Панамарева Олеся Николаевна
ГМУ имени адмирала
Ф.Ф. Ушакова,
г. Новороссийск, Россия
E-mail: onpanamar@mail.ru

Дроздова Ольга Валерьевна
Кубанский государственный
университет,
г. Новороссийск, Россия
E-mail: drozdovar95@mail.ru

Panamareva O.N.
Admiral Ushakov Maritime State
Universit,
Novorossiysk, Russia

Drozdova O.V.
Kuban State University,
Novorossiysk, Russia

УДК 004.056(075.8)

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ДЛЯ РЕАЛИЗАЦИИ МЕР ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ИНТЕРФЕЙСОВ ПОЛЬЗОВАТЕЛЕЙ ДЛЯ СИСТЕМ ПОДДЕРЖКИ ПРИНЯТИЯ РЕШЕНИЙ

О.С. Резниченко, Н.А. Клименко

DEVELOPMENT OF RECOMMENDATIONS FOR IMPLEMENTATION'S MEASURES OF IT-SECURITY FOR USER'S WEB-INTERFACE OF DECISION SUPPORT SYSTEMS

O.S. Reznichenko, N.A. Klimenko

Аннотация. В статье рассматриваются проблемы организации защиты пользовательского интерфейса систем поддержки принятия решений, реализованного в веб-среде, от вредоносных скриптов и деятельности злоумышленников. В исследовании предложены мероприятия, которые способствуют решению основных задач защиты веб-ресурса.

Ключевые слова: информационная безопасность, защита сервера, защита веб-ресурса, пользовательский интерфейс, система управления контентом, хостинг, администрирование веб-сервера.

Abstract. This article describe problems of implementation of user's web-interface protection of DSS from malicious scripts and malicious activity. In the research suggested activities that promote to the solution of the main tasks of web resource securing.

Keywords: IT-security, server security, web security, user interface, CMS, web hosting service, web administration.

В настоящее время все больше увеличивается интерес к решению вопросов информационной безопасности. Развитие информационных технологий и бизнеса в сети Интернет привело к необходимости уделять повышенное внимание защите систем, реализованных с помощью веб-приложений в облаке, от действий злоумышленников.

Сетевые ресурсы и сервер, на котором они расположены, связаны с информационной системой организации или могут быть ее частью и, как правило, непосредственно включены в корпоративную сеть. Существует множество методов несанкционированного использования сетевых ресурсов и проникновения в информационную сеть организации. Вопрос безопасности интерфейса пользователя систем поддержки принятия решений стал актуальным и для всех сфер современного бизнеса, применяющих их.

Реализация интерфейса пользователя любой системы поддержки принятия решений (СППР) веб-средствами требует проведения тщательных мероприятий по защите информации и доступа к данным.

Отсутствие системы защиты СППР может привести к реализации следующих угроз:

1) несанкционированное выполнение команд;
2) загрузка исполняемых кодов и модулей;
3) кража корпоративной и личной информации;
4) модификация контента сетевого сервиса;
5) изменение конфигурации сервера, на котором размещается сетевой сервис.

Источниками проникновения вредоносных скриптов могут являться:

1. Заражение рабочей станции администратора вирусом, перехватывающим FTP пароли и передающим их злоумышленнику или на сервер-распространитель вирусов. Субъектами угроз могут быть пользователи, имеющие доступ на сервер по каналу FTP.

2. Генерация пароля от файлового сервера с помощью специальных утилит для подбора паролей, является типовым методом при целенаправленной хакерской атаке.

3. Использование уязвимостей в скриптах или системах управления контентом – CMS.

4. Применение, внедрение модулей и компонентов, полученных из неизвестных источников, использование скриптов уже содержащих вирусы.

5. Халатность системных администраторов при настройке сервера на хосте.

6. Неопытность владельцев информационного ресурса.

7. Ненадлежащее хранение паролей и их передача по открытым, незащищенным каналам связи.

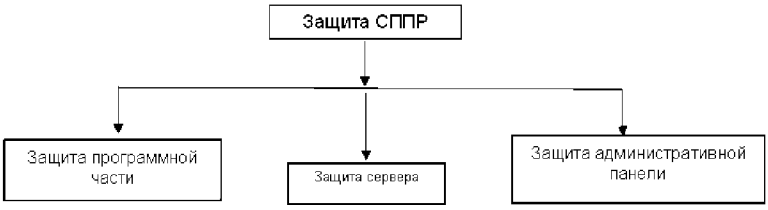
Основная задача защиты интерфейса пользователя СППР – разработка сетевого ресурса, предельно удовлетворяющего требованиям безопасности путем анализа потенциально опасных уязвимостей с последующим выполнением ряда работ для их устранения.

Безопасность интерфейса пользователя СППР, как и любого сайта. складывается из трех аспектов (см. рисунок):

безопасности программной части (CMS и скрипты);

безопасности сервера;

безопасности администрирования.



Компоненты защиты интерфейса пользователя СППР

В зависимости от задач и целей комплексная защита сетевого ресурса формируется из разных компонентов. Это позволяет найти разумный баланс между уровнем безопасности и денежными затратами.

В программную часть веб-ресурса входят скрипты, на которых основана работа интерфейса пользователя, а также файлы системы управления сайтами (CMS), если таковые применяются в качестве базы для ее реализации.

