занимают лидирующие позиции в выдаче поисковых систем. Это автоматически делает такие ресурсы объектом внимания злоумышленников, неправомерно использующих сайты для получения выгоды.

Была проведена начальная работа по разработке комплекса мер и набора методик для защиты сайтов на примере образовательных веб-ресурсов БГУИР. Необходимо было составить список популярных CMS, безопасность которых будет проанализирована в первую очередь. В качестве исследуемой совокупности были выбраны 260 млн сайтов, размещенных на более чем 50 популярных доменных зонах. С помощью распределенных вычислений на комплексе серверов проведен анализ наличия признаков более чем 600 CMS. Наиболее популярными оказались WordPress (более 14 млн. сайтов), Joomla (3 млн сайтов) и Drupal (700 тыс. сайтов).

Далее для 10 самых популярных CMS был проведен первичный количественный анализ наличия уязвимостей к данным системам и их компонентам. Были исследованы открытые базы данных, на подобии OSVDB и CVE. В результате можно сделать вывод о корреляции количества использования CMS в сети «Интернет» и количества уязвимостей к ним.

В структуре веб-узлов подразделений БГУИР, как и любого другого образовательного учреждения, работает немалое количество сайтов, использующих описанные системы. Их популярность уже создает сильнейшую угрозу информационной безопасности данных организаций. Проведенная работа подтверждает актуальность выбранного мной направления исследования информационной безопасности веб-узлов.

ОПТИМИЗАЦИЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕРЕЗ ОБУЧЕНИЕ СОТРУДНИКОВ

Д.В. Новоселецкий, Г.А. Пухир

Существующие на сегодняшний день программно-технические средства способны успешно противостоять угрозам информационной безопасности, но при этом с каждым годом растёт процент утечек, произошедших по вине персонала. По данным Infowatch, в 2014 г., по сравнению с 2013 г. возросла доля случайных утечек (49,7% против 39,4%), а в 55% случаев причиной утечек стали настоящие или бывшие сотрудники [1].

Осведомлённость персонала позволит не только снизить процент утечек, но и значительно сократить число жалоб на трудновыполнимые правила политики информационной безопасности.

Процесс обучения ни в коем случае не должен ограничиваться автографом после ознакомления с политикой безопасности. Необходима постоянная активная работа специалистов службы безопасности или руководства компании в отношении сотрудников: лекции, инструктажи, тренировочные мероприятия, имитирующие атаки. Должен быть разработан свод простых четких и понятных правил, которые рекомендуется располагать в хорошо заметных местах: на канцелярских принадлежностях, на дверях, на кулерах с водой, кофе-машинах и чайниках. Оценить успешность процесса обучения помогут заранее установленные критерии, например: количество открытых ссылок в письмах, имитирующих фишинг-атаку; количество подключенных к ПК накопителей, оставленных на столе в отсутствии сотрудника; количество не уничтоженных бумаг в мусоре. Любой процесс обучения должен сопровождаться поощрениями и наказаниями, здесь важно не забывать о том, что не столь эффективно само наказание, как осознание его неотвратимости. Знания сотрудников — это сила в защите компании.

Литература

1. Исследование утечек конфиденциальной информации в 2014 г. [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/report2014