УДК 004.056.53

РИСКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ БГУИР

Матюшкин С.И., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники[1]

г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук, доцент

Аннотация. Рассмотрены различные аспекты, связанные с рисками безопасности информационных систем, имеющие место в информационной системе БГУИР. Также приведены возможные варианты снижения рисков информационной безопасности, в частности риска нарушения доступности сетевых ресурсов БГУИР.

Ключевые слова. Информационная безопасность, интегрированная информационная система БГУИР, уязвимости, доступность информационного ресурса.

Обеспечение информационной безопасности информационной системы включает в себя комплекс мер для обеспечения бесперебойной работы и целостности обрабатываемой информации.

Безопасность определяется слабейшим звеном в системе защите. Можно ставить различные антивирусы, закрыть все порты на сервере, но если при этом пользовали ставят пароли типа 123456 или пишут их на бумажке на рабочем столе на ПК, то риски быть взломанным очень высоки. Поэтому фокус внимания всегда должен быть на наиболее слабых на данный момент звеньях.

Экономическое обоснование взлома. Зачем взламывают какую-либо систему? Для получения некой выгоды. И эта выгода может быть не только материальная. Если взлом стоит дешевле этой выгоды, то игра стоит свеч. Задача защиты сделать взлом невыгодным. Необходимо повысить стоимость взлома до такого уровня, чтобы он стал не привлекателен.

Риски взлома информационной системы:

– Утечка данных — будет потеряна конфиденциальность информации;
– Данные могут быть повреждены — информация потеряет целостность;
– Информация может стать недоступна пользователю — потеряна доступность;
– Ресурсы системы могут быть использованы для взлома других систем.

Все меры по безопасности так или иначе направлены на обеспечение конфиденциальности, целостности и доступности информации.

Человеческий фактор в информационной безопасности является самый важным моментом. У человека есть множество соблазнов и уязвимых мест. Кого-то можно подкупить, кого-то запугать, а кто-то может делать, не понимая к каким результатам могут привести его действия.

Более опасен для системы внутренний человек (сотрудник), а не человек с улицы. У него может быть много причин для помощи злоумышленнику: обидели на работе, не дают повышения, «подработка», компромат на него, некомпетентность, банальная глупость и т.д. Имея доступ во внутреннюю часть системы человек становится точкой входа для злоумышленника или сам становится им.

Защита должна соответствовать уровню угроз и модели злоумышленника. Важно представлять себе примерный портрет злоумышленника и его возможности.

Это позволит понять, что может сделать злоумышленник, какие цели преследует (что он сможет получить в случае успешного взлома) и какие варианты атаки он может реализовать.

Непрерывность состояния защищенности. Система безопасности должна работать непрерывно во времени. Необходимо предусмотреть факторы, которые могут прервать непрерывность состояния защищенности: выключили свет, уволился системный администратор, необходимо обновить какое-то программное обеспечение или ключ шифрования.

Подход риск менеджмента — риски информационной безопасности сайта. Информационная безопасность подразумевает работу с рисками, представляющими собой комбинацию вероятности реализации угрозы и критичность актива для бизнеса.

Угрозы информационной безопасности и меры противодействия угрозам безопасности

Первый вопрос — кто злоумышленник, и зачем ему нужно взламывать систему?

Что он получит? Какие возможности для взлома у него есть? Какой бюджет на взлом он может выделить? Понимая эти вопросы, можно адекватно выработать ряд мер защиты.

Основные меры защиты по угрозам для конфиденциальности, целостности и доступности информации на сайте информационной системы БГУИР.

Меры по обеспечению конфиденциальности

Протокол SSL (HTTPS). HTTPS соединение шифрует трафик между браузером и сервером. Это усложняет для злоумышленника получение данных в промежуточных узлах (например, извлечение пароля пользователя при входе). Также SSL дает некую гарантию пользователю, что он взаимодействует именно с нужным сайтом (в браузере отображается принадлежность сертификата).

Защита от разных атак на веб-приложение (XSS, SQL инъекции). Пользователь может ввести некий код через поля форм и этот код может негативно сказаться на работе системе. Например, XSS атака подразумевает ввод JS кода, который сохранится в базе сайта (например, при подаче заявки в систему единой технической поддержки), затем другой пользователь запросит эти данные из базы и этот вредоносный код JS выполнится от имени этого пользователя.

Атака SQL Injection — вводится код SQL, который видоизменяет SQL выполняемый на сервере. Это позволяет вводить прямые команды в БД (например, удалять данные или считывать данные из таблиц). Защита от SQL инъекций — весь код SQL выполнять в хранимых процедурах с параметрами без использования динамически генерируемых процедур.

