Матвеев В.А. Гибкий подход с использованием КАНБАН в управлении рисками информационной безопасности // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 5(31) ч.2 с. 15–19

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.9

ГИБКИЙ ПОДХОД С ИСПОЛЬЗОВАНИЕМ КАНБАН В УПРАВЛЕНИИ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Матвеев В.А.
ФГБОУ ВО «Национальный исследовательский ядерный университет «МИФИ», Москва, Россия (115409, город Москва, Каширское ш., д.31), e-mail: veevtammatveev@yandex.ru

В настоящее время разработка и внедрение программного обеспечения для нужд бизнеса является одним из важнейших направлений информационных технологий. В этом аспекте актуальность приобретают и вопросы информационной безопасности. От грамотного построения и использования системы защиты информации при разработке ПО зависит не только финансовое положение, но и репутация Компании, а также и соблюдение законодательства РФ. Постоянно меняющееся бизнес-окружение накладывает свои ограничения и правила, поэтому применение подходящих методологий влияет на эффективность управления рисками ИБ. Рассмотрен процесс повышения эффективности управления рисками, более действенное реагирование бизнеса и улучшения определенных SLA по управлению рисками.

Ключевые слова: Kanban, Agile, Information security, SLA, assessment, bot.

A FLEXIBLE APPROACH USING KANBAN TO MANAGE INFORMATION SECURITY RISK

Matveev V.A.
National Research Nuclear University MEPhI, Moscow, Russia (115409, Moscow Kashirskoye shosse, 31), e-mail: veevtammatveev@yandex.ru

Currently, the development and implementation of software for business needs is one of the most important areas of information technology. In this aspect, information security issues also become relevant. Not only the financial position, but also the reputation of the Company, as well as compliance with the legislation of the Russian Federation, depends on the competent construction and use of the information security system in software development. The constantly changing business environment imposes its own restrictions and rules, so the use of suitable methodologies affects the effectiveness of information security risk management. The process of improving the efficiency of risk management, a more effective response of the business and improving certain SLAs for risk management is considered.

Keywords: Kanban, Agile, Information security, SLA, assessment, bot.

На сегодняшний день, информационные технологии, в частности Интернет, являются важным звеном, дающим возможность успешно развиваться бизнесу. Сайты, онлайн сервисы, мобильные приложения и другие варианты использования технологии Интернет позволяют бизнесу и компаниям улучшать свои финансовые и рейтинговые показатели. Все больше компаний стараются не только внедрить различные сервисы, но и развивать их, делать более удобными для аудитории и для контроля сотрудниками. При разработке программного обеспечения изначально идет процесс планирования, в котором обсуждается все тонкости

программного продукта на выходе. Гибкая методология разработки программного обеспечения ориентирована на использовании итеративного подхода, при котором программный продукт создается поэтапно, реализуя определенный набор требований. При этом предполагается, что требования могут изменяться в процессе из-за появления различных нюансов. Команды, использующие гибкие методологии, формируются из высококвалифицированных и опытных разработчиков, которые распределяют между собой различные задачи в процессе создания программного продукта.

Выбор методики управления рисками информационной безопасности, подходящей для каждой организации, зависит от ряда условий ее деятельности [1]:

- зависимость деятельности организации от информационных технологий и значимость для ее деятельности рисков ИБ;
- необходимость детального изучения рисков ИБ и возможность проведения верхнеуровневой оценки рисков и определения базовых направлений по снижению рисков ИБ;
- наличие человеческих, финансовых и временных ресурсов для реализации процесса управления рисками ИБ;
- требования законодательства, регуляторов и других заинтересованных сторон к процессу управления рисками ИБ.

В зависимости от перечисленных условий для разных организаций будет оптимальным выбор разных методологий управления рисками, но, в любом случае, для успешного управления рисками ИБ, выбираемая или разрабатываемая организацией методология управления рисками должна:

- соответствовать потребностям организации;
- быть применимой к организации с учетом корпоративной культуры и имеющихся ресурсов;
- отражать в виде модели реальную ситуацию с перечнем рисков ИБ, являющихся актуальными для организации;
- обеспечивать повторяемость результатов при использовании ее разными группами экспертов;
- быть понятной и прозрачной для всех заинтересованных сторон, включая руководство компании, представителей регуляторов, внешних и внутренних аудиторов.

Рассмотрен проект одной из ведущей российской e-commerce компании, которой доверяют миллионы пользователей [2]. Соответственно в компании серьёзно подходят к вопросам информационной безопасности внутренних и внешних сервисов: бережно относятся к пользовательским данным и разрабатывают собственные сервисы с учётом рекомендаций по информационной безопасности. При этом все равно существует вероятность появления в них уязвимостей, создавая риски безопасности.

Для этого в компании создан проект RISK. Цель проекта RISK в том, чтобы через "управление" этими рисками/уязвимостями, сделать сервисы компании безопаснее.

RISK — это задача, в которой исследуется и исправляется в рамках SLA один конкретный риск безопасности. В задаче описываются следующие условия:

- фиксируется источник информирования о проблеме безопасности;
- исследование уязвимостей приведших к риску;
- оценка критичности риска;
- оценка предварительных действий по закрытию риска;
- анализ системного характера проблемы;
- анализ решений для устранения или снижения риска;
- приведение ссылок на созданные задачи на исправление в соответствующем проекте.

Помимо того, что это непосредственно задача, есть и более объёмное толкование (на самом деле их несколько, но тут мы будем исходить из одного). Воспользуемся для этого документом OWASP Top Ten 2017: Application Security Risks. Злоумышленники разными способами могут атаковать сервис и нанести сервису ущерб (Рисунок 1). Подобные пути представляют собой риски безопасности, которые могут (или не могут) быть достаточно серьезными, чтобы обращать на них внимание.

