УДК 004.056

РАЗРАБОТКА И СИСТЕМНЫЙ АНАЛИЗ МАТЕМАТИЧЕСКОЙ МОДЕЛИ УГРОЗ, МОДЕЛИ НАРУШИТЕЛЯ, ПРОЦЕДУР ЗАЩИТЫ WEB – ПРИЛОЖЕНИЙ НА ВСЕХ ЭТАПАХ ФУНКЦИОНИРОВАНИЯ

Власенко Александра Владимировна
к.т.н., доцент

Дзьобан Павел Игоревич
аспирант
Кубанский государственный технологический университет, Краснодар, Россия

В статье рассматривается актуальность разработки математической модели угроз и модели нарушителя, которая выражается в формализации процесса поиска уязвимостей в информационных системах данных на всех этапах взаимодействия пользователей и web-приложения, начиная с процедуры идентификации пользователя

Ключевые слова: СИСТЕМНЫЙ АНАЛИЗ, МОДЕЛИ УГРОЗ, АВТОРИЗАЦИЯ, АУТЕНТИФИКАЦИЯ

UDC 004.056

DEVELOPMENT AND SYSTEMS ANALYSIS O A MATHEMATICAL MODEL OF THREATS, AN INTRUDER MODEL AND PROCEDURES FOR PROTECTING WEB - APPLICATIONS FOR ALL STAGES OF FUNCTIONING

Vlasenko Alexandra Vladimirovna
Cand.Tech.Sci., associate professor

Dzyoban Pavel Igorevich
postgraduate student
Kuban State Technological University, Krasnodar, Russia

The article discusses the relevance of the development of a mathematical model of threats and an intruder model which has been expressed in formalization of the process of finding vulnerabilities in information systems data at all stages of interaction between users and web-based applications, starting from user authentication procedures

Keywords: SYSTEM ANALYSIS, THREAT MODELS, AUTHORIZATION, AUTHENTICATION

Модель нарушителя представляет собой некое описание типов злоумышленников, которые намеренно или случайно, своим действием или бездействием способны нанести ущерб Web – приложению.

Таблица 1 – Математическая модель угроз

Тип угрозы	Возможные последствия
Анализ сетевого трафика	Исследование характеристик сетевого трафика, перехват передаваемых данных, в том числе идентификаторов и паролей пользователей
Сканирование сети	Определение протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, активных сетевых сервисов, идентификаторов и паролей пользователей
Угроза выявления пароля	Выполнение любого действия, связанного с получением несанкционированного доступа
Подмена доверенного объекта сети	Изменение трассы прохождения сообщений, несанкционированное изменение маршрутно-адресных данных. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации
Навязывание ложного маршрута	Несанкционированное изменение маршрутно-адресных

сети	данных, анализ и модификация передаваемых данных, навязывание ложных сообщений	
Внедрение ложного объекта сети	Перехват и просмотр трафика. Несанкционированный доступ к сетевым ресурсам, навязывание ложной информации	
Отказ в обслуживании	Частичное исчерпание ресурсов	Снижение пропускной способности каналов связи, производительности сетевых устройств. Снижение производительности серверных приложений
	Полное исчерпание ресурсов	Невозможность передачи сообщений из-за отсутствия доступа к среде передачи, отказ в установлении соединения. Отказ в предоставлении сервиса (электронной почты, файлового и т.п.)
	Нарушение логической связанности между атрибутами, данными, объектами	Невозможность передачи сообщений из-за отсутствия корректных маршрутно-адресных данных. Невозможность получения услуг ввиду несанкционированной модификации идентификаторов, паролей и т.п.
	Использование ошибок в программах	Нарушение работоспособности сетевых устройств
Удаленный запуск приложений	Путем рассылки файлов, содержащих деструктивный исполняемый код, вирусное заражение	Нарушение конфиденциальности, целостности, доступности информации
	Путем переполнения буфера серверного приложения	
	Путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками либо используемыми штатными средствами	Скрытое управление системой

Чаще всего по глобальному признаку злоумышленники ранжируются на внешних и внутренних (соответственно, категории A и B). Однако такое деление не является достаточным. Поэтому ранжирование проводится с диверсификацией указанных категорий на подкатегории. Например, к внешним злоумышленникам причисляются нарушители из следующих групп: клиенты, которые могут нанести ущерб намеренно или по незнанию; подрядчики, нанятые на выполнение тех или иных работ (они в свою очередь, также могут совершать как намеренное, так и ненамеренное нарушение); квалифицированные хакеры и т. д. Внутренние злоумышленники подразделяются на тех, кто причиняет ущерб намеренно и ненамеренно; кроме того, данная категория может диверсифицироваться по признаку назначенных привилегий в информационной системе [1,2].