В ходе анализа мероприятий по защите программной части ресурса были предложены следующие рекомендации:

1) работать по безопасным протоколам SFTP и SCP, рекомендуемая программа в данном случае для работы с файловой системой веб-ресурса – WinSCP;

2) регулярно обновлять скрипты и CMS;

3) периодически сканировать сайт с помощью средств поиска уязвимостей, например, XSpider, Acunetix Web Vulnerability Scanner, утилиты для поиска SQL-инъекций, XSS, RFI и др.;

4) периодически проверять исходный код ресурса средствами статического анализа исходного кода (RIPS);

5) следует подключать веб-ресурс к панелям веб-мастеров поисковых систем (Яндекс, Google и др.);

6) обеспечить правильную настройку конфигурации веб-ресурса, включающую следующие мероприятия:

должны быть грамотно прописаны права на доступ к файлам и директориям;

закрыть доступ к файлам конфигурации и каталогам, хранящим резервные копии;

установить запрет на выполнение скриптов в директориях, предназначенных для загрузки внешних файлов;

7) периодически проводить аудит сайта (с помощью специалистов или программ XSpider 7.5 или Acunetix Web Vulnerability Scanner Enterprise);

8) регулярная проверка сайта детектором вредоносных скриптов (например, «AI-Bolit»).

Вторым не менее важным аспектом по обеспечению безопасности пользовательского интерфейса СППР является сервер, на котором собственно размещается сам веб-ресурс.

Существует два вида предоставления услуги хостинга: общий (shared) и выделенный (dedicated). Различие между данными видами в ответственности за безопасную настройку сервера: для shared-хостингов ответственным является администратор хостинг-компании, а для dedicated-сервера (VDS/VPS/DDS) – владелец сервера.

Для реализации интерфейса пользователя СППР наилучшим вариантом является выделенный сервер, при этом в ходе его настройки необходимо придерживаться следующих правил:

1) конфигурация сервера должна обеспечивать минимальную свободу действий при его настройке, так как неопытные пользователи могут нарушить работоспособность веб-ресурса;

2) в случае, если подключение к другим серверам не является необходимым для реализации интерфейса СППР, внешние соединения должны быть закрыты;

3) неиспользуемые функции должны быть отключены;

4) область видимости файловой системы, содержащей исполняемые скрипты, должна быть ограничена и организованы механизмы контроля ее целостности;

5) должна быть обеспечена организация системы резервного копирования и логирования административных действий;

6) выбирать хостинги, предоставляющие персональную настройку сервера.

Панель администратора является командным центром веб-ресурса, через нее можно получить доступ практически ко всем файлам и данным,

поэтому получение доступа в административную панель является приоритетной целью злоумышленников.

Были выделены следующие мероприятия по защите административной панели:

1) хранение паролей в надежном месте (применение специальных программ, например, KeePass);

2) регулярная смена паролей, при этом пароли должны состоять из разных комбинаций символов, цифр и знаков;

3) регулярная проверка на вирусы рабочего ПК, с которого происходит администрирование веб-ресурса;

4) закрытие доступа к административной панели по IP;

5) применение двойной авторизации (дополнительная авторизация средствами веб-сервера);

6) применение кодового слова (фразы) при открытии административной панели веб-сервера (разрешение доступа к каталогу на основе фрагмента, который содержится в поле «User Agent» браузера);

7) использование удобных для восприятия веб-адресов (SEF-компонентов);

8) скрытие использования систем управления контентом посредством удаления метатегов;

9) удаление не используемых модулей, компонентов, плагинов, скриптов;

10) замена префиксов в базах данных;

11) использование конфигурационного файла «.htaccess», который необходим для защиты информации о настройках веб-сервера.

Таким образом, чтобы обеспечить защиту пользовательского интерфейса СППР, реализованного в веб-среде, от вредоносных скриптов и деятельности злоумышленников, необходимо уделить достаточное количество времени и ресурсов проблеме безопасности.

Выполнение описанных выше мероприятий поспособствует решению основных задач защиты веб-ресурса. При этом нужно одновременно уделять достаточно внимания трем аспектам его защиты: поддержке ПО в актуальном состоянии, правильному подходу к вопросу настройки хостинга и слежки за правами доступа к веб-ресурсу и защите административной панели. Если хотя бы один из трех элементов будет слабым звеном, веб-интерфейс останется уязвимым.

Статья выполнена при поддержке Российского научного фонда, проект №14-38-00047, по теме «Прогнозирование и управление социальными рисками развития техногенных человекомерных систем в динамике про-

цессов трансформации среды обитания человека» с участием НИУ «БелГУ», ИСПИ РАН, ЮЗГУ.

Библиографический список

1. Информатика в экономике : учебное пособие / ред. проф. Б.Е. Одинцова, проф. А.Н. Романова. – М.: Вузовский учебник, 2008. – 478 с.

2. Куянцева Л.М. Информационное общество [Электронный ресурс] – Режим доступа: http://infdeyatchel.narod.ru/inf_ob.htm, свободный. – (дата обращения: 01.04.2014)

3. Шевнина Ю.С., Шевнина Ю.С., Павлов А.Ю. Разработка в информационной системе интерфейса пользователя, адаптированного к онтологической модели предметной области // Научные исследования и их практическое применение. Современное состояние и пути развития : сб. науч. тр. / Черноморье. – Одесса, 2005. – Т. 7: Технические науки. – С. 77–80.

4. Google Analytics. Средства веб-аналитики корпоративного уровня [Электронный ресурс]. – Режим доступа: http://www.google.com/analytics/, свободный (дата обращения 01.04.2014).

5. AWStats official web site [Электронный ресурс]. – Режим доступа: http://awstats.sourceforge.net/ свободный (дата обращения 01.04.2014).

Резниченко Олег Сергеевич
Белгородский государственный национальный исследовательский университет, г. Белгород, Россия
E-mail: oreznichenko@bsu.edu.ru

Reznichenko O.S.
Belgorod National Research University, Belgorod, Russia

Клименко Надежда Анатольевна
Белгородский государственный национальный исследовательский университет, г. Белгород, Россия
E-mail: n.a.klimenko@yandex.ru

Klimenko N.A.
Belgorod National Research University, Belgorod, Russia