Обновление программного обеспечения (ПО). Периодически разработчики находят уязвимости в ПО и выпускают обновления. Если не делать обновления, то есть риск, что этой уязвимостью воспользуются злоумышленники. Необходимо проводить профилактику сервера и ПО на нем.

Организационные меры и обучение сотрудников. Можно так построить бизнес-процесс, чтобы снизить вероятность утечки конфиденциальности и целостности.

Второе направление это обучение. Люди должны хорошо знать свой участок и роль в процессах. Что они могут, а что делать нельзя. Знать, какие бывают ситуации и как они должны реагировать на них.

Контроль целостности данных можно реализовывать через скрипты. Данные в системе нужно периодически проверять. Код сайта может содержать ошибки, которые будут приводить к нарушению целостности. В этом случае необходимо создать ряд скриптов, которые будут проверять по бизнес-логике целостность данных в таблицах. Можно запускать подобные скрипты ежедневно для нахождения коллизий в данных, после чего выдавать отчет на почту.

Правильная структура данных в базе данных. Если структура базы данных имеет проблемы, то при частичном обновлении данных может нарушиться целостность данных. Необходимо использовать нормализацию базы данных достаточного уровня, вводить ограничения, устанавливать внешние ключи и т.д.

Так как сайт информационной системы разрабатывался, а не просто был сделан из готовых блоков, то в нем могут быть ошибки. Они могут проявиться в ходе эксплуатации. Необходимо проводить профилактику приложения: анализировать системный журнал и быстродействие, искать проблемные точки. Это сказывается как на качестве системы, так и на состоянии защищенности. В ходе таких обзоров могут быть обнаружены бреши, которые на стадии разработки сайта никак себя не проявляли.

Защита от DOS. DOS атака это организация множества запросов на сайт с целью его перегрузки. Происходит отказ в обслуживании — сервер просто начинает не справляться с возникшей нагрузкой. Следует блокировать подозрительные IP адреса, и сервер просто не будет обрабатывать некоторые запросы. Тут главное не перестараться, т.к. таким образом, можно отсеять реальных пользователей вместе с ботами (программы, заходящие на сайт).

Нагрузочное тестирование. Проводите нагрузочные тесты, находите проблемные места в своем сайте про производительности. То, что хорошо работает на малом объеме, может очень тормозить на больших оборотах.

Резервный сервер. Если основной сервер выйдет из строя, надо иметь возможность быстро восстановить работу приложения на резервном сервере. В идеале сделать работу несколько серверов в связке, чтобы при выходе из строя одного сервера, запросы шли на другой сервер.

Мониторинг доступности и оповещения. Если возникла остановка работы сайта, то необходимо узнать об этом как можно раньше, чтобы сразу принять все меры по восстановлению сайта. Для этого используются средства мониторинга, которые опрашивают сайт. В случае падения они сообщают через e-mail или SMS о проблеме.

Рекомендации по обеспечению информационной безопасности

Для повышения безопасности, рекомендуется использовать сложные пароли, однако такие, которые можно запомнить. Это позволит избежать записывания паролей на бумаге. Например, "Para001medic+" – пароль, состоящий из специальных символов, цифр, символов в верхнем регистре, содержащий более 8 символов. Такой пароль трудно подобрать, но легко запомнить пользователю.

Минимальный доступ и убрать все ненужные элементы. У каждого пользователя должен быть минимальный уровень доступа, достаточный для его работы. Не нужно давать больше, чем ему нужно для выполнения служебных обязанностей. Атаке извне может быть подвергнут любой элемент вашей системы, и чем меньше возможностей у этого элемента, тем лучше.

Закрыть доступ через неиспользуемые порты на сервере. Каждый порт это потенциальная точка входа для злоумышленника.

Обновления. Ставьте обновления своевременно. Заведите регламент работ по обновлению основного ПО.

Инсайдеры. Инсайдер гораздо опаснее внешнего злоумышленника. У него уже есть доступ в системе. К нему есть некоторое доверие со стороны других людей в системе. Он может долгое время незаметно пакостить в системе. Создайте условия для максимальной удовлетворенности людей в системе, со всеми расставайтесь полюбовно, не оставляя долгов перед другими (особенно перед программистами и системными администраторами).

Используйте основы риск менеджмента. Проводите пересмотр рисков и мер по уменьшению критичности и вероятности возникновения риска.

Не публикуйте в общий доступ лишней информации. Внешний злоумышленник собирает информацию сначала из открытых источников. По крупицам ищет уязвимости системы, изучает структуру системы и возможные точки входа в него.

Не публикуйте в общий доступ информацию, чувствительную ко взлому. Тем самым вы уменьшите вероятность взлома внешним злоумышленником.