В идеальной модели, если в компании имеется положение, где описываются категории пользователей информационной системы (как внешних, так и внутренних), модель нарушителя может быть составлена на основании этого положения, дабы впоследствии результаты проведенной оценки рисков интегрировать в общую концепцию информационной безопасности компании.

Расчет информационных рисков.

Формула, чаще всего используемая при расчете рисков, представляет собой произведение трех параметров:

- стоимость ресурса (Asset Value, AV). Указанная величина характеризует ценность ресурса. При качественной оценке рисков стоимость ресурса чаще всего ранжируется в диапазоне от 1 до 3, где 1 — минимальная стоимость ресурса, 2 — средняя стоимость ресурса и 3 — максимальная стоимость ресурса. К примеру, сервер автоматизированной банковской системы имеет AV = 3, тогда как отдельный информационный киоск, предназначенный для обслуживания клиента, имеет AV = 1 по отношению к информационной банковской системе;

- мера уязвимости ресурса к угрозе (Exposure Factor, EF). Этот параметр показывает, в какой степени тот или иной ресурс уязвим по отношению к рассматриваемой угрозе. Например, с точки зрения банка ресурс автоматизированной банковской системы имеет наибольшую доступность. Таким образом, атаки с целью реализации отказа в обслуживании (Denial of Service, DoS) представляют для него максимальную угрозу. При качественной оценке рисков данная величина также ранжируется в диапазоне от 1 до 3, где 1 — минимальная мера уязвимости (слабое воздействие), 2 — средняя (ресурс подлежит восстановлению), 3 - максимальная (ресурс требует полной замены после реализации угрозы);

- оценка вероятности реализации угрозы (Annual Rate of Occurrence, ARO) демонстрирует, насколько вероятна реализация определенной угрозы за определенный период времени (как правило, в течение года) и также ранжируется по шкале от 1 до 3 (низкая, средняя, высокая).

На основании полученных данных выводится оценка ожидаемых потерь (уровень риска):

- оценка ожидаемого возможного ущерба от единичной реализации определенной угрозы (Single Loss Exposure, SLE) рассчитывается по формуле: SLE = AV x EF;

- итоговые ожидаемые потери от конкретной угрозы за определенный период времени (Annual Loss Exposure, ALE) характеризуют величину риска и рассчитывается по формуле: ALE = SLE x ARO.

Таким образом, конечная формула расчета рисков представляет собой произведение: ALE = ((AV x EF = SLE) x ARO).

В качестве сервера Web используется ПО Microsoft IIS и СУБД Microsoft SQL Server. Для упрощения расчета примем две модели нарушителей: внешний легальный пользователь и внешний хакер. Первого обозначим как A1, а второго — A2.

Таким образом, категории А1 свойственны следующие черты нарушителя:

- достаточная квалификация для эксплуатации возможностей Web - приложения;

- отсутствие цели нанести ущерб компании.

Для категории А2 характерны следующие черты нарушителя:

- необходимые технические познания для эксплуатации возможностей Web - приложения;

- навыки и опыт использования уязвимостей и недекларированных возможностей ОС, распространенного прикладного ПО;

- опыт взлома подобных систем;

- намерение нанести ущерб компании.

В отношении сервера Web могут быть идентифицированы следующие угрозы:

- нарушение целостности информации, хранящейся в СУБД Web - приложения;

- нарушение доступности сервера Web;

- нарушение конфиденциальности информации, хранящейся в СУБД Web - приложения.

Угроза нарушения целостности может возникнуть в результате реализации следующих механизмов:

- проведение атаки SQL Injection;

- проведение атаки Cross-Site Scripting;

- эскалация привилегий злоумышленника в системе в результате переполнения буфера ОС или СУБД.

Угроза нарушения конфиденциальности возможна вследствие реализации следующих механизмов:

- проведение атаки SQL Injection;

- проведение атаки Cross-Site Scripting;

- эскалация привилегий прав злоумышленника в системе в результате переполнения буфера ОС или СУБД.

Угроза нарушения доступности возникнет, если будут реализованы следующие механизмы:

- эскалация привилегий прав злоумышленника в системе в результате переполнения буфера ОС или СУБД;

- создание шторма сетевых пакетов против сервера Web;

- формирование некорректных пакетов, направленных на сервер Web и влекущих за собой крах службы.