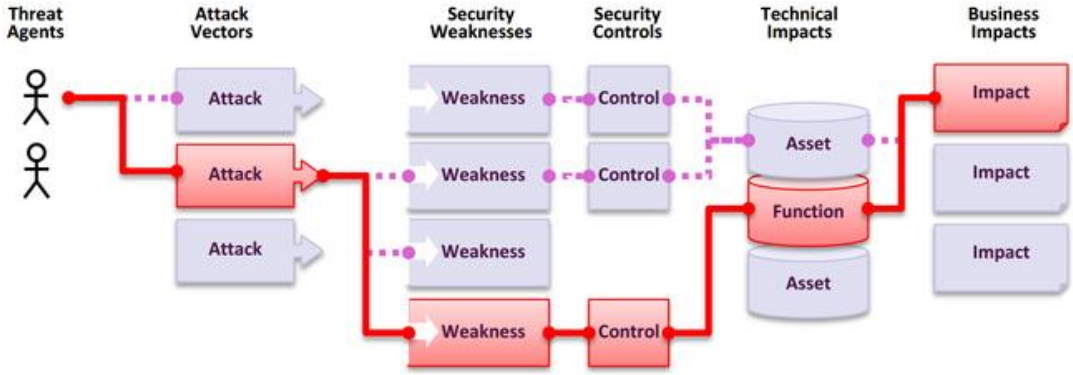

Рисунок 1 – Схема атаки злоумышленника
Источник: OWASP Top Ten 2017: Application Security Risks [3]

Иногда эти способы легко найти и эксплуатировать, иногда — очень сложно. Аналогичная ситуация с возможным ущербом: его может не быть совсем или он может дорого стоить бизнесу. Чтобы определить риски, придется оценить вероятности, связанные с источниками угроз, векторами атак и недостатками безопасности, а затем объединить их с оценкой технического и репутационного вреда для компании. Сумма этих факторов определяет совокупный риск.

RISK-тикет заводится тогда, когда каким-либо образом стало известно о какой-либо уязвимости в сервисах компании:

- пришёл репорт от внешнего исследователя безопасности через багбаунти-программу компании;
- статистический анализатор кода обнаружил потенциальную уязвимость.

После проведения первичного исследования, ответственным за исправления риска становится представитель направления или конкретный техлид, в сервисе которого была обнаружена проблема безопасности.

Ответственный за исправления риска следует соответствующей инструкции:

1. Обсудить с инженером ИБ, который завёл тикет, специфику риска безопасности, определить уровень его опасности и согласовать выбранное решение по исправлению;

2. Создать в проекте сервиса соответствующие тикеты на исправление и привязать их к RISK-тикету**;**

3. В соответствие с SLA обеспечить закрытие этих задач и таким образом закрыть RISK;

4. В случае решения тикета, призвать инженера ИБ для проверки исправления.

После того риск безопасности подтвердился инженером ИБ и передан на исправление начинается отчёт времени SLA исправления со стороны сервиса.

Применение элементов искусственного интеллекта в сфере электронной коммерции и услуг является, если и не главным, то одним из основных трендов современных информационных технологий. Среди них наиболее востребованы программируемые модули, так называемые «боты», позволяющие взаимодействовать с пользователями в режиме реального времени.

Боты позволяют минимизировать расходы, связанные с ежедневным и однотипным взаимодействием с большим количеством пользователей. Как и в других сферах бизнеса и производства, автоматизация рабочего процесса целесообразна в том случае, если задачи и цели этого процесса могут быть описаны и конкретизированы. Очевидно, что те функции, которые взяли на себя чат-боты, могут быть реализованы (и успешно реализуются) в более привычной форме – через веб-интерфейс или предустановленные приложения.

В рассмотренной e-commerce компании для форсирования выполнения SLA по исправлению рисков используются следующий процесс:

- Бот ИБ регулярно приходит в неактивные тикеты и уведомляет ответственного о том, что близок или уже исчерпан срок SLA;
- Тикеты эскалируются по следующему алгоритму:
    1. при игнорировании тикета на протяжении трех дней инженер ИБ оповещает ответственного о наличии проблемы;
    2. при очередном двухдневном игнорировании инженер подготавливает эскалацию до руководителей направлений;
    3. при дальнейшем однодневном простое — эскалация идет по тому же принципу с шагом один день до технического директора.

Вывод: в настоящей работе представлено описание возможности применения методологии Канбан в рамках управления рисками информационной безопасности, а также вариант улучшения рабочих процессов с помощью бота, который представляет собой дополнительно разработанный алгоритм по уведомлению и эскалации как инициатора задачи, так и исполнителя.

Список литературы

1. Методики управления рисками информационной безопасности и их оценки [Электронный ресурс] – Режим доступа: https://safe-surf.ru/specialists/article/5194/587935/
2. Проект RISK: как мы управляем уязвимостями эффективно [Электронный ресурс] – Режим доступа: https://habr.com/ru/companies/ozontech/articles/653517/
3. Application Security Risks [Электронный ресурс] – Режим доступа: https://owasp.org/www-project-top-ten/2017/Application_Security_Risks

References

1. Methods of information security risk management and their assessment [Electronic resource] – Access mode:: https://safe-surf.ru/specialists/article/5194/587935//
2. Project RISK: How We Manage Vulnerabilities Effectively [Electronic resource] – Access mode: https://habr.com/ru/companies/ozontech/articles/653517/
3. Application Security Risks [Electronic resource] – Access mode: https://owasp.org/www-project-top-ten/2017/Application_Security_Risks