На рабочих станциях, тем более на серверах, не должно быть ненужного ПО. Любое дополнительное ПО приносит потенциальную возможность получить вирус или другую вредоносную программу.

Уязвимости в ПО также могут быть точкой входа в систему. Поэтому ставьте приложения только из проверенных источников и давайте этим приложениям минимум необходимых прав. Не следует доверять введенным пользовательским данным. Когда сайт обрабатывает запрос от браузера, нельзя доверять введенным данным от пользователя.

Ежедневно должны создаваться резервные копии. Их нужно копировать на удаленное хранилище.

Нет смысла описывать угрозы, считать риски без проведения работ по повышению уровня защищенности. Реализовывать эти работы можно в виде регламентов обслуживания системы — т.е. это совокупность неких периодических действий, направленных на реализацию мер по обеспечению безопасности.

Регламент обслуживания сервера. Выполняет системный администратор, проверяет критичные параметры сервера (память, место на диске, процессор), изучает системные журналы, проводит обновление ПО, смотрит за резервными копиями.

Плановое обновление паролей. Вы можете проводить процедуру изменения пароля для важных точек входа — соединение с базой данных, доступ к хостинг-панелям, доступ к серверу и т.д.

Регламент пересмотра состава угроз и соответствующих мер (риск менеджмент). Хотя бы раз в полгода имеет смысл возвращаться к рискам информационной безопасности и заново проводить анализ рисков,

Интегрированная информационная система (ИИС) «БГУИР: Университет» ориентирована на автоматизацию учебных процессов и облегчение взаимодействия сотрудников и студентов БГУИР. Использование ИИС позволяет упростить учет информации о студентах, учебных группах, учебных планах специальностей. При обеспечении работоспособности и защищенности ИИС БГУИР необходимо учитывать все описанные выше меры безопасности. Однако, наиболее частыми проблемами, с которыми приходится иметь дело при эксплуатации интегрированной информационной системы БГУИР это перебои электропитания и попытки взлома из сети Интернет, что вызывает нарушение доступности информационных сервисов БГУИР.

Предложен способ повышения доступности за счет обеспечения бесперебойности электропитания серверного и сетевого оборудования.

Серверное оборудование предусматривает возможность установки двойного питания (2 блока питания в сервере). Установив по два блока питания в серверы, можно обеспечить подачу электропитания из двух источников. Так как здания запитываются от трехфазной сети, то подача питания с двух разных фаз через источники бесперебойного питания обеспечит:

1. Устойчивость к перебоям электропитания по любой из используемых фаз, что является наиболее частым случаем.

2. Увеличит вдвое время работы от источников электропитания.

3. Создаст запас времени для развертывания, запуска и переключения питания на дизель-генератор вместо одной из линий питания при отключении электроэнергии на всех линиях, сохраняя возможность автоматического переключения на вторую линию при восстановлении снабжения.

Сетевое оборудование имеет свои источники бесперебойного питания, но не имеет возможности двойного питания и запитывается от местных линий энергоснабжения. Для обеспечения возможности переключения сетевого оборудования на резервный дизель-генератор или другую линию энергоснабжения, необходимо сделать для них отдельную сеть электропроводки, которая будет запитываться в серверной комнате.

Список использованных источников:

1. Как защитить сайт? Обеспечение информационной безопасности сайта / Р.Ш. Раянов // https://falconspace.ru/blog/kak-zashchitit-sayt--obespechenie-informacionnoy-bezopasnosti-sayta

2. Обзор методов защиты корпоративной информации / Алексей Парфентьев // https://lib.itsec.ru/articles2/Inf_security/obzor-metodov-zaschity-korporativnoy-informatsii

3. Кейсы, реальные истории из практики клиентов / searchinform // https://searchinform.ru/cases/

4. Как обезопасить свой веб-сайт? / VDSina.ru // https://habr.com/ru/companies/vdsina/articles/503772/

5. Анализ и оценка информационной безопасности / Региональные системы // https://www.ec-rs.ru/blog/informacionnaja-bezopasnost/analiz-i-otsenka-informatsionnoy-bezopasnosti/?ysclid=lgc8qpmgur833212051

UDC 004.056.53

SECURITY RISKS OF THE BSUIR INFORMATION SYSTEM

Matyushkin S.I.

Belarusian State University of Informatics and Radioelectronics[1], Minsk, Republic of Belarus

Petrov S.N. – PhD, associate professor

Annotation. Various aspects related to the security risks of information systems that take place in the BSUIR information system are considered. Possible options for reducing information security risks, in particular the risk of disruption of the availability of BSUIR network resources, are also presented.

Keywords. Information security, integrated BSUIR information system, vulnerabilities, availability of an information resource.