Таким образом, идентифицированы следующие механизмы реализации угроз:

- проведение атаки SQL Injection;

- проведение атаки Cross-Site Scripting;

- эскалация привилегий прав злоумышленника в системе в результате переполнения буфера ОС или СУБД;

- создание шторма сетевых пакетов, направленных на сервер Web;

- формирование некорректных пакетов, направленных на сервер Web и влекущих за собой крах службы.

Атака наподобие SQL Injection может быть намеренно осуществлена злоумышленником категории А3, но не может быть проведена ни при каких обстоятельствах злоумышленником категории А1.

Атака Cross-Site Scripting также может быть предпринята злоумышленником категории А2, но ни в коем случае не злоумышленником категории А1.

Эскалация привилегий прав злоумышленника в системе может произойти в результате намеренных действий злоумышленника категории А2 и ненамеренных действий злоумышленника категории А1.

Создание шторма сетевых пакетов, направленных на сервер Web, может стать следствием намеренных действий злоумышленника категории

А2 и ненамеренных действий злоумышленника категории А1 (например, вследствие частого нажатия кнопки "Обновить" обозревателя Internet).

Формирование некорректных пакетов, направленных на сервер Web, влекущих за собой крах службы, может произойти в результате намеренных действий злоумышленника категории А2, но ни при каких обстоятельствах не случится в результате действий злоумышленника категории А1. Результаты идентификации угроз и построения модели нарушителя сведены в Таблицу 2.

Таблица 2 – Идентификация угроз Web - приложения

Ресурс	AV	Угроза (механизм реализации)	Модель нарушителя	F	ARO	SLE	ALE
Сервер Web-приложе-ния	3	Угроза нарушения целостности (SQL Injection, Cross-Site Scripting, эскалация привилегий	А1	3	2	9	18
		Угроза нарушения конфиденциальности (SQL Injection, Cross-Site Scripting, эскалация привилегий)	А2	3	2	9	18
		Угроза нарушения доступа целостности (эскалация привелегий, создание шторма пакетов, формирова-ние некоррект-ных пакетов)	А1, А2	2	3	6	18

Большинство из описанных параметров принимается на основе мнения эксперта. Это связано с тем, что количественная оценка вероятности реализации угрозы затруднена ввиду относительной новизны

информационных технологий и, как следствие, отсутствия достаточного количества статистических данных. В случае оценки стоимости ресурса (AV) количественная оценка (например, в денежном эквиваленте) чаще всего не проводится, и тогда оценка параметра SLE затруднена.

После ранжирования рисков определяются требующие первоочередного внимания; основным методом управления такими рисками является снижение, реже — передача. Риски среднего ранга могут передаваться или снижаться наравне с высокими рисками. Риски низшего ранга, как правило, принимаются и исключаются из дальнейшего анализа. Диапазон ранжирования рисков принимается исходя из проведенного расчета их качественных величин. Так, например, если величины рассчитанных рисков лежат в диапазоне от 1 до 18, низкие риски находятся в диапазоне от 1 до 7, средние — в диапазоне от 8 до 13, высокие — в диапазоне от 14 до 18.

Таким образом, управление рисками сводится к снижению величин высоких и средних рисков до характерных для низких рисков значений, при которых возможно их принятие. Снижение величины риска достигается за счет уменьшения одной или нескольких составляющих (AV, EF, SLE) путем принятия определенных мер. В основном это возможно применительно к EF и SLE, так как AV (стоимость ресурса) — фиксированный параметр. Однако возможно и его снижение. Например, если хранящаяся на сервере информация относится к конфиденциальной, но проверка выявила, что гриф "конфиденциально" в силу каких-либо причин может быть снят. В результате стоимость ресурса автоматически уменьшается. В системе Internet-банкинга, например, параметр EF можно уменьшить путем фиксации ответственности сторон в договорном порядке. В этом случае считается, что стороны предупреждены об ответственности, которую может повлечь за собой нарушение правил эксплуатации системы, и, таким образом, фактор уязвимости снижается.

Снижение параметра SLE, т. е. вероятности реализации угрозы, может быть достигнуто за счет технических мер. Например, при наличии угрозы кратковременного отключения электропитания установка источника бесперебойного питания снижает вероятность се реализации [3,4].

Возникшие (оставшиеся) после применения методики управления риски называются остаточными, и именно они применяются для обоснования инвестиций в информационную безопасность. Перерасчет рисков производится в отношении всех рисков, если они оценены как высокие и средние.

Ресурс сервера Web является критичным для функционирования компании, поэтому ему присвоено значение AV=3. Мере уязвимости ресурса к угрозе нарушения целостности (EF) тоже назначено максимальное значение (3), так как нарушение целостности хранимых в СУБД данных влечет за собой срыв поставок, если, например, удалены данные об оформленных, но еще не проведенных заказах. Вероятность реализации угрозы нарушения целостности оценена как средняя ввиду того, что не исключается эксплуатация широко известных уязвимостей и недостатков программирования (SQL Injection, Cross-Site Scripting). Параметры EF и ARO в отношении угроз нарушения конфиденциальности и доступности рассчитывались аналогично. Большинство параметров (кроме AV), как можно видеть, принимались исходя из экспертного мнения аудитора. Все идентифицированные риски являются высокими, поскольку реализация порождающих эти риски угроз неизбежно нанесет существенный ущерб компании. Таким образом, дальнейшие меры подразумевают снижение идентифицированных рисков.

Для снижения меры уязвимости (EF) в части реализации угрозы нарушения доступности рекомендуется пересмотреть исходный код сценариев Internet-магазина и добавить в него функции фильтрации

запросов SQL с целью предотвращения внедрения запросов SQL в запросы HTTP GET. Сходные меры могут быть предприняты в отношении атаки Cross-Site Scripting. Что касается эскалации привилегий злоумышленника, то на этот случай могут быть приняты такие меры, как установка недавно вышедших обновлений безопасности службы сервера Web, а также постоянный аудит и периодический пересмотр учетных записей пользователей и прав доступа на системном уровне. В результате этих действий автоматически снижается параметр ARO, установка обновлений безопасности уменьшает вероятность реализации описанных угроз.

Снижение степени уязвимости и вероятности реализации угрозы в части нарушения конфиденциальности достигается аналогично.

Риск нарушения доступности понижается путем установки обновлений безопасности, размещения межсетевого экрана перед сервером Web с учетом топологии сети и ограничения количества одновременных соединений со службой сервера Web с одного IP-адреса.

После идентификации перечисленных мер произведем расчет остаточных рисков и сведем их в таблицу. На ее основе можно сформировать таблицу снижения рисков. Из вышеизложенного можно сделать вывод, что риск снижен на величину от 66 до 83%, и это является приемлемым уровнем, в случае реализации комплексных и локально направленных мер на устранение вышеуказанных потенциальных злоумышленников [5].

Золотое правило безопасности web-приложений звучит так: не доверяйте пользовательскому вводу. Любые данные от клиента/пользователя должны проверяться на сервере для того, чтобы предотвратить прохождение скриптов или злонамеренных шестнадцатеричных кодов. Пользовательские данные часто передаются в качестве параметров для вызова другого кода на сервере и, будучи не проверены, могут серьезно нарушить безопасность системы.

Литература

1. Кришнамурти Б., Рексфорд Дж. Web-протоколы. Теория и практика. HTTP/1.1, взаимодействие протоколов, кэширование, измерение трафика. М.: Бином, 2002 г.- 592с.
2. Кузнецов С. Д. Базы данных. Модели и языки. М.: Бином-Пресс, 2008.- 720с.
3. Кузнецов С.Д. Проектирование и разработка корпоративных информационных систем. Центр Информационных Технологий, 1998.
4. Ларман К. Применение UML и шаблонов проектирования. М.: Издательство Вильяме, 2001.- 485с.
5. Менаске Д., Алмейда В. Производительность Web-служб Анализ, оценка и планирование. СПб: ООО "ДиаСофтЮП", 2003. 480с.

References

1. Krishnamurti B., Reksford Dzh. Web-protokoly. Teorija i praktika. HTTP/1.1, vzaimodejstvie protokolov, kjeshirovanie, izmerenie trafika. M.: Binom, 2002 g.- 592s.
2. Kuznecov S. D. Bazy dannyh. Modeli i jazyki. M.: Binom-Press, 2008.- 720s.
3. Kuznecov S.D. Proektirovanie i razrabotka korporativnyh informacionnyh sistem. Centr Informacionnyh Tehnologij, 1998.
4. Larman K. Primenenie UML i shablonov proektirovanija. M.: Izdatel'stvo Vil'jame, 2001.- 485s.
5. Menaske D., Almejda V. Proizvoditel'nost' Web-sluzhb Analiz, ocenka i planirovanie. SPb: OOO "DiaSoftJuP", 2003. 480s.